



Microsoft
Windows Server 2003

VPN mit Windows Server 2003: Überblick

Veröffentlicht im März 2003

Zusammenfassung

Dieses Whitepaper bietet Ihnen einen Überblick über die von Windows Server 2003 und Windows XP unterstützten VPN-Technologien. Es beschreibt die Features der beiden Betriebssysteme, die Ihnen die Administration von VPN-Verbindungen in Unternehmensnetzwerken erleichtern, und gibt Hintergrundinformationen zu den beiden Industriestandards Point-to-Point-Tunneling-Protocol (PPTP) und Layer-Two-Tunneling-Protocol mit Internet-Protocol-Security (L2TP/IPSec).

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der Microsoft Corporation zum Zeitpunkt der Veröffentlichung dar. Da Microsoft auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens Microsoft dar, und Microsoft kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Dokument dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIE INFORMATIONEN IN DIESEM DOKUMENT JEDE GEWÄHRLEISTUNG AUS, SEI SIE AUSDRÜECKLICH ODER KONKLUDENT.

Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze, darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

© 2003 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Active Directory, Windows, Windows NT und das Windows-Logo sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Die in diesem Dokument aufgeführten Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

| | |
|--|----|
| Einleitung | 1 |
| Verwendung von VPNs | 2 |
| Remotenzugriff über das Internet | 2 |
| Netzwerke über das Internet verbinden | 2 |
| Computer über ein Intranet verbinden | 3 |
| Grundlegende VPN-Anforderungen | 4 |
| Tunneling-Grundlagen | 4 |
| Tunneling-Protokolle | 5 |
| Wie Tunneling arbeitet | 6 |
| Tunneling-Protokolle und die grundlegenden VPN-Anforderungen | 6 |
| Point-to-Point-Protocol (PPP) | 6 |
| Phase 1: Herstellen der PPP-Verbindung | 7 |
| Phase 2: Benutzerauthentifizierung | 7 |
| Phase 3: PPP-Rückrufsteuerung | 8 |
| Phase 4: Network Layer Protokoll-Aufruf | 8 |
| Datenübertragungsphase | 9 |
| Point-to-Point-Tunneling-Protocol (PPTP) | 9 |
| Layer-Two-Tunneling-Protocol (L2TP) | 9 |
| PPTP im Vergleich mit L2TP/IPSec | 10 |
| Vorteile von L2TP/IPSec über PPTP | 11 |
| Vorteile von PPTP über L2TP/IPSec | 11 |
| Tunnelarten | 12 |
| Freiwilliger Tunnel | 12 |
| Erzwungener Tunnel | 12 |
| Erweiterte VPN-Sicherheitsfeatures | 13 |

| | |
|--|----|
| EAP-TLS und zertifikatsbasierte Authentifizierung | 13 |
| Digitale Zertifikate..... | 14 |
| Extensible Authentication Protocol (EAP) | 14 |
| EAP-Transport Level Security (EAP-TLS) | 14 |
| Quarantänesteuerung | 15 |
| RAS-Kontosperrung..... | 15 |
| Paketfilterung über RAS-Richtlinienprofile..... | 16 |
| VPN-Administration | 16 |
| VPN-Verbindungen autorisieren | 16 |
| Skalierbarkeit | 17 |
| RADIUS..... | 17 |
| Verbindungs-Manager und verwaltete VPN-Verbindungen..... | 17 |
| Client-Verbindungs-Manager | 17 |
| Verbindungs-Manager-Verwaltungskit | 18 |
| Connection Point Services | 18 |
| Konten, Überwachung und Alarme..... | 19 |
| Zusammenfassung | 19 |
| Weitere Links zum Thema..... | 20 |

Einleitung

Ein Virtual Private Network (VPN) ist die Erweiterung eines privaten Netzwerkes, das Verbindungen über gemeinsame Netzwerke oder ein öffentliches Netzwerk wie das Internet umfasst. Ein VPN ermöglicht es Ihnen, Daten zwischen zwei Computern über ein gemeinsames oder öffentliches Netzwerk so zu senden, als wären diese beiden Computer über eine private Point-To-Point-Verbindung miteinander verbunden. Die Konfiguration und Erstellung eines Virtual Private Network wird Virtual Private Networking genannt.

Um eine Point-To-Point-Verbindung zu emulieren, werden Daten mit einem Header eingekapselt oder verpackt, der mit Routinginformationen für den Transport über das gemeinsame oder öffentliche Netzwerk ausgestattet ist. Außerdem werden die Daten verschlüsselt, um deren Vertraulichkeit zu gewährleisten. Pakete, die im gemeinsamen oder öffentlichen Netzwerk abgefangen werden, sind ohne den Verschlüsselungsschlüssel nicht zu verarbeiten. Der Teil einer Verbindung, in den die privaten Daten gekapselt werden, wird auch als Tunnel bezeichnet. Der Teil einer Verbindung, in dem die privaten Daten verschlüsselt werden, wird auch VPN-Verbindung genannt.

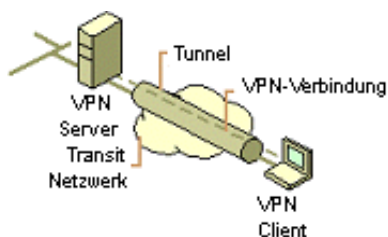


Abbildung 1: VPN-Verbindung

VPN-Verbindungen ermöglichen es Benutzern, sich von zu Hause oder unterwegs aus über einen sicheren Weg mit Hilfe der Routing-Infrastruktur eines öffentlichen Netzwerkes (zum Beispiel des Internets) mit einem Remoteserver der Organisation zu verbinden. Aus der Sicht des Benutzers ist die VPN-Verbindung eine Point-To-Point-Verbindung zwischen dem Computer des Benutzers und einem Server der Organisation. Das dazwischenliegende Netzwerk ist für den Benutzer irrelevant, da es für diesen so aussieht, als würden die Daten über eine dedizierte private Verbindung gesendet.

Außerdem ermöglicht es die VPN-Technologie Unternehmen, über ein öffentliches Netzwerk (zum Beispiel das Internet) eine Verbindung zu einer Zweigstelle oder einem anderen Unternehmen einzurichten und über diese Verbindung gesichert zu kommunizieren. Die VPN-Verbindung über das Internet arbeitet logisch als WAN (Wide Area Network) zwischen den Standorten.

In beiden Fällen ist die sichere Verbindung über das öffentliche Netzwerk für den Benutzer eine private Netzwerkkommunikation, trotz der Tatsache, dass diese Kommunikation über ein öffentliches Netzwerk stattfindet (daher der Name Virtual Private Network).

Die VPN-Technologie kommt einem aktuellen Trend in der Geschäftswelt entgegen: dem Trend zu vermehrter Telekommunikation und global verteilten Geschäftsstellen, in denen die Mitarbeiter die Gelegenheit haben müssen, zentrale Ressourcen zu nutzen, um miteinander kommunizieren zu können.

Damit Mitarbeiter unabhängig von ihrem Standort eine Verbindung mit den Computerressourcen des Unternehmens herstellen können, muss dieses eine skalierbare RAS-Lösung bereitstellen. In der Regel entscheiden sich Unternehmen entweder für eine MIS-Abteilungslösung (Management Information System) oder für ein VAN-Netzwerk (Value-added Network). Bei der MIS-Lösung wird eine interne Abteilung "Informationssysteme" mit der Beschaffung, Installation und Wartung des Modempools und

der Infrastruktur für ein privates Netzwerk beauftragt. Im Fall der VAN-Lösung wird ein Fremdunternehmen für die Beschaffung, Installation und Wartung des Modempools und der Telekommunikationsinfrastruktur bezahlt.

Keine der Lösungen bietet jedoch die erforderliche Skalierbarkeit in Bezug auf Kosten, Flexibilität der Verwaltung und Verbindungsnachfrage. Daher ist es sinnvoll, die Modempools und die Infrastruktur für das private Netzwerk durch eine kostengünstigere, auf Internettechnologie basierende Lösung zu ersetzen – damit sich das Unternehmen auf sein Kerngeschäft konzentrieren kann. Bei einer Internetlösung erfüllen, wie nachstehend beschrieben, schon wenige Internetverbindungen über einen Internet Service Provider (ISP) und VPN-Servercomputer die Anforderungen von Hunderten, ja Tausenden von Remoteclients und Zweigstellen an ein Remotenetzwerk.

Verwendung von VPNs

Die nächsten Abschnitte geben Ihnen eine detaillierte Beschreibung der am häufigsten genutzten VPN-Konfigurationen.

Remotezugriff über das Internet

VPNs ermöglichen den Remotezugriff auf Unternehmensressourcen über das öffentliche Internet unter Wahrung der Informationssicherheit. Abbildung 2 zeigt ein VPN, das einen Remotebenutzer mit dem Intranet eines Unternehmens verbindet. Eine solche Konfiguration wird auch Remote-Access-VPN-Verbindung genannt.

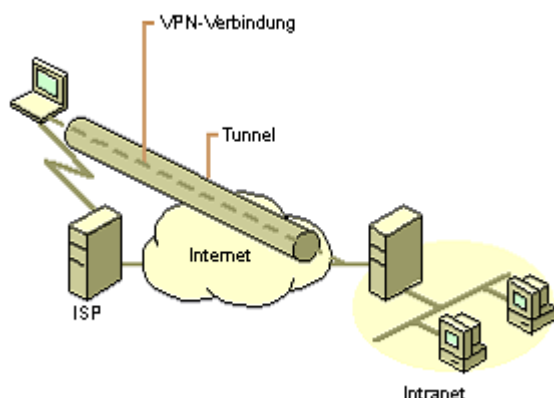


Abbildung 2: Eine VPN-Verbindung für die Anbindung eines Remote Access Clients an das Intranet der Organisation

Hierbei wählt sich der Benutzer für den Netzwerkzugriff nicht per Ferngespräch in einen Server (Network Access Server, NAS) ein, sondern per Ortsgespräch bei einem lokalen ISP. Die VPN-Software erzeugt unter Verwendung der Verbindung mit dem lokalen ISP ein virtuelles privates Netzwerk zwischen diesem Benutzer und dem VPN-Server des Unternehmens über das Internet.

