Inzicht VPDN

Inhoud

Inleiding

Een virtueel privé inbel-netwerk (VPDN) stelt een privé netwerkinbel in dienst in staat om over te spannen naar externe toegangsservers (gedefinieerd als de L2TP Access Concentrator [LAC]).

Wanneer een Point-to-Point Protocol (PPP)-client in een LAC inbellen, bepaalt de LAC dat deze PPP-sessie naar een L2TP-netwerkserver (LNS) voor die client moet worden doorgestuurd. LNS authenticeert de gebruiker en start de PPP onderhandeling. Zodra PPP de instelling is voltooid, worden alle frames via de LAC naar de client en de LNS verzonden.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor

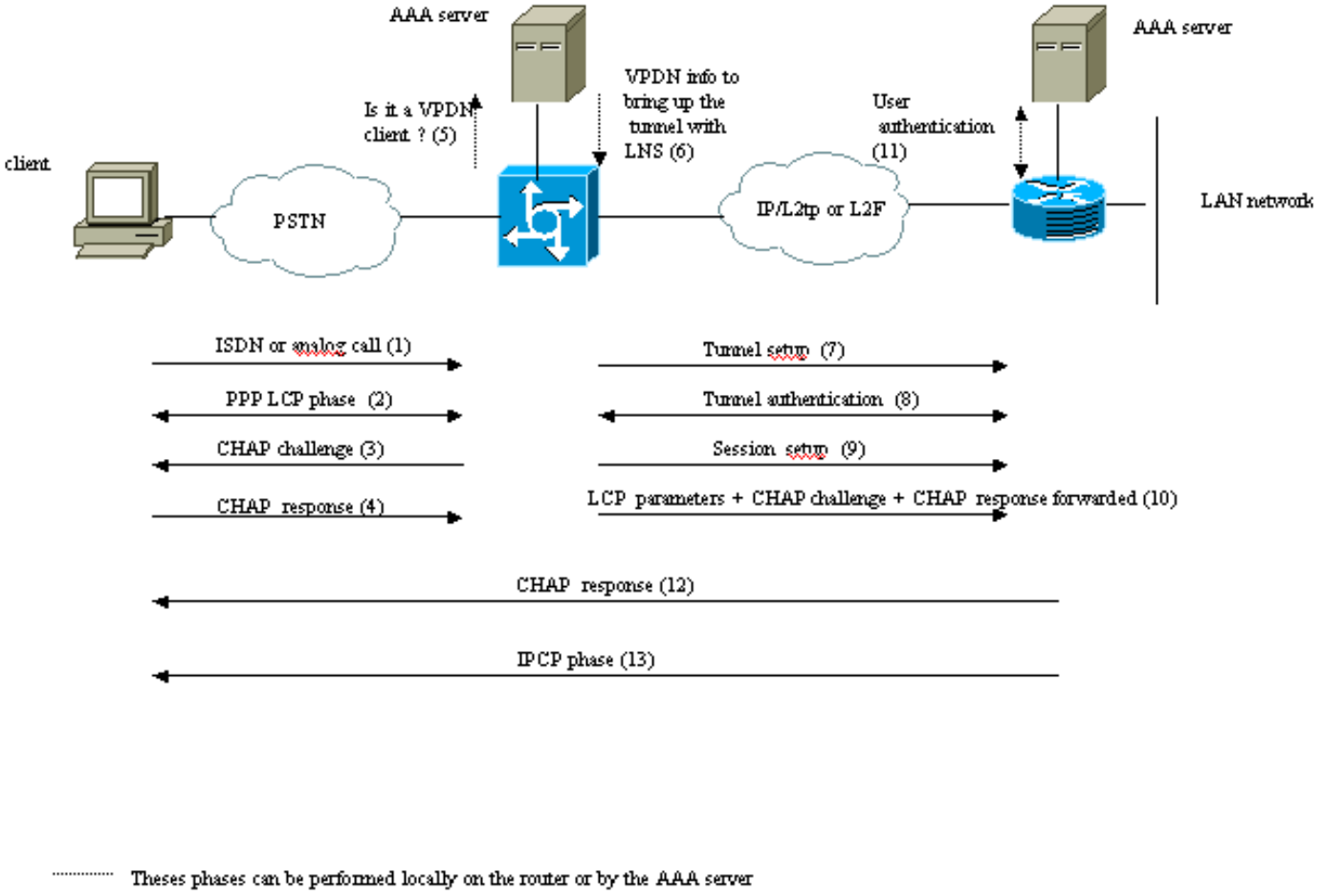
meer informatie over documentconventies.

