Bereitstellen von DFÜ- und VPN-RAS-Servern

(Engl. Originaltitel: Deploying Dial-Up and VPN Remote Access Servers)

Bereitstellen von DFÜ- und VPN-RAS-Servern

Um Remotebenutzern einen sicheren und zuverlässigen Zugriff auf Ihre Netzwerkressourcen zu ermöglichen, können Sie die RAS- und Sicherheitstechnologien für Microsoft® Windows® Server 2003 Standard Edition, Windows® Server 2003 Enterprise Edition, Windows® Server 2003 Datacenter Edition und Windows® Server 2003 Web Edition (in diesem Kapitel "Windows Server 2003-Familie" genannt) verwenden. Windows Server 2003 Web Edition, ist auf eine einzige VPN-Verbindung (virtuelles privates Netzwerk) für Point-to-Point-Tunneling-Protokoll (PPTP) und eine einzige VPN-Verbindung für Layer-Two-Tunneling-Protokoll (L2TP) beschränkt.

Mithilfe von Routing und RAS können Sie eine DFÜ-Lösung entwerfen und bereitstellen oder durch Bereitstellen einer VPN-Lösung das Internet nutzen.

Verwandte Informationen in den Resource Kits

- Weitere Informationen zum Entwerfen und Bereitstellen einer Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure oder PKI) finden Sie unter "Designing a Public Key Infrastructure" in *Designing and Deploying Directory and Security Services* dieses Kits (englischsprachig).
- Weitere Informationen zum Bereitstellen von Smartcards finden Sie unter "Deploying Smart Cards" in *Designing and Deploying Directory and Security Services* dieses Kits (englischsprachig).
- Weitere Informationen zum Entwerfen und Bereitstellen des Internetauthentifizierungsdienstes (Internet Authentication Service oder IAS) finden Sie unter "Deploying IAS" in diesem Buch (englischsprachig).
- Weitere Informationen zur Verwendung des Verbindungs-Managers zum Bereitstellen von RAS-Clients finden Sie unter "Deploying Remote Access Clients Using Connection Manager" in diesem Buch (englischsprachig).

Übersicht über das Bereitstellen von DFÜ- und VPN-RAS-Servern

Für einen einfachen Zugriff auf Ihr Unternehmensnetzwerk von Remotestandorten aus können Sie Benutzern ein DFÜ- oder ein VPN-Netzwerk bzw. eine Kombination aus beiden zur Verfügung stellen. DFÜ-Netzwerke ermöglichen Remotebenutzern eine direkte Einwählverbindung mit einem RAS-Server in Ihrem Unternehmensnetzwerk. Mithilfe eines virtuellen privaten Netzwerks können Remotebenutzer, die mit dem Internet verbunden sind, über eine VPN-Verbindung eine Verbindung mit einem VPN-Server im Unternehmensnetzwerk herstellen.

Bevor Sie sich für eine Lösung für Ihr Unternehmen entscheiden, sollten Sie die Kosteneffizienz der jeweiligen Lösung berücksichtigen und überlegen, in wieweit die Anforderungen des Unternehmens in Bezug auf Sicherheit und Zuverlässigkeit erfüllt werden.

Die Netzwerkinfrastruktur des Intranets ist ein wichtiges Element bei der Designentwicklung von Servern für den Remotezugriff. Ohne eine entsprechende Planung können RAS-Clients keine IP-Adressen erhalten und keine Intranetnamen auflösen. Außerdem können keine Pakete zwischen RAS-Clients und Intranetressourcen weitergeleitet werden.

Anhand des in diesem Kapitel beschriebenen Prozesses können Sie eine RAS-Lösung von Grund auf entwerfen und bereitstellen oder Ihre vorhandene Infrastruktur überprüfen und verbessern. Wenn in Ihrem Unternehmen bereits eine DFÜ- oder VPN-Instrastruktur eingerichtet ist, sollten Sie feststellen, ob vorhandene Komponenten ersetzt werden sollten. Hierfür gibt es viele Gründe:

- Die Komponenten sind bald veraltet oder können nicht fehlerfrei ausgeführt werden.
- Die Skalierbarkeit der vorhandenen Infrastruktur ist begrenzt.
- Für das gesamte Unternehmen sind höhere Sicherheitsanforderungen erforderlich.

Bei den in diesem Kapitel vorgestellten Bereitstellungsverfahren wird von den folgenden Voraussetzungen ausgegangen:

- Im Unternehmen wird Active Directory bereits eingesetzt.
- Eine Infrastruktur öffentlicher Schlüssel ist eingerichtet.
- Sie haben einen IAS-Server bereitgestellt.

Prozess zum Bereitstellen von DFÜ- und VPN-RAS-Servern

Um DFÜ- oder VPN-RAS-Server bereitzustellen, müssen Sie zunächst feststellen, welche Lösung für Ihre Netzwerkumgebung bei den gegebenen Sicherheits-, Skalierbarkeits- und finanziellen Anforderungen am besten geeignet ist. In Abbildung 6.1 wird gezeigt, wie eine RAS-Lösung bereitgestellt wird.

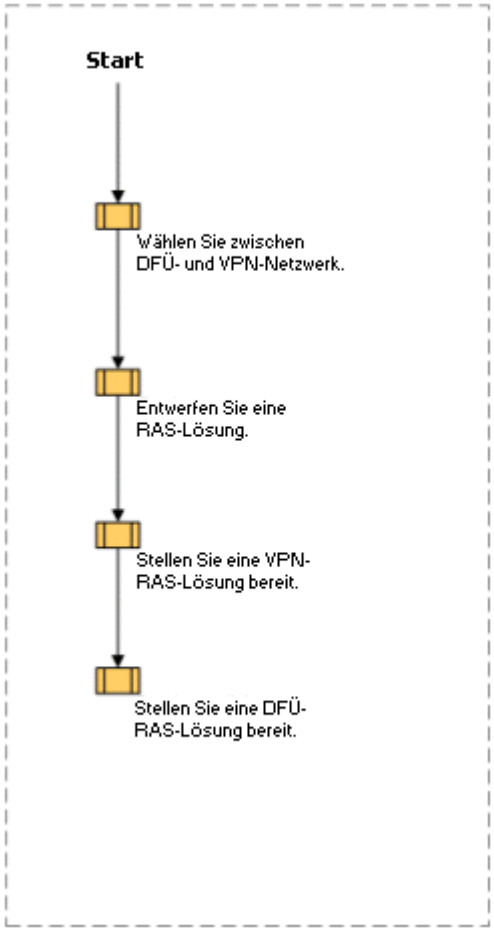

Abbildung 6.1 Prozess zum Bereitstellen von DFÜ- und VPN-RAS-Servern

Gründe für die Verwendung eines DFÜ- oder eines VPN-Netzwerks

Nach dem Einrichten einer sicheren Netzwerkarchitektur, die auf der Windows Server 2003-Familie basiert, muss als Nächstes entschieden werden, ob der Netzwerkzugriff für Remoteclients über ein DFÜ-Netzwerk, eine VPN-Lösung oder eine Kombination aus beiden zur Verfügung gestellt werden soll. Jede Methode hat Vor- und Nachteile, die Sie je nach Unternehmensanforderungen gegeneinander abwägen müssen. Eine DFÜ-Netzwerklösung bietet einen sicheren Datenpfad über eine Circuit-Switched-Verbindung. Direkte DFÜ-Verbindungen mit dem Unternehmensnetzwerk sind für mobile Benutzer sehr bequem. Eine VPN-Lösung wird über das Internet bereitgestellt. Aufgrund der öffentlichen Zugänglichkeit des Internets werden für VPN-Netzwerke eine Vielzahl von Sicherheitstechnologien wie Verschlüsselungstunnel und Authentifizierung eingesetzt. Um für eine VPN-Bereitstellung den höchsten Grad an Sicherheit zu gewährleisten, sollten Sie Layer-Two-Tunneling-Protokoll mit Internet Protocol Security (L2TP/IPSec) verwenden.

Sie können die Sicherheit und Verwaltbarkeit der RAS-Lösung erhöhen, indem Sie mithilfe von Internet Authentication Service (IAS) die VPN- oder DFÜ-Netzwerkauthentifizierung und -verwaltung zentralisieren. IAS ist eine Implementierung des RADIUS-Servers (Remote Authentication Dial-In User Service) in die Windows 2000 Server-Familie und eines RADIUS-Servers und Proxys in die Windows Server 2003-Familie.

DFÜ-Netzwerke

Bei einer DFÜ-Netzwerklösung wählen sich die Remotebenutzer an einem RAS-Server im Unternehmensnetzwerk ein. DFÜ-Verbindungen sind privater als eine Lösung, bei der ein öffentliches Netzwerk wie das Internet genutzt wird. Ein DFÜ-Netzwerk ist für das Unternehmen jedoch mit einer erheblichen Anfangsinvestition und während der gesamten Lebensdauer der Lösung mit laufenden Kosten verbunden. Die Kosten sind im Folgenden aufgeführt:

- **Kauf und Installation der Hardware.** Für DFÜ-Netzwerke fallen zunächst Kosten für Modems oder andere Kommunikationshardware, für Serverhardware sowie die Einrichtung eines Telefonanschlusses an.
- **Monatliche Telefongebühren.** Jeder für einen Remotezugriff genutzte Telefonanschluss erhöht die Kosten von DFÜ-Netzwerken. Wenn Sie gebührenfreie Nummern oder die Rückruffunktion verwenden, um für die Remotebenutzer die Kosten für Ferngespräche zu übernehmen, können beträchtliche Kosten entstehen. Die meisten Unternehmen können eine Pauschalgebühr für Ferngespräche einrichten, die der Einzelerstattung von Kosten für Benutzer mit höheren regionalen Gebühren vorzuziehen sind.
- **Laufende Supportkosten.** Die Zahl der RAS-Benutzer und die Komplexität des RAS-Entwurfs wirken sich erheblich auf die laufenden Supportkosten für DFÜ-Netzwerke aus. Es fallen z. B. Supportkosten für Netzwerksupporttechniker, Testumgebungen, Schulungen und das Helpdeskpersonal für den Support und die Verwaltung der Bereitstellung an. Diese Kosten stellen den größten Teil der Unternehmensinvestitionen dar.

Abbildung 6.2 zeigt ein Beispiel für einen einfachen DFÜ-Netzwerkentwurf.

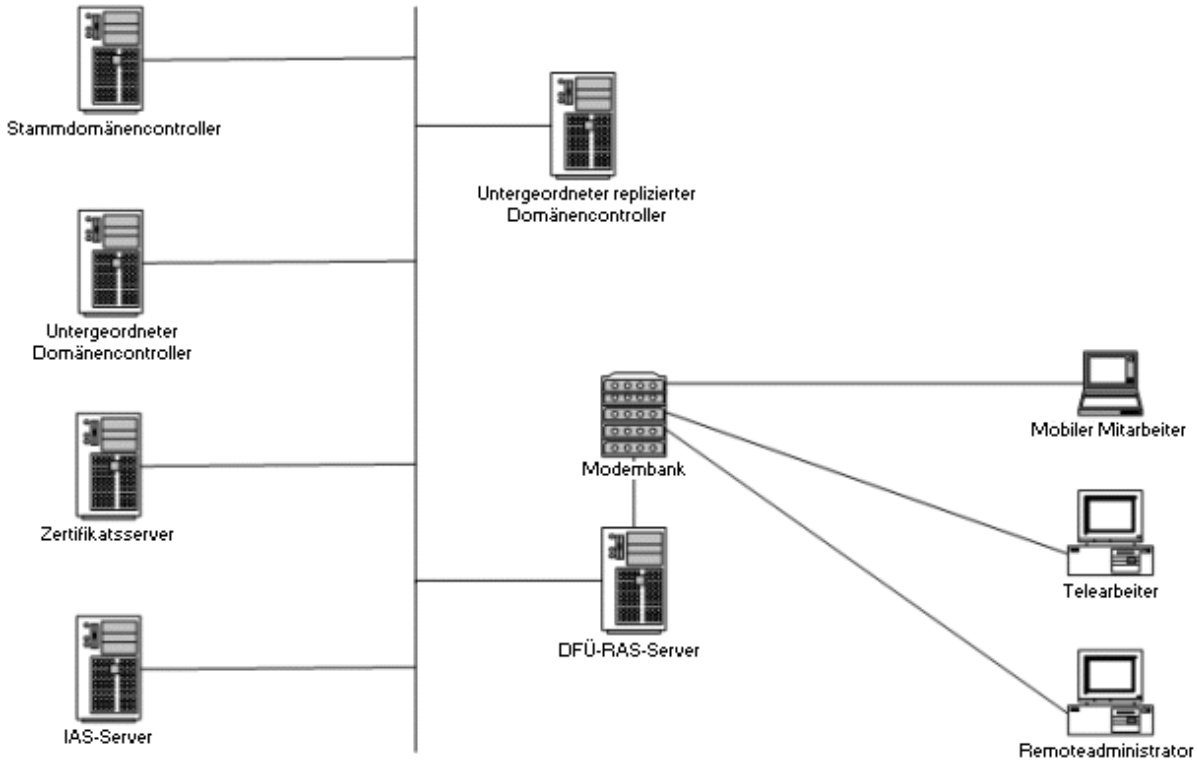

Abbildung 6.2 DFÜ-RAS-Beispielentwurf

Virtuelle private Netzwerke (VPN)

Bei einer VPN-Lösung stellen die Benutzer über das Internet eine Verbindung mit dem Unternehmensnetzwerk her. Dank einer Kombination aus Tunneling-, Authentifizierungs- und Verschlüsselungstechnologien werden dabei sichere Verbindungen hergestellt.

Viele Unternehmen mit hohen RAS-Anforderungen implementieren eine VPN-Lösung. Mit virtuellen privaten Netzwerken können die RAS-Kosten durch Verwendung der bestehenden Internetinfrastruktur deutlich verringert werden. Mithilfe von VPNs können Sie Ihre zentrale, interne DFÜ-RAS-Infrastruktur und Ihre Legacydienste teilweise oder ganz ersetzen.

