Kapitel 9 - Virtual Private Networking (VPN)

(Engl. Originaltitel: Chapter 9 - Virtual Private Networking)

Microsoft® Windows® 2000 umfasst eine umfangreiche Unterstützung für die Virtual Private Networking-Technologie, die die IP-Konnektivität des Internets einsetzt, um Remoteclients und Remoteniederlassungen zu verbinden. Wenn Sie zum Netzwerkfachpersonal gehören, sollten Sie die wichtigen Verwendungen von Virtual Private Networking für Ihre Organisation und die seiner Funktionsweise zugrunde liegenden Technologien verstehen: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), virtuelle private Netzwerke und Sicherheit, virtuelle private Netzwerke und Routing und Übersetzung, virtuelle private Netzwerke und Firewalls sowie die Problembehandlung bei Virtual Private Network-Verbindungen. Sie sollten mit TCP/IP, IP-Routing, IP Security (IPSec) und dem RAS-Server von Windows 2000 vertraut sein.

Inhalt dieses Kapitels

Verwandte Informationen im Resource Kit

- Weitere Informationen zu TCP/IP finden Sie unter "Introduction to TCP/IP" im *Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide* (englischsprachig).
- Weitere Informationen zu IPSec finden Sie unter "Internet Protocol Security" im *TCP/IP Core Networking Guide* (englischsprachig).
- Weitere Informationen zu IP-Unicast-Routing finden Sie in diesem Buch unter "Unicast IP Routing" (englischsprachig).
- Weitere Informationen zu Routing für Wählen bei Bedarf finden Sie in diesem Buch unter "Demand-Dial Routing" (englischsprachig).
- Weitere Informationen zum RAS-Server von Windows 2000 finden Sie in diesem Buch unter "Remote Access Server" (englischsprachig).

Übersicht über Virtual Private Networking

Ein virtuelles privates Netzwerk (VPN) ist die Erweiterung eines privaten Netzwerkes, zu der Verbindungen über freigegebene oder öffentliche Netzwerke wie das Internet gehören. Mit einem VPN können Sie Daten zwischen zwei Computern über ein freigegebenes oder öffentliches Netzwerk senden. Dabei werden die Eigenschaften einer privaten Punkt-zu-Punkt-Verbindung emuliert. Das Konfigurieren und Erstellen eines virtuellen privaten Netzwerkes wird Virtual Private Networking genannt.

Um eine Punkt-zu-Punkt-Verbindung zu emulieren, werden Daten eingekapselt (eingepackt) und mit einem Header versehen, der Routinginformationen enthält, die es den Daten ermöglichen, auf dem Weg zu ihrem Endpunkt das freigegebene oder öffentliche Netzwerk zu durchqueren. Um eine private Verbindung zu emulieren, werden die gesendeten Daten aus Gründen der Vertraulichkeit verschlüsselt. Pakete, die im freigegebenen oder öffentlichen Netzwerk abgefangen werden, können ohne die Verschlüsselungsschlüssel nicht entschlüsselt werden. Die Verbindung, in der die privaten Daten eingekapselt und verschlüsselt sind, wird VPN-Verbindung genannt.

Abbildung 9.1 illustriert das logische Konzept eines VPNs.

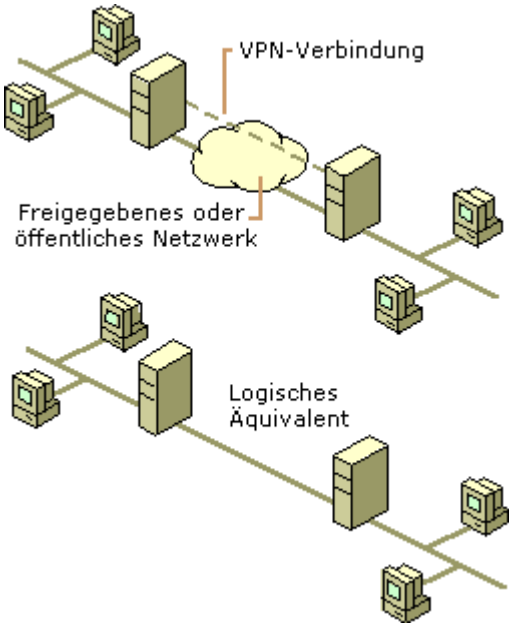

Abbildung 9.1 - Virtual Private Networking (VPN)

Mit VPN-Verbindungen können Benutzer, die zu Hause oder unterwegs arbeiten, mithilfe der von einem öffentlichen Netzwerk, wie beispielsweise dem Internet, bereitgestellten Infrastruktur eine RAS-Verbindung zu einem Organisationsserver aufbauen. Aus Sicht des Benutzers ist das VPN eine Punkt-zu-Punkt-Verbindung zwischen dem Computer, dem VPN-Client und einem Organisationsserver, dem VPN-Server. Die genaue Infrastruktur des freigegebenen oder öffentlichen Netzwerkes ist nicht von Bedeutung, da sie logisch so erscheint, als würden die Daten über eine dedizierte private Verbindung gesendet.

Mit VPN-Verbindungen können Organisationen außerdem umgeleitete Verbindungen zu geografisch separaten Zweigstellen oder zu anderen Organisationen über ein öffentliches Netzwerk, wie beispielsweise das Internet, verwenden und dabei sichere Kommunikation aufrechterhalten. Eine umgeleitete VPN-Verbindung über das Internet funktioniert logisch wie eine dedizierte WAN-Verbindung.

Durch die RAS-Verbindung und die umgeleitete Verbindung ermöglichen VPN-Verbindungen einer Organisation, Fernwählverbindungsleitungen oder Mietleitungen durch örtliche Wählverbindungsleistungen oder Mietleitungen zu einem Internetdienstanbieter (Internet Service Provider, ISP) zu ersetzen.

Elemente einer VPN-Verbindung

Eine VPN-Verbindung unter Microsoft® Windows® 2000 umfasst folgende Komponenten (siehe Abbildung 9.2):

VPN-Server. Ein Computer, der VPN-Verbindungen von VPN-Clients akzeptiert. Ein VPN-Server kann eine RAS-VPN-Verbindung oder eine Router-zu-Router-VPN-Verbindung bereitstellen. Weitere Informationen finden Sie weiter unten in diesem Kapitel unter "VPN-Verbindungen".

VPN-Client. Ein Computer, der eine VPN-Verbindung zu einem VPN-Server initiiert. Ein VPN-Client kann ein einzelner Computer sein, der eine RAS-VPN-Verbindung oder einen Router erhält, der eine Router-zu-Router-VPN-Verbindung erhält. Microsoft® Windows NT®, Version 4.0, Windows 2000, Microsoft® Windows® 95 und Microsoft® Windows® 98-basierte Computer können RAS-VPN-Verbindungen zu einem Windows 2000-basierten VPN-Server erstellen. Microsoft® Windows® 2000 Server und Microsoft® Windows NT® Server 4.0-basierte Computer, die den Routing- und RAS-Dienst (Routing and Remote Access Service, RRAS) ausführen, können Router-zu-Router-VPN-Verbindungen zu einem Windows 2000-basierten VPN-Server erstellen. Als VPN-Clients können auch alle nicht von Microsoft stammenden PPTP-Clients (Point-to-Point Tunneling Protocol) oder L2TP-Clients (Layer 2 Tunneling Protocol) fungieren, die IPSec verwenden.

Tunnel. Der Teil der Verbindung, in dem Ihre Daten eingekapselt werden.

VPN-Verbindung. Der Teil der Verbindung, in dem Ihre Daten verschlüsselt werden. Bei sicheren VPN-Verbindungen werden die Daten im selben Teil der Verbindung verschlüsselt und eingekapselt.

Anmerkung Es ist möglich, einen Tunnel zu erstellen und die Daten ohne Verschlüsselung durch den Tunnel zu senden. Dabei handelt es sich nicht um eine VPN-Verbindung, da die privaten Daten unverschlüsselt und problemlos lesbar über ein freigegebenes oder öffentliches Netzwerk gesendet werden.

Tunnelprotokolle. Kommunikationsstandards, die für das Verwalten von Tunnels und das Einkapseln von privaten Daten verwendet werden. (Getunnelte Daten müssen außerdem verschlüsselt werden, um eine VPN-Verbindung darzustellen.) Windows 2000 umfasst die PPTP- und L2TP-Tunnelprotokolle. Ausführliche Informationen zu diesen Protokollen finden Sie weiter unten in diesem Kapitel unter "Point-to-Point Tunneling Protocol" und "Layer 2 Tunneling Protocol und Internetprotokollsicherheit".

Getunnelte Daten. Daten, die normalerweise über eine private Punkt-zu-Punkt-Verbindung gesendet werden.

Transitnetzwerk. Das freigegebene oder öffentliche Netzwerk, das die eingekapselten Daten durchqueren. Bei Windows 2000 ist das Transitnetzwerk immer ein IP-Netzwerk. Das Transitnetzwerk kann das Internet oder ein privates IP-basiertes Intranet sein.

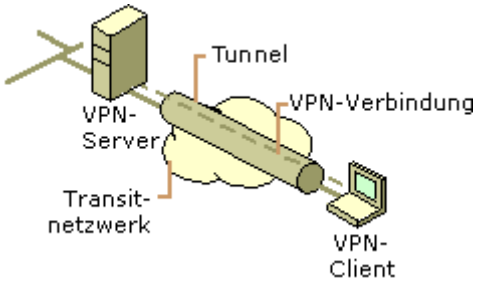

Abbildung 9.2: Komponenten einer VPN-Verbindung

VPN-Verbindungen

Das Erstellen des VPNs ähnelt stark dem Herstellen einer Punkt-zu-Punkt-Verbindung mithilfe von DFÜ-Netzwerkverfahren und Verfahren für das Routing für Wählen bei Bedarf. Es gibt zwei Arten von VPN-Verbindungen: die RAS-VPN-Verbindung und die Router-zu-Router-VPN-Verbindung.

RAS-VPN-Verbindung

Eine RAS-VPN-Verbindung wird von einem RAS-Client oder einem Computer mit einem einzigen Benutzer hergestellt, der eine Verbindung zu einem privaten Netzwerk herstellt. Der VPN-Server bietet Zugriff auf die Ressourcen des VPN-Servers oder auf das gesamte Netzwerk, mit dem der VPN-Server verknüpft ist. Die über die VPN-Verbindung gesendeten Pakete stammen vom RAS-Client.

Der RAS-Client (der VPN-Client) authentifiziert sich selbst gegenüber dem RAS-Server (dem VPN-Server), und der Server authentifiziert sich selbst zum Zweck der gemeinsamen Authentifizierung gegenüber dem Client.

Router-zu-Router-VPN-Verbindung

Eine Router-zu-Router-VPN-Verbindung wird von einem Router erstellt und verbindet zwei Bereiche eines privaten Netzwerkes. Der VPN-Server bietet eine umgeleitete Verbindung zu dem Netzwerk, mit dem der VPN-Server verknüpft ist. In einer Router-zu-Router-VPN-Verbindung stammen die Pakete, die von einem der Router über die VPN-Verbindung gesendet werden, normalerweise nicht von den Routern.

Der anrufende Router (der VPN-Client) authentifiziert sich selbst gegenüber dem antwortenden Router (dem VPN-Server), und der antwortende Router authentifiziert sich selbst zum Zweck der gemeinsamen Authentifizierung gegenüber dem anrufenden Router.

Eigenschaften von VPN-Verbindungen

VPN-Verbindungen, die PPTP und L2TP über IPSec verwenden, weisen folgende Eigenschaften auf:

- Einkapselung
- Authentifizierung
- Datenverschlüsselung
- Adress- und Namenserverzuweisung

Einkapselung

Mithilfe der VPN-Technologie können private Daten mit einem Header eingekapselt werden, der es den Daten ermöglicht, das Transitnetzwerk zu durchqueren.

Authentifizierung

Die Authentifizierung für VPN-Verbindungen kann zwei Formen annehmen:

- Benutzerauthentifizierung

  Damit die VPN-Verbindung hergestellt werden kann, authentifiziert der VPN-Server den VPN-Client, der die Verbindung herzustellen versucht, und überprüft, ob der VPN-Client über die entsprechenden Berechtigungen verfügt. Wenn gegenseitige Authentifizierung verwendet wird, authentifiziert der VPN-Client außerdem den VPN-Server und bietet so Schutz vor maskierten VPN-Servern.

- Datenauthentifizierung und -integrität

  Um zu überprüfen, ob die über die VPN-Verbindung gesendeten Daten vom anderen Ende der Verbindung stammen und nicht unterwegs geändert wurden, enthalten die Daten eine kryptografische Prüfsumme, die auf einem Verschlüsselungsschlüssel basiert, den nur der Absender und der Empfänger kennen.

Datenverschlüsselung

Damit die Vertraulichkeit der Daten beim Durchqueren des freigegebenen oder öffentlichen Transitnetzwerks sichergestellt ist, werden sie vom Absender verschlüsselt und vom Empfänger entschlüsselt. Der Verschlüsselungs- und der Entschlüsselungsprozess hängen davon ab, dass sowohl der Absender als auch der Empfänger einen gemeinsamen Verschlüsselungsschlüssel kennen.

Abgefangene Pakete, die über die VPN-Verbindung im Transitnetzwerk gesendet werden, sind für jeden unverständlich, der nicht den gemeinsamen Verschlüsselungsschlüssel besitzt. Die Länge des Verschlüsselungsschlüssels ist ein wichtiger Sicherheitsparameter. Beim Ermitteln des Verschlüsselungsschlüssels können rechnerische Techniken verwendet werden. Diese Techniken erfordern umso mehr Rechenleistung und Rechenzeit, je größer der Verschlüsselungsschlüssel wird. Es ist daher wichtig, den größtmöglichen Schlüssel zu verwenden.

Außerdem ist es umso einfacher, die verschlüsselten Daten zu entschlüsseln, je mehr Informationen mit demselben Schlüssel verschlüsselt sind. Bei manchen Verschlüsselungstechniken haben Sie die Möglichkeit, zu konfigurieren, wie oft die Verschlüsselungsschlüssel während einer Verbindung gewechselt werden.

Weitere Informationen dazu, wie Verschlüsselungsschlüssel für die VPN-Technologien in Windows 2000 verwaltet werden, finden Sie weiter unten in diesem Kapitel unter "VPN-Sicherheit".

Adress- und Namenserverzuweisung

Wenn ein VPN-Server konfiguriert wird, erstellt er eine virtuelle Schnittstelle, die die Schnittstelle darstellt, über die alle VPN-Verbindungen hergestellt werden. Wenn ein VPN-Client eine VPN-Verbindung herstellt, wird auf dem VPN-Client eine virtuelle Schnittstelle erstellt, die die mit dem VPN-Server verbundene Schnittstelle darstellt. Die virtuelle Schnittstelle auf dem VPN-Client ist mit der virtuellen Schnittstelle auf dem VPN-Server verbunden, der die Punkt-zu-Punkt-VPN-Verbindung erstellt.

Den virtuellen Schnittstellen des VPN-Clients und des VPN-Servers müssen IP-Adressen zugewiesen werden. Die Zuweisung dieser Adressen wird vom VPN-Server vorgenommen. Standardmäßig erhält der VPN-Server IP-Adressen für sich selbst und für VPN-Clients, die DHCP (Dynamic Host Configuration Protocol) verwenden. Sie können außerdem einen statischen Pool von IP-Adressen konfigurieren, die durch eine IP-Netzwerkkennung und eine Subnetzmaske definiert werden.

Die Namenserverzuweisung und die Zuweisung der DNS-Server (Domain Name System) und WINS-Server (Windows Internet Name Service) finden ebenfalls während des Herstellungsprozesses der VPN-Verbindung statt. Der VPN-Client erhält die IP-Adressen der DNS- und WNS-Server vom VPN-Server für das Intranet, mit dem der VPN-Server verknüpft ist.

Internet- und intranetbasierte VPN-Verbindungen

VPN-Verbindungen können immer verwendet werden, wenn eine sichere Punkt-zu-Punkt-Verbindung für das Verbinden von Benutzern oder Netzwerken benötigt wird. Typische VPN-Verbindungen sind entweder internetbasiert oder intranetbasiert.

Internetbasierte VPN-Verbindungen

Mithilfe einer internetbasierten VPN-Verbindung können Sie Telefonkosten vermeiden und gleichzeitig die globale Verfügbarkeit des Internets nutzen.

Remotezugriff über das Internet

Ein RAS-Client muss sich nicht über ein Ferngespräch oder ein Gespräch über eine gebührenfreie Nummer in einen Unternehmensnetzwerkserver oder einen ausgelagerten Network Access Server (NAS) einwählen, sondern er kann sich bei einem lokalen ISP einwählen. Durch die Verwendung der hergestellten physischen Verbindung zum lokalen ISP initiiert der RAS-Client eine VPN-Verbindung über das Internet zum VPN-Server der Organisation. Wenn die VPN-Verbindung erstellt ist, kann der RAS-Client auf die Ressourcen des privaten Intranets zugreifen.

Abbildung 9.3 zeigt den Remotezugriff über das Internet.

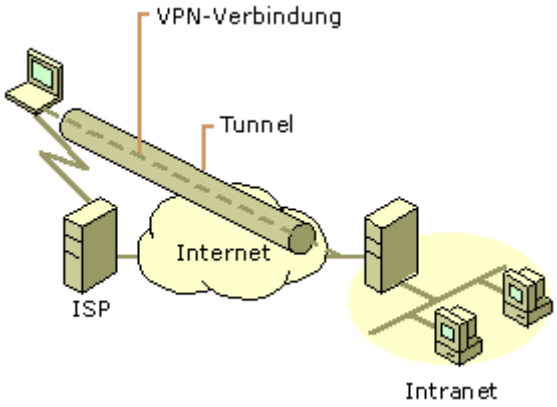

Abbildung 9.3: VPN-Verbindung, die einen Remoteclient mit einem privaten Intranet verbindet

Verbinden von Netzwerken über das Internet

Wenn Netzwerke über das Internet verbunden sind (siehe Abbildung 9.4), leitet ein Router Pakete über eine VPN-Verbindung an einen anderen Router weiter. Für die Router fungiert der VPN als Datenverbindungsebenen-Verbindung.

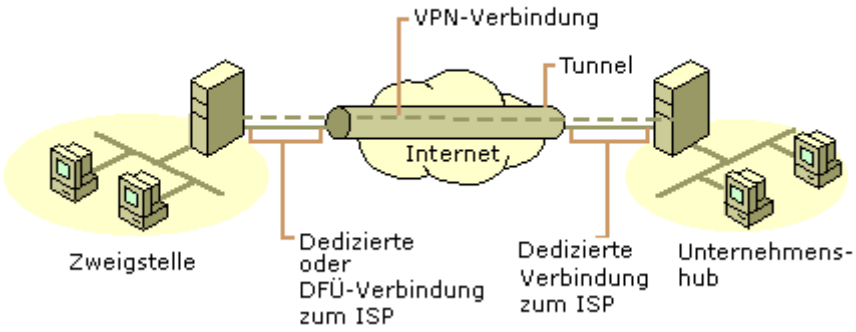

Abbildung 9.4: VPN-Verbindung für zwei Außenstellen über das Internet

Verbinden von Netzwerken mithilfe von WAN-Verbindungen Anstatt eine teure dedizierte WAN-Fernverbindung zwischen Büros zu verwenden, werden die Bürorouter mithilfe von dedizierten lokalen WAN-Verbindungen (Wide Area Network) zu einem lokalen ISP mit dem Internet verbunden. Dann wird von einem der Router eine Router-zu-Router-VPN-Verbindung über das Internet initiiert. Die Router können, wenn sie verbunden sind, geleiteten oder Routingprotokollverkehr mithilfe der VPN-Verbindung aneinander weiterleiten.

Verbinden von Netzwerken mithilfe von DFÜ-WAN-Verbindungen Ein Zweigstellenrouter muss sich nicht über ein Ferngespräch oder ein Gespräch über eine gebührenfreie Nummer in einen Unternehmensnetzwerkserver oder einen ausgelagerten NAS einwählen, sondern er kann sich bei einem lokalen ISP einwählen. Mithilfe der hergestellten Verbindung zum lokalen ISP wird vom Zweigstellenrouter eine Router-zu-Router-VPN-Verbindung über das Internet zum Unternehmenshubrouter initiiert. Der als VPN-Server fungierende Unternehmenshubrouter muss über eine dedizierte WAN-Verbindung mit einem lokalen ISP verbunden sein.

Weitere Informationen zum Konfigurieren von VPN-Verbindungen mithilfe einer DFÜ-Verbindung zu einem lokalen ISP finden Sie weiter unten in diesem Kapitel unter "Adressierung und Routing für VPNs".

Mithilfe einer DFÜ-WAN-Verbindung können beide Büros mit dem Internet verbunden sein. Dies ist jedoch nur machbar, wenn der ISP Routing für Wählen bei Bedarf an Kunden unterstützt; der ISP ruft den Router des Kunden an, wenn dem Kunden ein IP-Datagramm zugestellt werden soll. Routing für Wählen bei Bedarf an Kunden wird nicht von vielen ISPs unterstützt.

Intranetbasierte VPN-Verbindungen

Die intranetbasierte VPN-Verbindung nutzt die IP-Konnektivität in einem Organisationsintranet.

Remotezugriff über ein Intranet

In manchen Organisationsintranets sind die Daten einer Abteilung, beispielsweise der Personalabteilung, so kritisch, dass das Netzwerksegment der Abteilung physisch vom Rest des Intranets der Organisation getrennt ist. Dadurch werden zwar die Daten der Abteilung geschützt, es entstehen jedoch für die nicht physisch mit dem separaten Netzwerksegment verbundenen Benutzer Probleme beim Zugriff auf die Informationen.

Mit VPN-Verbindungen kann das Netzwerksegment der kritischen Abteilung physisch mit dem Organisationsintranet verbunden und gleichzeitig durch einen VPN-Server getrennt sein. Der VPN-Server bietet keine direkte umgeleitete Verbindung zwischen dem Unternehmensintranet und dem separaten Netzwerksegment. Benutzer im Unternehmensintranet, die über die entsprechenden Berechtigungen verfügen, können eine RAS-VPN-Verbindung zum VPN-Server herstellen und auf die geschützten Ressourcen des Netzwerkes der kritischen Abteilung zugreifen. Außerdem ist aus Gründen der Datenvertraulichkeit die gesamte Kommunikation über die VPN-Verbindung verschlüsselt. Für die Benutzer, die nicht über die Berechtigung zum Herstellen einer VPN-Verbindung verfügen, ist das separate Netzwerksegment ausgeblendet.

Abbildung 9.5 zeigt den Remotezugriff über ein Intranet.

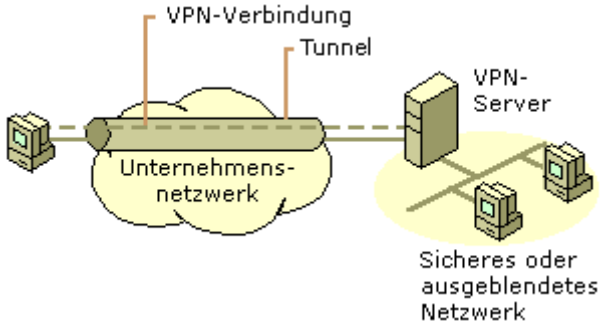

Abbildung 9.5: VPN-Verbindung, die Remotezugriff auf ein sicheres Netzwerk über ein Intranet zulässt

Verbinden von Netzwerken über ein Intranet

Sie können mithilfe einer Router-zu-Router-VPN-Verbindung ebenfalls zwei Netzwerke über ein Intranet verbinden. Diese Art von VPN-Verbindung kann möglicherweise nötig sein, damit beispielsweise zwei Abteilungen an verschiedenen Standorten, deren Daten sehr kritisch sind, miteinander kommunizieren können. Beispielsweise muss möglicherweise die Finanzabteilung mit der Personalabteilung kommunizieren, um Gehaltsinformationen auszutauschen.

Die Finanzabteilung und die Personalabteilung sind über das gemeinsame Intranet mit Computern verbunden, die als VPN-Clients oder VPN-Server fungieren können. Wenn die VPN-Verbindung hergestellt ist, können Benutzer auf Computern in beiden Netzwerken kritische Daten über das Unternehmensintranet austauschen.