Netzwerke über das Internet verbinden

Man unterscheidet zwei Verfahren, um lokale Netzwerke an Remotestandorten unter Verwendung von VPNs zu verbinden:

- **Verbinden einer Zweigstelle mit dem Unternehmens-LAN über eine Standleitung:** Anstatt eine teure Standleitung zwischen Zweigstelle und Firmenhub zu verwenden, können die Router der Zweigstelle und des Firmenhub die Verbindung mit dem Internet über eine lokale Standleitung und einen lokalen ISP herstellen. Die VPN-Software verwendet die lokalen ISP-

Verbindungen und das Internet, um ein virtuelles privates Netzwerk zwischen den Routern der Zweigstelle und des Firmenhub zu erstellen.

- **Verbinden einer Zweigstelle mit dem Unternehmens-LAN über eine DFÜ-Verbindung:**
Anstatt den Router der Zweigstelle über ein Ferngespräch in einen Unternehmens- oder ausgelagerten Server für den Netzwerkzugriff (Network Access Server, NAS) einwählen zu lassen, kann sich der Router der Zweigstelle in den lokalen ISP einwählen. Die VPN-Software verwendet die Verbindung mit dem lokalen ISP, um ein virtuelles privates Netzwerk zwischen den Routern der Zweigstelle und des Firmenhub über das Internet zu erstellen.

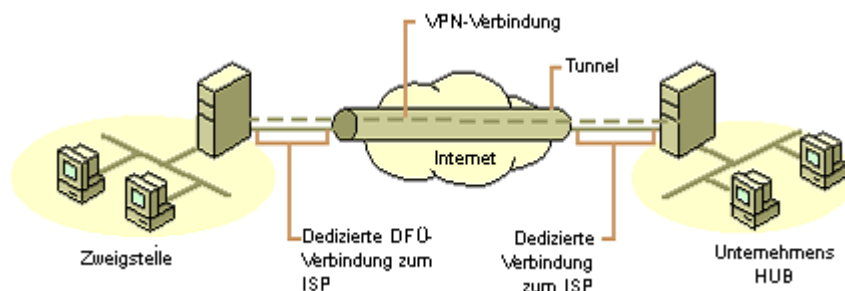


Abbildung 3: Zwei Remote-Standorte über eine VPN-Verbindung verbinden

In beiden Fällen sind es lokale Einrichtungen, die die Zweigstelle und das Unternehmen mit dem Internet verbinden. Der Router des Firmenhub, der als VPN-Server fungiert, muss mit einem lokalen ISP über eine Standleitung verbunden sein. Dieser VPN-Server muss rund um die Uhr für eingehenden VPN-Verkehr empfangsbereit sein.

Computer über ein Intranet verbinden

In einigen firmeneigenen Netzwerken verfügen bestimmte Abteilungen über derart vertrauliche Daten, dass das Abteilungs-LAN physikalisch vom übrigen firmeneigenen Netzwerk getrennt ist. Einerseits werden so die vertraulichen Abteilungsdaten geschützt, andererseits entstehen für Benutzer, die nicht physisch mit dem separaten LAN verbunden sind, Probleme beim Zugriff auf diese Daten.

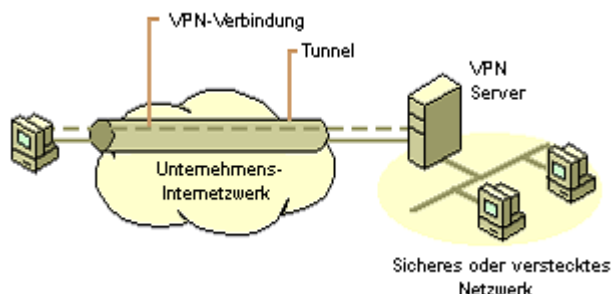


Abbildung 4: Verbinden von zwei Computern im Intranet unter Verwendung eines VPNs

Über ein VPN kann das Abteilungs-LAN einerseits physikalisch mit dem firmeneigenen Netzwerk verbunden werden, wobei es aber andererseits durch einen VPN-Server getrennt ist. Der VPN-Server fungiert nicht als Router zwischen dem firmeneigenen Netzwerk und Abteilungs-LAN. Ein Router würde die beiden Netzwerke verbinden, so dass jeder auf das sensible LAN zugreifen könnte. Mit Hilfe des VPNs kann der Netzwerkadministrator sicherstellen, dass nur Benutzer mit geeigneten Anmeldeinformationen (basierend auf unternehmensinternen Richtlinien) ein VPN mit dem Server einrichten und auf die geschützten Abteilungsressourcen zugreifen können. Darüber hinaus kann die gesamte Kommunikation über das VPN verschlüsselt werden, um die Vertraulichkeit der Daten

sicherzustellen. Benutzern ohne geeignete Anmeldeinformationen bleibt das Abteilungs-LAN verborgen.

Grundlegende VPN-Anforderungen

Ein Unternehmen, das mit einer Remotenetzwerklösung arbeitet, muss in der Regel den kontrollierten Zugriff auf die Unternehmensressourcen und –informationen gewährleisten. Die Lösung muss dafür sorgen, dass sich Clients an wechselnden Standorten oder Remoteclients mit LAN-Ressourcen verbinden können, und sie muss zulassen, dass sich Zweigstellen verbinden können, um Ressourcen und Informationen gemeinsam zu verwenden (LAN-zu-LAN-Verbindungen). Weiter muss die Lösung die Sicherheit und Integrität der Daten beim Transport im Internet sicherstellen. Dasselbe gilt für sensible Daten, die im firmeneigenen Netzwerk transportiert werden.

Daher sollte eine VPN-Lösung mindestens die folgenden Anforderungen erfüllen:

- **Benutzerauthentifizierung:** Die Lösung muss die Identität des Benutzers überprüfen und den VPN-Zugriff ausschließlich auf autorisierte Benutzer einschränken. Weiter muss sie Überwachungs- und Kontoführungseinträge führen, aus denen hervorgeht, wer wann auf welche Informationen zugegriffen hat.
- **Adressenverwaltung:** Die Lösung muss die Adresse eines Clients auf dem privaten Netz zuordnen und sicherstellen, dass private Adressen privat bleiben.
- **Datenverschlüsselung:** Die auf dem öffentlichen Netzwerk übertragenen Daten müssen für nicht autorisierte Clients auf dem Netzwerk unlesbar sein.
- **Schlüsselmanagement:** Die Lösung muss Verschlüsselungsschlüssel für den Client und den Server erzeugen und aktualisieren.

Eine Internet-VPN-Lösung auf der Basis des Point-To-Point-Tunneling-Protokolls (PPTP) oder des Layer-2-Tunneling-Protokolls (L2TP) erfüllt alle aufgeführten grundlegenden Anforderungen und nutzt die Vorteile der weltweiten Verfügbarkeit des Internets. Andere Lösungen, einschließlich des neuen IP-Security-Protokolls (IPSec) erfüllen nicht alle genannten Anforderungen, sind aber in Spezialfällen brauchbar.

Im restlichen Teil dieses Whitepaper werden die Grundlagen, Protokolle und Komponenten von VPNs eingehender beschrieben.

Tunneling-Grundlagen

Beim *Tunnelverfahren (Tunneling)* wird eine vorhandene Netzwerkinfrastruktur verwendet, um Daten für ein Netzwerk über ein anderes Netzwerk zu übertragen. Die zu übertragenden Daten (die *Datenpakete – auch Payload genannt*) können die Rahmen (auch Pakete oder Frames genannt) eines anderen Protokolls sein. Das Tunnelprotokoll sendet einen Rahmen nicht in der vom Ausgangsknoten erzeugten Form, sondern kapselt ihn in einen zusätzlichen Header. Er enthält Routinginformationen, aufgrund derer die gekapselten Datenpakete den dazwischen liegenden Transitnetzverbund (Transit Internetwork) passieren können.

Die gekapselten Pakete werden dann zwischen Tunnelendpunkten über das Netzwerk weitergeleitet. Der logische Pfad, den die gekapselten Pakete auf ihrem Weg durch das Netzwerk nehmen, wird *Tunnel* genannt. Sobald die gekapselten Rahmen ihr Ziel im Netzwerk erreichen, wird die Kapselung aufgehoben und der entkapselte Rahmen an seinen Zielort weitergeleitet. Das Tunnelverfahren umfasst den gesamten beschriebenen Prozess (Kapselung, Übertragung und Entkapselung der Pakete).

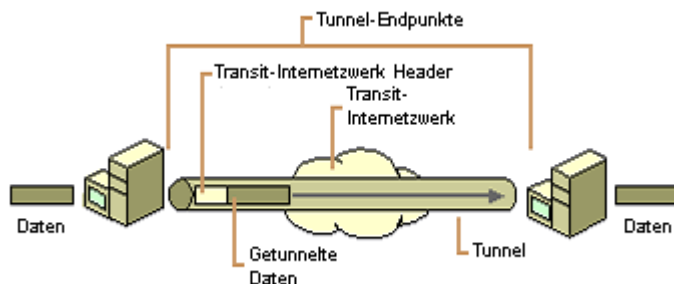


Abbildung 5: Tunneling

Der Transitnetzverbund kann jedes beliebige Netzwerk sein - das Internet als öffentliches Netzwerk ist das bekannteste reale Beispiel. Zahlreiche Beispiele für Tunnel, die über ein firmeneigenes Netzwerk durchgeführt werden, sind bekannt. Während das Internet eines der am meisten verbreiteten und kostengünstigsten Netzwerke darstellt, können die Verweise auf das Internet im vorliegenden Whitepaper durch jedes andere öffentliche oder private Netzwerk, das als Transitnetzverbund fungiert, ersetzt werden.