VPNs bieten zwei wichtige Vorteile:

- **Geringere Kosten.** Durch Verwendung des Internets als Verbindungsmedium fallen keine Telefongebühren für Ferngespräche an, und es wird weniger Hardware benötigt als bei einer DFÜ-Netzwerklösung.
- **Ausreichende Sicherheit.** Durch die Authentifizierung wird verhindert, dass nicht autorisierte Benutzer eine Verbindung herstellen können. Aufgrund sicherer Verschlüsselungsmethoden ist es für Hacker extrem schwierig, die über eine VPN-Verbindung gesendeten Daten zu übersetzen.

Abbildung 6.3 zeigt ein Beispiel für einen einfachen VPN-Entwurf.

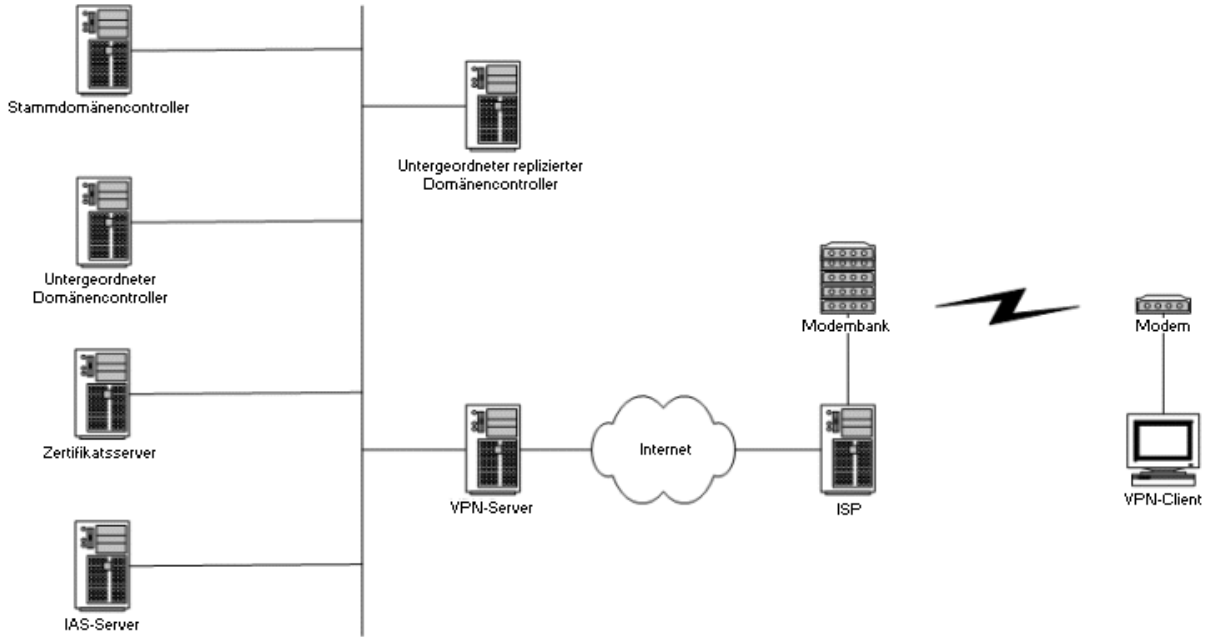

Abbildung 6.3 VPN-RAS-Beispielentwurf

Entwerfen einer RAS-Lösung

Nach Auswahl der RAS-Methode (DFÜ-Netzwerk, VPN oder beides) beginnt die Entwurfsphase. In Abbildung 6.4 wird gezeigt, wie eine RAS-Lösung entworfen wird.

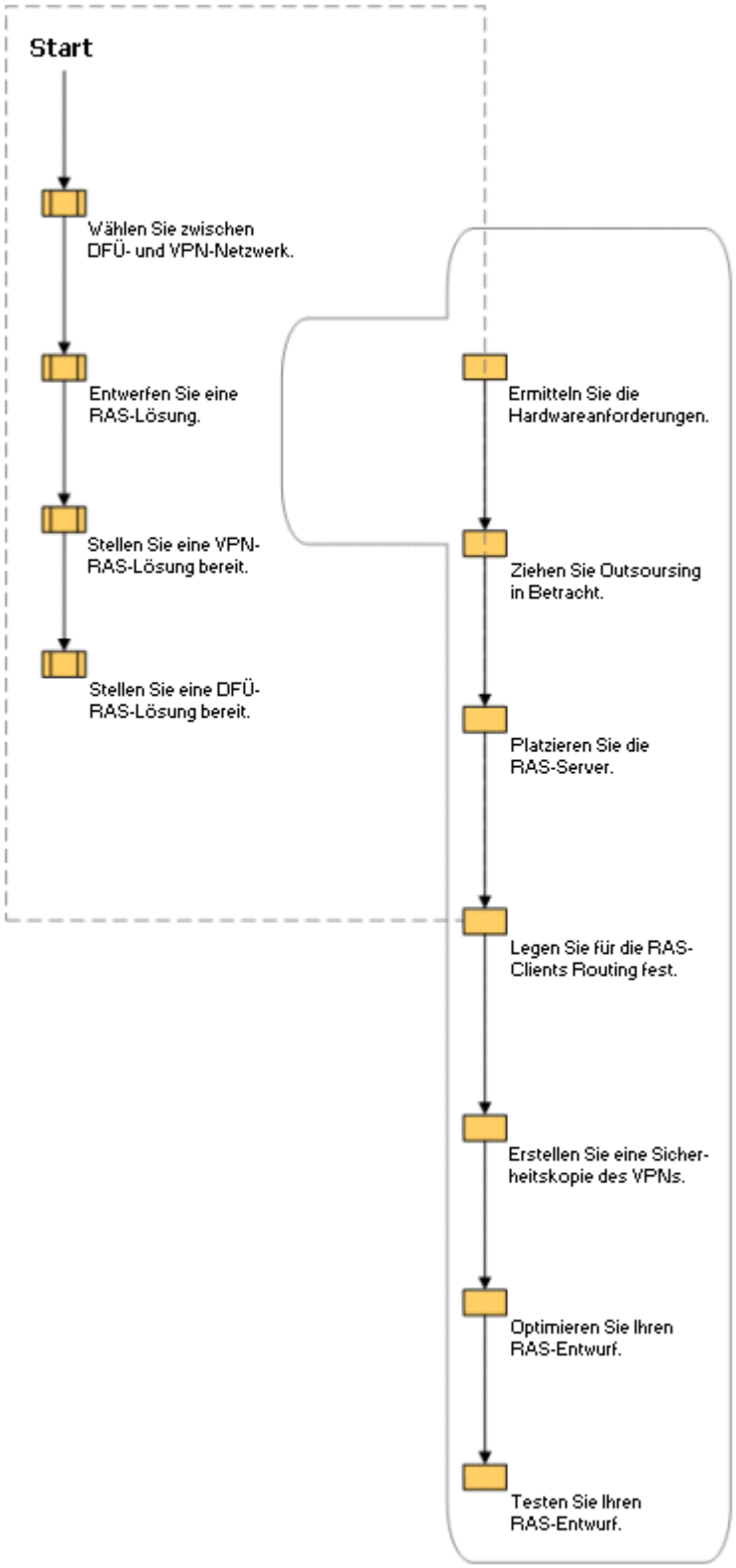

Abbildung 6.4 Entwerfen einer RAS-Lösung

Ermitteln der Hardwareanforderungen

Um eine optimale Leistung zu erzielen, sollten Sie für jede mögliche Ausstattung Ihrer Produktionsumgebung Tests durchführen. Stellen Sie fest, wie hoch die Speicherkapazität für Ihre DFÜ- bzw. VPN-Server sein muss und welche zusätzlichen Hardwaregeräte (z. B. Modembänke für eine DFÜ-Lösung) Sie benötigen. Bei der Auswahl der Serverhardware müssen Sie die CPU-, RAM- und Netzwerkhardware-Anforderungen berücksichtigen.

- Ermitteln der Hardwareanforderungen für DFÜ-Netzwerke
- Ermitteln der Hardwareanforderungen für eine VPN-Lösung

Ermitteln der Hardwareanforderungen für DFÜ-Netzwerke

Ermitteln Sie die Hardwareanforderungen für Ihren DFÜ-Netzwerkentwurf anhand der folgenden Richtlinien:

- Berücksichtigen Sie die zusätzlich zu den Servern erforderliche Hardware, wie z. B. Modembänke und Telefonanschlüsse. Richten Sie auf der Basis der maximalen Anzahl an DFÜ-RAS-Clients, die sich gleichzeitig einwählen werden, Modembänke und Telefonanschlüsse ein, die den Unternehmensanforderungen gerecht werden.
- Für jedes serverseitige Modem ist ein serieller Anschluss am RAS-Server erforderlich. Verwenden Sie für mehrere Modems (Modembänke) einen seriellen Mehrfachanschlussadapter oder eine HD-Kombinationskarte. Mithilfe eines seriellen Adapters mit mehreren Anschlüssen können Sie eine große Anzahl an analogen Modems oder ISDN-Modems mit einem RAS-Server verbinden. Eine HD-Kombinationskarte (High Density) kombiniert mehrere Modems und serielle Adapter in einem Gerät.
- Für eine optimale Leistung sollten Sie "intelligente" Kommunikationsadapter (serielle Karten mit mehreren Anschlüssen) verwenden, die den RAS-Server bei der Verarbeitung entlasten.

Ermitteln der Hardwareanforderungen für VPNs

Ermitteln Sie anhand der folgenden Richtlinien die Netzwerk-Hardwareanforderungen für Ihren VPN-Entwurf:

- Verwenden Sie für Schnittstellen im öffentlichen Netzwerk Netzwerkadapter mit hardwareseitiger Verschlüsselung.
- Legen Sie bei einer 10/100 Ethernetinfrastruktur für alle Geräte Vollduplex, 100 MBit/s fest.
- Verbinden Sie die Schnittstellen im privaten Netzwerk direkt mit einer Hochleistungsserver-Schnittstelle, die auch die Datenserver und Gateways verbindet, auf die RAS-Clients häufig zugreifen.

CPU-Anforderungen

Ermitteln Sie anhand der folgenden Richtlinien die Hardwareanforderungen für Ihren VPN-Entwurf:

- Für die Verarbeitung ein- und ausgehender Pakete sind CPU-Zyklen erforderlich. Durch eine höhere Verarbeitungskapazität können Sie den Durchsatz erhöhen.
- Die doppelte Geschwindigkeit eines einzelnen Prozessors ist effektiver als die doppelte Anzahl an Prozessoren.
- Bei Verwendung von Plattformen mit mehreren Prozessoren kann durch Verknüpfung je einer CPU mit einem Netzwerkadapter effizienter auf Interrupts reagiert werden. Dadurch können Zyklen freigegeben und die Leistungsdiskrepanz reduziert werden, die bei Verwendung einer großen Anzahl weniger leistungsfähiger CPUs und einer geringen Anzahl schnellerer, teurerer CPUs besteht.

RAM-Anforderungen

Ermitteln Sie anhand der folgenden Richtlinien die RAM-Anforderungen für VPN-Server:

- Jede aktive Verbindung benötigt einen kleinen Block (etwa 40 KB) nicht auslagerungsfähigen Speichers. Wenn Sie nicht mehr als 1.000 gleichzeitige Aufrufe von RAS-Benutzern verarbeiten müssen, sind 512 MB RAM angemessen. Wenn Sie eine Verarbeitungskapazität für mehr als 1.000 gleichzeitige Aufrufe benötigen, sollten Sie 1 GB RAM bereitstellen.
- Stellen Sie zusätzlich zur empfohlenen RAM-Kapazität für jeweils 1.000 zusätzliche gleichzeitige Aufrufe weitere 128 MB RAM für den Server zur Verfügung sowie 128 MB als Basis für den Remotezugriff und damit verbundene Dienste. Wenn der empfohlene Speicher für die Windows Server 2003-Familie z. B. 256 MB beträgt, sollten Sie für einen dedizierten RAS, der 1.000 gleichzeitige VPN-Aufrufe unterstützt, 512 MB RAM verwenden (256 KB + 128 KB + 128 KB).

Kapazitätsplanung

Die beiden wahrscheinlichsten Leistungseinschränkungen hängen mit der Anzahl gleichzeitiger Verbindungen und dem gesamten Datendurchsatz zusammen. Die Anzahl gleichzeitiger Verbindungen, die von einem VPN-Server unterstützt werden können, wird durch die Menge an verfügbarem nicht ausgelagertem Poolspeicher bestimmt. Die mögliche Anzahl an gleichzeitigen Verbindungen hängt auch von den verwendeten Optionen ab. Bei einer Komprimierung verwendet z. B. jede Verbindung eine große Menge an nicht ausgelagertem Speicher. Wird die Komprimierung deaktiviert, kann dadurch die Leistung deutlich verbessert werden.

Die verfügbare Verarbeitungsleistung eines VPN-Servers bestimmt die Datendurchsatzkapazität des Servers. Tunnelingprotokolle wirken sich ebenfalls auf den Datendurchsatz aus. Für PPTP-Verbindungen ist eine geringere Verarbeitungsleistung erforderlich als für L2TP/IPSec-Verbindungen. L2TP/IPSec-Verbindungen bieten jedoch die höchste Sicherheit. Mit hardwareseitiger Verschlüsselung können Sie die Auswirkungen von L2TP/IPSec auf die Verarbeitungsleistung reduzieren.

Outsourcingoptionen

Durch Auslagern eines Teils der RAS-Lösung bzw. der gesamten Lösung durch einen Großhandelsvertrag mit einem Internetdienstanbieter können manche Unternehmen ihre Installations- und Betriebskosten deutlich reduzieren. Sie können eine RAS-Lösung teilweise oder ganz auslagen, indem Sie einen Großhandelsvertrag mit einem Internetdienstanbieter (Internet Service Provider oder ISP) abschließen, der einen bestimmten Grad an Dienstverfügbarkeit gewährleistet. Ein ISP kann zu festen Kosten für einen großen geografischen Bereich den Zugriff auf umfassende Netzwerkverbindungen zur Verfügung stellen. Viele ISPs gewährleisten einen ähnlich hohen Grad an Dienstverfügbarkeit wie DFÜ-WAN-Verbindungen.