Abbildung 9.6 zeigt über ein Intranet verbundene Netzwerke.

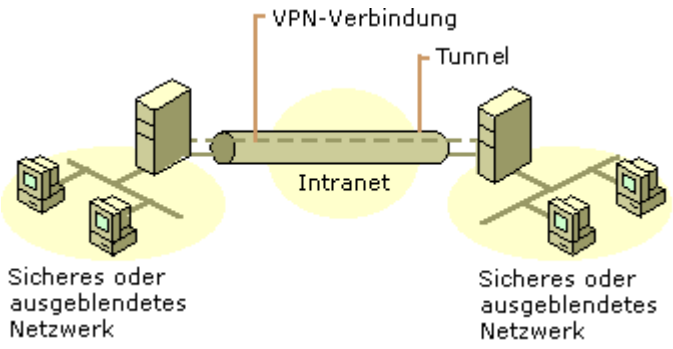

Abbildung 9.6: VPN-Verbindung, die zwei Netzwerke über ein Intranet verbindet

Kombinierte Internet- und Intranet-VPN-Verbindungen

Eine VPN-Verbindung ist ein Netzwerktool, das sichere Punkt-zu-Punkt-Verbindungen auf jede von Ihnen gewünschte Weise bereitstellen kann. Eine weniger gebräuchliche kombinierte Internet- und Intranet-VPN-Verbindung, Pass-Through-VPN-Verbindung genannt, (siehe Abbildung 9.7) ermöglicht einem mit dem Intranet eines Unternehmens verbundenen RAS-Client, über das Internet auf die Ressourcen des Intranets eines anderen Unternehmens zuzugreifen. In diesem Szenario durchläuft eine RAS-VPN-Verbindung ein Intranet und das Internet, um auf ein zweites Intranet zuzugreifen.

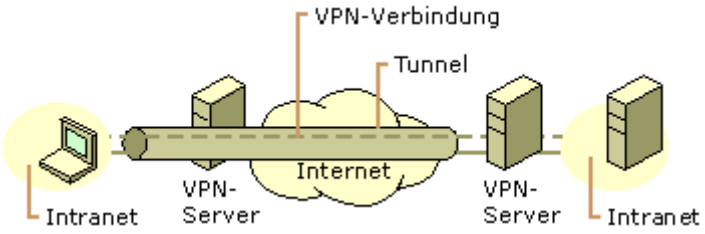

Abbildung 9.7: Pass-Through-VPN-Verbindung

Weitere Informationen zu Pass-Through-VPNs finden Sie weiter unten in diesem Kapitel unter "Pass-Through-VPN-Szenario".

Verwalten von Virtual Private Networking (VPN)

Virtual Private Networking muss wie jede andere Netzwerkressource verwaltet werden, und VPN-Sicherheitsfragen, insbesondere in Bezug auf Internet-VPN-Verbindungen, müssen sorgfältig behandelt werden. Bedenken Sie die folgenden Fragen:

- Wo sollen die Benutzerkontendaten gespeichert werden?
- Wie werden Adressen VPN-Clients zugewiesen?
- Wer darf VPN-Verbindungen erstellen?
- Wie überprüft der VPN-Server die Identität des Benutzers, der versucht, die VPN-Verbindung herzustellen?
- Wie zeichnet der VPN-Server die VPN-Aktivität auf?
- Wie kann der VPN-Server mit Branchenstandards entsprechenden Netzwerkverwaltungsprotokollen und Infrastrukturen verwaltet werden?

Verwalten der Benutzer

Da es administrativ nicht tragbar ist, für denselben Benutzer separate Benutzerkonten auf separaten Servern zu verwalten und zu versuchen, sie alle gleichzeitig aktuell zu halten, richten die meisten Administratoren eine Masterkontendatenbank auf einem Domänencontroller (PDC) oder auf einem RADIUS-Server (Remote Authentication Dial-in User Service) ein. Dies ermöglicht es dem VPN-Server, die Authentifizierungsinformationen an eine zentrale Authentifizierungsvorrichtung zu senden. Für die RAS-Einwahl und für den VPN-basierten Remotezugriff wird dasselbe Benutzerkonto verwendet.

Verwalten von Adressen und Namenservern

Auf dem VPN-Server müssen IP-Adressen verfügbar sein, die während der IPCP-Aushandlungsphase (IP Control Protocol) des Verbindungsherstellungsprozesses der virtuellen Schnittstelle des VPN-Servers und VPN-Clients zugewiesen werden können. Die dem VPN-Client zugewiesene IP-Adresse wird der virtuellen Schnittstelle des VPN-Clients zugewiesen.

Für Windows 2000-basierte VPN-Server werden die VPN-Clients zugewiesenen IP-Adressen standardmäßig durch DHCP erhalten. Sie können auch einen statischen IP-Adresspool konfigurieren.

Der VPN-Server muss außerdem mit DNS- und WINS-Serveradressen konfiguriert sein, um sie während der IPCP-Aushandlung dem VPN-Client zuzuweisen. Weitere Informationen dazu, wie der VPN-Server die IP-Adressen von DNS- und WINS-Servern zuweist, finden Sie in diesem Buch unter "Remote Access Server".

Verwalten des Zugriffs

Konfigurieren Sie für Windows 2000 die Einwähleigenschaften für Benutzerkonten und die RAS-Richtlinien für das Verwalten des Zugriffs für DFÜ-Netzwerke und VPN-Verbindungen.

Zugriff nach Benutzerkonten

Wenn Sie den Remotezugriff auf Benutzerbasis verwalten, legen Sie die RAS-Berechtigung für die Benutzerkonten, die VPN-Verbindungen erstellen dürfen, auf **Zugriff gestatten** fest. Wenn der VPN-Server nur VPN-Verbindungen zulässt, löschen Sie die Standard-RAS-Richtlinie namens **Zugriff zulassen, wenn Einwählrechte erteilt worden sind**. Erstellen Sie dann eine neue RAS-Richtlinie mit einem aussagekräftigen Namen, wie beispielsweise **VPN-Zugriff, wenn das Benutzerkonto es zulässt**.

Wenn der VPN-Server auch DFÜ-RAS-Dienste zulässt, löschen Sie die Standardrichtlinie nicht, sondern verschieben Sie sie so, dass sie als letzte Richtlinie ausgewertet wird.

Konfigurieren Sie als Beispiel für typische Einstellungen die RAS-Richtlinienberechtigungen als **RAS-Berechtigung verweigern**, und legen Sie die Bedingungen und Profileinstellungen gemäß den Tabellen 9.1 und 9.2 fest. Ausführliche Informationen zum Konfigurieren dieser Einstellungen finden Sie in der Microsoft Windows 2000 Server-Hilfe.

Tabelle 9.1: RAS-Richtlinienbedingungen für VPN-Zugriff nach Benutzerkonten

Bedingungen	**Einstellung**
NAS-Porttyp	**Virtuell**

Tabelle 9.2: Profileinstellungen für RAS-Richtlinien für VPN-Zugriff nach Benutzerkonten

Profileinstellungen	**Einstellung**
Registerkarte **Authentifizierung**	Aktivieren Sie **Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP v2)** und **Microsoft-verschlüsselte Authentifizierung (MS-CHAP).**
Registerkarte **Verschlüsselung**	Wählen Sie **Basisverschlüsselung, Starke Verschlüsselung** oder **Stärkste Verschlüsselung** aus. Deaktivieren Sie **Keine Verschlüsselung**.

Wenn Sie eine andere Authentifizierung, Verschlüsselung oder andere Einstellungen für PPTP- oder L2TP-Verbindungen definieren möchten, erstellen Sie separate RAS-Richtlinien. Verwenden Sie hierzu die RAS-Richtlinienbedingung **Tunneltyp**, und legen Sie sie entweder auf das **Point-to-Point Tunneling Protocol** oder auf das **Layer Two Tunneling Protocol** fest.

Zugriff nach Gruppenmitgliedschaft

Wenn Sie den Remotezugriff auf Gruppenbasis verwalten, legen Sie die RAS-Zugriffsberechtigung für alle Benutzerkonten auf **Zugriff über RAS-Richtlinien steuern** fest. Erstellen Sie eine Windows 2000-Gruppe, deren Mitglieder VPN-Verbindungen erstellen dürfen. Wenn der VPN-Server nur VPN-Verbindungen zulässt, löschen Sie die Standard-RAS-Richtlinie namens **Zugriff zulassen, wenn Einwählrechte erteilt worden sind**. Erstellen Sie dann eine neue RAS-Richtlinie mit einem aussagekräftigen Namen, wie beispielsweise **VPN-Zugriff, wenn Mitglied von Gruppe mit VPN-Berechtigung**.

Wenn der VPN-Server auch DFÜ-Netzwerk-RAS-Dienste zulässt, löschen Sie die Standardrichtlinie nicht, sondern verschieben Sie sie so, dass sie als letzte Richtlinie ausgewertet wird.

Konfigurieren Sie als Beispiel für typische Einstellungen die RAS-Richtlinienberechtigungen als **RAS-Berechtigung erteilen**, und legen Sie die Bedingungen und Profileinstellungen gemäß den Tabellen 9.3 und 9.4 fest. Ausführliche Informationen zum Konfigurieren dieser Einstellungen finden Sie in der Microsoft Windows 2000 Server-Hilfe.

Tabelle 9.3: RAS-Richtlinienbedingungen für VPN-Zugriff nach Windows 2000-Gruppen

Bedingungen	Einstellung
NAS-Porttyp	**Virtuell**
Windows-Gruppen	Windows 2000-Gruppe, deren Mitglieder VPN-Verbindungen erstellen dürfen.

Tabelle 9.4: Profileinstellungen für RAS-Richtlinien für VPN-Zugriff nach Windows 2000-Gruppen

Profileinstellungen	Einstellung
Registerkarte **Authentifizierung**	Aktivieren Sie **Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP v2)** und **Microsoft-verschlüsselte Authentifizierung (MS-CHAP)**.
Registerkarte **Verschlüsselung**	Wählen Sie **Basisverschlüsselung, Starke Verschlüsselung** oder **Stärkste Verschlüsselung** aus. Deaktivieren Sie **Keine Verschlüsselung**.

Verwalten der Authentifizierung

Der VPN-Server kann so konfiguriert werden, dass er entweder Windows oder RADIUS als Authentifizierungsanbieter verwendet. Wenn Windows als Authentifizierungsanbieter ausgewählt wird, werden die von Benutzern, die versuchen, VPN-Verbindungen herzustellen, gesendeten Benutzeranmeldeinformationen mithilfe typischer Windows-Authentifizierungsmechanismen authentifiziert.

Wenn RADIUS ausgewählt und als Authentifizierungsanbieter auf dem VPN-Server konfiguriert wird, werden Benutzeranmeldeinformationen und Parameter der Verbindungsanforderung als Serie von RADIUS-Anforderungsmeldungen an einen RADIUS-Server gesendet.

Der RADIUS-Server empfängt eine Benutzerverbindungsanforderung vom VPN-Server und authentifiziert den Benutzer mithilfe seiner Authentifizierungsdatenbank. Ein RADIUS-Server kann außerdem eine zentrale Speicherdatenbank mit anderen relevanten Benutzereigenschaften verwalten. Zusätzlich zu einer Ja- oder Nein-Antwort auf eine Authentifizierungsanforderung kann RADIUS den VPN-Server über andere geltende Verbindungsparameter für diesen Benutzer informieren - beispielsweise die maximale Sitzungsdauer, die statische IP-Adresszuweisung usw.

RADIUS kann auf Basis seiner eigenen Datenbank auf Authentifizierungsanforderungen reagieren oder als Front-End für einen anderen Datenbankserver, wie beispielsweise einen allgemeinen ODBC-Server (Open Database Connectivity) oder einen Windows 2000-PDC, fungieren. Das letztere Beispiel kann sich auf demselben Computer wie der RADIUS-Server oder an einem anderen Ort befinden. Außerdem kann ein RADIUS-Server als Proxyclient für einen RADIUS-Remoteserver fungieren.

Das RADIUS-Protokoll wird in RFC 2138 und RFC 2139 beschrieben. Weitere Informationen zum RADIUS-Protokoll und zum Windows 2000-basierten RADIUS-Server, der als Internetauthentifizierungsdienst bekannt ist, finden Sie in diesem Buch unter "Internet Authentication Service".

Verwalten der Kontoführung

Sie können den VPN-Server so konfigurieren, dass er entweder Windows oder RADIUS als Kontoführungsanbieter verwendet. Wenn Sie Windows als Kontoführungsanbieter auswählen, werden die Kontoführungsinformationen auf dem VPN-Server angesammelt, damit sie später analysiert werden können. Wenn Sie RADIUS auswählen, werden RADIUS-Kontoführungsmeldungen an den RADIUS-Server gesendet, damit sie dort angesammelt und später analysiert werden können.

Sie können die meisten RADIUS-Server so konfigurieren, dass sie Authentifizierungsanforderungseinträge in einer Kontoführungsdatei speichern. Es gibt viele Rechnungs- und Überwachungspakete von Drittanbietern, die RADIUS-Kontoführungseinträge lesen und verschiedene hilfreiche Berichte erstellen. Weitere Informationen zur RADIUS-Kontenführung finden Sie in RFC 2139.

Netzwerkverwaltung

Der als VPN-Server fungierende Computer kann als SNMP-Agent in einer SMTP-Umgebung (Simple Network Management Protocol) teilnehmen, wenn der SNMP-Dienst von Windows 2000 installiert ist. Der VPN-Server zeichnet Verwaltungsinformationen in verschiedenen Objektkennungen der Internet Management Information Base (MIB) II auf, die mit dem SNMP-Dienst von Windows 2000 installiert wird. Die Objekte in der Internet MIB II werden in RFC 1213 dokumentiert.

Point-to-Point Tunneling Protocol

Das Point-to-Point Tunneling Protocol (PPTP) kapselt PPP-Frames (Point-to-Point Protocol) für die Übertragung über ein IP-basiertes Netzwerk, wie beispielsweise das Internet oder ein privates Intranet, in IP-Datagramme ein. PPTP wird in RFC 2637 dokumentiert.

Das PPTP verwendet eine TCP-Verbindung, bekannt als PPTP-Steuerungsverbindung, um den Tunnel zu erstellen, aufrechtzuerhalten und zu beenden, und eine geänderte Version von Generic Routing Encapsulation (GRE), um PPP-Frames als getunnelte Daten einzukapseln. Die Nutzlast der eingekapselten PPP-Frames kann verschlüsselt und/oder komprimiert werden.

PPTP geht davon aus, dass zwischen einem PPTP-Client (einem VPN-Client, der das PPTP-Tunnelprotokoll verwendet) und einem PPTP-Server (einem VPN-Server, der das PPTP-Tunnelprotokoll verwendet) ein IP-Netzwerk verfügbar ist. Der PPTP-Client ist möglicherweise bereits mit einem IP-Netzwerk verknüpft, das den PPTP-Server erreichen kann, oder der PPTP-Client muss sich möglicherweise, wie im Fall von DFÜ-Internetbenutzern, bei einem Network Access Server (NAS) einwählen, um die IP-Verbindung herzustellen.

Die während der Erstellung einer PPTP-basierten VPN-Verbindung auftretende Authentifizierung verwendet dieselben Authentifizierungsmechanismen wie PPP-Verbindungen, beispielsweise Extensible Authentication Protocol (EAP), Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), CHAP, Shiva Password Authentication Protocol (SPAP) und Password Authentication Protocol (PAP). PPTP erbt die Verschlüsselung und/oder Komprimierung von PPP-Nutzlasten von PPP. Für Windows 2000 muss entweder EAP-Transport Level Security (EAP-TLS) oder MS-CHAP verwendet werden, damit die PPP-Nutzlasten mit Microsoft Punkt-zu-Punkt-Verschlüsselung (Microsoft Point-to-Point Encryption, MPPE) verschlüsselt werden.

MPPE bietet nur Linkverschlüsselung, keine Ende-zu-Ende-Verschlüsselung. Ende-zu-Ende-Verschlüsselung ist eine Datenverschlüsselung zwischen der Clientanwendung und dem Server, der die Ressource oder den Dienst verwaltet, auf die bzw. den die Clientanwendung zugreift. Wenn Ende-zu-Ende-Verschlüsselung erforderlich ist, kann IPSec verwendet werden, um den IP-Verkehr von Ende zu Ende zu verschlüsseln, nachdem der PPTP-Tunnel aufgebaut ist.

Bei internetbasierten PPTP-Servern ist der PPTP-Server ein PPTP-fähiger VPN-Server mit einer Schnittstelle im Internet und einer zweiten Schnittstelle im Intranet.

Tunnelverwaltung mit der PPTP-Steuerungsverbindung

Die PPTP-Steuerungsverbindung besteht zwischen der IP-Adresse des PPTP-Clients, der einen dynamisch zugewiesenen TCP-Port verwendet, und der IP-Adresse des PPTP-Servers, der den reservierten TCP-Port 1723 verwendet. Die PPTP-Steuerungsverbindung transportiert die PPTP-Anrufssteuerungs- und -verwaltungsmeldungen, die zum Verwalten des PPTP-Tunnels verwendet werden. Dazu gehört die Übertragung regelmäßiger PPTP-Echoanforderungs- und PPTP-Echorückmeldungsmeldungen (Echo-Request/Echo-Reply), um einen Konnektivitätsausfall zwischen dem PPTP-Client und dem PPTP-Server festzustellen. PPTP-Steuerungsverbindungspakete bestehen aus einem IP-Header, einem TCP-Header und einer PPTP-Steuerungsmeldung (siehe Abbildung 9.8). Das PPTP-Steuerungsverbindungspaket in Abbildung 9.8 enthält außerdem einen Datenverbindungsebenen-Header und -Nachspann.

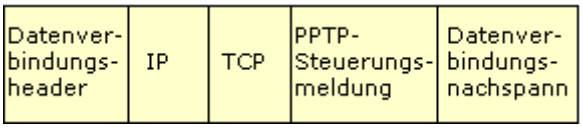

Abbildung 9.8: PPTP-Steuerungsverbindungspaket

Tabelle 9.5 enthält die primären PPTP-Steuerungsmeldungen, die über die PPTP-Steuerungsverbindung gesendet werden. Für alle PPTP-Steuerungsmeldungen wird der genaue PPTP-Tunnel durch die TCP-Verbindung angegeben.

Tabelle 9.5: PPTP-Anrufssteuerungs- und -Verbindungsverwaltungsmeldungen

Meldungstyp	**Zweck**
Start-Control-Connection-Request	Wird vom PPTP-Client gesendet, um die Steuerungsverbindung herzustellen. Für jeden PPTP-Tunnel muss eine Steuerungsverbindung hergestellt werden, bevor andere PPTP-Meldungen ausgegeben werden können.
Start-Control-Connection-Reply	Wird vom PPTP-Server als Antwort auf die Meldung "Start-Control-Connection-Request" gesendet.
Outgoing-Call-Request	Wird vom PPTP-Client gesendet, um einen PPTP-Tunnel zu erstellen. Die Meldung "Outgoing-Call-Request" enthält eine Anrufskennung, die im GRE-Header verwendet wird, um den getunnelten Verkehr eines bestimmten Tunnels zu identifizieren.
Outgoing-Call-Reply	Wird vom PPTP-Server als Antwort auf die Meldung "Outgoing-Call-Request" gesendet.
Echo-Request	Wird entweder vom PPTP-Client oder vom PPTP-Server als Keep-Alive-Mechanismus gesendet. Wenn die Echoanforderung nicht beantwortet wird, wird der PPTP-Tunnel schließlich beendet.
Echo-Reply	Die Antwort auf eine Echoanforderung. **Anmerkung:** Die PPTP-Meldungen "Echo-Request" und "Echo-Reply" sind nicht mit den ICMP-Meldungen "Echo Request" und "Echo Reply" verwandt.
WAN-Error-Notify	Wird vom PPTP-Server an alle VPN-Clients gesendet, um auf Fehler an der PPP-Schnittstelle des PPTP-Servers hinzuweisen.
Set-Link-Info	Wird vom PPTP-Client oder vom PPTP-Server an festgelegte PPP-ausgehandelte Optionen gesendet.
Call-Clear-Request	Wird vom PPTP-Client gesendet und gibt an, dass ein Tunnel beendet werden soll.
Call-Disconnect-Notify	Wird vom PPTP-Server als Antwort auf die Meldung "Call-Clear-Request" oder aus anderen Gründen gesendet und weist darauf hin, dass ein Tunnel beendet werden soll. Wenn der PPTP-Server den PPTP-Tunnel beendet, wird die Meldung "Call-Disconnect-Notify" gesendet.
Stop-Control-Connection-Request	Wird vom PPTP-Client oder vom PPTP-Server gesendet, um sich gegenseitig darüber zu informieren, dass die Steuerungsverbindung beendet wird.
Stop-Control-Connection-Reply	Wird als Antwort auf die Meldung "Stop-Control-Connection-Request" verwendet.

Informationen zur genauen Struktur von PPTP-Steuerungsverbindungsmeldungen finden Sie in RFC 2637.

PPTP-Datentunneling

PPTP-Datentunneling wird über mehrere Einkapselungsstufen durchgeführt.

Abbildung 9.9 zeigt die sich ergebende Struktur der mit PPTP getunnelten Daten.

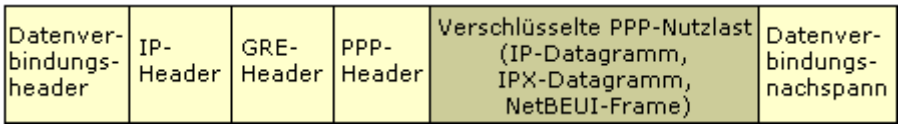

Abbildung 9.9: Mit PPTP getunnelte Daten

Einkapselung des PPP-Frames

Die anfängliche PPP-Nutzlast wird verschlüsselt und mit einem PPP-Header eingekapselt, um einen PPP-Frame zu erstellen. Der PPP-Frame wird dann mit einem geänderten GRE-Header eingekapselt. GRE wird in RFC 1701 und RFC 1702 dokumentiert und wurde als einfacher, schlichter Allzweckmechanismus für das Einkapseln von über IP-Netzwerken gesendeten Daten entworfen. GRE ist ein Clientprotokoll von IP, das das IP-Protokoll 47 verwendet.

Für PPTP wird der GRE-Header folgendermaßen geändert:

- Es wird ein Bestätigungsbit verwendet, um darauf hinzuweisen, dass ein 32-Bit-Bestätigungsfeld vorhanden und signifikant ist.
- Das Schlüsselfeld wird durch ein 16-Bit-Nutzlastlängenfeld und ein 16-Bit-Anrufskennungsfeld ersetzt. Das Anrufskennungsfeld wird während der Erstellung des PPTP-Tunnels vom PPTP-Client festgelegt.
- Es wird ein 32-Bit-Bestätigungsfeld hinzugefügt.

Innerhalb des GRE-Headers ist der Protokolltyp auf 0x880B festgelegt, den EtherType-Wert für einen PPP-Frame.

Anmerkung GRE wird manchmal von ISPs verwendet, um Routinginformationen innerhalb des Netzwerkes eines ISPs weiterzuleiten. Um zu verhindern, dass die Routinginformationen an Internetbackbone-Router weitergeleitet werden, filtern ISPs den GRE-Verkehr an den mit dem Internetbackbone verbundenen Schnittstellen heraus. Als Ergebnis dieser Filterung können PPTP-Tunnel mithilfe von PPTP-Steuerungsmeldungen erstellt werden, mit PPTP getunnelte Daten werden jedoch nicht weitergeleitet. Wenn Sie vermuten, dass dies ein Problem darstellt, wenden Sie sich an Ihren ISP.

Einkapselung von GRE-Paketen

Die sich ergebende mit GRE und PPP eingekapselte Nutzlast wird dann mit einem IP-Header eingekapselt, der die entsprechenden IP-Quell- und -Zieladressen für den PPTP-Client und den PPTP-Server enthält.