Lijst

- **client**: PC of router die aan een ver toegangsnetwerk is bevestigd, dat de initiator van een vraag is.
- **L2TP**: Layer 2 Tunnel Protocol. PPP definieert een insluitingsmechanisme om multiprotocol pakketten over laag 2 (L2) point-to-point links te verzenden. Meestal verkrijgt een gebruiker een L2-verbinding naar een Network Access Server (NAS) door middel van een techniek zoals een dialoogvenster met vaste telefonie (POTS), ISDN of ADSL (Asymmetric Digital Subscriber Line). De gebruiker voert dan PPP over die verbinding uit. In een dergelijke configuratie, verblijven het L2-eindpunt en het PPP-sessiepunt op hetzelfde fysieke apparaat (de NAS).L2TP breidt het PPP model uit door de L2 en PPP eindpunten toe te staan om op verschillende apparaten te verblijven die door een netwerk onderling verbonden zijn. Met L2TP heeft de gebruiker een L2 verbinding met een toegangsconcentrator, en de concentrator tunnels dan individuele PPP frames naar de NAS. Hierdoor kan de eigenlijke verwerking van PPP-pakketten worden gescheiden van de beëindiging van het L2-circuit.
- **L2F**: Layer 2 Forwarding Protocol. L2F is een tunneling-protocol dat ouder is dan L2TP.
- **LAC**: L2TP-toegangscentrator. Een knooppunt dat fungeert als één kant van een L2TP-tunneleindpunt en een peer to the LNS is. De LAC zit tussen een LNS en een client en stuurt pakketten naar en van elke client door. Packets die van de LAC naar de LNS worden verzonden moeten worden aangepast met het L2TP-protocol. De verbinding van de LAC naar de client is normaal gesproken via ISDN of analoog.
- **LNS**: L2TP-netwerkserver. Een knooppunt dat fungeert als één kant van een L2TP-tunneleindpunt en een peer tot de LAC is. LNS is het logische eindpunt van een PPP zitting die van de cliënt door LAC wordt getunneld.
- **Thuisgateway**: Dezelfde definitie als LNS in L2F-terminologie.
- **NAS**: Dezelfde definitie als LAC in L2F-terminologie.
- **Tunnel:** In L2TP-terminologie bestaat er een tunnel tussen een LAC-LNS-paar. De tunnel bestaat uit een bedieningsverbinding en nul of meer L2TP-sessies. De tunnel draagt ingekapselde PPP datagrammen en controleberichten tussen de LAC en de LNS. Het proces is hetzelfde voor L2F.
- **Sessie**: L2TP is op verbindingen gericht. LNS en LAC onderhouden een status voor elke oproep die wordt geïnitieerd of beantwoord door een LAC. Er wordt een L2TP-sessie gemaakt tussen de LAC en LNS wanneer een end-to-end PPP-verbinding wordt ingesteld tussen een client en de LNS. Datagrammen gerelateerd aan de PPP verbinding worden verzonden over de tunnel tussen de LAC en LNS. Er is een één-op-één relatie tussen de gevestigde L2TP-sessies en de bijbehorende oproepen. Het proces is hetzelfde voor L2F.

