VPDN im Überblick

Inhalt

Einführung

Ein Virtual Private Dial-up-Netzwerk (VPDN) ermöglicht es einem privaten Netzwerk, eine Einwahl in den Dienst über Remote-Zugriffsserver (definiert als L2TP Access Concentrator [LAC]) zu führen.

Wenn sich ein PPP-Client (Point-to-Point Protocol) in eine LAC einwählt, legt die LAC fest, dass diese PPP-Sitzung an einen L2TP-Netzwerkserver (LNS) für diesen Client weitergeleitet werden soll. Das LNS authentifiziert dann den Benutzer und startet die PPP-Aushandlung. Nach Abschluss der PPP-Einrichtung werden alle Frames über die LAC an den Client und das LNS gesendet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

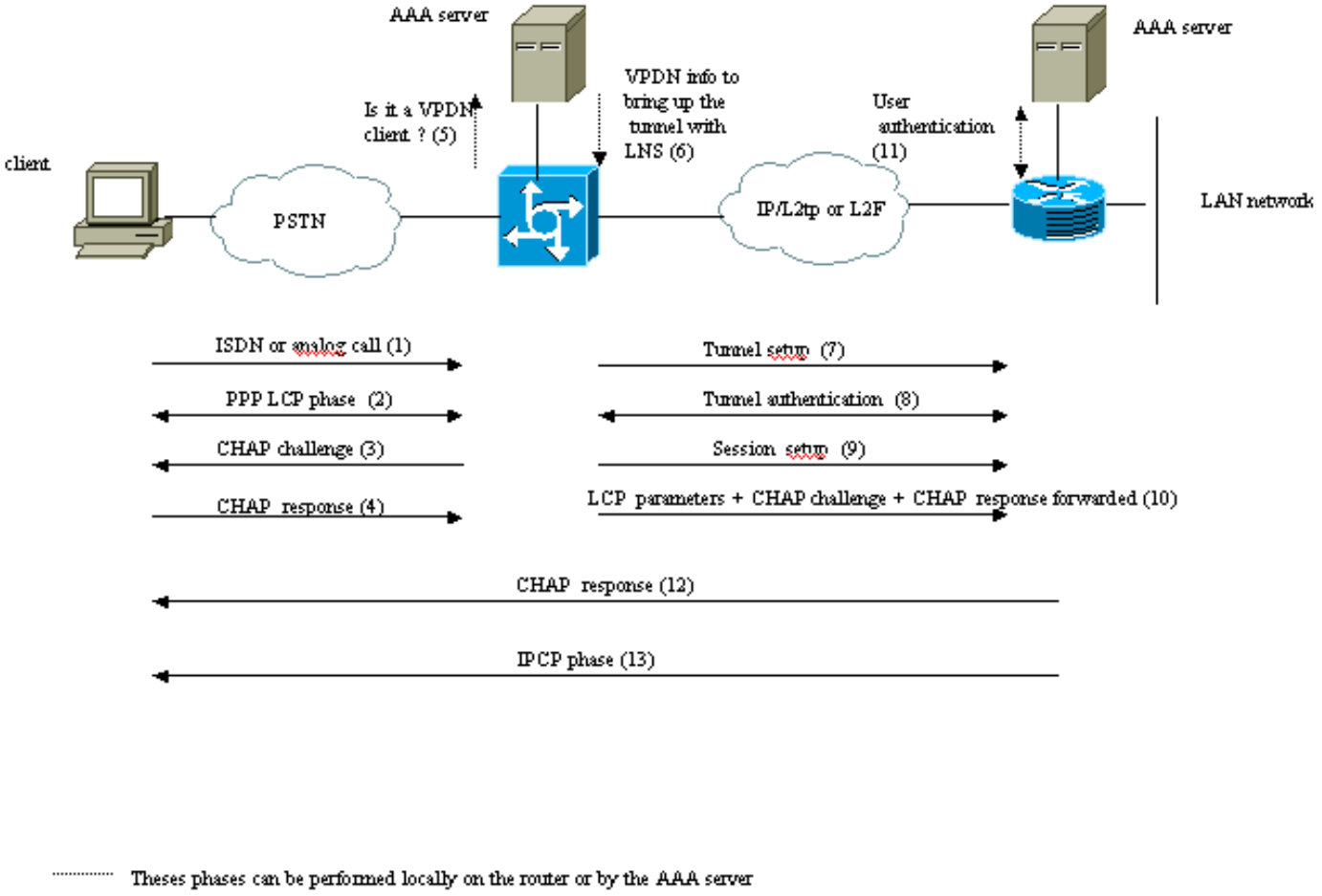
Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Glossar

