Virtuelle private Netzwerke

http://kickme.to/tiger/

Microsoft

Betriebssystem

Virtuelle private Netzwerke (VPN): Eine Übersicht

Whitepaper

Originalfassung:
http://technet.microsoft.com/cdonline/Content/Complete/windows/winnt/Winntas/prodfact/vpnovw.htm

Kurze Zusammenfassung

Dieses Whitepaper bietet eine Übersicht über virtuelle private Netzwerke (VPN). Es beschreibt die grundlegenden Anforderungen und die wichtigsten Schlüsseltechnologien, die das "Private Networking" über öffentliche Netzwerke ermöglichen.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0499

INHALT

EINFÜHRUNG

Ein virtuelles privates Netzwerk (VPN) verbindet die Komponenten eines Netzwerkes über ein anderes Netzwerk. Zu diesem Zweck ermöglicht das VPN dem Benutzer, einen *Tunnel* durch das Internet oder ein anderes öffentliches Netzwerk herzustellen. Hierbei gelten dieselben Sicherheits- und Leistungsmerkmale, die früher nur in privaten Netzwerken verfügbar waren (siehe Abbildung 1).

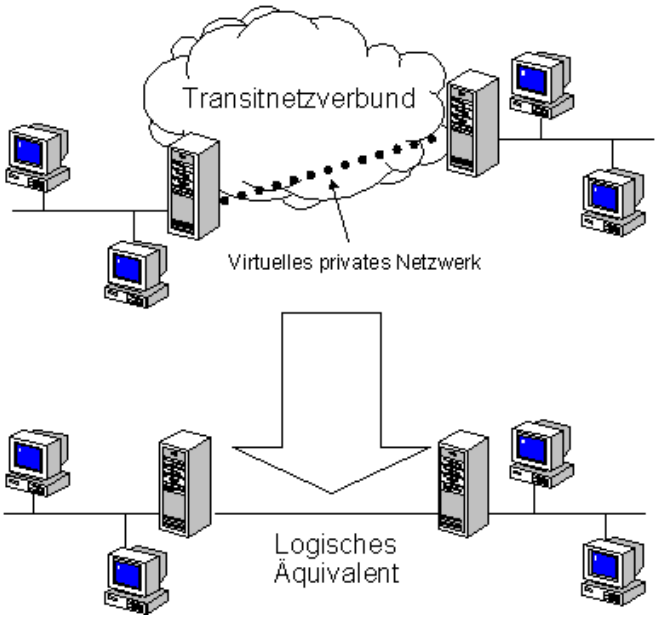

Abbildung 1: Virtuelles privates Netzwerk (VPN)

VPNs ermöglichen es Benutzern, die zu Hause oder unterwegs arbeiten, eine sichere Verbindung mit einem Unternehmensserver unter Verwendung der Routing-Infrastruktur eines öffentlichen Netzwerkes (wie z. B. des Internets) herzustellen. Aus der Sicht des Benutzers ist das VPN eine Punkt-zu-Punkt-Verbindung zwischen dem Computer des Benutzers und einem Unternehmensserver. Die Natur des zwischengeschalteten Netzwerkes ist für den Benutzer irrelevant; aus seiner Sicht werden die Daten wie über eine Standleitung übertragen.

Mithilfe der VPN-Technik kann ein Unternehmen darüber hinaus Verbindungen mit Zweigstellen oder anderen Unternehmen über ein öffentliches Netzwerk (wie z. B. das Internet) herstellen, unter Wahrung der sicheren Kommunikation. Die VPN-Verbindung über das Internet arbeitet logisch wie eine WAN-Verbindung (Wide Area Network) zwischen den Standorten.

In beiden Fällen stellt sich die sichere Verbindung über das Netzwerk dem Benutzer wie eine Kommunikation über ein privates Netzwerk dar - obwohl die Kommunikation real über ein öffentliches Netzwerk stattfindet. Daher die Bezeichnung *Virtuelles privates 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.

Damit Mitarbeiter unabhängig von ihrem Standort eine Verbindung mit den Computerressourcen des Unternehmens herstellen können, muss ein Unternehmen 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, was die Kosten, die Flexibilität der Verwaltung und die Verbindungsnachfrage betrifft. 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 Internetdienstanbieter (Internet Service Provider, ISPs) und VPN-Servercomputer die Anforderungen von Hunderten, ja Tausenden von Remoteclients und Zweigstellen an ein Remotenetzwerk.

Typische Einsatzfelder von VPNs

Die folgenden Abschnitte beschreiben einige häufig vorkommende VPN-Anwendungen.

Zugriff von Remotebenutzern 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.

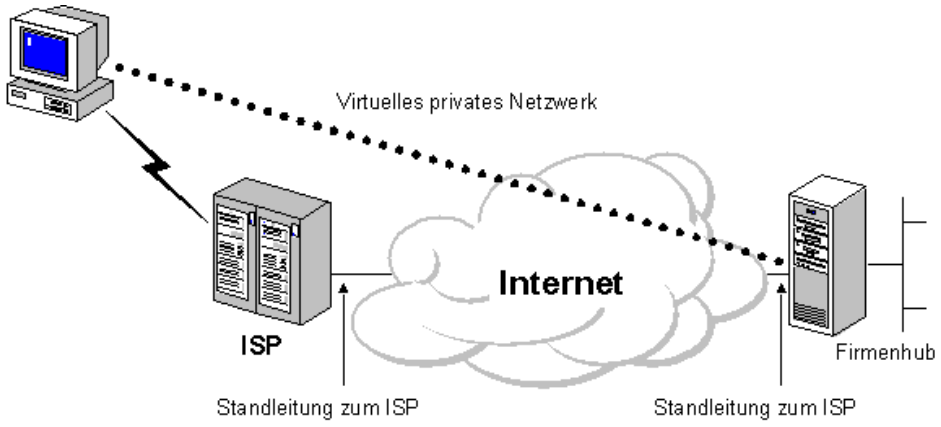

Abbildung 2: Verbinden eines Remoteclients mit einem privaten LAN unter Verwendung eines VPNs

Hierbei wählt sich der Benutzer nicht per Ferngespräch in einen Unternehmens- oder ausgelagerten Server für den Netzwerkzugriff (Network Access Server, NAS) ein, sondern per Ortsgespräch in einen 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.

Verbinden von Netzwerken über das Internet

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 Firmenhubs 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 Firmenhubs 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 Firmenhubs über das Internet zu erstellen.