Datenverbindungsebenen-Verschlüsselung

Damit das IP-Datagramm über eine LAN- oder WAN-Verbindung gesendet werden kann, wird es schließlich mit einem Header und einem Nachspann für die Datenverbindungsebenen-Technologie der ausgehenden physischen Schnittstelle eingekapselt. Wenn IP-Datagramme beispielsweise über eine Ethernetschnittstelle gesendet werden, wird das IP-Datagramm mit einem Ethernet-Header und -Nachspann eingekapselt. Wenn IP-Datagramme über eine Punkt-zu-Punkt-WAN-Verbindung gesendet werden, beispielsweise eine analoge Telefonleitung oder ISDN, wird das IP-Datagramm mit einem PPP-Header und -Nachspann eingekapselt.

Verarbeiten der mit PPTP getunnelten Daten

Wenn der PPTP-Client oder PPTP-Server die mit PPTP getunnelten Daten erhält, geht er folgendermaßen vor:

1. Er verarbeitet und entfernt den Datenverbindungsheader und den Datenverbindungsnachspann.
2. Er verarbeitet und entfernt den IP-Header.
3. Er verarbeitet und entfernt die GRE- und PPP-Header.
4. Er entschlüsselt und/oder dekomprimiert die PPP-Nutzlast (wenn nötig).
5. Er verarbeitet die Nutzlast zum Empfangen oder Weiterleiten.

PPTP-Pakete und Windows 2000-Netzwerkarchitektur

Abbildung 9.10 zeigt den Pfad, den getunnelte Daten von einem VPN-Client über eine RAS-VPN-Verbindung mithilfe eines analogen Modems durch die Windows 2000-Netzwerkarchitektur verwenden. Die folgenden Schritte erläutern diesen Prozess:

1. Ein IP-Datagramm, IPX-Datagramm oder NetBEUI-Frame wird von seinem entsprechenden Protokoll mithilfe der Network Driver Interface Specification (NDIS) an die virtuelle Schnittstelle gesendet, die die VPN-Verbindung darstellt.
2. NDIS sendet das Paket an NDISWAN, das die Daten verschlüsselt und/oder komprimiert und einen PPP-Header bereitstellt, der nur aus dem PPP-Protokollkennungsfeld besteht. Es werden keine Flags oder Rahmenprüfungssequenz-Felder (Frame Check Sequence, FCS) hinzugefügt. Dabei wird davon ausgegangen, dass die Adress- und Kontrollfeldkomprimierung während der LCP-Phase (Link Control Protocol) des PPP-Verbindungsprozesses ausgehandelt wurde. Weitere Informationen zu PPP und LCP finden Sie in diesem Buch unter "Remote Access Server".
3. NDISWAN sendet die Daten an den PPTP-Protokolltreiber, der den PPP-Frame mit einem GRE-Header einkapselt. Im GRE-Header wird das Anrufskennungsfeld auf den geeigneten Wert festgelegt, um den Tunnel zu identifizieren.
4. Der PPTP-Protokolltreiber sendet dann das sich ergebende Paket an den TCP/IP-Protokolltreiber.
5. Der TCP/IP-Protokolltreiber kapselt die mit PPTP getunnelten Daten mit einem IP-Header ein und sendet mithilfe von NDIS das sich ergebende Paket an die Schnittstelle, die die DFÜ-Verbindung zum lokalen ISP darstellt.
6. NDIS sendet das Paket an NDISWAN, das PPP-Header und -Nachspanne bereitstellt.
7. NDISWAN sendet den sich ergebenden PPP-Frame an den geeigneten WAN-Miniporttreiber, der die DFÜ-Hardware darstellt (beispielsweise den asynchronen Port für eine Modemverbindung).

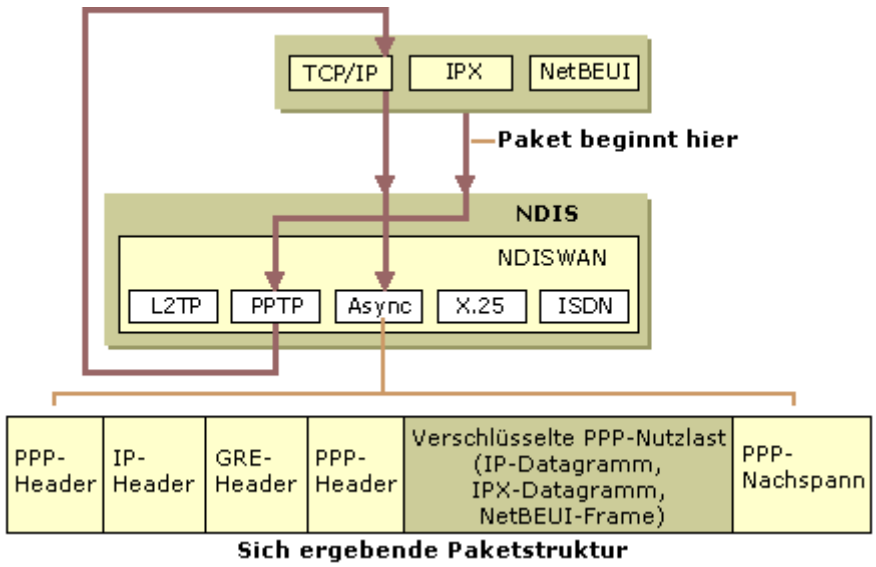

Abbildung 9.10: PPTP-Paketentwicklung

Anmerkung Es ist möglich, eine verschlüsselte PPP-Verbindung für die DFÜ-Verbindung mit dem ISP auszuhandeln. Es ist jedoch nicht nötig und nicht empfehlenswert, da die gesendeten privaten Daten, der getunnelte PPP-Frame, bereits verschlüsselt sind. Die zusätzliche Verschlüsselungsstufe wird nicht benötigt und kann die Leistung beeinträchtigen.

Verwenden des Netzwerklastenausgleichs mit PPTP

Mit dem Windows 2000-Netzwerklastenausgleich können Sie einen Cluster von PPTP-Servern erstellen, um die Verfügbarkeit von PPTP-Servern für VPN-Verbindungen zu verbessern. So erstellen Sie einen Cluster von PPTP-Servern mit Lastenausgleich:

1. Konfigurieren Sie jedes Mitglied des Clusters als Windows 2000-PPTP-Server. Weitere Informationen zum Konfigurieren eines Windows 2000-Servercomputers als PPTP-Server finden Sie in der Windows 2000 Server-Hilfe.
2. Konfigurieren Sie die Gruppe von PPTP-Servercomputern als Netzwerklastenausgleichs-Cluster. Weitere Informationen zum Konfigurieren des Netzwerklastenausgleichs finden Sie in der Microsoft Windows 2000 Advanced Server-Hilfe. Aktivieren Sie, wenn Sie den Netzwerklastenausgleich auf jedem PPTP-Server konfigurieren, den Netzwerklastenausgleich auf der Schnittstelle, die PPTP-Verbindungsanforderungen erhält.
3. Dadurch, dass Sie den Netzwerklastenausgleich auf jedem PPTP-Server konfigurieren, werden sowohl eine Cluster-IP-Adresse als auch eine dedizierte IP-Adresse als mehrfache IP-Adressen auf der Schnittstelle konfiguriert, die PPTP-Verbindungsanforderungen erhält. Um Probleme beim Erstellen von PPTP-Verbindungen mit Windows 95-, Windows NT 4.0- und Windows 98-PPTP-Clients zu vermeiden, entfernen Sie mithilfe der Eigenschaften des TCP/IP-Protokolls in den Netzwerk- und DFÜ-Verbindungen für jeden einzelnen PPTP-Server im Cluster die dedizierte IP-Adresse von der Schnittstelle, die PPTP-Verbindungsanforderungen erhält.
4. Das Entfernen der dedizierten IP-Adresse verhindert, dass einzelne Server mithilfe der dedizierten IP-Adresse remote verwaltet werden. Wenn Sie die Remoteverwaltung einzelner PPTP-Server im Cluster zulassen möchten, stellen Sie sicher, dass auf jedem Server im Cluster, der mit einem anderen Netzwerksegment verbunden ist als der Schnittstelle, die PPTP-Verbindungsanforderungen erhält, eine zusätzliche LAN-Schnittstelle vorhanden ist. Auf mit dem Internet verbundenen PPTP-Servern ist normalerweise eine zusätzliche Schnittstelle vorhanden, die mit dem Intranet verbunden ist, das mit einem anderen Netzwerksegment verbunden ist. Wenn Sie die dedizierte IP-Adresse von der Internetschnittstelle entfernt haben, können Sie den einzelnen PPTP-Server remote vom Internet aus verwalten, jedoch nicht vom Intranet aus.

Anmerkung Windows 95-, Windows NT 4.0- und Windows 98-PPTP-Clients können möglicherweise nur dann auf den PPTP-Cluster zugreifen, wenn die dedizierte IP-Adresse entfernt wird, da diese Clients ihre PPTP-Verbindungsanforderungen an die Cluster-IP-Adresse senden. Ein einzelner PPTP-Server antwortet möglicherweise auf die PPTP-Verbindungsanforderung von der dedizierten IP-Adresse, anstatt auf die von der Cluster-IP-Adresse. In diesem Fall bemerkt der PPTP-Client, dass für Anforderung und Antwort unterschiedliche IP-Adressen verwendet werden, geht davon aus, dass es sich bei diesem Verhalten um eine Verletzung der Sicherheit der PPTP-Verbindung handelt und beendet die Verbindung.

Layer 2 Tunneling Protocol und Internetprotokollsicherheit

Layer Two Tunneling Protocol (L2TP) ist eine Kombination aus PPTP und Layer 2 Forwarding (L2F), einer von Cisco® Systems, Inc. eingeführten Technologie. Anstatt zuzulassen, dass zwei inkompatible Tunnelprotokolle auf dem Markt miteinander konkurrieren und bei den Kunden für Verwirrung sorgen, schrieb die IETF vor, die beiden Technologien zu einem einzigen Tunnelprotokoll zu kombinieren, das die besten Features von PPTP und L2F vereint. L2TP wird in RFC 2661 dokumentiert.

L2TP kapselt PPP-Frames ein, die über IP-, X.25-, Frame Relay- oder ATM-Netzwerke gesendet werden sollen. Zurzeit ist nur L2TP über IP-Netzwerke definiert. Wenn L2TP-Frames über ein IP-Netzwerk gesendet werden, werden sie als UDP-Nachrichten (User Datagram Protocol) eingekapselt. L2TP kann als Tunnelprotokoll im Internet oder in privaten Intranets verwendet werden.

L2TP verwendet UDP-Nachrichten in IP-Netzwerken sowohl zur Tunnelverwaltung als auch für getunnelte Daten. Die Nutzlasten eingekapselter PPP-Frames können verschlüsselt und/oder komprimiert werden; Windows 2000-L2TP-Clients handeln die Verwendung von MPPE für L2TP-Verbindungen jedoch nicht aus. Die Verschlüsselung für L2TP-Verbindungen wird durch IPSec ESP bereitgestellt.

Es ist möglich, in Windows 2000 L2TP-Verbindungen zu erstellen, die nicht durch IPSec verschlüsselt werden. Dabei handelt es sich jedoch nicht um eine VPN-Verbindung, da die von L2TP eingekapselten privaten Daten nicht verschlüsselt sind. Nicht verschlüsselte L2TP-Verbindungen können vorübergehend für die Problembehandlung für eine L2TP-Verbindung über IPSec verwendet werden, da sie den IPSec-Authentifizierungs- und -Aushandlungsprozess umgehen.

L2TP geht davon aus, dass zwischen einem L2TP-Client (einem VPN-Client, der das L2TP-Tunnelprotokoll und IPSec verwendet) und einem L2TP-Server (einem VPN-Server, der das L2TP-Tunnelprotokoll und IPSec verwendet) ein IP-Netzwerk verfügbar ist. Der L2TP-Client ist möglicherweise bereits mit einem IP-Netzwerk verknüpft, das den L2TP-Server erreichen kann, oder der L2TP-Client muss sich möglicherweise, wie im Fall von DFÜ-Internetbenutzern, bei einem NAS einwählen, um die IP-Verbindung herzustellen.

Die während der Erstellung von L2TP-Tunneln auftretende Authentifizierung muss denselben Authentifizierungsmechanismus verwenden wie PPP-Verbindungen (beispielsweise EAP, MS-CHAP, CHAP, SPAP und PAP).

Bei internetbasierten L2TP-Servern ist der L2TP-Server ein L2TP-fähiger DFÜ-Server mit einer Schnittstelle im externen Netzwerk, dem Internet, und einer zweiten Schnittstelle im privaten Zielnetzwerk.

Die L2TP-Tunnelverwaltung und die getunnelten Daten weisen dieselbe Paketstruktur auf.

Tunnelverwaltung mit der L2TP-Steuerungsmeldungen

Im Gegensatz zu PPTP wird die L2TP-Tunnelverwaltung nicht über eine separate TCP-Verbindung durchgeführt. Der L2TP-Anrufssteuerungs- und -Verwaltungsverkehr wird in Form von UDP-Nachrichten zwischen dem L2TP-Client und dem L2TP-Server gesendet. In Windows 2000 verwenden der L2TP-Client und der L2TP-Server UDP-Port 1701.

Anmerkung Der L2TP-Client und der L2TP-Server in Windows 2000 verwenden immer UDP-Port 1701. Der Windows 2000-L2TP-Server unterstützt L2TP-Clients, die einen anderen UDP-Port als 1701 verwenden.

L2TP-Steuerungsmeldungen über IP werden als UDP-Datagramme gesendet. In der Windows 2000-Implementierung werden als UDP-Datagramme gesendete L2TP-Steuerungsmeldungen als die verschlüsselte Nutzlast von IPSec ESP gesendet (siehe Abbildung 9.11).

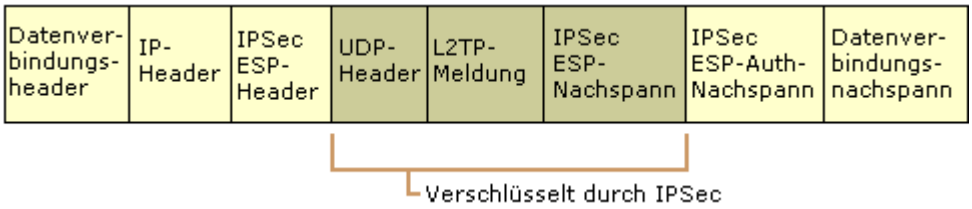

Abbildung 9.11: L2TP-Steuerungsmeldung

Da keine TCP-Verbindung verwendet wird, verwendet L2TP Nachrichtensequenzierung, um die Zustellung von L2TP-Nachrichten sicherzustellen. In der L2TP-Steuerungsmeldung werden die Felder "Next-Received" (entspricht dem TCP-Bestätigungsfeld) und "Next-Sent" (entspricht dem TCP-Sequenznummernfeld) verwendet, um die Sequenz der Steuerungsmeldungen zu verwalten. Pakete, die nicht in die Sequenz passen, werden gelöscht. Die Felder "Next-Sent" und "Next-Received" können auch für die sequenzielle Zustellung und Datenflusskontrolle für getunnelte Daten verwendet werden.

L2TP unterstützt mehrere Anrufe pro Tunnel. In der L2TP-Steuerungsmeldung und dem L2TP-Header für getunnelte Daten befindet sich eine Tunnelkennung, die den Tunnel identifiziert, und eine Anrufskennung, die einen Anruf innerhalb des Tunnels identifiziert.

Tabelle 9.6 enthält die wichtigsten L2TP-Steuerungsmeldungen.

Tabelle 9.6: L2TP-Steuerungsmeldungen

Meldungstyp	Zweck
Start-Control-Connection-Request	Wird vom L2TP-Client gesendet, um die Steuerungsverbindung herzustellen. Für jeden L2TP-Tunnel muss eine Steuerungsverbindung hergestellt werden, bevor andere L2TP-Meldungen ausgegeben werden können. Sie enthält eine Kennung für den zugewiesenen Tunnel, die verwendet wird, um den Tunnel zu identifizieren.
Start-Control-Connection-Reply	Wird vom L2TP-Server als Antwort auf die Meldung "Start-Control-Connection-Request" gesendet.
Start-Control-Connection-Connected	Wird als Antwort auf die Meldung "Start-Control-Connection-Reply" gesendet und weist darauf hin, dass der Tunnel erfolgreich aufgebaut wurde.
Outgoing-Call-Request	Wird vom L2TP-Client gesendet, um einen L2TP-Tunnel zu erstellen. Die Meldung Outgoing-Call-Request enthält eine Kennung für den zugewiesenen Anruf, die verwendet wird, um den Anruf in einem bestimmten Tunnel zu identifizieren.
Outgoing-Call-Reply	Wird vom L2TP-Server als Antwort auf die Meldung "Outgoing-Call-Request" gesendet.
Start-Control-Connection-Connected	Wird als Antwort auf eine erhaltene Meldung "Outgoing-Call-Reply" gesendet und weist darauf hin, dass der Anruf erfolgreich war.
Hello	Wird entweder vom L2TP-Client oder vom L2TP-Server als Keep-Alive-Mechanismus gesendet. Wenn die Meldung "Hello" nicht bestätigt wird, wird der L2TP-Tunnel schließlich beendet.
WAN-Error-Notify	Wird vom L2TP-Server an alle VPN-Clients gesendet, um auf Fehler an der PPP-Schnittstelle des L2TP-Servers hinzuweisen.
Set-Link-Info	Wird vom L2TP-Client oder vom L2TP-Server an festgelegte PPP-ausgehandelte Optionen gesendet.
Call-Disconnect-Notify	Wird entweder vom L2TP-Server oder vom L2TP-Client gesendet und gibt an, dass ein Anruf in einem Tunnel beendet werden soll.
Stop-Control-Connection-Notification	Wird entweder vom L2TP-Server oder vom L2TP-Client gesendet und gibt an, dass ein Tunnel beendet werden soll.

Die genaue Struktur von L2TP-Steuerungsmeldungen finden Sie im L2TP-Internet-Draft.

L2TP-Datentunneling

L2TP-Datentunneling wird über mehrere Einkapselungsstufen durchgeführt.

Abbildung 9.12 zeigt die sich ergebende Struktur der mit L2TP über IPSec getunnelten Daten.

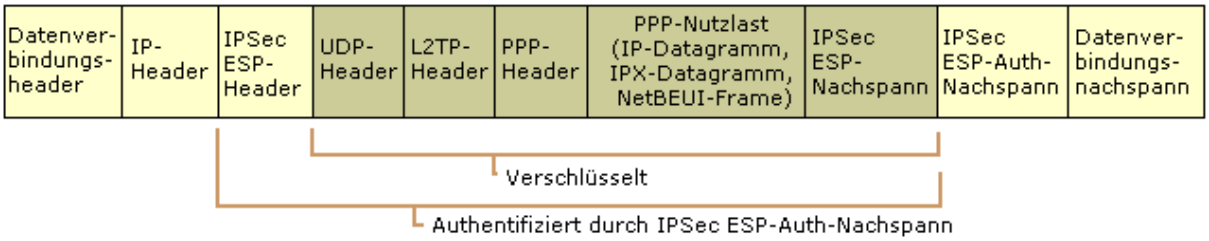

Abbildung 9.12: L2TP-Paketeinkapselung

L2TP-Einkapselung

Die anfängliche PPP-Nutzlast wird mit einem PPP-Header und einem L2TP-Header eingekapselt.

UDP-Einkapselung

Das mit L2TP eingekapselte Paket wird dann mit einem UDP-Header eingekapselt, in dem die Quell- und Zielports auf 1701 festgelegt sind.

IPSec-Einkapselung

Gemäß den IPSec-Richtlinien wird die UDP-Nachricht verschlüsselt und mit einem IPSec ESP-Header (Encapsulating Security Payload) und -Nachspann sowie einem IPSec Auth-Nachspann (Authentication) eingekapselt.

IP-Einkapselung

Das IPSec-Paket wird mit einem endgültigen IP-Header eingekapselt, der die IP-Quell- und -Zieladressen des VPN-Clients und des VPN-Servers enthält.

Datenverbindungsebenen-Verschlüsselung

Damit das IP-Datagramm über eine LAN- oder WAN-Verbindung gesendet werden kann, wird es schließlich mit einem Header und einem Nachspann für die Datenverbindungsebenen-Technologie der ausgehenden physischen Schnittstelle eingekapselt. Wenn IP-Datagramme beispielsweise über eine Ethernetschnittstelle gesendet werden, wird das IP-Datagramm mit einem Ethernet-Header und -Nachspann eingekapselt. Wenn IP-Datagramme über eine Punkt-zu-Punkt-WAN-Verbindung gesendet werden, beispielsweise eine analoge Telefonleitung oder ISDN, wird das IP-Datagramm mit einem PPP-Header und -Nachspann eingekapselt.

Entkapselung von mit L2TP über IPSec getunnelten Daten

Wenn der L2TP-Client oder L2TP-Server die mit L2TP über IPSec getunnelten Daten erhält, geht er folgendermaßen vor:

1. Er verarbeitet und entfernt den Datenverbindungsheader und den Datenverbindungsnachspann.
2. Er verarbeitet und entfernt den IP-Header.
3. Er verwendet den IPSec ESP Auth-Nachspann, um die IP-Nutzlast und den IPSec ESP-Header zu authentifizieren.
4. Er verwendet den IPSec ESP-Header, um den verschlüsselten Teil des Pakets zu entschlüsseln.

5. Er verarbeitet den UDP-Header und sendet das L2TP-Paket an L2TP.
6. L2TP verwendet die Tunnelkennung und die Anrufskennung im L2TP-Header, um den genauen L2TP-Tunnel zu identifizieren.
7. Er verwendet den PPP-Header, um die PPP-Nutzlast zu identifizieren und zur Verarbeitung an den entsprechenden Protokolltreiber weiterzuleiten.

L2TP über IPSec-Pakete und Windows 2000-Netzwerkarchitektur

Abbildung 9.13 zeigt den Pfad, den getunnelte Daten von einem VPN-Client über eine RAS-VPN-Verbindung mithilfe eines analogen Modems durch die Windows 2000-Netzwerkarchitektur verwenden. Die folgenden Schritte erläutern den Prozess:

1. Ein IP-Datagramm, IPX-Datagramm oder NetBEUI-Frame wird von seinem entsprechenden Protokoll an die virtuelle Schnittstelle gesendet, die die VPN-Verbindung darstellt.
2. NDIS sendet ein Paket an NDISWAN, das die Daten optional komprimiert und einen PPP-Header bereitstellt, der nur aus dem PPP-Protokollkennungsfeld besteht. Es werden keine Flags oder FCS-Felder hinzugefügt.
3. NDISWAN sendet den PPP-Frame an den L2TP-Protokolltreiber, der den PPP-Frame mit einem L2TP-Header einkapselt. Im L2TP-Header werden die Tunnelkennung und die Anrufskennung auf den geeigneten Wert festgelegt, der den Tunnel identifiziert.
4. Der L2TP-Protokolltreiber sendet dann das sich ergebende Paket an den TCP/IP-Protokolltreiber und weist ihn an, das L2TP-Paket als UDP-Nachricht mit den IP-Adressen des VPN-Clients und des VPN-Servers von UDP-Port 1701 an UDP-Port 1701 zu senden.
5. Der TCP/IP-Protokolltreiber erstellt ein IP-Paket mit dem entsprechenden IP-Header und UDP-Header. IPSec analysiert dann das IP-Paket und ordnet es einer aktuellen IPSec-Richtlinie zu. IPSec kapselt den UDP-Nachrichtenteil des IP-Pakets mit den entsprechenden ESP-Headern und -Nachspannen gemäß den Einstellungen in der Richtlinie ein und verschlüsselt ihn.

   Der ursprüngliche IP-Header, in dem das Protokollfeld auf 50 festgelegt ist, wird vorn am ESP-Paket hinzugefügt.

   Der TCP/IP-Protokolltreiber sendet dann mithilfe von NDIS das sich ergebende Paket an die Schnittstelle, die die DFÜ-Verbindung zum lokalen ISP darstellt.

6. NDIS sendet das Paket an NDISWAN.
7. NSIDWAN stellt PPP-Header und -Nachspanne bereit und sendet den sich ergebenden PPP-Frame an den entsprechenden WAN-Miniporttreiber, der die DFÜ-Hardware darstellt.