- **Client**: Ein PC oder Router, der bzw. der an ein Remote-Zugriffsnetzwerk angeschlossen ist, ist der Initiator eines Anrufs.
- **L2TP**: Layer-2-Tunnelprotokoll. PPP definiert einen Kapselungsmechanismus für die Übertragung von Multiprotokoll-Paketen über Layer-2-Point-to-Point-Verbindungen (L2). In der Regel erhält ein Benutzer eine L2-Verbindung zu einem Network Access Server (NAS) über eine Technik wie DFÜ-POTS (Plain Old Telefone Service), ISDN oder ADSL (Asymmetric Digital Subscriber Line). Der Benutzer führt dann PPP über diese Verbindung aus. In einer solchen Konfiguration befinden sich der L2-Terminationspunkt und der PPP-Sitzungsendpunkt auf demselben physischen Gerät (dem NAS).L2TP erweitert das PPP-Modell, indem es es ermöglicht, dass sich die L2- und PPP-Endpunkte auf verschiedenen Geräten befinden, die über ein Netzwerk verbunden sind. Bei L2TP verfügt der Benutzer über eine L2-Verbindung zu einem Zugriffskonzentrator, und der Konzentrator tunnelt anschließend einzelne PPP-Frames in das NAS-Gerät. Dadurch kann die eigentliche Verarbeitung von PPP-Paketen von der Terminierung des L2-Schaltkreises getrennt werden.
- **L2F**: Layer-2-Weiterleitungsprotokoll. L2F ist ein Tunneling-Protokoll, das älter als L2TP ist.
- **LAC**: L2TP-Zugriffskonzentrator. Ein Knoten, der als eine Seite eines L2TP-Tunnelendpunkts fungiert und ein Peer zum LNS ist. Die LAC befindet sich zwischen einem LNS und einem Client und leitet Pakete an und von jedem weiter. Pakete, die von der LAC an das LNS gesendet werden, erfordern Tunneling mit dem L2TP-Protokoll. Die Verbindung von der LAC zum Client erfolgt in der Regel über ISDN oder Analog.
- **LNS**: L2TP-Netzwerkserver. Ein Knoten, der als eine Seite eines L2TP-Tunnelendpunkts fungiert und ein Peer zur LAC ist. Das LNS ist der logische Endpunkt einer PPP-Sitzung, die vom Client durch die LAC getunnelt wird.
- **Home-Gateway**: Identische Definition wie LNS in L2F-Terminologie.
- **NAS**: Identische Definition wie LAC in L2F-Terminologie.
- **Tunnel**: In der L2TP-Terminologie existiert ein Tunnel zwischen einem LAC-LNS-Paar. Der Tunnel besteht aus einer Steuerungsverbindung und mindestens 0 L2TP-Sitzungen. Der Tunnel enthält gekapselte PPP-Datagramme und Kontrollnachrichten zwischen der LAC und dem LNS. Der Prozess ist für L2F identisch.
- **Sitzung**: L2TP ist verbindungsorientiert. Das LNS und die LAC verfügen über einen Status für jeden Anruf, der von einer LAC initiiert oder entgegengenommen wird. Zwischen dem LAC und dem LNS wird eine L2TP-Sitzung erstellt, wenn eine End-to-End-PPP-Verbindung zwischen einem Client und dem LNS hergestellt wird. Datagramme bezüglich der PPP-Verbindung werden über den Tunnel zwischen der LAC und dem LNS gesendet. Zwischen bestehenden L2TP-Sitzungen und den zugehörigen Anrufen besteht eine Eins-zu-Eins-Beziehung. Der Prozess ist für L2F identisch.