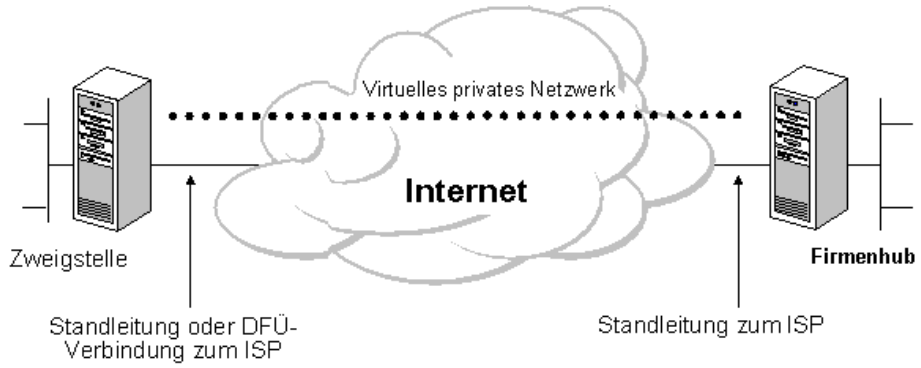

Abbildung 3: Verbinden von zwei Remotestandorten unter Verwendung eines VPNs

In beiden Fällen sind es lokale Einrichtungen, die die Zweigstelle und das Unternehmen mit dem Internet verbinden. Der Router des Firmenhubs, 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.

Verbinden von Computern über ein Intranet

In einigen firmeneigenen Netzwerken verfügen bestimmte Abteilungen über derart vertrauliche Daten, dass das Abteilungs-LAN physisch 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.

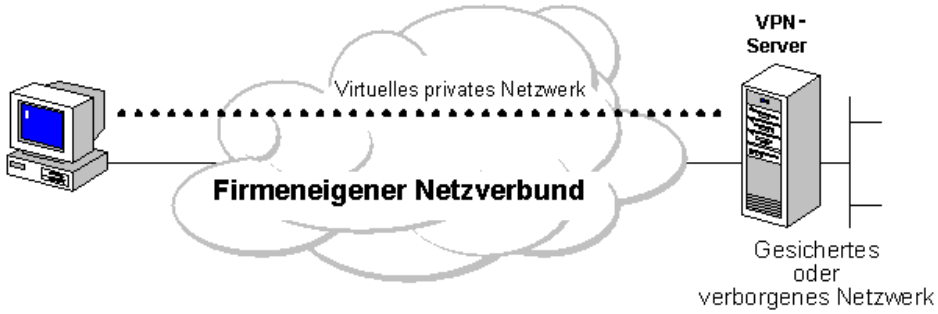

Abbildung 4: Verbinden von zwei Computern im Intranet unter Verwendung eines VPNs

Über ein VPN kann das Abteilungs-LAN einerseits physisch 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 sensitive LAN zugreifen könnte. Mithilfe 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 vorsehen, dass sich Clients an wechselnden Standorten oder Remoteclients mit LAN-Ressourcen verbinden können, und sie muss zulassen, dass sich Remotebüros 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 sensitive Daten, die im firmeneigenen Netzwerk transportiert werden.

Daher muss eine VPN-Lösung mindestens die folgenden Leistungsmerkmale bieten:

- **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.
- **Multiprotokollunterstützung**. Die Lösung muss mit den Protokollen arbeiten können, die im öffentlichen Netzwerk im Allgemeinen verwendet werden. Dazu zählen u. a. IP und Internetwork Packet Exchange (IPX).

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 nützlich.

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

GRUNDLAGEN DES TUNNELVERFAHRENS

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*) können die Rahmen (oder Pakete) 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 enthält den gesamten beschriebenen Prozess (Kapselung, Übertragung und Entkapselung der Pakete).

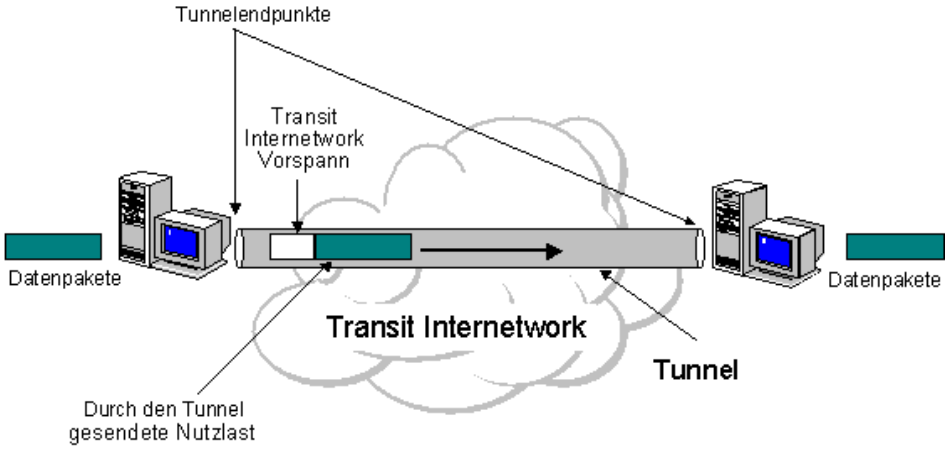

Abbildung 5: Tunnelverfahren (Tunneling)

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. Und während das Internet eines der verbreitetsten 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.

Tunneltechnologien sind bereits seit einiger Zeit bekannt. Zu den ausgereiftesten Technologien zählen:

- **SNA-Tunneling über IP-Netzwerke**. Wenn SNA-Verkehr (Systems Network Architecture) über ein Unternehmensnetzwerk gesendet wird, wird der SNA-Rahmen in einen UDP- und IP-Header gekapselt.

- **IPX-Tunneling für Novell NetWare über IP-Netzwerke**. Wenn ein IPX-Paket an einen NetWare-Server oder IPX-Router gesendet wird, verpackt der Server oder der Router das IPX-Paket in einen UDP- und IP-Header und sendet es dann über ein IP-Netzwerk. Der IP-zu-IPX-Router am Ziel entfernt den UDP- und IP-Header und leitet das Paket an das IPX-Ziel weiter.

Neue Tunneltechnologien sind in den letzten Jahren eingeführt worden. Zu den neueren Technologien, die in diesem Whitepaper primär diskutiert werden, zählen:

- **Point-to-Point-Tunneling-Protokoll (PPTP)**. PPTP ermöglicht es, IP-, IPX- oder NetBEUI-Verkehr zu verschlüsseln, in einen IP-Header zu kapseln und dann über ein privates IP-Netzwerk oder über ein öffentliches IP-Netzwerk, wie z. B. das Internet, zu senden.
- **Layer-2-Tunneling-Protokoll (L2TP)**. L2TP ermöglicht es, IP-, IPX- oder NetBEUI-Verkehr zu verschlüsseln und dann über ein Medium zu senden, das Punkt-zu-Punkt-Datagrammübermittlung unterstützt, wie z. B. IP, X.25, Frame Relay oder ATM.
- **IP-Security-Tunnelmodus (IPSec)**. IPSec-Tunnelmodus ermöglicht es, IP-Datenpakete zu verschlüsseln, in einen IP-Header zu kapseln und dann über ein privates IP-Netzwerk oder über ein öffentliches IP-Netzwerk, wie z. B. das Internet, zu senden.