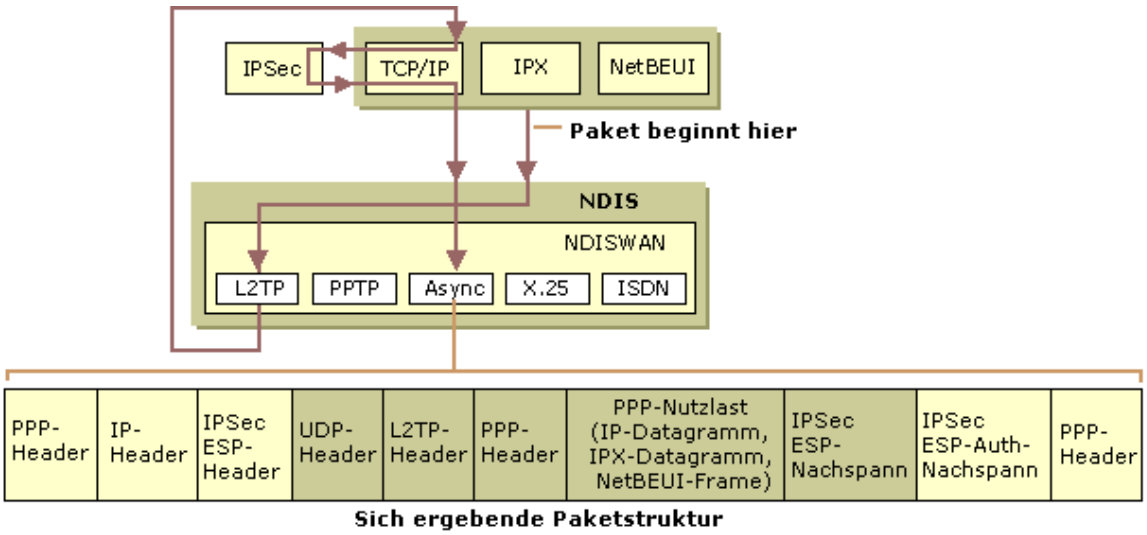

Abbildung 9.13: L2TP-Paketentwicklung

Anmerkung Es ist möglich, eine verschlüsselte PPP-Verbindung für die DFÜ-Verbindung mit einem ISP auszuhandeln. Es ist jedoch nicht nötig und nicht empfehlenswert, da die gesendeten privaten Daten, der getunnelte PPP-Frame, bereits mit IPSec verschlüsselt sind. Die zusätzliche Verschlüsselungsstufe wird nicht benötigt und kann die Leistung beeinträchtigen.

VPN-Sicherheit

Sicherheit ist ein wesentlicher Teil eines VPNs. In den folgenden Abschnitten werden die Sicherheitseinrichtungen von PPTP- und L2TP über IPSec-VPN-Verbindungen beschrieben.

PPTP-Verbindungen

PPTP bietet Benutzerauthentifizierung und Verschlüsselung.

Benutzerauthentifizierung mit PPP

Der Benutzer, der versucht, die VPN-Verbindung herzustellen, wird mithilfe von PPP-basierten Benutzerauthentifizierungsprotokollen, wie beispielsweise EAP, MS-CHAP, CHAP, SPAP und PAP, authentifiziert. Für PPTP-Verbindungen wird EAP-TLS mit Smartcards oder MS-CHAP, Version 2, empfohlen, da diese gegenseitige Authentifizierung bieten und es sich bei ihnen um die sichersten Methoden für den Austausch von Anmeldeinformationen handelt.

Verschlüsselung mit MPPE

PPTP erbt die MPPE-Verschlüsselung, die die Rivest-Shamir-Adleman (RSA) RC4-Streamverschlüsselung verwendet. MPPE ist nur verfügbar, wenn die Authentifizierungsprotokolle EAP-TLS oder MS-CHAP (Version 1 oder Version 2) verwendet werden.

MPPE kann 40-Bit-, 56-Bit- oder 128-Bit-Verschlüsselungsschlüssel verwenden. Der 40-Bit-Schlüssel bietet Abwärtskompabilität mit Nicht-Windows 2000-Clients. Standardmäßig wird während des Verbindungsherstellungsprozesses die höchste vom VPN-Client und vom VPN-Server unterstützte Schlüsselstärke ausgehandelt. Wenn der VPN-Server eine höhere Schlüsselstärke erfordert als der VPN-Client unterstützt, wird der Verbindungsversuch abgelehnt.

MPPE wurde ursprünglich für die Verschlüsselung über eine Punkt-zu-Punkt-Verbindung entwickelt, bei der Pakete in derselben Reihenfolge eintreffen, in der sie gesendet wurden, und bei der nur geringe Paketverluste auftreten. In dieser Umgebung hängt die Entschlüsselung der einzelnen Pakete von der Entschlüsselung des vorherigen Pakets ab.

Im Fall von VPNs jedoch können über das Internet gesendete IP-Datagramme in einer anderen Reihenfolge eintreffen als sie gesendet wurden. Dabei kann ein höherer Anteil der Pakete verloren gehen. MPPE wechselt daher bei VPN-Verbindungen für jedes Paket den Verschlüsselungsschlüssel. Die Entschlüsselung der einzelnen Pakete ist unabhängig vom vorherigen Paket. MPPE enthält eine Sequenznummer im MPPE-Header. Wenn Pakete verloren gehen oder in der falschen Reihenfolge eintreffen, werden die Verschlüsselungsschlüssel relativ zur Sequenznummer gewechselt.

PPTP-Paketfilterung

Ein PPTP-basierter VPN-Server weist normalerweise zwei physische Schnittstellen auf: eine Schnittstelle im freigegebenen oder öffentlichen Netzwerk wie dem Internet und die andere im privaten Intranet. Er verfügt außerdem über eine virtuelle Schnittstelle, die mit allen VPN-Clients verbunden ist. Damit der VPN-Server den Verkehr zwischen VPN-Clients weiterleitet, muss die IP-Weiterleitung auf allen Schnittstellen aktiviert sein. Das Aktivieren der Weiterleitung zwischen den beiden physischen Schnittstellen veranlasst jedoch den VPN-Server, den gesamten IP-Verkehr aus dem freigegebenen oder öffentlichen Netzwerk ins Intranet umzuleiten. Um das Intranet vor dem gesamten nicht über einen VPN-Client gesendeten Verkehr zu schützen, muss die PPTP-Paketfilterung so konfiguriert sein, dass der VPN-Server nur das Routing zwischen VPN-Clients und dem Intranet durchführt und nicht zwischen potenziell unberechtigten Benutzern im freigegebenen oder öffentlichen Netzwerk und im Intranet.

Die PPTP-Paketfilterung kann entweder auf dem VPN-Server oder auf einem zwischengeschalteten Firewall konfiguriert werden. Weitere Informationen finden Sie weiter unten in diesem Kapitel unter "VPNs und Firewalls".

L2TP über IPSec-Verbindungen

L2TP über IPSec bietet Benutzerauthentifizierung, gegenseitige Computerauthentifizierung, Verschlüsselung, Datenauthentifizierung und Datenintegrität.

Benutzerauthentifizierung mit L2TP über IPSec

Die Authentifizierung des VPN-Clients findet auf zwei verschiedenen Ebenen statt: Der Computer wird authentifiziert, und anschließend wird der Benutzer authentifiziert.

IPSec-Computerauthentifizierung

Die gegenseitige Computerauthentifizierung des VPN-Clients und des VPN-Servers wird durchgeführt, wenn Sie durch den Austausch von Computerzertifikaten eine IPSec ESP-Sicherheitszuordnung (Security Association, SA) einrichten. Es findet eine IPSec Phase I- und Phase II-Aushandlung statt, und es wird eine IPSec SA mit einem vereinbarten Verschlüsselungsalgorithmus, einem Hash-Algorithmus und Verschlüsselungsschlüsseln eingerichtet.

Damit L2TP über IPSec verwendet werden kann, muss sowohl auf dem VPN-Client als auch auf dem VPN-Server ein Computerzertifikat installiert sein. Sie können Computerzertifikate automatisch erhalten, indem Sie eine Windows 2000-Gruppenrichtlinie für automatische Einschreibung konfigurieren oder das Zertifikats-Snap-In manuell verwenden. Weitere Informationen finden Sie in der Windows 2000 Server-Hilfe.

L2TP-Authentifizierung auf Benutzerebene

Der Benutzer, der versucht, die L2TP-Verbindung herzustellen, wird mithilfe von PPP-basierten Benutzerauthentifizierungsprotokollen, wie beispielsweise EAP, MS-CHAP, CHAP, SPAP und PAP, authentifiziert. Da der PPP-Verbindungseinrichtungsprozess mit IPSec verschlüsselt wird, kann eine beliebige PPP-Authentifizierungsmethode verwendet werden. Eine gegenseitige Authentifizierung auf Benutzerebene findet statt, wenn Sie MS-CHAP v2 oder EAP-TLS verwenden.

L2TP-Tunnelauthentifizierung

L2TP bietet außerdem eine Möglichkeit, die Endpunkte eines L2TP-Tunnels während des Tunneleinrichtungsprozesses zu authentifizieren. Diese Methode wird L2TP-Tunnelauthentifizierung genannt. Windows 2000 führt standardmäßig keine L2TP-Tunnelauthentifizierung durch. Weitere Informationen zum Konfigurieren von Windows 2000 für die L2TP-Tunnelauthentifizierung finden Sie über die Microsoft Knowledge Base-Verknüpfung auf der Seite **Web Resources** unter http://www.microsoft.com/windows2000/techinfo/reskit/WebResources/default.asp (englischsprachig).

Verschlüsselung mit L2TP über IPSec

Die Verschlüsselung wird durch die Einrichtung der IPSec SA bestimmt. Folgende Verschlüsselungsalgorithmen sind verfügbar:

- DES mit einem 56-Bit-Schlüssel
- Dreifach-DES (3DES), verwendet 56-Bit-Schlüssel und wurde für Hochsicherheitsumgebungen entwickelt

Da IPSec für IP-Netzwerke entwickelt wurde, in denen Pakete verloren gehen und in der falschen Reihenfolge eintreffen konnten, wird jedes IPSec-Paket unabhängig von anderen IPSec-Paketen verschlüsselt.

Die anfänglichen Verschlüsselungsschlüssel werden vom IPSec-Authentifizierungsprozess abgeleitet. Bei mit DES verschlüsselten Verbindungen werden alle fünf Minuten oder jeweils nach der Übertragung von 250 Megabyte an Daten neue Verschlüsselungsschlüssel erzeugt. Bei mit 3DES verschlüsselten Verbindungen werden jede Stunde oder jeweils nach der Übertragung von 2 Gigabyte an Daten neue Verschlüsselungsschlüssel erzeugt. Bei mit AH geschützten Verbindungen werden jede Stunde oder jeweils nach der Übertragung von 2 Gigabyte an Daten neue Hash-Schlüssel erzeugt. Weitere Informationen zu IPSec finden Sie unter "Internet Protocol Security" im *TCP/IP Core Networking Guide*.

Datenauthentifizierung und -integrität mit L2TP über IPSec

Datenauthentifizierung und -integrität wird durch einen der folgenden Algorithmen bereitgestellt:

- den HMAC-MD5 (Hash Message Authentication Code, Message Digest 5), einen Hash-Algorithmus, der einen 128-Bit-Hash der authentifizierten Nutzlast erzeugt
- den HMAC-SHA (Secure Hash Algorithm), einen Hash-Algorithmus, der einen 160-Bit-Hash der authentifizierten Nutzlast erzeugt

L2TP über IPSec-Paketfilterung

Genau wie bei PPTP-basierten VPN-Verbindungen veranlasst das Aktivieren der Weiterleitung zwischen den Schnittstellen im öffentlichen oder freigegebenen Netzwerk und dem Intranet den VPN-Server, den gesamten IP-Verkehr vom freigegebenen oder öffentlichen Netzwerk an das Intranet umzuleiten. Um das Intranet vor dem gesamten nicht über einen VPN-Client gesendeten Verkehr zu schützen, müssen Sie die L2TP über IPSec-Paketfilterung so konfigurieren, dass der VPN-Server nur das Routing zwischen VPN-Clients und dem Intranet durchführt und nicht zwischen potenziell unberechtigten Benutzern im freigegebenen oder öffentlichen Netzwerk und im Intranet.

Die L2TP über IPSec-Paketfilterung kann entweder auf dem VPN-Server oder auf einem zwischengeschalteten Firewall konfiguriert werden. Weitere Informationen finden Sie weiter unten in diesem Kapitel unter "VPNs und Firewalls".

Adressierung und Routing für VPNs

Um die Funktionsweise von VPNs zu verstehen, müssen Sie wissen, wie Adressierung und Routing von der Erstellung von RAS-VPNs und Router-zu-Router-VPNs beeinflusst werden. Eine VPN-Verbindung erstellt eine virtuelle Schnittstelle, der eine entsprechende IP-Adresse zugewiesen werden muss. Außerdem müssen Routen geändert oder hinzugefügt werden, um sicherzustellen, dass der entsprechende Verkehr über die sichere VPN-Verbindung, anstatt über das freigegebene oder öffentliche Transitnetzwerk gesendet wird.

RAS-VPN-Verbindungen

Für RAS-VPN-Verbindungen erstellt ein Computer eine RAS-Verbindung zu einem VPN-Server. Während des Verbindungsprozesses weist der VPN-Server eine IP-Adresse für den RAS-VPN-Client zu und ändert die Standardroute auf dem Remoteclient so, dass der Standardroutenverkehr über die virtuelle Schnittstelle gesendet wird.

IP-Adressen und der DFÜ-VPN-Client

Für DFÜ-VPN-Clients, die eine Verbindung zum Internet herstellen, bevor sie eine VPN-Verbindung mit einem VPN-Server im Internet erstellen, werden zwei IP-Adressen zugewiesen:

- Beim Erstellen der PPP-Verbindung weist die IPCP-Aushandlung mit dem ISP-NAS eine öffentliche IP-Adresse zu.
- Beim Erstellen der PPP-Verbindung weist die IPCP-Aushandlung mit dem VPN-Server eine Intranet-IP-Adresse zu. Bei der vom VPN-Server zugewiesenen IP-Adresse kann es sich um eine öffentliche oder eine private IP-Adresse handeln, je nachdem, ob Ihre Organisation in ihrem Intranet öffentliche oder private Adressierung implementiert.

In jedem Fall muss die dem VPN-Client zugewiesene IP-Adresse für Hosts im Intranet erreichbar sein und umgekehrt. Die Routingtabelle des VPN-Servers muss entsprechende Einträge enthalten, damit alle Hosts im Intranet erreicht werden können, und die Routingtabellen der Router des Intranets müssen entsprechende Einträge enthalten, damit die VPN-Clients erreicht werden können.

Die durch das VPN gesendeten getunnelten Daten werden von der Adresse, die der VPN-Server dem VPN-Client zugewiesen hat, an eine Intranetadresse adressiert. Der äußere IP-Header wird zwischen der vom ISP zugewiesenen Adresse des VPN-Clients und der öffentlichen Adresse des VPN-Servers adressiert. Da die Router im Internet nur den äußeren IP-Header verarbeiten, leiten die Internetrouter die getunnelten Daten an die öffentliche IP-Adresse des VPN-Servers weiter.

Abbildung 9.14 zeigt ein Beispiel für DFÜ-Clientadressierung, in dem die Organisation private Adressen im Intranet verwendet und es sich bei den getunnelten Daten um ein IP-Datagramm handelt.

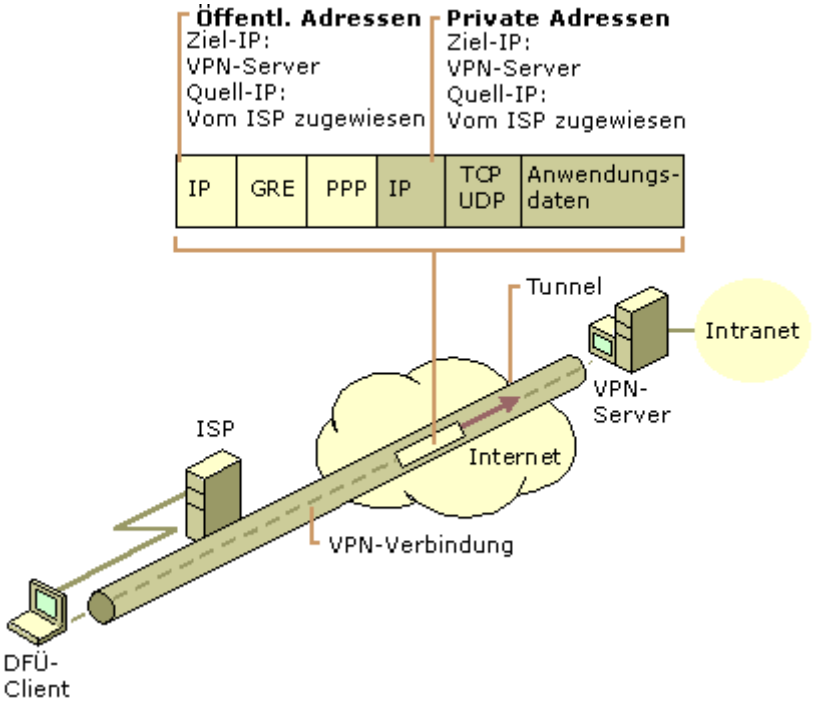

Abbildung 9.14: Öffentliche und private Adressen in mit PPTP getunnelten Daten

Standardrouten und DFÜ-Clients

Wenn ein typischer DFÜ-Client den ISP anwählt, empfängt er vom ISP-NAS eine öffentliche IP-Adresse. Im Rahmen des IPCP-Aushandlungsprozesses wird keine Standardgatewayadresse zugewiesen. Der DFÜ-Client muss daher, um alle Internetadressen zu erreichen, mithilfe der mit dem ISP verbundenen DFÜ-Schnittstelle eine Standardroute zu seiner Routingtabelle hinzufügen. Daraufhin kann der Client die IP-Datagramme an den ISP-NAS weiterleiten, von dem sie an seinen Standort im Internet umgeleitet werden.

Für DFÜ-Clients ohne andere TCP/IP-Schnittstellen ist dieses Verhalten erwünscht. Bei DFÜ-Clients, auf denen eine LAN-basierte Verbindung zu einem Intranet vorhanden ist, kann es jedoch zu Verwirrung führen. In diesem Szenario ist bereits eine Standardroute vorhanden, die auf den lokalen Intranetrouter zeigt. Wenn der DFÜ-Client eine Verbindung zu seinem ISP erstellt, bleibt die ursprüngliche Standardroute in der Routingtabelle, wird jedoch in einen höheren metrischen Wert geändert. Es wird eine neue Standardroute mit einem niedrigeren metrischen Wert hinzugefügt, die die ISP-Verbindung verwendet.

Als Ergebnis sind die Intranetstandorte, die sich nicht im direkt verknüpften Netzwerk des DFÜ-Clients befinden, während der Dauer der Verbindung zum ISP nicht erreichbar. Wenn die neue Standardroute nicht erstellt wird, sind alle Intranetstandorte erreichbar, Internetstandorte jedoch nicht.

Ein Windows 2000-basierter DFÜ-Client erstellt standardmäßig die Standardroute.

So verhindern Sie, dass die Standardroute erstellt wird

- Klicken Sie in den Eigenschaften des TCP/IP-Protokolls des DFÜ-Verbindungsobjekts im Dialogfeld **Erweiterte TCP/IP-Einstellungen** auf die Registerkarte **Allgemein**, und deaktivieren Sie das Kontrollkästchen **Standardgateway für das Remotenetzwerk verwenden**.

Wenn Sie Verbindungen sowohl zu Intranet- als auch zu Internetstandorten herstellen möchten, während die ISP-Verbindung aktiv ist, lassen Sie die Option **Standardgateway für das Remotenetzwerk verwenden** ausgewählt, und fügen Sie die Routen des Intranets zur Routingtabelle des DFÜ-Clients hinzu. Die Intranetrouten können mithilfe des Routenhilfsprogramms über statische persistente Routen hinzugefügt werden. Alternativ können Sie, wenn Routing Information Protocol (RIP), Version 1, als Intranetroutingprotokoll verwendet wird, den Routenüberwachungsdienst verwenden, um Routingprotokollverkehr der RIP-Version 1 abzufragen und Intranetrouten dynamisch hinzufügen. Während der Verbindung zum ISP sind alle Intranetstandorte über die Intranetrouten und alle Internetstandorte über die Standardroute erreichbar.

Standardrouten und VPNs über das Internet

Wenn der DFÜ-Client den ISP anruft, fügt er mithilfe der Verbindung zum ISP eine Standardroute hinzu (siehe Abbildung 9.15). Er kann jetzt über den Router am ISP-NAS alle Internetadressen erreichen.

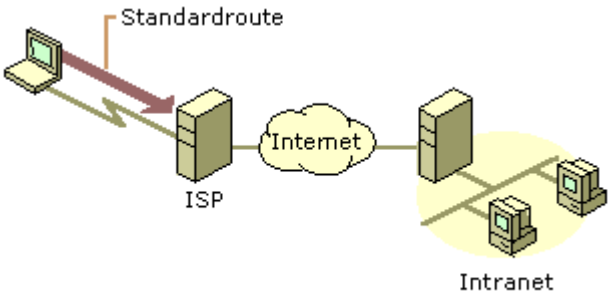

Abbildung 9.15: Beim Wählen eines ISPs erstellte Standardroute

Wenn der VPN-Client die VPN-Verbindung erstellt, werden eine weitere Standardroute und eine Hostroute zur IP-Adresse des Tunnelservers hinzugefügt (siehe Abbildung 9.16). Die vorherige Standardroute ist gespeichert, hat aber jetzt einen höheren metrischen Wert. Das Hinzufügen der neuen Standardroute bedeutet, dass alle Internetstandorte mit Ausnahme der IP-Adresse des Tunnelservers während der Dauer der VPN-Verbindung nicht erreichbar sind.

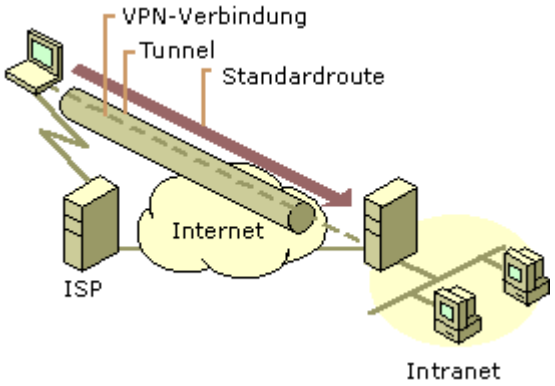

Abbildung 9.16: Beim Initiieren des VPNs erstellte Standardroute

Genau wie im Fall eines DFÜ-Clients, der eine Verbindung zum Internet herstellt, geschieht Folgendes, wenn ein DFÜ-VPN-Client, der Voluntary Tunneling verwendet, über das Internet eine VPN-Verbindung zu einem privaten Intranet erstellt:

- Wenn die VPN-Verbindung nicht aktiv ist, sind Internetstandorte erreichbar und Intranetstandorte nicht erreichbar,.
- Wenn die VPN-Verbindung aktiv ist, sind Internetstandorte erreichbar und Intranetstandorte nicht erreichbar,.

Bei den meisten mit dem Internet verbundenen VPN-Clients stellt dieses Verhalten kein Problem dar, da sie normalerweise entweder mit einer Intranet- oder Internetverbindung beschäftigt sind, jedoch nicht mit beiden.

Bei VPN-Clients, die gleichzeitigen Zugriff auf Intranet- und Internetressourcen wünschen, wenn das VPN verbunden ist, hängt die Lösung von der Art der IP-Adressierung im Intranet ab. Konfigurieren Sie in allen Fällen das VPN-Verbindungsobjekt so, dass es kein Standardgateway hinzufügt. Wenn die VPN-Verbindung erstellt ist, zeigt die Standardroute weiterhin auf den ISP-NAS und lässt den Zugriff auf alle Internetadressen zu.

