Welche VPN-Lösung ist die richtige für Sie?

Inhalt

Einführung

Virtual Private Networks (VPNs) werden zunehmend als kostengünstigere und flexiblere Methode zur Bereitstellung eines Netzwerks in einem großen Bereich beliebt. Mit technologischen Fortschritten kommen immer mehr Optionen zur Implementierung von VPN-Lösungen hinzu. In diesem technischen Hinweis werden einige dieser Optionen erläutert und beschrieben, wo sie am besten verwendet werden können.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

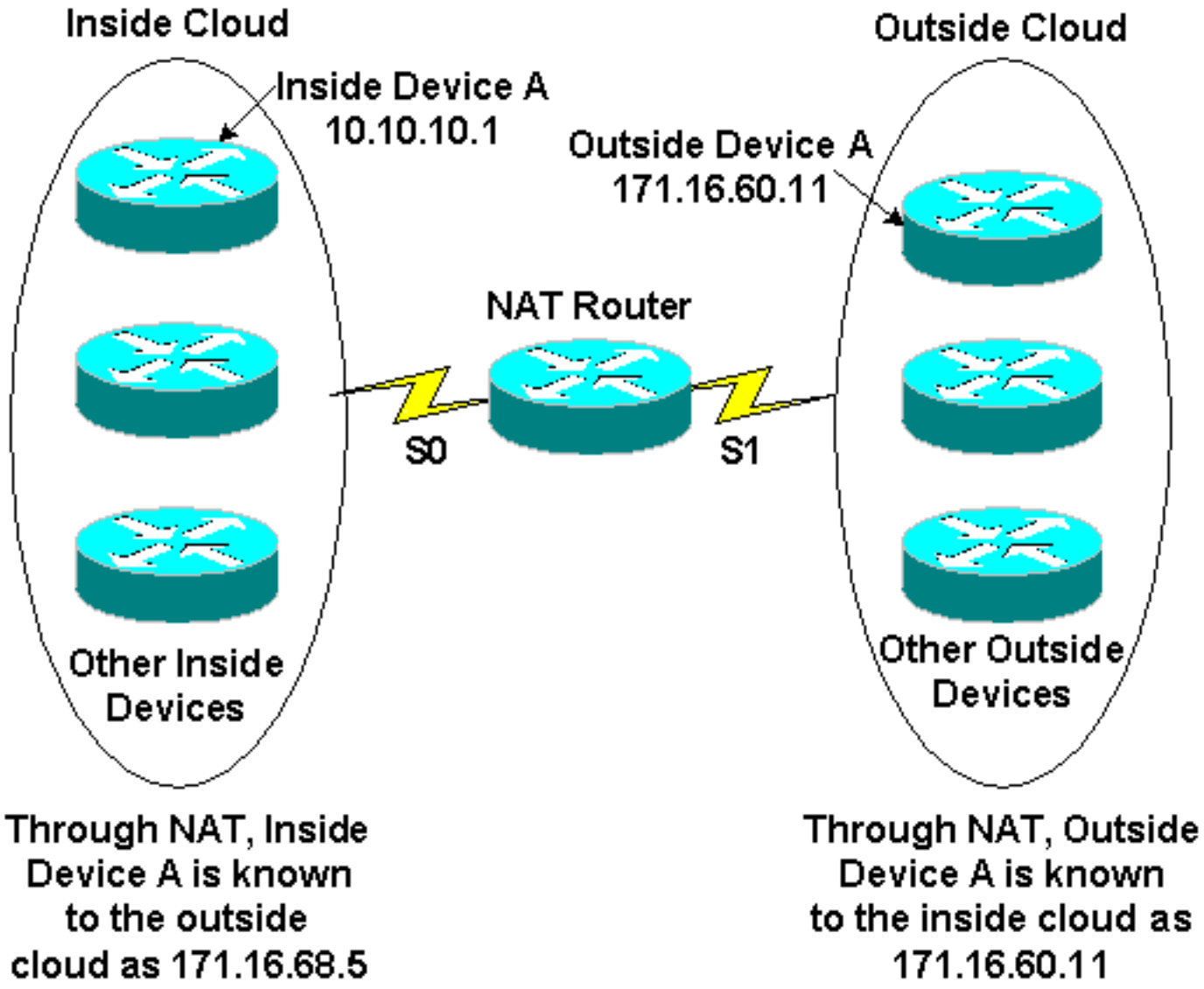
Hinweis: Cisco bietet auch Verschlüsselungsunterstützung für Nicht-IOS-Plattformen, darunter die Cisco Secure PIX Firewall, den Cisco VPN 3000 Concentrator und den Cisco VPN 5000 Concentrator.