Übersicht über den VPDN-Prozess

In der Beschreibung des VPDN-Prozesses unten wird die L2TP-Terminologie (LAC und LNS) verwendet.



1. Der Client ruft die LAC an (in der Regel über ein Modem oder eine ISDN-Karte).
2. Der Client und die LAC starten die PPP-Phase, indem sie die LCP-Optionen (Authentication Method Password Authentication Protocol [PAP] oder Challenge Handshake Authentication Protocol [CHAP], PPP Multilink, Komprimierung usw.) aushandeln.
3. Nehmen wir an, CHAP wurde in Schritt 2 ausgehandelt. Die LAC sendet eine CHAP-Herausforderung an den Client.
4. Die LAC erhält eine Antwort (z. B. username@DomainName und Passwort).
5. Basierend auf dem Domänennamen, der in der CHAP-Antwort empfangen wurde, oder dem in der ISDN-Einrichtungsnachricht empfangenen DNIS (Dialed Number Information Service), prüft die LAC, ob es sich bei dem Client um einen VPDN-Benutzer handelt. Dies erfolgt über die lokale VPDN-Konfiguration oder über einen AAA-Server (Authentication, Authorization, Accounting).
6. Da der Client ein VPDN-Benutzer ist, erhält die LAC einige Informationen (aus ihrer lokalen VPDN-Konfiguration oder von einem AAA-Server), die sie zum Herstellen eines L2TP- oder L2F-Tunnels mit dem LNS verwendet.
7. Die LAC erstellt einen L2TP- oder L2F-Tunnel mit dem LNS.
8. Auf der Grundlage des Namens, der in der Anfrage von der LAC empfangen wurde, prüft das LNS, ob die LAC einen Tunnel öffnen darf (das LNS überprüft die lokale VPDN-Konfiguration). Darüber hinaus authentifizieren sich die LAC und das LNS gegenseitig (sie verwenden ihre lokale Datenbank oder wenden sich an einen AAA-Server). Der Tunnel ist dann zwischen beiden Geräten aktiv. In diesem Tunnel können mehrere VPDN-Sitzungen abgehalten werden.
9. Für den Client username@DomainName wird eine VPDN-Sitzung vom LAC zum LNS ausgelöst. Pro Client ist eine VPDN-Sitzung vorhanden.

10. Die LAC leitet die von ihr ausgehandelten LCP-Optionen zusammen mit dem username@DomainName und dem vom Client erhaltenen Kennwort an das LNS weiter.
11. Das LNS klont einen virtuellen Zugriff aus einer in der VPDN-Konfiguration angegebenen virtuellen Vorlage. Das LNS übernimmt die von der LAC empfangenen LCP-Optionen und authentifiziert den Client lokal oder durch Kontaktaufnahme mit dem AAA-Server.
12. Das LNS sendet eine CHAP-Antwort an den Client.
13. Die IP Control Protocol (IPCP)-Phase wird ausgeführt und anschließend die Route installiert: Die PPP-Sitzung ist zwischen dem Client und dem LNS aktiv. Die LAC leitet die PPP-Frames einfach weiter. Die PPP-Frames werden zwischen der LAC und dem LNS getunnelt.