Overzicht van het VPDN-proces

In de beschrijving van het VPDN-proces hieronder, gebruiken we de L2TP-terminologie (LAC en LNS).



1. De client belt de LAC (meestal een modem of een ISDN-kaart).
2. De client en de LAC starten de PPP-fase door te onderhandelen over de LCP-opties (Wachtwoord voor verificatiemethode [PAP] of Challenge Handshake Authentication Protocol [CHAP], PPP multilink, compressie enzovoort).
3. Stel dat CHAP in stap 2 is onderhandeld. De LAC stuurt een CHAP-uitdaging naar de klant.
4. De LAC krijgt een antwoord (bijvoorbeeld username@DomainName en een wachtwoord).
5. Gebaseerd op de domeinnaam die in de reactie CHAP of de DNIS van het Verwante Aantal Informatieservice (Dited Number Information Service) in het ISDN setup-bericht wordt ontvangen, controleert LAC of de client een VPDN-gebruiker is. Dit doet u door de lokale VPDN-configuratie te gebruiken of contact op te nemen met een AAA-server (verificatie, autorisatie en accounting).
6. Omdat de client een VPDN-gebruiker is, krijgt de LAC informatie (van zijn lokale VPDN-configuratie of van een AAA-server) die het gebruikt om een L2TP- of L2F-tunnel op te halen met de LNS.
7. De LAC brengt een L2TP- of L2F-tunnel op met de LNS.
8. Op basis van de naam die in het verzoek van de LAC wordt ontvangen, controleert de LNS of de LAC een tunnel mag openen (de LNS controleert de lokale VPDN-configuratie). Bovendien authenticeren de LAC en LNS elkaar (ze gebruiken hun lokale database of nemen contact op met een AAA server). De Tunnel is dan tussen beide apparaten omhoog. In deze tunnel kunnen meerdere VPDN-sessies worden meegevoerd.
9. Voor de client username@DomainName wordt een VPDN-sessie gestart van de LAC naar de LNS. Er is één VPDN-sessie per client.
10. LAC zendt de LCP-opties door die het met de LNS-client heeft onderhandeld, samen met de username@DomainName en het wachtwoord dat van de client is ontvangen.

11. De LNS klonen een virtuele toegang vanaf een virtuele-sjabloon die in de VPDN-configuratie is gespecificeerd. LNS neemt de LCP-opties die van de LAC zijn ontvangen en authenticeert de client lokaal of door contact op te nemen met de AAA-server.
12. De LNS stuurt een reactie van de CHAP op de cliënt.
13. De IPCP-fase (IP Control Protocol) wordt uitgevoerd en de route is geïnstalleerd: de PPP-sessie wordt uitgevoerd tussen de client en de LNS. De LAC stuurt net de PPP-frames door. De PPP kaders worden tussen de LAC en de LNS getunneld.