NAT

Das Internet hat in kurzer Zeit ein explosionsartiges Wachstum erlebt, weit mehr, als die ursprünglichen Designer hätten vorhersehen können. Die begrenzte Anzahl von Adressen in IP-Version 4.0 ist ein Beleg für dieses Wachstum, und das Ergebnis ist, dass der Adressraum immer weniger verfügbar ist. Eine Lösung für dieses Problem ist Network Address Translation (NAT).

Mithilfe der NAT wird ein Router innerhalb/außerhalb von Grenzen konfiguriert, sodass die Außenstelle (normalerweise das Internet) eine oder mehrere registrierte Adressen erkennt, während innerhalb des Routers eine beliebige Anzahl von Hosts vorhanden sein kann, die ein privates Adressierungsschema verwenden. Um die Integrität des Adressenübersetzungsschemas zu wahren, muss NAT auf jedem Boundary Router zwischen dem internen (privaten) Netzwerk und dem externen (öffentlichen) Netzwerk konfiguriert werden. Einer der Vorteile von NAT im Hinblick auf die Sicherheit besteht darin, dass die Systeme im privaten Netzwerk keine eingehende IP-Verbindung vom externen Netzwerk empfangen können, es sei denn, das NAT-Gateway ist speziell für die Verbindung konfiguriert. Darüber hinaus ist NAT für die Quell- und Zielgeräte vollständig transparent. Der empfohlene NAT-Betrieb umfasst RFC 1918 , der geeignete private Netzwerkadressierungsschemata beschreibt. Der Standard für NAT wird in RFC 1631 beschrieben.

Die folgende Abbildung zeigt die NAT-Router-Grenzdefinition mit einem internen Adresspool für das Übersetzungsnetzwerk.

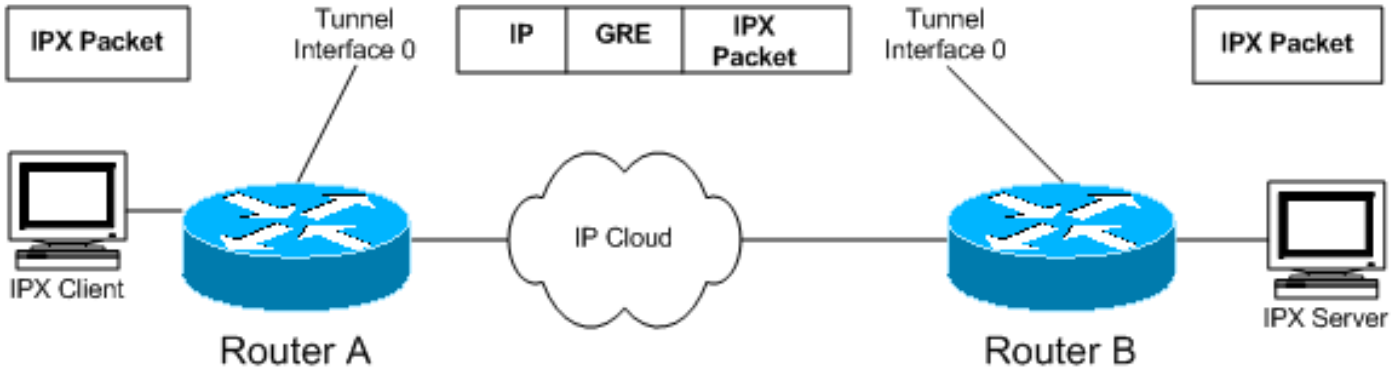


NAT wird in der Regel verwendet, um im Internet routbare IP-Adressen zu sparen, die teuer und zahlenmäßig begrenzt sind. NAT bietet auch Sicherheit, indem das interne Netzwerk vom Internet ferngehalten wird.

Weitere Informationen zum Arbeiten von NAT finden Sie unter Funktionsweise von NAT.