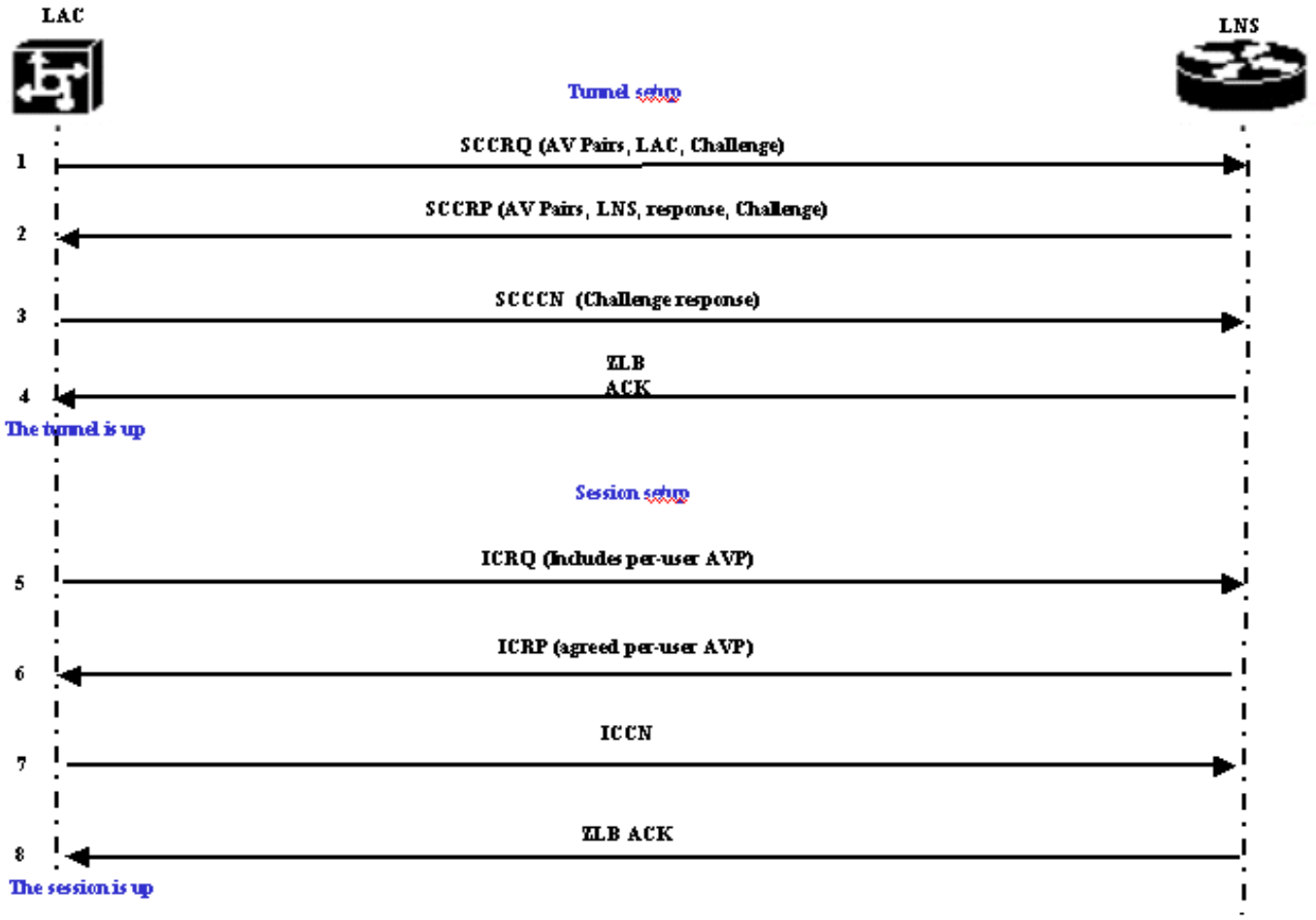
Tunneling-Protokolle

Ein VPDN-Tunnel kann entweder mit Layer-2-Forwarding (L2F) oder Layer-2-Tunneling Protocol (L2TP) erstellt werden.

- L2F wurde von Cisco in Request For Comments (RFC) 2341 eingeführt und wird auch zur Weiterleitung von PPP-Sitzungen für Multichassis Multilink PPP verwendet.
- L2TP, eingeführt in RFC 2661, kombiniert das Beste aus dem Cisco L2F-Protokoll und dem Microsoft Point-to-Point Tunneling Protocol (PPTP). Darüber hinaus unterstützt L2F nur Einwahl-VPDN, während L2TP sowohl Einwahl- als auch Auswahl-VPDN unterstützt.

Beide Protokolle verwenden den UDP-Port 1701, um einen Tunnel durch ein IP-Netzwerk zu erstellen und Link-Layer-Frames weiterzuleiten. Für L2TP besteht die Einrichtung für das Tunneling einer PPP-Sitzung aus zwei Schritten:

1. Einrichtung eines Tunnels zwischen der LAC und dem LNS. Diese Phase findet nur dann statt, wenn kein aktiver Tunnel zwischen beiden Geräten vorhanden ist.
2. Einrichten einer Sitzung zwischen der LAC und dem LNS.



