

Joseph Davies

Vier Kapitel aus:

Windows Server 2008 Networking und Netz- werkzugriffsschutz – Die technische Referenz

Microsoft[®]
Press

Dieses Buch ist die deutsche Übersetzung von: Joseph Davies and Tony Northrup with the Microsoft Networking Team:
Windows Server 2008 Networking and Network Access Protection (NAP)
Microsoft Press, Redmond, Washington 98052-6399
Copyright 2008 Microsoft Corporation

Das in diesem Buch enthaltene Programmmaterial ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor, Übersetzer und der Verlag übernehmen folglich keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programmmaterials oder Teilen davon entsteht.

Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen sowie E-Mail-Adressen und Logos sind frei erfunden, soweit nichts anderes angegeben ist. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen, E-Mail-Adressen und Logos ist rein zufällig.

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
10 09 08

ISBN 978-3-86645-919-9, Teilband von *Microsoft Windows Server 2008 – Die technische Referenz*

© Microsoft Press Deutschland
(ein Unternehmensbereich der Microsoft Deutschland GmbH)
Konrad-Zuse-Str. 1, D-85716 Unterschleißheim
Alle Rechte vorbehalten

Übersetzung: Detlef Johannis, Kempten, und Michael Ringel, Bonn
Korrektur: Claudia Mantel-Rehbach, München
Fachlektorat und Satz: Günter Jürgensmeier, München
Umschlaggestaltung: Hommer Design GmbH, Haar (www.HommerDesign.com)
Gesamtherstellung: Kösel, Krugzell (www.KoeselBuch.de)

Inhaltsverzeichnis

Teil III: Netzwerkzugriffsinfrastruktur	7
Kapitel 10: Drahtlose Netzwerke nach IEEE 802.11	9
Konzepte	9
Unterstützung der IEEE 802.11-Standards	10
Drahtlossicherheit	12
Komponenten von 802.11-Drahtlosnetzwerken	16
Planungs- und Entwurfsaspekte	16
Drahtlossicherheitstechnologien	17
Authentifizierungsmodi im drahtlosen Netzwerk	19
Intranetinfrastruktur	20
Anordnung der drahtlosen Zugriffspunkte	22
Authentifizierungsinfrastruktur	26
Drahtlosclients	27
PKI	38
802.1X-Erzwingung mit NAP	41
Bereitstellen von geschütztem Drahtloszugriff	42
Bereitstellen von Zertifikaten	42
Konfigurieren von Active Directory für Konten und Gruppen	44
Konfigurieren der NPS-Server	44
Bereitstellen drahtloser Zugriffspunkte	45
Konfigurieren von Drahtlosclients	48
Wartung	54
Verwalten der Benutzer- und Computerkonten	54
Verwalten der drahtlosen Zugriffspunkte	55
Aktualisieren von XML-Drahtlosprofilen	55
Problembehandlung	55
Problembehandlungstools von Windows für Drahtlosnetzwerke	56
Beheben von Problemen mit Drahtlosclients	63
Beheben von Problemen mit drahtlosen Zugriffspunkten	64
Beheben von Problemen mit der Authentifizierungsinfrastruktur	69
Zusammenfassung des Kapitels	75
Weitere Informationen	75
Kapitel 11: Verkabelte Netzwerke mit IEEE 802.1X-Authentifizierung	77
Konzepte	77
Komponenten von Kabelnetzwerken mit 802.1X-Authentifizierung	78
Planungs- und Entwurfsaspekte	79
Authentifizierungsmethoden im Kabelnetzwerk	79
Authentifizierungsmodi im Kabelnetzwerk	81
Authentifizierungsinfrastruktur	83
Kabelclients	84

PKI	89
802.1X-Erzwingung mit NAP	92
Bereitstellen des Kabelnetzwerkzugriffs mit 802.1X-Authentifizierung	93
Bereitstellen von Zertifikaten	93
Konfigurieren von Active Directory für Konten und Gruppen	95
Konfigurieren der NPS-Server	95
Konfigurieren von 802.1X-fähigen Switches	97
Konfigurieren verkabelter Clients	98
Wartung	102
Verwalten von Benutzer- und Computerkonten	102
Verwalten 802.1X-fähiger Switches	102
Aktualisieren von XML-Kabelprofilen	103
Problembehandlung	103
Problembehandlungstools von Windows für Kabelnetzwerke	103
Beheben von Problemen mit Kabelclients	108
Beheben von Problemen mit 802.1X-fähigen Switches	109
Beheben von Problemen mit der Authentifizierungsinfrastruktur	113
Zusammenfassung des Kapitels	119
Weitere Informationen	119
Kapitel 12: Remotezugriff-VPN-Verbindungen	121
Konzepte	121
Komponenten von Windows-Remotezugriff-VPNs	123
Planungs- und Entwurfsaspekte	125
VPN-Protokolle	125
Authentifizierungsmethoden	129
VPN-Server	131
Internetinfrastruktur	134
Intranetinfrastruktur	136
Gleichzeitiger Intranet- und Internetzugriff für VPN-Clients	139
Authentifizierungsinfrastruktur	141
VPN-Clients	142
PKI	146
VPN-Erzwingung mit NAP	149
Zusätzliche Sicherheitsaspekte	150
Starke Verschlüsselung der Verbindung	150
Paketfilterung für VPN-Verkehr auf dem VPN-Server	151
Firewallpaketfilterung für VPN-Verkehr	151
VPN-Server mit mehreren Aufgaben	159
Verhindern, dass Verkehr von VPN-Clients weitergeleitet wird	160
Gleichzeitiger Zugriff	161
Unbenutzte VPN-Protokolle	162
Bereitstellen von VPN-Remotezugriff	162
Bereitstellen von Zertifikaten	162
Konfigurieren der Internetinfrastruktur	166
Konfigurieren der Active Directory-Benutzerkonten und -Gruppen	167
Konfigurieren von RADIUS-Servern	167
Bereitstellen von VPN-Servern	169

Konfigurieren der Netzwerkinfrastruktur des Intranets	173
Bereitstellen von VPN-Clients	175
Wartung	180
Verwalten von Benutzerkonten	181
Verwalten von VPN-Servern	181
Aktualisieren von Verbindungs-Manager-Profilen	183
Problembehandlung	183
Tools für die Problembehandlung	183
Durchführen einer Problembehandlung für Remotezugriff-VPNs	187
Zusammenfassung des Kapitels	193
Weitere Informationen	193
Kapitel 13: Standort-zu-Standort-VPN-Verbindungen	195
Konzepte	195
Grundlagen von bei Bedarf herzustellenden Routingverbindungen	196
Komponenten von Windows-Standort-zu-Standort-VPNs	201
Planungs- und Entwurfsaspekte	202
VPN-Protokolle	202
Authentifizierungsmethoden	206
VPN-Router	207
Internetinfrastruktur	211
Standortnetzwerkinfrastruktur	213
Authentifizierungsinfrastruktur	215
PKI	217
Bereitstellen von Standort-zu-Standort-VPN-Verbindungen	220
Bereitstellen von Zertifikaten	220
Konfigurieren der Internetinfrastruktur	224
Konfigurieren der Active Directory-Benutzerkonten und -Gruppen	225
Konfigurieren von RADIUS-Servern	225
Bereitstellen von antwortenden Routern	227
Bereitstellen von anrufenden Routern	233
Konfigurieren der Standortnetzwerkinfrastruktur	238
Konfigurieren der Infrastruktur für die Standortverbindungen	240
Wartung	242
Verwalten von Benutzerkonten	242
Verwalten von VPN-Routern	243
Problembehandlung	244
Tools für die Problembehandlung	245
Durchführen einer Problembehandlung für Standort-zu-Standort-VPN-Verbindungen	245
Zusammenfassung des Kapitels	254
Weitere Informationen	254
Der Autor	257

T E I L I I I

Netzwerkzugriffsinfrastruktur

In diesem Teil:

Kapitel 10: Drahtlose Netzwerke nach IEEE 802.11	9
Kapitel 11: Verkabelte Netzwerke mit IEEE 802.1X-Authentifizierung	77
Kapitel 12: Remotezugriff-VPN-Verbindungen	121
Kapitel 13: Standort-zu-Standort-VPN-Verbindungen	195

Drahtlose Netzwerke nach IEEE 802.11

In diesem Kapitel:

Konzepte	9
Planungs- und Entwurfsaspekte	16
Bereitstellen von geschütztem Drahtloszugriff	42
Wartung	54
Problembehandlung	55
Zusammenfassung des Kapitels	75
Weitere Informationen	75

Dieses Kapitel beschreibt, wie man drahtlose lokale LAN-Netzwerke nach IEEE 802.11 plant, bereitstellt und wartet und wie man auftretende Probleme beheben kann (IEEE steht für das Institute of Electrical and Electronic Engineers, LAN bedeutet Local Area Network). Nach der Bereitstellung kann ein geschütztes Drahtlosnetzwerk noch auf die 802.1X-Erzwingungsmethoden für den Netzwerkzugriffsschutz (NAP) umgestellt werden, wie in Kapitel 17, »802.1X-Erzwingung«, beschrieben.

In diesem Kapitel wird vorausgesetzt, dass Sie über ein Grundwissen über die Bedeutung der Komponenten Active Directory, Public-Key-Infrastruktur (PKI), Gruppenrichtlinien und RADIUS (Remote Authentication Dial-In User Service) in einer Authentifizierungsinfrastruktur auf der Basis von Microsoft Windows für den Netzwerkzugriff verfügen. Weitere Informationen finden Sie in Kapitel 9, »Authentifizierungsinfrastruktur«.

Konzepte

Drahtlose lokale LAN-Netzwerke nach IEEE 802.11 haben folgende Vorteile:

- Drahtlose Netzwerke können ein herkömmlich verkabeltes Netzwerk erweitern oder ersetzen, wenn es zum Beispiel zu teuer, zu umständlich oder unmöglich ist, Kabel zu verlegen. Dazu können zum Beispiel folgende Anwendungsbereiche gehören:
 - Zur Verbindung von zwei Netzwerken, die sich in zwei verschiedenen Gebäuden befinden, die durch räumliche, rechtliche oder finanzielle Hindernisse voneinander getrennt sind, können Sie entweder eine Leitung von einer Telefongesellschaft mieten (dabei treten nicht nur die Installationskosten auf, sondern auch laufende Kosten), oder Sie erstellen eine Punkt-zu-Punkt-Funkverbindung mit der gebräuchlichen Technologie für drahtlose Netzwerke (auch dabei ergeben sich Installationskosten, aber keine nennenswerten laufenden Kosten). Die Kostenersparnis kann erheblich sein.
 - Mit der Technik für drahtlose Netzwerke lassen sich sehr schnell Netzwerke einrichten, die nur für relativ kurze Zeit gebraucht werden. Sie können zum Beispiel für eine Konferenz oder für eine Messe ein drahtloses Netzwerk einrichten, ohne die Kabel verlegen zu müssen, die für herkömmliche Ethernetnetzwerke erforderlich sind.

- Für manche Gebäude gelten vielleicht bestimmte Gesetze oder Vorschriften, die das Verlegen von Netzkabeln verbieten, beispielsweise in Gebäuden, die unter Denkmalschutz stehen. Dann ist ein drahtloses Netzwerk eine wichtige Alternative.
- Das Verzicht auf Kabel ist auch für Privatleute interessant, die in ihrer Wohnung oder in ihrem Haus mehrere Computer miteinander vernetzen möchten, ohne Löcher zu bohren und Kabel durch Wände und Decken zu verlegen.
- Höhere Produktivität für den mobilen Mitarbeiter, beispielsweise in folgenden Szenarios:
 - Der mobile Benutzer, der hauptsächlich mit einem Laptop oder Notebook arbeitet, kann seinen Standort wechseln und trotzdem mit dem Netzwerk verbunden bleiben. Dadurch kann der mobile Benutzer verschiedene Räume aufsuchen – Konferenzräume, Eingangshallen, Lobbys, Kantinen, Schulungsräume und so weiter – und weiterhin Zugriff auf Daten aus dem Netzwerk haben. Ohne drahtlosen Zugriff muss der Benutzer ein Kabel hinter sich her ziehen oder mit sich herumtragen und bleibt damit auf die engere Umgebung einer Netzanschlussdose beschränkt.
 - Drahtlose Netzwerke sind für Umgebungen gut geeignet, in denen Bewegung erforderlich ist. Im Einzelhandel ist es zum Beispiel von Vorteil, wenn ein Mitarbeiter Bestandsdaten direkt im Verkaufsraum mit einem drahtlos vernetzten Laptop oder Palmtop ins Warenwirtschaftssystem eingeben kann.
 - Selbst wenn keine Infrastruktur für Drahtlosnetzwerke vorhanden ist, können Laptops mit entsprechenden Drahtlosnetzwerkadaptern eigene Ad-hoc-Netzwerke bilden, um miteinander zu kommunizieren und Daten auszutauschen.
- Einfacher Zugriff auf das Internet an öffentlichen Plätzen über Hotspots. Außerhalb typischer Firmengelände ist über öffentlich zugängliche drahtlose Netzwerke ein Zugriff auf das Internet und sogar auf Firmennetzwerke möglich. Flughäfen, Restaurants, Bahnhöfe und andere öffentlich zugängliche Bereiche in den Städten können so ausgerüstet werden, dass sie diesen Dienst bieten. Wenn ein Vertreter sein Ziel erreicht und sich vielleicht im Büro eines Kunden mit dem Kunden trifft, könnte der Vertreter über ein lokales Drahtlosnetzwerk beschränkten Netzwerkzugriff erhalten. Das Netzwerk kann erkennen, dass der Benutzer ein Besucher ist, der nicht zur Firma gehört, und eine Verbindung herstellen, die zwar vom lokalen Firmennetzwerk isoliert ist, aber dem Besucher trotzdem den Internetzugang ermöglicht. Die Anbieter der drahtlosen Infrastruktur ermöglichen rund um die Welt drahtlose Verbindungen an öffentlich zugänglichen Orten. Viele Flughäfen, Konferenzzentren und Hotels bieten ihren Besuchern den drahtlosen Zugang zum Internet.

Unterstützung der IEEE 802.11-Standards

Die Betriebssysteme Windows Server 2008, Windows Vista, Windows XP und Windows Server 2003 bieten integrierte Unterstützung für drahtlose 802.11-LAN-Netzwerke. Ein installierter 802.11-Drahtlosnetzwerkadapter erscheint im Ordner *Netzwerkverbindungen* als eine *Drahtlosnetzwerkverbindung*. Auch wenn es eine integrierte Unterstützung für 802.11-Drahtlosnetzwerke gibt, hängen die Komponenten von Windows für Drahtlosnetzwerke von folgenden Aspekten ab:

- **Die Leistungsfähigkeit des Drahtlosnetzwerkadapters** Der installierte Drahtlosnetzwerkadapter muss die Standards für die drahtlosen Netzwerke oder Drahtlossicherheitsstandards unterstützen, die Sie brauchen. Windows Vista bietet zum Beispiel Konfigurationsoptionen für den Sicherheitsstandard Wi-Fi Protected Access (WPA). Unterstützt der Drahtlosnetzwerkadapter jedoch WPA nicht, können Sie WPA weder aktivieren noch die WPA-Sicherheitsoptionen einstellen.

- **Die Leistungsfähigkeit des Drahtlosnetzwerkadapertreibers** Damit Sie Einstellungen für ein Drahtlosnetzwerk vornehmen können, muss der Treiber des Drahtlosnetzwerkadapters in der Lage sein, Windows über seine Fähigkeiten zu informieren. Überprüfen Sie, ob der Treiber Ihres Drahtlosnetzwerkadapters für die Fähigkeiten von Windows Vista oder Windows XP entwickelt wurde, und überprüfen Sie mit Microsoft Update oder auf der Website des Herstellers des Drahtlosnetzwerkadapters, ob es sich um die neueste Version handelt.

Tabelle 10.1 listet die IEEE-Standards für drahtlose Netzwerke auf, die von Windows und von Drahtlosnetzwerkadaptern unterstützt werden, und nennt die maximale Bitrate, die Frequenzbereiche und den typischen Verwendungszweck.

Tabelle 10.1 802.11-Standards

Standard	Maximale Bitrate	Frequenzbereiche	Verwendung
802.11	2 MBit/s	S-Band ISM (Industrial, Scientific, and Medical), 2,4 bis 2,5 GHz	Veraltet, nicht weit verbreitet
802.11b	11 MBit/s	S-Band ISM	Weit verbreitet
802.11a	54 MBit/s	C-Band ISM (5,725 bis 5,875 GHz)	Wegen der Kosten und beschränkten Reichweite nicht weit verbreitet
802.11g	54 MBit/s	S-Band ISM	Weit verbreitet. 802.11g-Geräte sind abwärtskompatibel zu 802.11b-Geräten.
802.11n (noch in der Entwicklung)	250 MBit/s	C-Band und S-Band ISM	Erste Geräte sind seit August 2007 verfügbar (vor Verabschiedung des Standards). 802.11n-Geräte können zu Geräten nach den Standards 802.11a, b und g abwärtskompatibel sein.



Hinweis Das S-Band ISM liegt in einem Frequenzbereich, in dem auch Mikrowellenherde, schnurlose Telephone, Babymonitore, drahtlose Videokameras und Bluetooth-Geräte arbeiten. Das C-Band ISM verwendet denselben Frequenzbereich, in dem auch neuere schnurlose Telefone und andere Geräte arbeiten. Daher kann es zu Störungen kommen, wenn mehrere Geräte innerhalb ihrer Reichweiten gleichzeitig dieselben Frequenzen benutzen.

802.11-Betriebsarten

Für drahtlose LAN-Netzwerke sind nach den IEEE 802.11-Standards zwei Betriebsarten möglich:

- **Infrastrukturmodus** Das drahtlose Netzwerk enthält mindestens einen drahtlosen Zugriffspunkt (Access Point, AP). Dabei handelt es sich um ein Gerät, das drahtlos vernetzte Computer miteinander und mit einem herkömmlich verkabelten Netzwerk wie dem Internet oder einem Intranet verbinden kann.
- **Ad-hoc-Modus** Das drahtlose Netzwerk enthält keine drahtlosen Zugriffspunkte. Computer, die mit Drahtlosnetzwerkadaptern ausgerüstet sind, stellen untereinander direkte Verbindungen her und kommunizieren direkt miteinander. Drahtlosnetzwerke im Ad-hoc-Modus werden in diesem Kapitel aber nicht näher besprochen.

Unabhängig von der Betriebsart wird ein drahtloses Netzwerk aber durch eine *SSID* (*Service Set Identifier*) identifiziert, auch als Name des Drahtlosnetzwerks bekannt. Sie können die SSID eines drahtlosen Zugriffspunkts für den Infrastrukturmodus oder den noch nicht konfigurierten drahtlosen Client für den Ad-hoc-Modus konfigurieren. Der drahtlose Zugriffspunkt und der drahtlose Client senden

regelmäßig ihre SSID aus, damit andere Geräte das drahtlose Netzwerk entdecken und eine Verbindung herstellen können.

Drahtlossicherheit

Die Technologie für drahtlose Netzwerke nach IEEE 802.11 bietet zwar die beschriebenen Vorteile, aber sie bringt auch Sicherheitsrisiken mit sich, die es in verkabelten Netzwerken nicht gibt. Im Gegensatz zum geschlossenen Kabelsystem eines Ethernetnetzwerks, das sich physisch sichern lässt, werden Datenpakete im drahtlosen Netzwerk per Funk versendet und erreichen daher auch Bereiche außerhalb Ihres Büros. Jeder Computer in Reichweite eines drahtlosen (Funk)-Netzwerks kann die ausgestrahlten Pakete empfangen und eigene Pakete ausstrahlen. Ohne entsprechende Schutzmaßnahmen können Angreifer Ihr drahtloses Netzwerk verwenden, um sich Zugang zu Ihren vertraulichen Daten zu verschaffen oder um Angriffe auf Ihre Computer oder via Internet auf andere Computer durchzuführen.

Zum Schutz Ihres Drahtlosnetzwerks müssen Sie Authentifizierungen durchführen und Daten verschlüsseln:

- Zur Authentifizierung ist es erforderlich, dass Computer entweder gültige Anmeldeinformationen übermitteln (beispielsweise einen Benutzernamen und ein Kennwort) oder dass sie beweisen können, dass sie mit einem bestimmten Authentifizierungsschlüssel konfiguriert wurden. Nur dann wird ihnen erlaubt, Pakete ins Drahtlosnetzwerk zu übermitteln. Die Authentifizierung erschwert es also unbefugten Benutzern, sich Zugang zu Ihrem Netzwerk zu verschaffen.
- Verschlüsselung bedeutet, dass die Inhalte aller drahtlos übermittelten Pakete verschlüsselt werden, sodass nur der vorgesehene Empfänger den Inhalt der Pakete interpretieren kann. Die Verschlüsselung erschwert es Angreifern, die per Funk übermittelten Pakete zu lesen und zu verstehen. Sie erschwert es Angreifern auch, als gültig eingestufte Pakete zu senden und auf Ihre privaten Ressourcen oder auf das Internet zuzugreifen.

Drahtlose IEEE 802.11-LAN-Netzwerke unterstützen folgende Sicherheitsstandards:

- IEEE 802.11
- IEEE 802.1X
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)

IEEE 802.11

Der erste IEEE 802.11-Standard sah die Authentifizierungsmethoden *Keine Authentifizierung (offen)* und *Gemeinsam verwendet* sowie die WEP-Verschlüsselung (Wired Equivalent Privacy) vor. Zur Verschlüsselung verwendet WEP Schlüssel, die entweder 40 oder 104 Bit lang sind. Wie sich aber herausgestellt hat, war der ursprüngliche IEEE 802.11-Sicherheitsstandard relativ schwach. Da auch die Verwaltung der WEP-Verschlüsselungsschlüssel nicht genau festgelegt wurde, war auch die öffentliche und nichtöffentliche Bereitstellung relativ umständlich. Wegen ihrer Anfälligkeit für Angriffe und der raschen Verbreitung besserer Sicherheitsstandards wie WPA und WPA2 wird von der Verwendung dieser alten Methoden dringend abgeraten.

IEEE 802.1X

IEEE 802.1X war ein Standard, den es bereits für Ethernetswitches gab. Er wurde auf drahtlose 802.11-LANs angepasst, um eine bessere Authentifizierung zu ermöglichen, als mit den ursprünglichen 802.11-Standard möglich war. Die IEEE 802.1X-Authentifizierung wurde für mittlere und

große drahtlose LANs mit einer Authentifizierungsinfrastruktur entwickelt, die aus RADIUS-Servern (Remote Authentication Dial-In User Service) und Kontendatenbanken bestand, wie sie zum Beispiel in den Active Directory-Domänendiensten vorhanden sind.

IEEE 802.1X verhindert, dass ein drahtloser Knoten einem drahtlosen Netzwerk beitreten kann, bis der Knoten erfolgreich authentifiziert und autorisiert wurde. Bei der Authentifizierung wird überprüft, ob Drahtlosclients über gültige Anmeldeinformationen verfügen. Benutzer ohne Anmeldeinformationen können dem drahtlosen Netzwerk nicht beitreten. Bei der Autorisierung wird überprüft, ob der Drahtlosclient eine Verbindung mit dem drahtlosen Zugriffspunkt herstellen darf. IEEE 802.1X verwendet für den Austausch von Anmeldeinformationen EAP (Extensible Authentication Protocol). Die Authentifizierung nach IEEE 802.1X kann mit verschiedenen EAP-Authentifizierungsmethoden erfolgen, beispielsweise mit Benutzerkonten und Kennwörtern oder mit digitalen Zertifikaten.

Zur Behebung der Schlüsselverwaltungsprobleme des ursprünglichen 802.11-Standards kann die 802.1X-Authentifizierung mit dynamisch erstellten WEP-Schlüsseln erfolgen, die zwischen dem Drahtlosclient und einem RADIUS-Server ausgehandelt werden. Der RADIUS-Server sendet den WEP-Schlüssel an den drahtlosen Zugriffspunkt, nachdem die Authentifizierung abgeschlossen ist. Die Kombination von WEP-Verschlüsselung und dynamischen Schlüsseln, die bei jeder 802.1X-Authentifizierung neu bestimmt werden, wird *dynamisches WEP* genannt.

WPA

802.1X behebt zwar die Probleme des ursprünglichen 802.11-Standards mit der schwachen Authentifizierung und der fehlenden Schlüsselverwaltung, bietet aber keine Lösung für die Schwächen der WEP-Verschlüsselungsalgorithmen. Während der Entwicklung des Standards IEEE 802.11i für die Sicherheit im drahtlosen LAN, der im Abschnitt »WAP2« dieses Kapitels beschrieben wird, fanden sich Hersteller von Geräten für drahtlose Netzwerke zu einer Organisation namens Wi-Fi Alliance zusammen und entwickelten einen Interimsstandard, der *Wi-Fi Protected Access* (WPA) genannt wird. WPA ersetzte WEP mit einer wesentlich besseren Verschlüsselungsmethode namens TKIP (Temporal Key Integrity Protocol). Außerdem erlaubt WPA optional die Verwendung von AES (Advanced Encryption Standard) zur Verschlüsselung.

WPA ist in zwei verschiedenen Varianten verfügbar:

- **WPA-Enterprise** Verwendet die 802.1X-Authentifizierung und wurde für mittlere bis große Infrastrukturmodusnetzwerke entwickelt.
- **WPA-Personal** Verwendet zur Authentifizierung einen vorinstallierten Schlüssel (Preshared Key, PSK) und wurde für Infrastrukturmodusnetzwerke in kleinen Firmen und für Heimnetzwerke entwickelt.

WPA2

Der IEEE 802.11i-Standard ersetzt formal WEP und die anderen Sicherheitsfunktionen des ursprünglichen IEEE 802.11-Standards. Wi-Fi Protected Access 2 (WPA2) ist eine Zertifizierung, die von der Wi-Fi Alliance vorgenommen werden kann und die Kompatibilität zum IEEE 802.11i-Standard beschreibt. Das Ziel der WPA2-Zertifizierung ist, zusätzliche Sicherheitsfunktionen des IEEE 802.11i-Standards zu unterstützen, die von Produkten, die nur WPA unterstützen, nicht geboten werden. WPA2 erfordert zum Beispiel die Unterstützung der TKIP- und AES-Verschlüsselung. WPA umfasst auch Methoden für den schnellen Wechsel des Zugriffspunkts (fast roaming), wie zum Beispiel das PMK-Caching (Pairwise Master Key) und eine Vorauthentifizierung (pre-authentication).

So funktioniert's: Schneller Wechsel des Zugriffspunkts mit WPA2

Wenn ein Drahtlosclient eine Authentifizierung nach 802.1X durchführt, werden zwischen dem Drahtlosclient und dem drahtlosen Zugriffspunkt eine Reihe von Nachrichten ausgetauscht, um die Anmeldeinformationen zu übermitteln (802.1X-Authentifizierung) und um die paarigen transienten Schlüssel zu bestimmen (der 4-Wege-Handshake). Die paarigen transienten Schlüssel werden zur Verschlüsselung und zur Sicherung der Datenintegrität der WPA2-geschützten, drahtlos übermittelten Datenrahmen verwendet. Dieser Nachrichtenaustausch bringt aber eine Verzögerung des Verbindungsvorgangs mit sich. Wechselt ein Drahtlosclient von einem drahtlosen Zugriffspunkt zum nächsten, kann die für die 802.1X-Authentifizierung erforderliche Zeit zu spürbaren Unterbrechungen des Datenflusses führen, insbesondere bei zeitkritischen Übertragungen wie Gesprächen oder Videokonferenzen. Um die Verzögerungen zu minimieren, die beim Wechsel zu einem anderen drahtlosen Zugriffspunkt auftreten, können WPA2-fähige Geräte bei Bedarf eine PMK-Zwischenspeicherung und eine Vorauthentifizierung durchführen.

PMK-Caching

Wenn ein Drahtlosclient von einem drahtlosen Zugriffspunkt zum nächsten wechselt, muss er bei jedem neuen drahtlosen Zugriffspunkt eine vollständige 802.1X-Authentifizierung durchführen. WPA2 erlaubt dem Drahtlosclient und dem drahtlosen Zugriffspunkt, die Ergebnisse einer vollständigen 802.1X-Authentifizierung zwischenspeichern. Kehrt ein Client also zu einem drahtlosen Zugriffspunkt zurück, bei dem er sich zuvor bereits authentifiziert hat, braucht der Drahtlosclient nur das 4-Wege-Handshake durchzuführen und neue paarige transiente Schlüssel zu bestimmen. Im Association Request-Datenpaket gibt der Drahtlosclient eine PMK-Kennung an, die bei der ursprünglichen Authentifizierung festgelegt wurde und vom Drahtlosclient sowie vom drahtlosen Zugriffspunkt als PMK-Cacheeintrag zwischengespeichert wurde. PMK-Cacheeinträge werden nur für eine gewisse Zeit gespeichert, wobei sich die Speicherdauer auf dem Drahtlosclient und dem drahtlosen Zugriffspunkt einstellen lässt.

Um Wechsel der Zugangspunkte in Netzwerkinfrastrukturen zu erleichtern, in denen ein Switch als 802.1X-Authentifizierer verwendet wird, berechnen Windows Server 2008 und Windows Vista die PMK-Kennung so, dass der PMK, der bei der 802.1X-Authentifizierung beim Switch bestimmt wurde, beim Wechsel auf andere drahtlose Zugriffspunkte, die mit demselben Switch verbunden sind, weiter verwendet werden kann. Diese Technik wird *Opportunistisches PMK-Caching* genannt.

Vorauthentifizierung

Bei der Vorauthentifizierung kann ein drahtloser WPA2-Client bei Bedarf eine 802.1X-Authentifizierungen mit anderen drahtlosen Zugriffspunkten innerhalb seiner Reichweite durchführen, wenn er eine Verbindung mit dem aktuellen drahtlosen Zugriffspunkt herstellt. Der Drahtlosclient sendet den für die Vorauthentifizierung erforderlichen Datenverkehr über die vorhandene drahtlose Netzwerkverbindung an die weiteren drahtlosen Zugriffspunkte. Nach der Vorauthentifizierung bei einem drahtlosen Zugriffspunkt und der Speicherung der PMK und der dazugehörigen Daten im PMK-Zwischenspeicher braucht ein drahtloser Client bei einer Verbindung mit einem drahtlosen Zugriffspunkt, mit dem er eine Vorauthentifizierung durchgeführt hat, nur das 4-Wege-Handshake durchzuführen.

WPA2-Clients, die die Vorauthentifizierung unterstützen, können nur mit solchen drahtlosen Zugriffspunkten eine Vorauthentifizierung durchführen, die ihre Fähigkeit zur Vorauthentifizierung in den Beacon- und Probe Response-Datenpaketen bekannt geben.

WPA2 ist in zwei verschiedenen Varianten verfügbar:

- **WPA2-Enterprise** Verwendet die 802.1X-Authentifizierung und wurde für mittlere bis große Infrastrukturmodusnetzwerke entwickelt.
- **WPA2-Personal** Verwendet zur Authentifizierung einen vorinstallierten Schlüssel (Preshared Key, PSK) und wurde für Infrastrukturmodusnetzwerke in kleinen Firmen und für Heimnetzwerke entwickelt.

Tabelle 10.2 fasst die Sicherheitsstandards für drahtlose 802.11-LANs zusammen.

Tabelle 10.2 802.11-LAN-Drahtlossicherheitsstandards

Sicherheitsstandard	Authentifizierungsmethoden	Verschlüsselungsmethoden	Größe des Schlüssels	Kommentar
IEEE 802.11	<u>Offen und gemeinsame Schlüssel</u>	WEP	40 und 104 Bit	Schwache Authentifizierung und Verschlüsselung. Von der Verwendung wird dringend abgeraten.
IEEE 802.1X	EAP-Authentifizierungsmethoden	–	–	Sichere EAP-Methoden bieten eine sichere Authentifizierung.
WPA-Enterprise	802.1X	TKIP und AES (optional)	128 Bit	Sichere Authentifizierung (mit sicherer EAP-Methode) sowie sichere (TKIP) und sehr sichere (AES) Verschlüsselung.
WPA-Personal	PSK (Preshared Key)	TKIP und AES (optional)	128 Bit	Sichere Authentifizierung (mit sicherem PSK) sowie sichere (TKIP) und sehr sichere (AES) Verschlüsselung.
WPA2-Enterprise	802.1X	TKIP und AES	128 Bit	Sichere Authentifizierung (mit sicherer EAP-Methode) sowie sichere (TKIP) und sehr sichere (AES) Verschlüsselung.
WPA2-Personal	PSK	TKIP und AES	128 Bit	Sichere Authentifizierung (mit sicherem PSK) sowie sichere (TKIP) und sehr sichere (AES) Verschlüsselung.

Windows Server 2008 und Windows Vista unterstützen die folgenden Sicherheitsstandards für drahtlose 802.11-LANs (außerdem müssen der Drahtlosnetzwerkadapter und sein Treiber den Standard unterstützen):

- 802.11 mit WEP
- 802.1X
- WPA-Enterprise
- WPA-Personal
- WPA2-Enterprise
- WPA2-Personal



Hinweis Sofern nicht anders beschrieben, ist im folgenden Text mit WPA2 der Standard *WPA2-Enterprise* gemeint und mit WPA *WPA-Enterprise*.

Komponenten von 802.11-Drahtlosnetzwerken

Abbildung 10.1 zeigt die Komponenten von 802.11-Drahtlosnetzwerken auf der Basis von Windows:.

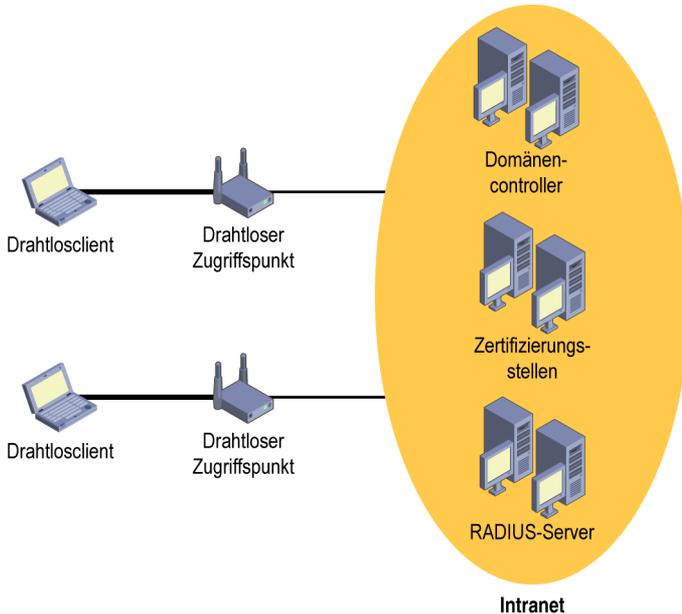


Abbildung 10.1 Komponenten eines nach 802.11 geschützten drahtlosen Netzwerks auf der Basis von Windows

Bei den Komponenten handelt es sich um:

- **Drahtlosclients** Leiten drahtlose Verbindungen mit drahtlosen Zugriffspunkten ein und kommunizieren nach der Herstellung der Verbindung mit Intranetressourcen und anderen Drahtlosclients
- **Drahtlose Zugriffspunkte** Warten auf Verbindungsversuche, führen die Authentifizierung durch, sorgen für die Einhaltung der Verbindungsanforderungen und leiten Datenpakete zwischen Drahtlosclients und Intranetressourcen weiter
- **RADIUS-Server** Führen die zentrale Authentifizierung, Autorisierung und Kontoführung für Verbindungsversuche von drahtlosen Zugriffspunkten und andere Arten von Zugriffsservern durch
- **Active Directory-Domänencontroller** Überprüfen Anmeldeinformationen von Benutzern für die Authentifizierung und senden Kontendaten für die Überprüfung der Autorisierung an die RADIUS-Server
- **Zertifizierungsstellen** Komponenten der Public-Key-Infrastruktur (PKI), die für Drahtlosclients Computer- und Benutzerzertifikate ausstellen, sowie Computerzertifikate für RADIUS-Server

Planungs- und Entwurfsaspekte

Bei der Planung und dem Entwurf eines geschützten 802.11-Drahtlosnetzwerks sollten Sie folgende Aspekte berücksichtigen:

- Drahtlossicherheitstechnologien
- Authentifizierungsmodi im drahtlosen Netzwerk
- Intranetinfrastruktur

- Anordnung der drahtlosen Zugriffspunkte
- Authentifizierungsinfrastruktur
- Drahtlosclients
- PKI
- 802.1X-Erzwingung mit NAP

Drahtlossicherheitstechnologien

Drahtlossicherheitstechnologien sind eine Kombination von Drahtlossicherheitsstandard (WPA2 oder WPA) und EAP-Authentifizierungsmethode. Zur Authentifizierung eines Computers oder des Benutzers, der versucht, eine geschützte drahtlose Verbindung herzustellen, unterstützen Windows Server 2008 und Windows Vista folgende EAP-Authentifizierungsmethoden:

- EAP-TLS
- PEAP-TLS (Protected EAP-TLS)
- PEAP-MS-CHAP v2 (PEAP-Microsoft Challenge Handshake Authentication Protocol Version 2)

EAP-TLS und PEAP-TLS werden zusammen mit einer PKI und Computerzertifikaten, Benutzerzertifikaten oder Smartcards verwendet. Bei EAP-TLS sendet der Drahtlosclient sein Computer-, Benutzer- oder Smartcardzertifikat zur Authentifizierung und der RADIUS-Server sendet sein Computerzertifikat zur Authentifizierung. Standardmäßig überprüft der Drahtlosclient das Zertifikat des RADIUS-Servers. Bei PEAP-TLS beginnen der Drahtlosclient und der RADIUS-Server eine verschlüsselte TLS-Sitzung und dann tauschen der Drahtlosclient und der RADIUS-Server Zertifikate aus. PEAP-TLS ist die sicherste Authentifizierungsmethode, weil der Zertifikataustausch zwischen dem Drahtlosclient und dem RADIUS-Server verschlüsselt wird.

Falls keine Computerzertifikate, Benutzerzertifikate oder Smartcards einsetzbar sind, verwenden Sie PEAP-MS-CHAP v2. PEAP-MS-CHAP v2 ist eine Authentifizierungsmethode auf Kennwortbasis, bei der der Austausch der Authentifizierungsnachrichten in einer verschlüsselten TLS-Sitzung erfolgt. Dadurch ist es für einen Angreifer wesentlich schwieriger, das Kennwort des aufgezeichneten Authentifizierungsdatenverkehrs mit einem Offline-Wörterbuchangriff zu bestimmen.

Trotz der verschlüsselten TLS-Sitzung sind EAP-TLS und PEAP-TLS beide wesentlich sicherer als PEAP-MS-CHAP v2, weil sie nicht auf Kennwörtern basieren.

Auswahl der Drahtlossicherheitstechnologien

Microsoft empfiehlt, eine der folgenden Kombinationen der Drahtlossicherheitstechnologien zu verwenden (sie werden hier in der Reihenfolge von der sichersten zur unsichersten Methode aufgelistet):

- WPA2 mit AES-Verschlüsselung, PEAP-TLS- oder EAP-TLS-Authentifizierung, Benutzer- und Computerzertifikaten
- WPA2 mit AES-Verschlüsselung, PEAP-MS-CHAP v2-Authentifizierung und der Anforderung an die Benutzer, sichere Benutzerkennwörter zu verwenden
- WPA mit EAP-TLS- oder PEAP-TLS-Authentifizierung und Benutzer- und Computerzertifikate
- WPA mit PEAP-MS-CHAP v2-Authentifizierung und der Anforderung an die Benutzer, sichere Benutzerkennwörter zu verwenden

Voraussetzungen für Drahtlossicherheitstechnologien

Folgende Voraussetzungen gelten für Drahtlossicherheitstechnologien:

- Um ein drahtloses Netzwerk zu schützen, müssen Sie entweder WPA oder WPA2 verwenden. Falls Sie WEP verwenden, ist Ihr Drahtlosnetzwerk nicht sicher. Das gilt auch für dynamisches WEP. Verwenden Sie also dynamisches WEP nicht, außer vielleicht in der Übergangsphase bei der Umstellung des Netzwerks auf WPA oder WPA2.
- EAP-TLS oder PEAP-TLS erfordert die Installation eines Computerzertifikats auf dem RADIUS-Server und eines Computerzertifikats, eines Benutzerzertifikats oder die Verwendung einer Smartcard auf allen drahtlosen Clientcomputern. Damit sich die Computerzertifikate der RADIUS-Server überprüfen lassen, muss auf allen Drahtlosclientcomputern das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle der Computerzertifikate der RADIUS-Server installiert werden. Damit sich die Computer- oder Benutzerzertifikate der Drahtlosclientcomputer überprüfen lassen, muss auf allen RADIUS-Servern das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle der Drahtlosclientzertifikate installiert werden.
- PEAP-MS-CHAP v2 erfordert auf jedem RADIUS-Server die Installation eines Computerzertifikats. Außerdem ist es erforderlich, auf den drahtlosen Clientcomputern die Stammzertifizierungsstellenzertifikate der Computerzertifikate der RADIUS-Server zu installieren.
- Für WPA2 muss vielleicht ein Teil der Netzwerkausrüstung ersetzt werden. Ältere Geräte für drahtlose Netzwerke, die nur 802.11 unterstützen, können gewöhnlich auf WPA, nicht aber auf WPA2 nachgerüstet werden.
- Wenn Sie planen, irgendwann die 802.1X-Erzwingung von NAP einzuführen, sollten Sie eine Authentifizierungsmethode auf der Basis von PEAP verwenden, wie PEAP-MS-CHAP v2 oder PEAP-TLS.

Empfehlungen für Drahtlossicherheitstechnologien

Für die Drahtlossicherheitstechnologien gelten folgende Empfehlungen:

- Stellen Sie die drahtlosen Zugriffspunkte nicht auf SSID-Unterdrückung ein. Die SSID (der Name des Drahtlosnetzwerks) ist standardmäßig in den Ankündigungsdatenpaketen enthalten, die von den drahtlosen Zugriffspunkten ausgestrahlt werden. Wenn Sie ihre drahtlosen Zugriffspunkte so einstellen, dass die Bekanntgabe der SSID in den Ankündigungsdatenpaketen unterdrückt wird, kann der Gelegenheitsanwender Ihr Netzwerk wahrscheinlich nicht mehr erkennen. Ein Angreifer, der sich mit der Technik auskennt, wird dadurch aber nicht davon abgehalten, andere Datenpakete aufzuzeichnen, die von Ihrem drahtlosen Zugriffspunkt zur Verwaltung ausgestrahlt werden, und Ihre SSID zu bestimmen. Drahtlosnetzwerke mit aktivierter SSID-Unterdrückung werden als *versteckte* oder *Non-broadcast*-Netzwerke bezeichnet.

Der Versuch, Drahtlosnetzwerke zu verstecken, bietet nicht nur einen äußerst schwachen Schutz, sondern stellt auch für autorisierte Drahtlosclients ein Problem dar, die automatisch eine Verbindung mit dem versteckten Drahtlosnetzwerk herstellen sollen. Da der Name des Drahtlosnetzwerks nicht ausgestrahlt wird, muss der Drahtlosclient Probe-Request-Nachrichten aussenden, in denen der Name des Drahtlosnetzwerks enthalten ist, um einen drahtlosen Zugriffspunkt für das Netzwerk zu finden. Diese Nachrichten geben also den Namen des Drahtlosnetzwerks bekannt und schwächen auf diese Weise den angestrebten Schutz.

- Verwenden Sie keine MAC-Adressenfilter (Media Access Control). MAC-Adressenfilterung bedeutet, dass Sie Ihre drahtlosen Zugriffspunkte mit den MAC-Adressen der zugelassenen Drahtlosclients konfigurieren können. Allerdings ist mit der MAC-Adressenfilterung auch der Verwal-

tungsaufwand verbunden, der erforderlich ist, um die Liste der zulässigen MAC-Adressen auf dem aktuellen Stand zu halten. Angreifer werden dadurch nicht davon abgehalten, zulässige MAC-Adressen auszuspiönieren.

- Falls Sie PEAP-MS-CHAP v2 verwenden müssen, schreiben Sie unbedingt sichere Kennwörter für Ihr Netzwerk vor. Sichere Kennwörter sind lang (länger als 8 Zeichen) und enthalten eine Kombination von Groß- und Kleinbuchstaben, Ziffern und Satzzeichen. In einer Active Directory-Umgebung können Sie mit den Gruppenrichtlinieneinstellungen unter *Computerkonfiguration\ Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinien* dafür sorgen, dass die Benutzer sichere Kennwörter verwenden müssen.

Authentifizierungsmodi im drahtlosen Netzwerk

Drahtlosclients auf Windows-Basis können in folgenden Modi Authentifizierungen durchführen:

- **Nur Computer** Windows führt mit den Anmeldeinformationen des Computers eine 802.1X-Authentifizierung durch, bevor der Anmeldebildschirm von Windows angezeigt wird. Auf diese Weise erhält der Drahtlosclient Zugriff auf Netzwerkressourcen, beispielsweise auf Active Directory-Domänencontroller, bevor sich ein Benutzer anmeldet. Windows versucht nach der Anmeldung des Benutzers keine Authentifizierung mit den Anmeldeinformationen des Benutzers.
- **Nur Benutzer** Standardmäßig führt Windows eine 802.1X-Authentifizierung mit den Anmeldeinformationen des Benutzers durch, nachdem seine Anmeldung abgeschlossen ist. Windows versucht keine Authentifizierung mit den Anmeldeinformationen des Computers, bevor sich der Benutzer anmeldet.
- **Computer oder Benutzer** Windows führt mit den Anmeldeinformationen des Computers eine 802.1X-Authentifizierung durch, bevor es den Windows-Anmeldebildschirm anzeigt. Windows führt eine weitere 802.1X-Authentifizierung mit den Anmeldeinformationen des Benutzers durch, nachdem sich der Benutzer angemeldet hat oder wenn der Drahtlosclient zu einem anderen drahtlosen Zugriffspunkt wechselt.

Mit dem Standardverhalten der Nur-Benutzer-Authentifizierung können sich folgende Probleme ergeben:

- Ein Benutzer kann auf dem Computer keine Domänenanmeldung durchführen, weil die lokal zwischengespeicherten Anmeldeinformationen für das Konto des Benutzers nicht verfügbar sind, keine Verbindung mit dem Domänencontroller besteht und sich die neuen Anmeldeinformationen nicht überprüfen lassen.
- Anmeldevorgänge bei Domänen sind nicht erfolgreich, weil während der Anmeldung des Benutzers keine Verbindung mit den Domänencontrollern der Active Directory-Domäne besteht. Anmeldeskripts sowie Aktualisierungen der Gruppenrichtlinien und Benutzerprofildaten schlagen ebenfalls fehl, was zu einer Reihe von Einträgen im Windows-Ereignisprotokoll führt.

Einige Netzwerkinfrastrukturen verwenden verschiedene virtuelle LANs (VLANs), um Drahtlosclients, die sich mit Computeranmeldeinformationen authentifiziert haben, von Drahtlosclients zu trennen, die sich mit Benutzeranmeldeinformationen authentifiziert haben. Wenn die Benutzerauthentifizierung beim Drahtlosnetzwerk und die Umschaltung auf das benutzerauthentifizierte VLAN nach der Anmeldung des Benutzers erfolgt, hat ein drahtloser Windows-Client während der Benutzeranmeldung keinen Zugriff auf Ressourcen aus dem benutzerauthentifizierten VLAN, beispielsweise auf Active Directory-Domänencontroller. Das kann zu erfolglosen Erstanmeldungen und zu erfolglosen Vorgängen bei Domänenanmeldungen führen, was beispielsweise die Ausführung von Anmeldeskripten und die Aktualisierungen von Gruppenrichtlinien und Benutzerprofildaten betrifft.

Um die Probleme mit der Verfügbarkeit der Netzwerkverbindungen bei Benutzeranmeldungen im Nur-Benutzer-Authentifizierungsmodus und im Benutzer-oder-Computer-Authentifizierungsmodus bei der Verwendung separater VLANs zu lösen, unterstützen Drahtlosclients unter Windows Server 2008 und Windows Vista das einmalige Anmelden (Single Sign-On). Beim einmaligen Anmelden können Sie festlegen, dass die Drahtlosnetzwerkauthentifizierung mit Benutzeranmeldeinformationen vor der Anmeldung des Benutzers erfolgt. Zur Aktivierung und Einstellung der einmaligen Anmeldung können Sie die Gruppenrichtlinienerweiterung *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* verwenden, um eine Windows Vista-Richtlinie zu konfigurieren, oder Sie geben den Befehl `netsh wlan` mit den entsprechenden Parametern ein. Weitere Informationen finden Sie im Verlauf dieses Kapitels im Abschnitt »Konfigurieren von Drahtlosclients«.

Voraussetzungen für Authentifizierungsmodi im drahtlosen Netzwerk

Nur Drahtlosclients, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird, unterstützen die einmalige Anmeldung (Single Sign-On).

Empfehlungen für die Authentifizierung im drahtlosen Netzwerk

Für die Authentifizierung im drahtlosen Netzwerk wird Folgendes empfohlen:

- Verwenden Sie den Modus Benutzer-oder-Computer-Authentifizierung. Die Benutzerauthentifizierung erfolgt nach der Benutzeranmeldung. Das ist der Standardauthentifizierungsmodus.
- Wenn Sie den Authentifizierungsmodus Nur-Benutzer verwenden, konfigurieren Sie Ihr Drahtlosprofil so, dass es die einmalige Anmeldung unterstützt und die Drahtlosauthentifizierung mit den Benutzeranmeldeinformationen vor der Benutzeranmeldung durchführt, um Probleme bei der ersten Anmeldung und der Domänenanmeldung zu vermeiden.
- Wenn Sie für computerauthentifizierte und benutzerauthentifizierte Drahtlosclients verschiedene VLANs verwenden und den Authentifizierungsmodus Computer oder Benutzer einsetzen, konfigurieren Sie Ihre Drahtlosprofile so, dass sie die einmalige Anmeldung unterstützen und die Drahtlosauthentifizierung mit den Benutzeranmeldeinformationen vor der Benutzeranmeldung durchführen, um Probleme bei der ersten Anmeldung und der Domänenanmeldung zu vermeiden.

Intranetinfrastruktur

Drahtlosclients brauchen im Prinzip dieselben TCP/IP-Einstellungen (Transmission Control Protocol/Internet Protocol) wie verkabelte Clients, wobei Sie Drahtlosclients allerdings wegen ihrer Mobilität etwas anders einstellen sollten. Bringen Sie Ihre Drahtlosclients daher in separaten Subnetzen unter, damit es im selben Subnetz keine Mischung von verkabelten Clients und Drahtlosclients gibt.

Subnetzdesign für Drahtlosclients

Für Drahtlosclients separate Subnetze einzurichten, hat folgende Vorteile:

- Verkabelte Netzwerkkomponenten brauchen nicht mit den Drahtlosclients um den Vorrat an IPv4-Adressen zu konkurrieren.
- Drahtlosclients sind anhand ihrer IPv4- und IPv6-Adresspräfixe leichter zu identifizieren. Das erleichtert die Verwaltung und die Problembehandlung.
- Separate IPv4-Subnetze geben Ihnen eine bessere Kontrolle über DHCP-Leasezeiten.
- Sie können jedes physische Subnetz (verkabelt oder drahtlos) in Active Directory mit bestimmten Standorten verknüpfen. Auf diese Weise können Sie für die Subnetze Gruppenrichtlinieneinstellungen vornehmen.

- Wenn sich Ihre drahtlosen Zugriffspunkte alle im selben Subnetz befinden, können Ihre Drahtlosclients reibungslos von einem Zugriffspunkt zum nächsten wechseln.

Wenn ein Drahtlosclient zu einem anderen drahtlosen Zugriffspunkt desselben Drahtlosnetzwerks wechselt, der sich im selben Subnetz befindet, nennt man diesen Vorgang auch *Network-layer roaming*. Bei diesem Zugriffspunktwechsel im selben Subnetz erneuert der Drahtlosclient seine aktuelle DHCP-Konfiguration. Wechselt ein Drahtlosclient zu einem anderen drahtlosen Zugriffspunkt, der sich in einem anderen Subnetz befindet, erhält der Drahtlosclient eine neue DHCP-Konfiguration, die im neuen Subnetz gilt. Allerdings können manche Anwendungen versagen, wenn sich die IPv4- oder IPv6-Adressen ändern, wie zum Beispiel manche E-Mail-Anwendungen.

Berücksichtigen Sie bei der Bestimmung eines IPv4-Subnetzpräfixes für Ihre Drahtlosclients, dass Sie für folgende Geräte jeweils mindestens eine IPv4-Adresse brauchen:

- Jede LAN-Schnittstelle eines drahtlosen Zugriffspunkts, der mit dem Drahtlossubnetz verbunden ist
- Jede Routerschnittstelle, die mit dem Drahtlossubnetz verbunden ist
- Jeder andere TCP/IP-fähige Host oder jedes TCP/IP-fähige Gerät, das mit dem Drahtlossubnetz verbunden ist
- Jeder Drahtlosclient, der mit dem Drahtlosnetzwerk verbunden ist. Wenn Sie zu wenige Adressen einplanen, erhalten alle Windows-Drahtlosclients, die eine Verbindung herzustellen versuchen, nachdem die verfügbaren IPv4-Adressen alle von DHCP an verbundene Drahtlosclients vergeben wurden, automatisch eine APIPA-Adresse ohne Standardgateway (APIPA bedeutet Automatic Private IP Addressing). Diese Konfiguration erlaubt keine Verbindung ins Intranet. Drahtlosclients mit APIPA-Konfigurationen versuchen in regelmäßigen Abständen, eine DHCP-Konfiguration zu erhalten

Da jedes IPv6-Subnetz eine sehr große Zahl von Hosts enthalten kann, brauchen Sie gewöhnlich nicht die Zahl der IPv6-Adressen zu berechnen, die für ein IPv6-Subnetzpräfix verfügbar sind.

DHCP-Planung für Drahtlosclients

Wenn Drahtlosclients und verkabelte Clients zu verschiedenen Subnetzen gehören, müssen Sie separate DHCP-Bereiche einrichten. Da Drahtlosclients leicht von einem Drahtlossubnetz zum nächsten wechseln können, sollten Sie die DHCP-Bereiche so konfigurieren, dass eine Lease in Drahtlossubnetzen nicht so lange gilt wie in verkabelten Subnetzen.

Für einen DHCP-Bereich eines verkabelten Netzwerks beträgt die Leasedauer gewöhnlich einige Tage. Da Drahtlosclients ihre Adressen nicht an den DHCP-Server zurückgeben, wenn sie in ein anderes Subnetz wechseln, sollten Sie die Leasedauer für DHCP-Bereiche, die für Drahtlossubnetze vorgesehen sind, auf einige Stunden beschränken. Wenn Sie die Leasedauer für Drahtlossubnetze verkürzen, kann sich der DHCP-Server die nicht länger von Drahtlosclients verwendeten, aber nicht zurückgegebenen IPv4-Adressen bereits im Lauf des Tages zurückholen und neu vergeben. Solche Adressen bleiben also nicht für Tage blockiert. Vergessen Sie bei der Bestimmung der optimalen Leasedauer für die Drahtlosclients in Ihrer Umgebung aber nicht, dass kürzere Leasezeiten eine höhere Belastung für den DHCP-Server bedeuten.

Weitere Informationen über die Konfiguration von DHCP-Bereichen finden Sie in Kapitel 3, »Dynamic Host Configuration Protocol«.

Anordnung der drahtlosen Zugriffspunkte

Eine sehr wichtige und zeitaufwendige Aufgabe beim Aufbau eines drahtlosen LANs ist die Bestimmung der Orte, an denen drahtlosen Zugriffspunkte aufgestellt werden müssen. Die drahtlosen Zugriffspunkte müssen so angeordnet werden, dass sie eine Etage, ein Gebäude oder das ganze Firmengelände nahtlos abdecken. Wird diese nahtlose Abdeckung erreicht, können sich Drahtlosbenutzer von einem Ort zum andern bewegen, ohne dabei eine deutliche Unterbrechung in der Netzwerkverbindung zu bemerken. Alles, was ihnen bei der Bewegung auffallen sollte, ist ein Wechsel der IPv4- und IPv6-Adressen, wenn sie von einem Subnetz ins nächste wechseln. Bei der Bestimmung der Aufstellungsorte der drahtlosen Zugriffspunkte ist es nicht damit getan, die Geräte zu installieren und einzuschalten. Drahtlose LANs sind Funknetze. Sie basieren auf Radiowellen. Radiowellen können gedämpft, reflektiert, abgeschirmt und gestört werden, beispielsweise durch Interferenzen.

Bei der Planung der Aufstellungsorte der drahtlosen Zugriffspunkte in einer Organisation sollten Sie folgende Aspekte berücksichtigen, die in den nächsten Abschnitten näher beschrieben werden:

- Anforderungen an die drahtlosen Zugriffspunkte
- Kanaltrennung
- Störungen in der Signalausbreitung
- Störungsquellen
- Anzahl der drahtlosen Zugriffspunkte



Hinweis Weitere Angaben und Empfehlungen für die Anordnung von drahtlosen Zugriffspunkten finden Sie in der Dokumentation der drahtlosen Zugriffspunkte und der verwendeten Antennen.

Anforderungen an die drahtlosen Zugriffspunkte

Stellen Sie eine Liste mit den Anforderungen auf, die an die drahtlosen Zugriffspunkte gestellt werden. Dazu gehören zum Beispiel folgende Punkte:

- WPA
- WPA2
- 802.1X und RADIUS
- 802.11a, b, g und n

Je nach Budget und der zu übertragenden Datenmenge brauchen Sie vielleicht drahtlose Zugriffspunkte, die 802.11b, 802.11a, 802.11g, 802.11n oder eine Kombination der Technologien bieten.

- **Gebäude- und Feuerschutzvorschriften** Für die Verwendung des Raums über abgehängten Decken gibt es Vorschriften. Wenn Sie in diesem Bereich drahtlose Zugriffspunkte aufstellen und verkabeln, müssen Sie darauf achten, dass die verwendeten Zugriffspunkte den Brandschutz- und Gebäudevorschriften entsprechen. Bei der Unterbringung von drahtlosen Zugriffspunkten über der abgehängten Decke müssen Sie sich zudem überlegen, wie Sie die Geräte am besten mit Strom versorgen. Erkundigen Sie sich beim Hersteller der Geräte, wie Sie die drahtlosen Zugriffspunkte am besten mit Strom versorgen können. Manche drahtlose Zugriffspunkte lassen sich über das Ethernetkabel mit Strom versorgen, mit dem sie ans verkabelte Netzwerk angeschlossen sind.
- **Vorkonfiguration und Remotekonfiguration** Die Vorkonfiguration der drahtlosen Zugriffspunkte vor der Aufstellung am Einsatzort kann den Aufbau des Netzwerks beschleunigen und die Arbeitskosten verringern, weil die rein mechanische Installation von weniger erfahrenen Mitarbeitern erledigt werden kann. Je nach Bauart können Sie drahtlose Zugriffspunkte über einen Konsolenan-

schluss (einen seriellen Anschluss), über Telnet oder über einen Webserver vorkonfigurieren, der im drahtlosen Zugriffspunkt integriert ist. Unabhängig davon, ob Sie eine Vorkonfigurierung durchführen oder nicht, sollten Sie darauf achten, dass eine Remoteverwaltung der drahtlosen Zugriffspunkte möglich ist, beispielsweise durch ein spezielles Konfigurationsprogramm des Herstellers, über einen integrierten Webserver oder mit Skripts.

- **Antennenarten** Überprüfen Sie, ob die drahtlosen Zugriffspunkte mit unterschiedlichen Antennenarten kombiniert werden können. In einem Gebäude mit mehreren Etagen könnte zum Beispiel eine Ringantenne am besten funktionieren, die das Signal gleichmäßig in alle Richtungen ausstrahlt, mit Ausnahme der vertikalen.



Hinweis Informationen darüber, welche Antennenart sich am besten für Ihr Drahtlosnetzwerk eignet, finden Sie in der Dokumentation Ihrer drahtlosen Zugriffspunkte.

- **IPsec-Unterstützung** Es ist zwar nicht zwingend erforderlich, aber nach Möglichkeit sollten Sie drahtlose Zugriffspunkte wählen, die IPsec (Internet Protocol security) und ESP (Encapsulating Security Payload) mit Verschlüsselung verwenden, damit der RADIUS-Datenverkehr zwischen den drahtlosen Zugriffspunkten und den RADIUS-Servern vertraulich bleibt. Verwenden Sie die 3DES-Verschlüsselung (Triple Data Encryption Standard) und für die IKE-Hauptmodusauthentifizierung (Internet Key Exchange) nach Möglichkeit Zertifikate.

Kanaltrennung

Die direkte Kommunikation zwischen einem 802.11b- oder 802.11g-Drahtlosnetzwerkadapter und einem drahtlosen Zugriffspunkt erfolgt über einen gemeinsamen Übertragungskanal, der einem bestimmten Frequenzbereich im S-Band ISM entspricht. Sie können den drahtlosen Zugriffspunkt auf einen bestimmten Kanal einstellen und der Drahtlosnetzwerkadapter stellt sich automatisch auf den Kanal des drahtlosen Zugriffspunkts mit dem stärksten Signal ein.

Um gegenseitige Störungen zwischen den 802.11b-Drahtloszugriffspunkten zu verringern, sollten Sie dafür sorgen, dass drahtlose Zugriffspunkte, deren Sendebereiche sich überschneiden, auf verschiedenen Kanälen senden. Die Standards 802.11b und 802.11g sehen für drahtlose Zugriffspunkte 14 Kanäle vor. In den USA lässt die FCC (Federal Communications Commission) die Kanäle 1 bis 11 zu. Im größten Teil Europas können Sie die Kanäle 1 bis 13 verwenden. In Japan haben Sie nur eine Wahl: Kanal 14. Abbildung 10.2 stellt die Kanalüberschneidungen für drahtlose Zugriffspunkte nach 802.11b und 802.11g in den USA dar.

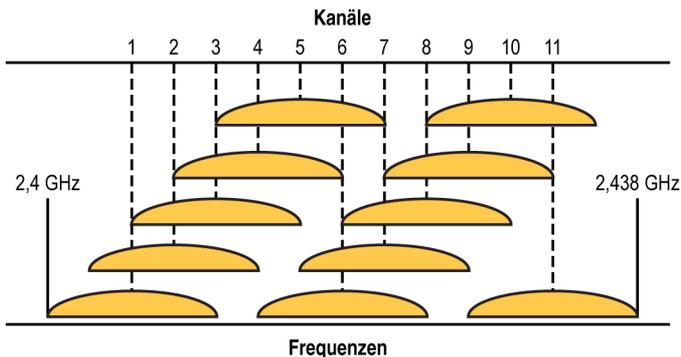


Abbildung 10.2 Kanalüberschneidungen von drahtlosen Zugriffspunkten nach 802.11b und 802.11g in den USA

Damit sich die Funksignale benachbarter Zugriffspunkte nicht gegenseitig stören, sollten Sie die Übertragungskanäle so einstellen, dass sie mindestens fünf Kanäle voneinander entfernt sind. Um in den USA die größtmögliche Anzahl verwendbarer Kanäle zu erreichen, können Sie Ihre drahtlosen Zugriffspunkte auf einen von drei Kanälen einstellen: 1, 6 oder 11. Auch wenn Sie weniger als drei praktisch verwendbare Kanäle brauchen, sollten Sie darauf achten, dass die von Ihnen gewählten Kanäle fünf Kanäle auseinander liegen.

Abbildung 10.3 zeigt ein Beispiel für die Anordnung von mehreren drahtlosen Zugriffspunkten auf verschiedenen Etagen eines Gebäudes. Die Kanäle wurden so gewählt, dass Zugriffspunkte, deren Sendebereiche sich überschneiden, auf hinreichend weit auseinanderliegenden Kanälen senden.

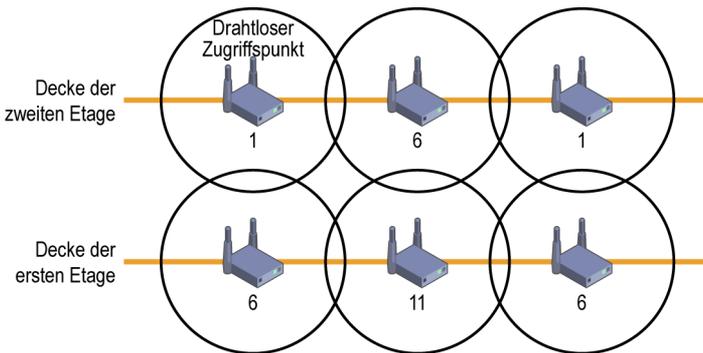


Abbildung 10.3 Ein Beispiel für die Verteilung von 802.11b-Kanalnummern

Störungen in der Signalausbreitung

Ein drahtloser Zugriffspunkt ist eine Kombination aus Funksender und -empfänger, wobei der Sender nur eine relativ geringe Reichweite hat. Der Raum um den drahtlosen Zugriffspunkt herum, in dem Sie Daten in den unterstützten Bitraten senden und empfangen können, wird in der englischsprachigen Dokumentation häufig *coverage volume* genannt (manchmal auch *coverage area*, wobei sich Funkwellen natürlich in drei Dimensionen ausbreiten). Im folgenden Text wird dieser Bereich einfach *Sendebereich* genannt. Welche Größe und Form der Bereich hat, in dem die einwandfreie Datenübertragung möglich ist, hängt von der Leistung des Senders, von der Bauweise der Antenne, von etwaigen Störungen in der Signalausbreitung und von anderen Störstrahlungsquellen ab.

Eine ideale Rundstrahlantenne strahlt die Radiowellen gleichmäßig in alle Richtungen ab. Je weiter der Empfänger vom Sender entfernt ist, desto schwächer ist das eingehende Signal und desto geringer die unterstützte Übertragungsrate. Abbildung 10.4 zeigt ein Beispiel für den Sendebereich eines drahtlosen Zugriffspunkts nach 802.11b und einer Rundstrahlantenne.

Störungen in der Signalausbreitung ändern die Form des Sendebereichs zum Beispiel durch eine unerwünschte Signalabschwächung, -abschirmung oder -reflektion. Solche Effekte wirken sich auf die optimale Aufstellung der drahtlosen Zugriffspunkte aus. Metallische Objekte innerhalb eines Gebäudes, in den Wänden oder Decken können die Ausbreitung der Radiowellen verändern. Einige Beispiele:

- Stahlträger
- Aufzugschächte
- Stahlarmierung im Beton
- Rohre von Heizungen und Klimaanlage
- Drahtgitter in den Gipsplatten, die zur Verkleidung verwendet wurden

- Wände, die Metall, Löschbeton oder Beton enthalten
- Schränke, Tische oder andere größere Einrichtungsgegenstände aus Metall

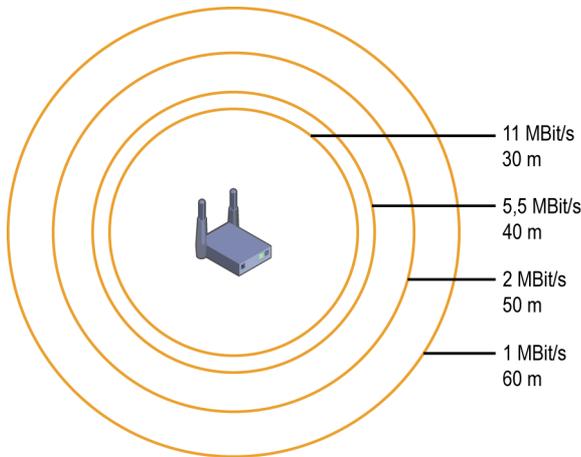


Abbildung 10.4 Ein idealisiertes Beispiel eines Sendebereichs

Störungsquellen

Jedes Gerät, das im selben Frequenzbereich wie Ihre Drahtlosnetzwerkgeräte sendet (im S-Band ISM mit dem Frequenzbereich von 2,4 GHz bis 2,5 GHz oder im C-Band ISM mit dem Frequenzbereich von 5,725 GHz bis 5,875 GHz), kann ein drahtloses Netzwerk stören. Solche Störungsquellen ändern auch die Form des Bereichs, der sich mit einem drahtlosen Zugriffspunkt abdecken lässt.

Zu den Geräten, die im S-Band ISM arbeiten, gehören folgende:

- Bluetooth-fähige Geräte
- Mikrowellenherde
- Schnurlose Telefone im 2,4-GHz-Bereich
- Kabellose Videokameras
- Medizinische Geräte
- Aufzugmotoren

Zu den Geräten, die im C-Band ISM arbeiten, gehören folgende:

- Schnurlose Telefone im 5-GHz-Bereich
- Kabellose Videokameras
- Medizinische Geräte

Anzahl der drahtlosen Zugriffspunkte

Wenn Sie abschätzen möchten, wie viele drahtlose Zugriffspunkte Sie aufstellen müssen, berücksichtigen Sie folgende Aspekte:

- Bauen Sie genügend drahtlose Zugriffspunkte auf, damit für alle Benutzer im vorgesehenen Sendebereich eine hinreichende Signalstärke zur Verfügung steht.
- Die üblichen drahtlosen Zugriffspunkte verwenden Antennen, die das Signal hauptsächlich horizontal abstrahlen, also auf die anderen Räume derselben Etage zu. Gewöhnlich deckt ein drahtloser Zugriffspunkt innerhalb eines Gebäudes eine kreisförmige Fläche mit einem Radius von

etwa 60 Metern ab. Stellen Sie so viele drahtlose Zugriffspunkte auf, dass sich die Sendebereiche der einzelnen Geräte hinreichend überlappen.

- Schätzen Sie ab, wie viele Benutzer höchstens gleichzeitig im Sendebereich eines Zugriffspunkts arbeiten.
- Schätzen Sie die Übertragungsrate ab, die jeder Benutzer im Durchschnitt braucht. Fügen Sie bei Bedarf weitere drahtlose Zugriffspunkte hinzu. Damit erreichen Sie Folgendes:
 - Die Bandbreite, die einem einzelnen Client im drahtlosen Netzwerk zur Verfügung steht, steigt.
 - Im selben Sendebereich können mehr Drahtlosbenutzer bedient werden.
 - Sie bestimmen auf der Grundlage des erforderlichen Datendurchsatzes, wie viele Benutzer eine Verbindung mit einem drahtlosen Zugriffspunkt herstellen können. Verschaffen Sie sich ein klares Bild vom Datendurchsatz, bevor Sie das Netzwerk errichten oder Änderungen vornehmen. Einige Hersteller bieten 802.11-Simulationsprogramme an, mit denen Sie den Datenverkehr im Netzwerk simulieren und den Datendurchsatz unter verschiedenen Bedingungen überprüfen können.
 - Es sind Reservegeräte verfügbar, falls ein drahtloser Zugriffspunkt ausfällt.
- Wenn Sie die Anordnung der drahtlosen Zugriffspunkte so optimieren möchten, dass Sie eine möglichst hohe Leistung erhalten, berücksichtigen Sie folgende Aspekte:
 - Überlasten Sie keinen drahtlosen Zugriffspunkt mit zu vielen Drahtlosclients. Auch wenn die meisten drahtlosen Zugriffspunkte Hunderte von Verbindungen unterstützen, liegt die praktische Grenze bei etwa 20 bis 25 verbundenen Clients. Eine durchschnittliche Belastung durch 2 bis 4 Benutzer pro drahtlosem Zugriffspunkt ist ein guter Durchschnittswert, um den Benutzern eine möglichst hohe Leistung zu bieten und das Drahtlosnetzwerk effektiv zu nutzen.
 - Wenn viele Menschen auf relativ engem Raum arbeiten müssen, verringern Sie die Sendeleistung der drahtlosen Zugriffspunkte. Dadurch verkleinert sich der Sendebereich und Sie können auf derselben Fläche mehr drahtlose Zugriffspunkte aufstellen, um einer größeren Zahl von Drahtlosclients eine höhere Bandbreite zur Verfügung zu stellen.

Authentifizierungsinfrastruktur

Die Authentifizierungsinfrastruktur hat folgende Aufgaben:

- Authentifizieren der Anmeldeinformationen der Drahtlosclients
- Autorisieren der Drahtlosverbindung
- Informieren der drahtlosen Zugriffspunkte über Verbindungsbeschränkungen
- Erfassen von Beginn und Ende der Drahtlosverbindung zu Buchhaltungszwecken

Die Authentifizierungsinfrastruktur für geschützte Drahtlosverbindungen besteht aus folgenden Komponenten:

- Drahtlose Zugriffspunkte
- RADIUS-Server
- Active Directory-Domänencontroller
- Ausstellende Zertifizierungsstellen einer PKI (optional)

Wenn Sie eine Windows-Domäne als Kontodatenbank für die Überprüfung von Benutzer- oder Computeranmeldeinformationen und zum Abrufen der Einwähleigenschaften verwenden, dann verwenden Sie unter Windows Server 2008 den Netzwerkrichtlinienserver (Network Policy Server, NPS). NPS ist ein voll funktionsfähiger und in Active Directory integrierter RADIUS-Server und -Proxy. Infor-

mationen über Entwurf und Planung eines RADIUS-Servers auf der Basis von NPS erhalten Sie in Kapitel 9.

NPS kommuniziert bei der Authentifizierung der Drahtlosverbindung über einen geschützten RPC-Kanal (Remote Procedure Call) mit einem Domänencontroller. Die Autorisierung der Verbindung führt NPS anhand der Einwähleigenschaften des für den Verbindungsversuch verwendeten Computer- oder Benutzerkontos und anhand der Netzwerkrichtlinien durch, die auf dem NPS-Server konfiguriert wurden.

NPS protokolliert alle RADIUS-Buchhaltungsinformationen in einer lokalen Protokolldatei (standardmäßig im Ordner `%SystemRoot%\System32\Logfiles`). Diese Einstellung lässt sich im Knoten *Kontoführung* des Netzwerkrichtlinienserver-Snap-Ins ändern.

Empfehlungen für die Authentifizierungsinfrastruktur

Für die Authentifizierungsinfrastruktur wird Folgendes empfohlen:

- Um Autorisierungen für Drahtlosverbindungen besser verwalten zu können, legen Sie in Active Directory eine universelle Gruppe für den Drahtloszugriff an, die globale Gruppen mit den Benutzer- und Computerkonten enthält, die Drahtlosverbindungen herstellen dürfen. Legen Sie zum Beispiel eine universelle Gruppe namens *Drahtloskonten* an. Sie nimmt globale Gruppen auf, die Sie nach den Erfordernissen der Zuständigkeitsbereiche oder Abteilungen Ihrer Organisation erstellen. Jede globale Gruppe enthält Benutzer- und Computerkonten, die für den drahtlosen Zugriff zugelassen sind. Wenn Sie Ihre NPS-Richtlinien für die Drahtlosverbindungen konfigurieren, geben Sie den Gruppennamen *Drahtloskonten* an.
- Starten Sie im Knoten *NPS* des Netzwerkrichtlinienserver-Snap-Ins den *802.1X konfigurieren*-Assistenten, um Richtlinien für drahtlose, nach 802.1X authentifizierte Verbindungen zu definieren. Erstellen Sie zum Beispiel Richtlinien für Drahtlosclients, die Mitglieder einer bestimmten Gruppe sind und eine bestimmte Authentifizierungsmethode verwenden sollen.

Drahtlosclients

Ein Windows-basierter Drahtlosclient ist ein Drahtlosclient, auf dem Windows Server 2008, Windows Vista, Windows XP mit Service Pack 2 oder Windows Server 2003 ausgeführt wird. Auf einem Windows-basierten Drahtlosclient können Sie die drahtlosen Verbindungen in folgender Weise konfigurieren:

- **Gruppenrichtlinien** Die Gruppenrichtlinienerweiterung *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* ist Teil des Zweigs *Computerkonfiguration* eines Gruppenrichtlinienobjekts. Mit ihr können Sie in einer Active Directory-Umgebung Einstellungen für das drahtlose Netzwerk vornehmen.
- **Befehlszeile** Mit *Netsh.exe* können Sie die Einstellungen für das drahtlose Netzwerk vornehmen (geben Sie den Befehl `netsh wlan` mit den erforderlichen Parametern ein). Allerdings ist diese Art der Einstellung des Drahtlosnetzwerks nur auf Drahtlosclients möglich, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird.



Hinweis Um die `netsh wlan`-Befehle auf einem Windows Server 2008 verwenden zu können, müssen Sie im Server-Manager die Funktion *WLAN-Dienst* hinzufügen.

- **XML-Drahtlosprofile** XML-Drahtlosprofile (Extensible Markup Language) sind XML-Dateien, die Einstellungen für ein drahtloses Netzwerk enthalten. XML-Drahtlosprofile können Sie mit dem Programm *Netsh* oder mit der Gruppenrichtlinienerweiterung *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* exportieren oder importieren.

- **Manuell** Auf einem Drahtlosclient, auf dem Windows Vista oder Windows Server 2008 ausgeführt wird, stellen Sie die Verbindung zum drahtlosen Netzwerk her, sobald Sie dazu aufgefordert werden, oder Sie verwenden im Netzwerk- und Freigabecenter den Assistenten für Netzwerkverbindungen. Auf einem Drahtlosclient, auf dem Windows XP mit SP2 oder Windows Server 2003 ausgeführt wird, stellen Sie die Verbindung mit dem Drahtlosnetzwerk her, wenn Sie dazu aufgefordert werden, oder Sie verwenden im Ordner *Netzwerkverbindungen* den Drahtlosnetzwerkinstallations-Assistenten.

Drahtlosnetzwerkrichtlinien (IEEE 802.11)-Gruppenrichtlinienerweiterung

Um die Einstellungen von Windows-Clients für drahtlose Netzwerke automatisch vornehmen zu können, unterstützten Windows Server 2008- und Windows Server 2003-Active Directory-Domänen eine *Drahtlosnetzwerkrichtlinien (IEEE 802.11)-Gruppenrichtlinienerweiterung*. Diese Erweiterung ermöglicht es Ihnen, Einstellungen für drahtlose Netzwerke als Teil der *Computerkonfiguration* eines Gruppenrichtlinienobjekts durchzuführen. Sie können mit der *Drahtlosnetzwerkrichtlinien (IEEE 802.11)-Gruppenrichtlinienerweiterung* eine Liste der bevorzugten Netzwerke und deren Einstellungen angeben, um auf Drahtlosclients, auf denen Windows Server 2008, Windows Vista, Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 ausgeführt wird, automatisch die erforderlichen Einstellungen für drahtlose Netzwerke vorzunehmen.

Für jedes bevorzugte Netzwerk können Sie Folgendes angeben:

- Verbindungseinstellungen, beispielsweise den Namen des drahtlosen Netzwerks, und ob das Netzwerk eine Kennung aussendet
- Sicherheitseinstellungen, beispielsweise die Authentifizierungs- und Verschlüsselungsmethode, den EAP-Typ und den Authentifizierungsmodus
- Erweiterte 802.1X Sicherheitseinstellungen wie das einmalige Anmelden (Single Sign-On, für Windows Server 2008- und Windows Vista-Drahtlosclients)

Diese Einstellungen werden automatisch auf Drahtlosclients durchgeführt, auf denen Windows Server 2008, Windows Vista, Windows XP mit SP2 oder Windows Server 2003 ausgeführt wird und die Mitglieder einer Windows Server 2008- oder Windows Server 2003-Active Directory-Domäne sind. Sie können Drahtlosnetzwerkrichtlinien im Snap-In Gruppenrichtlinienverwaltungs-Editor konfigurieren, und zwar im Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Drahtlosnetzwerkrichtlinien (IEEE 802.11)*.



Hinweis Um auf einem Computer, auf dem Windows Server 2008 ausgeführt wird, die Gruppenrichtlinieneinstellungen ändern zu können, müssen Sie eventuell im Server-Manager die Gruppenrichtlinienverwaltungsfunktion installieren.

Standardmäßig gibt es keine *Drahtlosnetzwerkrichtlinien (IEEE 802.11)-Richtlinien*. Um für eine Windows Server 2008-Active Directory-Domäne eine neue Richtlinie zu definieren, klicken Sie *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* in der Strukturansicht des Snap-Ins Gruppenrichtlinienverwaltungs-Editor mit der rechten Maustaste an und klicken dann auf *Eine neue Windows Vista-Richtlinie erstellen* oder auf *Eine neue Windows XP-Richtlinie erstellen*. Für jede Richtlinienart können Sie nur eine Richtlinie definieren. Eine Windows-XP-Richtlinie kann Profile mit Einstellungen für mehrere Drahtlosnetzwerke enthalten, von denen jedes Netzwerk über eine eindeutige SSID verfügen muss. Eine Windows Vista-Richtlinie kann auch Profile mit Einstellungen für mehrere Drahtlosnetzwerke enthalten, die über eindeutige SSIDs verfügen. Außerdem können verschiedene Profile mehrere Instanzen derselben SSID enthalten, jede mit anderen Einstellungen. Dadurch wird es möglich, Profile für gemischte Umgebungen zu erstellen, in denen Clients unterschiedliche Sicherheitstechnologien einsetzen, wie zum Beispiel WPA und WPA2.

Die Drahtlosnetzwerkrichtlinie für Windows Vista umfasst spezielle Einstellungen für Windows Server 2008- und Windows Vista-Drahtlosclients. Wenn beide Richtlinienarten konfiguriert werden, verwenden Drahtlosclients, auf denen Windows XP mit SP2 oder Windows Server 2003 ausgeführt wird, nur die Richtlinieneinstellungen für Windows XP, während Drahtlosclients, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird, nur die Windows Vista-Richtlinieneinstellungen verwenden. Sind keine Windows Vista-Richtlinieneinstellungen verfügbar, verwenden Windows Server 2008- und Windows Vista-Drahtlosclients die Windows XP-Richtlinieneinstellungen.

Windows Vista-Drahtlosnetzwerkrichtlinie

Das Eigenschaftendialogfeld einer Windows Vista-Drahtlosnetzwerkrichtlinie enthält eine Registerkarte *Allgemein* und eine Registerkarte *Netzwerkberechtigungen*. Abbildung 10.5 zeigt die Registerkarte *Allgemein*.

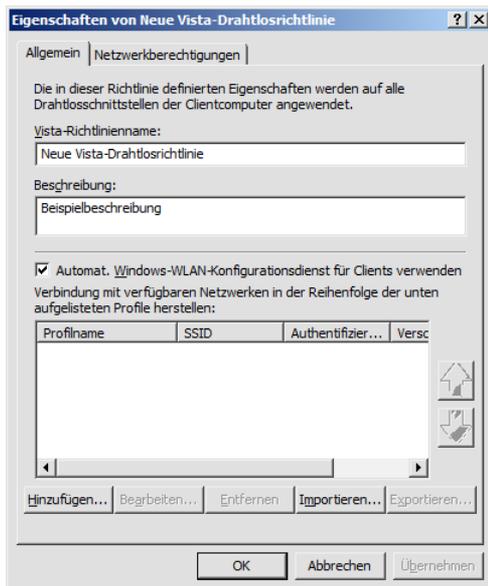


Abbildung 10.5 Die Registerkarte *Allgemein* einer Windows Vista-Drahtlosnetzwerkrichtlinie

Auf der Registerkarte *Allgemein* können Sie der Richtlinie einen Namen geben und eine Beschreibung der Richtlinie eingeben. Außerdem können Sie festlegen, ob der automatische WLAN-Konfigurationsdienst aktiviert werden soll, und Sie können eine Liste mit Drahtlosnetzwerken und ihren Einstellungen (auch *Profile* genannt) zusammenstellen, in der die Netzwerke in der gewünschten Reihenfolge angegeben werden. Auf der Registerkarte *Allgemein* können Sie Profile als XML-Dateien exportieren und importieren. Um ein Profil in eine XML-Datei zu exportieren, wählen Sie das Profil aus und klicken auf *Exportieren*. Um eine XML-Datei als Drahtlosprofil zu importieren, klicken Sie auf *Importieren* und suchen dann die gewünschte Datei heraus.

Abbildung 10.6 zeigt die Registerkarte *Netzwerkberechtigungen* für eine Windows Vista-Drahtlosnetzwerkrichtlinie.

Die Registerkarte *Netzwerkberechtigungen* ist in Windows Server 2008 und Windows Vista neu und ermöglicht die Festlegung, mit welchen namentlich aufgeführten Netzwerken eine Verbindung hergestellt werden darf und mit welchen nicht. Damit können Sie zum Beispiel eine Zulassungsliste oder eine Verbotsliste aufstellen.

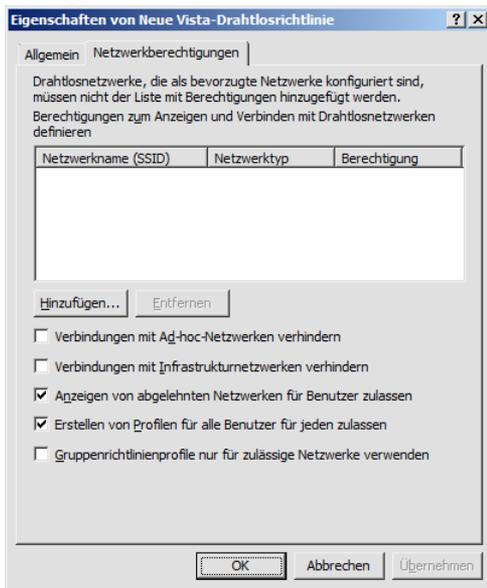


Abbildung 10.6 Die Registerkarte *Netzwerkberechtigungen* einer Windows Vista-Drahtlosnetzwerkrichtlinie

Um eine Zulassungsliste zu erstellen, geben Sie die Namen der Netzwerke an, mit denen ein Windows Server 2008- oder Windows Vista-Drahtlosclient eine Verbindung herstellen darf. Das ist zum Beispiel von Nutzen, wenn Netzwerkadministratoren die Laptops einer Organisation so einstellen müssen, dass sie mit bestimmten Netzwerken Verbindungen herstellen. Dabei kann es sich nicht nur um drahtlose Netzwerke der Organisation handeln, sondern zum Beispiel auch um drahtlose Netzwerke von Internetanbietern.

Um eine Verbotsliste zu erstellen, geben Sie die Namen der Drahtlosnetzwerke an, zu denen die Drahtlosclients keine Verbindung aufnehmen dürfen. Damit lässt sich zum Beispiel in einem von mehreren Organisationen genutzten Bürogebäude verhindern, dass die verwalteten Laptops Verbindungen mit anderen Drahtlosnetzwerken herstellen, die sich zwar in Reichweite des Drahtlosnetzwerks einer Organisation befinden, aber zu anderen Organisationen gehören. Außerdem lässt sich auf diese Weise verhindern, dass die verwalteten Laptops Verbindungen mit Netzwerken herstellen, die als unsicher bekannt sind.

Auf der Registerkarte *Netzwerkberechtigungen* sind auch Optionen verfügbar, mit denen sich Verbindungen mit Ad-hoc-Netzwerken oder mit Infrastrukturnetzwerken verhindern lassen, die es dem Benutzer ermöglichen, auch als abgelehnt eingestufte Netzwerke in der Liste der verfügbaren Netzwerke zu sehen, und die es jedem Benutzer erlauben, Profile für alle Benutzer zu erstellen. Ein *Profil für alle Benutzer* kann von jedem Benutzer, der auf dem Computer über ein Konto verfügt, zur Herstellung einer Verbindung mit einem bestimmten Drahtlosnetzwerk verwendet werden. Ist diese Option deaktiviert, können nur Mitglieder der Gruppen *Domänen-Admins* oder *Netzwerkconfigurations-Operatoren* Drahtlosprofile für alle Benutzer des Computers erstellen. Außerdem gibt es noch eine Option, mit der sich festlegen lässt, dass für die Verbindung mit zugelassenen Netzwerken nur Gruppenrichtlinien verwendet werden, also keine gleichnamigen lokalen Profile.

Zur Verwaltung der Drahtlosnetzwerkprofile wählen Sie im Dialogfeld *Eigenschaften von Neue Vista-Drahtlosrichtlinie* auf der Registerkarte *Allgemein* ein vorhandenes Profil aus und klicken auf *Bearbeiten*, oder Sie klicken auf *Hinzufügen* und wählen dann aus, ob das neue Drahtlosprofil für ein

Infrastrukturnetzwerk oder für ein Ad-hoc-Netzwerk vorgesehen ist. Das Dialogfeld *Eigenschaften von Neues Profil* eines Windows Vista-Drahtlosnetzwerkprofils enthält die beiden Registerkarten *Verbindung* und *Sicherheit*. Abbildung 10.7 zeigt die Standardregisterkarte *Verbindung* für ein Windows Vista-Drahtlosnetzwerkprofil.

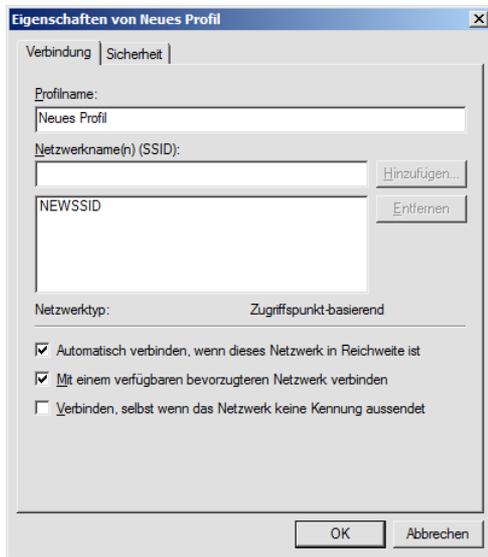


Abbildung 10.7 Die Registerkarte *Verbindung* eines Windows Vista-Drahtlosnetzwerkprofils

Auf der Registerkarte *Verbindung* können Sie dem Profil einen Namen geben und eine Liste der Netzwerknamen angeben, für die das Profil gelten soll. Um einen Namen in die Liste einzutragen, geben Sie den Namen im Textfeld *Netzwerkname(n) (SSID)* ein und klicken dann auf *Hinzufügen*. Sie können auch festlegen, ob der Drahtlosclient, der dieses Profil verwendet, automatisch versucht, eine Verbindung mit einem der genannten Netzwerke herzustellen, sobald es in Reichweite ist. Dabei erfolgen die Verbindungsversuche in der Reihenfolge, in der die Netzwerkprofile auf der Registerkarte *Allgemein* der Windows Vista-Drahtlosrichtlinie aufgeführt sind. Außerdem können Sie festlegen, ob die Verbindung mit dem Drahtlosnetzwerk getrennt werden soll, wenn ein höher priorisiertes Drahtlosnetzwerk verfügbar wird, und ob eine Verbindung auch erfolgen soll, wenn ein Netzwerk keine Kennung aussendet, wenn es sich also um ein verstecktes Netzwerk handelt.

Abbildung 10.8 zeigt die Registerkarte *Sicherheit* für ein Windows Vista-Drahtlosnetzwerkprofil.

Auf der Registerkarte *Sicherheit* können Sie die Authentifizierungs- und Verschlüsselungsmethoden für das im Profil beschriebene Drahtlosnetzwerk angeben. Unter den Authentifizierungsmethoden stehen *Offen*, *Gemeinsam verwendet*, *WPA-Personal* (WPA bedeutet Wi-Fi Protected Access), *WPA-Enterprise*, *WPA2-Personal*, *WPA2-Enterprise* und *Offen bei 802.1X* zur Verfügung. Bei den Verschlüsselungsmethoden haben Sie die Wahl unter *WEP* (Wired Equivalent Privacy), *TKIP* (Temporal Key Integrity Protocol) und *AES* (Advanced Encryption Standard). Welche Verschlüsselungsmethoden auswählbar sind, hängt aber von der gewählten Authentifizierungsmethode ab.

Wenn Sie als Authentifizierungsmethode *Offen bei 802.1X*, *WPA-Enterprise* oder *WPA2-Enterprise* wählen, können Sie auch die Netzwerkauthentifizierungsmethode (den EAP-Typ), den Authentifizierungsmodus (*Wiederholte Benutzerauthentifizierung*, *Computerauthentifizierung*, *Benutzerauthentifizierung* oder *Gastauthentifizierung*), die maximale Anzahl von Authentifizierungsfehlern, bevor die Authentifizierung abgebrochen wird, und die Zwischenspeicherung der Benutzerinformationen für

spätere Verbindungsversuche einstellen. Falls Sie keine Zwischenspeicherung einstellen, werden die Anmeldeinformationen des Benutzers aus der Registrierung gelöscht, wenn der Benutzer sich abmeldet. Meldet sich der Benutzer das nächste Mal an, wird er dann zur Eingabe der Anmeldeinformationen (wie Benutzername und Kennwort) aufgefordert.

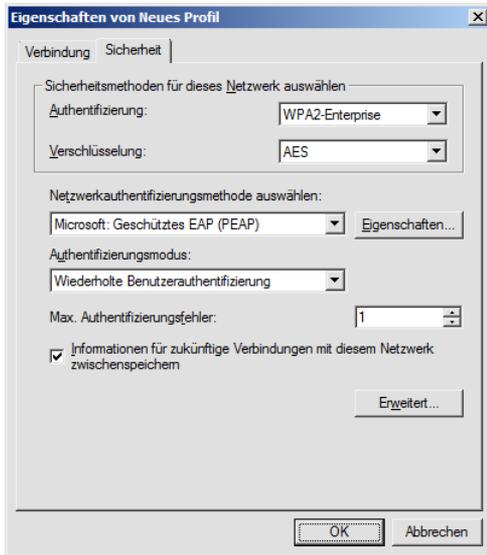


Abbildung 10.8 Die Registerkarte *Sicherheit* eines Windows Vista-Drahtlosnetzwerkprofils

Direkt von der Quelle: Speicherorte für zwischengespeicherte Anmeldeinformationen

Auf Drahtlosclients, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird, werden Anmeldeinformationen an folgendem Ort gespeichert:

HKEY_CURRENT_USER\Software\Microsoft\Wlansvc\UserData\Profiles\ProfilGUID\MSMUserData

Auf Drahtlosclients, auf denen Windows XP oder Windows Server 2003 ausgeführt wird, werden Anmeldeinformationen an folgendem Ort gespeichert:

HKEY_CURRENT_USER\Software\Microsoft\Eapol\UserEapInfo

*Clay Seymour, Support Escalation Engineer
Enterprise Platform Support*

Um für die Authentifizierungsmethoden *WPA-Enterprise*, *WPA2-Enterprise* oder *Offen bei 802.1X* erweiterte Sicherheitseinstellungen vorzunehmen, klicken Sie im Dialogfeld *Eigenschaften von Neues Profil* auf der Registerkarte *Sicherheit* auf *Erweitert*. Abbildung 10.9 zeigt das Standarddialogfeld *Erweiterte Sicherheitseinstellungen*.

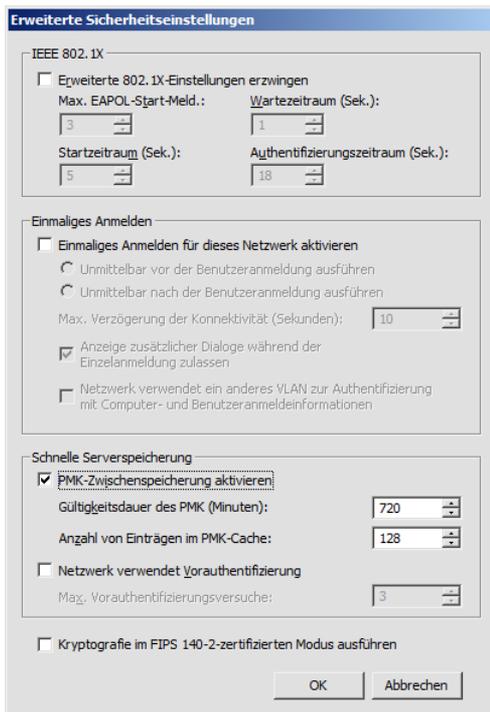


Abbildung 10.9 Das Dialogfeld *Erweiterte Sicherheitseinstellungen*

Im Abschnitt *IEEE 802.1X* lässt sich festlegen, wie viele EAPOL-Startnachrichten (EAP over LAN) gesendet werden, wenn auf die erste EAPOL-Startnachricht keine Antwort eintrifft. Außerdem lassen sich noch einige Zeiträume festlegen, nämlich die Wartezeit bis zur erneuten Übertragung von EAPOL-Startnachrichten, wenn keine Antwort auf die zuvor gesandte EAPOL-Startnachricht eintrifft, der Zeitraum, in dem der authentifizierende Client keine 802.1X-Authentifizierungsaktivität entwickelt, nachdem er vom Authentifizierer die Meldung über eine fehlerhafte Authentifizierung erhalten hat, sowie der Zeitraum, den der authentifizierende Client wartet, bevor er eine 802.1X-Anfrage erneut sendet, nachdem eine Endpunkt-zu-Endpunkt-802.1X-Authentifizierung eingeleitet wurde.

Mit den Optionen aus dem Abschnitt *Einmaliges Anmelden* (Single Sign-On) lässt sich festlegen, ob die Authentifizierung unmittelbar vor oder nach der Benutzeranmeldung erfolgt, mit wie vielen Sekunden Verzögerung die Benutzeranmeldung beginnen soll (damit die Authentifizierung vorher abgeschlossen werden kann), ob bei der Benutzeranmeldung zusätzliche Dialogfelder angezeigt werden dürfen und ob die Drahtlosnetzwerke aus dem Profil für die Computer- oder Benutzerauthentifizierung ein anderes virtuelles LAN (VLAN) verwenden und beim Wechsel vom computerauthentifizierten VLAN zum benutzerauthentifizierten VLAN eine DHCP-Erneuerung durchführen. Informationen über die Verwendung des einmaligen Anmeldens finden Sie im Abschnitt »Authentifizierungsmodi im drahtlosen Netzwerk« dieses Kapitels.

Im Abschnitt *Schnelle Serverspeicherung* (Fast Roaming, schneller Wechsel zu einem anderen Zugriffspunkt) können Sie Einstellungen für die PMK-Zwischenspeicherung (Pairwise Master Key) und die Vorauthentifizierung vornehmen. Der Abschnitt *Schnelle Serverspeicherung* wird nur angezeigt, wenn Sie auf der Registerkarte *Sicherheit* als Authentifizierungsmethode *WPA2-Enterprise* wählen. Bei der PMK-Zwischenspeicherung speichern Drahtlosclients und drahtlose Zugriffspunkte die Ergebnisse der 802.1X-Authentifizierungen in einem PMK-Cache. Wechselt der Client wieder auf

einen Zugriffspunkt, mit dem bereits eine Authentifizierung erfolgt ist, kann der Zugriff also deutlich schneller erfolgen. Sie können die maximale Speicherdauer und die maximale Anzahl von Einträgen im PMK-Cache festlegen. Bei einer Vorauthentifizierung kann ein Drahtlosclient mit anderen drahtlosen Zugriffspunkten bereits eine 802.1X-Authentifizierung durchführen, während er noch mit seinem aktuellen Zugriffspunkt verbunden ist. Wechselt der Drahtlosclient anschließend zu einem drahtlosen Zugriffspunkt, mit dem bereits eine Vorauthentifizierung erfolgt ist, ist die Zugriffszeit deutlich kürzer. Sie können die maximale Anzahl an Vorauthentifizierungsversuchen mit einem drahtlosen Zugriffspunkt einstellen.



Hinweis Der schnelle Wechsel zu einem anderen Zugriffspunkt (fast roaming) mit WPA2 ist etwas anderes als eine schnelle Wiederherstellung der Verbindung (fast reconnect). Bei der schnellen Wiederherstellung von Verbindungen wird in drahtlosen Umgebungen die Verzögerung minimiert, die entsteht, wenn ein Drahtlosclient mit PEAP von einem drahtlosen Zugriffspunkt zu einem anderen wechselt. Bei der schnellen Wiederherstellung von Verbindungen speichert der Netzwerkrichtlinienserver (Network Policy Server, NPS) Informationen über die PEAP-TLS-Sitzung, damit der Drahtlosclient bei einer Wiederherstellung der Verbindung keine PEAP-Authentifizierung durchzuführen braucht, sondern nur eine MS-CHAP v2-Authentifizierung (für PEAP-MS-CHAP v2) oder eine TLS-Authentifizierung (für PEAP-TLS). Die schnelle Wiederherstellung von Verbindungen ist für Windows-Drahtlosclients und NPS-Netzwerkrichtlinien standardmäßig aktiviert.

Mit einem letzten Kontrollkästchen können Sie angeben, ob die AES-Verschlüsselung in einem FIPS 140-2-zertifizierten Modus erfolgen soll (FIPS steht für Federal Information Processing Standard). FIPS 140-2 ist ein Sicherheitsstandard der amerikanischen Regierung für Computer, der bestimmte Anforderungen an den Entwurf und die Implementierung von Kryptografiemodule stellt. Windows Server 2008 und Windows Vista sind FIPS 140-2-zertifiziert. Wenn Sie den Modus FIPS 140-2-Zertifizierung aktivieren, führen Windows Server 2008 und Windows Vista die AES-Verschlüsselung mit Software durch, statt sich auf den Drahtlosnetzwerkadapter zu verlassen. Dieses Kontrollkästchen wird nur angezeigt, wenn Sie auf der Registerkarte *Sicherheit* die Authentifizierungsmethode *WPA2-Enterprise* wählen.

Windows XP-Drahtlosnetzwerkrichtlinie

Um eine neue Windows XP-Drahtlosnetzwerkrichtlinie zu erstellen, klicken Sie in der Strukturansicht des Snap-Ins Gruppenrichtlinienverwaltungs-Editor mit der rechten Maustaste auf *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* und klicken dann auf *Eine neue Windows XP-Richtlinie erstellen*. Das Eigenschaftendialogfeld einer Windows XP-Drahtlosrichtlinie weist die beiden Registerkarten *Allgemein* und *Bevorzugte Netzwerke* auf.

Abbildung 10.10 zeigt die Registerkarte *Allgemein* einer Windows XP-Drahtlosnetzwerkrichtlinie.

Auf der Registerkarte *Allgemein* können Sie einen Namen und eine Beschreibung für die Richtlinie eingeben und festlegen, ob der automatische Windows-WLAN-Konfigurationsdienst aktiviert ist, welche Netzwerkkarten gewünscht sind (alle verfügbaren Netzwerke, nur Infrastrukturnetzwerke oder nur Ad-hoc-Netzwerke) und ob auch zu nicht bevorzugten Netzwerken automatisch eine Verbindung hergestellt werden soll.

Abbildung 10.11 zeigt die Registerkarte *Bevorzugte Netzwerke* einer Windows XP-Drahtlosrichtlinie.

Auf der Registerkarte *Bevorzugte Netzwerke* können Sie eine Liste der bevorzugten Drahtlosnetzwerke verwalten und die einzelnen Netzwerke dabei in der Reihenfolge angeben, in der Verbindungsversuche erfolgen sollen. Um auf der Registerkarte *Bevorzugte Netzwerke* des Eigenschaftendialogfelds der Windows XP-Drahtlosrichtlinie Netzwerke zu verwalten, können Sie entweder ein vorhandenes Profil auswählen und dann auf *Bearbeiten* klicken, oder Sie klicken auf *Hinzufügen* und wählen dann,

ob das neue Drahtlosprofil für ein Infrastruktur- oder für ein Ad-hoc-Netzwerk vorgesehen ist. Das Eigenschaftendialogfeld eines bevorzugten Drahtlosnetzwerks weist die beiden Registerkarten *Netzwerkeigenschaften* und *IEEE 802.1X* auf.

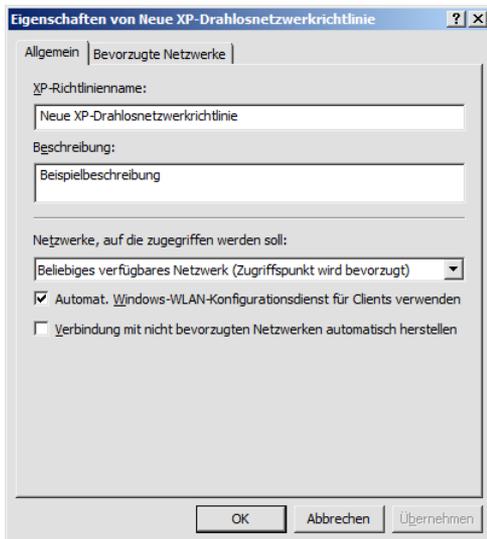


Abbildung 10.10 Die Registerkarte *Allgemein* einer Windows XP-Drahtlosnetzwerkrichtlinie

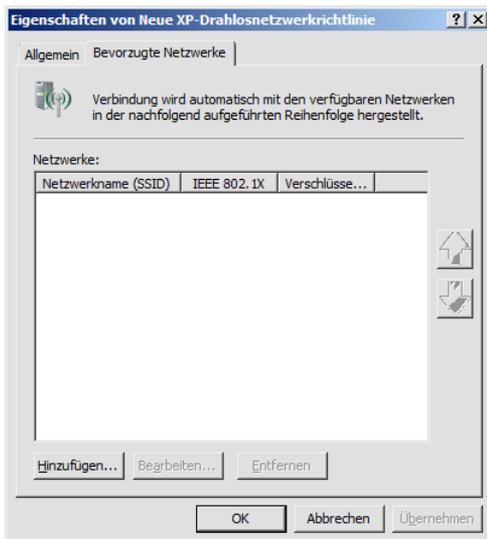


Abbildung 10.11 Die Registerkarte *Bevorzugte Netzwerke* einer Windows XP-Drahtlosrichtlinie

Abbildung 10.12 zeigt die Registerkarte *Netzwerkeigenschaften* für ein bevorzugtes Infrastrukturnetzwerk.

Auf der Registerkarte *Netzwerkeigenschaften* können Sie eine Beschreibung des bevorzugten Netzwerks eingeben und angeben, ob es sich um ein Netzwerk ohne Broadcastausstrahlung (Infrastruktur) handelt. Außerdem können Sie die Authentifizierungs- und Verschlüsselungsmethoden auswählen und

für WPA2 auch die Einstellungen für die schnelle Serverspeicherung (den schnellen Wechsel der Zugriffspunkte) vornehmen.

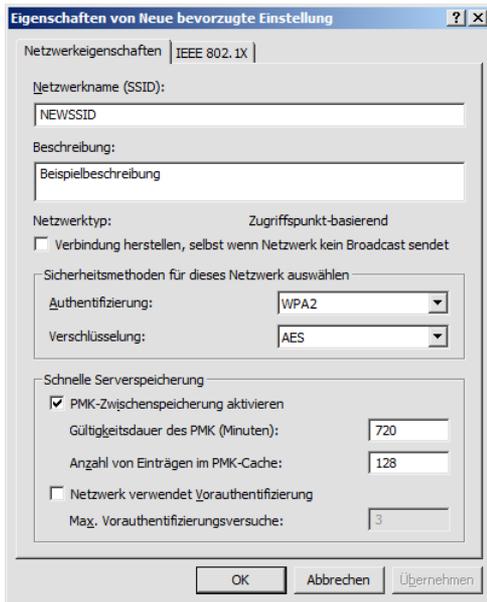


Abbildung 10.12 Die Registerkarte *Netzwerkeigenschaften* für ein bevorzugtes Infrastrukturnetzwerk

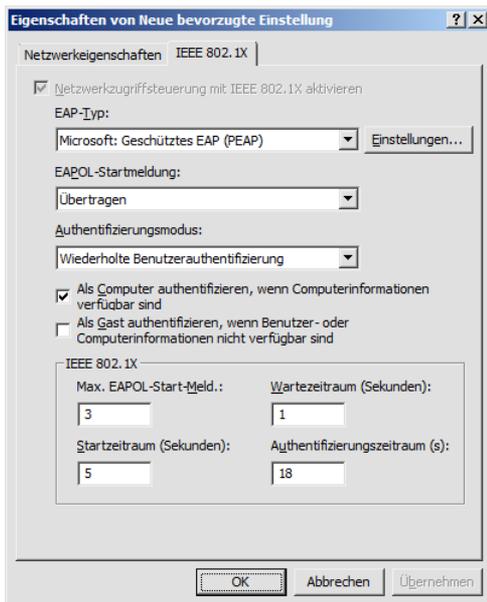


Abbildung 10.13 Die Registerkarte *IEEE 802.1X* für ein bevorzugtes Infrastrukturnetzwerk

Abbildung 10.13 zeigt die Standardregisterkarte *IEEE 802.1X* für ein bevorzugtes Drahtlosnetzwerk. Auf der Registerkarte *IEEE 802.1X* können Sie den EAP-Typ angeben und die entsprechenden Einstellungen vornehmen. Außerdem können Sie festlegen, wann die EAPOL-Startmeldung gesendet

werden soll, welcher Authentifizierungsmodus verwendet wird und ob die Anmeldung mit den Anmeldeinformationen des Computers erfolgt oder als Gast. Mit den letzten Optionen auf der Registerkarte nehmen Sie erweiterte 802.1X-Einstellungen vor.