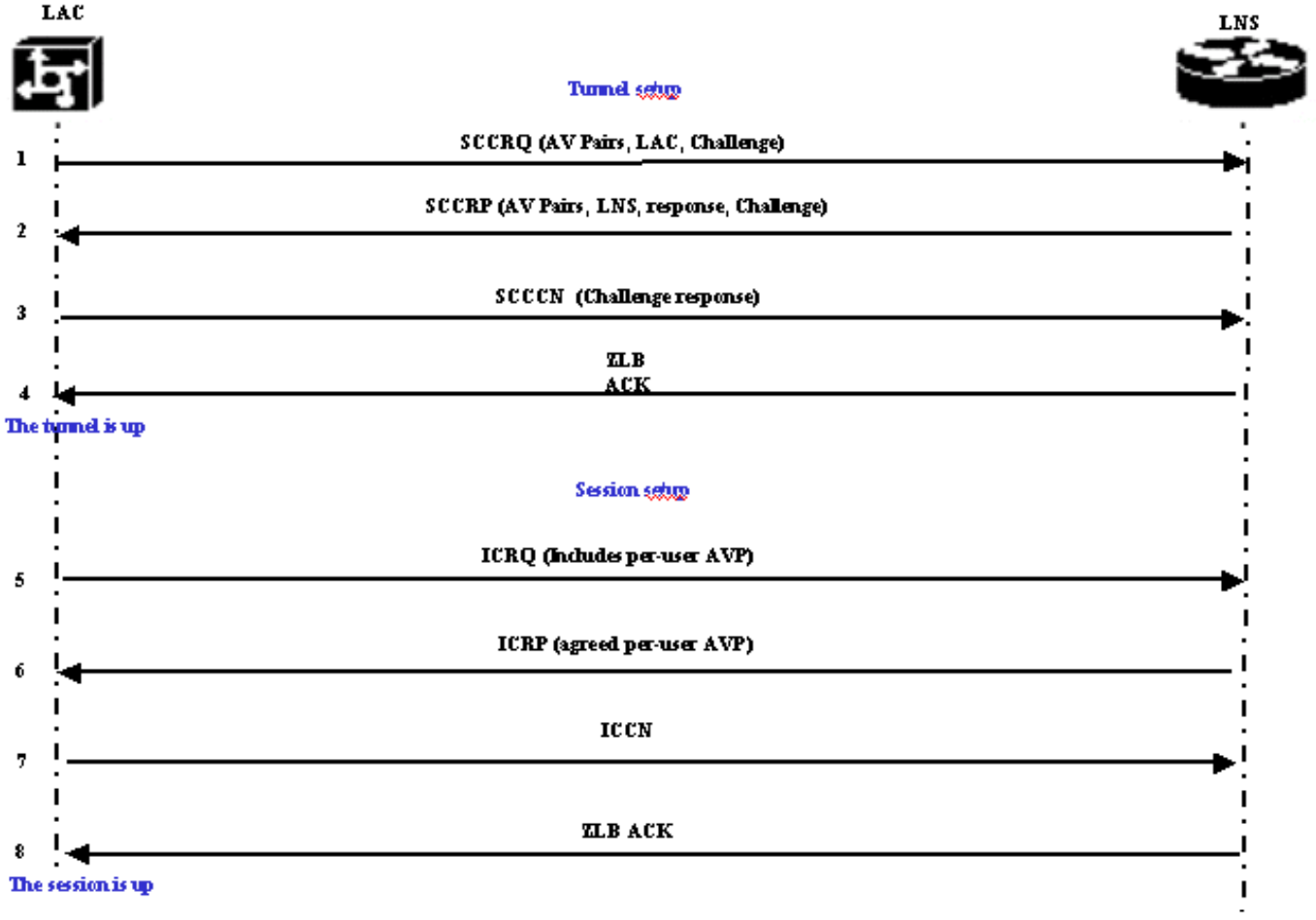
Tunneling-protocollen

Een VPDN-tunnel kan worden gebouwd met Layer 2 Forwarding (L2F) of Layer 2 Tunneling Protocol (L2TP).

- L2F is door Cisco geïntroduceerd in Application For Comments (RFC) 2341 en wordt ook gebruikt om PPP sessies te verzenden voor Multichassis Multilink PPP.
- L2TP, geïntroduceerd in RFC 2661, combineert de beste van het Cisco L2F-protocol en Microsoft Point-to-Point Tunneling Protocol (PPTP). Bovendien ondersteunt L2F alleen inbel-VPDN terwijl L2TP zowel inbel- als inbel-VPDN ondersteunt.

Beide protocollen gebruiken de UDP poort 1701 om een tunnel door een IP netwerk te bouwen om verbinding-laag frames door te sturen. Voor L2TP bestaat de instelling voor het tunnelen van een PPP-sessie uit twee stappen:

1. Het leggen van een tunnel tussen de LAC en de LNS. Deze fase vindt alleen plaats wanneer er geen actieve tunnel tussen beide apparaten bestaat.
2. Het instellen van een sessie tussen de LAC en de LNS.