Tunneling-Technologien (wie zum Beispiel SNA-Tunneling über IP-Netzwerke) gibt es schon seit einiger Zeit. Wenn SNA-Verkehr (System Network Architecture) über ein IP-Netzwerk geschickt wird, wird das SNA-Frame in einen UDP- oder IP-Header gekapselt. In den letzten Jahren wurden neue Tunneling-Technologien entwickelt. Dieses Whitepaper konzentriert sich primär auf diese neuen Technologien. Hierbei handelt es sich um:

- **Point-to-Point-Tunneling-Protocol (PPTP):** PPTP ermöglicht es, Netzwerkverkehr verschiedenster Protokolle zu verschlüsseln und dann mit einem IP-Header zu kapseln und so über ein IP-Netzwerk (zum Beispiel dem Internet) zu übertragen.
- **Layer-Two-Tunneling-Protocol (L2TP):** L2TP ermöglicht die Verschlüsselung und Versendung verschiedenster Netzwerkprotokolle über jedes Medium, das Point-to-Point-Datagram-Delivery unterstützt (zum Beispiel IP, X.25, Frame Relay oder ATM).
- **IPSec-Tunnelmodus:** Der IPSec-Tunnelmodus ermöglicht es, IP-Pakete zu verschlüsseln, diese dann in einen IP-Header zu kapseln und dann zum Beispiel über ein öffentliches IP-Netzwerk zu versenden. Beim IPSec-Tunnelmodus handelt es sich nicht um eine für VPN-Verbindungen empfohlene Technologie, da es keine Standardverfahren zur Benutzerauthentifizierung, zur IP-Adresszuweisung und zur Zuweisung der Nameserver-Adresse gibt. Die Verwendung des IPSec-Tunnelmodus für Site-To-Site VPN-Verbindungen ist mit Computern unter Windows Server 2003 möglich. Da IPSec-Tunnel nicht als logische Schnittstelle angezeigt werden, können keine Routen für die Nutzung des Tunnels zugewiesen werden und Routingprotokolle arbeiten nicht über IPSec-Tunnel. Aus diesen Gründen wird die Verwendung des IPSec-Tunnelmodus nur als VPN-Lösung für Site-To-Site VPN-Verbindungen empfohlen, bei denen ein Ende des Tunnels ein Drittanbieter-VPN-Server oder ein Sicherheitgateway ohne L2TP/IPSec-Unterstützung ist.

Tunneling-Protokolle

Um einen Tunnel einrichten zu können, müssen Tunnelclient und Tunnelserver dasselbe *Tunnelprotokoll* verwenden. Tunneltechnologie kann auf einem Schicht-2- oder einem Schicht-3-Tunnelprotokoll basieren. Beide Schichten entsprechen dem OSI-Referenzmodell (Open Systems Interconnection). Schicht-2-Protokolle entsprechen der Sicherungsschicht (Data-Link Layer) und verwenden *Rahmen* als Übertragungseinheit. PPTP-, L2TP- und Layer-2-Forwarding (L2F) sind Schicht-2-Tunnelprotokolle; sie kapseln Datenpakete in einen PPP-Rahmen, der über das Netzwerk gesendet wird. Der IPSec-Tunnelmodus ist ein Beispiel für ein Schicht-3-Tunneling-Protokoll und kapselt IP-Pakete in einen zusätzlichen IP-Header.

Wie Tunneling arbeitet

Bei Schicht-2-Tunneltechnologien, wie z. B. PPTP und L2TP, ist ein Tunnel mit einer Sitzung vergleichbar. Beide Tunnelendpunkte müssen mit dem Tunnel einverstanden sein und Konfigurationsvariablen wie z. B. Adresszuweisung, Verschlüsselungs- oder Komprimierungsparameter aushandeln. In den meisten Fällen werden die über den Tunnel übertragenen Daten unter Verwendung eines datagrammbasierten Protokolls gesendet.

Sobald ein Tunnel eingerichtet ist, können die getunnelten Daten gesendet werden. Der Tunnelclient oder der Server bereitet die Daten mit einem Übertragungsprotokoll für die Übertragung vor. Wenn der Tunnelclient beispielsweise Datenpakete an den Tunnelserver sendet, fügt er zuerst einen Header für das Übertragungsprotokoll zu den Datenpaketen hinzu. Dann sendet der Client die gekapselten Datenpakete über das Netzwerk, wo sie an den Tunnelserver weitergeleitet werden. Der Tunnelserver nimmt die Pakete entgegen, entfernt den Header des Tunneldaten-Übertragungsprotokolls und leitet die Datenpakete an das Zielnetzwerk weiter. Die Informationen, die zwischen Tunnelserver und Tunnelclient ausgetauscht werden, werden genauso behandelt.

Tunneling-Protokolle und die grundlegenden VPN-Anforderungen

Da sie auf dem PPP-Protokoll basieren, verfügen PPTP und L2TP über einige der nützlichen Features von PPP:

- **Benutzerauthentifizierung:** PPTP und L2TP übernimmt die Benutzerauthentifizierungsschemata von PPP – und zwar auch die später in diesem Whitepaper besprochenen EAP-Verfahren. Mit dem EAP-Protokoll (Extensible Authentication Protocol) unterstützen PPTP- und L2TP-Verbindungen eine große Zahl von Authentifizierungsverfahren (unter anderem Einmal-Passwörter und Smartcards).
- **Dynamische Adresszuweisung:** PPTP- und L2TP-Verbindungen unterstützen die dynamische Zuweisung von Clientadressen basierend auf dem NCP-Aushandlungsmechanismus (Network Control Protocol). IP verwendet zum Beispiel das Internet Protocol Control Protocol (IPCP) zu Aushandlung einer IP-Adresse.
- **Datenkomprimierung:** PPTP und L2TP unterstützen PPP-basierte Kompression. Die Microsoft-Implementierungen von PPTP und L2TP verwenden die Microsoft Point-to-Point-Compression (MPPC).
- **Datenverschlüsselung:** PPTP und L2TP unterstützen PPP-basierte Mechanismen zur Datenverschlüsselung. Die Microsoft-Implementierung von PPTP unterstützt die Verwendung von Microsoft Point-to-Point Encryption (MPPE), die auf dem RSA/RC4-Algorithmus basiert. Die Microsoft-Implementierung von L2TP verwendet IPsec-Verschlüsselung, um den Datenstrom zwischen VPN-Client und VPN-Server zu schützen.
- **Schlüsselverwaltung:** MPPE für PPTP-Verbindungen ist von dem Initialschlüssel, der während der Benutzerauthentifizierung erzeugt wird, abhängig. Dieser wird regelmäßig erneuert. IPsec für L2TP/IPsec-Verbindungen handelt während des IKE-Austausches explizit einen allgemeinen Schlüssel aus. Auch dieser wird regelmäßig erneuert.

Point-to-Point-Protocol (PPP)

Da PPTP und L2TP stark von den ursprünglich für PPP festgelegten Leistungsmerkmalen abhängen, lohnt es sich, dieses Protokoll näher zu untersuchen. PPP wurde entwickelt, um Daten über Wählleitungen oder dedizierte Punkt-zu-Punkt-Verbindungen (Standleitungen) zu senden. PPP kapselt IP-Pakete in PPP-Rahmen und überträgt dann die PPP-gekapselten Pakete über eine Punkt-zu-Punkt-Verbindung. PPP wird zwischen einem DFÜ-Client und einem NAS verwendet.

Es gibt bei der Aushandlung einer PPP-Verbindung vier eindeutige Phasen. Jede dieser vier Phasen muss erfolgreich abgeschlossen werden, bevor eine PPP-Verbindung für eine Datenübertragung bereit ist.

Phase 1: Herstellen der PPP-Verbindung

PPP verwendet das Link-Control-Protokoll (LCP), um die physische Verbindung einzurichten, zu verwalten und zu beenden. In der LCP-Anfangsphase werden grundlegende Kommunikationsoptionen ausgewählt. Während dieser Phase werden Authentifizierungsprotokolle ausgewählt, jedoch erst in der Benutzerauthentifizierungsphase (Phase 2) implementiert. Ähnlich wird mit dem LCP festgelegt, ob die beiden Peers die Verwendung einer Komprimierung und/oder Verschlüsselung aushandeln sollen. Die Komprimierungs- und Verschlüsselungsalgorithmen selbst, sowie weitere Einzelheiten werden aber erst in Phase 4 ausgewählt.

Phase 2: Benutzerauthentifizierung

In der zweiten Phase gibt der Client-PC die Anmeldeinformationen dem RAS-Server bekannt. Ein sicheres Authentifizierungsverfahren bietet Schutz vor Wiederholungsangriffen und vor Imitationen des Remoteclients. Ein *Wiederholungsangriff* tritt auf, wenn ein Dritter eine erfolgreiche Verbindung überwacht, Pakete sammelt und diese verwendet, um die Antworten des Remoteclients zu wiederholen und sich dadurch eine authentifizierte Verbindung zu verschaffen. Von einer *Imitation des Remoteclients* wird gesprochen, wenn ein Dritter eine authentifizierte Verbindung übernimmt. Der Eindringling wartet, bis die Verbindung authentifiziert wurde, fängt dann die Verbindungsparameter ab, trennt die Verbindung des authentifizierten Benutzers und übernimmt dann selbst die authentifizierte Verbindung.