Aktivieren Sie basierend auf dem Typ der verwendeten Intranetadressierung den gleichzeitigen Zugriff auf Intranet- und Internetressourcen folgendermaßen:

Öffentliche Adressen Fügen Sie statische persistente Routen für die öffentlichen Netzwerkkennungen des Intranets hinzu, und verwenden Sie dabei die IP-Adresse der virtuellen Schnittstelle des VPN-Servers als Gateway-IP-Adresse.

Private Adressen Fügen Sie statische persistente Routen für die privaten Netzwerkkennungen des Intranets hinzu, und verwenden Sie dabei die IP-Adresse der virtuellen Schnittstelle des VPN-Servers als Gateway-IP-Adresse.

Überlappende oder ungültige Adressen Wenn das Intranet überlappende oder ungültige Adressen (IP-Netzwerkkennungen, die nicht privat sind und nicht vom Internet Network Information Center [InterNIC] eingetragen oder von einem ISP erhalten wurden) verwendet, können diese IP-Adressen von öffentlichen Adressen im Internet dupliziert werden. Wenn auf dem VPN-Client statische persistente Routen für die überlappenden Netzwerkkennungen des Intranets hinzugefügt werden, sind die Standorte im Internet für die überlappenden Adressen nicht erreichbar.

In jedem dieser Fälle müssen dem VPN-Client statische persistente Routen für die Netzwerkkennungen des Intranets hinzugefügt werden. Wenn die persistenten Routen hinzugefügt werden, werden sie in der Registrierung gespeichert. Bei Windows NT 4.0, Service Pack 3 und höher, und bei Windows 2000 werden die persistenten Routen erst dann tatsächlich der IP-Routingtabelle hinzugefügt (und sind über den Befehl **route print** an der Windows 2000-Eingabeaufforderung sichtbar), wenn die IP-Adresse des Gateways erreichbar ist. Die IP-Adresse des Gateways wird erreichbar, wenn die VPN-Verbindung hergestellt wird.

Geben Sie für jede einzelne Route die folgende Routenhilfsprogrammsyntax an einer Windows 2000-Eingabeaufforderung ein:

```
ROUTE ADD <Intranetnetzwerkkennung> MASK <Netzmaske> <IP-Adresse der
virtuellen Schnittstelle des VPN-Servers> -p
```

Die Gateway-IP-Adresse in den Routenbefehlen für die einzelnen Intranetrouten entspricht der der virtuellen Schnittstelle des VPN-Servers zugewiesenen IP-Adresse, nicht der IP-Adresse der Internetschnittstelle des VPN-Servers.

Sie können die IP-Adresse der virtuellen Schnittstelle des VPN-Servers anhand der IP-Adresse der **internen** Schnittstelle unter **IP Routing** - **Allgemein** im Routing und RAS-Snap-In ermitteln. Wenn Sie DHCP verwenden, um IP-Adressen für DFÜ-Netzwerke und VPN-Clients zu erhalten, entspricht die IP-Adresse der virtuellen Schnittstelle des VPN-Servers der ersten IP-Adresse, die beim Anfordern von DHCP-Adressen erhalten wird. Wenn Sie einen statischen IP-Adresspool konfiguriert haben, entspricht die IP-Adresse der virtuellen Schnittstelle des VPN-Servers der ersten IP-Adresse im statischen IP-Adresspool. Sie können die IP-Adresse der virtuellen Schnittstelle des VPN-Servers auch ermitteln, indem Sie auf das VPN-Verbindungsobjekt doppelklicken, wenn die VPN-Verbindung aktiv ist. Klicken Sie im daraufhin angezeigten Dialogfeld **Status** auf die Registerkarte **Details**.

Vorsicht In allen diesen Fällen müssen Sie die Routen sehr sorgfältig hinzufügen, um sicherzustellen, dass der private Verkehr in das Intranet mithilfe der VPN-Verbindung und nicht mithilfe der PPP-Verbindung zum ISP weitergeleitet wird. Wenn die falschen Routen hinzugefügt werden, wird der Verkehr, den Sie in verschlüsselter Form über das VPN weiterleiten möchten, stattdessen unverschlüsselt über das Internet gesendet. Wenn Ihr Intranet beispielsweise die öffentliche Netzwerkkennung 207.46.130.0/24 (Subnetzmaske 255.255.255.0) verwendet und Sie versehentlich eine dauerhafte persistente Route für 207.46.131.0/24 hinzufügen, wird der gesamte Verkehr nicht verschlüsselt und über die VPN-Verbindung gesendet, sondern als Nur-Text über das Internet an das Intranetnetzwerk 207.46.130.0/24 weitergeleitet.

Router-zu-Router-VPN-Verbindungen

Für Router-zu-Router-VPN-Verbindungen handelt es sich bei der Routingschnittstelle, die für das Weiterleiten von Paketen verwendet wird, um eine folgendermaßen konfigurierte Schnittstelle für Wählen bei Bedarf:

- Geben Sie auf der Registerkarte **Allgemein** den Hostnamen oder die IP-Adresse des VPN-Servers ein.
- Wählen Sie auf der Registerkarte **Sicherheit** entweder **Kennwort und Daten verschlüsselt senden** oder **Benutzerdefiniert** aus. Wenn Sie **Benutzerdefiniert** auswählen, müssen Sie außerdem die entsprechenden Optionen für Verschlüsselung und Authentifizierung auswählen.
- Wählen Sie auf der Registerkarte **Netzwerk** den entsprechenden Servertyp und die Protokolle aus, die umgeleitet werden sollen. Wenn Sie den Servertyp auf **Automatisch** festlegen, wird erst versucht, eine L2TP über IPSec-Verbindung und dann eine PPTP-Verbindung herzustellen.
- Geben Sie unter **Anmeldeinformationen für die Schnittstelle** den Benutzernamen, das Kennwort und den Domänennamen ein, die zum Überprüfen des anrufenden Routers verwendet werden.

Die Erstellung der Schnittstellen für Wählen bei Bedarf wird durch den Assistenten für Wählen bei Bedarf automatisiert.

Die Namen der Schnittstellen für Wählen bei Bedarf und die Anmeldeinformationen des anrufenden Routers müssen möglicherweise gut aufeinander abgestimmt sein, um eine Router-zu-Router-VPN-Verbindung sicherzustellen. Weitere Informationen finden Sie in diesem Buch unter "Demand-Dial Routing".

Temporäre oder persistente Router-zu-Router-VPNs

Router-zu-Router-VPN-Verbindungen können entweder temporär oder persistent sein.

- Temporäre Router-zu-Router-VPN-Verbindungen werden erstellt, wenn Pakete über die VPN-Schnittstelle für Wählen bei Bedarf umgeleitet werden sollen, und werden nach einer angegebenen Leerlaufzeit beendet. Die Leerlaufzeit wird sowohl auf dem VPN-Client (dem anrufenden Router) als auch auf dem VPN-Server (dem angerufenen Router) konfiguriert. Die Standardleerlaufzeit für Schnittstellen für Wählen bei Bedarf auf dem VPN-Client ist unbegrenzt. Die Standardleerlaufzeit für VPN-Verbindungen auf dem VPN-Server beträgt 20 Minuten. Beide Leerlaufzeiten können konfiguriert werden. Verwenden Sie temporäre Router-zu-Router-VPN-Verbindungen für Zweigstellen, die DFÜ-Verbindungen zu ihren lokalen ISPs verwenden.
- Persistente Router-zu-Router-VPN-Verbindungen werden erstellt, wenn der Router gestartet wird, und bleiben unabhängig vom gesendeten Verkehr verbunden. Wenn die VPN-Verbindung beendet wird, wird automatisch versucht, sie wieder herzustellen. Verwenden Sie persistente Router-zu-Router-VPN-Verbindungen, um Büros zu verbinden, die permanente Verbindungen zum Internet verwenden.

So konfigurieren Sie entweder eine persistente oder temporäre Verbindung

1. Wählen Sie im Routing und RAS-Snap-In die Option **Routingschnittstellen** aus.
2. Klicken Sie mit der rechten Maustaste auf das Schnittstellenobjekt für Wählen bei Bedarf, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie auf der Registerkarte **Optionen** unter **Verbindungstyp** entweder **Wählen bei Bedarf** oder **Persistent** aus.

VPNs, die DFÜ-ISP-Verbindungen verwenden

Wenn sowohl der VPN-Server als auch der VPN-Client direkt über eine permanente WAN-Verbindung, wie beispielsweise T1 oder Frame Relay, mit dem Internet verbunden sind, kann die VPN-Verbindung persistent und 24 Stunden am Tag verfügbar sein. Wenn jedoch eine permanente WAN-Verbindung nicht möglich oder praktikabel ist, können Sie eine Router-zu-Router-VPN-Verbindung für Wählen bei Bedarf konfigurieren, die einen DFÜ-ISP verwendet.

Eine Router-zu-Router-VPN-Verbindung für Wählen bei Bedarf, die eine DFÜ-ISP-Verbindung verwendet, besteht aus den folgenden zwei Schnittstellen für Wählen bei Bedarf:

- einer Schnittstelle für Wählen bei Bedarf für die Einwahl bei einem lokalen ISP
- einer Schnittstelle für Wählen bei Bedarf für die Router-zu-Router-VPN-Verbindung

Eine Router-zu-Router-VPN-Verbindung bei Bedarf wird automatisch eingerichtet, wenn der Zweigstellenrouter Verkehr empfängt, der über die VPN-Verbindung weitergeleitet werden soll. Wenn der Zweigstellenrouter beispielsweise ein Paket empfängt, das an den Unternehmenshauptsitz umgeleitet werden soll, verwendet er zuerst eine DFÜ-Verbindung, um eine Verbindung zu einem lokalen ISP herzustellen. Wenn die Internetverbindung hergestellt ist, erstellt der Zweigstellenrouter, der VPN-Client, eine Router-zu-Router-VPN-Verbindung zum Unternehmenshauptsitzrouter, dem VPN-Server.

So konfigurieren Sie eine VPN-Verbindung für Wählen bei Bedarf auf dem Zweigstellenrouter

1. Erstellen Sie für die Internetverbindung eine Schnittstelle für Wählen bei Bedarf, die für die entsprechenden Geräte (ein Modem oder ISDN-Gerät), die Telefonnummer des lokalen ISPs und den Benutzernamen und das Kennwort für den Internetzugriff konfiguriert ist.
2. Erstellen Sie für die Router-zu-Router-VPN-Verbindung zum Unternehmenshauptsitzrouter eine Schnittstelle für Wählen bei Bedarf, die für PPTP oder L2TP, die IP-Adresse oder den Hostnamen der Schnittstelle des VPN-Servers des Unternehmenshauptsitzes im Internet und einen Benutzernamen und ein Kennwort, das vom VPN-Server überprüft werden kann, konfiguriert ist. Der Benutzername muss mit dem Namen der Schnittstelle für Wählen bei Bedarf auf dem VPN-Server des Unternehmenshauptsitzes übereinstimmen.

3. Erstellen Sie eine statische Hostroute für die IP-Adresse der Internetschnittstelle des VPN-Servers, die die Schnittstelle für Wählen bei Bedarf verwendet, die zur Einwahl beim lokalen ISP verwendet wird.
4. Erstellen Sie eine statische Route oder Routen für die IP-Netzwerkkennungen des Unternehmensintranets, das die VPN-Schnittstelle für Wählen bei Bedarf verwendet.

So konfigurieren Sie den Unternehmenshauptsitzrouter

1. Erstellen Sie eine Schnittstelle für Wählen bei Bedarf für die VPN-Verbindung mit der Zweigstelle, die für ein VPN-Gerät konfiguriert ist (PPTP oder L2TP-Port). Der Name der Schnittstelle für Wählen bei Bedarf muss dem Benutzernamen in den Authentifizierungsinformationen entsprechen, die vom Zweigstellenrouter zum Erstellen der VPN-Verbindung verwendet werden.
2. Erstellen Sie eine statische Route oder Routen für die IP-Netzwerkkennungen der Zweigstelle, die die VPN-Schnittstelle für Wählen bei Bedarf verwendet.

Die Router-zu-Router-VPN-Verbindung wird automatisch durch folgenden Prozess vom Zweigstellenrouter initiiert.

1. Pakete, die von einem Benutzer in der Zweigstelle an einen Standort im Unternehmenshubnetzwerk gesendet werden, werden vom Benutzer an den Zweigstellenrouter weitergeleitet.
2. Der Zweigstellenrouter überprüft seine Routingtabelle und findet eine Route zu der Netzwerkkennung des Unternehmensintranets, die die VPN-Schnittstelle für Wählen bei Bedarf verwendet.
3. Der Zweigstellenrouter überprüft den Status der VPN-Schnittstelle für Wählen bei Bedarf und stellt fest, dass sie sich in getrenntem Zustand befindet.
4. Der Zweigstellenrouter ruft die Konfiguration der VPN-Schnittstelle für Wählen bei Bedarf ab.
5. Der Zweigstellenrouter versucht auf Basis der Konfiguration der VPN-Schnittstelle für Wählen bei Bedarf, eine Router-zu-Router-VPN-Verbindung an der IP-Adresse des VPN-Servers im Internet zu initialisieren.
6. Um ein VPN einzurichten, muss entweder eine TCP-Verbindung (mithilfe von PPTP) oder eine IPSec-Aushandlung mit dem VPN-Server eingerichtet werden. Das VPN-Herstellungspaket wird erstellt.
7. Um das VPN-Herstellungspaket an den Unternehmenshauptsitzrouter weiterzuleiten, überprüft der Zweigstellenrouter seine Routingtabelle und findet die Hostroute, die die ISP-Schnittstelle für Wählen bei Bedarf verwendet.
8. Der Zweigstellenrouter überprüft den Status der ISP-Schnittstelle für Wählen bei Bedarf und stellt fest, dass sie sich in einem getrenntem Zustand befindet.
9. Der Zweigstellenrouter ruft die Konfiguration der ISP-Schnittstelle für Wählen bei Bedarf ab.
10. Basierend auf der Konfiguration der ISP-Schnittstelle für Wählen bei Bedarf verwendet der Zweigstellenrouter sein Modem oder seinen ISDN-Adapter, um seinen lokalen ISP anzuwählen und eine Verbindung zu ihm herzustellen.
11. Wenn die ISP-Verbindung hergestellt ist, wird das VPN-Herstellungspaket vom Zweigstellenrouter an den Unternehmenshauptsitzrouter gesendet.
12. Zwischen dem Zweigstellenrouter und dem Unternehmenshauptsitzrouter wird ein VPN ausgehandelt. Im Rahmen der Aushandlung sendet der Zweigstellenrouter Authentifizierungsinformationen, die vom Unternehmenshauptsitzrouter überprüft werden.
13. Der Unternehmenshauptsitzrouter überprüft seine Schnittstellen für Wählen bei Bedarf und findet eine, die mit dem während der Authentifizierung gesendeten Benutzernamen übereinstimmt und ändert die Schnittstelle in einen verbundenen Status.
14. Der Zweigstellenrouter leitet das Paket über das VPN weiter, und der VPN-Server leitet es an den entsprechenden Intranetstandort weiter.

Statisches oder dynamisches Routing

Wenn die Schnittstellen für Wählen bei Bedarf erstellt sind und die Wahl zwischen temporären und persistenten Verbindungen getroffen wurde, müssen Sie eine der folgenden Methoden für das Hinzufügen von Routinginformationen zur Routingtabelle wählen:

1. Für temporäre Verbindungen können Sie die für das Erreichen von Netzwerkkennungen in den anderen Büros geeigneten statischen Routen manuell hinzufügen. Die manuelle Konfiguration statischer Routen eignet sich für kleine Implementierungen mit wenigen Routen.
2. Für temporäre Verbindungen können Sie autostatische Aktualisierungen verwenden, um die statischen Routen, die über die Router-zu-Router-VPN-Verbindung verfügbar sind, automatisch zu aktualisieren.

Autostatische Routen eignen sich gut für größere Implementierungen mit einer großen Menge an Routinginformationen. Weitere Informationen zu autostatischen Aktualisierungen finden Sie in diesem Buch unter "Demand-Dial Routing".

3. Führen Sie für persistente Verbindungen die entsprechenden Routingprotokolle über die Router-zu-Router-VPN-Verbindung aus, und behandeln Sie dabei die VPN-Verbindung als Punkt-zu-Punkt-Verbindung.

Anmerkung Im Gegensatz zu Routing für Wählen bei Bedarf mithilfe von physischen Verbindungen können Sie eine für die VPN-Schnittstelle für Wählen bei Bedarf konfigurierte IP-Route nicht verwenden, um alle über das VPN verfügbaren Intranetrouten zusammenzufassen. Da der Router mit dem Internet verbunden ist, müssen Sie die Standardroute verwenden, um alle Routen des Internets zusammenzufassen, und sie so konfigurieren, dass sie die Internetschnittstelle verwendet.

Authentifizierung über vorinstallierten Schlüssel für Router-zu-Router-VPN-Verbindungen, die L2TP über IPSec verwenden

Standardmäßig sind sowohl der L2TP-Client als auch der L2TP-Server für Windows 2000 zertifikatbasierte IPSec-Authentifizierung vorkonfiguriert. Wenn Sie eine L2TP über IPSec-Verbindung herstellen, wird automatisch eine IPSec-Richtlinie erstellt, die angibt, dass der Internetschlüsselaustausch (Internet Key Exchange, IKE) während der Aushandlung der Sicherheitseinstellungen für L2TP zertifikatbasierte Authentifizierung verwendet. Dies bedeutet, dass sowohl auf dem L2TP-Client als auch auf dem L2TP-Server ein Computerzertifikat installiert sein muss, bevor eine erfolgreiche L2TP über IPSec-Verbindung hergestellt werden kann. Beide Computerzertifikate müssen entweder von derselben Zertifizierungsstelle (Certificate Authority, CA) stammen, oder das Stammzertifikat der CA jedes einzelnen Computers muss als vertraute Stammzertifizierungsstelle auf dem anderen Computer im Speicher für vertrauenswürdige Stammzertifikate installiert sein. Weitere Informationen zu IPSec finden Sie unter "Internet Protocol Security" im *TCP/IP Core Networking Guide*.

In manchen Fällen wird eine zertifikatbasierte IPSec-Authentifizierungsmethode für L2TP-basierte Router-zu-Router-VPN-Verbindungen nicht gewünscht. Dies kann beispielsweise der Fall sein, wenn es sich um eine kleine Organisation handelt und Sie keine Zertifikatinfrastruktur bereitstellen möchten oder Sie Verbindungen zu Routern herstellen, die keine zertifikatbasierte IPSec-Authentifizierung unterstützen. In diesen Fällen können Sie die IPSec-Richtlinie so konfigurieren, dass sie beim Erstellen von Router-zu-Router-VPN-Verbindungen vorinstallierte Schlüssel verwendet. Der vorinstallierte Authentifizierungsschlüssel fungiert als einfaches Kennwort in der IKE-Aushandlung. Wenn beide Seiten nachweisen können, dass sie dasselbe Kennwort kennen, dann vertrauen sie einander und fahren fort, indem sie private, symmetrische Verschlüsselungsschlüssel und spezielle Sicherheitseinstellungen für L2TP-Verkehr aushandeln.

Das Verwenden eines vorinstallierten IKE-Schlüssels gilt allgemein nicht als so sicher wie das Verwenden von Zertifikaten, da die IKE-Authentifizierung (und das implizite Vertrauen) nur von dem Schlüsselwert abhängt, der im Nur-Text-Format in der IPSec-Richtlinie gespeichert ist. Jeder, der die Richtlinie anzeigt, kann den Wert des vorinstallierten Schlüssels sehen. Wenn ein unberechtigter Benutzer den vorinstallierten Schlüssel anzeigt, kann er sein System so konfigurieren, dass es erfolgreich eine IPSec-Sicherheit mit Ihrem System herstellt. Die L2TP-Verbindung erfordert jedoch Authentifizierung auf Benutzerebene mithilfe eines PPP-Authentifizierungsprotokolls. Ein unberechtigter Benutzer müsste daher sowohl den vorinstallierten Schlüssel als auch die richtigen Benutzeranmeldeinformationen kennen, um die L2TP über IPSec-Verbindung erfolgreich herzustellen.

Um eine Authentifizierung über vorinstallierten Schlüssel für Router-zu-Router-VPN-Verbindungen durchzuführen, die L2TP über IPSec verwenden, müssen Sie eine Registrierungseinstellung ändern und dann die IPSec-Richtlinieneinstellungen konfigurieren.

Um zu verhindern, dass der Routing- und RAS-Dienst automatisch eine IPSec-Richtlinie für L2TP-Verkehr erstellt, legen Sie den Wert von **ProhibitIpSec** auf **1** (**HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RasMan \Parameters**) fest. **ProhibitIpSec** ist standardmäßig auf **0** festgelegt. Wenn **ProhibitIpSec** auf **1** festgelegt ist, werden die Verschlüsselungseinstellungen auf der auf dem anrufenden Router konfigurierten Schnittstelle für Wählen bei Bedarf zugunsten der Verschlüsselungseinstellungen der manuell konfigurierten IPSec-Richtlinie ignoriert. Der Computer muss neu gestartet werden, damit die Änderungen an dieser Registrierungseinstellung wirksam werden.

Wo Sie die IPSec-Einstellungen konfigurieren, hängt von folgenden Faktoren ab:

- Wenn es sich bei dem VPN-Server um einen alleinstehenden Server oder ein Mitglied einer Windows NT 4.0-Domäne handelt, müssen Sie eine IPSec-Richtlinie für den lokalen Computer konfigurieren.
- Wenn der VPN-Server Mitglied einer Windows 2000-Domäne ist, werden lokale IPSec-Richtlinien von zugewiesenen Domänen-IPSec-Richtlinien überschrieben. Um eine IPSec-Richtlinie zu erstellen, die nur auf den VPN-Server angewendet wird, erstellen Sie eine Organisationseinheit (Organizational Unit, OU) im Verzeichnisdienst Active Directory™, platzieren das VPN-Servercomputerkonto in der OU und verwenden die Gruppenrichtlinie, um IPSec-Richtlinien für die VPN-Server-OU zu erstellen und zuzuweisen. Die für die VPN-Server-OU erstellten IPSec-Richtlinien werden auf den VPN-Server übertragen.

Vor dem Erstellen einer IPSec-Richtlinie müssen Sie entscheiden, ob alle Standorte, die verbunden werden, denselben vorinstallierten Schlüssel verwenden oder ob jede einzelne Verbindung einen separaten vorinstallierten Schlüssel verwendet. Diese Entscheidung wirkt sich darauf aus, wie die IPSec-Filterlisten und -Richtlinien konfiguriert werden.

Wenn ein Administrator oder Unternehmen beide Endpunkte des L2TP-Tunnels steuert, kann derselbe vorinstallierte Schlüssel verwendet werden.

Verschiedene vorinstallierte Schlüssel können verwendet werden, wenn L2TP-Tunnel zwischen Systemen konfiguriert werden, die nicht derselben Verwaltungs- oder Unternehmenssicherheitskontrolle unterliegen. Beispielsweise kann ein Windows 2000-VPN-Server so konfiguriert werden, dass er mit sechs verschiedenen Geschäftspartnern kommuniziert, von denen jeder einen anderen vorinstallierten IKE-Schlüssel für L2TP-Verbindungen benötigt.

Die folgenden Abschnitte erörtern als Beispiel die IPSec-Konfiguration, die für einen Router erforderlich ist, der L2TP über IPSec-Authentifizierung über vorinstallierten Schlüssel für Router-zu-Router-VPN-Verbindungen zwischen einem Unternehmenshubbüro in New York und zwei Zweigstellen, einer in Boston und einer in London, verwendet.

Anmerkung Wenn Sie einen Windows 2000-VPN-Server haben, der mit anderen L2TP-Clients oder Servern mithilfe der zertifikatbasierten Standard-IPSec-Authentifizierung kommuniziert, und Sie für einen L2TP/IPSec-Tunnel IPSec-Authentifizierung über vorinstallierten Schlüssel verwenden möchten, dann müssen Sie für die Systeme, die bereits Zertifikatauthentifizierung verwenden, Regeln für die Verwendung von Zertifikatauthentifizierung sowie eine Regel für die Authentifizierung über vorinstallierten Schlüssel in dieselbe IPSec-Richtlinie aufnehmen.