Konfiguration auf der Befehlszeile

Unter Windows Vista können Sie einige der Einstellungen, die in den Eigenschaftendialogfeldern der drahtlosen Verbindungen aus dem Ordner *Netzwerkverbindungen* oder in der Gruppenrichtlinienerweiterung *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* erfolgen, auch auf einer Befehlszeile vornehmen. Die Konfiguration der Drahtlosnetzwerke auf der Befehlszeile kann in folgenden Situationen die Bereitstellung von drahtlosen Netzwerken erleichtern:

- **Automatisches Einstellen der Drahtlosnetzwerke mit Skripten (ohne Gruppenrichtlinien)** Die *Drahtlosnetzwerkrichtlinien (IEEE 802.11)*-Gruppenrichtlinienerweiterung ist nur in einer Active Directory-Domäne wirksam. In einer Umgebung, in der es keine Gruppenrichtlinieninfrastruktur gibt, kann ein Skript verwendet werden, das die Konfiguration der Drahtlosverbindungen automatisch durchführt. Das Skript lässt sich manuell starten oder automatisch, zum Beispiel im Rahmen eines Skripts bei der Anmeldung.
- **Hinzufügen eines Drahtlosclients zum geschützten drahtlosen Netzwerks einer Organisation** Ein Drahtlosclientcomputer, der nicht Mitglied der Domäne ist, kann keine Verbindung mit dem geschützten Drahtlosnetzwerk der Organisation aufnehmen. Der Computer kann aber erst dann ein Mitglied der Domäne werden, wenn er erfolgreich eine Verbindung mit dem geschützten Drahtlosnetzwerk der Organisation hergestellt hat. Ein Befehlszeilenskript bietet eine Methode, um eine Verbindung mit dem geschützten Drahtlosnetzwerk einer Organisation herzustellen und der Domäne beizutreten.

Um die Konfiguration von Drahtlosclients durchzuführen, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, geben Sie den Befehl `netsh wlan` mit den entsprechenden Parametern ein.



Weitere Informationen Informationen über die Syntax des Befehls `netsh wlan` finden Sie in »Netsh Commands for Wireless Local Area Network (WLAN)« unter <http://go.microsoft.com/fwlink/?LinkID=81751>.

XML-Drahtlosnetzwerkprofile

Um für Drahtlosclients, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, die Konfiguration auf der Befehlszeile zu erleichtern, können Sie die Konfiguration eines Drahtlosprofils in eine XML-Datei exportieren, die sich anschließend auf anderen Drahtlosclients importieren lässt. Sie können ein Drahtlosprofil auf dem Drahtlosclient mit dem Befehl `netsh wlan export profile` exportieren oder auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds der Windows Vista-Drahtlosrichtlinie. Für den Import eines Drahtlosprofils verwenden Sie den Befehl `netsh wlan add profile`.

Planungsaspekte für Drahtlosclients

Bei der Planung des drahtlosen Netzwerks sollten Sie für die Clients außerdem folgende Aspekte berücksichtigen:

- Wenn Sie verhindern möchten, dass Ihre Windows Vista- oder Windows Server 2008-Drahtlosclients mit bestimmten drahtlosen Netzwerken Verbindungen herstellen, richten Sie auf der Registerkarte *Netzwerkberechtigungen* des Eigenschaftendialogfelds der Windows Vista-Drahtlosrichtlinie eine Liste der abgelehnten Drahtlosnetzwerke ein oder verwenden den Befehl `netsh wlan add filter`.

- Wenn Sie Ihre Windows Vista- oder Windows Server 2008-Drahtlosclients so konfigurieren möchten, dass nur zu bestimmten Netzwerken Verbindungen hergestellt werden, stellen Sie auf der Registerkarte *Netzwerkberechtigungen* des Eigenschaftendialogfelds der Windows Vista-Drahtlosrichtlinie eine Liste der zugelassenen Netzwerke zusammen oder verwenden den Befehl `netsh wlan add filter`.

Anforderungen an Drahtlosclients

Drahtlosclients müssen bestimmte Voraussetzungen erfüllen:

- Wenn WPA2 verwendet werden soll, muss auf den Drahtlosclients Windows XP mit SP2 und dem WPA2-Update für Windows XP mit Service Pack 2, Windows Vista oder Windows Server 2008 ausgeführt werden.
- Die Konfiguration auf der Befehlszeile mit dem Befehl `netsh wlan`, der Export und Import von XML-Drahtlosprofilen und die einmalige Anmeldung (Single Sign-On) werden nur von Drahtlosclients unterstützt, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird.
- Um eine 802.1X-Erzwingung mit Netzwerkzugriffsschutz bereitzustellen, müssen Sie Ihre Drahtlosclients auf eine Authentifizierungsmethode auf der Basis von PEAP einstellen.

Empfehlungen für Drahtlosclients

Für Drahtlosclients gelten folgende Empfehlungen:

- Wenn nur eine kleine Anzahl von Drahtlosclients eingerichtet werden muss, können Sie die Clients manuell konfigurieren.
- Für eine unternehmensweite Bereitstellung eines Drahtlosnetzwerks in einer Active Directory-Umgebung verwenden Sie die Gruppenrichtlinienerweiterung *Drahtlosnetzwerkrichtlinien* (IEEE 802.11).
- Für eine Bereitstellung eines Drahtlosnetzwerks mit Skripten erstellen Sie XML-Drahtlosprofile und konfigurieren die Drahtlosclients mit einem Skript, das den Befehl `netsh wlan add profile` enthält.

PKI

Um drahtlose Verbindungen mit PEAP-TLS oder EAP-TLS authentifizieren zu können, muss eine PKI (Public Key Infrastructure) vorhanden sein, die für Drahtlosclients Computer- und Benutzerzertifikate ausstellen kann, und für RADIUS-Server Computerzertifikate. Für eine Authentifizierung auf der Basis von PEAP-MS-CHAP v2 ist keine PKI erforderlich. Es ist auch möglich, von einem anderen Anbieter Zertifikate zu kaufen und auf den NPS-Servern zu installieren. Dann müssen Sie wahrscheinlich auch das Stammzertifizierungsstellenzertifikat der Computerzertifikate dieses Anbieters auf Ihren Drahtlosclientcomputern installieren.

PKI für Smartcards

Die Verwendung von Smartcards zur Benutzerauthentifizierung stellt unter Windows die sicherste Form der Benutzerauthentifizierung dar. Für drahtlose Verbindungen können Sie bei den Authentifizierungsmethoden EAP-TLS oder PEAP-TLS Smartcards einsetzen. Die einzelnen Smartcards werden an Benutzer ausgegeben, die über einen Computer mit einem Smartcardleser verfügen. Um sich am Computer anzumelden, muss der Benutzer die Smartcard in den Smartcardleser einlegen und die PIN (Personal Identification Number) der Smartcard eingeben. Wenn der Benutzer versucht, eine

drahtlose Verbindung herzustellen, wird im Zuge dieses Vorgangs auch das Smartcardzertifikat übermittelt.

PKI für Benutzerzertifikate

Statt Smartcards können zur Benutzerauthentifizierung auch Benutzerzertifikate verwendet werden, die in der Windows-Registrierung gespeichert wurden. Allerdings ist diese Art der Authentifizierung nicht so sicher wie eine Smartcard. Wird eine Smartcard verwendet, steht das ausgestellte Benutzerzertifikat nur dann zur Authentifizierung zur Verfügung, wenn der Benutzer im Besitz der Smartcard ist und die PIN kennt, mit der die Anmeldung am Computer erfolgt. Bei der Verwendung von Benutzerzertifikaten steht das Benutzerzertifikat zur Authentifizierung zur Verfügung, wenn sich der Benutzer mit einem Domänenbenutzernamen und dem dazugehörigen Kennwort am Computer anmeldet. Wie Smartcards können Benutzerzertifikate bei der Authentifizierung von Drahtlosnetzwerkverbindungen mit EAP-TLS oder PEAP-TLS verwendet werden.

Um Ihre Organisationen mit Benutzerzertifikaten zu versorgen, bauen Sie zuerst eine PKI auf. Dann müssen Sie für jeden Benutzer ein Benutzerzertifikat installieren. Am einfachsten ist dies, wenn die Windows-Zertifikatdienste als Unternehmenszertifizierungsstelle installiert werden. Dann konfigurieren Sie mit Gruppenrichtlinien eine automatische Registrierung für die Ausstellung von Benutzerzertifikaten. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von Zertifikaten« dieses Kapitels.

Wenn der Drahtlosclient für eine drahtlose Verbindung eine Benutzerauthentifizierung durchführen möchte, übermittelt der Drahtlosclient im Rahmen dieses Vorgangs das Benutzerzertifikat.

PKI für Computerzertifikate

Computerzertifikate werden für die Computerauthentifizierung von Drahtloszugriffen mit den Authentifizierungsmethoden EAP-TLS oder PEAP-TLS in der Windows-Registrierung gespeichert. Um Ihre Organisationen mit Computerzertifikaten zu versorgen, bauen Sie zuerst eine PKI auf. Dann müssen Sie auf jedem Computer ein Computerzertifikat installieren. Am einfachsten ist das, wenn die Windows Active Directory-Zertifikatdienste oder die Zertifikatdienste als Unternehmenszertifizierungsstelle installiert werden. Dann konfigurieren Sie mit Gruppenrichtlinien eine automatische Registrierung für die Ausstellung von Computerzertifikaten. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von Zertifikaten« dieses Kapitels.

Wenn der Drahtlosclient für eine drahtlose Verbindung eine Computerauthentifizierung durchführen möchte, übermittelt der Drahtlosclient im Rahmen dieses Vorgangs das Computerzertifikat.

Anforderungen an eine PKI

Eine PKI für ein geschütztes Drahtlosnetzwerk muss einige Anforderungen erfüllen:

- Für eine Computerauthentifizierung mit EAP-TLS oder PEAP-TLS müssen Sie auf jedem Drahtlosclient ein Computerzertifikat installieren (auch *Maschinenzertifikat* genannt).
- Das Computerzertifikat des Drahtlosclients muss gültig sein und sich von NPS-Servern überprüfen lassen. Die NPS-Server müssen über ein Stammzertifizierungsstellenzertifikat für die Zertifizierungsstelle verfügen, die das Computerzertifikat des Drahtlosclients ausgestellt hat.
- Für eine Benutzerauthentifizierung mit EAP-TLS oder PEAP-TLS müssen Sie eine Smartcard verwenden oder auf jedem Drahtlosclient ein Benutzerzertifikat installieren.
- Die Smartcard- oder die Benutzerzertifikate der Drahtlosclients müssen gültig sein und sich von den NPS-Servern überprüfen lassen. Die NPS-Server müssen über ein Stammzertifizierungsstellenzertifikat verfügen, das die Zertifikate ausstellt.

lenzertifikat für die Zertifizierungsstellen verfügen, die die Smartcard- oder Benutzerzertifikate der Drahtlosclients ausgestellt haben.

- Sie müssen auf jedem Drahtlosclient das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle der Computerzertifikate der NPS-Server installieren.
- Die Computerzertifikate der NPS-Server müssen gültig und für jeden Drahtlosclient überprüfbar sein. Die Drahtlosclients müssen über das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstellen verfügen, die die Computerzertifikate der NPS-Server ausgestellt haben.
- Für eine EAP-TLS-Authentifizierung müssen das Benutzer-, Smartcard- oder Computerzertifikat des Drahtlosclients folgende Bedingungen erfüllen:
 - Das Zertifikat muss einen geheimen Schlüssel enthalten.
 - Das Zertifikat muss von einer Unternehmenszertifizierungsstelle ausgestellt oder in Active Directory mit einem Benutzer- oder Computerkonto verknüpft worden sein.
 - Für das Zertifikat muss auf dem NPS-Server eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle bestehen und es muss alle Prüfungen bestehen, die vom CryptoAPI durchgeführt und in den Netzwerkrichtlinien für drahtlose Verbindungen angegeben werden.
 - Das Zertifikat muss für die Clientauthentifizierung vorgesehen sein (es enthält im Feld *Erweiterte Schlüsselverwendung* den Eintrag *Clientauthentifizierung* mit der Objektkennung 1.3.6.1.5.5.7.3.2).
 - Das Feld *Alternativer Antragstellername* muss den Benutzerprinzipalnamen (User Principal Name, UPN) des Benutzer- oder Computerkontos enthalten.
- Für eine EAP-TLS-Authentifizierung muss das Computerzertifikat des NPS-Servers folgende Bedingungen erfüllen:
 - Das Zertifikat muss einen geheimen Schlüssel enthalten.
 - Das Feld *Antragsteller* muss einen Wert enthalten.
 - Für das Zertifikat muss auf den Drahtlosclients eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle bestehen und es muss alle Prüfungen bestehen, die vom CryptoAPI durchgeführt und in den Netzwerkrichtlinien für drahtlose Verbindungen angegeben werden.
 - Das Zertifikat muss für die Serverauthentifizierung vorgesehen sein (es enthält im Feld *Erweiterte Schlüsselverwendung* den Eintrag *Serverauthentifizierung* mit der Objektkennung 1.3.6.1.5.5.7.3.1).
 - Das Zertifikat muss mit dem erforderlichen CSP-Wert (Cryptographic Service Provider) des Anbieters Microsoft RSA SChannel Cryptographic Provider konfiguriert sein.
 - Wird das Feld *Alternativer Antragstellername* des Zertifikats benutzt, muss es den DNS-Namen des NPS-Servers enthalten.

Empfehlungen für eine PKI

Für eine PKI, die den geschützten Drahtloszugriff ermöglichen soll, gelten folgende Empfehlungen:

- Wenn Sie zur Erstellung von Computerzertifikaten für EAP-TLS oder PEAP-TLS eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle verwenden, konfigurieren Sie Ihre Active Directory-Domäne mit einer Computerkonfigurationsgruppenrichtlinie für die automatische Registrierung von Computerzertifikaten. Jeder Computer, der Mitglied der Domäne ist, fordert dann nach der nächsten Aktualisierung der Computerkonfigurationsgruppenrichtlinien automatisch ein Computerzertifikat an.

- Wenn Sie zur Erstellung von Benutzerzertifikaten für EAP-TLS oder PEAP-TLS, die in der Registrierung gespeichert werden, eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle verwenden, konfigurieren Sie Ihre Active Directory-Domäne mit einer Benutzerkonfigurationsgruppenrichtlinie für die automatische Registrierung von Benutzerzertifikaten. Jeder Benutzer, der sich erfolgreich bei der Domäne anmeldet, fordert dann nach der nächsten Aktualisierung der Benutzerkonfigurationsgruppenrichtlinien automatisch ein Benutzerzertifikat an.
- Wenn Sie für Ihre NPS-Server von einem anderen Anbieter Computerzertifikate für die PEAP-MS-CHAP v2-Authentifizierung gekauft haben und die Drahtlosclients nicht über das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Computerzertifikats des NPS-Servers verfügen, sorgen Sie mit einer entsprechenden Gruppenrichtlinie dafür, dass das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Computerzertifikats des NPS-Servers auf Ihren Drahtlosclients installiert wird. Jeder Computer, der Mitglied der Domäne ist, erhält und installiert dann automatisch das Stammzertifizierungsstellenzertifikat, wenn die Computerkonfigurationsgruppenrichtlinien aktualisiert werden.
- Für die EAP-TLS-, PEAP-TLS- und PEAP-MS-CHAP v2-Authentifizierung ist es möglich, Drahtlosclients so einzustellen, dass sie das Zertifikat des NPS-Servers nicht überprüfen. In diesem Fall ist es nicht erforderlich, auf den NPS-Servern Computerzertifikate und auf den Drahtlosclients die dazugehörigen Stammzertifizierungsstellenzertifikate zu installieren. Allerdings wird empfohlen, dass Drahtlosclients die Zertifikate des NPS-Servers überprüfen, damit sich Drahtlosclients und NPS-Server gegenseitig überprüfen können. Durch eine gegenseitige Authentifizierung können Sie Ihre Drahtlosclients davor schützen, eine Verbindung mit irgendeinem nichtautorisierten drahtlosen Zugriffspunkt herzustellen, der mit ebenfalls nichtautorisierten Zugriffsservern arbeitet.

802.1X-Erzwingung mit NAP

NAP für Windows Server 2008, Windows Vista und Windows XP mit Service Pack 3 bietet Komponenten und Programmierschnittstellen (Application Programming Interfaces, APIs), mit denen Sie die Einhaltung der Integritätsrichtlinien für den Netzwerkzugriff oder die Netzwerkkommunikation erzwingen können. Entwickler und Netzwerkadministratoren können Lösungen für die Überprüfung von Computern entwickeln, die Verbindungen mit ihren Netzwerken herstellen, erforderliche Updates oder den Zugriff auf erforderliche Ressourcen zur Verfügung stellen und den Zugriff durch nicht konforme Computer einschränken.

Die 802.1X-Erzwingung ist eine der NAP-Erzwingungsmethoden von Windows Server 2008, Windows Vista und Windows XP. Bei der 802.1X-Erzwingung muss ein mit 802.1X authentifizierter Drahtlosclient beweisen, dass er die Integritätsanforderungen des Systems erfüllt, bevor er Zugang zum Intranet erhält. Hält ein Drahtlosclient die Integritätsanforderungen des Systems nicht ein, verschiebt der drahtlose Zugriffspunkt den Drahtlosclient in ein eingeschränktes Netzwerk, in denen die Server verfügbar sind, die erforderlich sind, um den Drahtlosclient so weit aufzurüsten, dass er die Integritätsregeln einhält. Der drahtlose Zugriffspunkt erreicht diese Einschränkung des Zugriffs durch Paketfilter oder durch eine entsprechende VLAN-Kennung, die der Drahtlosverbindung zugewiesen wird. Nach der Korrektur des Integritätszustands kann der Drahtlosclient seinen Integritätszustand erneut überprüfen lassen. Sofern er konform ist, werden die Beschränkungen aufgehoben, denen er im eingeschränkten Teil des Drahtlosnetzwerks unterliegt.

Damit die 802.1X-Erzwingung funktioniert, müssen Sie über ein geschütztes Drahtlosnetzwerk verfügen, das eine Authentifizierungsmethode auf der Basis von PEAP verwendet. Einzelheiten über die

Bereitstellung der 802.1X-Erzwingung nach dem erfolgreichen Aufbau eines geschützten Drahtlosnetzwerks finden Sie in Kapitel 17.

Bereitstellen von geschütztem Drahtloszugriff

Um mit Windows Server 2008 und Windows Vista ein geschütztes Drahtlosnetzwerk aufzubauen, gehen Sie folgendermaßen vor:

1. Stellen Sie die erforderlichen Zertifikate bereit.
2. Konfigurieren Sie Active Directory für Benutzerkonten und -Gruppen.
3. Konfigurieren Sie NPS-Server.
4. Stellen Sie drahtlose Zugriffspunkte bereit.
5. Konfigurieren Sie die Drahtlosclients.

Bereitstellen von Zertifikaten

In den folgenden Authentifizierungskonfigurationen braucht jeder Drahtlosclient ein Computerzertifikat:

- **Computerauthentifizierung mit EAP-TLS oder PEAP-TLS und Computerzertifikaten** Jeder Drahtlosclient braucht ein Computerzertifikat.
- **Benutzerauthentifizierung mit EAP-TLS oder PEAP-TLS und mit Smartcard oder registrierungsbasierten Benutzerzertifikaten** Jeder Drahtlosbenutzer braucht eine Smartcard oder jeder Drahtlosclient-computer braucht ein Benutzerzertifikat.
- **Benutzer- oder Computerauthentifizierung mit PEAP-MS-CHAP v2** Jeder Drahtlosclient braucht das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Computerzertifikats des NPS-Servers.

Bereitstellen von Computerzertifikaten

Zur Installation von Computerzertifikaten für eine EAP-TLS- oder PEAP-TLS-Authentifizierung muss eine PKI vorhanden sein, die diese Zertifikate ausstellen kann. Sobald diese PKI vorhanden ist, können Sie auf folgende unterschiedliche Weisen auf Drahtlosclients und NPS-Servern Computerzertifikate installieren:

- Durch das Konfigurieren der automatischen Registrierung von Computerzertifikaten auf den Computern einer Active Directory-Domäne (empfohlen)
- Durch die Anforderung eines Computerzertifikats mit dem Zertifikate-Snap-In
- Durch den Import eines Computerzertifikats mit dem Zertifikate-Snap-In
- Durch die Ausführung eines CAPICOM-Skripts, das ein Computerzertifikat anfordert

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« von Kapitel 9.

Bereitstellen von Benutzerzertifikaten

Auf folgende Arten können Sie auf Drahtlosclients Benutzerzertifikate installieren:

- Durch das Konfigurieren der automatischen Registrierung von Benutzerzertifikaten für die Benutzer in einer Active Directory-Domäne (empfohlen)
- Durch die Anforderung eines Benutzerzertifikats mit dem Zertifikate-Snap-In

- Durch den Import eines Benutzerzertifikats mit dem Zertifikate-Snap-In
- Durch das Anfordern eines Zertifikats über das Web
- Durch die Ausführung eines CAPICOM-Skripts, das ein Benutzerzertifikat anfordert

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« von Kapitel 9.

Bereitstellen von Stammzertifizierungsstellenzertifikaten

Wenn Sie eine PEAP-MS-CHAP v2-Authentifizierung einsetzen, müssen Sie wahrscheinlich auf Ihren Drahtlosclients die Stammzertifizierungsstellenzertifikate der Computerzertifikate Ihrer NPS-Server installieren. Falls das Stammzertifizierungsstellenzertifikat des Ausstellers der Computerzertifikate, die auf den NPS-Servern installiert sind, bereits als Stammzertifizierungsstellenzertifikate auf Ihren Drahtlosclients installiert ist, ist keine weitere Konfiguration erforderlich. Handelt es sich bei Ihrer Stammzertifizierungsstelle zum Beispiel um eine Online-Stammzertifizierungsstelle auf der Basis von Windows Server 2008, wird das Stammzertifizierungsstellenzertifikat über Gruppenrichtlinien automatisch auf jedem Computer installiert, der Mitglied der Domäne ist.

Bei der Überprüfung, ob auf Ihren Drahtlosclients das korrekte Stammzertifizierungsstellenzertifikat installiert ist, müssen Sie auf zwei Punkte achten:

- Wie heißt die Stammzertifizierungsstelle der Computerzertifikate, die auf den NPS-Servern installiert wurden?
- Wurde auf Ihren Drahtlosclients ein Zertifikat der Stammzertifizierungsstelle installiert?

So bestimmen Sie die Stammzertifizierungsstelle der Computerzertifikate der NPS-Server

1. Erweitern Sie in der Strukturansicht des Zertifikate-Snap-Ins für das Computerkonto des NPS-Servers den Knoten *Zertifikate (Lokaler Computer oder Computername)*, erweitern Sie dann den Knoten *Eigene Zertifikate* und klicken Sie auf *Zertifikate*.
2. Klicken Sie im Detailbereich mit einem Doppelklick auf das Computerzertifikat, das vom NPS-Server für die PEAP-MS-CHAP v2-Authentifizierung verwendet wird.
3. Achten Sie im Eigenschaftendialogfeld *Zertifikate* auf der Registerkarte *Zertifizierungspfad* auf den Namen am Anfang des Zertifizierungspfads. Das ist der Name der Stammzertifizierungsstelle.

So finden Sie heraus, ob auf Ihrem Drahtlosclient ein Zertifikat von der Stammzertifizierungsstelle installiert ist

1. Erweitern Sie in der Strukturansicht des Zertifikate-Snap-Ins für das Computerkonto des Drahtlosclients den Knoten *Zertifikate (Lokaler Computer oder Computername)*, erweitern Sie dann den Knoten *Vertrauenswürdige Stammzertifizierungsstellen* und klicken Sie auf *Zertifikate*.
2. Überprüfen Sie im Detailbereich, ob in der Liste der Zertifikate der Name der Stammzertifizierungsstelle der Computerzertifikate zu finden ist, die für den NPS-Server ausgestellt wurden.

Sie müssen die Stammzertifizierungsstellenzertifikate der Herausgeber der Computerzertifikate der NPS-Server auf jedem Drahtlosclient installieren, auf dem sie noch nicht verfügbar sind. Am einfachsten lassen sich Stammzertifizierungsstellenzertifikate über Gruppenrichtlinien auf allen Drahtlosclients installieren. Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« von Kapitel 9.

Konfigurieren von Active Directory für Konten und Gruppen

Zur Vorbereitung von Active Directory für den Drahtloszugriff konfigurieren Sie die Benutzer- und Computerkonten, die für die Authentifizierung der drahtlosen Verbindungen verwendet werden, auf folgende Weise:

- Stellen Sie auf der Registerkarte *Einwählen* die Netzwerkzugriffsberechtigung auf *Zugriff gestatten* oder *Zugriff über NPS-Netzwerkrichtlinien steuern*. Bei dieser Einstellung wird der Zugang zum Netzwerk mit den NPS-Netzwerkrichtlinien gesteuert. Standardmäßig wird die Netzwerkzugriffsberechtigung in neuen Benutzer- und Computerkonten auf *Zugriff über NPS-Netzwerkrichtlinien steuern* gestellt.
- Fassen Sie die Computer- und Benutzerkonten zu geeigneten universellen oder globalen Gruppen zusammen, um die Verwaltung des Netzwerkzugriffs zu vereinfachen.

Konfigurieren der NPS-Server

Konfigurieren Sie Ihre NPS-Server, wie in Kapitel 9 beschrieben. Gehen Sie dazu folgendermaßen vor:

1. Installieren Sie auf jedem NPS-Server ein Computerzertifikat.
2. Installieren Sie auf jedem NPS-Server bei Bedarf die Stammzertifizierungsstellenzertifikate der Computer- oder Benutzerzertifikate der Drahtlosclients.
3. Konfigurieren Sie auf dem primären NPS-Server die Protokollierung.
4. Fügen Sie zum primären NPS-Server die RADIUS-Clients (die drahtlosen Zugriffspunkte) hinzu.
5. Erstellen Sie auf dem primären NPS-Server die Richtlinien, die zusammen mit den Gruppen, zu denen die für Drahtloszugriffe vorgesehenen Konten gehören, die drahtlosen Zugriffe steuern.

Einzelheiten zu den Schritten 1 bis 4 finden Sie in Kapitel 9.

So erstellen Sie Richtlinien für drahtlose Verbindungen

1. Klicken Sie in der Strukturansicht des Netzwerkrichtlinienserver-Snap-Ins auf *NPS*.
2. Wählen Sie im Detailbereich aus der Dropdownliste unter *Standardkonfiguration* die Konfiguration *RADIUS-Server für drahtlose oder verkabelte 802.1X-Verbindungen* aus und klicken Sie dann auf *802.1X konfigurieren*.
3. Wählen Sie auf der Seite *802.1X-Verbindungstyp auswählen* des Assistenten zum Konfigurieren von 802.1X die Option *Sichere Drahtlosverbindungen* und geben Sie dann im Textfeld *Name* einen Namen für die Richtlinie ein (oder verwenden Sie den Namen, den der Assistent vorgibt). Klicken Sie auf *Weiter*.
4. Fügen Sie auf der Seite *802.1X-Switches angeben* nach Bedarf die RADIUS-Clients hinzu (in diesem Fall also Ihre drahtlosen Zugriffspunkte). Klicken Sie auf *Weiter*.
5. Stellen Sie auf der Seite *Authentifizierungsmethode konfigurieren* den gewünschten EAP-Typ ein, der für die drahtlosen Verbindungen verwendet werden soll.

Zur Konfiguration von EAP-TLS wählen Sie in der Dropdownliste *Typ* den Eintrag *Microsoft: Smartcard- oder anderes Zertifikat* und klicken dann auf *Konfigurieren*. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* das Computerzertifikat aus, das für drahtlose Verbindungen verwendet werden soll, und klicken Sie dann auf *OK*. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure

Channel) nicht. Die SChannel-Unterstützung ist aber erforderlich, damit NPS das Zertifikat für die EAP-TLS-Authentifizierung verwenden kann.

Zur Konfiguration von PEAP-MS-CHAP v2 wählen Sie in der Dropdownliste *Typ* den Eintrag *Microsoft: Geschütztes EAP (PEAP)* und klicken dann auf *Konfigurieren*. Wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP bearbeiten* das Computerzertifikat aus, das für die drahtlosen Verbindungen verwendet werden soll, und klicken Sie dann auf *OK*. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Die SChannel-Unterstützung ist aber erforderlich, damit NPS das Zertifikat für die PEAP-Authentifizierung verwenden kann.

Zur Konfiguration von PEAP-TLS wählen Sie in der Dropdownliste *Typ* den Eintrag *Microsoft: Geschütztes EAP (PEAP)* und klicken dann auf *Konfigurieren*. Wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP bearbeiten* das Computerzertifikat aus, das für die drahtlosen Verbindungen verwendet werden soll. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Klicken Sie unter *EAP-Typen* auf *Gesichertes Kennwort (EAP-MSCHAP v2)* und dann auf *Entfernen*. Klicken Sie auf *Hinzufügen*. Klicken Sie im Dialogfeld *EAP hinzufügen* auf *Smartcard- oder anderes Zertifikat* und dann auf *OK*. Klicken Sie im Dialogfeld *Eigenschaften für geschütztes EAP bearbeiten* unter *EAP-Typen* auf *Smartcard- oder anderes Zertifikat* und klicken Sie dann auf *Bearbeiten*. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* das Computerzertifikat aus, das für die drahtlosen Verbindungen verwendet werden soll, und klicken Sie dann auf *OK*. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

6. Klicken Sie auf *Weiter*. Fügen Sie auf der Seite *Benutzergruppen angeben* die Gruppen mit den Konten für drahtlose Computer und Benutzer hinzu (beispielsweise eine von Ihnen definierte Gruppe *DrahtlosKonten*).
7. Klicken Sie auf der Seite *VLAN (virtuelles LAN) konfigurieren* auf *Konfigurieren*, falls Sie RADIUS-Attribute und deren Werte angeben möchten, mit denen Ihre drahtlosen Zugriffspunkte für das passende VLAN konfiguriert werden. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Abschließen neuer sicherer verkabelter und drahtloser IEEE 802.1X-Verbindungen und RADIUS-Clients* auf *Fertig stellen*.

Nachdem Sie auf dem primären NPS-Server die gewünschte Protokollierung eingestellt, die RADIUS-Clients hinzugefügt und die Sicherheitseinstellungen vorgenommen haben, kopieren Sie die Konfiguration auf den sekundären und auf alle weiteren vorgesehenen NPS-Server. Weitere Informationen finden Sie in Kapitel 9.

Bereitstellen drahtloser Zugriffspunkte

Gehen Sie zur Bereitstellung Ihrer drahtlosen Zugriffspunkte folgendermaßen vor:

1. Suchen Sie anhand von Bauplänen nach geeigneten Orten für die Aufstellung von drahtlosen Zugriffspunkten.
2. Bauen Sie die drahtlosen Zugriffspunkte für einen Test auf.
3. Führen Sie eine Standortüberprüfung (site survey) durch und messen Sie die Signalstärke in allen Bereichen.

4. Suchen Sie bei Bedarf andere Aufstellungsorte für die drahtlosen Zugriffspunkte oder entfernen Sie Störquellen.
5. Überprüfen Sie den Sendebereich.
6. Tragen Sie die Zahl und Anordnung der drahtlosen Zugriffspunkte in die Baupläne ein.
7. Konfigurieren Sie TCP/IP, das Sicherheitssystem und die RADIUS-Server.

Diese Schritte werden in den folgenden Abschnitten ausführlicher beschrieben.



Hinweis Eine Alternative zur Standortüberprüfung (site survey) besteht darin, einen einzelnen drahtlosen Zugriffspunkt nacheinander an verschiedenen Stellen aufzustellen und zu überprüfen, ob sich Störungen ergeben und welche Aufstellungsorte am besten geeignet sind. Auf diese Weise können Sie auch abschätzen, ob sich der Standort überhaupt für ein drahtloses Netzwerk eignet, bevor Sie zahlreiche drahtlose Zugriffspunkte installieren.

Ermitteln der geeigneten Aufstellungsorte für drahtlose Zugriffspunkte

Beschaffen oder erstellen Sie Pläne von jedem Gebäude und jeder Etage, auf der ein drahtloses Netzwerk verwendet werden soll. Suchen Sie auf den Plänen die Büros, Konferenzräume, Lobbys und andere Bereiche heraus, in denen ein drahtloser Netzwerkzugriff möglich sein soll.

Es kann sinnvoll sein, mit dem Drahtlosnetzwerk das gesamte Gebäude abzudecken, also nicht nur bestimmte Bereiche innerhalb des Gebäudes. Dadurch lassen sich Verbindungsprobleme vermeiden, die sonst zum Beispiel entstehen können, wenn jemand mit einem Laptop sein Büro verlässt und den Laptop in einem anderen Teil des Gebäudes verwenden möchte.

Zeichnen Sie auf den Plänen die Störquellen ein, die sich auf das Drahtlosnetzwerk auswirken können, und kennzeichnen Sie Baumaterialien oder Objekte, die Funksignale schwächen, reflektieren oder abschirmen. Verteilen Sie die drahtlosen Zugriffspunkte anschließend so, dass kein drahtloser Zugriffspunkt weiter als etwa 60 bis 65 Meter vom nächsten drahtlosen Zugriffspunkt entfernt ist.

Nachdem Sie auf diese Weise die Aufstellungsorte der drahtlosen Zugriffspunkte ermittelt haben, müssen Sie die verwendeten Übertragungskanäle bestimmen und jeden drahtlosen Zugriffspunkt auf seinen vorgesehenen Kanal einstellen.

So wählen Sie die Kanäle für die drahtlosen Zugriffspunkte

1. Finden Sie heraus, welche Drahtlosnetzwerke von anderen Organisationen im selben Gebäude betrieben werden. Informieren Sie sich über die Aufstellungsorte der drahtlosen Zugriffspunkte und über die verwendeten Kanäle.

Funksignale durchdringen Decken und Wände. Daher müssen auch drahtlose Zugriffspunkte, die im Prinzip dicht beieinander stehen, aber vielleicht nur durch eine Decke oder den Fußboden voneinander getrennt sind, auf Kanäle eingestellt werden, die sich möglichst wenig gegenseitig stören. Wenn eine andere Organisation in der Etage über oder unter Ihnen ein Drahtlosnetzwerk betreibt, können die drahtlosen Zugriffspunkte dieser Organisation durchaus Ihr geplantes Netzwerk stören, und umgekehrt. Informieren Sie daher die benachbarte Organisation über Ihre Pläne und informieren Sie sich über die Anordnung und die Kanaleinstellung der drahtlosen Zugriffspunkte dieser Organisation, damit Sie Ihre eigenen drahtlosen Zugriffspunkte auf eine andere Kanalnummer einstellen können.

2. Finden Sie heraus, wo sich die Funksignale verschiedener drahtloser Netzwerke aus Ihrer eigenen Organisation überlappen.

- Nachdem Sie die Bereiche ermittelt haben, in denen sich Ihr geplantes Drahtlosnetzwerk mit einem anderen internen oder externen Drahtlosnetzwerk überlappt, weisen Sie Ihren drahtlosen Zugriffspunkten geeignete Kanalnummern zu.

So weisen Sie den drahtlosen Zugriffspunkten Kanalnummern zu

- Weisen Sie dem ersten drahtlosen Zugriffspunkt die Kanalnummer 1 zu.
- Weisen Sie den drahtlosen Zugriffspunkten, die den Sendebereich des ersten drahtlosen Zugriffspunkts überlappen, die Kanäle 6 und 11 zu, um sicherzustellen, dass diese drahtlosen Zugriffspunkte nicht auch andere drahtlose Zugriffspunkte in ihrer Reichweite stören, die auf demselben Kanal senden.
- Weisen Sie auch den restlichen drahtlosen Zugriffspunkten nach diesem Muster Kanalnummern zu. Achten Sie dabei darauf, dass zwei drahtlose Zugriffspunkte, deren Sendebereiche sich überlappen, mindestens fünf Kanäle voneinander getrennt sind.

Bauen Sie die drahtlosen Zugriffspunkte für einen Test auf

Bauen Sie die drahtlosen Zugriffspunkte für einen ersten Test auf. Orientieren Sie sich dabei an den Aufstellungsorten und Kanalnummern, die Sie bisher auf der Grundlage der Baupläne ermittelt haben.

Führen Sie eine Standortüberprüfung durch

Führen Sie eine Standortüberprüfung (site survey) durch, indem Sie mit einem Laptop, der mit einem 802.11-Drahtlosadapter und einer geeigneten Site-Survey-Software ausgerüstet ist, durch das Gebäude gehen. (Die meisten Drahtlosadapter und drahtlosen Zugriffspunkte werden mit einer Site-Survey-Software ausgeliefert). Bestimmen Sie die Signalstärken und Bitraten in den Sendebereichen der installierten drahtlosen Zugriffspunkte.

Optimieren Sie die drahtlosen Zugriffspunkte und entfernen Sie Störungsquellen

In den Bereichen, in denen das Signal zu schwach ist, können Sie folgende Verbesserungen durchführen, damit den Empfängern ein stärkeres Signal zur Verfügung steht:

- Stellen Sie die für den ersten Test aufgestellten drahtlosen Zugriffspunkte so um, dass die Signalstärke in den betreffenden Bereichen verbessert wird.
- Entfernen Sie Geräte, die störende Signale aussehenden, oder stellen Sie die Geräte woanders auf (beispielsweise Bluetooth-Geräte oder Mikrowellenherde).
- Stellen Sie metallische Gegenstände, die sich auf die Signalausbreitung auswirken, anders auf oder entfernen Sie diese Gegenstände (beispielsweise Metallschränke oder andere größere metallische Gegenstände).
- Fügen Sie weitere drahtlose Zugriffspunkte hinzu, falls die bisherige Anzahl noch nicht ausreicht, um die Signalstärke zu verbessern.



Hinweis Wenn Sie weitere drahtlose Zugriffspunkte aufstellen, müssen Sie vielleicht die Kanalnummern benachbarter drahtloser Zugriffspunkte ändern.

- Kaufen Sie Antennen, die besser zu den Verhältnissen passen, die im Gebäude herrschen.

Sie können zum Beispiel die Interferenzen zwischen drahtlosen Zugriffspunkten verringern, die auf verschiedenen Etagen stehen, indem Sie Antennen mit einer flachen Ausstrahlungscharakteristik beschaffen (der Sendebereich hat dann zum Beispiel nicht mehr die Form einer Kugel, sondern eines Donuts). Dadurch schwächt sich die Ausstrahlung in vertikaler Richtung ab.

Überprüfen Sie den Sendebereich

Führen Sie eine weitere Standortüberprüfung durch und achten Sie darauf, ob sich die geänderte Konfiguration oder die Umstellung der drahtlosen Zugriffspunkte in der gewünschten Weise auf die Signalstärke auswirkt. Es sollte also keine Bereiche mit zu schwachen Sendesignalen mehr geben.

Aktualisieren Sie Ihre Pläne

Aktualisieren Sie die Gebäude- und Etagenpläne, damit die richtige Anzahl der drahtlosen Zugriffspunkte und die richtigen Aufstellungsorte erkennbar sind. Zeichnen Sie für jeden Zugriffspunkt den Sendebereich ein und die Abstände, an denen sich die Übertragungsraten ändern.

Konfigurieren des Sicherheitssystems, der RADIUS-Server und von TCP/IP

Konfigurieren Sie Ihre drahtlosen Zugriffspunkte mit folgenden Werten:

- Einen Namen für das Drahtlosnetzwerk und ein sicheres Administratorkennwort
- Eine statische IPv4-Adresse, eine Subnetzmaske und ein Standardgateway für das Drahtlossubnetz, zu dem der Zugriffspunkt gehört
- WPA2 oder WPA mit 802.1X-Authentifizierung (WPA2-Enterprise oder WPA-Enterprise)
- Führen Sie folgende RADIUS-Einstellungen durch:
 - Die IP-Adresse oder den Namen eines primären RADIUS-Servers, das gemeinsame geheime RADIUS-Kennwort, die UDP-Ports für die Authentifizierung und Kontoführung, sowie die Einstellungen für die Fehlererkennung
 - Die IP-Adresse oder den Namen eines sekundären RADIUS-Servers, das gemeinsame geheime RADIUS-Kennwort, die UDP-Ports für die Authentifizierung und Kontoführung, sowie die Einstellungen für die Fehlererkennung

Um den RADIUS-Datenverkehr gleichmäßig zwischen den beiden NPS-Servern aufzuteilen, konfigurieren Sie die Hälfte der drahtlosen Zugriffspunkte mit dem primären NPS-Server als primären RADIUS-Server und mit dem sekundären NPS-Server als sekundären RADIUS-Server. Dann konfigurieren Sie die andere Hälfte der drahtlosen Zugriffspunkte mit dem sekundären NPS-Server als primären RADIUS-Server und dem primären NPS-Server als sekundären RADIUS-Server.

Falls die drahtlosen Zugriffspunkte herstellereigenschaften Attribute (Vendor-Specific Attributes, VSAs) oder zusätzliche RADIUS-Attribute erfordern, müssen Sie die herstellereigenschaften Attribute oder RADIUS-Attribute zu den Drahtlosnetzwerkrichtlinien der NPS-Server hinzufügen. Wenn Sie die herstellereigenschaften Attribute oder RADIUS-Attribute zu den Drahtlosnetzwerkrichtlinien des primären NPS-Servers hinzugefügt haben, können Sie die Konfiguration des primären NPS-Servers auf den sekundären NPS-Server übertragen.

Konfigurieren von Drahtlosclients

Die Clients eines drahtlosen Netzwerks können Sie auf folgende drei Arten konfigurieren:

- Mit Gruppenrichtlinien
- Durch die Konfiguration und Bereitstellung von XML-Drahtlosprofilen
- Manuell

Konfigurieren von Drahtlosclients durch Gruppenrichtlinien

Zur Einstellung der Gruppenrichtlinien für drahtlose Netzwerke nach IEEE 802.11 gehen Sie folgendermaßen vor:

1. Öffnen Sie auf einem Computer, auf dem Windows Server 2008 ausgeführt wird und der Mitglied Ihrer Active Directory-Domäne ist, das Snap-In Gruppenrichtlinienverwaltung.
2. Erweitern Sie in der Strukturansicht den Knoten *Gesamtstruktur*, erweitern Sie *Domänen* und klicken Sie dann auf den Namen der Domäne, zu der Ihre Drahtlosclients gehören.
3. Klicken Sie auf der Registerkarte *Verknüpfte Gruppenrichtlinienobjekte* das entsprechende Gruppenrichtlinienobjekt mit der rechten Maustaste an (das Standardobjekt ist *Default Domain Policy*) und klicken Sie dann auf *Bearbeiten*.
4. Erweitern Sie in der Strukturansicht des Snap-Ins Gruppenrichtlinienverwaltungs-Editor den Knoten des Gruppenrichtlinienobjekts, dann *Computerkonfiguration*, dann *Richtlinien*, dann *Windows-Einstellungen*, anschließend *Sicherheitseinstellungen* und schließlich *Drahtlosnetzwerkrichtlinien (IEEE 802.11)*.
5. Klicken Sie *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* mit der rechten Maustaste an und klicken Sie dann entweder auf *Eine neue Windows Vista-Richtlinie erstellen* oder auf *Eine neue Windows XP-Richtlinie erstellen*.

Bei einer neuen Windows Vista-Drahtlosrichtlinie fahren Sie folgendermaßen fort:

1. Geben Sie auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds der neu erstellten Windows Vista-Drahtlosnetzwerkrichtlinie einen Namen und eine Beschreibung für die Richtlinie ein.
2. Fügen Sie auf der Registerkarte *Netzwerkberechtigungen* nach Bedarf die Namen der zugelassenen und der abgelehnten Netzwerke hinzu.
3. Klicken Sie auf der Registerkarte *Allgemein* auf *Hinzufügen*, um ein Drahtlosnetzwerkprofil hinzuzufügen, und klicken Sie dann auf *Infrastruktur*, um ein Infrastruktur-Drahtlosnetzwerk anzugeben.
4. Geben Sie auf der Registerkarte *Verbindung* den Namen (die SSID) des Drahtlosnetzwerks und optional eine Beschreibung ein. Nehmen Sie dann nach Bedarf die Verbindungseinstellungen vor.
5. Legen Sie auf der Registerkarte *Sicherheit* die Authentifizierungs- und Verschlüsselungsmethoden fest.
 - Für WPA2 wählen Sie in der Liste *Authentifizierung* den Eintrag *WPA2-Enterprise* und in der Liste *Verschlüsselung* den Eintrag *AES*.
 - Für WPA wählen Sie in der Liste *Authentifizierung* den Eintrag *WPA-Enterprise* und als *Verschlüsselung* entweder *TKIP* oder *AES*. Wählen Sie aber nur dann AES, wenn Ihre Drahtlosclients und Ihre drahtlosen Zugriffspunkte WPA mit AES-Verschlüsselung unterstützen.
6. Wählen Sie in der Dropdownliste *Netzwerkauthentifizierungsmethode auswählen* den EAP-Typ aus.
 - Für EAP-TLS:
 - a. Wählen Sie *Smartcard- oder anderes Zertifikat* und klicken Sie dann auf *Eigenschaften*.
 - b. Nehmen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* nach Bedarf die EAP-TLS-Einstellungen vor und klicken Sie dann auf *OK*. Standardmäßig verwendet EAP-TLS ein Zertifikat auf Registrierungsbasis und überprüft das Serverzertifikat.
 - Für PEAP-MS-CHAP v2 ist keine zusätzliche Konfiguration erforderlich. PEAP-MS-CHAP v2 ist die Standardauthentifizierungsmethode.

Legen Sie nach Bedarf den Authentifizierungsmodus und die anderen Einstellungen fest.

7. Um die erweiterten Einstellungen für 802.1X vorzunehmen, einschließlich der einmaligen Anmeldung (Single Sign-On) und der Einstellungen für den schnellen Wechsel der Zugriffspunkte (Fast Roaming), klicken Sie auf *Erweitert* und nehmen die gewünschten Einstellungen vor. Klicken Sie auf *OK*, wenn Sie fertig sind.
8. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*, um die Änderungen zu speichern.

Für eine neue Windows XP-Drahtlosrichtlinie gehen Sie folgendermaßen vor:

1. Nehmen Sie im Eigenschaftendialogfeld der neu erstellten Windows XP-Drahtlosnetzwerkrichtlinie auf der Registerkarte *Allgemein* die erforderlichen Einstellungen vor.
2. Klicken Sie auf der Registerkarte *Bevorzugte Netzwerke* auf *Hinzufügen*, um ein bevorzugtes Netzwerk hinzuzufügen, und klicken Sie dann auf *Infrastruktur*, um ein Infrastruktur-Drahtlosnetzwerk anzugeben.
3. Geben Sie auf der Registerkarte *Netzwerkeigenschaften* den Namen (die SSID) des Drahtlosnetzwerks und optional eine Beschreibung ein. Legen Sie fest, ob das Netzwerk Broadcasts sendet, und legen Sie dann die Sicherheitsmethoden fest.
 - Für WPA2 wählen Sie in der Dropdownliste *Authentifizierung* den Eintrag *WPA2* und in der Dropdownliste *Verschlüsselung* den Eintrag *AES*.
 - Für WPA wählen Sie in der Dropdownliste *Authentifizierung* den Eintrag *WPA* und in der Dropdownliste *Verschlüsselung* den Eintrag *TKIP*. Wählen Sie aber nur dann AES, wenn Ihre Drahtlosclients und Ihre drahtlosen Zugriffspunkte WPA mit AES-Verschlüsselung unterstützen.
4. Geben Sie auf der Registerkarte *IEEE 802.1X* den EAP-Typ an.
 - Für EAP-TLS:
 - a. Wählen Sie in der Dropdownliste *EAP-Typ* den Eintrag *Smartcard- oder anderes Zertifikat* und klicken Sie dann auf *Einstellungen*.
 - b. Nehmen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* nach Bedarf die EAP-TLS-Einstellungen vor und klicken Sie dann auf *OK*. Standardmäßig verwendet EAP-TLS ein Zertifikat auf Registrierungsbasis und überprüft das Serverzertifikat.
 - Für PEAP-MS-CHAP v2 ist keine zusätzliche Konfiguration erforderlich. PEAP-MS-CHAP v2 ist die Standardauthentifizierungsmethode.
5. Geben Sie auf der Registerkarte *IEEE 802.1X* auch den Authentifizierungsmodus an und nehmen Sie nach Bedarf weitere Einstellungen vor.
6. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*, um die Änderungen zu speichern.



Hinweis Wenn Sie in den Dialogfeldern der *Drahtlosnetzwerkrichtlinien* (IEEE 802.11)-Gruppenrichtlinien-erweiterung Hilfe brauchen, drücken Sie auf die Taste F1.

Wenn Ihre Drahtlosclients mit Windows Server 2008, Windows Vista, Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 das nächste Mal die Computerkonfigurations-Gruppenrichtlinien aktualisieren, werden die Drahtlosnetzwerkeinstellungen aus dem Gruppenrichtlinienobjekt automatisch angewendet.

Konfigurieren und Bereitstellen von Drahtlosprofilen

Sie können Drahtlosclients, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, auch für ein Drahtlosnetzwerk konfigurieren, indem Sie mit dem Befehl `netsh wlan add profile` ein Drahtlosprofil importieren, das im XML-Format vorliegt. Um die XML-Datei mit dem Drahtlosprofil zu erstellen, konfigurieren Sie einen Client, auf dem Windows Vista oder Windows Server 2008 ausgeführt wird, mit allen für ein Drahtlosnetzwerk erforderlichen Einstellungen, einschließlich Authentifizierungsmethode, Verschlüsselungsmethoden und EAP-Typ. Dann exportieren Sie diese Konfiguration mit dem Befehl `netsh wlan export profile` in eine XML-Datei. Sie können ein XML-Profil auch in einer Windows Vista-Drahtlosrichtlinie erstellen, konfigurieren und exportieren.

Manuelles Konfigurieren von Drahtlosclients

Wenn Sie nur eine kleine Anzahl von Drahtlosclients einrichten müssen, können Sie die Verbindungen auf jedem Computer manuell konfigurieren. Auf Drahtlosclients, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird, verwenden Sie den Assistenten für drahtlose Netzwerke oder den Assistenten für Netzwerkverbindungen. Auf Drahtlosclients, auf denen Windows XP mit SP2 ausgeführt wird, verwenden Sie den Assistenten für neue Verbindungen. Die folgenden Abschnitte beschreiben, wie Sie die Authentifizierungsmethoden EAP-TLS, PEAP-TLS und PEAP-MS-CHAP v2 auf drahtlosen Windows-Clients konfigurieren können.

EAP-TLS

Um manuell eine EAP-TLS-Authentifizierung auf einem Drahtlosclient zu konfigurieren, auf dem Windows Server 2008 oder Windows Vista ausgeführt wird, gehen Sie folgendermaßen vor:

1. Klicken Sie im Netzwerk- und Freigabecenter auf die Aufgabe *Drahtlosnetzwerke verwalten*. Klicken Sie im Fenster *Drahtlosnetzwerke verwalten* mit einem Doppelklick auf den Namen Ihres Drahtlosnetzwerks.
2. Wählen Sie auf der Registerkarte *Sicherheit* in der Dropdownliste *Sicherheitsstyp* den Typ *WPA-Enterprise* oder *WPA2-Enterprise*. Wählen Sie in der Dropdownliste *Wählen Sie eine Methode für die Netzwerkauthentifizierung aus* den Eintrag *Smartcard- oder anderes Zertifikat* und klicken Sie dann auf *Einstellungen*.
3. Um ein Benutzerzertifikat zu verwenden, das in die Registrierung eingetragen wurde, wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* die Option *Zertifikat auf diesem Computer verwenden*. Für ein Benutzerzertifikat, das auf der Smartcard gespeichert wurde, wählen Sie *Eigene Smartcard verwenden*.

Wenn Sie das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der NPS-Server angeben möchten, die die TLS-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Um manuell eine EAP-TLS-Authentifizierung auf einem Drahtlosclient zu konfigurieren, auf dem Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 ausgeführt wird, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der Drahtlosverbindung. Klicken Sie auf der Registerkarte *Drahtlosnetzwerke* in der Liste *Bevorzugte Netzwerke* auf den Namen des gewünschten Netzwerks und klicken Sie dann auf *Eigenschaften*.

2. Wählen Sie auf der Registerkarte *Authentifizierung* das Kontrollkästchen *Netzwerkzugriffsteuerung mit IEEE 802.1X aktivieren* und den EAP-Typ *Smartcard- oder anderes Zertifikat*. Das ist die Standardeinstellung.
3. Klicken Sie auf *Eigenschaften*. Wenn Sie ein Benutzerzertifikat verwenden möchten, das in die Registrierung eingetragen wurde, wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* die Option *Zertifikat auf diesem Computer verwenden*. Falls Sie ein Benutzerzertifikat verwenden, das auf der Smartcard gespeichert wurde, wählen Sie *Eigene Smartcard verwenden*.

Wenn Sie das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Falls Sie die Namen der Authentifizierungsserver angeben möchten, die die TLS-Authentifizierung durchführen sollen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein.

4. Klicken Sie auf *OK*, um die Änderungen am EAP-Typ *Smartcard- oder anderes Zertifikat* zu speichern.

PEAP-TLS

Um manuell eine PEAP-TLS-Authentifizierung auf einem Drahtlosclient zu konfigurieren, auf dem Windows Server 2008 oder Windows Vista ausgeführt wird, gehen Sie folgendermaßen vor:

1. Klicken Sie im Netzwerk- und Freigabecenter auf die Aufgabe *Drahtlosnetzwerke verwalten*. Klicken Sie im Fenster *Drahtlosnetzwerke verwalten* mit einem Doppelklick auf den Namen Ihres Drahtlosnetzwerks.
2. Wählen Sie auf der Registerkarte *Sicherheit* in der Dropdownliste *Sicherheitstyp* den Typ *WPA-Enterprise* oder *WPA2-Enterprise*. In *Wählen Sie eine Methode für die Netzwerkauthentifizierung aus* wählen Sie *Geschütztes EAP (PEAP)* und klicken dann auf *Einstellungen*.
3. Wenn Sie das Computerzertifikat des NPS-Servers für die PEAP-Authentifizierung überprüfen möchten, wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP* das Kontrollkästchen *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der NPS-Server angeben möchten, die die PEAP-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben die Namen ein.
4. Klicken Sie in der Dropdownliste *Authentifizierungsmethode auswählen* auf *Smartcard- oder anderes Zertifikat*. Klicken Sie auf *Konfigurieren*. Wenn Sie ein Benutzerzertifikat verwenden möchten, das in die Registrierung eingetragen wurde, wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* die Option *Zertifikat auf diesem Computer verwenden*. Für ein Benutzerzertifikat, das auf der Smartcard gespeichert wurde, wählen Sie *Eigene Smartcard verwenden*. Wenn Sie bei der Benutzerauthentifizierung das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie das Kontrollkästchen *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der NPS-Server angeben möchten, die die TLS-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein.
5. Klicken Sie auf *OK*, um die Änderungen am PEAP-Typ *Smartcard- oder anderes Zertifikat* zu speichern. Klicken Sie auf *OK*, um die Änderungen am Typ *Geschütztes EAP* zu speichern. Klicken Sie auf *OK*, um die Eigenschaften der Drahtlosnetzwerkconfiguration zu speichern.
6. Schließen Sie alle drei geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Um manuell eine PEAP-TLS-Authentifizierung auf einem Drahtlosclient zu konfigurieren, auf dem Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 ausgeführt wird, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der Drahtlosverbindung. Klicken Sie auf der Registerkarte *Drahtlosnetzwerke* in der Liste *Bevorzugte Netzwerke* auf den Namen des gewünschten Netzwerks und klicken Sie dann auf *Eigenschaften*. Das Eigenschaftendialogfeld des eingetragenen Drahtlosnetzwerks öffnet sich.
2. Wählen Sie auf der Registerkarte *Authentifizierung* das Kontrollkästchen *Netzwerkzugriffsteuerung mit IEEE 802.1X aktivieren* und den EAP-Typ *Geschütztes EAP (PEAP)*.
3. Klicken Sie auf *Eigenschaften*. Wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP* das Kontrollkästchen *Serverzertifikat überprüfen*, um bei der PEAP-Authentifizierung das Computerzertifikat des NPS-Servers zu überprüfen (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der Server angeben möchten, die die PEAP-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein. Klicken Sie in der Dropdownliste *Authentifizierungsmethode auswählen* auf *Smartcard- oder anderes Zertifikat*.
4. Klicken Sie auf *Konfigurieren*. Wenn Sie ein Benutzerzertifikat verwenden möchten, das in die Registrierung eingetragen wurde, wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* die Option *Zertifikat auf diesem Computer verwenden*. Verwenden Sie dagegen ein Benutzerzertifikat, das auf der Smartcard gespeichert wurde, wählen Sie *Eigene Smartcard verwenden*.

Wenn Sie bei der Benutzerauthentifizierung das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie das Kontrollkästchen *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der NPS-Server angeben möchten, die die TLS-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein.

5. Klicken Sie auf *OK*, um die Änderungen am PEAP-Typ *Smartcard- oder anderes Zertifikat* zu speichern. Klicken Sie auf *OK*, um die Änderungen am Typ *Geschütztes EAP* zu speichern. Klicken Sie auf *OK*, um die Eigenschaften der Drahtlosnetzwerkkonfiguration zu speichern.
6. Schließen Sie alle geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

PEAP-MS-CHAP v2

Um manuell eine PEAP-MS-CHAP v2-Authentifizierung auf einem Drahtlosclient zu konfigurieren, auf dem Windows Server 2008 oder Windows Vista ausgeführt wird, gehen Sie folgendermaßen vor:

1. Klicken Sie im Netzwerk- und Freigabecenter auf die Aufgabe *Drahtlosnetzwerke verwalten*. Klicken Sie im Fenster *Drahtlosnetzwerke verwalten* mit einem Doppelklick auf den Namen Ihres Drahtlosnetzwerks.
2. Wählen Sie auf der Registerkarte *Sicherheit* in der Dropdownliste *Sicherheitstyp* den Typ *WPA-Enterprise* oder *WPA2-Enterprise*. Wählen Sie in der Dropdownliste *Wählen Sie eine Methode für die Netzwerkauthentifizierung* aus den Eintrag *Geschütztes EAP (PEAP)* und klicken Sie dann auf *Einstellungen*.
3. Wenn Sie das Computerzertifikat des NPS-Servers für die PEAP-Authentifizierung überprüfen möchten, wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP* das Kontrollkästchen *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der NPS-Server angeben möchten, die die PEAP-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben die Namen ein.

4. Wählen Sie in *Authentifizierungsmethode auswählen* den Eintrag *Gesichertes Kennwort (EAP-MS-CHAP v2)* und schließen Sie dann die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Um manuell eine PEAP-MS-CHAP v2-Authentifizierung auf einem Drahtlosclient zu konfigurieren, auf dem Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 ausgeführt wird, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der Drahtlosverbindung. Klicken Sie auf der Registerkarte *Drahtlosnetzwerke* in der Liste *Bevorzugte Netzwerke* auf den Namen des gewünschten Netzwerks und klicken Sie dann auf *Eigenschaften*. Das Eigenschaftendialogfeld des eingetragenen Drahtlosnetzwerks öffnet sich.
2. Wählen Sie auf der Registerkarte *Authentifizierung* das Kontrollkästchen *Netzwerkzugriffsteuerung mit IEEE 802.1X aktivieren* und den PEAP-Typ *Geschütztes EAP (PEAP)*.
3. Klicken Sie auf *Eigenschaften*. Wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP* das (standardmäßig aktivierte) Kontrollkästchen *Serverzertifikat überprüfen*, damit das Computerzertifikat des NPS-Servers überprüft wird. Wenn Sie die Namen der Authentifizierungsserver angeben möchten, die die Authentifizierung durchführen sollen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben die Namen ein. Klicken Sie unter *Authentifizierungsmethode wählen* auf *Gesichertes Kennwort (EAP-MSCHAP v2)* und schließen Sie dann die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Wartung

Für Drahtlosnetzwerke fallen in folgenden Bereichen Wartungsarbeiten an:

- Verwalten von Benutzer- und Computerkonten
- Verwalten von drahtlosen Zugriffspunkten
- Aktualisieren von Drahtlosprofilen

Verwalten der Benutzer- und Computerkonten

Wenn in Active Directory ein neues Benutzer- oder Computerkonto eingerichtet wird und diesem Benutzer- oder Computerkonto der Drahtloszugriff erlaubt werden soll, fügen Sie das neue Konto zur entsprechenden, für Drahtlosverbindungen vorgesehenen Gruppe hinzu. Fügen Sie das neue Konto zum Beispiel zur Sicherheitsgruppe *Drahtloskonten* hinzu, die Sie zu diesem Zweck definiert und in den Netzwerkrichtlinien für Drahtlosverbindungen angegeben haben.

Wenn Benutzer- oder Computerkonten in Active Directory gelöscht werden, sind keine weiteren Maßnahmen mehr erforderlich, um zu verhindern, dass mit diesen Konten Drahtlosverbindungen hergestellt werden können.

Bei Bedarf können Sie zusätzliche universelle Gruppen und Netzwerkrichtlinien erstellen, um Drahtloszugriffe für unterschiedliche Benutzergruppen einzurichten. Sie können zum Beispiel eine globale Gruppe *AuftragnehmerMitDrahtloszugriff* einrichten, die den Mitgliedern der Gruppe *AuftragnehmerMitDrahtloszugriff* nur während der üblichen Bürozeiten oder für spezielle Intranetressourcen den drahtlosen Zugriff ermöglicht.

Verwalten der drahtlosen Zugriffspunkte

Nach ihrer Bereitstellung erfordern drahtlose Zugriffspunkte kaum Wartungsarbeiten. Der größte Teil der Änderungen an der Konfiguration von drahtlosen Zugriffspunkten ist eine Folge von Kapazitätsanpassungen oder Änderungen in der Infrastruktur des Netzwerks.

Hinzufügen eines drahtlosen Zugriffspunkts

Um einen drahtlosen Zugriffspunkt zum Netzwerk hinzuzufügen, gehen Sie folgendermaßen vor:

1. Befolgen Sie die in diesem Kapitel unter »Bereitstellen drahtloser Zugriffspunkte« beschriebenen Planungs- und Bereitstellungsschritte, um einen neuen drahtlosen Zugriffspunkt zu Ihrem Drahtlosnetzwerk hinzuzufügen.
2. Fügen Sie den drahtlosen Zugriffspunkt als einen RADIUS-Client zu Ihren NPS-Servern hinzu.

Entfernen eines drahtlosen Zugriffspunkts

Wenn Sie einen drahtlosen Zugriffspunkt entfernen, entfernen Sie den drahtlosen Zugriffspunkt auch als RADIUS-Client aus der Konfiguration Ihres NPS-Servers.

Konfiguration von Änderungen in NPS-Servern

Wenn sich bei den NPS-Servern Änderungen ergeben, weil zum Beispiel ein NPS-Server aus dem Intranet entfernt oder zum Intranet hinzugefügt wird, tun Sie Folgendes:

1. Sorgen Sie dafür, dass die drahtlosen Zugriffspunkte auf neuen NPS-Servern als RADIUS-Clients eingetragen sind und dass die entsprechenden Netzwerkrichtlinien für den Drahtloszugriff eingestellt sind.
2. Aktualisieren Sie bei Bedarf die Konfiguration der drahtlosen Zugriffspunkte, damit die neue Serverkonfiguration entsprechend berücksichtigt wird.

Aktualisieren von XML-Drahtlosprofilen

Zur Aktualisierung von XML-Drahtlosprofilen und zur Anwendung der aktualisierten Profile auf Ihre Windows Vista- oder Windows Server 2008-Drahtlosclients gehen Sie folgendermaßen vor:

1. Wenn Sie einen Windows Vista- oder Windows Server 2008-Drahtlosclient verwenden oder eine Windows Vista-Drahtlosrichtlinie erstellt haben, erstellen Sie im Gruppenrichtlinienverwaltungs-Editor oder mit dem Befehl `netsh wlan export profile` das aktualisierte XML-Drahtlosprofil.
2. Führen Sie auf Ihren Drahtlosclients in einem Skript den Befehl `netsh wlan add profile` aus, um das XML-Drahtlosprofil auf Ihren Drahtlosclients zu importieren, oder importieren Sie es mit einer anderen Methode.

Problembehandlung

Wegen der Vielzahl an Komponenten und Vorgängen kann die Behebung von Problemen mit drahtlosen Verbindungen schwierig werden. Dieser Abschnitt beschreibt folgende Aspekte:

- Die Tools, die Windows Server 2008 und Windows Vista zur Behebung von Problemen mit drahtlosen Verbindungen bereitstellen
- Die Behebung von Verbindungsproblemen auf Drahtlosclients
- Die Behebung von Verbindungsproblemen auf drahtlosen Zugriffspunkten
- Die Behebung von Problemen mit Drahtlosverbindungen auf NPS-Servern

Direkt von der Quelle: Tipps zur Behebung von Problemen mit drahtlosen Verbindungen

Einer der schwierigsten Aspekte bei der Behebung von Problemen in drahtlosen Netzwerken ist es, den richtigen Anfang zu finden. Gewöhnlich zeigen sich die Symptome zwar auf dem Client, aber er ist nur ein Teil in einer Kette von Geräten und Technologien, die versagen können.

Wenn ein Drahtlosclient das gewünschte Drahtlosnetzwerk nicht sieht oder keine Verbindung (*association* oder Zuordnung) mit einem drahtlosen Zugriffspunkt herstellen kann, liegt das Problem irgendwo zwischen Client und Zugriffspunkt. Die meisten dieser Probleme lassen sich durch eine Aktualisierung der Treiber oder Firmware des Drahtlosnetzwerkadapters und des Zugriffspunkts lösen. Die Installation der aktuellsten Treiber und Firmware ist also der unvermeidliche erste Schritt zur Problembehebung.

Schlägt die Authentifizierung fehl, liegt dies normalerweise nicht an Hardwareproblemen. Überprüfen Sie zuerst die Systemereignisprotokolle auf der Clientseite. Windows XP und Windows Server 2003 führen zwar keine Protokolle, die speziell für die Diagnose von Problemen vorgesehen sind, aber Windows Server 2008 und Windows Vista zeichnen einige recht nützliche Daten auf, die Ihnen Hinweise auf Konfigurationsprobleme geben können, beispielsweise auf ein fehlendes Zertifikat.

Nach der Überprüfung dieser Protokolle sollten Sie auf dem NPS-Server das Protokoll *Windows-Protokolle\Sicherheit* überprüfen. Wenn eine Authentifizierung fehlgeschlagen ist, wird es einen NPS-Ereigniseintrag mit dem Schlüsselwort *Überwachungsfehler* (Audit Failure) geben. Wenn Sie aber keine Protokolleinträge vorfinden, die im Zusammenhang mit einer versuchten Authentifizierung im Drahtlosnetzwerk stehen, ist dies ein deutlicher Hinweis darauf, dass der NPS-Server keine Authentifizierungsanfrage erhalten hat oder dass der Vorgang die vorgesehenen Zeitgrenzen überschritten hat. Sehen Sie sich den drahtlosen Zugriffspunkt genau an und überprüfen Sie, ob seine RADIUS-Einstellungen zum NPS-Server passen.

*Clay Seymour, Support Escalation Engineer
Enterprise Platform Support*

Problembehandlungstools von Windows für Drahtlosnetzwerke

Microsoft bietet folgende Programme zur Unterstützung der Problembehandlung bei drahtlosen Netzwerken an:

- TCP/IP-Problembehandlungstools
- Den Ordner *Netzwerkverbindungen*
- Netsh wlan-Befehle
- Netzwerkdiagnoseframework-Unterstützung für Drahtlosverbindungen
- Drahtlos-Diagnose-Ablaufverfolgung
- NPS-Authentifizierungs- und -Kontoführungsprotokolle
- NPS-Ereignisprotokollierung
- SChannel-Protokollierung
- SNMP-Agent
- Zuverlässigkeits- und Leistungsüberwachungs-Snap-In
- Network Monitor 3.1

TCP/IP-Problembehandlungstools

Die Programme Ping, Tracert und Pathping verwenden die ICMP-Nachrichten Echo und Echo Reply sowie die ICMPv6-Nachrichten Echo Request und Echo Reply, um Verbindungen zu überprüfen, den Pfad zu einem Ziel anzuzeigen und die Pfadintegrität zu überprüfen (ICMP bedeutet Internet Control Message Protocol). Mit dem Programm Route lassen sich die IPv4- und IPv6-Routingtabellen anzeigen. Das Programm Nslookup kann bei der Behebung von Problemen mit der DNS-Namensauflösung (Domain Name System) verwendet werden.

Der Ordner *Netzwerkverbindungen*

Im Ordner *Netzwerkverbindungen* können Sie das Eigenschaftendialogfeld einer drahtlosen Verbindung öffnen und ihren Status überprüfen, beispielsweise ihre TCP/IP-Konfiguration.

Wurde dem Drahtlosnetzwerkadapter eine APIPA-Adresse (Automatic Private IP Addressing) im Bereich 169.254.0.0/16 oder die konfigurierte alternative Konfiguration zugewiesen, verfügt der Drahtlosclient zwar immer noch über eine Verbindung (eine Zuordnung oder Assoziation) mit dem drahtlosen Zugriffspunkt, aber entweder ist die Authentifizierung fehlgeschlagen oder der DHCP-Server ist nicht verfügbar. Schlägt die Authentifizierung fehl und ist die Zuordnung noch gültig, dann ist der drahtlose Zugriffspunkt aktiviert und TCP/IP führt die normale Konfigurierung durch. Ist kein DHCP-Server verfügbar (authentifiziert oder nicht), weist Windows Vista automatisch eine APIPA-Adresse zu, sofern keine alternative Adresse eingestellt wurde.

Direkt von der Quelle: APIPA in Windows Vista

Vielleicht ist Ihnen schon aufgefallen, dass drahtlose Windows Vista-Clients schneller oder häufiger eine automatische APIPA-Adresse zuweisen als ältere Windows-Versionen. Ein Computer, auf dem Windows Vista ausgeführt wird, wartet nur sechs Sekunden auf die Antwort eines DHCP-Servers, bevor er eine APIPA-Adresse verwendet, und versucht dann weiterhin, Kontakt zu einem DHCP-Server aufzunehmen. Im Gegensatz dazu wartet ein Windows-XP-Computer eine volle Minute, bevor er auf eine APIPA-Adresse zurückgreift. Diese Verhaltensänderung wurde absichtlich eingeführt und soll Ad-hoc-Verbindungen erleichtern, bei denen gewöhnlich keine DHCP-Server verfügbar sind.

*Tim Quinn, Support Escalation Engineer
Enterprise Platform Support*

Netsh Wlan-Befehle

Um Informationen zur Behebung von Problemen mit Drahtlosverbindungen zu sammeln, können Sie folgende netsh wlan-Befehle eingeben:

- **netsh wlan show autoconfig** Zeigt an, ob die automatische Konfigurationslogik aktiviert wurde
- **netsh wlan show blockednetworks** Zeigt an, ob in der Liste der verfügbaren Netzwerke auch blockierte Netzwerke sichtbar sind
- **netsh wlan show createalluserprofile** Zeigt an, ob jeder ein Profil für alle Benutzer erstellen darf
- **netsh wlan show drivers** Zeigt die Eigenschaften der Treiber der installierten Drahtlosnetzwerkadapter an
- **netsh wlan show filters** Zeigt die Listen mit den zugelassenen und abgelehnten (blockierten) Netzwerken an

- **netsh wlan show interfaces** Zeigt die Eigenschaften der installierten Drahtlosnetzwerkadapter an
- **netsh wlan show networks** Zeigt eine Liste mit den Eigenschaften der verfügbaren Drahtlosnetzwerken an
- **netsh wlan show profiles** Zeigt eine Liste der Gruppenrichtlinien und lokalen Drahtlosnetzwerkprofilen an
- **netsh wlan show settings** Zeigt die globalen Drahtlosnetzwerkeinstellungen, beispielsweise den Status der automatischen WLAN-Konfiguration, und ob jeder Benutzer ein Profil für alle Benutzer erstellen darf
- **netsh wlan show tracing** Zeigt den Status der Drahtlosablaufverfolgung und den Speicherort der Ablaufverfolgungsprotokolle (standardmäßig `%SystemRoot%\Tracing\Wireless`)
- **netsh wlan show all** Zeigt alle verfügbaren Informationen über Drahtlosnetzwerkadapter und über die verfügbaren Drahtlosnetzwerke

Netzwerkdiagnoseframework-Unterstützung für Drahtlosverbindungen

Um dem Benutzer den Umgang mit Verbindungsproblemen zu erleichtern, enthält Windows Vista ein Netzwerkdiagnoseframework (NDF). Es setzt sich aus verschiedenen Technologien, Richtlinien und Hilfsklassen zusammen, die den Benutzer bei der Diagnose unterstützen und eine automatische Korrektur des Problems durchführen, sofern dies möglich ist. Wenn ein Benutzer unter Windows Vista Probleme mit Netzwerkverbindungen hat, bietet das Netzwerkdiagnoseframework ihm die Möglichkeit, das Problem im aktuellen Kontext zu diagnostizieren und zu reparieren. Das bedeutet, dass die Diagnose- und Lösungsanweisungen dem Benutzer in der Anwendung oder in dem Dialogfeld angezeigt werden, in dem das Problem aufgetreten ist, oder im Zusammenhang mit der fehlgeschlagenen Netzwerkoperation.

Windows Vista enthält auch eine Hilfsklasse für die Untersuchung von fehlgeschlagenen Verbindungsversuchen in Drahtlosnetzwerken. Wenn eine Drahtlosverbindung fehlschlägt, zeigt Windows ein Dialogfeld mit Informationen über den Fehler an. Das Dialogfeld weist auch eine *Diagnose-Schaltfläche* auf, mit der das NDF-Problembehandlungstool für Drahtlosnetzwerke gestartet wird. In der Diagnosesitzung kann der Benutzer bestimmte Verbindungsprobleme beheben, ohne die IT-Abteilung zu bemühen. Das NDF-Problembehandlungstool kann dem Benutzer bei vielen Problemen behilflich sein, die sich in Drahtlosnetzwerken ergeben können, wie zum Beispiel:

- Das Funksignal des Netzwerkadapters wurde abgeschaltet.
- Der drahtlose Zugriffspunkt wird nicht mit Strom versorgt.
- Eine fehlende oder abweichende Einstellung der Sicherheitsoptionen, Verschlüsselungstypen oder Netzwerkschlüssel zwischen dem drahtlosen Zugriffspunkt und den Drahtlosclients
- Kabelverbindungen wurden getrennt.
- Zertifikate fehlen.

Windows protokolliert alle Verbindungsversuche, die im Drahtlosnetzwerk stattfinden, im Systemereignisprotokoll. Wenn die Windows-Netzwerkdiagnose ausgeführt wird, bewirkt sie im Systemereignisprotokoll zusätzliche Einträge mit folgenden Informationen:

- Der Name des Drahtlosnetzwerkadapters und die Eignung des Treibers für Windows Vista
- Eine Liste der sichtbaren Drahtlosnetzwerke mit Signalstärken, Kanälen, Protokollen (wie 802.11b oder 802.11g) und Betriebsmodi (Ad-hoc oder Infrastruktur)
- Die Liste der bevorzugten Netzwerke und die Konfiguration jedes Netzwerks

- Die Diagnoseergebnisse, beispielsweise »Die Drahtlosverbindung auf diesem Computer scheint ordnungsgemäß zu funktionieren«, »Möglicherweise funktioniert die Internetverbindung auf dem Drahtlosrouter oder dem Zugriffspunkt nicht ordnungsgemäß« oder »Dieser Computer hat eine niedrige Signalstärke von ContosoWLAN«.
- Die Reparaturoption, die dem Benutzer angezeigt wurde, wie zum Beispiel »Bewegen Sie den Computer an eine andere Position, um mögliche Störquellen auszuschalten. Versuchen Sie dann erneut, eine Verbindung mit ContosoWLAN herzustellen«.
- Die Reparaturoptionen, die der Benutzer gewählt hat, und das Ergebnis des Reparaturversuchs.

Sie können diese Ereignisprotokolleinträge im Ereignisanzeige-Snap-In überprüfen, um sich ein genaueres Bild von der Netzwerkumgebung zu dem Zeitpunkt zu machen, an dem das Problem auftrat, ohne diese Situation wieder herbeiführen zu müssen. Außerdem sind Sie nicht mehr so stark darauf angewiesen, aus den Beschreibungen der Benutzer die richtigen Schlüsse zu ziehen.

Um zusätzliche Informationen über den Ablauf der Verbindungsversuche und anderer Netzwerkvorgänge übersichtlicher präsentieren zu können, erstellt Windows ein separates Diagnoseprotokoll.

So greifen Sie auf das Diagnoseprotoll zu

1. Erweitern Sie in der Strukturansicht des Ereignisanzeige-Snap-Ins den Knoten *Anwendungs- und Dienstprotokolle\Microsoft\Windows\Diagnostics-Networking*.
2. Klicken Sie auf *Operational*.
3. Überprüfen Sie im Detailbereich die Ereigniseinträge für die Drahtlosdiagnosesitzung.

Drahtlos-Diagnose-Ablaufverfolgung

Von Zeit zu Zeit müssen Sie sich mit einem Drahtlosnetzwerkproblem vielleicht an Microsoft oder an Supportspezialisten aus Ihrem Haus wenden. Für eine genaue Analyse brauchen Microsoft oder Ihre Supportspezialisten ausführliche Informationen über den Zustand des Computers und der Drahtloskomponenten von Windows, sowie über ihre Interaktionen beim Auftreten des Problems. Diese Informationen erhalten Sie unter Windows Vista von der Drahtlos-Diagnose-Ablaufverfolgung. Um die Drahtlos-Diagnose-Ablaufverfolgung zu verwenden, müssen Sie die Ablaufverfolgung aktivieren, das Problem reproduzieren, die Ablaufverfolgung beenden und dann den Ablaufbericht speichern.

Die Drahtlos-Diagnose-Ablaufverfolgung können Sie auf eine der folgenden Weisen starten:

- Geben Sie in einer Eingabeaufforderung den Befehl `netsh wlan set tracing mode=yes`.
- Erweitern Sie in der Strukturansicht des Snap-Ins Zuverlässigkeits- und Leistungsüberwachung den Knoten *Sammlungssätze\System*. Klicken Sie mit der rechten Maustaste auf *Wireless Diagnostics (Drahtlos-Diagnose)* und klicken dann auf *Starten*.

Nachdem Sie das Problem reproduziert haben, können Sie die Drahtlos-Diagnose-Ablaufverfolgung auf eine der folgenden Weisen beenden:

- Geben Sie in einer Eingabeaufforderung den Befehl `netsh wlan set tracing mode=no` ein.
- Erweitern Sie in der Strukturansicht des Snap-Ins Zuverlässigkeits- und Leistungsüberwachung den Knoten *Sammlungssätze\System*. Klicken Sie mit der rechten Maustaste auf *Wireless Diagnostics (Drahtlos-Diagnose)* und klicken Sie dann auf *Anhalten*.



Hinweis Es ist wichtig, dass Sie die Drahtlos-Diagnose-Ablaufverfolgung anhalten, bevor Sie die Ablaufprotokolle überprüfen oder in ein lesbares Format konvertieren.

Wenn Sie den Bericht einsehen möchten, den die Drahtlos-Diagnose-Ablaufverfolgung erstellt hat,

erweitern Sie in der Strukturansicht des Snap-Ins Zuverlässigkeits- und Leistungsüberwachung den Knoten *Berichte\System\Wireless Diagnostics*.

Der Bericht bietet folgende Informationen:

- Drahtlosnetzwerkconfiguration einschließlich zugelassener und abgelehnter (blockierter) Drahtlosnetzwerke
- Die aktuelle TCP/IP-Konfiguration (einschließlich der Informationen, die der Befehl `Ipconfig /all` liefert)
- Eine Liste mit allen Verbindungsversuchen und ausführliche Informationen über jeden Schritt des Verbindungsvorgangs
- Eine ausführliche Liste aller Windows-Netzwerkdiagnoseereignisse
- Die Zertifikatkonfiguration des Drahtlosclients
- Drahtlosnetzwerkprofile und ihre Speicherorte
- Informationen über die Drahtlosnetzwerkadapertreiber
- Systemdateien für Drahtlosnetzwerke und Versionsangaben
- Rohdaten der Netzwerkablaufverfolgung
- Computerfabrikat und -modell
- Betriebssystemversion
- Eine Liste aller Dienste, ihrer aktuellen Zustände und ihrer Prozesskennungen

Dieser Bericht und die dazugehörigen Dateien werden standardmäßig im Ordner *%SystemRoot%\Tracing\Wireless* gespeichert.

Zusätzlich zur Ablaufverfolgung in drahtlosen Netzwerken unterstützen Windows Server 2008 und Windows Vista die Ablaufverfolgung für Komponenten der RAS-Verbindungsverwaltung und der Routing- und RAS-Dienste, die auch für Drahtlosverbindungen verwendet werden. Wie bei Drahtlosnetzwerken liefert eine Ablaufverfolgung für diese Komponenten Informationen, mit denen Sie komplexe Probleme mit bestimmten Komponenten beheben können. Die Informationen aus diesen zusätzlichen Ablaufverfolgungsdateien sind gewöhnlich nur für Microsoft-Supportmitarbeiter von Nutzen, von denen Sie bei der Bearbeitung eines Supportproblems vielleicht darum gebeten werden, Ablaufprotokolldateien für einen Verbindungsversuch zu erstellen. Diese zusätzliche Ablaufverfolgung können Sie mit dem Programm `Netsh` aktivieren.

Der Befehl zur Aktivierung oder Deaktivierung der Ablaufverfolgung für eine bestimmte Komponente der RAS-Verbindungsverwaltung und der Routing- und RAS-Dienste lautet:

```
netsh ras diagnostics set rastracing Komponente enabled|disabled
```

Darin ist *Komponente* eine Komponente aus der Liste, die in der Registrierung unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing* zu finden ist.

Der Befehl für die Aktivierung der Ablaufverfolgung für alle Komponenten lautet:

```
netsh ras diagnostics set rastracing * enabled
```

Mit folgendem Befehl lässt sich die Ablaufverfolgung für alle Komponenten deaktivieren:

```
netsh ras diagnostics set rastracing * disabled
```

Die Ablaufprotokolldateien werden im Ordner *%SystemRoot%\Tracing* gespeichert. Für die Drahtlosauthentifizierung sind folgende Protokolldateien am interessantesten:

- **Svchost_rastls.log** TLS-Authentifizierungsaktivitäten
- **Svchost_raschap.log** MS-CHAP v2-Authentifizierungsaktivitäten

NPS-Authentifizierungs- und -Kontoführungsprotokolle

Standardmäßig unterstützt NPS die Protokollierung von Authentifizierungs- und Kontoführungsdaten für Drahtlosverbindungen in lokalen Protokolldateien. Diese Protokollierung erfolgt getrennt von den Ereignissen, die unter *Windows-Protokolle/Sicherheit* aufgezeichnet werden. Sie können die Informationen aus den Protokollen verwenden, um die Benutzung des Drahtlosnetzwerks und die Authentifizierungsversuche zu überwachen. Eine Authentifizierungs- und Kontoführungsprotokollierung ist besonders zur Behebung von Problemen nützlich, die sich durch Netzwerkrichtlinien ergeben können. Für jeden Authentifizierungsversuch wird der Name der Netzwerkrichtlinie aufgezeichnet, die den Verbindungsversuch zugelassen oder abgelehnt hat. Die Einstellungen für die Authentifizierungs- und Kontoführungsprotokollierung können Sie im Knoten *Kontoführung* des Snap-Ins Netzwerkrichtlinienserver vornehmen.

Die Authentifizierungs- und Kontoführungsdaten werden in einer oder mehreren konfigurierbaren Protokolldateien im Ordner *%SystemRoot%\System32\LogFiles* gespeichert. Die Protokolldateien werden im IAS-Format (Internet Authentication Service) oder in einem datenbankkompatiblen Format gespeichert. Das bedeutet, dass ein Datenbankprogramm die Protokolldateien direkt zur Analyse einlesen kann. NPS kann die Authentifizierungs- und Kontoführungsinformationen auch an eine SQL Server-Datenbank senden.

NPS-Ereignisprotokollierung

Überprüfen Sie auf dem NPS-Server das Protokoll *Windows-Protokolle\Sicherheit* auf abgewiesene (Ereignis-ID 6273) oder zugelassene (Ereignis-ID 6272) Verbindungsversuche. NPS-Ereignisprotokolleinträge enthalten viele Informationen über den Verbindungsversuch. Darunter sind auch der Name der Verbindungsanforderungsrichtlinie, die für den Verbindungsversuch verwendet wurde (der *Proxyrichtliniename* in der Beschreibung des Ereignisses), und die Netzwerkrichtlinie, die den Verbindungsversuch zugelassen oder abgelehnt hat (das Feld *Netzwerkrichtliniename* in der Beschreibung des Ereignisses). Die NPS-Ereignisprotokollierung für zugelassene oder abgelehnte Verbindungsversuche ist standardmäßig aktiviert. Sie können sie im Netzwerkrichtlinienserver-Snap-In konfigurieren, und zwar auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds des NPS-Servers.

NPS-Ereignisse lassen sich im Ereignisanzeige-Snap-In anzeigen. Die Überprüfung der NPS-Ereigniseinträge im Protokoll *Windows-Protokolle/Sicherheit* ist eine der wichtigsten Methoden, um Informationen über fehlgeschlagene Authentifizierungen zu erhalten.

SChannel-Protokollierung

Eine SChannel-Protokollierung (Secure Channel) bedeutet die Aufzeichnung von Informationen über SChannel-Ereignisse im Systemereignisprotokoll. Standardmäßig werden nur SChannel-Fehlermeldungen aufgezeichnet. Um Informationen über Fehler, Warnungen, Informationen und Erfolgsmeldungen zu erhalten, stellen Sie den Registrierungswert *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging* auf **4** (es ist ein DWORD-Wert). Wenn die SChannel-Protokollierung alle Ereignisse aufzeichnet, ist es möglich, mehr Informationen über den Zertifikataustausch und den Überprüfungsvorgang auf dem NPS-Server zu erhalten.

SNMP-Agent

Sie können die SNMP-Agentensoftware (Simple Network Management Protocol) von Windows Server 2008 verwenden, um in einer SNMP-Konsole Statusinformationen über Ihre NPS-Server zu erhalten. NPS unterstützt die RADIUS Authentication Server MIB (RFC 2619, MIB bedeutet Management

Information Base) und die RADIUS Accounting Server MIB (RFC 2621). Installieren Sie den optionalen SNMP-Dienst als Feature mit dem Server-Manager.

Der SNMP-Dienst kann in Zusammenarbeit mit Ihrer vorhandenen Netzwerkverwaltungsinfrastruktur auf SNMP-Basis dazu verwendet werden, NPS-RADIUS-Server oder -Proxys zu überwachen.

Zuverlässigkeits- und Leistungsüberwachungs-Snap-In

Sie können das Zuverlässigkeits- und Leistungsüberwachungs-Snap-In verwenden, um Leistungsindikatoren zu überwachen, Protokolle zu erstellen und für bestimmte NPS-Komponenten und Programmprozesse Schwellenwerte für Warnungen festzulegen. Sie können die Diagramme und Berichte auch zur Identifizierung von potenziellen Problemen, zur Behebung von vorhandenen Problemen und zur Effizienzprüfung der NPS-Server verwenden.

Mit dem Zuverlässigkeits- und Leistungsüberwachungs-Snap-In können Sie die Leistungsindikatoren von folgenden NPS-Leistungsobjekten überwachen:

- NPS-Kontoführungsclients
- NPS-Kontoführungsproxy
- NPS-Kontoführungsserver
- NPS-Authentifizierungsclients
- NPS-Authentifizierungsproxy
- NPS-Authentifizierungsserver
- NPS-Richtlinienmodul
- NPS-Remotekontoführungsserver
- NPS-Remoteauthentifizierungsserver



Weitere Informationen Weitere Informationen über die Verwendung des Zuverlässigkeits- und Leistungsüberwachungs-Snap-Ins finden Sie im Hilfe- und Supportcenter von Windows Server 2008.

Network Monitor 3.1

Sie können den Microsoft Network Monitor 3.1 (oder höher) oder einen kommerziellen Paketanalytiker (solche Programme werden auch *Netzwerk-Sniffer* genannt) verwenden, um die Authentifizierungen und Datenübertragungen zu untersuchen, die im Netzwerk erfolgen. Der Network Monitor 3.1 bietet Parser für RADIUS, 802.1X, EAPOL und EAP. Ein *Parser* ist eine Komponente des Network Monitors, die die Felder eines Protokollheaders voneinander trennen sowie den Aufbau des Headers und die Werte der Felder anzeigen kann. Ohne einen geeigneten Parser zeigt der Network Monitor 3.1 die im Header enthaltenen Bytes in Hexadezimalform an. Die Interpretation dieser Bytes bleibt dann Ihnen überlassen.



Auf der CD Sie erreichen die Downloadwebsite für den Network Monitor auch über einen Link, den Sie auf der Begleit-CD dieses Buchs finden.

Bei der Untersuchung der Authentifizierung von Drahtlosclients können Sie den Network Monitor 3.1 verwenden, um die Datenpakete aufzuzeichnen, die während der Authentifizierung zwischen dem Drahtlosclient und dem drahtlosen Zugriffspunkt ausgetauscht werden. Mit dem Network Monitor 3.1 können Sie die einzelnen Datenpakete untersuchen und herauszufinden versuchen, warum die Authentifizierung fehlgeschlagen ist. Der Network Monitor eignet sich auch zur Aufzeichnung der RADIUS-

Nachrichten, die zwischen einem drahtlosen Zugriffspunkt und seinem RADIUS-Server ausgetauscht werden, und zur Überprüfung der RADIUS-Attribute jeder Nachricht.

Die korrekte Interpretation der Datenpakete, die mit dem Network Monitor 3.1 aufgezeichnet werden, setzt eine gründliche Kenntnis von EAPOL, RADIUS und anderen Protokollen voraus. Die mit dem Network Monitor 3.1 aufgezeichneten Datenpakete können Sie bei Bedarf auch in Dateien speichern und zur Analyse an den Microsoft-Support senden.

Beheben von Problemen mit Drahtlosclients

Bei der Behebung von Problemen mit drahtlosen Netzwerkverbindungen sollten Sie zuerst überprüfen, ob sich dieselben Probleme auf mehreren oder allen Ihren Drahtlosclients zeigen. Haben alle Drahtlosclients Schwierigkeiten, könnte die Ursache in Ihrer Authentifizierungsinfrastruktur liegen. Haben nur einige der Drahtlosclients Probleme, könnte die Ursache bei einem oder mehreren drahtlosen Zugriffspunkten oder bei den einzelnen Clients liegen.

Die folgenden Beschreibungen sind Beispiele für Probleme, die auf drahtlosen Windows-Clients häufiger auftreten:

- **Das drahtlose Netzwerk ist nicht zu finden.** Überprüfen Sie mit den Hilfsprogrammen des Herstellers, ob Sie sich in der Reichweite eines drahtlosen Zugriffspunkts des Netzwerks befinden. Sie können den drahtlosen Zugriffspunkt oder den Client umstellen, die Sendeleistung des drahtlosen Zugriffspunkts erhöhen oder Störquellen und Gegenstände entfernen, die sich negativ auf die Reichweite auswirken.
- **Fehler bei der Authentifizierung.** Einige Drahtlosnetzwerkadapter verfügen über eine Verbindungsanzeige (ein Lämpchen in Form einer LED), die auf gesendete oder empfangene Datenpakete hinweist. Da die IEEE 802.1X-Authentifizierung erfolgt, bevor der Drahtlosnetzwerkadapter tatsächlich Nutzdaten überträgt oder empfängt, lässt sich an der Verbindungsanzeige nicht ablesen, ob eine 802.1X-Authentifizierung erfolgt. Weist die Anzeige nicht auf Datenverkehr im Funknetz hin, kann eine fehlgeschlagene 802.1X-Authentifizierung die Ursache sein.

Überprüfen Sie, ob das Benutzer- oder Computerkonto für den Drahtlosclient vorhanden ist, ob es aktiviert ist, ob es vielleicht gesperrt ist (über Konteneigenschaften oder eine RAS-Kontosperre) und ob der Verbindungsversuch zu den zugelassenen Anmeldezeiten erfolgt.

Überprüfen Sie, ob es für den Verbindungsversuch mit dem verwendeten Computer- oder Benutzerkonto eine passende Netzwerkrichtlinie gibt. Wenn Sie die Konten zum Beispiel auf Gruppenebene mit Netzwerkrichtlinien verwalten, überprüfen Sie, ob das Benutzer- oder Computerkonto Mitglied der Gruppe ist, für die die Netzwerkrichtlinie festgelegt wurde.

Überprüfen Sie, ob das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstellen der NPS-Serverzertifikate auf den Drahtlosclientcomputern im lokalen Computerspeicher für vertrauenswürdige Stammzertifizierungsstellen vorhanden ist.

Überprüfen Sie bei einem Drahtlosclient mit EAP-TLS- oder PEAP-TLS-Authentifizierung, ob das Computer- oder Benutzerzertifikat die Bedingungen erfüllt, die im Abschnitt »Überprüfen des Zertifikats des Drahtlosclients« beschrieben werden.

Überprüfen Sie bei einem Drahtlosclient mit PEAP-MS-CHAP v2-Authentifizierung, ob das Kennwort des Drahtlosclients abgelaufen ist. Sorgen Sie dafür, dass auf den NPS-Servern im Dialogfeld *EAP-MSCHAPv2*-Eigenschaften das Kontrollkästchen *Client kann Kennwort ändern, nachdem es abgelaufen ist* aktiviert ist.

- **Es ist keine Authentifizierung mit einem Zertifikat möglich.** Die häufigste Ursache für dieses Problem ist, dass noch kein Benutzer- oder Computerzertifikat installiert wurde. Je nach der eingestellten Authentifizierungsmethode müssen alle beide installiert sein. Überprüfen Sie im Zertifikate-Snap-In, ob Sie ein Computerzertifikat, ein Benutzerzertifikat oder beide installiert haben.

Eine weitere Ursache für diese Meldung kann darin bestehen, dass sich die installierten Zertifikate nicht für die Drahtlosauthentifizierung eignen oder nicht von allen NPS-Servern überprüft werden können. Weitere Informationen finden Sie im Abschnitt »Beheben von Problemen mit der Überprüfung von Zertifikaten« dieses Kapitels.

Beheben von Problemen mit drahtlosen Zugriffspunkten

Wenn Sie mehrere drahtlose Zugriffspunkte einsetzen und über einen dieser Zugriffspunkte keine Verbindung herstellen und keine Authentifizierung durchführen können, kann das Problem bei diesem Zugriffspunkt liegen. Dieser Abschnitt beschreibt die gebräuchlichen Hilfsmittel zur Behebung von Problemen mit drahtlosen Zugriffspunkten und die üblichen Probleme, die bei der Verbindungsherstellung und Authentifizierung auf einem Zugriffspunkt auftreten können.

Hilfsmittel zur Behebung von Problemen mit drahtlosen Zugriffspunkten

Welche Hilfsmittel Ihnen bei der Problembehandlung zur Verfügung stehen, hängt zwar von den Herstellern der Geräte ab, aber die häufiger anzutreffenden sind folgende:

- LEDs
- Standortüberprüfungssoftware (Site-Survey-Software)
- SNMP-Unterstützung
- Diagnosetools

Diese Hilfsmittel werden in den folgenden Abschnitten genauer beschrieben. Informieren Sie sich in der Dokumentation Ihres drahtlosen Zugriffspunkts über die Hilfsmittel, die Ihnen zur Problembehandlung zur Verfügung stehen.

LEDs

Die meisten drahtlosen Zugriffspunkte verfügen über ein oder mehrere kleine Lämpchen (Leuchtdioden, LEDs), die außen am Gehäuse des Geräts angebracht sind und einen schnellen Überblick über den Betriebszustand des Geräts ermöglichen:

- Ein Lämpchen zeigt an, ob das Gerät mit Strom versorgt wird.
- Ein Lämpchen zeigt den allgemeinen Betriebszustand an. Dieses Lämpchen könnte zum Beispiel zeigen, ob eine Assoziation zwischen dem drahtlosen Zugriffspunkt und einem Drahtlosclient besteht.
- Ein Lämpchen zeigt die Übertragungsaktivität an. Dieses Lämpchen könnte zum Beispiel bei jedem eingehenden Datenpaket blinken.
- Ein Lämpchen weist auf Datenkollisionen hin. Blinkt es sehr häufig, sollten Sie mit den Methoden, die der Hersteller vorschlägt, die Leistung des Geräts überprüfen.
- Ein Lämpchen zeigt den Datenverkehr im Kabelnetzwerk an. Dieses Lämpchen könnte zum Beispiel bei jedem eingehenden Datenpaket blinken.

Vielleicht verfügt der drahtlose Zugriffspunkt statt der Lämpchen über ein LCD (Liquid Crystal Display), auf der verschiedene Symbole den Zustand des Geräts angeben. Informieren Sie sich in der Dokumentation des Geräts über die Bedeutung der Lämpchen oder der Symbole auf der LCD-Anzeige.

Standortüberprüfungssoftware (Site-Survey-Software)

Standortüberprüfungssoftware, die Sie bei der Bereitstellung von drahtlosen Zugriffspunkten zur Bestimmung des optimalen Aufstellungsorts verwenden können, wird gewöhnlich von einer CD-ROM aus dem Lieferumfang des drahtlosen Zugriffspunkts oder des Drahtlosnetzwerkadapters auf einen drahtlosnetzwerkfähigen Laptop installiert.

Wie in diesem Kapitel bereits unter der Überschrift »Bereitstellen drahtloser Zugriffspunkte« beschrieben, dient die Standortüberprüfungssoftware zur Ermittlung des Sendebereichs (coverage volume) und der Abstände von einem drahtlosen Zugriffspunkt, an denen sich die Datenübertragungsraten ändern. Wenn Drahtlosclients mit einem bestimmten drahtlosen Zugriffspunkt keine Verbindung herstellen können, überprüfen Sie den Sendebereich dieses drahtlosen Zugriffspunkts mit der Standortüberprüfungssoftware. Vielleicht hat es unter den Geräten eine Änderung gegeben, die zu Interferenzen führt, oder vielleicht wurden seit der letzten Standortüberprüfung neue Objekte aufgestellt, die die Ausbreitung der Funkwellen stören.

SNMP-Unterstützung

Viele drahtlose Zugriffspunkte sind mit einem SNMP-Agenten (Simple Network Management Protocol) ausgerüstet, der die folgenden SNMP-MIBs (Management Information Bases) unterstützt:

- IEEE 802.11 MIB
- IEEE 802.1 PAE (Port Access Entity) MIB
- SNMP Management MIB (beschrieben in RFC 1157)
- SNMP MIB II (beschrieben in RFC 1213)
- Bridge MIB (beschrieben in RFC 1286)
- Ethernet Interface MIB (beschrieben in RFC 1398)
- IETF Bridge MIB (beschrieben in RFC 1493)
- Remote Monitoring (RMON) MIB (beschrieben in RFC 1757)
- RADIUS Client Authentication MIB (beschrieben in RFC 2618)

Der SNMP-Agent auf dem drahtlosen Zugriffspunkt kann zusammen mit Ihrer vorhandenen SNMP-Netzwerkverwaltungsinfrastruktur zur Konfiguration der drahtlosen Zugriffspunkte, zur Festlegung von Trapbedingungen und zur Überwachung der Belastung der drahtlosen Zugriffspunkte dienen.

Diagnosetools

Diagnosetools für drahtlose Zugriffspunkte können folgende Form haben:

- Diagnoseprogramme, die über das Hauptkonfigurationsprogramm eines drahtlosen Zugriffspunkts gestartet werden, beispielsweise ein Windows-Programm von der Produkt-CD des Herstellers des drahtlosen Zugriffspunkts oder eine Reihe von Webseiten.
- Diagnosetools, die über ein Befehlszeilenprogramm oder auf eine andere Weise zugänglich sind und zum Beispiel einen Terminalzugriff auf den drahtlosen Zugriffspunkt ermöglichen.

Welche Diagnosetools die Hersteller bereitstellen, hängt vom Hersteller und vom drahtlosen Zugriffspunkt ab. Sinn dieser Diagnosetools ist es aber immer, die aktuelle Konfiguration der drahtlosen Zugriffspunkte überprüfen und die ordnungsgemäße Funktion der Geräte (Hardwareebene) sicherstellen zu können.

Häufiger auftretende Probleme mit drahtlosen Zugriffspunkten

Die folgenden Probleme treten bei drahtlosen Zugriffspunkten häufiger auf:

- Der drahtlose Zugriffspunkt ist nicht zu sehen.
- Es ist keine Authentifizierung beim drahtlosen Zugriffspunkt möglich.
- Über den drahtlosen Zugriffspunkt hinaus ist keine Kommunikation möglich.

Diese Probleme werden in den folgenden Abschnitten näher besprochen.

Der drahtlose Zugriffspunkt ist nicht zu sehen

Wenn Drahtlosclients einen drahtlosen Zugriffspunkt bei der Suche nach Netzwerken nicht sehen, kann dies eine der folgenden Ursachen haben:

- **Der drahtlose Zugriffspunkt sendet keine Kennung.** Alle drahtlosen Zugriffspunkte sollten regelmäßig Beacon-Nachrichten ausstrahlen, die ihre SSID enthalten (sofern das Gerät nicht auf die Unterdrückung der SSID in Beacon-Nachrichten eingestellt wurde) und die Fähigkeiten der Geräte beschreiben (beispielsweise die unterstützten Übertragungsraten und die Sicherheitsoptionen). Um zu prüfen, ob ein Zugriffspunkt seine Kennung ausstrahlt, können Sie die Standortüberprüfungssoftware oder einen Paketanalysator verwenden, der die Beacon-Nachrichten aufzeichnet. Vielleicht enthält bereits die Produkt-CD-ROM vom Hersteller des Zugriffspunkts einen einfachen Paketanalysator, der die Beacon-Nachrichten und andere Verwaltungsnachrichten aufzeichnen kann.
- **Der drahtlose Zugriffspunkt ist nicht auf den richtigen Kanal eingestellt.** Wenn der drahtlose Zugriffspunkt denselben Kanal wie ein benachbarter drahtloser Zugriffspunkt verwendet, können die sich überlagernden Funksignale dazu führen, dass Drahtlosclients nur schwer stabile Verbindungen herstellen können. Ändern Sie bei Bedarf die Kanaleinstellung.
- **Der drahtlose Zugriffspunkt beschreibt seine Fähigkeiten falsch.** Überprüfen Sie, ob der drahtlose Zugriffspunkt so eingestellt ist, dass er mit der gewünschten Technik arbeitet (wie 802.11b, 802.11a oder 802.11g) und die gewünschten Übertragungsraten und Sicherheitsfunktionen verwendet (WPA oder WPA2). Wenn Sie das Beacon-Datenpaket mit einem Protokollanalysator auffangen, können Sie die eingestellten Werte mit den Werten aus dem Beacon-Datenpaket vergleichen.
- **Der drahtlose Zugriffspunkt sendet im vorgesehenen Sendebereich nicht mit hinreichender Leistung.** Überprüfen Sie mit Ihrer Standortüberprüfungssoftware, ob der tatsächliche Sendebereich des drahtlosen Zugriffspunkts mit dem geplanten Sendebereich übereinstimmt. Falls es neue Quellen für Signalabschwächungen, Reflektionen und Interferenzen gibt, ordnen Sie diese neuen Störquellen oder den drahtlosen Zugriffspunkt anders an.

Es ist keine Authentifizierung beim drahtlosen Zugriffspunkt möglich

Falls Sie mehrere drahtlose Zugriffspunkte verwenden und Ihre Drahtlosclients mit keinem dieser Geräte eine Verbindung herstellen können, gibt es vielleicht ein Problem in Ihrer Authentifizierungsinfrastruktur. Wie man solche Probleme beheben kann, beschreibt der noch folgende Abschnitt »Beheben von Problemen mit der Authentifizierungsinfrastruktur« dieses Kapitels. Falls Sie mehrere drahtlose Zugriffspunkte verwenden und die Drahtlosclients nur mit der Authentifizierung bei einem bestimmten Zugriffspunkt Schwierigkeiten haben, müssen Sie die Authentifizierungseinstellung dieses drahtlosen Zugriffspunkts überprüfen. Überprüfen Sie folgende drei Bereiche der Authentifizierungskonfiguration:

- 802.1X-Konfiguration
- RADIUS-Konfiguration
- WPA-Konfiguration

802.1X-Konfiguration

Sorgen Sie dafür, dass die 802.1X-Authentifizierung des drahtlosen Zugriffspunkts aktiviert ist. Bei einigen Zugriffspunkten wird die 802.1X-Authentifizierung als EAP-Authentifizierung bezeichnet.

RADIUS-Konfiguration

Die RADIUS-Konfiguration umfasst folgende Elemente:

- **RADIUS-Konfiguration der drahtlosen Zugriffspunkte** Sorgen Sie dafür, dass der drahtlose Zugriffspunkt korrekt für RADIUS konfiguriert ist. Der drahtlose Zugriffspunkt sollte folgende Einstellungen aufweisen:
 - Die IPv4- oder IPv6-Adresse eines primären RADIUS-Servers (einer Ihrer NPS-Server)
 - Die UDP-Zielports (UDP bedeutet User Datagram Protocol) für den RADIUS-Datenverkehr, der an den primären RADIUS-Server gesendet wird (UDP-Port 1812 für den RADIUS-Authentifizierungsdatenverkehr und UDP-Port 1813 für den RADIUS-Kontoführungsdatenverkehr)
 - Den gemeinsamen geheimen RADIUS-Schlüssel für den primären RADIUS-Server
 - Die IPv4- oder IPv6-Adresse eines sekundären RADIUS-Servers (ein weiterer Ihrer NPS-Server)
 - Die UDP-Zielports für den RADIUS-Datenverkehr, der an den sekundären RADIUS-Server gesendet wird
 - Den gemeinsamen geheimen RADIUS-Schlüssel für den sekundären RADIUS-Server
- **Erreichbarkeit der NPS-Server** Überprüfen Sie auf folgende Weise, ob der primäre und der sekundäre NPS-Server für den drahtlosen Zugriffspunkt erreichbar sind:
 - Wenn der drahtlose Zugriffspunkt über einen »Ping« verfügt – er kann an ein beliebiges IPv4-Ziel eine ICMP-Echo-Nachricht (Internet Control Message Protocol) senden –, versuchen Sie, die IPv4-Adressen des primären und sekundären NPS-Servers mit dem Ping zu erreichen.
 - Kann der drahtlose Zugriffspunkt keinen Ping aussenden, versuchen Sie, die IPv4-Adressen des primären und sekundären NPS-Servers von einem anderen Netzwerkknoten aus mit dem Programm Ping zu erreichen. Dieser Knoten muss sich in dem Subnetz befinden, zu dem auch der drahtlose Zugriffspunkt gehört.

Ist der Ping vom Netzwerkknoten erfolgreich und der Ping vom drahtlosen Zugriffspunkt nicht, überprüfen Sie die IPv4-Konfiguration des drahtlosen Zugriffspunkts. Sorgen Sie dafür, dass er mit der korrekten IPv4-Adresse, der richtigen Subnetzmaske und dem richtigen Standardgateway für das dazugehörige Kabelnetzwerk konfiguriert ist. Funktioniert keiner der Pings, beheben Sie die Verbindungsprobleme zwischen dem angeschlossenen Subnetz und den RADIUS-Servern.



Hinweis Ein negatives Ergebnis beim Ping-Test bedeutet nicht zwangsläufig, dass keine Verbindung besteht. Es könnte auf dem Weg zwischen dem drahtlosen Zugriffspunkt und den RADIUS-Servern ein Router vorhanden sein, der ICMP-Nachrichten herausfiltert. Vielleicht wurden auch die NPS-Server mit Paketfiltern ausgestattet, die ICMP-Nachrichten verwerfen.

Um sicherzustellen, dass der RADIUS-Datenverkehr den primären und den sekundären NPS-Server erreicht, verwenden Sie auf den NPS-Servern einen Netzwerkniffer wie den Network Monitor 3.1. Damit können Sie den RADIUS-Datenverkehr aufzeichnen und untersuchen, der bei einem Authentifizierungsversuch zwischen dem drahtlosen Zugriffspunkt und den RADIUS-Servern ausgetauscht wird.