Windows Server 2003 und Windows XP unterstützen die folgenden PPP-Authentifizierungsprotokolle:

- **Password-Authentication-Protokoll (PAP):** PAP ist ein einfaches Klartext-Authentifizierungsverfahren. Der NAS fordert den Benutzernamen und das Kennwort an, und PAP gibt beide als Klartext (unverschlüsselt) zurück. Offensichtlich ist das Authentifizierungsverfahren nicht sicher, da ein Dritter ohne weiteres Benutzernamen und Kennwort abfangen und verwenden kann, um selbst Zugriff auf den NAS und seine Ressourcen zu erhalten. PAP bietet keinen Schutz vor Wiederholungsangriffen oder Imitationen des Remoteclients, sobald das Kennwort des Benutzers bekannt ist.
- **Challenge-Handshake Authentication-Protokoll (CHAP):** CHAP ist ein verschlüsseltes Authentifizierungsverfahren, bei dem das Kennwort nicht auf der Verbindung übertragen wird. Der NAS sendet eine Herausforderung (Challenge), bestehend aus einer Sitzungs-ID und einem zufälligen Herausforderungsstring, an den Remoteclient. Der Remoteclient muss unter Verwendung des MD5-Hashing-Algorithmus den Benutzernamen sowie die verschlüsselte Herausforderung, Sitzungs-ID und das Kennwort des Clients zurückgeben. Der Benutzername wird im Klartext übertragen.
CHAP ist insofern eine Weiterentwicklung von PAP, als dass das Klartextkennwort nicht über die Verbindung übertragen wird. Stattdessen wird das Kennwort verwendet, um aus der ursprünglichen Herausforderung ein verschlüsseltes Hash zu erstellen. Der Server kennt das Klartextkennwort des Benutzers und kann daher die Operation replizieren und das Ergebnis mit dem Kennwort vergleichen, das in der Antwort des Clients gesendet wurde. CHAP schützt vor Wiederholungsangriffen, indem bei jedem Authentifizierungsversuch ein zufälliger Herausforderungsstring verwendet wird. CHAP schützt vor Imitationen des Remoteclients, indem in nicht vorhersehbarer Weise während der gesamten Verbindungszeit wiederholt Herausforderungen (Challenges) an den Remoteclient gesendet werden.
- **Microsoft-Challenge-Handshake Authentication Protocol (MS-CHAP):** MS-CHAP ist CHAP sehr ähnlich. Wie bei CHAP auch, sendet der NAS eine Challenge, die aus einer Session-ID

und einem zufälligen Challenge-String besteht, an den Remote Client. Dieser muss den Benutzernamen und eine verschlüsselte Form des Challenge-Strings, der Sitzungs-ID und das MD4-gehashte Passwort zurückschicken. Die Verwendung des MD4-Hashes bietet eine zusätzliche Sicherheit, da der Server hier gehashte Passwörter statt Klartext-Passwörter speichern kann. MS-CHAP bietet außerdem zusätzliche Fehlercodes (unter anderem einen Code für abgelaufene Passwörter) und zusätzliche verschlüsselte Client-Server-Nachrichten. Diese ermöglichen dem Benutzer eine Passwortänderung. Bei MS-CHAP generieren sowohl der Access Client als auch der NAS unabhängig voneinander einen initialen Verschlüsselungsschlüssel für die nachfolgende Datenverschlüsselung durch MPPE. Daher ist MS-CHAP eine Voraussetzung für eine Datenverschlüsselung auf Basis von MPPE.

- **MS-CHAP Version 2 (MS-CHAP v2):** MS-CHAP v2 ist ein aktualisierter verschlüsselter Authentifizierungsmechanismus, der eine stärkere Sicherheit beim Austausch von Benutzernamen und Passwort und in der Festsetzung von Verschlüsselungsschlüsseln bietet. Mit MS-CHAP v2 sendet der NAS eine Challenge an den Access Client, die aus einer Sitzungs-ID und einem zufälligen Challenge-String besteht. Der Client sendet eine Antwort, die den Benutzernamen, einen zufälligen Partner-Challenge-String und eine verschlüsselte Form des empfangenen Challenge-Strings, des Partner-Challenge-Strings, der Sitzungs-ID und des Benutzerpassworts enthält. Der NAS prüft die Antwort des Clients und sendet eine Antwort zurück, die den Erfolg oder Fehlschlag des Verbindungsversuches anzeigt. Sie enthält außerdem eine auf dem gesendeten Challenge-String basierende Authentifizierungsantwort, den Partner-Challenge-String, die verschlüsselte Antwort des Clients und das Benutzerpasswort. Der Client prüft die Authentifizierungsantwort, und wenn diese korrekt ist, verwendet er die Verbindung. Wenn die Authentifizierungsantwort nicht korrekt ist, trennt der Client die Verbindung.

Mit diesem Verfahren bietet MS-CHAP v2 eine gegenseitige Authentifizierung – der NAS prüft, dass der Client das Benutzerpasswort kennt, und der Client prüft, ob der Server das Benutzerpasswort kennt. MS-CHAP v2 legt außerdem zwei Verschlüsselungsschlüssel fest: Einen für die versendeten Daten und einen für die empfangenen Daten.
- **Extensible Authentication Protocol (EAP):** EAP ist ein neues PPP-Authentifizierungsprotokoll, das eine beliebige Authentifizierungsmethode ermöglicht. EAP wird im Abschnitt *Extensible Authentication Protocol (EAP)* dieses Whitepapers beschrieben. Es unterscheidet sich von anderen Authentifizierungsprotokollen darin, dass es während des Authentifizierungsprozesses keine Authentifizierungen durchführt. In Phase 2 wird bei EAP nur die Verwendung einer allgemeinen EAP-Authentifizierungsmethode ausgehandelt (auch EAP-Typ genannt). Die tatsächliche Authentifizierung findet erst nach Phase 2 statt.

Während der Phase 2 der PPP-Verbindungsconfiguration sammelt der NAS die Authentifizierungsdaten und prüft sie über seine Benutzerdatenbank oder einen zentralen Authentifizierungs-Datenbankserver (zum Beispiel ein Windows Domänencontroller), oder die Authentifizierungsdaten werden an einen RADIUS-Server weitergeleitet.

Phase 3: PPP-Rückrufsteuerung

Die PPP-Implementierung von Microsoft schließt eine optionale Rückrufsteuerungsphase ein. In dieser Phase wird das Callback-Control-Protokoll (CBCP) unmittelbar nach der Authentifizierungsphase verwendet. Wurde der Rückruf konfiguriert, so trennen Remoteclient und NAS die Verbindung nach der Authentifizierung. Der NAS ruft dann den Remoteclient unter einer festgelegten Telefonnummer zurück. So wird eine zusätzliche Sicherheitsstufe für DFÜ-Netzwerkverbindungen geschaffen. Der NAS gestattet Verbindungen von Remoteclients nur von bestimmten, vorher festgelegten Telefonnummern. Ein Rückruf kann nur für Einwahlverbindungen und nicht für VPN-Verbindungen verwendet werden.

Phase 4: Network Layer Protokoll-Aufruf

Sobald die vorangehenden Phasen abgeschlossen sind, startet PPP die verschiedenen Schicht-3-Protokolle (Network Control Protocols, NCPs), die in Phase 1 (Herstellung der PPP-Verbindung) ausgewählt wurden. Während dieser Phase wird zum Beispiel IPCP verwendet, um dem Client eine dynamische IP-Adresse zuzuweisen, oder das Compression-Control-Protocol (CCP) wird zur Aushandlung von Datenkomprimierung (über MPPC) und Datenverschlüsselung (über MPPE) verwendet.

Datenübertragungsphase

Sobald die vier Aushandlungsphasen abgeschlossen sind, beginnt PPP damit, Daten zwischen den beiden Peers weiterzuleiten. Jedes übertragene Datenpaket wird in einen PPP-Header eingeschlossen, der vom empfangenden System entfernt wird. Wurde Datenkomprimierung in Phase 1 ausgewählt und in Phase 4 ausgehandelt, so werden die Daten vor der Übertragung komprimiert. Wenn Datenverschlüsselung ausgewählt und ausgehandelt wurde, werden die Daten vor der Übertragung verschlüsselt.

Point-to-Point-Tunneling-Protocol (PPTP)

PPTP kapselt PPP-Frames für den Transport über ein IP-Netzwerk, wie zum Beispiel das Internet, in IP-Datagramme. PPTP kann für Remote-Zugriff-Verbindungen und Router-zu-Router VPN-Verbindungen verwendet werden und ist in RFC 2637 dokumentiert.

Das Point-to-Point Tunneling Protocol (PPTP) verwendet eine TCP-Verbindung für die Tunnelverwaltung und eine modifizierte Generic-Routing-Encapsulation-Version (GRE) zur Kapselung von PPP-Frames. Der Payload eines gekapselten PPP-Frames kann verschlüsselt und/oder komprimiert werden. Die Struktur eines PPTP-Paketes mit einem IP-Datagramm sehen Sie in Abbildung 6.

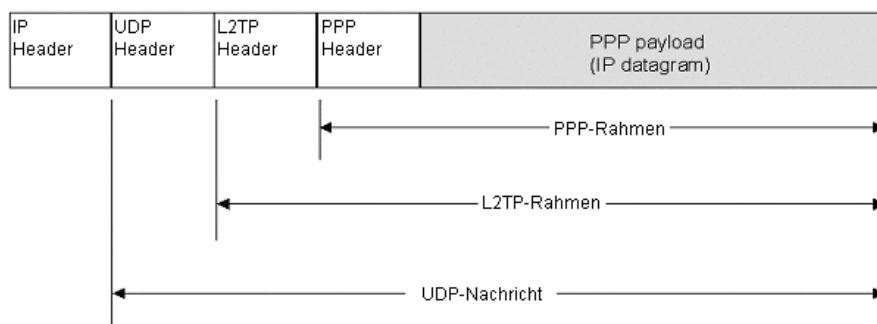


Abbildung 6: Struktur eines PPTP-Paketes, das ein IP-Datagramm enthält

Layer-Two-Tunneling-Protocol (L2TP)

L2TP ist eine Kombination von PPTP und Layer-2-Forwarding (L2F) und wurde von Cisco Systems entwickelt. L2TP fasst die besten Features von PPTP und L2F zusammen. L2TP kapselt PPP-Frames, damit diese über ein IP, X.25, Frame Relay oder ATM-Netzwerk übertragen werden können. Wenn es mit IP zum Datagrammtransport konfiguriert wurde, kann L2TP als Tunneling-Protokoll über das Internet verwendet werden. L2TP ist in RFC 2661 dokumentiert.

Bei L2TP über IP-Netzwerke werden zur Tunnelverwaltung UDP und einige L2TP-Nachrichten verwendet. Außerdem werden die Tunneldaten über UDP als L2TP gekapselte PPP-Frames versendet. Der Payload von gekapselten PPP-Frames kann verschlüsselt und/oder komprimiert werden. Die

Microsoft-Implementierung von L2TP verwendet zur Verschlüsselung allerdings kein MPPE. Abbildung 7 zeigt die Struktur eines L2TP-Pakets, das ein IP-Datagramm enthält.