GRE-Kapselungstunneln

GRE-Tunnel (Generic Routing Encapsulation) stellen einen bestimmten Pfad im gemeinsam genutzten WAN bereit und kapseln den Datenverkehr mit neuen Paket-Headern ein, um die Bereitstellung für bestimmte Ziele sicherzustellen. Das Netzwerk ist privat, da der Datenverkehr nur an einem Endpunkt in einen Tunnel gelangen und nur am anderen Endpunkt verbleiben kann. Tunnel bieten keine wahre Vertraulichkeit (wie bei der Verschlüsselung), können jedoch verschlüsselten Datenverkehr übertragen. Tunnel sind logische Endpunkte, die auf den physischen Schnittstellen konfiguriert sind, über die der Datenverkehr übertragen wird.



Wie im Diagramm gezeigt, kann GRE-Tunneling auch verwendet werden, um Nicht-IP-Datenverkehr in IP einzukapseln und über das Internet oder das IP-Netzwerk zu senden. Beispiele für Nicht-IP-Datenverkehr sind die Protokolle Internet Packet Exchange (IPX) und AppleTalk. Informationen zum Konfigurieren der GRE finden Sie unter "Konfigurieren einer GRE-Tunnel-Schnittstelle" unter Konfigurieren der GRE.

GRE ist die richtige VPN-Lösung für Sie, wenn Sie ein Multiprotokoll-Netzwerk wie IPX oder AppleTalk haben und Datenverkehr über das Internet oder ein IP-Netzwerk senden müssen. Die GRE-Kapselung wird im Allgemeinen zusammen mit anderen Mitteln zur Sicherung des Datenverkehrs verwendet, z. B. IPSec.

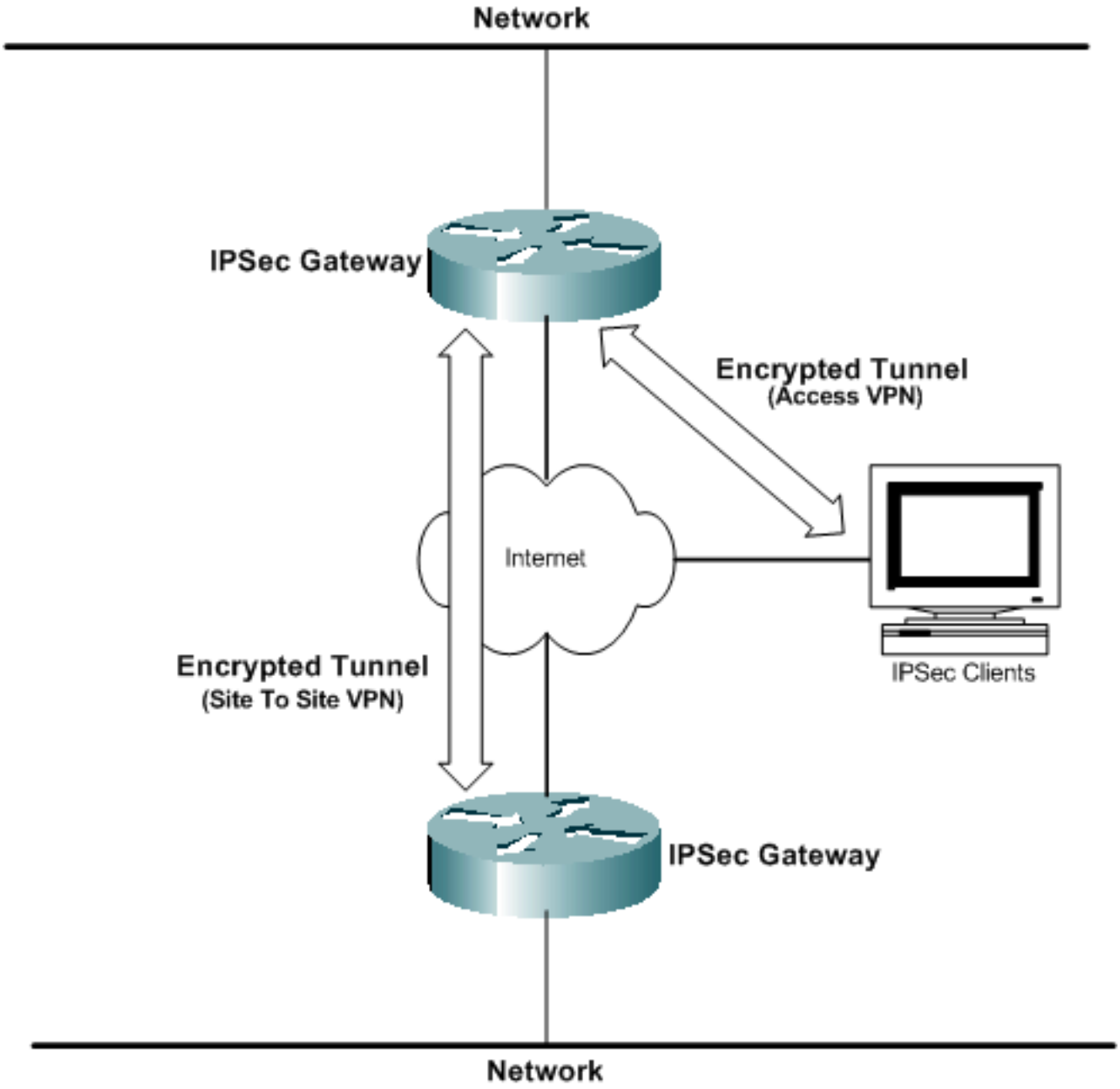
Weitere technische Details zu GRE finden Sie unter RFC 1701 und RFC 2784 .