- **Konfiguration der NPS-Server** Wenn der RADIUS-Datenverkehr den primären und den sekundären NPS-Server erreicht, überprüfen Sie, ob der primäre und sekundäre NPS-Server mit einem RADIUS-Client konfiguriert sind, der dem drahtlosen Zugriffspunkt entspricht. Dazu gehören folgende Werte:
 - Die IPv4-Adresse der Kabelnetzwerkschnittstelle des drahtlosen Zugriffspunkts
 - Die UDP-Zielpor­ts für den RADIUS-Datenverkehr, der vom drahtlosen Zugriffspunkt gesendet wird (UDP-Port 1812 für den RADIUS-Authentifizierungsdatenverkehr und UDP-Port 1813 für den RADIUS-Kontoführungsdatenverkehr)
 - Das gemeinsame geheime RADIUS-Kennwort, das auf dem drahtlosen Zugriffspunkt konfiguriert wurde
 Überprüfen Sie das Protokoll *Windows-Protokolle\Sicherheit* auf Authentifizierungsfehler­einträge, die den Verbindungsversuchen mit dem drahtlosen Zugriffspunkt entsprechen. Um die Ereigniseinträge für fehlgeschlagene Authentifizierungen überprüfen zu können, sehen Sie sich in der Ereignisanzeige die Ereigniseinträge aus dem Sicherheitsereignisprotokoll mit der Ereignis-ID 6273 an.
- **IPsec für den RADIUS-Datenverkehr** Wenn Sie zur Verschlüsselung des RADIUS-Datenverkehrs zwischen dem drahtlosen Zugriffspunkt und dem NPS-Server IPsec verwenden, überprüfen Sie die IPsec-Einstellungen auf dem drahtlosen Zugriffspunkt und auf dem NPS-Server und sorgen Sie dafür, dass beide erfolgreich Sicherheitszuordnungen aushandeln und sich gegenseitig authentifizieren können.



Hinweis Weitere Informationen über die Einstellung der IPsec-Richtlinien unter Windows Server 2008 zum Schutz des RADIUS-Datenverkehrs finden Sie in Kapitel 4, »Windows-Firewall mit erweiterter Sicherheit«. Informationen über die Konfiguration von IPsec für einen drahtlosen Zugriffspunkt finden Sie in der Produktdokumentation Ihres drahtlosen Zugriffspunkts.

WPA- oder WPA2-Konfiguration

Sofern Ihr drahtloser Zugriffspunkt WPA- oder WPA2-fähig ist und Sie zum Schutz des Drahtlosnetzwerks WPA oder WPA2 verwenden möchten, sorgen Sie dafür, dass WPA oder WPA2 aktiviert ist.

Über den drahtlosen Zugriffspunkt hinaus ist keine Kommunikation möglich

Der drahtlose Zugriffspunkt ist eine unsichtbare Bridge und ein Schicht-2-Switch, der Datenpakete zwischen dem Kabelnetzwerk, mit dem er verbunden ist, und den verbundenen Drahtlosclients weiterleitet. Wenn Drahtlosclients zwar eine Verbindung herstellen und sich authentifizieren können, aber keine Orte jenseits des drahtlosen Zugriffspunkts erreichen, könnte dies einen oder mehrere der folgenden Gründe haben.

- **Der drahtlose Zugriffspunkt leitet die Datenpakete nicht als Bridge weiter.** Alle unsichtbaren Bridges unterstützen das Spanning-Tree-Protokoll, das eine Schleifenbildung bei der Überbrückung der Netzwerksegmente verhindern soll. Das Spanning-Tree-Protokoll verwendet eine Reihe von Multicast-Nachrichten, um Informationen über die Brückenkonfiguration zu kommunizieren und die Brückenschnittstellen automatisch so zu konfigurieren, dass Datenpakete weitergeleitet oder die Weiterleitung gesperrt wird, um Schleifen zu verhindern. Während der Spanning-Tree-Algorithmus die Weiterleitung oder Sperrung von Schnittstellen überprüft, leitet die Bridge keine Datenpakete weiter. Überprüfen Sie den Weiterleitungsstatus des drahtlosen Zugriffspunkts und die Bridgekonfiguration.

- **Der drahtlose Zugriffspunkt wurde nicht mit den korrekten VLAN-IDs konfiguriert.** Viele drahtlose Zugriffspunkte unterstützen VLANs. Dabei handelt es sich um Switchanschlüsse, die auf der Verwaltungsebene so zusammengefasst werden, dass sie im selben Subnetz erscheinen. Jede Gruppe erhält eine separate VLAN-ID. Überprüfen Sie, ob die VLAN-IDs für Ihren Drahtlosclient und Ihre verkabelten Schnittstellen korrekt konfiguriert sind. Vielleicht verwenden Sie zum Beispiel eine VLAN-ID für authentifizierte Drahtlosclients (die Verbindung erfolgt mit dem Intranet der Organisation) und eine separate VLAN-ID für Gäste mit drahtlosen Computern (die Verbindung erfolgt mit einem anderen Subnetz oder mit dem Internet).

Beheben von Problemen mit der Authentifizierungsinfrastruktur

Wenn Sie mehrere drahtlose Zugriffspunkte verwenden und mit keinem dieser Zugriffspunkte eine Authentifizierung durchführen können, liegt vielleicht ein Problem mit der Authentifizierungsinfrastruktur vor, die aus Ihren NPS-Servern, der PKI und den Active Directory-Konten besteht. In diesem Abschnitt beschreiben wir häufiger auftretende Probleme mit der NPS-Authentifizierung und Autorisierung, sowie mit der Überprüfung von Authentifizierungen auf Zertifikat- oder Kennwortbasis.

Beheben von Problemen mit der NPS-Authentifizierung und Autorisierung

Zur Behebung der häufiger auftretenden Probleme mit der NPS-Authentifizierung und Autorisierung sorgen Sie für Folgendes:

- **Dass der drahtlose Zugriffspunkt die NPS-Server erreichen kann** Um dies zu überprüfen, versuchen Sie, von jedem der NPS-Server aus die IP-Adresse des drahtlosen Zugriffspunkts im Kabelnetzwerk anzupingen. Sorgen Sie außerdem dafür, dass keine IPsec-Richtlinien, IP-Paketfilter oder anderen Mechanismen, die den Netzwerkzugriff einschränken können, den Austausch von RADIUS-Nachrichten zwischen dem drahtlosen Zugriffspunkt und seinen konfigurierten NPS-Servern verhindern. Für den RADIUS-Datenverkehr mit den NPS-Servern werden eine IPv4- oder IPv6-Quelladresse des drahtlosen Zugriffspunkts, eine IPv4- oder IPv6-Zieldresse des NPS-Servers, der UDP-Zielport 1812 für Authentifizierungsnachrichten und der UDP-Zielport 1813 für Kontoführungsnachrichten verwendet. Für den RADIUS-Datenverkehr von den NPS-Servern werden eine IPv4- oder IPv6-Quelladresse des NPS-Servers, eine IPv4- oder IPv6-Zieldresse des drahtlosen Zugriffspunkts, der UDP-Quellport 1812 für Authentifizierungsnachrichten und der UDP-Quellport 1813 für Kontoführungsnachrichten verwendet. Diese Beispiele setzen voraus, dass Sie die RADIUS UDP-Ports verwenden, die in den RFCs 2865 und 2866 für die RADIUS-Authentifizierung und Autorisierung definiert werden.
- **Dass jedes NPS-Server/Drahtloszugriffspunkt-Paar mit einem gemeinsamen geheimen RADIUS-Kennwort konfiguriert ist** Es muss zwar nicht jedes NPS-Server/Drahtloszugriffspunkt-Paar über ein eigenes gemeinsames geheimes RADIUS-Kennwort verfügen, aber das verwendete Kennwort muss auf beiden Partnern eines Paares dasselbe sein. Wenn Sie zum Beispiel die NPS-Konfiguration von einem NPS-Server auf einen anderen kopieren, überprüfen Sie alle Kennwortpaare zwischen den NPS-Servern und den drahtlosen Zugriffspunkten.
- **Dass die NPS-Server einen Active Directory-Domänencontroller und einen globalen Katalogserver erreichen können** Der NPS-Server verwendet einen globalen Katalogserver, um die Benutzerprinzipalnamen (User Principal Name, UPN) der Computer- oder Benutzerzertifikate oder den MS-CHAP v2-Kontonamen zum definierten Namen des entsprechenden Kontos in Active Directory aufzulösen. Der NPS-Server verwendet einen Active Directory-Domänencontroller, um die Anmeldeinformationen des Computer- und Benutzerkontos zu überprüfen und um die Kontoeigenschaften abzurufen, die für die Bewertung der Autorisierung erforderlich sind.

- **Dass die Computerkonten der NPS-Server in den entsprechenden Domänen Mitglieder der Sicherheitsgruppe RAS- und IAS-Server sind** Das Hinzufügen der NPS-Servercomputerkonten zur Sicherheitsgruppe *RAS- und IAS-Server* der entsprechenden Domäne geschieht normalerweise bei der Konfiguration der NPS-Server. Um das NPS-Servercomputerkonto zu den entsprechenden Domänen hinzuzufügen, können Sie den Befehl `netsh nps add registeredserver` verwenden.
- **Dass keine konfigurierten Beschränkungen ungewollt den Zugriff verhindern** Sorgen Sie dafür, dass das Benutzer- oder Computerkonto nicht gesperrt, abgelaufen oder deaktiviert ist und dass die Verbindungsversuche innerhalb der vorgesehenen Anmeldezeiten erfolgen.
- **Dass das Benutzerkonto nicht von der RAS-Kontosperrung gesperrt wurde** Die RAS-Kontosperrung zählt Authentifizierungsversuche und sperrt den Zugang nach der vorgesehenen Anzahl von Fehlversuchen, damit das Kennwort des Benutzers nicht so leicht durch Online-Wörterbuchangriffe ermittelt werden kann. Wenn die RAS-Kontosperrung aktiviert ist, können Sie den Sperrungszähler eines Kontos zurücksetzen, indem Sie auf dem NPS-Server den Registrierungswert `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout\Domänenname:Kontoname` löschen.
- **Dass die Verbindung autorisiert ist** Zur Autorisierung müssen die Parameter des Verbindungsversuchs Folgendes erfüllen:
 - Alle Bedingungen von mindestens einer Netzwerkrichtlinie erfüllen. Wenn es keine passende Richtlinie gibt, werden alle Drahtlosauthentifizierungsanforderungen abgelehnt.
 - Durch das Benutzerkonto eine Netzwerkzugriffsberechtigung erhalten (Einstellung auf *Zugriff gestatten*). Falls für das Benutzerkonto die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* gewählt wurde, muss die Zugriffsberechtigung der ersten passenden Netzwerkrichtlinie *Zugriff gewähren* lauten.
 - Mit allen Einstellungen des Profils übereinstimmen. Überprüfen Sie, ob in den Authentifizierungseinstellungen des Profils EAP-TLS oder PEAP-MS-CHAP v2 aktiviert und korrekt eingestellt wurde.
 - Zu den Einstellungen der Einwähleigenschaften des Benutzer- oder Computerkontos passen. Wenn Sie den Namen der Netzwerkrichtlinie ermitteln möchten, die zur Ablehnung des Verbindungsversuchs geführt hat, sorgen Sie dafür, dass die NPS-Ereignisprotokollierung für abgelehnte Authentifizierungsversuche aktiviert ist. Suchen Sie dann in der Ereignisanzeige im Protokoll *Windows-Protokolle\Sicherheit* nach Ereigniseinträgen mit der Ereignis-ID 6273. Im Text des Ereigniseintrags für den Verbindungsversuch finden Sie den Netzwerkrichtliniennamen im Feld *Netzwerkrichtliniennamen*.
- **Dass Sie den Modus Ihrer Domäne nicht vom gemischten Modus in den einheitlichen Modus geändert haben** Falls Sie Ihre Active Directory-Domäne gerade vom gemischten Modus auf den einheitlichen Modus umgestellt haben, können die NPS-Server nicht länger gültige Verbindungsanforderungen authentifizieren. Sie müssen jeden Domänencontroller der Domäne neu starten, damit die Änderung durch Replikation wirksam wird.

Beheben von Problemen mit der Überprüfung von Zertifikaten

Die Behebung von Problemen, die bei der Überprüfung von Zertifikaten für die EAP-TLS- oder PEAP-TLS-Authentifizierung auftreten, umfasst die Überprüfung der Computer- und Benutzerzertifikate des Drahtlosclients und der Computerzertifikate der NPS-Server.

Überprüfen des Zertifikats des Drahtlosclients

Damit ein NPS-Server das Zertifikat eines Drahtlosclients überprüfen kann, müssen für jedes Zertifikat aus der Zertifikatkette des Zertifikats, das der Drahtlosclient gesendet hat, folgende Bedingungen erfüllt sein:

- **Das aktuelle Datum liegt im Gültigkeitszeitraum des Zertifikats.** Zertifikate werden mit einem Gültigkeitszeitraum ausgestellt, vor dessen Beginn sie noch nicht verwendet werden können. Nach dem Ablauf des Gültigkeitszeitraums sind auch die Zertifikate abgelaufen und können nicht mehr verwendet werden.
- **Das Zertifikat wurde nicht gesperrt.** Ausgestellte Zertifikate können jederzeit gesperrt werden. Jede ausstellende Zertifizierungsstelle führt eine Liste der Zertifikate, die nicht mehr als gültig akzeptiert werden sollten, und veröffentlicht diese Liste in Form einer Zertifikatsperrliste (Certificate Revocation List, CRL). Der Server versucht zuerst, das Zertifikat mit dem OSCP-Protokoll zu überprüfen (OSCP bedeutet Online Certificate Status Protocol). Ist die OSCP-Überprüfung erfolgreich, so ist auch die Überprüfung des Zertifikats erfolgreich. Andernfalls versucht er, das Benutzer- oder Computertzertifikat anhand der Zertifikatsperrliste zu überprüfen. Standardmäßig überprüft der NPS-Server alle Zertifikate aus der Zertifikatkette des Drahtlosclients (die Reihe der Zertifikate vom Zertifikat des Drahtlosclients bis hinauf zur Stammzertifizierungsstelle) daraufhin, ob eines dieser Zertifikate gesperrt wurde. Wurde eines dieser Zertifikate gesperrt, schlägt die Zertifikatüberprüfung fehl. Dieses Verhalten kann in der Registrierung geändert werden, wie im weiteren Verlauf des Kapitels beschrieben.

Wenn Sie die Zertifikatsperrlisten-Verteilungspunkte für ein Zertifikat anzeigen möchten, klicken Sie das Zertifikat im Detailbereich des Zertifikate-Snap-Ins mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Sperrlisten-Verteilungspunkte*. Zur Überprüfung, ob das Zertifikat gesperrt ist, muss der NPS-Server in der Lage sein, die Zertifikatsperrlisten-Verteilungspunkte zu erreichen.

Die Überprüfung der Zertifikatsperrung funktioniert nur so gut wie das System, das die Zertifikatsperrlisten veröffentlicht und verteilt. Wird die Zertifikatsperrliste nicht häufig genug aktualisiert, kann ein bereits gesperrtes Zertifikat vielleicht noch verwendet und als gültig eingestuft werden, weil die veröffentlichte Zertifikatsperrliste, die der NPS-Server verwendet, veraltet ist. Überprüfen Sie, ob die den NPS-Servern zugänglichen Zertifikatsperrlisten noch gelten oder bereits veraltet sind. Wenn die den NPS-Servern verfügbaren Zertifikatsperrlisten abgelaufen sind, schlagen EAP-TLS- und PEAP-TLS-Authentifizierungen fehl.

- **Das Zertifikat verfügt über eine gültige digitale Signatur.** Zertifizierungsstellen signieren die Zertifikate, die sie ausstellen, digital. Der NPS-Server überprüft die digitale Signatur jedes Zertifikats aus der Kette (mit Ausnahme des Stammzertifizierungsstellenzertifikats) mit dem öffentlichen Schlüssel der ausstellenden Zertifizierungsstelle.

Das Zertifikat des Drahtlosclients muss zudem für den Verwendungszweck *Clientauthentifizierung* vorgesehen sein (der Verwendungszweck wird auch *Erweiterte Schlüsselverwendung*, *Enhanced Key Usage* oder *EKU* genannt) und im Feld *Alternativer Antragstellernamen* entweder den Benutzerprinzipalnamen eines gültigen Benutzerkontos oder den vollständig qualifizierten Domänennamen (FQDN) eines gültigen Computerkontos aufweisen.

Wenn Sie sich im Zertifikate-Snap-In die erweiterte Schlüsselverwendung (EKU) eines Zertifikats ansehen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Erweiterte Schlüsselverwendung*.

Wenn Sie im Zertifikate-Snap-In das Feld *Alternativer Antragstellername* anzeigen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Alternativer Antragstellername*.

- **Auf dem NPS-Server muss das erforderliche Zertifikat korrekt installiert worden sein.** Um der Zertifikatkette vertrauen zu können, die der Drahtlosclient vorlegt, muss der NPS-Server im Zertifikat-speicher *Vertrauenswürdige Stammzertifizierungsstellen* des Speichers *Lokaler Computer* über das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Zertifikats des Drahtlosclients verfügen.



Hinweis Zusätzlich zur normalen Zertifikatüberprüfung überprüft der NPS-Server auch, ob die ursprüngliche EAP-Response/Identity-Nachricht denselben Namen angibt, der im Feld *Alternativer Antragstellername* des übermittelten Zertifikats angegeben wird. Das hindert Angreifer daran, sich als einen anderen Benutzer oder Computer auszugeben als den, der in der EAP-Response/Identity-Nachricht genannt wird.

Welche Voraussetzungen das Zertifikat des Drahtlosclients außerdem erfüllen muss, wurde bereits im Abschnitt »Anforderungen an eine PKI« dieses Kapitels beschrieben.

Standardmäßig prüft NPS, ob die von den Drahtlosclients vorgelegten Zertifikate gesperrt sind. Wie der NPS-Server die Prüfung durchführt, können Sie auf dem NPS-Server mit den folgenden Registrierungsdaten unter *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13* einstellen:

- **IgnoreNoRevocationCheck** Wird dieser Wert auf 1 gestellt, akzeptiert NPS EAP-TLS-Authentifizierungen, selbst wenn es keine Sperrungsüberprüfung der Zertifikatkette des Clients (ausgenommen des Stammzertifizierungsstellenzertifikats) durchführen oder beenden kann. Gewöhnlich schlagen Zertifikatssperrungsüberprüfungen deswegen fehl, weil das Zertifikat keine Angaben über Sperrlisten enthält.

IgnoreNoRevocationCheck wird standardmäßig auf 0 gestellt (deaktiviert). NPS lehnt eine EAP-TLS- oder PEAP-TLS-Authentifizierung ab, wenn es die Sperrungsüberprüfung der Zertifikatkette des Clients (einschließlich des Stammzertifizierungsstellenzertifikats) nicht beenden und dabei feststellen kann, dass keines der Zertifikate gesperrt wurde.

Stellen Sie IgnoreNoRevocationCheck auf 1, um EAP-TLS- oder PEAP-TLS-Authentifizierungen auch dann zu akzeptieren, wenn das Zertifikat keine Angaben über Zertifikatssperrlisten-Verteilungspunkte enthält, wie manche Zertifikate von anderen Zertifizierungsstellen.

- **IgnoreRevocationOffline** Wird dieser Wert auf 1 gestellt, akzeptiert NPS EAP-TLS- oder PEAP-TLS-Authentifizierungen auch dann, wenn ein Server, auf dem die Zertifikatssperrliste gespeichert ist, nicht im Netzwerk verfügbar ist. IgnoreRevocationOffline wird standardmäßig auf 0 gestellt. NPS lehnt eine EAP-TLS- oder PEAP-TLS-Authentifizierung ab, wenn es nicht auf die Zertifikatssperrlisten zugreifen und daher die Sperrungsüberprüfung der Zertifikatkette des Clients nicht beenden und dabei feststellen kann, dass keines der Zertifikate gesperrt wurde. Kann es keine Verbindung mit einem der Zertifikatssperrlisten-Verteilungspunkte aufnehmen, wird das Zertifikat bei der EAP-TLS- oder PEAP-TLS-Authentifizierung als ungültig angesehen.

Stellen Sie IgnoreRevocationOffline auf 1, damit das Zertifikat bei der Sperrungsüberprüfung nicht beispielsweise wegen schlechter Verbindungen, die einen erfolgreichen Abschluss der Sperrungsprüfung verhindern, als ungültig eingestuft wird.

- **NoRevocationCheck** Wird dieser Wert auf 1 gestellt, führt NPS keine Sperrungsprüfung mit dem Zertifikat des Drahtlosclients durch. Bei der Sperrungsprüfung wird überprüft, ob das Zertifikat

des Drahtlosclients oder eines der Zertifikate aus dessen Zertifikatkette gesperrt wurde. Standardmäßig wird `NoRevocationCheck` auf 0 gestellt.

- **NoRootRevocationCheck** Wird dieser Wert auf 1 gestellt, führt NPS keine Sperrungsüberprüfung des Stammzertifizierungsstellenzertifikats des Drahtlosclients durch. Dieser Eintrag deaktiviert nur die Sperrungsprüfung des Stammzertifizierungsstellenzertifikats des Clients. Mit den restlichen Zertifikaten aus der Zertifikatkette des Drahtlosclients wird weiterhin eine Sperrungsprüfung durchgeführt. Standardmäßig wird `NoRootRevocationCheck` auf 0 gestellt.

Sie können `NoRootRevocationCheck` verwenden, wenn Clients authentifiziert werden sollen, in deren Stammzertifizierungsstellenzertifikate keine Zertifikatsperrlisten-Verteilungspunkte angegeben sind, wie in manchen Zertifikaten von anderen Zertifizierungsstellen. Außerdem kann dieser Wert Verzögerungen verhindern, wie sie zum Beispiel eintreten, wenn die Sperrliste eines Zertifikats nicht zugänglich oder abgelaufen ist.

Diese Registrierungswerte müssen als `DWORD`-Typen hinzugefügt werden (ein Registrierungsdatentyp, dessen Wert in Hexadezimalform mit maximal 4 Bytes angegeben wird) und auf 0 oder 1 gestellt werden. Die drahtlosen Windows-Clients verwenden diese Werte nicht.

Überprüfen der Zertifikate der NPS-Server

Damit der Drahtlosclient das Zertifikat des NPS-Servers überprüfen kann, müssen alle Zertifikate aus der Zertifikatkette des Zertifikats, das vom NPS-Server übermittelt wird, folgende Bedingungen erfüllen:

- **Das aktuelle Datum liegt im Gültigkeitszeitraum des Zertifikats.** Zertifikate werden mit einem Gültigkeitszeitraum ausgestellt, vor dessen Beginn sie noch nicht verwendet werden können. Nach dem Ablauf des Gültigkeitszeitraums sind auch die Zertifikate abgelaufen und können nicht mehr verwendet werden.
- **Das Zertifikat verfügt über eine gültige digitale Signatur.** Zertifizierungsstellen signieren die Zertifikate, die sie ausstellen, digital. Der Drahtlosclient überprüft die digitale Signatur jedes Zertifikats aus der Kette mit Ausnahme des Stammzertifizierungsstellenzertifikats mit dem öffentlichen Schlüssel der ausstellenden Zertifizierungsstelle.

Außerdem muss das Zertifikat des NPS-Servers für den Verwendungszweck *Serverauthentifizierung* vorgesehen sein. Die Objektkennung (OID) dieses Eintrags in der erweiterten Schlüsselverwendung ist 1.3.6.1.5.5.7.3.1. Wenn Sie die erweiterte Schlüsselverwendung eines Zertifikats im Zertifikate-Snap-In überprüfen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Erweiterte Schlüsselverwendung*.

Schließlich muss noch das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Zertifikats des NPS-Servers auf dem Drahtlosclient im Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* des Speichers *Lokaler Computer* verfügbar sein, damit der Drahtlosclient der Zertifikatkette vertrauen kann, die der NPS-Server vorgelegt hat.

Welche Voraussetzungen das Computerzertifikat des NPS-Servers außerdem erfüllen muss, wurde bereits im Abschnitt »Anforderungen an eine PKI« dieses Kapitels beschrieben.

Beachten Sie bitte, dass der Drahtlosclient keine Sperrungsüberprüfung für die Zertifikate aus der Zertifikatkette des Computerzertifikats des NPS-Servers durchführt. Im Normalfall verfügt der Drahtlosclient noch nicht über eine Verbindung mit dem Netzwerk und kann daher weder auf eine Webseite noch auf andere Ressourcen zugreifen, die für eine Sperrungsüberprüfung erforderlich wären.

Beheben von Problemen bei der Authentifizierung mit Kennwörtern

Die Behebung von Problemen bei der PEAP-MS-CHAP v2-Authentifizierung mit Kennwörtern umfasst die Überprüfung des Namens und des Kennworts des Drahtlosbenutzers und die Überprüfung des Computerzertifikats des NPS-Servers.

Überprüfen der Anmeldeinformationen des Drahtlosclients

Wenn Sie zur Authentifizierung PEAP-MS-CHAP v2 verwenden, müssen der Name und das Kennwort, das der Drahtlosclient übermittelt, mit den Anmeldeinformationen für ein gültiges Konto übereinstimmen. Eine erfolgreiche Überprüfung der MS-CHAP v2-Anmeldeinformationen durch die NPS-Server hängt von Folgendem ab:

- Der Domänenteil des Namens entspricht dem Namen einer Domäne, bei der es sich entweder um die Domäne des NPS-Servers oder um eine Domäne handelt, für die eine bidirektionale Vertrauensstellung mit der Domäne des NPS-Servers besteht.
- Der Kontoteil des Namens entspricht einem gültigen Konto aus der Domäne.
- Das Kennwort ist das richtige Kennwort für das Konto.

Zur Überprüfung der Anmeldeinformationen für das Benutzerkonto veranlassen Sie den Benutzer dazu, sich auf einem Computer, der bereits über eine herkömmliche (Ethernet-)Kabelverbindung mit dem Netzwerk verbunden ist, bei seiner Domäne anzumelden. Dabei wird deutlich, ob das Problem bei den Anmeldeinformationen oder bei der Konfiguration der Authentifizierungsinfrastruktur liegt.

Überprüfen der Zertifikate der NPS-Server

Damit der Drahtlosclient das Zertifikat des NPS-Servers bei einer PEAP-MS-CHAP v2-Authentifizierung überprüfen kann, müssen alle Zertifikate aus der Zertifikatkette des Zertifikats, das vom NPS-Server übermittelt wird, folgende Bedingungen erfüllen:

- **Das aktuelle Datum liegt im Gültigkeitszeitraum des Zertifikats.** Zertifikate werden mit einem Gültigkeitszeitraum ausgestellt, vor dessen Beginn sie noch nicht verwendet werden können. Nach dem Ablauf des Gültigkeitszeitraums sind auch die Zertifikate abgelaufen und können nicht mehr verwendet werden.
- **Das Zertifikat verfügt über eine gültige digitale Signatur.** Zertifizierungsstellen signieren die Zertifikate, die sie ausstellen, digital. Der Drahtlosclient überprüft die digitale Signatur jedes Zertifikats aus der Kette mit Ausnahme des Stammzertifizierungsstellenzertifikats mit dem öffentlichen Schlüssel der ausstellenden Zertifizierungsstelle.

Außerdem muss das Zertifikat des NPS-Servers für den Verwendungszweck *Serverauthentifizierung* vorgesehen sein (Objektkennung 1.3.6.1.5.5.7.3.1). Wenn Sie die erweiterte Schlüsselverwendung eines Zertifikats im Zertifikate-Snap-In überprüfen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Erweiterte Schlüsselverwendung*.

Schließlich muss noch das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Zertifikats des NPS-Servers auf dem Drahtlosclient im Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* des Speichers *Lokaler Computer* verfügbar sein, damit der Drahtlosclient der Zertifikatkette vertrauen kann, die der NPS-Server vorgelegt hat.

Welche Voraussetzungen das Computerzertifikat des NPS-Servers außerdem erfüllen muss, wurde bereits im Abschnitt »Anforderungen an eine PKI« dieses Kapitels beschrieben.

Zusammenfassung des Kapitels

Der Aufbau eines geschützten Drahtlosnetzwerks erfordert die Konfiguration der Active Directory-, PKI-, Gruppenrichtlinien- und RADIUS-Elemente einer Authentifizierungsinfrastruktur auf Basis von Windows sowie die Bereitstellung und Konfiguration von drahtlosen Zugriffspunkten und Drahtlosclients. Die Wartungsarbeiten nach dem Aufbau des drahtlosen Netzwerks umfassen die Verwaltung der drahtlosen Zugriffspunkte, die Änderung ihrer Konfiguration bei Änderungen in der Infrastruktur sowie die Aktualisierung und Bereitstellung von Drahtlosnetzwerkprofilen. Bei drahtlosen Verbindungen tritt häufiger das Probleme auf, dass wegen Fehlern bei der Authentifizierung oder Autorisierung keine Verbindung aufgebaut werden kann oder dass Ressourcen aus dem Intranet für einen Drahtlosclient nicht zugänglich sind.

Weitere Informationen

Weitere Informationen über die Unterstützung von Drahtlosnetzwerken unter Windows Server 2008 und Windows Vista finden Sie hier:

- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- Microsoft Wireless Networking (<http://www.microsoft.com/wifi>)

Weitere Informationen über Active Directory finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Server 2008 Active Directory – Die technische Referenz* in der technischen Referenz zu Windows Server 2008 (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008

Weitere Informationen über PKI finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- »Public Key Infrastructure for Microsoft Windows Server« (<http://www.microsoft.com/pki>)
- *Microsoft Windows Server 2008 – PKI und Zertifikatsicherheit* von Brian Komar (Microsoft Press, 2008)

Weitere Informationen über Gruppenrichtlinien finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista* (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- Microsoft Windows Server Group Policy (<http://www.microsoft.com/gp>)

Weitere Informationen über RADIUS and NPS finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>

- Das Hilfe und Support-System von Windows Server 2008
- Microsoft Network Policy Server (<http://www.microsoft.com/nps>)

Weitere Informationen über NAP und die 802.1X-Erzwingung finden Sie hier:

- Kapitel 14, »Grundlagen des Netzwerkzugriffsschutzes«
- Kapitel 15, »Vorbereiten des Netzwerkzugriffsschutzes«
- Kapitel 17, »802.1X-Erzwingung«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- Network Access Protection (<http://www.microsoft.com/nap>)

Verkabelte Netzwerke mit IEEE 802.1X-Authentifizierung

In diesem Kapitel:

Konzepte	77
Planungs- und Entwurfsaspekte	79
Bereitstellen des Kabelnetzwerkzugriffs mit 802.1X-Authentifizierung	93
Wartung	102
Problembehandlung	103
Zusammenfassung des Kapitels	119
Weitere Informationen	119

Dieses Kapitel beschreibt, wie man LAN-Kabelnetzwerke, die die IEEE 802.1X-Authentifizierung verwenden, plant, bereitstellt und wartet und wie man auftretende Probleme beheben kann (IEEE steht für das Institute of Electrical and Electronic Engineers, LAN bedeutet Local Area Network). Nach der Bereitstellung kann ein geschütztes Kabelnetzwerk noch auf die 802.1X-Erzwingungsmethoden für den Netzwerkzugriffsschutz (NAP) umgestellt werden, wie in Kapitel 17, »802.1X-Erzwingung«, beschrieben.

In diesem Kapitel wird vorausgesetzt, dass Sie über ein Grundwissen über die Bedeutung der Komponenten Active Directory, Public-Key-Infrastruktur (PKI), Gruppenrichtlinien und RADIUS (Remote Authentication Dial-In User Service) in einer Authentifizierungsinfrastruktur auf der Basis von Windows für den Netzwerkzugriff verfügen. Weitere Informationen finden Sie in Kapitel 9, »Authentifizierungsinfrastruktur«.

Konzepte

Viele moderne Ethernetswitches unterstützen eine Netzwerkzugangskontrolle auf Portbasis. Damit lässt sich die Kommunikation über einen Switchport verhindern, bis der Computer, der auf den Port zugreift, authentifiziert und autorisiert wurde. Der Standard, mit dem die Benutzung von Ports authentifiziert wird, ist IEEE 802.1X. Die IEEE 802.1X-Authentifizierung wurde für mittlere bis große verkabelte LANs entwickelt, die über eine Authentifizierungsinfrastruktur mit RADIUS-Servern und Kontendatenbanken wie beispielsweise Active Directory verfügen. IEEE 802.1X hindert einen verkabelten Netzwerkknoten daran, Datenpakete aus dem Netzwerk anzunehmen oder ins Netzwerk zu senden, bis er erfolgreich authentifiziert und autorisiert wurde.

Bei der Authentifizierung wird überprüft, ob verkabelte Netzwerkknoten über gültige Anmeldeinformationen verfügen. Benutzer ohne Anmeldeinformationen können Ihrem Kabelnetzwerk nicht beitreten. Bei der Autorisierung wird überprüft, ob der verkabelte Client eine Verbindung mit dem Switch herstellen darf. IEEE 802.1X verwendet für den Austausch von Anmeldeinformationen EAP (Extensible Authentication Protocol). Eine Authentifizierung nach IEEE 802.1X kann mit verschiedenen

EAP-Authentifizierungsmethoden erfolgen, beispielsweise mit Benutzerkonten und Kennwörtern oder mit digitalen Zertifikaten.

Komponenten von Kabelnetzwerken mit 802.1X-Authentifizierung

Abbildung 11.1 zeigt die Komponenten eines verkabelten Netzwerks auf Windows-Basis mit 802.1X-Authentifizierung.

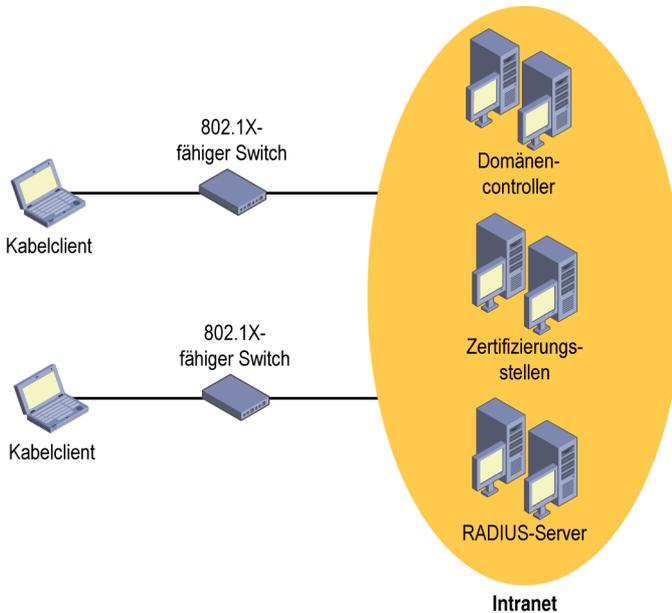


Abbildung 11.1 Komponenten von Kabelnetzwerken auf Windows-Basis mit 802.1X-Authentifizierung

Bei den Komponenten handelt es sich um:

- **Kabelclients** Netzwerkknoten, die die 802.1X-Authentifizierung für LAN-Verbindungen unterstützen und eine Verbindung mit 802.1X-fähigen verkabelten Switches herstellen
- **802.1X-fähige Switches** Switches, die an ihren Anschlüssen die 802.1X-Authentifizierung erzwingen, die dazugehörigen Verbindungsvoraussetzungen überprüfen und Datenpakete zwischen Kabelclients und Intranetressourcen weiterleiten
- **RADIUS-Server** Computer, die für 802.1X-fähige Switches und andere Arten von Zugriffsservern die zentrale Authentifizierung, Autorisierung und Kontoführung über Netzwerkzugriffsversuche durchführen
- **Active Directory-Domänencontroller** Computer, die Benutzer- und Computeranmeldeinformationen zur Authentifizierung überprüfen und Informationen über die dazugehörigen Konten zu Bewertung der Autorisierung an die RADIUS-Server weiterleiten
- **Zertifizierungsstellen** Komponenten der PKI, die Computer- oder Benutzerzertifikate für Kabelclients und Computerzertifikate für RADIUS-Server ausstellen

Planungs- und Entwurfsaspekte

Bei der Planung und dem Entwurf eines geschützten Kabelnetzwerks mit 802.1X-Authentifizierung sollten Sie folgende Aspekte berücksichtigen:

- Authentifizierungsmethoden im Kabelnetzwerk
- Authentifizierungsmodi im Kabelnetzwerk
- Authentifizierungsinfrastruktur
- Kabelclients
- PKI
- 802.1X-Erzwingung mit NAP

Authentifizierungsmethoden im Kabelnetzwerk

Windows Server 2008 und Windows Vista unterstützen die folgenden EAP-Authentifizierungsmethoden für die Authentifizierung im Kabelnetzwerk:

- EAP-TLS (Transport Layer Security)
- PEAP-MS-CHAP v2 (Protected EAP-Microsoft Challenge Handshake Authentication Protocol version 2)
- PEAP-TLS

EAP-TLS und PEAP-TLS werden zusammen mit einer PKI und Computerzertifikaten, Benutzerzertifikaten oder Smartcards verwendet. Bei EAP-TLS sendet der Kabelclient sein Computer-, Benutzer- oder Smartcardzertifikat zur Authentifizierung und der RADIUS-Server sendet ein Computerzertifikat zur Authentifizierung. Standardmäßig überprüft der Kabelclient das Zertifikat des RADIUS-Servers.

Falls keine Computer-, Benutzer- oder Smartcardzertifikate einsetzbar sind, verwenden Sie PEAP-MS-CHAP v2. PEAP-MS-CHAP v2 ist eine Authentifizierungsmethode auf Kennwortbasis, bei der der Austausch der Authentifizierungsnachrichten in einer verschlüsselten TLS-Sitzung erfolgt. Dadurch wird es für einen Angreifer wesentlich schwieriger, das Kennwort des aufgezeichneten Authentifizierungsdatenverkehrs mit einem Offline-Wörterbuchangriff zu bestimmen.

EAP-TLS und PEAP-TLS sind beide wesentlich sicherer als PEAP-MS-CHAP v2, weil sie nicht auf Kennwörtern basieren.

So funktioniert's: PEAP-MS-CHAP v2

MS-CHAP v2 ist ein Challenge-Response-Protokoll zur gegenseitigen Authentifizierung auf Kennwortbasis, das zur Verschlüsselung der Antworten die Standardalgorithmen MD4 (Message Digest) und DES (Data Encryption Standard) verwendet. Der authentifizierende Server stellt den Zugriffsklient auf die Probe und der Zugriffsklient stellt den authentifizierenden Server auf die Probe. Erfolgt auf eine dieser beiden Proben (challenges) keine korrekte Antwort, wird die Verbindung abgelehnt. Ursprünglich hat Microsoft MS-CHAP v2 als ein PPP-Authentifizierungsprotokoll (Point-to-Point Protocol) entwickelt, um DFÜ- und VPN-Verbindungen (Virtuelles Privates Netzwerk) besser zu schützen.

Obwohl MS-CHAP v2 einen besseren Schutz als andere Challenge-Response-Authentifizierungsprotokolle auf PPP-Basis bietet, ist es trotzdem für Offline-Wörterbuchangriffe anfällig. Ein Angreifer könnte eine erfolgreiche MS-CHAP v2-Authentifizierung aufzeichnen und systematisch

Kennwörter raten, bis das richtige gefunden ist. Kombiniert man PEAP mit MS-CHAP v2, wird der Datenverkehr bei der MS-CHAP v2-Authentifizierung durch eine relativ sichere TLS-Sitzung geschützt.

Eine PEAP-MS-CHAP v2-Authentifizierung erfolgt in zwei Teilen. Im ersten Teil wird mit PEAP eine verschlüsselte TLS-Sitzung eingeleitet, im zweiten Teil wird MS-CHAP v2 als EAP-Typ für den Austausch der Anmeldeinformationen zur Authentifizierung des Netzwerkzugriffs verwendet.

PEAP Teil 1: Erstellen der TLS-Sitzung

1. Der 802.1X-fähige Switch sendet dem verkabelten Client eine EAP-Request/Identity-Nachricht.
2. Der verkabelte Client antwortet mit einer EAP-Response/Identity-Nachricht, in der die Identität des verkabelten Clients angegeben wird (Benutzer- oder Computername).
3. Der Switch sendet dem RADIUS-Server eine EAP-Response/Identity-Nachricht. Von diesem Punkt an erfolgt die logische Kommunikation zwischen dem RADIUS-Server und dem Kabelclient, wobei der Switch die Nachrichten nur durchreicht.
4. Der RADIUS-Server sendet dem Kabelclient eine EAP-Request/Start PEAP-Nachricht.
5. Der verkabelte Client und der RADIUS-Server tauschen einige TLS-Nachrichten aus, in denen der RADIUS-Server dem Kabelclient sein Computerzertifikat mit der Zertifikatkette zur Überprüfung sendet und der Kabelclient und der RADIUS-Server die Verschlüsselungsschlüssel und die Verschlüsselungsmethode für die TLS-Sitzung bestimmen.

Am Ende der PEAP-Verhandlung hat der RADIUS-Server dem Kabelclient seine Identität bewiesen. Beide Knoten haben die gegenseitig verwendeten Verschlüsselungsschlüssel für die TLS-Sitzung bestimmt, und zwar mit Kryptografiemethoden, die mit öffentlichen Schlüsseln arbeiten, nicht mit Kennwörtern. Alle nachfolgenden EAP-Nachrichten, die zwischen dem Kabelclient und dem RADIUS-Server ausgetauscht werden, werden in der PEAP TLS-Sitzung verschlüsselt.

PEAP Teil 2: Authentifizieren mit MS-CHAP v2

1. Der RADIUS-Server sendet eine EAP-Request/Identity-Nachricht.
2. Der Kabelclient antwortet mit einer EAP-Response/Identity-Nachricht, in der die Identität (Benutzer- oder Computername) des Kabelclients angegeben wird.
3. Der RADIUS-Server sendet eine EAP-Request/EAP-MS-CHAP v2-Challenge-Nachricht, die eine Testzeichenfolge (challenge string) enthält.
4. Der verkabelte Client antwortet mit einer EAP-Response/EAP-MS-CHAP v2-Response-Nachricht, die nicht nur die Antwort auf die Testzeichenfolge des RADIUS-Servers enthält, sondern auch eine Testzeichenfolge für den RADIUS-Server.
5. Der RADIUS-Server sendet eine EAP-Request/EAP-MS-CHAP v2-Success-Nachricht, mit der er angibt, dass die Antwort des Clients korrekt war. Außerdem enthält die Nachricht die Antwort auf die Testzeichenfolge des Kabelclients.
6. Der Kabelclient antwortet mit einer EAP-Response/EAP-MS-CHAP v2-Ack-Nachricht, mit der er angibt, dass die Antwort des RADIUS-Servers korrekt ist.
7. Der RADIUS-Server sendet eine EAP-Success-Nachricht.

Am Ende dieses Datenaustausches zur gegenseitigen Authentifizierung ist Folgendes geschehen:

- Der Kabelclient hat seine Kenntnis des korrekten Kennworts bewiesen (die Antwort auf die Testzeichenfolge des RADIUS-Servers).

- Der RADIUS-Server hat seine Kenntnis des korrekten Kennworts bewiesen (die Antwort auf die Testzeichenfolge des Kabelclients).

Der gesamte Datenverkehr wurde in der TLS-Sitzung verschlüsselt, die im ersten Teil der PEAP-Authentifizierung erstellt wurde. Um nun einen Offline-Wörterbuchangriff durchzuführen, müsste der Angreifer zuerst die TLS-verschlüsselten Nachrichten entschlüsseln – eine entmutigende Aufgabe der Kryptoanalyse.

Voraussetzungen für die Authentifizierungsmethoden

Für die Authentifizierungsmethoden im Kabelnetzwerk gelten folgende Voraussetzungen:

- EAP-TLS erfordert die Installation eines Computerzertifikats auf jedem RADIUS-Server und eines Computerzertifikats, eines Benutzerzertifikats oder die Verwendung einer Smartcard auf allen verkabelten Clientcomputern. Damit sich die Computerzertifikate der RADIUS-Server überprüfen lassen, muss auf allen Kabelclientcomputern das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle der Computerzertifikate der RADIUS-Server installiert werden. Damit sich die Computer- oder Benutzerzertifikate der Kabelclients überprüfen lassen, müssen auf allen RADIUS-Servern die Stammzertifizierungsstellenzertifikate der ausstellenden Zertifizierungsstellen der Kabelclientzertifikate installiert werden.
- PEAP-MS-CHAP v2 erfordert auf jedem RADIUS-Server die Installation eines Computerzertifikats. Außerdem ist es erforderlich, auf den verkabelten Clientcomputern die Stammzertifizierungsstellenzertifikate der Computerzertifikate der RADIUS-Server zu installieren, damit sich die Computerzertifikate der RADIUS-Server überprüfen lassen.
- Wenn Sie planen, irgendwann die 802.1X-Erzwingung von NAP einzuführen, sollten Sie eine Authentifizierungsmethode auf der Basis von PEAP, wie PEAP-MS-CHAP v2 oder PEAP-TLS, verwenden.

Empfehlungen für die Authentifizierungsmethoden im Kabelnetzwerk

Für Authentifizierungsmethoden im Kabelnetzwerk gilt folgende Empfehlung:

- Wenn Sie PEAP-MS-CHAP v2 verwenden müssen, schreiben Sie in Ihrem Netzwerk sichere Kennwörter vor. Sichere Kennwörter sind lang (länger als acht Zeichen) und enthalten eine Mischung aus Groß- und Kleinbuchstaben, Ziffern und Satzzeichen. In einer Active Directory-Umgebung können Sie die Gruppenrichtlinieneinstellungen unter *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinien* einsetzen, um Benutzer dazu zu bringen, sichere Benutzerkennwörter zu verwenden.

Authentifizierungsmodi im Kabelnetzwerk

Verkabelte Clients auf Windows-Basis können in folgenden Modi Authentifizierungen durchführen:

- **Nur Computer** Windows führt mit den Anmeldeinformationen des Computers eine 802.1X-Authentifizierung durch, bevor der Anmeldebildschirm von Windows angezeigt wird. Auf diese Weise erhält der verkabelte Client Zugriff auf Netzwerkressourcen, beispielsweise auf Active Directory-Domänencontrollern, bevor sich ein Benutzer anmeldet. Windows versucht nach der Anmeldung des Benutzers keine Authentifizierung mit den Anmeldeinformationen des Benutzers.
- **Nur Benutzer** Standardmäßig führt Windows eine 802.1X-Authentifizierung mit den Anmeldeinformationen des Benutzers durch, nachdem die Anmeldung des Benutzers abgeschlossen wurde.

Windows versucht keine Authentifizierung mit den Anmeldeinformationen des Computers, bevor oder nachdem sich der Benutzer angemeldet hat.

- **Computer oder Benutzer** Windows führt mit den Anmeldeinformationen des Computers eine 802.1X-Authentifizierung durch, bevor es den Windows-Anmeldebildschirm anzeigt. Windows führt eine weitere 802.1X-Authentifizierung mit den Anmeldeinformationen des Benutzers durch, nachdem sich der Benutzer angemeldet hat.

Ein zusätzlicher Vorteil der Authentifizierungsarten *Nur Computer* oder *Computer oder Benutzer* besteht darin, dass die Ressourcen des authentifizierten Computers, beispielsweise freigegebene Ordner, anderen Computern zur Verfügung stehen, ohne dass ein Benutzer auf dem Computer angemeldet sein muss.

Mit dem Verhalten der Nur-Benutzer-Authentifizierung können sich folgende Probleme ergeben:

- Ein Benutzer kann auf dem Computer keine Domänenanmeldung durchführen, weil die lokal zwischengespeicherten Anmeldeinformationen für das Konto des Benutzers nicht verfügbar sind, keine Verbindung mit dem Domänencontroller besteht und sich die neuen Anmeldeinformationen nicht überprüfen lassen.
- Anmeldevorgänge bei Domänen sind nicht erfolgreich, weil während der Anmeldung des Benutzers keine Verbindung mit den Domänencontrollern der Active Directory-Domäne besteht. Anmeldeskripts sowie Aktualisierungen der Gruppenrichtlinien und Benutzerprofildaten schlagen ebenfalls fehl, was zu einer Reihe von Einträgen im Windows-Ereignisprotokoll führt.

Außerdem verwenden einige Netzwerkinfrastrukturen verschiedene virtuelle LANs (VLANs), um verkabelte Clients, die sich mit Computeranmeldeinformationen authentifiziert haben, von verkabelten Clients zu trennen, die sich mit Benutzeranmeldeinformationen authentifiziert haben. Wenn die Benutzerauthentifizierung beim verkabelten Netzwerk und die Umschaltung auf das benutzerauthentifizierte VLAN nach der Anmeldung des Benutzers erfolgt, hat ein verkabelter Windows-Client während der Benutzeranmeldung keinen Zugriff auf Ressourcen aus dem benutzerauthentifizierten VLAN, beispielsweise auf Active Directory-Domänencontroller. Das kann zu erfolglosen Erstanmeldungen und zu erfolglosen Vorgängen bei Domänenanmeldungen führen, was beispielsweise die Ausführung von Anmeldeskripten, Aktualisierungen von Gruppenrichtlinien und von Benutzerprofildaten betrifft.

Um die Probleme mit der Verfügbarkeit der Netzwerkverbindungen bei Benutzeranmeldungen im Nur-Benutzer-Authentifizierungsmodus und im Benutzer-oder-Computer-Authentifizierungsmodus bei der Verwendung separater VLANs zu lösen, unterstützen verkabelte Clients unter Windows Vista mit Service Pack 1 und Windows Server 2008 das einmalige Anmelden (Single Sign-On). Beim einmaligen Anmelden können Sie festlegen, dass die Netzwerkauthentifizierung mit Benutzeranmeldeinformationen vor der Anmeldung des Benutzers erfolgt. Zur Aktivierung und Einstellung der einmaligen Anmeldung können Sie die Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* verwenden oder Sie geben den Befehl `netsh lan` mit den entsprechenden Parametern ein. Weitere Informationen finden Sie im Verlauf dieses Kapitels im Abschnitt »Konfigurieren verkabelter Clients«.

Empfehlungen für die Authentifizierung im verkabelten Netzwerk

Für die Authentifizierung im verkabelten Netzwerk wird Folgendes empfohlen:

- Verwenden Sie den Modus Benutzer-oder-Computer-Authentifizierung. Die Benutzerauthentifizierung erfolgt nach der Benutzeranmeldung. Das ist der Standardauthentifizierungsmodus.
- Wenn Sie den Authentifizierungsmodus Nur Benutzer verwenden, konfigurieren Sie Ihre Kabelnetzwerkprofile so, dass sie die einmalige Anmeldung unterstützen und die Authentifizierung mit

den Benutzeranmeldeinformationen im verkabelten Netzwerk vor der Benutzeranmeldung durchführen, um Probleme mit der ersten Anmeldung und der Domänenanmeldung zu vermeiden.

- Wenn Sie für computerauthentifizierte und benutzerauthentifizierte verkabelte Clients verschiedene VLANs verwenden und den Authentifizierungsmodus Computer oder Benutzer einsetzen, konfigurieren Sie Ihre Kabelnetzwerkprofile so, dass sie die einmalige Anmeldung unterstützen und die Authentifizierung mit den Benutzeranmeldeinformationen im Kabelnetzwerk vor der Benutzeranmeldung durchführen, um Probleme bei der ersten Anmeldung und der Domänenanmeldung zu vermeiden.

Authentifizierungsinfrastruktur

Die Authentifizierungsinfrastruktur hat folgende Aufgaben:

- Authentifizieren der Anmeldeinformationen der Kabelclients
- Autorisieren der Kabelverbindung
- Informieren der 802.1X-fähigen Switches über Beschränkungen in Kabelverbindungen
- Erfassen von Beginn und Ende der Kabelverbindungen zu Buchhaltungszwecken

Die Authentifizierungsinfrastruktur für Verbindungen im Kabelnetzwerk, die nach 802.1X authentifiziert werden, besteht aus folgenden Komponenten:

- 802.1X-fähige Switches
- RADIUS-Server
- Active Directory-Domänencontroller
- Ausstellende Zertifizierungsstellen einer PKI (optional)

Wenn Sie eine Windows-Domäne als Kontodatenbank für die Überprüfung von Benutzer- oder Computeranmeldeinformationen und zum Speichern der Einwähleigenschaften verwenden, dann verwenden Sie unter Windows Server 2008 den Netzwerkrichtlinienserver (Network Policy Server, NPS). NPS ist ein voll funktionsfähiger und in Active Directory integrierter RADIUS-Server und RADIUS-Proxy, der den Internetauthentifizierungsdienst von Windows Server 2003 ersetzt. Informationen über Entwurf und Planung eines RADIUS-Servers auf der Basis von NPS erhalten Sie in Kapitel 9.

NPS kommuniziert bei der Authentifizierung der verkabelten Verbindung über einen geschützten RPC-Kanal (Remote Procedure Call) mit einem Domänencontroller. Die Autorisierung der Verbindung führt NPS anhand der Einwähleigenschaften des für den Verbindungsversuch verwendeten Computer- oder Benutzerkontos und anhand der Netzwerkrichtlinien durch, die auf dem NPS-Server konfiguriert wurden.

NPS protokolliert alle RADIUS-Buchhaltungsinformationen in einer lokalen Protokolldatei (standardmäßig im Ordner `%SystemRoot%\System32\Logfiles`). Diese Einstellung lässt sich im Knoten *Kontoführung* des Netzwerkrichtlinienserver-Snap-Ins ändern.

Empfehlungen für die Authentifizierungsinfrastruktur

Für die Authentifizierungsinfrastruktur von geschützten Kabelnetzwerken wird Folgendes empfohlen:

- Um Authorisierungen für Kabelverbindungen besser verwalten zu können, legen Sie in Active Directory eine universelle Gruppe an. Diese Gruppe nimmt globale Gruppen mit den Benutzer- und Computerkonten auf, die im Kabelnetzwerk Verbindungen mit 802.1X-Authentifizierung herstellen dürfen. Legen Sie zum Beispiel eine universelle Gruppe namens *KabelKonten* an. Sie nimmt globale Gruppen auf, die Sie nach den Erfordernissen der Zuständigkeitsbereiche oder

Abteilungen Ihrer Organisation erstellen. Jede globale Gruppe enthält Benutzer- und Computerkonten, die für die Erstellung von Verbindungen im Kabelnetzwerk zugelassen sind. Wenn Sie Ihre NPS-Richtlinien für die Kabelverbindungen konfigurieren, geben Sie den Gruppennamen *KabelKonten* an.

- Starten Sie im Knoten *NPS* des Netzwerkrichtlinienserver-Snap-Ins den *802.1X konfigurieren*-Assistenten, um Richtlinien für die nach 802.1X authentifizierten Kabelverbindungen zu definieren. Erstellen Sie zum Beispiel Richtlinien für Kabelclients, die Mitglieder einer bestimmten Gruppe sind und eine bestimmte Authentifizierungsmethode verwenden sollen.

Kabelclients

Ein Windows-basierter Kabelclient ist ein Computer, auf dem Windows Server 2008, Windows Vista, Windows XP mit Service Pack 2 oder Windows Server 2003 ausgeführt wird. Auf Kabelclients, auf denen Windows Vista oder Windows Server 2008 verwendet wird, können Sie Kabelverbindungen auf folgende Art konfigurieren:

- **Gruppenrichtlinien** Die Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* ist Teil des Zweigs *Computerkonfiguration* eines Gruppenrichtlinienobjekts. Mit ihr können Sie in einer Active Directory-Umgebung Einstellungen für das verkabelte Netzwerk vornehmen. Diese Gruppenrichtlinienerweiterung ist aber nur auf Computern wirksam, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird.
- **Befehlszeile** Einstellungen für Verbindungen im Kabelnetzwerk können mit *Netsh.exe* vorgenommen werden. Rufen Sie *Netsh* mit dem Parameter *lan* und den übrigen erforderlichen Parametern auf.
- **XML-Kabelprofile** XML-Kabelprofile (Extensible Markup Language) sind XML-Dateien, die Einstellungen für ein herkömmlich verkabeltes Netzwerk enthalten. Diese Einstellungen können auf einem Windows Vista- oder Windows Server 2008-Kabelclient mit dem Programm *Netsh* exportiert und auf einem anderen Windows Vista- oder Windows Server 2008-Kabelclient importiert werden.

Sie können Windows-Kabelclients auf folgende Weise auch manuell konfigurieren:

- Auf einzelnen Kabelclients, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, können Sie das Dienste-Snap-In verwenden, um den Dienst *Automatische Konfiguration (verkabelt)* zu starten und für den automatischen Start zu konfigurieren. Anschließend wechseln Sie in den Ordner *Netzwerkverbindungen* und nehmen auf der Registerkarte *Authentifizierung* des Eigenschaftendialogfelds einer LAN-Verbindung die 802.1X-Authentifizierungseinstellung vor.
- In einer Active Directory-Domäne können Sie den Dienst für die automatische Konfiguration verkabelter Netzwerke mit Gruppenrichtlinien starten und für den automatischen Start konfigurieren. Stellen Sie die den Startmodus des Dienstes in *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Systemdienste\Automatische Konfiguration (verkabelt)* auf *Automatisch*.
- Wird auf dem Kabelclient Windows XP oder Windows Server 2003 ausgeführt, wechseln Sie in den Ordner *Netzwerkverbindungen* und nehmen die 802.1X-Authentifizierungseinstellung auf der Registerkarte *Authentifizierung* des Eigenschaftendialogfelds einer LAN-Verbindung vor.

Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)*

Um die Einstellungen von Windows-Clients für verkabelte Netzwerke automatisch vornehmen zu können, unterstützten Windows Server 2008- und Windows Server 2003-Active Directory-Domänen

eine Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)*. Diese Erweiterung ermöglicht es Ihnen, Einstellungen für verkabelte Netzwerke als Teil der *Computerkonfiguration* eines Gruppenrichtlinienobjekts durchzuführen. Sie können mit der Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* die EAP-Authentifizierungsmethode wählen und andere Einstellungen für Kabelclients vornehmen, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird.

Diese Einstellungen werden auf Kabelclients heruntergeladen und angewendet, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird und die Mitglieder einer Windows Server 2008- oder Windows Server 2003-Active Directory-Domäne sind. Eine Windows Server 2003-Active Directory-Domäne muss erweitert werden, um die neue Erweiterung unterstützen zu können.



Weitere Informationen Informationen über die Erweiterung einer Windows Server 2003-Active Directory-Domäne finden Sie in »Active Directory Schema Extensions for Windows Vista Wireless and Wired Group Policy Enhancements« unter <http://technet.microsoft.com/en-us/library/bb727029.aspx>.

Die Richtlinien für verkabelte Netzwerke können Sie im Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für verkabelte Netzwerke (IEEE 802.3)* des Snap-Ins Gruppenrichtlinienverwaltungs-Editor konfigurieren. Standardmäßig gibt es keine Richtlinien für verkabelte Netzwerke. Um eine neue Richtlinie zu erstellen, klicken Sie in der Konsolensicht des Gruppenrichtlinienverwaltungs-Editors den Knoten *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* mit der rechten Maustaste an und klicken dann auf *Eine neue Windows Vista-Richtlinie erstellen*.



Hinweis Um die Gruppenrichtlinieneinstellungen auf einem Computer zu ändern, auf dem Windows Server 2008 ausgeführt wird, müssen Sie vielleicht noch im Server-Manager die Gruppenrichtlinienverwaltungsfunktion installieren.

Das Eigenschaftendialogfeld einer Windows Vista-Richtlinie für verkabelte Verbindungen enthält die Registerkarten *Allgemein* und *Sicherheit*. Abbildung 11.2 zeigt die Registerkarte *Allgemein*.

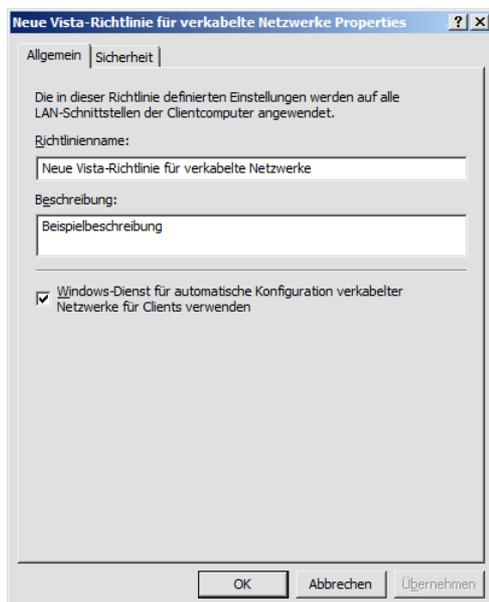


Abbildung 11.2 Die Registerkarte *Allgemein* einer Windows Vista-Richtlinie für verkabelte Netzwerke

Auf der Registerkarte *Allgemein* können Sie einen Namen und eine Beschreibung der Richtlinie eingeben und festlegen, ob der Windows-Dienst für die automatische Konfiguration verkabelter Netzwerke verwendet werden soll.

Abbildung 11.3 zeigt die Standardregisterkarte *Sicherheit* einer Windows Vista-Richtlinie für verkabelte Netzwerke.

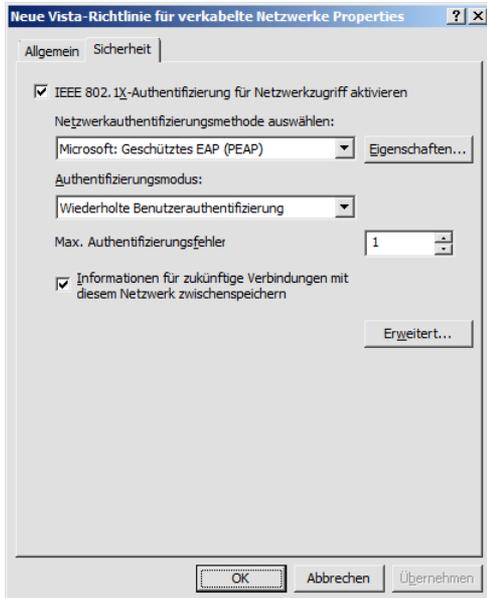


Abbildung 11.3 Die Registerkarte *Sicherheit* einer Windows Vista-Richtlinie für verkabelte Netzwerke

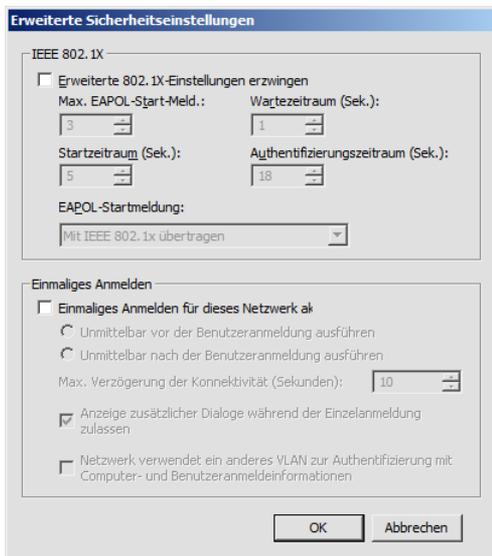


Abbildung 11.4 Das Dialogfeld *Erweiterte Sicherheitseinstellungen* einer Windows Vista-Richtlinie für verkabelte Netzwerke

Auf der Registerkarte *Sicherheit* können Sie die 802.1X-Authentifizierung aktivieren oder deaktivieren, die Authentifizierungsmethoden PEAP-MS-CHAP v2 oder EAP-TLS auswählen und konfigurieren, den Authentifizierungsmodus auswählen (*Wiederholte Benutzerauthentifizierung*, *Nur Computer, Benutzerauthentifizierung* oder *Gastauthentifizierung*) und die Zahl der Authentifizierungsversuche festlegen, die fehlschlagen dürfen, bevor die Authentifizierung abgebrochen wird. Außerdem können Sie noch entscheiden, ob die Informationen für zukünftige Verbindungen zwischengespeichert werden sollen. Ist das Kontrollkästchen für diese letzte Option nicht markiert, werden die Benutzeranmeldedaten aus der Registrierung gelöscht, sobald sich der Benutzer abmeldet. Die Folge ist, dass der Benutzer bei der nächsten Anmeldung zur Eingabe seiner Anmeldeinformationen aufgefordert wird (zum Beispiel zur Eingabe des Benutzernamens und des Kennworts).

Nach einem Klick auf die Schaltfläche *Erweitert* der Registerkarte *Sicherheit* können Sie erweiterte Einstellungen für 802.1X und für das einmalige Anmelden (Single Sign-On) vornehmen. Abbildung 11.4 zeigt das Standarddialogfeld *Erweiterte Sicherheitseinstellungen* einer Windows Vista-Richtlinie für verkabelte Netzwerke.

Im Dialogfeld *Erweiterte Sicherheitseinstellungen* können Sie folgende 802.1X-Einstellungen vornehmen:

- **Max. EAPOL-Start-Meld.** Die Anzahl der aufeinanderfolgenden EAPOL-Startnachrichten (EAPOL steht für EAP over LAN), die gesendet werden, wenn die erste EAPOL-Startnachricht unbeantwortet bleibt
- **Wartezeitraum** Der Zeitraum bis zur nächsten Sendung einer EAPOL-Startnachricht, wenn die zuvor ausgesendete EAPOL-Startnachricht unbeantwortet bleibt
- **Startzeitraum** Die Zeitraum, in dem der authentifizierende Client keine 802.1X-Authentifizierungsaktivität entwickelt, nachdem er vom Authentifizierer die Meldung über eine fehlerhafte Authentifizierung erhalten hat
- **Authentifizierungszeitraum** Der Zeitraum, den der authentifizierende Client wartet, bevor er eine 802.1X-Anfrage erneut sendet, nachdem eine Endpunkt-zu-Endpunkt-802.1X-Authentifizierung eingeleitet wurde

Kabelclients, auf denen Windows Vista mit SP1 oder Windows Server 2008 ausgeführt wird, unterstützen bei verkabelten Verbindungen das einmalige Anmelden (Single Sign-On). In der Erweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* können folgende Einstellungen für das einmalige Anmelden vorgenommen werden:

- **Unmittelbar vor der Benutzeranmeldung ausführen** Vor der Benutzeranmeldung eine 802.1X-Benutzerauthentifizierung durchführen.
- **Unmittelbar nach der Benutzeranmeldung ausführen** Nach der Benutzeranmeldung eine 802.1X-Benutzerauthentifizierung durchführen.
- **Max. Verzögerung der Konnektivität (Sekunden)** Die angegebene Anzahl an Sekunden warten, damit die 802.1X-Benutzerauthentifizierung abgeschlossen werden kann, bevor die Benutzeranmeldung beginnt.
- **Anzeige zusätzlicher Dialoge während der Einzelanmeldung zulassen** Zusätzliche Dialogfelder für die Benutzerauthentifizierung anzeigen, die über die üblichen Eingabefelder des Windows-Anmeldebildschirms hinausgehen. Wenn zum Beispiel ein EAP-Typ vom Benutzer die Bestätigung des Zertifikats erwartet, das der RADIUS-Server bei der Authentifizierung übermittelt hat, kann zu diesem Zweck ein Dialogfeld angezeigt werden.

- **Netzwerk verwendet ein anderes VLAN für die Authentifizierung mit Computer- und Benutzeranmeldeinformationen** Nach der Durchführung der Benutzerauthentifizierung wird eine DHCP-Erneuerung (Dynamic Host Configuration Protocol) der TCP/IP-Konfiguration (Transmission Control Protocol/Internet Protocol) des Kabelnetzwerkadapters eingeleitet. Wählen Sie diese Option, wenn es für Kabelclients, die auf Computer- oder Benutzerebene authentifiziert werden, unterschiedliche VLANs gibt und sich diese VLANs in verschiedenen IPv4- oder IPv6-Subnetzen befinden.

Informationen über die Verwendung der einmaligen Anmeldung finden Sie im Abschnitt »Authentifizierungsmodi im Kabelnetzwerk« dieses Kapitels.

Konfiguration auf der Befehlszeile

Unter Windows Vista und Windows Server 2008 können Sie einige der Einstellungen, die in den Eigenschaftendialogfeldern der verkabelten Verbindungen aus dem Ordner *Netzwerkverbindungen* oder in der Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* erfolgen, auch auf einer Befehlszeile vornehmen. Die Konfiguration der Kabelnetzwerke auf der Befehlszeile kann in folgenden Situationen die Bereitstellung von verkabelten Netzwerken erleichtern:

- **Automatisches Einstellen der Kabelnetzwerke mit Skripten (ohne Gruppenrichtlinien)** Die Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* ist nur in einer Active Directory-Domäne wirksam. In einer Umgebung, in der es keine Gruppenrichtlinieninfrastruktur gibt, kann ein Skript verwendet werden, das die Konfiguration der Kabelverbindungen automatisch durchführt. Das Skript lässt sich manuell starten oder automatisch, zum Beispiel im Rahmen eines Anmeldeskripts bei der Anmeldung.
- **Hinzufügen eines Kabelclients zum geschützten verkabelten Netzwerk einer Organisation** Ein Kabelclientcomputer, der kein Mitglied der Domäne ist, kann keine Verbindung mit dem durch eine 802.1X-Authentifizierung geschützten Kabelnetzwerk der Organisation aufnehmen. Der Computer kann aber erst dann ein Mitglied der Domäne werden, wenn er erfolgreich eine Verbindung mit dem geschützten Kabelnetzwerk der Organisation hergestellt hat. Ein Befehlszeilenskript bietet eine Methode, um eine Verbindung mit dem geschützten Kabelnetzwerk einer Organisation herzustellen und der Domäne beizutreten.

Um die Konfiguration von Kabelclients durchzuführen, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, geben Sie den Befehl `netsh lan` mit den entsprechenden Parametern ein.



Weitere Informationen Weitere Informationen über die Syntax des Befehls `netsh lan` finden Sie in »Netsh Commands for Wireless Local Area Network (LAN)« unter <http://technet.microsoft.com/en-us/windowsvista/aa905084.aspx>.

XML-Kabelnetzwerkprofile

Um für Kabelclients, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, die Konfiguration auf der Befehlszeile zu erleichtern, können Sie die Konfiguration eines Kabelprofils in eine XML-Datei exportieren, die sich anschließend auf anderen Kabelclients importieren lässt. Sie können ein Kabelprofil auf dem Kabelclient mit dem Befehl `netsh lan export profile` exportieren. Für den Import eines Kabelprofils verwenden Sie den Befehl `netsh lan add profile`.



Weitere Informationen Beispiele für die Profile von verkabelten Verbindungen finden Sie in »Wired Profile Samples« unter <http://msdn2.microsoft.com/en-us/library/aa816372.aspx>.

Anforderungen an Kabelclients

Kabelclients müssen bestimmte Voraussetzungen erfüllen:

- Die Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* wirkt nur auf Computern, auf denen Windows Server 2008 oder Windows Vista verwendet wird. Anders als bei der Gruppenrichtlinienerweiterung *Drahtlosnetzwerkrichtlinien (IEEE 802.11)* unterstützen Computer, auf denen Windows XP oder Windows Server 2003 ausgeführt wird, keine Konfiguration der Authentifizierung im Kabelnetzwerk auf Gruppenrichtlinienbasis.
- Eine einmalige Anmeldung (Single Sign-On) wird nur von Kabelclients unterstützt, auf denen Windows Vista mit SP1 oder Windows Server 2008 ausgeführt wird.
- Um eine 802.1X-Erzwingung mit Netzwerkzugriffsschutz bereitzustellen, müssen Sie Ihre Kabelclients auf eine Authentifizierungsmethode auf der Basis von PEAP einstellen.

Empfehlungen für Kabelclients

Für Kabelclients gelten folgende Empfehlungen:

- Wenn nur eine kleine Anzahl von Kabelclients eingerichtet werden muss, können Sie die Clients manuell konfigurieren oder die Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* verwenden.
- Für die Bereitstellung eines Kabelnetzwerks in einer Active Directory-Umgebung für eine mittlere oder große Organisation verwenden Sie die Gruppenrichtlinienerweiterung *Richtlinien für verkabelte Netzwerke (IEEE 802.3)*.
- Für eine Bereitstellung eines Kabelnetzwerks mit Skripten für eine mittlere oder große Organisation erstellen Sie XML-Kabelprofile und konfigurieren die Kabelclients mit einem Skript, das den Befehl `netsh lan add profile` enthält.

PKI

Um Kabelverbindungen mit EAP-TLS authentifizieren zu können, muss eine PKI (Public Key Infrastructure) vorhanden sein, die für Kabelclients Computer- und Benutzerzertifikate ausstellen kann, und für RADIUS-Server Computerzertifikate. Für eine Authentifizierung auf der Basis von PEAP-MS-CHAP v2 ist keine PKI erforderlich, um Computerzertifikate für RADIUS-Server auszustellen. Es ist auch möglich, von einem anderen Anbieter Zertifikate zu kaufen und auf den RADIUS-Servern zu installieren. Allerdings müssen Sie dann wahrscheinlich auch das Stammzertifizierungsstellenzertifikat der Computerzertifikate dieses Anbieters auf Ihren Kabelclientcomputern installieren.

PKI für Smartcards

Die Verwendung von Smartcards zur Benutzerauthentifizierung stellt unter Windows die sicherste Form der Benutzerauthentifizierung dar. Für Kabelverbindungen können Sie bei den Authentifizierungsmethoden EAP-TLS oder PEAP-TLS Smartcards einsetzen. Die einzelnen Smartcards werden an Benutzer ausgegeben, die über einen Computer mit einem Smartcardleser verfügen. Um sich am Computer anzumelden, muss der Benutzer die Smartcard in den Smartcardleser einlegen und eine PIN (Personal Identification Number) eingeben. Wenn der Benutzer versucht, eine verkabelte Verbindung herzustellen, wird im Zuge dieses Vorgangs auch das Smartcardzertifikat übermittelt. Weitere Informationen über die Verwendung von Smartcards finden Sie im Hilfe und Support-System von Windows Server 2008.

PKI für Benutzerzertifikate

Statt Smartcards können auch Benutzerzertifikate zur Benutzerauthentifizierung verwendet werden, die in der Windows-Registrierung gespeichert wurden. Allerdings ist diese Art der Authentifizierung nicht so sicher wie eine Smartcard. Wird eine Smartcard verwendet, steht das ausgestellte Benutzerzertifikat nur dann zur Authentifizierung zur Verfügung, wenn der Benutzer im Besitz der Smartcard ist und die PIN kennt, mit der die Anmeldung am Computer erfolgt. Bei der Verwendung von Benutzerzertifikaten steht das Benutzerzertifikat zur Authentifizierung zur Verfügung, wenn sich der Benutzer mit einem Domänenbenutzernamen und dem dazugehörigen Kennwort am Computer anmeldet. Wie Smartcards können Benutzerzertifikate bei der Authentifizierung von Kabelnetzwerkverbindungen mit der Authentifizierungsmethode EAP-TLS verwendet werden.

Um Ihre Organisationen mit Benutzerzertifikaten zu versorgen, gehen Sie folgendermaßen vor:

1. Stellen Sie eine PKI bereit.
2. Installieren Sie für jeden Benutzer ein Benutzerzertifikat. Am einfachsten ist dies, wenn die Windows-Zertifikatdienste als Unternehmenszertifizierungsstelle installiert werden. Dann konfigurieren Sie mit Gruppenrichtlinien eine automatische Registrierung für die Ausstellung von Benutzerzertifikaten. Weitere Informationen finden Sie im Verlauf dieses Kapitels im Abschnitt »Bereitstellen von Zertifikaten«.

Wenn der Kabelclient für eine verkabelte Verbindung eine Benutzerauthentifizierung durchführen möchte, übermittelt der Kabelclient im Rahmen dieses Vorgangs das Benutzerzertifikat.

PKI für Computerzertifikate

Computerzertifikate werden für die Computerauthentifizierung von verkabelten Verbindungen mit der Authentifizierungsmethode EAP-TLS verwendet und in der Windows-Registrierung gespeichert. Um Ihre Organisationen mit Computerzertifikaten zu versorgen, gehen Sie folgendermaßen vor:

1. Stellen Sie eine PKI bereit.
2. Installieren Sie auf jedem verkabelten Clientcomputer ein Computerzertifikat. Am einfachsten ist dies, wenn die Windows Active Directory-Zertifikatdienste oder die Zertifikatdienste als Unternehmenszertifizierungsstelle installiert werden. Dann konfigurieren Sie mit Gruppenrichtlinien eine automatische Registrierung für die Ausstellung von Computerzertifikaten. Weitere Informationen finden Sie im Verlauf dieses Kapitels im Abschnitt »Bereitstellen von Zertifikaten« dieses Kapitels.

Wenn der Kabelclient für eine verkabelte Verbindung eine Computerauthentifizierung durchführen möchte, übermittelt der Kabelclient im Rahmen dieses Vorgangs das Computerzertifikat.

Anforderungen an eine PKI

Eine PKI für ein geschütztes Kabelnetzwerk muss einige Anforderungen erfüllen:

- Für eine Computerauthentifizierung mit EAP-TLS müssen Sie auf jedem Kabelclient ein Computerzertifikat installieren (auch *Maschinenzertifikat* genannt).
- Das Computerzertifikat des Kabelclients muss gültig sein und sich von NPS-Servern überprüfen lassen. Die NPS-Server müssen über ein Stammzertifizierungsstellenzertifikat für die Zertifizierungsstelle verfügen, die das Computerzertifikat des Kabelclients ausgestellt hat.
- Für eine Benutzerauthentifizierung mit EAP-TLS müssen Sie eine Smartcard verwenden oder auf jedem Kabelclient ein Benutzerzertifikat installieren.

- Die Smartcard- oder die Benutzerzertifikate der Kabelclients müssen gültig sein und sich von den NPS-Servern überprüfen lassen. Die NPS-Server müssen über ein Stammzertifizierungsstellenzertifikat für die Zertifizierungsstellen verfügen, die die Smartcard- oder Benutzerzertifikate der Kabelclients ausgestellt haben.
- Sie müssen auf jedem verkabelten Client das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle der Computerzertifikate der NPS-Server installieren.
- Die Computerzertifikate der NPS-Server müssen gültig und für jeden Kabelclient überprüfbar sein. Die Kabelclients müssen über das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstellen verfügen, die die Computerzertifikate der NPS-Server ausgestellt haben.
- Für eine EAP-TLS-Authentifizierung müssen das Benutzer-, Smartcard- oder Computerzertifikat des Kabelclients folgende Bedingungen erfüllen:
 - Das Zertifikat muss einen geheimen Schlüssel enthalten.
 - Das Zertifikat muss von einer Unternehmenszertifizierungsstelle ausgestellt oder in Active Directory mit einem Benutzer- oder Computerkonto verknüpft worden sein.
 - Für das Zertifikat muss auf dem NPS-Server eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle bestehen und es muss alle Prüfungen bestehen, die vom CryptoAPI durchgeführt und in den Netzwerkrichtlinien für verkabelte Verbindungen angegeben werden.
 - Das Zertifikat muss für die Clientauthentifizierung vorgesehen sein (es enthält im Feld *Erweiterte Schlüsselverwendung* den Eintrag *Clientauthentifizierung* mit der Objektkennung 1.3.6.1.5.5.7.3.2).
 - Das Feld *Alternativer Antragstellername* muss den Benutzerprinzipalnamen (User Principal Name, UPN) des Benutzer- oder Computerkontos enthalten.
- Für eine EAP-TLS-Authentifizierung muss das Computerzertifikat des NPS-Servers folgende Bedingungen erfüllen:
 - Das Zertifikat muss einen geheimen Schlüssel enthalten.
 - Das Feld *Antragsteller* muss einen Wert enthalten.
 - Für das Zertifikat muss auf den Kabelclients eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle bestehen und es muss alle Prüfungen bestehen, die vom CryptoAPI durchgeführt und in den Netzwerkrichtlinien für verkabelte Verbindungen angegeben werden.
 - Das Zertifikat muss für die Serverauthentifizierung vorgesehen sein (es enthält im Feld *Erweiterte Schlüsselverwendung* den Eintrag *Serverauthentifizierung* mit der Objektkennung 1.3.6.1.5.5.7.3.1).
 - Das Zertifikat muss mit dem erforderlichen CSP-Wert (Cryptographic Service Provider) des Anbieters Microsoft RSA SChannel Cryptographic Provider konfiguriert sein.
 - Wird das Feld *Alternativer Antragstellername* des Zertifikats benutzt, muss es den DNS-Namen des NPS-Servers enthalten.

Empfehlungen für eine PKI

Für eine PKI, die den geschützten Zugriff im Kabelnetzwerk ermöglichen soll, gelten folgende Empfehlungen:

- Wenn Sie zur Erstellung von Computerzertifikaten für EAP-TLS eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle verwenden, konfigurieren Sie Ihre Active Directory-Domäne mit einer Computerkonfigurationsgruppenrichtlinie für die

automatische Registrierung von Computerzertifikaten. Jeder Computer, der Mitglied der Domäne ist, fordert dann nach der nächsten Aktualisierung der Computerkonfigurationsgruppenrichtlinien automatisch ein Computerzertifikat an.

- Wenn Sie zur Erstellung von Benutzerzertifikaten für EAP-TLS, die in der Registrierung gespeichert werden, eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle verwenden, konfigurieren Sie Ihre Active Directory-Domäne mit einer Benutzerkonfigurationsgruppenrichtlinie für die automatische Registrierung von Benutzerzertifikaten. Jeder Benutzer, der sich erfolgreich bei der Domäne anmeldet, fordert dann nach der nächsten Aktualisierung der Benutzerkonfigurationsgruppenrichtlinien automatisch ein Benutzerzertifikat an.
- Wenn Sie für Ihre NPS-Server von einem anderen Anbieter Computerzertifikate für die PEAP-MS-CHAP v2-Authentifizierung gekauft haben und die Kabelclients nicht über das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Computerzertifikats des NPS-Servers verfügen, sorgen Sie mit einer entsprechenden Gruppenrichtlinie dafür, dass das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Computerzertifikats des NPS-Servers auf Ihren Kabelclients installiert wird. Jeder Computer, der Mitglied der Domäne ist, erhält und installiert dann automatisch das Stammzertifizierungsstellenzertifikat, wenn die Computerkonfigurationsgruppenrichtlinien aktualisiert werden.
- Für die EAP-TLS- und PEAP-MS-CHAP v2-Authentifizierung ist es möglich, Kabelclients so einzustellen, dass sie das Zertifikat des NPS-Servers nicht überprüfen. In diesem Fall ist es nicht erforderlich, auf den NPS-Servern Computerzertifikate und auf den Kabelclients die dazugehörigen Stammzertifizierungsstellenzertifikate zu installieren. Allerdings wird es empfohlen, dass Kabelclients die Zertifikate des NPS-Servers überprüfen, damit sich Kabelclients und NPS-Server gegenseitig überprüfen können. Durch solch eine gegenseitige Authentifizierung können Sie Ihre Kabelclients davor schützen, eine Verbindung mit irgendeinem nichtautorisierten Switch herzustellen, der mit ebenfalls nichtautorisierten Zugriffsservern arbeitet.

802.1X-Erzwingung mit NAP

NAP für Windows Server 2008, Windows Vista und Windows XP mit Service Pack 3 bieten Komponenten und Programmierschnittstellen (Application Programming Interfaces, APIs), mit denen Sie die Einhaltung der Integritätsrichtlinien für den Netzwerkzugriff oder die Netzwerkkommunikation erzwingen können. Entwickler und Netzwerkadministratoren können Lösungen für die Überprüfung von Computern entwickeln, die Verbindungen mit ihren Netzwerken herstellen, erforderliche Updates oder den Zugriff auf erforderliche Ressourcen zur Verfügung stellen und den Zugriff durch nicht konforme Computer einschränken.

Die 802.1X-Erzwingung ist eine der NAP-Erzwingungsmethoden von Windows Server 2008, Windows Vista und Windows XP. Bei der 802.1X-Erzwingung muss ein mit 802.1X authentifizierter Kabelclient beweisen, dass er die Integritätsanforderungen des Systems erfüllt, bevor er Zugang zum Intranet erhält. Zu den Integritätsanforderungen kann zum Beispiel gehören, ein Antivirusprogramm zu verwenden. Hält ein Kabelclient die Integritätsanforderungen des Systems nicht ein, kann der 802.1X-fähige Switch den Kabelclient in ein eingeschränktes Netzwerk verschieben, in dem die erforderlichen Ressourcen verfügbar sind, um den Kabelclient so weit aufzurüsten, dass er die Integritätsregeln einhält. Der Switch erreicht diese Einschränkung des Zugriffs durch Paketfilter oder durch eine entsprechende VLAN-Kennung, die der Kabelverbindung zugewiesen wird. Nach der Korrektur des Integritätszustands kann der Kabelclient seinen Integritätszustand erneut überprüfen lassen. Sofern er konform ist, werden die Beschränkungen aufgehoben, denen er im eingeschränkten Teil des Kabelnetzwerks unterliegt.

Damit die 802.1X-Erzwingung funktioniert, müssen Sie über ein geschütztes Kabelnetzwerk mit 802.1X-Authentifizierung verfügen, das eine Authentifizierungsmethode auf der Basis von PEAP verwendet. Einzelheiten über die Bereitstellung der 802.1X-Erzwingung nach dem erfolgreichen Aufbau eines geschützten Kabelnetzwerks mit 802.1X-Authentifizierung finden Sie in Kapitel 17.

Bereitstellen des Kabelnetzwerkzugriffs mit 802.1X-Authentifizierung

Um mit Windows Server 2008 und Windows Vista ein verkabeltes Netzwerk mit 802.1X-Authentifizierung bereitzustellen, gehen Sie folgendermaßen vor:

- Stellen Sie die erforderlichen Zertifikate bereit.
- Konfigurieren Sie Active Directory für Konten und Gruppen.
- Konfigurieren Sie NPS-Server.
- Konfigurieren Sie 802.1X-fähige Switches.
- Konfigurieren Sie Kabelclients.

Bereitstellen von Zertifikaten

Sie müssen Zertifikate bereitstellen, wenn Sie Folgendes tun:

- **Computerauthentifizierung mit EAP-TLS und Computerzertifikaten** Jeder Kabelclient braucht ein Computerzertifikat.
- **Benutzerauthentifizierung mit EAP-TLS und Smartcard oder registrierungsbasierten Benutzerzertifikaten** Jeder Benutzer einer Kabelverbindung braucht eine Smartcard oder jeder Kabelclientcomputer braucht ein Benutzerzertifikat.
- **Benutzer- oder Computerauthentifizierung mit PEAP-MS-CHAP v2** Jeder Kabelclient braucht das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Computerzertifikats des NPS-Servers.

Für jede dieser Konfigurationen braucht jeder NPS-Server ein Computerzertifikat.

Bereitstellen von Computerzertifikaten

Zur Installation von Computerzertifikaten für eine EAP-TLS-Authentifizierung muss eine PKI vorhanden sein, die diese Zertifikate ausstellen kann. Sobald diese PKI vorhanden ist, können Sie auf folgende Weise auf Kabelclients und NPS-Servern Computerzertifikate installieren:

- Durch das Konfigurieren der automatischen Registrierung von Computerzertifikaten auf den Computern einer Active Directory-Domäne (empfohlen)
- Durch die Anforderung eines Computerzertifikats mit dem Zertifikate-Snap-In
- Durch den Import eines Computerzertifikats mit dem Zertifikate-Snap-In
- Durch die Ausführung eines CAPICOM-Skripts, das ein Computerzertifikat anfordert

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« von Kapitel 9.

Bereitstellen von Benutzerzertifikaten

Auf folgende Weise können Sie auf Kabelclients Benutzerzertifikate installieren:

- Durch das Konfigurieren der automatischen Registrierung von Benutzerzertifikaten für die Benutzer in einer Active Directory-Domäne (empfohlen)
- Durch die Anforderung eines Benutzerzertifikats mit dem Zertifikate-Snap-In
- Durch den Import eines Benutzerzertifikats mit dem Zertifikate-Snap-In
- Durch das Anfordern eines Zertifikats über das Web
- Durch die Ausführung eines CAPICOM-Skripts, das ein Benutzerzertifikat anfordert

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« von Kapitel 9.

Bereitstellen von Stammzertifizierungsstellenzertifikaten

Wenn Sie eine PEAP-MS-CHAP v2-Authentifizierung einsetzen, müssen Sie wahrscheinlich auf Ihren Kabelclients die Stammzertifizierungsstellenzertifikate der Computerzertifikate Ihrer NPS-Server installieren. Falls das Stammzertifizierungsstellenzertifikat des Ausstellers der Computerzertifikate, die auf den NPS-Servern installiert sind, bereits als Stammzertifizierungsstellenzertifikate auf Ihren Kabelclients installiert ist, ist keine weitere Konfiguration erforderlich. Handelt es sich bei Ihrer Stammzertifizierungsstelle zum Beispiel um eine Online-Stammzertifizierungsstelle auf der Basis von Windows Server 2008, wird das Stammzertifizierungsstellenzertifikat über Gruppenrichtlinien automatisch auf jedem Computer installiert, der Mitglied der Domäne ist.

Bei der Überprüfung, ob auf Ihren Kabelclients das korrekte Stammzertifizierungsstellenzertifikat installiert ist, müssen Sie auf zwei Punkte achten:

1. Wie heißt die Stammzertifizierungsstelle der Computerzertifikate, die auf den NPS-Servern installiert wurden?
2. Wurde auf Ihren Kabelclients ein Zertifikat der Stammzertifizierungsstelle installiert?

So bestimmen Sie die Stammzertifizierungsstelle der Computerzertifikate der NPS-Server

1. Erweitern Sie in der Strukturansicht des Zertifikate-Snap-Ins für das Computerkonto des NPS-Servers den Knoten *Zertifikate (Lokaler Computer oder Computername)*, erweitern Sie dann den Knoten *Eigene Zertifikate* und klicken Sie auf *Zertifikate*.
2. Klicken Sie im Detailbereich mit einem Doppelklick auf das Computerzertifikat, das vom NPS-Server für die PEAP-MS-CHAP v2-Authentifizierung verwendet wird.
3. Achten Sie im Eigenschaftendialogfeld *Zertifikate* auf der Registerkarte *Zertifizierungspfad* auf den Namen am Anfang des Zertifizierungspfads. Das ist der Name der Stammzertifizierungsstelle.

So finden Sie heraus, ob auf Ihrem Kabelclient ein Zertifikat von der Stammzertifizierungsstelle installiert ist

1. Erweitern Sie in der Strukturansicht des Zertifikate-Snap-Ins für das Computerkonto des Kabelclients den Knoten *Zertifikate (Lokaler Computer oder Computername)*, erweitern Sie dann den Knoten *Vertrauenswürdige Stammzertifizierungsstellen* und klicken Sie auf *Zertifikate*.
2. Überprüfen Sie im Detailbereich, ob in der Liste der Zertifikate der Name der Stammzertifizierungsstelle der Computerzertifikate zu finden ist, die für den NPS-Server ausgestellt wurden.

Sie müssen die Stammzertifizierungsstellenzertifikate der Herausgeber der Computerzertifikate der NPS-Server auf jedem Kabelclient installieren, auf dem sie noch nicht verfügbar sind. Am einfachsten

lassen sich Stammzertifizierungsstellenzertifikate über Gruppenrichtlinien auf allen Kabelclients installieren. Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« von Kapitel 9.

Konfigurieren von Active Directory für Konten und Gruppen

Zur Vorbereitung von Active Directory für den Zugriff im Kabelnetz konfigurieren Sie die Benutzer- und Computerkonten, die für die Authentifizierung der Kabelverbindungen verwendet werden, auf folgende Weise:

- Stellen Sie auf der Registerkarte *Einwählen* die Netzwerkzugriffsberechtigung auf *Zugriff gestatten* oder *Zugriff über NPS-Netzwerkrichtlinien steuern*. Bei dieser Einstellung wird der Zugang zum Netzwerk mit den NPS-Netzwerkrichtlinien gesteuert. Standardmäßig wird die Netzwerkzugriffsberechtigung in einheitlichen Domänen in neuen Benutzer- und Computerkonten auf *Zugriff über NPS-Netzwerkrichtlinien steuern* gestellt.
- Fassen Sie die Computer- und Benutzerkonten zu geeigneten universellen oder globalen Gruppen zusammen, um die Verwaltung des Netzwerkzugriffs zu vereinfachen.

Konfigurieren der NPS-Server

Konfigurieren Sie Ihre NPS-Server, wie in Kapitel 9 beschrieben. Gehen Sie dazu folgendermaßen vor:

1. Installieren Sie auf jedem NPS-Server ein Computerzertifikat.
2. Installieren Sie auf jedem NPS-Server bei Bedarf die Stammzertifizierungsstellenzertifikate der Computer- oder Benutzerzertifikate oder der Smartcardzertifikate der Kabelclients.
3. Falls Sie eine EAP-Methode verwenden, die auf Windows Server 2008 nicht verfügbar ist, installieren Sie diese Methode auf jedem NPS-Server.
4. Konfigurieren Sie auf dem primären NPS-Server die Protokollierung.
5. Fügen Sie zum primären NPS-Server die RADIUS-Clients (die 802.1X-fähigen Switches) hinzu.
6. Erstellen Sie auf dem primären NPS-Server die Richtlinien, die zusammen mit den Gruppen, zu denen die für Kabelverbindungszugriffe vorgesehenen Konten gehören, die Zugriffe im Kabelnetzwerk steuern.

Einzelheiten zu den Schritten 1 bis 4 finden Sie in Kapitel 9.

So erstellen Sie Richtlinien für Kabelverbindungen

1. Klicken Sie in der Strukturansicht des Netzwerkrichtlinienserver-Snap-Ins auf *NPS*.
2. Wählen Sie im Detailbereich aus der Dropdownliste unter *Standardkonfiguration* die Konfiguration *RADIUS-Server für drahtlose oder verkabelte 802.1X-Verbindungen* aus und klicken Sie dann auf *802.1X konfigurieren*.
3. Wählen Sie auf der Seite *802.1X-Verbindungstyp auswählen* des Assistenten zum Konfigurieren von 802.1X die Option *Sichere verkabelte (Ethernet)-Verbindungen* und geben Sie dann im Textfeld *Name* einen Namen für die Richtlinie ein (oder verwenden Sie den Namen, den der Assistent vorgibt). Klicken Sie auf *Weiter*.
4. Fügen Sie auf der Seite *802.1X-Switches angeben* nach Bedarf die RADIUS-Clients hinzu (in diesem Fall also Ihre 802.1X-fähigen Switches). Klicken Sie auf *Weiter*.

5. Stellen Sie auf der Seite *Authentifizierungsmethode konfigurieren* den gewünschten EAP-Typ ein, der für die verkabelten Verbindungen verwendet werden soll.

Zur Konfiguration von EAP-TLS wählen Sie in der Dropdownliste *Typ* den Eintrag *Microsoft: Smartcard- oder anderes Zertifikat* und klicken dann auf *Konfigurieren*. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* das Computerzertifikat aus, das für verkabelte Verbindungen verwendet werden soll, und klicken Sie dann auf *OK*. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Die SChannel-Unterstützung ist aber erforderlich, damit NPS das Zertifikat für die EAP-TLS-Authentifizierung verwenden kann.

Zur Konfiguration von PEAP-MS-CHAP v2 wählen Sie in der Dropdownliste *Typ* den Eintrag *Microsoft: Geschütztes EAP (PEAP)* und klicken dann auf *Konfigurieren*. Wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP bearbeiten* das Computerzertifikat aus, das für die verkabelten Verbindungen verwendet werden soll, und klicken Sie dann auf *OK*. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Die SChannel-Unterstützung ist aber erforderlich, damit NPS das Zertifikat für die PEAP-Authentifizierung verwenden kann.

Zur Konfiguration von PEAP-TLS wählen Sie in der Dropdownliste *Typ* den Eintrag *Microsoft: Geschütztes EAP (PEAP)* und klicken dann auf *Konfigurieren*. Wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP bearbeiten* das Computerzertifikat aus, das für die verkabelten Verbindungen verwendet werden soll. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Klicken Sie unter *EAP-Typen* auf *Gesichertes Kennwort (EAP-MSCHAP v2)* und dann auf *Entfernen*. Klicken Sie auf *Hinzufügen*. Klicken Sie im Dialogfeld *EAP hinzufügen* auf *Smartcard- oder anderes Zertifikat* und dann auf *OK*. Klicken Sie im Dialogfeld *Eigenschaften für geschütztes EAP bearbeiten* unter *EAP-Typen* auf *Smartcard- oder anderes Zertifikat* und klicken Sie dann auf *Bearbeiten*. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* das Computerzertifikat aus, das für die verkabelten Verbindungen verwendet werden soll, und klicken Sie dann auf *OK*. Wenn Sie das Zertifikat nicht auswählen können, unterstützt der Kryptografiedienstanbieter für das Zertifikat SChannel (Secure Channel) nicht. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

6. Klicken Sie auf *Weiter*. Fügen Sie auf der Seite *Benutzergruppen angeben* die Gruppen mit den Konten für verkabelte Computer und Benutzer hinzu (beispielsweise eine von Ihnen definierte Gruppe *KabelKonten*).
7. Klicken Sie auf der Seite *VLAN (virtuelles LAN) konfigurieren* auf *Konfigurieren*, falls Sie RADIUS-Attribute und deren Werte angeben möchten, mit denen Ihre 802.1X-fähigen Switches für das passende VLAN konfiguriert werden. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Abschließen neuer sicherer verkabelter und drahtloser IEEE 802.1X-Verbindungen und RADIUS-Clients* auf *Fertig stellen*.

Der Assistent zum Konfigurieren von 802.1X erstellt eine Verbindungsanforderungsrichtlinie und eine Netzwerkrichtlinie für die verkabelte Verbindung. Der Assistent zum Konfigurieren von 802.1X konfiguriert die Netzwerkrichtlinie mit nur einer EAP-Methode. Wenn Sie weitere EAP-Methoden benötigen, können Sie im Eigenschaftendialogfeld der Netzwerkrichtlinie weitere EAP-Methoden konfigurieren.

Nachdem Sie auf dem primären NPS-Server die gewünschte Protokollierung eingestellt, die RADIUS-Clients hinzugefügt und die Sicherheitseinstellungen vorgenommen haben, kopieren Sie die Konfigu-

ration auf den sekundären und auf alle weiteren vorgesehenen NPS-Server. Weitere Informationen finden Sie in Kapitel 9.

Konfigurieren von 802.1X-fähigen Switches

Konfigurieren Sie Ihre 802.1X-fähigen Switches mit folgenden Werten:

- Einer statischen IPv4-Adresse, eine Subnetzmaske und ein Standardgateway für das Subnetz, zu dem der Switch gehört
- VLANs nach Bedarf
- Den folgenden RADIUS-Einstellungen:
 - Die IPv4-Adresse, IPv6-Adresse oder den DNS-Namen eines primären RADIUS-Servers, das gemeinsame geheime RADIUS-Kennwort, die UDP-Ports für die Authentifizierung und Kontoführung sowie die Einstellungen für die Fehlererkennung
 - Die IPv4-Adresse, IPv6-Adresse oder den DNS-Namen eines sekundären RADIUS-Servers, das gemeinsame geheime RADIUS-Kennwort, die UDP-Ports für die Authentifizierung und Kontoführung sowie die Einstellungen für die Fehlererkennung

Um den RADIUS-Datenverkehr gleichmäßig zwischen den beiden NPS-Servern aufzuteilen, konfigurieren Sie die Hälfte der 802.1X-fähigen Switches mit dem primären NPS-Server als primären RADIUS-Server und dem sekundären NPS-Server als sekundären RADIUS-Server. Dann konfigurieren Sie die andere Hälfte der 802.1X-fähigen Switches mit dem sekundären NPS-Server als primären RADIUS-Server und dem primären NPS-Server als sekundären RADIUS-Server.

Falls die 802.1X-fähigen Switches für spezielle Funktionen oder angepasste Konfigurationen herstellerspezifische Attribute (Vendor-Specific Attributes, VSAs) oder zusätzliche RADIUS-Attribute erfordern, müssen Sie die herstellerspezifischen Attribute oder RADIUS-Attribute zu den Kabelnetzwerkrichtlinien der NPS-Server hinzufügen. Wenn Sie die herstellerspezifischen Attribute oder RADIUS-Attribute zu den Kabelnetzwerkrichtlinien des primären NPS-Servers hinzugefügt haben, können Sie die Konfiguration des primären NPS-Servers auf den sekundären NPS-Server übertragen.

Direkt von der Quelle: RADIUS-Attribute für VLANs

Wenn Ihre Netzwerkgeräte mit virtuellen lokalen Netzwerken (VLANs, Virtual Local Area Networks) arbeiten können, beispielsweise Routern, Switches und Zugriffscontrollern, können Sie NPS-Netzwerkrichtlinien konfigurieren, mit denen die Zugriffsserver angewiesen werden, Mitglieder von Active Directory-Gruppen diesen VLANs zuzuordnen.

Bevor Sie in NPS Netzwerkrichtlinien für VLANs konfigurieren, definieren Sie in Active Directory Gruppen, die Sie bestimmten VLANs zuordnen möchten. Wenn Sie dann die NPS-Netzwerkrichtlinie für das verkabelte Netzwerk erstellen, fügen Sie eine Gruppe als Bedingung zur Netzwerkrichtlinie hinzu. Sie können für jede Gruppe, die Sie einem VLAN zuordnen möchten, eine separate NPS-Netzwerkrichtlinie erstellen.

Wenn Sie eine Netzwerkrichtlinie für VLANs erstellen, müssen Sie die RADIUS-Standardattribute Tunnel-Medium-Type, Tunnel-Pvt-Group-ID und Tunnel-Type konfigurieren. Einige Hardwarehersteller verlangen außerdem die Verwendung des RADIUS-Standardattributs Tunnel-Tag.

Diese Attribute lassen sich auf der Seite *VLAN (virtuelles LAN) konfigurieren* des Assistenten zum Konfigurieren von 802.1X für eine NPS-Netzwerkrichtlinie konfigurieren. Sie können die Attribute auch nachträglich konfigurieren, nachdem Sie mit dem Assistenten eine Netzwerkrichtlinie erstellt haben.

Fügen Sie auf der Seite *VLAN (virtuelles LAN) konfigurieren* des Assistenten zum Konfigurieren von 802.1X die folgenden RADIUS-Standardattribute und nach Bedarf herstellerspezifische RADIUS-Attribute hinzu:

- **Tunnel-Medium-Type** Wählen Sie den Wert: *802 (includes all 802 media plus Ethernet canonical format)*.
- **Tunnel-Pvt-Group-ID** Geben Sie die Nummer des VLANs, dem die Gruppenmitglieder zugeordnet werden, als ganze Zahl ein. Wenn Ihr Verkaufs-VLAN beispielsweise VLAN 4 ist, geben Sie die Zahl 4 ein.
- **Tunnel-Type** Wählen Sie den Wert *Virtual LANs (VLAN)*.
- **Tunnel-Tag** Einige Hardwaregeräte verwenden dieses Attribut nicht. Falls Ihr Gerät dieses Attribut verwendet, finden Sie den entsprechenden Wert in der Dokumentation Ihrer Hardware.



Hinweis Um diese Attribute nach der Erstellung der Netzwerkrichtlinie hinzuzufügen, erweitern Sie in der Konsole Netzwerkrichtlinienserver den Knoten *Richtlinien* und klicken auf *Netzwerkrichtlinien*. Klicken Sie die gesuchte Richtlinie im Detailbereich mit der rechten Maustaste an und klicken Sie dann auf *Eigenschaften*. Im Eigenschaftendialogfeld der Richtlinie klicken Sie auf die Registerkarte *Einstellungen*. Sorgen Sie dafür, dass unter *RADIUS-Attribute* die Option *Standard* gewählt ist, und klicken Sie auf *Hinzufügen*. Fügen Sie im Dialogfeld *Standard-RADIUS-Attribut hinzufügen* die Attribute *Tunnel-Medium-Type*, *Tunnel-Pvt-Group-ID* und *Tunnel-Type* hinzu. Wählen Sie unter *RADIUS-Attribute* die Option *Herstellerspezifisch* und klicken Sie dann auf *Hinzufügen*. Fügen Sie im Dialogfeld *Herstellerspezifisches Attribut hinzufügen* das Attribut *Tunnel-Tag* hinzu.

*James McIllece, Technical Writer
Windows Server User Assistance*

Konfigurieren verkabelter Clients

Die Clients eines verkabelten Netzwerks können Sie auf folgende drei Arten konfigurieren:

- Mit Gruppenrichtlinien
- Mit XML-Kabelprofilen
- Manuell

Konfigurieren verkabelter Clients durch Gruppenrichtlinien

Zur Einstellung der Gruppenrichtlinien für verkabelte Netzwerke gehen Sie folgendermaßen vor:

1. Öffnen Sie auf einem Computer, auf dem Windows Server 2008 ausgeführt wird und der Mitglied Ihrer Active Directory-Domäne ist, das Snap-In Gruppenrichtlinienverwaltung.
2. Erweitern Sie in der Strukturansicht *Gesamtstruktur*, erweitern Sie *Domänen* und klicken Sie dann auf den Namen der Domäne, zu der Ihre verkabelten Clients gehören.
3. Klicken Sie auf der Registerkarte *Verknüpfte Gruppenrichtlinienobjekte* das entsprechende Gruppenrichtlinienobjekt mit der rechten Maustaste an (das Standardobjekt ist *Default Domain Policy*) und klicken Sie dann auf *Bearbeiten*.

4. Erweitern Sie in der Strukturansicht des Snap-Ins Gruppenrichtlinienverwaltungs-Editor den Knoten des Gruppenrichtlinienobjekts und wechseln Sie dann zu *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Systemdienste*. Klicken Sie im Detailbereich mit einem Doppelklick auf *Automatische Konfiguration (verkabelt)*. Wählen Sie im Dialogfeld *Eigenschaften von Automatische Konfiguration (verkabelt)* das Kontrollkästchen *Diese Richtlinieneinstellung definieren*, wählen Sie dann *Automatisch* und klicken Sie auf *OK*.
5. Wechseln Sie in der Strukturansicht zum Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für verkabelte Netzwerke (IEEE 802.3)*.
6. Klicken Sie *Richtlinien für verkabelte Netzwerke (IEEE 802.3)* mit der rechten Maustaste an und klicken Sie dann auf *Eine neue Windows Vista-Richtlinie erstellen*.
7. Geben Sie auf der Registerkarte *Allgemein* einen Namen und eine Beschreibung für die Richtlinie ein. Falls Sie mehr Informationen brauchen, drücken Sie auf *F1*.
8. Wählen Sie auf der Registerkarte *Sicherheit* den EAP-Typ und den Authentifizierungsmodus und nehmen Sie alle erforderlichen Einstellungen vor. Falls Sie mehr Informationen brauchen, drücken Sie auf *F1*.

Für eine EAP-TLS-Authentifizierung wählen Sie *Smartcard- oder anderes Zertifikat* und klicken dann auf *Eigenschaften*. Im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* nehmen Sie nach Bedarf die EAP-TLS-Einstellungen vor und klicken dann auf *OK*. Standardmäßig verwendet EAP-TLS ein Zertifikat auf Registrierungsbasis und überprüft das Serverzertifikat.

Für eine PEAP-MS-CHAP v2 ist keine zusätzliche Konfiguration erforderlich. PEAP-MS-CHAP v2 ist die Standardauthentifizierungsmethode.

9. Klicken Sie auf *OK*.

Wenn Ihre Kabelclients mit Windows Server 2008 oder Windows Vista das nächste Mal die Computerkonfigurations-Gruppenrichtlinien aktualisieren, werden die Einstellungen für verkabelte Netzwerke aus dem Gruppenrichtlinienobjekt automatisch angewendet. Sie können die Aktualisierung eines vorhandenen Gruppenrichtlinienobjekts auch manuell einleiten, indem Sie in einer Eingabeaufforderung den Befehl `gpupdate` verwenden. Handelt es sich um ein neues Gruppenrichtlinienobjekt, müssen Sie den verkabelten Client neu starten.

Nach der Anwendung der Richtlinien für verkabelte Netzwerke zeigt die Registerkarte *Authentifizierung* des Eigenschaftendialogfelds einer LAN-Verbindung die Meldung »Diese Einstellungen werden vom Administrator verwaltet« und Benutzer können die Einstellungen auf der Registerkarte *Authentifizierung* nicht ändern (das Eigenschaftendialogfeld der LAN-Verbindung ist zum Beispiel über den Ordner *Netzwerkverbindungen* zugänglich).

Konfigurieren und Bereitstellen von Kabelprofilen

Sie können Kabelclients, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, auch für ein Kabelnetzwerk konfigurieren, indem Sie mit dem Befehl `netsh lan add profile` ein Kabelprofil importieren, das im XML-Format vorliegt. Um eine XML-Datei mit dem Profil der verkabelten Verbindung zu erstellen, konfigurieren Sie einen Client, auf dem Windows Vista oder Windows Server 2008 ausgeführt wird, mit allen für ein Kabelnetzwerk erforderlichen Einstellungen, einschließlich der Authentifizierungsmethode, der Verschlüsselungsmethoden und dem EAP-Typ. Dann exportieren Sie diese Konfiguration mit dem Befehl `netsh lan export profile` in eine XML-Datei.