Derselbe vorinstallierte Schlüssel für alle Verbindungen

Um denselben vorinstallierten Schlüssel für alle Router-zu-Router-VPN-Verbindungen zu verwenden, die L2TP über IPSec verwenden, nehmen Sie folgende Konfigurationen vor:

1. Erstellen Sie mithilfe des Routing und RAS-Snap-Ins die entsprechenden Schnittstellen für Wählen bei Bedarf. Erstellen Sie in unserem Beispiel eine Schnittstelle für Wählen bei Bedarf für die Verbindung zur Zweigstelle in Boston und eine Schnittstelle für Wählen bei Bedarf zur Zweigstelle in London.
2. Erstellen Sie mithilfe des IP-Sicherheitsrichtlinien-Snap-Ins eine IPSec-Filteraktion, die keine unsichere L2TP-Kommunikation zulässt.
3. Erstellen Sie eine IPSec-Filterliste, die Filter für alle L2TP über IPSec-Verbindungen enthält, die denselben Wert für den vorinstallierten IKE-Authentifizierungsschlüssel verwenden. Jeder Filter in der Filterliste gehört zu einem bestimmten Standort. In unserem Beispiel würden Sie eine Filterliste mit zwei Filtern konfigurieren, einem, der den L2TP-Verkehr zum Router in Boston definiert, und einem der den L2TP-Verkehr zum Router in London definiert.
4. Erstellen Sie eine neue IPSec-Richtlinie, die eine einzige aktive Regel verwendet, eine Regel, die die Filteraktion, die keine unsichere L2TP-Kommunikation zulässt, die Filterliste für alle L2TP über IPSec-Verbindungen und einen vorinstallierten Schlüssel als Authentifizierungsmethode verwendet.

Erstellen der Filteraktion

Um eine Filteraktion zu erstellen, die keine unsichere L2TP-Kommunikation zulässt, erstellen Sie eine Filteraktion mit folgenden Eigenschaften:

Auf der Registerkarte **Allgemein**:

- Name: L2TP schützen (Beispiel)
- Beschreibung: Erfordert eingehende Aushandlung. Verwirft eingehenden Klartext. Erzwingt ausgehende Aushandlung. (Beispiel)

Auf der Registerkarte **Sicherheitsmethoden**:

- Wählen Sie **Sicherheit aushandeln**, und fügen Sie mindestens den Typ **Hoch** zur Liste hinzu. Fügen Sie nach Bedarf weitere Typen hinzu.
- Deaktivieren Sie die Kontrollkästchen **Unsichere Kommunikation annehmen, aber immer mit IPSec antworten.** und **Unsichere Kommunikation mit Computern zulassen, die IPSec nicht unterstützen**. Aktivieren Sie bei Bedarf das Kontrollkästchen **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)**.

Das hier erörterte Beispiel verwendet für alle Ziele dieselbe Verschlüsselungsstärke. Möglicherweise müssen Sie jedoch, abhängig von den IPSec-Sicherheitsfunktionen des Remotesystems, für ein Ziel spezielle Filteraktionen erstellen. Eine Filteraktion für Boston erfordert möglicherweise nur 3DES-Verschlüsselung, wohingegen eine Filteraktion für London aufgrund von Exportbeschränkungen für Kryptografie möglicherweise nur DES erfordert. Um sowohl 3DES als auch DES in derselben Filteraktion zu verwenden, nehmen Sie beide in die Sicherheitsmethodenliste der Filteraktion auf, und setzen Sie dabei 3DES an die erste Stelle, um sicherzustellen, dass es nach Möglichkeit zuerst ausgewählt wird.

Erstellen der Filterliste für denselben vorinstallierten Schlüssel für alle Verbindungen

Um eine Filterliste zu konfigurieren, die alle L2TP-basierten Router-zu-Router-VPN-Verbindungen enthält, erstellen Sie eine Filterliste mit folgenden Eigenschaften:

- Name: L2TP-Verbindungen (Beispiel)
- Beschreibung: Ziele für L2TP-Verbindungen mit vorinstalliertem Schlüssel (Beispiel)

Erstellen Sie dann für jedes Ziel innerhalb des Filters einen Filter mit der folgenden Konfiguration:

Auf der Registerkarte **Adressierung**:

- Wählen Sie unter **Quelladresse** die Option **Spezielle IP-Adresse** aus, und geben Sie die IP-Adresse einer Internetschnittstelle des lokalen Routers ein. Geben Sie in unserem Beispiel die IP-Adresse der Internetschnittstelle des Routers in New York ein.
- Wählen Sie unter **Zieladresse** die Option **Spezielle IP-Adresse** aus, und geben Sie die IP-Adresse einer Internetschnittstelle des Routers am anderen Ende dieser Router-zu-Router-VPN-Verbindung ein. Geben Sie in unserem Beispiel für die Boston-Verbindung die IP-Adresse der Internetschnittstelle des Routers in Boston ein.
- Wählen Sie **Gespiegelt** aus.

Auf der Registerkarte **Protokoll**:

- Wählen Sie unter **Wählen Sie einen Protokolltyp:** die Option **UDP** aus.
- Wählen Sie unter **Legen Sie den Port des IP-Protokolls fest:** die Option **Von diesem Port** aus, geben Sie **1701** ein, und wählen Sie dann **Zu diesem Port** aus.

Auf der Registerkarte **Beschreibung**:

- Geben Sie unter **Beschreibung** eine Beschreibung dieses Filters ein, die seinen Verbindungsendpunkt beschreibt. Geben Sie beispielsweise für die bei Bedarf herzustellende Wählverbindung in Boston die folgende Beschreibung ein: "L2TP nach Boston". Diese Beschreibung wird im IPSec-Überwachungsdienstprogramm angezeigt.

Konfigurieren einer IPSec-Richtlinie für denselben vorinstallierten Schlüssel

Um eine IPSec-Richtlinie zu konfigurieren, die denselben vorinstallierten Schlüssel für alle auf L2TP über IPSec basierenden Router-zu-Router-VPN-Verbindungen verwendet, erstellen Sie eine IPSec-Richtlinie mit den folgenden Eigenschaften:

Auf der Registerkarte **Allgemein**:

- Name: L2TP-Verbindungen mit vorinstalliertem Schlüssel (Beispiel)
- Beschreibung: IPSec-Authentifizierung über vorinstallierten Schlüssel für Router-zu-Router-VPN-Verbindungen, die L2TP über IPSec verwenden (Beispiel)
- Ändern Sie die Einstellungen **Auf neue Richtlinien überprüfen, alle:** und **Erweitert** nach Bedarf.

Auf der Registerkarte **Regeln**:

- Deaktivieren Sie die **Standardantwortregel**.

Fügen Sie eine Regel mit den folgenden Eigenschaften hinzu:

Auf der Registerkarte **IP-Filterliste**:

- Wählen Sie die IP-Filterliste aus, die allen L2TP-Verbindungen zu allen Zweigstellen entspricht. Wählen Sie für unser Beispiel die IP-Filterliste namens **L2TP-Verbindungen** aus.

Auf der Registerkarte **Filteraktion**:

- Wählen Sie die Filteraktion aus, die keine unsichere L2TP-Kommunikation zulässt. Wählen Sie für unser Beispiel die Filteraktion namens **L2TP schützen** aus.

Auf der Registerkarte **Authentifizierungsmethoden**:

- Konfigurieren Sie unter **Reihenfolge der Authentifizierungsmethoden:** eine einzige Methode, die den vorinstallierten Schlüssel verwendet. Geben Sie den vorinstallierten Schlüssel ein, den alle Router, zu denen dieser Router eine L2TP über IPSec-Verbindung mit vorinstalliertem Schlüssel herstellt, gemeinsam haben. Wählen Sie beim Konfigurieren eines vorinstallierten Schlüssels einen Schlüssel aus, der mindestens 20 Zeichen lang ist und eine zufällige Mischung aus Groß- und Kleinbuchstaben, Zahlen und Interpunktionszeichen verwendet.

Auf der Registerkarte **Tunneleinstellungen**:

- Wählen Sie **Diese Regel spezifiziert keinen IPSec-Tunnel** aus.

Auf der Registerkarte **Verbindungstyp**:

- Wählen Sie **Alle Netzwerkverbindungen** aus.

Da die Filterliste alle Ziele für L2TP-basierte Router-zu-Router-VPN-Verbindungen enthält, ist innerhalb der IPSec-Richtlinie nur eine einzige Regel erforderlich.

Verschiedene vorinstallierte Schlüssel für verschiedene Verbindungen

Um verschiedene vorinstallierte Schlüssel für alle Router-zu-Router-VPN-Verbindungen zu verwenden, die L2TP über IPSec verwenden, nehmen Sie folgende Konfigurationen vor:

1. Erstellen Sie die entsprechenden Schnittstellen für Wählen bei Bedarf. Erstellen Sie in unserem Beispiel eine Schnittstelle für Wählen bei Bedarf für die Verbindung zur Zweigstelle in Boston und eine Schnittstelle für Wählen bei Bedarf zur Zweigstelle in London.
2. Erstellen Sie eine Filteraktion, die keine unsichere L2TP-Kommunikation zulässt.
3. Erstellen Sie eine IPSec-Filterliste, die einen einzigen Filter für die L2TP über IPSec-Verbindung zu einem bestimmten Standort enthält. Konfigurieren Sie in unserem Beispiel eine Filterliste mit einem Filter, der den L2TP-Verkehr zum Router in Boston definiert. Konfigurieren Sie dann eine weitere Filterliste mit einem Filter, der den L2TP-Verkehr zum Router in London definiert.
4. Erstellen Sie eine neue IPSec-Richtlinie, die eine Reihe von Regeln verwendet; jede Regel verwendet die Filteraktion, die keine unsichere L2TP-Kommunikation zulässt, die Filterliste für eine bestimmte L2TP über IPSec-Verbindung und den vorinstallierten Schlüssel als Authentifizierungsmethode.

Erstellen der Filteraktion

Die Konfiguration der Filteraktion für die verschiedenen vorinstallierten Schlüssel für verschiedene Verbindungen entspricht der Filteraktion für denselben vorinstallierten Schlüssel für alle Verbindungen.

Erstellen der Filterliste für verschiedene vorinstallierte Schlüssel für alle Verbindungen

Um eine Filterliste für eine bestimmte Router-zu-Router-VPN-Verbindung zu konfigurieren, erstellen Sie eine Filterliste mit folgenden Eigenschaften (am Beispiel der Verbindung nach Boston):

- Name: L2TP-Verbindung mit vorinstalliertem Schlüssel nach Boston (Beispiel)
- Beschreibung: Ziel in Boston für L2TP-Verbindung mit vorinstalliertem Schlüssel (Beispiel)

Erstellen Sie dann einen einzigen Filter mit der folgenden Konfiguration:

Auf der Registerkarte **Adressierung**:

- Wählen Sie unter **Quelladresse** die Option **Spezielle IP-Adresse** aus, und geben Sie die IP-Adresse einer Internetschnittstelle des lokalen Routers ein. Geben Sie in unserem Beispiel die IP-Adresse der Internetschnittstelle des Routers in New York ein.
- Wählen Sie unter **Zieladresse** die Option **Spezielle IP-Adresse** aus, und geben Sie die IP-Adresse einer Internetschnittstelle des Routers am anderen Ende dieser Router-zu-Router-VPN-Verbindung ein. Geben Sie in unserem Beispiel die IP-Adresse der Internetschnittstelle des Routers in Boston ein.
- Wählen Sie **Gespiegelt** aus.

Auf der Registerkarte **Protokoll**:

- Wählen Sie einen Protokolltyp: Wählen Sie **UDP** aus.
- Legen Sie den Port des IP-Protokolls fest: Wählen Sie **Von diesem Port**, geben Sie **1701** ein, und wählen Sie dann **Zu diesem Port** aus.

Auf der Registerkarte **Beschreibung**:

- Geben Sie unter **Beschreibung** eine Beschreibung dieses Filters ein, die den Verbindungsendpunkt beschreibt. Geben Sie beispielsweise für die bei Bedarf herzustellende Wählverbindung nach Boston die folgende Beschreibung ein: "L2TP nach Boston". Diese Beschreibung wird im IPSec-Überwachungsdienstprogramm angezeigt.

Wiederholen Sie dieses Verfahren für jede einzelne Router-zu-Router-VPN-Verbindung, die L2TP über IPSec verwendet. Konfigurieren Sie für unser Beispiel eine weitere IPSec-Filterliste für die Verbindung zum Router in London.

Konfigurieren einer IPSec-Richtlinie für verschiedene vorinstallierte Schlüssel für die einzelnen Verbindungen

Um eine IPSec-Richtlinie zu konfigurieren, die verschiedene vorinstallierte Schlüssel für die einzelnen auf L2TP basierenden Router-zu-Router-VPN-Verbindungen verwendet, erstellen Sie eine IPSec-Richtlinie mit den folgenden Eigenschaften:

Auf der Registerkarte **Allgemein**:

- Name: L2TP-Verbindungen mit vorinstalliertem Schlüssel (Beispiel)
- Beschreibung: IPSec-Authentifizierung über vorinstallierten Schlüssel für Router-zu-Router-VPN-Verbindungen, die L2TP über IPSec verwenden (Beispiel)
- Ändern Sie die Einstellungen **Auf neue Richtlinien überprüfen, alle:** und **Erweitert** nach Bedarf.

Auf der Registerkarte **Regeln**:

- Deaktivieren Sie die **Standardantwortregel**.

Fügen Sie für jede einzelne Router-zu-Router-VPN-Verbindung, die L2TP verwendet, eine Regel mit folgenden Eigenschaften hinzu (am Beispiel der Verbindung nach Boston):

Auf der Registerkarte **IP-Filterliste**:

- Wählen Sie die IP-Filterliste aus, die einer L2TP über IPSec-Verbindung entspricht. Wählen Sie für unser Beispiel die IP-Filterliste namens **L2TP-Verbindung mit vorinstalliertem Schlüssel nach Boston** aus.

Auf der Registerkarte **Filteraktion**:

- Wählen Sie die Filteraktion aus, die keine unsichere L2TP-Kommunikation zulässt. In unserem Beispiel würden Sie die Filteraktion namens **L2TP schützen** auswählen.

Auf der Registerkarte **Authentifizierungsmethoden**:

- Konfigurieren Sie unter **Reihenfolge der Authentifizierungsmethoden:** eine einzige Methode, die den vorinstallierten Schlüssel verwendet. Geben Sie den vorinstallierten Schlüssel ein, den die beiden Router in dieser Router-zu-Router-VPN-Verbindung gemeinsam haben. Geben Sie für unser Beispiel den vorinstallierten Schlüssel ein, den die Router in New York und Boston für die VPN-Verbindung von New York nach Boston verwenden. Wählen Sie beim Konfigurieren eines vorinstallierten Schlüssels einen Schlüssel aus, der mindestens 20 Zeichen lang ist und eine zufällige Mischung aus Groß- und Kleinbuchstaben, Zahlen und Interpunktionszeichen verwendet.

Auf der Registerkarte **Tunneleinstellungen**:

- Wählen Sie **Diese Regel spezifiziert keinen IPSec-Tunnel** aus.

Auf der Registerkarte **Verbindungstyp**:

- Wählen Sie **Alle Netzwerkverbindungen** aus.

Fügen Sie für jede einzelne Router-zu-Router-VPN-Verbindung, die L2TP über IPSec verwendet, eine separate Regel hinzu. Fügen Sie für unser Beispiel eine weitere Regel für die Verbindung zum Router in London hinzu.

Anmerkung Für eine eingehende L2TP über IPSec-Verbindung fragt der Routing- und RAS-Dienst IPSec ab, um den ausgehandelten Verschlüsselungstyp festzustellen. Die Abfrage bezieht sich auf die für eine IPSec-Sicherheitszuordnung (Security Association, SA) für IP-Verkehr zu UDP-Port 1701 verwendete Verschlüsselung. Wenn eine IPSec-SA für IP-Verkehr zu UDP-Port 1701 vorhanden ist, wird der für die IPSec-SA verwendete Verschlüsselungstyp zurückgegeben. Wenn **ProhibitIpSec** auf **0** festgelegt ist, wird immer eine IPSec-SA für diesen Verkehrstyp gefunden, da L2TP-Verkehrsfilter automatisch vom Routing- und RAS-Dienst erstellt werden. Der Verschlüsselungstyp wird dann mit den durch die Profileinstellungen der entsprechenden RAS-Richtlinie für die L2TP-Verbindung erlaubten Verschlüsselungstypen verglichen. Wenn der von der IPSec-Abfrage zurückgegebene Verschlüsselungstyp nicht mit den erlaubten Verschlüsselungsstärken im RAS-Richtlinienprofil übereinstimmt, wird der Verbindungsversuch abgelehnt. Wenn **ProhibitIpSec** auf **1** festgelegt ist und kein spezieller Filter für UDP-Port 1701 konfiguriert ist, findet die Abfrage keine SA für IP-Verkehr zu UDP-Port 1701, und es wird davon ausgegangen, dass keine Verschlüsselung vorliegt. Dies kann dazu führen, dass der Verbindungsversuch abgelehnt wird, wenn in der Verschlüsselungseinstellung im entsprechenden RAS-Richtlinienprofil die Einstellung **Keine Verschlüsselung** deaktiviert ist. Daher kann die Trennung verschlüsselter L2TP über IPSec-Verbindungen eintreten, wenn ein IPSec-Filter vorhanden ist, der den vorinstallierten Schlüssel für den gesamten IP-Verkehr verwendet, und kein spezieller Filter für UDP-Port 1701 konfiguriert ist.

Verwenden von IPSecPol zum Erstellen der IPSec-Richtlinie

IPSec-Richtlinien für L2TP über IPSec-Verbindungen mit vorinstalliertem Schlüssel können auch mithilfe des Resource Kit-Tools IPSecPol konfiguriert werden. Weitere Informationen finden Sie in der Hilfe zu den Windows 2000 Resource Kit-Tools.

VPNs und Firewalls

Ein Firewall verwendet Paketfilterung, um den Fluss sehr spezieller Netzwerkverkehrstypen zuzulassen oder nicht zuzulassen. IP-Paketfilterung bietet Ihnen eine Möglichkeit, genau zu definieren, welcher IP-Verkehr den Firewall durchqueren darf. IP-Paketfilterung ist wichtig, wenn Sie private Intranets mit öffentlichen Netzwerken wie dem Internet verbinden.

VPN-Server und Firewallkonfigurationen

Es gibt zwei Ansätze zum Verwenden eines Firewalls mit einem VPN-Server:

- Der VPN-Server ist mit dem Internet verknüpft, und der Firewall befindet sich zwischen dem VPN-Server und dem Intranet.
- Der Firewall ist mit dem Internet verknüpft, und der VPN-Server befindet sich zwischen dem Firewall und dem Intranet.

VPN-Server vor dem Firewall

Wenn der VPN-Server, wie in Abbildung 9.17 gezeigt, sich vor dem mit dem Internet verknüpften Firewall befindet, müssen Sie Paketfilter zu der Internetschnittstelle hinzufügen, die nur VPN-Verkehr zu und von der IP-Adresse der Schnittstelle des VPN-Servers im Internet zulassen.

Für eingehenden Verkehr werden die getunnelten Daten, wenn sie vom VPN-Server entschlüsselt werden, an den Firewall weitergeleitet, der seine Filter anwendet, um zuzulassen, dass der Verkehr an Intranetressourcen weitergeleitet wird. Da der einzige Verkehr, der den VPN-Server durchquert, von authentifizierten VPN-Clients erzeugt wird, kann Firewallfilterung in diesem Szenario verwendet werden, um zu verhindern, dass VPN-Benutzer auf bestimmte Intranetressourcen zugreifen.

Da der einzige im Intranet zugelassene Internetverkehr durch den VPN-Server verlaufen muss, verhindert dieser Ansatz außerdem die Freigabe von FTP-Ressourcen (File Transfer Protocol) oder Webintranetressourcen für Nicht-VPN-Internetbenutzer.

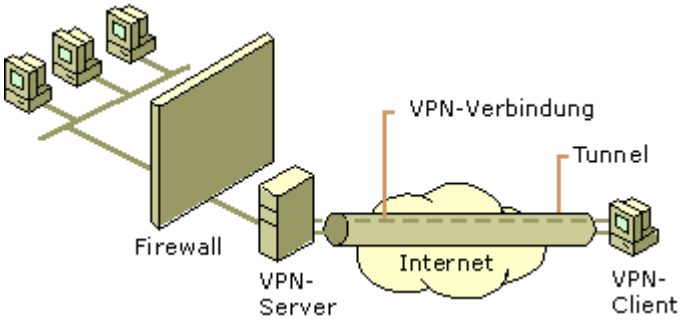

Abbildung 9.17: VPN-Server im Internet vor dem Firewall

Konfigurieren Sie für die Internetschnittstelle auf dem VPN-Server mithilfe des RAS-Snap-Ins die folgenden Eingabe- und Ausgabefilter.

PPTP-Paketfilter

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 (0x06BB).
- Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom PPTP-Client zum PPTP-Server zu.
- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokollkennung 47 (0x2F).
- Dieser Filter lässt mit PPTP getunnelte Daten vom PPTP-Client zum PPTP-Server zu.
- Ziel-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Quellport [eingerichtet] 1723 (0x06BB).
- Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wenn Sie **TCP [eingerichtet]** auswählen, wird nur dann Verkehr akzeptiert, wenn der VPN-Server die TCP-Verbindung initiiert hat.

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 (0x06BB).

  Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom VPN-Server zum VPN-Client zu.

- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokollkennung 47 (0x2F).

  Dieser Filter lässt mit PPTP getunnelte Daten vom VPN-Server zum VPN-Client zu.

- Quell-IP-Adresse der Internetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Zielport [eingerichtet] 1723 (0x06BB).

  Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wenn Sie **TCP [eingerichtet]** auswählen, wird nur dann Verkehr gesendet, wenn der VPN-Server die TCP-Verbindung initiiert hat.

Paketfilter für L2TP über 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 (0x01F4).

  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 (0x6A5).

  Dieser Filter lässt L2TP-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 (0x01F4).

  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 (0x6A5).

  Dieser Filter lässt L2TP-Verkehr vom VPN-Server zum VPN-Client zu.

Für IPSec ESP-Verkehr für das IP-Protokoll 50 sind keine Filter erforderlich. Die Routing- und RAS-Dienstfilter werden angewendet, nachdem das IPSec-Modul von TCP/IP den ESP-Header entfernt hat.

VPN-Server hinter dem Firewall

In einer gebräuchlicheren Konfiguration (siehe Abbildung 9.18) ist der Firewall mit dem Internet verbunden, und der VPN-Server ist eine weitere Intranetressource, die mit einer entmilitarisierten Zone (Demilitarized Zone, DMZ) verbunden ist. Die DMZ ist ein IP-Netzwerksegment, das normalerweise für Internetbenutzer verfügbare Ressourcen, wie beispielsweise Webserver und FTP-Server, enthält. Der VPN-Server hat eine Schnittstelle in der DMZ und eine Schnittstelle im Intranet.

Bei diesem Ansatz muss der Firewall mit Eingabe- und Ausgabefiltern auf seiner Internetschnittstelle konfiguriert werden, um das Weiterleiten von Tunnelverwaltungsverkehr und getunnelten Daten zum VPN-Server zuzulassen. Zusätzliche Filter können das Weiterleiten von Verkehr an Webserver, FTP-Server und andere Servertypen in der DMZ zulassen.

Da der Firewall nicht über die Verschlüsselungsschlüssel für jede einzelne VPN-Verbindung verfügt, kann er nur anhand der Nur-Text-Header der getunnelten Daten filtern, was bedeutet, dass alle getunnelten Daten durch den Firewall weitergeleitet werden. Dies stellt jedoch kein Sicherheitsproblem dar, da die VPN-Verbindung einen Authentifizierungsprozess erfordert, der nicht autorisierten Zugriff jenseits des VPN-Servers verhindert.