IPSec-Verschlüsselung

Die Verschlüsselung von Daten, die über ein gemeinsam genutztes Netzwerk gesendet werden, ist die am häufigsten mit VPNs verbundene VPN-Technologie. Cisco unterstützt die IP Security (IPSec)-Datenverschlüsselungsmethoden. IPSec ist ein Framework offener Standards, das Datensicherheit, Datenintegrität und Datenauthentifizierung zwischen den beteiligten Peers auf Netzwerkebene bietet.

Die IPSec-Verschlüsselung ist ein IETF-Standard (Internet Engineering Task Force), der in der IPSec-Clientsoftware symmetrische 168-Bit-Verschlüsselungsalgorithmen DES (Data Encryption Standard) 56-Bit und 3DES (3DES) unterstützt. Die GRE-Konfiguration ist mit IPSec optional. IPSec unterstützt auch Zertifikatsbehörden und die Verhandlung über Internet Key Exchange (IKE). IPSec-Verschlüsselung kann in eigenständigen Umgebungen zwischen Clients, Routern und Firewalls bereitgestellt oder zusammen mit L2TP-Tunneling in Access-VPNs verwendet werden. IPSec wird auf verschiedenen Betriebssystemplattformen unterstützt.

IPSec-Verschlüsselung ist die richtige VPN-Lösung für Sie, wenn Sie echte Datensicherheit für Ihre Netzwerke wünschen. IPSec ist ebenfalls ein offener Standard, sodass die Interoperabilität zwischen verschiedenen Geräten einfach zu implementieren ist.



PPTP und MPPE

Das Point-to-Point Tunneling Protocol (PPTP) wurde von Microsoft entwickelt. wird in RFC 2637 beschrieben. PPTP wird häufig in Windows 9x/ME, Windows NT und Windows 2000 sowie in Windows XP-Clientsoftware bereitgestellt, um freiwillige VPNs zu ermöglichen.

Microsoft Point-to-Point Encryption (MPPE) ist ein informativer IETF-Entwurf von Microsoft, der eine RC4-basierte 40-Bit- oder 128-Bit-Verschlüsselung verwendet. MPPE ist Teil der PPTP-Client-Softwarelösung von Microsoft und in VPN-Architekturen für den freiwilligen Zugriff nützlich. PPTP/MPPE wird auf den meisten Cisco Plattformen unterstützt.

Die PPTP-Unterstützung wurde der Cisco IOS Softwareversion 12.0.5.XE5 auf den Cisco 7100- und 7200-Plattformen hinzugefügt. Die Unterstützung für weitere Plattformen wurde in Cisco IOS 12.1.5.T hinzugefügt. Die Cisco Secure PIX Firewall und der Cisco VPN 3000 Concentrator unterstützen auch PPTP-Clientverbindungen.

Da PPTP Nicht-IP-Netzwerke unterstützt, ist es nützlich, wenn sich die Remote-Benutzer beim

Unternehmensnetzwerk anmelden müssen, um auf heterogene Unternehmensnetzwerke zuzugreifen.

Informationen zur Konfiguration von PPTP finden Sie unter Konfigurieren von PPTP.