De LAC besluit dat er een tunnel geïnitieerd moet worden van de LAC naar de LNS.

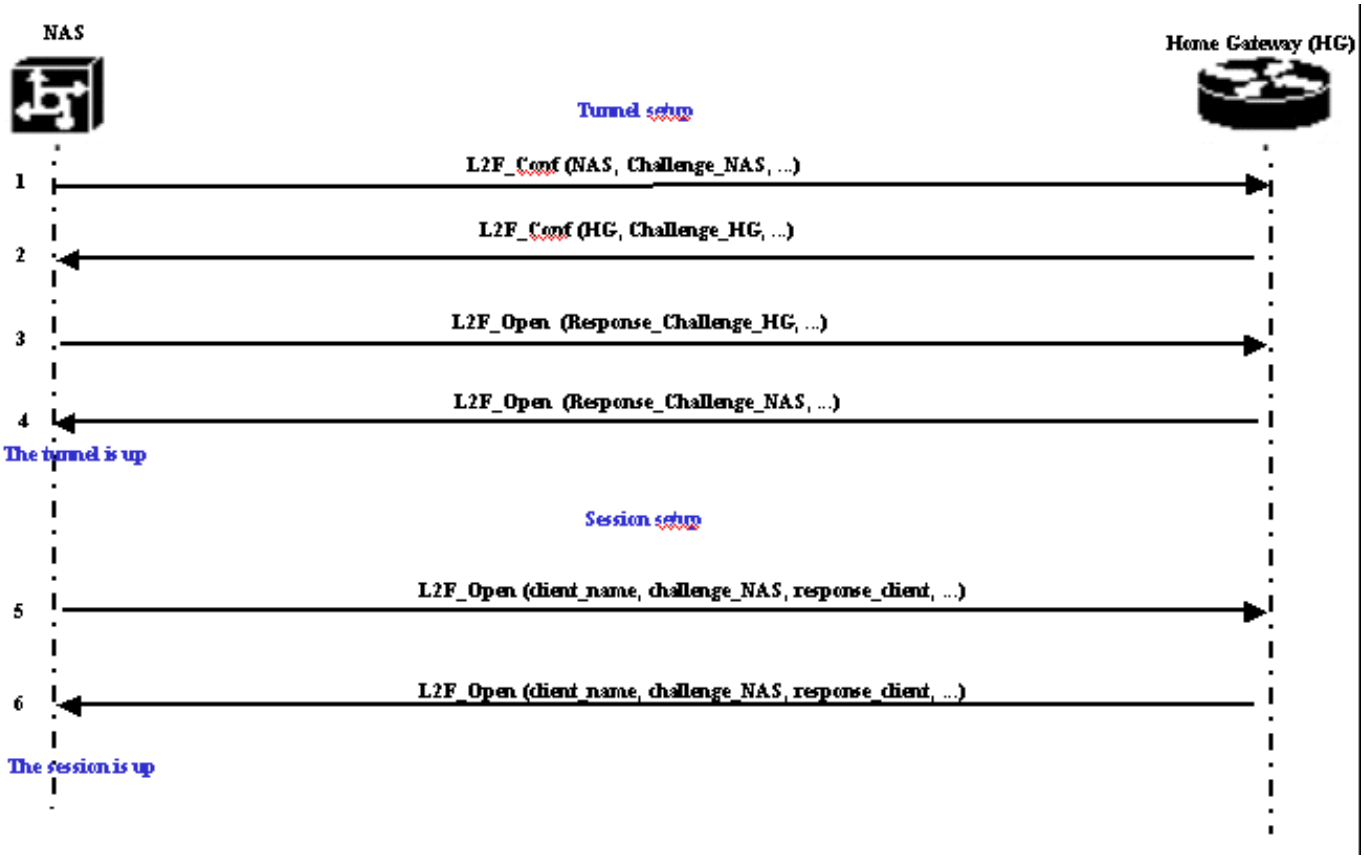
1. LAC stuurt een Start-Control-Connection-Application (SCCRQ). Er staan een CHAP-uitdaging en AV-paren in dit bericht.
2. LNS reageert met een Start-Control-Connection-Reactie (SCCRP). Een CHAP-uitdaging, de reactie op de uitdaging van LAC en AV-paren zijn in deze boodschap opgenomen.
3. LAC verstuurt een Start-Control-Connected Grid (SCN). De reactie van CHAP is in dit bericht opgenomen.
4. De LNS reageert met een Lichaamsbevestiging van nul lengte (ZLB ACK). Deze ontvangstbevestiging kan in een ander bericht worden overgebracht. De tunnel is omhoog.
5. De LAC stuurt een inkomende-Call-Aanvraag (ICRQ) naar de LNS.
6. LNS reageert met een ICRP-bericht (Inkomend-Call-antwoord).
7. De LAC stuurt een inkomende-Call-Connected (ICCON).
8. De LNS reageert met een ZLB-ACK. Deze ontvangstbevestiging kan ook in een ander bericht worden overgebracht.
9. De sessie is voorbij.