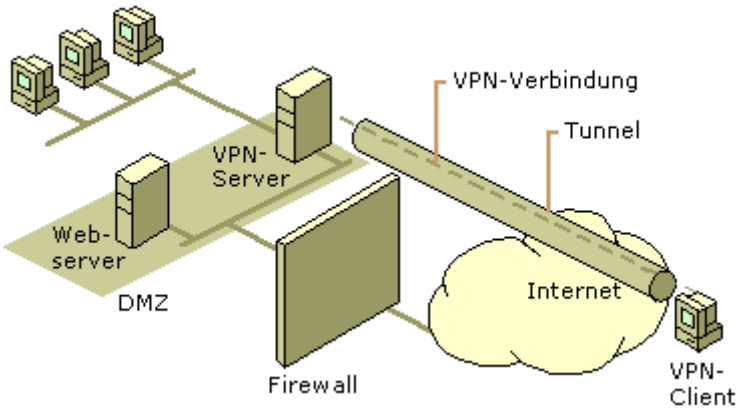

Abbildung 9.18: VPN-Server hinter dem Firewall im Internet

Konfigurieren Sie für die Internetschnittstelle auf dem Firewall mithilfe der Konfigurationssoftware des Firewalls die folgenden Eingabe- und Ausgabefilter.

PPTP-Paketfilter

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 DMZ-Schnittstelle des VPN-Servers und TCP-Zielport 1723 (0x06BB).

  Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom PPTP-Client zum PPTP-Server zu.

- Ziel-IP-Adresse der DMZ-Schnittstelle des VPN-Servers und IP-Protokollkennung 47 (0x2F).

  Dieser Filter lässt mit PPTP getunnelte Daten vom PPTP-Client zum PPTP-Server zu.

- Ziel-IP-Adresse der DMZ-Schnittstelle des VPN-Servers und TCP-Quellport [eingerichtet] 1723 (0x06BB).

  Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wenn Sie **TCP [eingerichtet]** auswählen, wird nur dann Verkehr akzeptiert, wenn der VPN-Server die TCP-Verbindung initiiert hat.

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 DMZ-Schnittstelle des VPN-Servers und TCP-Quellport 1723 (0x06BB).

  Dieser Filter lässt PPTP-Tunnelverwaltungsverkehr vom VPN-Server zum VPN-Client zu.

- Quell-IP-Adresse der DMZ-Schnittstelle des VPN-Servers und IP-Protokollkennung 47 (0x2F).

  Dieser Filter lässt mit PPTP getunnelte Daten vom VPN-Server zum VPN-Client zu.

- Quell-IP-Adresse der DMZ-Schnittstelle des VPN-Servers und TCP-Zielport [eingerichtet] 1723 (0x06BB).

  Dieser Filter ist nur erforderlich, wenn der VPN-Server als VPN-Client (anrufender Router) in einer Router-zu-Router-VPN-Verbindung fungiert. Wenn Sie **TCP [eingerichtet]** auswählen, wird nur dann Verkehr gesendet, wenn der VPN-Server die TCP-Verbindung initiiert hat.

Paketfilter für L2TP über 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 DMZ-Schnittstelle des VPN-Servers und UDP-Zielport 500 (0x01F4).

  Dieser Filter lässt IKE-Verkehr zum VPN-Server zu.

- Ziel-IP-Adresse der DMZ-Schnittstelle des VPN-Servers und IP-Protokollkennung 50 (0x32).

  Dieser Filter lässt IPSec ESP-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 DMZ-Schnittstelle des VPN-Servers und UDP-Quellport 500 (0x01F4).

  Dieser Filter lässt IKE-Verkehr vom VPN-Server zu.

- Quell-IP-Adresse der DMZ-Schnittstelle des VPN-Servers und IP-Protokollkennung 50 (0x32).

  Dieser Filter lässt IPSec ESP-Verkehr vom VPN-Server zum VPN-Client zu.

Für L2TP-Verkehr am UDP-Port 1701 sind keine Filter erforderlich. Am Firewall wird der gesamte L2TP-Verkehr einschließlich der Tunnelverwaltung und der getunnelten Daten als IPSec ESP-Nutzlast verschlüsselt.

VPNs und Übersetzer für Netzwerkadressen

Ein Übersetzer für Netzwerkadressen (Network Address Translator, NAT) ist ein IP-Router mit der Fähigkeit, die IP-Adresse und die TCP/UDP-Portnummern von Paketen bei deren Weiterleitung zu übersetzen. Denken wir an das kleine Unternehmen, das mehrere Computer mit dem Internet verbinden möchte. Normalerweise muss es für jeden Computer in seinem Netzwerk eine öffentliche Adresse erhalten. Mit einem NAT benötigt das kleine Unternehmen jedoch keine mehrfachen öffentlichen Adressen. Es kann private Adressen (wie in RFC 1597 dokumentiert) im Netzwerksegment des kleinen Unternehmens verwenden und den NAT verwenden, um die privaten Adressen einer oder mehrerer von einem ISP zugewiesener öffentlicher IP-Adressen zuzuordnen. Die NAT-Funktionalität wird in RFC 1631 dokumentiert.

Wenn beispielsweise ein kleines Unternehmen das Netzwerk 10.0.0.0/8 für sein privates Netzwerk verwendet und ihm vom ISP die öffentliche IP-Adresse *w.x.y.z* zugewiesen wurde, ordnet der NAT statisch oder dynamisch alle für Netzwerk 10.0.0.0/8 verwendeten privaten IP-Adressen der IP-Adresse *w.x.y.z* zu.

Für ausgehende Pakete werden die Quell-IP-Adresse und die TCP/UDP-Portnummern *w.x.y.z* und einer möglicherweise geänderten TCP/UDP-Portnummer zugeordnet. Für eingehende Pakete werden die Ziel-IP-Adresse und die TCP/UDP-Portnummern der privaten IP-Adresse und der ursprünglichen TCP/UDP-Portnummer zugeordnet.

NAT übersetzt standardmäßig IP-Adressen und TCP/UDP-Ports. Wenn die IP-Adresse und die Portinformationen sich nur in den IP- und TCP/UDP-Headern befinden, kann das Anwendungsprotokoll transparent übersetzt werden, beispielsweise beim HTTP-Verkehr (HyperText Transfer Protocol) im World Wide Web.

Manche Anwendungen und Protokolle speichern jedoch IP-Adressen oder TCP/UDP-Informationen in ihren eigenen Headern. FTP speichert beispielsweise die punktierte Dezimalschreibweise von IP-Adressen im FTP-Header für den Befehl FTP PORT. Wenn der NAT die IP-Adresse im FTP-Header nicht korrekt übersetzt, können Verbindungsprobleme auftreten. Außerdem verwenden manche Protokolle zum Identifizieren von Datenströmen keine TCP- oder UDP-Header, sondern Felder in anderen Headern.

Wenn die NAT-Komponente zusätzlich die Nutzlast außerhalb der IP-, TCP- und UDP-Header übersetzen und anpassen muss, ist ein NAT-Editor erforderlich. Ein NAT-Editor ändert ansonsten nicht übersetzbare Nutzlasten entsprechend ab, so dass sie über einen NAT weitergeleitet werden können.

Adress- und Portzuordnung für VPN-Verkehr

Damit PPTP und L2TP über IPSec-Tunnel über einen NAT funktionieren, muss der NAT in der Lage sein, mehrere Datenströme zu und von einer einzigen IP-Adresse zuzuordnen.

PPTP-Verkehr

PPP-Verkehr besteht aus einer TCP-Verbindung für die Tunnelverwaltung und GRE-Einkapselung für getunnelte Daten. Die TCP-Verbindung kann vom NAT übersetzt werden, da die Quell-TCP-Portnummern transparent übersetzt werden können. Die mit GRE eingekapselten Daten können jedoch ohne einen Editor nicht vom NAT übersetzt werden.

Bei getunnelten Daten wird der Tunnel anhand der Quell-IP-Adresse und des Anrufskennungsfeldes im GRE-Header identifiziert. Wenn auf der privaten Seite eines NATs mehrere PPTP-Clients Tunneling zum selben PPTP-Server durchführen, verwendet der gesamte getunnelte Verkehr dieselbe Quell-IP-Adresse. Da die PPTP-Clients nicht wissen, dass sie übersetzt werden, wählen sie möglicherweise beim Aufbauen des PPTP-Tunnels dieselbe Anrufskennung. Es ist daher möglich, dass getunnelte Daten von mehreren PPTP-Clients auf der privaten Seite des NATs dieselbe Quell-IP-Adresse und dieselbe Anrufskennung aufweisen, wenn sie übersetzt werden.

Um dieses Problem zu umgehen, muss ein NAT-Editor für PPTP die PPTP-Tunnelerstellung überwachen und andere als die vom PPTP-Client verwendeten Zuordnungen zu einer öffentlichen IP-Adresse und eindeutigen Anrufskennung für eine vom PPTP-Server im Internet empfangene private IP-Adresse und Anrufskennung erstellen.

Das NAT-Routingprotokoll des Routing- und RAS-Dienstes enthält einen PPTP-Editor, der die GRE-Anrufskennung übersetzt, um zwischen mehreren PPTP-Tunneln auf der privaten Seite des NATs zu unterscheiden.

L2TP über IPSec-Verkehr

L2TP über IPSec-Verkehr kann nicht von einem NAT übersetzt werden, da die UDP-Portnummer verschlüsselt ist und ihr Wert durch eine kryptografische Prüfsumme geschützt ist. L2TP über IPSec kann aus folgenden zusätzlichen Gründen selbst mit einem Editor nicht übersetzt werden:

Mehrere IPSec ESP-Datenströme können nicht unterschieden werden

Der ESP-Header enthält ein Feld namens Sicherheitsparameterindex (Security Parameters Index, SPI). Der SPI wird in Verbindung mit der Ziel-IP-Adresse im Nur-Text-IP-Header und dem IPSec-Sicherheitsprotokoll (ESP oder Authentifizierungsheader [Authenticating Header, AH]) verwendet, um eine IPSec-Sicherheitszuordnung (Security Association, SA) zu identifizieren.

Für ausgehenden Verkehr vom NAT wird die Ziel-IP-Adresse nicht geändert. Für eingehenden Verkehr zum NAT muss die Ziel-IP-Adresse einer privaten IP-Adresse zugeordnet sein. Genau wie im Fall mehrerer PPTP-Clients auf der privaten Seite eines NATs entspricht die Ziel-IP-Adresse des eingehenden Verkehrs für mehrere IPSec ESP-Datenströme derselben Adresse. Um IPSec ESP-Datenströme voneinander zu unterscheiden, können die Ziel-IP-Adresse und der SPI einer privaten Ziel-IP-Adresse und einem privaten SPI zugeordnet sein. Da jedoch der ESP Auth-Nachspann eine kryptografische Prüfsumme enthält, die den ESP-Header und seine Nutzlast überprüft, kann der SPI nicht geändert werden, ohne die kryptografische Prüfsumme als ungültig zu kennzeichnen.

TCP- und UDP-Prüfsummen können nicht geändert werden

In L2TP über IPSec-Paketen enthalten UDP- und TCP-Header eine Prüfsumme, die die Quell- und Ziel-IP-Adresse des Nur-Text-IP-Headers beinhaltet. Die Adressen im Nur-Text-IP-Header können nicht geändert werden, ohne die Prüfsumme in den TCP- und UDP-Headern als ungültig zu kennzeichnen. Die TCP- und UDP-Prüfsummen können nicht aktualisiert werden, da sie sich innerhalb des verschlüsselten Teils der ESP-Nutzlast befinden.

Pass-Through-VPN-Szenario

Wie weiter oben in diesem Kapitel unter "Internet- und intranetbasierte VPN-Verbindungen" beschrieben, ermöglicht ein Pass-Through-VPN einem mit dem Intranet eines Unternehmens verbundenen RAS-Client, über das Internet auf die Ressourcen des Intranets eines anderen Unternehmens zuzugreifen. Eine RAS-VPN-Verbindung wird über ein Intranet und das Internet an ein anderes Intranet weitergeleitet.

In einem typischen Fall sind Firma A und Firma B Geschäftspartner, und ein Mitarbeiter von Firma A besucht Firma B. Wenn der Mitarbeiter von Firma A an einer Besprechung teilnimmt und einen Laptopcomputer mit dem Intranet von Firma B verbindet, erhält er eine Intranet-IP-Adresskonfiguration von Firma B. Wenn der Mitarbeiter von Firma A eine Verbindung zum Intranet von Firma A herstellen muss, ist dies mit einer der folgenden Methoden möglich:

- Mithilfe einer Telefonleitung im Konferenzraum kann der Mitarbeiter von Firma A direkt den RAS-Server von Firma A anwählen, um eine DFÜ-Verbindung zum Intranet von Firma A herzustellen, oder er kann einen lokalen ISP anwählen und eine VPN-Verbindung zum Intranet von Firma A herstellen.
- Wie in Abbildung 9.19 gezeigt, kann der Mitarbeiter von Firma A mithilfe der VPN-Technologie und der entsprechenden Infrastruktur über das Intranet von Firma B einen Tunnel zum Internet erstellen und dann einen weiteren Tunnel über das Intranet von Firma B und das Internet zum Intranet von Firma A erstellen.

Mit der letzteren Methode wird die VPN-Verbindung zum Intranet von Firma A durch das Aktivieren von zwei Verbindungsobjekten im Ordner **Verbindungen** mithilfe der vorhandenen lokalen physischen Netzwerkverbindung erstellt. Tunnel 2 befindet sich im Inneren von Tunnel 1 im Intranet von Firma B.

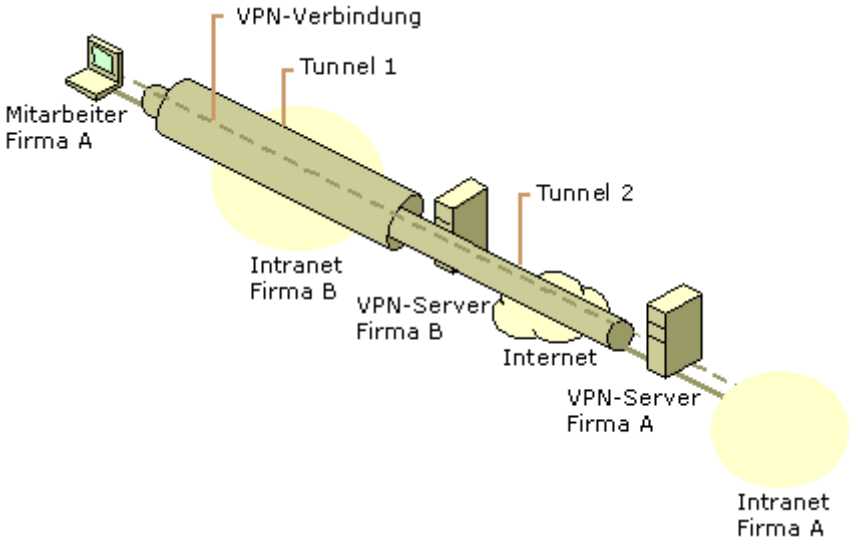

Abbildung 9.19: Pass-Through-VPN-Szenario

Konfiguration des VPN-Servers von Firma A

Konfigurieren Sie den VPN-Server von Firma A so, dass er RAS-VPN-Verbindungen von Remoteclients im Internet akzeptiert. Verwenden Sie entsprechende RAS-Richtlinien, die strenge Authentifizierung und starke Verschlüsselung erfordern.

Konfiguration des VPN-Servers von Firma B

Konfigurieren Sie den VPN-Server von Firma B folgendermaßen:

1. Konfigurieren Sie den VPN-Server von Firma B so, dass er RAS-VPN-Verbindungen akzeptiert. Weitere Informationen finden Sie in der Windows 2000 Server-Hilfe.
2. Konfigurieren Sie den IP-Adresspool, der eine Reihe von öffentlichen IP-Adressen enthält.
3. Erstellen Sie eine Windows 2000-Gruppe, die die Benutzerkonten für besuchende Mitarbeiter anderer Firmen enthält, die Pass-Through-VPN-Verbindungen herstellen. Erstellen Sie beispielsweise die Gruppe **VPN_PassThrough**.
4. Erstellen Sie das Benutzerkonto, das vom besuchenden Mitarbeiter von Firma A verwendet wird.

Wenn dieser VPN-Server nur für Pass-Through-VPNs für die besuchenden Mitarbeiter von Geschäftspartnern verwendet werden soll, löschen Sie die Standard-RAS-Richtlinie namens **Zugriff zulassen, wenn Einwählrechte erteilt worden sind**, und erstellen Sie eine RAS-Richtlinie namens **VPN Pass-Through für Geschäftspartner**, für die die RAS-Richtlinienberechtigungseinstellung **RAS-Berechtigung erteilen** ausgewählt ist. Legen Sie dann die Bedingungen und Profileinstellungen gemäß den Tabellen 9.7 und 9.8 fest. Ausführliche Informationen zum Konfigurieren dieser Einstellungen finden Sie in der Microsoft Windows 2000 Server-Hilfe.

Tabelle 9.7: RAS-Richtlinienbedingungen für den VPN-Server von Firma B

Bedingungen	**Einstellung**
NAS-Porttyp	**Virtuell**
ID der Empfängerstation	IP-Adresse der VPN-Serverschnittstelle, die VPN-Verbindungen akzeptiert
Windows-Gruppen	beispielsweise **VPN_PassThrough**

Tabelle 9.8: Profileinstellungen für RAS-Richtlinien für den VPN-Server von Firma B

Profileinstellungen	**Einstellung**
Registerkarte **Authentifizierung**	Aktivieren Sie **Microsoft-verschlüsselte Authentifizierung (MS-CHAP).**
Registerkarte **Verschlüsselung**	Wählen Sie **Basisverschlüsselung, Starke Verschlüsselung** oder **Keine Verschlüsselung** aus.

Die in den Tabellen 9.7 und 9.8 beschriebenen RAS-Richtlinieneinstellungen gehen davon aus, dass Sie den Remotezugriff auf Gruppenbasis verwalten, indem Sie die RAS-Zugriffsberechtigung für alle Benutzerkonten auf **Zugriff über RAS-Richtlinien steuern** festlegen.

Anmerkung Die Profileinstellungen für RAS-Richtlinien erfordern keine Verschlüsselung. Der Tunnel vom Mitarbeiter von Firma A zum VPN-Server von Firma B muss nicht verschlüsselt werden, da der Tunnel vom Mitarbeiter von Firma A zum VPN-Server von Firma A im Internet verschlüsselt ist. Wenn Sie die Verschlüsselung des ersten Tunnels erzwingen, tritt die Verschlüsselung unnötigerweise zwei Mal ein und kann die Leistung beeinträchtigen.

Filterkonfiguration

Um sicherzustellen, dass der mit dem Internet verbundene VPN-Server von Firma B auf das Akzeptieren und Weiterleiten von Pass-Through-VPN-Verkehr beschränkt ist, konfigurieren Sie mithilfe des Routing und RAS-Snap-Ins die folgenden Filter:

So konfigurieren Sie PPTP-Filterung

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

- Ziel-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Zielport 1723.
- Ziel-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokoll 47.

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

- Quell-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und TCP-Quellport 1723.
- Quell-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und IP-Protokoll 47.

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

- Ziel-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und TCP-Quellport 1723.
- Ziel-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und IP-Protokoll 47.

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

- Quell-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und TCP-Zielport 1723.
- Quell-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und IP-Protokoll 47.

So konfigurieren Sie L2TP über IPSec-Filterung

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

- Ziel-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 1701.
- Ziel-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Zielport 500.

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

- Quell-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 1701.
- Quell-IP-Adresse der Intranetschnittstelle des VPN-Servers, Subnetzmaske 255.255.255.255 und UDP-Quellport 500.

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

- Ziel-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und IP-Protokoll 50.
- Ziel-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und UDP-Quellport 500.

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

- Quell-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und IP-Protokoll 50.
- Quell-IP-Adresse und Subnetzmaske des öffentlichen IP-Adresspools und UDP-Zielport 500.

Konfiguration des VPN-Clientcomputers für ein Pass-Through-VPN

Die folgenden Abschnitte beschreiben die Konfiguration eines Windows 2000-basierten VPN-Clients für PPTP und L2TP über IPSec für ein Pass-Through-VPN.

So konfigurieren Sie eine PPTP-Verbindung

Erstellen Sie folgendermaßen ein VPN-Verbindungsobjekt, das den Mitarbeiter von Firma A mit dem VPN-Server von Firma B verbindet:

- Geben Sie auf der Registerkarte **Allgemein** den Hostnamen oder die IP-Adresse der Intranetschnittstelle des VPN-Servers von Firma B ein.
- Wählen Sie auf der Registerkarte **Sicherheit** die Option **Kennwort verschlüsselt senden, Daten unverschlüsselt senden** aus.
- Wählen Sie auf der Registerkarte **Netzwerk** die Option **Point-to-Point Tunneling Protocol (PPTP)** als angewählten Servertyp aus.

Erstellen Sie folgendermaßen ein VPN-Verbindungsobjekt, das den Mitarbeiter von Firma A mit dem Internet-VPN-Server von Firma A verbindet:

- Geben Sie auf der Registerkarte **Allgemein** den Hostnamen oder die IP-Adresse der Internetschnittstelle des VPN-Servers von Firma A ein.
- Wählen Sie auf der Registerkarte **Sicherheit** entweder **Kennwort und Daten verschlüsselt senden** oder **Benutzerdefiniert** aus. Wenn Sie **Benutzerdefiniert** auswählen, müssen Sie außerdem die entsprechenden Optionen für Verschlüsselung und Authentifizierung auswählen.
- Wählen Sie auf der Registerkarte **Netzwerk** die Option **Point-to-Point Tunneling Protocol (PPTP)** als angewählten Servertyp aus.

So konfigurieren Sie eine L2TP über IPSec-Verbindung

Erstellen Sie folgendermaßen ein VPN-Verbindungsobjekt, das den Mitarbeiter von Firma A mit dem VPN-Server von Firma B verbindet:

- Geben Sie auf der Registerkarte **Allgemein** den Hostnamen oder die IP-Adresse der Intranetschnittstelle des VPN-Servers von Firma B ein.
- Wählen Sie auf der Registerkarte **Sicherheit** die Option **Kennwort verschlüsselt senden, Daten unverschlüsselt senden** aus.
- Wählen Sie auf der Registerkarte **Netzwerk** die Option **Layer-2 Tunneling Protocol (L2TP)** als angewählten Servertyp aus.

Erstellen Sie folgendermaßen ein VPN-Verbindungsobjekt, das den Mitarbeiter von Firma A mit dem Internet-VPN-Server von Firma A verbindet:

- Geben Sie auf der Registerkarte **Allgemein** den Hostnamen oder die IP-Adresse der Internetschnittstelle des VPN-Servers von Firma A ein.
- Wählen Sie auf der Registerkarte **Sicherheit** entweder **Kennwort und Daten verschlüsselt senden** oder **Benutzerdefiniert** aus. Wenn Sie **Benutzerdefiniert** auswählen, müssen Sie außerdem die entsprechenden Optionen für Verschlüsselung und Authentifizierung auswählen.
- Wählen Sie auf der Registerkarte **Netzwerk** die Option **Layer-2 Tunneling Protocol (L2TP)** als angewählten Servertyp aus.

Erstellen der Pass-Through-VPN-Verbindung

Wenn die folgende Pass-Through-VPN-Verbindung hergestellt ist, kann der Mitarbeiter von Firma A während der Dauer der VPN-Verbindung mit dem VPN-Server von Firma A auf alle Intranetressourcen von Firma A zugreifen.

So erstellen Sie eine Pass-Through-Verbindung

Der Mitarbeiter von Firma A erstellt mithilfe des folgenden Prozesses eine Pass-Through-VPN-Verbindung zum VPN-Server von Firma A im Internet:

1. Doppelklicken Sie im Ordner **Verbindungen** auf das Verbindungsobjekt, das den Tunnel zum VPN-Server von Firma B im Intranet von Firma B erstellt.
2. Wenn Sie nach den Benutzeranmeldeinformationen gefragt werden, geben Sie die Anmeldeinformationen für das Benutzerkonto bei Firma B ein.
3. Doppelklicken Sie im Ordner **Verbindungen** auf das Verbindungsobjekt, das das VPN zum VPN-Server von Firma A im Internet erstellt.
4. Wenn Sie nach den Benutzeranmeldeinformationen gefragt werden, geben Sie die Anmeldeinformationen für das Firmenkonto von Firma A ein.