Wenn Sie eine DFÜ-Netzwerklösung bereitstellen, können Sie durch Auslagern der Bereitstellung verhindern, dass Gebühren für Ferngespräche anfallen.

Bei einer VPN-Lösung hat das Auslagern den bedeutsamen Vorteil, dass ein ISP viele der zur Unterstützung des VPN-Zugriffs erforderlichen Komponenten zur Verfügung stellen kann, darunter die folgenden:

- Netzwerkzugriffsserver (Network Access Server oder NAS) für den Zugriff von unterschiedlichen geografischen Zugriffspunkten aus.
- RADIUS-Proxyserver für sicheres Routing von Zugriffsanforderungen an das Unternehmen.
- Telefonbuchunterstützung für die Übermittlung der aktuellen Zugriffsnummern an das Unternehmen oder direkt an den Client.

Auslagern von Netzwerkzugriffsservern

VPN-Benutzer wählen sich zunächst an einem NAS ein. Die NAS-Server können in Ihrer VPN-Lösung eine Schwachstelle darstellen, es sei denn, in der Auslagerungsvereinbarung sind für die NAS-Server des Internetdienstanbieters z. B. die erforderliche Verbindungsgeschwindigkeit, Geräteunterstützung und Dienstverfügbarkeit angegeben. Bei einer Auslagerung müssen Sie sicherstellen, dass die NAS-Server des ISPs Ihre Zugriffsanforderungen erfüllen.

Auslagern der Authentifizierung

Wenn Sie Ihre VPN-Lösung auslagern, können Sie mit dem ISP einen Vertrag über die Authentifizierungsdienste abschließen. Der ISP kann auch einen RADIUS-Proxy verwenden und die Authentifizierungsanforderungen an einen von Ihnen verwalteten RADIUS-Server senden.

Platzieren von RAS-Servern

Bei der Platzierung von RAS-Servern im Netzwerk sollten Sie die Platzierung der Firewall sowie anderer Netzwerkressourcen berücksichtigen. Platzieren Sie die RAS-Server in der Nähe der für RAS-Clients erforderlichen Netzwerkressourcen. Zu diesen Ressourcen können eine Zertifizierungsstelle (Certification Authority oder CA), ein Domänencontroller (Domain Controller oder DC) oder Datei- und Anwendungsserver gehören.

Bei einem DFÜ-RAS-Entwurf werden Server i. A. hinter der Firewall platziert. Da ein VPN-Entwurf Internetkonnektivität einschließt, spielt die Serverplatzierung in Bezug auf die Firewall eine noch wichtigere Rolle.

Wenn Sie eine VPN-RAS-Lösung entwerfen, können Sie in Bezug auf die Serverplatzierung unter den folgenden Optionen auswählen:

- **VPN-Server hinter der Firewall.** Die Firewall ist mit dem Internet verknüpft, und der VPN-Server befindet sich zwischen der Firewall und dem Intranet.
- **VPN-Server vor der Firewall.** Der VPN-Server ist mit dem Internet verknüpft, und die Firewall befindet sich zwischen dem VPN-Server und dem Intranet.
- **VPN-Server zwischen zwei Firewalls.** Eine Firewall befindet sich zwischen dem VPN-Server und dem Intranet und eine zweite Firewall zwischen dem VPN-Server und dem Internet. Hier handelt es sich um eine Perimeternetzwerkkonfiguration.

Jede Platzierung bietet unterschiedliche Entwurfsoptionen.

VPN-Server hinter der Firewall

Die häufigste Konfiguration für einen VPN-RAS-Entwurf besteht in der Platzierung des VPN-Servers hinter einer Firewall. Bei dieser Konfiguration ist die Firewall mit dem Internet verbunden, und der VPN-Server ist eine mit dem Perimeternetzwerk verbundene Intranetressource. Der VPN-Server hat eine Schnittstelle im Perimeternetzwerk und im Intranet. Die Internetfirewall (die Firewall zwischen dem Internet und dem VPN-Server) filtert den gesamten von Internetclients ausgehenden Datenverkehr. Die Intranetfirewall (die Firewall zwischen dem VPN-Server und dem Intranet) filtert den von VPN-Clients ausgehenden Datenverkehr.

Für diese Platzierung müssen die folgenden Konfigurationen durchgeführt werden:

- Konfigurieren Sie die Internetfirewall und den VPN-Server mit den gleichen Paketfiltern, die Sie verwenden würden, wenn sich der VPN-Server hinter der Firewall befinden würde.
- Konfigurieren Sie für die Intranetfirewall entsprechend Ihren Netzwerksicherheitsrichtlinien die Regeln für den auf den VPN-Clients ein- und ausgehenden Intranetverkehr.

Bei dieser Herangehensweise müssen Sie die Internetschnittstelle auf der Firewall mit Ein- und Ausgabefiltern konfigurieren, die einen Datenverkehr zum VPN-Server ermöglichen. Sie können zusätzliche Filter angeben, um den Datenverkehr zu den Webservern, FTP-Servern (File Transfer Protocol) und anderen Arten von Servern im Perimeternetzwerk zu ermöglichen.

Um eine zusätzliche Sicherheitsstufe zu erzielen, können Sie die Perimeternetzwerk-Schnittstelle auf dem VPN-Server auch mit PPTP- oder L2TP/IPSec-Paketfiltern konfigurieren.

VPN-Server vor der Firewall

Eine weitere Möglichkeit besteht in der Platzierung des VPN-Servers vor der direkt mit dem Internet verbundenen Firewall. Bei der Implementierung dieses Entwurfs müssen Sie der Internetschnittstelle Paketfilter hinzufügen, die nur den VPN-Verkehr zu und von der IP-Adresse der Internetschnittstelle des VPN-Servers zulassen.

Bei eingehendem Verkehr entschlüsselt der VPN-Server die über Tunneling gesendeten Daten und leitet sie an die Firewall weiter. Die Firewall fungiert als Filter für Intranetverkehr und kann den Zugriff auf bestimme Ressourcen verhindern, Daten auf Viren hin überprüfen, Eindringversuche erkennen und andere Funktionen ausführen.

Festlegen von Routing für RAS-Clients

Da RAS-Clients normalerweise keine Routingprotokolle wie RIP oder OSPF unterstützen, weisen die Clients häufig sehr einfache Routingtabellen auf. Ein Computer in einem kleinen LAN verfügt z. B. über eine Route zum eigenen Subnetz im LAN und möglicherweise über eine Standardroute zu einem Gatewayrouter im LAN für jede andere Art von Datenverkehr. Ohne eine Unterstützung von Routingprotokollen können RAS-Clients nicht die optimale Route für ein bestimmtes Ziel ermitteln.

Routing für VPN-RAS-Clients

Für die Weiterleitung von Paketen an ein Remotenetzwerk sollte auf dem RAS-Client eine Standardroute eingerichtet werden. Bei dieser Konfiguration wird jedes Paket, das nicht für das direkte lokale LAN-Segment vorgesehen ist, an das Remotenetzwerk gesendet. Während eine Verbindung hergestellt wird, fügen alle RAS-Clients ihren Routingtabellen standardmäßig eine Standardroute hinzu und erhöhen den metrischen Wert der vorhandenen Standardroute, um sicherzustellen, dass nur die neueste Standardroute verwendet wird. Die neueste Standardroute verweist auf die neue Verbindung. Dadurch ist sichergestellt, dass alle Pakete, die nicht an das LAN-Segment adressiert sind, an das Remotenetzwerk gesendet werden. Wenn VPN-Clients eine Verbindung herstellen und eine neue Standardroute erstellen, kann auf zuvor verfügbare Internetsites nicht mehr zugegriffen werden. Dieses Verhalten ist angemessen, wenn VPN-Clients nur auf das Unternehmensnetzwerk zugreifen müssen. Für Clients, die weiterhin auf das Internet zugreifen müssen, während die Verbindung mit dem Unternehmensnetzwerk besteht, wird jedoch keine neue Standardroute erstellt. Stattdessen müssen den Routingtabellen des VPN-Clients spezielle Routen hinzugefügt werden, die über die VPN-Verbindung Pakete an das Unternehmensnetzwerk weiterleiten. Zugleich erfolgt der Internetzugriff über die vorhandene Standardroute, die die Verbindung mit dem ISP verwendet. Diese Konfiguration wird als "Split Tunneling" bezeichnet.

Konfigurieren von Split Tunneling

Mithilfe von Split Tunneling können VPN-Clients auf das Remotenetzwerk zugreifen, während der Zugriff auf das Internet weiter möglich ist. Sie können die für Split Tunneling erforderlichen Routen auf unterschiedliche Art und Weise konfigurieren:

- Wenn der VPN-Client über eine konfigurierte Verbindung ohne Standardroute verfügt, fügt der VPN-Client eine Route hinzu, die aus der dem VPN-Client für diese Verbindung zugewiesenen IP-Adresse abgeleitet wird. Bei einem einfachen Zielnetzwerk, wie z. B. in einer kleinen Niederlassung, genügt diese Route für das Weiterleiten von Paketen an das Zielnetzwerk. Bei einem komplexen Netzwerk sind jedoch mehrere Routen erforderlich, damit die Pakete an das Remotenetzwerk gesendet werden können.
- Ein Windows XP-Client verwendet nach Herstellen der Verbindung eine DHCPINFORM-Nachricht, um zusätzliche Informationen zur Verbindung abzurufen, wie z. B. mehrere Routen für das Zielnetzwerk. (Diese zusätzlichen Informationen sind nur verfügbar, wenn der DHCP-Server so konfiguriert wurde, dass er diese Informationen zur Verfügung stellt, und der Netzwerkzugriffsserver (Network Access Server oder NAS) so konfiguriert wurde, dass er die DHCPINFORM-Nachricht an den DHCP-Server weitergibt.)

- Wenn der RAS-Client mithilfe des Verbindungs-Managers verwaltet wird, kann der Netzwerkadministrator eine Routingtabelle für diese RAS-Clients vorbereiten. Eine Benutzeraktion nach Herstellen der Verbindung kann der verwalteten Verbindung zugeordnet sein, die die Routingtabelle des Clients bei jeder Verbindung aktualisiert.
- In Situationen, die weiter oben nicht beschrieben wurden, hat der Endbenutzer oder Netzwerkadministrator noch die Möglichkeit, ein Programm oder eine Batchdatei zu schreiben, das bzw. die die Routingtabelle des Clients durch Hinzufügen der erforderlichen Routen zum Remotenetzwerk aktualisiert.

Split Tunneling: Sicherheitsaspekte

Einige Netzwerkadministratoren sehen Split Tunneling als unnötiges Sicherheitsrisiko an. Sie haben die Befürchtung, dass ein Angreifer das Unternehmensnetzwerk gefährdet, indem er dafür sorgt, dass der Datenverkehr mithilfe des RAS-Clients zwischen dem Internet und dem Unternehmensnetzwerk übertragen wird. Um dies zu verhindern, können Sie den Profileinstellungen für RAS-Richtlinien für die VPN-Verbindung Paketfilter hinzufügen, die nur eingehenden Datenverkehr zulassen, dessen Quelle der RAS-Client ist.

Abrufen von IP-Adressen für RAS-Clients

Anhand der folgenden Methoden können Sie IP-Adressen abrufen, die RAS-Clients zugewiesen werden:

Dynamic Host Configuration Protocol (DHCP)

Der Routing- und RAS-Dienst weist RAS-Clients IP-Adressen zu. Der Routing- und RAS-Dienst kann IP-Adressen von einem DHCP-Server abrufen.

Statischer Pool von IP-Adressen

Sie können einen statischen Pool von IP-Adressen konfigurieren, die RAS-Clients zugewiesen werden sollen. Für den statischen Pool können Sie sowohl einen subnetzinternen als auch einen subnetzexternen Bereich von IP-Adressen angeben.

Sichern eines virtuellen privaten Netzwerks

Die Sicherheit eines VPN basiert auf den verwendeten Tunneling-, Authentifizierungs- und Verschlüsselungsprotokollen. Für den höchsten Grad an Sicherheit sollten Sie ein RAS-VPN verwenden, das auf L2TP/IPSec basiert. Wenn Sie eine PPTP-basierte VPN-Lösung verwenden möchten, um die Kosten zu reduzieren und die Verwaltbarkeit und Interoperabilität zu verbessern, sollten Sie Microsoft Challenge-Handshake Authentication-Protokoll, Version 2 (MS-CHAPv2) als Authentifizierungsprotokoll verwenden.

In diesem Abschnitt werden folgende Themen behandelt:

- Auswählen von VPN-Protokollen
- Auswählen von Authentifizierungsprotokollen
- Auswählen von Verschlüsselungsstufen
- Verwenden einer Zertifikatsinfrastruktur

Auswählen von VPN-Protokollen

Stellen Sie bei Ihrem VPN-Entwurf fest, welches VPN-Protokoll Ihren Anforderungen optimal gerecht wird. Die Windows Server 2003-Familie unterstützt zwei VPN-Protokolle: PPTP und L2TP/IPSec.

Point-to-Point-Tunneling-Protokoll (PPTP)

PPTP verwendet PPP-Benutzerauthentifizierung (Point-to-Point Protocol) und Punkt-zu-Punkt-Verschlüsselung (Microsoft Point-to-Point Encryption, MPPE), um IP-, IPX- und NetBEUI-Verkehr zu kapseln und zu verschlüsseln. PPTP ist bei Verwendung mit MS-CHAP v2 für eine kennwortbasierte Authentifizierung und sichere Kennwörter eine äußerst sichere VPN-Technologie. Sie können eine PKI mit Smartcards oder Benutzerzertifikaten und Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mit PPTP implementieren.

PPTP ist weit verbreitet und kann problemlos bereitgestellt und für die meisten NATs (Network Address Tanslators) verwendet werden.