Die LAC entscheidet, dass ein Tunnel von der LAC zum LNS initiiert werden muss.

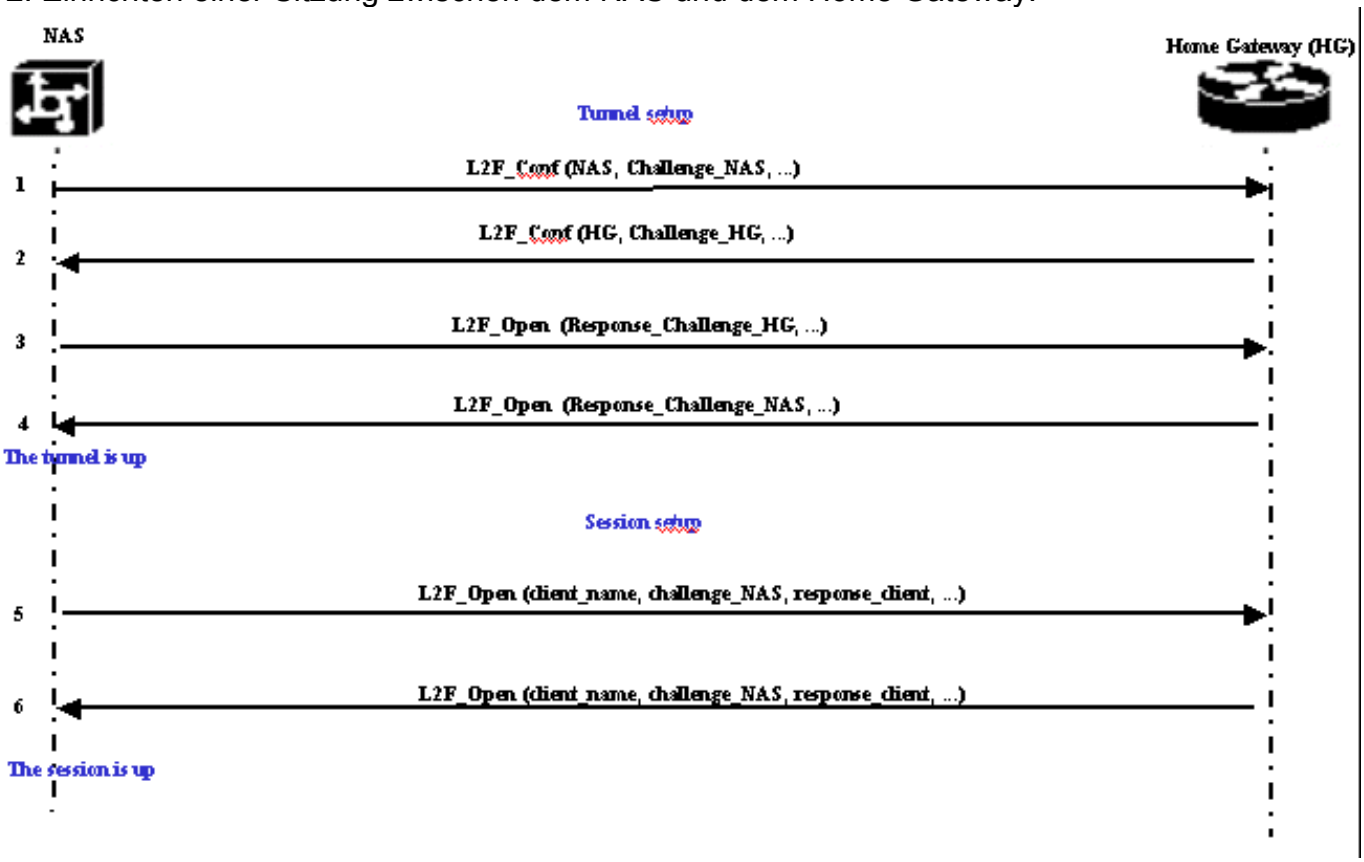
1. Die LAC sendet eine Start-Control-Connection-Request (SCCRQ). Eine CHAP-Herausforderung und AV-Paare sind in dieser Nachricht enthalten.
2. Das LNS reagiert mit einer Start-Control-Connection-Reply (SCCRP). Eine CHAP-Herausforderung, die Antwort auf die LAC-Herausforderung und AV-Paare sind in dieser Nachricht enthalten.
3. Die LAC sendet ein Start-Control-Connection-Connected (SCCCN). Die CHAP-Antwort ist in dieser Nachricht enthalten.
4. Das LNS reagiert mit einer Zero-Length Body Acknowledgement (ZLB ACK). Diese Bestätigung kann in einer anderen Nachricht erfolgen. Der Tunnel ist aktiv.
5. Die LAC sendet eine Incoming Call Request (ICRQ) an das LNS.
6. Das LNS antwortet mit einer ICRP-Nachricht (Incoming-Call-Reply).
7. Die LAC sendet eine ICCN (Incoming-Call Connected).
8. Das LNS antwortet mit einem ZLB ACK. Diese Bestätigung kann auch in einer anderen Nachricht erfolgen.
9. Die Sitzung ist beendet.