Direkt von der Quelle: Kontrolle der Authentifizierungs- und Anforderungsmodi

In Windows XP haben wir einen Teil des Verhaltens bei Authentifizierungen und Anforderungen mit den Registrierungswerten `AuthMode` und `SupplicantMode` gesteuert. Unter Windows Vista steuern wir das Verhalten nun direkt in den Profilen. In der Registrierung von Windows Vista gibt es also keine entsprechenden `AuthMode`- und `SupplicantMode`-Werte mehr. Für den Anforderungsmodus unter Windows XP würden wir den Wert ändern, damit ein 802.1X-fähiger Client eine Authentifizierung mit einem passiven Switch einleiten kann. Unter Windows Vista ist die Standardeinstellung, alle 802.1X-Authentifizierungsversuche einzuleiten. Daher gibt es keinen Grund, diese Einstellung unter Windows Vista zu ändern. Der Registrierungswert `AuthMode` wird in Windows XP dazu benutzt, das Verhalten bei der Computerauthentifizierung zu steuern. In erster Linie dient der Wert dazu, bei Bedarf Benutzerauthentifizierungen zu beschränken. Um dies unter Windows Vista zu ändern, müssen Sie die entsprechende Datei exportieren und den resultierenden XML-Code bearbeiten. Bei einem Standardprofil sollten Sie die folgende Zeile aus dem Element `OneX` ändern, und zwar von

```
<authMode>machineOrUser</authMode>
```

nach

```
<authMode>machine</authMode>
```

*Clay Seymour, Support Escalation Engineer
Enterprise Platform Support*

Manuelles Konfigurieren verkabelter Clients

Wenn Sie nur eine kleine Anzahl verkabelter Clients konfigurieren müssen, können Sie die LAN-Einstellungen auf jedem Client manuell vornehmen. Die Registerkarte *Authentifizierung* wird auf Clients, auf denen Windows Server 2008 oder Windows Vista ausgeführt wird, durch den Dienst *Automatische Konfiguration (verkabelt)* aktiviert. Da dieser Dienst nicht automatisch gestartet wird, erscheint auch die Registerkarte *Authentifizierung* für LAN-Verbindungen nicht automatisch. Sie müssen den Dienst *Automatische Konfiguration (verkabelt)* im Dienste-Snap-In für den automatischen Start konfigurieren. Für verkabelte Clients, auf denen Windows XP oder Windows Server 2003 ausgeführt wird, wird die Registerkarte *Authentifizierung* vom Dienst *Konfigurationsfreie drahtlose Verbindung* aktiviert, der standardmäßig gestartet wird.

Die folgenden Abschnitte beschreiben, wie Sie die EAP-TLS- und PEAP-MS-CHAP v2-Authentifizierung manuell für verkabelte Windows-Clients konfigurieren können.

EAP-TLS

Um manuell eine EAP-TLS-Authentifizierung auf einem verkabelten Client zu konfigurieren, auf dem Windows Server 2008 oder Windows Vista ausgeführt wird, gehen Sie folgendermaßen vor:

1. Klicken Sie im Ordner *Netzwerkverbindungen* Ihre LAN-Verbindung mit der rechten Maustaste an und klicken Sie dann auf *Eigenschaften*.
2. Klicken Sie auf die Registerkarte *Authentifizierung* und klicken Sie dann auf *IEEE 802.1X-Authentifizierung aktivieren*. In der Dropdownliste *Wählen Sie eine Methode für die Netzwerkauthentifizierung aus* wählen Sie *Smartcard- oder anderes Zertifikat* und klicken dann auf *Einstellungen*.

3. Im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* wählen Sie *Zertifikat auf diesem Computer verwenden*, wenn Sie ein in der Registrierung eingetragenes Benutzerzertifikat verwenden möchten, oder *Eigene Smartcard verwenden*, falls das Benutzerzertifikat auf einer Smartcard gespeichert ist.

Wenn Sie das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Wenn Sie die Namen der NPS-Server angeben möchten, die die TLS-Authentifizierung durchführen müssen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Um manuell eine EAP-TLS-Authentifizierung auf einem verkabelten Client zu konfigurieren, auf dem Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 ausgeführt wird, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der LAN-Verbindung.
2. Klicken Sie auf die Registerkarte *Authentifizierung* und sorgen Sie dafür, dass das Kontrollkästchen *IEEE 802.1X-Authentifizierung für dieses Netzwerk aktivieren* aktiviert und der EAP-Typ *Smartcard- oder anderes Zertifikat* gewählt ist. (Das sind die vorgegebenen Standardeinstellungen.)
3. Klicken Sie auf *Eigenschaften*. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* die Option *Zertifikat auf diesem Computer verwenden*, wenn Sie ein Benutzerzertifikat auf Registrierungsbasis verwenden möchten, oder die Option *Eigene Smartcard verwenden*, wenn ein Benutzerzertifikat verwendet werden soll, das auf einer Smartcard gespeichert ist.

Wenn Sie das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie *Serverzertifikat überprüfen* (empfohlen und standardmäßig aktiviert). Falls Sie die Namen der Authentifizierungsserver angeben möchten, die die TLS-Authentifizierung durchführen sollen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein. Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

PEAP-MS-CHAP v2

Um manuell eine PEAP-MS-CHAP v2-Authentifizierung auf einem verkabelten Client zu konfigurieren, auf dem Windows Server 2008 oder Windows Vista ausgeführt wird, gehen Sie folgendermaßen vor:

1. Klicken Sie im Ordner *Netzwerkverbindungen* Ihre LAN-Verbindung mit der rechten Maustaste an und klicken Sie dann auf *Eigenschaften*.
2. Klicken Sie auf die Registerkarte *Authentifizierung* und wählen Sie das Kontrollkästchen *IEEE 802.1X-Authentifizierung aktivieren*. PEAP-MS-CHAP v2 ist die Standardauthentifizierungsmethode. Klicken Sie auf *OK*.

Um manuell eine PEAP-MS-CHAP v2-Authentifizierung auf einem verkabelten Client zu konfigurieren, auf dem Windows XP mit SP2, Windows XP mit SP1 oder Windows Server 2003 ausgeführt wird, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der LAN-Verbindung.
2. Klicken Sie auf die Registerkarte *Authentifizierung*, wählen Sie das Kontrollkästchen *IEEE 802.1X-Authentifizierung aktivieren* und wählen Sie dann in der Dropdownliste den EAP-Typ *Geschütztes EAP (PEAP)*.
3. Klicken Sie auf *Eigenschaften*. Wenn Sie das Computerzertifikat des NPS-Servers überprüfen möchten, wählen Sie im Dialogfeld *Eigenschaften für geschütztes EAP* das Kontrollkästchen

Serverzertifikat überprüfen (empfohlen und standardmäßig aktiviert). Falls Sie die Namen der Authentifizierungsserver angeben möchten, die die Authentifizierung durchführen sollen, wählen Sie *Verbindung mit diesen Servern herstellen* und geben dann die Namen ein. Klicken Sie in der Dropdownliste *Authentifizierungsmethode auswählen* auf *Gesichertes Kennwort (EAP-MSCHAP v2)* (standardmäßig vorgewählt). Schließen Sie die beiden geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Wartung

Für verkabelte Netzwerke mit 802.1X-Authentifizierung fallen in drei Bereichen Wartungsarbeiten an:

- Verwalten von Benutzer- und Computerkonten
- Verwalten 802.1X-fähiger Switches
- Aktualisieren von XML-Kabelprofilen

Verwalten von Benutzer- und Computerkonten

Wenn in Active Directory ein neues Benutzer- oder Computerkonto eingerichtet wird und diesem Benutzer- oder Computerkonto der Zugang zum Kabelnetzwerk erlaubt werden soll, fügen Sie das neue Konto zur entsprechenden, für Kabelverbindungen vorgesehenen Gruppe hinzu. Fügen Sie das neue Konto zum Beispiel zur Sicherheitsgruppe *KabelKonten* hinzu, die Sie zu diesem Zweck definiert und in den Netzwerkrichtlinien für Kabelverbindungen angegeben haben.

Wenn Benutzer- oder Computerkonten in Active Directory gelöscht werden, sind keine weiteren Maßnahmen mehr erforderlich, um zu verhindern, dass mit diesen Konten Kabelverbindungen hergestellt werden können.

Bei Bedarf können Sie zusätzliche universelle Sicherheitsgruppen und Netzwerkrichtlinien erstellen, um Kabelverbindungen für unterschiedliche Benutzergruppen zu ermöglichen. Sie können zum Beispiel eine globale Gruppe *AuftragnehmerMitKabelnetzzugriff* einrichten, die den Mitgliedern der Gruppe *AuftragnehmerMitKabelnetzzugriff* nur während der üblichen Bürozeiten oder für spezielle Intranetressourcen einen Zugriff über das Kabelnetzwerk ermöglicht.

Verwalten 802.1X-fähiger Switches

Nach ihrer Bereitstellung erfordern 802.1X-fähige Switches kaum Wartungsarbeiten. Der größte Teil der Änderungen an der Konfiguration von 802.1X-fähigen Switches ist eine Folge von Kapazitätsanpassungen oder Änderungen in der Infrastruktur des Netzwerks.

Hinzufügen eines 802.1X-fähigen Switches

So fügen Sie einen 802.1X-fähigen Switch hinzu:

1. Folgen Sie den Bereitstellungsschritten, die im Abschnitt »Konfigurieren von 802.1X-fähigen Switches« beschrieben wurden, um einen neuen 802.1X-fähigen Switch zu Ihrem Kabelnetzwerk hinzuzufügen.
2. Fügen Sie den 802.1X-fähigen Switch als RADIUS-Client zu Ihren NPS-Servern hinzu.

Entfernen eines 802.1X-fähigen Switches

Aktualisieren Sie bei der Entfernung eines 802.1X-fähigen Switches auch die Konfiguration Ihrer NPS-Server, indem Sie den 802.1X-fähigen Switch als RADIUS-Client aus der Konfiguration entfernen.

Konfiguration von Änderungen in NPS-Servern

Wenn sich bei den NPS-Servern Änderungen ergeben, weil zum Beispiel ein NPS-Server aus dem Intranet entfernt oder zum Intranet hinzugefügt wird, tun Sie Folgendes:

1. Sorgen Sie dafür, dass die 802.1X-fähigen Switches auf neuen NPS-Servern als RADIUS-Clients eingetragen sind und dass die entsprechenden Netzwerkrichtlinien für den Zugriff im verkabelten Netzwerk konfiguriert sind.
2. Aktualisieren Sie bei Bedarf die Konfiguration der 802.1X-fähigen Switches, damit die neue Serverkonfiguration entsprechend berücksichtigt wird.

Aktualisieren von XML-Kabelprofilen

Zur Aktualisierung von XML-Kabelprofilen und zum Import der aktualisierten Profile auf Ihren Windows Vista- oder Windows Server 2008-Kabelclients gehen Sie folgendermaßen vor:

1. Wenn Sie einen Windows Vista- oder Windows Server 2008-Kabelclient verwenden, erstellen Sie mit dem Befehl `netsh lan export profile` das aktualisierte XML-Kabelprofil.
2. Führen Sie auf Ihren Kabelclients in einem Skript den Befehl `netsh lan add profile` aus, um das XML-Kabelprofil auf Ihren Kabelclients zu importieren, oder importieren Sie es mit einer anderen Methode.

Problembehandlung

Dieser Abschnitt beschreibt Folgendes:

- Die Tools, die Windows Server 2008 und Windows Vista zur Behebung von Problemen mit verkabelten Verbindungen bereitstellen
- Die Behebung von Verbindungsproblemen auf Kabelclients
- Die Behebung von Verbindungsproblemen auf 802.1X-fähigen Switches
- Die Behebung von Problemen mit Kabelverbindungen auf NPS-Servern

Problembehandlungstools von Windows für Kabelnetzwerke

Microsoft bietet folgende Programme zur Unterstützung der Problembehandlung bei verkabelten Netzwerken an:

- TCP/IP-Problembehandlungstools
- Der Ordner *Netzwerkverbindungen*
- Netsh lan-Befehle
- Netzwerkdiagnoseframework-Unterstützung für Kabelverbindungen
- LAN-Diagnose und -Ablaufverfolgung
- NPS-Authentifizierungs- und -Kontoführungsprotokolle
- NPS-Ereignisprotokollierung

- SChannel-Protokollierung
- SNMP-Agent
- Zuverlässigkeits- und Leistungsüberwachungs-Snap-In
- Network Monitor 3.1

TCP/IP-Problembehandlungstools

Die Programme Ping, Tracert und Pathping verwenden die ICMP-Nachrichten Echo und Echo Reply sowie die ICMPv6-Nachrichten Echo Request und Echo Reply, um Verbindungen zu überprüfen, den Pfad zu einem Ziel anzuzeigen und die Pfadintegrität zu überprüfen (ICMP bedeutet Internet Control Message Protocol). Mit dem Programm Route lassen sich die IPv4- und IPv6-Routingtabellen anzeigen. Das Programm Nslookup kann bei der Behebung von Problemen mit der DNS-Namensauflösung (Domain Name System) verwendet werden.

Der Ordner Netzwerkverbindungen

Im Ordner *Netzwerkverbindungen* können Sie das Eigenschaftendialogfeld einer verkabelten Verbindung öffnen und ihren Status überprüfen, beispielsweise ihre TCP/IP-Konfiguration.

Wurde dem Kabelnetzwerkadapter eine APIPA-Adresse (Automatic Private IP Addressing) im Bereich 169.254.0.0/16 oder die konfigurierte alternative Konfiguration zugewiesen, ist der Kabelclient zwar mit dem 802.1X-fähigen Switch verbunden, aber entweder ist die Authentifizierung fehlgeschlagen oder der DHCP-Server ist nicht verfügbar. Schlägt die Authentifizierung fehl, führt TCP/IP die normale Konfiguration durch. Ist kein DHCP-Server verfügbar (authentifiziert oder nicht), weist Windows Vista automatisch eine APIPA-Adresse zu, sofern keine alternative Adresse eingestellt wurde.

Netsh Lan-Befehle

Um Informationen zur Behebung von Problemen mit Kabelverbindungen zu sammeln, können Sie folgende netsh lan-Befehle eingeben:

- **netsh lan show interfaces** Zeigt Informationen über die installierten LAN-Adapter an, und ob die Geräte, mit denen sie verbunden sind, eine 802.1X-Authentifizierung unterstützen
- **netsh lan show profiles** Zeigt eine Liste der Gruppenrichtlinien und lokalen Kabelnetzwerkprofilen an
- **netsh lan show settings** Zeigt den Status des Dienstes für die automatische Konfiguration verkabelter LAN-Verbindungen an
- **netsh lan show tracing** Zeigt den Status der Ablaufverfolgung im Kabelnetzwerk an

Um weitere Informationen über den Diagnoseprozess liefern zu können, erstellt Windows ein ausführliches, vom Systemereignisprotokoll getrenntes Diagnoseprotokoll.

So greifen Sie auf das Protokoll der LAN-Diagnose (verkabelt) zu

1. Erweitern Sie in der Strukturansicht des Ereignisanzeige-Snap-Ins den Knoten *Anwendungs- und Dienstprotokolle\Microsoft\Windows\Wired-AutoConfig*.
2. Klicken Sie auf *Operational*.
3. Im Detailbereich können Sie sich die Ereignisseinträge für die Diagnosesitzung im verkabelten Netzwerk ansehen.

LAN-Diagnose-Ablaufverfolgung

Die Erstellung eines Diagnoseberichts für verkabelte Netzwerke erfolgt in drei Schritten. Zuerst aktivieren Sie die Ablaufverfolgung, dann reproduzieren Sie den Verbindungsfehler und schließlich beenden Sie die Ablaufverfolgung.

Ist die Ablaufverfolgung aktiviert, wird sie im Hintergrund ausgeführt, während Sie versuchen, das Problem zu reproduzieren. Wird die Ablaufverfolgung abgeschaltet, so wird ein Prozess ausgeführt, der automatisch den Microsoft-Diagnosebericht für verkabelte Netzwerke zusammenstellt.

So erstellen Sie einen Microsoft-Diagnosebericht für verkabelte Netzwerke

1. Klicken Sie im Ordner *Verwaltung* auf *Computerverwaltung*.
2. Erweitern Sie in der Konsole Computerverwaltung den Knoten *Zuverlässigkeit und Leistung\Sammlungssätze\System\LAN Diagnostics (LAN-Diagnose)*.
3. Klicken Sie *LAN Diagnostics (LAN-Diagnose)* mit der rechten Maustaste an und klicken Sie dann auf *Starten*.
4. Melden Sie sich vom Netzwerk ab und wieder an oder reproduzieren Sie auf andere Weise die fragliche Fehlerbedingung.
5. Kehren Sie in die Konsole Computerverwaltung zurück, erweitern Sie den Knoten *Zuverlässigkeit und Leistung\Sammlungssätze\System\LAN Diagnostics (LAN-Diagnose)*, klicken Sie *LAN Diagnostics (LAN-Diagnose)* mit der rechten Maustaste an und klicken Sie dann auf *Anhalten*, um die Ablaufverfolgung für das LAN zu beenden.
6. Erweitern Sie in der Zuverlässigkeits- und Leistungsüberwachung den Knoten *Berichte\System\LAN Diagnostics (LAN-Diagnose)* und klicken Sie dann auf *wired*, um die oberste Ebene des *Microsoft-Diagnoseberichts für verkabelte Netzwerke* zu öffnen.

Von Zeit zu Zeit müssen Sie sich mit einem Kabelnetzwerkproblem vielleicht an Microsoft oder an andere Supportspezialisten aus Ihrem Haus wenden. Für eine genaue Analyse brauchen Microsoft oder Ihre Supportspezialisten ausführliche Informationen über den Zustand des Computers und der Kabelnetzwerkkomponenten von Windows sowie über ihre Interaktionen beim Auftreten des Problems. Diese Informationen erhalten Sie unter Windows Vista von der LAN-Diagnose-Ablaufverfolgung in Windows Vista, die den Microsoft-Diagnosebericht für verkabelte Netzwerke generiert. Zu diesem Zweck werden Protokolldateien erstellt und verwendet, die umfangreiche Informationen über bestimmte Aspekte der Kabelnetzwerkkomponenten enthalten.

So öffnen Sie die LAN-Ablaufprotokolle

1. Erweitern Sie im Microsoft-Diagnosebericht für verkabelte Netzwerke den Abschnitt *Problembehandlungsinformationen für verkabelte Netzwerke*.
2. Öffnen Sie *Ablaufverfolgung für verkabeltes Netzwerk*.

Die nützlichsten Protokolle sind:

- *OneX-Ablaufverfolgung*
- *MSMSEC-Ablaufverfolgung*
- *Dienstablauferfolgung der automatischen Konfiguration für verkabelte Netzwerke*

Zusätzlich zur Ablaufverfolgung in verkabelten Netzwerken unterstützen Windows Server 2008 und Windows Vista eine Ablaufverfolgung für Komponenten der RAS-Verbindungsverwaltung und der Routing- und RAS-Dienste, die auch für Kabelverbindungen mit 802.1X-Authentifizierung verwendet werden. Wie bei Kabelnetzwerken liefert eine Ablaufverfolgung für diese Komponenten Informatio-

nen, mit denen Sie komplexe Probleme mit bestimmten Komponenten beheben können. Die Informationen aus diesen zusätzlichen Ablaufverfolgungsdateien sind gewöhnlich nur für Microsoft-Supportmitarbeiter von Nutzen, von denen Sie bei Bearbeitung eines Supportproblems vielleicht darum gebeten werden, Ablaufprotokolldateien für einen Verbindungsversuch zu erstellen. Diese zusätzliche Ablaufverfolgung können Sie mit dem Programm Netsh aktivieren.

Der Befehl zur Aktivierung oder Deaktivierung der Ablaufverfolgung für eine bestimmte Komponente der RAS-Verbindungsverwaltung und der Routing- und RAS-Dienste lautet:

```
netsh ras diagnostics set rastracing Komponente enabled|disabled
```

Darin ist *Komponente* eine Komponente aus der Liste, die in der Registrierung unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing* zu finden ist.

Der Befehl für die Aktivierung der Ablaufverfolgung für alle Komponenten lautet:

```
netsh ras diagnostics set rastracing * enabled
```

Mit folgendem Befehl lässt sich die Ablaufverfolgung für alle Komponenten deaktivieren:

```
netsh ras diagnostics set rastracing * disabled
```

Die Ablaufprotokolldateien werden im Ordner *%SystemRoot%\Tracing* gespeichert. Für die Authentifizierung von Kabelverbindungen sind folgende Protokolldateien am interessantesten:

- **Svchost_rastls.log** TLS-Authentifizierungsaktivitäten
- **Svchost_raschap.log** MS-CHAP v2-Authentifizierungsaktivitäten

NPS-Authentifizierungs- und -Kontoführungsprotokolle

Standardmäßig unterstützt NPS die Protokollierung von Authentifizierungs- und Kontoführungsdaten für Kabelverbindungen in lokalen Protokolldateien. Diese Protokollierung erfolgt getrennt von den Ereignissen, die unter *Windows-Protokolle/Sicherheit* aufgezeichnet werden. Sie können die Informationen aus den Protokollen verwenden, um die Verwendung des Kabelnetzwerks und die Authentifizierungsversuche zu überwachen. Eine Authentifizierungs- und Kontoführungsprotokollierung ist besonders zur Behebung von Problemen nützlich, die sich durch Netzwerkrichtlinien ergeben können. Für jeden Authentifizierungsversuch wird der Name der Netzwerkrichtlinie aufgezeichnet, die den Verbindungsversuch zugelassen oder abgelehnt hat. Die Einstellungen für die Authentifizierungs- und Kontoführungsprotokollierung können Sie im Knoten *Kontoführung* des Snap-Ins Netzwerkrichtlinienserver vornehmen.

Die Authentifizierungs- und Kontoführungsdaten werden in einer oder mehreren konfigurierbaren Protokolldateien im Ordner *%SystemRoot%\System32\LogFiles* gespeichert. Die Protokolldateien werden im IAS-Format (Internet Authentication Service) oder in einem datenbankkompatiblen Format gespeichert. Das bedeutet, dass ein Datenbankprogramm die Protokolldateien direkt zur Analyse einlesen kann. NPS kann die Authentifizierungs- und Kontoführungsinformationen auch an eine SQL Server-Datenbank senden.

NPS-Ereignisprotokollierung

Überprüfen Sie auf dem NPS-Server das Protokoll *Windows-Protokolle\Sicherheit* auf abgewiesene (Ereignis-ID 6273) oder zugelassene (Ereignis-ID 6272) Verbindungsversuche. NPS-Ereignisprotokolleinträge enthalten viele Informationen über den Verbindungsversuch. Darunter sind auch der Name der Verbindungsanforderungsrichtlinie, die für den Verbindungsversuch verwendet wurde (der *Proxyrichtliniennamen* in der Beschreibung des Ereignisses), und die Netzwerkrichtlinie, die den Verbindungsversuch zugelassen oder abgelehnt hat (das Feld *Netzwerkrichtliniennamen* in der Beschreibung des Ereignisses). Die NPS-Ereignisprotokollierung für zugelassene oder abgelehnte Verbin-

dungsversuche ist standardmäßig aktiviert. Sie können sie im Netzwerkrichtlinienserver-Snap-In konfigurieren, und zwar auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds des NPS-Servers. NPS-Ereignisse lassen sich im Ereignisanzeige-Snap-In anzeigen. Die Überprüfung der NPS-Ereigniseinträge im Protokoll *Windows-Protokolle\Sicherheit* ist eine der wichtigsten Methoden, um Informationen über fehlgeschlagene Authentifizierungen zu erhalten.

SChannel-Protokollierung

Eine SChannel-Protokollierung (Secure Channel) bedeutet die Aufzeichnung von Informationen über SChannel-Ereignisse im Systemereignisprotokoll. Standardmäßig werden nur SChannel-Fehlermeldungen aufgezeichnet. Um Informationen über Fehler, Warnungen, Informationen und Erfolgsmeldungen zu erhalten, stellen Sie den Registrierungswert *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging* auf **4** (es ist ein DWORD-Wert). Wenn die SChannel-Protokollierung alle Ereignisse aufzeichnet, ist es möglich, mehr Informationen über den Zertifikataustausch und den Überprüfungsvorgang auf dem NPS-Server zu erhalten.

SNMP-Agent

Sie können die SNMP-Agentensoftware (Simple Network Management Protocol) von Windows Server 2008 verwenden, um in einer SNMP-Konsole Statusinformationen über Ihre NPS-Server zu erhalten. NPS unterstützt die RADIUS Authentication Server MIB (RFC 2619, MIB bedeutet Management Information Base) und die RADIUS Accounting Server MIB (RFC 2621). Installieren Sie den optionalen SNMP-Dienst als Feature mit dem Server-Manager.

Der SNMP-Agent kann in Zusammenarbeit mit Ihrer vorhandenen Netzwerkverwaltungsinfrastruktur auf SNMP-Basis dazu verwendet werden, NPS-RADIUS-Server oder -Proxys zu überwachen.

Zuverlässigkeits- und Leistungsüberwachungs-Snap-In

Sie können das Zuverlässigkeits- und Leistungsüberwachungs-Snap-In verwenden, um Leistungsindikatoren zu überwachen, Protokolle zu erstellen und für bestimmte NPS-Komponenten und Programmprozesse Schwellenwerte für Warnungen festlegen. Sie können die Diagramme und Berichte auch zur Identifizierung von potenziellen Problemen, zur Behebung von vorhandenen Problemen und zur Effizienzprüfung der NPS-Server verwenden.

Mit dem Zuverlässigkeits- und Leistungsüberwachungs-Snap-In können Sie die Leistungsindikatoren von folgenden NPS-Leistungsobjekten überwachen:

- NPS-Kontoführungsclients
- NPS-Kontoführungsproxy
- NPS-Kontoführungsserver
- NPS-Authentifizierungsclients
- NPS-Authentifizierungsproxy
- NPS-Authentifizierungsserver
- NPS-Richtlinienmodul
- NPS-Remotekontoführungsserver
- NPS-Remoteauthentifizierungsserver



Weitere Informationen Weitere Informationen über die Verwendung des Zuverlässigkeits- und Leistungsüberwachungs-Snap-Ins finden Sie im Hilfe- und Supportcenter von Windows Server 2008.

Network Monitor 3.1

Sie können den Microsoft Network Monitor 3.1 (oder höher) oder einen kommerziellen Paketanalytiker (solche Programme werden auch *Netzwerk-Sniffer* genannt) verwenden, um die Authentifizierungen und Datenübertragungen zu untersuchen, die im Netzwerk erfolgen. Der Network Monitor 3.1 bietet Parser für RADIUS, 802.1X, EAPOL und EAP. Ein *Parser* ist eine Komponente des Network Monitors, die die Felder eines Protokollheaders voneinander trennen sowie den Aufbau des Headers und die Werte der Felder anzeigen kann. Ohne einen geeigneten Parser zeigt der Network Monitor 3.1 die im Header enthaltenen Bytes in Hexadezimalform an. Die Interpretation dieser Bytes bleibt dann Ihnen überlassen.



Auf der CD Sie erreichen die Downloadwebsite für den Network Monitor auch über einen Link, den Sie auf der Begleit-CD dieses Buchs finden.

Bei der Untersuchung der Authentifizierung von Kabelclients können Sie den Network Monitor 3.1 verwenden, um die Datenpakete aufzuzeichnen, die während der Authentifizierung zwischen dem Kabelclient und dem 802.1X-fähigen Switch ausgetauscht werden. Mit dem Network Monitor 3.1 können Sie die einzelnen Datenpakete untersuchen und herauszufinden versuchen, warum die Authentifizierung fehlgeschlagen ist. Der Network Monitor eignet sich auch zur Aufzeichnung der RADIUS-Nachrichten, die zwischen einem 802.1X-fähigen Switch und seinem RADIUS-Server ausgetauscht werden, und zur Überprüfung der RADIUS-Attribute jeder Nachricht.

Die korrekte Interpretation der Datenpakete, die mit dem Network Monitor 3.1 aufgezeichnet werden, setzt eine gründliche Kenntnis von EAPOL, RADIUS und anderen Protokollen voraus. Die mit dem Network Monitor 3.1 aufgezeichneten Datenpakete können Sie bei Bedarf auch in Dateien speichern und zur Analyse an den Microsoft-Support senden.

Beheben von Problemen mit Kabelclients

Bei der Behebung von Problemen mit verkabelten Netzwerkverbindungen sollten Sie zuerst überprüfen, ob sich dieselben Probleme auf mehreren oder allen Ihren Kabelclients zeigen. Haben alle Kabelclients Schwierigkeiten, könnte die Ursache in Ihrer Authentifizierungsinfrastruktur liegen. Haben alle Kabelclients Probleme, die mit einem bestimmten Switch verbunden sind, könnte die Ursache bei dem 802.1X-fähigen Switch oder seinen RADIUS-Servern liegen. Sind nur bestimmte Kabelclients von Problemen betroffen, könnten die Probleme bei diesen Clients liegen.

Die folgenden Beschreibungen sind Beispiele für Probleme, die häufiger auf verkabelten Windows-Clients auftreten:

Fehler bei der Authentifizierung

- Überprüfen Sie, ob das Benutzer- oder Computerkonto für den Kabelclient vorhanden ist, ob es aktiviert ist, ob es vielleicht gesperrt ist (über Konteneigenschaften oder eine RAS-Kontosperre) und ob der Verbindungsversuch zu den zugelassenen Anmeldezeiten erfolgt.
- Überprüfen Sie, ob es für den Verbindungsversuch mit dem verwendeten Computer- oder Benutzerkonto eine passende Netzwerkrichtlinie gibt. Wenn Sie die Konten zum Beispiel auf Gruppenebene mit Netzwerkrichtlinien verwalten, überprüfen Sie, ob das Benutzer- oder Computerkonto Mitglied der Gruppe ist, für die die Netzwerkrichtlinie festgelegt wurde.
- Überprüfen Sie, ob das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstellen der NPS-Serverzertifikate auf den Kabelclientcomputern im lokalen Computerspeicher für vertrauenswürdige Stammzertifizierungsstellen vorhanden ist.

- Überprüfen Sie bei einem Kabelclient mit EAP-TLS-Authentifizierung, ob das Computer- oder Benutzerzertifikat die Bedingungen erfüllt, die im Abschnitt »Überprüfen des Zertifikats des Kabelclients« beschrieben werden.
- Überprüfen Sie bei einem Kabelclient mit PEAP-MS-CHAP v2-Authentifizierung, ob das Kennwort des Kabelclients abgelaufen ist. Sorgen Sie dafür, dass auf den NPS-Servern im Dialogfeld *EAP-MSCHAPv2-Eigenschaften* das Kontrollkästchen *Client kann Kennwort ändern, nachdem es abgelaufen ist* aktiviert ist.

Es ist keine Authentifizierung mit einem Zertifikat möglich

- Die häufigste Ursache für dieses Problem ist, dass noch kein Benutzer- oder Computerzertifikat installiert wurde. Je nach der eingestellten Authentifizierungsmethode müssen alle beide installiert sein. Überprüfen Sie im Zertifikate-Snap-In, ob Sie ein Computerzertifikat, ein Benutzerzertifikat oder beide installiert haben.
- Eine weitere Ursache für diese Meldung kann darin bestehen, dass sich die installierten Zertifikate nicht für die Authentifizierung einer verkabelten Verbindung eignen oder nicht von allen NPS-Servern überprüft werden können. Weitere Informationen finden Sie im Abschnitt »Beheben von Problemen mit der Überprüfung von Zertifikaten« dieses Kapitels.

Beheben von Problemen mit 802.1X-fähigen Switches

Wenn Sie mehrere 802.1X-fähige Switches einsetzen und über einen dieser Switches keine Verbindung herstellen und keine Authentifizierung durchführen können, kann das Problem bei diesem Switch liegen. Dieser Abschnitt beschreibt die gebräuchlichen Hilfsmittel zur Behebung von Problemen mit 802.1X-fähigen Switches und die üblichen Probleme, die bei der Verbindungsherstellung und Authentifizierung bei einem Switch auftreten können.

Hilfsmittel zur Behebung von Problemen mit 802.1X-fähigen Switches

Welche Hilfsmittel Ihnen bei der Behebung von Problemen mit 802.1X-fähigen Switches zur Verfügung stehen, hängt zwar von den Herstellern der Geräte ab, aber die häufiger anzutreffenden Problembehandlungstools sind folgende:

- LEDs
- SNMP-Unterstützung
- Diagnosetools

Diese Hilfsmittel werden in den folgenden Abschnitten genauer beschrieben. Informieren Sie sich in der Dokumentation Ihres 802.1X-fähigen Switchs über die Hilfsmittel, die Ihnen zur Problembehandlung zur Verfügung stehen.

LEDs

Die meisten 802.1X-fähigen Switches verfügen über ein oder mehrere kleine Lämpchen (Leuchtdioden, LEDs), die außen am Gehäuse des Geräts angebracht sind und einen schnellen Überblick über den Betriebszustand des Geräts ermöglichen. Sie könnten zum Beispiel folgende Lämpchen vorfinden:

- Ein Lämpchen zeigt an, ob der 802.1X-fähige Switch mit Strom versorgt wird.
- Ein Lämpchen zeigt den allgemeinen Betriebszustand an. Dieses Lämpchen könnte zum Beispiel anzeigen, ob der 802.1X-fähige Switch über authentifizierte Kabelclients verfügt.

- Ein Lämpchen zeigt die Übertragungsaktivität an. Dieses Lämpchen könnte zum Beispiel bei jedem eingehenden oder ausgehenden Datenpaket blinken.
- Ein Lämpchen weist auf Datenkollisionen hin. Blinkt es sehr häufig, sollten Sie mit den Methoden, die der Hersteller des 802.1X-fähigen Switches vorschlägt, die Leistung des Geräts überprüfen.

Vielleicht verfügt der Switch statt der Lämpchen über ein LCD (Liquid Crystal Display), auf dem verschiedene Symbole den Zustand des Geräts angeben. Informieren Sie sich in der Dokumentation des 802.1X-fähigen Switchs über die Bedeutung der Lämpchen oder der Symbole auf der LCD-Anzeige.

SNMP-Unterstützung

Viele 802.1X-fähige Switches sind mit einem SNMP-Agenten (Simple Network Management Protocol) ausgerüstet, der die folgenden SNMP Management Information Bases (MIBs) unterstützt:

- IEEE 802.1 PAE (Port Access Entity) MIB
- SNMP Management MIB (beschrieben in RFC 1157)
- SNMP MIB II (beschrieben in RFC 1213)
- Bridge MIB (beschrieben in RFC 1286)
- Ethernet Interface MIB (beschrieben in RFC 1398)
- IETF Bridge MIB (beschrieben in RFC 1493)
- Remote Monitoring (RMON) MIB (beschrieben in RFC 1757)
- RADIUS Client Authentication MIB (beschrieben in RFC 2618)

Der SNMP-Agent kann zusammen mit Ihrer vorhandenen SNMP-Netzwerkverwaltungsinfrastruktur zur Konfiguration der 802.1X-fähigen Switches, zur Festlegung von Trapbedingungen und zur Überwachung der Belastung der Switches dienen.

Diagnosetools

Diagnosetools für 802.1X-fähige Switches können folgende Form haben:

- Diagnoseprogramme, die über das Hauptkonfigurationsprogramm eines Switchs gestartet werden, beispielsweise ein Windows-Programm von der Produkt-CD des Herstellers des Switchs oder eine Reihe von Webseiten
- Diagnosetools, die über ein Befehlszeilenprogramm oder auf eine andere Weise zugänglich sind und zum Beispiel einen Terminalzugriff auf den 802.1X-fähigen Switch ermöglichen

Welche Diagnosetools die Hersteller bereitstellen, hängt vom Hersteller und vom Switch ab. Sinn dieser Diagnosetools ist es aber immer, die aktuelle Konfiguration des 802.1X-fähigen Switchs überprüfen und die ordnungsgemäße Funktion der Geräte (auf der Ebene der Hardware) sicherstellen zu können.

Häufiger auftretende Probleme mit 802.1X-fähige Switches

Die folgenden Probleme treten bei 802.1X-fähigen Switches häufiger auf:

- Clients können sich nicht beim Switch authentifizieren.
- Über den Switch hinaus ist keine Kommunikation möglich.

Diese Probleme werden in den folgenden Abschnitten näher besprochen.

Es ist keine Authentifizierung beim 802.1X-fähigen Switch möglich

Falls Sie mehrere 802.1X-fähige Switches verwenden und Ihre Kabelclients mit keinem dieser Geräte eine Verbindung herstellen können, gibt es vielleicht ein Problem in Ihrer Authentifizierungsinfrastruktur. Wie man solche Probleme beheben kann, beschreibt der noch folgende Abschnitt »Beheben von Problemen mit der Authentifizierungsinfrastruktur« dieses Kapitels. Falls Sie mehrere 802.1X-fähige Switches verwenden und die Kabelclients nur mit der Authentifizierung bei einem bestimmten Switch Schwierigkeiten haben, müssen Sie die Authentifizierungseinstellung dieses Switchs überprüfen. Überprüfen Sie folgende Bereiche der Authentifizierungskonfiguration:

- 802.1X-Konfiguration
- RADIUS-Konfiguration

802.1X-Konfiguration

Sorgen Sie dafür, dass die 802.1X-Authentifizierung des Switchs aktiviert ist.

RADIUS-Konfiguration

Die RADIUS-Konfiguration umfasst folgende Elemente:

- **RADIUS-Konfiguration des 802.1X-fähigen Switches** Sorgen Sie dafür, dass der 802.1X-fähige Switch korrekt als ein RADIUS-Client für RADIUS konfiguriert ist. Der Switch sollte folgende Einstellungen aufweisen:
 - Die IPv4- oder IPv6-Adresse eines primären RADIUS-Servers (einer Ihrer NPS-Server)
 - Die UDP-Zielports (UDP bedeutet User Datagram Protocol) für den RADIUS-Datenverkehr, der an den primären RADIUS-Server gesendet wird (UDP-Port 1812 für den RADIUS-Authentifizierungsdatenverkehr und UDP-Port 1813 für den RADIUS-Kontoführungsdatenverkehr)
 - Den gemeinsamen geheimen RADIUS-Schlüssel für den primären RADIUS-Server
 - Die IPv4- oder IPv6-Adresse eines sekundären RADIUS-Servers (ein weiterer Ihrer NPS-Server)
 - Die UDP-Zielports für den RADIUS-Datenverkehr, der an den sekundären RADIUS-Server gesendet wird
 - Den gemeinsamen geheimen RADIUS-Schlüssel für den sekundären RADIUS-Server
- **Erreichbarkeit der NPS-Server** Überprüfen Sie auf folgende Weise, ob der primäre und der sekundäre NPS-Server für den 802.1X-fähigen Switch erreichbar sind:
 - Wenn der Switch über einen »Ping« verfügt – er kann an ein beliebiges Unicast-IPv4-Ziel eine ICMP-Echo-Nachricht (Internet Control Message Protocol) senden oder an ein IPv6-Ziel eine ICMPv6-Nachricht –, versuchen Sie, die IPv4- oder IPv6-Adressen des konfigurierten primären und sekundären NPS-Servers mit dem Ping zu erreichen.
 - Kann der Switch keinen Ping aussenden, versuchen Sie, die IPv4- oder IPv6-Adressen des konfigurierten primären und sekundären NPS-Servers von einem anderen Netzwerkknoten aus mit dem Programm Ping zu erreichen. Dieser Knoten muss sich in dem Subnetz befinden, zu dem auch der Switch gehört.

Ist der IPv4-Ping vom Netzwerkknoten erfolgreich und der Ping vom 802.1X-fähigen Switch nicht, überprüfen Sie die IPv4-Konfiguration des Switchs. Sorgen Sie dafür, dass er mit der korrekten IPv4-Adresse, der richtigen Subnetzmaske und dem richtigen Standardgateway für das dazugehörige Kabelnetzwerk konfiguriert ist. Funktioniert keiner der Pings, beheben Sie die Verbindungsprobleme zwischen dem angeschlossenen Subnetz und den NPS-Servern.



Hinweis Ein negatives Ergebnis beim Ping-Test bedeutet nicht zwangsläufig, dass keine IPv4-Verbindung besteht. Es könnte auf dem Weg zwischen dem Switch und den RADIUS-Servern ein Router vorhanden sein, der ICMP-Nachrichten herausfiltert. Vielleicht wurden auch die NPS-Server mit Paketfiltern ausgestattet, die ICMP-Nachrichten verwerfen.

Um sicherzustellen, dass der RADIUS-Datenverkehr die NPS-Server erreicht, verwenden Sie auf den NPS-Servern einen Netzwerksniffer wie den Network Monitor 3.1. Damit können Sie den RADIUS-Datenverkehr aufzeichnen und untersuchen, der bei einem Authentifizierungsversuch zwischen dem 802.1X-fähigen Switch und den RADIUS-Servern ausgetauscht wird.

- **Konfiguration der NPS-Server** Wenn der RADIUS-Datenverkehr den primären und den sekundären NPS-Server erreicht, überprüfen Sie, ob die NPS-Server, die den konfigurierten primären und sekundären RADIUS-Servern des 802.1X-fähigen Switches entsprechen, mit einem RADIUS-Client konfiguriert sind, der dem Switch entspricht. Dazu gehören folgende Werte:
 - Die IPv4- oder IPv6-Adresse der Kabelnetzwerkschnittstelle des Switchs
 - Die UDP-Zielports für den RADIUS-Datenverkehr, der vom Switch gesendet wird (UDP-Port 1812 für den RADIUS-Authentifizierungsdatenverkehr und UDP-Port 1813 für den RADIUS-Kontoführungsdatenverkehr)
 - Das gemeinsame geheime RADIUS-Kennwort, das auf dem Switch konfiguriert wurde
 Überprüfen Sie das Systemereignisprotokoll auf Authentifizierungsfehlerereignisse, die den Verbindungsversuchen mit dem Switch entsprechen. Um die Ereigniseinträge über fehlerhafte Authentifizierungen durchzusehen, zeigen Sie mit der Ereignisanzeige die Einträge des Systemereignisprotokolls mit der Quelle NPS und der Ereignis-ID 2 an.
- **IPsec für den RADIUS-Datenverkehr** Wenn Sie zur Verschlüsselung des RADIUS-Datenverkehrs zwischen dem 802.1X-fähigen Switch und dem NPS-Server IPsec verwenden, überprüfen Sie die IPsec-Einstellungen auf dem 802.1X-fähigen Switch und auf dem NPS-Server und sorgen Sie dafür, dass beide erfolgreich Sicherheitszuordnungen aushandeln und sich gegenseitig authentifizieren können.



Weitere Informationen Weitere Informationen über die Einstellung der IPsec-Richtlinien unter Windows Server 2008 zum Schutz des RADIUS-Datenverkehrs finden Sie in Kapitel 4, »Windows-Firewall mit erweiterter Sicherheit«. Informationen über die Konfiguration von IPsec für einen 802.1X-fähigen Switch finden Sie in der Produktdokumentation Ihres Switches.

Über den 802.1X-fähigen Switch hinaus ist keine Kommunikation möglich

Der 802.1X-fähige Switch ist eine unsichtbare Bridge und ein Schicht-2-Switch, der Datenpakete zwischen dem Kabelnetzwerk, mit dem er verbunden ist, und den verbundenen Kabelclients weiterleitet. Wenn Kabelclients zwar eine Verbindung herstellen und sich authentifizieren können, aber keine Orte jenseits des Switches erreichen, könnte dies einen oder mehrere der folgenden Gründe haben:

- **Der Switch leitet die Datenpakete nicht als Bridge weiter.** Alle unsichtbaren Bridges unterstützen das Spanning-Tree-Protokoll, das eine Schleifenbildung bei der Überbrückung der Netzwerksegmente verhindern soll. Das Spanning-Tree-Protokoll verwendet eine Reihe von Multicast-Nachrichten, um Informationen über die Brückenkonfiguration zu kommunizieren und die Brückenschnittstellen automatisch so zu konfigurieren, dass Datenpakete weitergeleitet oder die Weiterleitung gesperrt wird, um Schleifen zu verhindern. Während der Spanning-Tree-Algorithmus die Weiterleitung oder Sperrung von Schnittstellen überprüft, leitet die Bridge keine Datenpakete weiter. Überprüfen Sie den Weiterleitungsstatus des Switches und die Bridgekonfiguration.

- **Der 802.1X-fähige Switch wurde nicht mit den korrekten VLAN-IDs konfiguriert.** Viele 802.1X-fähige Switches unterstützen VLANs. Dabei handelt es sich um Switchanschlüsse, die verwaltungsmäßig so zusammengefasst werden, dass sie im selben Subnetz erscheinen. Jede Gruppe erhält eine separate VLAN-ID. Überprüfen Sie, ob die VLAN-IDs für Ihre Kabelclients korrekt konfiguriert sind. Vielleicht verwenden Sie zum Beispiel eine VLAN-ID für authentifizierte Kabelclients (die Verbindung erfolgt mit dem Intranet der Organisation) und eine separate VLAN-ID für Gäste mit verkabelten Computern (die Verbindung erfolgt mit einem anderen Subnetz oder mit dem Internet).

Beheben von Problemen mit der Authentifizierungsinfrastruktur

Wenn Sie mehrere 802.1X-fähige Switches verwenden und mit keinem dieser Switches eine Authentifizierung durchführen können, liegt vielleicht ein Problem mit der Authentifizierungsinfrastruktur vor, die aus Ihren NPS-Servern, der PKI und den Active Directory-Konten besteht. In diesem Abschnitt beschreiben wir häufiger auftretende Probleme mit der NPS-Authentifizierung und Autorisierung, sowie mit der Überprüfung von Authentifizierungen auf Zertifikat- oder Kennwortbasis.

Beheben von Problemen mit der NPS-Authentifizierung und Autorisierung

Zur Behebung der häufiger auftretenden Probleme mit der NPS-Authentifizierung und Autorisierung sorgen Sie für Folgendes:

- **Dass der Switch die NPS-Server erreichen kann** Um dies zu überprüfen, versuchen Sie, von jedem der NPS-Server aus die IP-Adresse des Switchs im Kabelnetzwerk anzupingen. Sorgen Sie außerdem dafür, dass keine IPsec-Richtlinien, IP-Paketfilter oder andere Mechanismen, die den Netzwerkzugriff einschränken können, den Austausch von RADIUS-Nachrichten zwischen dem Switch und seinen konfigurierten NPS-Servern verhindern. Für den RADIUS-Datenverkehr mit den NPS-Servern werden eine IPv4- oder IPv6-Quelladresse des Switchs, eine IPv4- oder IPv6-Zielladresse des NPS-Servers, der UDP-Ziellport 1812 für Authentifizierungsnachrichten und der UDP-Ziellport 1813 für Kontoführungsnachrichten verwendet. Für den RADIUS-Datenverkehr von den NPS-Servern werden eine IPv4- oder IPv6-Quelladresse des NPS-Servers, eine IPv4- oder IPv6-Zielladresse des Switchs, der UDP-Quellport 1812 für Authentifizierungsnachrichten und der UDP-Quellport 1813 für Kontoführungsnachrichten verwendet. Diese Beispiele setzen voraus, dass Sie die RADIUS UDP-Ports verwenden, die in den RFCs 2865 und 2866 für die RADIUS-Authentifizierung und Autorisierung definiert werden.
- **Dass jedes NPS-Server/Switch-Paar mit einem gemeinsamen geheimen RADIUS-Kennwort konfiguriert ist** Es muss zwar nicht jedes NPS-Server/Switch-Paar über ein eigenes gemeinsames geheimes RADIUS-Kennwort verfügen, aber das verwendete Kennwort muss auf beiden Partnern eines Paares dasselbe sein. Wenn Sie zum Beispiel die NPS-Konfiguration von einem NPS-Server auf einen anderen kopieren, muss das NPS-Server/Switch-Paar für den NPS-Server, von dem die Konfiguration kopiert wird, dasselbe gemeinsame geheime Kennwort verwenden wie das NPS-Server/Switch-Paar des NPS-Servers, auf den die Konfiguration kopiert wird.
- **Dass die NPS-Server einen Active Directory-Domänencontroller und einen globalen Katalogserver erreichen können** Der NPS-Server verwendet einen globalen Katalogserver, um die Benutzerprinzipalnamen (User Principal Name, UPN) des Computerzertifikats, des Benutzerzertifikats, der Smartcard oder des MS-CHAP v2-Kontonamens in den definierten Namen des entsprechenden Kontos in Active Directory aufzulösen. Der NPS-Server verwendet einen Active Directory-Domänencontroller, um die Anmeldeinformationen des Computer- und Benutzerkontos zu über-

prüfen und um die Konteneigenschaften abzurufen, die für die Bewertung der Autorisierung erforderlich sind.

- **Dass die Computerkonten der NPS-Server in den entsprechenden Domänen Mitglieder der Sicherheitsgruppe RAS- und IAS-Server sind** Das Hinzufügen der NPS-Servercomputerkonten zur Sicherheitsgruppe *RAS- und IAS-Server* der entsprechenden Domäne geschieht normalerweise bei der Konfiguration der NPS-Server. Um das NPS-Servercomputerkonto zu den entsprechenden Domänen hinzuzufügen, können Sie den Befehl `netsh nps add registeredserver` verwenden. Weitere Informationen finden Sie in Kapitel 9.
- **Dass keine konfigurierten Beschränkungen ungewollt den Zugriff verhindern** Sorgen Sie dafür, dass das Benutzer- oder Computerkonto nicht gesperrt, abgelaufen oder deaktiviert ist und dass die Verbindungsversuche in den vorgesehenen Anmeldezeiten erfolgen.
- **Dass das Benutzerkonto nicht von der RAS-Kontosperrung gesperrt wurde** Die RAS-Kontosperrung zählt Authentifizierungsversuche und sperrt den Zugang nach der vorgesehenen Anzahl von Fehlversuchen, damit das Kennwort des Benutzers nicht so leicht durch Online-Wörterbuchangriffe ermittelt werden kann. Wenn die RAS-Kontosperrung aktiviert ist, können Sie den Sperrungszähler eines Kontos zurücksetzen, indem Sie auf dem NPS-Server den Registrierungswert `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\Account-Lockout\Domänenname:Kontoname` löschen.
- **Dass die Verbindung autorisiert ist** Zur Autorisierung müssen die Parameter des Verbindungsversuchs:
 - Alle Bedingungen von mindestens einer Netzwerkrichtlinie erfüllen. Wenn es keine passende Richtlinie gibt, werden alle Authentifizierungsanforderungen für die Kabelverbindung abgelehnt.
 - Durch das Benutzerkonto eine Netzwerkzugriffsberechtigung erhalten (Einstellung auf *Zugriff gestatten*). Falls für das Benutzerkonto die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* gewählt wurde, muss die Zugriffsberechtigung der ersten passenden Netzwerkrichtlinie auf *Zugriff gewähren* lauten.
 - Mit allen Einstellungen des Profils übereinstimmen. Überprüfen Sie, ob in den Authentifizierungseinstellungen des Profils EAP-TLS oder PEAP-MS-CHAP v2 aktiviert und korrekt eingestellt wurde.
 - Zu den Einstellungen der Einwähleigenschaften des Benutzer- oder Computerkontos passen. Wenn Sie den Namen der Netzwerkrichtlinie ermitteln möchten, die zur Ablehnung des Verbindungsversuchs geführt hat, sorgen Sie dafür, dass die NPS-Ereignisprotokollierung für abgelehnte Authentifizierungsversuche aktiviert ist. Suchen Sie dann in der Ereignisanzeige im Protokoll *Windows-Protokolle\Sicherheit* nach Ereigniseinträgen mit der Ereignis-ID 6273. Im Text des Ereigniseintrags für den Verbindungsversuch finden Sie den Netzwerkrichtlinienamen im Feld *Netzwerkrichtliniename*.
- **Dass Sie den Modus Ihrer Domäne nicht vom gemischten Modus in den einheitlichen Modus geändert haben** Falls Sie Ihre Active Directory-Domäne gerade vom gemischten Modus auf den einheitlichen Modus umgestellt haben, können die NPS-Server nicht länger gültige Verbindungsanforderungen authentifizieren. Sie müssen jeden Domänencontroller der Domäne neu starten, damit die Änderung durch Replikation wirksam wird.

Beheben von Problemen mit der Überprüfung von Zertifikaten

Die Behebung von Problemen, die bei der Überprüfung von Zertifikaten für die EAP-TLS-Authentifizierung auftreten, umfasst die Überprüfung der Computer- und Benutzerzertifikate des Kabelclients und der Computerzertifikate der NPS-Server.

Überprüfen des Zertifikats des Kabelclients

Damit ein NPS-Server das Zertifikat eines verkabelten Clients überprüfen kann, müssen für jedes Zertifikat aus der Zertifikatkette des Zertifikats, das der Kabelclient gesendet hat, folgende Bedingungen erfüllt sein:

- **Das aktuelle Datum liegt im Gültigkeitszeitraum des Zertifikats.** Zertifikate werden mit einem Gültigkeitszeitraum ausgestellt, vor dessen Beginn sie noch nicht verwendet werden können. Nach dem Ablauf des Gültigkeitszeitraums sind auch die Zertifikate abgelaufen und können nicht mehr verwendet werden.
- **Das Zertifikat wurde nicht gesperrt.** Ausgestellte Zertifikate können jederzeit gesperrt werden. Jede ausstellende Zertifizierungsstelle führt eine Liste der Zertifikate, die nicht mehr als gültig akzeptiert werden sollten, und veröffentlicht diese Liste in Form einer Zertifikatsperrliste (Certificate Revocation List, CRL). Der NPS-Server versucht zuerst, das Zertifikat mit dem OSCP-Protokoll zu überprüfen (OSCP bedeutet Online Certificate Status Protocol). Ist die OSCP-Überprüfung erfolgreich, so ist auch die Überprüfung des Zertifikats erfolgreich. Andernfalls versucht er, das Benutzer- oder Computerzertifikat anhand der Zertifikatsperrliste zu überprüfen. Standardmäßig überprüft der NPS-Server alle Zertifikate aus der Zertifikatkette des Kabelclients (die Reihe der Zertifikate vom Zertifikat des Kabelclients bis hinauf zur Stammzertifizierungsstelle) darauf hin, ob eines dieser Zertifikate gesperrt wurde. Wurde eines dieser Zertifikate gesperrt, schlägt die Zertifikatüberprüfung fehl. Dieses Verhalten kann in der Registrierung geändert werden, wie im weiteren Verlauf des Kapitels beschrieben.

Wenn Sie die Zertifikatsperrlisten-Verteilungspunkte für ein Zertifikat anzeigen möchten, klicken Sie das Zertifikat im Detailbereich des Zertifikate-Snap-Ins mit einem Doppelklick an, klicken auf die Registerkarte *Details* und klicken dann auf das Feld *Sperrlisten-Verteilungspunkte*. Zur Überprüfung, ob das Zertifikat gesperrt ist, muss der NPS-Server in der Lage sein, die Zertifikatsperrlisten-Verteilungspunkte zu erreichen.

Die Überprüfung der Zertifikatsperrung funktioniert nur so gut wie das System, das die Zertifikatsperrlisten veröffentlicht und verteilt. Wird die Zertifikatsperrliste nicht häufig genug aktualisiert, kann ein bereits gesperrtes Zertifikat vielleicht noch verwendet und als gültig eingestuft werden, weil die veröffentlichte Zertifikatsperrliste, die der NPS-Server verwendet, veraltet ist. Überprüfen Sie, ob die den NPS-Servern zugänglichen Zertifikatsperrlisten noch gelten oder bereits veraltet sind. Wenn die den NPS-Servern verfügbaren Zertifikatsperrlisten abgelaufen sind, schlagen EAP-TLS-Authentifizierungen fehl.

- **Das Zertifikat verfügt über eine gültige digitale Signatur.** Zertifizierungsstellen signieren die Zertifikate, die sie ausstellen, digital. Der NPS-Server überprüft die digitale Signatur jedes Zertifikats aus der Kette (mit Ausnahme des Stammzertifizierungsstellenzertifikats) mit dem öffentlichen Schlüssel der ausstellenden Zertifizierungsstelle.

Das Zertifikat des Kabelclients muss zudem für den Verwendungszweck *Clientauthentifizierung* vorgesehen sein (der Verwendungszweck wird auch *Erweiterte Schlüsselverwendung*, *Enhanced Key Usage* oder *EKU* genannt) und im Feld *Alternativer Antragstellernamen* entweder den Benutzerprinzipalnamen eines gültigen Benutzerkontos oder den vollständig qualifizierten Domänennamen (FQDN) eines gültigen Computerkontos aufweisen.

Wenn Sie sich im Zertifikate-Snap-In die erweiterte Schlüsselverwendung (EKU) eines Zertifikats ansehen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Erweiterte Schlüsselverwendung*. Zur Überprüfung des Felds *Alternativer Antragstellername* klicken Sie auf das Feld *Alternativer Antragstellername*.

Um der Zertifikatkette vertrauen zu können, die der Kabelclient vorlegt, muss der NPS-Server im Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* des Speichers *Lokaler Computer* über das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Zertifikats des Kabelclients verfügen.



Hinweis Zusätzlich zur normalen Zertifikatüberprüfung überprüft der NPS-Server auch, ob die ursprüngliche EAP-Response/Identity-Nachricht denselben Namen angibt, der im Feld *Alternativer Antragstellername* des übermittelten Zertifikats angegeben wird. Das hindert Angreifer daran, sich als einen anderen Benutzer oder Computer auszugeben als den, der in der EAP-Response/Identity-Nachricht genannt wird.

Welche Voraussetzungen das Zertifikat des Kabelclients außerdem erfüllen muss, wurde bereits im Abschnitt »Anforderungen an eine PKI« dieses Kapitels beschrieben.

Standardmäßig prüft NPS, ob die von den Kabelclients vorgelegten Zertifikate gesperrt sind. Wie der NPS-Server die Prüfung durchführt, können Sie auf dem NPS-Server mit den folgenden Registrierungswerten unter *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13* einstellen:

- **IgnoreNoRevocationCheck** Wird dieser Wert auf 1 gestellt, akzeptiert NPS EAP-TLS-Authentifizierungen, selbst wenn es keine Sperrungsüberprüfung der Zertifikatkette des Clients (ausgenommen des Stammzertifizierungsstellenzertifikats) durchführen oder beenden kann. Gewöhnlich schlagen Zertifikatssperrungsüberprüfungen deswegen fehl, weil das Zertifikat keine Angaben über Sperrlisten enthält.

IgnoreNoRevocationCheck wird standardmäßig auf 0 gestellt (deaktiviert). NPS lehnt eine EAP-TLS-Authentifizierung ab, wenn es die Sperrungsüberprüfung der Zertifikatkette des Clients (einschließlich des Stammzertifizierungsstellenzertifikats) nicht beenden und dabei feststellen kann, dass keines der Zertifikate gesperrt wurde.

Stellen Sie IgnoreNoRevocationCheck auf 1, um EAP-TLS-Authentifizierungen auch dann zu akzeptieren, wenn das Zertifikat keine Angaben über Zertifikatssperrlisten-Verteilungspunkte enthält, wie manche Zertifikate von anderen Zertifizierungsstellen.

- **IgnoreRevocationOffline** Wird dieser Wert auf 1 gestellt, akzeptiert NPS EAP-TLS-Authentifizierungen auch dann, wenn ein Server, auf dem die Zertifikatssperrliste gespeichert ist, nicht im Netzwerk verfügbar ist. IgnoreRevocationOffline wird standardmäßig auf 0 gestellt. NPS lehnt eine EAP-TLS-Authentifizierung ab, wenn es nicht auf die Zertifikatssperrlisten zugreifen und daher die Sperrungsüberprüfung der Zertifikatkette des Clients nicht beenden und dabei feststellen kann, dass keines der Zertifikate gesperrt wurde. Kann es keine Verbindung mit einem der Zertifikatssperrlisten-Verteilungspunkte aufnehmen, wird das Zertifikat bei der EAP-TLS-Authentifizierung als ungültig angesehen.

Stellen Sie IgnoreRevocationOffline auf 1, damit das Zertifikat bei der Sperrungsüberprüfung nicht beispielsweise wegen schlechter Verbindungen, die einen erfolgreichen Abschluss der Sperrungsprüfung verhindern, als ungültig eingestuft wird.

- **NoRevocationCheck** Wird dieser Wert auf 1 gestellt, führt NPS keine Sperrungsprüfung mit dem Zertifikat des Kabelclients durch. Bei der Sperrungsprüfung wird überprüft, ob das Zertifikat des

Kabelclients oder eines der Zertifikate aus dessen Zertifikatkette gesperrt wurde. Standardmäßig wird `NoRevocationCheck` auf 0 gestellt.

- **NoRootRevocationCheck** Wird dieser Wert auf 1 gestellt, führt NPS keine Sperrungsüberprüfung des Stammzertifizierungsstellenzertifikats des Kabelclients durch. Dieser Eintrag deaktiviert nur die Sperrungsprüfung des Stammzertifizierungsstellenzertifikats des Clients. Mit den restlichen Zertifikaten aus der Zertifikatkette des Kabelclients wird weiterhin eine Sperrungsprüfung durchgeführt. Standardmäßig wird `NoRootRevocationCheck` auf 0 gestellt.

Sie können `NoRootRevocationCheck` verwenden, wenn Clients authentifiziert werden sollen, in deren Stammzertifizierungsstellenzertifikate keine Zertifikatssperrlisten-Verteilungspunkte angegeben sind, wie in manchen Zertifikaten von anderen Zertifizierungsstellen. Außerdem kann dieser Wert Verzögerungen verhindern, wie sie zum Beispiel eintreten, wenn die Sperrliste eines Zertifikats nicht zugänglich oder abgelaufen ist.

Diese Registrierungswerte müssen als `DWORD`-Typen hinzugefügt werden (ein Registrierungsdatentyp, dessen Wert in Hexadezimalform mit maximal 4 Bytes angegeben wird) und auf 0 oder 1 gestellt werden. Die verkabelten Windows-Clients verwenden diese Werte nicht.

Überprüfen der Zertifikate der NPS-Server

Damit der verkabelte Client das Zertifikat des NPS-Servers überprüfen kann, müssen alle Zertifikate aus der Zertifikatkette des Zertifikats, das vom NPS-Server übermittelt wird, folgende Bedingungen erfüllen:

- **Das aktuelle Datum liegt im Gültigkeitszeitraum des Zertifikats.** Zertifikate werden mit einem Gültigkeitszeitraum ausgestellt, vor dessen Beginn sie noch nicht verwendet werden können. Nach dem Ablauf des Gültigkeitszeitraums sind auch die Zertifikate abgelaufen und können nicht mehr verwendet werden.
- **Das Zertifikat verfügt über eine gültige digitale Signatur.** Zertifizierungsstellen signieren die Zertifikate, die sie ausstellen, digital. Der Kabelclient überprüft die digitale Signatur jedes Zertifikats aus der Kette, mit Ausnahme des Stammzertifizierungsstellenzertifikats, mit dem öffentlichen Schlüssel der ausstellenden Zertifizierungsstelle.

Außerdem muss das Zertifikat des NPS-Servers für den Verwendungszweck *Serverauthentifizierung* vorgesehen sein. Die Objektkennung (OID) dieses Eintrags in der erweiterten Schlüsselverwendung ist 1.3.6.1.5.5.7.3.1. Wenn Sie die erweiterte Schlüsselverwendung eines Zertifikats im Zertifikate-Snap-In überprüfen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Erweiterte Schlüsselverwendung*.

Schließlich muss noch das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Zertifikats des NPS-Servers auf dem Kabelclient im Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* des Speichers *Lokaler Computer* verfügbar sein, damit der Kabelclient der Zertifikatkette vertrauen kann, die der NPS-Server vorgelegt hat.

Welche Voraussetzungen das Computerzertifikat des NPS-Servers außerdem erfüllen muss, wurde bereits im Abschnitt »Anforderungen an eine PKI« dieses Kapitels beschrieben.

Beachten Sie bitte, dass der Kabelclient keine Sperrungsüberprüfung für die Zertifikate aus der Zertifikatkette des Computerzertifikats des NPS-Servers durchführt. Im Normalfall verfügt der Kabelclient noch nicht über eine Verbindung mit dem Netzwerk und kann daher weder auf eine Webseite noch auf andere Ressourcen zugreifen, die für eine Sperrungsüberprüfung erforderlich wären.

Beheben von Problemen bei der Authentifizierung auf Kennwortbasis

Die Behebung von Problemen bei der PEAP-MS-CHAP v2-Authentifizierung auf Kennwortbasis umfasst die Überprüfung des Namens und des Kennworts des Kabelclientbenutzers und die Überprüfung des Computerzertifikats des NPS-Servers.

Überprüfen der Anmeldeinformationen des Kabelclients

Wenn Sie zur Authentifizierung PEAP-MS-CHAP v2 verwenden, müssen der Name und das Kennwort, das der verkabelte Client übermittelt, mit den Anmeldeinformationen für ein gültiges Konto übereinstimmen. Eine erfolgreiche Überprüfung der MS-CHAP v2-Anmeldeinformationen durch die NPS-Server hängt von Folgendem ab:

- Der Domänenteil des Namens entspricht dem Namen einer Domäne, bei der es sich entweder um die Domäne des NPS-Servers oder um eine Domäne handelt, für die eine bidirektionale Vertrauensstellung mit der Domäne des NPS-Servers besteht.
- Der Kontoteil des Namens entspricht einem gültigen Konto aus der Domäne.
- Das Kennwort ist das richtige Kennwort für das Konto.

Zur Überprüfung der Anmeldeinformationen für das Benutzerkonto veranlassen Sie den Benutzer dazu, sich auf einem Computer, der bereits über eine herkömmliche (Ethernet)-Kabelverbindung mit dem Netzwerk verbunden ist, bei seiner Domäne anzumelden. Dabei wird deutlich, ob das Problem bei den Anmeldeinformationen oder bei der Konfiguration der Authentifizierungsinfrastruktur liegt.

Überprüfen der Zertifikate der NPS-Server

Damit der verkabelte Client das Zertifikat des NPS-Servers bei einer PEAP-MS-CHAP v2-Authentifizierung überprüfen kann, müssen alle Zertifikate aus der Zertifikatkette des Zertifikats, das vom NPS-Server übermittelt wird, folgende Bedingungen erfüllen:

- **Das aktuelle Datum liegt im Gültigkeitszeitraum des Zertifikats.** Zertifikate werden mit einem Gültigkeitszeitraum ausgestellt, vor dessen Beginn sie noch nicht verwendet werden können. Nach dem Ablauf des Gültigkeitszeitraums sind auch die Zertifikate abgelaufen und können nicht mehr verwendet werden.
- **Das Zertifikat verfügt über eine gültige digitale Signatur.** Zertifizierungsstellen signieren die Zertifikate, die sie ausstellen, digital. Der Kabelclient überprüft die digitale Signatur jedes Zertifikats aus der Kette, mit Ausnahme des Stammzertifizierungsstellenzertifikats, mit dem öffentlichen Schlüssel der ausstellenden Zertifizierungsstelle.

Außerdem muss das Zertifikat des NPS-Servers für den Verwendungszweck *Serverauthentifizierung* vorgesehen sein (Objektkennung 1.3.6.1.5.5.7.3.1). Wenn Sie die erweiterte Schlüsselverwendung eines Zertifikats im Zertifikate-Snap-In überprüfen möchten, klicken Sie das Zertifikat im Detailbereich mit einem Doppelklick an, klicken auf die Registerkarte *Details* und dann auf das Feld *Erweiterte Schlüsselverwendung*.

Schließlich muss noch das Stammzertifizierungsstellenzertifikat der ausstellenden Zertifizierungsstelle des Zertifikats des NPS-Servers auf dem Kabelclient im Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* des Speichers *Lokaler Computer* verfügbar sein, damit der Kabelclient der Zertifikatkette vertrauen kann, die der NPS-Server vorgelegt hat.

Zusammenfassung des Kapitels

Der Aufbau eines geschützten Kabelnetzwerks erfordert die Konfiguration der Active Directory-, PKI-, Gruppenrichtlinien- und RADIUS-Elemente einer Authentifizierungsinfrastruktur auf Basis von Windows. Die Wartungsarbeiten nach dem Aufbau des verkabelten Netzwerks umfassen die Verwaltung der 802.1X-fähigen Switches, die Änderung ihrer Konfiguration bei Änderungen in der Infrastruktur sowie die Aktualisierung und Bereitstellung von Kabelnetzwerkprofilen. Bei verkabelten Verbindungen treten häufiger die Probleme auf, dass wegen Fehlern bei der Authentifizierung oder Autorisierung keine Verbindung aufgebaut werden kann oder dass Ressourcen aus dem Intranet für einen Kabelclient nicht zugänglich sind.

Weitere Informationen

Weitere Informationen über die Unterstützung von Kabelnetzwerken unter Windows Server 2008 und Windows Vista finden Sie hier:

- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- »Wired Networking with 802.1X Authentication« (<http://technet.microsoft.com/en-us/network/bb545365.aspx>)

Weitere Informationen über Active Directory finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Server 2008 Active Directory – Die technische Referenz* in der technischen Referenz zu Windows Server 2008 (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008

Weitere Informationen über PKI finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- »Public Key Infrastructure for Windows Server« (<http://www.microsoft.com/pki>)
- *Microsoft Windows Server 2008 – PKI und Zertifikatsicherheit* von Brian Komar (Microsoft Press, 2008)

Weitere Informationen über Gruppenrichtlinien finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista* (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- »Microsoft Windows Server Group Policy« (<http://www.microsoft.com/gp>)

Weitere Informationen über RADIUS und NPS finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>

- Das Hilfe und Support-System von Windows Server 2008
- »Network Policy Server« (<http://www.microsoft.com/nps>)

Weitere Informationen über NAP und die 802.1X-Erzwingung finden Sie hier:

- Kapitel 14, »Grundlagen des Netzwerkzugriffsschutzes«
- Kapitel 15, »Vorbereiten des Netzwerkzugriffsschutzes«
- Kapitel 17, »802.1X-Erzwingung«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Das Hilfe und Support-System von Windows Server 2008
- »Network Access Protection« (<http://www.microsoft.com/nap>)

Remotezugriff-VPN-Verbindungen

In diesem Kapitel:

Konzepte	121
Planungs- und Entwurfsaspekte	125
Zusätzliche Sicherheitsaspekte	150
Bereitstellen von VPN-Remotezugriff	162
Wartung	180
Problembehandlung	183
Zusammenfassung des Kapitels	193
Weitere Informationen	193

Dieses Kapitel beschreibt Entwurf, Bereitstellung, Wartung und Problembehandlung von Remotezugriff-VPN-Verbindungen (Virtual Private Network). Nachdem Sie die Remotezugriff-VPN-Lösung bereitgestellt haben, können Sie ihre Konfiguration für die VPN-Erzwingungsmethode des Netzwerkzugriffsschutzes (Network Access Protection, NAP) anpassen, wie in Kapitel 18, »VPN-Erzwingung«, beschrieben.

Dieses Kapitel setzt voraus, dass Sie die Rollen von Active Directory, die Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure, PKI), Gruppenrichtlinien und RADIUS (Remote Authentication Dial-up User Service) innerhalb einer Windows-Authentifizierungsinfrastruktur für Netzwerkzugriff kennen. Diese Elemente sind in Kapitel 9, »Authentifizierungsinfrastruktur«, genauer beschrieben.



Weitere Informationen Dieses Kapitel beschreibt nicht die Planung und Bereitstellung von DFÜ-RAS. Weitere Informationen zu diesen Themen finden Sie in Windows Server 2008-Hilfe und Support oder in der Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>.

Konzepte

Ein VPN ist die Erweiterung eines nichtöffentlichen Netzwerks, das Verbindungen über gemeinsam genutzte oder öffentliche Netzwerke wie zum Beispiel das Internet umfasst. Mit einem VPN können Sie Daten zwischen zwei Computern über ein gemeinsam genutztes oder öffentliches Netzwerk austauschen, wobei eine vertrauliche Punkt-zu-Punkt-Verbindung entsteht. Dabei können Sie zum Beispiel eine WAN-Verbindung (Wide Area Network) nutzen, die Ihnen Ihr Telefon- oder Internetprovider zur Verfügung stellt.

Um eine Punkt-zu-Punkt-Verbindung zu emulieren, werden die Daten gekapselt und mit einem Header versehen, der Routinginformationen enthält. Diese Routinginformationen ermöglichen es, die Daten über das gemeinsam genutzte oder öffentliche Netzwerk zu leiten, sodass sie ihren Endpunkt erreichen. Um eine vertrauliche Verbindung zu ermöglichen, werden die Daten verschlüsselt. Die Verbindung, bei der die vertraulichen Daten gekapselt und verschlüsselt werden, ist die sogenannte VPN-Verbindung.

Benutzer, die zu Hause arbeiten oder auf Dienstreise sind, können mithilfe von VPN-Verbindungen eine Remotezugriffsverbindung zu einem Server ihrer Organisation aufbauen, indem sie die Infrastruktur nutzen, die von einem öffentlichen Netzwerk wie zum Beispiel dem Internet bereitgestellt wird. Aus Sicht des Benutzers ist die VPN-Verbindung eine Punkt-zu-Punkt-Verbindung zwischen dem Computer (der VPN-Client) und einem Server der Organisation (der VPN-Server). Die Details der Infrastruktur des gemeinsam genutzten oder öffentlichen Netzwerks sind irrelevant, weil es so aussieht, als ob die Daten über eine dedizierte, vertrauliche Verbindung übertragen werden.

Organisationen können mithilfe von VPN-Verbindungen auch routingfähige Verbindungen mit weit auseinander liegenden Büros oder anderen Organisationen über ein öffentliches Netzwerk wie zum Beispiel das Internet herstellen, aber dabei trotzdem eine sichere Kommunikation gewährleisten. Eine routingfähige VPN-Verbindung über das Internet funktioniert wie eine dedizierte WAN-Verbindung. Weitere Informationen über routingfähige VPN-Verbindungen finden Sie in Kapitel 13, »Standort-zu-Standort-VPN-Verbindungen«.

Bei Remotezugriff- und routingfähigen Verbindungen kann eine Organisation DFÜ- oder Mietleitungen durch VPN-Verbindungen ersetzen, um die Verbindung zu einem Internetprovider (Internet Service Provider, ISP) herzustellen.

In den Betriebssystemen Windows Server 2008 und Windows Vista gibt es drei Arten von Remotezugriff-VPN-Technologien:

- **Point-to-Point Tunneling Protocol (PPTP)** PPTP nutzt PPP-Authentifizierungsmethoden (Point-to-Point Protocol) für die Benutzerauthentifizierung und MPPE (Microsoft Point-to-Point Encryption) für die Datenverschlüsselung.
- **Layer Two Tunneling Protocol mit Internet Protocol Security (L2TP/IPsec)** L2TP/IPsec nutzt PPP-Authentifizierungsmethoden für die Benutzerauthentifizierung und IPsec für Peerauthentifizierung auf Computerebene, Datenauthentifizierung, Datenintegrität und Datenverschlüsselung.
- **Secure Socket Tunneling Protocol (SSTP)** SSTP nutzt PPP-Authentifizierungsmethoden für Benutzerauthentifizierung und HTTP-Kapselung (Hypertext Transfer Protocol) über einen SSL-Kanal (Secure Sockets Layer) für Datenauthentifizierung, Datenintegrität und Datenverschlüsselung. Die Kombination von HTTP-Kapselung über den SSL-Kanal wird auch als TLS-Kanal (Transport Layer Security) bezeichnet.

Ein Remotezugriffsclient (ein einzelner Benutzercomputer) baut eine Remotezugriff-VPN-Verbindung zu einem nichtöffentlichen Netzwerk über einen VPN-Server auf. Der VPN-Server kann Zugriff auf das gesamte Netzwerk ermöglichen, an das der VPN-Server angeschlossen ist. Die Pakete, die der Remoteclient über die VPN-Verbindung sendet, stammen vom Remotezugriffsclientcomputer.

Während des Verbindungsaufbaus authentifiziert sich der Remotezugriffsclient (der VPN-Client) beim RAS-Server (dem VPN-Server). Bei Authentifizierungsmethoden, die eine gegenseitige Authentifizierung unterstützen, authentifiziert sich außerdem der Server gegenüber dem Client.



Hinweis Der Einsatz des IPsec-Tunnelmodus als Remotezugriff-VPN-Technologie wird in Windows-VPN-Clients oder -Servern nicht unterstützt, weil es keinen Industriestandard für Benutzerauthentifizierung und IP-Adressenkonfiguration über einen IPsec-Tunnel gibt. Der IPsec-Tunnelmodus wird in den RFCs (Request For Comments) 2401, 2402 und 2406 beschrieben.

Direkt von der Quelle: Verbesserungen an PPTP und L2TP/IPsec

In Windows Server 2008 und Windows Vista wurde die VPN-Sicherheit in folgenden Punkten verbessert:

- **PPTP** MPPE-Verschlüsselung mit 40-Bit- und 56-Bit-Schlüsseln wurde in Windows Server 2008 und Windows Vista standardmäßig deaktiviert. PPTP-Verbindungen unterstützen jetzt in der Standardeinstellung nur noch 128-Bit-MPPE-Schlüssel. Falls ein Windows Vista-VPN-Client eine Verbindung zu einem Windows Server 2003-VPN-Server herstellt oder ein Windows XP-VPN-Client eine Verbindung zu einem Windows Server 2008-VPN-Server, ist dieser Verbindungsaufbau nur erfolgreich, wenn sowohl der VPN-Client als auch der VPN-Server so konfiguriert sind, dass sie 128-Bit-MPPE-Verschlüsselung benutzen.

Sie können Windows Server 2008 und Windows Vista so konfigurieren, dass sie für PPTP-Verbindungen 40-Bit- und 56-Bit-MPPE-Schlüssel benutzen, indem Sie den Registrierungswert `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters\AllowPPTPWeakCrypto` auf 1 setzen und den Computer dann neu starten. Davon wird aber abgeraten.

- **L2TP/IPsec** Bei L2TP-Verbindungen wurde in Windows Server 2008 und Windows Vista die Nutzung von IPsec mit DES (Data Encryption Standard) und dem HMAC (Hashed Message Authentication Code) MD5 (Message Digest 5) standardmäßig deaktiviert. L2TP/IPsec-Verbindungen unterstützen jetzt in der Standardeinstellung nur noch 3DES-Verschlüsselung und den HMAC SHA1 (Secure Hash Algorithm-1). Falls ein Windows Vista-VPN-Client eine Verbindung zu einem Windows Server 2003-VPN-Server aufbaut oder ein Windows XP-VPN-Client eine Verbindung zu einem Windows Server 2008-VPN-Server, ist der Verbindungsaufbau nur erfolgreich, falls sowohl der VPN-Client als auch der VPN-Server so konfiguriert sind, dass sie 3DES-Verschlüsselung und den HMAC SHA1 benutzen. Allerdings wurde Unterstützung für AES (Advanced Encryption Standard) mit 128-Bit- oder 256-Bit-Schlüsseln neu hinzugefügt.

Sie können Windows Server 2008 und Windows Vista so konfigurieren, dass sie für L2TP/IPsec-Verbindungen DES-Verschlüsselung und den HMAC MD5 einsetzen, indem Sie den Registrierungswert `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters\AllowL2TPWeakCrypto` auf 1 setzen und den Computer dann neu starten. Davon wird allerdings abgeraten.

*Samir Jain, Lead Program Manager
India Development Center*

Komponenten von Windows-Remotezugriff-VPNs

Abbildung 12.1 zeigt die Komponenten von Windows-Remotezugriff-VPNs.

Die Komponenten sind:

- **VPN-Clients** VPN-Clients bauen Remotezugriff-VPN-Verbindungen zu VPN-Servern auf und kommunizieren mit Intranetressourcen, sobald die Verbindung hergestellt wurde.
- **VPN-Server** VPN-Server nehmen Remotezugriff-VPN-Verbindungsversuche entgegen, erzwingen Authentifizierungs- und Verbindungsanforderungen und leiten Pakete zwischen VPN-Clients und Intranetressourcen weiter.

- **RADIUS-Server** RADIUS-Server stellen eine zentralisierte Authentifizierungs- und Autorisierungsverarbeitung sowie Kontoführung für Netzwerkzugriffsversuche von mehreren VPN-Servern (und anderen Arten von Zugriffsservern) zur Verfügung.
- **Active Directory-Domänencontroller** Active Directory-Domänencontroller überprüfen im Rahmen der Authentifizierung die Benutzeranmeldeinformationen und stellen Benutzerkontoinformationen zur Verfügung, die zum Auswerten der Autorisierung benötigt werden.
- **Zertifizierungsstellen** Zertifizierungsstellen (Certification Authority, CA) sind Teil der PKI. Sie stellen für die Computer- und Benutzerauthentifizierung von VPN-Verbindungen Computer- oder Benutzerzertifikate für VPN-Clients sowie Computerzertifikate für VPN-Server und RADIUS-Server aus.



Weitere Informationen Computerzertifikate sind Zertifikate, die im lokalen Computerzertifikatspeicher gespeichert werden und alle Eigenschaften haben, um eine Authentifizierung für PPP, SSL oder IPsec durchzuführen. Weitere Informationen über Zertifikatanforderungen für PPP- oder SSL-Authentifizierung finden Sie in »Network Access Authentication and Certificates« unter <http://go.microsoft.com/fwlink/?LinkID=20016>. Weitere Informationen über Zertifikatanforderungen für IPsec-Authentifizierung finden Sie in »How IPsec Works« unter <http://go.microsoft.com/fwlink/?LinkID=67907>.

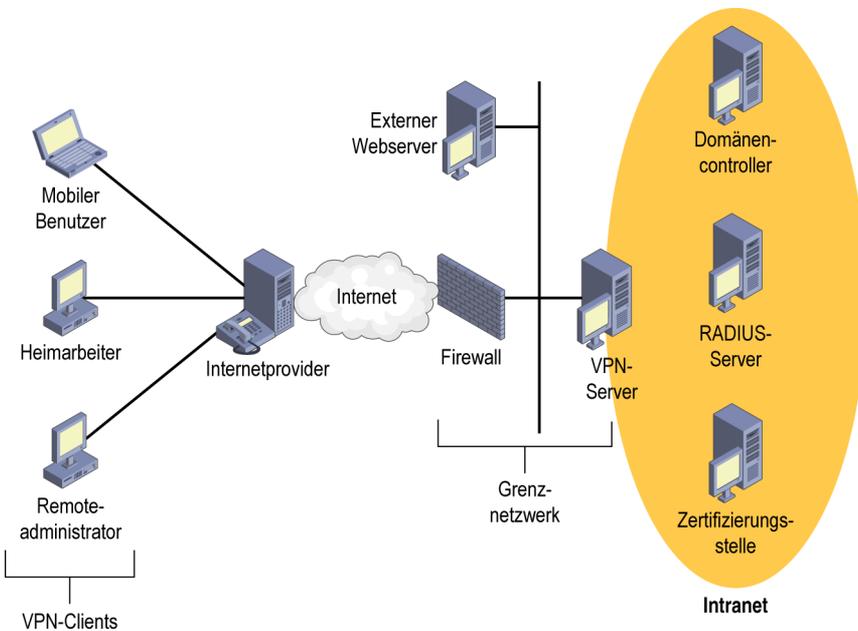


Abbildung 12.1 Komponenten von Windows-Remotezugriff-VPNs

Typische Nutzer von Remotezugriff-VPN-Verbindungen sind:

- Notebookbenutzer, die eine Verbindung ins Intranet herstellen, um E-Mail und andere Ressourcen abzurufen, während sie auf Dienstreise sind
- Heimarbeiter, die von zu Hause aus über das Internet auf Intranetressourcen zugreifen
- Remoteadministratoren, die über das Internet eine Verbindung zu einem nichtöffentlichen Netzwerk herstellen und Netzwerk- oder Anwendungsdienste konfigurieren

Planungs- und Entwurfsaspekte

Beim Bereitstellen einer Remotezugriff-VPN-Lösung müssen Sie folgende Planungs- und Entwurfsfragen beantworten:

- VPN-Protokolle
- Authentifizierungsmethoden
- VPN-Server
- Internetinfrastruktur
- Intranetinfrastruktur
- Gleichzeitiger Intranet- und Internetzugriff für VPN-Clients
- Authentifizierungsinfrastruktur
- VPN-Clients
- PKI
- VPN-Erzwingung mit NAP

VPN-Protokolle

Windows Server 2008 unterstützt folgende Remotezugriff-VPN-Protokolle:

- **PPTP** PPTP benutzt PPP-Benutzerauthentifizierung und MPPE-Verschlüsselung. Wenn MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol) oder PEAP-MS-CHAP v2 (Protected EAP) in Kombination mit starken Kennwörtern eingesetzt wird, ist PPTP eine sichere VPN-Technologie. Für zertifikatbasierte Authentifizierung kann EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) mit Registrierungszertifikaten oder Smartcards kombiniert werden. PPTP wird auf breiter Basis unterstützt, ist einfach bereitzustellen und kann über die meisten NATs (Network Address Translator) geleitet werden. PPTP wird von den Betriebssystemen Windows Server 2008, Windows Vista, Windows Server 2003 und Windows XP unterstützt.
- **L2TP/IPsec** L2TP benutzt PPP-Benutzerauthentifizierung und IPsec-Paketenschutz. L2TP/IPsec verwendet Zertifikate (in der Standardeinstellung) und den IPsec-Computerauthentifizierungsprozess, um die geschützte IPsec-Sitzung auszuhandeln, und dann PPP-Benutzerauthentifizierung, um den Benutzer des VPN-Clientcomputers zu authentifizieren. Wegen der Nutzung von IPsec bietet L2TP/IPsec für jedes Paket Vertraulichkeit der Daten (Verschlüsselung), Datenintegrität (Beweis, dass die Daten nicht während der Übertragung geändert wurden) und Authentifizierung der Datenherkunft (Beweis, dass die Daten vom autorisierten Benutzer stammen). L2TP/IPsec setzt aber eine PKI voraus, um Computerzertifikate für jeden L2TP/IPsec-VPN-Client auszustellen. L2TP/IPsec wird in Windows Server 2008, Windows Vista, Windows Server 2003 und Windows XP unterstützt.
- **SSTP** SSTP benutzt PPP-Benutzerauthentifizierung und einen HTTP-über-SSL-Kanal für Kapselung und Verschlüsselung. Weil SSTP mit SSL-Verkehr arbeitet (über TCP-Port 443), kann SSTP in vielen unterschiedlichen Netzwerkkonfigurationen eingesetzt werden, zum Beispiel wenn VPN-Clients oder -Server hinter NATs (Network Address Translation), Firewalls oder Proxyservern liegen, die PPTP- oder L2TP/IPsec-Verkehr blockieren oder einfach nicht weiterleiten können. SSTP wird nur in Windows Server 2008 und Windows Vista SP1 unterstützt.

Entwurfsmöglichkeiten für VPN-Protokolle

- Wenn PEAP-MS-CHAP v2, EAP-MS-CHAP v2 oder MS-CHAP v2 für die Authentifizierung benutzt wird, benötigt PPTP keine Zertifikatinfrastruktur, um Zertifikate an jeden VPN-Client auszustellen.
- PPTP-VPN-Verbindungen bieten Vertraulichkeit der Daten (Verschlüsselung) für alle Pakete. PPTP-VPN-Verbindungen bieten keine Datenintegrität oder Authentifizierung der Datenherkunft.
- Wegen der Nutzung von IPsec bieten L2TP/IPsec-VPN-Verbindungen Vertraulichkeit der Daten, Datenintegrität und Authentifizierung der Datenherkunft.
- SSTP-VPN-Clients und -Server können hinter NATs, Firewalls oder Webproxies liegen. SSTP unterstützt aber keine VPN-Clients oder -Server, die hinter authentifizierenden Webproxies liegen.
- In der Standardeinstellung unterstützt ein VPN-Server, der unter Windows Server 2008 läuft, alle drei Typen von VPN-Verbindungen gleichzeitig. Sie können für einige Remotezugriff-VPN-Verbindungen (zum Beispiel von VPN-Clients, bei denen kein Computerzertifikat installiert ist) PPTP einsetzen, bei anderen Remotezugriff-VPN-Verbindungen (zum Beispiel von VPN-Clients, die ein Computerzertifikat installiert haben) L2TP/IPsec, und bei VPN-Clients, die unter Windows Vista SP1 laufen, SSTP.
- Falls Sie eine Kombination aus mehreren VPN-Protokollen verwenden, können Sie separate Netzwerkrichtlinien erstellen, die unterschiedliche Verbindungseinstellungen für PPTP-, L2TP/IPsec- oder SSTP-Verbindungen definieren.
- In Windows Server 2008 und Windows Vista kann IPv6-Verkehr als IPv4-getunnelter Verkehr oder nativer IPv6-Verkehr innerhalb des VPN-Tunnels über eine PPTP-VPN-Verbindung gesendet werden. Weitere Informationen finden Sie im Abschnitt »So funktioniert's: IPv6 und VPN-Verbindungen« weiter unten in diesem Kapitel.
- In Windows Server 2008 und Windows Vista unterstützen L2TP/IPsec- und SSTP-VPN-Verbindungen IPv6-Verkehr als IPv4-getunnelten Verkehr, als nativen IPv6-Verkehr innerhalb des VPN-Tunnels und für VPN-Verbindungen über IPv6. Weitere Informationen finden Sie im Abschnitt »So funktioniert's: IPv6 und VPN-Verbindungen« weiter unten in diesem Kapitel.

Anforderungen an VPN-Protokolle

- PPTP-VPN-Clients können hinter einem NAT liegen, falls das NAT einen NAT-Editor enthält, der weiß, wie PPTP-getunnelte Daten richtig umgesetzt werden müssen. Zum Beispiel enthalten die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing, ICS) des Ordners *Netzwerkverbindungen* und die NAT-Routingprotokollkomponente von Routing und RAS einen NAT-Editor, der PPTP-Verkehr zu und von PPTP-Clients, die hinter dem NAT liegen, richtig umsetzen kann. VPN-Server dürfen nicht hinter einem NAT liegen, sofern es nicht mehrere öffentliche IP-Adressen gibt und eine öffentliche IP-Adresse 1:1 der nichtöffentlichen IP-Adresse des VPN-Servers zugeordnet ist. Falls es nur eine einzige öffentliche Adresse gibt, muss das NAT so konfiguriert sein, dass es die PPTP-getunnelten Daten zum VPN-Server umsetzt und weiterleitet. Die meisten NATs, die eine einzige öffentliche IPv4-Adresse nutzen (zum Beispiel ICS und die NAT-Routingprotokollkomponente), können so konfiguriert werden, dass sie eingehenden Verkehr anhand der IPv4-Adresse sowie der TCP- und UDP-Ports erlauben. PPTP-getunnelte Daten verwenden aber keine TCP- oder UDP-Header. Daher darf ein VPN-Server nicht hinter einem Computer liegen, auf dem ICS oder die NAT-Routingprotokollkomponente laufen, wenn lediglich eine einzige öffentliche IPv4-Adresse benutzt wird.

- L2TP/IPsec-VPN-Clients oder -Server dürfen nur dann hinter einem NAT liegen, wenn sowohl der Client als auch der Server IPsec NAT-T (NAT-Traversal) unterstützen. IPsec NAT-T wird in Windows Server 2008, Windows Vista, Windows Server 2003 und Windows XP SP2 unterstützt.
- L2TP/IPsec unterstützt standardmäßig Computerzertifikate, dies ist die empfohlene Authentifizierungsmethode für IPsec. Sie können aber auch einen vorinstallierten Schlüssel konfigurieren, um L2TP/IPsec-Verbindungen zu authentifizieren. Das wird nicht empfohlen, sofern es nicht als Übergangslösung für die Authentifizierungsmethode beim Bereitstellen einer PKI implementiert wird. Eine Computerzertifikatsauthentifizierung setzt eine PKI voraus, damit Computerzertifikate für den VPN-Servercomputer und alle VPN-Clientcomputer ausgestellt werden können.
- SSTP wird nur in Windows Server 2008 (als VPN-Server oder -Client) und Windows Vista SP1 (als VPN-Client) unterstützt.
- SSTP benutzt einen verschlüsselten SSL-Kanal, um alle Daten zu schützen, die über die VPN-Verbindung gesendet werden. Damit dieser verschlüsselte Kanal aufgebaut werden kann, braucht der VPN-Server ein Computerzertifikat und der VPN-Clientcomputer muss in der Lage sein, das Computerzertifikat des VPN-Servers zu überprüfen. Das bedeutet, dass auf den VPN-Clients das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert sein muss, die das Computerzertifikat des VPN-Servers ausgestellt hat.
- Falls Sie nativen IPv6-Verkehr innerhalb des VPN-Tunnels über eine VPN-Wählverbindung senden wollen, müssen Sie L2TP/IPsec benutzen. Weitere Informationen finden Sie im Abschnitt »So funktioniert's: IPv6 und VPN-Verbindungen«.
- Falls Sie VPN-Wählverbindungen über das IPv6-Internet einsetzen wollen, müssen Sie L2TP/IPsec benutzen.

Empfohlene Vorgehensweise für VPN-Protokolle

- Falls Sie bereits eine PKI haben, sollten Sie L2TP/IPsec verwenden, nicht PPTP.
- Falls Sie nicht alle VPN-Protokolle einsetzen, sollten Sie im Snap-In *Routing und RAS* im Knoten *Ports* die Zahl der Ports für unbenutzte VPN-Protokolle auf den Wert 0 setzen.

So funktioniert's: IPv6 und VPN-Verbindungen

Für VPN-Verbindungen bieten Windows Server 2008 und Windows Vista folgende Unterstützung für IPv6:

- IPv4-getunnelter IPv6-Verkehr
- Nativer IPv6-Verkehr innerhalb des VPN-Tunnels
- VPN-Verbindungen über IPv6

IPv4-getunnelter IPv6-Verkehr

In Windows XP und Windows Server 2003 konnten Sie IPv6-Verkehr über eine VPN-Verbindung senden, aber nur, wenn er bereits mit einem IPv4-Header gekapselt war (IPv4-Tunnel). Bei der Unterstützung von IPv4-getunneltem IPv6-Verkehr kann ein Remotezugriffsklient eine VPN-Verbindung über das IPv4-Internet aufbauen und dann IPv4-getunnelten IPv6-Verkehr nutzen, um mit IPv6/IPv4-Knoten oder IPv6-Knoten im Intranet zu kommunizieren.

IPv4-getunnelter IPv6-Verkehr, der über eine VPN-Verbindung gesendet wird, besteht aus IPv6-Paketen, die in einem IPv4-Header gekapselt sind (das ist der IPv4-Tunnel). Diese Pakete sind wiederum in einem PPP-Header und einem VPN-Protokollheader (zum Beispiel PPTP oder L2TP/IPsec) gekapselt, und diese wiederum in einem letzten IPv4-Header. So ist es möglich, die Pakete durch das IPv4-Internet zu befördern.

PPTP, L2TP/IPsec und SSTP in Windows Server 2008 und Windows Vista unterstützen IPv4-getunnelten IPv6-Verkehr. IPv4-getunnelter IPv6-Verkehr, der über eine VPN-Verbindung gesendet wird, setzt IPCP-Unterstützung (Internet Protocol Control Protocol) auf dem VPN-Client und dem VPN-Server, Unterstützung für IPv6-Übergangstechnologie auf dem VPN-Client und eine IPv6-Übergangstechnologieinfrastruktur (zum Beispiel ISATAP) im Intranet voraus. IPCP ist ein PPP-Netzwerksteuerungsprotokoll, das es PPP-Hosts erlaubt, Einstellungen für die Nutzung von IPv4 über eine PPP-Verbindung zu konfigurieren.

Nativer IPv6-Verkehr innerhalb des VPN-Tunnels

Windows Server 2008 und Windows Vista unterstützen VPN-Verbindungen mit nativem IPv6-Verkehr innerhalb des VPN-Tunnels. Der VPN-Client baut eine VPN-Verbindung mit einem VPN-Server über das IPv4-Internet auf und handelt dann die Verwendung von IPv6 über die PPP-Verbindung aus. IPv6-Pakete werden vom VPN-Protokoll innerhalb des VPN-Tunnels gekapselt. Bei nativer Unterstützung für IPv6-Verkehr innerhalb des VPN-Tunnels kann ein Remotezugriffsklient eine VPN-Verbindung über das IPv4-Internet aufbauen und dann über nativen IPv6-Verkehr mit IPv6-Knoten im Intranet kommunizieren.

Nativer IPv6-Verkehr innerhalb des VPN-Tunnels besteht aus IPv6-Paketen, die mit einem PPP-Header und einem VPN-Protokollheader gekapselt werden. Diese Pakete werden wiederum mit einem letzten IPv4-Header gekapselt. So ist es möglich, die Pakete durch das IPv4-Internet zu befördern.

Nativer IPv6-Verkehr innerhalb des VPN-Tunnels setzt IPV6CP-Unterstützung (IPv6 Control Protocol) auf dem VPN-Client und dem VPN-Server, IPv6-Routing-Unterstützung auf dem VPN-Server und eine native IPv6-Routinginfrastruktur im Intranet voraus. PPTP, L2TP/IPsec und SSTP in Windows Server 2008 und Windows Vista unterstützen nativen IPv6-Verkehr innerhalb des VPN-Tunnels. IPV6CP ist ein PPP-Netzwerksteuerungsprotokoll, das es PPP-Hosts erlaubt, Einstellungen für die Nutzung von IPv6 über eine PPP-Verbindung zu konfigurieren.



Hinweis Windows XP und Windows Server 2003 unterstützen keinen nativen IPv6-Verkehr innerhalb des VPN-Tunnels.

VPN-Verbindungen über IPv6

Windows Server 2008 und Windows Vista unterstützen auch VPN-Verbindungen über IPv6. Der VPN-Client baut über das IPv6-Internet eine VPN-Verbindung mit einem VPN-Server auf und handelt dann die Nutzung von IPv6 oder IPv4 über die PPP-Verbindung aus. Wenn VPN-Verbindungen über IPv6 unterstützt werden, kann der Remotezugriffsklient eine VPN-Verbindung über das IPv6-Internet aufbauen und dann entweder nativen IPv6- oder IPv4-Verkehr einsetzen, um mit Knoten im Intranet zu kommunizieren.

Verkehr für VPN-Verbindungen über IPv6 besteht aus IPv6- oder IPv4-Paketen, die mit einem PPP-Header und einem VPN-Protokollheader gekapselt werden. Diese Pakete werden wiederum mit einem letzten IPv6-Header gekapselt. So ist es möglich, die Pakete durch das IPv6-Internet zu befördern.

SSTP und L2TP/IPsec in Windows Server 2008 und Windows Vista unterstützen VPN-Verbindungen über IPv6. VPN-Verbindungen über IPv6 setzen native IPv6-Unterstützung für VPN-Protokolle auf dem VPN-Client und dem VPN-Server, IPv6-Routingunterstützung auf dem VPN-Server und Verbindungen zum IPv6-Internet voraus.

Native IPv6-Fähigkeit für VPN-Verbindungen (also die Fähigkeit, native IPv6-Pakete über eine VPN-Verbindung zu senden) ist bei nativem IPv6-Verkehr innerhalb des VPN-Tunnels und VPN-Verbindungen über IPv6 gegeben.



Hinweis Windows XP und Windows Server 2003 bieten keine Unterstützung für VPN-Verbindungen über IPv6 oder native IPv6-Fähigkeiten für VPN-Verbindungen.

Authentifizierungsmethoden

Zum Authentifizieren des Benutzers, der versucht, eine VPN-Verbindung aufzubauen, unterstützt Windows Server 2008 eine Vielzahl von Authentifizierungsprotokollen, darunter folgende:

- MS-CHAP v2
- EAP-MS-CHAP v2
- EAP-TLS
- PEAP-MS-CHAP v2
- PEAP-TLS



Hinweis In Windows Server 2008 und Windows Vista wurde die Unterstützung für MS-CHAP (Microsoft Challenge Handshake Authentication Protocol, auch als MS-CHAP v1 bezeichnet), SPAP (Shiva Password Authentication Protocol) und EAP-MD5 (EAP-Message Digest 5) aus Sicherheitsgründen entfernt.

EAP-TLS und PEAP-TLS werden in Kombination mit einer PKI und Benutzerzertifikaten oder Smartcards eingesetzt. Bei EAP-TLS sendet der VPN-Client sein Benutzerzertifikat für die Authentifizierung, und der Authentifizierungsserver sendet ein Computerzertifikat für die Authentifizierung. In der Standardeinstellung überprüft der VPN-Client das Zertifikat des VPN-Servers. Bei PEAP-TLS bauen der VPN-Client und der Authentifizierungsserver einen verschlüsselten TLS-Kanal auf, und danach tauschen VPN-Client und Authentifizierungsserver ihre Zertifikate aus. Sowohl EAP-TLS als auch PEAP-TLS sind viel sicherer als PEAP-MS-CHAP v2 oder MS-CHAP v2, weil sie nicht mit Kennwörtern arbeiten. PEAP-TLS ist die sicherste Authentifizierungsmethode, weil der Zertifikataustausch zwischen dem VPN-Client und dem Authentifizierungsserver verschlüsselt abläuft.

Sofern keine Benutzerzertifikate oder Smartcards zur Verfügung stehen, sollten Sie PEAP-MS-CHAP v2, EAP-MS-CHAP v2 oder MS-CHAP v2 verwenden. PEAP-MS-CHAP v2 sollten Sie gegenüber MS-CHAP v2 oder EAP-MS-CHAP v2 den Vorzug geben, weil der Nachrichtenaustausch bei MS-CHAP v2 mit einem verschlüsselten TLS-Kanal geschützt ist, sodass es für böswillige Benutzer schwieriger wird, den Nachrichtenaustausch abzuhören und mithilfe eines Offline-Wörterbuchangriffs das Kennwort des Benutzers zu ermitteln.

Entwurfsmöglichkeiten für Authentifizierungsprotokolle

- MS-CHAP v2, EAP-MS-CHAP v2 und PEAP-MS-CHAP v2 sind Authentifizierungsprotokolle, die mit Kennwörtern arbeiten.
- EAP-TLS und PEAP-TLS sind zertifikatbasierte Authentifizierungsprotokolle.

- Bei L2TP/IPsec-Verbindungen kann jedes beliebige Benutzerauthentifizierungsprotokoll verwendet werden, weil die Authentifizierung stattfindet, nachdem der VPN-Client und der VPN-Server einen IPsec-geschützten Kanal eingerichtet haben. Es wird allerdings die Verwendung von PEAP-MS-CHAP v2, MS-CHAP v2, EAP-MS-CHAP v2, EAP-TLS oder PEAP-TLS empfohlen, um sichere Benutzerauthentifizierung und gegenseitige Authentifizierung mit dem Authentifizierungsserver zu bieten.

Anforderungen an Authentifizierungsprotokolle

- Für verschlüsselte PPTP-Verbindungen müssen Sie MS-CHAP v2, EAP-MS-CHAP v2, PEAP-MS-CHAP v2, EAP-TLS oder PEAP-TLS verwenden. Nur diese Authentifizierungsprotokolle bieten einen Mechanismus, um für jede Sitzung einen neuen Verschlüsselungsschlüssel zu generieren, mit dem VPN-Client und VPN-Server die PPTP-Daten verschlüsseln, die über die VPN-Verbindung gesendet werden.
- PEAP-MS-CHAP v2 und EAP-MS-CHAP v2 werden von VPN-Clients unterstützt, die unter Windows Server 2008 und Windows Vista laufen. MS-CHAP v2 wird von VPN-Clients unterstützt, die unter Windows Server 2008, Windows Vista, Windows Server 2003 oder Windows XP laufen.
- PEAP-MS-CHAP v2 erfordert die Installation eines Computerzertifikats auf dem Authentifizierungsserver (manchmal der VPN-Server, meist aber ein RADIUS-Server) und auf jedem VPN-Clientcomputer die Installation des Stammzertifizierungsstellenzertifikats der Zertifizierungsstelle, die das Computerzertifikat ausgestellt hat. PEAP-MS-CHAP v2 wird nur von VPN-Clients unterstützt, die unter Windows Server 2008 oder Windows Vista laufen.
- Für SSTP-Verbindungen müssen Sie MS-CHAP v2, EAP-MS-CHAP v2, PEAP-MS-CHAP v2, EAP-TLS oder PEAP-TLS verwenden. Nur diese Authentifizierungsprotokolle bieten einen Mechanismus, um für jede Sitzung einen neuen Verschlüsselungsschlüssel zu generieren, den VPN-Client und VPN-Server benutzen, um Angriffe auf die SSTP-VPN-Verbindung durch böswillige Benutzer zu verhindern, die zwischen VPN-Client und -Server die Verbindung abhören.
- Wenn Sie die VPN-Erzwingung mit NAP bereitstellen wollen, müssen Sie eine PEAP-Authentifizierungsmethode verwenden.

Empfohlene Vorgehensweise für Authentifizierungsprotokolle

- Verwenden Sie für Ihre Remotezugriff-VPN-Konfiguration die sicherste Authentifizierungsmethode, die zur Verfügung steht. Die sicherste Authentifizierungsmethode ist der Einsatz von PEAP-TLS oder EAP-TLS mit Zertifikaten. Verwenden Sie andernfalls PEAP-MS-CHAP v2, MS-CHAP v2 oder EAP-MS-CHAP v2 für die Authentifizierung.
- Falls Sie Smartcards verwenden oder eine PKI haben, die Benutzerzertifikate ausstellt, sollten Sie PEAP-TLS oder EAP-TLS für Ihre VPN-Verbindungen einsetzen. PEAP-TLS wird von VPN-Clients unterstützt, die unter Windows Server 2008 oder Windows Vista laufen. EAP-TLS wird von VPN-Clients unterstützt, die unter Windows Server 2008, Windows Vista, Windows Server 2003 oder Windows XP laufen.
- Falls Sie ein Authentifizierungsprotokoll verwenden müssen, das mit Kennwörtern arbeitet (zum Beispiel PEAP-MS-CHAP v2, MS-CHAP v2 oder EAP-MS-CHAP v2), sollten Sie in Ihrem Netzwerk die Verwendung sicherer Kennwörter verpflichtend machen. Sichere Kennwörter sind lang (mehr als 8 Zeichen) und enthalten eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Interpunktionszeichen. In einer Active Directory-Domäne können Sie über den Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwort-*

richtlinien in den Gruppenrichtlinieneinstellungen die Verwendung sicherer Benutzerkennwörter vorschreiben.

VPN-Server

Ein VPN-Server ist ein Computer, der unter Windows Server 2008 läuft und auf dem Routing und RAS installiert sind. Er erfüllt folgende Aufgaben:

- Er nimmt PPTP-Verbindungsversuche, IPsec-Aushandlungen für L2TP-Verbindungsversuche und SSL-Aushandlungen für SSTP-Verbindungsversuche entgegen.
- Er fordert eine Authentifizierung und Autorisierung der VPN-Verbindungen, bevor er erlaubt, Intranetdaten zu und von den VPN-Clients zu leiten.
- Er agiert als Router, der Pakete zwischen VPN-Clients und Ressourcen im Intranet weiterleitet.

Auf einem VPN-Server sind normalerweise mindestens zwei Netzwerkkarten installiert: mindestens eine Netzwerkkarte, die mit dem Internet verbunden ist, und mindestens eine Netzwerkkarte, die mit dem Intranet verbunden ist.

Konfigurieren von Routing und RAS

Wenn Sie Routing und RAS konfigurieren und aktivieren, fordert der Setup-Assistent für den Routing- und RAS-Server Sie auf, auszuwählen, welche Rolle der Computer wahrnimmt. Für VPN-Server müssen Sie die Konfigurationsoption *RAS (DFÜ oder VPN)* wählen. Weitere Informationen über den Setup-Assistenten für den Routing- und RAS-Server finden Sie im Abschnitt »Bereitstellen von VPN-Servern« weiter unten in diesem Kapitel. Wenn die Option *RAS (DFÜ oder VPN)* ausgewählt wurde, agiert der Routing- und RAS-Server in der Rolle eines DFÜ- oder VPN-Servers, der Remotezugriff-VPN-Verbindungen unterstützt.

Wenn Sie im Setup-Assistenten für den Routing- und RAS-Server die Option *RAS (DFÜ oder VPN)* auswählen, können Sie folgende Konfigurationseinstellungen vornehmen:

1. Sie müssen zuerst angeben, ob VPN, DFÜ oder beide diese Zugriffsarten benötigt werden.
2. Anschließend müssen Sie auswählen, welche Netzwerkschnittstelle mit dem Internet verbunden ist. In der Standardeinstellung werden für die hier ausgewählte Schnittstelle automatisch IPv4- und IPv6-Paketfilter konfiguriert, die ausschließlich VPN-Verkehr zulassen. Jeglicher andere Verkehr wird stillschweigend verworfen.