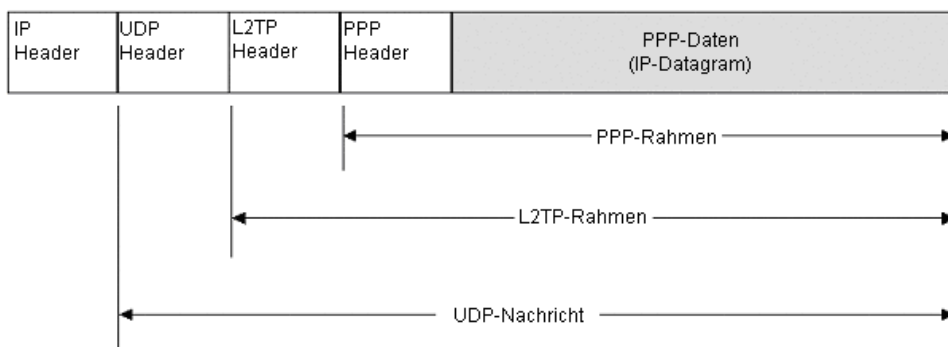


Abbildung 7: Struktur eines L2TP-Pakets das ein IP-Datagramm enthält

Bei der Microsoft-Implementierung von L2TP wird IPSec-Encapsulating-Security_Payload (ESP) zur Verschlüsselung des L2TP-Verkehrs genutzt. Die Kombination von L2TP (das Tunneling-Protokoll) und IPSec (die Verschlüsselungsmethode) wird L2TP/IPSec genannt. L2TP/IPSec wird in RFC 3193 beschrieben.

Das Ergebnis der Bearbeitung eines IP-Pakets, das eine L2TP-Nachricht enthält durch ESP, sehen Sie in Abbildung 8.

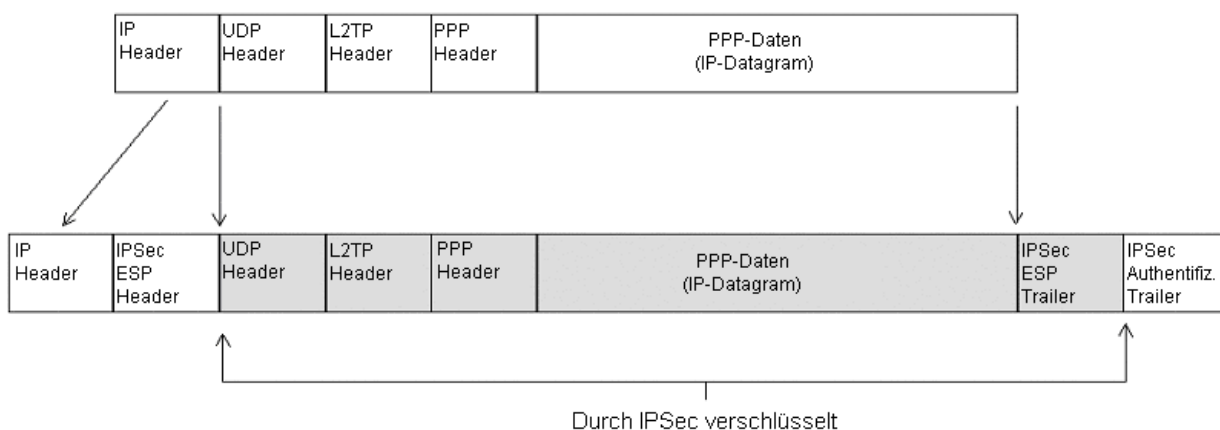


Abbildung 8: Verschlüsselung von L2TP-Verkehr durch IPSec ESP

PPTP im Vergleich mit L2TP/IPSec

Sowohl PPTP als auch L2TP/IPSec verwendet PPP für die Kapselung der Daten. Dann werden zusätzliche Header für den Transport der Daten über das Netzwerk hinzugefügt. In den folgenden Punkten unterscheiden sich die beiden Protokolle:

- Bei PPTP beginnt die Verschlüsselung nach dem PPP-Verbindungs Aufbau. Mit L2TP/IPSec wird die Datenverschlüsselung vor dem PPP-Verbindungs Aufbau durch die IPSec-Sicherheitszuordnung durchgeführt.

- PPTP-Verbindungen nutzen MPPE – eine Verschlüsselung, die auf dem Rivest-Shamir-Aldeman-(RSA) RC-4-Verschlüsselungsalgorithmus basiert und 40, 56 oder 128 Bit lange Verschlüsselungsschlüssel verwendet. Die Daten werden als Bit-Stream verschlüsselt. L2TP/IPSec-Verbindungen verwenden zur Verschlüsselung den Data Encryption Standard (DES). Hierbei handelt es sich um eine Block-Verschlüsselung mit einem 56-Bit Schlüssel bei DES oder drei 56-Bit Schlüssel bei 3-DES. Die Block-Verschlüsselung verschlüsselt Daten in diskreten Blöcken (im Fall von DES sind dies 64-Bit-Blöcke).
- PPTP-Verbindungen benötigen nur eine Authentifizierung auf Benutzerebene über ein PPP-basierendes Authentifizierungsprotokoll. L2TP/IPSec hingegen erfordert zusätzlich zu dieser Authentifizierung auf Benutzerebene auch noch eine Authentifizierung auf Computerebene über Computerzertifikate.

Vorteile von L2TP/IPSec über PPTP

Die Verwendung von L2TP/IPSec über PPTP mit Windows Server 2003 bietet Ihnen die folgenden Vorteile:

- IPSec ESP bietet Ihnen für jedes einzelne Paket eine Authentifizierung (ein Beweis dafür, dass die Daten durch den autorisierten Benutzer gesendet wurden), eine Sicherstellung der Datenintegrität (ein Beweis dafür, dass die Daten während der Übertragung nicht verändert wurden), einen Schutz vor Wiederholungs-Angriffen (verhindert, dass abgefangene Pakete erneut gesendet werden) und eine Datenvertraulichkeit (über die Verschlüsselung). PPTP bietet Ihnen im Gegensatz dazu nur eine Sicherung der Datenvertraulichkeit auf Paketebene.
- L2TP/IPSec-Verbindungen unterstützen eine stärkere Authentifizierung, da sie sowohl eine Authentifizierung auf Computerebene (über Zertifikate) und auf Benutzerebene (über ein PPP-Authentifizierungsprotokoll) erfordern.
- PPP-Pakete werden während der Benutzerauthentifizierung verschlüsselt verschickt. Dies liegt daran, dass der PPP-Verbindungsaufbau bei L2TP/IPSec nach der IPSec-Sicherheitszuordnung stattfindet. Wenn die PPP-Autorisierung abgefangen wird, können diese Daten bei manchen PPP-Authentifizierungsprotokollen für einen Offline- Wörterbuchangriff verwendet werden. So könnte der Angreifer Benutzerpasswörter erlangen. Durch die Verschlüsselung der PPP-Authentifizierung werden solche Angriffe sehr viel schwieriger.

Vorteile von PPTP über L2TP/IPSec

Die folgenden Vorteile haben Sie bei der Nutzung von PPTP über L2TP/IPSec mit Windows Server 2003:

- Für PPTP ist keine Zertifizierungsinfrastruktur erforderlich. L2TP/IPSec benötigt eine solche Infrastruktur zum Ausstellen von Computerzertifikaten für den VPN-Server und alle VPN-Clients.
- PPTP-Clients können auch unter Verwendung von NAT (Network Address Translator) betrieben werden. Allerdings nur, wenn die NAT-Implementierung die Verarbeitung von PPTP-Verkehr unterstützt. L2TP/IPSec-basierte VPN-Clients und Server können nicht mit NAT zusammen betrieben werden. Es sei den, sowohl Server als auch Client unterstützen IPSec-NAT-Traversal (NAT-T). IPSec-NAT-T wird von Windows Server 2003, dem Microsoft L2TP/IPSec VPN-Client und dem L2TP/IPSec NAT-T Update für Windows XP und Windows 2000 zur Verfügung gestellt.

Weitere Informationen finden Sie in *Microsoft L2TP/IPSec VPN Client* unter

<http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp>

(englischsprachig) und *L2TP/IPSec NAT-T Update for Windows XP and Windows 2000* unter <http://support.microsoft.com/default.aspx?scid=kb;en-us;818043> (englischsprachig).

Tunnelarten

Tunnel können auf unterschiedliche Arten eingerichtet werden:

- **Freiwillige Tunnel (auch Voluntary-Tunnel genannt):** Ein Benutzer oder Clientcomputer kann eine VPN-Anforderung absetzen, um einen freiwilligen Tunnel zu erstellen. In diesem Fall stellt der Computer des Benutzers einen Endpunkt dar und fungiert als Tunnelclient.
- **Erzwungene Tunnel (auch Compulsory-Tunnel oder Mandatory-Tunnel):** Ein VPN-fähiger Server für den DFÜ-Zugriff konfiguriert und erstellt einen erzwungenen Tunnel. Im Fall eines erzwungenen Tunnels stellt der Computer des Benutzers keinen Endpunkt dar. Tunnelendpunkt ist ein anderes Medium - der RAS-Server. Er befindet sich zwischen dem Computer des Benutzers und dem Tunnelserver und fungiert als Tunnelclient.

Derzeit scheint sich der freiwillige Tunnel als der beliebtere Tunneltyp herauszustellen. In den folgenden Abschnitten werden beide Tunneltypen ausführlicher beschrieben.

Freiwilliger Tunnel

Ein freiwilliger Tunnel entsteht, wenn eine Arbeitsstation oder ein Routingserver mit Hilfe der Tunnelclient-Software eine virtuelle Verbindung mit dem Ziertunnelserver erstellt. Zu diesem Zweck muss das geeignete Tunnelprotokoll auf dem Clientcomputer installiert werden. Für die in diesem Whitepaper beschriebenen Protokolle erfordern freiwillige Tunnel eine IP-Verbindung (LAN oder Einwahl).