Verwenden eines NATs

Ein NAT übersetzt die IP-Adressen und TCP/UDP-Anschlussnummern von Paketen, die zwischen einem privaten Netzwerk und dem Internet weitergeleitet werden. Der NAT und das private Netzwerk können den anderen Computern im privaten Netzwerk Konfigurationsinformationen für IP-Adressen bereitstellen. Der NAT kann als vereinfachte Form des DHCP-Servers fungieren, der eine IP-Adresse, eine Subnetzmaske, einen Standardgateway und die IP-Adresse eines DNS-Servers zuweist. Der NAT kann zum DNS-Server für die Computer im privaten Netzwerk werden. Wenn der NAT von einem Computer im privaten Netzwerk Namensauflösungsanforderungen erhält, leitet er die Anforderung an einen bestimmten internetbasierten DNS-Server weiter und gibt eine Antwort an den anfordernden Computer im privaten Netzwerk zurück.

Bereitstellen eines NAT-Editors

Damit VPN-Clients unterstützt werden, die sich hinter NAT-Geräten (Network Address Translation) befinden, müssen die NATs über einen NAT-Editor verfügen, der den PPTP-Verkehr übersetzen kann.

Ein NAT-Editor ist erforderlich, da mit PPTP getunnelte Daten anstelle von TCP- oder UDP-Headern (User Data Protocol) GRE-Header (Generic Routing Encapsulation) verwenden. Der NAT-Editor verwendet das Anrufskennungsfeld im GRE-Header, um den PPTP-Datenstrom zu identifizieren und IP-Adressen und Aufruf-IDs für PPTP-Datenpakete zu übersetzen, die zwischen einem privaten Netzwerk und dem Internet weitergeleitet werden. Die NAT-Routingprotokollkomponente des Routing- und RAS-Dienstes verfügt über einen NAT-Editor für PPTP-Verkehr.

Layer-Two-Tunneling-Protokoll über IPSec (L2TP/IPSec)

Dies ist die sicherste Kombination. L2TP/IPSec setzt die PPP-Benutzerauthentifizierung und die IPSec-Verschlüsselung ein, um den IP-Verkehr zu kapseln und zu verschlüsseln. Bei dieser Kombination werden mithilfe einer zertifikatsbasierten Computer-ID-Authentifizierung neben der PPP-basierten Benutzerauthentifizierung IPSec-Sicherheitszuweisungen generiert. L2TP/IPSec bietet für jedes Paket Datenintegrität, eine Authentifizierung des Datenursprungs, Datenvertraulichkeit und Schutz vor Replay-Attacken.

Die Microsoft® Windows Server 2003-Familie sowie die Betriebssysteme Microsoft® Windows® 2000 und Windows® XP unterstützen L2TP/IPSec. Um L2TP/IPSec mit den Betriebssystemen Microsoft® Windows® 98, Windows® Me oder Windows NT® Workstation, Version 4.0, zu verwenden, müssen Sie den Microsoft L2TP/IPSec-VPN-Client (Mls2tp.exe) downloaden und installieren. Weitere Informationen zu **Mls2tp.exe** finden Sie über die Verknüpfung zum Microsoft L2TP/IPSec-VPN-Client auf der Seite **Web Resources** unter http://www.microsoft.com/windows/reskits/webresources/default.asp (englischsprachig).

Unterstützen von IPSec-NAT-Traversierung (NAT-T)

Mithilfe der IPSec-NAT-Traversierung (NAT-T) können IPSec-Clients und -Server ausgeführt werden, während sie sich hinter einem NAT befinden. Für die Verwendung von NAT-T müssen der RAS-VPN-Client und der RAS-Server IPSec NAT-T-fähig sein.

IPSec NAT-T ermöglicht eine UDP-Einkapselung von IPSec-Paketen, so dass der mit Internet Key Exchange (IKE) und Encapsulating Security Payload (ESP) geschützte Datenverkehr einen NAT durchlaufen kann. IKE erkennt automatisch, dass ein NAT vorhanden ist und verwendet eine UDP-ESP-Einkapselung (User Datagram Protocol-Encapsulating Security Payload), damit der mit ESP geschützte IPSec-Verkehr den NAT durchlaufen kann.

IPSec NAT-T wird von der Windows Server 2003-Familie unterstützt.

In Tabelle 6.1 sind die Vorteile und die Einschränkungen zusammengefasst, die mit der Verwendung der PPTP- und L2TP-Protokolle verbunden sind.

Tabelle 6.1 Vorteile und Einschränkungen von PPTP und L2TP

Faktor	Vorteile und Einschränkungen von PPTP	Vorteile und Einschränkungen von L2TP
Clientbetriebssystem	PPTP wird auf Clients unterstützt, die die folgenden Betriebssysteme ausführen: Microsoft® Windows XP, Windows Server 2003, Windows NT Workstation, Version 4.0, Windows Me und Windows 98.	• Die L2TP-Unterstützung ist auf Computern unter Windows XP oder Windows Server 2003 im Lieferumfang enthalten. • Ist **Mls2tp.exe** installiert, wird L2TP auch auf Computern unter Windows 98, Windows Me oder Windows NT Workstation 4.0 unterstützt.
Zertifikate	PPTP benötigt keine Zertifikatsinfrastruktur, um Computerzertifikate auszugeben.	Damit Computerzertifikate an den VPN-Server und alle VPN-Clients ausgegeben werden können, benötigt L2TP/IPSec eine Zertifikatsinfrastruktur.
Sicherheit	PPTP bietet Datenvertraulichkeit (aufgezeichnete Pakete können ohne den Verschlüsselungsschlüssel nicht übersetzt werden). PPTP bietet keine Datenintegrität (Nachweis, dass die Daten während der Übertragung nicht geändert wurden) und keine Datenauthentifizierung (Nachweis, dass die Daten vom autorisierten Benutzer gesendet wurden).	L2TP/IPSec bietet Datenvertraulichkeit, Datenintegrität, eine Authentifizierung des Datenursprungs und Wiederholungsschutz.
Leistung	Ein VPN-Server unterstützt mehr PPTP-Verbindungen als L2TP-Verbindungen.	Eine IPSec-Verschlüsselung ist prozessorintensiv. Ein VPN-Server unterstützt weniger L2TP-Verbindungen als PPTP-Verbindungen. Durch Erhöhung der CPU oder Verwendung von NICs mit Verschlüsselungshardware kann die Anzahl möglicher Verbindungen erhöht werden.
NAT	PPTP-basierte VPN-Clients können sich hinter einem NAT befinden, vorausgesetzt, der NAT verfügt über einen PPTP-Editor. Weitere Informationen finden Sie unter "NAT-Entwurfsaspekte" weiter unten in diesem Abschnitt. PPTP-basierte VPN-Clients können sich hinter einem NAT befinden. Weitere Informationen finden Sie unter "NAT-Entwurfsaspekte" weiter unten in diesem Abschnitt.	L2TP/IPSec-Clients oder -Server können sich nicht hinter einem NAT befinden, es sei denn, sie unterstützen IPSec NAT-T.

Weitere Informationen zum Bereitstellen von Zertifikatsdiensten für die Unterstützung von L2TP/IPSec finden Sie unter "Deploying a Public Key Infrastructure" in *Designing and Deploying Directory and Security Services* dieses Kits (englischsprachig).

Auswählen von Authentifizierungsprotokollen

Um den Benutzer zu authentifizieren, der eine PPP-Verbindung herzustellen versucht, unterstützt Windows Server 2003 eine Vielzahl von PPP-Authentifizierungsprotokollen, darunter die folgenden:

- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication-Protokoll (CHAP)
- Microsoft Challenge-Handshake Authentication-Protokoll (MS-CHAP)
- MS-CHAP v2 (MS-CHAP v2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)

Für PPTP-Verbindungen ist MS-CHAP, MS-CHAP v2 oder EAP-TLS erforderlich. Nur diese drei Authentifizierungsprotokolle bieten die Möglichkeit, auf dem VPN-Client und dem VPN-Server den gleichen Verschlüsselungsschlüssel zu generieren. MPPE verwendet diesen Verschlüsselungsschlüssel, um alle über die VPN-Verbindung gesendeten PPTP-Daten zu verschlüsseln. MS-CHAP und MS-CHAP v2 sind kennwortbasierte Authentifizierungsprotokolle.

Werden keine Benutzerzertifikate oder Smartcards verwendet, sollte MS CHAP v2 eingesetzt werden. Dieses Authentifizierungsprotokoll ist sicherer als MS CHAP und ermöglicht eine gegenseitige Authentifizierung. Bei einer gegenseitigen Authentifizierung authentifiziert der VPN-Server den VPN-Client, und der VPN-Client authentifiziert den VPN-Server.

> **Anmerkung** Wenn Sie ein kennwortbasiertes Authentifizierungsprotokoll verwenden müssen, sollten Sie in Ihrem Netzwerk die Verwendung von sicheren Kennwörtern erzwingen. Sichere Kennwörter sind lang (mehr als 8 Zeichen) und enthalten eine zufällige Mischung aus Groß- und Kleinbuchstaben sowie Zahlen und Satzzeichen. "f3L*q02~>xR3w#4o" ist z. B. ein sicheres Kennwort. In einer unter dem Verzeichnisdienst Active Directory erstellten Domäne sollten Sie Gruppenrichtlinieneinstellungen verwenden, um sichere Benutzerkennwörter zu erzwingen.

EAP-TLS ist für die Verwendung mit einer Zertifikatsinfrastruktur sowie mit Benutzerzertifikaten oder Smartcards vorgesehen. Mit EAP-TLS sendet der VPN-Client seine Benutzerzertifikate für die Authentifizierung, und der Authentifizierungsserver für den VPN-Server sendet ein Computerzertifikat für die Authentifizierung. Dies ist die sicherste Authentifizierungsmethode, da sie nicht auf Kennwörtern basiert. Weitere Informationen zur EAP-TLS-Authentifizierung finden Sie unter "Connecting Remote Sites" in diesem Buch (englischsprachig).

Sie können Zertifizierungsstellen von Drittanbietern verwenden, vorausgesetzt, das Zertifikat im Computerspeicher des IAS-Servers enthält den Zertifikatszweck der Serverauthentifizierung, auch als erweiterte Schlüsselverwendung (Enhanced Key Usage oder EKU) bekannt. Eine EKU wird mithilfe einer Objektkennung (Object Identifier oder OID) identifiziert. Die OID für die Serverauthentifizierung lautet 1.3.6.1.5.5.7.3.1. Darüber hinaus muss der Kryptografiedienstanbieter (Cryptographic Service Provider oder CSP) für die Zertifikate SChannel unterstützen. Wenn der Kryptografiedienstanbieter SChannel nicht unterstützt, kann der IAS-Server das Zertifikat nicht verwenden, und das Zertifikat ist auf der Registerkarte **Authentifizierung** in den Eigenschaften eines Profils für eine RAS-Richtlinie unter **Smartcard- oder andere Zertifikateigenschaften** nicht auswählbar. Außerdem muss das Benutzerzertifikat, das auf einem RAS-Client unter Windows Server 2003 installiert ist, den CA-Zertifikatszweck (OID "1.3.6.1.5.5.7.3.2") enthalten. Das Zertifikat muss in der Eigenschaft **Alternativer Antragstellername** den voll gekennzeichneten Domänennamen (Fully Qualified Domain Name oder FQDN) des Computerkontos auf dem IAS-Server enthalten.

Bei L2TP/IPSec-Verbindungen können Sie ein beliebiges Authentifizierungsprotokoll verwenden, da die Authentifizierung erst erfolgt, nachdem der VPN-Client und der VPN-Server einen sicheren Verbindungskanal aufgebaut haben. Dies wird als "IPSec-Sicherheitszuordnung" (Security Association oder SA) bezeichnet. Sie sollten auf jeden Fall entweder MS-CHAP v2 oder EAP-TLS verwenden, um eine Benutzerauthentifizierung mit einer höheren Sicherheit bereitzustellen.

Berücksichtigen Sie bei der Auswahl eines Authentifizierungsprotokolls für VPN-Verbindungen die folgenden Faktoren:

- Wenn Sie Smartcards verwenden oder über eine Zertifikatsinfrastruktur verfügen, die Benutzerzertifikate ausgibt, sollten Sie das Authentifizierungsprotokoll EAP-TLS sowohl für PPTP- als auch für L2TP-Verbindungen verwenden. Nur VPN-Clients unter Windows 2000, Windows XP oder Windows Server 2003 unterstützen EAP-TLS.
- Verwenden Sie MS-CHAP v2, wenn Sie ein kennwortbasiertes Authentifizierungsprotokoll verwenden müssen, und erzwingen Sie mithilfe von Gruppenrichtlinien sichere Kennwörter. MS-CHAP v2 wird von Computern unter Windows XP, Windows Server 2003, Windows 2000, Windows NT 4.0 mit Service Pack 4 und höher, Windows Me oder Windows 98 unterstützt.

  Windows .NET IAS kann eine Authentifizierung im Auftrag eines als RADIUS-Client konfigurierten Zugriffsservers durchführen. Sie können eine Reihe von Protokollen verwenden, um Benutzer, die auf ein DFÜ-, VPN- oder drahtloses Netzwerk zugreifen möchten, und wechselnde Benutzer vor dem Netzwerkzugriff zu authentifizieren.

Bevor Sie IAS bereitstellen, müssen Sie festlegen, welche Authentifizierungsprotokolle zur Authentifizierung von RAS-Clients verwendet werden sollen. Verwenden Sie die sichersten Protokolle, die Ihre Netzwerkzugriffsserver und Clients unterstützen. Wenn Sie einen hohen Grad an Sicherheit benötigen, können Sie IAS so konfigurieren, dass nur einige äußerst sichere Authentifizierungsprotokolle zugelassen werden. Für mehr Flexibilität in Ihrem Unternehmen können Sie IAS so konfigurieren, dass auch weniger sichere Authentifizierungsprotokolle zugelassen werden. Weitere Informationen zum Entwerfen und Bereitstellen von IAS finden Sie unter "Deploying IAS" in diesem Buch (englischsprachig).