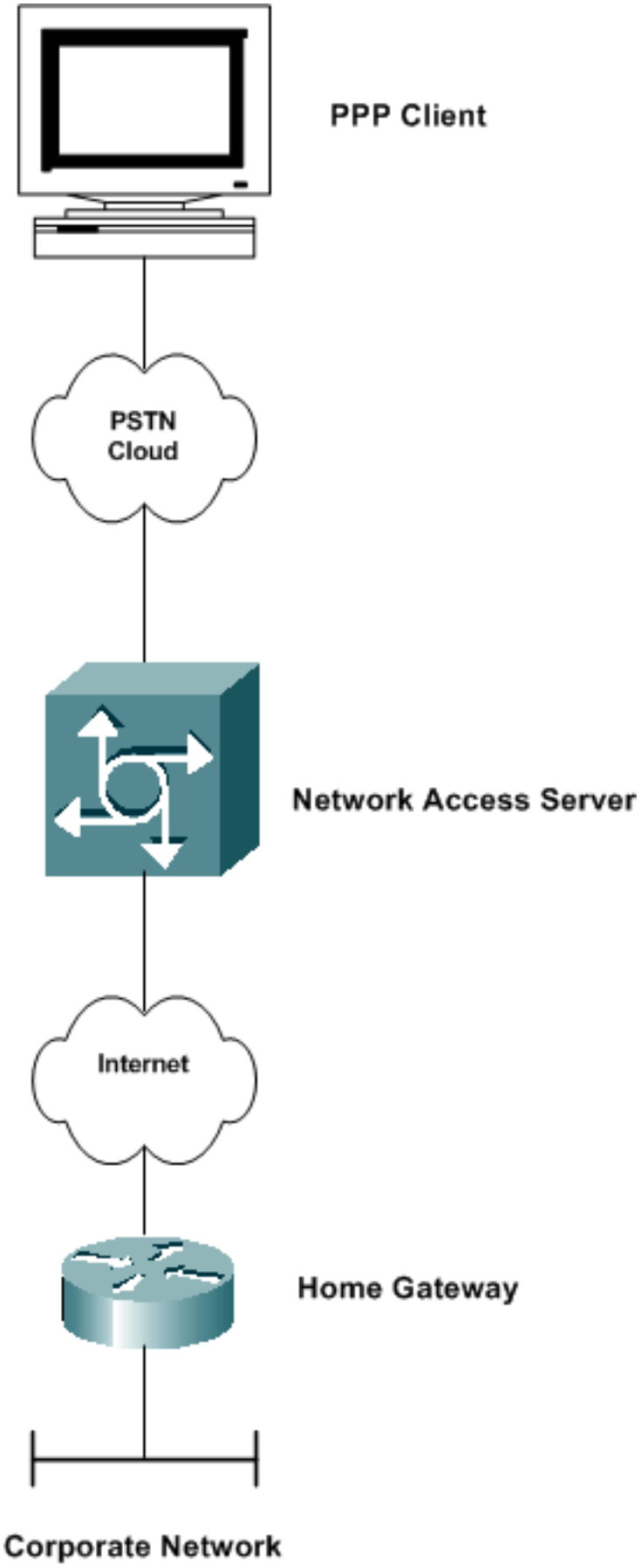
VPDN und L2TP

VPDN

Virtual Private Dialup Network (VPDN) ist ein Cisco-Standard, der es einem privaten Netzwerk ermöglicht, sich über Remote-Zugriffsserver zu erstrecken. Im Kontext von VPDN wird der Zugangs-Server (z. B. ein AS5300), an den sich der Anruf richtet, in der Regel als Network Access Server (NAS) bezeichnet. Das Ziel des Einwahlbenutzers wird als Heim-Gateway (HGW) bezeichnet.

Das grundlegende Szenario besteht darin, dass sich ein PPP-Client (Point-to-Point Protocol) bei einem lokalen NAS einwählt. Das NAS-Gerät legt fest, dass die PPP-Sitzung an einen Home-Gateway-Router für diesen Client weitergeleitet werden soll. Der HGW authentifiziert dann den Benutzer und startet die PPP-Aushandlung. Nach Abschluss der PPP-Einrichtung werden alle Frames über das NAS-Gerät an die Client- und Home-Gateways gesendet. Diese Methode integriert mehrere Protokolle und Konzepte.

Informationen zur Konfiguration von VPDN finden Sie unter *Konfigurieren eines virtuellen privaten DFÜ-Netzwerks* in der Konfiguration von Sicherheitsfunktionen.