Im Einwählfall muss der Client eine DFÜ-Verbindung mit dem Netzwerk herstellen, bevor er einen Tunnel einrichten kann. Dies ist der häufigste Fall. Das bekannteste Beispiel ist der Internetbenutzer, der sich über einen ISP einwählen und eine Internetverbindung erhalten muss, bevor ein Tunnel über das Internet erstellt werden kann.

Bei einem über ein LAN angeschlossenen Computer verfügt der Benutzer bereits über eine Netzwerkverbindung, über die die gekapselten Datenpakete an den ausgewählten LAN-Tunnelserver weitergeleitet werden können. Dies trifft auf einen Client in einem Firmen-LAN zu, der einen Tunnel initiiert, um ein privates oder verborgenes Subnetz auf diesem LAN zu erreichen (beispielsweise das weiter oben erwähnte Personalnetzwerk).

Häufig besteht die falsche Vorstellung, dass VPNs auf eine DFÜ-Verbindung angewiesen sind. Tatsächlich erfordern sie nur ein IP-Netzwerk. Bestimmte Clients (z. B. Heimcomputer) verwenden DFÜ-Verbindungen in das Internet, um die IP-Übertragung einzurichten. Dabei handelt es sich jedoch um eine Vorstufe bei der Vorbereitung der Tunnelerstellung, die kein Teil des Tunnelprotokolls ist.

Erzwungener Tunnel

Einige Hersteller von Servern für den DFÜ-Zugriff haben die Möglichkeit vorgesehen, einen Tunnel im Auftrag des DFÜ-Clients zu erstellen. Der Computer oder das Netzwerkgerät, der beziehungsweise das den Tunnel für den Clientcomputer bereitstellt, wird gewöhnlich bei PPTP als Front-End-Processor (FEP), bei L2TP als L2TP-Access-Concentrator (LAC) und bei IPSec als IP-Security-Gateway bezeichnet. Im vorliegenden Whitepaper reicht es aus, diese Funktionalität unabhängig vom Tunnelprotokoll mit dem Begriff FEP zu umschreiben. Damit der FEP seine Funktion durchführen kann, muss das entsprechende Tunnelprotokoll installiert sein, und der FEP muss in der Lage sein, den Tunnel einzurichten, wenn der Clientcomputer die Verbindung herstellt.

Im obigen Internetbeispiel wählt sich der Clientcomputer beim lokalen ISP in einen Tunneling-fähigen NAS ein. Beispielsweise könnte ein Unternehmen vertraglich mit einem ISP vereinbart haben, dass

dieser bundesweit FEPs bereitstellt. Die FEPs können über das Internet Tunnel zu einem Tunnelserver einrichten, der mit dem privaten Unternehmensnetzwerk verbunden ist. Auf diese Weise werden Anrufe aus allen Landesteilen in einer einzigen Internetverbindung auf dem Unternehmensnetzwerk gebündelt.

Diese Konfiguration wird als erzwungener Tunnel bezeichnet, da der Client dazu gezwungen ist, den vom FEP erstellten Tunnel zu verwenden. Sobald die Anfangsverbindung hergestellt ist, wird der gesamte Netzwerkverkehr zum und vom Client automatisch durch den Tunnel gesendet. Bei Verwendung des erzwungenen Tunnels richtet der Clientcomputer eine einzige PPP-Verbindung ein. Wenn sich ein Client in den NAS einwählt, wird ein Tunnel erstellt, und der gesamte Netzwerkverkehr wird automatisch durch den Tunnel geleitet. Ein FEP kann so konfiguriert werden, dass alle DFÜ-Clients an einen bestimmten Tunnelserver getunnelt werden. Der FEP kann Clients aber auch individuell tunneln, abhängig vom Benutzernamen oder Ziel.

Anders als im Fall der separaten Tunnel, die für jeden freiwilligen Client erstellt werden, kann ein Tunnel zwischen FEP und Tunnelserver von mehreren DFÜ-Clients gemeinsam verwendet werden. Wenn sich ein zweiter Client in den FEP einwählt, um ein Ziel zu erreichen, für das bereits ein Tunnel vorhanden ist, braucht keine neue Instanz des Tunnels zwischen FEP und Tunnelserver erstellt werden. Stattdessen wird der Datenverkehr für den neuen Client über den vorhandenen Tunnel übertragen. Da mehrere Clients einen Tunnel gemeinsam verwenden können, wird der Tunnel erst beendet, wenn der letzte Tunnelbenutzer die Verbindung trennt.

Erweiterte VPN-Sicherheitsfeatures

Da das Internet die VPN-Erstellung von jedem beliebigen Ort aus ermöglicht, brauchen Netzwerke starke Sicherheitsfunktionen, um den unerwünschten Zugriff auf private Netzwerke zu verhindern und um private Daten beim Durchqueren des öffentlichen Netzwerkes zu schützen. Benutzerauthentifizierung und Datenverschlüsselung wurden bereits erläutert. Dieser Abschnitt stellt Ihnen die erweiterten Sicherheitsfeatures vor, die Ihnen bei Windows Server 2003 und Windows XP VPN-Verbindungen zur Verfügung stehen.

EAP-TLS und zertifikatsbasierte Authentifizierung

Die symmetrische Verschlüsselung (auch Verschlüsselung mit privatem Schlüssel oder konventionelle Verschlüsselung genannt) basiert auf einem Geheimschlüssel, der von den beiden kommunizierenden Parteien gemeinsam verwendet wird. Der Absender verwendet den Geheimschlüssel bei der mathematischen Operation, die Klartext in verschlüsselten Text umwandelt. Empfangsseitig dient derselbe Geheimschlüssel zur Umwandlung des verschlüsselten Textes in Klartext. Beispiele für symmetrische Verschlüsselungsverfahren sind der RSA RC4-Algorithmus (Basis der Microsoft Punkt-zu-Punkt-Verschlüsselung - MPPE) und die DES-Verschlüsselung (Data Encryption Standard), die für die IPSec-Verschlüsselung verwendet wird.

Die asymmetrische Verschlüsselung (auch Verschlüsselung mit öffentlichem Schlüssel genannt) verwendet für jeden Benutzer zwei verschiedene Schlüssel: einen privaten Schlüssel, den allein der betreffende Benutzer kennt, und den zugehörigen öffentlichen Schlüssel, auf den jeder zugreifen kann. Der private und der öffentliche Schlüssel stehen über einen mathematischen Verschlüsselungsalgorithmus in Beziehung. Ein Schlüssel wird für die Verschlüsselung verwendet, der andere Schlüssel für die Entschlüsselung - abhängig vom implementierten Kommunikationsdienst.

Darüber hinaus gestatten Verschlüsselungstechnologien mit öffentlichen Schlüsseln, Nachrichten mit digitalen Signaturen zu versehen. Eine digitale Signatur stellt einen Teil der Nachricht dar, die mithilfe des Privatschlüssels des Absenders verschlüsselt wurde. Beim Empfangen der Nachricht verwendet der Empfänger den öffentlichen Schlüssel des Absenders, um die digitale Signatur zu entschlüsseln und dadurch die Identität des Absenders zu überprüfen.

Digitale Zertifikate

Bei der symmetrischen Verschlüsselung verfügen Absender und Empfänger über einen gemeinsamen geheimen Schlüssel. Die Verteilung des geheimen Schlüssels muss (mit geeigneten Schutzmaßnahmen) erfolgt sein, bevor eine verschlüsselte Kommunikation stattfindet. Bei der asymmetrischen Verschlüsselung verwendet der Absender dagegen einen privaten Schlüssel, um Nachrichten zu verschlüsseln oder digital zu signieren, während der Empfänger die Nachricht mit einem öffentlichen Schlüssel entschlüsselt. Der öffentliche Schlüssel kann an jeden, der eine verschlüsselte oder digital signierte Nachricht erhalten soll, frei verteilt werden. Nur den privaten Schlüssel muss der Absender geheim halten und schützen.

Um die Integrität des öffentlichen Schlüssels zu wahren, wird er mit einem Zertifikat veröffentlicht. Ein Zertifikat ist eine Datenstruktur, die von einer Zertifizierungsstelle (auch Certification Authority oder CA genannt) signiert ist – dieser Zertifizierungsstelle können die Benutzer dieses Zertifikats vertrauen. Das Zertifikat enthält mehrere Werte, wie zum Beispiel dem Zertifikatsnamen und seinen Verwendungszweck, Informationen zur Identität des Besitzers des öffentlichen Schlüssels, den öffentlichen Schlüssel selbst, ein Ablaufdatum und den Namen der Zertifizierungsstelle. Die Zertifizierungsstelle signiert das Zertifikat mit ihrem eigenen privaten Schlüssel. Wenn der Empfänger über den öffentlichen Schlüssel der Zertifizierungsstelle verfügt, kann dieser prüfen ob, das Zertifikat wirklich von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde. Wenn dies der Fall ist, ist sichergestellt, dass die enthaltenen Informationen zuverlässig sind. Zertifikate können elektronisch (über einen Webzugriff oder per E-Mail), über eine Smartcard oder über eine Diskette bereitgestellt werden.

Zusammenfassend kann man sagen, Zertifikate mit öffentlichen Schlüsseln bieten ein bequemes und zuverlässiges Verfahren zur Identitätsprüfung eines Absenders. IPSec kann dieses Verfahren für eine optionale Authentifizierung nutzen, und RAS-Server können, wie im Abschnitt *EAP-Transport Level Security (EAP-TLS)* beschrieben, eine Benutzerauthentifizierung durchführen.

Extensible Authentication Protocol (EAP)

Wie bereits erwähnt, verfügen die meisten PPP-Implementierungen über eingeschränkte Authentifizierungsmethoden. EAP ist eine von der IETF vorgeschlagene PPP-Erweiterung, die beliebige Authentifizierungsverfahren für die Überprüfung einer PPP-Verbindung zulässt. Ziel der EAP-Entwicklung war es, das dynamische Hinzufügen von Plug-In-Modulen für die Authentifizierung an den client- und serverseitigen Endpunkten einer Verbindung zu ermöglichen. Auf diese Weise können Hersteller jederzeit ein neues Authentifizierungsschema bereitstellen. EAP bietet höchste Flexibilität, was die Einzigartigkeit und die Variationsmöglichkeit der Authentifizierung betrifft.