Tunnelprotokolle

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. Schicht 3-Protokolle entsprechen der Vermittlungsschicht (Network Layer) und verwenden *Pakete*. IP-über-IP (IP-over-IP) und IP-Security-Tunnelmodus (IPSec) sind Beispiele für Schicht 3-Tunnelprotokolle. Diese Protokolle kapseln IP-Pakete in einen zusätzlichen IP-Header, bevor sie sie über ein Netzwerk senden.

Funktionsweise des Tunnelingverfahrens

Für 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. Ein Tunnelverwaltungsprotokoll dient als Verwaltungsinstrument für den Tunnel.

Schicht 3-Tunneltechnologien gehen davon aus, dass alle Konfigurationsparameter bereits ausgehandelt wurden, häufig in manuellen Vorgängen. Für diese Protokolle besteht unter Umständen keine Tunnelverwaltungsphase. Für Schicht 2-Protokolle (PPTP und L2TP) muss jedoch ein Tunnel erstellt, verwaltet und schließlich beendet werden.

Sobald ein Tunnel eingerichtet ist, können die getunnelten Daten gesendet werden. Der Tunnelclient oder der Server bereitet die Daten mit einem Übertragungsprotokoll für Tunneldaten für die Übertragung vor. Wenn der Tunnelclient beispielsweise Datenpakete an den Tunnelserver sendet, fügt er zuerst einen Header für das Übertragungsprotokoll für Tunneldaten 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 ähnlich behandelt.

Tunnelprotokolle und grundlegende Anforderungen an Tunnelverfahren

Da Schicht 2-Protokolle (wie z. B. PPTP und L2TP) auf dem wohldefinierten PPP-Protokoll basieren, sind sie von vornherein mit einer Reihe nützlicher Leistungsmerkmale ausgestattet. Diese Merkmale und ihre Schicht 3-Entsprechungen erfüllen die grundlegenden VPN-Anforderungen wie folgt.

- **Benutzerauthentifizierung**. Schicht 2-Tunnelprotokolle enthalten die Benutzerauthentifizierungsverfahren von PPP, einschließlich der weiter unten beschriebenen EAP-Verfahren. Viele Schicht 3-Tunnelverfahren gehen davon aus, dass die Endpunkte wohlbekannt (und authentifiziert) waren, bevor der Tunnel eingerichtet wurde. Eine Ausnahme bildet die IPSec ISAKMP-Aushandlung, die die gegenseitige Authentifizierung der Tunnelendpunkte bietet. (Die meisten IPSec-Implementierungen unterstützen nur computergestützte Zertifikate und keine Benutzerzertifikate. Daher kann jeder Benutzer, der Zugriff auf einen der beiden Endpunktcomputer besitzt, den Tunnel verwenden. Diese potenzielle Sicherheitslücke kann ausgeschaltet werden, wenn IPSec zusammen mit einem Schicht 2-Protokoll wie z. B. L2TP verwendet wird.)
- **Token Card-Unterstützung**. Unter Verwendung des Extensible Authentication-Protokolls (EAP, Schicht 2) können Tunnelprotokolle eine Vielzahl von Authentifizierungsmethoden unterstützen - u. a. Einmalkennwörter, kryptografische Rechner und Smartcards. Schicht 3-Tunnelprotokolle können ähnliche Methoden verwenden; z. B. definiert IPSec in seiner ISAKMP/Oakley-Aushandlung die Authentifizierung über öffentliche Schlüsselzertifikate.
- **Dynamische Adresszuweisung**. Schicht 2-Tunnelverfahren unterstützen die dynamische Zuweisung von Clientadressen auf der Basis der Aushandlungsmethode des Network Control-Protokolls (Network Control Protocol, NCP). Schicht 3-Tunnelverfahren gehen davon aus, dass eine

Adresse bereits zugewiesen wurde, bevor der Tunnel initiiert wurde. Verfahren für die Zuweisung von Adressen im IPSec-Tunnelmodus werden derzeit entwickelt, sind aber noch nicht verfügbar.

- **Datenkompression**. Schicht 2-Tunnelprotokolle unterstützen PPP-basierte Komprimierungsverfahren. Beispielsweise verwenden die PPTP- und L2TP-Implementierungen von Microsoft die MPPC-Komprimierung (Microsoft Point-to-Point Compression). Die IETF (Internet Engineering Task Force) entwickelt ähnliche Mechanismen (wie z. B. IP-Komprimierung) für die Schicht 3-Tunnelprotokolle.
- **Datenverschlüsselung**. Schicht 2-Tunnelprotokolle unterstützen PPP-basierte Datenverschlüsselungsverfahren. Die PPTP-Implementierung von Microsoft unterstützt die optionale Verwendung der Microsoft Punkt-zu-Punkt-Verschlüsselung (MPPE, Microsoft Point-to-Point Encryption), die auf dem RSA/RC4-Algorithmus basiert. Schicht 3-Tunnelprotokolle können ähnliche Methoden verwenden; beispielsweise definiert IPSec verschiedene optionale Datenverschlüsselungsverfahren, die während des ISAKMP/Oakley-Austausches ausgehandelt werden. Die Microsoft-Implementierung des L2TP-Protokolls verwendet die IPSec-Verschlüsselung, um den Datenstrom vom Client zum Tunnelserver zu schützen.
- **Schlüsselmanagement**. MPPE, ein Schicht 2-Protokoll, beruht auf dem Anfangsschlüssel, der bei der Benutzerauthentifizierung generiert wird, und aktualisiert diesen regelmäßig. IPSec handelt während des ISAKMP-Austausches explizit einen gemeinsamen Schlüssel aus und aktualisiert diesen ebenfalls regelmäßig.
- **Multiprotokollunterstützung**. Das Schicht 2-Tunnelverfahren unterstützt viele Datenpaketprotokolle. Daher können Tunnelclients ganz einfach unter Verwendung von IP, IPX, NetBEUI usw. auf ihre Unternehmensnetzwerke zugreifen. Im Gegensatz dazu unterstützen Schicht 3-Tunnelprotokolle, wie z. B. IPSec-Tunnelmodus, in der Regel nur Zielnetzwerke, die das IP-Protokoll verwenden.

Point-to-Point-Protokoll (PPP)

Da Schicht 2-Protokolle 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, IPX und NetBEUI-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.

In einer PPP-basierten DFÜ-Sitzung werden vier Aushandlungsphasen unterschieden. Alle vier Phasen müssen erfolgreich beendet worden sein, bevor die PPP-Verbindung Benutzerdaten übertragen kann.

Phase 1: Herstellung 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 der Verbindungsaufbauphase (Phase 1) werden Authentifizierungsprotokolle ausgewählt; sie werden aber erst in der Verbindungsauthentifizierungsphase (Phase 2) implementiert. Ähnlich wird im LCP festgelegt, ob die beiden Peers die Verwendung der 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 Konversationsparameter ab, trennt die Verbindung des authentifizierten Benutzers und übernimmt dann selbst die authentifizierte Verbindung.