Hinweis: Die oben angegebenen Meldungen zum Öffnen eines Tunnels oder einer Sitzung enthalten Attribute Value Pairs (AVPs), die in RFC 2661 definiert sind. Sie beschreiben Eigenschaften und Informationen (z. B. Bearercap, Hostname, Anbietername und Fenstergröße). Einige AV-Paare sind obligatorisch, andere optional.

Hinweis: Eine Tunnel-ID wird verwendet, um Flex- und Demultiplex-Tunnel zwischen der LAC und dem LNS zu multiplizieren. Eine Sitzungs-ID wird verwendet, um eine bestimmte Sitzung mit dem Tunnel zu identifizieren.

Für L2F ist die Konfiguration für das Tunneling einer PPP-Sitzung identisch mit der für L2TP. Sie umfasst:

1. Einrichtung eines Tunnels zwischen dem NAS und dem Home Gateway. Diese Phase findet nur dann statt, wenn kein aktiver Tunnel zwischen beiden Geräten vorhanden ist.
2. Einrichten einer Sitzung zwischen dem NAS und dem Home Gateway.



Das NAS entscheidet, dass ein Tunnel vom NAS zum Home Gateway initiiert werden muss.

1. Das NAS-Gerät sendet eine L2F_Conf-Nachricht an das Home-Gateway. Eine CHAP-Herausforderung ist in dieser Nachricht enthalten.
2. Das Home-Gateway reagiert mit einer L2F_Conf. Eine CHAP-Herausforderung ist in dieser Nachricht enthalten.
3. Das NAS sendet ein L2F_Open. Die CHAP-Antwort der Home Gateway-Herausforderung ist in dieser Nachricht enthalten.
4. Das Home-Gateway reagiert mit L2F_Open. Die CHAP-Antwort auf die NAS-Herausforderung ist in dieser Nachricht enthalten. Der Tunnel ist aktiv.
5. Das NAS sendet ein L2F_Open-Signal an das Home-Gateway. Das Paket enthält den Benutzernamen des Clients (client_name), die vom NAS-Gerät an den Client gesendete CHAP-Herausforderung (Promotion_NAS) und seine Antwort (response_client).
6. Das Home-Gateway akzeptiert den Client, indem es L2F_OPEN zurücksendet. Der Datenverkehr kann nun in beide Richtungen zwischen dem Client und dem Home Gateway fließen.

Hinweis: Ein Tunnel ist mit einer CLID (Client-ID) gekennzeichnet. Die Multiplex-ID (MID) identifiziert eine bestimmte Verbindung innerhalb des Tunnels.

Konfigurieren von VPDN

Informationen zur Konfiguration von VPDN finden Sie im Handbuch zur Konfiguration virtueller privater Netzwerke und im Abschnitt zur Konfiguration von VPN.

Zugehörige Informationen

- Support-Seiten für die Dial- und Access-Technologie
- Technischer Support und Dokumentation - Cisco Systems