EAP ist in RFC 2284 dokumentiert und wird von Windows Server 2003 und Windows XP unterstützt.

EAP-Transport Level Security (EAP-TLS)

EAP-TLS ist ein IETF-Standard (RFC 2716) einer starken Authentifizierungsmethode auf der Basis von Zertifikaten für öffentliche Schlüssel. Mit EAP-TLS legt der Client dem Einwahlservers ein Benutzerzertifikat, und der Server dem Client ein Serverzertifikat vor. Ersteres bietet dem Server eine strenge Benutzerauthentifizierung, und letzteres stellt sicher, dass der Benutzer genau den gewünschten Server erreicht hat. Beide Systeme stützen sich auf eine Kette vertrauter Stellen, um die Gültigkeit des angebotenen Zertifikats zu überprüfen.

Das Benutzerzertifikat könnte im DFÜ-Clientcomputer oder in einer externen Smartcard gespeichert werden. In jedem Fall ist der Zugriff auf das Zertifikat nicht ohne Benutzeridentifikation (PIN-Nummer oder Austausch von Benutzername und Kennwort) zwischen Benutzer und Clientcomputer möglich.

Dieses Verfahren entspricht genau dem Ansatz "something-you-know-plus-something-you-have" („einen Teil kennen, einen Teil besitzen“), der von fast allen Sicherheitsexperten empfohlen wird.

EAP-TLS wird von Windows Server 2003 und Windows XP unterstützt. Wie MS-CHAP gibt EAP-TLS einen Verschlüsselungsschlüssel zurück, um die nachfolgende Datenverschlüsselung durch MPPE zu ermöglichen.

Quarantänesteuerung

Die Quarantänesteuerung ist ein neues Feature der Windows Server 2003 Familie. Es ermöglicht eine Verzögerung des Remotezugriffs auf ein privates Netzwerk. Diese Verzögerung gilt, bis die Konfiguration des RAS-Computers durch ein administratives Script überprüft wurde. Wenn ein RAS-Computer eine Verbindung zum RAS-Server initiiert, wird der Benutzer authentifiziert, und dem Computer wird eine IP-Adresse zugewiesen. Die Verbindung wird allerdings im Quarantäne-Modus durchgeführt, der den Netzwerkzugriff einschränkt. Das Script wird auf dem RAS-Computer ausgeführt. Wenn es vollständig und erfolgreich ausgeführt wurde, startet es eine Benachrichtigungskomponente und informiert den RAS-Server, dass der RAS-Client den aktuellen Netzwerkrichtlinien entspricht. Der RAS-Server entfernt dann den Quarantäne-Modus, und der RAS-Client bekommt einen normalen Netzwerkzugriff.

Die Quarantänesteuerung setzt sich aus den folgenden Komponenten zusammen:

- Ein RAS-Server unter Windows Server 2003, auf dem der Quarantine Notification Listener Dienst ausgeführt wird.
- Ein RADIUS-Server unter Windows Server 2003 und dem Internet Authentication Service (IAS), für den eine Quarantäne-Richtlinie mit der passenden Quarantäne-Einstellung konfiguriert ist.
- Ein mit dem Windows Server 2003 Verbindungs-Manager-Verwaltungskit erstelltes Profil mit einem entsprechenden Script und einer Benachrichtigung.
- Einen RAS-Client unter Windows Server 2003, Windows XP, Windows 2000, Windows Millennium Edition oder Windows 98 Second Edition

Weitere Informationen finden Sie im Hilfe- und Supportcenter von Windows Server 2003 und im Whitepaper Microsoft Windows Server 2003-Quarantänesteuerung unter <http://www.microsoft.com/germany/ms/technetdatenbank/showArticle.asp?siteid=600285>

RAS-Kontosperrung

Die RAS-Kontosperrung definiert, wie oft die RAS-Authentifizierung eines gültigen Benutzerkontos fehlschlagen darf, bevor der Remotezugriff für diesen Benutzer gesperrt wird. Dies ist speziell für VPN-Verbindungen über das Internet wichtig. Böswillige Benutzer aus dem Internet könnten versuchen auf das Netzwerk des Unternehmens zuzugreifen, indem sie einen gültigen Benutzernamen verwenden und das Passwort zu erraten versuchen. Während so eines Wörterbuchangriffes werden Hunderte oder Tausende von Anfragen gesendet. Mit aktivierter RAS-Kontosperrung wird ein Wörterbuchangriff nach einer bestimmten Anzahl von fehlgeschlagenen Versuchen unterbunden.

Das Feature unterscheidet nicht zwischen einem böswilligen Benutzer und einem Benutzer, der möglicherweise nur sein Passwort vergessen hat. Diese versuchen häufig mehrere Passwörter und könnten hierbei ihr Konto versehentlich sperren.

Wenn Sie das Feature aktivieren, besteht für einen böswilligen Benutzer die Möglichkeit, ein beliebiges Konto einfach durch mehrere ungültige Authentifizierungsversuche zu sperren. Damit wird dann natürlich auch der legitime Benutzer ausgesperrt.

Die RAS-Kontosperrung wird über Registrierungseinstellungen auf dem authentifizierenden Computer konfiguriert. Wenn der RAS-Server für die Windows-Authentifizierung konfiguriert ist, bearbeiten Sie die Registrierung auf diesem Server. Wenn der RAS-Server für eine RADIUS-Authentifizierung konfiguriert ist und IAS verwendet wird, dann bearbeiten Sie die Registrierung auf dem IAS-Server. Weitere Informationen hierzu finden Sie in im Hilfe- und Supportcenter von Windows Server 2003 unter dem Begriff *RAS-Kontosperrung*.

Anmerkung: Die RAS-Kontosperrung hat nichts mit der Einstellung **Kontosperrung** unter der Registerkarte **Konto** in den Eigenschaften eines Benutzerkontos bei der Administration von Kontosperrungsrichtlinien zu tun.

Paketfilterung über RAS-Richtlinienprofile

Sie können Paketfilter für RAS-Verbindungen über die Verbindungseinschränkungen der RAS-Richtlinien definieren. Bei einem Verbindungsversuch definieren diese Paketfilter den von und zu dem VPN-Client gestatteten IP-Verkehr.

Sie können dieses Feature verwenden, um zu verhindern, dass VPN-Clients Pakete versenden, die sie nicht erstellt haben. Wenn ein RAS-Client eine VPN-Verbindung erstellt, erstellt er standardmäßig auch eine Standardroute. Hierdurch wird dann der gesamte Verkehr für die Standardroute über die VPN-Verbindung gesendet. Wenn andere Computer Verkehr zum VPN-Client weiterleiten (diesen also als Router verwenden), dann wird dieser Verkehr ebenfalls über die VPN-Verbindung gesendet. Da der VPN-Server solche Computer jedoch nicht authentifiziert hat, ist dies ein Sicherheitsproblem. Der vom anderen Computer weitergeleitete Verkehr hat nämlich denselben Netzwerkzugriff, wie der Verkehr, der vom authentifizierten RAS-Client stammt.

Um zu verhindern, dass der VPN-Server solch einen Netzwerkverkehr entgegennimmt, konfigurieren Sie einen Paketfilter über die RAS-Richtlinie. Die Standard-RAS-Richtlinie von Windows Server 2003 entspricht bereits dieser Konfiguration.

VPN-Administration

Bei der Auswahl einer VPN-Technologie ist es wichtig, administrative Schwierigkeiten zu berücksichtigen. In großen Netzwerken ist es notwendig Benutzerinformationen zentral zu speichern, damit der Administrator diese Informationen abfragen und bearbeiten kann. Jeder Zugangs- oder Tunnelserver kann seine eigene interne Benutzerdatenbank pflegen. Aus der administrativen Sicht ist eine Verwaltung von Benutzerkonten über mehrere Datenbanken jedoch ausgeschlossen. Mit Active Directory steht Ihnen eine Lösung zur Verfügung, mit der Sie die Benutzerinformationen für alle Windows Server 2003 VPNs zentral speichern und verwalten können.

VPN-Verbindungen autorisieren

Um eine Autorisierung und Beschränkungen für VPN-Verbindungen zur Verfügung zu stellen wird bei Windows Server 2003 VPN-Verbindungen eine Kombination von Einwahl-Eigenschaften von Benutzerkonten und RAS-Richtlinien verwendet.

RAS-Richtlinien sind ein Satz von Regeln, die definieren, ob und wie Verbindungen akzeptiert oder abgelehnt werden. Für akzeptierte Verbindungen können außerdem Verbindungseinschränkungen festgelegt werden. Bei jeder Regel gibt es eine oder mehrere Bedingungen, Profileinstellungen und Berechtigungen. Bei Verbindungsversuchen werden RAS-Richtlinien der Reihe nach angewandt, und zwar so lange, bis der Verbindungsversuch allen Bedingungen einer Richtlinie entspricht. Wenn der Verbindungsversuch keiner Richtlinie entspricht, wird er abgewiesen.

Wenn der Verbindungsversuch allen Bedingungen einer Richtlinie entspricht und über die entsprechenden Berechtigungen verfügt, dann definiert das RAS-Richtlinienprofil die Verbindungseinschränkungen. Auch über die RAS-Eigenschaften des Benutzerkontos werden einige Einschränkungen definiert. Diese sind im Konfliktfall den Einschränkungen in der RAS-Richtlinie übergeordnet. Die Einschränkungen umfassen unter anderem Verbindungseinstellungen (zum Beispiel die maximale Verbindungsdauer), einen IP-Paketfilter, erforderliche Authentifizierungsprotokolle und erforderliche Verschlüsselungsstärken.

Skalierbarkeit

Redundanz und Lastverteilung können entweder über DNS oder über Network Load Balancing erreicht werden:

- Um Anfragen auf mehrere VPN-Server zu verteilen, kann das Round-Robin-Verfahren verwendet werden. In diesem Fall gibt es auf dem DNS-Server für einen DNS-Namen (zum Beispiel www.microsoft.com) mehrere IP-Adressen, auf die die Last verteilt wird.
- Beim Network Load Balancing bietet ein Cluster von VPN-Servern eine Hochverfügbarkeit und Lastverteilung sowohl für PPTP, als auch für L2TP/IPSec-Verbindungen.