Die meisten PPP-Implementierungen bieten begrenzte Authentifizierungsmethoden, in der Regel das Password Authentication-Protokoll (PAP), das Challenge Handshake Authentication-Protokoll (CHAP) und das Microsoft Challenge-Handshake Authentication-Protokoll (MSCHAP).

- **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 Benutzername 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.

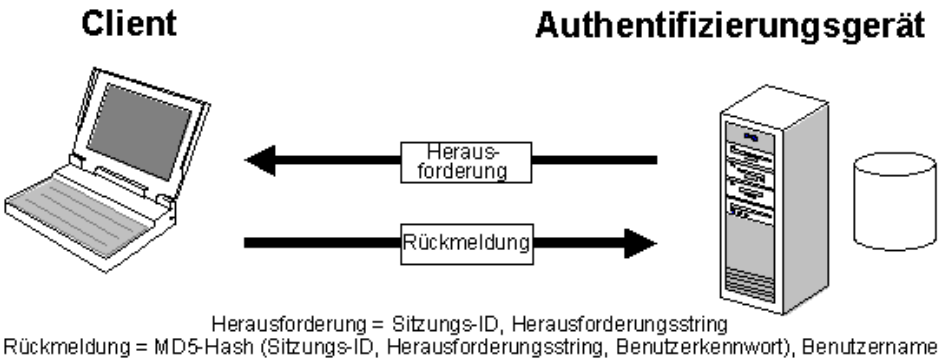

Abbildung 6: Der CHAP-Prozess

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-Protokoll (MS-CHAP)**. MS-CHAP ist ein verschlüsseltes Authentifizierungsverfahren, das ähnlich wie CHAP arbeitet. Wie in CHAP sendet der NAS eine Herausforderung (Challenge), bestehend aus einer Sitzungs-ID und einem zufälligen Herausforderungsstring, an den Remoteclient. Der Remoteclient muss den Benutzernamen und ein MD4-Hash, bestehend aus dem Herausforderungsstring, der Sitzungs-ID und dem MD4-hashcodierten Kennwort, zurückgeben. Diese Konstruktion, bei der ein Hash des MD4-hashcodierten Kennwortes bearbeitet wird, schafft eine zusätzliche Sicherheitsstufe, da so auf dem Server hashcodierte Kennwörter anstelle von Klartext-Kennwörtern gespeichert werden können. MS-CHAP bietet auch weitere Fehlercodes, einschließlich eines "Kennwort abgelaufen“- Codes, und zusätzliche verschlüsselte Client-Server-Meldungen, die es Benutzern ermöglichen, das Kennwort zu ändern. In MS-CHAP erzeugen Client und NAS unabhängig voneinander einen Anfangsschlüssel für die spätere Datenverschlüsselung durch MPPE. Daher ist MS-CHAP-Authentifizierung eine notwendige Voraussetzung für die MPPE-basierte Datenverschlüsselung.

In Phase 2 der Konfiguration der PPP-Verbindung sammelt der NAS die Authentifizierungsdaten. Anschließend überprüft er sie mit seiner eigenen Benutzerdatenbank oder mit einem zentralen Authentifizierungsdatenbankserver, wie er beispielsweise von einem primären Domänencontroller (PDC) für Microsoft®

Windows NT® oder einem RADIUS-Server (Remote Authentication Dial-in User Service) für Remoteauthentifizierung verwaltet wird.

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.

Phase 4: Starten der NCPs

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, um die vom Remoteclient verwendeten Protokolle zu konfigurieren. Beispielsweise kann das IP Control-Protokoll (IPCP) dem DFÜ-Benutzer eine dynamische Adresse zuweisen. In der PPP-Implementierung von Microsoft wird das Komprimierungssteuerungsprotokoll verwendet, um die Datenkomprimierung (mit MPPC) und Datenverschlüsselung (mit MPPE) auszuhandeln, da beide in derselben Routine implementiert wurden.

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-Protokoll (PPTP)

PPTP ist ein Schicht 2-Protokoll, das PPP-Rahmen in IP-Datagramme kapselt, um sie über ein IP-Netzwerk, wie z. B. das Internet, zu übertragen. PPTP kann auch in privaten LAN-zu-LAN-Netzwerken verwendet werden.

PPTP ist im RFC-Entwurf "Point-to-Point Tunneling Protocol“ (pptp-draft-ietf-ppext-pptp-02.txt) dokumentiert. Der Entwurf wurde bei der IETF im Juni 1996 von den am PPTP-Forum beteiligten Unternehmen eingereicht; hierzu zählen Microsoft, Ascend Communications, 3Com/Primary Access, ECI Telematics und US Robotics (jetzt 3Com).

Hinweis: *Internet-Entwurfsdokumente sind Gegenstand ständiger Weiterentwicklung. Kopien von Internet-Drafts erhalten Sie über www.ietf.org.*

Das Point-to-Point Tunneling-Protokoll (PPTP) verwendet eine TCP-Verbindung für die Tunnelverwaltung und mit dem GRE-Verfahren (Generic Routing Encapsulation) gekapselte PPP-Rahmen für getunnelte Daten. Die Datenpakete der gekapselten PPP-Rahmen können verschlüsselt und/oder komprimiert vorliegen. Abbildung 7 zeigt, wie ein PPTP-Paket vor der Übertragung zusammengestellt wird. In der Zeichnung ist ein DFÜ-Client dargestellt, der einen Tunnel über ein Netzwerk erstellt. Der endgültige Rahmenaufbau zeigt die Kapselung für einen DFÜ-Client (PPP-Gerätetreiber).