Zum Beispiel können Sie keinen Ping-Test mehr für die Internetschnittstelle des VPN-Servers durchführen. Falls Sie andere Dienste auf dem VPN-Server ausführen (zum Beispiel Internetinformationsdienste), müssen Sie von Hand Paketfilter und Ausnahmen zur Windows-Firewall hinzufügen, die den Verkehr zu und von diesen anderen Diensten erlauben.

3. Falls mehrere Netzwerkkarten mit dem Intranet verbunden sind, müssen Sie anschließend auswählen, über welche Schnittstelle die DHCP-, DNS- und WINS-Konfiguration abgerufen wird.
4. Anschließend müssen Sie angeben, ob Sie die IPv4-Adressen, die Remotezugriffsclyents zugewiesen werden, mit DHCP abrufen oder als Adressbereich definieren wollen. Falls Sie einen Adressbereich verwenden wollen, müssen Sie die gewünschten Adressbereiche hinzufügen.
5. Anschließend müssen Sie angeben, ob Sie RADIUS für die Authentifizierung und Kontoführung der VPN-Verbindungen verwenden wollen. Falls Sie RADIUS wählen, müssen Sie primäre und alternative RADIUS-Server und den gemeinsamen geheimen Schlüssel für RADIUS konfigurieren.

Wenn Sie im Setup-Assistenten für den Routing- und RAS-Server die Option *RAS (DFÜ oder VPN)* auswählen und konfigurieren, werden folgende Änderungen an der Konfiguration des Systems durchgeführt:

- Der Routing- und RAS-Dienst wird als IPv4-RAS-Server, LAN-Router und Router für Wählen bei Bedarf aktiviert. Er führt die Authentifizierung und Kontoführung entweder lokal oder über RADIUS durch. Falls nur eine einzige Netzwerkkarte mit dem Intranet verbunden ist, wird automatisch diese Netzwerkkarte verwendet, um die DHCP-, DNS- und WINS-Konfiguration abzurufen. Andernfalls wird die Netzwerkkarte, die im Assistenten angegeben wurde, verwendet, um DHCP-, DNS- und WINS-Konfiguration abzurufen. Falls statische IPv4-Adressbereiche angegeben wurden, werden sie konfiguriert.
- Abhängig von der Windows Server 2008-Version werden bis zu 128 PPTP-Ports, 128 L2TP-Ports und 128 SSTP-Ports erstellt. Jeder Port steht für eine mögliche Remotezugriff-VPN-Verbindung. Alle lassen sowohl eingehende Remotezugriffsverbindungen als auch ein- und ausgehende bei Bedarf herzustellende Wählverbindungen zu (für Standort-zu-Standort-VPN-Verbindungen).
- Die ausgewählte Internetschnittstelle wird mit eingehenden und ausgehenden IPv4- und IPv6-Paketfiltern konfiguriert, die ausschließlich VPN-Verkehr zulassen.
- Die DHCP-Relay-Agent-Komponente wird zur internen Schnittstelle hinzugefügt. Die interne Schnittstelle ist eine logische Schnittstelle, die die Verbindung zu allen anderen authentifizierten Remotezugriffsclients bildet. Falls der VPN-Server ein DHCP-Client ist, während der Assistent ausgeführt wird, wird der DHCP-Relay-Agent automatisch mit der IPv4-Adresse eines DHCP-Servers konfiguriert. Andernfalls müssen Sie die Eigenschaften des DHCP-Relay-Agenten von Hand mit der IPv4-Adresse eines DHCP-Servers in Ihrem Intranet konfigurieren. IPv4-Remotezugriffsclients senden eine DHCPInform-Nachricht, um zusätzliche Konfigurationseinstellungen abzurufen, zum Beispiel DNS-Einstellungen und statische Routen. Der DHCP-Relay-Agent leitet DHCPInform-Nachrichten zwischen VPN-Remotezugriffsclients und einem DHCP-Server im Intranet weiter.
- Die IGMP-Komponente (Internet Group Management Protocol) wird hinzugefügt und die interne Schnittstelle wird für den IGMP-Routermodus konfiguriert. Alle anderen LAN-Schnittstellen werden für den IGMP-Proxymodus konfiguriert. Falls Ihr Intranet IPv4-multicastfähig ist, ist es VPN-Remotezugriffsclients anschließend möglich, IPv4-Multicastverkehr zu senden und zu empfangen.

Entwurfsmöglichkeiten für VPN-Server

- Der VPN-Server kann so konfiguriert werden, dass er IPv4-Adressen über DHCP abrufen oder von Hand konfigurierte Adressbereiche (die sogenannten *statischen Pools* mit Adressen) verwendet. Wird DHCP benutzt, um IPv4-Adressen abzurufen, vereinfacht das die Konfiguration. Sie müssen dann aber sicherstellen, dass der DHCP-Bereich für das Subnetz, in dem sich die Intranetverbindung des VPN-Servers befindet, genug Adressen für alle Computer, die direkt an das Subnetz angeschlossen sind, plus die maximale Zahl von Remotezugriffsclients hat.
Falls Sie einen statischen Pool von Adressen verwenden wollen, gibt es unter Umständen zusätzliche Punkte zum Thema Routing zu berücksichtigen. Weitere Informationen finden Sie im Abschnitt »Konfigurieren der Netzwerkinfrastruktur des Intranets« weiter unten in diesem Kapitel.
- Der VPN-Server kann Authentifizierung und Autorisierung für VPN-Verbindungen entweder selbst erledigen oder dies einem RADIUS-Server überlassen. Wenn Sie den VPN-Server konfigurieren, können Sie wählen, ob Sie Windows oder RADIUS für Authentifizierung und Kontoführung einsetzen wollen.

Wenn der VPN-Server so konfiguriert ist, dass Windows Authentifizierung und Kontoführung erledigt ist, ist er ein Mitglied einer Active Directory-Domäne und kommuniziert mit einem Active Directory-Domänencontroller, um die Anmeldeinformationen des VPN-Clients zu überprüfen und die Einwähleigenschaften für das Benutzerkonto des VPN-Clients zu ermitteln. Der VPN-Server braucht die Benutzerkontoeigenschaften und die lokal konfigurierten Netzwerkrichtlinien, um die VPN-Verbindung zu autorisieren. In der Standardeinstellung protokolliert der VPN-Server Kontoführungsinformationen zur VPN-Verbindung in lokalen Kontoführungsprotokolldateien.

Wenn der VPN-Server so konfiguriert ist, dass er die Authentifizierung und Kontoführung an RADIUS weiterleitet, greift er auf einen konfigurierten RADIUS-Server zurück, um die Anmeldeinformationen des VPN-Clients zu überprüfen, den Verbindungsversuch zu autorisieren und Kontoführungsinformationen zur VPN-Verbindung zu protokollieren. In dieser Konfiguration braucht der VPN-Server nicht Mitglied einer Active Directory-Domäne zu sein. Falls der RADIUS-Server ein Windows Server 2008-Computer ist, auf dem der Netzwerkrichtlinienserver (Network Policy Server, NPS) läuft, muss er Mitglied einer Active Directory-Domäne sein.

- Der Setup-Assistent für den Routing- und RAS-Server aktiviert nicht automatisch die IPv6-Unterstützung für Remotezugriff-VPN-Verbindungen. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von VPN-Servern« weiter unten in diesem Kapitel.

Anforderungen an VPN-Server

- Der VPN-Server muss eine manuelle TCP/IP-IPv4-Konfiguration für seine Internetschnittstelle und die Intranetschnittstellen haben. Weil Konflikte bei der Standardroute auftreten könnten, sollten Sie Ihre Intranetschnittstellen von Hand mit IPv4-Adresse, Subnetzmaske, DNS-Servern und WINS-Servern konfigurieren. Konfigurieren Sie aber kein Standardgateway auf den Intranetschnittstellen des VPN-Servers. Der VPN-Server kann selbst eine manuelle TCP/IP-Konfiguration haben, aber trotzdem DHCP verwenden, um die IPv4-Adressen abzurufen, die er den VPN-Clients zuweist.
- Für VPN-Verbindungen, die mit den Authentifizierungsprotokollen PEAP-MS-CHAP v2, EAP-TLS oder PEAP-TLS arbeiten, müssen Sie auf dem Authentifizierungsserver (entweder der VPN-Server oder der RADIUS-Server) ein Computerzertifikat installieren, das vom VPN-Client überprüft werden kann. Unter Umständen müssen Sie auf Ihrem VPN-Client auch das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installieren, die das Computerzertifikat des Authentifizierungsservers ausgestellt hat.
- Für SSTP-VPN-Verbindungen müssen Sie auf dem VPN-Server ein Computerzertifikat installieren, das vom VPN-Client überprüft werden kann. Unter Umständen müssen Sie auf Ihrem VPN-Client auch das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installieren, die das Computerzertifikat des VPN-Servers ausgestellt hat.
- Für L2TP/IPsec-VPN-Verbindungen müssen Sie auf dem VPN-Server ein Computerzertifikat installieren, das vom VPN-Client überprüft werden kann.
- Falls Sie den VPN-Server für lokale Authentifizierung oder RADIUS-Authentifizierung konfigurieren und der RADIUS-Server ein Computer ist, der NPS ausführt, weist die Standardnetzwerkrichtlinie mit dem Namen *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver* alle Verbindungsversuche ab, sofern nicht in den Einwähleigenschaften des Benutzerkontos die RAS-Berechtigung den Zugriff gestattet. Falls Sie diese Netzwerkrichtlinie für Ihre VPN-Verbindungen verwenden wollen, müssen Sie den Richtlinientyp auf *Zugriff gestatten* ändern. Falls Sie Autorisierung und Verbindungseinstellungen für VPN-Verbindungen anhand der Gruppe oder des Verbindungstyps verwalten wollen, müssen Sie zusätzliche NPS-Richtlinien konfigurieren. Weitere

Informationen finden Sie im Abschnitt »Konfigurieren von RADIUS-Servern« weiter unten in diesem Kapitel.

Empfohlene Vorgehensweise für VPN-Server

- Legen Sie fest, welche Verbindung des VPN-Servers an das Internet angeschlossen ist. VPN-Server, die an das Internet angebunden sind, haben üblicherweise mindestens zwei LAN-Verbindungen: eine, die mit dem Internet verbunden ist (entweder direkt oder über ein Grenznetzwerk), und eine, die mit dem Intranet der Organisation verbunden ist. Um diesen Unterschied für die Arbeit im Setup-Assistenten für den Routing- und RAS-Server deutlich zu machen, sollten Sie die Verbindungen im Ordner *Netzwerkverbindungen* mit Namen versehen, die ihre Aufgabe oder Rolle beschreiben. Wenn zum Beispiel die Verbindung »LAN-Verbindung 2« mit dem Internet verbunden ist, können Sie diese Verbindung in »Internet« umbenennen.

Internetinfrastruktur

Damit ein VPN-Client erfolgreich Verkehr mit einem VPN-Server über das Internet austauschen kann, müssen folgende Bedingungen erfüllt sein:

- Der DNS-Name oder die IP-Adresse des VPN-Servers ist erreichbar.
- Der VPN-Server ist erreichbar.
- VPN-Verkehr zu und vom VPN-Server ist zugelassen.

Auflösbarkeit des VPN-Servernamens

In den meisten Fällen geben Sie den VPN-Server anhand seines vollqualifizierten Domänennamens (Fully Qualified Domain Name, FQDN) an, nicht anhand seiner IPv4- oder IPv6-Adresse. Sie können einen FQDN (zum Beispiel *vpn.example.microsoft.com*) verwenden, sofern der Name in eine IPv4- oder IPv6-Adresse aufgelöst werden kann. Daher müssen Sie sicherstellen, dass der Name, den Sie beim Konfigurieren einer VPN-Verbindung für Ihre VPN-Server angeben, über Internet-DNS-Server in eine IPv4- oder IPv6-Adresse aufgelöst werden kann.

Wenn Sie statt Adressen Namen verwenden, können Sie auch einen Lastausgleich über DNS-Round-Robin implementieren, sofern Sie mehrere VPN-Server mit demselben DNS-Hostnamen haben. Sie können dann in DNS mehrere Einträge anlegen, die einen bestimmten Hostnamen in unterschiedliche IPv4-Adressen auflösen. In diesem Fall senden die DNS-Server alle Adressen als Antwort auf eine DNS-Namensabfrage zurück, wobei sie normalerweise die Reihenfolge der Adressen in nachfolgenden Abfragen nach dem Zufallsprinzip vertauschen. Weil die meisten DNS-Clients die erste Adresse aus einer Antwort auf eine DNS-Abfrage verwenden, werden die VPN-Clientverbindungen also über die VPN-Server verteilt, zumindest solange beide VPN-Server verfügbar sind. Um die Verfügbarkeit des VPN-Servers sicherzustellen, können Sie den Netzwerklastenausgleich nutzen.

Erreichbarkeit des VPN-Servers

Damit der VPN-Server erreichbar ist, muss er eine öffentliche IPv4-Adresse oder eine globale IPv6-Adresse haben, an die Pakete durch die Routinginfrastruktur des IPv4- oder IPv6-Internets weitergeleitet werden. Falls Sie von einem Internetprovider oder einer Internetregistrierung eine statische öffentliche IPv4-Adresse oder ein globales IPv6-Adresspräfix zugewiesen bekommen haben, ist das normalerweise kein Problem. Bei manchen IPv4-Konfigurationen wird der VPN-Server mit einer nichtöffentlichen IPv4-Adresse konfiguriert, hat aber eine öffentliche statische IPv4-Adresse, über die er im Internet erreicht werden kann. Ein Gerät zwischen dem Internet und dem VPN-Server übersetzt

die öffentliche in die tatsächliche IPv4-Adresse des VPN-Servers, und umgekehrt, wenn Pakete zu und vom VPN-Server geleitet werden.

Auch wenn die Routinginfrastruktur die Erreichbarkeit sicherstellt, ist der VPN-Server unter Umständen trotzdem nicht erreichbar, weil Firewalls, Paketfilteringsrouter, NATs, Sicherheitsgateways oder andere Gerätetypen verhindern, dass Pakete vom VPN-Servercomputer gesendet oder empfangen werden.

VPN-Server und Firewallkonfiguration

Es gibt zwei Ansätze, eine Firewall mit einem VPN-Server zu kombinieren:

- **Der VPN-Server ist direkt an das Internet angeschlossen, und die Firewall liegt zwischen dem VPN-Server und dem Intranet.** Bei dieser Konfiguration muss der VPN-Server mit Paketfiltern konfiguriert sein, die ausschließlich VPN-Verkehr in und aus seiner Internetschnittstelle erlauben. Die Firewall kann so konfiguriert sein, dass sie bestimmte Typen von Remotezugriffsverkehr erlaubt.
- **Die Firewall ist an das Internet angeschlossen, und der VPN-Server liegt zwischen Firewall und Intranet.** Bei dieser Konfiguration sind sowohl die Firewall als auch der VPN-Server an ein Subnetz angeschlossen, das als *Grenznetzwerk* (engl. perimeter network oder screened subnet) bezeichnet wird. Firewall und VPN-Server müssen mit Paketfiltern konfiguriert sein, die ausschließlich VPN-Verkehr in und aus dem Internet erlauben.

Einzelheiten zur Konfiguration von Paketfiltern für den VPN-Server und die Firewall in diesen zwei Konfigurationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« weiter unten in diesem Kapitel.

Anforderungen an die Internetinfrastruktur

- Stellen Sie sicher, dass die FQDNs Ihrer VPN-Server aus dem Internet aufgelöst werden können. Tragen Sie dazu entsprechende DNS-Adress- (A) oder IPv6-Adresseinträge (AAAA) in Ihre Internet-DNS-Server oder den DNS-Server Ihres Internetproviders ein. Testen Sie die Auflösbarkeit mit dem Tool Ping, indem Sie alle Ihre VPN-Server anpingen, wenn sie direkt mit dem IPv4- oder IPv6-Internet verbunden sind.
- Aufgrund von Paketfiltern kann es sein, dass der Ping-Befehl das Ergebnis »Anforderungszeitüberschreitung« anzeigt. Prüfen Sie aber, ob der angegebene Name vom Tool Ping in die richtige Adresse aufgelöst werden konnte. Mit dem Befehlszeilenargument -4 können Sie Ping zwingen, eine IPv4-Adresse zu verwenden. Und mit dem Befehlszeilenargument -6 können Sie Ping zwingen, eine IPv6-Adresse zu verwenden. Sie können die Namensauflösung auch mit dem Tool Nslookup testen.
- Stellen Sie sicher, dass die IPv4- oder IPv6-Adressen Ihrer VPN-Server aus dem Internet erreichbar sind, indem Sie mit dem Tool Ping die FQDN oder Adresse Ihres VPN-Servers mit einem 5-Sekunden-Zeitlimit anpingen (verwenden Sie das Befehlszeilenargument -w 5), wenn er direkt mit dem Internet verbunden ist. Falls Sie die Meldung »Ziel nicht erreichbar« erhalten, ist der VPN-Server nicht erreichbar.

Empfohlene Vorgehensweise für die Internetinfrastruktur

Konfigurieren Sie auf den Firewall- und VPN-Serverschnittstellen, die mit dem Internet und dem Grenznetzwerk verbunden sind, die Paketfilterung für PPTP-Verkehr, L2TP-Verkehr, SSTP-Verkehr oder alle Verkehrstypen. Weitere Informationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« weiter unten in diesem Kapitel.

Intranetinfrastruktur

Die Intranetinfrastruktur stellt sicher, dass der VPN-Client Pakete mit Knoten im Intranet austauschen kann, indem er den VPN-Server als IPv4- oder IPv6-Router nutzt. Ohne geeigneten Intranetinfrastrukturentwurf sind VPN-Clients unter Umständen nicht in der Lage, folgende Aktionen durchzuführen:

- Auflösen von Intranetnamen
- Abrufen einer IPv4-Adresse oder eines IPv6-Subnetzpräfixes, das aus dem Intranet erreichbar ist
- Erreichen von Intranetzielen

Intranetnamensauflösung

Stellen Sie sicher, dass jeder VPN-Server mit den IPv4- oder IPv6-Adressen Ihrer Intranet-DNS-Server konfiguriert ist. Falls Sie WINS für die Auflösung von NetBIOS-Namen im Intranet einsetzen, müssen auf den VPN-Servern auch die IPv4-Adressen Ihrer Intranet-WINS-Server konfiguriert sein. Der VPN-Server sollte von Hand mit DNS- und WINS-Servern konfiguriert werden.

Im Rahmen des PPP-Verbindungs-aushandlungsprozesses für IPv4 erhalten VPN-Clients die IPv4-Adressen der DNS- und WINS-Server. In der Standardeinstellung erben die VPN-Clients die DNS- und WINS-Serveradressen, die auf dem VPN-Server konfiguriert sind. Sobald die PPP-Verbindungs-aushandlung abgeschlossen ist, sendet ein VPN-Client, der unter Windows Server 2008, Windows Vista, Windows Server 2003 oder Windows XP läuft, eine DHCPInform-Nachricht zum VPN-Server. Sofern der VPN-Server richtig konfiguriert ist, leitet er die DHCPInform-Nachricht an einen DHCP-Server weiter, der mit einer DHCPAck-Nachricht antwortet. Der VPN-Server sendet die DHCPAck-Nachricht an den VPN-Client. Die Nachricht kann einen DNS-Domänennamen, zusätzliche DNS-Serveradressen für DNS-Server (die vor den DNS-Servern abgefragt werden, die über die PPP-Aushandlung konfiguriert wurden) und WINS-Serveradressen (die die WINS-Serveradressen ersetzen, die bei der PPP-Aushandlung konfiguriert wurden) enthalten. Das Weiterleiten der DHCP-Nachrichten wird von der DHCP-Relay-Agent-Routingprotokollkomponente von Routing und RAS übernommen, die automatisch vom Setup-Assistenten für den Routing- und RAS-Server hinzugefügt wird.

Falls der VPN-Server seine Intranetschnittstellen über DHCP konfiguriert (das wird nicht empfohlen), leitet der VPN-Server die DHCPInform-Nachrichten an den DHCP-Server weiter, der benutzt wurde, als der Setup-Assistent für den Routing- und RAS-Server ausgeführt wurde. Falls der VPN-Server eine statische TCP/IP-Konfiguration auf seiner Intranetschnittstelle hat (empfohlen), muss die DHCP-Relay-Agent-Routingprotokollkomponente mit der IPv4-Adresse mindestens eines DHCP-Servers in Ihrem Intranet konfiguriert werden. Sie können die IPv4-Adressen von DHCP-Servern im Snap-In *Routing und RAS* zur DHCP-Relay-Agent-Routingprotokollkomponente hinzufügen. Öffnen Sie dazu unter *IPv4* das Eigenschaftendialogfeld des Elements *DHCP-Relay-Agent* und klicken Sie auf die Registerkarte *Allgemein*.

Um die IPv6-Adressen von DNS-Servern für VPN-Verbindungen, die nativen IPv6-Verkehr unterstützen, dynamisch zu konfigurieren, benutzen Windows Vista- oder Windows Server 2008-VPN-Clients die Routerankündigungsnachricht, die vom VPN-Server gesendet wird, sobald die IPV6CP-Aushandlung abgeschlossen ist. Falls in der Routerankündigungsnachricht das Flag »Other Stateful Configuration« (O-Flag) gesetzt ist, sendet der VPN-Client eine DHCPv6-Information-Request-Nachricht zum VPN-Server. Sofern auf dem Windows Server 2008-VPN-Server der DHCPv6-Relay-Agent richtig konfiguriert ist, leitet er die Information-Request-Nachricht an einen DHCPv6-Server weiter. Die DHCPv6-Reply-Nachricht wird im Gegenzug an den VPN-Client weitergeleitet. Sie kann die IPv6-Adressen von DNS-Servern im Intranet enthalten.

Anforderungen an die Intranetnamensauflösung

- Testen Sie mit den Tools Ping und Net vom VPN-Servercomputer aus die DNS- und WINS-Namensauflösung für Intranetressourcen. Falls die Namensauflösung vom VPN-Server aus nicht funktioniert, klappt sie möglicherweise auch nicht für die VPN-Clients. Führen Sie eine Problembehandlung durch und beseitigen Sie alle Namensauflösungsprobleme des VPN-Servers, bevor Sie die VPN-Verbindungen testen.
- Weil die Intranetschnittstellen des VPN-Servers von Hand mit TCP/IP-Einstellungen konfiguriert werden, kann der Setup-Assistent für den Routing- und RAS-Server die DHCP-Relay-Agent-Routingprotokollkomponente nicht automatisch konfigurieren. Sie müssen die IPv4-Adresse mindestens eines DHCP-Servers in Ihrem Intranet von Hand zur DHCP-Relay-Agent-Komponente hinzufügen. Falls Sie das nicht tun, verwirft der VPN-Server DHCPInform-Nachrichten, die von den VPN-Clients gesendet wurden, und die VPN-Clients erhalten keine aktualisierten DNS- und WINS-Serveradressen oder den DNS-Domänennamen.
- Falls Sie ein SOHO-Netzwerk (Small Office/Home Office) haben, das aus lediglich einem einzigen Subnetz besteht und keine DHCP-, DNS- oder WINS-Server enthält, müssen Sie entweder einen DNS-Server oder einen WINS-Server konfigurieren, um Namen für Computer im SOHO-Subnetz und VPN-Clients aufzulösen, oder die NetBIOS-Broadcastnamensauflösung aktivieren, wodurch die NetBIOS-über-TCP/IP-Namensauflösung zwischen verbundenen VPN-Clients und Computern im SOHO-Netzwerk ermöglicht wird. Sie können die NetBIOS-Broadcastnamensauflösung im Snap-In *Routing und RAS* aktivieren. Aktivieren Sie im Eigenschaftendialogfeld eines VPN-Servers auf der Registerkarte *IPv4* das Kontrollkästchen *Broadcastnamensauflösung aktivieren*.
- Damit DHCPv6-Nachrichten zwischen IPv6-fähigen VPN-Clients und einem DHCPv6-Intranetserver weitergeleitet werden, müssen Sie die DHCPv6-Relay-Agent-Routingprotokollkomponente hinzufügen und konfigurieren. Weitere Informationen dazu finden Sie im Abschnitt »Bereitstellen von VPN-Servern« weiter unten in diesem Kapitel.

Empfohlene Vorgehensweise für Intranetnamensauflösung

Um sicherzustellen, dass VPN-Clients die aktuellste Liste der IPv4-Adressen von DNS- und WINS-Servern erhalten, sollten Sie die DHCP-Relay-Agent-Komponente von Routing und RAS von Hand konfigurieren, statt es dem VPN-Server zu überlassen, VPN-Clients mit den IPv4-Adressen seiner eigenen DNS- und WINS-Server zu konfigurieren.

Routing des VPN-Servers ins Internet und Intranet

Der VPN-Server ist ein IPv4- und IPv6-Router, der Pakete zwischen VPN-Clients und Knoten im Intranet weiterleitet. Daher muss er mit dem richtigen Satz Routen konfiguriert werden, sodass er jede beliebige Internetadresse (weil ein VPN-Client von überall im Internet eine Verbindung herstellen kann) und alle Intranetadressen erreichen kann. Für IPv4- wie auch IPv6-Verkehr benötigt der VPN-Server folgende Einstellungen:

- Eine Standardroute, die auf eine Firewall oder einen Router verweist, der direkt mit dem Internet verbunden ist. Diese Route macht alle Adressen im Internet erreichbar.
- Mindestens eine Route, die den in Ihrem Intranet benutzten Adressraum abdeckt und auf einen benachbarten Intranetrouter verweist. Diese Routen machen alle Adressen in Ihrem Intranet vom VPN-Server aus erreichbar. Ohne diese Routen sind Intranethosts, die an ein anderes Intranetsubnetz angeschlossen sind als der VPN-Server, nicht erreichbar.

Um eine Standardroute einzurichten, die in das Internet verweist, müssen Sie die Internetschnittstelle des VPN-Servers mit einem Standardgateway konfigurieren. Sie dürfen aber kein Standardgateway für die Intranetschnittstellen eintragen. Falls Sie Ihre Intranetschnittstellen mit Standardgateways konfigurieren, haben Sie mehrere Standardrouten in den IPv4- und IPv6-Routingtabellen des VPN-Servers. Wenn mehrere Standardrouten vorhanden sind, kann das aufgrund der Art und Weise, wie TCP/IP die Standardroute für die Weiterleitung von Standardroutenverkehr auswählt, dazu führen, dass Standardroutenverkehr ins Intranet weitergeleitet wird statt ins Internet. Dann sind keine Internetziele erreichbar.

Sie haben folgende Möglichkeiten, um Intranetrouten zur Routingtabelle des VPN-Servers hinzuzufügen:

- Fügen Sie statische IPv4- und IPv6-Routen mit dem Snap-In *Routing und RAS* hinzu. Sie brauchen nicht für jedes Subnetz in Ihrem Intranet eine eigene Route hinzuzufügen. Zumindest müssen Sie aber die Routen hinzufügen, die den IPv4- oder IPv6-Adressraum abdecken, der in Ihrem Intranet benutzt wird.

Falls Ihr Intranet zum Beispiel den nichtöffentlichen IPv4-Adressraum 10.0.0.0/8 für seine Subnetze und Hosts verwendet, brauchen Sie nicht für jedes Subnetz eine eigene Route hinzuzufügen. Tragen Sie einfach eine Route für 10.0.0.0 mit der Subnetzmaske 255.0.0.0 ein, die auf einen benachbarten Router in dem Intranetsubnetz verweist, an das Ihr VPN-Server angeschlossen ist.

- Falls Sie in Ihrem Intranet RIP (Routing Information Protocol) einsetzen, können Sie die RIP-Komponente des Routing- und RAS-Dienstes hinzufügen und konfigurieren, sodass der VPN-Server sich als RIP-Router an der Bekanntgabe von Intranetroutinginformationen beteiligt.

Falls Ihr Intranet nur ein einziges Subnetz umfasst, ist keine weitere Konfiguration erforderlich.

Routing von VPN-Clients in das Intranet

Ob VPN-Clients aus dem Intranet heraus für IPv4-Verkehr erreichbar sind, hängt davon ab, wie der VPN-Server die IPv4-Adressen ermittelt, die er den VPN-Clients zuweist. Die IPv4-Adressen, die den VPN-Clients zugewiesen werden, sobald sie eine Verbindung herstellen, können aus folgenden Bereichen stammen:

- Ein *subnetzinterner Adressbereich* (engl. on-subnet address range) ist ein Adressbereich des Intranetsubnetzes, an das der VPN-Server angeschlossen ist.

Ein subnetzinterner Adressbereich wird benutzt, wenn der VPN-Server so konfiguriert ist, dass er die IP-Adressen für VPN-Clients über DHCP abrufen, oder wenn die von Hand konfigurierten Pools der IPv4-Adressen innerhalb des Adressbereichs des angeschlossenen Subnetzes liegen.

- Ein *subnetzexterner Adressbereich* (engl. off-subnet address range) ist ein Adressbereich, der für ein anderes Subnetz steht, mit dem der VPN-Server logisch verbunden ist.

Ein subnetzexterner Adressbereich wird benutzt, wenn der VPN-Server von Hand mit Pools von IPv4-Adressen aus einem anderen Subnetz konfiguriert wurde.

Falls Sie einen subnetzinternen Adressbereich verwenden, ist keine zusätzliche Routingkonfiguration erforderlich, weil der VPN-Server als ARP-Proxy (Address Resolution Protocol) für alle Pakete agiert, die an VPN-Clients gesendet werden. Router und Hosts im Subnetz des VPN-Servers leiten Pakete, die an die VPN-Clients gerichtet sind, zum VPN-Server weiter, der sie dann an den richtigen VPN-Client sendet.

Falls Sie einen subnetzexternen Adressbereich verwenden, müssen Sie die Routen, die den subnetzexternen Adressbereich abdecken, zur Intranetroutinginfrastruktur hinzufügen, sodass Verkehr, der an die VPN-Clients gerichtet ist, zum VPN-Server weitergeleitet und von dort vom VPN-Server an den

jeweiligen VPN-Client gesendet wird. Damit Sie die Adressbereiche für alle Routen optimal zusammenfassen können, sollten Sie Adressbereiche wählen, die sich mit einem einzigen Präfix und einer Subnetzmaske ausdrücken lassen.

Sie können Routen, die den subnetzexternen Adressbereich abdecken, zur Routinginfrastruktur des Intranets hinzufügen, indem Sie für den subnetzexternen Adressbereich statische Routen, die auf die Intranetschnittstelle des VPN-Servers verweisen, zu einem benachbarten Router des VPN-Servers hinzufügen. Konfigurieren Sie den benachbarten Router so, dass er diese statische Route über das dynamische Routingprotokoll, das in Ihrem Intranet eingesetzt wird, an andere Router im Intranet weitergibt.

Falls Ihr Intranet lediglich ein einziges Subnetz umfasst, müssen Sie entweder auf jedem Intranethost persistente Routen des subnetzexternen Adressbereichs konfigurieren, die auf die Intranetschnittstelle des VPN-Servers verweisen, oder auf jedem Intranethost den VPN-Server als Standardgateway eintragen. Daher wird empfohlen, dass Sie für ein SOHO-Netzwerk, das nur aus einem einzigen Subnetz besteht, einen subnetzinternen Adresspool verwenden.

Bei IPv6-VPN-Verbindungen definiert das Subnetzpräfix, das VPN-Clients in der Routerankündigungsnachricht zugewiesen wird, immer ein anderes Subnetz als das, an das der VPN-Server angeschlossen ist. Alle VPN-Clients bekommen dasselbe Subnetzpräfix, und dies ist immer ein subnetzexternes Präfix. Damit die VPN-Clients aus dem Intranet heraus erreichbar sind, müssen Sie das Subnetzpräfix als Route, die zum VPN-Server verweist, zu Ihrer IPv6-Routinginfrastruktur hinzufügen.

Anforderungen an die Intranetroutinginfrastruktur

- Konfigurieren Sie die Internetschnittstelle des VPN-Servers mit einem Standardgateway, aber konfigurieren Sie *nicht* die Intranetschnittstellen des VPN-Servers mit einem Standardgateway.
- Fügen Sie statische IPv4- und IPv6-Routen zum VPN-Server hinzu, die alle Adressen abdecken, die in Ihrem Intranet benutzt werden. Falls Sie RIP als Protokoll für dynamisches IPv4-Routing einsetzen, können Sie stattdessen auch RIP auf dem VPN-Server konfigurieren und aktivieren. Falls Sie ein anderes Routingprotokoll als RIP verwenden, können Sie unter Umständen das entsprechende Routenweitergabeverfahren nutzen. Falls Sie zum Beispiel IGRP (Interior Gateway Routing Protocol) verwenden, können Sie den benachbarten Intranetrouter des VPN-Servers so konfigurieren, dass er auf der Schnittstelle, die mit dem Subnetz des VPN-Servers verbunden ist, RIP benutzt und auf allen anderen Schnittstellen IGRP.
- Fügen Sie das IPv6-Subnetzpräfix für IPv6-fähige VPN-Clients als Route, die auf den VPN-Server verweist, zu Ihrer IPv6-Routinginfrastruktur hinzu.

Empfohlene Vorgehensweise für die Intranetroutinginfrastruktur

Konfigurieren Sie den VPN-Server nach Möglichkeit mit einem subnetzinternen Adressbereich, indem Sie die IPv4-Adressen entweder über DHCP abrufen oder von Hand subnetzinterne Adresspools konfigurieren.

Gleichzeitiger Intranet- und Internetzugriff für VPN-Clients

Wenn ein Windows-VPN-Client eine VPN-Verbindung herstellt, fügt er in der Standardeinstellung automatisch eine neue Standardroute für die VPN-Verbindung hinzu und ändert die vorhandene Standardroute so, dass sie eine höhere Metrik hat. Da die neue Standardroute hinzugefügt wird, sind außer der IPv4-Adresse des VPN-Servers und Zielen, die über andere Routen angesprochen werden, keine Internetziele mehr erreichbar, während die VPN-Verbindung besteht.

Sie können verhindern, dass die Standardroute erstellt wird, indem Sie die VPN-Verbindung so konfigurieren, dass sie nicht das Standardgateway des Remotenetzwerks benutzt. Gehen Sie für VPN-Verbindungen im Ordner *Netzwerkverbindungen* folgendermaßen vor:

1. Öffnen Sie in den Eigenschaften der VPN-Verbindung auf der Registerkarte *Netzwerk* das Eigenschaftendialogfeld der Komponente *Internetprotokoll (TCP/IP)* oder *Internetprotokoll Version 4 (TCP/IPv4)*.
2. Klicken Sie auf *Erweitert*.
3. Deaktivieren Sie im Dialogfeld *Erweiterte TCP/IP-Einstellungen* auf der Registerkarte *IP-Einstellungen* das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden*.

Wenn das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* deaktiviert ist, wird beim Herstellen der Verbindung keine Standardroute erstellt. Es wird allerdings eine Route erstellt, die der Internetadressklasse der zugewiesenen IPv4-Adresse entspricht. Falls zum Beispiel während des Verbindungsprozesses die Adresse 10.0.12.119 zugewiesen wird, erstellt der Windows-VPN-Client eine Route für das Klassenadresspräfix 10.0.0.0 mit der Subnetzmaske 255.0.0.0.

Abhängig von der Einstellung des Kontrollkästchens *Standardgateway für das Remotenetzwerk verwenden* gibt es zwei Möglichkeiten, während die VPN-Verbindung aktiv ist:

- Internetziele sind erreichbar; Intranetziele sind nicht erreichbar, sofern sie nicht der Adressklasse der zugewiesenen IP-Adresse entsprechen. (Das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* ist deaktiviert.)
- Alle Intranetziele sind erreichbar; Internetziele sind nicht erreichbar, sofern es sich nicht um die Adresse des VPN-Servers oder Ziele handelt, die über andere Routen angesprochen werden. (Das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* ist aktiviert.)

Bei den meisten ans Internet angeschlossenen VPN-Clients verursacht dieses Verhalten keine Probleme, weil sie meist entweder mit dem Intranet oder dem Internet kommunizieren, aber nicht mit beiden gleichzeitig.

Wenn Sie wollen, dass VPN-Clients gleichzeitigen Zugriff auf Intranet- und Internetressourcen haben, während die VPN-Verbindung aktiv ist (das sogenannte *getrennte Tunneln* oder engl. *split tunneling*), haben Sie folgende Möglichkeiten:

- Aktivieren Sie das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* (dies ist die Standardeinstellung) und erlauben Sie Internetzugriff über das Intranet der Organisation. Internetverkehr zwischen dem VPN-Client und Internethosts wird durch Firewalls oder Proxyserver geleitet, als wäre der VPN-Client physisch ans Intranet der Organisation angeschlossen. Die Leistung sinkt dabei zwar etwas, aber diese Methode erlaubt es, den Internetzugriff entsprechend den Netzwerkrichtlinien der Organisation zu filtern und zu überwachen, während der VPN-Client mit dem Unternehmensnetzwerk verbunden ist.
- Falls die IPv4-Adressierung innerhalb Ihres Intranets mit einem einzigen klassenbasierten Adresspräfix arbeitet, können Sie das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* deaktivieren. Das geht zum Beispiel, wenn Ihr Intranet das nichtöffentliche IPv4-Adresspräfix 10.0.0.0/8 verwendet.
- Falls die IPv4-Adressierung innerhalb Ihres Intranets nicht mit einem einzigen klassenbasierten Adresspräfix arbeitet, können Sie eine der folgenden Lösungen wählen:
 - Die DHCP-Option *Statische Routen ohne Klassen*
 - Das Verbindungs-Manager-Verwaltungskit
 - Eine Befehlsdatei (.cmd) auf dem VPN-Client

Weitere Informationen über diese Methoden finden Sie im Abschnitt »Konfigurieren von gleichzeitigem Zugriff auf Internet und Intranet« weiter unten in diesem Kapitel.



Hinweis Bei nativen IPv6-VPN-Clients wird die Standardroute anhand der vom VPN-Server geschickten Routerankündigung hinzugefügt. Falls das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* für das Protokoll TCP/IPv6 aktiviert ist, wird die Schnittstellenmetrik der VPN-Verbindung (die zur Metrik der IPv6-Standardroute wird, die diese VPN-Verbindung benutzt) auf einen geringen Wert gesetzt, sodass die Standardroute über die VPN-Verbindung die niedrigste Metrik hat. Falls das Kontrollkästchen *Standardgateway für das Remotenetzwerk verwenden* deaktiviert ist, wird die Schnittstellenmetrik der VPN-Verbindung auf einen statischen Wert oder eine automatische Metrik gesetzt. Dieser Wert ist aber niemals die niedrigste Metrik. Daher kann es sein, dass die Standardroute über die VPN-Verbindung nicht die geringste Metrik hat.

Authentifizierungsinfrastruktur

Die Authentifizierungsinfrastruktur hat folgende Aufgaben:

- Authentifizieren der Anmeldeinformationen von VPN-Clients
- Autorisieren der VPN-Verbindung
- Aufzeichnen von Aufbau und Beendigung der VPN-Verbindung für Kontoführungszwecke

Die Authentifizierungsinfrastruktur für Remotezugriff-VPN-Verbindungen besteht aus folgenden Komponenten:

- Der VPN-Servercomputer
- Ein RADIUS-Servercomputer
- Ein Domänencontroller
- Eine ausstellende Zertifizierungsstelle einer PKI (optional)

Durchführen der Authentifizierung mit Windows oder RADIUS

Ein VPN-Server, der unter Windows Server 2008 läuft, kann so konfiguriert werden, dass er entweder Windows oder RADIUS für die Authentifizierung und Kontoführung verwendet. RADIUS bietet zentralisierte Authentifizierungs-, Autorisierungs- und Kontoführungsdienste, wenn Sie mehrere VPN-Server oder eine Mischung aus heterogenen DFÜ- und VPN-Geräten oder anderen Arten von Zugriffsservern haben, zum Beispiel Drahtloszugriffspunkte.

Wenn der VPN-Server Windows für die Authentifizierung nutzt, führt er die Authentifizierung der VPN-Verbindung durch, indem er über einen geschützten RPC-Kanal (Remote Procedure Call, Remoteprozeduraufruf) mit einem Domänencontroller kommuniziert. Die Autorisierung des Verbindungsversuchs führt er über die Einwähleigenschaften des Benutzerkontos und lokal konfigurierte Netzwerkrichtlinien durch. Wenn der VPN-Server RADIUS für die Authentifizierung nutzt, überlässt er die Durchführung von Authentifizierung und Autorisierung einem RADIUS-Server.

Wenn der VPN-Server Windows für die Authentifizierung nutzt, zeichnet er VPN-Verbindungsinformationen in einer lokalen Protokolldatei (in der Standardeinstellung `%SystemRoot%\System32\Logfiles\Logfile.log`) auf. Die entsprechenden Einstellungen werden im Knoten *Kontoführung* des Snap-Ins *Netzwerkrichtlinienserver* konfiguriert. Wenn der VPN-Server RADIUS für die Authentifizierung nutzt, erledigt der RADIUS-Server die Protokollierung der Kontoführungsinformationen.

Falls Sie RADIUS verwenden und eine Windows-Domäne als Benutzerkontodatenbank einsetzen, anhand derer die Benutzeranmeldeinformationen überprüft und Einwähleigenschaften abgerufen wer-

den, sollten Sie NPS unter Windows Server 2008 verwenden. NPS ist ein leistungsfähiger RADIUS-Server und -Proxy, der eng in Active Directory sowie Routing und RAS integriert ist.

Wenn NPS als RADIUS-Server eingesetzt wird, erfüllt es folgende Aufgaben:

- NPS führt die Authentifizierung der VPN-Verbindung durch, indem es über einen geschützten RPC-Kanal mit einem Domänencontroller kommuniziert. NPS führt die Autorisierung des Verbindungsversuchs anhand der Einwähleigenschaften des Benutzerkontos und der auf dem NPS-Server konfigurierten Netzwerkrichtlinien durch.
- NPS zeichnet in der Standardeinstellung alle RADIUS-Kontoführungsinformationen in einer lokalen Protokolldatei (in der Standardeinstellung *%SystemRoot%\System32\Logfiles\Logfile.log*) auf. Diese Einstellungen können Sie im Knoten *Kontoführung* des Snap-Ins *Netzwerkrichtlinienserver* konfigurieren.

Empfohlene Vorgehensweise für die Authentifizierungsinfrastruktur

- Falls Sie mehrere VPN-Server haben und Authentifizierungs-, Autorisierungs- und Kontoführungsdienste zentralisieren wollen, oder falls Sie eine heterogene Mischung aus Netzwerkzugriffsgaräten haben, sollten Sie einen RADIUS-Server verwenden und den VPN-Server so konfigurieren, dass er RADIUS für Authentifizierung und Kontoführung benutzt.
- Falls Sie den Active Directory-Domänendienst als Benutzerkontodatenbank einsetzen, sollten Sie NPS als Ihren RADIUS-Server verwenden. In Kapitel 9 finden Sie weitere Informationen zu Entwurf und Planung von NPS-RADIUS-Servern.
- Um die Autorisierung für Remotezugriff-VPN-Verbindungen besser verwalten zu können, sollten Sie in Active Directory eine universelle Gruppe für VPN-Zugriff anlegen, die globale Gruppen für alle Benutzerkonten enthält, die Remotezugriff-VPN-Verbindungen herstellen dürfen. Zum Beispiel können Sie eine universelle Gruppe namens *VPNBenutzer* erstellen, deren Mitglieder globale Gruppen sind, die den geografischen oder organisatorischen Aufbau Ihrer Organisation widerspiegeln. Jede globale Gruppe enthält Benutzerkonten, für die VPN-RAS erlaubt ist. Wenn Sie Ihre NPS-Richtlinien für VPN-Verbindungen konfigurieren, geben Sie den Gruppennamen *VPNBenutzer* an.
- Unabhängig davon, ob der VPN-Server für lokale oder RADIUS-Authentifizierung konfiguriert ist, sollten Sie eine VPN-spezifische Netzwerkrichtlinie verwenden, um VPN-Verbindungen zu autorisieren und Verbindungseinschränkungen sowie Anforderungen zu definieren. Zum Beispiel können Sie mithilfe von Netzwerkrichtlinien den Zugriff aufgrund der Gruppenmitgliedschaft gewähren, sichere Verschlüsselung fordern, die Benutzung bestimmter Authentifizierungsmethoden (zum Beispiel PEAP-MS-CHAP v2 oder EAP-TLS) fordern oder den Verkehr mithilfe von IP-Paketfilterung einschränken.

VPN-Clients

Der VPN-Client kann ein beliebiger Computer sein, sofern er in der Lage ist, eine PPTP-Verbindung mit MPPE-Verschlüsselung, eine L2TP-Verbindung mit IPsec-Verschlüsselung oder eine SSTP-Verbindung mit SSL-Verschlüsselung aufzubauen. Ein Windows-VPN-Client, der unter Windows Vista, Windows Server 2008, Windows Server 2003 oder Windows XP läuft, kann PPTP- und L2TP/IPsec-VPN-Verbindungen aufbauen. Ein Windows-VPN-Client, der unter Windows Vista SP1 oder Windows Server 2008 läuft, kann zusätzlich SSTP-VPN-Verbindungen aufbauen.

Sie können VPN-Verbindungen auf dem Windows-VPN-Client entweder von Hand oder mithilfe der Verbindungs-Manager-Komponenten aus Windows Server 2008 konfigurieren. Wie die manuelle

Konfiguration der VPN-Verbindungen im Einzelnen abläuft, hängt von der verwendeten Windows-Version ab. Es gibt für die unterschiedlichen Versionen folgende Möglichkeiten:

- Bei einem VPN-Client, der unter Windows Vista oder Windows Server 2008 läuft, müssen Sie im Netzwerk- und Freigabecenter auf *Verbindung mit einem Netzwerk herstellen* klicken. Um eine VPN-Verbindung aufzubauen, müssen Sie die IP-Adresse oder den DNS-Namen des VPN-Servers im Internet angeben.
- Bei einem VPN-Client, der unter Windows XP oder Windows Server 2003 läuft, müssen Sie den Assistenten für neue Verbindungen aus dem Ordner *Netzwerkverbindungen* starten.

Verbindungs-Manager

Wenn Sie die Konfiguration von VPN-Verbindungen für ein großes Unternehmensnetzwerk skalieren, treten unter Umständen folgende Probleme auf:

- Je nachdem, welche Windows-Version auf einem Clientcomputer läuft, müssen VPN-Verbindungen auf unterschiedliche Weise konfiguriert werden.
- Um Konfigurationsfehler zu vermeiden, sollte die IT-Abteilung das Konfigurieren der VPN-Verbindung übernehmen, nicht der Benutzer.
- Eine Konfigurationsmethode muss sich für Hunderte oder Tausende von Clientcomputern in einer großen Organisation skalieren lassen.
- Unter Umständen muss für eine VPN-Verbindung eine Mehrfacheinwahl konfiguriert werden, das heißt, ein Benutzer muss eine DFÜ-Verbindung ins Internet herstellen, bevor er eine VPN-Verbindung mit dem Intranet der Organisation aufbauen kann.

Der Verbindungs-Manager beseitigt alle diese Probleme beim Konfigurieren von VPN-Verbindungen in einem großen Unternehmen. Der Verbindungs-Manager besteht aus folgenden Komponenten:

- Verbindungs-Manager-Clientwählprogramm
- Verbindungs-Manager-Verwaltungskit
- Connection Point Services

Verbindungs-Manager-Clientwählprogramm

Das Verbindungs-Manager-Clientwählprogramm ist eine Software, die auf jedem VPN-Client installiert wird. Sie umfasst erweiterte Features, die den Leistungsumfang der grundlegenden Remote-zugriffsnetzwerkfunktionen erweitern. Aber das Verbindungs-Manager-Clientwählprogramm bietet dem Benutzer auch eine einfacher bedienbare Oberfläche für die Verbindungsherstellung. Es beschränkt die Zahl der Konfigurationsoptionen, die ein Benutzer verändern kann. So ist sichergestellt, dass der Benutzer immer erfolgreich eine Verbindung aufbauen kann. Zum Beispiel beherrscht das Verbindungs-Manager-Clientwählprogramm folgende Funktionen:

- Verwenden angepasster Grafiken, Symbole, Meldungen und Hilfetexte
- Automatischer Aufbau einer DFÜ-Verbindung, bevor die VPN-Verbindung hergestellt wird
- Ausführen benutzerdefinierter Aktionen während verschiedener Phasen des Verbindungsprozesses, zum Beispiel Aktionen vor und nach dem Herstellen der Verbindung (die ausgeführt werden, bevor oder nachdem die DFÜ- oder VPN-Verbindung abgeschlossen ist)
- Bei DFÜ-Verbindungen kann der Benutzer abhängig vom momentanen Standort aus einer Liste von Telefonnummern auswählen

Ein *angepasstes Profil für das Verbindungs-Manager-Clientwählprogramm* (kurz als Verbindungs-Manager-Profil, Paket oder engl. *package* bezeichnet) ist eine selbstentpackende ausführbare Datei,

die von einem Netzwerkadministrator mit dem Verbindungs-Manager-Verwaltungskit erstellt wird. Das Verbindungs-Manager-Profil wird über CD-ROMs, E-Mail, eine Website oder eine Dateifreigabe an die VPN-Benutzer verteilt. Wenn der Benutzer das Verbindungs-Manager-Profil ausführt, konfiguriert es automatisch die angepasste DFÜ- oder VPN-Verbindung. Das Verbindungs-Manager-Profil setzt keine bestimmte Windows-Version voraus. Es konfiguriert Verbindungen für Computer, die unter Windows Server 2008, Windows Vista, Windows Server 2003 oder Windows XP laufen.

Verbindungs-Manager-Verwaltungskit

Ein angepasstes Verbindungs-Manager-Profil erstellen Sie mit dem Verbindungs-Manager-Verwaltungskit (Connection Manager Administration Kit, CMAK). Mit dem Verbindungs-Manager-Verwaltungskit können Sie Clientwählprogramm- und Verbindungssoftware entwickeln, die es Ihren Benutzern erlaubt, eine Verbindung zum Netzwerk herzustellen, wobei sie nur die Verbindungsfeatures verwenden können, die Sie freigegeben haben. Das Verbindungs-Manager-Profil unterstützt eine Vielzahl von Features, die die Implementierung der Verbindungsunterstützung für Sie und Ihre Benutzer sowohl vereinfachen als auch erweitern. Die meisten dieser Features können mit dem Verbindungs-Manager-Verwaltungskit genutzt werden. Mit dem Verbindungs-Manager-Verwaltungskit können Sie Verbindungs-Manager-Profile erstellen und das Verbindungs-Manager-Clientwählprogramm so anpassen, dass die Verbindung die Besonderheiten Ihrer Organisation widerspiegelt. Sie können damit festlegen, welche Funktionen und Features Sie zur Verfügung stellen wollen und auf welche Weise Ihre Benutzer die DFÜ- oder VPN-Verbindung angeboten bekommen.

Connection Point Services

Connection Point Services (CPS) erlauben Ihnen, benutzerdefinierte Telefonbücher für DFÜ-Verbindungs-Manager-Profile automatisch zu verteilen und zu aktualisieren. Diese Telefonbücher enthalten mindestens einen POP-Eintrag (Point Of Presence), wobei jeder POP eine Telefonnummer angibt, die DFÜ-Zugriff auf ein Intranet oder (häufiger) auf einen Internetzugriffspunkt bietet. Die Telefonbücher liefern Benutzern vollständige POP-Informationen. Wenn sie auf Reisen sind, können sie auf diese Weise Verbindungen mit unterschiedlichen Internetzugriffspunkten herstellen, und bleiben nicht auf einen einzigen POP beschränkt.

Ohne die Fähigkeit, Telefonbücher zu aktualisieren (was CPS automatisch erledigt), müssten Benutzer Kontakt mit dem technischen Support Ihrer Organisation aufnehmen, um sich über Änderungen an den POP-Daten zu informieren und ihre Clientwählprogrammsoftware zu aktualisieren.

CPS hat zwei Komponenten:

- **Telefonbuchverwaltung** Ein Tool zum Erstellen und Verwalten der Telefonbuchdatenbank und zum Veröffentlichen neuer Telefonbuchdaten im Telefonbuchdienst
- **Telefonbuchdienst** Eine Erweiterung der Microsoft Internetinformationsdienste 7.0 (Internet Information Services, IIS). Ein Verbindungs-Manager-Profil kann so konfiguriert werden, dass es beim Telefonbuchdienst, der auf einem angegebenen IIS-Server läuft, sicherstellt, dass sein Telefonbuch auf dem neuesten Stand ist. Ist das nicht der Fall, lädt der Remotezugriffsklient automatisch ein Telefonbuchupdate herunter.

Entwurfsmöglichkeiten für VPN-Clients

- Falls Sie eine kleine Zahl von VPN-Clients haben, können Sie die VPN-Verbindungen auf jedem Computer von Hand konfigurieren.
- Falls Sie eine große Zahl von VPN-Clients haben oder unterschiedliche Windows-Versionen verwenden, sollten Sie mit den Verbindungs-Manager-Komponenten aus Windows Server 2008 ein

Verbindungs-Manager-Profil erstellen, das angepasste VPN-Konfigurationseinstellungen enthält. Für DFÜ-Verbindungen sollten Sie außerdem eine Telefonbuchdatenbank verwalten.

Anforderungen an VPN-Clients

- Für L2TP/IPsec-Verbindungen müssen Sie ein Computerzertifikat auf dem VPN-Clientcomputer installieren.
- Für die Authentifizierungsmethoden PEAP-TLS oder EAP-TLS müssen Sie entweder ein Benutzerzertifikat auf dem VPN-Clientcomputer installieren oder Smartcards an Ihre Benutzer ausgeben.
- Für SSTP-Verbindungen müssen Sie sicherstellen, dass bei den VPN-Clients das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert ist, die das Computerzertifikat des VPN-Servers ausgestellt hat.
- Falls Ihre VPN-Clients bei den Authentifizierungsmethoden PEAP-MS-CHAP v2 oder PEAP-TLS das Zertifikat des Authentifizierungsservers überprüfen (empfohlen), müssen Sie sicherstellen, dass auf den VPN-Clients das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert ist, die das Computerzertifikat des Authentifizierungsservers ausgestellt hat.

Entwurfsmöglichkeiten für Verbindungs-Manager-Profile

- Der Name des Verbindungs-Manager-Profiles sollte seinen Zweck und seine Verwendungsmöglichkeiten widerspiegeln, weil dieser Name für die Verbindung im Ordner *Netzwerkverbindungen* angezeigt wird, sobald das Profil auf dem VPN-Client installiert wurde.
- Sie können Einstellungen aus vorhandenen Profilen in neue Profile zusammenführen. Die neuen Profile erben die Einstellungen der Basisprofile.
- Der VPN-Clientcomputer muss unter Umständen eine DFÜ-Verbindung herstellen, um Internetzugriff aufzubauen, bevor er die VPN-Verbindung herstellen kann.
- Falls VPN-Clients gleichzeitigen Zugriff auf Internet und Intranet brauchen, können Sie das Verbindungs-Manager-Profil so konfigurieren, dass es statische Routen für Intranetziele zur Routingtabelle des VPN-Clients hinzufügt. Weitere Informationen finden Sie im Abschnitt »Konfigurieren von gleichzeitigem Zugriff auf Internet und Intranet« weiter unten in diesem Kapitel.
- Das Verbindungs-Manager-Profil kann so konfiguriert werden, dass es beim VPN-Client automatisch die Internet Explorer-Proxyeinstellungen für die Intranetproxyserver einträgt.
- Falls Sie während verschiedener Phasen des VPN-Verbindungsaufbaus bestimmte Programme ausführen müssen, um zum Beispiel bestimmte Dienste zu deaktivieren oder ein Windows-Programm zu starten (dies sind sogenannte *Aktionen*), können Sie benutzerdefinierte Aktionen konfigurieren. Zum Beispiel können Sie Aktionen konfigurieren, die ausgeführt werden, bevor die Verbindung hergestellt wird (eine sogenannte Pre-Connect-Aktion) oder nachdem die Verbindung aufgebaut ist (Post-Connect-Aktion).
- Falls Sie ein eigenes Anmeldebild mit dem Logo Ihrer Organisation anzeigen wollen, wenn Ihre Benutzer die VPN-Verbindung aktivieren, können Sie dafür eine Bitmapdatei mit den Abmessungen 330 × 140 Pixel erstellen.
- Falls Sie ein eigenes Bild mit dem Logo Ihrer Organisation anzeigen wollen, wenn Ihre Benutzer auf das Telefonbuch zugreifen, können Sie dafür eine Bitmapdatei mit den Abmessungen 114 × 309 Pixel erstellen.

- Falls Sie eigene Programm- und Titelzeilensymbole für die VPN-Verbindung im Netzwerk- und Freigabecenter oder dem Ordner *Netzwerkverbindungen* anzeigen wollen, können Sie dafür Bitmapdateien mit den Abmessungen 32 × 32 Pixel beziehungsweise 16 × 16 Pixel erstellen.
- Falls Sie Ihren Benutzern eine angepasste Hilfe für die VPN-Verbindung zur Verfügung stellen wollen, können Sie dafür eine Hilfedatei im CHM-Format (Compiled Help Module) erstellen.
- Sie können Dateien hinzufügen, die zusammen mit dem Verbindungs-Manager-Profil installiert werden, zum Beispiel Organisationsdaten, Support- oder Problembehandlungstools.
- Sie müssen festlegen, wie Sie das Verbindungs-Manager-Profil an Ihre Benutzer verteilen. Weitere Informationen finden Sie im Abschnitt »Verteilen von Verbindungs-Manager-Profilen« weiter unten in diesem Kapitel.

Anforderungen an Verbindungs-Manager-Profile

- Falls Sie eine Mischung von VPN-Clients haben, die unter Windows Vista, Windows Server 2008, Windows Server 2003 und/oder Windows XP laufen, müssen Sie unterschiedliche Verbindungs-Manager-Profile erstellen: eines für VPN-Clients, die unter Windows Vista oder Windows Server 2008 laufen, und eines für VPN-Clients, die unter Windows Server 2003 oder Windows XP laufen.

PKI

Um eine zertifikatbasierte Authentifizierung für L2TP-Verbindungen und eine Smartcard- oder benutzerzertifikatbasierte Authentifizierung für VPN-Verbindungen über PEAP-TLS oder EAP-TLS durchführen zu können, muss eine PKI (Public Key Infrastructure) vorhanden sein. Die PKI stellt die Zertifikate für VPN-Clients, VPN-Server und RADIUS-Server aus. Während des Authentifizierungsprozesses werden die Zertifikate übergeben, sodass die Gegenstelle das Zertifikat überprüfen kann.

Bei PEAP-MS-CHAP v2-Authentifizierung und SSTP-VPN-Verbindungen ist keine PKI nötig. Sie können Zertifikate von einer öffentlichen Zertifizierungsstelle kaufen und auf Ihrem Authentifizierungsserver (für PEAP-MS-CHAP v2) oder VPN-Server (für SSTP) installieren. Unter Umständen müssen Sie die Zertifikate der Stammzertifizierungsstelle und Zwischenzertifizierungsstelle, die Ihre Computerzertifikate ausgestellt haben, auf Ihre VPN-Clientcomputer verteilen.

Computerzertifikate für L2TP/IPsec-Verbindungen

Wenn Sie für L2TP/IPsec-Verbindungen die Zertifikatauthentifizierung einsetzen, können Sie die Liste der Zertifizierungsstellen (Certification Authority, CA) nicht konfigurieren. Stattdessen sendet jeder IPsec-Peer eine Liste der Stammzertifizierungsstellen, deren Zertifikat er für die Authentifizierung akzeptiert. Die Stammzertifizierungsstellen in dieser Liste entsprechen den Stammzertifizierungsstellen, die Computerzertifikate für den Computer ausgestellt haben. Falls zum Beispiel Computer A Computerzertifikate von den Stammzertifizierungsstellen CertAuth1 und CertAuth2 ausgestellt bekommen hat, meldet er seinem IPsec-Peer, dass er für die Authentifizierung nur Zertifikate von CertAuth1 und CertAuth2 akzeptiert. Falls der IPsec-Peer, Computer B, kein gültiges Computerzertifikat besitzt, das entweder von CertAuth1 oder von CertAuth2 ausgestellt wurde, schlägt die IPsec-Ausbehandlung fehl.

Auf dem VPN-Client muss ein gültiges Computerzertifikat installiert sein, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der VPN-Server vertraut. Außerdem muss der VPN-Server ein gültiges Computerzertifikat installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der VPN-Client vertraut.

Falls zum Beispiel der VPN-Client Computerzertifikate von den Stammzertifizierungsstellen CertAuth1 und CertAuth2 ausgestellt bekommen hat, meldet er dem VPN-Server während der IPsec-Sicherheitsaushandlung, dass er für die Authentifizierung nur Zertifikate von CertAuth1 und CertAuth2 akzeptiert. Falls der VPN-Server kein gültiges Computerzertifikat hat, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer Zertifikatkette liegt, die entweder zu CertAuth1 oder zu CertAuth2 zurückführt, schlägt die IPsec-Aushandlung fehl.

Eine Organisation hat üblicherweise eine einzige Stammzertifizierungsstelle und mindestens eine ausstellende Zertifizierungsstelle, die unterhalb der Stammzertifizierungsstelle Computerzertifikate ausstellt. Deswegen haben alle Computer innerhalb der Organisation einerseits Computerzertifikate von einer ausstellenden Zertifizierungsstelle der einzigen Stammzertifizierungsstelle *und* fordern für die Authentifizierung Zertifikate von ausstellenden Zertifizierungsstellen derselben Stammzertifizierungsstelle an.

Gehen Sie folgendermaßen vor, um Computerzertifikate für L2TP/IPsec-Verbindungen in Ihrer Organisation bereitzustellen:

1. Stellen Sie eine PKI bereit.
2. Installieren Sie auf jedem Computer ein Computerzertifikat. Das lässt sich am einfachsten mit Windows Active Directory-Zertifikatdiensten durchführen oder indem Zertifikatdienste als Unternehmenszertifizierungsstelle installiert und Gruppenrichtlinieneinstellungen für die automatische Registrierung von Computerzertifikaten konfiguriert werden. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von Zertifikaten« weiter unten in diesem Kapitel.

PKI für Smartcards

Der Einsatz von Smartcards bietet die sicherste Form der Benutzerauthentifizierung in Windows Server 2008. Für Remotezugriff-VPN-Verbindungen können Sie Smartcards mit den Authentifizierungsmethoden EAP-TLS oder PEAP-TLS nutzen.

Die einzelnen Smartcards werden an Benutzer verteilt, deren Computer ein Smartcardlesegerät besitzen. Um sich an seinem Computer anzumelden, muss der Benutzer die Smartcard in das Lesegerät einschieben und die zugehörige Geheimzahl (Personal Identification Number, PIN) eingeben. Wenn der Benutzer versucht, eine VPN-Verbindung herzustellen, wird das Smartcardzertifikat während des Verbindungsaushandlungsprozesses gesendet.

Folgende Voraussetzungen müssen erfüllt sein, damit Sie auf dem VPN-Client EAP-TLS von Hand für Smartcards konfigurieren können:

- Die VPN-Verbindung muss so konfiguriert sein, dass sie EAP mit dem EAP-Typ *Smartcard- oder anderes Zertifikat* benutzt. Wählen Sie dazu im Eigenschaftendialogfeld für den EAP-Typ *Smartcard- oder anderes Zertifikat* die Option *Eigene Smartcard verwenden*.
- Falls Sie bei VPN-Clients, die unter Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP SP2 oder Windows XP SP1 laufen, das Computerzertifikat des Authentifizierungsservers überprüfen wollen, müssen Sie das Kontrollkästchen *Serverzertifikat überprüfen* aktivieren (dies ist auch die Standardeinstellung). Sie können die Namen der Authentifizierungsserver konfigurieren, indem Sie das Kontrollkästchen *Verbindung mit diesen Servern herstellen* aktivieren und dann die Servernamen eingeben. Sie können fordern, dass das Computerzertifikat eines Servers von bestimmten vertrauenswürdigen Stammzertifizierungsstellen ausgestellt wurde, indem Sie im Abschnitt *Vertrauenswürdige Stammzertifizierungsstellen* die gewünschten Zertifizierungsstellen auswählen.

Eine Anleitung, wie Sie das Verbindungs-Manager-Verwaltungskit so konfigurieren, dass EAP-TLS Smartcards benutzt, finden Sie im Abschnitt »Konfigurieren und Bereitstellen von Verbindungs-Manager-Profilen mit dem Verbindungs-Manager-Verwaltungskit« weiter unten in diesem Kapitel.

In der Standardeinstellung ist EAP als Authentifizierungstyp aktiviert. Ist das nicht der Fall, können Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des VPN-Servers öffnen und auf der Registerkarte *Sicherheit* die Schaltfläche *Authentifizierungsmethoden* anklicken, um das gleichnamige Dialogfeld zu öffnen. Dort können Sie EAP aktivieren.

Sie können EAP-TLS-Authentifizierung in der NPS-Netzwerkrichtlinie für Remotezugriff-VPN-Verbindungen konfigurieren, indem Sie im Eigenschaftendialogfeld der Netzwerkrichtlinie sicherstellen, dass EAP aktiviert ist. Wählen Sie auf der Registerkarte *Einschränkungen* unter *Einschränkungen* den Punkt *Authentifizierungsmethoden* aus und fügen Sie den Eintrag *Smartcard- oder anderes Zertifikat* zur Liste *EAP-Typen* hinzu. Falls auf dem Authentifizierungsserver mehrere Computerzertifikate installiert sind, können Sie die Eigenschaften des EAP-Typs *Smartcard- oder anderes Zertifikat* konfigurieren und dann auswählen, welches Computerzertifikat während der EAP-TLS-Authentifizierung übergeben werden soll.

PKI für Benutzerzertifikate

Benutzerzertifikate werden für die Benutzerauthentifizierung in der Windows-Registrierung gespeichert. Sie können anstelle von Smartcards verwendet werden. Dies ist aber keine so sichere Form der Authentifizierung. Werden Smartcards eingesetzt, wird das Benutzerzertifikat, das während des Authentifizierungsprozesses ausgestellt wurde, nur zugänglich gemacht, wenn der Benutzer die Smartcard hat und die PIN weiß, sodass er sich am Computer anmelden kann. Werden Benutzerzertifikate eingesetzt, wird dagegen das Benutzerzertifikat, das während des Authentifizierungsprozesses ausgestellt wurde, nur zugänglich gemacht, wenn sich der Benutzer mit einem Domänenbenutzernamen und dem zugehörigen Kennwort am Computer anmeldet.

Werden Benutzerzertifikate für Remotezugriff-VPN-Verbindungen verwendet, arbeitet die Authentifizierung wie bei der Verwendung von Smartcards mit den Authentifizierungsmethoden EAP-TLS oder PEAP-TLS.

Gehen Sie folgendermaßen vor, um Benutzerzertifikate in Ihrer Organisation bereitzustellen:

1. Stellen Sie eine PKI bereit.
2. Installieren Sie für jeden Benutzer ein Benutzerzertifikat. Das lässt sich am einfachsten durchführen, indem Zertifikatdienste als Unternehmenszertifizierungsstelle installiert und Gruppenrichtlinieneinstellungen für die automatische Registrierung von Benutzerzertifikaten konfiguriert werden. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von Zertifikaten« weiter unten in diesem Kapitel.

Wenn der Benutzer versucht, eine VPN-Verbindung aufzubauen, sendet der VPN-Clientcomputer während des Authentifizierungsprozesses das Benutzerzertifikat.

Anforderungen an die PKI

- Für L2TP/IPsec-Remotezugriff-VPN-Verbindungen, die eine Computerzertifikatsauthentifizierung für IPsec durchführen, müssen Sie auf allen VPN-Clients und VPN-Servern Computerzertifikate installieren.

Das Computerzertifikat des VPN-Clients muss gültig sein, und der VPN-Server muss es überprüfen können. Der VPN-Server muss ein Stammzertifizierungsstellenzertifikat für die Zertifizierungsstelle haben, die das Computerzertifikat des VPN-Clients ausgestellt hat.

Das Computerzertifikat des VPN-Servers muss gültig sein, und der VPN-Client muss es überprüfen können. Der VPN-Client muss ein Stammzertifizierungsstellenzertifikat für die Zertifizierungsstelle haben, die das Computerzertifikat des VPN-Servers ausgestellt hat.

- Um VPN-Verbindungen mithilfe eines Smartcard- oder Benutzerzertifikats bei Verwendung von EAP-TLS oder PEAP-TLS authentifizieren zu können, muss der VPN-Client ein Benutzerzertifikat auf Smartcard oder in der Registrierung installiert haben. Der Authentifizierungsserver muss ein Computerzertifikat installiert haben.

Das Smartcard- oder Benutzerzertifikat des VPN-Clients muss gültig sein, und der Authentifizierungsserver muss es überprüfen können. Der Authentifizierungsserver muss das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle haben, die das Zertifikat des VPN-Clients ausgestellt hat.

Der VPN-Client muss das Computerzertifikat des Authentifizierungsservers überprüfen können. Der VPN-Client muss das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle haben, die das Computerzertifikat des Authentifizierungsservers ausgestellt hat.

- Um VPN-Verbindungen mit PEAP-TLS authentifizieren zu können, muss der Authentifizierungsserver ein Computerzertifikat installiert haben.

Der VPN-Client muss das Computerzertifikat des Authentifizierungsservers überprüfen können. Der VPN-Client muss das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle haben, die das Computerzertifikat des Authentifizierungsservers ausgestellt hat.

- Für SSTP-VPN-Verbindungen müssen Sie ein Computerzertifikat auf dem VPN-Server installieren.

Das Computerzertifikat des VPN-Servers muss gültig sein, und der VPN-Client muss es überprüfen können. Der VPN-Client muss das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle haben, die das Computerzertifikat des VPN-Servers ausgestellt hat.

Empfohlene Vorgehensweise für die PKI

- Falls Sie eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle einsetzen und Computerzertifikate für L2TP/IPsec brauchen, sollten Sie Ihre Active Directory-Domäne über Gruppenrichtlinien im Zweig *Computerkonfiguration* so konfigurieren, dass die Computerzertifikate automatisch registriert werden. Jeder Computer, der Mitglied der Domäne ist, fordert automatisch ein Computerzertifikat an, wenn er die entsprechenden Gruppenrichtlinien aktualisiert.
- Falls Sie eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle einsetzen und Benutzerzertifikate für EAP-TLS oder PEAP-TLS in der Registrierung speichern wollen, sollten Sie Ihre Active Directory-Domäne über Gruppenrichtlinien im Zweig *Benutzerkonfiguration* so konfigurieren, dass die Benutzerzertifikate automatisch registriert werden. Jeder Benutzer, der sich erfolgreich an der Domäne angemeldet hat, fordert automatisch ein Benutzerzertifikat an, wenn die entsprechenden Gruppenrichtlinien aktualisiert werden.

VPN-Erzwingung mit NAP

Netzwerkzugriffsschutz (Network Access Protection, NAP) für Windows Server 2008, Windows Vista und Windows XP mit Service Pack 3 stellt Komponenten und einen Satz Programmierschnittstellen (Application Programming Interface, API) zur Verfügung, mit denen Sie erzwingen können, dass bei Netzwerkzugriff oder Kommunikation bestimmte Integritätsrichtlinien erfüllt werden. Entwickler und Netzwerkadministratoren können Lösungen erstellen, mit denen Computer, die auf das Netzwerk

zugreifen wollen, überprüft werden. Den Computern können benötigte Updates oder Zugriff auf erforderliche Ressourcen zur Verfügung gestellt werden, und der Zugriff für Computer, die die Anforderungen nicht erfüllen, kann eingeschränkt werden.

VPN-Erzwingung ist eine der NAP-Erzwingungsmethoden, die in Windows Server 2008, Windows Vista und Windows XP mit Service Pack 3 enthalten sind. Bei der VPN-Erzwingung muss ein VPN-Remotezugriffsklient beweisen, dass er die Integritätsanforderungen erfüllt, bevor er vollständigen Zugriff auf das Intranet bekommt. Falls der VPN-Client die Integritätsanforderungen nicht erfüllt, ordnet der VPN-Server diesen VPN-Client einem eingeschränkten Netzwerk zu. In diesem eingeschränkten Netzwerk stehen Server zur Verfügung, mit deren Ressourcen sich der VPN-Client aktualisieren kann, sodass er die Anforderungen erfüllt. Der VPN-Server erzwingt auch den eingeschränkten Zugriff über IP-Paketfilter, die auf die VPN-Verbindung angewendet werden. Sobald der VPN-Client seinen Integritätsstatus korrigiert hat, überprüft er seinen Integritätsstatus neu. Falls er diesmal die Anforderungen erfüllt, werden die IP-Paketfilter, die den Zugriff auf das eingeschränkte Netzwerk begrenzen, von der VPN-Verbindung entfernt.

Damit die VPN-Erzwingung funktioniert, müssen Sie bereits eine funktionierende VPN-Bereitstellung mit Windows Server 2008-VPN-Servern zur Verfügung haben, bei der eine PEAP-Authentifizierungsmethode eingesetzt wird. Wie Sie die VPN-Erzwingung bereitstellen, nachdem Sie eine Remotezugriff-VPN-Lösung erfolgreich bereitgestellt haben, erfahren Sie in Kapitel 18, »VPN-Erzwingung«.

Zusätzliche Sicherheitsaspekte

Wenn Sie eine Remotezugriff-VPN-Lösung bereitstellen, müssen Sie folgende zusätzliche Sicherheitsaspekte beachten:

- Starke Verschlüsselung der Verbindung
- Paketfilterung auf dem VPN-Server
- Firewallpaketfilterung für VPN-Verkehr
- VPN-Server mit mehreren Aufgaben
- Verhindern, dass Verkehr von VPN-Clients weitergeleitet wird
- Gleichzeitiger Zugriff
- Unbenutzte VPN-Protokolle

Starke Verschlüsselung der Verbindung

Im Bezug auf die Verschlüsselung können Sie Verbindungsverschlüsselung oder die Kombination aus Endpunkt-zu-Endpunkt-Verschlüsselung und Verbindungsverschlüsselung nutzen:

- *Verbindungsverschlüsselung* (engl. link encryption) verschlüsselt die Daten ausschließlich auf der Verbindung durch das Internet zwischen dem VPN-Client und dem VPN-Server. Bei PPTP-Verbindungen müssen Sie MPPE in Kombination mit MS-CHAP v2-, PEAP-MS-CHAP v2-, EAP-TLS- oder PEAP-TLS-Authentifizierung verwenden. Für L2TP/IPsec-Verbindungen stellt IPsec die Verschlüsselung zur Verfügung. Für SSTP-Verbindungen stellt SSL die Verschlüsselung bereit.
- *Endpunkt-zu-Endpunkt-Verschlüsselung* (engl. end-to-end encryption) verschlüsselt die Daten zwischen dem Quellhost und seinem Ziel. Nachdem die VPN-Verbindung aufgebaut ist, können Sie die Daten zwischen dem VPN-Client im Internet und dem Knoten im Intranet mit IPsec verschlüsseln. Weitere Informationen über IPsec und Endpunkt-zu-Endpunkt-Schutz von IP-Verkehr finden Sie in Kapitel 4, »Windows-Firewall mit erweiterter Sicherheit«.

Sie können den VPN-Server so konfigurieren, dass er Verbindungsverschlüsselung verpflichtend macht, indem Sie die gewünschten Verschlüsselungsstärken in den Verschlüsselungseinstellungen der Netzwerkrichtlinie wählen, die für Remotezugriff-VPN-Verbindungen verwendet wird. Aktivieren Sie auf keinen Fall das Kontrollkästchen *Keine Verschlüsselung*.

Paketfilterung für VPN-Verkehr auf dem VPN-Server

Um sicherzustellen, dass der VPN-Server außer dem VPN-Verkehr keinerlei Verkehr auf seiner Internetschnittstelle sendet oder empfängt (sofern der VPN-Server keine anderen Dienste hostet, die aus dem Internet erreichbar sind), müssen Sie sicherstellen, dass für die Internetschnittstelle des VPN-Servers ein- und ausgehende IPv4- und IPv6-Paketfilter für PPTP-, L2TP/IPsec- und SSTP-Verkehr konfiguriert sind. Weil ein VPN-Server ein IPv4- und IPv6-Router ist, leitet der VPN-Server unter Umständen unerwünschten Internetverkehr in Ihr Intranet weiter, wenn keine Filter für den VPN-Verkehr auf der Internetschnittstelle konfiguriert sind. Diese Filter werden automatisch hinzugefügt, wenn Sie den Setup-Assistenten für den Routing- und RAS-Server ausführen und dabei die Optionen verwenden, die im Abschnitt »Bereitstellen von VPN-Servern« weiter unten in diesem Kapitel beschrieben werden.

Firewallpaketfilterung für VPN-Verkehr

Es ist allgemein üblich, Intranethosts (zum Beispiel einen VPN-Server) mit einer Firewall vor Internethosts zu schützen. Falls Sie eine Firewall haben, müssen Sie dafür Paketfilter konfigurieren, die Verkehr zu und von VPN-Clients im Internet und dem VPN-Server zulassen.

Firewalls werden für einen VPN-Server meist folgendermaßen implementiert:

- Der VPN-Server ist direkt an das Internet angeschlossen, und die Firewall liegt zwischen dem VPN-Server und dem Intranet.
- Die Firewall ist direkt an das Internet angeschlossen, und der VPN-Server liegt zwischen der Firewall und dem Intranet.
- Es werden zwei Firewalls benutzt: eine zwischen dem VPN-Server und dem Intranet, die zweite zwischen dem VPN-Server und dem Internet.

VPN-Server vor der Firewall

Um sicherzustellen, dass der VPN-Server keinerlei Verkehr außer VPN-Verkehr über seine Internetschnittstelle sendet oder empfängt, müssen Sie ein- und ausgehende PPTP-, L2TP/IPsec- und SSTP-Filter auf der Schnittstelle konfigurieren, die die Verbindung ins Internet bildet. Weil der Setup-Assistent für den Routing- und RAS-Server für die Internetschnittstelle standardmäßig IPv4- und IPv6-Routing aktiviert, wird Verkehr, der über die Internetschnittstelle empfangen wird, weitergeleitet, falls keine VPN-Paketfilter für diese Internetschnittstelle konfiguriert werden.

Wenn der VPN-Server vor der Firewall an das Internet angeschlossen ist, müssen Sie Paketfilter zur Internetschnittstelle hinzufügen, die ausschließlich VPN-Verkehr zu und von der IPv4- oder IPv6-Adresse der Internetschnittstelle des VPN-Servers zulassen.

Bei eingehendem Verkehr entschlüsselt der VPN-Server die getunnelten Daten und leitet sie an die Firewall weiter. Die Firewall agiert in dieser Konfiguration als Filter für Intranetverkehr. Sie kann verhindern, dass auf bestimmte Ressourcen zugegriffen wird. Außerdem kann sie zum Beispiel Daten nach Viren durchsuchen und Intrusion-Detection-Funktionen übernehmen. Abbildung 12.2 zeigt den Aufbau, wenn der VPN-Server vor der Firewall liegt.

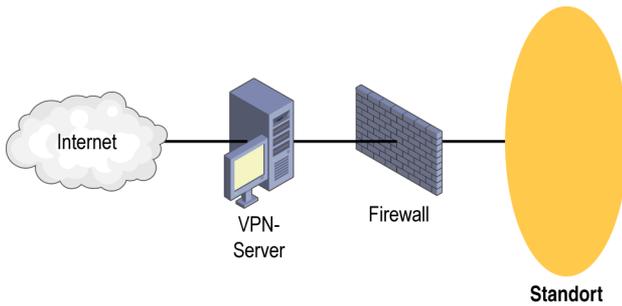


Abbildung 12.2 Der VPN-Server liegt vor der Firewall

Die Firewall ist mit geeigneten Regeln für Intranetverkehr zu und von VPN-Clients konfiguriert. Diese Regeln entsprechen Ihren Netzwerksicherheitsrichtlinien.

Für die Internetschnittstelle auf dem VPN-Server können Sie die eingehenden und ausgehenden Filter für IPv4- und IPv6-VPN-Verkehr im Snap-In *Routing und RAS* konfigurieren. Diese Filter werden automatisch konfiguriert, wenn Sie den Setup-Assistenten für den Routing- und RAS-Server ausführen und dabei die Konfigurationsoption *Remotezugriff (DFÜ oder VPN)* wählen, den Typ *VPN-RAS* verwenden, die richtige Internetschnittstelle einstellen und auf der Seite *VPN-Verbindung* das Kontrollkästchen *Sicherheit auf der ausgewählten Schnittstelle durch Einrichten statischer Paketfilter aktivieren* aktiviert lassen (das ist die Standardeinstellung). Außerdem fügt der Setup-Assistent für den Routing- und RAS-Server automatisch dieselben Ports in der Windows-Firewall hinzu und aktiviert sie.

Die folgenden Abschnitte beschreiben diese Filter genauer, für den Fall, dass Sie sie von Hand konfigurieren müssen.

Filter für PPTP-Verkehr

Bei folgenden IPv4-Eingabefiltern (auch als *eingehende Filter* bezeichnet) für PPTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Zielport 1723

Dieser Filter erlaubt PPTP-Tunnelverwaltungsverkehr zum VPN-Server.

- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokoll-ID 47

Dieser Filter erlaubt PPTP-getunnelte Daten zum VPN-Server.

- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und Quellport 1723 vom Typ *TCP [eingrichtet]*

Dieser Filter ist nur nötig, wenn der VPN-Server der anrufende Router in einer Standort-zu-Standort-VPN-Verbindung (auch als Router-zu-Router-Verbindung bezeichnet) ist. Verkehr vom Typ *TCP [eingrichtet]* wird nur angenommen, wenn der VPN-Server die TCP-Verbindung aufgebaut hat.

Bei den folgenden IPv4-Ausgabefiltern (auch als *ausgehende Filter* bezeichnet) für PPTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Quellport 1723
Dieser Filter erlaubt PPTP-Tunnelverwaltungsverkehr vom VPN-Server.
- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokoll-ID 47
Dieser Filter erlaubt PPTP-getunnelte Daten vom VPN-Server.
- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und Zielport 1723 vom Typ *TCP [eingerichtet]*
Dieser Filter ist nur nötig, wenn der VPN-Server der VPN-Client (anrufende Router) in einer Standort-zu-Standort-VPN-Verbindung ist. Verkehr vom Typ *TCP [eingerichtet]* wird nur gesendet, wenn der VPN-Server die TCP-Verbindung aufgebaut hat.

Bei folgenden IPv6-Eingabefiltern für PPTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und TCP-Zielport 1723
- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und IP-Protokoll-ID 47
- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und Quellport 1723 vom Typ *TCP [eingerichtet]*

Bei den folgenden IPv6-Ausgabefiltern für PPTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und TCP-Quellport 1723
- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und IP-Protokoll-ID 47
- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und Zielport 1723 vom Typ *TCP [eingerichtet]*

Filter für L2TP/IPsec-Verkehr

Bei folgenden IPv4-Eingabefiltern für L2TP/IPsec-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 500
Dieser Filter erlaubt IKE-Verkehr (Internet Key Exchange) zum VPN-Server.
- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 4500
Dieser Filter erlaubt IPsec-NAT-T-Verkehr zum VPN-Server.
- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 1701
Dieser Filter erlaubt L2TP-Verkehr zum VPN-Server.

Bei den folgenden IPv4-Ausgabefiltern für L2TP/IPSec-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 500

Dieser Filter erlaubt IKE-Verkehr vom VPN-Server.

- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 4500.

Dieser Filter erlaubt IPsec-NAT-T-Verkehr vom VPN-Server.

- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 1701

Dieser Filter erlaubt L2TP-Verkehr vom VPN-Server.

Für IPsec-ESP-Verkehr (Encapsulating Security Protocol) mit der IP-Protokollnummer 50 sind keine Filter nötig. Die Filter des Routing- und RAS-Dienstes werden angewendet, nachdem die IPsec-Komponenten den ESP-Header entfernt haben.

Bei folgenden IPv6-Eingabefiltern für L2TP/IPSec-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und UDP-Zielport 500
- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und UDP-Zielport 4500
- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und UDP-Zielport 1701

Bei den folgenden IPv6-Ausgabefiltern für L2TP/IPSec-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und UDP-Quellport 500
- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und UDP-Quellport 4500
- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und UDP-Quellport 1701

Filter für SSTP-Verkehr

Beim folgenden IPv4-Eingabefilter für SSTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Ziel-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Zielport 443

Dieser Filter erlaubt SSTP-Verkehr zum VPN-Server.

Beim folgenden IPv4-Ausgabefilter für SSTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Quell-IPv4-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Quellport 443

Dieser Filter erlaubt SSTP-Verkehr vom VPN-Server.

Beim folgenden IPv6-Eingabefilter für SSTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Ziel-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und TCP-Zielport 443

Beim folgenden IPv6-Ausgabefilter für SSTP-Verkehr ist als Filteraktion die Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* ausgewählt:

- Quell-IPv6-Adresse der Internetschnittstelle des VPN-Servers, Präfixlänge 128 und TCP-Quellport 443

VPN-Server hinter der Firewall

Weiter verbreitet ist die Konfiguration, dass die Firewall mit dem Internet verbunden ist und der VPN-Server eine Intranetressource ist, die an das Grenznetzwerk (auch als Umkreisnetzwerk, engl. perimeter network oder screened subnet bezeichnet) angeschlossen ist. Das Grenznetzwerk ist ein Subnetz, dessen Ressourcen Internetbenutzern zur Verfügung gestellt werden. Das können zum Beispiel Web- und FTP-Server sein. Der VPN-Server hat jeweils eine Schnittstelle zum Grenznetzwerk und zum Intranet. Bei diesem Ansatz muss die Firewall auf ihrer Internetschnittstelle mit ein- und ausgehenden Filtern konfiguriert werden, die Tunnelverwaltungsverkehr und getunnelte Daten zum VPN-Server durchlassen. Zusätzliche Filter können Verkehr zu Web-, FTP- und anderen Servern im Grenznetzwerk zulassen. Damit eine weitere Sicherheitsschicht zur Verfügung steht, sollte auch der VPN-Server auf seiner Grenznetzwerkschnittstelle mit Paketfiltern für VPN-Verkehr konfiguriert werden.

Die Firewall agiert in dieser Konfiguration als Filter für Internetverkehr. Sie kann ein- und ausgehenden Verkehr auf bestimmte Ressourcen im Grenznetzwerk einschränken, Intrusion-Detection-Funktionen übernehmen, Denial-of-Service-Angriffe verhindern und andere Aufgaben durchführen.

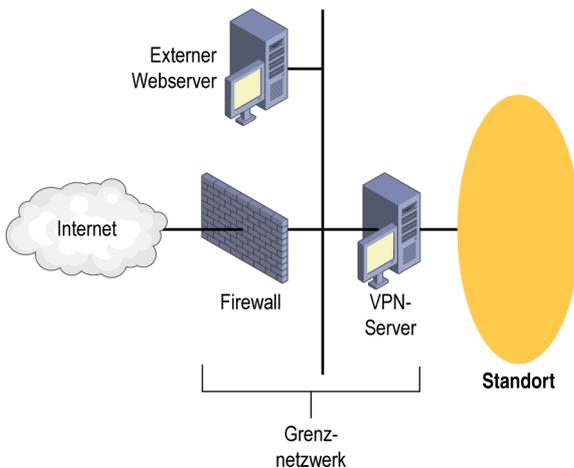


Abbildung 12.3 Der VPN-Server liegt hinter der Firewall im Grenznetzwerk

Weil die Firewall nicht für jede VPN-Verbindung den entsprechenden Verschlüsselungsschlüssel besitzt, kann sie Filter nur auf Basis der Klartextheader von getunnelten Daten anwenden. Anders ausgedrückt: Alle getunnelten Daten werden durch die Firewall gelassen. Das ist aber keine Sicherheitslücke, weil die VPN-Verbindung einen Authentifizierungsprozess erfordert, der unautorisierten Zugriff hinter dem VPN-Server verhindert. Abbildung 12.3 zeigt den Aufbau, bei dem der VPN-Server hinter der Firewall im Grenznetzwerk liegt.

Konfigurieren Sie auf der Firewall für die Internet- und Grenznetzwerkschnittstellen ein- und ausgehende Filter für VPN-Verkehr. Dafür können Sie die Konfigurationssoftware der Firewall verwenden. Für Internetschnittstelle und Grenznetzwerkschnittstelle können getrennte eingehende ausgehende Paketfilter konfiguriert werden.

Die Tabellen 12.1 und 12.2 fassen die Paketfilter zusammen, die auf den Internet- und Grenznetzwerkschnittstellen der Firewall konfiguriert sein sollten.

Tabelle 12.1 Paketfilter der Internetschnittstelle

Filtertyp	IP-Version	VPN-Protokoll	Verkehr
Eingabe	IPv4	PPTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB)
Eingabe	IPv4	PPTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F)
Eingabe	IPv4	PPTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)*
Eingabe	IPv4	L2TP/IPsec	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 500 (0x1F4)
Eingabe	IPv4	L2TP/IPsec	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 4500 (0x1194)
Eingabe	IPv4	L2TP/IPsec	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Eingabe	IPv6	L2TP/IPsec	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 500 (0x1F4)
Eingabe	IPv6	L2TP/IPsec	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 4500 (0x1194)
Eingabe	IPv6	L2TP/IPsec	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Eingabe	IPv4	SSTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 443 (0x1BB)
Eingabe	IPv6	SSTP	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 443 (0x1BB)
Ausgabe	IPv4	PPTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)
Ausgabe	IPv4	PPTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F)
Ausgabe	IPv4	PPTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)*
Ausgabe	IPv4	L2TP/IPsec	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 500 (0x1F4)
Ausgabe	IPv4	L2TP/IPsec	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 4500 (0x1194)
Ausgabe	IPv4	L2TP/IPsec	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Ausgabe	IPv6	L2TP/IPsec	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 500 (0x1F4) ▶

Filtertyp	IP-Version	VPN-Protokoll	Verkehr
Ausgabe	IPv6	L2TP/IPsec	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 4500 (0x1194)
Ausgabe	IPv6	L2TP/IPsec	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Ausgabe	IPv4	SSTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 443 (0x1BB)
Ausgabe	IPv6	SSTP	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 443 (0x1BB)

* Diese Filter sind nur nötig, wenn der VPN-Server der anrufende Router in einer Standort-zu-Standort-VPN-Verbindung ist. Die Filter sollten nur in Kombination mit den PPTP-Paketfiltern verwendet werden, die in »VPN-Server vor der Firewall« weiter oben in diesem Kapitel beschrieben sind. Sie werden für die Grenznetzwerkschnittstelle des VPN-Servers konfiguriert. Da der gesamte Verkehr zugelassen wird, der an TCP-Port 1723 des VPN-Servers fließt, besteht die Möglichkeit, dass dieser Port für Netzwerkangriffe aus dem Internet missbraucht wird.

Tabelle 12.2 Paketfilter der Grenznetzwerkschnittstelle

Filtertyp	IP-Version	VPN-Protokoll	Verkehr
Eingabe	IPv4	PPTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)
Eingabe	IPv4	PPTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F)
Eingabe	IPv4	PPTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)*
Eingabe	IPv6	PPTP	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)
Eingabe	IPv6	PPTP	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F)
Eingabe	IPv6	PPTP	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB)*
Eingabe	IPv4	L2TP/IPsec	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 500 (0x1F4)
Eingabe	IPv4	L2TP/IPsec	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 4500 (0x1194)
Eingabe	IPv4	L2TP/IPsec	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Eingabe	IPv6	L2TP/IPsec	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 500 (0x1F4)
Eingabe	IPv6	L2TP/IPsec	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Quellport 4500 (0x1194)
Eingabe	IPv6	L2TP/IPsec	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Eingabe	IPv4	SSTP	Quell-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 443 (0x1BB)
Eingabe	IPv6	SSTP	Quell-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Quellport 443 (0x1BB) ▶

Filtertyp	IP-Version	VPN-Protokoll	Verkehr
Ausgabe	IPv4	PPTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB)
Ausgabe	IPv4	PPTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F)
Ausgabe	IPv4	PPTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB)*
Ausgabe	IPv6	PPTP	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB)
Ausgabe	IPv6	PPTP	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F)
Ausgabe	IPv6	PPTP	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB)*
Ausgabe	IPv4	L2TP/IPsec	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 500 (0x1F4)
Ausgabe	IPv4	L2TP/IPsec	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 4500 (0x1194)
Ausgabe	IPv4	L2TP/IPsec	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Ausgabe	IPv6	L2TP/IPsec	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 500 (0x1F4)
Ausgabe	IPv6	L2TP/IPsec	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und UDP-Zielport 4500 (0x1194)
Ausgabe	IPv6	L2TP/IPsec	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32)
Ausgabe	IPv4	SSTP	Ziel-IPv4-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 443 (0x1BB)
Ausgabe	IPv6	SSTP	Ziel-IPv6-Adresse der Grenznetzwerkschnittstelle des VPN-Servers und TCP-Zielport 443 (0x1BB)

* Diese Filter sind nur nötig, wenn der VPN-Server der anrufende Router in einer Standort-zu-Standort-VPN-Verbindung ist. Die Filter sollten nur in Kombination mit den PPTP-Paketfiltern verwendet werden, die in »VPN-Server vor der Firewall« weiter oben in diesem Kapitel beschrieben sind. Sie werden für die Grenznetzwerkschnittstelle des VPN-Servers konfiguriert. Da der gesamte Verkehr zugelassen wird, der an TCP-Port 1723 des VPN-Servers fließt, besteht die Möglichkeit, dass dieser Port für Netzwerkangriffe aus dem Internet missbraucht wird.

Für L2TP-Verkehr über den UDP-Port 1701 werden keine Filter benötigt. Jeglicher L2TP-Verkehr, der bei der Firewall ankommt, also auch Tunnelverwaltungsverkehr und getunnelte Daten, sind als IPsec-ESP-Nutzdaten verschlüsselt.

Es gibt keine IPv6-Filter für PPTP-Verkehr, weil Routing und RAS keine Unterstützung für IPv6 über PPTP-Verbindungen bietet.

VPN-Server zwischen zwei Firewalls

Bei einer weiteren Konfiguration liegt der VPN-Servercomputer im Grenznetzwerk zwischen zwei Firewalls. Die Internetfirewall, also die Firewall zwischen dem Internet und dem VPN-Server, filtert den gesamten Internetverkehr von allen Internetclients. Die Intranetfirewall, also die Firewall zwischen dem VPN-Server und dem Intranet, filtert den Intranetverkehr von VPN-Clients. Abbildung 12.4 zeigt den Aufbau, bei dem der VPN-Server zwischen zwei Firewalls im Grenznetzwerk liegt.

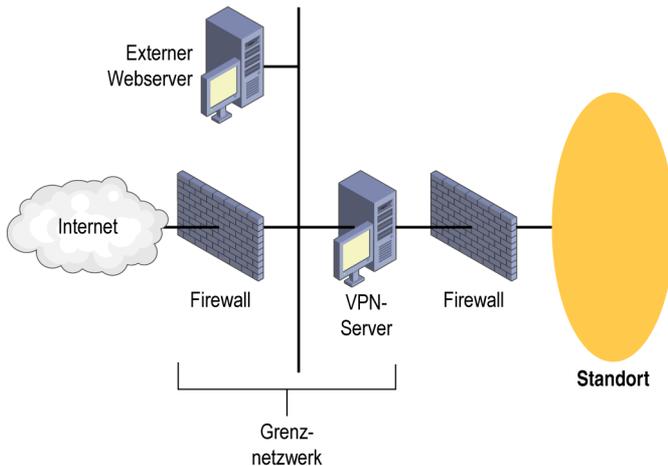


Abbildung 12.4 Der VPN-Server liegt zwischen zwei Firewalls im Grenznetzwerk

Bei diesem Ansatz sollten Sie folgende Konfiguration vornehmen:

- Konfigurieren Sie Ihre Internetfirewall und den VPN-Server mit den Paketfiltern, die im Abschnitt »VPN-Server hinter der Firewall« weiter oben in diesem Kapitel beschrieben sind.
- Konfigurieren Sie Ihre Intranetfirewall mit den geeigneten Regeln für Intranetverkehr zu und von VPN-Clients, wie durch Ihre Netzwerksicherheitsrichtlinien vorgegeben.

VPN-Server mit mehreren Aufgaben

Aufgrund der Routen, die auf VPN-Remotegriffclients automatisch erstellt werden, kann es passieren, dass ein VPN-Client unverschlüsselten Verkehr zum VPN-Server sendet, statt den verschlüsselten Tunnel der VPN-Verbindung zu benutzen. Zum Beispiel kann es sein, dass der VPN-Client eine Verbindung zu anderen Diensten herstellt, die auf dem VPN-Server laufen, ohne den Verkehr über die VPN-Verbindung zu senden. Nur Verkehr, der an die öffentliche IP-Adresse des VPN-Servers gerichtet ist, wird im Klartext gesendet. Falls Verkehr vom Client dagegen die IPv4-Adresse der internen Schnittstelle des VPN-Servers benutzt, wird er verschlüsselt.

Wenn ein Remotegriff-VPN-Client eine VPN-Verbindung mit einem VPN-Server aufbaut, erstellt er eine Reihe von Routen in der IPv4-Routingtabelle auf dem VPN-Client. Darunter sind folgende Routen:

- **Eine Standardroute, die die VPN-Verbindung benutzt** Die neue Standardroute für die VPN-Verbindung ersetzt praktisch die vorhandene Standardroute, solange die Verbindung besteht. Sobald die Verbindung hergestellt wurde, wird jeglicher Verkehr, der nicht an eine Adresse im direkt angeschlossenen Netzwerk oder an die Adresse des VPN-Servers gerichtet ist, verschlüsselt über die VPN-Verbindung gesendet.
- **Eine Hostroute zur Internet-IPv4-Adresse des VPN-Servers** Die Hostroute für die Adresse des VPN-Servers wird erstellt, damit der VPN-Server erreichbar ist. Fehlt diese Hostroute, kann kein VPN-Verkehr zum VPN-Server gesendet werden.

Da es die Hostroute zum VPN-Server gibt, wird jeglicher Verkehr, der an Anwendungen oder Dienste auf dem VPN-Server übertragen wird und an die Internet-IPv4-Adresse des VPN-Servers gerichtet ist, nicht über die VPN-Verbindung gesendet, sondern unverschlüsselt über das Internet.

Wenn zum Beispiel ein Remotezugriff-VPN-Client eine VPN-Verbindung mit einem VPN-Server herstellt und dann über die Internetadresse des VPN-Servers auf eine freigegebene Datei auf dem VPN-Servercomputer zugreift, wird dieser Verkehr nicht über die VPN-Verbindung gesendet. Der Dateifreigabeverkehr läuft im Klartext über das Internet.

Und falls auf dem VPN-Server Paketfilter konfiguriert sind, die ausschließlich VPN-Verbindungsverkehr über die Internetschnittstelle erlauben, wird jeglicher andere Verkehr, der an den VPN-Server gesendet wird, einfach verworfen. Alle Versuche, Kontakt mit Anwendungen oder Diensten aufzunehmen, die auf dem VPN-Server laufen, schlagen fehl, weil der Verkehr, mit dem der Zugriff auf diese Dienste erreicht werden soll, nicht über die VPN-Verbindung gesendet wird.

Welche IPv4-Adresse der VPN-Client verwendet, um auf Dienste des VPN-Servers zuzugreifen, hängt davon ab, wie der Name des VPN-Servers aufgelöst wird. Normalerweise geben Benutzer und Anwendungen Netzwerkressourcen anhand ihres Namens an, nicht über ihre IPv4-Adressen. Der Name muss sich entweder mit DNS oder WINS in eine IPv4-Adresse auflösen lassen. Falls die DNS- und WINS-Infrastrukturen des Intranets keinen Eintrag enthalten, der den Namen des VPN-Servers der öffentlichen IPv4-Adresse der Internetschnittstelle des VPN-Servers zuordnet, wird Verkehr, der an Dienste des VPN-Servers gerichtet ist, immer über die VPN-Verbindung gesendet.

Gehen Sie folgendermaßen vor, um zu verhindern, dass der VPN-Server die öffentliche IPv4-Adresse seiner Internetschnittstelle im Intranet-DNS registriert:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der Komponente *Internetprotokoll Version 4 (TCP/IPv4)* für die Internetverbindung.
2. Klicken Sie auf der Registerkarte *Allgemein* auf *Erweitert*.
3. Deaktivieren Sie im Dialogfeld *Erweiterte TCP/IP-Einstellungen* auf der Registerkarte *DNS* das Kontrollkästchen *Adressen dieser Verbindung in DNS registrieren* und klicken Sie dreimal auf *OK*.

Falls Sie in Ihrem Intranet NetBIOS über TCP/IP einsetzen, können Sie folgendermaßen verhindern, dass der VPN-Server die öffentliche IPv4-Adresse seiner Internetschnittstelle bei Intranet-WINS-Servern registriert:

1. Öffnen Sie im Ordner *Netzwerkverbindungen* das Eigenschaftendialogfeld der Komponente *Internetprotokoll Version 4 (TCP/IPv4)* für die Internetverbindung.
2. Klicken Sie auf der Registerkarte *Allgemein* auf *Erweitert*.
3. Wählen Sie im Dialogfeld *Erweiterte TCP/IP-Einstellungen* auf der Registerkarte *WINS* die Option *NetBIOS über TCP/IP deaktivieren* und klicken Sie dreimal auf *OK*.

Bevor die VPN-Verbindung hergestellt wird, löst der VPN-Client über die Internet-DNS-Infrastruktur den Namen des VPN-Servercomputers in seine öffentlichen IPv4-Adressen auf. Sobald die VPN-Verbindung hergestellt ist, verwendet der VPN-Client die DNS- und WINS-Infrastrukturen des Intranets, um den Namen des VPN-Servercomputers in seine Intranet IPv4-Adressen aufzulösen. Das gilt natürlich nur, wenn der VPN-Client entweder während des PPP-Verbindungsprozesses oder über die Weiterleitung der DHCPInform-Nachricht mit den DNS- und WINS-Servern im Intranet konfiguriert wurde.

Verhindern, dass Verkehr von VPN-Clients weitergeleitet wird

Sobald ein VPN-Client erfolgreich eine VPN-Verbindung aufgebaut hat, wird standardmäßig jedes Paket, das über die Verbindung gesendet wird, vom VPN-Server empfangen und weitergeleitet. Unter anderem können folgende Pakete über die Verbindung gesendet werden:

- Pakete, die vom VPN-Clientcomputer stammen
- Pakete, die der VPN-Clientcomputer weiterleitet, nachdem er sie von anderen Computern empfangen hat

Wenn der Clientcomputer die VPN-Verbindung aufbaut, erstellt er in der Standardeinstellung eine Standardroute, sodass jeglicher Verkehr, für den die Standardroute zuständig ist, über die VPN-Verbindung übertragen wird. Falls andere Computer Verkehr an den VPN-Client weiterleiten, den VPN-Clientcomputer also wie einen Router behandeln, wird auch dieser Verkehr über die VPN-Verbindung weitergeleitet. Das ist eine Sicherheitslücke, weil der VPN-Server den Computer, der seinen Verkehr an den VPN-Clientcomputer weiterleitet, nicht authentifiziert hat. Der Computer, der Verkehr über den VPN-Clientcomputer weiterleitet, hat dieselben Fähigkeiten, Pakete in das Intranet zu senden, wie der authentifizierte VPN-Clientcomputer.

Um zu verhindern, dass VPN-Server über die VPN-Verbindung Verkehr von anderen Computern als den authentifizierten VPN-Clientcomputern weiterleiten, sollten Sie in der Netzwerkrichtlinie für Ihre VPN-Verbindungen eingehende IPv4-Paketfilter konfigurieren, die jeglichen Verkehr verwerfen, der nicht von VPN-Clients stammt. Die Standardnetzwerkrichtlinie (mit dem Namen *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver*) enthält einen einzelnen IPv4-Eingabefilter mit der Filteraktion *Nur die unten aufgeführten Pakete zulassen* und den Einstellungen aus Tabelle 12.3.

Tabelle 12.3 Eingabefiltereinstellungen

Feld im IP-Paketfilter	Einstellung
Quelladresse	Benutzeradresse
Quellnetzwerkmaske	Benutzermaske
Zieladresse	Beliebig
Zielmaske	Beliebig
Protokoll	Beliebig



Hinweis Das Snap-In *Routing und RAS* zeigt zwar *Benutzeradresse* und *Benutzermaske* an, aber der tatsächliche Filter, der für jeden Remotezugriffsserver erstellt wird, gilt für die IPv4-Adresse, die dem Client zugewiesen wird, und die Subnetzmaske 255.255.255.255.

Mit diesem eingehenden IPv4-Paketfilter verwirft der VPN-Server jeglichen Verkehr, der über die VPN-Verbindung gesendet wird, sofern er nicht von den VPN-Clients selbst stammt.

Gleichzeitiger Zugriff

Wenn ein VPN-Clientcomputer gleichzeitig Zugriff auf das Internet und Ihr Intranet hat und Routen besitzt, die eine Erreichbarkeit beider Netzwerke sicherstellen, kann es sein, dass ein böswilliger Internetbenutzer den verbundenen VPN-Clientcomputer missbraucht, um das nichtöffentliche Intranet über die authentifizierte VPN-Verbindung zu erreichen. Das ist möglich, falls beim VPN-Clientcomputer IPv4-Routing aktiviert ist. IPv4-Routing können Sie auf Windows-Computern von Hand aktivieren, indem Sie den Registrierungswert `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter` (Datentyp `REG_DWORD`) auf 1 setzen.

Falls Ihre VPN-Clients gleichzeitigen Zugriff brauchen, können Sie unerwünschten Verkehr aus dem Internet folgendermaßen blockieren:

- Definieren Sie in den Netzwerkrichtlinien für die VPN-Verbindungen IPv4-Paketfilter, um eingehenden Verkehr auf der VPN-Verbindung zu verwerfen, sofern er nicht vom VPN-Client selbst

gesendet wurde. Bei der Standardnetzwerkrichtlinie (mit dem Namen *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver*) ist dieser IPv4-Paketfilter standardmäßig konfiguriert.

- Verwenden Sie das Netzwerkzugriffsschutzfeature in Windows Server 2008, Windows Vista und Windows XP mit Service Pack 3, um zu prüfen, ob bei VPN-Clients, die eine Verbindung herstellen wollen, das IPv4-Routing aktiviert ist. Erlauben Sie in diesem Fall keinen uneingeschränkten Remotezugriff, bis das Feature deaktiviert wurde.

Unbenutzte VPN-Protokolle

Falls Sie nicht alle VPN-Protokolle verwenden, sollten Sie im Snap-In *Routing und RAS* den Knoten *Ports* anzeigen und bei den unbenutzten VPN-Protokollen die Zahl der Ports auf 0 setzen. So verhindern Sie, dass Verbindungen zum VPN-Server über andere Protokolle hergestellt werden, die nicht für Remotezugriff-VPN-Verbindungen vorgesehen sind.

Bereitstellen von VPN-Remotezugriff

Gehen Sie folgendermaßen vor, um VPN-Remotezugriff mithilfe von Windows Server 2008 bereitzustellen:

- Stellen Sie Zertifikate bereit.
- Konfigurieren Sie die Internetinfrastruktur.
- Konfigurieren Sie die RADIUS-Server.
- Stellen Sie VPN-Server bereit.
- Konfigurieren Sie die Intranetinfrastruktur.
- Stellen Sie VPN-Clients bereit.

Bereitstellen von Zertifikaten

Sie müssen Zertifikate bereitstellen, falls Sie folgende Methoden benutzen:

- **L2TP/IPsec-Verbindungen mit Zertifikatauthentifizierung** Jeder VPN-Clientcomputer und VPN-Server muss ein Computertzertifikat haben.

Der Routing- und RAS-Dienst unterstützt die Konfiguration eines vorinstallierten Schlüssels für die IPsec-Authentifizierung von L2TP/IPsec-Verbindungen. Sie können im Snap-In *Routing und RAS* das Eigenschaftendialogfeld eines VPN-Servers öffnen, auf der Registerkarte *Sicherheit* eine benutzerdefinierte IPsec-Richtlinie aktivieren und den vorinstallierten Schlüssel eingeben. VPN-Clients, die unter Windows Server 2008, Windows Vista, Windows XP oder Windows Server 2003 laufen, unterstützen auch für IPsec die Konfiguration eines vorinstallierten Schlüssels. (Klicken Sie im Eigenschaftendialogfeld einer VPN-Verbindung auf der Registerkarte *Netzwerk* auf die Schaltfläche *IPSec-Einstellungen*.) Die Authentifizierung durch vorinstallierte Schlüssel für L2TP/IPsec-Verbindungen ist aber eine unsichere Form der Authentifizierung, sie wird daher nicht empfohlen.