Problembehandlung bei VPNs

Für die Problembehandlung bei VPNs müssen Sie die Probleme bei IP-Verbindungen, beim Herstellen von RAS-Verbindungen und bei Bedarf herzustellenden Wählverbindungen, Routing und IPSec behandeln.

Häufige VPN-Probleme

VPN-Probleme fallen normalerweise in die folgenden Kategorien:

- Verbindungsversuch wird abgelehnt, obwohl er akzeptiert werden sollte.
- Verbindungsversuch wird akzeptiert, obwohl er abgelehnt werden sollte.
- Standorte jenseits des VPN-Servers können nicht erreicht werden.
- Es kann kein Tunnel aufgebaut werden.

Verwenden Sie die folgenden Problembehandlungstipps, um das Konfigurations- oder Infrastrukturproblem zu isolieren, das das genannte VPN-Problem verursacht hat.

Verbindungsversuch wird abgelehnt, obwohl er akzeptiert werden sollte

- Überprüfen Sie mithilfe des Befehls "Ping", ob der Hostname oder die IP-Adresse des VPN-Servers erreichbar ist. Wenn ein Hostname verwendet wird, überprüfen Sie, ob der Hostname an seine korrekte IP-Adresse aufgelöst wird. Wenn der Befehl "Ping" nicht erfolgreich ausgeführt wird, verhindert möglicherweise die Paketfilterung die Zustellung von ICMP-Nachrichten vom oder an den VPN-Server.
- Überprüfen Sie, ob der Routing- und RAS-Dienst auf dem VPN-Server ausgeführt wird.
- Überprüfen Sie bei RAS-VPN-Verbindungen, ob der Fernzugriff auf dem VPN-Server aktiviert ist. Überprüfen Sie bei Router-zu-Router-VPN-Verbindungen, ob auf dem VPN-Server Routing für Wählen bei Bedarf aktiviert ist.
- Überprüfen Sie bei RAS-VPN-Verbindungen, ob auf den PPTP- und L2TP-Ports eingehender Remotezugriff aktiviert ist. Überprüfen Sie bei Router-zu-Router-VPN-Verbindungen, ob auf den PPTP- und L2TP-Ports eingehende und ausgehende bei Bedarf herzustellende Wählverbindungen aktiviert sind.
- Überprüfen Sie, ob der VPN-Client und der VPN-Server in Verbindung mit einer RAS-Richtlinie so konfiguriert sind, dass sie mindestens eine gemeinsame Authentifizierungsmethode verwenden.
- Überprüfen Sie, ob der VPN-Client und der VPN-Server in Verbindung mit einer RAS-Richtlinie so konfiguriert sind, dass sie mindestens eine gemeinsame Verschlüsselungsmethode verwenden.
- Überprüfen Sie, ob die Parameter der Verbindung über Berechtigungen durch RAS-Richtlinien verfügen.

  Damit die Verbindung aufgebaut wird, müssen die Parameter des Verbindungsversuchs folgende Bedingungen erfüllen:

  - Sie müssen mit allen Bedingungen mindestens einer RAS-Richtlinie übereinstimmen.
  - Das Benutzerkonto muss ihnen RAS-Berechtigung (auf **Zugriff gestatten** festgelegt) erteilen, oder für die RAS-Berechtigung der entsprechenden RAS-Richtlinie muss die Option **RAS-Berechtigung erteilen** ausgewählt sein, wenn für das Benutzerkonto die Option **Zugriff über RAS-Richtlinien steuern** ausgewählt ist.
  - Sie müssen mit allen Einstellungen des Profils übereinstimmen.
  - Sie müssen mit allen Einstellungen der Einwähleigenschaften des Benutzerkontos übereinstimmen.

  Weitere Informationen zu RAS-Richtlinien finden Sie in der Windows 2000 Server-Hilfe und in diesem Buch unter "Remote Access Server".

- Überprüfen Sie, ob die Einstellungen des RAS-Richtlinienprofils nicht im Konflikt zu Eigenschaften des RAS-Routers stehen.

  Die Eigenschaften des RAS-Richtlinienprofils und die Eigenschaften des RAS-Servers enthalten beide Einstellungen für Folgendes:

  - Mehrfachverbindung
  - Bandwidth Allocation-Protokoll
  - Authentifizierungsprotokolle

  Wenn die Einstellungen des Profils der übereinstimmenden RAS-Richtlinie im Konflikt zu den Einstellungen des VPN-Servers stehen, wird der Verbindungsversuch abgelehnt. Wenn beispielsweise das übereinstimmende RAS-Richtlinienprofil angibt, dass das Authentifizierungsprotokoll EAP-TLS verwendet werden muss, und EAP-TLS auf dem VPN-Server nicht aktiviert ist, lehnt der VPN-Server den Verbindungsversuch ab.

Wenn der VPN-Server ein Mitgliedsserver in einer für Windows 2000-Authentifizierung konfigurierten Windows 2000-Domäne im gemischten oder im einheitlichen Modus ist, überprüfen Sie Folgendes:

  - Die Sicherheitsgruppe **RAS- und IAS-Server** ist vorhanden. Wenn nicht, erstellen Sie die Gruppe, und legen Sie den Gruppentyp auf **Sicherheit** und den Gruppenbereich auf **Lokale Domäne** fest.
  - Die Sicherheitsgruppe **RAS- und IAS-Server** verfügt über die **Leseberechtigung** für das Objekt **RAS- und IAS-Server-Zugriffsüberprüfung**.
  - Das Computerkonto des VPN-Servercomputers ist Mitglied der Sicherheitsgruppe **RAS- und IAS-Server**. Mithilfe des Befehls **netsh ras show registeredserver** können Sie die aktuelle Registrierung anzeigen. Mithilfe des Befehls **netsh ras add registeredserver** können Sie den Server in einer angegebenen Domäne registrieren.
  - Wenn Sie den VPN-Servercomputer zur Sicherheitsgruppe **RAS- und IAS-Server** hinzufügen oder aus ihr entfernen, wird die Änderung nicht sofort wirksam (aufgrund der Art und Weise, wie Windows 2000 Active Directory-Informationen zwischenspeichert). Damit die Änderung sofort wirksam wird, müssen Sie den VPN-Servercomputer neu starten.

- Überprüfen Sie bei RAS-VPN-Verbindungen, ob für die vom VPN-Client verwendeten LAN-Protokolle auf dem VPN-Server Fernzugriff aktiviert ist.
- Überprüfen Sie, ob keiner der PPTP- oder L2TP-Ports auf dem VPN-Server bereits verwendet wird. Ändern Sie ggf. die Anzahl der PPTP oder L2TP-Ports, um mehr gleichzeitige Verbindungen zu ermöglichen.
- Überprüfen Sie, ob das Tunnelprotokoll des VPN-Clients vom VPN-Server unterstützt wird.

  Auf RAS-VPN-Clients unter Windows 2000 ist standardmäßig die Servertypoption **Automatisch** ausgewählt. Dies bedeutet, dass sie zuerst versuchen, eine L2TP über IPSec-basierte VPN-Verbindung herzustellen, und dann eine PPTP-basierte VPN-Verbindung versuchen. Wenn weder die Servertypoption **Point-to-Point Tunneling Protocol (PPTP)** noch **Layer-2 Tunneling Protocol (L2TP)** ausgewählt ist, überprüfen Sie, ob das ausgewählte Tunnelprotokoll vom VPN-Server unterstützt wird.

  Ein Windows 2000 Server-basierter Computer, der den Routing- und RAS-Dienst ausführt, ist standardmäßig ein PPTP- und L2TP-Server mit fünf L2TP-Ports und fünf PPTP-Ports. Um einen reinen PPTP-Server zu erstellen, legen Sie die Anzahl der L2TP-Ports auf Null fest. Um einen reinen L2TP-Server zu erstellen, legen Sie die Anzahl der PPTP-Ports auf Null fest.

- Überprüfen Sie bei RAS-Verbindungen, die L2TP über IPSec verwenden, ob auf dem VPN-Client und dem VPN-Server Computerzertifikate installiert sind. Weitere Informationen zur Problembehandlung bei IPSec-Verbindungen finden Sie unter "Internet Protocol Security" im *TCP/IP Core Networking Guide*.
- Überprüfen Sie, ob die Anmeldeinformationen des VPN-Clients, die aus dem Benutzernamen, dem Kennwort und dem Domänennamen bestehen, korrekt sind und vom VPN-Server überprüft werden können.
- Wenn der VPN-Server mit statischen IP-Adresspools konfiguriert ist, überprüfen Sie, ob genügend Adressen vorhanden sind.

  Wenn alle Adressen in den statischen Pools verbundenen VPN-Clients zugewiesen sind, kann der VPN-Server keine IP-Adresse für TCP/IP-basierte Verbindungen finden, und der Verbindungsversuch wird abgelehnt.

- Wenn der VPN-Client so konfiguriert ist, dass er seine eigene IPX-Knotennummer anfordert, überprüfen Sie, ob der VPN-Server so konfiguriert ist, dass er zulässt, dass IPX-Clients ihre eigene IPX-Knotennummer anfordern.
- Wenn der VPN-Server mit einer Reihe von IPX-Netzwerknummern konfiguriert ist, überprüfen Sie, ob die IPX-Netzwerknummern sich in einem Bereich befinden, der nicht an einer anderen Stelle in Ihrem IPX-Netzwerk verwendet wird.
- Überprüfen Sie die Konfiguration des Authentifizierungsanbieters.

Der VPN-Server kann so konfiguriert werden, dass er entweder Windows 2000 oder RADIUS zum Authentifizieren der Anmeldeinformationen des VPN-Clients verwendet.

- Wenn der VPN-Server Mitglied einer Windows 2000-Domäne im einheitlichen Modus ist, überprüfen Sie, ob der VPN-Server der Domäne beigetreten ist.
- Wenn der VPN-Server unter Windows NT, Version 4.0, Service Pack 4 und höher, Mitglied einer Windows 2000-Domäne im gemischten Modus oder der VPN-Server unter Windows 2000 Mitglied einer Windows NT 4.0-Domäne ist, der auf Benutzerkonteneigenschaften für ein Benutzerkonto in einer vertrauenswürdigen Windows 2000-Domäne zugreift, überprüfen Sie mithilfe des Befehls **net localgroup "Pre-Windows 2000 Compatible Access"**, ob die Gruppe **Jeder** zu der Gruppe **Prä-Windows 2000 kompatibler Zugriff** hinzugefügt ist. Wenn nicht, geben Sie den Befehl **net localgroup "Pre-Windows 2000 Compatible Access" everyone /add** auf einem Domänencontrollercomputer ein, und starten Sie dann den Domänencontrollercomputer neu.
- Wenn es sich um einen VPN-Server unter Windows NT, Version 4.0, Service Pack 3 und früher, handelt, der Mitglied einer Windows 2000-Domäne im gemischten Modus ist, überprüfen Sie, ob der Gruppe **Jeder** die Berechtigung "Inhalt auflisten" und "Eigenschaften lesen" sowie Leseberechtigungen für den Stammknoten Ihrer Domäne und für alle Unterobjekte der Stammdomäne erteilt wurden.
- Überprüfen Sie bei einer RADIUS-Authentifizierung, ob der VPN-Servercomputer mit dem RADIUS-Server kommunizieren kann.
- Überprüfen Sie bei PPTP-Verbindungen, die MS-CHAP v1 verwenden und versuchen, 40-Bit-MPPE-Verschlüsselung auszuhandeln, ob das Kennwort des Benutzers nicht länger als 14 Zeichen ist.

Verbindungsversuch wird akzeptiert, obwohl er abgelehnt werden sollte

- Stellen Sie sicher, dass die Parameter der Verbindung über keine Berechtigungen durch RAS-Richtlinien verfügen.

  Eine Verbindung kann aus den folgenden Gründen abgelehnt werden:

  Den Parametern des Verbindungsversuchs muss durch die RAS-Berechtigung des Benutzerkontos (wobei **Zugriff verweigern** ausgewählt ist) die Zugriffsberechtigung verweigert werden.

  Für das Benutzerkonto ist die Option **Zugriff über RAS-Richtlinien steuern** ausgewählt, und für die RAS-Berechtigung der ersten RAS-Richtlinie, die mit den Parametern des Verbindungsversuchs übereinstimmt, ist die Option **RAS-Berechtigung verweigern** ausgewählt.

  Weitere Informationen zu RAS-Richtlinien finden Sie in der Windows 2000 Server-Hilfe.

Standorte jenseits des VPN-Servers können nicht erreicht werden

- Überprüfen Sie für RAS-VPNs, ob entweder das Protokoll für Routing oder die Option **Gesamtes Netzwerk** für von den VPN-Clients verwendete LAN-Protokolle ausgewählt ist.
- Überprüfen Sie für RAS-VPNs die IP-Adresspools des VPN-Servers.

  Wenn der VPN-Server so konfiguriert ist, dass er einen statischen IP-Adresspool verwendet, überprüfen Sie, ob die Routen zu dem von den statischen IP-Adresspools definierten Adressbereich durch die Hosts und Router des Intranets erreichbar sind. Wenn nicht, muss eine IP-Route, die aus den statischen IP-Adresspools des VPN-Servers gemäß der Definition der IP-Adresse und -Maske des Bereichs besteht, zu den Routern des Intranets hinzugefügt oder das Routingprotokoll Ihrer umgeleiteten Infrastruktur auf dem VPN-Server aktiviert werden. Wenn die Routen zu den RAS-VPN-Clientteilnetzen nicht vorhanden sind, können RAS-VPN-Clients keinen Verkehr von Standorten im Intranet erhalten. Routen für die Teilnetze werden entweder durch statische Routingeinträge oder durch ein Routingprotokoll, wie beispielsweise Open Shortest Path First (OSPF) oder Routing Information Protocol (RIP), implementiert.

Wenn der VPN-Server so konfiguriert ist, dass er DHCP für die IP-Adresszuweisung verwendet, und kein DHCP-Server verfügbar ist, weist der VPN-Server Adressen aus dem APIPA-Bereich (Automatic Private IP Addressing) 169.254.0.1 bis 169.254.255.254 zu. Das Zuweisen von APIPA-Adressen für RAS-Clients funktioniert nur, wenn das Netzwerk, mit dem der VPN-Server verknüpft ist, ebenfalls APIPA-Adressen verwendet.

Wenn der VPN-Server APIPA-Adressen verwendet, wenn ein DHCP-Server verfügbar ist, überprüfen Sie, ob der richtige Adapter für das Erhalten von von DHCP zugewiesenen IP-Adressen ausgewählt ist. Standardmäßig wählt der VPN-Server den für das Erhalten von IP-Adressen über DHCP verwendeten Adapter zufällig aus. Wenn mehr als ein LAN-Adapter vorhanden ist, wählt der Routing- und RAS-Dienst möglicherweise einen LAN-Adapter, für den kein DHCP-Server verfügbar ist. Sie können auf der Registerkarte **IP** in den Eigenschaften eines RAS-Servers im Routing and Remote Access-Snap-In manuell einen LAN-Adapter auswählen.

Wenn die statischen IP-Adresspools einen Bereich von IP-Adressen darstellen, die eine Teilmenge des Bereichs von IP-Adressen für das Netzwerk, mit dem der VPN-Server verknüpft ist, darstellen, überprüfen Sie, ob der Bereich der IP-Adressen in dem statischen IP-Adresspool nicht, entweder durch statische Konfiguration oder durch DHCP, anderen TCP/IP-Knoten zugewiesen ist.

- Überprüfen Sie bei Router-zu-Router-VPN-Verbindungen, ob auf beiden Seiten der Router-zu-Router-VPN-Verbindung Routen vorhanden sind, die den bidirektionalen Verkehrsaustausch unterstützen.

  Im Gegensatz zu einer RAS-VPN-Verbindung erstellt eine Router-zu-Router-VPN-Verbindung nicht automatisch eine Standardroute. Sie müssen auf beiden Seiten der Router-zu-Router-VPN-Verbindung Routen erstellen, damit der Verkehr zu und von der anderen Seite der Router-zu-Router-VPN-Verbindung umgeleitet werden kann.

  Sie können statische Routen manuell zur Routingtabelle hinzufügen, oder Sie können sie über Routingprotokolle hinzufügen. Für persistente VPN-Verbindungen können Sie Open Shortest Path First (OSPF) oder Routing Information Protocol (RIP) über die VPN-Verbindung aktivieren. Für VPN-Verbindungen für Wählen bei Bedarf können Sie Routen automatisch durch eine autostatische RIP-Aktualisierung aktualisieren.

- Überprüfen Sie bei von zwei Seiten initiierten Router-zu-Router-VPN-Verbindungen, ob die Router-zu-Router-VPN-Verbindung nicht vom VPN-Server als RAS-Verbindung interpretiert wird.

  Wenn der Benutzername aus den Anmeldeinformationen des anrufenden Routers im Routing and Remote Access-Snap-In unter **RAS-Clients** angezeigt wird, hat der VPN-Server den anrufenden Router als RAS-Client interpretiert. Überprüfen Sie, ob der Benutzername in den Anmeldeinformationen des anrufenden Routers mit dem Namen der Schnittstelle für Wählen bei Bedarf auf dem VPN-Server übereinstimmt.

- Überprüfen Sie bei von einer Seite initiierten Router-zu-Router-VPN-Verbindungen, ob die Routen des Intranets des anrufenden Routers in den Einwähleigenschaften des vom anrufenden Router verwendeten Benutzerkontos als statische Routen konfiguriert sind.
- Überprüfen Sie, ob in den Profileigenschaften der von der auf dem VPN-Server (oder dem RADIUS-Server, falls der Internetauthentifizierungsdienst verwendet wird) konfigurierten VPN-Verbindung verwendeten RAS-Richtlinie keine TCP/IP-Paketfilter konfiguriert sind, die das Senden oder Empfangen von TCP/IP-Verkehr verhindern.
- Überprüfen Sie bei VPN-Verbindungen für Wählen bei Bedarf, ob auf den Schnittstellen für Wählen bei Bedarf des anrufenden Routers und des antwortenden Routers keine Paketfilter konfiguriert sind, die das Senden oder Empfangen von Verkehr verhindern.

Es kann kein Tunnel aufgebaut werden

- Überprüfen Sie, ob die Paketfilterung auf einer Routerschnittstelle zwischen dem VPN-Client und dem VPN-Server das Weiterleiten von Tunnelprotokollverkehr verhindert.

  Auf einem Windows 2000-basierten VPN-Server kann IP-Paketfilterung sowohl über die erweiterten TCP/IP-Eigenschaften als auch über das Routing and Remote Access-Snap-In konfiguriert werden. Überprüfen Sie beide Stellen auf Filter, die möglicherweise VPN-Verbindungsverkehr ausschließen.

  Weitere Informationen zu VPN-Verbindungsverkehr und Paketfilterung finden Sie weiter oben in diesem Kapitel unter "VPNs und Firewalls".

- Überprüfen Sie, ob der Winsock-Proxyclient nicht gerade auf dem VPN-Server ausgeführt wird.

  Wenn der Winsock-Proxyclient aktiv ist, werden Winsock-API-Aufrufe, wie beispielsweise die zum Erstellen von Tunneln und zum Senden getunnelter Daten verwendeten, abgefangen und an einen konfigurierten Proxyserver weitergeleitet.

  Ein Proxyserver-basierter Computer ermöglicht einer Organisation das Zugreifen auf bestimmte Typen von Internetressourcen (normalerweise Web und FTP), ohne diese Organisation direkt mit dem Internet zu verbinden. Die Organisation kann stattdessen von InterNIC zugewiesene private IP-Netzwerkkennungen (wie beispielsweise 10.0.0.0/8) verwenden.

  Proxyserver werden normalerweise verwendet, damit private Benutzer in einer Organisation so auf öffentliche Internetressourcen zugreifen können, als seien sie direkt mit dem Internet verbunden. VPN-Verbindungen werden normalerweise verwendet, damit autorisierte öffentliche Internetbenutzer so auf private Organisationsressourcen zugreifen können, als seien sie direkt mit dem privaten Netzwerk verbunden. Ein einziger Computer kann als Proxyserver (für private Benutzer) und als VPN-Server (für autorisierte Internetbenutzer) fungieren, um in beiden Fällen den Informationsaustausch zu erleichtern.

Weitere Informationen zur Problembehandlung bei RAS-VPN-Verbindungen finden Sie in diesem Buch unter "Remote Access Server". Weitere Informationen zur Problembehandlung bei Router-zu-Router-VPN-Verbindungen finden Sie in diesem Buch unter "Demand-Dial Routing".

Tools für die Problembehandlung

Die folgenden Tools, die es Ihnen ermöglichen, zusätzliche Informationen zur Quelle Ihres VPN-Problems zu sammeln, sind in Windows 2000 enthalten.

Grund für Nichterreichbarkeit

Wenn eine Schnittstelle für Wählen bei Bedarf eine Verbindung nicht herstellen kann, bleibt die Schnittstelle im unerreichbaren Zustand. Klicken Sie mit der rechten Maustaste auf die Schnittstelle, und wählen Sie **Grund für Nichterreichbarkeit** aus, um mehr Informationen darüber zu erhalten, warum die Schnittstelle keine Verbindung herstellen konnte.

Ereignisprotokollierung

Die Registerkarte **Ereignisprotokollierung** in den Eigenschaften eines VPN-Servers weist vier Protokollstufen auf. Wählen Sie **Möglichst viele Informationen protokollieren** aus, und versuchen Sie erneut, die Verbindung herzustellen. Überprüfen Sie, nachdem die Verbindung nicht zustande gekommen ist, das Systemereignisprotokoll auf während des Verbindungsprozesses protokollierte Ereignisse. Wenn Sie mit dem Anzeigen der RAS-Ereignisse fertig sind, wählen Sie die Option **Fehler und Warnungen protokollieren** auf der Registerkarte **Ereignisprotokollierung** aus, um Systemressourcen zu sparen.

Ablaufverfolgung

Die Ablaufverfolgung zeichnet die Reihenfolge von Programmierungsfunktionen in einer Datei auf, die während eines Prozesses aufgerufen werden. Aktivieren Sie die Ablaufverfolgung für RAS- und VPN-Komponenten, wie in diesem Buch unter "Routing- and Remote Access Service" beschrieben, und versuchen Sie erneut, die Verbindung herzustellen. Wenn Sie die Nachverfolgungsinformationen angezeigt haben, setzen Sie die Nachverfolgungseinstellungen auf ihre Standardwerte zurück, um Systemressourcen zu sparen.

Nachverfolgungsinformationen können komplex und sehr detailliert sein. Meistens sind diese Informationen nur für Supportfachpersonal von Microsoft oder für Netzwerkadministratoren nützlich, die sehr viel Erfahrung mit dem Routing- und RAS-Dienst haben. Nachverfolgungsinformationen können als Dateien gespeichert und zur Analyse an den Support von Microsoft gesendet werden.

Netzwerkmonitor

Verwenden Sie den Netzwerkmonitor, ein Tool für das Abfangen und Analysieren von Paketen, um den während des VPN-Verbindungsprozesses und der Datenübertragung zwischen einem VPN-Server und einem VPN-Client gesendeten Verkehr anzuzeigen. Die verschlüsselten Teile des VPN-Verkehrs können Sie mit dem Netzwerkmonitor nicht interpretieren.

Für die richtige Interpretation des RAS- und VPN-Verkehrs mit dem Netzwerkmonitor benötigen Sie umfassende Kenntnisse von PPP, PPTP, IPSec und anderen Protokollen. Weitere Informationen zu PPP finden Sie in diesem Buch unter "Remote Access Server". Mit dem Netzwerkmonitor erfasste Informationen können als Dateien gespeichert und zur Analyse an den Support von Microsoft gesendet werden.

Weitere Ressourcen

Weitere Informationen zu RFCS (Request For Comment Proposals) finden Sie unter "Internet Engineering Task Force" auf der Seite **Web Resources** unter http://www.microsoft.com/windows2000/techinfo/reskit/WebResources/default.asp (englischsprachig).