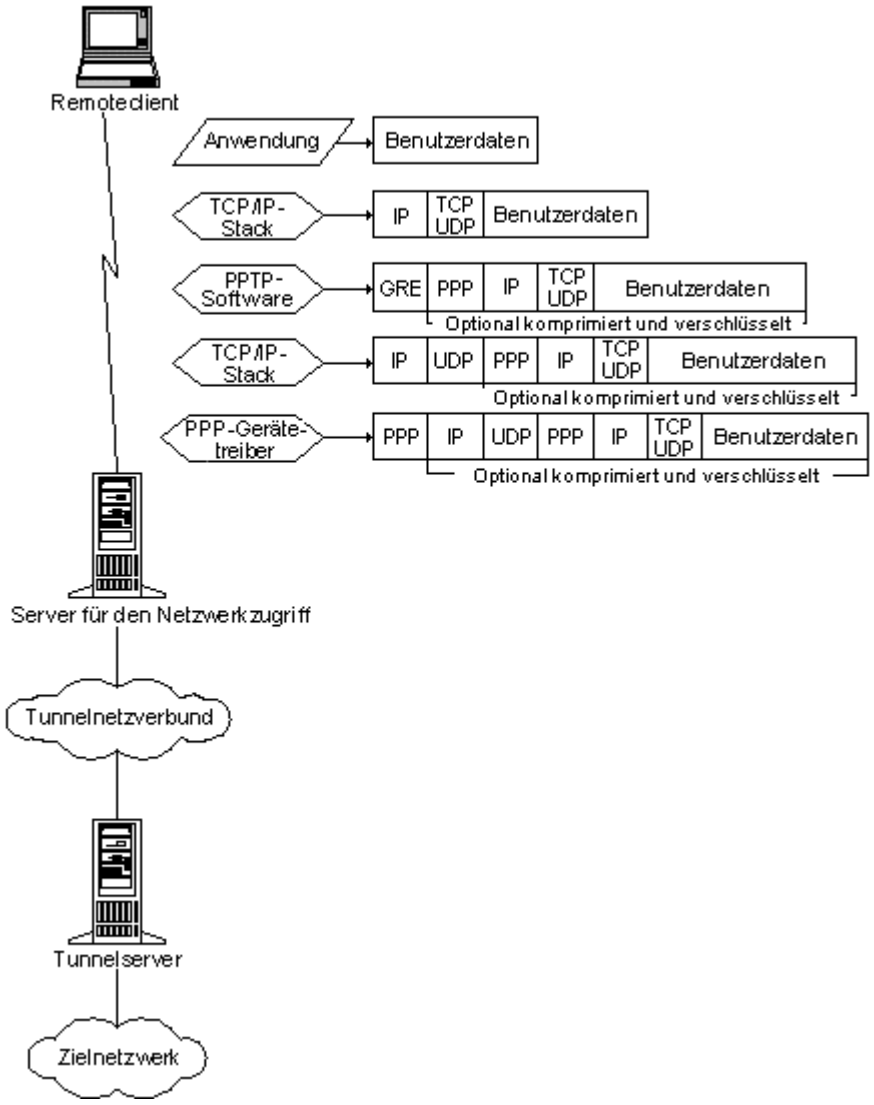

Abbildung 7. Aufbau eines PPTP Pakets

Layer 2 Forwarding (L2F)

L2F, eine von Cisco stammende Technologie, ist ein Übertragungsprotokoll, mit dem Server für den DFÜ-Zugriff den DFÜ-Verkehr in PPP-Rahmen kapseln und

über WAN-Verbindungen an einen L2F-Server (einen Router) übertragen können. Der L2F-Server entkapselt dann die Pakete und schleust sie in das Netzwerk ein. Im Gegensatz zu PPTP und L2TP hat L2F keinen definierten Client. L2F kann nur beim erzwungenen Tunneling verwendet werden. (Weitere Informationen über freiwilliges und erzwungenes Tunneling finden Sie unter "Tunneltypen“ weiter unten.)

Layer 2 Tunneling-Protokoll (L2TP)

L2TP ist eine Kombination aus PPTP und L2F. Die Entwickler dieses Protokolls hoffen, dass L2TP die besten Merkmale von PPTP und L2F in sich vereint.

L2TP ist ein Netzwerkprotokoll, das PPP-Rahmen kapselt, um sie über IP-, X.25-, Frame Relay- oder Asynchronous Transfer Mode (ATM)-Netzwerke zu senden. Wurde L2TP so konfiguriert, dass IP für den Datagrammtransport eingesetzt wird, kann das Protokoll als Tunnelprotokoll im Internet verwendet werden. L2TP kann auch direkt, also ohne eine IP-Transportschicht, über verschiedenen WAN-Medien (wie z. B. Frame Relay) verwendet werden.

L2TP ist im RFC-Entwurf "*Layer 2 Tunneling Protocol L2TP*" (draft-ietf-pppext-l2tp-09.txt) dokumentiert. Der Entwurf wurde bei der IETF im Januar 1998 eingereicht.

L2TP über IP-Netzwerke verwendet UDP und eine Reihe von L2TP-Meldungen für die Tunnelverwaltung. L2TP verwendet UDP auch, um L2TP-gekapselte PPP-Rahmen als Tunneldaten zu senden. Die Datenpakete der gekapselten PPP-Rahmen können verschlüsselt und/oder komprimiert vorliegen. Abbildung 8 zeigt, wie ein L2TP-Paket vor der Übertragung zusammengestellt wird. In der Zeichnung ist ein DFÜ-Client dargestellt, der einen Tunnel über ein Netzwerk erstellt. Der endgültige Rahmenaufbau zeigt die Kapselung für einen DFÜ-Client (PPP-Gerätetreiber). Die Kapselung setzt L2TP über IP voraus.