Bevor der IAS-Server für die Authentifizierung von Benutzeranmeldeinformationen und der Eigenschaften von Zugriffskonten von Benutzern auf Active Directory-Domänen zugreifen kann, muss der IAS-Server in diesen Domänen registriert werden.

Auswählen von Verschlüsselungsstufen

In einem virtuellen privaten Netzwerk schützen Sie Ihre Daten, indem Sie sie zwischen den Endpunkten der VPN-Verbindung verschlüsseln. Wenn private Daten über ein öffentliches Netzwerk gesendet werden, sollten Sie stets eine Datenverschlüsselung für VPN-Verbindungen verwenden, um zu verhindern, dass Daten abgefangen werden. Für VPN-Verbindungen verwendet Windows Server 2003 MPPE mit PPTP und IPSec-Verschlüsselung mit L2TP.

> **Anmerkung** Nicht verschlüsselte PPTP-Verbindungen (bei denen die PPP-Nutzlast im Nur-Text-Format gesendet wird) und nicht verschlüsselte L2TP-Verbindungen (bei denen der PPP-Frame im Nur-Text-Format gesendet wird) sind nicht sicher und werden für VPN-Verbindungen über das Internet nicht empfohlen.

Um eine erfolgreiche Verschlüsselung und Entschlüsselung sicherzustellen, müssen der Absender und der Empfänger einen gemeinsamen Verschlüsselungsschlüssel verwenden. Die Länge des Verschlüsselungsschlüssels ist ein wichtiger Sicherheitsparameter, besonders wenn Daten über öffentliche Netzwerke übertragen werden. Verwenden Sie die längste Schlüsselgröße, um den höchsten Grad an Sicherheit zu gewährleisten.

Linkverschlüsselung

Die Linkverschlüsselung verschlüsselt nur die Daten der Verknüpfung zwischen dem VPN-Client und dem VPN-Server. Für PPTP-Verbindungen müssen Sie MPPE mit MS-CHAP- oder EAP-TLS-Authentifizierung verwenden. Für L2TP über IPSec-Verbindungen bietet IPSec eine Verschlüsselung für die Verknüpfung zwischen dem VPN-Client und dem VPN-Server. Wenn zwischen dem VPN-Client und dem VPN-Server eine Datenverschlüsselung durchgeführt wird, müssen Sie die Daten für die Kommunikationsverbindung zwischen einem DFÜ-Client und dessen ISP nicht verschlüsseln. Ein mobiler Benutzer könnte sich z. B. über eine DFÜ-Netzwerkverbindung bei einem lokalen ISP einwählen. Nach Herstellen der Internetverbindung stellt der Benutzer mit dem VPN-Unternehmensserver eine VPN-Verbindung her. Da die VPN-Verbindung verschlüsselt wird, ist für die DFÜ-Netzwerkverbindung zwischen dem Benutzer und dem ISP keine Verschlüsselung erforderlich.

End-to-End-Verschlüsselung

Bei einer End-to-End-Verschlüsselung werden die Daten zwischen dem Quell- und dem Zielhost verschlüsselt. Nach Herstellen einer VPN-Verbindung kann für die End-to-End-Verschlüsselung IPSec verwendet werden.

Die Datenverschlüsselung für PPTP-Verbindungen ist nur verfügbar, wenn MS-CHAP, MS-CHAP v2- oder das EAP-TLS-Protokoll verwendet wird. Die Datenverschlüsselung für L2TP-Verbindungen basiert auf IPSec, so dass kein spezielles Authentifizierungsprotokoll benötigt wird. IPSec erzwingt die Verschlüsselung, und die Verbindung wird verweigert, wenn der Server die Datenverschlüsselung ablehnt.

Ermitteln Sie für jede RAS-Richtlinie, die PPTP- oder L2TP-Verbindungen unterstützt, die unterstützten Verschlüsselungsebenen:

- **Keine Verschlüsselung.** Ermöglicht Verbindungen, die keine Datenverschlüsselung verwenden.
- **Basisverschlüsselung.** Ermöglicht Verbindungen, die für die Datenverschlüsselung IPSec 56-Bit Data Encryption Standard (DES) oder 40-Bit MPPE verwenden.
- **Starke Verschlüsselung.** Ermöglicht Verbindungen, die für die Datenverschlüsselung IPSec 56-Bit DES oder 56-Bit MPPE verwenden.
- **Stärkste Verschlüsselung.** Ermöglicht Verbindungen, die für die Datenverschlüsselung IPSec Triple DES (3DES) oder 128-Bit MPPE verwenden.

Tabelle 6.2 zeigt, welche Authentifizierungsmethoden bestimmte Verschlüsselungsanforderungen unterstützen.

Tabelle 6.2 Verschlüsselungsunterstützung

Anforderung	Authentifizierungsprotokolle	Erzwingen der Verschlüsselung
Sicheres Kennwort ohne Datenverschlüsselung	CHAP, MS-CHAP v1, MS-CHAP v2	Optional (Verbindung auch ohne Verschlüsselung)
Sicheres Kennwort mit MPPE-Datenverschlüsselung	MS-CHAP v1, MS-CHAP v2	Erforderlich (Verbindung trennen, falls Server dies ablehnt)
Smartcard ohne Datenverschlüsselung	EAP-TLS	Optional (Verbindung auch ohne Verschlüsselung)
Smartcard mit Datenverschlüsselung	EAP-TLS	Erforderlich (Verbindung trennen, falls Server dies ablehnt)

Verwenden einer Zertifikatsinfrastruktur

Ob für Ihren RAS-Entwurf eine Zertifikatsinfrastruktur erforderlich ist, hängt von den für Remoteclients eingesetzten Authentifizierungsmethoden ab. Wenn Sie Smartcards oder Benutzerzertifikate mit EAP-TLS-Authentifizierung verwenden, ist eine Zertifikatsinfrastruktur erforderlich. Für L2TP-basierte VPN-Verbindungen ist ein Zertifikat nötig. Für PPTP-basierte VPN-Verbindungen ist eine Zertifikatsinfrastruktur erforderlich, wenn Smartcards oder Benutzerzertifikate sowie eine EAP-TLS-Authentifizierung verwendet werden. Kennwortbasierte Authentifizierungsprotokolle wie z. B. MS-CHAPv2 verwenden für die Authentifizierung keine Zertifikate. Daher ist keine Zertifikatsinfrastruktur erforderlich.

Wenn Sie eine Zertifikatsinfrastruktur für PPTP-basierte VPN-Verbindungen benötigen, müssen Sie auf dem Authentifizierungsserver für den VPN-Server ein Computerzertifikat installieren. Installieren Sie entweder für jede an VPN-Clientbenutzer ausgegebene Smartcard ein Zertifikat oder auf jedem VPN-Client ein Benutzerzertifikat.

Eine Zertifikatsinfrastruktur ist für L2TP-basierte VPN-Verbindungen erforderlich, da Zertifikate für die Aushandlung der Zertifizierung verwendet werden. Eine Zertifikatsinfrastruktur ist auch hier erforderlich, wenn Sie Smartcards oder Benutzerzertifikate und EAP-TLS für die Benutzerauthentifizierung verwenden.

Für L2TP-basierte VPN-Verbindungen müssen Sie auf allen VPN-Clients und dem VPN-Server ein Computerzertifikat installieren.

Weitere Informationen zum Entwerfen und Bereitstellen von IAS finden Sie unter "Deploying IAS" in diesem Buch (englischsprachig). Weitere Informationen zum Entwerfen und Bereitstellen einer PKI finden Sie unter "Designing a Public Key Infrastructure" in *Designing and Deploying Directory and Security Services* dieses Kits (englischsprachig).

Optimieren des RAS-Entwurfs

Sie sollten nicht nur durch Aktualisieren der Serverhardware die Leistung erhöhen, sondern auch die Verfügbarkeit, Sicherheit und Leistung verbessern, indem Sie die folgenden Elemente in Ihren RAS-Entwurf integrieren:

- Redundante Server für eine höhere Verfügbarkeit
- Netzwerklastenausgleich für eine höhere Verfügbarkeit und Leistung
- Kontosperren für eine höhere Sicherheit

Bessere Verfügbarkeit mit redundanten Servern

RAS-Lösungen mit redundanten Servern bieten eine höhere Verfügbarkeit für RAS-Clients. Wenn eine eingeschränkte Verfügbarkeit von Diensten kein wichtiges Problem darstellt, können Sie Ihre primären RAS-Server als Sicherungsserver für die jeweils anderen primären Server verwenden. Wenn eine eingeschränkte Verfügbarkeit verhindert werden soll, sollten Sie zum Schutz vor Ausfällen einen redundanten Server einrichten.

Wenn für eine oder mehrere Benutzergruppen die Möglichkeit des Zugriffs mit hoher Priorität bestehen soll, sollten Sie für diese Benutzergruppen separate RAS-Server verwenden.

Erhöhen der Leistung mit Netzwerklastenausgleich

Mithilfe von Netzwerklastenausgleich, der mit Produkten der Windows Server 2003-Familie zur Verfügung steht, können Sie die Leistung und Verfügbarkeit von VPN-Servern erhöhen. Beim Netzwerklastenausgleich wird der von RAS-VPN-Clients ausgehende Datenverkehr auf mehrere VPN-Server verteilt. Das Netzwerklastenausgleichsfeature bietet auch eine Failover-Funktion für den Fall, dass ein VPN-Server ausfällt.

> **Anmerkung** Wenn ein VPN-Server ausfällt, kann auch auf die von diesem Server verarbeiteten Clientsitzungen nicht mehr zugegriffen werden. Clients werden aufgefordert, sich erneut anzumelden, und die neue Sitzung wird von einem der übrigen Hosts verarbeitet.

Um für VPN-Clients Lastenausgleich zur Verfügung zu stellen, sollten Sie die Standardportregeln verwenden und alle Hosts wie folgt konfigurieren:

- Legen Sie für den Port den Bereich 0–65535 (Standardeinstellung) fest. Der Standardbereich umfasst sämtliche Ports, so dass die Portregel gültig bleibt, auch wenn in den Portnummern, die Sie verwenden möchten, eine Änderung vorgenommen wird.
- Verwenden Sie die Standardeinstellungen für die Filtermethode, die Verteilung von Lastgewicht/gleichen Lasten und die Affinitätsregeln.

Weitere Informationen zur Verwendung von Netzwerklastenausgleich in einem VPN-Szenario finden Sie unter "Deploying Network Load Balancing" in *Planning Server Deployments* dieses Kits (englischsprachig).

Erhöhen der Sicherheit mithilfe mit der Kontosperrfunktion

Um Wörterbuchangriffe auf Remoteserverkonten zu verhindern, können Sie für den Remotezugriff die Kontosperrfunktion verwenden. Denken Sie bei Verwendung dieser Methode daran, dass bei aktivierter Kontosperrung ein unberechtigter Benutzer absichtlich mit mehreren Authentifizierungen für ein Benutzerkonto eine Sperrung des Kontos erzwingen könnte, so dass sich der autorisierte Benutzer nicht mehr anmelden kann.

> **Anmerkung** Die Kontosperrung für den Remotezugriff wird in der Windows Server 2003-Registrierung konfiguriert. Die Remotezugriffs-Kontosperrung ist von Kontosperrrichtlinien für Domänen- oder lokale Benutzerkonten getrennt zu sehen.