Opmerking: De hierboven gebruikte berichten voor het openen van een tunnel of een sessie draden de Waarde Paren van Kenmerken (AVP's), gedefinieerd in RFC 2661. Ze beschrijven eigenschappen en informatie (zoals Bearercap, hostname, leveranciersnaam en venstergrootte). Sommige AV-paren zijn verplicht en andere zijn optioneel.

Opmerking: Een Tunnel-ID wordt gebruikt om tunnels tussen de LAC en de LNS te multiplexen en demultiplexen. Een sessie-ID wordt gebruikt om een bepaalde sessie met de tunnel te identificeren.

Voor L2F is de instelling voor het tunnelen van een PPP-sessie hetzelfde als voor L2TP. Het gaat om:

1. Het leggen van een tunnel tussen de NAS en de Thuisgateway. Deze fase vindt alleen plaats wanneer er geen actieve tunnel tussen beide apparaten bestaat.
2. Het instellen van een sessie tussen de NAS en de startgateway.



De NAS besluit dat een tunnel geïnitieerd moet worden van de NAS naar de Thuisgateway.

1. NAS stuurt een L2F_Conf naar startgateway. In dit bericht is een CHAP-uitdaging opgenomen.
2. De startgateway reageert met een L2F_Conf. In dit bericht is een CHAP-uitdaging opgenomen.
3. De NAS stuurt een L2F_Open. De CHAP-respons van de Home Gateway-uitdaging is in dit bericht opgenomen.
4. De startgateway reageert met een L2F_Open. De CHAP-respons van de NAS-uitdaging is in dit bericht opgenomen. De tunnel is omhoog.
5. NAS stuurt een L2F_Open naar de startgateway. Het pakket bevat de gebruikersnaam van de client (client_name), de CHAP-uitdaging die door NAS naar de client wordt gestuurd (challenge_NAS) en de respons (response_client).
6. De startgateway, door de L2F_OPEN terug te sturen, accepteert de client. Het verkeer is nu vrij om in beide richtingen tussen de client en de gateway van het startpunt te lopen.

Opmerking: Er wordt een tunnel geïdentificeerd met een CLID (Client-ID). Multiplex-ID (MID) identificeert een bepaalde verbinding binnen de tunnel.

VPDN configureren

Raadpleeg voor informatie over het configureren van VPDN de handleiding Virtual Private Networks en ga naar de sectie over het configureren van VPN.

Gerelateerde informatie

- Ondersteuningspagina's voor bellen en toegang
- Technische ondersteuning en documentatie – Cisco Systems