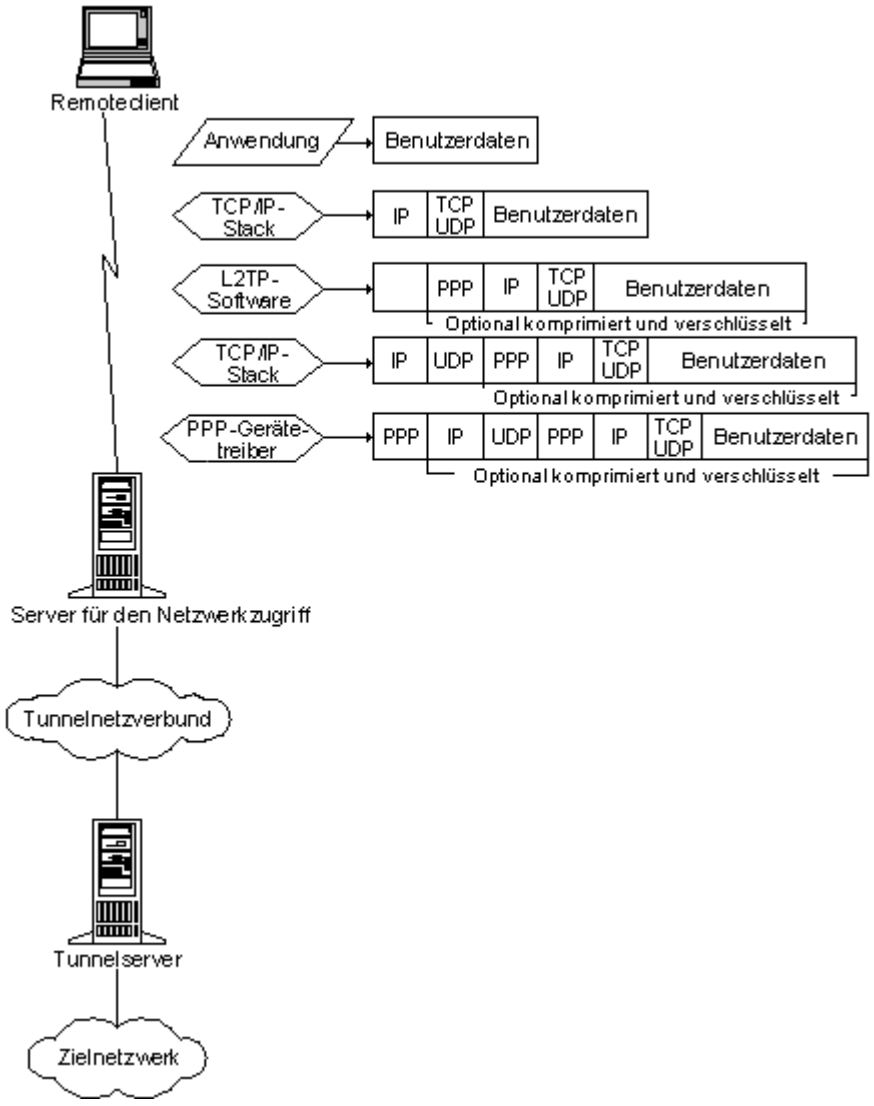

Abbildung 8. Aufbau eines L2TP-Pakets

PPTP und L2TP - ein Vergleich

PPTP und L2TP versehen die Daten mittels PPP mit einem ersten "Umschlag“ und fügen dann weitere Header für den Transport über das Netzwerk hinzu. Beide Protokolle ähneln sich stark, weisen aber auch die folgenden Unterschiede auf:

- PPTP erfordert, dass als Netzwerk ein IP-Netzwerk verwendet wird. L2TP erfordert nur, dass die Tunnelmedien paketorientierte Punkt-zu-Punkt-Verbindungen bieten. L2TP kann über IP (unter Verwendung von UDP), Frame Relay Permanent Virtual Circuits (PVCs), virtuelle X.25-Verbindungen (Virtual Circuits, VCs) oder ATM VCs verwendet werden.
- PPTP unterstützt nur einen einzigen Tunnel zwischen Endpunkten. L2TP lässt die Verwendung mehrerer Tunnel zwischen Endpunkten zu. Mit L2TP können

verschiedene Tunnel für Dienste unterschiedlicher Qualität erstellt werden.

- L2TP bietet Headerkomprimierung. Bei aktivierter Headerkomprimierung arbeitet L2TP mit einem Overhead von 4 Byte, bei PPTP fallen dagegen 6 Byte an.
- L2TP bietet Tunnelauthentifizierung, PPTP nicht. Werden die Protokolle jedoch über IPSec verwendet, steht in jedem Fall Tunnelauthentifizierung durch IPSec zur Verfügung, so dass die Schicht 2-Tunnelauthentifizierung nicht erforderlich ist.

Internet Protocol Security (IPSec)-Tunnelmodus

IPSec ist eine Schicht 3-Protokollnorm, die die sichere Informationsübertragung über ein IP-Netzwerk unterstützt. IPSec wird im Abschnitt "Erweiterte Sicherheitsfunktionen“ weiter unten ausführlich beschrieben. Ein Aspekt von IPSec darf jedoch im Kontext der Tunnelprotokolle nicht unerwähnt bleiben. IPSec definiert die Verschlüsselungsverfahren für den IP-Verkehr, und darüber hinaus das Paketformat für einen "IP-über-IP-Tunnelmodus“, der gewöhnlich als *IPSec-Tunnelmodus* bezeichnet wird. Ein IPSec-Tunnel besteht aus einem Tunnelclient und einem Tunnelserver; beide sind für die Verwendung von IPSec-Tunneling und einem ausgehandelten Verschlüsselungsverfahren konfiguriert.

IPSec-Tunnelmodus verwendet die ausgehandelte Sicherheitsmethode (sofern eine ausgehandelt wurde), um ganze IP-Pakete für die sichere Übertragung über ein privates oder öffentliches IP-Netzwerk zu kapseln und zu verschlüsseln. Die verschlüsselten Datenpakete werden dann erneut mit einem Klartext-IP-Header gekapselt und in das Netzwerk zur Weitergabe an den Tunnelserver gesendet. Nach Empfang dieses Datagramms verarbeitet und entfernt der Tunnelserver den Klartext-IP-Header; anschließend entschlüsselt er den Inhalt, um das ursprüngliche Datenpakete-IP-Paket zurückzugewinnen. Das Datenpakete-IP-Paket wird dann normal verarbeitet und an sein Ziel auf dem Zielnetzwerk weitergeleitet.

Der IPSec-Tunnelmodus weist die folgenden Leistungsmerkmale und Einschränkungen auf:

- Er unterstützt nur IP-Verkehr.
- Er arbeitet auf der untersten Ebene des IP-Stacks. Daher erben Anwendungen und höhere Protokolle sein Verhalten.
- Er wird durch eine *Sicherheitsrichtlinie* - einer Reihe von Regeln für Filter - gesteuert. Die Sicherheitsrichtlinie richtet die verfügbaren Verschlüsselungs- und Tunnelverfahren in der gewünschten Reihenfolge ein und ebenso die verfügbaren Authentifizierungsmethoden. Sobald zu übertragende Daten vorhanden sind, führen die beiden Computer eine gegenseitige Authentifizierung durch und handeln dann die zu verwendenden Verschlüsselungsverfahren aus. Danach werden die gesamten Daten mittels des ausgehandelten Verschlüsselungsverfahrens verschlüsselt und in einen

Tunnelheader gekapselt.

Weitere Informationen über IPSec finden Sie unter "Erweiterte Sicherheitsfunktionen“ weiter unten.

Tunneltypen

Tunnel können auf verschiedene Weise erstellt werden:

- **Freiwillige Tunnel**: 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**: 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.

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

Freiwillige Tunnel

Ein freiwilliger Tunnel entsteht, wenn eine Arbeitsstation oder ein Routingserver mithilfe der Tunnelclient-Software eine virtuelle Verbindung mit dem Zieltunnelserver 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.

Erzwungene 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 bzw. das den Tunnel für den Clientcomputer bereitstellt, wird gewöhnlich in PPTP als Front End Processor (FEP), in L2TP als L2TP Access Concentrator (LAC) und in 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.

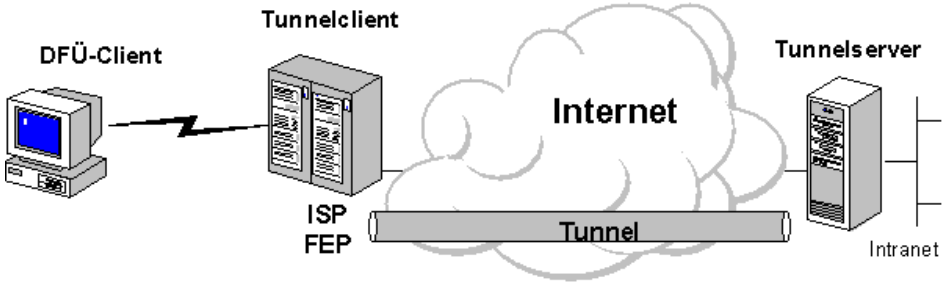

Abbildung 9: Erzwungener Tunnel

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 Front End Processor (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 zu 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 SICHERHEITSFUNKTIONEN

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 geht einen Schritt weiter und beschäftigt sich mit den mächtigeren Authentifizierungs- und Verschlüsselungsfunktionen von EAP und IPSec.