Um die Kontosperrung zu aktivieren, müssen Sie den folgenden Registrierungsschlüssel in der Windows Server 2003-Registrierung auf dem Server ändern, der die Remotezugriffsanforderungen authentifiziert:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout
```

Legen Sie den **MaxDenials**-Wert des oben genannten Registrierungsschlüssels auf **1** oder höher fest. **MaxDenials** ist die maximale Anzahl fehlgeschlagener Versuche, bevor das Konto gesperrt wird. **MaxDenials** ist standardmäßig auf **0** festgelegt, und die Kontosperrung ist deaktiviert.

Um den Zeitraum zu ändern, nach dessen Ablauf der Zähler für die fehlgeschlagenen Versuche zurückgesetzt wird, müssen Sie für den **ResetTime (mins)**-Wert des o. a. Registrierungsschlüssels die erforderliche Anzahl an Minuten festlegen. **ResetTime (mins)** ist standardmäßig auf 0xb40 oder 2.880 Minuten (48 Stunden) festgelegt.

Wenn der RAS-Server für die Windows-Authentifizierung konfiguriert wurde, müssen Sie die Registrierung auf dem RAS-Server ändern. Wenn der RAS-Server für die RADIUS-Authentifizierung konfiguriert wurde und Sie IAS verwenden, müssen Sie die Registrierung auf dem IAS-Server ändern.

Um ein gesperrtes Benutzerkonto manuell zurückzusetzen, bevor der Zähler für die fehlgeschlagenen Versuche automatisch zurückgesetzt wird, müssen Sie den o. a. Registrierungsschlüssel löschen.

> **Wichtig** Fehlerhafte Änderungen an den Registrierungseinstellungen können systemweite Fehler verursachen. Dies kann dazu führen, dass Sie das Betriebssystem neu installieren müssen. Erstellen Sie eine Sicherheitskopie der Registrierung, bevor Sie diese ändern. Sie sollten mit dem Verfahren zur Wiederherstellung der Registrierung vertraut sein, falls ein Problem auftritt. Weitere Informationen finden Sie unter "Restore System State Data" im Hilfe- und Supportcenter für Windows Server 2003 (englischsprachig).

Wenn Ihr Unternehmen Smartcards verwendet, steuert der Smartcardhersteller die Kontosperrung für ungültige persönliche Identifikationsnummern (PINs). Für die Wiederherstellung nach einer Kontosperrung aufgrund einer ungültigen PIN muss die Smartcard möglicherweise ersetzt werden.

Weitere Informationen zur Kontosperrung für den Remotezugriff finden Sie unter "Remote Access Server" im *Internetworking Guide* des *Microsoft® Windows® Server 2003 Resource Kits* (englischsprachig).

Testen des RAS-Entwurfs

Wenn Sie den Entwurf der RAS-Lösung abgeschlossen haben, sollten Sie den Entwurf testen. Sie sollten u. a. einzelne VPN-Clientzugriffe auf VPN-Server sowie den gesamten Entwurf für die externe Konnektivität umfassend testen. Wenn Sie mehrere Remotezugriffslösungen integrieren, sollten Sie diese noch einmal zusammen testen, nachdem Sie sie einzeln getestet haben.

Aufgrund der möglichen Sicherheitslücken, die beim Senden von Daten über das Internet bestehen, sollten Sie den Netzwerkperimeter während der Testphase auf jeden Fall vom Intranet trennen. Integrieren Sie Ihren Netzwerkperimeter erst ins Intranet, wenn Sie sicher sind, dass Sie alle Sicherheitsaspekte berücksichtigt haben.

Testen Sie die ISP-Infrastruktur, einschließlich des RADIUS-Proxys (falls vorhanden), sowie eine repräsentative Gruppe von Beispielzugriffspunkten.

Tests sind für die Sicherheit einer externen Konnektivitätslösung von entscheidender Bedeutung. Mithilfe von Tests können Sie sicherstellen, dass die Verbindungen wie geplant funktionieren. Bevor Sie die Tests durchführen, sollten Sie sowohl die internen als auch die externen Verbindungen simulieren, um sicherzustellen, dass keine Teile Ihres Netzwerks angegriffen und beschädigt werden.

Tools zum Testen eines RAS-Entwurfs

Die folgenden Tools sind für das Testen eines RAS-Entwurfs sehr nützlich:

- TCP/IP-Problembehandlungstools, einschließlich Netsh, Ping, Pathping, Route und Tracert
- RAS-Protokollierung Das Protokoll enthält Authentifizierungs- und Kontoinformationen
- Ereignisanzeige
- Netzwerkmonitor
- Ereignisablaufverfolgung für den Remotezugriff (wird über Netsh oder die Registrierung aktiviert).

Bereitstellen einer VPN-RAS-Lösung

Stellen Sie vor Bereitstellen eines RASs sicher, dass Active Directory sowie eine PKI installiert sind. Sie müssen auch bereits einen IAS-Server bereitgestellt haben.

In Abbildung 6.5 wird gezeigt, wie eine RAS-Lösung bereitgestellt wird.

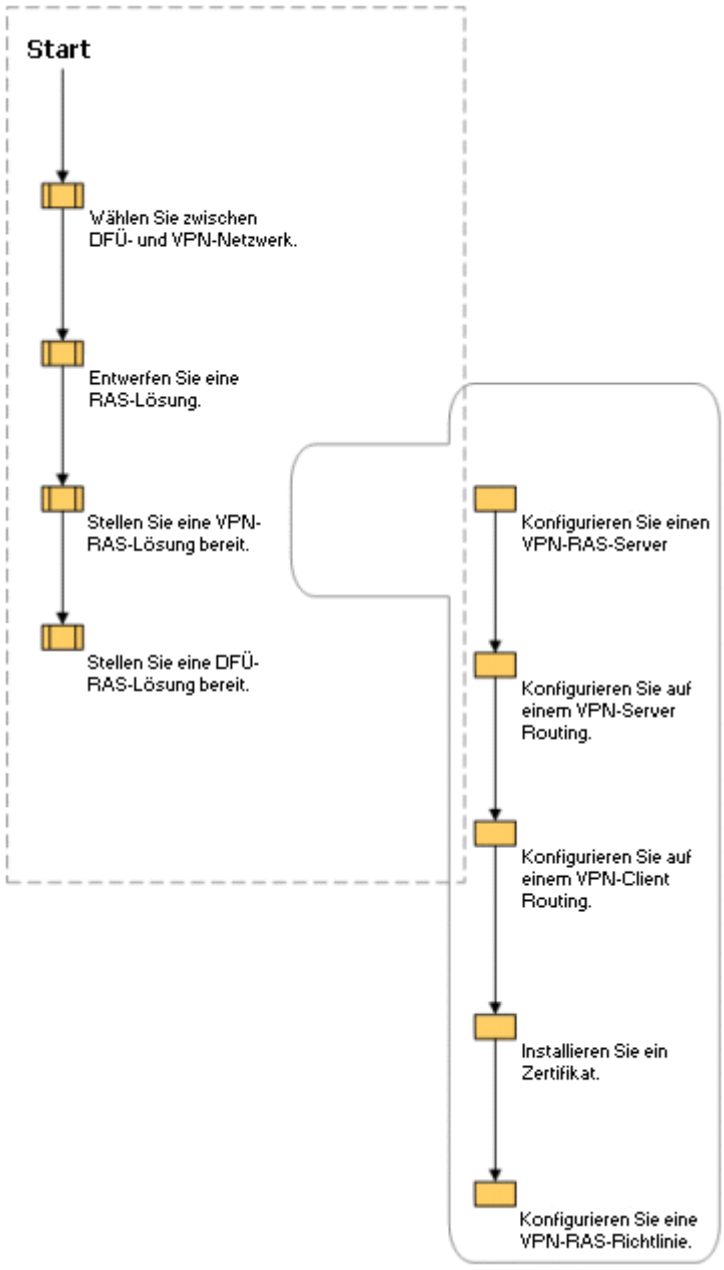

Abbildung 6.5 Bereitstellung einer VPN-RAS-Lösung

Konfigurieren eines VPN-RAS-Servers

Sie können einen Server als VPN-Server konfigurieren, indem Sie den **Setup-Assistenten für den Routing- und RAS-Server** ausführen. Starten Sie den Assistenten wie folgt:

So starten Sie den Setup-Assistenten für den Routing- und RAS-Server

1. Klicken Sie im Startmenü auf **Serververwaltung**.
2. Klicken Sie im Fenster **Serververwaltung** auf **Funktion hinzufügen oder entfernen**, und klicken Sie anschließend im Fenster **Serverkonfigurations-Assistent** auf **Weiter**.
3. Wählen Sie im Fenster **Serverfunktion** die Option **RAS/VPN-Server** aus, und klicken Sie auf **Weiter**.
4. Klicken Sie im Fenster **Zusammenfassung der Auswahl** auf **Weiter**, um den **Setup-Assistent für den Routing- und RAS-Server** auszuführen.

Konfigurieren von TCP/IP auf einem VPN-Server

Aufgrund von Routingproblemen bei der automatischen Konfiguration von TCP/IP sollten Sie einen VPN-Server nicht als DHCP-Client konfigurieren. Sie sollten TCP/IP stattdessen auf den Intranetschnittstellen eines VPN-Servers manuell konfigurieren.

Es ist i. A. einfacher, auf den Namen eines VPN-Servers statt auf seine IP-Adresse zu verweisen, da Namen leichter im Gedächtnis bleiben. Sie können jeden Namen verwenden, der über das Internet in eine IP-Adresse aufgelöst werden kann (z. B. "VPN1.Corporate.Contoso.com"). Wenn Sie eine VPN-Verbindung konfigurieren, müssen Sie Ihren VPN-Servern Namen geben, die mithilfe der Internet-DNS-Infrastruktur in IP-Adressen aufgelöst werden können.

Damit auf einen VPN-Server zugegriffen werden kann, müssen Sie der Internetschnittstelle des VPN-Servers eine öffentliche IP-Adresse von einem ISP oder aus einer Internetregistrierung zuweisen. Bei manchen Konfigurationen wird der VPN-Server mit einer privaten IP-Adresse konfiguriert, und er verfügt über eine statische IP-Adresse, unter der er im Internet bekannt ist. Wenn Pakete auf dem VPN-Server ein- oder ausgehen, übersetzt ein NAT, der sich zwischen dem Internet und dem VPN-Server befindet, die öffentlichen in die privaten IP-Adressen.

- Konfigurieren Sie die Internetschnittstelle des VPN-Servers mit einem Standardgateway. Konfigurieren Sie die Intranetschnittstelle des VPN-Servers nicht mit einem Standardgateway.
- Fügen Sie auf dem VPN-Server statische IP-Routen hinzu, um die im Intranet verwendeten IP-Adressen zusammenzufassen. Wenn Sie als dynamisches Routingprotokoll RIP oder OSPF verwenden, müssen Sie RIP bzw. OSPF auf dem VPN-Server konfigurieren und aktivieren. Wenn Sie ein anderes Routingprotokoll als RIP oder OSPF verwenden, wie z. B. Interior Gateway Routing Protocol (IGRP), müssen Sie auf dem am dichtesten am VPN-Server gelegenen Intranetrouter die Schnittstelle, die mit dem Subnetz verbunden ist, in dem sich der VPN-Server befindet, mit RIP oder OSPF konfigurieren. Konfigurieren Sie alle anderen Schnittstellen des Routers mit IGRP.
- Um den VPN-Server mit einem Subnetzadressbereich zu konfigurieren, müssen Sie den VPN-Server so konfigurieren, dass er über DHCP IP-Adressen erhält. Sie können auch Adresspools manuell konfigurieren.

  Anmerkung Stellen Sie beim Zugriff auf die auf dem VPN-Server ausgeführten Dienste sicher, dass die NetBIOS- und DNS-Namen des VPN-Servers nicht mit der öffentlichen IP-Adresse im Intranet registriert sind.

Konfigurieren der Internet- oder Perimeternetzwerk-Schnittstelle

Konfigurieren Sie das TCP/IP mit einer öffentlichen IP-Adresse, einer Subnetzmaske und der IP-Adresse der Firewall als Standardgateway (wenn der VPN-Server mit einem Perimeternetzwerk verbunden ist) oder eines Routers des ISP (wenn der VPN-Server direkt mit dem Internet verbunden ist).

So verhindern Sie, dass der VPN-Server auf einem Intranet-DNS-Server eine dynamische Registrierung der öffentlichen IP-Adresse der Internetschnittstelle durchführt

1. Zeigen Sie die Eigenschaften der Komponente **Internetprotokoll (TCP/IP)** der Internetverbindung im Ordner **Netzwerkverbindungen** an.
2. Klicken Sie auf **Erweitert**. Klicken Sie im Dialogfeld **Erweiterte TCP/IP-Einstellungen** auf die Registerkarte **DNS**, und deaktivieren Sie dann das Kontrollkästchen **Adressen dieser Verbindung in DNS registrieren**.

So verhindern Sie, dass der VPN-Server auf Intranet-WINS-Servern die öffentliche IP-Adresse der Internetschnittstelle registriert

1. Zeigen Sie die Eigenschaften der Komponente **Internetprotokoll (TCP/IP)** der Internetverbindung im Ordner **Netzwerkverbindungen** an.
2. Klicken Sie auf **Erweitert**. Klicken Sie im Dialogfeld **Erweiterte TCP/IP-Einstellungen** auf die Registerkarte **WINS**, und aktivieren Sie **NetBIOS über TCP/IP deaktivieren**.

Konfigurieren der Intranetschnittstelle

Konfigurieren Sie für die Intranetverbindung auf jedem VPN-Server TCP/IP manuell mit einer IP-Adresse, einer Subnetzmaske, Intranet-DNS-Servern und Intranet-WINS-Servern. Konfigurieren Sie für die Intranetverbindung keinen Standardgateway, um Standardroutenkonflikte mit der Standardroute zu vermeiden, die zum Internet führt.

Konfigurieren der Namensauflösung auf einem VPN-Server

Wenn Sie zum Auflösen von Hostnamen DNS oder zum Auflösen von NetBIOS-Namen Windows Internet Name Service (WINS) verwenden, müssen Sie sicherstellen, dass der VPN-Server mit den IP-Adressen der betreffenden DNS- und WINS-Server konfiguriert ist. Der VPN-Server wird mit DNS- und WINS-Servern manuell konfiguriert. Während der PPP-Aushandlung erhalten die VPN-Clients die IP-Adressen von DNS- und WINS-Servern. Die VPN-Clients erben standardmäßig die auf dem VPN-Server konfigurierten IP-Adressen der DNS- und WINS-Server. VPN-Clients, die eine DHCPINFORM-Nachricht senden können (Windows 2000, Windows XP, Windows Server 2003) erhalten ihre DNS- und WINS-Server-IP-Adressen vom DHCP-Server.

Wenn Sie bei der Clientkonfiguration Ihren VPN-Servern nicht mit IP-Adressen, sondern mit Namen angeben, können Sie die Vorteile des Netzwerklastenausgleichs mithilfe von DNS-Round-Robin nutzen. Innerhalb von DNS können Sie mehrere Einträge vornehmen, die einen bestimmten Namen in unterschiedliche IP-Adressen auflösen. Wenn bei einer DNS-Namensabfrage ein Name mehr als einer IP-Adresse zugeordnet ist, sendet der DNS-Server alle IP-Adressen in zufälliger Reihenfolge zurück. In der Regel verwenden DNS-Clients die erste IP-Adresse in einer DNS-Abfrageantwort. Wenn Sie mehrere VPN-Server mit demselben Namen registrieren, werden auf diese Weise die VPN-Clientverbindungen mit Round Robin auf die VPN-Server verteilt.

Konfigurieren von Paketfiltern für einen VPN-Server vor einer Firewall

Wenn sich ein mit dem Internet verbundener VPN-Server vor einer Firewall befindet, müssen Sie die Eingabe- und Ausgabepaketfilter auf dem VPN-Server so konfigurieren, dass nur VPN-Verkehr zu und von der IP-Adresse der Internetschnittstelle des VPN-Servers zugelassen wird.

Konfigurieren von Paketfiltern für PPTP

Konfigurieren Sie die folgenden Eingabefilter, wobei die Filteraktion auf **Alle Pakete verwerfen, mit Ausnahme derjenigen, die die unten aufgeführten Kriterien erfüllen** festgelegt ist:

- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Zielport 1723. Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr zum VPN-Server zu.
- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-ID 47. Dieser Filter lässt mit PPTP getunnelte Daten zum VPN-Server zu.
- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Quellport [eingerichtet] 1723. Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. TCP-Verkehr wird nur dann akzeptiert, wenn der VPN-Server die TCP-Verbindung initiiert.

Konfigurieren Sie die folgenden Ausgabefilter, wobei die Filteraktion auf **Alle Pakete verwerfen, mit Ausnahme derjenigen, die die unten aufgeführten Kriterien erfüllen** festgelegt ist:

- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Quellport 1723. Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom VPN-Server zu.
- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokoll-ID 47. Dieser Filter lässt mit PPTP getunnelte Daten vom VPN-Server zu.
- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Zielport [eingerichtet] 1723. Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. TCP-Verkehr wird nur dann gesendet, wenn der VPN-Server die TCP-Verbindung initiiert.

Konfigurieren von Paketfiltern für L2TP/IPSec

Konfigurieren Sie die folgenden Eingabefilter, wobei die Filteraktion auf **Alle Pakete verwerfen, mit Ausnahme derjenigen, die die unten aufgeführten Kriterien erfüllen** festgelegt ist:

- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 500. Dieser Filter lässt IKE-Verkehr (Internet Key Exchange) zum VPN-Server zu.
- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 1701. Dieser Filter lässt L2TP-Verkehr vom VPN-Server zum VPN-Client zu.
- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 4500. Dieser Filter lässt NAT-T-Verkehr vom VPN-Client zum VPN-Server zu.

Konfigurieren Sie die folgenden Ausgabefilter, wobei die Filteraktion auf **Alle Pakete verwerfen, mit Ausnahme derjenigen, die die unten aufgeführten Kriterien erfüllen** festgelegt ist:

- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 500. Dieser Filter lässt IKE-Verkehr vom VPN-Server zu.
- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 1701. Dieser Filter lässt L2TP-Verkehr vom VPN-Server zum VPN-Client zu.
- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 4500. Dieser Filter aktiviert NAT-T.
- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 4500. Dieser Filter lässt IPSec NAT-T-Verkehr vom VPN-Server zum VPN-Client zu.

Konfigurieren von Paketfiltern für einen VPN-Server hinter einer Firewall

Bei dieser Konfiguration ist die Firewall mit dem Internet verbunden, und der VPN-Server ist eine mit dem Perimeternetzwerk verbundene Intranetressource. Der VPN-Server hat eine Schnittstelle im Perimeternetzwerk und im Intranet.

Konfigurieren von PPTP-Filtern auf der Intranetschnittstelle

Konfigurieren Sie die folgenden Eingabepaketfilter auf der Internetschnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB). Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom PPTP-Client zum PPTP-Server zu.
- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F). Dieser Filter lässt mit PPTP getunnelte Daten vom PPTP-Client zum PPTP-Server zu.
- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB). Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wird der gesamte Datenverkehr vom TCP-Port 1723 an den VPN-Server zugelassen, besteht die Gefahr von Netzwerkangriffen von Quellen im Internet, die diesen Port verwenden.

Konfigurieren Sie die folgenden Ausgabefilter auf der Internetschnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB). Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom VPN-Server zum VPN-Client zu.
- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F). Dieser Filter lässt mit PPTP getunnelte Daten vom VPN-Server zum VPN-Client zu.
- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB). Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wird der gesamte Datenverkehr vom VPN-Server an den TCP-Port 1723 zugelassen, besteht die Gefahr von Netzwerkangriffen von Quellen im Internet, die diesen Port verwenden.

Konfigurieren von PPTP-Filtern auf der Perimeternetzwerk-Schnittstelle

Konfigurieren Sie die folgenden Eingabefilter auf der Perimeternetzwerk-Schnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB). Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom VPN-Server zum VPN-Client zu.
- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F). Dieser Filter lässt mit PPTP getunnelte Daten vom VPN-Server zum VPN-Client zu.
- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB). Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wird der gesamte Datenverkehr vom VPN-Server an den TCP-Port 1723 zugelassen, besteht die Gefahr von Netzwerkangriffen von Quellen im Internet, die diesen Port verwenden.

Konfigurieren Sie die folgenden Ausgabefilter auf der Perimeternetzwerk-Schnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Zielport 1723 (0x6BB). Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr zum VPN-Server zu.
- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 47 (0x2F). Dieser Filter lässt mit PPTP getunnelte Daten zum VPN-Server zu.
- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und TCP-Quellport 1723 (0x6BB). Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wird der gesamte Datenverkehr vom TCP-Port 1723 zum VPN-Server zugelassen, besteht die Gefahr von Netzwerkangriffen von Quellen im Internet, die diesen Port verwenden.

Konfigurieren von L2TP/IPSec-Filtern auf der Intranetschnittstelle

Konfigurieren Sie die folgenden Eingabefilter auf der Internetschnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und UDP-Zielport 500 (0x1F4). Dieser Filter lässt IKE-Verkehr zum VPN-Server zu.
- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32). Dieser Filter lässt IPSec ESP-Verkehr zum VPN-Server zu.

Konfigurieren Sie die folgenden Ausgabefilter auf der Internetschnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und UDP-Quellport 500 (0x1F4). Dieser Filter lässt IKE-Verkehr vom VPN-Server zu.
- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32). Dieser Filter lässt IPSec ESP-Verkehr vom VPN-Server zu. Für L2TP-Verkehr am UDP-Port 1701 sind keine Filter erforderlich. An der Firewall wird der gesamte L2TP-Verkehr einschließlich der Tunnelverwaltung und der getunnelten Daten als IPSec ESP-Nutzlast verschlüsselt.

Konfigurieren von L2TP/IPSec-Filtern auf der Perimeterschnittstelle

Konfigurieren Sie die folgenden Eingabepaketfilter auf der Perimeternetzwerk-Schnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und UDP-Quellport 500 (0x1F4). Dieser Filter lässt IKE-Verkehr vom VPN-Server zu.
- Quell-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32). Dieser Filter lässt IPSec ESP-Verkehr vom VPN-Server zu.

Konfigurieren Sie die folgenden Ausgabepaketfilter auf der Perimeternetzwerk-Schnittstelle der Firewall, um die folgenden Arten von Datenverkehr zuzulassen:

- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und UDP-Zielport 500 (0x1F4). Dieser Filter lässt IKE-Verkehr zum VPN-Server zu.
- Ziel-IP-Adresse der Perimeternetzwerk-Schnittstelle des VPN-Servers und IP-Protokoll-ID 50 (0x32). Dieser Filter lässt IPSec ESP-Verkehr zum VPN-Server zu. Für L2TP-Verkehr am UDP-Port 1701 sind keine Filter erforderlich. An der Firewall wird der gesamte L2TP-Verkehr einschließlich der Tunnelverwaltung und der getunnelten Daten als IPSec ESP-Nutzlast verschlüsselt.

Konfigurieren von Routing auf einem VPN-Server

Damit ein VPN-Server Datenverkehr ordnungsgemäß an die jeweiligen Speicherorte im Intranet weiterleitet, muss er wie folgt konfiguriert werden:

- Statische Routen, die alle möglichen IP-Adressen im Intranet zusammenfassen.

  Oder

- Routingprotokolle, mit denen der VPN-Server als dynamischer Router fungieren und den Routingtabellen automatisch Routen für Intranetsubnetze hinzufügen kann.

Wenn Sie IP-Adresspools auf einem Ihrer VPN-Server manuell konfigurieren und einer der Pools ein subnetzexterner Pool ist, muss Ihre Intranetroutinginfrastruktur Routen enthalten, die die subnetzexternen Adresspools abbilden. Fügen Sie hierfür den Routern neben den VPN-Servern statische Routen hinzu, die subnetzexterne Adresspools abbilden. Verwenden Sie dann das Routingprotokoll des Intranets, um die subnetzexternen Routen an andere Router weiterzugeben. Wenn Sie statische Routen hinzufügen, müssen Sie angeben, dass es sich beim Gateway oder der nächsten Abschnittsadresse um die Intranetschnittstelle des VPN-Servers handelt.

Wenn Sie RIP oder OSPF verwenden, können Sie auch einen VPN-Server, der subnetzexterne Adresspools verwendet, als RIP- oder OSPF-Router konfigurieren. Für OSPF müssen Sie den VPN-Server als autonomen Systemgrenzrouter (Autonomous System Boundary Router oder ASBR) konfigurieren. Weitere Informationen finden Sie unter "OSPF Design Considerations" im Hilfe- und Supportcenter für Windows Server 2003 (englischsprachig).

Weitere Informationen zum Hinzufügen von statischen Routen finden Sie unter "Add a Static Route" im Hilfe- und Supportcenter für Windows Server 2003. Informationen zum Konfigurieren des VPN-Servers als RIP-Router finden Sie unter "Configure RIP for IP" im Hilfe- und Supportcenter für Windows Server 2003. Informationen zum Konfigurieren des VPN-Servers als OSPF-Router finden Sie unter "OSPF Design Considerations" und "Configure OSPF" im Hilfe- und Supportcenter für Windows Server 2003 (alle englischsprachig).

Konfigurieren von Routing auf einem VPN-Client

Wenn ein Windows-basierter VPN-Client eine VPN-Verbindung herstellt, fügt der VPN-Client standardmäßig automatisch eine neue Standardroute für die VPN-Verbindung hinzu und legt einen höheren metrischen Wert für die vorhandene Standardroute fest. Da eine neue Standardroute hinzugefügt wird, sind während der Dauer der VPN-Verbindung keine Internetstandorte erreichbar, mit Ausnahme der IP-Adresse des Tunnelservers.

So verhindern Sie, dass der VPN-Client während der Dauer einer VPN-Verbindung eine neue Standardroute erstellt

1. Zeigen Sie die Eigenschaften der Komponente **Internetprotokoll (TCP/IP)** der VPN-Verbindung im Ordner **Netzwerkverbindungen** an.
2. Klicken Sie auf **Erweitert**. Klicken Sie im Dialogfeld **Erweiterte TCP/IP-Einstellungen** auf die Registerkarte **Allgemein**, und deaktivieren Sie dann das Kontrollkästchen **Standardgateway für das Remotenetzwerk verwenden**.

Ist diese Einstellung deaktiviert, wird keine Standardroute erstellt. Es wird jedoch eine Route erstellt, die der Internetadressklasse der zugewiesenen IP-Adresse entspricht. Wenn die während des Verbindungsaufbaus zugewiesene IP-Adresse z. B. 10.0.12.119 lautet, erstellt der Windows Server 2003-basierte oder Windows XP-basierte VPN-Client eine Route für die klassenbasierte Netzwerk-ID 10.0.0.0 mit der Subnetzmaske 255.0.0.0.

Basierend auf der Einstellung **Standardgateway für das Remotenetzwerk verwenden** hat der Client einen umfassenden Zugriff entweder auf Internetadressen oder auf Adressen im Intranet, jedoch nicht beides:

- Wird der Standardgateway im Remotenetzwerk nicht verwendet, sind Standorte im Internet erreichbar. Es kann dagegen nur auf Intranetstandorte zugegriffen werden, die der Adressklasse der zugewiesenen IP-Adresse entsprechen.
- Wird der Standardgateway im Remotenetzwerk verwendet, sind alle Intranetstandorte erreichbar. Im Internet kann dagegen nur auf die IP-Adresse des VPN-Servers sowie auf die über andere Routen verfügbaren Standorte zugegriffen werden.

Für die meisten VPN-Clients mit einer Internetverbindung stellt dies kein Problem dar, da der Client normalerweise entweder mit einer Intranet- oder mit einer Internetverbindung beschäftigt ist, nicht mit beidem.

Für VPN-Clients, die über eine VPN-Verbindung gleichzeitig auf Intranet- und auf Internetressourcen zugreifen müssen, stehen drei Konfigurationsoptionen zur Verfügung:

