Informazioni sulla VPDN

Sommario

Introduzione

Una VPDN (Virtual Private Dial-up Network) consente a un servizio di connessione remota di rete privata di collegarsi ai server di accesso remoto (definiti come L2TP Access Concentrator [LAC]).

Quando un client PPP (Point-to-Point Protocol) effettua una chiamata a un LAC, il LAC determina che deve inoltrare la sessione PPP a un server di rete L2TP (LNS) per quel client. Il servizio LNS quindi autentica l'utente e avvia la negoziazione PPP. Al termine dell'installazione del PPP, tutti i frame vengono inviati tramite il LAC al client e all'LNS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

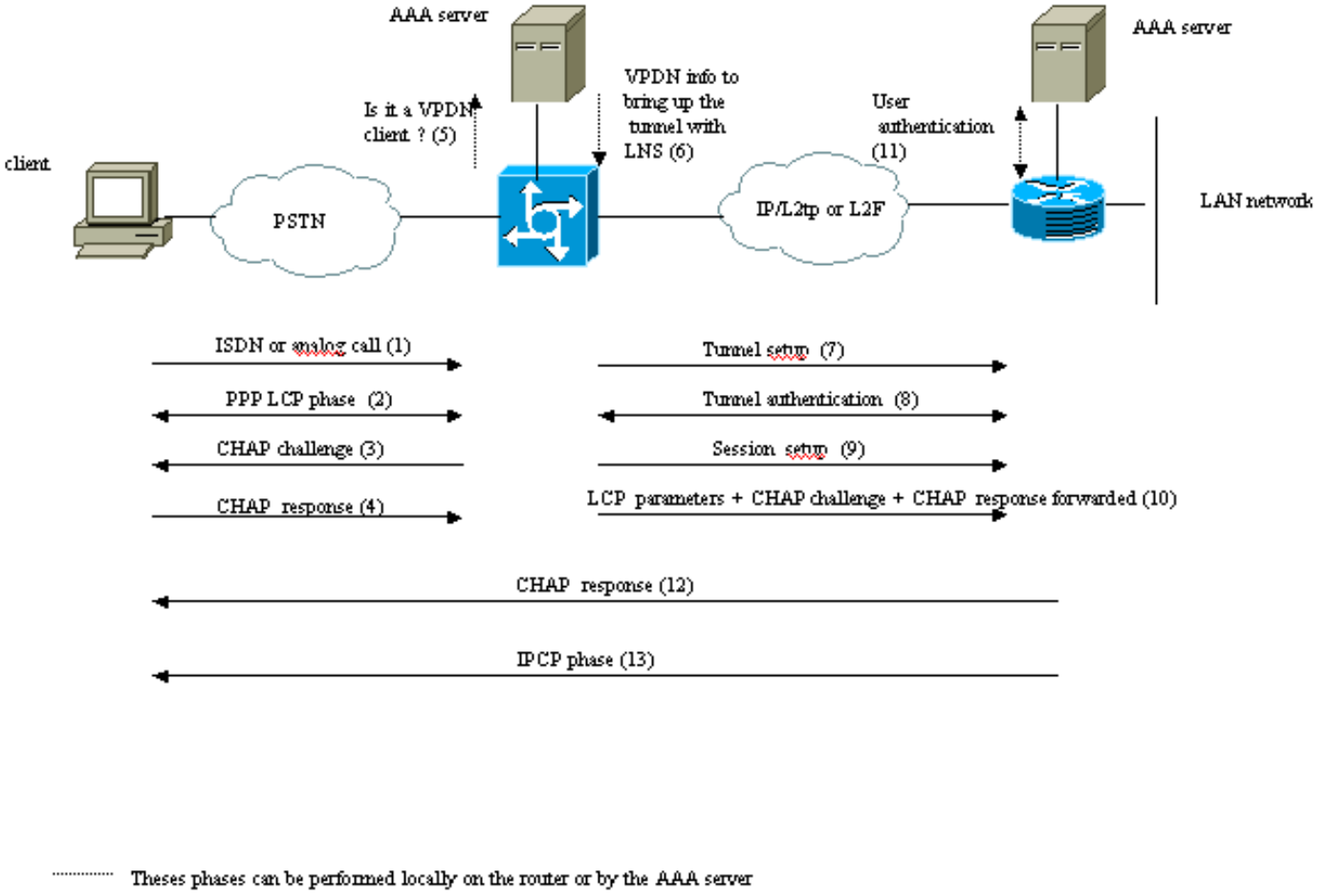
nei suggerimenti tecnici.