- **EAP-TLS- oder PEAP-TLS-Authentifizierung mit Benutzerzertifikaten, die auf Smartcards oder in der Registrierung gespeichert sind** Jeder VPN-Clientcomputer braucht ein Smartcard- oder Benutzerzertifikat, und jeder Authentifizierungsserver ein Computertzertifikat.

Sie können die VPN-Clients so konfigurieren, dass sie das Zertifikat des Authentifizierungsservers nicht überprüfen. In diesem Fall sind auf den Authentifizierungsservern keine Computertzerti-

fikate erforderlich. Es wird aber empfohlen, das Zertifikat des Authentifizierungsservers vom VPN-Client überprüfen zu lassen, sodass eine gegenseitige Authentifizierung zwischen VPN-Clients und Authentifizierungsservern gewährleistet wird. Das soll verhindern, dass sich ein VPN-Client bei einem eingeschleusten Authentifizierungsserver authentifiziert.

- **PEAP-MS-CHAP v2-Authentifizierung** Jeder Authentifizierungsserver braucht ein Computerzertifikat, und jeder VPN-Client braucht das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle, die das Computerzertifikat des Authentifizierungsservers ausgestellt hat.

Sie können die VPN-Clients so konfigurieren, dass sie das Zertifikat des Authentifizierungsservers nicht überprüfen. In diesem Fall sind auf den Authentifizierungsservern keine Computerzertifikate erforderlich. Es muss dann auch nicht auf dem VPN-Client das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert sein, die das Zertifikat des Authentifizierungsservers ausgestellt hat. Es wird aber empfohlen, das Zertifikat des Authentifizierungsservers vom VPN-Client überprüfen zu lassen, sodass eine gegenseitige Authentifizierung zwischen VPN-Clients und Authentifizierungsservern gewährleistet ist.

- **SSTP-Verbindungen** Jeder VPN-Server braucht ein Computerzertifikat, und jeder VPN-Client braucht das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle, die das Computerzertifikat des VPN-Servers ausgestellt hat.

Beim VPN-Servercomputerzertifikat kann als erweiterte Schlüsselverwendung (EKU, Enhanced Key Usage) der Zweck *Serverauthentifizierung* oder *Alle* eingetragen sein. Das Computerzertifikat muss gültig sein, darf also nicht abgelaufen sein. Außerdem muss es einen Zertifikatsperrlistenverteilungspunkt haben, der aus dem Internet erreichbar ist. Der VPN-Client überprüft während der SSL-Authentifizierung, ob das Computerzertifikat gesperrt wurde. Dazu prüft er die Zertifikatsperrliste unter dem Verteilungspunkt, der im Computerzertifikat angegeben ist. Ob ein Zertifikat gesperrt ist, kann auch über OCSP (Online Certificate Status Protocol) geprüft werden. Dieses Protokoll ruft über HTTP eine digital signierte Antwort über den Status eines Zertifikats ab.

Außerdem muss der Name der Eigenschaft *Antragsteller* im Computerzertifikat des VPN-Servers dem Namen des VPN-Servers entsprechen, der auf dem VPN-Client im Ordner *Netzwerkverbindungen* im Eigenschaftendialogfeld der VPN-Verbindung angezeigt wird. Dieser Name muss auf jeden Fall übereinstimmen, unabhängig davon, ob Sie den VPN-Server über DNS-Hostnamen, IPv4-Adressen oder IPv6-Adressen angeben.

Bereitstellen von Computerzertifikaten

Damit Sie ein Computerzertifikat installieren können, muss eine PKI vorhanden sein, die die Zertifikate ausstellt. Wenn die PKI bereitgestellt wurde, haben Sie folgende Möglichkeiten, um Computerzertifikate auf VPN-Clients, VPN-Servern oder Authentifizierungsservern zu installieren:

- Konfigurieren Sie die automatische Registrierung von Computerzertifikaten für die Computer in einer Active Directory-Domäne.
- Fordern Sie im Snap-In *Zertifikate* ein Computerzertifikat an.
- Importieren Sie ein Computerzertifikat im Snap-In *Zertifikate*.
- Fordern Sie ein Zertifikat über das Web an.
- Führen Sie ein CAPICOM-Skript aus, das ein Computerzertifikat anfordert.

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« in Kapitel 9.

Bereitstellen der Stammzertifizierungsstellenzertifikate

In folgenden Fällen müssen Sie unter Umständen die Zertifikate der Stammzertifizierungsstellen bereitstellen:

- Sie arbeiten mit PEAP-MS-CHAP v2-Authentifizierung.
- Sie verwenden SSTP-Verbindungen.

Stammzertifizierungsstellenzertifikate für PEAP-MS-CHAP v2

Falls Sie PEAP-MS-CHAP v2-Authentifizierung einsetzen, müssen Sie unter Umständen auf Ihren VPN-Clients die Stammzertifizierungsstellenzertifikate für das Computerzertifikat installieren, das Ihre Authentifizierungsserver (die VPN-Server oder RADIUS-Server) übergeben. Falls das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle, die die Computerzertifikate der Authentifizierungsserver ausgestellt hat, bereits als eines der Stammzertifizierungsstellenzertifikate auf Ihren VPN-Clients installiert ist, ist keine weitere Konfiguration erforderlich. Falls zum Beispiel Ihre Stammzertifizierungsstelle eine Windows Server 2008- oder Windows Server 2003-Online-Organisations-Stammzertifizierungsstelle ist, wird das Stammzertifizierungsstellenzertifikat über Gruppenrichtlinien automatisch auf allen Domänenmitgliedscomputern installiert.

Gehen Sie folgendermaßen vor, um zu überprüfen, ob das richtige Stammzertifizierungsstellenzertifikat auf Ihren VPN-Clients installiert ist:

1. Stellen Sie fest, welche Stammzertifizierungsstelle für die Computerzertifikate zuständig ist, die auf den Authentifizierungsservern installiert sind.
2. Prüfen Sie, ob ein Zertifikat für diese Stammzertifizierungsstelle auf Ihren VPN-Clients installiert ist.

So ermitteln Sie die Stammzertifizierungsstelle für die Computerzertifikate, die auf den Authentifizierungsservern installiert sind

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Zertifikate* den Knoten des Computerkontos des Authentifizierungservers, den Knoten *Zertifikate (Lokaler Computer)* beziehungsweise *Zertifikate (<Computername>)* und dann den Knoten *Eigene Zertifikate*. Klicken Sie auf *Zertifikate*.
2. Klicken Sie in der Detailansicht doppelt auf das Computerzertifikat, das für PEAP-MS-CHAP v2-Authentifizierung benutzt wird.
3. Sehen Sie sich im Eigenschaftendialogfeld *Zertifikat* auf der Registerkarte *Zertifizierungspfad* den Namen ganz oben im Zertifizierungspfad an. Dies ist der Name der Stammzertifizierungsstelle.

So prüfen Sie, ob ein Zertifikat für die Stammzertifizierungsstelle auf einem VPN-Client installiert ist

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Zertifikate* den Knoten des Computerkontos des VPN-Clients, den Knoten *Zertifikate (Lokaler Computer)* beziehungsweise *Zertifikate (<Computername>)* und dann den Knoten *Vertrauenswürdige Stammzertifizierungsstellen*. Klicken Sie auf *Zertifikate*.
2. Prüfen Sie, ob die Liste der Zertifikate in der Detailansicht den Namen der Stammzertifizierungsstelle enthält, über die die Computerzertifikate der Authentifizierungsserver ausgestellt wurden.

Bei VPN-Clients, bei denen die Stammzertifizierungsstellenzertifikate der Herausgeber, die die Computerzertifikate der Authentifizierungsserver ausgestellt haben, nicht installiert sind, müssen Sie diese Zertifikate installieren. Am einfachsten können Sie ein Stammzertifizierungsstellenzertifikat auf allen Ihren VPN-Clients mithilfe von Gruppenrichtlinien installieren. Weitere Informationen finden Sie unter »Bereitstellen der Public-Key-Infrastruktur« in Kapitel 9.

Stammzertifizierungsstellenzertifikate für SSTP-Verbindungen

Falls Sie SSTP-Verbindungen verwenden, müssen Sie unter Umständen die Stammzertifizierungsstellenzertifikate für die Computerzertifikate installieren, die Ihre VPN-Server übergeben. Falls das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle, die die Computerzertifikate der VPN-Server ausgestellt hat, bereits als eines der Stammzertifizierungsstellenzertifikate auf Ihren VPN-Clients installiert ist, ist keine weitere Konfiguration erforderlich. Falls zum Beispiel Ihre Stammzertifizierungsstelle eine Windows Server 2008- oder Windows Server 2003-Online-Organisations-Stammzertifizierungsstelle ist, wird das Stammzertifizierungsstellenzertifikat über Gruppenrichtlinien automatisch auf allen Domänenmitgliedscomputern installiert.

Gehen Sie folgendermaßen vor, um zu überprüfen, ob das richtige Stammzertifizierungsstellenzertifikat auf Ihren VPN-Clients installiert ist:

1. Stellen Sie fest, welche Stammzertifizierungsstelle für die Computerzertifikate zuständig ist, die auf den VPN-Servern installiert sind.
2. Prüfen Sie, ob ein Zertifikat für diese Stammzertifizierungsstelle auf Ihren VPN-Clients installiert ist.

So ermitteln Sie die Stammzertifizierungsstelle für die Computerzertifikate, die auf den VPN-Servern installiert sind

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Zertifikate* den Knoten des Computerkontos des VPN-Servers, den Knoten *Zertifikate (Lokaler Computer)* beziehungsweise *Zertifikate (<Computername>)* und dann den Knoten *Eigene Zertifikate*. Klicken Sie auf *Zertifikate*.
2. Klicken Sie in der Detailansicht doppelt auf das Computerzertifikat, das für SSL-Authentifizierung benutzt wird.
3. Notieren Sie sich auf der Registerkarte *Zertifizierungspfad* den Namen ganz oben im Zertifizierungspfad. Dies ist der Name der Stammzertifizierungsstelle.

So prüfen Sie, ob ein Zertifikat für die Stammzertifizierungsstelle auf einem VPN-Client installiert ist

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Zertifikate* den Knoten des Computerkontos des VPN-Clients, den Knoten *Zertifikate (Lokaler Computer)* beziehungsweise *Zertifikate (<Computername>)* und dann den Knoten *Vertrauenswürdige Stammzertifizierungsstellen*. Klicken Sie auf *Zertifikate*.
2. Prüfen Sie, ob die Liste der Zertifikate in der Detailansicht den Namen der Stammzertifizierungsstelle enthält, über die die Computerzertifikate der VPN-Server ausgestellt wurden.

Bei Windows Server 2008- oder Windows Vista SP1-VPN-Clients, bei denen die Stammzertifizierungsstellenzertifikate der Herausgeber, die die Computerzertifikate der VPN-Server ausgestellt haben, nicht installiert sind, müssen Sie diese Zertifikate installieren. Am einfachsten können Sie ein Stammzertifizierungsstellenzertifikat auf allen Ihren VPN-Clients mithilfe von Gruppenrichtlinien installieren. Weitere Informationen finden Sie unter »Bereitstellen der Public-Key-Infrastruktur« in Kapitel 9.

Bereitstellen von Benutzerzertifikaten

Sie haben folgende Möglichkeiten, um Benutzerzertifikate auf VPN-Clientcomputern bereitzustellen:

- Konfigurieren Sie die automatische Registrierung von Benutzerzertifikaten für die Benutzer in einer Active Directory-Domäne.
- Fordern Sie im Snap-In *Zertifikate* ein Benutzerzertifikat an.

- Importieren Sie ein Benutzerzertifikat im Snap-In *Zertifikate*.
- Fordern Sie ein Zertifikat über das Web an.
- Führen Sie ein CAPICOM-Skript aus, das ein Benutzerzertifikat anfordert.

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« in Kapitel 9.

Konfigurieren der Internetinfrastruktur

Gehen Sie folgendermaßen vor, um die Internetinfrastruktur für Remotezugriff-VPN-Verbindungen zu konfigurieren:

- Richten Sie VPN-Server im Grenznetzwerk oder im Internet ein.
- Installieren Sie Windows Server 2008 auf VPN-Servern und konfigurieren Sie deren Internetschnittstellen.
- Fügen Sie Adresseinträge zu den Internet-DNS-Servern hinzu.

Einrichten von VPN-Servern im Grenznetzwerk oder Internet

Überlegen Sie, wo Sie die VPN-Server im Bezug auf Ihre Internetfirewall anordnen wollen. Üblich ist eine Konfiguration, bei der die VPN-Server hinter der Firewall im Grenznetzwerk liegen, also zwischen dem Internet und Ihrem Intranet. In diesem Fall müssen Sie auf der Firewall Paketfilter konfigurieren, die VPN-Verkehr zu und von den IPv4- oder IPv6-Adressen der Grenznetzwerkschnittstellen der VPN-Server erlauben. Weitere Informationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« weiter oben in diesem Kapitel.

Installieren von Windows Server 2008 auf VPN-Servern und Konfigurieren der Internetschnittstellen

Installieren Sie Windows Server 2008 auf dem VPN-Servercomputer. Geben Sie den Schnittstellen im Ordner *Netzwerkverbindungen* aussagekräftige Namen, die verraten, mit welchem Netzwerk sie verbunden sind. Verbinden Sie den VPN-Server über eine Netzwerkkarte entweder mit dem Internet oder dem Grenznetzwerk, und über eine andere Netzwerkkarte mit dem Intranet. Bevor Sie den Setup-Assistenten für den Routing- und RAS-Server ausführen, leitet der VPN-Servercomputer keine IPv4- oder IPv6-Pakete zwischen Internet und Intranet weiter.

Konfigurieren Sie für die Verbindung, die mit dem IPv4-Internet oder -Grenznetzwerk verbunden ist, das Protokoll *TCP/IP (IPv4)* mit einer öffentlichen IPv4-Adresse und einer Subnetzmaske. Stellen Sie als Standardgateway entweder die Firewall (falls der VPN-Server an ein Grenznetzwerk angeschlossen ist) oder einen Router des Internetproviders ein (falls der VPN-Server direkt mit dem Internet verbunden ist). Konfigurieren Sie keine IPv4-Adressen von DNS-Servern oder WINS-Servern für die Verbindung.

Konfigurieren Sie für die Verbindung, die mit dem IPv6-Internet oder -Grenznetzwerk verbunden ist, das Protokoll *TCP/IP (IPv6)* mit einer globalen IPv6-Adresse und einem 64-Bit-Präfix. Stellen Sie als Standardgateway entweder die Firewall (falls der VPN-Server an ein Grenznetzwerk angeschlossen ist) oder einen Router des Internetproviders ein (falls der VPN-Server direkt mit dem IPv6-Internet verbunden ist). Konfigurieren Sie keine IPv6-Adressen von DNS-Servern für die Verbindung.

Hinzufügen von Adresseinträgen zu den Internet-DNS-Servern

Sie müssen sicherstellen, dass der Name des VPN-Servers (zum Beispiel *vpn.example.microsoft.com*) in seine öffentliche IPv4-Adresse oder globale IPv6-Adresse aufgelöst werden kann. Dazu müssen Sie entweder DNS-Adresseinträge (A) oder IPv6-Adresseinträge (AAAA) zu Ihrem Internet-DNS-Server hinzufügen (falls Sie selbst die DNS-Namensauflösung für Internetbenutzer zur Verfügung stellen) oder Ihren Internetprovider beauftragen, A- beziehungsweise AAAA-Einträge zu seinen DNS-Servern hinzuzufügen (falls Ihr Internetprovider die DNS-Namensauflösung für Internetbenutzer zur Verfügung stellt). Überprüfen Sie, ob der Name des VPN-Servers in seine öffentliche IPv4-Adresse oder globale IPv6-Adresse aufgelöst werden kann, wenn er mit dem Internet verbunden ist.

Konfigurieren der Active Directory-Benutzerkonten und -Gruppen

Gehen Sie folgendermaßen vor, um Benutzerkonten und Gruppen in Active Directory zu konfigurieren:

1. Stellen Sie sicher, dass alle Benutzer von VPN-Clientcomputern ein entsprechendes Benutzerkonto haben.
2. Stellen Sie die RAS-Berechtigung in den Benutzerkonten der VPN-Clients auf *Zugriff gestatten* oder *Zugriff verweigern*, falls Sie den Remotезugriff individuell für jeden Benutzer verwalten wollen. Sie können die Verwaltung auch für ganze Gruppen durchführen, indem Sie für die RAS-Berechtigung in den Benutzerkonten die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* wählen.
3. Organisieren Sie die Benutzerkonten der VPN-Clients in geeigneten universellen und verschachtelten Gruppen, um die gruppenabhängigen Netzwerkrichtlinien nutzen zu können.

Konfigurieren von RADIUS-Servern

Falls Sie RADIUS für Authentifizierung, Autorisierung und Kontoführung von VPN-Verbindungen einsetzen, müssen Sie Ihre NPS-RADIUS-Server wie in Kapitel 9 beschrieben konfigurieren und bereitstellen. Dazu sind folgende Schritte erforderlich:

1. Installieren Sie ein Computertzertifikat auf den NPS-Servern (für EAP-TLS-, PEAP-TLS- oder PEAP-MS-CHAP v2-Authentifizierung).
2. Konfigurieren Sie die Protokollierung.
3. Fügen Sie alle VPN-Server als RADIUS-Clients zum NPS-Server hinzu.

Der NPS-Server benutzt eine Netzwerkrichtlinie, um Remotезugriff-VPN-Verbindungen zu autorisieren. Für Remotезugriff-VPN-Verbindungen können Sie die Standardnetzwerkrichtlinie mit dem Namen *Verbindungen mit Microsoft-Routing- und Remotезugriffsserver* verwenden. Bei dieser Netzwerkrichtlinie ist in der Standardeinstellung allerdings der Richtlinientyp *Zugriff verweigern* eingestellt.

Gehen Sie folgendermaßen vor, um diese Netzwerkrichtlinie so zu konfigurieren, dass sie Remotезugriff-VPN-Verbindungen annimmt:

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Netzwerkrichtlinienserver* unter *Richtlinien* auf *Netzwerkrichtlinien*.
2. Klicken Sie doppelt auf die Netzwerkrichtlinie *Verbindungen mit Microsoft-Routing- und Remotезugriffsserver*.

3. Wählen Sie auf der Registerkarte *Übersicht* unter *Zugriffsberechtigung* die Option *Zugriff gewähren* aus und klicken Sie auf *OK*.

Sie können auch den Assistenten *VPN oder DFÜ konfigurieren* verwenden, um einen Satz Richtlinien zu erstellen, die für Remotezugriff-VPN-Verbindungen optimiert sind.

So erstellen Sie einen Satz von Richtlinien für die Remotezugriff-VPN-Verbindungen

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Netzwerkrichtlinienserver* auf *NPS*.
2. Wählen Sie in der Detailansicht unter *Standardkonfiguration* in der Dropdownliste den Eintrag *RADIUS-Server für DFÜ- oder VPN-Verbindungen* aus und klicken Sie auf *VPN oder DFÜ konfigurieren*.
3. Klicken Sie im Assistenten *VPN oder DFÜ konfigurieren* auf der Seite *Auswählen des DFÜ- oder VPN-Verbindungstyps* auf *Verbindungen für virtuelles privates Netzwerk (VPN)* und geben Sie den Namen der neuen NPS-Netzwerkrichtlinie ein (oder verwenden Sie den Namen, den der Assistent eingetragen hat). Klicken Sie auf *Weiter*.
4. Fügen Sie auf der Seite *Angeben des DFÜ- oder VPN-Servers* nach Bedarf Ihre VPN-Server als RADIUS-Clients hinzu. Klicken Sie auf *Weiter*.
5. Auf der Seite *Authentifizierungsmethoden konfigurieren* ist bereits MS-CHAP v2 aktiviert. Wenn Sie einen EAP-Authentifizierungstyp aktivieren und konfigurieren wollen, müssen Sie das Kontrollkästchen *Extensible Authentication-Protokoll* aktivieren, in der Dropdownliste einen EAP-Typ auswählen und bei Bedarf auf *Konfigurieren* klicken (zum Beispiel um festzulegen, welches Computerzertifikat für EAP-TLS-, PEAP-TLS- oder PEAP-MS-CHAP v2-Authentifizierung verwendet werden soll). Klicken Sie auf *Weiter*.
6. Fügen Sie auf der Seite *Benutzergruppen angeben* die Gruppen hinzu, deren Benutzerkonten Remotezugriff-VPN-Verbindungen herstellen dürfen (zum Beispiel *VPNBenutzer*), und klicken Sie auf *Weiter*.
7. Fügen Sie auf der Seite *Angeben von IP-Filtern* IPv4- und IPv6-Eingabe- und Ausgabepaketfilter hinzu, die auf alle Remotezugriff-VPN-Verbindungen angewendet werden sollen. Klicken Sie auf *Weiter*.
8. Aktivieren Sie auf der Seite *Angeben von Verschlüsselungseinstellungen* die erlaubten Verschlüsselungsstärken und klicken Sie auf *Weiter*.
9. Geben Sie auf der Seite *Bereichsname angeben* bei Bedarf den Bereichsnamen ein und aktivieren Sie das Kontrollkästchen *Bereichsname vor Authentifizierung des Benutzernamens entfernen*. Weitere Informationen über Bereichsnamen finden Sie in Kapitel 9. Klicken Sie auf *Weiter*.
10. Klicken Sie auf der Seite *Abschließen der neuen DFÜ- oder VPN-Verbindungen und RADIUS-Clients* auf *Fertig stellen*.

Der Assistent *VPN oder DFÜ konfigurieren* erstellt eine Verbindungsanforderungsrichtlinie und eine Netzwerkrichtlinie für Remotezugriff-VPN-Verbindungen. Außerdem konfiguriert der Assistent *VPN oder DFÜ konfigurieren* die Netzwerkrichtlinie mit einer einzigen EAP-Methode. Weitere EAP-Methoden können Sie auf der Registerkarte *Einstellungen* im Eigenschaftendialogfeld der Netzwerkrichtlinie konfigurieren.

Wenn Sie den primären NPS-Server mit den gewünschten Protokollierungs-, RADIUS-Client- und Richtlinieneinstellungen konfiguriert haben, können Sie die Konfiguration auf den sekundären oder auf weitere NPS-Server kopieren. Weitere Informationen finden Sie in Kapitel 9.

Bereitstellen von VPN-Servern

Gehen Sie folgendermaßen vor, um die VPN-Server für Remotezugriff-VPN-Verbindungen bereitzustellen:

1. Installieren Sie Computerzertifikate.
2. Konfigurieren Sie die Verbindung des VPN-Servers zum Intranet.
3. Installieren Sie die Rolle *Netzwerkrichtlinien- und Zugriffsdienste*.
4. Führen Sie den Setup-Assistenten für den Routing- und RAS-Server aus.
5. Fügen Sie native IPv6-Fähigkeiten hinzu (optional).

Installieren von Computerzertifikaten

Für L2TP/IPsec- oder SSTP-Verbindungen, oder falls der VPN-Server der Authentifizierungsserver ist und Sie PEAP-MS-CHAP v2-, EAP-TLS- oder PEAP-TLS-Authentifizierung einsetzen, müssen Sie ein Computerzertifikat auf dem VPN-Server installieren. Welche Methoden zur Verfügung stehen, um ein Computerzertifikat zu installieren, ist im Abschnitt »Bereitstellen von Zertifikaten« weiter oben in diesem Kapitel beschrieben.

Konfigurieren der Verbindung des VPN-Servers zum Intranet

Bei IPv4 müssen Sie die Verbindung des VPN-Servers zum Intranet mit einer manuellen TCP/IP-IPv4-Konfiguration versehen, die IPv4-Adresse, Subnetzmaske, Intranet-DNS-Server und Intranet-WINS-Server umfasst. Bei IPv6 müssen Sie die Verbindung des VPN-Servers zum Intranet mit einer manuellen TCP/IP-IPv6-Konfiguration versehen, die IPv6-Adresse, 64-Bit-Präfix und Intranet-DNS-Server umfasst. In beiden Fällen müssen Sie verhindern, dass Konflikte bei der Standardroute auftreten, weil die Standardroute in das IPv4- oder IPv6-Internet verweist. Deshalb dürfen Sie kein Standardgateway für die Intranetverbindung konfigurieren.

Installieren der Rolle *Netzwerkrichtlinien- und Zugriffsdienste*

Um Routing und RAS sowie das Verbindungs-Manager-Verwaltungskit zu installieren, müssen Sie im Server-Manager die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* und das Feature *Verbindungs-Manager-Verwaltungskit* installieren.

Ausführen des Setup-Assistenten für den Routing- und RAS-Server

Der Setup-Assistent für den Routing- und RAS-Server automatisiert die Konfiguration vieler Elemente des VPN-Servers. Die generierte Standardkonfiguration können Sie anschließend an Ihre speziellen Bereitstellungsanforderungen anpassen.

So führen Sie den Setup-Assistenten für den Routing- und RAS-Server aus

1. Klicken Sie im Startmenü auf *Verwaltung* und dann auf *Routing und RAS*.
2. Klicken Sie mit der rechten Maustaste auf Ihren Servernamen und wählen Sie den Befehl *Routing und RAS konfigurieren und aktivieren*. Klicken Sie auf der Seite *Willkommen* im Setup-Assistenten für den Routing- und RAS-Server auf *Weiter*.
3. Wählen Sie auf der Seite *Konfiguration* die Option *RAS (DFÜ oder VPN)* und klicken Sie auf *Weiter*.
4. Aktivieren Sie auf der Seite *RAS* das Kontrollkästchen *VPN*. Falls der VPN-Server auch DFÜ-RAS-Verbindungen unterstützen soll, können Sie zusätzlich das Kontrollkästchen *DFÜ* aktivieren. Klicken Sie auf *Weiter*.

5. Klicken Sie auf der Seite *VPN-Verbindung* auf die Verbindung, die mit dem Internet oder Ihrem Grenznetzwerk verbunden ist. Stellen Sie sicher, dass das Kontrollkästchen *Sicherheit auf der ausgewählten Schnittstelle durch Einrichten statischer Paketfilter aktivieren* aktiviert ist, und klicken Sie auf *Weiter*. Abbildung 12.5 zeigt ein Beispiel.

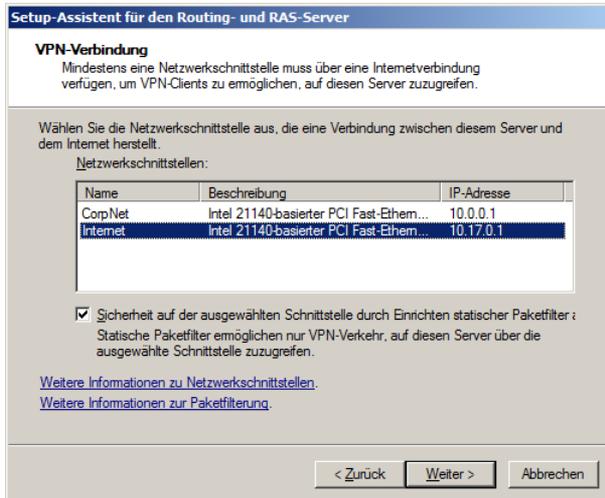


Abbildung 12.5 Die Assistentenseite *VPN-Verbindung*

6. Wählen Sie auf der Seite *Netzwerkauswahl* (wird nur angezeigt, falls Sie mehrere Netzwerkkarten mit dem Standort verbunden haben) die Verbindung aus, von der Routing und RAS die DHCP-, DNS- und WINS-Konfiguration für Remotezugriff-VPN-Clients abrufen soll. Klicken Sie auf *Weiter*, falls diese Seite angezeigt wird.
7. Wählen Sie auf der Seite *IP-Adresszuweisung* die Option *Automatisch* aus, falls der VPN-Server die IPv4-Adressen für Remotezugriff-VPN-Clients über DHCP abrufen soll. Stattdessen können Sie auch die Option *Aus einem angegebenen Adressbereich* wählen, wenn Sie eine oder mehrere statische Adressbereiche verwenden wollen. Falls irgendwelche der statischen Adressbereiche aus einem Adressbereich stammen, der außerhalb des eigenen Subnetzes liegt, müssen Routen zur Routinginfrastruktur hinzugefügt werden, damit die VPN-Clients erreichbar sind. Klicken Sie auf *Weiter*, wenn Sie die IPv4-Adresszuweisung abgeschlossen haben.
8. Falls Sie den VPN-Server für Authentifizierung und Autorisierung einsetzen, müssen Sie auf der Seite *Mehrere RAS-Server verwalten* die Option *Nein, Routing und RAS zum Authentifizieren von Verbindungsanforderungen verwenden* wählen. Falls Sie RADIUS für Authentifizierung und Autorisierung einsetzen, müssen Sie die Option *Ja, diesen Server für die Verwendung eines RADIUS-Servers einrichten* wählen. Klicken Sie auf *Weiter*.
9. Falls Sie in Schritt 8 RADIUS ausgewählt haben, können Sie auf der Seite *RADIUS-Serverauswahl* den primären (muss immer eingetragen werden) und alternativen (optional) RADIUS-Server sowie den gemeinsamen geheimen Schlüssel für RADIUS konfigurieren (Abbildung 12.6). Klicken Sie auf *Weiter*, wenn Sie damit fertig sind.
10. Klicken Sie auf der Seite *Fertigstellen des Assistenten* im Setup-Assistenten für den Routing- und RAS-Server auf *Fertig stellen*.

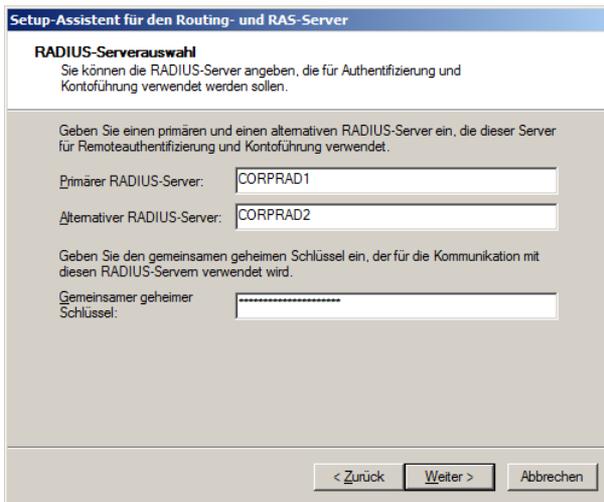


Abbildung 12.6 Die Assistentenseite *RADIUS-Serverauswahl*

11. Falls der Setup-Assistent für den Routing- und RAS-Server die DHCP-Relay-Agent-Komponente nicht automatisch mit den IPv4-Adressen der DHCP-Server im Intranet konfigurieren kann, bekommen Sie eine entsprechende Meldung angezeigt. Klicken Sie auf *OK* oder auf *Hilfe*, um weitere Informationen zu erhalten.

Falls Ihr VPN-Server nicht als Standort-zu-Standort-VPN-Router agiert, können Sie bei Bedarf herzustellen Routingverbindungen deaktivieren und auf diese Weise einen dedizierten Remotезugriff-VPN-Server einrichten.

So deaktivieren Sie bei Bedarf herzustellende Routingverbindungen für Standort-zu-Standort-VPN-Verbindungen

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf den Namen des Servers und wählen Sie den Befehl *Eigenschaften*.
2. Wählen Sie auf der Registerkarte *Allgemein* unter *IPv4-Router* die Option *Nur LAN-Routing* und klicken Sie auf *OK*.

Hinzufügen nativer IPv6-Fähigkeiten

Native IPv6-Fähigkeiten für Remotезugriff-VPN-Verbindungen (das heißt IPv6-Pakete entweder innerhalb des VPN-Tunnels oder über eine native IPv6-VPN-Verbindung) wird in vielen Intranets vorerst nicht benötigt. Aus diesem Grund verzichtet der Setup-Assistent für den Routing- und RAS-Server darauf, native IPv6-Fähigkeiten für Remotезugriff-VPN-Verbindungen über das IPv4- oder IPv6-Internet automatisch zu aktivieren.

Um für Remotезugriff-VPN-Verbindungen in Routing und RAS native IPv6-Fähigkeiten zu konfigurieren, müssen Sie folgendermaßen vorgehen:

- Aktivieren Sie IPv6-Routing für Remotезugriffsverbindungen.
- Konfigurieren Sie das Routerankündigungsverhalten.
- Konfigurieren Sie den DHCPv6-Relay-Agent so, dass er DHCPv6-Nachrichten zwischen VPN-Clients und DHCPv6-Servern im Intranet weiterleitet.

So konfigurieren Sie die Unterstützung von nativem IPv6-Verkehr über VPN-Verbindungen auf dem VPN-Server

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf den Namen des VPN-Servers und wählen Sie den Befehl *Eigenschaften*.
2. Aktivieren Sie auf der Registerkarte *Allgemein* das Kontrollkästchen *IPv6-RAS-Server* und klicken Sie auf *Übernehmen*.
3. Stellen Sie auf der Registerkarte *IPv6* sicher, dass die Kontrollkästchen *IPv6-Weiterleitung aktivieren* und *Standardroutenankündigung aktivieren* aktiviert sind. Geben Sie das Subnetzpräfix ein, das IPv6-VPN-Clients zugewiesen wird, wenn Sie eine Verbindung herstellen. Sie brauchen keine Präfixlänge anzugeben. Zum Beispiel können Sie für das Subnetzpräfix 2001:db8:4a2c:29::/64 den Text »2001:db8:4a2c:29::« eingeben. Abbildung 12.7 zeigt ein Beispiel.

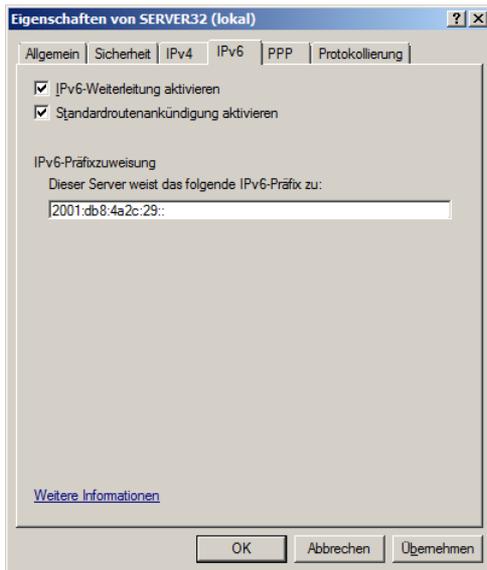


Abbildung 12.7 Die Registerkarte *IPv6* im Eigenschaftendialogfeld des Routing- und RAS-Servers

4. Klicken Sie auf *OK*. Sie werden nun aufgefordert, den Routing- und RAS-Dienst neu zu starten.
5. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv6*.
6. Klicken Sie mit der rechten Maustaste auf *Allgemein* und wählen Sie den Befehl *Neues Routingprotokoll*.
7. Klicken Sie im Dialogfeld *Neues Routingprotokoll* auf *OK*, um die Komponente *DHCPv6-Relay-Agent* hinzuzufügen.
8. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *DHCPv6-Relay-Agent*, wählen Sie den Befehl *Neue Schnittstelle*, wählen Sie *Intern* aus und klicken Sie zweimal auf *OK*.
9. Klicken Sie mit der rechten Maustaste auf *DHCPv6-Relay-Agent* und wählen Sie den Befehl *Eigenschaften*.
10. Geben Sie auf der Registerkarte *Server* die globalen Adressen Ihrer DHCPv6-Server im Intranet ein und klicken Sie auf *OK*.

Konfigurieren der Netzwerkinfrastruktur des Intranets

Gehen Sie folgendermaßen vor, um die Intranetnetzwerkinfrastruktur für Remotезugriff-VPN-Verbindungen bereitzustellen:

1. Konfigurieren Sie das Routing auf dem VPN-Server.
2. Überprüfen Sie, ob Namensauflösung und Intraneterreichbarkeit auf dem VPN-Server funktionieren.
3. Konfigurieren Sie das Routing für Adresspools außerhalb des eigenen Subnetzes (bei Bedarf).
4. Konfigurieren Sie das Routing für das IPv6-Subnetzpräfix der Remotезugriffscients.

Konfigurieren des Routings auf dem VPN-Server

Damit Ihre VPN-Server Verkehr an Intranetadressen richtig weiterleiten können, müssen Sie folgende Konfigurationen vornehmen:

- Fügen Sie statische Routen hinzu, die den gesamten im Intranet benutzten IPv4- und IPv6-Adressraum abdecken.
- Falls Sie einen RIP-fähigen IPv4-Router in dem Intranetsubnetz verwenden, an das der VPN-Server angeschlossen ist, müssen Sie das RIP-Routingprotokoll hinzufügen, damit der VPN-Server Routen mit benachbarten RIP- Routern austauschen und automatisch Routen für Intranetsubnetze zu seiner Routingtabelle hinzufügen kann.

So fügen Sie statische IPv4-Routen hinzu

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv4*.
2. Klicken Sie mit der rechten Maustaste auf *Statische Routen* und wählen Sie den Befehl *Neue statische Route*.
3. Wählen Sie im Dialogfeld *Statische IPv4-Route* (Abbildung 12.8) die richtige Schnittstelle aus und geben Sie Ziel, Netzwerkmaske, Gateway und Metrik für die statische Route ein. Klicken Sie auf *OK*.

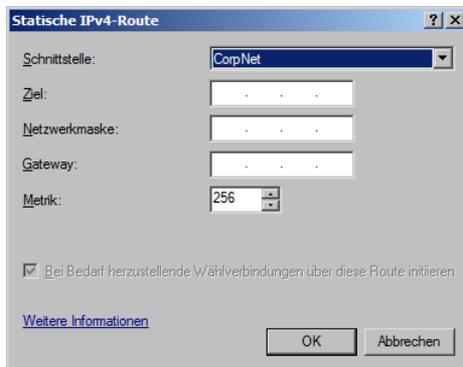


Abbildung 12.8 Das Dialogfeld *Statische IPv4-Route*

4. Wiederholen Sie die Schritte 2 und 3, wenn Sie weitere statische IPv4-Routen hinzufügen wollen.

So fügen Sie statische IPv6-Routen hinzu

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv6*.
2. Klicken Sie mit der rechten Maustaste auf *Statische Routen* und wählen Sie den Befehl *Neue statische Route*.
3. Wählen Sie im Dialogfeld *Statische IPv6-Route* (Abbildung 12.9) die richtige Schnittstelle aus und geben Sie Ziel, Präfixlänge, Gateway und Metrik für die statische Route ein. Klicken Sie auf *OK*.

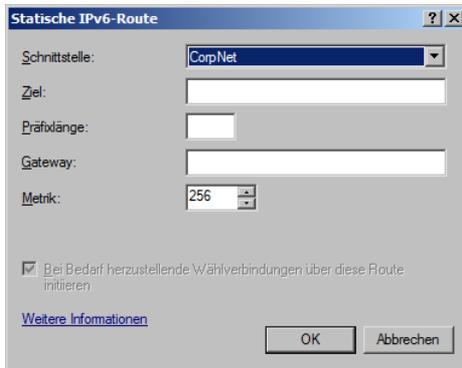


Abbildung 12.9 Das Dialogfeld *Statische IPv6-Route*

4. Wiederholen Sie die Schritte 2 und 3, wenn Sie weitere statische IPv6-Routen hinzufügen wollen.



Hinweis Sie müssen nur dann statische IPv6-Routen hinzufügen, wenn Sie Ihre VPN-Server mit nativen IPv6-Fähigkeiten konfiguriert haben.

So konfigurieren Sie den VPN-Server als RIP-Router

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv4*.
2. Klicken Sie mit der rechten Maustaste auf *Allgemein* und wählen Sie den Befehl *Neues Routingprotokoll*.
3. Klicken Sie im Dialogfeld *Neues Routingprotokoll* auf *RIP, Version 2, für das Internetprotokoll*. Klicken Sie auf *OK*.
4. Klicken Sie mit der rechten Maustaste auf *RIP* und wählen Sie den Befehl *Neue Schnittstelle*.
5. Wählen Sie die Intranetschnittstelle des VPN-Servers aus und klicken Sie auf *OK*.
6. Konfigurieren Sie im Dialogfeld *Eigenschaften von RIP* das RIP-Routingprotokoll, sodass es den Einstellungen des benachbarten RIP-Routers im Intranetsubnetz des VPN-Servers entspricht. Klicken Sie auf *OK*.

Überprüfen von Namensauflösung und Erreichbarkeit auf dem VPN-Server

Überprüfen Sie, ob der VPN-Server Namen von Intranetressourcen auflösen und erfolgreich damit kommunizieren kann. Dafür können Sie den Befehl *Ping* und den *Windows Internet Explorer* verwenden. Außerdem können Sie *Laufwerk-* und *Druckerverbindungen* zu bekannten Intranetservern herstellen.

Konfigurieren des Routings für Adresspools außerhalb des eigenen Subnetzes

Falls Sie die VPN-Server mit IPv4-Adresspools konfiguriert haben und irgendwelche dieser Pools außerhalb des eigenen Subnetzes liegen, müssen Sie sicherzustellen, dass die Routen für diese subnetzexternen Adresspools in Ihrer Intranet-IPv4-Routinginfrastruktur eingetragen sind. Sie können statische Routen für die subnetzexternen Adresspools zu den benachbarten Routern des VPN-Servers hinzufügen und die Routen dann mithilfe des in Ihrem Intranet verwendeten Routingprotokolls an andere Router weiterverbreiten. Wenn Sie die statischen Routen hinzufügen, müssen Sie angeben, dass das Gateway oder die Adresse des nächsten Abschnitts (engl. hop) die Intranetschnittstelle des VPN-Servers ist.

Konfigurieren des Routings für das IPv6-Subnetzpräfix von Remotezugriffsclients

Um sicherzustellen, dass IPv6-fähige Remotezugriffsclients aus dem Intranet heraus erreichbar sind, müssen Sie eine statische Route für das Subnetzpräfix der Remotezugriffsclients zu den benachbarten IPv6-Routern des VPN-Servers hinzufügen und diese Routen dann mithilfe des Routingprotokolls, das in Ihrem Intranet eingesetzt wird, an andere Router weiterverbreiten. Wenn Sie die statischen Routen hinzufügen, müssen Sie angeben, dass das Gateway oder die Adresse des nächsten Abschnitts die verbindungslokale Adresse der Intranetschnittstelle des VPN-Servers ist.

Bereitstellen von VPN-Clients

Gehen Sie folgendermaßen vor, um VPN-Clients für Remotezugriff-VPN-Verbindungen bereitzustellen:

- Konfigurieren Sie die VPN-Clients von Hand.
- Konfigurieren Sie mit dem Verbindungs-Manager-Verwaltungskit Verbindungs-Manager-Profile und stellen Sie diese Profile bereit.
- Konfigurieren Sie den gleichzeitigen Zugriff auf Internet und Intranet.

VPN-Clients manuell konfigurieren

Falls Sie nur wenige VPN-Clients haben, können Sie VPN-Verbindungen für jeden VPN-Client von Hand konfigurieren. Bei Windows Server 2008- und Windows Vista-VPN-Clients können Sie dafür den Assistenten *Eine Verbindung oder ein Netzwerk einrichten* verwenden. Bei Windows XP- und Windows Server 2003-VPN-Clients können Sie den Assistenten für neue Verbindungen benutzen.

Konfigurieren und Bereitstellen von Verbindungs-Manager-Profilen mit dem Verbindungs-Manager-Verwaltungskit

Wenn Sie eine große Zahl von VPN-Clients haben, die unter unterschiedlichen Windows-Versionen laufen, sollten Sie mit dem Verbindungs-Manager-Verwaltungskit ein Verbindungs-Manager-Profil für Ihre Benutzer erstellen. Das fertige Verbindungs-Manager-Profil (eine selbstentpackende ausführbare Datei) müssen Sie an Ihre Benutzer verteilen. Jeder Benutzer muss das Verbindungs-Manager-Profil ausführen, das daraufhin automatisch eine VPN-Verbindung im Ordner *Netzwerkverbindungen* dieses Benutzers anlegt.

So konfigurieren Sie ein Verbindungs-Manager-Profil für eine VPN-Verbindung

1. Klicken Sie im Startmenü auf *Verwaltung* und dann auf *Verbindungs-Manager-Verwaltungskit*. Falls das Verbindungs-Manager-Verwaltungskit noch nicht installiert ist, müssen Sie im Server-Manager auf *Features hinzufügen* klicken und den Eintrag *Verbindungs-Manager-Verwaltungskit* aus der Liste auswählen.

2. Klicken Sie auf der Seite *Willkommen* im Assistenten für das Microsoft Verbindungs-Manager-Verwaltungskit auf *Weiter*.
3. Wählen Sie auf der Seite *Zielbetriebssystem auswählen* entweder die Option *Windows Vista* oder *Windows Server 2003*, *Windows XP* oder *Windows 2000* aus, je nachdem, an welchen Satz von VPN-Clientcomputern dieses Verbindungs-Manager-Profil verteilt wird. Klicken Sie auf *Weiter*.
4. Klicken Sie auf der Seite *Verbindungs-Manager-Profil erstellen oder ändern* auf *Weiter*, um ein neues Profil zu erstellen.
5. Geben Sie auf der Seite *Dienst- und Dateinamen angeben* den Namen des Profils ein, unter dem es im Ordner *Netzwerkverbindungen* angezeigt wird. Geben Sie außerdem den Namen ein, unter dem das Profil auf dem Datenträger gespeichert wird. Klicken Sie auf *Weiter*.
6. Geben Sie auf der Seite *Bereichsname angeben* einen Bereichsnamen ein und legen Sie bei Bedarf fest, wo er relativ zum Benutzernamen erscheint. Ein Bereichsname gibt normalerweise an, wo das Benutzerkonto gespeichert ist. Dabei wird das Benutzerkonto anhand des Domänen- oder Organisationsnamens identifiziert. Falls Sie keinen Bereichsnamen anzugeben brauchen, können Sie einfach auf *Weiter* klicken.
7. Geben Sie auf der Seite *Informationen von anderen Profilen zusammenführen* bei Bedarf an, welche vorhandenen Profile in diesem neuen Profil zusammengeführt werden sollen, und klicken Sie auf *Weiter*.
8. Aktivieren Sie auf der Seite *Unterstützung für VPN-Verbindungen hinzufügen* (Abbildung 12.10) das Kontrollkästchen *Telefonbuch aus diesem Profil*. Geben Sie unter *VPN-Servername oder IP-Adresse* den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN), die öffentliche IPv4-Adresse oder die globale IPv6-Adresse der Internetschnittstelle des VPN-Servers ein. Stattdessen können Sie auch die Option *Benutzer kann VPN-Server selbst wählen* auswählen und dann eine Textdatei angeben, die eine Liste mit Namen oder Adressen Ihrer VPN-Server enthält. Klicken Sie auf *Weiter*.

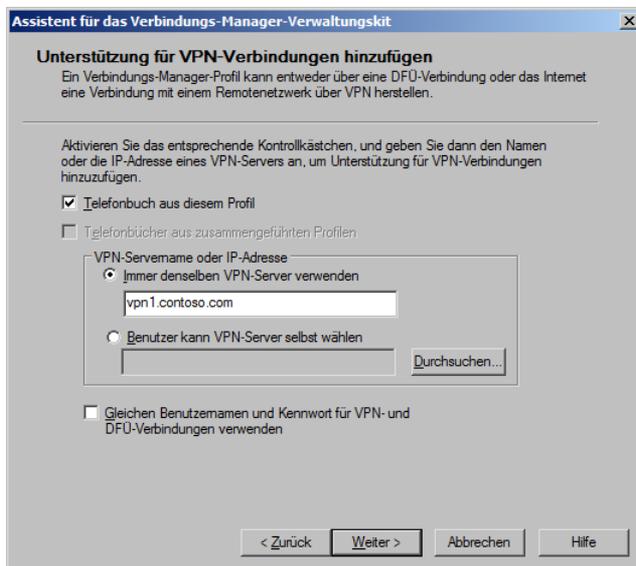


Abbildung 12.10 Die Assistentenseite *Unterstützung für VPN-Verbindungen hinzufügen*

9. Klicken Sie auf der Seite *VPN-Eintrag erstellen oder ändern* auf *Bearbeiten*, um die Einstellungen des Standard-VPN-Eintrags zu ändern. Tragen Sie im Dialogfeld *VPN-Eintrag bearbeiten* die gewünschten Einstellungen auf den Registerkarten *Allgemein*, *IPv4*, *IPv6*, *Sicherheit* (Authentifizierungsprotokolle und Verschlüsselungsanforderungen) und *Erweitert* ein. Abbildung 12.11 zeigt die Standardeinstellungen für einen neuen Eintrag auf der Registerkarte *Sicherheit*. Klicken Sie auf *OK* und dann auf *Weiter*.

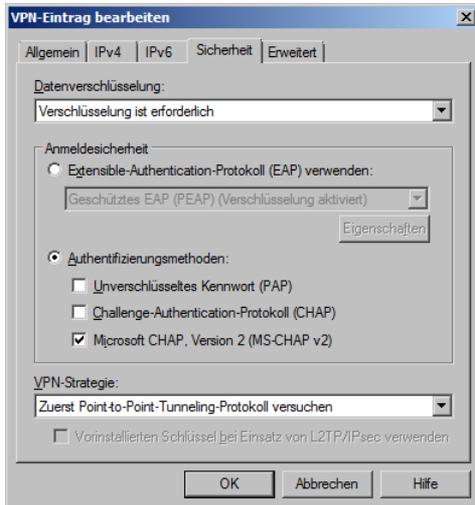


Abbildung 12.11 Hinzufügen eines neuen VPN-Eintrags

10. Deaktivieren Sie auf der Seite *Benutzerdefiniertes Telefonbuch hinzufügen* das Kontrollkästchen *Automatischer Download von Telefonbuchupdates*. (Die VPN-Verbindung braucht nicht automatisch eine DFÜ-Verbindung aufzubauen.) Klicken Sie auf *Weiter*.
11. Klicken Sie auf der Seite *DFÜ-Netzwerkeinträge konfigurieren* auf *Weiter*.
12. Falls Sie mit dem Verbindungs-Manager-Profil Routen für gleichzeitigen Internet- und Intranetzugriff zu den VPN-Clients hinzufügen wollen, können Sie auf der Seite *Routingtabellenaktualisierungen angeben* die Option *Routingtabellenaktualisierung definieren* auswählen und dann die Datei oder einen URL angeben, in dem die Routen enthalten sind. Klicken Sie auf *Weiter*.
13. Falls Sie auf den VPN-Clients einen Proxyserver im Intranet konfigurieren wollen, müssen Sie auf der Seite *Proxyeinstellungen für Internet Explorer automatisch konfigurieren* entweder die Option *Internet Explorer-Proxyeinstellungen für den aktuellen Benutzer automatisch in die Tunnelschnittstelle kopieren* oder *Proxyeinstellungen automatisch konfigurieren* auswählen und dann die Datei angeben, in der die Proxyeinstellungen definiert sind. Klicken Sie auf *Weiter*.
14. Konfigurieren Sie auf der Seite *Benutzerdefinierte Aktionen hinzufügen* nach Bedarf benutzerdefinierte Aktionen. Klicken Sie auf *Weiter*.
15. Falls Sie eine eigene Bitmap im Anmeldedialogfeld des Benutzers anzeigen wollen, können Sie auf der Seite *Benutzerdefinierte Anmeldungsbitmap anzeigen* die Option *Benutzerdefinierte Grafik* auswählen und dann eine Bitmapdatei mit den Abmessungen 330 × 140 Pixel eintragen. Klicken Sie auf *Weiter*.
16. Falls Sie eine eigene Bitmap im Telefonbuchdialogfeld anzeigen wollen, können Sie auf der Seite *Benutzerdefinierte Telefonbuchbitmap anzeigen* die Option *Benutzerdefinierte Grafik* auswählen

und dann eine Bitmapdatei mit den Abmessungen 114×309 Pixel eintragen. Klicken Sie auf *Weiter*.

17. Falls Sie im Netzwerk- und Freigabecenter oder im Ordner *Netzwerkverbindungen* eigene Bitmaps anzeigen wollen, können Sie auf der Seite *Benutzerdefinierte Symbole anzeigen* die Option *Benutzerdefinierte Symbole* auswählen und dann Bitmapdateien mit den Abmessungen 32×32 beziehungsweise 16×16 Pixel eintragen. Klicken Sie auf *Weiter*.
18. Falls Sie zum Profil eine eigene Hilfedatei zur Verfügung stellen wollen, können Sie auf der Seite *Benutzerdefinierte Hilfedatei einfügen* die Option *Benutzerdefinierte Hilfedatei* auswählen und dann den Speicherort der CHM-Datei eintragen. Klicken Sie auf *Weiter*.
19. Falls Sie im Anmeldedialogfeld einen Standardtext zum Support anzeigen wollen, können Sie auf der Seite *Benutzerdefinierte Supportinformationen anzeigen* im Textfeld *Supportinformationen* den gewünschten Text eingeben. Klicken Sie auf *Weiter*.
20. Falls Sie während der Installation des Verbindungs-Manager-Profiles eine eigene Lizenzvereinbarung anzeigen wollen, können Sie auf der Seite *Benutzerdefinierten Lizenzvertrag anzeigen* die Datei eintragen, die den Text der Lizenzvereinbarung enthält. Klicken Sie auf *Weiter*.
21. Falls Sie zusammen mit dem Verbindungs-Manager-Profil zusätzliche Dateien auf dem Computer des Benutzers installieren wollen, können Sie auf der Seite *Zusätzliche Dateien mit dem Verbindungs-Manager-Profil installieren* die gewünschten Dateien auswählen. Klicken Sie auf *Weiter*.
22. Klicken Sie auf der Seite *Verbindungs-Manager-Profil und zugehöriges Installationsprogramm erstellen* auf *Weiter*.
23. Klicken Sie auf der Seite *Das Verbindungs-Manager-Profil ist vollständig und kann verteilt werden* auf *Fertig stellen*.

Direkt von der Quelle: Verbesserungen an Verbindungs-Manager-Profilen

Remotezugriffsverbindungen, deren Verbindungs-Manager-Profile unter Windows Server 2003 erstellt wurden, unterstützen keine dynamischen DNS-Updates durch die Remotezugriffsclients. Das Problem lässt sich dadurch umgehen, dass Sie innerhalb des Verbindungs-Manager-Profiles ein Post-Connect-Aktionsskript festlegen, das die Registrierung beim Intranet-DNS-Server durchführt, sobald die VPN-Verbindung aufgebaut wurde. Die neue Version des Verbindungs-Managers, die in Windows Server 2008 enthalten ist, bietet die Möglichkeit, dynamische DNS-Updates für die Clients durchzuführen. Sie können dynamische DNS-Updates auf der Seite *DFÜ-Netzwerkeinträge konfigurieren* im Assistenten für das Microsoft Verbindungs-Manager-Verwaltungskit konfigurieren, indem Sie auf der Registerkarte *Erweitert* im Eigenschaftendialogfeld eines DFÜ- oder VPN-Netzwerkeintrags die gewünschte Einstellung vornehmen. Verbindungs-Manager-Profile für Windows Vista bieten außerdem Unterstützung für das Einstellen von IPv6-Konfigurationsoptionen.

*Tim Quinn, Support Escalation Engineer
Enterprise Platform Support*

Verteilen von Verbindungs-Manager-Profilen

Es gibt mehrere Möglichkeiten, wie Sie Ihr Verbindungs-Manager-Profil verteilen können. Wählen Sie eine der folgenden Methoden aus oder bieten Sie mehrere Methoden an, aus denen Ihre Benutzer auswählen dürfen.

Verteilen von Verbindungs-Manager-Profilen auf CD oder Datenträger

Sie können CDs oder Datenträger verteilen, die Ihr selbstinstallierendes Verbindungs-Manager-Profil enthalten. Ein Datenträger kann eine Diskette sein oder (üblicher bei modernen Computern, die kein Diskettenlaufwerk mehr haben) ein USB-Flashlaufwerk (Universal Serial Bus).

Diese Verteilungsmethode bietet den Vorteil, dass Sie jedem Benutzer ein eigenes Exemplar übergeben oder mit der Post senden können. Allerdings kann das teuer werden, und die Sicherheit ist sehr gering.

Verteilen von Verbindungs-Manager-Profilen über E-Mail

Sie können ein Verbindungs-Manager-Profil als E-Mail an Ihre Benutzer senden. Falls Sie diese Methode nutzen, sollten Sie sicherstellen, dass die Benutzer *.exe*-Dateien empfangen können, weil nicht alle E-Mail-Systeme ausführbare Dateien als Anhänge erlauben. Manchmal lässt sich ein solches Problem umgehen, indem Sie das Verbindungs-Manager-Profil vor dem Absenden im Zip-Format komprimieren.

Verteilen von Verbindungs-Manager-Profilen als Download

Sie können eine Website einrichten, von der die Benutzer das Verbindungs-Manager-Profil herunterladen. Benutzer mit Desktop- und mobilen Computern können die Datei direkt von einer Website innerhalb Ihres Intranets auf ihren Computer herunterladen.

Es ist auch möglich, das Verbindungs-Manager-Profil als Download von einer Website im Internet anzubieten. Analysieren Sie aber eventuelle Sicherheitsgefahren für Ihre Organisation, bevor Sie Ihr Verbindungs-Manager-Profil in einer Internetsite veröffentlichen.

Vorinstallieren von Verbindungs-Manager-Profilen

Sie können das Verbindungs-Manager-Profil auf jedem Clientcomputer einzeln vorinstallieren. Diese Methode hat den Vorteil, dass Benutzer nichts selbst installieren müssen. Das vermeidet Probleme bei den Benutzern und Anrufe beim Helpdesk. Allerdings müssen bei dieser Methode während der Installation Administratoren oder Helpdeskmitarbeiter tätig werden. Das kann während der Rolloutphase Ihrer Bereitstellung eine starke Belastung bedeuten. Diese Methode ist nützlich, wenn es nur wenige Clientcomputer gibt oder alle Clientcomputer und -geräte in Ihrer Organisation zentral verwaltet werden.

Kombinieren mehrerer Verteilungsmethoden

Sie können auch eine Kombination der genannten Verteilungsmethoden nutzen. Zum Beispiel kann ein Unternehmen die Verbindungs-Manager-Profile auf CD an Benutzer verteilen, die an einem Remotestandort mit ihren Computern arbeiten, Downloads für lokale Mitarbeiter zur Verfügung stellen, die tragbare Computer haben, und das Verbindungs-Manager-Profil auf allen neuen tragbaren Computern vorinstallieren.

Konfigurieren von gleichzeitigem Zugriff auf Internet und Intranet

Sie haben folgende Möglichkeiten, um gleichzeitigen Zugriff auf das IPv4-Internet und Ihr Intranet zu konfigurieren:

- DHCP-Option *Statische Routen ohne Klassen*
- Verbindungs-Manager-Verwaltungskit

Verwenden der DHCP-Option *Statische Routen ohne Klassen*

VPN-Clients, die unter Windows Server 2008, Windows Vista, Windows XP oder Windows Server 2003 laufen, senden eine DHCPInform-Nachricht zum VPN-Server, sobald die PPP-Aushandlung abgeschlossen ist. Darin fordern sie einen Satz von DHCP-Optionen an. Dies dient dazu, auf dem VPN-Client eine aktualisierte Liste der DNS- und WINS-Server sowie den DNS-Domännennamen abzurufen, der der VPN-Verbindung zugewiesen ist. Die DHCPInform-Nachricht wird vom VPN-Server an einen DHCP-Server im Intranet weitergeleitet, und die Antwort wird zum VPN-Client zurückgeleitet.

Die DHCPInform-Nachricht enthält eine Anforderung nach der DHCP-Option *Statische Routen ohne Klassen*. Um gleichzeitigen Zugriff zu ermöglichen, enthält die DHCP-Option *Statische Routen ohne Klassen* einen Satz von Routen für den Adressraum Ihres Intranets. Diese Routen werden automatisch zur Routingtabelle des anfordernden VPN-Clients hinzugefügt und automatisch wieder entfernt, sobald die VPN-Verbindung beendet wird. Die Option *Statische Routen ohne Klassen* (Optionsnummer 121) muss von Hand auf einem DHCP-Server konfiguriert werden, der unter Windows Server 2008 oder Windows Server 2003 läuft.

Um mithilfe der DHCP-Option *Statische Routen ohne Klassen* gleichzeitigen Zugriff zu implementieren, müssen Sie diese Option für den Bereich des Intranetssubnetzes konfigurieren, in dem der VPN-Server liegt. Fügen Sie einen Routensatz hinzu, der den IPv4-Adressraum für das Intranet Ihrer Organisation abdeckt. Falls Sie zum Beispiel für das Intranet Ihrer Organisation den nichtöffentlichen IPv4-Adressraum nutzen, muss die DHCP-Option *Statische Routen ohne Klassen* folgende drei Routen enthalten:

- 10.0.0.0 mit der Subnetzmaske 255.0.0.0
- 172.16.0.0 mit der Subnetzmaske 255.240.0.0
- 192.168.0.0 mit der Subnetzmaske 255.255.0.0

Die Router-IP-Adresse für jede Route, die zur Option *Statische Routen ohne Klassen* hinzugefügt wird, muss die IPv4-Adresse einer Routerschnittstelle in dem Intranetssubnetz sein, an das der VPN-Server angeschlossen ist. Falls der VPN-Server zum Beispiel an das Intranetssubnetz 10.89.192.0/20 angeschlossen ist und die IPv4-Adresse des Intranetrouters in diesem Subnetz 10.89.192.1 lautet, müssen Sie als Router-IP-Adresse für jede Route 10.89.192.1 eintragen.

Verwenden des Verbindungs-Manager-Verwaltungskits

Sie können das Verbindungs-Manager-Verwaltungskit in Windows Server 2008 verwenden, um spezifische Routen als Teil des Verbindungs-Manager-Profiles zu konfigurieren, das an VPN-Clients verteilt wird. Weitere Informationen über das Verbindungs-Manager-Verwaltungskit und Verbindungs-Manager-Profile finden Sie im Abschnitt »VPN-Clients« weiter oben in diesem Kapitel.



Weitere Informationen Weitere Informationen über das Konfigurieren von gleichzeitigem Zugriff mit dem Verbindungs-Manager-Verwaltungskit finden Sie in »Split Tunneling for Concurrent Access to the Internet and an Intranet« unter <http://technet.microsoft.com/en-us/library/bb878117.aspx>.

Wartung

Bei einer Remotezugriff-VPN-Lösung müssen folgende Wartungsaufgaben durchgeführt werden:

- Verwalten von Benutzerkonten
- Verwalten von VPN-Servern
- Aktualisieren von Verbindungs-Manager-Profilen

Verwalten von Benutzerkonten

Wenn ein neues Benutzerkonto in Active Directory angelegt wurde und Sie wollen, dass dieser Benutzer Remotezugriff-VPN-Verbindungen aufbauen darf, können Sie das neue Benutzerkonto zur entsprechenden Gruppe hinzufügen, die zur Verwaltung des VPN-Zugriffs dient. Zum Beispiel können Sie das Konto zur Sicherheitsgruppe *Schweiz_VPNBenutzer* hinzufügen, die wiederum Mitglied der universellen Gruppe *VPNBenutzer* ist. Die Netzwerkrichtlinie für VPN-Verbindungen ist dabei so konfiguriert, dass sie Mitgliedern der Gruppe *VPNBenutzer* Zugriff gewährt.

Wenn Benutzerkonten in Active Directory gelöscht werden, sind keine weiteren Aktionen nötig, um Remotezugriff-VPN-Verbindungen zu verhindern.

Bei Bedarf können Sie zusätzliche universelle Gruppen und Netzwerkrichtlinien erstellen, um Remotezugriff für unterschiedliche Benutzergruppen zu erlauben oder verbieten. Zum Beispiel können Sie eine globale Gruppe namens *Lieferanten* und eine Netzwerkrichtlinie erstellen, die Mitgliedern der Gruppe *Lieferanten* Remotezugriff-VPN-Verbindungen ausschließlich während der normalen Geschäftszeiten oder nur auf bestimmte Intranetressourcen erlaubt.

Verwalten von VPN-Servern

Sie müssen unter Umständen VPN-Server verwalten, wenn Sie einen VPN-Server in Ihrer Remotezugriff-VPN-Lösung hinzufügen oder entfernen. Wenn VPN-Server erst einmal bereitgestellt wurden, benötigen sie kaum noch Wartung. Die meisten Änderungen an einer funktionierenden VPN-Serverkonfiguration machen Kapazitätsprobleme und Änderungen an der Netzwerkinfrastruktur nötig.

Hinzufügen eines VPN-Servers

1. Folgen Sie den Anleitungen in den Abschnitten zu Entwurfsaspekten und Bereitstellung in diesem Kapitel, um einen neuen VPN-Server im Internet einzurichten.
2. Aktualisieren Sie im Internet-DNS die FQDN für die IPv4- oder IPv6-Adresse des neuen VPN-Servers oder fügen Sie einen neuen Eintrag hinzu.
3. Aktualisieren Sie Ihre RADIUS-Serverkonfiguration, sodass der VPN-Server als RADIUS-Client eingetragen ist.

Entfernen eines VPN-Servers

Gehen Sie folgendermaßen vor, um einen VPN-Server zu entfernen:

1. Aktualisieren oder entfernen Sie im Internet-DNS den FQDN für die IPv4- oder IPv6-Adresse des VPN-Servers.
2. Aktualisieren Sie Ihre RADIUS-Serverkonfiguration, indem Sie den VPN-Server als RADIUS-Client entfernen.
3. Fahren Sie den VPN-Server herunter und entfernen Sie ihn.

Vergrößern der Zahl möglicher Verbindungen

In der Standardeinstellung konfiguriert der Setup-Assistent für den Routing- und RAS-Server Routing und RAS mit der folgenden Zahl von Ports (jeder Port kann genau eine VPN-Verbindung unterstützen):

- 128 PPTP-Ports
- 128 L2TP-Ports
- 128 SSTP-Ports

Sie können die maximale Zahl von Ports für ein VPN-Protokoll folgendermaßen erhöhen:

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf *Ports* und wählen Sie den Befehl *Eigenschaften*.
2. Klicken Sie im Dialogfeld *Eigenschaften von Ports* doppelt auf das WAN-Miniport-Gerät, das dem gewünschten VPN-Protokoll zugeordnet ist.
3. Tragen Sie im Dialogfeld *Gerät konfigurieren* im Feld *Maximale Portanzahl* die maximale Zahl von Ports ein und klicken Sie zweimal auf *OK*.

Konfigurationsschritte bei Änderungen an Infrastrukturservern

Infrastrukturserver sind unter anderem DHCP-, DNS-, WINS- und RADIUS-Server (NPS). Falls sich die Änderungen an solchen Infrastrukturservern auf die Konfiguration des VPN-Servers auswirken, müssen Sie unter Umständen die Konfiguration des VPN-Servers an die neue Infrastruktur anpassen.

DHCP

Der Routing- und RAS-Dienst auf dem VPN-Server greift auf die DHCP-Relay-Agent- und DHCPv6-Relay-Agent-Routingprotokollkomponenten zurück, um DHCP- und DHCPv6-Nachrichten zwischen VPN-Clients und DHCP- oder DHCPv6-Server im Intranet weiterzuleiten. Falls sich die IPv4- oder IPv6-Adressen der konfigurierten DHCP- oder DHCPv6-Server ändern (zum Beispiel weil DHCP- oder DHCPv6-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie die Liste der DHCP- und DHCPv6-Adressen bei den DHCP-Relay-Agent- und DHCPv6-Relay-Agent-Routingprotokollkomponenten auf dem VPN-Server ändern.

DNS

Der VPN-Server sendet die IPv4-Adressen seiner konfigurierten DNS-Server während der PPP-Aushandlung an die VPN-Clients. Unter Umständen werden auf dem VPN-Client weitere IPv4-Adressen von DNS-Servern konfiguriert, wenn sie in den Antworten auf die DHCPInform-Nachricht enthalten sind. Falls sich die IPv4-Adressen der konfigurierten DNS-Server ändern (zum Beispiel weil DNS-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie die DNS-Serverkonfiguration auf dem VPN-Server und die Option *DNS-Server* auf dem DHCP-Server ändern, damit die VPN-Clients keine falschen IPv4-Adressen für die DNS-Server konfigurieren.

Bei nativen IPv6-VPN-Verbindungen lesen die VPN-Clients die IPv6-Adressen aus der Antwort auf die DHCPv6-Information-Request-Nachricht aus. Falls sich die IPv6-Adressen der konfigurierten DNS-Server ändern (zum Beispiel weil DNS-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie die DNS-Serverkonfiguration auf dem VPN-Server und die Option für die IPv6-DNS-Server auf dem DHCPv6-Server ändern, damit die VPN-Clients keine falschen IPv6-Adressen für die DNS-Server konfigurieren.

WINS

Der VPN-Server sendet während der PPP-Aushandlung die IPv4-Adressen seiner konfigurierten WINS-Server an die VPN-Client. Unter Umständen werden auf dem VPN-Client weitere IPv4-Adressen von WINS-Servern konfiguriert, wenn sie in den Antworten auf die DHCPInform-Nachricht enthalten sind. Falls sich die IPv4-Adressen der konfigurierten WINS-Server ändern (zum Beispiel weil WINS-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie die WINS-Serverkonfiguration auf dem VPN-Server und die Option für NetBIOS-Namensserver auf dem DHCP-Server ändern, damit die VPN-Clients keine falschen IPv4-Adressen für die WINS-Server konfigurieren.

RADIUS

Falls der VPN-Server so konfiguriert ist, dass er RADIUS-Authentifizierung nutzt, und sich die IPv4-Adressen der RADIUS-Server ändern (zum Beispiel weil RADIUS-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie folgendermaßen vorgehen:

1. Stellen Sie sicher, dass die VPN-Server auf den neuen RADIUS-Servern als RADIUS-Clients eingetragen sind.
2. Aktualisieren Sie die Konfiguration der VPN-Server, sodass sie die IPv4-Adressen der neuen RADIUS-Server enthalten.

Aktualisieren von Verbindungs-Manager-Profilen

Gehen Sie folgendermaßen vor, um ein Verbindungs-Manager-Profil zu aktualisieren:

1. Erstellen Sie mit dem Verbindungs-Manager-Verwaltungskit ein aktualisiertes Verbindungs-Manager-Profil.
2. Verteilen Sie das aktualisierte Verbindungs-Manager-Profil über E-Mail, eine Dateifreigabe oder andere Methoden an Ihre VPN-Clientbenutzer. Stellen Sie dabei eine Anleitung oder einen automatisierten Prozess zur Verfügung, um das Profil auszuführen und die VPN-Verbindungseinstellungen zu aktualisieren.

Problembehandlung

Weil so viele unterschiedliche Komponenten und Prozesse beteiligt sind, kann die Problembehandlung von Remotezugriff-VPN-Verbindungen recht schwierig sein. Dieser Abschnitt beschreibt, welche Tools in Windows Server 2008 und Windows Vista zur Verfügung stehen, um eine Problembehandlung für Remotezugriff-VPN-Verbindungen durchzuführen, und welche Probleme bei Remotezugriff-VPN-Verbindungen am häufigsten auftreten.

Tools für die Problembehandlung

Microsoft stellt für die Problembehandlung von VPN-Verbindungen auf dem VPN-Server folgende Tools zur Verfügung:

- TCP/IP-Problembehandlungstools
- Authentifizierungs- und Kontoführungsprotokollierung
- Ereignisprotokollierung
- NPS-Ereignisprotokollierung
- PPP-Protokollierung
- Ablaufverfolgung
- Network Monitor 3.1

Außerdem stellen Windows Server 2008 und Windows Vista folgende Tools zur Verfügung, mit denen Sie eine Problembehandlung für VPN-Verbindungen auf dem VPN-Client durchführen können:

- TCP/IP-Problembehandlungstools
- Unterstützung für Remotezugriffsverbindungen im Netzwerkdiagnose-Framework

TCP/IP-Problembehandlungstools

Die Tools Ping, Tracert und Pathping nutzen ICMP-Echo- und -Echo-Reply-Nachrichten sowie ICMPv6-Echo-Request- und -Echo-Reply-Nachrichten, um die Konnektivität zu überprüfen, den Pfad zu einem Ziel anzuzeigen und zu überprüfen, ob der Pfad vollständig ist. Mit dem Befehl `route print` können Sie die IPv4- und IPv6-Routingtabellen anzeigen. Auf dem VPN-Server können Sie stattdessen auch den Befehl `netsh routing ip show rtmroutes` oder das Snap-In *Routing und RAS* verwenden, um Routen anzuzeigen. Mit dem Tool Nslookup können Sie DNS- und Namensauflösungsprobleme untersuchen.

Authentifizierungs- und Kontoführungsprotokollierung

Ein VPN-Server, der unter Windows Server 2008 läuft, unterstützt die Protokollierung von Authentifizierungs- und Kontoführungsinformationen über Remotезugriff-VPN-Verbindungen in lokalen Protokolldateien, wenn Routing und RAS so konfiguriert ist, dass es die Authentifizierung und Kontoführung lokal durchführt. Diese Protokollierung findet getrennt von der Aufzeichnung von Ereignissen im Ereignisprotokoll *Windows-Protokolle\Sicherheit* statt. Mithilfe der aufgezeichneten Informationen können Sie die Nutzung des Remotезugriffs und Authentifizierungsversuche verfolgen. Authentifizierungs- und Kontoführungsprotokollierung ist insbesondere nützlich, wenn Sie Probleme im Zusammenhang mit einer Netzwerkrichtlinie untersuchen. Zu jedem Authentifizierungsversuch wird der Name der Netzwerkrichtlinie aufgezeichnet, die den Verbindungsversuch erlaubt oder zurückgewiesen hat.

Sie können die Authentifizierungs- und Kontoführungsprotokollierung aktivieren, indem Sie das Snap-In *Netzwerkrichtlinienserver* öffnen, auf *Kontoführung* und dann auf *Protokollierung für lokale Dateien konfigurieren* klicken. Auf der Registerkarte *Einstellungen* können Sie die entsprechenden Einstellungen konfigurieren.

Die Authentifizierungs- und Kontoführungsinformationen werden in einer oder mehreren konfigurierbaren Protokolldateien gespeichert, die im Ordner `%SystemRoot%\System32\LogFiles` liegen. Die Protokolldateien werden im IAS-Format (Internet Authentication Service, Internetauthentifizierungsdienst) oder einem datenbankkompatiblen Format gespeichert, sodass jedes Datenbankprogramm die Protokolldatei zu Analyse Zwecken direkt einlesen kann. Routing und RAS kann Authentifizierungs- und Kontoführungsinformationen auch an eine SQL-Datenbank (Structured Query Language) senden.

Falls der VPN-Server so konfiguriert ist, dass er RADIUS für Authentifizierung und Kontoführung verwendet, und falls der RADIUS-Server ein Computer ist, der Windows Server 2008 und NPS ausführt, werden die Authentifizierungs- und Kontoführungsprotokolle im Ordner `%SystemRoot%\System32\LogFiles` auf dem NPS-Servercomputer gespeichert. NPS für Windows Server 2008 kann Authentifizierungs- und Kontoführungsinformationen auch an eine Microsoft SQL Server-Datenbank senden.

Ereignisprotokollierung

Wenn Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld eines VPN-Servers öffnen, finden Sie auf der Registerkarte *Protokollierung* Optionen für vier Stufen der Protokollierung. Dies betrifft die Einträge, die in das Ereignisprotokoll *Windows-Protokolle\System* geschrieben werden. Am meisten Informationen erhalten Sie, wenn Sie die Option *Alle Ereignisse protokollieren* wählen und dann versuchen, die Verbindung erneut aufzubauen. Wenn der Verbindungsaufbau abbricht, können Sie im Ereignisprotokoll *Windows-Protokolle\System* nach Ereignissen mit den Ereignisquellen *Ras-Server*, *RemoteAccess* oder *RasSstp* suchen, die während des Verbindungsprozesses aufgezeichnet wurden. Nachdem Sie sich die Ereignisse angesehen haben, sollten Sie auf der Registerkarte *Proto-*

kollierung wieder die Option *Fehler und Warnungen protokollieren* auswählen, um die Systemressourcen zu schonen.

NPS-Ereignisprotokollierung

Falls Ihre VPN-Server so konfiguriert sind, dass sie RADIUS-Authentifizierung verwenden, und Ihre RADIUS-Server Computer sind, die Windows Server 2008 und NPS ausführen, können Sie im Knoten *Windows-Protokolle\Sicherheit* der Ereignisanzeige nach NPS-Ereignissen im Zusammenhang mit zurückgewiesenen (Ereignis-ID 6273) oder angenommenen (Ereignis-ID 6272) Verbindungsversuchen suchen. NPS-Ereignisprotokolleinträge enthalten zahlreiche Informationen über den Verbindungsversuch, darunter den Namen der verwendeten Verbindungsanforderungsrichtlinie (das Feld »Proxyrichtliniename« in der Beschreibung des Ereignisses) und die Netzwerkrichtlinie, die den Verbindungsversuch angenommen oder zurückgewiesen hat (das Feld »Netzwerkrichtliniename« in der Beschreibung des Ereignisses). Die NPS-Ereignisprotokollierung für zurückgewiesene oder angenommene Verbindungsversuche ist in der Standardeinstellung aktiviert. Sie können die entsprechenden Einstellungen im Snap-In *Netzwerkrichtlinienserver* im Eigenschaftendialogfeld eines NPS-Servers auf der Registerkarte *Allgemein* konfigurieren.

PPP-Protokollierung

Die PPP-Protokollierung zeichnet die Abfolge der Programmfunktionen und PPP-Steuermeldungen während einer PPP-Verbindung auf. Sie ist eine wertvolle Informationsquelle, wenn Sie eine Problembehandlung wegen einer fehlgeschlagenen PPP-Verbindung durchführen. Sie können die PPP-Protokollierung im Snap-In *Routing und RAS* aktivieren, indem Sie das Eigenschaftendialogfeld eines VPN-Servers öffnen und auf der Registerkarte *Protokollierung* das Kontrollkästchen *Zusätzliche Routing- und RAS-Informationen protokollieren* aktivieren.

In der Standardeinstellung ist das PPP-Protokoll in der Datei *Ppp.log* im Ordner *%SystemRoot%\Tracing* gespeichert.

Ablaufverfolgung

Der Routing- und RAS-Dienst besitzt leistungsfähige Ablaufverfolgungsfunktionen, die Sie nutzen können, wenn Sie komplexe Netzwerkprobleme untersuchen. Sie können Komponenten von Windows Server 2008 anweisen, Ablaufverfolgungsinformationen in Dateien zu protokollieren. Dafür können Sie das Tool *Netsh* verwenden oder bestimmte Registrierungswerte ändern.

Aktivieren der Ablaufverfolgung mit Netsh

Mit dem Tool *Netsh* können Sie die Ablaufverfolgung für bestimmte Komponenten oder für alle Komponenten gleichzeitig aktivieren beziehungsweise deaktivieren. Verwenden Sie die folgende Syntax, um die Ablaufverfolgung für eine bestimmte Komponente zu aktivieren oder zu deaktivieren:

```
netsh ras diagnostics set rastracing Komponente enabled|disabled
```

Dabei steht *Komponente* für eine Komponente in der Liste der Routing- und RAS-Dienstkomponenten, die Sie in der Windows Server 2008-Registrierung unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing* finden. Zum Beispiel können Sie mit dem folgenden Befehl die Ablaufverfolgung für die RASAUTH-Komponente aktivieren:

```
netsh ras diagnostics set rastracing rasauth enabled
```

Der folgende Befehl aktiviert die Ablaufverfolgung für alle Komponenten:

```
netsh ras diagnostics set rastracing * enabled
```

Aktivieren der Ablaufverfolgung über die Registrierung

Sie können die Ablaufverfolgungsfunktion auch konfigurieren, indem Sie Einstellungen im Zweig *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing* der Windows-Registrierung ändern.

Sie können die Ablaufverfolgung für jede einzelne Routing- und RAS-Dienstkomponente aktivieren, indem Sie die weiter unten beschriebenen Registrierungswerte setzen. Sie können die Ablaufverfolgung für Komponenten aktivieren und deaktivieren, während der Routing- und RAS-Dienst läuft. Jede Komponente beherrscht die Ablaufverfolgung. Zu jeder Komponente gibt es einen eigenen Unterschlüssel unter dem Registrierungsschlüssel *Tracing*.

Um die Ablaufverfolgung für eine Komponente zu aktivieren, können Sie die folgenden Registrierungseinträge unter dem jeweiligen Protokollschlüssel konfigurieren:

- **EnableFileTracing (REG_DWORD)** Sie können die Protokollierung von Ablaufverfolgungsinformationen in eine Datei aktivieren, indem Sie *EnableFileTracing* auf den Wert 1 setzen. Der Standardwert ist 0.
- **FileDirectory (REG_EXPAND_SZ)** Sie können den Standardspeicherort der Ablaufverfolgungsdateien ändern, indem Sie in *FileDirectory* den gewünschten Pfad eintragen. Der Dateiname der Protokolldatei enthält den Namen der Komponente, deren Ablaufverfolgung aktiviert wurde. In der Standardeinstellung liegen Protokolldateien im Ordner *%SystemRoot%\Tracing*.
- **FileTracingMask (REG_DWORD)** Der Registrierungseintrag *FileTracingMask* legt fest, wie viele Ablaufverfolgungsinformationen in der Datei protokolliert werden. Der Standardwert ist 0xFFFF0000.
- **MaxFileSize (REG_DWORD)** Sie können die Größe der Protokolldatei ändern, indem Sie *MaxFileSize* einen anderen Wert zuweisen. Der Standardwert ist 0x10000 (64 KByte).



Hinweis Die Ablaufverfolgung verbraucht Systemressourcen und sollte nur gezielt aktiviert werden, um Netzwerkprobleme zu untersuchen. Sobald die Ablaufverfolgungsdaten aufgezeichnet oder das Problem identifiziert wurde, sollten Sie die Ablaufverfolgung sofort wieder deaktivieren. Lassen Sie die Ablaufverfolgung auf Multiprozessorcomputern nicht aktiviert.

Ablaufverfolgungsinformationen können komplex und detailliert sein. In den meisten Fällen sind diese Informationen nur für Microsoft-Supportmitarbeiter oder Netzwerkadministratoren nützlich, die sich mit Routing und RAS gut auskennen. Die Protokolldateien der Ablaufverfolgung können bei Bedarf zu Analyse-zwecken an den Microsoft-Support gesendet werden.

Network Monitor 3.1

Mit Microsoft Network Monitor 3.1 oder einem anderen Packet Analyzer (auch als *Netzwerksniffer* bezeichnet) können Sie den Verkehr aufzeichnen und ansehen, der während des VPN-Verbindungsprozesses und des Datentransfers zwischen einem VPN-Server und dem VPN-Client ausgetauscht wird, oder den RADIUS-Verkehr zwischen einem VPN-Server und einem RADIUS-Server. Network Monitor 3.1 umfasst Parser für RADIUS, PPTP, PPP, L2TP, IPsec, HTTP, SSL und EAP. Ein *Parser* ist eine Komponente in Network Monitor 3.1, die die Felder eines Protokollheaders extrahieren und ihre Struktur und Werte anzeigen kann. Steht kein Parser zur Verfügung, zeigt Network Monitor 3.1 einen Header in Form von Hexadezimalzahlen an, die Sie selbst interpretieren müssen.



Auf der CD Auf der Begleit-CD finden Sie einen Link zur Downloadsite des Network Monitors.

Um den Remotezugriff- und VPN-Verkehr mit Network Monitor 3.1 richtig interpretieren zu können, müssen Sie sich mit den Details von PPP, PPTP, IPsec, SSL, RADIUS und anderen Protokollen auskennen. Die Aufzeichnungen von Network Monitor 3.1 können als Dateien gespeichert und zur Analyse an den Microsoft Customer Support geschickt werden.

Unterstützung für Remotezugriffsverbindungen im Netzwerkdiagnose-Framework

Um die Benutzerfreundlichkeit für den Fall zu verbessern, dass Netzwerkverbindungsprobleme auftreten, enthält Windows Vista das Netzwerkdiagnose-Framework (Network Diagnostics Framework, NDF). Dies ist ein Satz von Technologien und Richtlinien, die eine Gruppe von Problembehandlungstools (die sogenannten *Hilfsklassen* oder engl. *helper classes*) aktivieren, um bei der Diagnose zu helfen und Netzwerkprobleme nach Möglichkeit automatisch zu beseitigen. Wenn bei einem Windows Vista-Benutzer ein Netzwerkproblem auftritt, bietet NDF dem Benutzer die Möglichkeit, das Problem direkt im Kontext dieses Problems zu diagnostizieren und reparieren. Das bedeutet, dass die Bewertungs- und Auflösungs-schritte der Diagnose dem Benutzer entweder innerhalb der Anwendung oder des Dialogfelds präsentiert werden, in der/dem das Problem auftrat, oder im Kontext der fehlgeschlagenen Netzwerkoperation.

Wenn der Benutzer versucht, eine Aufgabe abzuschließen, die Netzwerkkonnektivität voraussetzt (zum Beispiel das Aufrufen einer Website im Browser oder das Senden einer E-Mail-Nachricht), bekommt er eine Fehlermeldung angezeigt, die ihn darauf aufmerksam macht, dass die Aufgabe nicht abgeschlossen werden kann (zum Beispiel »Seite kann nicht angezeigt werden« oder »Server nicht erreichbar«). NDF ergänzt die Fehlermeldung um eine Möglichkeit, das Problem zu diagnostizieren. Während der Diagnose analysiert NDF, warum die Operation fehlgeschlagen ist, und beschreibt eine Lösung für das Problem oder zeigt eine Liste von Ursachen und Lösungsmöglichkeiten an. Das alles in einfacher Sprache, sodass der Benutzer in die Lage versetzt wird, das Problem selbst zu beseitigen. Windows Vista enthält eine Problembehandlungsfunktion, die fehlgeschlagene Remotezugriffsverbindungen diagnostizieren kann. Falls eine Remotezugriffsverbindung nicht aufgebaut werden kann, zeigt Windows ein Dialogfeld mit Informationen über den Fehler an. Das Dialogfeld enthält eine Diagnoseschaltfläche, die das NDF-Problembehandlungsmodul für Remotezugriff startet. Innerhalb der Diagnosesitzung kann der Benutzer das Problem mit der Remotezugriffsverbindung beseitigen, ohne einen IT-Supportmitarbeiter fragen zu müssen.

Durchführen einer Problembehandlung für Remotezugriff-VPNs

Probleme mit Remotezugriff-VPN lassen sich normalerweise in folgende Kategorien unterteilen:

- Verbindungsversuch wird zurückgewiesen, obwohl er angenommen werden müsste
- L2TP/IPsec-Authentifizierungsprobleme
- SSTP-Authentifizierungsprobleme
- Verbindungsversuch wird angenommen, obwohl er zurückgewiesen werden müsste
- Adressen hinter dem VPN-Server können nicht erreicht werden
- Tunnel kann nicht aufgebaut werden

Mit den folgenden Problembehandlungstipps können Sie die Konfigurations- oder Infrastrukturprobleme isolieren, die für das Problem verantwortlich sind.

Verbindungsversuch wird zurückgewiesen, obwohl er angenommen werden müsste

Falls ein Verbindungsversuch zurückgewiesen wird, obwohl er eigentlich angenommen werden müsste, sollten Sie folgende Punkte überprüfen:

- Prüfen Sie mit dem Befehl Ping, ob der FQDN des VPN-Servers richtig in seine IPv4-Adresse aufgelöst wird. Der Ping-Test selbst schlägt unter Umständen fehl, weil Paketfilter verhindern, dass ICMP-Nachrichten zu und vom VPN-Server übertragen werden.
- Überprüfen Sie bei Kennwortauthentifizierung, ob die Benutzeranmeldeinformationen des VPN-Clients (Benutzername, Kennwort und Domänenname) richtig sind und vom Authentifizierungsserver (der VPN-Server oder RADIUS-Server) validiert werden.
- Überprüfen Sie, ob das Benutzerkonto des VPN-Clients gesperrt, abgelaufen oder deaktiviert ist und ob die Verbindung außerhalb der konfigurierten Anmeldezeiten hergestellt wird. Falls das Kennwort des Kontos abgelaufen ist, sollten Sie prüfen, ob der Remotezugriff-VPN-Client PEAP-MS-CHAP v2 oder MS-CHAP v2 benutzt. PEAP-MS-CHAP v2 und MS-CHAP v2 sind die einzigen Authentifizierungsprotokolle in Windows Server 2008, die es ermöglichen, ein abgelaufenes Kennwort während des Verbindungsprozesses zu ändern.

Wenn das Kennwort bei einem Konto mit Administratorrechten abgelaufen ist, können Sie das Kennwort über ein anderes Administratorkonto zurücksetzen.

- Überprüfen Sie, ob das Benutzerkonto aufgrund einer RAS-Kontosperrung gesperrt wurde.
- Überprüfen Sie, ob der Routing- und RAS-Dienst auf dem VPN-Server läuft.
- Überprüfen Sie bei SSTP-VPN-Verbindungen, ob der *SSTP-Dienst* auf dem VPN-Server läuft.
- Öffnen Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des VPN-Servers und prüfen Sie auf der Registerkarte *Allgemein*, ob der VPN-Server als IPv4- oder IPv6-RAS-Server aktiviert ist.
- Öffnen Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des Knotens *Ports* und überprüfen Sie, ob für die Geräte *WAN-Miniport (PPTP)*, *WAN-Miniport (L2TP)* und *WAN Miniport (SSTP)* eingehender Remotezugriff aktiviert ist.
- Überprüfen Sie, ob der VPN-Client, der VPN-Server und die Netzwerkrichtlinie für VPN-Verbindungen so konfiguriert sind, dass sie mindestens eine gemeinsame Authentifizierungsmethode verwenden.
- Überprüfen Sie, ob der VPN-Client und die Netzwerkrichtlinie für VPN-Verbindungen so konfiguriert sind, dass sie mindestens eine gemeinsame Verschlüsselungsstärke verwenden.
- Überprüfen Sie, ob die Parameter der Verbindung in den Netzwerkrichtlinien zugelassen werden.

Damit die Verbindung zugelassen wird, müssen die Parameter des Verbindungsversuchs folgende Voraussetzungen erfüllen:

- Sie muss alle Bedingungen mindestens einer Netzwerkrichtlinie erfüllen.
- Sie muss im Benutzerkonto die RAS-Berechtigung zugewiesen haben (Einstellung *Zugriff gestatten*). Oder falls beim Benutzerkonto die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* ausgewählt ist, muss bei der passenden Netzwerkrichtlinie der Richtlinientyp *Zugriff gestatten* ausgewählt sein.
- Sie muss mit allen Einstellungen der Netzwerkrichtlinie übereinstimmen.
- Sie muss mit allen Einstellungen in den Einwähleigenschaften des Benutzerkontos übereinstimmen.

Sie können den Namen der Netzwerkrichtlinie ermitteln, die den Verbindungsversuch zurückgewiesen hat, indem Sie im Ereignisprotokoll *Windows-Protokolle\Sicherheit* nach Ereignissen im Zusammenhang mit zurückgewiesenen (Ereignis-ID 6273) beziehungsweise angenommenen (Ereignis-ID 6272) Verbindungsversuchen suchen. Die Netzwerkrichtlinie, die den Verbindungsversuch angenommen oder zurückgewiesen hat, ist in der Beschreibung des Ereignisses im Feld »Netzwerkrichtliniename« aufgeführt.

- Falls Sie mit dem Konto eines Domänenadministrators angemeldet waren, als Sie den Setup-Assistenten für den Routing- und RAS-Server ausgeführt und Routing und RAS so konfiguriert haben, dass es die Authentifizierung lokal durchführt, fügt der Assistent das Computerkonto des VPN-Servers automatisch zur domänenlokalen Sicherheitsgruppe *RAS- und IAS-Server* hinzu. Diese Gruppenmitgliedschaft erlaubt es dem VPN-Servercomputer, auf Benutzerkontoinformationen zuzugreifen. Falls der VPN-Server nicht auf Benutzerkontoinformationen zugreifen kann, sollten Sie folgende Punkte überprüfen:
 - Das Computerkonto des VPN-Servercomputers muss in allen Domänen, die Benutzerkonten enthalten, für die der VPN-Server den Remotezugriff authentifiziert, Mitglied der Sicherheitsgruppe *RAS- und IAS-Server* sein. Sie können an einer Eingabeaufforderung den Befehl `netsh nps show registeredserver` ausführen, um sich die aktuellen Mitgliedschaften anzusehen. Mit dem Befehl `netsh nps add registeredserver` können Sie den Server in einer Domäne, in der dieser VPN-Server Mitglied ist, oder in anderen Domänen registrieren. Stattdessen können Sie oder Ihr Domänenadministrator das Computerkonto des VPN-Servercomputers auch in allen Domänen, die Benutzerkonten enthalten, für die der VPN-Server den Remotezugriff authentifiziert, zur Sicherheitsgruppe *RAS- und IAS-Server* hinzufügen.
 - Wenn Sie den VPN-Servercomputer zur Sicherheitsgruppe *RAS- und IAS-Server* hinzufügen oder daraus entfernen, wird die Änderung nicht sofort wirksam (wegen der Art, wie Windows Server 2008 Active Directory-Informationen zwischenspeichert). Damit die Änderung wirksam wird, müssen Sie den VPN-Servercomputer neu starten.
- Überprüfen Sie, ob noch PPTP-, L2TP- oder SSTP-Ports auf den VPN-Servern frei sind. Falls nötig, können Sie mehr Verbindungen erlauben. Öffnen Sie dazu im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des Knotens *Ports* und erhöhen Sie die Zahl der PPTP-, L2TP- oder SSTP-Ports.
- Überprüfen Sie, ob der VPN-Server das VPN-Protokoll des VPN-Clients unterstützt.

In der Standardeinstellung wird bei einem VPN-Client, der unter Windows Server 2008, Windows Vista, Windows Server 2003 oder Windows XP läuft, der VPN-Typ automatisch ausgewählt. Falls der VPN-Typ PPTP, L2TP/IPsec oder SSTP ausgewählt ist, müssen Sie sicherstellen, dass der VPN-Server das ausgewählte Tunnelprotokoll unterstützt.

Wenn Sie den Setup-Assistenten für den Routing- und RAS-Server ausführen und einen VPN-Server konfigurieren, wird ein Windows Server 2008-Computer, auf dem der Routing- und RAS-Dienst läuft, als PPTP-, L2TP- und SSTP-Server mit 128 PPTP-Ports, 128 L2TP-Ports und 128 SSTP-Ports eingerichtet. Falls der Server ausschließlich PPTP unterstützen soll, können Sie die Zahl der L2TP- und SSTP-Ports auf 0 setzen. Einen Server, der nur L2TP unterstützt, können Sie einrichten, indem Sie die Zahl der SSTP-Ports auf 0 und die Zahl der PPTP-Ports auf 1 setzen und für das Gerät *WAN-Miniport (PPTP)* eingehende Remotezugriffverbindungen und bei Bedarf herzustellende Wählverbindungen deaktivieren. Diese Einstellungen können Sie im Snap-In *Routing und RAS* im Dialogfeld des Knotens *Ports* vornehmen. Einen Server, der ausschließlich SSTP unterstützt, können Sie einrichten, indem Sie die Zahl der L2TP-Ports auf 0 und die Zahl der PPTP-

Ports auf 1 setzen und für das Gerät *WAN-Miniport (PPTP)* eingehende Remotezugriffverbindungen und bei Bedarf herzustellende Wählverbindungen deaktivieren.

- Falls der VPN-Server mit statischen IPv4-Adresspools konfiguriert wurde, sollten Sie überprüfen, ob genug Adressen für alle Verbindungen zur Verfügung stehen. Falls alle Adressen aus den statischen Pools bereits vorhandenen VPN-Clients zugewiesen wurden, kann der VPN-Server neuen TCP/IP-Verbindungen keine IPv4-Adresse mehr zuweisen und der Verbindungsversuch wird zurückgewiesen.
- Überprüfen Sie, wie der VPN-Server die Authentifizierung durchführt. Der VPN-Server kann so konfiguriert sein, dass er die Anmeldeinformationen des VPN-Clients entweder lokal oder über RADIUS authentifiziert.
 - Bei RADIUS-Authentifizierung müssen Sie sicherstellen, dass der VPN-Servercomputer mit dem RADIUS-Server kommunizieren kann.
 - Bei lokaler Authentifizierung müssen Sie sicherstellen, dass der VPN-Server Mitglied der Active Directory-Domäne ist und das Computerkonto des VPN-Servercomputers zur Sicherheitsgruppe *RAS- und IAS-Server* hinzugefügt wurde.

L2TP/IPsec-Authentifizierungsprobleme

Die folgenden Probleme sind am häufigsten die Ursache, wenn L2TP/IPsec-Verbindungen fehlschlagen:

- **Kein Zertifikat** In der Standardeinstellung von L2TP/IPsec-Verbindungen tauschen VPN-Server und VPN-Client ihre Computerzertifikate aus, um eine IPsec-Peerauthentifizierung durchzuführen. Prüfen Sie auf VPN-Client und VPN-Server im Snap-In *Zertifikate* die Zertifikatspeicher des lokalen Computers, um sicherzustellen, dass passende Zertifikate vorhanden sind.
- **Falsches Zertifikat** Falls Zertifikate vorhanden sind, müssen sie überprüfbar sein. Anders als beim manuellen Konfigurieren von IPsec-Regeln ist die Liste der Zertifizierungsstellen bei L2TP/IPsec-Verbindungen nicht konfigurierbar. Stattdessen sendet jeder Computer, der an der L2TP-Verbindung beteiligt ist, an seinen IPsec-Peer eine Liste der Stammzertifizierungsstellen, deren Zertifikat er für die Authentifizierung akzeptiert. Die Stammzertifizierungsstellen in dieser Liste sind die Stammzertifizierungsstellen, die Computerzertifikate für den Computer ausgestellt haben. Falls zum Beispiel Computer A Computerzertifikate von den Stammzertifizierungsstellen CertAuth1 und CertAuth2 ausgestellt bekommen hat, meldet er seinem IPsec-Peer während der Hauptmodusaushandlung, dass er für die Authentifizierung ausschließlich Zertifikate von CertAuth1 und CertAuth2 akzeptiert. Falls der IPsec-Peer, Computer B, kein gültiges Computerzertifikat hat, das von CertAuth1 oder CertAuth2 ausgestellt wurde, schlägt die IPsec-Sicherheitsaushandlung fehl. Der VPN-Client muss ein gültiges Computerzertifikat für die IPsec-Authentifizierung installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der VPN-Server vertraut. Außerdem muss der VPN-Server ein gültiges Computerzertifikat installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der VPN-Client vertraut.
- **Ein NAT liegt zwischen Remotezugriffsklient und RAS-Server** Falls ein NAT zwischen dem VPN-Client und dem VPN-Server liegt, müssen beide Computer IPsec-NAT-T unterstützen. VPN-Clients, die unter Windows Server 2008, Windows Vista, Windows Server 2003 oder Windows XP SP2

laufen, unterstützen IPsec-NAT-T. VPN-Server, die unter Windows Server 2008 oder Windows Server 2003 laufen, unterstützen IPsec-NAT-T.

- **Eine Firewall liegt zwischen Remotezugriffsclient und RAS-Server** Falls eine Firewall zwischen einem Windows-VPN-Client und einem Windows Server 2008-VPN-Server liegt und Sie keine L2TP/IPsec-Verbindung aufbauen können, sollten Sie prüfen, ob die Firewall die Weiterleitung von L2TP/IPsec-Verkehr erlaubt. Weitere Informationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« weiter oben in diesem Kapitel.

SSTP-Authentifizierungsprobleme

Die folgenden Probleme sind am häufigsten die Ursache, wenn SSTP-Verbindungen fehlschlagen:

- **Kein Zertifikat** SSTP-Verbindungen setzen voraus, dass der VPN-Server während der SSL-Authentifizierung ein Computerzertifikat an den VPN-Client sendet. Prüfen Sie im Snap-In *Zertifikate*, ob auf dem VPN-Server ein passendes Computerzertifikat installiert ist.
- **Zertifikatüberprüfung schlägt fehl** Auf dem VPN-Client muss das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert sein, die das Computerzertifikat des VPN-Servers ausgestellt hat. Ermitteln Sie den Namen der Stammzertifizierungsstelle, die das Computerzertifikat des VPN-Servers ausgestellt hat, und prüfen Sie dann, ob ein passendes Zertifikat auf Ihren VPN-Clients installiert ist. Prüfen Sie außerdem folgende Punkte:
 - Überprüfen Sie, ob das Computerzertifikat des VPN-Servers abgelaufen ist oder gesperrt wurde.
 - Überprüfen Sie, ob die Sperrlisten-Verteilungspunkte, die in der entsprechenden Eigenschaft im Computerzertifikat des VPN-Servers aufgeführt sind, im Internet erreichbar sind.
 - Überprüfen Sie, ob auf dem VPN-Client im Eigenschaftendialogfeld der VPN-Verbindung (im Ordner *Netzwerkverbindungen*) auf der Registerkarte *Allgemein* als Name des VPN-Servers derselbe Name eingetragen ist wie in der Eigenschaft *Antragsteller* im Computerzertifikat des VPN-Servers. Diese Namen müssen übereinstimmen, unabhängig davon, ob Sie die VPN-Server über DNS-Hostnamen, IPv4-Adressen oder IPv6-Adressen ansprechen.

Verbindungsversuch wird angenommen, obwohl er zurückgewiesen werden müsste

Falls ein Verbindungsversuch angenommen wird, obwohl er eigentlich zurückgewiesen werden müsste, sollten Sie folgende Punkte überprüfen:

- Überprüfen Sie, ob die RAS-Berechtigung im Benutzerkonto entweder *Zugriff verweigern* oder *Zugriff über NPS-Netzwerkrichtlinien steuern* lautet. Falls die zweite Option aktiv ist, müssen Sie sicherstellen, dass bei der ersten passenden Netzwerkrichtlinie der Typ *Zugriff verweigern* eingestellt ist. Sie können den Namen der Netzwerkrichtlinie ermitteln, die den Verbindungsversuch angenommen hat, indem Sie im Ereignisprotokoll *Windows-Protokolle\Sicherheit* nach Ereignissen zu diesem Verbindungsversuch suchen. Die Textbeschreibung des Ereignisses enthält den Richtliniennamen. Die Netzwerkrichtlinie, die den Verbindungsversuch angenommen oder zurückgewiesen hat, ist in der Beschreibung des Ereignisses im Feld »Netzwerkrichtliniename« aufgeführt.
- Falls Sie eine Netzwerkrichtlinie erstellt haben, die explizit alle Verbindungen zurückweist, sollten Sie die Bedingungen, den Typ und die Einstellungen dieser Richtlinie überprüfen und nachsehen, ob sie an der richtigen Stelle in der Liste der Netzwerkrichtlinien liegt.

Adressen hinter dem VPN-Server können nicht erreicht werden

Falls ein VPN-Client Adressen, die im Intranet hinter dem VPN-Server liegen, nicht erreichen kann, sollten Sie folgende Punkte überprüfen:

- Öffnen Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des VPN-Servers und prüfen Sie auf der Registerkarte *Allgemein*, ob die Kontrollkästchen *IPv4-RAS-Server* und *IPv6-RAS-Server* aktiviert sind.
- Überprüfen Sie im Snap-In *Routing und RAS* im Eigenschaftendialogfeld des VPN-Servers, ob auf den Registerkarten *IPv4* und *IPv6* die Weiterleitung für die Protokolle IPv4 oder IPv6 aktiviert ist.
- Überprüfen Sie die IPv4-Adresspools des VPN-Servers.

Falls der VPN-Server so konfiguriert ist, dass er einen subnetzexternen IPv4-Adresspool verwendet, sollten Sie prüfen, ob der Adressbereich des IPv4-Adresspools von Hosts und Routern im Intranet erreichbar ist. Falls nicht, müssen Sie die IPv4-Routen für die IPv4-Adresspools des VPN-Servers zu den Routern im Intranet hinzufügen. Falls Sie das Routingprotokoll RIP verwenden, können Sie stattdessen auch RIP auf dem VPN-Server aktivieren. Falls die Routen für die subnetzexternen Adresspools nicht vorhanden sind, können Remotezugriff-VPN-Clients keinen Verkehr von Adressen im Intranet empfangen.

Falls der VPN-Server so konfiguriert ist, dass er IPv4-Adressen für Remotezugriffscients mithilfe von DHCP abrufen, und kein DHCP-Server verfügbar ist, weist der VPN-Server Adressen aus dem APIPA-Adressbereich (Automatic Private IP Addressing) von 169.254.0.1 bis 169.254.255.254 zu. Die Nutzung von APIPA-Adressen für Remotezugriffscients funktioniert nur, wenn das Netzwerk, an das der VPN-Server angeschlossen ist, ebenfalls mit APIPA-Adressen arbeitet.

Falls der VPN-Server APIPA-Adressen verwendet, obwohl ein DHCP-Server verfügbar ist, sollten Sie prüfen, ob die mit DHCP zugewiesenen IPv4-Adressen über die richtige Netzwerkschnittstelle angefordert werden. Diese Einstellung wird im Setup-Assistenten für den Routing- und RAS-Server vorgenommen. Sie können von Hand einen LAN-Adapter aus der Liste der Adapter auswählen, indem Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des VPN-Servers öffnen und den Adapter auf der Registerkarte *IPv4* einstellen.

Falls die IPv4-Adresspools innerhalb des eigenen Subnetzes liegen (also ein Bereich von IPv4-Adressen, die ein Teil des IP-Adressbereichs für das Netzwerk sind, an das der VPN-Server angeschlossen ist), sollten Sie überprüfen, ob der Bereich der IPv4-Adressen in den IPv4-Adresspools nicht über manuelle Konfiguration oder DHCP anderen TCP/IP-Knoten zugewiesen wurde.

- Überprüfen Sie, ob das IPv6-Subnetzpräfix, das IPv6-fähigen VPN-Clients zugewiesen wird, eine Route in Ihrer IPv6-Routinginfrastruktur bildet, die zur Intranetschnittstelle des VPN-Servers zurückführt.
- Überprüfen Sie, ob es in den Einstellungen der Netzwerkrichtlinie für VPN-Verbindungen IPv4- oder IPv6-Eingabe- oder -Ausgabepaketfilter gibt, die das Senden oder Empfangen von Verkehr verhindern.

Tunnel kann nicht aufgebaut werden

Falls ein VPN-Client keinen Tunnel zum VPN-Server aufbauen kann, sollten Sie folgende Punkte überprüfen:

- Überprüfen Sie, ob die Paketfilterung auf der Routerschnittstelle zwischen dem VPN-Client und dem VPN-Server die Weiterleitung von VPN-Verkehr verhindert. Welche Verkehrstypen für VPN-Verbindungen erlaubt sein müssen, ist im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« weiter oben in diesem Kapitel beschrieben.

Auf einem Windows Server 2008-VPN-Server kann die IPv4-Paketfilterung getrennt in der Windows-Firewall mit erweiterter Sicherheit und im Snap-In *Routing und RAS* konfiguriert werden. Suchen Sie an beiden Stellen nach Filtern, die unter Umständen VPN-Verbindungsverkehr blockieren.

- Überprüfen Sie, ob der Winsock-Proxyclient (Windows Sockets) momentan auf dem VPN-Client läuft.

Wenn der Winsock-Proxyclient aktiv ist, werden Aufrufe der Winsock-API, mit denen zum Beispiel Tunnel erstellt und getunnelte Daten gesendet werden, abgefangen und zu einem konfigurierten Proxyserver weitergeleitet.

Wird in einer Organisation ein Proxyserver verwendet, können die Computer auf bestimmte Internetressourcen (normalerweise Web und FTP) zugreifen, ohne dass eine direkte Verbindung zwischen der Organisation und dem Internet bestehen muss. Die Organisation kann stattdessen nicht-öffentliche IP-Adresspräfixe verwenden, z.B. 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16.

Proxyserver werden normalerweise eingesetzt, damit interne Benutzer in einer Organisation Zugriff auf öffentliche Internetressourcen haben, als wären sie direkt an das Internet angeschlossen. VPN-Verbindungen sind normalerweise dazu vorgesehen, dass autorisierte öffentliche Internetbenutzer Zugriff auf interne Ressourcen der Organisation bekommen, als wären sie direkt mit dem internen Netzwerk verbunden. Derselbe Computer kann als Proxyserver (für interne Benutzer) und VPN-Server (für autorisierte Internetbenutzer) agieren, um beide Arten des Informationsaustauschs zu unterstützen.