RADIUS

Das RADIUS-Protokoll ist ein gängiges Verfahren zur Handhabung der Authentifizierung und Verwaltung von Remotebenutzern. Es basiert auf dem UDP-Protokoll. RADIUS-Server können zum Beispiel für eine Authentifizierung über PPP, PAP, CHAP, MS-CHAP, MS-CHAP v2 und EAP verwendet werden.

Darüber hinaus bietet RADIUS einen Proxydienst, um Authentifizierungsanfragen an weiter entfernte RADIUS-Server weiterzuleiten. Beispielsweise haben sich viele ISPs Firmenkonsortien angeschlossen, damit Abonnenten mit wechselnden Standorten die lokalen Dienste des nächstgelegenen ISPs für die Internetwahl verwenden können. Diese Allianzen nutzen die Vorteile des RADIUS-Proxydienstes. Wenn ein ISP einen Benutzernamen als Abonnent eines entfernten Netzwerkes erkennt, leitet der ISP die Zugriffsanforderung mit Hilfe eines RADIUS-Proxys an das betreffende Netzwerk weiter.

Windows Server 2003 stellt einen RADIUS-Server und -Proxy über den Internet Authentication Service (IAS) zur Verfügung.

Verbindungs-Manager und verwaltete VPN-Verbindungen

Um die Konfiguration für eine große Zahl von VPN-Clients bereitzustellen, können Sie den Verbindungsmanager verwenden. Der Verbindungsmanager setzt sich aus den folgenden Komponenten zusammen:

- Client-Verbindungs-Manager
- Verbindungs-Manager-Verwaltungskit (VMVK)
- Connection Point Services (CPS)

Client-Verbindungs-Manager

Der Client-Verbindungs-Manager ist eine Software, die auf jedem VPN-Client installiert ist. Sie vereinfacht den Verbindungsaufbau für den Benutzer und beschränkt die Verbindungseinstellungen, die

für diesen änderbar sind. Die Benutzer können über den Verbindungs-Manager zum Beispiel folgendes durchführen:

- Die gewünschte Telefonnummer für einen physikalischen Standort auswählen.
- Benutzerdefinierte Graphiken, Symbole, Nachrichten und Hilfeinformationen verwenden.
- Vor dem Aufbau der VPN-Verbindung automatisch eine DFÜ-Verbindung aufbauen.
- Benutzerdefinierte Aktionen während unterschiedlicher Phasen der Verbindung (zum Beispiel vor dem Verbindungsaufbau oder nach dem Verbindungsaufbau) ausführen.

Ein benutzerdefiniertes Client-Verbindungs-Manager-Paket (auch Profil genannt) ist eine selbstextrahierende Datei, die mit dem Verbindungs-Manager-Verwaltungskit (VMVK) von einem Administrator erstellt wurde. Dieses Profil wird per CD-ROM, E-Mail, Website oder Freigabe an die VPN-Benutzer verteilt. Wenn ein Benutzer ein solches Profil ausführt, werden die entsprechenden DFÜ- und VPN-Verbindungen automatisch konfiguriert. Eine bestimmte Windows-Version ist hierfür nicht notwendig – Verbindungen können unter Windows Server 2003, Windows XP, Windows 2000, Windows NT® 4.0, Windows Millennium Edition und Windows 98 konfiguriert werden.

Verbindungs-Manager-Verwaltungskit

Das Verbindungs-Manager-Verwaltungskit (VMVK) ist ein optionales Verwaltungswerkzeug. Sie können es über die folgenden Wege installieren:

- **Software (in der Systemsteuerung) auf einem Windows Server 2003:** Aktivieren Sie die Verbindungsmanager-Komponente in der Kategorie „Verwaltungs- und Überwachungsprogramme“ der Windows-Komponenten.
- **Windows Server 2003 Administration Tools auf einem Computer unter Windows XP Professional:** Sie müssen die Datei Adminpak.msi aus dem Ordner \I386 der Windows Server 2003-CD-ROM installieren. Danach können Sie das Verbindungs-Manager-Verwaltungskit über die Verwaltung starten.

Das Verbindungs-Manager-Verwaltungskit ist ein Assistent, der Sie durch eine Vielzahl von Optionen bei der Konfiguration und Verteilung eines Profils eines VPN-Benutzers leitet.

Connection Point Services

Connection Point Services (CPS) ermöglichen es Ihnen benutzerdefinierte Telefonbücher zu erstellen, verteilen und zu aktualisieren. Telefonbücher enthalten einen oder mehrere Point of Presence (POP) Einträge. Für jeden POP ist eine Telefonnummer für den Zugriff auf ein DFÜ-Netzwerk oder das Internet definiert.

CPS setzt sich zusammen aus:

- **Telefonbuchverwaltung:** Ein Werkzeug zur Erstellung, Verwaltung, Verteilung und Aktualisierung von Telefonbuch-Dateien auf einem Telefonbuch-Server.
- **Telefonbuch-Server:** Ein Computer unter Windows Server 2003 mit installierten Internetinformationsdiensten (IIS) - inklusive des FTP-Publishing Dienstes – und einer Internet Server Application Programming Interface (ISAPI)-Erweiterung, die Telefonbuch-Aktualisierungsanfragen der Clients verarbeitet.

Die Telefonbuchverwaltung wird über die Datei Pbainst.exe aus dem Verzeichnis Valueadd\Msft\Mgmt\Pba der Windows Server 2003-CD-ROM installiert.

Sie können die Telefonbuchverwaltung verwenden, um Telefonbucheinträge zu erstellen und diese im Ordner *SystemRoot\Programme\PBA\TelefonbuchDateiname* auf dem Telefonbuch-Server zu veröffentlichen.

Nachdem das Telefonbuch konfiguriert und veröffentlicht ist, wird ein Verbindungs-Manager-Profil erstellt. Dieses enthält dann die folgenden Konfigurationsdaten:

- Aktualisierungen werden automatisch heruntergeladen.
- Die Telefonbuch-Datei.
- Den Namen des Telefonbuch-Servers.

Konten, Überwachung und Alarme

Um ein VPN-System richtig verwalten zu können, müssen Netzwerkadministratoren verfolgen können, wer das System verwendet, wie viele Verbindungen hergestellt werden, sowie welche ungewöhnlichen Situationen, Fehlerbedingungen und Hinweise auf Geräteausfälle auftreten. Diese Informationen können für die Abrechnung, Überwachung und Fehlerbenachrichtigung verwendet werden.

Beispielsweise muss ein Administrator möglicherweise wissen, wer sich mit dem System wie lange verbunden hat, um Abrechnungsdaten zu erstellen. Ungewöhnliche Aktivitäten könnten auf falsche Systemverwendung oder nicht ausreichende Systemressourcen schließen lassen. Die Echtzeitüberwachung der Ressourcen (beispielsweise starke Aktivitäten eines Modems und Inaktivität eines zweiten Modems) könnten Warnungen erzeugen, die den Systemadministrator auf eine Modemstörung hinweisen. Der Tunnelserver muss diese Informationen liefern, und das System muss Ereignisprotokolle, Berichte und einen Datenspeicher bereitstellen, um die Daten entsprechend bearbeiten zu können.

Das RADIUS-Protokoll definiert einige Kontoführungsanforderungen, die unabhängig von den oben beschriebenen Authentifizierungsanforderungen sind. Diese Meldungen von RAS an den RADIUS-Server fordern den letzteren auf, Kontoführungseinträge zu Beginn eines Aufrufs, am Ende des Aufrufs und in festgelegten Abständen während des Aufrufs zu erzeugen. Windows 2003 erzeugt diese Kontoführungsanforderungen von RADIUS unabhängig von den Zugriffs-Authentifizierungsanforderungen (die an den Domänencontroller oder an einen RADIUS-Server weitergeleitet werden könnten). Auf diese Weise kann ein Administrator einen RADIUS-Kontoführungsserver unabhängig davon konfigurieren, ob RADIUS für die Authentifizierung verwendet wird oder nicht. Ein Kontoführungsserver kann dann für jede VPN-Verbindung Datensätze für die spätere Auswertung sammeln. Einige Fremdhersteller haben bereits Abrechnungs- und Überwachungspakete geschrieben, die die RADIUS-Kontoführungsdatensätze lesen und verschiedene nützliche Berichte erstellen.

Zusammenfassung

VPNs ermöglichen Benutzern und Unternehmen eine sichere Verbindung mit Remoteservern, Zweigstellen oder andere Unternehmen über ein öffentliches Netzwerk. VPN-Technologie kommt dem aktuellen Trend in der Geschäftswelt zu vermehrter Telekommunikation und global verteilten Geschäftsstellen entgegen, in denen die Mitarbeiter die Gelegenheit haben müssen, zentrale Ressourcen zu nutzen, um miteinander kommunizieren zu können.

Virtuelle Private Netzwerke unter Windows Server 2003 und Windows XP verwenden die Industriestandards PPTP und L2TP/IPSec. Sie bieten Ihnen erweiterte Sicherheits-Features, wie zum Beispiel eine zertifikatsbasierte Authentifizierung und administrative Features (zentralisierte

Authentifizierung und Kontenverwaltung über RADIUS und ein VPN-Client-Bereitstellung über den Verbindungs-Manager).

Weitere Links zum Thema

In den folgenden Quellen finden Sie zusätzliche Informationen:

- *Windows VPN-Website* unter <http://www.microsoft.com/vpn> (englischsprachig).
- *Microsoft L2TP/IPSec VPN-Client* unter <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp> (englischsprachig).
- *Internet Authentication Service Website* unter <http://www.microsoft.com/windows2000/technologies/communications/ias/default.asp> (englischsprachig).

Aktuelle Informationen zu Windows Server 2003 finden Sie auf der *Windows Server 2003 Website* unter <http://www.microsoft.com/germany/windowsserver2003>.