L2TP

Layer 2 Tunneling Protocol (L2TP) ist ein IETF-Standard, der die besten Attribute von PPTP und L2F enthält. L2TP-Tunnel werden hauptsächlich im Zwangsmodus (d. h. DFÜ-NAS zu HGW) für den Zugriff auf VPNs für IP- und Nicht-IP-Datenverkehr verwendet. Windows 2000 und Windows

XP haben dieses Protokoll als Mittel zur VPN-Clientverbindung nativ unterstützt.

L2TP wird verwendet, um PPP mithilfe von IP über ein öffentliches Netzwerk wie das Internet zu tunneln. Da der Tunnel auf Layer 2 stattfindet, sind die Protokolle der oberen Schicht über den Tunnel nicht bekannt. Wie GRE kann L2TP auch jedes Layer-3-Protokoll kapseln. Der UDP-Port 1701 wird verwendet, um L2TP-Datenverkehr durch den Initiator des Tunnels zu senden.

Hinweis: 1996 hat Cisco ein Layer-2-Weiterleitungsprotokoll (L2F) erstellt, um das Auftreten von VPDN-Verbindungen zu ermöglichen. L2F wird weiterhin für andere Funktionen unterstützt, wurde aber durch L2TP ersetzt. Das Point-to-Point Tunneling Protocol (PPTP) wurde 1996 ebenfalls als Internet-Entwurf der IETF erstellt. PPTP stellte eine Funktion bereit, die dem GRE-ähnlichen Tunnelprotokoll für PPP-Verbindungen ähnelte.

Weitere Informationen zu L2TP finden Sie unter Layer 2 Tunnel Protocol.

PPPoE

PPP over Ethernet (PPPoE) ist ein informatives RFC, das hauptsächlich in DSL-Umgebungen (Digital Subscriber Line) eingesetzt wird. PPPoE nutzt die vorhandene Ethernet-Infrastruktur, um Benutzern die Möglichkeit zu geben, mehrere PPP-Sitzungen innerhalb desselben LAN zu initiieren. Diese Technologie ermöglicht die Auswahl von Layer-3-Services, eine neue Anwendung, mit der Benutzer über eine einzige Remote-Zugriffsverbindung gleichzeitig eine Verbindung zu mehreren Zielen herstellen können. PPPoE mit Password Authentication Protocol (PAP) oder Challenge Handshake Authentication Protocol (CHAP) wird häufig verwendet, um den zentralen Standort darüber zu informieren, welche Remote-Router mit dem Protokoll verbunden sind.

PPPoE wird hauptsächlich in DSL-Bereitstellungen von Service Providern und in überbrückten Ethernet-Topologien verwendet.

Weitere Informationen zur Konfiguration von PPPoE finden Sie unter Konfigurieren von PPPoE over Ethernet und IEEE 802.1Q VLAN.

MPLS-VPN

Multiprotocol Label Switching (MPLS) ist ein neuer IETF-Standard, der auf Cisco Tag Switching basiert und eine automatisierte Bereitstellung, schnelle Bereitstellung und Skalierbarkeit ermöglicht. Service Provider müssen daher kosteneffizient Zugriff auf VPN-Services für Intranet- und Extranet-Umgebungen bereitstellen. Cisco arbeitet eng mit Service Providern zusammen, um einen reibungslosen Übergang zu MPLS-fähigen VPN-Services zu gewährleisten. MPLS verwendet ein Label-basiertes Paradigma und markiert Pakete beim Betreten des Anbieternetzwerks, um die Weiterleitung über einen verbindungslosen IP-Core zu beschleunigen. MPLS verwendet Route Distinguisher, um die VPN-Zugehörigkeit zu identifizieren und den Datenverkehr innerhalb einer VPN-Community einzudämmen.

MPLS bietet zudem einen verbindungsorientierten Ansatz für das IP-Routing-Paradigma, indem Label-Switched-Pfade eingerichtet werden, die auf Topologieinformationen basieren und nicht auf dem Datenverkehrsfluss. MPLS VPN wird in der Service Provider-Umgebung weit verbreitet.

Informationen zur Konfiguration von MPLS-VPN finden Sie unter Konfigurieren eines einfachen MPLS-VPN.

Zugehörige Informationen

- IPSec-Support-Seite
- So funktionieren virtuelle private Netzwerke
- NAT-Support-Seite
- GRE-Support-Seite
- VPDN-Support-Seite
- PPTP-Support-Seite
- PPPoE-Support-Seite
- Technischer Support - Cisco Systems