Zusammenfassung des Kapitels

Um eine Remotezugriff-VPN-Lösung bereitzustellen, müssen Sie die Active Directory-, PKI-, Gruppenrichtlinien- und RADIUS-Komponenten einer Windows-Authentifizierungsinfrastruktur konfigurieren und VPN-Server im Internet planen und bereitstellen. Wenn eine Remotezugriff-VPN-Lösung einmal bereitgestellt ist, umfasst die Wartung das Verwalten von VPN-Servern, das Anpassen ihrer Konfiguration an Änderungen der Infrastrukturserver und das Aktualisieren und Bereitstellen von Verbindungs-Manager-Profilen. Ursachen für Probleme bei VPN-Verbindungen können sein, dass aufgrund von Authentifizierungs- oder Autorisierungsfehlern keine Verbindung hergestellt werden kann und Intranetressourcen vom VPN-Client aus nicht erreichbar sind.

Weitere Informationen

Weitere Informationen über die VPN-Unterstützung in Windows finden Sie hier:

- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Virtual Private Networks« (<http://www.microsoft.com/vpn>)

Weitere Informationen über VPN-Internetstandards finden Sie hier:

- RFC 2637, »Point-to-Point Tunneling Protocol (PPTP)«
- RFC 2661, »Layer Two Tunneling Protocol (L2TP)«
- RFC 3193, »Securing L2TP using IPsec«

Weitere Informationen über Active Directory finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«

- *Windows Server 2008 Active Directory – Die technische Referenz* von Stan Reimer, Mike Mulcare, Conan Kezema und Byron Wright, mit dem Microsoft Active Directory Team, einzeln erhältlich oder als Bestandteil der technischen Referenz zu Windows Server 2008 (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support

Weitere Informationen über die PKI finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Public Key Infrastructure for Windows Server« (<http://www.microsoft.com/pki>)
- *Microsoft Windows Server 2008 – PKI und Zertifikatsicherheit* von Brian Komar (Microsoft Press, 2008)

Weitere Informationen über Gruppenrichtlinien finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista* von Derek Melber (Group Policy MVP), mit dem Windows Group Policy Team (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Microsoft Windows Server Group Policy« (<http://www.microsoft.com/gp>)

Weitere Informationen über RADIUS und NPS finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Network Policy Server« (<http://www.microsoft.com/nps>)

Weitere Informationen über NAP und VPN-Erzwingung finden Sie hier:

- Kapitel 14, »Grundlagen des Netzwerkzugriffsschutzes«
- Kapitel 15, »Vorbereiten des Netzwerkzugriffsschutzes«
- Kapitel 18, »VPN-Erzwingung«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Network Policy Server« (<http://www.microsoft.com/nap>)

Standort-zu-Standort-VPN-Verbindungen

In diesem Kapitel:

Konzepte	195
Planungs- und Entwurfsaspekte	202
Bereitstellen von Standort-zu-Standort-VPN-Verbindungen	220
Wartung	242
Problembehandlung	244
Zusammenfassung des Kapitels	254
Weitere Informationen	254

Dieses Kapitel beschreibt Entwurf, Bereitstellung, Wartung und Problembehandlung von Standort-zu-Standort-VPN-Verbindungen (Virtual Private Network). Dieses Kapitel setzt voraus, dass Sie die Rollen von Active Directory, Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure, PKI), Gruppenrichtlinien und RADIUS (Remote Authentication Dial-up User Service) innerhalb einer Windows-Authentifizierungsinfrastruktur für Netzwerkzugriff kennen. Diese Elemente sind in Kapitel 9, »Authentifizierungsinfrastruktur«, genauer beschrieben.



Weitere Informationen Dieses Kapitel beschreibt nicht die Planung und Bereitstellung von Standort-zu-Standort-DFÜ-Verbindungen. Weitere Informationen zu diesen Themen finden Sie in Windows Server 2008-Hilfe und Support oder in der Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>.

Konzepte

Wie in Kapitel 12, »Remotezugriff-VPN-Verbindungen«, beschrieben, ist ein VPN die Erweiterung eines nichtöffentlichen Netzwerks, die Verbindungen über gemeinsam genutzte oder öffentliche Netzwerke wie zum Beispiel das Internet verwendet. Organisationen können mithilfe von VPN-Verbindungen routingfähige Verbindungen aufbauen, die als *Standort-zu-Standort-Verbindungen* (engl. site-to-site connection), *Standort-zu-Standort-Verbindungen* oder *Router-zu-Router-Verbindungen* (engl. router-to-router connection) bezeichnet werden. Sie dienen der Verbindung von weit auseinander liegenden Büros oder zu anderen Organisationen, wobei die Kommunikation trotz der Verbindung über das öffentliche Internet geschützt bleibt.

Eine Standort-zu-Standort-VPN-Verbindung über das Internet arbeitet logisch betrachtet als dedizierte WAN-Verbindung. Wird eine Standort-zu-Standort-VPN-Verbindung eingesetzt, kann eine Organisation preisgünstige Breitband- oder Standleitungsverbindungen zu einem Internetprovider nutzen. Somit können die hohen Kosten für DFÜ- oder Mietleitungen vermieden werden. Computer, die Standort-zu-Standort-VPN-Verbindungen nutzen, werden als VPN-Router bezeichnet.

Im Betriebssystem Windows Server 2008 gibt es zwei Arten von Standort-zu-Standort-VPN-Technologien:

- **Point-to-Point Tunneling Protocol (PPTP)** PPTP nutzt PPP-Authentifizierungsmethoden (Point-to-Point Protocol) für die Benutzerauthentifizierung und MPPE (Microsoft Point-to-Point Encryption) für die Datenverschlüsselung.
- **Layer Two Tunneling Protocol mit Internet Protocol Security (L2TP/IPsec)** L2TP/IPsec nutzt PPP-Authentifizierungsmethoden für die Benutzerauthentifizierung und IPsec für Peerauthentifizierung auf Computerebene, Datenauthentifizierung, Datenintegrität und Datenverschlüsselung.



Hinweis SSTP (Secure Socket Tunneling Protocol), das ebenfalls in Windows Server 2008 und Windows Vista mit Service Pack 1 zur Verfügung steht, kann nur für Remotezugriff-VPN-Verbindungen genutzt werden.

Ein VPN-Router kann jeder beliebige Computer sein, der in der Lage ist, eine routingfähige PPTP-Verbindung über MPPE oder eine routingfähige L2TP-Verbindung mit IPsec-Verschlüsselung aufzubauen.

Ein VPN-Router, der eine Standort-zu-Standort-VPN-Verbindung herstellt, wird als *anrufender Router* (engl. calling router) bezeichnet. Ein VPN-Router, der eingehende Standort-zu-Standort-Verbindungen entgegennimmt, wird als *antwortender Router* (engl. answering router) bezeichnet. Während des Verbindungsprozesses authentifiziert sich der anrufende Router beim antwortenden Router. Wird eine Authentifizierungsmethode eingesetzt, die gegenseitige Authentifizierung unterstützt, authentifiziert sich außerdem der antwortende Router beim anrufenden Router.



Hinweis Der Einsatz des IPsec-Tunnelmodus als Standort-zu-Standort-VPN-Technologie wird in Windows-VPN- Routern nicht unterstützt, weil es keinen Industriestandard für Benutzerauthentifizierung und IP-Adressenkonfiguration über einen IPsec-Tunnel gibt. Der IPsec-Tunnelmodus wird in den RFCs (Request For Comments) 4301, 4302 und 4303 beschrieben.

Grundlagen von bei Bedarf herzustellenden Routingverbindungen

Der Routing- und RAS-Dienst in Windows Server 2008 unterstützt *bei Bedarf herzustellende Routingverbindungen* (engl. demand-dial routing oder dial-on-demand routing) über DFÜ-Verbindungen (zum Beispiel analoge Telefonleitungen oder ISDN), VPN-Verbindungen und PPPoE-Verbindungen (PPP over Ethernet). Unter bei Bedarf herzustellendem Routing versteht man die Weiterleitung von Paketen über eine PPP-Verbindung (Point-to-Point Protocol). Die PPP-Verbindung wird in Routing und RAS als eine Schnittstelle für Wählen bei Bedarf (engl. demand-dial interface) aufgelistet. Sie kann Verbindungen über DFÜ oder nichtdauerhafte Kommunikationswege herstellen, aber auch Verbindungen über dauerhafte (persistente) Kommunikationswege. Mithilfe von bei Bedarf herzustellenden Wählverbindungen können Sie statt Mietleitungen normale Telefonleitungen einsetzen, wenn nicht allzu viel Verkehr übertragen werden muss, und Zweigstellen über den Internetanschluss mit VPN-Verbindungen ausstatten.

Bei Bedarf herzustellende Routingverbindungen sind etwas anderes als Remotezugriff (engl. remote access). Beim Remotezugriff stellt ein einzelner Computer eine Verbindung zu einem Netzwerk her. Dagegen werden mit bei Bedarf herzustellenden Routingverbindungen zwei Abschnitte eines Netzwerks miteinander verbunden. Bei beiden wird aber PPP als Protokoll eingesetzt, um die Verbindung auszuhandeln und zu authentifizieren und die über die Verbindung übertragenen Daten zu kapseln. In Routing und RAS sind Remotezugriff und bei Bedarf herzustellende Wählverbindungen so implementiert, dass sie einzeln oder in Kombination benutzt werden können. Sie haben folgende Eigenschaften gemein:

- Verhalten aufgrund der Einwähleigenschaften von Benutzerkonten
- Sicherheit (Authentifizierungsprotokolle und Verschlüsselung)
- Verwenden von Windows oder RADIUS (Remote Authentication Dial-In User Service) für Authentifizierung, Autorisierung und Kontoführung
- Verwenden von Netzwerkrichtlinien für die Autorisierung
- IPv4-Adresszuweisung und -Konfiguration
- Problembehandlungsfunktionen, darunter Ereignisprotokollierung, Windows- oder RADIUS-Authentifizierungs- und Kontoführungsprotokollierung sowie Ablaufverfolgung

Auch wenn das Konzept von bei Bedarf herzustellenden Routingverbindungen recht simpel ist, kann die Konfiguration solcher Routingverbindungen sehr komplex sein. Diese Komplexität ist auf folgende Faktoren zurückzuführen:

- **Adressierung der Verbindungsendpunkte** Die Verbindung muss über öffentliche Datennetze aufgebaut werden, zum Beispiel das Internet. Ein vollqualifizierter Domänenname, eine IPv4-Adresse oder eine IPv6-Adresse muss den Endpunkt der Verbindung identifizieren.
- **Authentifizierung und Autorisierung von bei Bedarf herzustellenden Wählverbindungen** Eingehende Verbindungen, die der antwortende Router entgegennimmt, müssen authentifiziert und autorisiert werden. Die Authentifizierung wertet die Anmeldeinformationen aus, die der anrufende Router während des Verbindungsaufbauvorgangs übergibt. Die übergebenen Anmeldeinformationen müssen einem Konto entsprechen. Die Autorisierung wird auf Basis der Einwähleigenschaften des Kontos und der Netzwerkrichtlinien gewährt.
- **Unterscheidung zwischen Remotezugriffsclients und anrufenden Routern** Bei Bedarf herzustellende Routingverbindungen und Remotezugriff können auf demselben Windows Server 2008-Computer genutzt werden. Sowohl Remotezugriffsclients als auch bei Bedarf wählende Router können eine Verbindung aufbauen. Der Windows Server 2008-Computer, der einen Verbindungsversuch beantwortet, kann einen Remotezugriffsclient anhand des Benutzernamens von einem bei Bedarf wählenden Router unterscheiden. Der Benutzername wird vom anrufenden Router in den Anmeldeinformationen gesendet, die für die Authentifizierung gebraucht werden. Falls der Benutzername mit dem Namen einer Schnittstelle für Wählen bei Bedarf auf dem antwortenden Router übereinstimmt, handelt es sich um eine bei Bedarf herzustellende Wählverbindung. Andernfalls ist die eingehende Verbindung eine Remotezugriffsverbindung.
- **Konfiguration beider Enden der Verbindung** Beide Enden der Verbindung müssen konfiguriert werden. Das gilt sogar dann, wenn immer dasselbe Ende der Verbindung die bei Bedarf herzustellende Wählverbindung aufbaut. Falls Sie nur eine Seite der Verbindung konfigurieren, können Pakete nur in einer Richtung erfolgreich weitergeleitet werden. Kommunikation ist normalerweise nur möglich, wenn Informationen in beiden Richtungen übertragen werden können.
- **Konfiguration von statischen Routen** Sie sollten keine dynamischen Routingprotokolle über bei Bedarf herzustellenden Wählverbindungen verwenden, die nur zeitweise aufgebaut werden. Daher müssen Routen für IPv4- oder IPv6-Adresspräfixe, die über die Schnittstelle für Wählen bei Bedarf verfügbar sind, als statische Routen zu den Routingtabellen der bei Bedarf wählenden Router hinzugefügt werden. Sie können statische Routen von Hand hinzufügen oder autostatische Aktualisierungen nutzen. Außerdem müssen diese Routen zu Ihrer Routinginfrastruktur hinzugefügt werden, damit die Erreichbarkeit von Remotestandorten sichergestellt ist.

Zusammengefasst lässt sich also sagen, dass eine Standort-zu-Standort-VPN-Verbindung eine bei Bedarf herzustellende Wählverbindung ist, die ein VPN-Protokoll wie zum Beispiel PPTP oder L2TP/IPsec nutzt, um zwei Abschnitte eines privaten Netzwerks miteinander zu verbinden. Der anrufende

Router baut die Verbindung mithilfe einer Schnittstelle für Wählen bei Bedarf auf. Der antwortende Router wartet auf Verbindungsversuche, empfängt den Verbindungsversuch vom anrufenden Router und schließt die Verbindungsherstellung mithilfe einer Schnittstelle für Wählen bei Bedarf ab. Sobald die Verbindung erfolgreich hergestellt ist, agieren sowohl anrufender als auch antwortender Router als IPv4- oder IPv6-Router, die Pakete zwischen zwei Standorten eines Unternehmensnetzwerks über die VPN-Verbindung weiterleiten.

Direkt von der Quelle: Der Name der Schnittstelle für Wählen bei Bedarf und der Benutzername müssen übereinstimmen

Wenn Standort-zu-Standort-VPN-Verbindungen für Wählen bei Bedarf zwischen VPN-Routern eingerichtet werden, wird oft der Fehler gemacht, dass der Benutzername nicht mit dem Namen der Schnittstelle für Wählen bei Bedarf auf dem antwortenden Router übereinstimmt. Es werden zwei separate Tunnel aufgebaut, falls der Benutzername des anrufenden Routers anders lautet als der Name der Schnittstelle für Wählen bei Bedarf auf dem antwortenden Router. Routing und RAS verwendet den Benutzernamen, um festzustellen, ob eine lokale Schnittstelle für Wählen bei Bedarf mit dem Tunnel verknüpft werden soll. Falls eine Übereinstimmung gefunden wird, werden die zwei Schnittstellen verknüpft und beide werden als verbunden eingestuft. Verkehr kann in beiden Richtungen über einen VPN-Tunnel weitergeleitet werden. Falls der Benutzername nicht übereinstimmt, werden zwei Tunnel als getrennte Remotezugriffsklientverbindungen eingerichtet, jeweils ein Tunnel für jede Richtung. Häufig gibt es einen dazwischen liegenden Router, der nur einen gleichzeitigen VPN-Tunnel unterstützt. Dieses Problem macht sich dadurch bemerkbar, dass zwar eine bei Bedarf herzustellende Wählerverbindung von VPNRouter1 zu VPNRouter2 aufgebaut werden kann, auch eine von VPNRouter2 zu VPNRouter1, aber niemals beide gleichzeitig. Falls eine Verbindung besteht, schlägt der Versuch, die zweite aufzubauen, fehl. Dabei ist egal, in welcher Richtung die erste Verbindung verläuft. Dieses Problem lässt sich am häufigsten bei Routern beobachten, die für den Privatgebrauch gedacht sind, aber in kleinen Zweigstellen bereitgestellt werden. Das Problem lässt sich dadurch beseitigen, dass die Kontokonfiguration der Verbindung für Wählen bei Bedarf angepasst wird.

*Tim Quinn, Support Escalation Engineer
Enterprise Platform Support*

Routenaktualisierungen für bei Bedarf herzustellende Verbindungen

Typische Routingprotokolle verbreiten Routinginformationen, indem sie regelmäßig Nachrichten aus-senden. Zum Beispiel gibt RIP (Routing Information Protocol) für IPv4 den Inhalt seiner Routing-tabelle alle 30 Sekunden auf allen Schnittstellen bekannt. Dieses Verhalten ist bei dauerhaft verbun-denen LAN- oder WAN-Leitungen kein Problem. Aber bei DFÜ-WAN-Leitungen, die bei Aktivität automatisch aufgebaut werden, kann dieses Verhalten bewirken, dass der Router alle 30 Sekunden den anderen Router anruft. Die entstehende Telefonrechnung könnte bei der Buchhaltung für Missfallen sorgen. Daher sollten Sie Routingprotokolle nicht über zeitweise aufgebaute DFÜ-WAN-Leitungen betreiben.

Falls Sie keine Routingprotokolle einsetzen, um die Routingtabellen der VPN-Router zu aktualisieren, müssen Sie die Routen als statische Routen hinzufügen. Die statischen Routen, die den IPv4- oder IPv6-Adresspräfixen entsprechen, die über eine Schnittstelle für Wählen bei Bedarf zur Verfügung stehen, können von Hand oder automatisch konfiguriert werden. Die automatische Eintragung von statischen IPv4-Routen für Schnittstellen für Wählen bei Bedarf wird als *autostatische Aktualisierung*

(engl. autostatic update) bezeichnet. Sie wird unterstützt, wenn Sie in Routing und RAS das Routingprotokoll RIP für IPv4 konfigurieren.

Wenn eine Schnittstelle für Wählen bei Bedarf für autostatische Aktualisierungen konfiguriert ist und die entsprechende Anweisung bekommt, sendet sie eine RIP-für-IPv4-Anforderung über eine aktive Verbindung, mit der sie alle Routen der Router auf der anderen Seite der Verbindung anfordert. Die Antwort auf diese Anforderung wird ausgewertet und die entsprechenden IPv4-Routen der abgefragten Router werden automatisch als statische Routen in die Routingtabelle des anfordernden Routers eingetragen. Die statischen Routen sind dauerhaft, das heißt, sie bleiben auch dann in der Routingtabelle, wenn die Schnittstelle die Verbindung unterbricht oder der Router neu gestartet wird. Eine autostatische Aktualisierung ist ein einmaliger, unidirektionaler Austausch von Routinginformationen.

Weitere Informationen finden Sie im Abschnitt »Konfigurieren der Infrastruktur für die Standortverbindungen« weiter unten in diesem Kapitel.



Hinweis Das »auto« in »autostatisch« bezieht sich darauf, dass die benötigten Routen automatisch als statische Routen zur Routingtabelle hinzugefügt werden. Das Anfordern von Routen wird durch eine explizite Aktion eingeleitet, entweder im Snap-In *Routing und RAS* oder mit einem Netsh-Befehl, während die Verbindung über die Schnittstelle für Wählen bei Bedarf aufgebaut ist. Autostatische Aktualisierungen werden nicht jedes Mal automatisch durchgeführt, wenn eine bei Bedarf herzustellende Wählverbindung aufgebaut wird.

Bei Bedarf hergestellte und persistente Verbindungen

Eine Standort-zu-Standort-VPN-Verbindung kann eine bei Bedarf hergestellte oder eine persistente Verbindung sein:

- Eine bei Bedarf hergestellte Standort-zu-Standort-Verbindung wird aufgebaut, wenn Verkehr über die Verbindung weitergeleitet werden muss und die Verbindung noch nicht besteht. Eine Verbindung kann automatisch aufgebaut werden, wenn Sie auf dem anrufenden Router statische Routen konfigurieren, die eine bei Bedarf herzustellende Wählverbindung aufbauen. Wenn Verkehr über die Route weitergeleitet werden muss, wird die Verbindung aufgebaut und der Verkehr wird weitergeleitet. Bei Bedarf hergestellte Verbindungen werden nach der eingestellten Leerlaufzeit wieder beendet. Weitere Informationen über das Konfigurieren der Trennung nach einer bestimmten Leerlaufzeit finden Sie im Abschnitt »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.
- Eine persistente (dauerhafte) Standort-zu-Standort-Verbindung ist immer verbunden. Falls die Verbindung getrennt wird, wird sofort versucht, sie wieder aufzubauen. Weitere Informationen über das Konfigurieren einer persistenten Verbindung finden Sie im Abschnitt »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.

In der Standardeinstellung arbeitet eine Schnittstelle für Wählen bei Bedarf mit Verbindungen bei Bedarf, die nach 5 Minuten Leerlauf getrennt werden.

Bedingungen für das Aufbauen einer bei Bedarf hergestellten Verbindung

Sie können verhindern, dass anrufende Router unnötige Verbindungen bei Bedarf aufbauen. Es stehen folgende Möglichkeiten zur Verfügung, um einzuschränken, wann der anrufende Router Standort-zu-Standort-VPN-Verbindungen aufbaut:

- **Filter für Wählen bei Bedarf** Mit Filtern für Wählen bei Bedarf (engl. demand-dial filtering) können Sie steuern, für welche Arten von IPv4- oder IPv6-Verkehr eine bei Bedarf herzustellende

Wählverbindung aufgebaut wird und für welche nicht. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.

- **Hinauswählzeiten** Mit Hinauswählzeiten können Sie festlegen, zu welchen Zeiten ein anrufender Router eine Standort-zu-Standort-VPN-Verbindung aufbauen darf und wann nicht. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.

Sie können außerdem mithilfe von Netzwerkrichtlinien konfigurieren, zu welchen Zeiten der antwortende Router eingehende bei Bedarf herzustellende Wählverbindungen annehmen darf.

Bidirektional und unidirektional aufgebaute Verbindungen

Bei bidirektional aufgebauten Verbindungen (engl. two-way initiated connection) kann jeder VPN-Router der anrufende Router oder der antwortende Router sein. Welche Rolle ein Router jeweils einnimmt, hängt lediglich davon ab, wer die Verbindung aufbaut. Beide VPN-Router müssen so konfiguriert sein, dass sie eine Standort-zu-Standort-VPN-Verbindung aufbauen und annehmen. Sie können bidirektional aufgebaute Verbindungen verwenden, wenn die Standort-zu-Standort-VPN-Verbindung nicht rund um die Uhr aktiv ist und Verkehr von beiden Routern den Aufbau einer Verbindung auslösen soll. Für bidirektional aufgebaute Standort-zu-Standort-VPN-Verbindungen gelten folgende Anforderungen:

- Beide VPN-Router müssen über eine permanente WAN-Verbindung mit dem Internet verbunden sein.
- Beide VPN-Router müssen als LAN-Router und Router für Wählen bei Bedarf konfiguriert sein.
- Es müssen Benutzerkonten für beide VPN-Router hinzugefügt werden, damit der antwortende Router die Authentifizierungsanmeldeinformationen des anrufenden Routers überprüfen kann.
- Auf beiden Routern müssen Schnittstellen für Wählen bei Bedarf vollständig konfiguriert werden, und zwar unter demselben Namen wie das Benutzerkonto, das der anrufende Router verwendet. Dazu gehören Einstellungen für Hostname, Anmeldeinformationen für das Benutzerkonto und die IPv4- oder IPv6-Adresse des antwortenden Routers.

Tabelle 13.1 zeigt eine Beispielkonfiguration für bidirektional aufgebaute bei Bedarf herzustellende Routingverbindungen zwischen Router 1, einem bei Bedarf wählenden Router im Standort *Seattle* einer Organisation, und Router 2, einem bei Bedarf wählenden Router im Standort *New York*.

Tabelle 13.1 Beispielkonfiguration für bidirektional aufgebaute bei Bedarf herzustellende Routingverbindungen

Router	Name der Schnittstelle für Wählen bei Bedarf	Benutzerkontoname in den Benutzeranmeldeinformationen
Router 1	DD_NewYork	DD_Seattle
Router 2	DD_Seattle	DD_NewYork

Beachten Sie, dass der Name des Benutzerkontos in den Benutzeranmeldeinformationen der Schnittstelle für Wählen bei Bedarf eines Routers dem Namen der Schnittstelle für Wählen bei Bedarf auf dem anderen Router entspricht.

Bei unidirektional aufgebauten Verbindungen (engl. one-way initiated connection) ist immer der eine VPN-Router der anrufende Router, und der andere VPN-Router ist immer der antwortende Router. Unidirektional aufgebaute Verbindungen eignen sich gut für eine speichenförmige Topologie mit dauerhaften Verbindungen. Bei einer solchen Topologie ist der Zweigstellenrouter (am Ende einer Speiche) der einzige Router, der die Verbindung zum Hauptstellenrouter (in der Achse) aufbaut. Für unidirektional aufgebaute Verbindungen gelten folgende Anforderungen:

- Beide VPN-Router müssen als LAN-Router und Router für Wählen bei Bedarf konfiguriert sein.
- Es muss ein Benutzerkonto mit den Authentifizierungsanmeldeinformationen des anrufenden Routers hinzugefügt werden, das der antwortende Router überprüfen kann.
- Auf dem antwortenden Router muss eine Schnittstelle für Wählen bei Bedarf konfiguriert werden, und zwar unter demselben Namen wie das Benutzerkonto, das der anrufende Router verwendet. Diese Schnittstelle für Wählen bei Bedarf wird nicht benutzt, um eine Verbindung aufzubauen, daher braucht sie nicht mit Hostname, Benutzerkontoanmeldeinformationen und IPv4- oder IPv6-Adresse des anrufenden Routers konfiguriert zu werden.

Komponenten von Windows-Standort-zu-Standort-VPNs

Abbildung 13.1 zeigt die Komponenten von Standort-zu-Standort-VPNs in einer Windows-Umgebung.

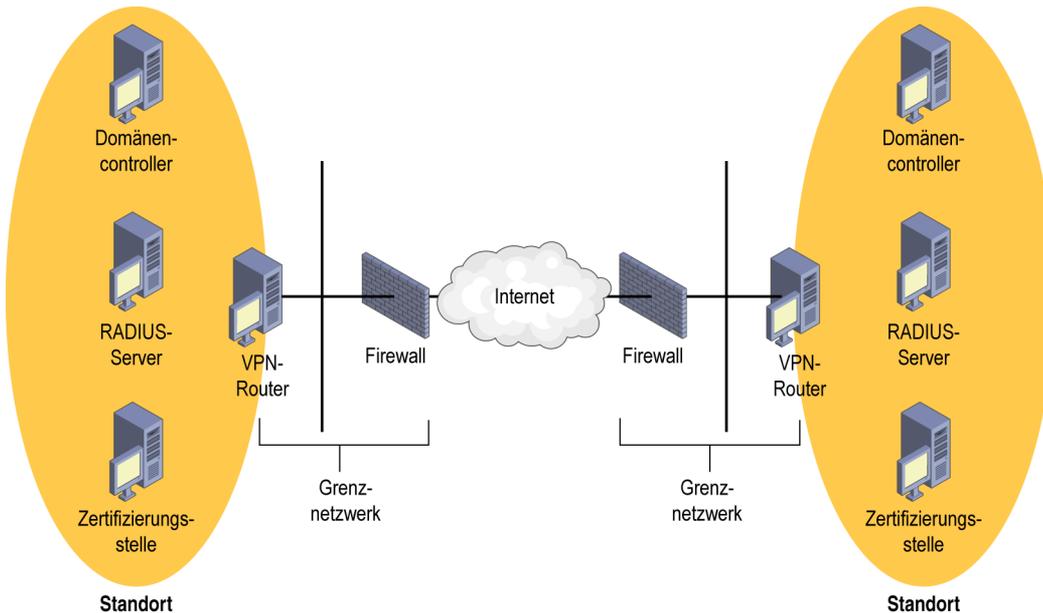


Abbildung 13.1 Komponenten von Standort-zu-Standort-VPNs in einer Windows-Umgebung

Die Komponenten sind:

- **VPN-Router** VPN-Routern bauen als anrufende Router Standort-zu-Standort-VPN-Verbindungen zu antwortenden Routern auf und leiten Pakete über eine bei Bedarf herzustellende VPN-Wählverbindung. Als antwortende Router nehmen sie Standort-zu-Standort-VPN-Verbindungsversuche an, erzwingen die Authentifizierungs- und Verbindungsanforderungen und leiten Pakete über die bei Bedarf herzustellende VPN-Wählverbindung weiter.
- **RADIUS-Server** RADIUS-Server stellen für antwortende Router, Remotezugriff-VPN-Server und andere Arten von Zugriffsservern eine zentralisierte Authentifizierungs- und Autorisierungsverarbeitung sowie Kontoführung für Netzwerkzugriffsversuche zur Verfügung.
- **Active Directory-Domänencontroller** Active Directory-Domänencontroller überprüfen die Benutzeranmeldeinformationen im Rahmen der Authentifizierung und stellen antwortenden Routern Benutzerkontoinformationen für die Durchführung der Autorisierung zur Verfügung.

- **Zertifizierungsstellen** Zertifizierungsstellen sind Teil der PKI. Sie stellen Computer- oder Benutzerzertifikate für anrufende Router und Computerzertifikate für antwortende Router und RADIUS-Server aus, die bei der Authentifizierung von Standort-zu-Standort-VPN-Verbindungen verwendet werden.

Planungs- und Entwurfsaspekte

Beim Bereitstellen einer Standort-zu-Standort-VPN-Lösung müssen Sie folgende Planungs- und Entwurfsfragen beantworten:

- VPN-Protokolle
- Authentifizierungsmethoden
- VPN-Router
- Internetinfrastruktur
- Standortnetzwerkinfrastruktur
- Authentifizierungsinfrastruktur
- PKI

VPN-Protokolle

Windows Server 2008 unterstützt folgende Standort-zu-Standort-VPN-Protokolle:

- **PPTP** PPTP benutzt PPP-Benutzerauthentifizierung und MPPE-Verschlüsselung. Wenn MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol) in Kombination mit starken Kennwörtern eingesetzt wird, ist PPTP eine sichere VPN-Technologie. Für zertifikatbasierte Authentifizierung kann EAP-TLS mit Registrierungszertifikaten kombiniert werden. PPTP ist einfach bereitzustellen und kann über die meisten NATs (Network Address Translator) geleitet werden.
- **L2TP/IPsec** L2TP benutzt PPP-Benutzerauthentifizierung und IPsec-Verschlüsselung. L2TP/IPsec verwendet in der Standardeinstellung Zertifikate und den IPsec-Computerauthentifizierungsprozess, um die geschützte IPsec-Sitzung auszuhandeln, und danach die PPP-Benutzerauthentifizierung. L2TP/IPsec ist sicherer als PPTP.

Ein neues Feature von L2TP/IPsec in Windows Server 2008 ist die Verifizierung der Felder *Alternativer Antragstellername* und *Erweiterte Schlüsselverwendung* aus dem Computerzertifikat des antwortenden Routers. Das hilft dabei, Man-in-the-Middle-Angriffe zu erkennen. Dieses Feature ist in der Standardeinstellung aktiviert. Sie können es im Eigenschaftendialogfeld einer bei Bedarf herzustellenden Wählverbindung auf der Registerkarte *Netzwerk* konfigurieren, indem Sie mit der Schaltfläche *IPSec-Einstellungen* das gleichnamige Dialogfeld öffnen.

Entwurfsmöglichkeiten für VPN-Protokolle

- Wenn MS-CHAP v2 für die Authentifizierung benutzt wird, benötigt PPTP keine PKI, um Zertifikate an jeden VPN-Router auszustellen.
- PPTP bietet Vertraulichkeit der Daten für alle Pakete. PPTP-VPN-Verbindungen bieten keine Datenintegrität oder Authentifizierung der Datenherkunft.
- L2TP/IPsec bietet für jedes Paket Vertraulichkeit der Daten (Verschlüsselung), Datenintegrität (Beweis, dass die Daten nicht während der Übertragung geändert wurden) und Authentifizierung

der Datenherkunft (Beweis, dass die Daten vom autorisierten Benutzer stammen). L2TP/IPsec bietet viel besseren Schutz für VPN-Pakete als PPTP.

- In der Standardeinstellung unterstützt ein Windows Server 2008-VPN-Router für Standort-zu-Standort-VPN-Verbindungen PPTP und L2TP/IPsec. Sie können für einige VPN-Verbindungen (zum Beispiel von anrufenden Routern, bei denen kein Computerzertifikat installiert ist) PPTP einsetzen und für andere Verbindungen (zum Beispiel von anrufenden Routern, die ein Computerzertifikat installiert haben) L2TP/IPsec.
- Falls Sie beide VPN-Protokolle verwenden, können Sie separate Netzwerkrichtlinien erstellen, die unterschiedliche Verbindungseinstellungen für PPTP- oder L2TP/IPsec-Verbindungen definieren.

Anforderungen an VPN-Protokolle

- Verschlüsselte PPTP-Wählverbindungen benötigen die Authentifizierungsprotokolle MS-CHAP v2 oder EAP-TLS.
- PPTP-basierte anrufende Router können hinter einem NAT liegen, falls das NAT einen NAT-Editor enthält, der weiß, wie PPTP-getunnelte Daten richtig umgesetzt werden müssen. Zum Beispiel enthalten die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing, ICS) des Ordners *Netzwerkverbindungen* und die NAT-Routingprotokollkomponente von Routing und RAS einen NAT-Editor, der PPTP-Verkehr zu und von PPTP-Clients, die hinter dem NAT liegen, richtig umsetzen kann. Antwortende Router dürfen nicht hinter einem NAT liegen, sofern es nicht mehrere öffentliche IP-Adressen gibt und eine öffentliche IP-Adresse 1:1 der privaten IP-Adresse des antwortenden Routers zugeordnet ist. Falls es nur eine einzige öffentliche Adresse gibt, muss das NAT so konfiguriert sein, dass es die PPTP-getunnelten Daten zum antwortenden Router umsetzt und weiterleitet. Die meisten NATs, die eine einzige öffentliche Adresse nutzen (zum Beispiel ICS und die NAT-Routingprotokollkomponente), können so konfiguriert werden, dass sie eingehenden Verkehr anhand der IP-Adresse und TCP- und UDP-Ports erlauben. PPTP-getunnelte Daten verwenden aber keine TCP- oder UDP-Header. Daher darf ein antwortender Router nicht hinter einem Computer liegen, auf dem ICS oder die NAT-Routingprotokollkomponente laufen, wenn lediglich eine einzige öffentliche IPv4-Adresse benutzt wird.
- L2TP/IPsec-basierte anrufende Router dürfen nur dann hinter einem NAT liegen, wenn beide Router IPsec NAT-T (NAT-Traversal) unterstützen. IPsec NAT-T wird in den Betriebssystemen Windows Server 2008 und Windows Server 2003 unterstützt. L2TP/IPsec-basierte antwortende Router dürfen nicht hinter einem NAT liegen.
- L2TP/IPsec unterstützt standardmäßig Computerzertifikate, dies ist die empfohlene Authentifizierungsmethode für IPsec. Eine Computerzertifikatsauthentifizierung setzt eine PKI voraus, damit Computerzertifikate für die VPN-Routercomputer ausgestellt werden können.
- Falls Sie VPN-Wählverbindungen über das IPv6-Internet einsetzen wollen, müssen Sie L2TP/IPsec benutzen. Weitere Informationen finden Sie im Abschnitt »So funktioniert's: IPv6 und VPN-Verbindungen« weiter unten in diesem Kapitel.

Empfohlene Vorgehensweise für VPN-Protokolle

- Falls Sie bereits eine PKI haben, sollten Sie L2TP/IPsec verwenden.
- L2TP/IPsec-Verbindungen unterstützen auch eine Authentifizierung mithilfe von vorinstallierten Schlüsseln. Ein vorinstallierter Schlüssel ist eine Zeichenfolge, die auf den anrufenden und den antwortenden Routern eingetragen wird. Vorinstallierte Schlüssel sind eine relativ unsichere Authentifizierungsmethode. Daher wird empfohlen, die Authentifizierung mit vorinstallierten Schlüsseln nur zu verwenden, während Ihre PKI bereitgestellt wird oder wenn VPN-Router von

Fremdherstellern eine Authentifizierung durch vorinstallierte Schlüssel benötigen. Sie können die Authentifizierung durch vorinstallierte Schlüssel für den anrufenden Router im Eigenschaftendialogfeld einer bei Bedarf herzustellenden Wählverbindung auf der Registerkarte *Netzwerk* aktivieren, indem Sie mit der Schaltfläche *IPSec-Einstellungen* das gleichnamige Dialogfeld öffnen. Sie können die Authentifizierung durch vorinstallierte Schlüssel für den antwortenden Router im Snap-In *Routing und RAS* im Eigenschaftendialogfeld eines Servers auf der Registerkarte *Sicherheit* aktivieren.

So funktioniert's: IPv6 und VPN-Verbindungen

Windows Server 2008 und Windows Vista bieten erweiterte Unterstützung für IPv6, das in der Standardeinstellung installiert und aktiviert ist. Nativer IPv6-Betrieb wird von praktisch allen Netzwerkanwendungen und -diensten unterstützt, die in Windows Server 2008 und Windows Vista enthalten sind. Für Standort-zu-Standort-VPN-Verbindungen bieten Windows Server 2008 und Windows Vista folgende Unterstützung für IPv6-Verkehr:

- IPv4-getunnelter IPv6-Verkehr
- Nativer IPv6-Verkehr innerhalb des VPN-Tunnels
- VPN-Verbindungen über IPv6

IPv4-getunnelter IPv6-Verkehr

Mit Windows Server 2003 können Sie IPv6-Verkehr über eine Standort-zu-Standort-VPN-Verbindung senden, aber nur, wenn er bereits mit einem IPv4-Header gekapselt ist. IPv4-Tunnel für IPv6-Verkehr sind ein Mechanismus, der von IPv6-Übergangstechnologien eingesetzt wird, zum Beispiel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), um IPv6-Konnektivität zwischen IPv6/IPv4-Hosts über ein Intranet zur Verfügung zu stellen, das nur IPv4-Routing unterstützt.

Bei der Unterstützung von IPv4-getunneltem IPv6-Verkehr kann ein anrufender Router eine Standort-zu-Standort-VPN-Verbindung über das IPv4-Internet aufbauen und dann IPv4-getunnelten IPv6-Verkehr weiterleiten. IPv4-getunnelter IPv6-Verkehr, der über eine Standort-zu-Standort-VPN-Verbindung gesendet wird, hat folgenden Aufbau:

- IPv6-Pakete sind in einen IPv4-Header gekapselt (das ist der IPv4-Tunnel). Diese Pakete sind wiederum in einem PPP-Header und einem VPN-Protokollheader (zum Beispiel PPTP oder L2TP/IPsec) gekapselt, und diese wiederum in einem letzten IPv4-Header. So ist es möglich, die Pakete durch das IPv4-Internet zu befördern.

PPTP und L2TP/IPsec in Windows Server 2008 unterstützen IPv4-getunnelten IPv6-Verkehr. IPv4-getunnelter IPv6-Verkehr, der über eine VPN-Verbindung gesendet wird, setzt IPCP-Unterstützung (Internet Protocol Control Protocol) auf den VPN-Routern und eine IPv6-Übergangstechnologieinfrastruktur (zum Beispiel ISATAP) im Intranet voraus. IPCP ist ein PPP-Netzwerksteuerungsprotokoll, das es PPP-Hosts erlaubt, Einstellungen für die Nutzung von IPv4 über eine PPP-Verbindung zu konfigurieren.

Nativer IPv6-Verkehr innerhalb des VPN-Tunnels

Windows Server 2008 unterstützt VPN-Verbindungen mit nativem IPv6-Verkehr innerhalb des VPN-Tunnels. Der anrufende Router baut eine Standort-zu-Standort-VPN-Verbindung mit einem antwortenden Router über das IPv4-Internet auf und handelt dann die Verwendung von IPv6 über die PPP-Verbindung aus. IPv6-Pakete werden vom VPN-Protokoll innerhalb des VPN-Tunnels

gekapselt. Bei nativer Unterstützung für IPv6-Verkehr innerhalb des VPN-Tunnels kann ein VPN-Router eine Standort-zu-Standort-VPN-Verbindung über das IPv4-Internet aufbauen und dann nativen IPv6-Verkehr durch die VPN-Verbindung weiterleiten.

Nativer IPv6-Verkehr innerhalb des VPN-Tunnel hat folgenden Aufbau:

- IPv6-Pakete sind in einem PPP-Header und einem VPN-Protokollheader gekapselt, und diese wiederum in einem letzten IPv4-Header. So ist es möglich, die Pakete durch das IPv4-Internet zu befördern.

Nativer IPv6-Verkehr innerhalb des VPN-Tunnels setzt IPV6CP-Unterstützung (IPv6 Routing und Internet Protocol Version 6 Control Protocol) auf den VPN- Routern und eine native IPv6-Routing-Infrastruktur im Intranet voraus. PPTP und L2TP/IPsec in Windows Server 2008 unterstützen nativen IPv6-Verkehr innerhalb des VPN-Tunnels. IPV6CP ist ein PPP-Netzwerksteuerungsprotokoll, das es PPP-Hosts erlaubt, Einstellungen für die Nutzung von IPv6 über eine PPP-Verbindung zu konfigurieren.



Hinweis Windows Server 2003 unterstützt keinen nativen IPv6-Verkehr innerhalb des VPN-Tunnels.

VPN-Verbindungen über IPv6

Windows Server 2008 unterstützt auch Standort-zu-Standort-VPN-Verbindungen über IPv6. Der VPN-Client baut über das IPv6-Internet eine VPN-Verbindung zu einem VPN-Server auf und handelt dann die Verwendung von IPv6 oder IPv4 über die PPP-Verbindung aus. Wenn VPN-Verbindungen über IPv6 unterstützt werden, können VPN-Router Standort-zu-Standort-VPN-Verbindungen über das IPv6-Internet aufbauen und dann nativen IPv6- oder IPv4-Verkehr über die Verbindung weiterleiten.

Pakete für VPN-Verbindungen über IPv6 haben folgenden Aufbau:

- IPv6- oder IPv4-Pakete sind in einem PPP-Header und einem VPN-Protokollheader gekapselt, und diese wiederum in einem letzten IPv6-Header. So ist es möglich, die Pakete durch das IPv6-Internet zu befördern.

L2TP/IPsec in Windows Server 2008 unterstützt Standort-zu-Standort-VPN-Verbindungen über IPv6. VPN-Verbindungen über IPv6 setzen native IPv6-Unterstützung für VPN-Protokolle auf den VPN-Routern, IPv6-Routingunterstützung auf den VPN-Routern und Verbindungen ins IPv6-Internet voraus.

Native IPv6-Fähigkeit für Standort-zu-Standort-VPN-Verbindungen (also die Fähigkeit, native IPv6-Pakete über eine Standort-zu-Standort-VPN-Verbindung zu senden) ist bei nativem IPv6-Verkehr innerhalb des VPN-Tunnels und VPN-Verbindungen über IPv6 gegeben.



Hinweis Windows Server 2003 bietet keine Unterstützung für VPN-Verbindungen über IPv6 oder native IPv6-Fähigkeiten für Standort-zu-Standort-VPN-Verbindungen.

Authentifizierungsmethoden

Zum Authentifizieren des anrufenden Routers, der versucht, eine VPN-Verbindung aufzubauen, unterstützt Windows Server 2008 eine Vielzahl von Authentifizierungsprotokollen, darunter folgende:

- **MS-CHAP v2** MS-CHAP v2 ist eine Authentifizierungsmethode, die mit Kennwörtern arbeitet und gegenseitige Authentifizierung bietet.
- **EAP-TLS** EAP-TLS ist eine zertifikatbasierte Authentifizierungsmethode, die in Kombination mit einer PKI eingesetzt wird. EAP-TLS bietet ebenfalls gegenseitige Authentifizierung. Bei EAP-TLS sendet der anrufende Router sein Benutzerzertifikat für die Authentifizierung, und der Authentifizierungsserver (entweder der antwortende Router oder ein RADIUS-Server) sendet ein Computerzertifikat für die Authentifizierung.



Hinweis In Windows Server 2008 wurde die Unterstützung für MS-CHAP (Microsoft Challenge Handshake Authentication Protocol, auch als MS-CHAP v1 bezeichnet), SPAP (Shiva Password Authentication Protocol) und EAP-MD5 (EAP-Message Digest 5) aus Sicherheitsgründen entfernt. Anders als bei Remotezugriff-VPN-Verbindungen bietet Windows Server 2008 bei Standort-zu-Standort-VPN-Verbindungen keine Unterstützung für die Verwendung der Authentifizierungsprotokolle EAP-MS-CHAP v2, PEAP-TLS (Protected EAP) oder PEAP-MS-CHAP v2.

Entwurfsmöglichkeiten für Authentifizierungsprotokolle

- Falls Sie bereits eine PKI haben, sollten Sie EAP-TLS für Ihre Standort-zu-Standort-VPN-Verbindungen verwenden. Falls keine PKI bereitgestellt wurde oder dies für Ihr Netzwerk nicht machbar ist, sollten Sie MS-CHAP v2 verwenden.
- EAP-TLS ist viel sicherer als MS-CHAP v2, weil es nicht mit Kennwörtern arbeitet und wesentlich widerstandsfähiger gegenüber Offline-Wörterbuchangriffen ist.

Anforderungen an Authentifizierungsprotokolle

- Für verschlüsselte PPTP-Verbindungen müssen Sie MS-CHAP v2 oder EAP-TLS verwenden. Nur diese Authentifizierungsprotokolle bieten einen Mechanismus, um für jede Sitzung einen neuen Verschlüsselungsschlüssel zu generieren, mit dem die VPN-Router die PPTP-Daten verschlüsseln, die über die VPN-Verbindung gesendet werden.
- EAP-TLS setzt eine PKI voraus, um Benutzer- und Computerzertifikate auszustellen.

Empfohlene Vorgehensweise für Authentifizierungsprotokolle

- Falls Sie MS-CHAP v2 verwenden müssen, sollten Sie in Ihrem Netzwerk die Verwendung sicherer Kennwörter verpflichtend machen. Sichere Kennwörter sind lang (mehr als 8 Zeichen) und enthalten eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Interpunktionszeichen. Ein gutes Beispiel für ein sicheres Kennwort beim Benutzerkonto des anrufenden Routers ist »f3L*q02~>xR3w#4o«. In einer Active Directory-Domäne können Sie über den Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinien* in den Gruppenrichtlinieneinstellungen die Verwendung sicherer Benutzerkennwörter vorschreiben.
- Bei EAP-TLS überprüft der anrufende Router in der Standardeinstellung das Computerzertifikat des antwortenden Routers. Sie können anrufende Router so konfigurieren, dass sie das Zertifikat des Authentifizierungsservers nicht überprüfen. Dann sind auf den Authentifizierungsservern keine Computerzertifikate erforderlich. Es wird allerdings empfohlen, dass anrufende Router das Zertifikat des Authentifizierungsservers überprüfen, damit eine gegenseitige Authentifizierung des

anrufenden Routers und des Authentifizierungsservers gewährleistet ist. Das hilft zu verhindern, dass der anrufende Router sich gegenüber einem eingeschleusten Authentifizierungsserver authentifiziert.

- Bei L2TP/IPsec-Verbindungen können Sie jedes beliebige Benutzerauthentifizierungsprotokoll verwenden, weil die Authentifizierung stattfindet, nachdem die VPN-Router einen IPsec-geschützten Kanal eingerichtet haben. Es wird allerdings empfohlen, EAP-TLS oder MS-CHAP v2 zu verwenden, um sichere Benutzerauthentifizierung und gegenseitige Authentifizierung mit dem Authentifizierungsserver zu gewährleisten.

VPN-Router

VPN-Router bauen VPN-Wählverbindungen auf oder nehmen sie entgegen. Ein anrufender Router erfüllt folgende Aufgaben:

- Er baut VPN-Verbindungen für eine persistente Verbindung aufgrund der Aktion eines Administrators oder beim Empfang eines weitergeleiteten Pakets auf, das über eine Route geleitet werden muss, die über die VPN-Schnittstelle für Wählen bei Bedarf führt.
- Er wartet, bis Authentifizierung und Autorisierung durchgeführt wurden, bevor er Pakete weiterleitet.
- Er agiert als Router, der Pakete zwischen Knoten in seinem Standort und Knoten im Standort des antwortenden Routers weiterleitet.

Ein antwortender Router erfüllt folgende Aufgaben:

- Er nimmt VPN-Verbindungsversuche entgegen.
- Er authentifiziert und autorisiert VPN-Verbindungen, bevor er erlaubt, Daten auszutauschen.
- Er agiert als Router, der Pakete zwischen Knoten in seinem Standort und Knoten im Standort des anrufenden Routers weiterleitet.

Konfigurieren von Routing und RAS

Wenn Sie Routing und RAS konfigurieren und aktivieren, fordert der Setup-Assistent für den Routing- und RAS-Server Sie auf, auszuwählen, welche Rolle der Computer wahrnimmt. Für VPN-Server müssen Sie die Konfigurationsoption *RAS (DFÜ oder VPN)* wählen. Wenn die Option *RAS (DFÜ oder VPN)* ausgewählt wurde, ist der Routing- und RAS-Server so konfiguriert, dass er sowohl Remotezugriff- als auch Standort-zu-Standort-VPN-Verbindungen unterstützt.



Hinweis Microsoft empfiehlt, im Setup-Assistenten für den Routing- und RAS-Server statt der Option *Sichere Verbindung zwischen zwei privaten Netzwerken* die Option *RAS (DFÜ oder VPN)* zu wählen, weil Sie bei der Option *Sichere Verbindung zwischen zwei privaten Netzwerken* nicht aufgefordert werden, die Internetschnittstelle auszuwählen, für die automatisch Paketfilter für den VPN-Verkehr konfiguriert werden. Sie werden auch nicht aufgefordert, RADIUS-Server zu konfigurieren. Und schließlich werden bei Auswahl dieser Option nur eine beschränkte Zahl von PPTP- und L2TP-Ports erstellt.

Wenn Sie im Setup-Assistenten für den Routing- und RAS-Server die Option *RAS (DFÜ oder VPN)* auswählen, können Sie folgende Konfigurationseinstellungen vornehmen:

1. Sie müssen zuerst angeben, ob VPN, DFÜ oder beide Zugriffsarten benötigt werden.
2. Anschließend müssen Sie auswählen, welche Netzwerkschnittstelle mit dem Internet verbunden ist. In der Standardeinstellung werden für die hier ausgewählte Schnittstelle automatisch Paketfilter konfiguriert, die ausschließlich VPN-Verkehr zulassen. Jeglicher andere Verkehr wird still-

schweigend verworfen. Zum Beispiel können Sie keinen Ping-Test mehr für die Internetschnittstelle des VPN-Routers durchführen.

3. Falls mehrere Netzwerkkarten mit dem Intranet verbunden sind, müssen Sie anschließend auswählen, über welche Schnittstelle die DHCP-, DNS- und WINS-Konfiguration abgerufen wird.
4. Anschließend müssen Sie angeben, ob Sie die IPv4-Adressen, die anrufenden Routern und Remotezugriffsclients zugewiesen werden, mit DHCP abrufen oder als Adressbereich definieren wollen. Falls Sie einen Adressbereich verwenden wollen, müssen Sie die gewünschten Adressbereiche hinzufügen.
5. Anschließend müssen Sie angeben, ob Sie RADIUS für die Authentifizierung und Kontoführung der VPN-Verbindungen verwenden wollen. Falls Sie RADIUS wählen, müssen Sie Namen, IPv4-Adressen oder IPv6-Adressen der primären und alternativen RADIUS-Server und den gemeinsamen geheimen Schlüssel für RADIUS konfigurieren.

Wenn Sie im Setup-Assistenten für den Routing- und RAS-Server die Option *RAS (DFÜ oder VPN)* auswählen und konfigurieren, werden folgende Änderungen an der Konfiguration des Systems durchgeführt:

- Der Routing- und RAS-Dienst wird als IPv4-RAS-Server, LAN-Router und Router für Wählen bei Bedarf aktiviert. Er führt die Authentifizierung und Kontoführung entweder lokal oder über RADIUS durch.
- Falls nur eine einzige Netzwerkkarte mit dem Intranet verbunden ist, wird automatisch diese Netzwerkkarte verwendet, um die DHCP-, DNS- und WINS-Konfiguration abzurufen. Andernfalls wird die Netzwerkkarte verwendet, die im Assistenten angegeben wurde.
- Falls IPv4-Adressbereiche für die VPN-Schnittstellen der anrufenden Router angegeben wurden, werden sie konfiguriert.
- Entweder Windows oder RADIUS wird so konfiguriert, dass es die Authentifizierung und Kontoführung von VPN-Verbindungsversuchen durchführt.
- Abhängig von der Windows Server 2008-Version werden bis zu 128 PPTP-Ports und 128 L2TP-Ports erstellt. Jeder Port steht für eine mögliche Remotezugriff-VPN-Verbindung. Alle lassen sowohl eingehende Remotezugriffsverbindungen als auch ein- und ausgehende bei Bedarf herzustellende Wahlverbindungen zu (für Standort-zu-Standort-VPN-Verbindungen).
- Die ausgewählte Internetschnittstelle wird mit eingehenden und ausgehenden IPv4- und IPv6-Paketfiltern konfiguriert, die ausschließlich VPN-Verkehr zulassen.
- Die DHCP-Relay-Agent-Komponente wird zur internen Schnittstelle hinzugefügt. Die *interne Schnittstelle* ist eine logische Schnittstelle, die die Verbindung zu allen anderen authentifizierten Remotezugriffsclients bildet. Der DHCP-Relay-Agent wird für Standort-zu-Standort-VPN-Verbindungen nicht benutzt.
- Die IGMP-Komponente (Internet Group Management Protocol) wird hinzugefügt und die interne Schnittstelle wird für den IGMP-Routermodus konfiguriert. Alle anderen LAN-Schnittstellen werden für den IGMP-Proxymodus konfiguriert. Das erlaubt es VPN-Routern, IPv4-Multicastverkehr über die Schnittstelle für Wählen bei Bedarf weiterzuleiten.



Weitere Informationen Weitere Informationen finden Sie in der Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>.

Entwurfsmöglichkeiten für VPN-Router

- Der VPN-Router kann so konfiguriert werden, dass er IPv4-Adressen über DHCP abrufen oder von Hand konfigurierte Adressbereiche (die sogenannten *statischen Pools* mit Adressen) verwendet. Wird DHCP benutzt, um IPv4-Adressen abzurufen, vereinfacht das die Konfiguration. Sie müssen dann aber sicherstellen, dass der DHCP-Bereich für das Subnetz, in dem sich die Intranetverbindung des VPN-Routers befindet, genug Adressen für alle Computer, die direkt an das Subnetz angeschlossen sind, plus die maximale Zahl von PPTP- und L2TP-Ports hat.

Falls es in Ihrem statischen Pool nicht genug Adressen gibt, können anrufende Router trotzdem eine Verbindung aufbauen. Anrufende und antwortende Router fordern während des Verbindungsaufbauvorgangs jeweils eine IPv4-Adresse vom anderen Router an. Aber falls einer der Router keine Adresse mehr übrig hat, die er zuweisen könnte, setzen beide Router den Verbindungsaufbauvorgang fort. Die VPN-Schnittstelle in der Punkt-zu-Punkt-Verbindung hat keine IPv4-Adresse zugewiesen. Dies wird als eine *unnummerierte Verbindung* bezeichnet. VPN-Router, die unter Windows Server 2008 laufen, unterstützen zwar unnummerierte Verbindungen, aber die Routingprotokollkomponente für RIP über IPv4 innerhalb von Routing und RAS funktioniert nicht über eine unnummerierte Verbindung.

- Der antwortende Router kann Authentifizierung und Autorisierung für VPN-Verbindungen entweder selbst erledigen oder dies einem RADIUS-Server überlassen. Wenn Sie einen antwortenden Router konfigurieren, können Sie wählen, ob Sie Windows oder RADIUS für Authentifizierung und Kontoführung einsetzen wollen.

Wenn der antwortende Router so konfiguriert ist, dass Windows Authentifizierung und Kontoführung erledigt, ist er Mitglied einer Active Directory-Domäne und kommuniziert mit einem Active Directory-Domänencontroller, um die Anmeldeinformationen des anrufenden Routers zu überprüfen und die Einwähleigenschaften für das Benutzerkonto des anrufenden Routers zu ermitteln. Der antwortende Router braucht die Benutzerkontoeigenschaften und die lokal konfigurierten Netzwerkrichtlinien, um die VPN-Verbindung zu autorisieren. In der Standardeinstellung protokolliert der antwortende Router Kontoführungsinformationen zur VPN-Verbindung in lokalen Kontoführungsprotokolldateien.

Wenn der antwortende Router so konfiguriert ist, dass er die Authentifizierung und Kontoführung an RADIUS weiterleitet, greift er auf einen konfigurierten RADIUS-Server zurück, um die Anmeldeinformationen des anrufenden Routers zu überprüfen, den Verbindungsversuch zu autorisieren und Kontoführungsinformationen zur VPN-Verbindung zu protokollieren.

- Der Setup-Assistent für den Routing- und RAS-Server aktiviert nicht automatisch die IPv6-Unterstützung für Standort-zu-Standort-VPN-Verbindungen. Weitere Informationen finden Sie in den Abschnitten »Bereitstellen von antwortenden Routern« und »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.
- Falls Sie bei Verbindungen, die nur bei Bedarf aufgebaut werden, verhindern wollen, dass Verbindungen zu bestimmten Tageszeiten oder für bestimmte Verkehrstypen hergestellt werden, können Sie Hinauswählzeiten oder Filter für Wählen bei Bedarf konfigurieren. Klicken Sie dazu mit der rechten Maustaste auf die Netzwerkschnittstelle des anrufenden Routers für Wählen bei Bedarf. Filter für Wählen bei Bedarf werden angewendet, bevor die Verbindung hergestellt wird. IPv4- oder IPv6-Paketfilter werden angewendet, nachdem die Verbindung aufgebaut wurde. Wenn Sie verhindern wollen, dass eine bei Bedarf herzustellende Wählverbindung für Verkehr aufgebaut wird, der von den IPv4- oder IPv6-Paketfiltern verworfen wird, sollten Sie Ihre IPv4- oder IPv6-

Paketfilter auf die Filter für Wählen bei Bedarf abstimmen. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.

Anforderungen an VPN-Router

- Der VPN-Router muss eine manuelle TCP/IP-IPv4-Konfiguration für seine Internetschnittstelle und die Intranetschnittstellen haben. Weil Konflikte bei der Standardroute auftreten könnten, sollten Sie die Intranetschnittstellen von Hand mit IPv4-Adresse, Subnetzmaske, DNS-Servern und WINS-Servern konfigurieren. Konfigurieren Sie aber kein Standardgateway auf den Intranetschnittstellen des VPN-Routers. Der VPN-Router kann selbst eine manuelle TCP/IP-Konfiguration haben, aber trotzdem DHCP verwenden, um die IPv4-Adressen abzurufen, die er den anrufenden Routern zuweist.
- Für VPN-Verbindungen, die mit dem Authentifizierungsprotokoll EAP-TLS arbeiten, müssen Sie auf dem Authentifizierungsserver (entweder dem antwortenden Router oder dem RADIUS-Server) ein Computerzertifikat installieren, das vom anrufenden Router überprüft werden kann. Außerdem müssen Sie auf dem anrufenden Router ein Benutzerzertifikat installieren, das vom Authentifizierungsserver überprüft werden kann.



Hinweis *Computerzertifikate* sind Zertifikate, die im lokalen Computerzertifikatspeicher gespeichert sind und bei denen die Eigenschaften vorhanden sind, die benötigt werden, um eine TLS- oder IPsec-Authentifizierung durchzuführen. Weitere Informationen über Zertifikatanforderungen für TLS-Authentifizierung finden Sie unter <http://go.microsoft.com/fwlink/?LinkID=20016>. Weitere Informationen über Zertifikatanforderungen für IPsec-Authentifizierung finden Sie unter <http://go.microsoft.com/fwlink/?LinkID=67907>.

- Für L2TP/IPsec-Verbindungen, die Zertifikatauthentifizierung verwenden (empfohlen), müssen Sie Computerzertifikate sowohl auf dem antwortenden als auch dem anrufenden Router installieren.
- Falls Sie den antwortenden Router für lokale Authentifizierung oder RADIUS-Authentifizierung konfigurieren und der RADIUS-Server ein Computer ist, der NPS (Network Policy Server, Netzwerkrichtlinienserver) ausführt, weist die Standardnetzwerkrichtlinie mit dem Namen *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver* alle Verbindungsversuche ab, sofern nicht in den Einwähleigenschaften des Benutzerkontos die Netzwerkzugriffsberechtigung den Zugriff gestattet. Falls Sie diese Netzwerkrichtlinie für Ihre Standort-zu-Standort-VPN-Verbindungen verwenden wollen, müssen Sie den Richtlinientyp auf *Zugriff gestatten* ändern. Falls Sie Autorisierung und Verbindungseinstellungen für Standort-zu-Standort-VPN-Verbindungen anhand der Gruppe oder des Verbindungstyps verwalten wollen, müssen Sie zusätzliche NPS-Richtlinien konfigurieren. Weitere Informationen finden Sie im Abschnitt »Authentifizierungsinfrastruktur« weiter unten in diesem Kapitel.

Empfohlene Vorgehensweise für VPN-Server

- Legen Sie fest, welche Verbindung des VPN-Routers an das Internet angeschlossen ist. VPN-Router, die an das Internet angebunden sind, haben üblicherweise mindestens zwei LAN-Verbindungen: eine, die mit dem Internet verbunden ist (entweder direkt oder über ein Grenznetzwerk), und eine, die mit dem Intranet der Organisation verbunden ist. Um diesen Unterschied für die Arbeit im Setup-Assistenten für den Routing- und RAS-Server deutlich zu machen, sollten Sie die Verbindungen im Ordner *Netzwerkverbindungen* mit Namen versehen, die ihre Aufgabe oder Rolle beschreiben. Wenn zum Beispiel die Verbindung »LAN-Verbindung« mit dem Standort verbunden

ist, können Sie diese Verbindung in »Standort« umbenennen, und die Verbindung »LAN-Verbindung 2«, die mit dem Internet verbunden ist, in »Internet«.

Internetinfrastruktur

Damit ein anrufender Router erfolgreich Verkehr mit einem antwortenden Router über das Internet austauschen kann, müssen folgende Bedingungen erfüllt sein:

- Der DNS-Name des antwortenden Routers kann aufgelöst werden.
- Der antwortende Router ist erreichbar.
- VPN-Verkehr zu und von beiden VPN-Routern ist zugelassen.

Auflösbarkeit des Namens des antwortenden Routers

In der Schnittstelle für Wählen bei Bedarf des anrufenden Routers geben Sie den antwortenden Router üblicherweise anhand seines vollqualifizierten Domänennamens (Fully Qualified Domain Name, FQDN) an, nicht anhand seiner IPv4- oder IPv6-Adresse. Sie können einen FQDN (zum Beispiel *vpn.example.microsoft.com*) verwenden, sofern der Name in eine IPv4- oder IPv6-Adresse aufgelöst werden kann. Daher müssen Sie sicherstellen, dass der Name, den Sie beim Konfigurieren einer bei Bedarf herzustellenden Wählverbindung als antwortenden Router angeben, in eine IPv4- oder IPv6-Adresse aufgelöst werden kann.

Erreichbarkeit des antwortenden Routers

Damit der antwortende Router erreichbar ist, muss er eine öffentliche IPv4-Adresse oder eine globale IPv6-Adresse haben, an die Pakete durch die Routinginfrastruktur des IPv4- oder IPv6-Internets weitergeleitet werden. Falls Sie von einem Internetprovider oder einer Internetregistrierung eine statische öffentliche IPv4-Adresse zugewiesen bekommen haben, ist das normalerweise kein Problem. Bei manchen Konfigurationen wird der VPN-Server mit einer privaten IPv4-Adresse konfiguriert, hat aber eine öffentliche statische IPv4-Adresse, über die er im Internet erreicht werden kann. Ein Gerät zwischen dem Internet und dem antwortenden Router übersetzt die öffentliche in die tatsächliche IPv4-Adresse des antwortenden Routers, und umgekehrt, wenn Pakete zu und vom antwortenden Router geleitet werden.

Auch wenn die Routinginfrastruktur des IPv4- oder IPv6-Internets die Erreichbarkeit sicherstellt, ist der antwortende Router unter Umständen trotzdem nicht erreichbar, weil Firewalls, Paketfilterungsrouten, NATs, Sicherheitsgateways oder andere Gerätetypen verhindern, dass Pakete vom antwortenden Routercomputer gesendet oder empfangen werden.

VPN-Router und Firewallkonfiguration

Folgende Konfigurationen werden häufig verwendet, um Firewalls mit einem VPN-Router zu kombinieren:

- **Der VPN-Router ist direkt an das Internet angeschlossen, und die Firewall liegt zwischen dem VPN-Router und dem Intranet.** Bei dieser Konfiguration gibt es keine separate Firewall zwischen dem VPN-Server und dem Internet. Der VPN-Server führt seine eigene Paketfilterung durch. Der VPN-Router muss mit Paketfiltern konfiguriert sein, die ausschließlich VPN-Verkehr in und aus seiner Internetschnittstelle erlauben. Die Firewall für das Intranet kann so konfiguriert sein, dass sie bestimmte Typen von Standort-zu-Standort-Verkehr erlaubt.

Diese Firewallkonfiguration wird verwendet, wenn Sie Microsoft Internet Security and Acceleration Server auf dem VPN-Router ausführen.

- **Die Firewall ist an das Internet angeschlossen, und der VPN-Router liegt zwischen Firewall und Intranet.** Bei dieser Konfiguration sind sowohl die Firewall als auch der VPN-Router an ein Subnetz angeschlossen, das als *Grenznetzwerk* (engl. perimeter network oder screened subnet) bezeichnet wird. Firewall und VPN-Router müssen mit Paketfiltern konfiguriert sein, die ausschließlich VPN-Verkehr in und aus dem Internet erlauben.
- **Es werden zwei Firewalls benutzt, eine zwischen dem VPN-Server und dem Intranet, die andere zwischen dem VPN-Server und dem Internet.** Bei dieser Konfiguration filtert eine Firewall den Verkehr zwischen dem Internet und dem Grenznetzwerk, und eine weitere den Verkehr zwischen den Computern im Grenznetzwerk und dem Intranet. Die Internetfirewall und der VPN-Router müssen mit Paketfiltern konfiguriert sein, die ausschließlich VPN-Verkehr in und aus dem Internet erlauben. Die Intranetfirewall kann so konfiguriert sein, dass sie bestimmte Typen von Standort-zu-Standort-Verkehr erlaubt.

Einzelheiten zur Konfiguration von Paketfiltern für den VPN-Router und die Firewall in diesen Konfigurationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« in Kapitel 12.

Anforderungen an die Internetinfrastruktur

- Konfigurieren Sie Ihre Schnittstelle für Wählen bei Bedarf nach Möglichkeit mit den IPv4- oder IPv6-Adressen der antwortenden Router. Falls Sie Namen verwenden, müssen Sie sicherstellen, dass die FQDNs Ihrer antwortenden Router aufgelöst werden können. Schreiben Sie dazu entsprechende Einträge in die Datei *Hosts* oder tragen Sie DNS-Adress- (A) oder IPv6-Adresseinträge (AAAA) in Ihre Internet-DNS-Server oder den DNS-Server Ihres Internetproviders ein. Testen Sie die Auflösbarkeit mit dem Tool Ping, indem Sie alle Ihre antwortenden Router anpingen, wenn sie direkt mit dem IPv4- oder IPv6-Internet verbunden sind.

Aufgrund von Paketfiltern kann es sein, dass der Ping-Befehl das Ergebnis »Anforderungszeitüberschreitung« anzeigt. Prüfen Sie aber, ob der angegebene Name vom Tool Ping in die richtige Adresse aufgelöst werden konnte. Mit dem Befehlszeilenargument -4 können Sie Ping zwingen, eine IPv4-Adresse zu verwenden. Und mit dem Befehlszeilenargument -6 können Sie Ping zwingen, eine IPv6-Adresse zu verwenden. Sie können die Namensauflösung auch mit dem Tool Nslookup testen.

- Stellen Sie sicher, dass die IPv4- oder IPv6-Adressen Ihrer antwortenden Router aus dem Internet erreichbar sind, indem Sie mit dem Tool Ping die FQDN oder Adresse eines antwortenden Routers mit einem 5-Sekunden-Zeitlimit anpingen (verwenden Sie das Befehlszeilenargument -w 5), wenn er direkt mit dem Internet verbunden ist. Falls Sie die Meldung »Ziel nicht erreichbar« erhalten, ist der antwortende Router nicht erreichbar.

Empfohlene Vorgehensweise für die Internetinfrastruktur

Konfigurieren Sie für Standort-zu-Standort-VPN-Verbindungen auf den Firewall- und VPN-Router-schnittstellen, die mit dem Internet und dem Grenznetzwerk verbunden sind, die Paketfilterung für PPTP-Verkehr, L2TP/IPSec-Verkehr oder beide Verkehrstypen. Weitere Informationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« in Kapitel 12.

Standortnetzwerkinfrastruktur

Die Netzwerkinfrastruktur des Standorts ist ein wichtiges Element im VPN-Entwurf. Ohne geeigneten Standortnetzwerkinfrastrukturentwurf sind VPN-Router unter Umständen nicht in der Lage, folgende Aktionen durchzuführen:

- Auflösen von Intranetnamen
- Abrufen einer IPv4-Adresse, die aus dem Intranet erreichbar ist
- Erreichen von Intranetziteln

Intranetnamensauflösung

Falls der anrufende Router mit den IP-Adressen von DNS- (Domain Name System) oder WINS-Servern (Windows Internet Name Service) konfiguriert ist, fordert der antwortende Router während der PPP-Verbindungsaushandlung keine IPv4-Adressen von DNS- und WINS-Servern an. Falls der anrufende Router nicht mit den IPv4-Adressen von DNS- und WINS-Servern konfiguriert ist, fordert er DNS- und WINS-Server an. Der antwortende Router fordert niemals IPv4-Adressen der DNS- und WINS-Server vom anrufenden Router an.

Im Unterschied zu Windows-Remotenzugriffsclients sendet der anrufende Router keine DHCPInform-Nachricht an den antwortenden Router, um zusätzliche TCP/IP-Konfigurationsinformationen abzurufen.

In der Standardeinstellung registriert sich der anrufende Router nicht selbst bei den DNS- oder WINS-Servern, die er vom antwortenden Router erhalten hat. Dieses Verhalten können Sie ändern, indem Sie den Registrierungswert *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\PPP\ControlProtocols\BuiltIn\RegisterRoutersWithNameServers* auf 1 setzen.

Routing des VPN-Routers ins Internet und Intranet

Jeder VPN-Router ist ein IPv4- oder IPv6-Router. Daher muss er mit dem richtigen Satz IPv4- und IPv6-Routen konfiguriert werden, sodass alle Adressen im Internet und dem Standort des VPN-Routers erreichbar sind. Jeder VPN-Router braucht folgende Einstellungen:

- **Eine Standardroute, die auf eine Firewall oder einen Router verweist, der direkt mit dem IPv4- oder IPv6-Internet verbunden ist.** Diese Route macht alle Adressen im IPv4- oder IPv6-Internet erreichbar.
- **Mindestens eine Route, die den innerhalb des Standorts des VPN-Routers benutzten IPv4- und IPv6-Adressraum abdeckt und auf einen benachbarten Standortrouter verweist.** Diese Routen machen alle Adressen im Standort des VPN-Routers vom VPN-Router aus erreichbar. Ohne diese Routen sind Knoten im Standort des VPN-Routers, die an ein anderes Subnetz als der VPN-Router angeschlossen sind, nicht erreichbar.

Um eine einzige Standardroute einzurichten, die in das Internet verweist, müssen Sie die Internet-schnittstelle mit einem Standardgateway konfigurieren und dann von Hand die Standortschnittstelle ohne Standardgateway einrichten.

Sie haben folgende Möglichkeiten, um Standortrouten zur Routingtabelle jedes VPN-Routers hinzuzufügen:

- Fügen Sie statische IPv4- oder IPv6-Routen mit dem Snap-In *Routing und RAS* hinzu. Sie brauchen nicht für jedes Subnetz in Ihrem Standort eine eigene Route hinzuzufügen. Zumindest müssen Sie aber die Routen hinzufügen, die den gesamten Adressraum abdecken, der in Ihrem Standort benutzt wird. Falls Ihr Standort zum Beispiel den privaten IPv4-Adressraum 10.0.0.0/8 für seine Subnetze und Hosts verwendet, brauchen Sie nicht für jedes Subnetz eine eigene Route hin-

zuzufügen. Tragen Sie einfach eine Route für 10.0.0.0 mit der Subnetzmaske 255.0.0.0 ein, die auf einen benachbarten Router in dem Standortsubnetz verweist, an das Ihr VPN-Router angeschlossen ist. Oder falls Ihr Standort das IPv6-Adresspräfix 2001:db8:5ef2::/48 verwendet, brauchen Sie lediglich eine einzige Route mit diesem Präfix als statische IPv6-Route hinzuzufügen.

- Falls Sie in Ihrem Standort RIP als IPv4-Routingprotokoll einsetzen, können Sie die RIP-Routingprotokollkomponente des Routing- und RAS-Dienstes hinzufügen und konfigurieren, sodass der VPN-Router sich als dynamischer Router an der Bekanntgabe von IPv4-Routinginformationen beteiligt.

Falls Ihr Standort nur ein einziges Subnetz umfasst, ist keine weitere Konfiguration erforderlich.

Wenn eine Standort-zu-Standort-VPN-Verbindung hergestellt wird, sendet jeder Router Verkehr über eine logische VPN-Schnittstelle, die dem PPTP- oder L2TP-Port der bei Bedarf herzustellenden Wahlverbindung entspricht. Während der PPP-Aushandlung können diesen VPN-Schnittstellen IPv4- und IPv6-Adressen zugewiesen werden. Ob die VPN-Schnittstellen der VPN-Router erreichbar sind, hängt davon ab, wie die VPN-Router IPv4- und IPv6-Adressen für Remotezugriffsclients und anrufende Router abrufen.

Die IPv6-Adresse, die VPN-Routern zugewiesen wird, beginnt mit einem einheitlichen IPv6-Subnetzpräfix, das für das IPv6-Subnetz aller Remotezugriff- und Standort-zu-Standort-VPN-Verbindungen steht. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von antwortenden Routern« und »Bereitstellen von anrufenden Routern« weiter unten in diesem Kapitel.

Die IPv4-Adressen, die den VPN-Routern zugewiesen werden, sobald sie eine Verbindung herstellen, können aus folgenden Bereichen stammen:

- **Ein subnetzinterner Adressbereich, also ein Adressbereich des Standortsubnetzes, an das der VPN-Router angeschlossen ist** Ein subnetzinterner Adressbereich wird benutzt, wenn der VPN-Router so konfiguriert ist, dass er die IPv4-Adressen über DHCP abrufen, oder wenn die von Hand konfigurierten Pools der IPv4-Adressen innerhalb des Adressbereichs des angeschlossenen Standortsubnetzes liegen.
- **Ein subnetzexterner Adressbereich, also ein Adressbereich, der für ein anderes Subnetz steht, mit dem der VPN-Router logisch verbunden ist** Ein subnetzexterner Adressbereich wird benutzt, wenn der VPN-Router von Hand mit einem Pool von IP-Adressen aus einem anderen Subnetz konfiguriert ist.

Subnetzinterner Adressbereich

Falls Sie einen subnetzinternen Adressbereich verwenden, ist keine zusätzliche Routingkonfiguration erforderlich, weil der VPN-Router als ARP-Proxy (Address Resolution Protocol) für alle Pakete agiert, die an die VPN-Schnittstellen der anderen verbundenen VPN-Router gesendet werden. Router und Hosts im Standortsubnetz senden Pakete, die an die VPN-Schnittstellen von verbundenen VPN-Routern gerichtet sind, und der VPN-Router leitet sie dann an die richtigen VPN-Router weiter.

Subnetzexterner Adressbereich

Falls Sie einen subnetzexternen Adressbereich verwenden, müssen Sie die Routen, die den subnetzexternen Adressbereich abdecken, zur Standortroutinginfrastruktur hinzufügen, sodass Verkehr, der an die VPN-Schnittstellen von verbundenen VPN-Routern gerichtet ist, zum VPN-Router weitergeleitet und von dort vom VPN-Router an den jeweiligen VPN-Router in einem anderen Standort gesendet wird. Damit Sie die Adressbereiche für alle Routen optimal zusammenfassen können, sollten Sie Adressbereiche wählen, die sich mit einem einzigen Präfix und einer Subnetzmaske ausdrücken lassen.

Sie können Routen, die den subnetzexternen Adressbereich abdecken, zur Routinginfrastruktur des Standorts hinzufügen, indem Sie für den subnetzexternen Adressbereich statische IPv4-Routen, die auf die Standortschnittstelle des VPN-Routers verweisen, zum benachbarten Router hinzufügen. Benutzen Sie das dynamische Routingprotokoll, das in Ihrem Standort eingesetzt wird, um den benachbarten Router so zu konfigurieren, dass er diese statische Route an andere Router im Standort weitergibt.

Falls Ihr Standort lediglich ein einziges Subnetz umfasst, müssen Sie entweder auf jedem Standort persistenten Routen des subnetzexternen Adressbereichs konfigurieren, die auf die Standortschnittstelle des VPN-Routers verweisen, oder auf jedem Standort den VPN-Router als Standardgateway eintragen. Daher wird empfohlen, dass Sie für ein SOHO-Netzwerk, das nur aus einem einzigen Subnetz besteht, einen subnetzinternen Adresspool verwenden.

Weil das Routing für subnetzexterne Adressbereiche eine zusätzliche Hostkonfiguration erfordert, wird empfohlen, dass Sie für ein SOHO-Netzwerk (Small Office/Home Office), das nur aus einem einzigen Subnetz besteht, einen subnetzinternen Adresspool verwenden.

Anforderungen an die Standortnetzwerkinfrastruktur

- Konfigurieren Sie die Internetschnittstelle des VPN-Routers mit einem Standardgateway, aber konfigurieren Sie *nicht* die Standortschnittstellen des VPN-Servers mit einem Standardgateway.
- Fügen Sie statische IPv4- und IPv6-Routen zum VPN-Router hinzu, die den gesamten Adressraum abdecken, der in dem Standort benutzt wird, in dem der VPN-Router liegt. Falls Sie RIP als Protokoll für dynamisches IPv4-Routing einsetzen, können Sie stattdessen auch RIP auf dem VPN-Router konfigurieren und aktivieren. Falls Sie ein anderes Routingprotokoll als RIP verwenden, können Sie unter Umständen das entsprechende Routenweitergabeverfahren nutzen. Falls Sie zum Beispiel IGRP (Interior Gateway Routing Protocol) verwenden, können Sie den benachbarten Intranetrouter des VPN-Routers so konfigurieren, dass er auf der Schnittstelle, die mit dem Subnetz des VPN-Routers verbunden ist, RIP benutzt und auf allen anderen Schnittstellen IGRP.
- Fügen Sie das IPv6-Subnetzpräfix für Ihre VPN-Verbindungen als Route, die auf den VPN-Router verweist, zu Ihrer IPv6-Routinginfrastruktur hinzu.

Empfohlene Vorgehensweise für die Standortnetzwerkinfrastruktur

Konfigurieren Sie den VPN-Router nach Möglichkeit mit einem subnetzinternen IPv4-Adressbereich, indem Sie die IPv4-Adressen entweder über DHCP abrufen oder von Hand subnetzinterne Adresspools konfigurieren.

Authentifizierungsinfrastruktur

Die Authentifizierungsinfrastruktur hat folgende Aufgaben:

- Authentifizieren der Anmeldeinformationen von anrufenden Routern
- Autorisieren der VPN-Verbindung
- Aufzeichnen von Aufbau und Beendigung der VPN-Verbindung für Kontoführungszwecke

Die Authentifizierungsinfrastruktur für Standort-zu-Standort-VPN-Verbindungen besteht aus folgenden Komponenten:

- Der antwortende Router oder ein RADIUS-Server
- Ein Domänencontroller

Ein VPN-Router, der unter Windows Server 2008 läuft, kann so konfiguriert werden, dass er entweder Windows oder RADIUS für die Authentifizierung und Kontoführung verwendet. Wenn Sie Routing und RAS so konfigurieren, dass es Windows für die Authentifizierung nutzt, führt der antwortende Router die Authentifizierung der VPN-Verbindung durch, indem er über einen geschützten RPC-Kanal (Remote Procedure Call, Remoteprozeduraufruf) mit einem Domänencontroller kommuniziert. Die Autorisierung des Verbindungsversuchs wird über die Einwähleigenschaften des Benutzerkontos und lokal konfigurierte Netzwerkrichtlinien durchgeführt. Wenn Sie den VPN-Router so konfigurieren, dass er RADIUS nutzt, überlässt der antwortende Router die Durchführung von Authentifizierung und Autorisierung einem RADIUS-Server.

Wenn Sie die Kontoführung durch Windows durchführen lassen, zeichnet der antwortende Router in der Standardeinstellung VPN-Verbindungsinformationen in einer lokalen Protokolldatei auf. Die entsprechenden Einstellungen werden im Knoten *Kontoführung* des Snap-Ins *Netzwerkrichtlinienserver* konfiguriert. Wenn Sie die Kontoführung durch RADIUS durchführen lassen, sendet der antwortende Router RADIUS-Kontoführungsnachrichten zu den VPN-Verbindungen an einen RADIUS-Server, der die Kontoführungsinformationen protokolliert.

Falls Sie RADIUS verwenden, sollten Sie NPS (Network Policy Server, Netzwerkrichtlinienserver) unter Windows Server 2008 verwenden. NPS ist ein leistungsfähiger RADIUS-Server und -Proxy, der eng in Active Directory sowie Routing und RAS integriert ist.

Wenn NPS als RADIUS-Server eingesetzt wird, erfüllt es folgende Aufgaben:

- NPS führt die Authentifizierung der VPN-Verbindung durch, indem es über einen geschützten RPC-Kanal mit einem Domänencontroller kommuniziert. NPS führt die Autorisierung des Verbindungsversuchs anhand der Einwähleigenschaften des Benutzerkontos und der auf dem NPS-Server konfigurierten Netzwerkrichtlinien durch.
- NPS zeichnet in der Standardeinstellung alle RADIUS-Kontoführungsinformationen in einer lokalen Protokolldatei (in der Standardeinstellung `%SystemRoot%\System32\Logfiles\Logfile.log`) auf. Diese Einstellungen können Sie im Knoten *Kontoführung* des Snap-Ins *Netzwerkrichtlinienserver* konfigurieren.

Domänenbenutzerkonten und -gruppen

Active Directory-Domänen enthalten die Benutzerkonten und Gruppen, mit denen Routing und RAS oder NPS VPN-Verbindungsversuche authentifizieren und autorisieren. Benutzerkonten enthalten den Benutzernamen und eine kryptografische Form des Kennworts eines Benutzers. Anhand dieser Daten können die Benutzeranmeldeinformationen des anrufenden Routers überprüft werden. Weitere Kontoeigenschaften legen fest, ob das Benutzerkonto aktiviert, deaktiviert oder gesperrt ist und ob es sich nur während bestimmter Zeiten anmelden darf. Falls das Benutzerkonto deaktiviert oder gesperrt ist oder sich während des Zeitraums der VPN-Verbindung nicht anmelden darf, wird der Standort-zu-Standort-VPN-Verbindungsversuch abgewiesen. Auch falls das Benutzerkonto des anrufenden Routers so konfiguriert ist, dass es sein Kennwort bei der nächsten Anmeldung ändern muss, schlägt der Standort-zu-Standort-VPN-Verbindungsversuch fehl, weil das Kennwort in einem interaktiven Prozess geändert werden muss, der während der Verbindungsherstellung nicht durchgeführt werden kann.

Bei Bedarf wählende Router müssen in der Lage sein, Verbindungen ohne Benutzereingriff herzustellen. Daher müssen die Benutzerkonten für anrufende Router auf der Registerkarte *Konto* des Eigenschaftendialogfelds des Benutzerkontos entsprechend angepasst werden. Stellen Sie sicher, dass das Kontrollkästchen *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* deaktiviert und das Kontrollkästchen *Kennwort läuft nie ab* aktiviert sind. Wenn Sie Einwählkonten mit dem Assistenten

für eine Schnittstelle für Wählen bei Bedarf erstellen, werden diese Kontoeinstellungen automatisch konfiguriert.

Sie sollten für jeden anrufenden Router ein eigenes Benutzerkonto verwenden. Jedes Benutzerkonto sollte einen Namen haben, der einer Schnittstelle für Wählen bei Bedarf entspricht, die auf dem anrufenden Router konfiguriert ist. Wenn Sie Einwählkonten mit dem Assistenten für eine Schnittstelle für Wählen bei Bedarf erstellen, wird diese Beziehung zwischen den Benutzerkonten, die für anrufende Routern in verschiedenen Standorten verwendet werden, und den Schnittstellen für Wählen bei Bedarf automatisch erstellt.

Empfohlene Vorgehensweise für die Authentifizierungsinfrastruktur

- Falls Sie mehrere VPN-Server und -Router haben und Authentifizierungs-, Autorisierungs- und Kontoführungsdienste zentralisieren wollen, oder falls Sie eine heterogene Mischung aus Netzwerkzugriffsgeräten haben, sollten Sie einen RADIUS-Server verwenden und den VPN-Router so konfigurieren, dass er RADIUS für Authentifizierung und Kontoführung benutzt.
- Falls Sie eine Windows-Domäne als Benutzerkontodatenbank einsetzen, sollten Sie NPS als Ihren RADIUS-Server verwenden. In Kapitel 9 finden Sie weitere Informationen zu Entwurf und Planung von NPS-RADIUS-Servern.
- Um die Autorisierung für Standort-zu-Standort-VPN-Verbindungen besser verwalten zu können, sollten Sie in Active Directory eine universelle Gruppe anlegen, die globale Gruppen für alle Benutzerkonten enthält, die Standort-zu-Standort-VPN-Verbindungen herstellen dürfen. Zum Beispiel können Sie eine universelle Gruppe namens *VPNRouter* erstellen, deren Mitglieder globale Gruppen sind, die den geografischen oder organisatorischen Aufbau Ihrer Organisation widerspiegeln. Jede globale Gruppe enthält Benutzerkonten, die Standort-zu-Standort-VPN-Verbindungen herstellen dürfen. Wenn Sie Ihre Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen konfigurieren, geben Sie den Gruppennamen *VPNRouter* an.
- Unabhängig davon, ob die Authentifizierung lokal oder auf einem NPS-Server durchgeführt wird, sollten Sie eine VPN-spezifische Netzwerkrichtlinie verwenden, um VPN-Verbindungen zu autorisieren und Verbindungseinschränkungen sowie Anforderungen zu definieren. Zum Beispiel können Sie mithilfe von Netzwerkrichtlinien den Zugriff mit VPN-Verbindungen aufgrund der Gruppenmitgliedschaft gewähren, sichere Verschlüsselung fordern oder die Benutzung bestimmter Authentifizierungsmethoden (zum Beispiel MS-CHAP v2 oder EAP-TLS) fordern.

PKI

Um eine zertifikatbasierte Authentifizierung für L2TP-Verbindungen und eine EAP-TLS-Authentifizierung für Standort-zu-Standort-VPN-Verbindungen durchführen zu können, muss eine Zertifikatsinfrastruktur vorhanden sein. Diese PKI (Public Key Infrastructure) stellt die Zertifikate aus, die während des Authentifizierungsprozesses übergeben und von der Gegenstelle überprüft werden.

Computerzertifikate für L2TP/IPsec-Verbindungen

Wenn Sie für eine Regel innerhalb einer IPsec-Richtlinie in Windows von Hand die Zertifikatauthentifizierung konfigurieren, können Sie die Liste der Stammzertifizierungsstellen (Certification Authority, CA) konfigurieren, deren Zertifikate für die Authentifizierung akzeptiert werden. Für L2TP-Verbindungen wird die IPsec-Regel für L2TP-Verkehr automatisch konfiguriert, die Liste der Stammzertifizierungsstellen ist hier nicht konfigurierbar. Stattdessen sendet der Computer bei der L2TP-Verbindung eine Liste der Stammzertifizierungsstellen an seinen IPsec-Peer, deren Zertifikat er für die Authentifizierung akzeptiert. Die Stammzertifizierungsstellen in dieser Liste entsprechen den Stammzertifizie-

rungsstellen, die die im Computerzertifikatspeicher abgelegten Computerzertifikate ausgestellt haben. Falls zum Beispiel Computer A Computerzertifikate von den Stammzertifizierungsstellen CertAuth1 und CertAuth2 ausgestellt bekommen hat, meldet er seinem IPsec-Peer während der Hauptmodusaushandlung, dass er für die Authentifizierung nur Zertifikate von CertAuth1 und CertAuth2 akzeptiert. Falls der IPsec-Peer, Computer B, kein gültiges Computerzertifikat besitzt, das entweder von CertAuth1 oder von CertAuth2 ausgestellt wurde, schlägt die IPsec-Sicherheitsaushandlung fehl.

Bevor Sie eine L2TP/IPsec-Verbindung herstellen können, müssen folgende Voraussetzungen erfüllt sein:

- Sowohl der anrufende Router als auch der antwortende Router haben Computerzertifikate von derselben Zertifizierungsstelle ausgestellt bekommen.
- Sowohl der anrufende als auch der antwortende Router haben Computerzertifikate von Zertifizierungsstellen ausgestellt bekommen, die in einer gültigen Zertifikatkette liegen, die zur selben Stammzertifizierungsstelle reicht.

Im Allgemeinen muss der anrufende Router ein gültiges Computerzertifikat installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der antwortende Router vertraut. Außerdem muss der antwortende Router ein gültiges Computerzertifikat installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der anrufende Router vertraut.

Normalerweise werden die Computerzertifikate für alle Computer in einer Organisation von einer einzigen Zertifizierungsstelle ausgestellt. Deswegen haben alle Computer innerhalb der Organisation einerseits Computerzertifikate von derselben Zertifizierungsstelle *und* fordern für die Authentifizierung Zertifikate von derselben Zertifizierungsstelle an.

Informationen über das Installieren von Computerzertifikaten auf VPN-Routern für L2TP-Verbindungen finden Sie in Kapitel 12.



Hinweis Routing und RAS unterstützt die Konfiguration eines vorinstallierten Schlüssels für die IPsec-Authentifizierung von L2TP/IPsec-Verbindungen. Sie können den antwortenden Router entsprechend konfigurieren, indem Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des VPN-Routers öffnen, auf der Registerkarte *Sicherheit* das Kontrollkästchen *Benutzerdefinierte IPsec-Richtlinie für L2TP-Verbindung zulassen* aktivieren und dann den vorinstallierten Schlüssel eingeben. Den anrufenden Router können Sie konfigurieren, indem Sie das Eigenschaftendialogfeld einer Schnittstelle für Wählen bei Bedarf öffnen, auf der Registerkarte *Netzwerk* auf die Schaltfläche *IPSec-Einstellungen* klicken und dann den vorinstallierten Schlüssel eingeben. Beachten Sie aber, dass die Authentifizierung von L2TP/IPsec-Verbindungen durch vorinstallierte Schlüssel nicht sicher ist. Daher wird von ihrer Verwendung abgeraten, sofern es sich nicht um eine temporäre Lösung während der Bereitstellung einer Zertifikatinfrastruktur oder um eine Verbindung zu VPN-Routern von Fremdherstellern handelt, die keine Zertifikatauthentifizierung unterstützen.

PKI für EAP-TLS

Um für eine Standort-zu-Standort-VPN-Verbindung eine EAP-TLS-Authentifizierung durchführen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Der anrufende Router muss mit einem Benutzerzertifikat konfiguriert sein, das er während des EAP-TLS-Authentifizierungsprozesses übergeben kann.

- Der Authentifizierungsserver (der antwortende Router oder ein RADIUS-Server) muss mit einem Computerzertifikat konfiguriert sein, das er während des EAP-TLS-Authentifizierungsprozesses übergeben kann.

Die EAP-TLS-Authentifizierung war erfolgreich, wenn folgende Bedingungen erfüllt sind:

- Der anrufende Router übergibt ein gültiges Benutzerzertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der antwortende Router vertraut.
- Der Authentifizierungsserver übergibt ein gültiges Computerzertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der anrufende Router vertraut.

Bei einer Windows Server 2008- oder Windows Server 2003-Zertifizierungsstelle ist ein Zertifikat vom Typ *Router (Offlineanforderung)* ein spezieller Benutzerzertifikatstyp für bei Bedarf herzustellende Wählverbindungen. Ein Zertifikat vom Typ *Router (Offlineanforderung)* muss angefordert und einem Active Directory-Benutzerkonto zugeordnet werden. Wenn der anrufende Router versucht, eine VPN-Verbindung aufzubauen, wird während des Authentifizierungsprozesses das Zertifikat vom Typ *Router (Offlineanforderung)* gesendet. Falls das Zertifikat gültig ist, kann der Authentifizierungsserver feststellen, von welchem Benutzerkonto er die Einwähleigenschaften abrufen soll.

Informationen über das Konfigurieren von Benutzer- und Computerzertifikaten für EAP-TLS-Authentifizierung finden Sie im Abschnitt »Bereitstellen von Zertifikaten« weiter unten in diesem Kapitel.

Anforderungen an die PKI

- Für L2TP/IPsec-Standort-zu-Standort-VPN-Verbindungen, die Zertifikate für die IPsec-Authentifizierung benutzen, müssen Sie Computerzertifikate auf dem anrufenden und dem antwortenden Router installieren.
- Um Standort-zu-Standort-VPN-Verbindungen mit EAP-TLS authentifizieren zu können, muss der anrufende Router ein Benutzerzertifikat installiert haben und der Authentifizierungsserver (entweder der antwortende Router oder der RADIUS-Server) muss ein Computerzertifikat installiert haben.
- Für die EAP-TLS-Authentifizierung müssen folgende Anforderungen an das Benutzerzertifikat des anrufenden Routers erfüllt sein:
 - Das Zertifikat muss einen privaten Schlüssel enthalten.
 - Das Zertifikat muss von einer Unternehmenszertifizierungsstelle ausgestellt oder einem Benutzerkonto in Active Directory zugeordnet sein.
 - Das Zertifikat muss in einer Kette liegen, die bis zu einer vertrauenswürdigen Stammzertifizierungsstelle auf dem NPS-Server führt. Es muss alle Prüfungen bestehen, die von der CryptoAPI durchgeführt werden und in der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen angegeben sind.
 - Das Zertifikat muss im Feld *Erweiterte Schlüsselverwendung* den Zweck *Clientauthentifizierung* eingetragen haben. (Die Objektkennung für Clientauthentifizierung ist 1.3.6.1.5.5.7.3.2.)
 - Das Feld *Alternativer Antragstellername* muss den Benutzerprinzipalnamen (User Principal Name, UPN) des Benutzerkontos enthalten.
- Für die EAP-TLS-Authentifizierung müssen folgende Anforderungen an das Computerzertifikat des antwortenden Routers oder NPS-Servers erfüllt sein:
 - Das Zertifikat muss einen privaten Schlüssel enthalten.

- Das Feld *Antragsteller* muss einen Wert enthalten.
- Das Zertifikat muss in einer Kette liegen, die bis zu einer vertrauenswürdigen Stammzertifizierungsstelle auf dem anrufenden Router führt. Es muss alle Prüfungen bestehen, die von der CryptoAPI durchgeführt werden und in der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen angegeben sind.
- Das Zertifikat muss im Feld *Erweiterte Schlüsselverwendung* den Zweck *Serverauthentifizierung* eingetragen haben. (Die Objektkennung für Serverauthentifizierung ist 1.3.6.1.5.5.7.3.1.)
- Als erforderlicher Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) ist *Microsoft RSA SChannel Cryptographic Provider* eingetragen.
- Sofern das Feld *Alternativer Antragstellername* benutzt wird, muss es den FQDN des Servers enthalten.

Empfohlene Vorgehensweise für die PKI

Falls Sie eine Windows Server 2008-Unternehmenszertifizierungsstelle als ausstellende Zertifizierungsstelle einsetzen und Computerzertifikate für L2TP/IPsec brauchen, sollten Sie Ihre Active Directory-Domäne über Gruppenrichtlinien im Zweig *Computerkonfiguration* so konfigurieren, dass die Computerzertifikate automatisch registriert werden. Jeder Computer, der Mitglied der Domäne ist, fordert automatisch ein Computerzertifikat an, wenn er die entsprechenden Gruppenrichtlinien aktualisiert. Weitere Informationen finden Sie im Abschnitt »Bereitstellen von Zertifikaten« weiter unten in diesem Kapitel.

Bereitstellen von Standort-zu-Standort-VPN-Verbindungen

Das Bereitstellen von Standort-zu-Standort-VPN-Verbindungen mit Windows Server 2008 umfasst folgende Aufgaben:

- Bereitstellen von Zertifikaten
- Konfigurieren der Internetinfrastruktur
- Konfigurieren von Benutzerkonten und Gruppen in Active Directory
- Konfigurieren von RADIUS-Servern
- Bereitstellen der antwortenden Router
- Bereitstellen der anrufenden Router
- Konfigurieren der Standortnetzwerkinfrastruktur
- Konfigurieren der Infrastruktur für die Standortverbindungen

Bereitstellen von Zertifikaten

Sie müssen Zertifikate bereitstellen, falls Sie folgende Methoden benutzen:

- L2TP/IPsec-Verbindungen mit Zertifikatauthentifizierung
Jeder VPN-Routercomputer braucht ein Computerzertifikat.
- EAP-TLS-Authentifizierung mit in der Registrierung gespeicherten Benutzerzertifikaten
Jeder anrufende Router braucht ein Benutzerzertifikat und jeder Authentifizierungsserver ein Computerzertifikat.

Bereitstellen von Computerzertifikaten

Damit Sie ein Computerzertifikat installieren können, muss eine PKI vorhanden sein, die die Zertifikate ausstellt. Wenn die PKI bereitgestellt wurde, haben Sie folgende Möglichkeiten, um Computerzertifikate auf VPN-Routern oder Authentifizierungsservern zu installieren:

- Konfigurieren Sie die automatische Registrierung von Computerzertifikaten für die Computer in einer Active Directory-Domäne.
- Fordern Sie im Snap-In *Zertifikate* ein Computerzertifikat an.
- Importieren Sie ein Computerzertifikat im Snap-In *Zertifikate*.
- Fordern Sie ein Zertifikat über das Web an.
- Führen Sie ein CAPICOM-Skript aus, das ein Computerzertifikat anfordert.

Weitere Informationen finden Sie im Abschnitt »Bereitstellen der Public-Key-Infrastruktur« in Kapitel 9.

Bereitstellen von Benutzerzertifikaten für anrufende Router

Falls Sie eine Windows Server 2008-Zertifizierungsstelle verwenden, können anrufende Router ein Zertifikat vom Typ *Router (Offlineanforderung)* benutzen. Das Zertifikat muss bei der Anforderung einem Active Directory-Benutzerkonto zugeordnet werden, das vom anrufenden Router verwendet wird. Gehen Sie folgendermaßen vor, um für einen anrufenden Router ein Zertifikat vom Typ *Router (Offlineanforderung)* bereitzustellen:

1. Legen Sie ein Benutzerkonto für den anrufenden Router an. Sie können dafür den Assistenten für eine Schnittstelle für Wählen bei Bedarf oder das Snap-In *Active Directory-Benutzer und -Computer* verwenden. Es wird empfohlen, den Assistenten für eine Schnittstelle für Wählen bei Bedarf zu benutzen.
2. Konfigurieren Sie die Windows Server 2008-Zertifizierungsstelle so, dass sie Zertifikate vom Typ *Router (Offlineanforderung)* ausstellt. Eine entsprechende Anleitung finden Sie im Abschnitt »So konfigurieren Sie die Windows Server 2008-Zertifizierungsstelle so, dass sie Zertifikate vom Typ *Router (Offlineanforderung)* ausstellt« weiter unten.
3. Fordern Sie ein Zertifikat vom Typ *Router (Offlineanforderung)* an. Eine entsprechende Anleitung finden Sie im Abschnitt »So fordern Sie ein Zertifikat vom Typ *Router (Offlineanforderung)* an« weiter unten.
4. Exportieren Sie das Zertifikat vom Typ *Router (Offlineanforderung)* in eine *.cer*-Datei. Eine entsprechende Anleitung finden Sie im Abschnitt »So exportieren Sie das Zertifikat vom Typ *Router (Offlineanforderung)* in eine *.cer*-Datei« weiter unten.
5. Ordnen Sie die *.cer*-Zertifikatsdatei dem richtigen Benutzerkonto zu. Eine entsprechende Anleitung finden Sie im Abschnitt »So ordnen Sie die *.cer*-Zertifikatsdatei dem richtigen Benutzerkonto zu« weiter unten.
6. Exportieren Sie das Zertifikat vom Typ *Router (Offlineanforderung)* in eine *.pfx*-Datei. Eine entsprechende Anleitung finden Sie im Abschnitt »So exportieren Sie das Zertifikat vom Typ *Router (Offlineanforderung)* in eine *.pfx*-Datei« weiter unten.
7. Senden Sie die *.pfx*-Zertifikatsdatei mit dem Zertifikat vom Typ *Router (Offlineanforderung)* an den Netzwerkadministrator des anrufenden Routers.
8. Importieren Sie die *.pfx*-Zertifikatsdatei mit dem Zertifikat vom Typ *Router (Offlineanforderung)* auf dem anrufenden Router. Eine entsprechende Anleitung finden Sie im Abschnitt »So importie-

ren Sie die *.pfx*-Zertifikatsdatei mit dem Zertifikat vom Typ *Router (Offlineanforderung)* auf dem anrufenden Router« weiter unten.

So konfigurieren Sie die Windows Server 2008-Zertifizierungsstelle so, dass sie Zertifikate vom Typ *Router (Offlineanforderung)* ausstellt

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Zertifizierungsstelle* den Namen der Zertifizierungsstelle.
2. Klicken Sie mit der rechten Maustaste auf *Zertifikatvorlagen*, wählen Sie *Neu* und klicken Sie auf *Auszustellende Zertifikatvorlage*.
3. Klicken Sie im Dialogfeld *Zertifikatvorlagen aktivieren* auf *Router (Offlineanforderung)*. Abbildung 13.2 zeigt den entsprechenden Eintrag. Klicken Sie auf *OK*.

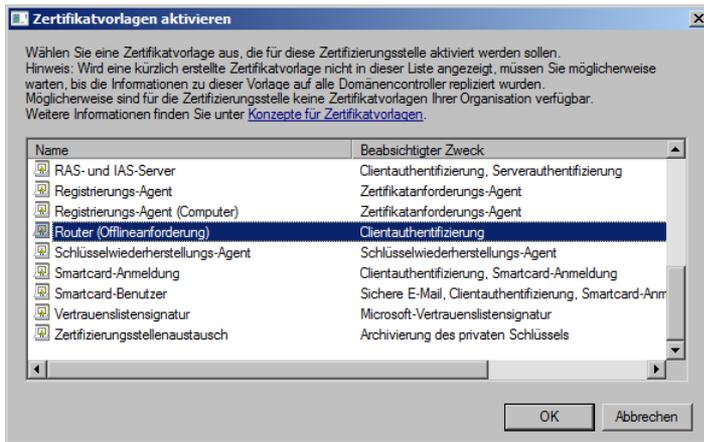


Abbildung 13.2 Dialogfeld *Zertifikatvorlagen aktivieren*

So fordern Sie ein Zertifikat vom Typ *Router (Offlineanforderung)* an

1. Öffnen Sie den Windows Internet Explorer.
2. Geben Sie in der Adressleiste die Adresse der Zertifizierungsstelle ein, die Ihre Computerzertifikate ausstellt. Die Adresse besteht aus dem Namen des Servers, gefolgt von »/certsrv«, zum Beispiel *http://ca1/certsrv*.
3. Klicken Sie auf der Seite *Willkommen* auf *Ein Zertifikat anfordern*, dann auf *Erweiterte Zertifikatanforderung* und schließlich auf *Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen*.
4. Wählen Sie im Feld *Zertifikatsvorlage* den Eintrag *Router (Offlineanforderung)* oder den Namen der Vorlage aus, den Ihnen der Administrator der Zertifizierungsstelle genannt hat.
5. Geben Sie im Feld *Name* den Namen des Benutzerkontos ein, das vom anrufenden Router verwendet wird.
6. Aktivieren Sie unter *Schlüsselloptionen* die Kontrollkästchen *Schlüssel als "Exportierbar" markieren* und *Zertifikat in lokalem Zertifikatspeicher aufbewahren*.
7. Stellen Sie die anderen Optionen wie gewünscht ein und klicken Sie auf *Einsenden*.
8. Es wird eine Meldung angezeigt, in der Sie bestätigen müssen, dass Sie dieser Website vertrauen und ein Zertifikat anfordern wollen. Klicken Sie auf *Ja*.

9. Klicken Sie auf der Seite *Zertifikat wurde ausgestellt* auf *Dieses Zertifikat installieren*.

Eine Meldung informiert Sie, dass ein neues Zertifikat erfolgreich installiert wurde.



Hinweis Damit ein Zertifikat vom Typ *Router (Offlineanforderung)* über die Webregistrierung angefordert werden kann, muss eine Windows Server 2008-Zertifizierungsstelle installiert sein. Dafür müssen Sie die Rolle *Active Directory-Zertifikatdienste* mit dem Rollendienst *Zertifizierungsstellen-Webregistrierung* installieren.

So exportieren Sie das Zertifikat vom Typ *Router (Offlineanforderung)* in eine *.cer*-Datei

1. Öffnen Sie eine MMC-Konsole mit dem Snap-In *Zertifikate – Lokaler Computer*.
2. Erweitern Sie *Eigene Zertifikate* und klicken Sie auf *Zertifikate*.
3. Klicken Sie in der Detailansicht mit der rechten Maustaste auf das Zertifikat vom Typ *Router (Offlineanforderung)*, das über die Webregistrierung angefordert wurde, wählen Sie *Alle Aufgaben* und klicken Sie auf *Exportieren*.
4. Klicken Sie auf der Seite *Willkommen auf Weiter*.
5. Klicken Sie im Zertifikatexport-Assistenten auf *Nein, privaten Schlüssel nicht exportieren*. Klicken Sie auf *Weiter*.
6. Wählen Sie die Option *DER-codiert-binär X.509 (.CER)* als Exportdateiformat aus und klicken Sie auf *Weiter*.
7. Geben Sie den Namen für die Zertifikatsdatei ein, klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

So ordnen Sie die *.cer*-Zertifikatsdatei dem richtigen Benutzerkonto zu

1. Öffnen Sie das Snap-In *Active Directory-Benutzer und -Computer*. Wählen Sie im Menü *Ansicht* den Befehl *Erweiterte Features*.
2. Erweitern Sie in der Konsolenstruktur den gewünschten Domänensystemcontainer und den Ordner, der das Benutzerkonto für den anrufenden Router enthält.
3. Klicken Sie in der Detailansicht mit der rechten Maustaste auf das Benutzerkonto, dem Sie ein Zertifikat zuordnen wollen, und wählen Sie den Befehl *Namenszuordnungen*.
4. Klicken Sie auf der Registerkarte *X.509-Zertifikate* auf *Hinzufügen*.
5. Wählen Sie im Dialogfeld *Zertifikat hinzufügen* die *.cer*-Zertifikatsdatei aus und klicken Sie auf *Öffnen*. Klicken Sie auf *OK*.

So exportieren Sie das Zertifikat vom Typ *Router (Offlineanforderung)* in eine *.pfx*-Datei

1. Öffnen Sie eine MMC-Konsole mit dem Snap-In *Zertifikate – Lokaler Computer*.
2. Erweitern Sie *Eigene Zertifikate* und klicken Sie auf *Zertifikate*.
3. Klicken Sie in der Detailansicht mit der rechten Maustaste auf das Zertifikat vom Typ *Router (Offlineanforderung)*, das über die Webregistrierung angefordert wurde, wählen Sie *Alle Aufgaben* und klicken Sie auf *Exportieren*.
4. Klicken Sie auf der Seite *Willkommen* im Zertifikatexport-Assistenten auf *Weiter*.
5. Wählen Sie auf der Seite *Privaten Schlüssel exportieren* die Option *Ja, privaten Schlüssel exportieren* aus. Klicken Sie auf *Weiter*.
6. Wählen Sie auf der Seite *Format der zu exportierenden Datei* die Option *Privater Informationsaustausch – PKCS #12 (.PFX)* als Exportdateiformat aus. Aktivieren Sie das Kontrollkästchen *Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen* und klicken Sie auf *Weiter*.