Symmetrische und asymmetrische Verschlüsselung (Privater und Öffentlicher Schlüssel)

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)), die DES-Verschlüsselung (Data Encryption Standard), die IDEA-Verschlüsselung (International Data Encryption Algorithm) und die von der US-Regierung vorgeschlagene (und im Clipper-Chip implementierte) Skipjack-Verschlüsselungstechnik.

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. Privater und öffentlicher 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.

Zertifikate

Bei der symmetrischen Verschlüsselung verfügen Absender und Empfänger über einen gemeinsamen Geheimschlüssel. Die Verteilung des Geheimschlüssels 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 darf frei an alle Personen verteilt werden, die verschlüsselte oder digital signierte Nachrichten empfangen müssen. Der Absender muss allein seinen privaten Schlüssel sorgfältig schützen.

Um die Integrität des öffentlichen Schlüssels sicherzustellen, wird dieser mit einem *Zertifikat* veröffentlicht. Ein Zertifikat (oder Zertifikat für öffentlichen Schlüssel) ist eine Datenstruktur, die von einer Zertifizierungsstelle (Certificate Authority, CA) digital signiert wurde. Die Zertifizierungsstelle ist eine Institution, der die Benutzer des Zertifikats vertrauen können. Das Zertifikat enthält eine Reihe von Werten, wie z. B. Name und Verwendung des Zertifikats, identifizierende Informationen über den Besitzer des öffentlichen Schlüssels, den öffentlichen Schlüssel selbst, ein Ablaufdatum und den Namen der Zertifizierungsstelle. Die Zertifizierungsstelle signiert das Zertifikat mit ihrem privaten Schlüssel. Wenn der Empfänger den öffentlichen Schlüssel der Zertifizierungsstelle kennt, kann er überprüfen, ob das Zertifikat tatsächlich von der vertrauten Zertifizierungsstelle stammt und daher zuverlässige Informationen und einen gültigen öffentlichen Schlüssel enthält. Zertifikate können elektronisch (über das Web oder per E-Mail), auf Smartcards oder auf Disketten verteilt werden.

Zusammenfassend sind Zertifikate für öffentliche Schlüssel eine bequeme und zuverlässige Methode, um die Identität eines Absenders zu verifizieren. IPSec kann diese Methode optional für die Ende-zu-Ende-Authentifizierung verwenden. RAS-Server können Zertifikate für öffentliche Schlüssel für die Benutzerauthentifizierung verwenden, wie unter "Transaction-level Security (EAP-TLS)“ weiter unten beschrieben.

Extensible Authentication-Protokoll (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 Microsoft Windows® 2000 implementiert.

Transaction-level Security (EAP-TLS)

EAP-TLS wurde bei der IETF als Entwurf ("Draft Proposal“) einer strengen Authentifizierungsmethode auf der Basis von Zertifikaten für öffentliche Schlüssel eingereicht. Mit EAP-TLS legt der Client dem Einwählserver ein Benutzerzertifikat vor, und der Server legt 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 ist die spezielle EAP-Methode, die in Microsoft Windows 2000 implementiert wurde. Wie MS-CHAP gibt EAP-TLS einen Verschlüsselungsschlüssel zurück, um die nachfolgende Datenverschlüsselung durch MPPE zu ermöglichen.

IP Security (IPSec)

IP Security (IPSec) wurde von der IETF als Ende-zu-Ende-Verfahren entwickelt, das die Datensicherheit bei der IP-basierten Kommunikation sicherstellen soll. IPSec wurde in einer Reihe von RFCs definiert, insbesondere in RFC 1825, RFC 1826 und RFC 1827; dort werden die Gesamtarchitektur, ein Authentifizierungsheader zur Überprüfung der Datenintegrität und ein ESP (Encapsulation Security Payload) für Datenintegrität und Datenverschlüsselung beschrieben.

IPSec definiert zwei Funktionen, die die Vertraulichkeit sicherstellen: Datenverschlüsselung und Datenintegrität. Wie von der IETF definiert, verwendet IPSec einen Authentifizierungsheader (Authentication Header, AH), um die Authentifizierung und Integrität der Quelle ohne Verschlüsselung zu gewährleisten, sowie die eingekapselten Sicherheitsdatenpakete (ESP), um Authentifizierung und Integrität zusammen mit Verschlüsselung zu bieten. Bei IPSec kennen nur der Absender und der Empfänger den Sicherheitsschlüssel. Wenn die Authentifizierungsdaten gültig sind, weiß der Empfänger, dass die Kommunikation vom gewünschten Absender kam und dass während der Übertragung keine Änderungen vorgenommen wurden.

IPSec kann man sich als Schicht unterhalb des TCP/IP-Stacks vorstellen. Diese Schicht wird auf jedem Computer durch eine Sicherheitsrichtlinie und durch eine ausgehandelte Sicherheitszuordnung zwischen Absender und Empfänger gesteuert. Die Richtlinie besteht aus einer Reihe von Filtern und dem zugehörigen Sicherheitsverhalten. Wenn die IP-Adresse, das Protokoll und die Anschlussnummer des Pakets mit einem Filter übereinstimmen, unterliegt das Paket dem zugeordneten Sicherheitsverhalten.

Ausgehandelte Sicherheitszuordnung

Das erste Paket löst eine Aushandlung einer Sicherheitszuordnung zwischen Absender und Empfänger aus. ISAKMP/Oakley ist das Standardprotokoll für diese

Aushandlung. Während eines ISAKMP/Oakley-Austausches verständigen sich die beiden Computer auf die Authentifizierungs- und Datensicherheitsmethoden, führen die gegenseitige Authentifizierung durch und erzeugen dann einen gemeinsamen Schlüssel für die nachfolgende Datenverschlüsselung.

Sobald die Sicherheitszuordnung eingerichtet wurde, kann die Datenübertragung für beide Computer fortgeführt werden, wobei Datensicherheitsmaßnahmen auf die Pakete angewendet werden, die zum Remoteserver übertragen werden. Die Maßnahmen können einfach darin bestehen, dass die Integrität der übertragenen Daten sichergestellt wird, sie können aber auch die Verschlüsselung umfassen.

Authentifizierungsheader

Datenintegrität und Datenauthentifizierung für IP-Datenpakete können durch einen Authentifizierungsheader gewährleistet werden, der sich zwischen dem IP-Header und dem Transportheader befindet. Der Authentifizierungsheader umfasst Authentifizierungsdaten und eine Sequenznummer; sie dienen dazu, den Absender zu identifizieren, sicherzustellen, dass die Nachricht unterwegs nicht geändert wurde, und einen Wiederholungsangriff zu verhindern.