- Aktivieren Sie das Kontrollkästchen **Standardgateway für das Remotenetzwerk verwenden** (Standardeinstellung), und ermöglichen Sie den Internetzugriff über das Unternehmensintranet.

  Internetverkehr zwischen dem VPN-Client und Internethosts durchquert Firewalls oder Proxyserver, so als wäre der VPN-Client mit dem Unternehmensintranet physisch verbunden. Diese Methode kann sich zwar auf die Leistung auswirken, sie bietet einem Unternehmen jedoch die Möglichkeit, den Internetzugriff auf seine Netzwerkrichtlinien zu filtern und zu überwachen, während der VPN-Client mit dem Unternehmensnetzwerk verbunden ist.

- Wenn die Adressierung im Intranet auf einer einzelnen klassenbasierten Netzwerk-ID basiert, sollten Sie das Kontrollkästchen **Standardgateway für das Remotenetzwerk verwenden** deaktivieren. Das beste Beispiel hierfür ist die Verwendung des privaten IP-Adressbereichs 10.0.0.0/8 durch das Intranet.
- Wenn die Adressierung im Intranet nicht auf einer einzelnen klassenbasierten Netzwerk-ID basiert, sollten Sie das Kontrollkästchen **Standardgateway für das Remotenetzwerk verwenden** ebenfalls deaktivieren. Wenden Sie anschließend die weiter oben in diesem Kapitel beschriebenen Split Tunneling-Methoden an.

Installieren eines Zertifikats

Wenn ein VPN-Client L2TP/IPSec-Verbindungen herstellt, muss im lokalen Zertifikatsspeicher des Clients ein Computerzertifikat installiert werden. Das Zertifikat ermöglicht eine Authentifizierung für das Einrichten einer IPSec-Sicherheitszuordnung (Security Association oder SA). Für eine Authentifizierung auf Benutzerebene mit dem EAP-TLS-Protokoll (Extensible Authentication Protocol-Transport Layer Security) ist entweder ein Benutzerzertifikat oder eine Smartcard erforderlich. Um ein Zertifikat installieren zu können, muss eine Zertifizierungsstelle vorhanden und erreichbar sein. Sie können durch eine automatische Registrierung ein Zertifikat auf einem Computer in einer Windows .NET-Domäne installieren oder das Snap-In **Zertifikate** verwenden. Außerdem besteht die Möglichkeit, mit einem Webbrowser eine Verbindung zwischen dem VPN-Client und dem CA-Webregistrierungstool herzustellen, um ein Zertifikat zu installieren. Gehen Sie bei dieser Methode wie folgt vor:

So verwenden Sie das CA-Webregistrierungstool, um auf einem VPN-Client ein Zertifikat zu installieren

1. Stellen Sie mit einem Webbrowser eine Verbindung zwischen dem VPN-Client und dem CA-Webregistrierungstool unter **http://***ServerName***/certsrv** her, wobei *ServerName* für den Namen des Servers steht, auf dem die Zertifizierungsstelle installiert ist. Klicken Sie auf **Zertifikat anfordern**.
2. Klicken Sie auf **Erweiterte Zertifikatanforderung**, und klicken Sie dann auf **Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen**, um ein Webformular anzuzeigen. Geben Sie im Webformular die erforderlichen Informationen ein, und klicken Sie dann auf die entsprechende Schaltfläche zum Übermitteln der Daten.
3. Klicken Sie auf **Dieses Zertifikat installieren**.

Konfigurieren einer VPN-RAS-Richtlinie

Eine RAS-Richtlinie erzwingt die Autorisierung einer VPN-Verbindung sowie Verbindungseinschränkungen, die auf zahlreichen Kriterien basieren, wie z. B. dem Vergleich eines oder mehrerer erforderlicher Attribute mit den Einstellungen eines Verbindungsversuchs.

Weitere Informationen zur Verwendung von Windows .NET-RAS-Richtlinien finden Sie unter "Remote access policies" im Hilfe- und Supportcenter für Windows Server"2003 (englischsprachig).

Verschlüsselungseinstellungen

Treffen Sie unter den folgenden Verschlüsselungseinstellungen eine Auswahl, um die Verschlüsselungsstufe zu aktivieren, die für Ihre Umgebung am besten geeignet ist:

Basisverschlüsselung

Microsoft Punkt-zu-Punkt-Verschlüsselung mit einer 40-Bit-Schlüsselverschlüsselung wird für PPTP-VPN-Verbindungen verwendet. 56-Bit-DES-Verschlüsselung (Data Encryption Standard) wird für L2TP/IPSec-VPN-Verbindungen verwendet.

Starke Verschlüsselung

MPPE mit einem 56-Bit-Schlüssel wird für PPTP-VPN-Verbindungen verwendet. Für L2TP/IPSec-VPN-Verbindungen wird eine 56-Bit-DES-Verschlüsselung verwendet.

Stärkste Verschlüsselung

MPPE mit einem 128-Bit-Schlüssel wird für PPTP-VPN-Verbindungen verwendet. Für L2TP/IPSec-VPN-Verbindungen wird eine 3DES-Verschlüsselung (Triple DES) verwendet.

Ausführliche Informationen zu Verschlüsselungseinstellungen finden Sie unter "Elements of a remote access policy" im Hilfe- und Supportcenter für Windows Server 2003 (englischsprachig).

Bereitstellen eines DFÜ-RAS-Servers

Ein DFÜ-RAS-Server muss über ein Modem oder einen Mehrfachanschlussadapter verfügen. Darüber hinaus muss ein DFÜ-RAS-Server auf einen analogen Telefonanschluss zugreifen können. Wenn ein DFÜ-RAS-Server den Zugriff auf ein Netzwerk ermöglicht, muss der Server einen Netzwerkadapter und eine Verbindung mit dem Netzwerk aufweisen.

In Abbildung 6.6 wird gezeigt, wie eine DFÜ-RAS-Lösung bereitgestellt wird.

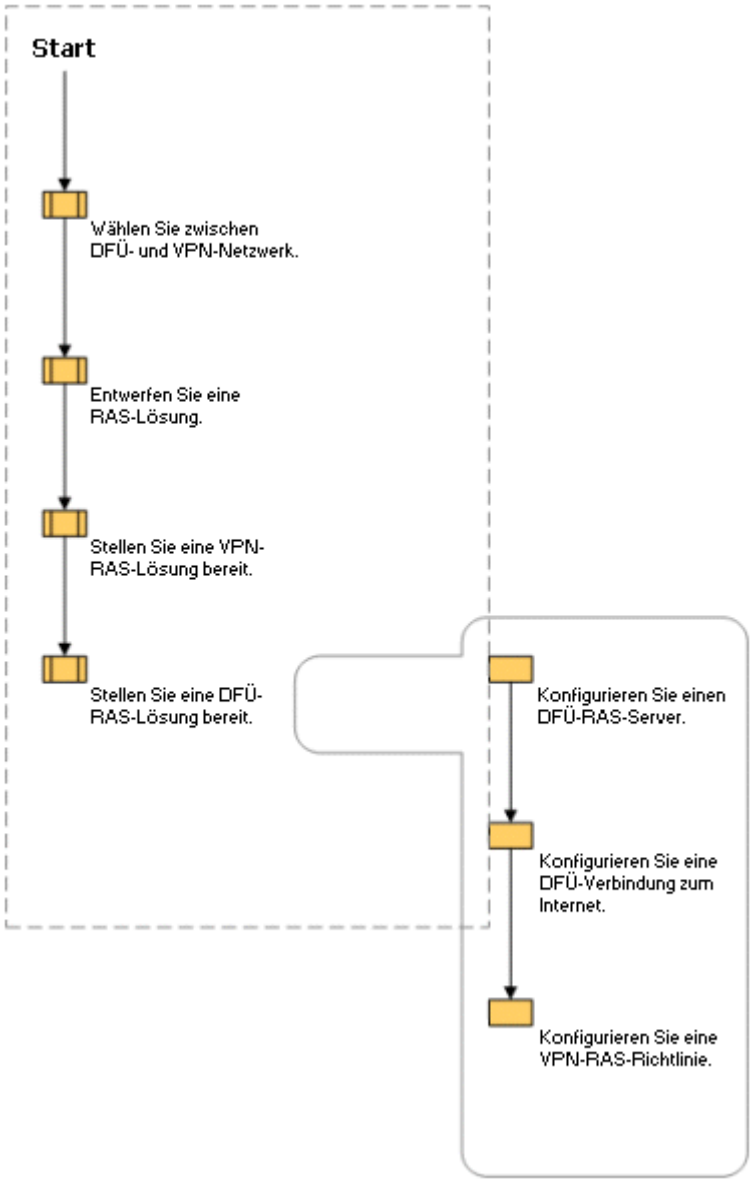

Abbildung 6.6 Bereitstellen einer DFÜ-RAS-Lösung

Konfigurieren eines DFÜ-RAS-Servers

Sie können einen Computer unter Windows Server 2003 als DFÜ-RAS-Server konfigurieren, um einen DFÜ-Zugriff auf das Unternehmensintranet zu ermöglichen.

Konfigurieren eines Windows Server 2003 als DFÜ-RAS-Server

Sie können einen Server als DFÜ-RAS-Server konfigurieren, indem Sie den **Setup-Assistenten für den Routing- und RAS-Server** ausführen. Starten Sie den Assistenten wie folgt:

So starten Sie den Setup-Assistenten für den Routing- und RAS-Server

1. Klicken Sie im Startmenü auf **Serververwaltung**.
2. Klicken Sie im Fenster **Serververwaltung** auf **Funktion hinzufügen oder entfernen**, und klicken Sie anschließend im Fenster **Serverkonfigurations-Assistent** auf **Weiter**.
3. Wählen Sie im Fenster **Serverfunktion** die Option **RAS/VPN-Server** aus, und klicken Sie auf **Weiter**.
4. Klicken Sie im Fenster **Zusammenfassung der Auswahl** auf **Weiter**, um den **Setup-Assistent für den Routing- und RAS-Server** auszuführen.

Konfigurieren Sie die Eigenschaften eines DFÜ-RAS-Servers, indem Sie im Snap-In Routing und RAS mit der rechten Maustaste auf den Server klicken und die Option **Eigenschaften** auswählen. Konfigurieren Sie die folgenden Einstellungen, um mehreren DFÜ-Netzwerkclients den Zugriff auf das Unternehmensintranet zu ermöglichen:

- Stellen Sie sicher, dass auf der Registerkarte **Allgemein** das Kontrollkästchen **RAS-Server** aktiviert ist.
- Klicken Sie auf der Registerkarte **Sicherheit** auf **Authentifizierungsmethoden**. Im Dialogfeld **Authentifizierungsmethoden** wird der Server standardmäßig so konfiguriert, dass er bestimmte Authentifizierungsmethoden akzeptiert. Mithilfe von RAS-Richtlinien können Sie steuern, welche Authentifizierungsmethoden akzeptiert werden sollen.
- Wählen Sie unter **Authentifizierungsanbieter** auf der Registerkarte **Sicherheit** eine Methode zur Überprüfung von Anmeldeinformationen für DFÜ-Netzwerkclients aus, und konfigurieren Sie sie.
- Wählen Sie unter **Kontoanbieter** auf der Registerkarte **Sicherheit** den Kontoanbieter für die Aufzeichnung von DFÜ-Clientnetzwerkaktivitäten aus, und konfigurieren Sie ihn.
- Stellen Sie sicher, dass auf der Registerkarte **IP** die Kontrollkästchen **IP-Routing aktivieren** und **IP-basierte RAS- und Verbindungen für Wählen bei Bedarf zulassen** aktiviert sind. Wenn Sie mit einem DHCP-Server IP-Adressen für RAS-Clients zuweisen, klicken Sie auf **DHCP (Dynamic Host Configuration-Protokoll)**. Klicken Sie andernfalls auf **Statischen Adresspool**, und konfigurieren Sie IP-Adressbereiche, die DFÜ-Netzwerkclients dynamisch zugewiesen werden. Wenn der statische IP-Adresspool aus IP-Adressbereichen für ein separates Subnetz besteht, müssen Sie entweder auf dem RAS-Computer ein IP-Routingprokoll aktivieren oder allen Routern in dem separaten Intranet für jeden Bereich statische IP-Routen hinzufügen. Werden die Routen nicht hinzugefügt, können RAS-Clients von Ressourcen im Intranet keinen Datenverkehr empfangen.

Konfigurieren einer DFÜ-Verbindung mit dem Intranet

Ein LAN-Adapter ermöglicht die Verbindung eines DFÜ-RAS-Servers mit dem Intranet. Konfigurieren Sie die folgenden TCP/IP-Einstellungen auf dem LAN-Adapter:

- Die von einem Netzwerkadministrator zugewiesene IP-Adresse und Subnetzmaske.
- Den Standardgateway eines lokalen Routers.
- Die IP-Adressen des DNS- und des WINS-Servers.

Konfigurieren einer Verbindung mit DFÜ-Netzwerkclients

Um die gleichzeitige Verbindung mehrerer DFÜ-Clients zu ermöglichen, benötigen Sie eine mit einem Telekommunikationsanbieter verbundene Modembank. Der Modembankadapter umfasst Treiber, die auf dem DFÜ-RAS-Server installiert sind. Mithilfe der Treiber des Modembankadapters kann die Modembank als Gerät mit mehreren Modemanschlüssen fungieren.

Konfigurieren von Einwahlanschlüssen

Alle Modembankanschlüsse sind in Routing und RAS unter **Anschlüsse** separat aufgelistet. Konfigurieren Sie alle aktiven Modembankanschlüsse für RAS.

Konfigurieren einer DFÜ-RAS-Richtlinie

Eine RAS-Richtlinie erzwingt die Autorisierung einer DFÜ-Verbindung sowie Verbindungseinschränkungen, die auf zahlreichen Kriterien basieren, wie z. B. dem Vergleich eines oder mehrerer erforderlicher Attribute mit den Einstellungen eines Verbindungsversuchs.

Weitere Informationen zur Verwendung von Windows .NET-RAS-Richtlinien finden Sie unter "Remote access policies" im Hilfe- und Supportcenter für Windows Server 2003 (englischsprachig).

Verschlüsselungseinstellungen

Wählen Sie unter den folgenden Verschlüsselungseinstellungen aus, um die Verschlüsselungsstufe zu aktivieren, die für Ihre Umgebung am besten geeignet ist.

- **Basisverschlüsselung** unter Verwendung von MPPE mit einem 40-Bit-Schlüssel.
- **Starke Verschlüsselung** unter Verwendung von MPPE mit einem 56-Bit-Schlüssel.
- **Stärkste Verschlüsselung** unter Verwendung von MPPE mit einem 128-Bit-Schlüssel.

Ausführliche Informationen zu Verschlüsselungseinstellungen finden Sie unter "Elements of a remote access policy" im Hilfe- und Supportcenter für Windows Server 2003 (englischsprachig).

Weitere Ressourcen

Diese Ressourcen bieten zusätzliche Informationen und Tools, die mit diesem Kapitel zusammenhängen.

Verwandte Informationen in den Resource Kits

- Weitere Informationen zum Entwerfen und Bereitstellen einer PKI finden Sie unter "Designing a Public Key Infrastructure" in *Designing and Deploying Directory and Security Services* dieses Kits (englischsprachig).
- Weitere Informationen zum Bereitstellen von Smartcards finden Sie unter "Deploying Smart Cards" in *Designing and Deploying Directory and Security Services* dieses Kits (englischsprachig).
- Weitere Informationen zum Entwerfen und Bereitstellen von IAS finden Sie unter "Deploying IAS" in diesem Buch (englischsprachig).
- Weitere Informationen zur EAP-TLS-Authentifizierung finden Sie unter "Connecting Remote Sites" in diesem Buch (englischsprachig).
- Weitere Informationen zur Verwendung des Verbindungs-Managers zum Bereitstellen von RAS-Clients finden Sie unter "Deploying Remote Access Clients Using Connection Manager" in diesem Buch (englischsprachig).

Beta-Disclaimer

Vielen Dank für Ihr Interesse an der Whistler Server Resource Kit-Dokumentation. Ihr Feedback können Sie über das Konto **microsoft.betanews** in der **microsoft.beta.whistler.documentation**-Newsgroup abgeben. Führen Sie hierfür die folgenden Schritte durch:

1. Schreiben Sie einen neuen Newsgroupbeitrag.
2. Tragen Sie in die Betreffzeile Ihrer Nachricht den Titel des Kapitels ein.
3. Fügen Sie in das Nachrichtenfeld Ihre Kommentare ein, und geben Sie die jeweilige Seitenzahl sowie Textänderungen an.

Sie können auch das Kapitel mit Ihren Kommentaren an docbeta@microsoft.com schicken.