7. Geben Sie auf der Seite *Kennwort* ein Kennwort in die Felder *Kennwort* und *Kennwort eingeben und bestätigen* ein, das den privaten Schlüssel des Zertifikats schützt. Dieses Kennwort wird gebraucht, um das Zertifikat zu importieren. Klicken Sie auf *Weiter*.
8. Geben Sie auf der Seite *Zu exportierende Datei* den Namen der Zertifikatdatei ein und klicken Sie auf *Weiter*.
9. Klicken Sie auf der Seite *Fertigstellen des Assistenten* auf *Fertig stellen*.

So importieren Sie die .pfx-Zertifikatsdatei mit dem Zertifikat vom Typ Router (Offlineanforderung) auf dem anrufenden Router

1. Öffnen Sie eine MMC-Konsole mit dem Snap-In *Zertifikate – Aktueller Benutzer*.
2. Wählen Sie den Knoten *Eigene Zertifikate* aus.
3. Klicken Sie mit der rechten Maustaste auf den Knoten *Eigene Zertifikate*, wählen Sie *Alle Aufgaben* und klicken Sie auf *Importieren*.
4. Klicken Sie auf der Seite *Willkommen* des Zertifikatimport-Assistenten auf *Weiter*.
5. Geben Sie auf der Seite *Zu importierende Datei* den Dateinamen des Zertifikats an, das Sie importieren wollen, und klicken Sie auf *Weiter*. (Sie können auch auf *Durchsuchen* klicken und die Datei auswählen.)
6. Geben Sie das Kennwort ein, mit dem der private Schlüssel geschützt wird, und klicken Sie auf *Weiter*.
7. An diesem Punkt haben Sie zwei Möglichkeiten:
 - Falls das Zertifikat automatisch anhand des Zertifikattyps dem passenden Speicher zugeordnet werden soll, können Sie die Option *Zertifikatspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)* auswählen.
 - Falls Sie selbst angeben wollen, wo das Zertifikat gespeichert werden soll, müssen Sie *Alle Zertifikate in folgendem Speicher speichern* auswählen, auf *Durchsuchen* klicken und den verwendeten Zertifikatspeicher auswählen.
8. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Konfigurieren der Internetinfrastruktur

Gehen Sie folgendermaßen vor, um die Internetinfrastruktur für Standort-zu-Standort-VPN-Verbindungen zu konfigurieren:

- Richten Sie die VPN-Router im Grenznetzwerk oder im Internet ein.
- Installieren Sie Windows Server 2008 auf den VPN-Routercomputern und konfigurieren Sie deren Internetschnittstellen.
- Fügen Sie Adresseinträge zu den Internet-DNS-Servern hinzu (sofern nötig).

Einrichten von VPN-Routern im Grenznetzwerk oder Internet

Überlegen Sie, wo Sie die VPN-Router im Bezug auf Ihre Internetfirewall anordnen wollen. Üblich ist eine Konfiguration, bei der die VPN-Router hinter der Firewall im Grenznetzwerk liegen, also zwischen dem Internet und Ihrem Standort. In diesem Fall müssen Sie auf der Firewall Paketfilter konfigurieren, die PPTP- und L2TP/IPSec-Verkehr zu und von den IPv4- oder IPv6-Adressen der Grenznetzwerkschnittstellen der VPN-Router erlauben. Weitere Informationen finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« in Kapitel 12.

Installieren von Windows Server 2008 auf VPN-Routern und Konfigurieren der Internetschnittstellen

Installieren Sie Windows Server 2008 auf den VPN-Routercomputern. Verbinden Sie einen VPN-Router über eine Netzwerkkarte entweder mit dem Internet oder dem Grenznetzwerk, und über eine andere Netzwerkkarte mit dem Standort. Bevor Sie den Setup-Assistenten für den Routing- und RAS-Server ausführen, leitet der VPN-Routercomputer keine IPv4- oder IPv6-Pakete zwischen Internet und Standort weiter.

Konfigurieren Sie für die Verbindung mit dem IPv4-Internet oder -Grenznetzwerk das Protokoll *TCP/IP (IPv4)* mit einer öffentlichen IPv4-Adresse und einer Subnetzmaske. Stellen Sie als Standardgateway entweder die Firewall (falls der Router an ein Grenznetzwerk angeschlossen ist) oder einen Router des Internetproviders ein (falls der Router direkt mit dem Internet verbunden ist). Konfigurieren Sie keine IPv4-Adressen von DNS-Servern oder WINS-Servern für die Verbindung.

Konfigurieren Sie für die Verbindung mit dem IPv6-Internet oder -Grenznetzwerk das Protokoll *TCP/IP (IPv6)* mit einer globalen IPv6-Adresse und einem 64-Bit-Präfix. Stellen Sie als Standardgateway entweder die Firewall (falls der VPN-Router an ein Grenznetzwerk angeschlossen ist) oder einen Router des Internetproviders ein (falls der VPN-Router direkt mit dem IPv6-Internet verbunden ist). Konfigurieren Sie keine IPv6-Adressen von DNS-Servern für die Verbindung.

Hinzufügen von Adresseinträgen zu den Internet-DNS-Servern

Sie müssen entweder DNS-Adresseinträge (A) oder IPv6-Adresseinträge (AAAA) für die antwortenden Router zu Ihrem Internet-DNS-Server hinzufügen (falls Sie selbst die DNS-Namensauflösung für Internetbenutzer zur Verfügung stellen) oder Ihren Internetprovider beauftragen, A- beziehungsweise AAAA-Einträge zu seinen DNS-Servern hinzuzufügen (falls Ihr Internetprovider die DNS-Namensauflösung für Internetbenutzer übernimmt). Überprüfen Sie, ob der Name des antwortenden Routers in seine öffentliche IPv4-Adresse oder globale IPv6-Adresse aufgelöst werden kann, wenn er mit dem Internet verbunden ist.

Konfigurieren der Active Directory-Benutzerkonten und -Gruppen

Falls Sie die Einstellungen im Assistenten für eine Schnittstelle für Wählen bei Bedarf so wählen, dass Benutzerkonten für anrufende Router automatisch hinzugefügt werden, werden die Konten automatisch mit den richtigen Benutzerkontoeinstellungen für bei Bedarf herzustellende Wählverbindungen konfiguriert. Falls Sie Benutzerkonten für anrufende Router von Hand anlegen, müssen Sie sicherstellen, dass sie folgende Einstellungen haben:

- Auf der Registerkarte *Einwählen* muss unter *Netzwerkzugriffsberechtigung* die Option *Zugriff gestatten* oder *Zugriff über NPS-Netzwerkrichtlinien steuern* ausgewählt sein.
- Auf der Registerkarte *Konto* muss das Kontrollkästchen *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* deaktiviert und das Kontrollkästchen *Kennwort läuft nie ab* aktiviert sein.

Organisieren Sie die Benutzerkonten Ihrer anrufenden Router in geeigneten universellen und globalen Sicherheitsgruppen, um die gruppenabhängigen Netzwerkrichtlinien nutzen zu können.

Konfigurieren von RADIUS-Servern

Falls Sie RADIUS für Authentifizierung, Autorisierung und Kontoführung von Standort-zu-Standort-VPN-Verbindungen einsetzen, müssen Sie Ihre NPS-RADIUS-Server wie in Kapitel 9 beschrieben konfigurieren und bereitstellen. Dazu sind folgende Schritte erforderlich:

- Installieren Sie ein Computerzertifikat auf den NPS-Servern, falls Sie EAP-TLS-Authentifizierung einsetzen.
- Konfigurieren Sie die Protokollierung.
- Fügen Sie alle antwortenden Router als RADIUS-Clients zum NPS-Server hinzu.

Der NPS-Server benutzt eine Netzwerkrichtlinie, um VPN-Verbindungen zu autorisieren. Für Standort-zu-Standort-VPN-Verbindungen können Sie die Standardnetzwerkrichtlinie mit dem Namen *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver* verwenden. Bei dieser Netzwerkrichtlinie ist in der Standardeinstellung allerdings der Richtlinientyp *Zugriff verweigern* eingestellt.

So verwenden Sie die Netzwerkrichtlinie *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver*

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Netzwerkrichtlinienserver* unter *Richtlinien* auf *Netzwerkrichtlinien*.
2. Klicken Sie doppelt auf die Netzwerkrichtlinie *Verbindungen mit Microsoft-Routing- und Remotezugriffsserver*.
3. Aktivieren Sie auf der Registerkarte *Übersicht* unter *Richtlinienstatus* das Kontrollkästchen *Richtlinie aktiviert* und klicken Sie auf *OK*.

Sie können auch den Assistenten *VPN oder DFÜ konfigurieren* verwenden, um einen Satz Richtlinien zu erstellen, die für Standort-zu-Standort-VPN-Verbindungen optimiert sind. Dabei verwenden Sie den Namen der universellen Gruppe für Ihre VPN-Router.

So erstellen Sie einen Satz von Richtlinien für die Standort-zu-Standort-VPN-Verbindungen

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Netzwerkrichtlinienserver* auf *NPS*.
2. Wählen Sie in der Detailansicht unter *Standardkonfiguration* in der Dropdownliste den Eintrag *RADIUS-Server für DFÜ- oder VPN-Verbindungen* aus und klicken Sie auf *VPN oder DFÜ konfigurieren*.
3. Klicken Sie im Assistenten *VPN oder DFÜ konfigurieren* auf der Seite *Auswählen des DFÜ- oder VPN-Verbindungstyps* auf *Verbindungen für virtuelles privates Netzwerk (VPN)* und geben Sie den Namen der neuen NPS-Netzwerkrichtlinie ein (oder verwenden Sie den Namen, den der Assistent eingetragen hat). Klicken Sie auf *Weiter*.
4. Fügen Sie auf der Seite *Angeben des DFÜ- oder VPN-Servers* nach Bedarf Ihre antwortenden Router als RADIUS-Clients hinzu. Klicken Sie auf *Weiter*.
5. Auf der Seite *Authentifizierungsmethoden konfigurieren* ist bereits MS-CHAP v2 aktiviert. Wenn Sie einen EAP-Authentifizierungstyp aktivieren und konfigurieren wollen, müssen Sie das Kontrollkästchen *Extensible Authentication-Protokoll* aktivieren, in der Dropdownliste einen EAP-Typ auswählen und bei Bedarf auf *Konfigurieren* klicken (zum Beispiel um festzulegen, welches Computerzertifikat für EAP-TLS-Authentifizierung verwendet werden soll).

Wenn Sie EAP-TLS aktivieren und konfigurieren wollen, müssen Sie das Kontrollkästchen *Extensible Authentication-Protokoll* aktivieren. Wählen Sie in der Dropdownliste *Typ* den Eintrag *Smartcard- oder anderes Zertifikat* aus und klicken Sie auf *Konfigurieren*. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* das Computerzertifikat aus, das für Standort-zu-Standort-VPN-Verbindungen benutzt werden soll, und klicken Sie auf *OK*. Falls Sie das gewünschte Zertifikat nicht auswählen können, bietet der Kryptografiedienstanbieter für das Zertifikat keine Unterstützung für einen sicheren Kanal (SChannel). SChannel-Unterstützung ist erforderlich, damit NPS das Zertifikat für die EAP-TLS-Authentifizierung benutzen kann.

6. Klicken Sie auf *Weiter*. Fügen Sie auf der Seite *Benutzergruppen angeben* die Gruppen hinzu, deren Benutzerkonten Standort-zu-Standort-VPN-Verbindungen herstellen dürfen (zum Beispiel *VPNRouter*), und klicken Sie auf *Weiter*.
7. Klicken Sie auf der Seite *Angeben von IP-Filtern* auf *Weiter*.
8. Aktivieren Sie auf der Seite *Angeben von Verschlüsselungseinstellungen* die erlaubten Verschlüsselungsstärken und klicken Sie auf *Weiter*.
9. Klicken Sie auf der Seite *Bereichsname angeben* auf *Weiter*.
10. Klicken Sie auf der Seite *Abschließen der neuen DFÜ- oder VPN-Verbindungen und RADIUS-Clients* auf *Fertig stellen*.

Der Assistent *VPN oder DFÜ konfigurieren* erstellt eine Verbindungsanforderungsrichtlinie und eine Netzwerkrichtlinie für VPN-Verbindungen. Außerdem konfiguriert der Assistent *VPN oder DFÜ konfigurieren* die Netzwerkrichtlinie mit einer einzigen EAP-Methode. Weitere EAP-Methoden können Sie auf der Registerkarte *Einstellungen* im Eigenschaftendialogfeld der Netzwerkrichtlinie konfigurieren.

Wenn Sie den primären NPS-Server mit den gewünschten Protokollierungs-, RADIUS-Client- und Richtlinieneinstellungen konfiguriert haben, können Sie die Konfiguration auf den sekundären oder weitere NPS-Server kopieren. Weitere Informationen finden Sie in Kapitel 9.

Bereitstellen von antwortenden Routern

Gehen Sie folgendermaßen vor, um einen antwortenden Router für eine Standort-zu-Standort-VPN-Verbindung bereitzustellen:

- Installieren Sie Computerzertifikate.
- Konfigurieren Sie die Verbindung des antwortenden Routers zum Standort.
- Installieren Sie die Rolle *Netzwerkrichtlinien- und Zugriffsdienste*.
- Führen Sie den Setup-Assistenten für den Routing- und RAS-Server aus.
- Fügen Sie native IPv6-Fähigkeiten hinzu.
- Konfigurieren Sie eine Schnittstelle für Wählen bei Bedarf.

Installieren von Computerzertifikaten

Für L2TP/IPsec-Verbindungen oder falls der antwortende Router der Authentifizierungsserver ist und Sie die EAP-TLS-Authentifizierung einsetzen, müssen Sie ein Computerzertifikat auf dem antwortenden Router installieren. Welche Methoden zur Verfügung stehen, um ein Computerzertifikat zu installieren, ist im Abschnitt »Bereitstellen von Zertifikaten« weiter oben in diesem Kapitel beschrieben.

Konfigurieren der Verbindung des antwortenden Routers zum Standort

Bei IPv4 müssen Sie die Verbindung des antwortenden Routers zum Intranet mit einer manuellen TCP/IP-IPv4-Konfiguration versehen, die IPv4-Adresse, Subnetzmaske, Intranet-DNS-Server und Intranet-WINS-Server umfasst. Bei IPv6 müssen Sie die Verbindung des antwortenden Routers zum Intranet mit einer manuellen TCP/IP-IPv6-Konfiguration versehen, die IPv6-Adresse, 64-Bit-Präfix und Intranet-DNS-Server umfasst.

In beiden Fällen müssen Sie verhindern, dass Konflikte bei der Standardroute auftreten, weil die Standardroute in das IPv4- oder IPv6-Internet verweist. Deshalb dürfen Sie kein Standardgateway für die Intranetverbindung konfigurieren.

Installieren der Rolle *Netzwerkrichtlinien- und Zugriffsdienste*

Um Routing und RAS zu installieren, müssen Sie im Server-Manager die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* installieren.

Ausführen des Setup-Assistenten für den Routing- und RAS-Server

Der Setup-Assistent für den Routing- und RAS-Server automatisiert die Konfiguration vieler Elemente des antwortenden Routers. Die generierte Standardkonfiguration können Sie anschließend an Ihre speziellen Bereitstellungsanforderungen anpassen.

So führen Sie den Setup-Assistenten für den Routing- und RAS-Server aus

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf Ihren Servernamen und wählen Sie den Befehl *Routing und RAS konfigurieren und aktivieren*.
2. Klicken Sie auf der Seite *Willkommen* im Setup-Assistenten für den Routing- und RAS-Server auf *Weiter*.
3. Wählen Sie auf der Seite *Konfiguration* die Option *RAS (DFÜ oder VPN)* und klicken Sie auf *Weiter*.
4. Aktivieren Sie auf der Seite *RAS* das Kontrollkästchen *VPN* und klicken Sie auf *Weiter*.
5. Klicken Sie auf der Seite *VPN-Verbindung* auf die Verbindung, die mit dem Internet oder Ihrem Grenznetzwerk verbunden ist. Stellen Sie sicher, dass das Kontrollkästchen *Sicherheit auf der ausgewählten Schnittstelle durch Einrichten statischer Paketfilter aktivieren* aktiviert ist, und klicken Sie auf *Weiter*. Abbildung 13.3 zeigt ein Beispiel.

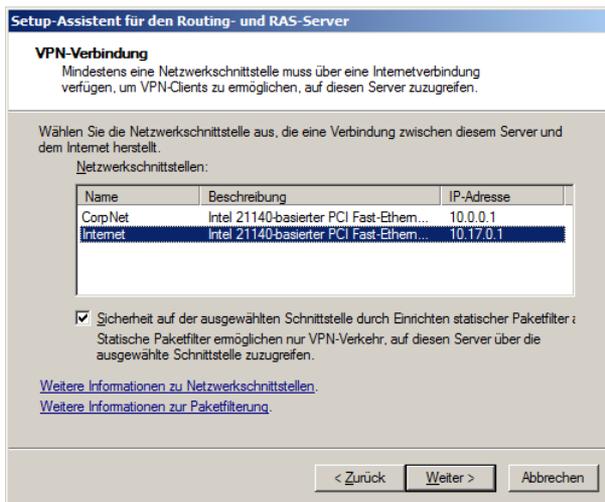


Abbildung 13.3 Die Assistentenseite *VPN-Verbindung*

6. Wählen Sie auf der Seite *Netzwerkauswahl* (wird nur angezeigt, falls Sie mehrere Netzwerkkarten mit dem Standort verbunden haben) die Verbindung aus, von der Routing und RAS die DHCP-, DNS- und WINS-Konfiguration für anrufende Router oder Remotezugriff-VPN-Clients abrufen soll. Klicken Sie auf *Weiter*, falls diese Seite angezeigt wird.
7. Wählen Sie auf der Seite *IP-Adresszuweisung* die Option *Automatisch* aus, falls der antwortende Router die IPv4-Adressen für anrufende Router und Remotezugriff-VPN-Clients über DHCP

abrufen soll. Stattdessen können Sie auch die Option *Aus einem angegebenen Adressbereich* wählen, wenn Sie eine oder mehrere IPv4-Adressbereiche verwenden wollen. Klicken Sie auf *Weiter*, wenn Sie die IPv4-Adresszuweisung abgeschlossen haben.

8. Falls Sie den antwortenden Router für die Authentifizierung und Autorisierung von eingehenden VPN-Verbindungsanforderungen einsetzen, müssen Sie auf der Seite *Mehrere RAS-Server verwalten* die Option *Nein, Routing und RAS zum Authentifizieren von Verbindungsanforderungen verwenden* wählen. Falls Sie RADIUS für Authentifizierung und Autorisierung einsetzen, müssen Sie die Option *Ja, diesen Server für die Verwendung eines RADIUS-Servers einrichten* wählen. Klicken Sie auf *Weiter*.
9. Falls Sie in Schritt 8 RADIUS ausgewählt haben, können Sie auf der Seite *RADIUS-Serverauswahl* den primären (muss immer eingetragen werden) und alternativen (optional) RADIUS-Server sowie den gemeinsamen geheimen Schlüssel für RADIUS konfigurieren (Abbildung 13.4). Klicken Sie auf *Weiter*, wenn Sie damit fertig sind.

Abbildung 13.4 Die Assistentenseite *RADIUS-Serverauswahl*

10. Klicken Sie auf der Seite *Fertigstellen des Assistenten* im Setup-Assistenten für den Routing- und RAS-Server auf *Fertig stellen*.
11. Falls der Setup-Assistent für den Routing- und RAS-Server die DHCP-Relay-Agent-Komponente nicht automatisch mit den IPv4-Adressen der DHCP-Server im Intranet konfigurieren kann, bekommen Sie eine entsprechende Meldung angezeigt. Klicken Sie auf *OK* oder auf *Hilfe*, um weitere Informationen zu erhalten.

Hinzufügen nativer IPv6-Fähigkeiten

Native IPv6-Fähigkeiten für Standort-zu-Standort-VPN-Verbindungen (das heißt IPv6-Pakete entweder innerhalb des VPN-Tunnels oder über eine native IPv6-VPN-Verbindung) werden in vielen Intranets vorerst nicht benötigt. Aus diesem Grund verzichtet der Setup-Assistent für den Routing- und RAS-Server darauf, native IPv6-Fähigkeiten für Standort-zu-Standort-VPN-Verbindungen über das IPv4- oder IPv6-Internet automatisch zu aktivieren.

Um für Standort-zu-Standort-VPN-Verbindungen in Routing und RAS native IPv6-Fähigkeiten zu konfigurieren, müssen Sie folgendermaßen vorgehen:

- Aktivieren Sie IPv6-Routing für LAN und bei Bedarf herzustellende Wählverbindungen.
- Konfigurieren Sie das Routerankündigungsverhalten.

So konfigurieren Sie die Unterstützung von nativem IPv6-Verkehr auf dem antwortenden Router

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf den Namen des VPN-Servers und wählen Sie den Befehl *Eigenschaften*.
2. Aktivieren Sie auf der Registerkarte *Allgemein* das Kontrollkästchen *IPv6-Router* und wählen Sie die Option *LAN und bei Bedarf wählendes Routing*.
3. Stellen Sie auf der Registerkarte *IPv6* sicher, dass die Kontrollkästchen *IPv6-Weiterleitung aktivieren* und *Standardroutenankündigung aktivieren* aktiviert sind. Geben Sie das Subnetzpräfix ein, das IPv6-VPN-Router zugewiesen wird, wenn sie eine Routererkennung durchführen. Sie brauchen keine Präfixlänge anzugeben. Sie können z.B. für das Subnetzpräfix 2001:db8:4a2c:29::/64 den Text »2001:db8:4a2c:29:« eingeben. Abbildung 13.5 zeigt ein Beispiel. Klicken Sie auf *OK*. Klicken Sie erneut auf *OK*, wenn Sie aufgefordert werden, den Router neu zu starten.

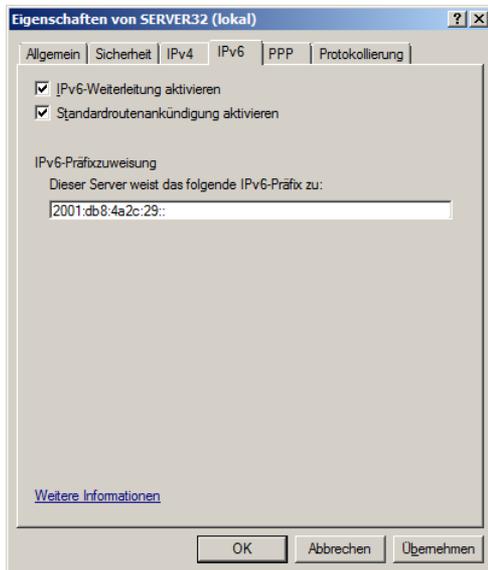


Abbildung 13.5 Die Registerkarte *IPv6* im Eigenschaftendialogfeld des Routing- und RAS-Servers

Konfigurieren einer Schnittstelle für Wählen bei Bedarf

Gehen Sie folgendermaßen vor, um mit dem Snap-In *Routing und RAS* auf dem antwortenden Router eine Schnittstelle für Wählen bei Bedarf zu erstellen und konfigurieren:

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf *Netzwerkschnittstellen* und wählen Sie den Befehl *Neue Schnittstelle für Wählen bei Bedarf*.
2. Klicken Sie auf der Seite *Willkommen* im Assistenten für eine Schnittstelle für Wählen bei Bedarf auf *Weiter*.
3. Geben Sie auf der Seite *Schnittstellename* den Namen der Schnittstelle für Wählen bei Bedarf ein. Bei einer bidirektional aufgebauten Verbindung ist dies derselbe Name wie der Benutzername in den Benutzeranmeldeinformationen, die der anrufende Router verwendet. Klicken Sie auf *Weiter*.

4. Wählen Sie auf der Seite *Verbindungstyp* die Option *Verbindung über ein virtuelles privates Netzwerk (VPN) herstellen* aus und klicken Sie auf *Weiter*.
5. Wählen Sie auf der Seite *VPN-Typ* nach Bedarf die Option *Automatische Auswahl, Point-to-Point-Tunneling-Protokoll (PPTP)* oder *Layer-2-Tunneling-Protokoll (L2TP)* aus und klicken Sie auf *Weiter*.
6. Geben Sie auf der Seite *Zieladresse* den Namen, die IPv4-Adresse oder die IPv6-Adresse des anrufenden Routers ein. Bei einer unidirektional aufgebauten Standort-zu-Standort-VPN-Verbindung können Sie diesen Schritt überspringen, weil der antwortende Router niemals diese Schnittstelle benutzt, um eine Verbindung zum anrufenden Router herzustellen.
7. Aktivieren Sie auf der Seite *Protokolle und Sicherheit* das Kontrollkästchen *Benutzerkonto hinzufügen, über das sich ein Remoterouter einwählen kann*, sofern Sie noch keine Benutzerkonten für die anrufenden Router erstellt haben. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Statische Routen für Remotenetzwerke* auf *Hinzufügen*, um eine statische Route hinzuzufügen, die der Schnittstelle für Wählen bei Bedarf zugewiesen wird. Abbildung 13.6 zeigt ein Beispiel.



Abbildung 13.6 Das Dialogfeld *Statische Route*

Fügen Sie alle statischen IPv4- und IPv6-Routen hinzu, die den IPv4- und IPv6-Adressraum des Standorts des anrufenden Routers abdecken. Klicken Sie auf *Weiter*.

9. Falls Sie vorher auf der Seite *Protokolle und Sicherheit* das Kontrollkästchen *Benutzerkonto hinzufügen, über das sich ein Remoterouter einwählen kann* aktiviert hatten, wird die Seite *Anmeldeinformationen für Einwählen* angezeigt (Abbildung 13.7).

Geben Sie in die Felder *Kennwort* und *Kennwort bestätigen* das Kennwort des Benutzerkontos ein, das der anrufende Router verwendet, und klicken Sie auf *Weiter*. Das Kennwort muss die Kennwortkomplexitätsanforderungen für Ihre Domäne erfüllen.

Bei diesem Schritt wird automatisch ein Benutzerkonto mit demselben Namen wie die Schnittstelle für Wählen bei Bedarf angelegt. Das geschieht, damit ein anrufender Router einen Benutzerkontonamen verwendet, der dem Namen einer Schnittstelle für Wählen bei Bedarf entspricht, wenn er eine Verbindung zu diesem antwortenden Router aufbaut. Auf diese Weise kann der antwortende Router erkennen, dass die eingehende Verbindung vom anrufenden Router eine bei Bedarf herzustellende Wählverbindung ist und keine Remotezugriffsverbindung.

10. Geben Sie auf der Seite *Anmeldeinformationen für Hinauswählen* im Feld *Benutzername* den Benutzernamen, im Feld *Domäne* den Namen der Kontodomäne und in den Feldern *Kennwort* und *Kennwort bestätigen* das Kontokennwort ein. Abbildung 13.8 zeigt ein Beispiel.

Anmeldeinformationen für Einwählen
 Konfiguriert den Benutzernamen und das Kennwort, die der Remoterouter beim Einwählen in diesen Server verwendet.

Sie müssen die Anmeldeinformationen festlegen, die Remoterouter verwenden, um eine Verbindung mit dieser Schnittstelle herzustellen. Die unten eingegebenen Informationen werden zum Erstellen eines Benutzerkontos verwendet.

Benutzername:

Kennwort:

Kennwort bestätigen:

< Zurück Weiter > Abbrechen

Abbildung 13.7 Die Seite *Anmeldeinformationen für Einwählen*

Anmeldeinformationen für Herauswählen
 Geben Sie den Benutzernamen und das Kennwort, die für die Verbindung mit dem Remoterouter verwendet werden sollen, an.

Sie müssen die Anmeldeinformationen festlegen, die diese Schnittstelle beim Herstellen einer Verbindung mit dem Remoterouter verwendet. Diese Einstellungen müssen mit den auf dem Remoterouter konfigurierten übereinstimmen.

Benutzername:

Domäne:

Kennwort:

Kennwort bestätigen:

< Zurück Weiter > Abbrechen

Abbildung 13.8 Die Seite *Anmeldeinformationen für Herauswählen*

Bei einer unidirektional aufgebauten Standort-zu-Standort-VPN-Verbindung können Sie im Feld *Benutzername* einen beliebigen Namen eingeben und die übrigen Felder leer lassen, weil dieser Router niemals diese Schnittstelle verwendet, um eine Verbindung zu einem anderen Router herzustellen. Klicken Sie auf *Weiter*.

11. Klicken Sie auf der Seite *Fertigstellen des Assistenten* auf *Fertig stellen*.

Das Ergebnis dieser Konfiguration ist eine VPN-Schnittstelle für Wählen bei Bedarf, die im Knoten *Netzwerkschnittstellen* des Snap-Ins *Routing und RAS* aufgeführt wird. Über diese Schnittstelle sind IPv4- und IPv6-Routing aktiviert. Falls Sie auf der Seite *Protokolle und Sicherheit* das Kontrollkästchen *Benutzerkonto hinzufügen, über das sich ein Remoterouter einwählen kann* aktiviert haben, wird ein Benutzerkonto mit demselben Namen wie die Schnittstelle für Wählen bei Bedarf automatisch mit den richtigen Konto- und Einwähleinstellungen hinzugefügt.

Bereitstellen von anrufenden Routern

Gehen Sie folgendermaßen vor, um einen anrufenden Router für eine Standort-zu-Standort-VPN-Verbindung bereitzustellen:

- Installieren Sie Computerzertifikate.
- Installieren Sie Benutzerzertifikate.
- Konfigurieren Sie die Verbindung des anrufenden Routers zum Standort.
- Installieren Sie die Rolle *Netzwerkrichtlinien- und Zugriffsdienste*.
- Führen Sie den Setup-Assistenten für den Routing- und RAS-Server aus.
- Fügen Sie native IPv6-Fähigkeiten hinzu.
- Konfigurieren Sie eine Schnittstelle für Wählen bei Bedarf.
- Konfigurieren Sie Leerlaufzeitlimits oder eine persistente Verbindung.
- Konfigurieren Sie Filter für Wählen bei Bedarf.
- Konfigurieren Sie Hinauswählzeiten.
- Konfigurieren Sie die EAP-TLS-Authentifizierung.

Installieren von Computerzertifikaten

Für L2TP/IPsec-Verbindungen müssen Sie ein Computerzertifikat auf dem anrufenden Router installieren. Welche Methoden zur Verfügung stehen, um ein Computerzertifikat zu installieren, ist im Abschnitt »Bereitstellen von Zertifikaten« weiter oben in diesem Kapitel beschrieben.

Installieren von Benutzerzertifikaten

Für EAP-TLS-authentifizierte Verbindungen müssen Sie ein Benutzerzertifikat auf dem anrufenden Router installieren. Welche Methoden zur Verfügung stehen, um ein Benutzerzertifikat zu installieren, ist im Abschnitt »Bereitstellen von Zertifikaten« weiter oben in diesem Kapitel beschrieben.

Konfigurieren der Verbindung des anrufenden Routers zum Standort

Bei IPv4 müssen Sie die Verbindung des anrufenden Routers zum Intranet mit einer manuellen TCP/IP-IPv4-Konfiguration versehen, die IPv4-Adresse, Subnetzmaske, Intranet-DNS-Server und Intranet-WINS-Server umfasst. Bei IPv6 müssen Sie die Verbindung des anrufenden Routers zum Intranet mit einer manuellen TCP/IP-IPv6-Konfiguration versehen, die IPv6-Adresse, 64-Bit-Präfix und Intranet-DNS-Server umfasst. In beiden Fällen müssen Sie verhindern, dass Konflikte bei der Standardroute auftreten, weil die Standardroute in das IPv4- oder IPv6-Internet verweist. Deshalb dürfen Sie kein Standardgateway für die Intranetverbindung konfigurieren.

Installieren der Rolle *Netzwerkrichtlinien- und Zugriffsdienste*

Um Routing und RAS zu installieren, müssen Sie im Server-Manager die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* installieren.

Ausführen des Setup-Assistenten für den Routing- und RAS-Server

Wenn Sie in Windows Server 2008 die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* installiert haben, können Sie den Setup-Assistenten für den Routing- und RAS-Server ausführen, um den anrufenden Router zu konfigurieren.

So führen Sie den Setup-Assistenten für den Routing- und RAS-Server aus

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf Ihren Servernamen und wählen Sie den Befehl *Routing und RAS konfigurieren und aktivieren*.
2. Klicken Sie auf der Seite *Willkommen* im Setup-Assistenten für den Routing- und RAS-Server auf *Weiter*.
3. Wählen Sie auf der Seite *Konfiguration* die Option *RAS (DFÜ oder VPN)* und klicken Sie auf *Weiter*.
4. Aktivieren Sie auf der Seite *RAS* das Kontrollkästchen *VPN* und klicken Sie auf *Weiter*.
5. Klicken Sie auf der Seite *VPN-Verbindung* auf die Verbindung mit dem Internet oder Ihrem Grenznetzwerk und dann auf *Weiter*.
6. Wählen Sie auf der Seite *Netzwerkauswahl* (wird nur angezeigt, falls Sie mehrere Netzwerkkarten mit dem Standort verbunden haben) die Verbindung aus, von der Routing und RAS die DHCP-, DNS- und WINS-Konfiguration für andere anrufende Router oder Remotezugriff-VPN-Clients abrufen soll. Klicken Sie auf *Weiter*, falls diese Seite angezeigt wird.
7. Wählen Sie auf der Seite *IP-Adresszuweisung* die Option *Automatisch* aus, falls der anrufende Router die IPv4-Adressen für andere anrufende Router und Remotezugriff-VPN-Clients über DHCP abrufen soll. Stattdessen können Sie auch die Option *Aus einem angegebenen Adressbereich* wählen, wenn Sie eine oder mehrere IPv4-Adressbereiche verwenden wollen. Klicken Sie auf *Weiter*, wenn Sie die IPv4-Adresszuweisung abgeschlossen haben.
8. Falls Sie den anrufenden Router für die Authentifizierung und Autorisierung von anderen anrufenden Routern einsetzen, müssen Sie auf der Seite *Mehrere RAS-Server verwalten* die Option *Nein, Routing und RAS zum Authentifizieren von Verbindungsanforderungen verwenden* wählen. Falls Sie RADIUS für Authentifizierung und Autorisierung einsetzen, müssen Sie die Option *Ja, diesen Server für die Verwendung eines RADIUS-Servers einrichten* wählen. Klicken Sie auf *Weiter*.
9. Falls Sie in Schritt 8 RADIUS ausgewählt haben, können Sie auf der Seite *RADIUS-Serverauswahl* die Namen, IPv4-Adressen oder IPv6-Adressen des primären (muss immer eingetragen werden) und alternativen (optional) RADIUS-Servers sowie den gemeinsamen geheimen Schlüssel für RADIUS konfigurieren. Klicken Sie auf *Weiter*, wenn Sie damit fertig sind.
10. Klicken Sie auf der Seite *Fertigstellen des Assistenten* im Setup-Assistenten für den Routing- und RAS-Server auf *Fertig stellen*.
11. Falls der Setup-Assistent für den Routing- und RAS-Server die DHCP-Relay-Agent-Komponente nicht automatisch mit den IPv4-Adressen der DHCP-Server im Intranet konfigurieren kann, bekommen Sie eine entsprechende Meldung angezeigt. Klicken Sie auf *OK* oder auf *Hilfe*, um weitere Informationen zu erhalten.

Hinzufügen nativer IPv6-Fähigkeiten

Native IPv6-Fähigkeiten für Standort-zu-Standort-VPN-Verbindungen (das heißt IPv6-Pakete entweder innerhalb des VPN-Tunnels oder über eine native IPv6-VPN-Verbindung) wird in vielen Intranets vorerst nicht benötigt. Aus diesem Grund verzichtet der Setup-Assistent für den Routing- und RAS-Server darauf, native IPv6-Fähigkeiten für Standort-zu-Standort-VPN-Verbindungen über das IPv4- oder IPv6-Internet automatisch zu aktivieren.

Um für Standort-zu-Standort-VPN-Verbindungen in Routing und RAS native IPv6-Fähigkeiten zu konfigurieren, müssen Sie folgendermaßen vorgehen:

- Aktivieren Sie IPv6-Routing für LAN und bei Bedarf herzustellende Wählverbindungen.
- Konfigurieren Sie das Routerankündigungsverhalten.

So konfigurieren Sie die Unterstützung von nativem IPv6-Verkehr auf dem antwortenden Router

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf den Namen des VPN-Servers und wählen Sie den Befehl *Eigenschaften*.
2. Aktivieren Sie auf der Registerkarte *Allgemein* das Kontrollkästchen *IPv6-Router* und wählen Sie die Option *LAN und bei Bedarf wählendes Routing*.
3. Stellen Sie auf der Registerkarte *IPv6* sicher, dass die Kontrollkästchen *IPv6-Weiterleitung aktivieren* und *Standardroutenankündigung aktivieren* aktiviert sind. Geben Sie dasselbe Subnetzpräfix ein wie beim antwortenden Router. Sie brauchen keine Präfixlänge anzugeben. Klicken Sie auf *OK*. Klicken Sie erneut auf *OK*, wenn Sie aufgefordert werden, den Router neu zu starten.

Konfigurieren einer Schnittstelle für Wählen bei Bedarf

Gehen Sie folgendermaßen vor, um mit dem Snap-In *Routing und RAS* auf dem anrufenden Router eine Schnittstelle für Wählen bei Bedarf zu erstellen und konfigurieren:

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf *Netzwerkschnittstellen* und wählen Sie den Befehl *Neue Schnittstelle für Wählen bei Bedarf*.
2. Klicken Sie auf der Seite *Willkommen* im Assistenten für eine Schnittstelle für Wählen bei Bedarf auf *Weiter*.
3. Geben Sie auf der Seite *Schnittstellename* den Namen der Schnittstelle für Wählen bei Bedarf ein. Bei einer bidirektional aufgebauten Verbindung ist dies derselbe Name wie der Benutzername in den Benutzeranmeldeinformationen, die ein anderer anrufender Router verwendet. Klicken Sie auf *Weiter*.
4. Wählen Sie auf der Seite *Verbindungstyp* die Option *Verbindung über ein virtuelles privates Netzwerk (VPN) herstellen* aus und klicken Sie auf *Weiter*.
5. Wählen Sie auf der Seite *VPN-Typ* nach Bedarf die Option *Automatische Auswahl, Point-to-Point-Tunneling-Protokoll (PPTP)* oder *Layer-2-Tunneling-Protokoll (L2TP)* aus und klicken Sie auf *Weiter*.
6. Geben Sie auf der Seite *Zieladresse* den Namen, die IPv4-Adresse oder die IPv6-Adresse des anrufenden Routers ein.
7. Aktivieren Sie auf der Seite *Protokolle und Sicherheit* für eine bidirektional aufgebaute Verbindung das Kontrollkästchen *Benutzerkonto hinzufügen, über das sich ein Remoterouter einwählen kann*, sofern Sie noch keine Benutzerkonten für die anrufenden Router erstellt haben. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Statische Routen für Remotenetzwerke* auf *Hinzufügen*, um eine statische Route hinzuzufügen, die der Schnittstelle für Wählen bei Bedarf zugewiesen wird. Fügen Sie alle statischen IPv4- und IPv6-Routen hinzu, die den IPv4- und IPv6-Adressraum des Standorts des antwortenden Routers abdecken. Klicken Sie auf *Weiter*.
9. Falls Sie vorher auf der Seite *Protokolle und Sicherheit* das Kontrollkästchen *Benutzerkonto hinzufügen, über das sich ein Remoterouter einwählen kann* aktiviert hatten, wird die Seite *Anmeldeinformationen für Einwählen* angezeigt. Geben Sie in die Felder *Kennwort* und *Kennwort bestätigen*.

gen das Kennwort des Benutzerkontos ein, das der andere anrufende Router verwendet, und klicken Sie auf *Weiter*. Das Kennwort muss die Kennwortkomplexitätsanforderungen für Ihre Domäne erfüllen.

Bei diesem Schritt wird automatisch ein Benutzerkonto mit demselben Namen wie die Schnittstelle für Wählen bei Bedarf angelegt. Das geschieht, damit ein anderer anrufender Router einen Benutzerkontonamen verwendet, der dem Namen einer Schnittstelle für Wählen bei Bedarf entspricht, wenn er eine Verbindung zu diesem Router aufbaut. Auf diese Weise kann dieser Router erkennen, dass die eingehende Verbindung eine bei Bedarf herzustellende Wählverbindung ist und keine Remotezugriffsverbindung.

10. Geben Sie auf der Seite *Anmeldeinformationen für Hinauswählen* im Feld *Benutzername* den Benutzernamen, im Feld *Domäne* den Namen der Kontodomäne und in den Feldern *Kennwort* und *Kennwort bestätigen* das Kontokennwort ein. Klicken Sie auf *Weiter*.

11. Klicken Sie auf der Seite *Fertigstellen des Assistenten* auf *Fertig stellen*.

Das Ergebnis dieser Konfiguration ist eine Schnittstelle für Wählen bei Bedarf, über die IPv4- und IPv6-Routing aktiviert sind. Falls Sie auf der Seite *Protokolle und Sicherheit* das Kontrollkästchen *Benutzerkonto hinzufügen, über das sich ein Remoterouter einwählen kann* aktiviert haben, wird ein Benutzerkonto mit demselben Namen wie die Schnittstelle für Wählen bei Bedarf automatisch mit den richtigen Konto- und Einwähleinstellungen hinzugefügt.

Konfigurieren von Leerlaufzeitlimits oder einer persistenten Verbindung

In der Standardeinstellung konfiguriert der Assistent für eine Schnittstelle für Wählen bei Bedarf eine solche Schnittstelle mit einem Leerlaufzeitlimit von 5 Minuten, nach dem die Verbindung getrennt wird. Sie können das Verhalten für die automatische Trennung auf dem anrufenden Router im Snap-In *Routing und RAS* konfigurieren. Öffnen Sie dort über den Knoten *Netzwerkschnittstellen* das Eigenschaftendialogfeld der Schnittstelle für Wählen bei Bedarf und klicken Sie auf die Registerkarte *Optionen*.

Sie können eine automatische Trennung nach der angegebenen Leerlaufzeit für einen antwortenden Router konfigurieren, indem Sie im Snap-In *Netzwerkrichtlinienserver* das Eigenschaftendialogfeld der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen öffnen und auf der Registerkarte *Einschränkungen* die gewünschten Einstellungen für das Leerlaufzeitlimit eintragen.

Sie können eine persistente Verbindung für den anrufenden Router konfigurieren, indem Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld der Schnittstelle für Wählen bei Bedarf öffnen und auf der Registerkarte *Optionen* die Option *Persistente Verbindung* wählen.

Sie können eine persistente Verbindung für den antwortenden Router konfigurieren, indem Sie im Snap-In *Netzwerkrichtlinienserver* das Eigenschaftendialogfeld der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen öffnen, auf der Registerkarte *Einschränkungen* auf *Leerlaufzeitlimit* klicken und das Kontrollkästchen *Verbindung nach maximaler Leerlaufzeit trennen* deaktivieren.

Konfigurieren von Filtern für Wählen bei Bedarf

Sie können Filter für Wählen bei Bedarf konfigurieren, die auf IPv4- oder IPv6-Verkehr angewendet werden. Klicken Sie dazu im Snap-In *Routing und RAS* im Knoten *Netzwerkschnittstellen* mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf und wählen Sie den Befehl *Filter für Wählen bei Bedarf einrichten* oder *IPv6-Filter für Wählen bei Bedarf einrichten*.

Folgendermaßen können Sie verhindern, dass der anrufende Router eine Verbindung für Verkehr aufbaut, der überhaupt nicht über die Schnittstelle für Wählen bei Bedarf erlaubt ist:

- Falls Sie für die Schnittstelle für Wählen bei Bedarf im Knoten *IPv4\Allgemein* oder *IPv6\Allgemein* des Snap-Ins *Routing und RAS* einen Satz von ausgehenden IPv4- oder IPv6-Paketfiltern mit der Option *Alle Pakete übertragen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* konfiguriert haben, müssen Sie denselben Satz von Filtern für Wählen bei Bedarf konfigurieren, wobei Sie unter *Verbindung initiieren* die Option *Für den gesamten Datenverkehr mit Ausnahme der folgenden Einträge* auswählen.
- Falls Sie für die Schnittstelle für Wählen bei Bedarf im Knoten *IPv4\Allgemein* oder *IPv6\Allgemein* des Snap-Ins *Routing und RAS* einen Satz von ausgehenden IPv4- oder IPv6-Paketfiltern mit der Option *Alle Pakete verwerfen außer den Paketen, die die unten aufgeführten Kriterien erfüllen* konfiguriert haben, müssen Sie denselben Satz von Filtern für Wählen bei Bedarf konfigurieren, wobei Sie unter *Verbindung initiieren* die Option *Nur für folgenden Datenverkehr* auswählen.

Konfigurieren von Hinauswählzeiten

Sie können Hinauswählzeiten konfigurieren, indem Sie im Snap-In *Routing und RAS* im Knoten *Netzwerkschnittstellen* mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf klicken und den Befehl *Hinauswählzeiten* wählen. Wählen Sie aus, zu welchen Zeiten eine bei Bedarf herzustellende Wählverbindung aufgebaut werden darf, und klicken Sie auf *OK*.

Sie können auf dem antwortenden Router konfigurieren, zu welchen Zeiten eingehende bei Bedarf herzustellende Wählverbindungen zugelassen sind. Öffnen Sie dazu im Snap-In *Netzwerkrichtlinien-server* das Eigenschaftendialogfeld der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen und konfigurieren Sie auf der Registerkarte *Einschränkungen* die Einstellung unter *Tag- und Uhrzeiteinschränkungen*.

Konfigurieren der EAP-TLS-Authentifizierung

Gehen Sie folgendermaßen vor, um auf dem anrufenden Router EAP-TLS für Benutzerzertifikate zu konfigurieren:

1. Klicken Sie im Snap-In *Routing und RAS* im Knoten *Netzwerkschnittstellen* doppelt auf die Schnittstelle für Wählen bei Bedarf.
2. Klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *Sicherheit*, wählen Sie die Option *Erweitert (benutzerdefinierte Einstellungen)* und klicken Sie auf *Einstellungen*.
3. Wählen Sie unter *Anmeldesicherheit* die Option *Extensible-Authentication-Protokoll (EAP) verwenden* aus, wählen Sie in der Dropdownliste den Eintrag *Smartcard- oder anderes Zertifikat (Verschlüsselung aktiviert)* und klicken Sie auf die Schaltfläche *Eigenschaften*.
4. Wählen Sie im Dialogfeld *Smartcard- oder andere Zertifikateigenschaften* die Option *Zertifikat auf diesem Computer verwenden* aus. Die Überprüfung des Computerzertifikats des Authentifizierungsservers ist in der Standardeinstellung aktiviert. Falls Sie die Namen der Authentifizierungsserver (zum Beispiel der RADIUS-Server) konfigurieren wollen, können Sie das Kontrollkästchen *Verbindung mit diesen Servern herstellen* aktivieren und dann die Servernamen eingeben. Wenn Sie wollen, dass das Computerzertifikat des Servers mithilfe eines Zertifikats einer bestimmten vertrauenswürdigen Stammzertifizierungsstelle ausgestellt sein muss, können Sie im Listefeld *Vertrauenswürdige Stammzertifizierungsstellen* die gewünschte Zertifizierungsstelle aktivieren.
5. Klicken Sie dreimal auf *OK*.

Sie können das Zertifikat auswählen, das während der EAP-TLS-Authentifizierung verwendet wird, indem Sie mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf klicken und den Befehl *Anmeldeinformationen festlegen* wählen. Wählen Sie im Dialogfeld *Anmeldeinformationen für die Schnittstelle* unter *Benutzername auf dem Zertifikat* den richtigen Benutzer oder *Router (Offline-anforderung)* aus und klicken Sie auf *OK*.

Konfigurieren der Standortnetzwerkinfrastruktur

Gehen Sie folgendermaßen vor, um die Netzwerkinfrastruktur eines Standorts für Standort-zu-Standort-VPN-Verbindungen bereitzustellen:

- Konfigurieren Sie das Routing auf den VPN-Routern.
- Überprüfen Sie die Erreichbarkeit auf jedem VPN-Router.
- Konfigurieren Sie das Routing für Adresspools außerhalb des eigenen Subnetzes.
- Konfigurieren Sie das Routing für das IPv6-Subnetzpräfix der VPN-Router.

Konfigurieren des Routings auf den VPN-Routern

Damit Ihre VPN-Router Verkehr an Adressen innerhalb des eigenen Standorts richtig weiterleiten können, müssen Sie diese VPN-Router mit statischen IPv4- und IPv6-Routen konfigurieren, die alle IPv4- und IPv6-Adressräume abdecken, die innerhalb des Standorts benutzt werden. Bei IPv4 können Sie RIP als IPv4-Routingprotokoll einsetzen, sodass der VPN-Router automatisch IPv4-Routen für die Standortsnetze zu seiner Routingtabelle hinzufügen kann.

So fügen Sie statische IPv4-Routen für standortinternen Verkehr hinzu

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv4*.
2. Klicken Sie mit der rechten Maustaste auf *Statische Routen* und wählen Sie den Befehl *Neue statische Route*.
3. Wählen Sie im Dialogfeld *Statische IPv4-Route* (Abbildung 13.9) die Standortschnittstelle aus und geben Sie Ziel, Netzwerkmaske, Gateway und Metrik für die statische Route ein. Klicken Sie auf *OK*.

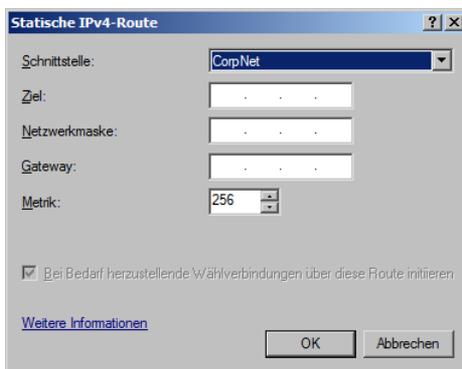


Abbildung 13.9 Das Dialogfeld *Statische IPv4-Route*

4. Wiederholen Sie die Schritte 2 und 3, wenn Sie weitere statische IPv4-Routen hinzufügen wollen.

So fügen Sie statische IPv6-Routen für standortinternen Verkehr hinzu

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv6*.
2. Klicken Sie mit der rechten Maustaste auf *Statische Routen* und wählen Sie den Befehl *Neue statische Route*.
3. Nehmen Sie im Dialogfeld *Statische IPv6-Route* (Abbildung 13.10) folgende Einstellungen vor:
 - a. Wählen Sie die Standortschnittstelle aus.
 - b. Geben Sie im Feld *Ziel* das Adresspräfix ein.
 - c. Geben Sie im Feld *Präfixlänge* die Präfixlänge für das Adresspräfix ein. Bei Subnetzadresspräfixen beträgt die Präfixlänge 64.
 - d. Geben Sie im Feld *Gateway* die verbindungslokale Adresse eines benachbarten Intranet-IPv6-Routers ein.
 - e. Geben Sie im Feld *Metrik* die Metrik für die Route ein.

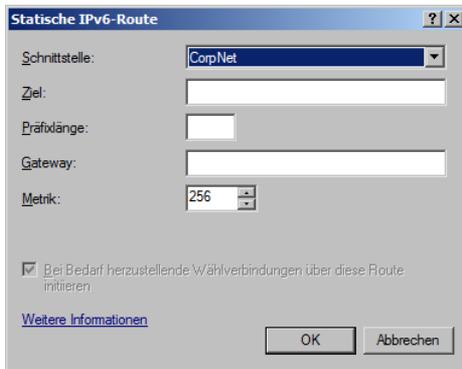


Abbildung 13.10 Das Dialogfeld *Statische IPv6-Route*

4. Klicken Sie auf *OK*.
5. Wiederholen Sie die Schritte 2 bis 4, wenn Sie weitere statische IPv6-Routen hinzufügen wollen.



Hinweis Sie brauchen nur dann statische IPv6-Routen für den Standort hinzuzufügen, wenn Sie Ihre VPN-Router mit nativen IPv6-Fähigkeiten konfiguriert haben.

So konfigurieren Sie den VPN-Router als RIP-Router für IPv4

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv4*.
2. Klicken Sie mit der rechten Maustaste auf *Allgemein* und wählen Sie den Befehl *Neues Routingprotokoll*.
3. Klicken Sie im Listenfeld *Routingprotokolle* auf *RIP, Version 2, für das Internetprotokoll*. Klicken Sie auf *OK*.
4. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *RIP* und wählen Sie den Befehl *Neue Schnittstelle*.
5. Klicken Sie auf die Standortschnittstelle des VPN-Routers und dann auf *OK*.

6. Konfigurieren Sie im Dialogfeld *Eigenschaften von RIP* das RIP-Routingprotokoll, sodass es den Einstellungen des benachbarten RIP-Routers im Intranetsubnetz des VPN-Routers entspricht. Klicken Sie auf *OK*.

Überprüfen der Erreichbarkeit aller VPN-Router

Überprüfen Sie auf jedem VPN-Router, ob der VPN-Routercomputer erfolgreich mit Ressourcen innerhalb des eigenen Standorts kommunizieren kann. Dafür können Sie den Befehl Ping und den Windows Internet Explorer verwenden. Außerdem können Sie Laufwerk- und Druckerverbindungen zu bekannten Servern innerhalb des Standorts herstellen.

Konfigurieren des Routings für Adresspools außerhalb des eigenen Subnetzes

Falls Sie irgendwelche VPN-Router mit IPv4-Adresspools konfiguriert haben und irgendwelche dieser Adressbereiche außerhalb des eigenen Subnetzes liegen, müssen Sie sicherzustellen, dass die IPv4-Routen für diese subnetzexternen Adressbereiche in Ihrer Standortroutinginfrastruktur eingetragen sind, damit die VPN-Schnittstellen von anrufenden Routern erreichbar sind. Sie können das sicherstellen, indem Sie Routen für die subnetzexternen Adressbereiche zu den benachbarten Routern des VPN-Routers hinzufügen und die Routen dann mithilfe des in Ihrem Standort verwendeten Routingprotokolls an andere Router weiterverbreiten. Wenn Sie die statischen Routen hinzufügen, müssen Sie angeben, dass das Gateway oder die Adresse des nächsten Abschnitts (engl. hop) die Standortchnittstelle des VPN-Routers ist.

Konfigurieren des Routings für das IPv6-Subnetzpräfix von VPN-Routern

Um sicherzustellen, dass die VPN-Schnittstellen von IPv6-fähigen VPN-Routern aus dem Intranet heraus erreichbar sind, müssen Sie eine statische Route für das Subnetzpräfix der anrufenden Router zu den benachbarten IPv6-Routern des VPN-Routers hinzufügen und diese Routen dann mithilfe des Routingprotokolls, das in Ihrem Standort eingesetzt wird, an andere Router weiterverbreiten. Wenn Sie die statischen Routen hinzufügen, müssen Sie angeben, dass das Gateway oder die Adresse des nächsten Abschnitts die verbindungslokale IPv6-Adresse der Intranetschnittstelle des VPN-Routers ist.

Konfigurieren der Infrastruktur für die Standortverbindungen

Um die Standortverbindungs-Netzwerkinfrastruktur bereitzustellen, müssen Sie auf allen VPN-Routern einen Satz von Routen für den IPv4- und IPv6-Adressraum konfigurieren, der in den anderen Standorten (über die Standort-zu-Standort-VPN-Verbindung) verfügbar ist. Im Assistenten für eine Schnittstelle für Wählen bei Bedarf können Sie auf der Seite *Statische Routen für Remotenetzwerke* statische IPv4- oder IPv6-Routen hinzufügen, die der Schnittstelle für Wählen bei Bedarf zugewiesen werden. Diese Routen decken den IPv4- und IPv6-Adressraum im Standort des anderen VPN-Routers ab. Falls Sie weitere Routen hinzufügen müssen, haben Sie folgende Möglichkeiten zur Auswahl:

- Konfigurieren Sie von Hand statische Routen auf allen VPN-Routern.
- Führen Sie autostatische Aktualisierungen auf allen VPN-Routern durch.
- Konfigurieren Sie Routingprotokolle, die über die Standort-zu-Standort-VPN-Verbindung arbeiten.

Statische Routen manuell auf allen VPN-Routern konfigurieren

Zusätzliche statische IPv4- oder IPv6-Routen können Sie von Hand konfigurieren.

So fügen Sie statische IPv4-Routen für Standortverbindungsverkehr hinzu

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv4*.
2. Klicken Sie mit der rechten Maustaste auf *Statische Routen* und wählen Sie den Befehl *Neue statische Route*.
3. Wählen Sie im Dialogfeld *Statische IPv4-Route* die Schnittstelle für Wählen bei Bedarf aus und geben Sie Ziel, Netzwerkmaske und Metrik für die statische Route ein, die die Verbindung zum anderen Standort über die bei Bedarf herzustellende Wählverbindung herstellt. Sie können auch das Kontrollkästchen *Bei Bedarf herzustellende Wählverbindungen über diese Route initiieren* aktivieren, um bei Bedarf eine Wählverbindung aufzubauen, wenn Verkehr über diese Route weitergeleitet werden muss. Klicken Sie auf *OK*.
4. Wiederholen Sie die Schritte 2 und 3, wenn Sie weitere statische IPv4-Routen hinzufügen wollen.



Hinweis Weil die bei Bedarf herzustellende Wählverbindung eine Punkt-zu-Punkt-Verbindung ist, können Sie bei den Routen solcher Schnittstellen das Feld *Gateway* nicht konfigurieren.

So fügen Sie statische IPv6-Routen für Standortverbindungsverkehr hinzu

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv6*.
2. Klicken Sie mit der rechten Maustaste auf *Statische Routen* und wählen Sie den Befehl *Neue statische Route*.
3. Wählen Sie im Dialogfeld *Statische IPv6-Route* die Schnittstelle für Wählen bei Bedarf aus und geben Sie Ziel, Präfixlänge und Metrik für die statische Route ein, die die Verbindung zum anderen Standort über die bei Bedarf herzustellende Wählverbindung aufbaut. Sie können auch das Kontrollkästchen *Bei Bedarf herzustellende Wählverbindungen über diese Route initiieren* aktivieren, um bei Bedarf eine Wählverbindung aufzubauen, wenn Verkehr über diese Route weitergeleitet werden muss. Klicken Sie auf *OK*.
4. Wiederholen Sie die Schritte 2 und 3, wenn Sie weitere statische IPv6-Routen hinzufügen wollen.



Hinweis Statische IPv6-Standortverbindungsrouen brauchen Sie nur hinzuzufügen, wenn Sie Ihre VPN-Router mit nativen IPv6-Fähigkeiten konfiguriert haben.

Durchführen autostatischer Aktualisierungen auf allen VPN-Routern

Falls für die Schnittstelle für Wählen bei Bedarf auf beiden VPN-Routern RIP für IPv4 aktiviert ist, können Sie autostatische Aktualisierungen verwenden, um automatisch statische IPv4-Routen zu konfigurieren, wenn die VPN-Verbindung aufgebaut ist.

So leiten Sie eine autostatische Aktualisierung ein

1. Erweitern Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* den Knoten *IPv4* und klicken Sie auf *Allgemein*.
2. Sehen Sie sich in der Detailansicht die Spalte *Betriebsstatus* der Schnittstelle für Wählen bei Bedarf an. Stellen Sie sicher, dass eine Verbindung besteht.
3. Klicken Sie mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf und wählen Sie den Befehl *Routen aktualisieren*.

Sie können auch an einer Eingabeaufforderung Netsh-Befehle ausführen, um autostatische Aktualisierungen durchzuführen. Mit einer Kombination aus Netsh-Skripten und der Aufgabenplanung können Sie regelmäßige Aktualisierungen automatisieren. Führen Sie die folgenden Netsh-Befehle aus, um eine automatisierte autostatische Aktualisierung mithilfe von RIP für IP für die angegebene Schnittstelle für Wählen bei Bedarf durchzuführen:

```
netsh interface set interface name=Schnittstelle connect=CONNECTED
netsh routing ip rip update name=Schnittstelle
netsh interface set interface name=Schnittstelle connect=DISCONNECTED
```

Zum Beispiel aktualisieren Sie mit den folgenden Netsh-Befehlen die IP-Routen für eine bei Bedarf herzustellende Wählverbindung namens CorpHub:

```
netsh interface set interface name=CorpHub connect=CONNECTED
netsh routing ip rip update name=CorpHub
netsh interface set interface name=CorpHub connect=DISCONNECTED
```

Sie können diese Befehle aus einer Batchdatei heraus ausführen oder in eine Netsh-Skriptdatei eintragen. Zum Beispiel könnte die Skriptdatei *Corphub.scp* die folgenden Netsh-Befehle für die Schnittstelle CorpHub ausführen:

```
interface set interface name=CorpHub connect=CONNECTED
routing ip rip update name=CorpHub
interface set interface name=CorpHub connect=DISCONNECTED
```

Das Skript *Corphub.scp* können Sie mit dem folgenden Befehl an einer Eingabeaufforderung ausführen:

```
netsh -f corphub.scp
```

Wenn Sie die Batchdatei oder Netsh-Skriptdatei erstellt haben, können Sie die Batchdatei oder das Netsh-Skript mithilfe der Aufgabenplanung regelmäßig ausführen lassen.

Konfigurieren von Routingprotokollen

Falls die Standort-zu-Standort-VPN-Verbindung dauerhaft aufgebaut bleibt, können Sie auf der Schnittstelle für Wählen bei Bedarf auf beiden VPN-Routern auch das Routingprotokoll RIP für IPv4 konfigurieren, sodass alle VPN-Router automatisch mit IPv4-Routen aktualisiert werden.

Wartung

Bei einer Standort-zu-Standort-VPN-Lösung müssen folgende Wartungsaufgaben durchgeführt werden:

- Verwalten von Benutzerkonten
- Verwalten von VPN-Routern

Verwalten von Benutzerkonten

Wenn ein neues Benutzerkonto für einen anrufenden Router in Active Directory angelegt wurde (entweder von Hand oder im Assistenten für eine Schnittstelle für Wählen bei Bedarf), müssen Sie das neue Benutzerkonto zur entsprechenden Gruppe für Standort-zu-Standort-VPN-Verbindungen hinzufügen. Zum Beispiel können Sie das Konto zur Sicherheitsgruppe *VPNRouter* hinzufügen, die in der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen eingetragen ist.

Wenn Benutzerkonten in Active Directory gelöscht werden, sind keine weiteren Aktionen nötig, um Standort-zu-Standort-VPN-Verbindungen zu verhindern.

Verwalten von VPN-Routern

Sie müssen unter Umständen VPN-Router verwalten, wenn Sie einen VPN-Router in Ihrer Standort-zu-Standort-VPN-Lösung hinzufügen oder entfernen. Wenn VPN-Router erst einmal bereitgestellt wurden, benötigen sie kaum noch Wartung. Die meisten Änderungen an einer funktionierenden Konfiguration werden aufgrund von Kapazitätsproblemen und Änderungen an der Netzwerkinfrastruktur nötig.

Hinzufügen eines VPN-Routers

Gehen Sie folgendermaßen vor, um einen VPN-Router hinzuzufügen:

1. Folgen Sie den Anleitungen in den Abschnitten zu Entwurfsaspekten und Bereitstellung in diesem Kapitel, um einen neuen VPN-Router im Internet einzurichten.
2. Stellen Sie sicher, dass anrufende Router, die antwortende Router über ihre Name ansprechen, den neuen antwortenden Router anhand seines Namens erreichen können. Aktualisieren Sie dazu im Internet-DNS die entsprechenden A- und AAAA-Datensätze für die IPv4- oder IPv6-Adresse des neuen antwortenden Routers oder fügen Sie einen neuen Eintrag hinzu.
3. Aktualisieren Sie Ihre RADIUS-Serverkonfiguration, sodass der antwortende Router als RADIUS-Client eingetragen ist.

Entfernen eines VPN-Routers

Gehen Sie folgendermaßen vor, um einen VPN-Router zu entfernen:

1. Aktualisieren oder entfernen Sie im Internet-DNS den FQDN für die IPv4- oder IPv6-Adresse des antwortenden Routers.
2. Aktualisieren Sie Ihre RADIUS-Serverkonfiguration, indem Sie den antwortenden Router als RADIUS-Client entfernen.
3. Fahren Sie den VPN-Router herunter und entfernen Sie ihn.
4. Aktualisieren oder löschen Sie bei den anrufenden Routern, die dem antwortenden Router zugeordnet waren, die Schnittstelle für Wählen bei Bedarf, die so konfiguriert ist, dass sie eine Verbindung zu dem antwortenden Router herstellt, den Sie gerade entfernt haben.

Vergrößern der Zahl möglicher Verbindungen

In der Standardeinstellung konfiguriert der Setup-Assistent für den Routing- und RAS-Server Routing und RAS mit einer eingeschränkten Zahl von PPTP- und L2TP-Ports. Sie können die maximale Zahl von Ports für ein VPN-Protokoll folgendermaßen erhöhen:

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* mit der rechten Maustaste auf *Ports* und wählen Sie den Befehl *Eigenschaften*.
2. Klicken Sie im Dialogfeld *Eigenschaften von Ports* doppelt auf das WAN-Miniport-Gerät, das dem gewünschten VPN-Protokoll zugeordnet ist.
3. Tragen Sie im Dialogfeld *Gerät konfigurieren* im Feld *Maximale Portanzahl* die maximale Zahl von Ports ein und klicken Sie zweimal auf *OK*.

Konfigurationsschritte bei Änderungen an Infrastrukturservern

Infrastrukturserver sind unter anderem DNS-, WINS- und RADIUS-Server (NPS). Falls sich die Änderungen an solchen Infrastrukturserver auf die Konfiguration des VPN-Routers auswirken, müssen Sie unter Umständen die Konfiguration des VPN-Routers an die neue Infrastruktur anpassen.

DNS und WINS

Falls der anrufende Router dies anfordert, sendet der antwortende Router während der PPP-Aushandlung die IPv4-Adressen seiner konfigurierten DNS- und WINS-Server an den anrufenden Router.

Falls sich die IPv4-Adressen der konfigurierten DNS- oder WINS-Server ändern (zum Beispiel weil DNS- oder WINS-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie die DNS- oder WINS-Serverkonfiguration auf dem antwortenden Router ändern, damit die anrufenden Router keine falschen IPv4-Adressen für die DNS- oder WINS-Server konfigurieren.

RADIUS

Falls ein antwortender Router so konfiguriert ist, dass er RADIUS-Authentifizierung nutzt, und sich die IPv4- oder IPv6-Adressen der RADIUS-Server ändern (zum Beispiel weil RADIUS-Server im Intranet hinzugefügt oder entfernt werden), müssen Sie folgendermaßen vorgehen:

1. Stellen Sie sicher, dass die antwortenden Router auf den neuen RADIUS-Servern als RADIUS-Clients eingetragen sind.
2. Aktualisieren Sie die Konfiguration der antwortenden Router, sodass sie die Namen, IPv4-Adressen oder IPv6-Adressen der neuen RADIUS-Server enthalten.

Hinzufügen von Standort- oder Remotestandortrouten

Falls sich der Adressraum eines Standorts ändert, an den ein VPN-Router angeschlossen ist, und Routen, die in der Routingtabelle des VPN-Routers die Standortschnittstelle benutzen, hinzugefügt oder entfernt werden müssen, können Sie im Snap-In *Routing und RAS* den Knoten *IPv4\Statische Routen* oder *IPv6\Statische Routen* öffnen und die Routen nach Bedarf hinzufügen oder löschen.

Und falls sich der Adressraum eines Remotestandorts ändert, zu dem ein VPN-Router Verbindungen herstellt, und Routen, die in der Routingtabelle des VPN-Routers die Schnittstelle für Wählen bei Bedarf benutzen, hinzugefügt oder entfernt werden müssen, können Sie im Snap-In *Routing und RAS* den Knoten *IPv4\Statische Routen* oder *IPv6\Statische Routen* öffnen und die Routen nach Bedarf hinzufügen oder löschen.

Problembehandlung

Weil so viele unterschiedliche Komponenten und Prozesse beteiligt sind, kann die Problembehandlung von Standort-zu-Standort-VPN-Verbindungen recht schwierig sein. Dieser Abschnitt beschreibt, welche Tools in Windows Server 2008 zur Verfügung stehen, um eine Problembehandlung für Standort-zu-Standort-VPN-Verbindungen durchzuführen, und welche Probleme am häufigsten bei Standort-zu-Standort-VPN-Verbindungen auftreten.

Tools für die Problembehandlung

Microsoft stellt für die Problembehandlung von VPN-Verbindungen auf dem VPN-Router folgende Tools zur Verfügung:

- TCP/IP-Problembehandlungstools
- Authentifizierungs- und Kontoführungsprotokollierung
- Ereignisprotokollierung
- NPS-Ereignisprotokollierung
- PPP-Protokollierung
- Ablaufverfolgung
- Network Monitor 3.1

Informationen über diese Tools finden Sie in Kapitel 12.

Bei Standort-zu-Standort-VPN-Verbindungen können Sie auch den Befehl *Grund für Nichterreichbarkeit* nutzen. Wenn eine Schnittstelle für Wählen bei Bedarf keine Verbindung herstellen kann, bleibt die Schnittstelle in einem nichterreichbaren Zustand. Routing und RAS zeichnet in diesem Fall auf, warum der Verbindungsversuch fehlgeschlagen ist.

So sehen Sie sich den Grund für die Nichterreichbarkeit an

1. Klicken Sie in der Konsolenstruktur des Snap-Ins *Routing und RAS* auf *Netzwerkschnittstellen*.
2. Klicken Sie in der Detailansicht mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf und wählen Sie den Befehl *Grund für Nichterreichbarkeit*. Routing und RAS zeigt eine Meldung an, die Informationen über den Verbindungsfehler enthält.

Durchführen einer Problembehandlung für Standort-zu-Standort-VPN-Verbindungen

Probleme mit Standort-zu-Standort-VPN-Verbindungen lassen sich normalerweise in folgende Kategorien unterteilen:

- Verbindung kann nicht hergestellt werden.
- Adressen hinter den VPN-Routern können nicht erreicht werden
- Die VPN-Schnittstellen von VPN-Routern können nicht erreicht werden
- Bei Bedarf herzustellende Verbindungen werden nicht automatisch aufgebaut

Mit den folgenden Problembehandlungstipps können Sie die Konfigurations- oder Infrastrukturprobleme isolieren, die für das Problem verantwortlich sind.

Verbindung kann nicht hergestellt werden

Wenn ein anrufender Router keine Verbindung zu einem antwortenden Router herstellen kann, sollten Sie folgende Punkte überprüfen:

- Falls die Schnittstelle für Wählen bei Bedarf auf dem anrufenden Router den Namen des antwortenden Routers trägt, können Sie mit dem Tool Ping überprüfen, ob der Hostname des antwortenden Routers in seine richtige IPv4- oder IPv6-Adresse aufgelöst wird, wenn Sie mit dem Internet verbunden sind. Der Ping-Test selbst schlägt unter Umständen fehl, weil Paketfilter verhindern, dass ICMP-Nachrichten (Internet Control Message Protocol) oder ICMPv6-Nachrichten zu und vom antwortenden Router übertragen werden.

- Falls Sie eine Kennwortauthentifizierung einsetzen, sollten Sie prüfen, ob die Anmeldeinformationen des anrufenden Routers (Benutzername, Kennwort und Domänenname) richtig sind und vom antwortenden Router validiert werden.
- Überprüfen Sie, ob das Benutzerkonto des anrufenden Routers gesperrt, abgelaufen oder deaktiviert ist und ob die Verbindung außerhalb der konfigurierten Anmeldezeiten hergestellt wird.
- Überprüfen Sie, ob das Benutzerkonto des anrufenden Routers so konfiguriert ist, dass es sein Kennwort bei der nächsten Anmeldung ändern muss, oder ob das Kennwort abgelaufen ist. Ein anrufender Router kann ein abgelaufenes Kennwort nicht während des Verbindungsprozesses ändern, daher wird ein solcher Verbindungsversuch zurückgewiesen.
- Überprüfen Sie, ob das Benutzerkonto aufgrund einer RAS-Kontosperrung gesperrt ist.
- Stellen Sie sicher, dass auf dem antwortenden Router der Routing- und RAS-Dienst läuft.
- Stellen Sie im Snap-In *Routing und RAS* im Eigenschaftendialogfeld des antwortenden Routers auf der Registerkarte *Allgemein* sicher, dass beim antwortenden Router LAN-Routing und bei Bedarf wählendes Routing aktiviert sind.
- Stellen Sie auf anrufenden und antwortenden Routern im Snap-In *Routing und RAS* im Eigenschaftendialogfeld des Knotens *Ports* sicher, dass für die Geräte *WAN-Miniport (PPTP)* und *WAN-Miniport (L2TP)* das Kontrollkästchen *Bei Bedarf herzustellende Routingverbindungen (e eingehend und ausgehend)* aktiviert ist.
- Stellen Sie sicher, dass der anrufende Router, der antwortende Router und die Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen so konfiguriert sind, dass sie mindestens eine gemeinsame Authentifizierungsmethode verwenden.
- Stellen Sie sicher, dass der anrufende Router und die Netzwerkrichtlinie für VPN-Verbindungen so konfiguriert sind, dass sie mindestens eine gemeinsame Verschlüsselungsstärke verwenden.
- Stellen Sie sicher, dass die Parameter der Verbindung in den Netzwerkrichtlinien autorisiert werden.

Damit die Verbindung zugelassen wird, müssen die Parameter des Verbindungsversuchs folgende Voraussetzungen erfüllen:

- Sie muss alle Bedingungen mindestens einer Netzwerkrichtlinie erfüllen.
- Sie muss im Benutzerkonto die RAS-Berechtigung zugewiesen haben (Einstellung *Zugriff gestatten*). Oder falls beim Benutzerkonto die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* ausgewählt ist, muss bei der passenden Netzwerkrichtlinie der Richtlinientyp *Zugriff gestatten* ausgewählt sein.
- Sie muss mit allen Einstellungen der Netzwerkrichtlinie übereinstimmen.
- Sie muss mit allen Einstellungen in den Einwähleigenschaften des Benutzerkontos übereinstimmen.

Sie können den Namen der Netzwerkrichtlinie ermitteln, die den Verbindungsversuch zurückgewiesen hat, indem Sie im Ereignisprotokoll *Windows-Protokolle\Sicherheit* nach NPS-Ereignissen zu zurückgewiesenen (Ereignis-ID 6273) beziehungsweise angenommenen (Ereignis-ID 6272) Verbindungsversuchen suchen. Die Netzwerkrichtlinie, die den Verbindungsversuch angenommen oder zurückgewiesen hat, ist in der Beschreibung des Ereignisses im Feld »Netzwerkrichtlinienname« aufgeführt.

- Falls Sie mit dem Konto eines Domänenadministrators angemeldet waren, als Sie den Setup-Assistenten für den Routing- und RAS-Server ausgeführt haben, fügt der Assistent das Computerkonto des VPN-Routers automatisch zur Sicherheitsgruppe *RAS- und IAS-Server* hinzu. Diese Gruppen-

mitgliedschaft erlaubt es dem antwortenden Routercomputer, auf Benutzerkontoinformationen zuzugreifen. Das ist nötig, falls er so konfiguriert ist, dass er die Authentifizierung lokal durchführt statt über einen RADIUS-Server. Falls der antwortende Router nicht auf Benutzerkontoinformationen zugreifen kann, sollten Sie folgende Punkte überprüfen:

- Das Computerkonto des antwortenden Routercomputers muss in allen Domänen, die Benutzerkonten enthalten, die der antwortende Router authentifiziert, Mitglied der Sicherheitsgruppe *RAS- und IAS-Server* sein. Sie können an einer Eingabeaufforderung den Befehl `netsh nps show registeredserver` ausführen, um sich die aktuellen Mitgliedschaften anzusehen. Mit dem Befehl `netsh nps add registeredserver` können Sie den Server in einer Domäne, in der dieser antwortende Router Mitglied ist, oder in anderen Domänen registrieren. Stattdessen können Sie das Computerkonto des antwortenden Routercomputers auch in allen Domänen, die Benutzerkonten enthalten, für die der antwortende Router Standort-zu-Standort-VPN-Verbindungen authentifiziert, zur Sicherheitsgruppe *RAS- und IAS-Server* hinzufügen..
- Wenn Sie den antwortenden Routercomputer zur Sicherheitsgruppe *RAS- und IAS-Server* hinzufügen oder daraus entfernen, wird die Änderung nicht sofort wirksam (wegen der Art, wie Windows Server 2008 Active Directory-Informationen zwischenspeichert). Damit die Änderung wirksam wird, müssen Sie den antwortenden Routercomputer neu starten.
- Stellen Sie auf dem anrufenden und dem antwortenden Router im Snap-In *Routing und RAS* im Eigenschaftendialogfeld des Servers auf der Registerkarte *Allgemein* sicher, dass für IPv4 oder IPv6 die Option *LAN und bei Bedarf wählendes Routing* ausgewählt ist.
- Überprüfen Sie, ob noch PPTP- oder L2TP-Ports auf dem anrufenden und dem antwortenden Router frei sind. Falls nötig, können Sie mehr gleichzeitige Verbindungen erlauben. Öffnen Sie dazu im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des Knotens *Ports* und erhöhen Sie die Zahl der PPTP- oder L2TP-Ports.
- Stellen Sie sicher, dass der antwortende Router das Tunnelprotokoll des anrufenden Routers unterstützt.

In der Standardeinstellung versucht eine Schnittstelle für Wählen bei Bedarf, die in Windows Server 2008 mit automatischem VPN-Typ konfiguriert wurde, zuerst eine PPTP-VPN-Verbindung aufzubauen und dann eine L2TP/IPsec-VPN-Verbindung. Falls als Servertyp PPTP (Point-to-Point Tunneling Protocol) oder L2TP (Layer-2 Tunneling Protocol) ausgewählt ist, müssen Sie sicherstellen, dass der antwortende Router das ausgewählte Tunnelprotokoll unterstützt.

- Überprüfen Sie, wie der antwortende Router die Authentifizierung durchführt. Der antwortende Router kann so konfiguriert sein, dass er die Anmeldeinformationen des anrufenden Routers entweder lokal oder über RADIUS authentifiziert.
 - Bei lokaler Authentifizierung müssen Sie sicherstellen, dass der antwortende Router Mitglied der Active Directory-Domäne ist und das Computerkonto des antwortenden Routers zur Sicherheitsgruppe *RAS- und IAS-Server* hinzugefügt wurde.
 - Bei RADIUS-Authentifizierung müssen Sie sicherstellen, dass der antwortende Routercomputer mit dem RADIUS-Server kommunizieren kann.
- Überprüfen Sie, ob Paketfilter auf einer Router- oder Firewallschnittstelle, die zwischen dem anrufenden und dem antwortenden Router liegt, die Weiterleitung von VPN-Verkehr verhindert. Details zu Paketfiltern für VPN-Verkehr auf VPN-Router und Firewall finden Sie im Abschnitt »Firewallpaketfilterung für VPN-Verkehr« in Kapitel 12.

L2TP/IPsec-Authentifizierungsprobleme

Die folgenden Probleme sind am häufigsten die Ursache, wenn Standort-zu-Standort-L2TP/IPsec-Verbindungen fehlschlagen:

- **Kein Zertifikat** In der Standardeinstellung von Standort-zu-Standort-L2TP/IPsec-Verbindungen tauschen anrufender und antwortender Router ihre Computerzertifikate aus, um eine IPsec-Peer-authentifizierung durchzuführen. Prüfen Sie auf dem anrufenden und dem antwortenden Router im Snap-In *Zertifikate* die Zertifikatspeicher des lokalen Computers, um sicherzustellen, dass passende Zertifikate vorhanden sind.
- **Falsches Zertifikat** Falls Zertifikate vorhanden sind, müssen sie überprüfbar sein. Anders als beim manuellen Konfigurieren von IPsec-Regeln ist die Liste der Zertifizierungsstellen bei L2TP/IPsec-Verbindungen nicht konfigurierbar. Stattdessen sendet jeder Router, der an der L2TP-Verbindung beteiligt ist, an seinen IPsec-Peer eine Liste der Stammzertifizierungsstellen, deren Zertifikat er für die Authentifizierung akzeptiert. Die Stammzertifizierungsstellen in dieser Liste sind die Stammzertifizierungsstellen, die Computerzertifikate für den Computer ausgestellt haben. Falls zum Beispiel Router A Computerzertifikate von den Stammzertifizierungsstellen CertAuth1 und CertAuth2 ausgestellt bekommen hat, meldet er seinem IPsec-Peer während der Hauptmodus-aushandlung, dass er für die Authentifizierung ausschließlich Zertifikate von CertAuth1 und CertAuth2 akzeptiert. Falls der IPsec-Peer, Router B, kein gültiges Computerzertifikat hat, das von CertAuth1 oder CertAuth2 ausgestellt wurde, schlägt die IPsec-Sicherheitsaushandlung fehl.

Der anrufende Router muss ein gültiges Computerzertifikat installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der antwortende Router vertraut. Außerdem muss der antwortende Router ein gültiges Computerzertifikat installiert haben, das von einer Zertifizierungsstelle ausgestellt wurde, die in einer gültigen Zertifikatkette liegt, die von der ausstellenden Zertifizierungsstelle bis zu einer Stammzertifizierungsstelle reicht, der der anrufende Router vertraut.

EAP-TLS-Authentifizierungsprobleme

Wenn EAP-TLS für die Authentifizierung benutzt wird, übergibt der anrufende Router ein Benutzerzertifikat. Dies ist ein Zertifikat vom Typ *Router (Offlineanforderung)*, das von Windows-Zertifikatdiensten ausgestellt wurde. Der Authentifizierungsserver (der antwortende Router oder RADIUS-Server) übergibt im Gegenzug ein Computerzertifikat.

Stellen Sie sicher, dass der anrufende und der antwortende Router richtig konfiguriert sind, indem Sie folgende Punkte überprüfen:

- Öffnen Sie auf dem anrufenden Router das Eigenschaftendialogfeld der Schnittstelle für Wählen bei Bedarf und klicken Sie auf die Registerkarte *Sicherheit*. Öffnen Sie das Dialogfeld *Erweiterte Sicherheitseinstellungen* für die Schnittstelle für Wählen bei Bedarf und stellen Sie sicher, dass EAP als Authentifizierungsprotokoll konfiguriert ist. Überprüfen Sie die Einstellungen in den Eigenschaften für den EAP-Typ *Smartcard- oder anderes Zertifikat*. Stellen Sie sicher, dass das richtige Zertifikat ausgewählt ist, wenn Sie die Anmeldeinformationen für die Schnittstelle für Wählen bei Bedarf konfigurieren.
- Stellen Sie auf dem antwortenden Router sicher, dass EAP als Authentifizierungsmethode aktiviert ist und EAP-TLS in der passenden Netzwerkrichtlinie aktiviert wurde. Stellen Sie sicher, dass in der Netzwerkrichtlinie für Standort-zu-Standort-VPN-Verbindungen unter der Einstellung *Authentifizierungsmethode* des EAP-Typs *Smartcard- oder anderes Zertifikat* das richtige Computerzertifikat des Authentifizierungsservers (der antwortende Router oder NPS-Server) ausgewählt ist.

Damit der Authentifizierungsserver (der antwortende Router oder NPS-Server) das Zertifikat des anrufenden Routers überprüfen kann, müssen für jedes Zertifikat in der Zertifikatkette, die vom anrufenden Router übergeben wurde, folgende Bedingungen erfüllt sein:

- Das aktuelle Datum muss innerhalb der Gültigkeitsdauer des Zertifikats liegen.

Wenn Zertifikate ausgestellt werden, bekommen sie einen Gültigkeitszeitraum zugewiesen. Vor diesem Zeitraum können sie nicht benutzt werden, und danach gelten sie als abgelaufen.

- Das Zertifikat darf nicht gesperrt sein.

Ausgestellte Zertifikate können jederzeit gesperrt werden. Ob ein Zertifikat gesperrt ist, lässt sich über OCSP (Online Certificate Status Protocol) prüfen. OCSP nutzt HTTP, um eine digital signierte Antwort zum Status eines Zertifikats abzurufen. Jede ausstellende Zertifizierungsstelle veröffentlicht auch eine aktuelle Zertifikatsperrliste (Certificate Revocation List, CRL). Eine solche Zertifikatsperrliste enthält praktisch eine Liste aller Zertifikate, die als nicht mehr gültig betrachtet werden sollen. In der Standardeinstellung prüft der Authentifizierungsserver bei allen Zertifikaten in der Zertifikatkette des anrufenden Routers (die Reihe der Zertifikate vom Zertifikat des anrufenden Routers bis zur Stammzertifizierungsstelle), ob sie gesperrt wurden. Falls irgendein Zertifikat in der Kette gesperrt wurde, schlägt die Zertifikatüberprüfung fehl.

Falls die Zertifikatsperrliste lokal verfügbar ist, kann sie direkt überprüft werden. In bestimmten Fällen kann die Zertifikatsperrliste erst überprüft werden, nachdem die Verbindung hergestellt wurde. Falls die Zertifikatsperrliste zum Beispiel in der Stammzertifizierungsstelle gespeichert ist, kann ein Authentifizierungsserver in einem Standort, der keine Verbindung zum Standort der Stammzertifizierungsstelle hat, nicht auf die Zertifikatsperrliste zugreifen. Dieses Problem lässt sich auf zwei Arten lösen:

- Veröffentlichen Sie die Zertifikatsperrliste in Active Directory. Sobald die Zertifikatsperrliste in Active Directory veröffentlicht wurde, verfügt der lokale Domänencontroller im Standort über die aktuellste Zertifikatsperrliste, nachdem die Active Directory-Synchronisierung durchgeführt wurde.
- Setzen Sie auf dem VPN-Router den Registrierungswert `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\PPP\EAP\13\IgnoreRevocationOffline` auf 1.

Sie können sich die Sperrlisten-Verteilungspunkte eines Zertifikats ansehen, indem Sie im Snap-In *Zertifikate* die Zertifikateigenschaften öffnen, auf die Registerkarte *Details* klicken und dort das Feld *Sperrlisten-Verteilungspunkte* markieren.

Die Zertifikatsperrungsüberprüfung mithilfe von CRLs kann nur funktionieren, wenn das Veröffentlichungs- und Verteilungssystem für die Zertifikatsperrliste einwandfrei arbeitet. Falls die Zertifikatsperrliste, die in einem Zertifikat genannt ist, nicht oft aktualisiert wird, kann ein Zertifikat, das gesperrt wurde, auch weiterhin benutzt werden und gilt als gültig, weil die veröffentlichte Zertifikatsperrliste, die der Authentifizierungsserver prüft, nicht auf dem aktuellen Stand ist.

- Das Zertifikat muss eine gültige digitale Signatur haben.

Zertifizierungsstellen versehen die ausgestellten Zertifikate mit einer digitalen Signatur. Der Authentifizierungsserver prüft die digitale Signatur jedes Zertifikats in der Kette (mit Ausnahme des Stammzertifizierungsstellenzertifikats), indem er den öffentlichen Schlüssel der Zertifizierungsstelle abrufen, die das Zertifikat ausgestellt hat, und die digitale Signatur mathematisch validiert.

Das Zertifikat des anrufenden Routers muss auch den Zweck *Clientauthentifizierung* eingetragen haben. Diese bedeutet, dass als erweiterte Schlüsselverwendung (Enhanced Key Usage, EKU) die OID 1.3.6.1.5.5.7.3.2 eingetragen ist. Außerdem muss im Feld *Alternativer Antragstellername* des Zertifikats der UPN eines gültigen Benutzerkontos eingetragen sein.

Sie können sich die EKU für ein Zertifikat im Snap-In *Zertifikate* ansehen, indem Sie im Detailabschnitt doppelt auf das Zertifikat klicken, die Registerkarte *Details* wählen und auf das Feld *Erweiterte Schlüsselerwendung* klicken. Das Feld *Alternativer Antragstellername* können Sie sich genauso ansehen.

Damit der Authentifizierungsserver der Zertifikatkette, die der anrufende Router übergibt, vertrauen kann, muss auf dem Authentifizierungsserver im Speicher *Vertrauenswürdige Stammzertifizierungsstellen* das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert sein, die das Zertifikat des anrufenden Routers ausgestellt hat.

Der Authentifizierungsserver prüft auch, ob die in der EAP-Response/Identity-Nachricht angegebene Identität mit dem Namen in der Eigenschaft *Alternativer Antragstellername* des Zertifikats übereinstimmt. Das verhindert, dass ein böswilliger Benutzer sich als ein anderer Benutzer ausgibt, der in der EAP-Response/Identity-Nachricht aufgeführt ist.

Weitere Anforderungen an das Benutzerzertifikat des anrufenden Routers sind im Abschnitt »Anforderungen an die PKI« weiter oben in diesem Kapitel beschrieben.

Falls der Authentifizierungsserver ein antwortende Router oder NPS-Server ist, der unter Windows Server 2008 läuft, können die folgenden Registrierungswerte im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rasman\PPP\EAP\13` das Verhalten von EAP-TLS beim Durchführen der Zertifikatsperrprüfung ändern:

- **IgnoreNoRevocationCheck** Wenn dieser Eintrag den Wert 1 hat, erlaubt der Authentifizierungsserver EAP-TLS-Clients, selbst dann eine Verbindung herzustellen, wenn er gar keine oder keine vollständige Zertifikatsperrprüfung für die Zertifikatkette des anrufenden Routers (außer dem Stammzertifikat) durchführen kann. Normalerweise schlagen Zertifikatsperrprüfung fehl, weil das Zertifikat keine Zertifikatsperrlisteninformationen enthält.

IgnoreNoRevocationCheck hat in der Standardeinstellung den Wert 0 (deaktiviert). Ein EAP-TLS-Client kann nur dann eine Verbindung zum Server herstellen, wenn der Server die Zertifikatsperrprüfung für die Zertifikatkette des Clients (inklusive Stammzertifikat) abgeschlossen und sichergestellt hat, dass keines der Zertifikate gesperrt wurde.

Mit diesem Registrierungswert können Sie dafür sorgen, dass Clients authentifiziert werden, obwohl das Zertifikat keine Sperrlisten-Verteilungspunkte enthält. Das kann zum Beispiel bei Zertifikaten von anderen Organisationen der Fall sein.

- **IgnoreRevocationOffline** Wenn dieser Eintrag den Wert 1 hat, erlaubt der Authentifizierungsserver den EAP-TLS-Clients, auch dann eine Verbindung herzustellen, wenn ein Server, der eine Zertifikatsperrliste speichert, nicht im Netzwerk verfügbar ist. *IgnoreRevocationOffline* hat in der Standardeinstellung den Wert 0. Bei dieser Standardeinstellung erlaubt der Authentifizierungsserver Clients nur dann, eine Verbindung herzustellen, wenn er eine Zertifikatsperrprüfung für ihre Zertifikatkette durchführen und sicherstellen kann, dass keines ihrer Zertifikate gesperrt wurde. Wenn er keine Verbindung zu einem Server bekommt, der eine Sperrliste speichert, stuft EAP-TLS das Zertifikat so ein, als wäre es gesperrt.

Wenn Sie *IgnoreRevocationOffline* auf 1 setzen, verhindern Sie, dass die Zertifikatüberprüfung aufgrund von Netzwerkausfällen fehlschlägt, die bewirken können, dass Zertifikatsperrprüfungen nicht erfolgreich abgeschlossen werden.

- **NoRevocationCheck** Wenn dieser Eintrag den Wert 1 hat, verhindert der Authentifizierungsserver, dass EAP-TLS eine Zertifikatsperrprüfung für das Zertifikat des anrufenden Routers durchführt. Die Zertifikatsperrprüfung stellt sicher, dass das Zertifikat des anrufenden Routers und die Zerti-

fikate in seiner Zertifikatkette nicht gesperrt wurden. *NoRevocationCheck* hat in der Standardeinstellung den Wert 0.

- **NoRootRevocationCheck** Wenn dieser Eintrag den Wert 1 hat, verhindert der Authentifizierungsserver, dass EAP-TLS eine Zertifikatsperrprüfung für das Stammzertifizierungsstellenzertifikat des anrufenden Routers durchführt. *NoRootRevocationCheck* hat in der Standardeinstellung den Wert 0. Dieser Eintrag verhindert nur die Zertifikatsperrprüfung für das Stammzertifizierungsstellenzertifikat des Clients. Für die übrige Zertifikatkette des anrufenden Routers wird trotzdem eine Zertifikatsperrprüfung durchgeführt.

Mithilfe von *NoRootRevocationCheck* können Sie dafür sorgen, dass Clients trotzdem authentifiziert werden, wenn das Zertifikat keine Sperrlisten-Verteilungspunkte enthält. Das kann zum Beispiel bei Zertifikaten der Fall sein, die für andere Organisationen ausgestellt wurden. Außerdem kann *NoRootRevocationCheck* verhindern, dass aufgrund der Zertifikatprüfung Verzögerungen auftreten, weil eine Zertifikatsperrliste offline oder abgelaufen ist.

Alle diese Registrierungswerte müssen als DWORD-Typ hinzugefügt werden, gültige Werte sind 0 oder 1. Der anrufende Router braucht diese Werte nicht.

Damit der anrufende Router das Zertifikat des Authentifizierungsservers im Rahmen der EAP-TLS-Authentifizierung überprüft, müssen für jedes Zertifikat in der Zertifikatkette, das vom Authentifizierungsserver gesendet wurde, folgende Bedingungen erfüllt sein:

- Das aktuelle Datum muss innerhalb der Gültigkeitsdauer des Zertifikats liegen.
- Das Zertifikat muss eine gültige digitale Signatur haben.

Außerdem muss im Computerzertifikat des Authentifizierungsservers die EKU *Serverauthentifizierung* (OID 1.3.6.1.5.5.7.3.1) eingetragen sein. Sie können sich die EKU für ein Zertifikat im Snap-In *Zertifikate* ansehen, indem Sie im Detailabschnitt doppelt auf das Zertifikat klicken, die Registerkarte *Details* wählen und auf das Feld *Erweiterte Schlüsselverwendung* klicken.

Damit der anrufende Router der Zertifikatkette, die der Authentifizierungsserver übergibt, vertrauen kann, muss auf dem anrufenden Router im Speicher *Vertrauenswürdige Stammzertifizierungsstellen* des lokalen Computers das Stammzertifizierungsstellenzertifikat der Zertifizierungsstelle installiert sein, die das Zertifikat des Authentifizierungsservers ausgestellt hat.

Weitere Anforderungen an das Computerzertifikat des Authentifizierungsservers sind im Abschnitt »Anforderungen an die PKI« weiter oben in diesem Kapitel beschrieben

Beachten Sie, dass der anrufende Router keine Zertifikatsperrprüfung für die Zertifikate in der Zertifikatkette des Computerzertifikats des Authentifizierungsservers durchführt. Es wird angenommen, dass der anrufende Router noch keine Verbindung zum Netzwerk hat und daher keinen Zugriff auf eine Webseite oder andere Ressourcen hat, die er für die Zertifikatsperrprüfung braucht.

Adressen hinter den VPN-Routern können nicht erreicht werden

Falls Verkehr nicht zwischen Adressen innerhalb der Standorte, die hinter den VPN-Routern liegen, ausgetauscht werden kann, sollten Sie folgende Punkte überprüfen:

- Öffnen Sie auf dem anrufenden und dem antwortenden Router jeweils im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des Servers und stellen Sie sicher, dass auf der Registerkarte *Allgemein* für IPv4 oder IPv6 die Option *LAN und bei Bedarf wählendes Routing* ausgewählt ist.
- Stellen Sie sicher, dass im Snap-In *Routing und RAS* die Schnittstelle für Wählen bei Bedarf, über die Verkehr gesendet wird, zu den Knoten *IPv4\Allgemein* oder *IPv6\Allgemein* hinzugefügt wurde.

Das wird automatisch erledigt, wenn Sie die Schnittstelle mit dem Assistenten für eine Schnittstelle für Wählen bei Bedarf anlegen.

- Stellen Sie sicher, dass es in den Standorten von anrufendem und antwortendem Router jeweils Routen gibt, die dafür sorgen, dass alle Adressen in beiden Netzwerken erreichbar sind. Im Unterschied zu einer Remotezugriffsverbindung legt eine bei Bedarf herzustellende Wählverbindung nicht automatisch eine Standardroute an. Sie müssen Routen auf beiden Seiten der bei Bedarf herzustellenden Wählverbindung anlegen, sodass Verkehr zu und von der Gegenseite der bei Bedarf herzustellenden Wählverbindung weitergeleitet werden kann.

Sie können statische IPv4- oder IPv6-Routen von Hand hinzufügen, während Sie die Schnittstelle für Wählen bei Bedarf anlegen. Oder Sie verwenden das Snap-In *Routing und RAS*. Wenn Sie eine persistente Wählverbindung haben, können Sie für diese Verbindung RIP für IPv4 aktivieren. Bei Wählverbindungen, die nur bei Bedarf aufgebaut werden, können Sie Routen mithilfe von auto-statischen Aktualisierungen über RIP für IPv4 automatisch aktualisieren.

- Stellen Sie bei bidirektional aufgebauten Standort-zu-Standort-VPN-Verbindungen sicher, dass der antwortende Router die Standort-zu-Standort-VPN-Verbindung nicht als Remotezugriffsverbindung interpretiert.

Bei bidirektional aufgebauten Verbindungen kann jeder Router die Rolle des anrufenden Routers oder des antwortenden Routers einnehmen. Die Benutzernamen und die Namen der Schnittstellen für Wählen bei Bedarf müssen zueinander passen. Zum Beispiel funktionieren bidirektional aufgebaute Verbindungen in folgenden Szenarien:

- Router 1 hat eine Schnittstelle für Wählen bei Bedarf, die den Namen *NEW-YORK* trägt. Sie ist so konfiguriert, dass sie *SEATTLE* als Benutzernamen verwendet, wenn sie Anmeldeinformationen für die Authentifizierung sendet.
- Router 2 hat eine Schnittstelle für Wählen bei Bedarf, die den Namen *SEATTLE* trägt. Sie ist so konfiguriert, dass sie *NEW-YORK* als Benutzernamen verwendet, wenn sie Anmeldeinformationen für die Authentifizierung sendet.

Dieses Beispiel setzt voraus, dass Router 2 den Benutzernamen *SEATTLE* und Router 1 den Benutzernamen *NEW-YORK* validieren kann.

Falls es sich bei der Verbindung um eine bei Bedarf herzustellende Wählverbindung handelt, zeigt der Port, auf dem die Verbindung empfangen wurde, den Status *Aktiv* an, und die entsprechende Schnittstelle für Wählen bei Bedarf meldet *Verbindung hergestellt*. Falls der Name des Benutzerkontos, der in den Anmeldeinformationen des anrufenden Routers übergeben wurde, im Snap-In *Routing und RAS* unter *RAS-Clients* aufgeführt wird, hat der antwortende Router den anrufenden Router als Remotezugriffsklient interpretiert.

- Überprüfen Sie, ob IPv4- oder IPv6-Paketfilter in der Schnittstelle für Wählen bei Bedarf des anrufenden und des antwortenden Routers verhindern, dass Verkehr gesendet oder empfangen werden kann.

Sie können jede Schnittstelle für Wählen bei Bedarf so konfigurieren, dass ein- und ausgehende IPv4- oder IPv6-Filter genau steuern, welche Art von Verkehr in und aus der Schnittstelle für Wählen bei Bedarf erlaubt oder blockiert wird.

Die VPN-Schnittstellen von VPN-Routern können nicht erreicht werden

Die VPN-Schnittstellen der VPN-Router sind die Schnittstellen auf den beiden Seiten der Standort-zu-Standort-VPN-Verbindung, die die Endpunkte des VPN-Tunnels bilden. Falls kein Verkehr zwischen den VPN-Schnittstellen gesendet oder empfangen werden kann, sollten Sie folgende Punkte überprüfen:

- Überprüfen Sie die IPv4-Adresspools des anrufenden und des antwortenden Routers.

Falls der VPN-Router so konfiguriert ist, dass er einen IPv4-Adresspool verwendet, sollten Sie sicherstellen, dass der Adressbereich des IPv4-Adresspools von Hosts und Routern im Standort erreichbar ist. Falls nicht, müssen Sie die IPv4-Routen für die statischen IP-Adresspools des VPN-Routers zu den Routern im Standort hinzufügen. Dafür müssen Sie die Adressbereiche anhand ihrer IPv4-Adresse und der Subnetzmaske angeben. Stattdessen können Sie auch RIP für IPv4 auf dem VPN-Router aktivieren.

Falls der VPN-Router so konfiguriert ist, dass er IPv4-Adressen mithilfe von DHCP (Dynamic Host Configuration Protocol) abrufen, und kein DHCP-Server verfügbar ist, weist der VPN-Router Adressen aus dem APIPA-Adressbereich (Automatic Private IP Addressing) zu, der von 169.254.0.1 bis 169.254.255.254 reicht. Die Nutzung von APIPA-Adressen für VPN-Router funktioniert nur, wenn das Netzwerk, an das der VPN-Router angeschlossen ist, ebenfalls mit APIPA-Adressen arbeitet.

Falls der VPN-Router APIPA-Adressen verwendet, obwohl ein DHCP-Server verfügbar ist, sollten Sie prüfen, ob die mit DHCP zugewiesenen IPv4-Adressen über die richtige Netzwerkschnittstelle angefordert werden. In der Standardeinstellung ruft der VPN-Router die IPv4-Adressen mit DHCP über den Adapter ab, den Sie im Setup-Assistenten für den Routing- und RAS-Server ausgewählt haben. Sie können von Hand einen LAN-Adapter aus der Liste der Adapter auswählen, indem Sie im Snap-In *Routing und RAS* das Eigenschaftendialogfeld des VPN-Routers öffnen und den Adapter in der Dropdownliste auf der Registerkarte *IPv4* wählen.

Falls die IPv4-Adresspools ein Teilbereich der IP-Adressen im Standortsubnetz sind, an das der VPN-Router angeschlossen ist, sollten Sie überprüfen, ob der Bereich der IPv4-Adressen in den IPv4-Adresspools über statische Konfiguration oder DHCP anderen TCP/IP-Knoten zugewiesen wurde.

- Überprüfen Sie das IPv6-Subnetzpräfix, das vom anrufenden und antwortenden Router angekündigt wird.

Das IPv6-Subnetzpräfix muss für anrufenden und antwortenden Router gleich sein. Außerdem muss es über eine Route in den Routinginfrastrukturen beider Standorte erreichbar sein.

Bei Bedarf herzustellende Verbindungen werden nicht automatisch aufgebaut

Falls eine Verbindung bei Bedarf nicht automatisch aufgebaut wird, sollten Sie folgende Punkte überprüfen:

- Stellen Sie im Eigenschaftendialogfeld des anrufenden Routers auf der Registerkarte *Allgemein* sicher, dass für IPv4 oder IPv6 die Option *LAN und bei Bedarf wählendes Routing* ausgewählt ist.
- Stellen Sie sicher, dass richtige statische Routen vorhanden sind und dass sie mit der richtigen Schnittstelle für Wählen bei Bedarf konfiguriert sind. Bei statischen Routen, die eine Schnittstelle für Wählen bei Bedarf nutzen, sollten Sie im Eigenschaftendialogfeld der Route sicherstellen, dass das Kontrollkästchen *Bei Bedarf herzustellende Wahlverbindungen über diese Route initiieren* aktiviert ist.

- Überprüfen Sie, ob der Status für die Schnittstelle für Wählen bei Bedarf als *Nicht erreichbar* angezeigt wird.
- Überprüfen Sie, ob der Status für die Schnittstelle für Wählen bei Bedarf als *Deaktiviert* angezeigt wird.

Falls eine Schnittstelle für Wählen bei Bedarf deaktiviert ist, können Sie diese Schnittstelle aktivieren, indem Sie im Snap-In *Routing und RAS* den Knoten *Netzwerkschnittstellen* öffnen, mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf klicken und den Befehl *Aktivieren wählen*.

- Überprüfen Sie, ob die Hinauswählzeiten, die für die Schnittstelle für Wählen bei Bedarf konfiguriert wurden, den Verbindungsversuch verhindern.

Sie können die Hinauswählzeiten konfigurieren, indem Sie im Snap-In *Routing und RAS* den Knoten *Netzwerkschnittstellen* öffnen, mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf klicken und den Befehl *Hinauswählzeiten wählen*.

- Überprüfen Sie, ob Filter für Wählen bei Bedarf einen Verbindungsversuch über die Schnittstelle für Wählen bei Bedarf verhindern.

Sie können Filter für Wählen bei Bedarf konfigurieren, indem Sie im Snap-In *Routing und RAS* den Knoten *Netzwerkschnittstellen* öffnen, mit der rechten Maustaste auf die Schnittstelle für Wählen bei Bedarf klicken und den Befehl *IP-Filter für Wählen bei Bedarf einrichten* oder *IPv6-Filter für Wählen bei Bedarf einrichten* wählen.

Zusammenfassung des Kapitels

Um eine Standort-zu-Standort-VPN-Lösung bereitzustellen, müssen Sie die Active Directory-, PKI-, Gruppenrichtlinien- und RADIUS-Komponenten einer Windows-Authentifizierungsinfrastruktur konfigurieren und anrufende sowie antwortende VPN-Router im Internet planen und bereitstellen. Wenn eine Standort-zu-Standort-VPN-Lösung einmal bereitgestellt ist, umfasst die Wartung das Verwalten von anrufenden und antwortenden Routern und das Anpassen ihrer Konfiguration an Änderungen der Infrastrukturserver und von Routen. Ursachen für Probleme bei Standort-zu-Standort-VPN-Verbindungen können sein, dass aufgrund von Authentifizierungs- oder Autorisierungsfehlern keine Verbindung hergestellt werden kann und Standortressourcen hinter einem VPN-Router nicht erreichbar sind.

Weitere Informationen

Weitere Informationen über die VPN-Unterstützung in Windows finden Sie hier:

- Kapitel 12, »Remotenzugriff-VPN-Verbindungen«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Virtual Private Networks« (<http://www.microsoft.com/vpn>)

Weitere Informationen über VPN-Internetstandards finden Sie hier:

- RFC 2637, »Point-to-Point Tunneling Protocol (PPTP)«
- RFC 2661, »Layer Two Tunneling Protocol (L2TP)«
- RFC 3193, »Securing L2TP Using IPsec«

Weitere Informationen über Active Directory finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Server 2008 Active Directory – Die technische Referenz* von Stan Reimer, Mike Mulcare, Conan Kezema und Byron Wright, mit dem Microsoft Active Directory Team, einzeln erhältlich oder als Bestandteil der technischen Referenz zu Windows Server 2008 (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support

Weitere Informationen über die PKI finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Public Key Infrastructure for Windows Server« (<http://www.microsoft.com/pki>)
- *Microsoft Windows Server 2008 – PKI und Zertifikatsicherheit* von Brian Komar (Microsoft Press, 2008)

Weitere Informationen über Gruppenrichtlinien finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- *Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista* (Microsoft Press, 2008)
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Microsoft Windows Server Group Policy« (<http://www.microsoft.com/gp>)

Weitere Informationen über RADIUS und NPS finden Sie hier:

- Kapitel 9, »Authentifizierungsinfrastruktur«
- Windows Server 2008 Technical Library unter <http://technet.microsoft.com/windowsserver/2008>
- Windows Server 2008-Hilfe und Support
- »Network Policy Server« (<http://www.microsoft.com/nps>)

Der Autor

Joseph Davies

Joseph Davies ist Fachautor für die Microsoft Corporation. Er arbeitet seit 1992 als Autor und Trainer zu den Themen TCP/IP, Netzwerke und Sicherheit. Seit 2001 schreibt er Whitepapers, TechNet-Artikel, Websites und Microsoft Press-Bücher für die Microsoft Windows Networking Technology-Teams. Er ist Autor der monatlichen TechNet-Kolumne »The Cable Guy« (<http://www.microsoft.com/technet/community/columns/cableguy/default.aspx>).

Joseph Davies ist Koautor von *Virtuelle Private Netzwerke mit Microsoft Windows Server 2003* (2004), *Microsoft Windows Server 2003 – TCP/IP-Protokolle und -Dienste* (2003) und *Microsoft Windows 2000 TCP/IP-Protokolle und Dienste* (2000), alle von Microsoft Press. Er ist Autor von *Understanding IPv6, Second Edition* (Microsoft Press, 2008), *Windows Server 2008 TCP/IP-Protokolle und Dienste* (Microsoft Press, 2008), *TCP/IP Fundamentals for Microsoft Windows* (TechNet, 2006), *Drahtlose Netzwerke mit Microsoft Windows* (Microsoft Press, 2004) und *Understanding IPv6* (Microsoft Press, 2003), das die Preise Puget Sound Society for Technical Communication Best of Show und International STC Distinguished gewonnen hat.