Der IPSec-Authentifizierungsheader bietet keine Datenverschlüsselung. Klartextnachrichten können gesendet werden, wobei der Authentifizierungsheader sicherstellt, dass sie von einem bestimmten Benutzer stammen und während der Übertragung nicht verändert wurden.

ESP-Header (Encapsulation Security Header)

Encapsulation Security Payload (ESP) bietet für die Vertraulichkeit und den Schutz der Daten vor Mitlesen durch Dritte ein Verschlüsselungverfahren für die IP-Datenpakete. ESP stellt darüber hinaus Datenauthentifizierungs- und Datenintegritätsdienste bereit. Daher sind ESP-Header eine Alternative zu den AH-Headern in IPSec-Paketen.

BENUTZERVERWALTUNG

Bei der Auswahl einer VPN-Technologie dürfen Verwaltungsaspekte auf keinen Fall außer Acht gelassen werden. Große Netzwerke müssen Verzeichnisinformationen benutzerspezifisch in einem zentralen Datenspeicher - dem *Verzeichnisdienst* - speichern, damit Administratoren und Anwendungen diese Informationen ergänzen, ändern oder abfragen können. Jeder Zugriffs- oder Tunnelserver könnte zwar seine eigene interne Datenbank mit den Benutzereigenschaften, wie z. B. Namen, Kennwörter und Einwählberechtigungen, verwalten. Da es jedoch verwaltungstechnisch ungünstig ist, mehrere Benutzerkonten auf mehreren Servern zu führen und gleichzeitig aktuell zu halten, richten Administratoren in der Regel eine Masterdatenbank mit allen Konten auf dem Verzeichnisserver, dem primären Domänencontroller oder einem RADIUS-Server ein.

Unterstützung in RAS

Microsoft Remote Access Service (RAS) arbeitet mit Benutzerinformationen, die im Domänencontroller oder auf einem RADIUS-Server benutzerspezifisch gespeichert werden. Die Verwendung eines Domänencontrollers vereinfacht die Systemverwaltung, da die Einwählberechtigungen eine Teilmenge der Benutzerinformationen sind, die der Administrator ohnehin in einer einzigen Datenbank verwaltet.

Microsoft RAS wurde ursprünglich als Zugriffsserver für DFÜ-Benutzer entwickelt. RAS ist auch ein Tunnelserver für PPTP- und L2TP-Verbindungen. Daher übernehmen diese Schicht 2-VPN-Lösungen die gesamte Verwaltungsstruktur, die für DFÜ-Netzwerke bereits vorhanden ist.

In Windows 2000 nutzt RAS die Vorteile des neuen Active Directory, einer unternehmensweiten replizierten Datenbank auf der Basis des Lightweight Directory Access-Protokolls (LDAP).

LDAP ist ein Industriestandardprotokoll für den Zugriff auf Verzeichnisdienste, das als einfache Alternative zum X.500 DAP-Protokoll entwickelt wurde. LDAP ist erweiterbar, herstellerunabhängig und basiert auf Normen. Die Integration mit Active Directory ermöglicht es dem Administrator, viele Verbindungseigenschaften für DFÜ- oder VPN-Sitzungen Benutzern oder Gruppen individuell zuzuweisen. Die Eigenschaften können benutzerbezogene Filter, erforderliche Authentifizierungs- oder Verschlüsselungsmethoden, tageszeitabhängige Einschränkungen und vieles mehr definieren.

Skalierbarkeit

Redundanz und Lastenausgleich erfolgt unter Verwendung von Round Robin-DNS, wobei Anforderungen auf mehrere VPN-Tunnelserver mit einem gemeinsamen Sicherheitsumkreis aufgeteilt werden. Ein Sicherheitsumkreis hat einen externen DNS-Namen - beispielsweise vpnx.support.bigcompany.com -, aber mehrere IP-Adressen; die Lasten werden zufällig auf alle IP-Adressen verteilt. Alle Server können Authentifizierungsanfragen an die gemeinsame Datenbank richten, wie z. B. ein Windows NT-Domänencontroller. Datenbanken von Windows NT-Domänen

werden aufgrund des Designs repliziert.

RADIUS

Das RADIUS-Protokoll (Remote Authentication Dial-in User Service) ist eine bekannte Methode, um die Remote-Benutzerauthentifizierung und -Autorisierung zu verwalten. RADIUS ist ein sehr einfaches, auf UDP basierendes Protokoll. RADIUS-Server können im Internet beliebig platziert werden und bieten ihrem Client-NAS die Authentifizierung (einschließlich PPP PAP, CHAP, MSCHAP und EAP).

RADIUS-Server bieten darüber hinaus 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 Interneteinwahl verwenden können. Diese Alllianzen nutzen die Vorteile des RADIUS-Proxydienstes. Wenn ein ISP einen Benutzernamen als Abonnent eines entfernten Netzwerkes erkennt, leitet der ISP die Zugriffsanforderung mithilfe eines RADIUS-Proxys an das betreffende Netzwerk weiter.

KONTOFÜHRUNG, ÜBERWACHUNG UND FEHLERBENACHRICHTIGUNG

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.

Microsoft Windows NT 4 unterstützt in RAS die Kontoführung, Überwachung und Fehlerbenachrichtigung.

Das RADIUS-Protokoll definiert eine Suite von 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 2000 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 es Benutzern und Firmen, sichere Verbindungen mit Remoteservern, Zweigstellen oder anderen Unternehmen über ein öffentliches Netzwerk herzustellen - unter Wahrung der sicheren Kommunikation. In allen aufgeführten Fällen stellt sich die sichere Verbindung über das Netzwerk dem Benutzer wie eine Kommunikation über ein privates Netzwerk dar - obwohl die Kommunikation real über ein öffentliches Netzwerk stattfindet. 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.

Dieses Whitepaper bietet eine Übersicht über VPN. Es beschreibt die grundlegenden Anforderungen an sinnvolle VPN-Technologien: Benutzerauthentifizierung, Adressenverwaltung, Schlüsselverwaltung und Multiprotokollunterstützung. Es erläutert, wie Schicht 2-Protokolle, insbesondere PPTP und L2TP, diese Anforderungen erfüllen und wie IPSec (ein Schicht 3-Protokoll) diese Anforderungen zukünftig erfüllen wird.

Weitere Informationen

Weitere Informationen über Windows NT Server finden Sie in Microsoft TechNet oder in unserer WWW-Site unter **http://www.microsoft.com/germany/backoffice/ntserver** oder unter **http://www.microsoft.com/ntserver** (englischsprachig) und im Windows NT Server-Forum im Microsoft Network (Suchbegriff: MSNTS).