Glossario

- **Cliente**: PC o router collegato a una rete di accesso remoto, che è l'iniziatore di una chiamata.
- **L2TP**: Protocollo tunnel di livello 2. Il protocollo PPP definisce un meccanismo di incapsulamento per il trasporto di pacchetti multiprotocollo sui collegamenti point-to-point di layer 2 (L2). In genere, un utente ottiene una connessione L2 a un server di accesso alla rete (NAS) utilizzando una tecnica quale POTS (Plain Old Telephone Service), ISDN o ADSL (Asymmetric Digital Subscriber Line). L'utente esegue quindi il protocollo PPP su tale connessione. In una configurazione di questo tipo, il punto di terminazione L2 e l'endpoint della sessione PPP risiedono sullo stesso dispositivo fisico (il NAS).L2TP estende il modello PPP consentendo agli endpoint L2 e PPP di risiedere su dispositivi diversi interconnessi tramite una rete. Con L2TP, l'utente dispone di una connessione L2 a un concentratore di accesso e il concentratore esegue il tunneling dei singoli frame PPP al NAS. Ciò consente l'elaborazione effettiva dei pacchetti PPP da separare dalla terminazione del circuito L2.
- **L2F**: Protocollo di inoltro di livello 2. L2F è un protocollo di tunneling precedente a L2TP.
- **LAC**: L2TP Access Concentrator. Nodo che agisce come un lato di un endpoint del tunnel L2TP ed è un peer dell'LNS. Il LAC si trova tra un LNS e un client e inoltra i pacchetti da e verso ciascuno di essi. I pacchetti inviati dal LAC all'LAN richiedono il tunneling con il protocollo L2TP. La connessione tra il LAC e il client avviene in genere tramite ISDN o analogico.
- **LNS**: Server di rete L2TP. Nodo che agisce come un lato di un endpoint del tunnel L2TP ed è un peer del LAC. Il sistema LNS è il punto di terminazione logico di una sessione PPP di cui il LAC sta eseguendo il tunneling dal client.
- **Gateway domestico**: Stessa definizione di LNS nella terminologia L2F.
- **NAS**: Stessa definizione di LAC nella terminologia L2F.
- **Tunnel:** Nella terminologia L2TP, esiste un tunnel tra una coppia LAC-LNS. Il tunnel è costituito da una connessione di controllo e da zero o più sessioni L2TP. Il tunnel contiene datagrammi PPP incapsulati e messaggi di controllo tra il LAC e il LNS. Il processo è lo stesso per L2F.
- **Sessione**: L2TP è orientato alla connessione. I numeri LNS e LAC mantengono uno stato per ogni chiamata avviata o a cui viene risposto da un LAC. Una sessione L2TP viene creata tra il LAC e l'LNS quando viene stabilita una connessione PPP end-to-end tra un client e l'LNS. I datagrammi relativi alla connessione PPP vengono inviati sul tunnel tra il LAC e l'LNS. Esiste una relazione uno-a-uno tra le sessioni L2TP stabilite e le chiamate associate. Il processo è lo stesso per L2F.

Panoramica del processo VPDN

Nella descrizione del processo VPDN riportata di seguito, utilizziamo la terminologia L2TP (LAC e LNS).



1. Il client chiama il LAC (in genere utilizzando un modem o una scheda ISDN).
2. Il client e il LAC avviano la fase PPP negoziando le opzioni LCP (metodo di autenticazione Password Authentication Protocol [PAP] o Challenge Handshake Authentication Protocol [CHAP], PPP multilink, compressione e così via).
3. Si supponga che la protezione CHAP sia stata negoziata nel passaggio 2. Il LAC invia una richiesta di verifica della protezione CHAP al client.
4. Il LAC riceve una risposta (ad esempio, username@DomainName e password).
5. In base al nome di dominio ricevuto nella risposta CHAP o al DNIS (Dialed Number Information Service) ricevuto nel messaggio di installazione ISDN, il LAC controlla se il client è un utente VPDN. A tale scopo, utilizza la configurazione VPDN locale o contatta un server di autenticazione, autorizzazione e accounting (AAA).
6. Poiché il client è un utente VPDN, il LAC riceve alcune informazioni (dalla sua configurazione VPDN locale o da un server AAA) che utilizza per connettere un tunnel L2TP o L2F al LAN.
7. Il LAC richiama un tunnel L2TP o L2F con il sistema LNS.
8. In base al nome ricevuto nella richiesta dal LAC, il LNS controlla se il LAC è autorizzato ad aprire un tunnel (il LNS controlla la sua configurazione VPDN locale). Inoltre, il LAC e il LNS si autenticano a vicenda (usano il database locale o contattano un server AAA). Il tunnel è quindi attivo tra entrambi i dispositivi. In questo tunnel è possibile trasportare diverse sessioni VPDN.
9. Per il client username@DomainName, viene attivata una sessione VPDN dal LAC all'LNS. È presente una sessione VPDN per client.
10. Il LAC inoltra le opzioni LCP negoziate al sistema LNS con il client, insieme alla chiave username@DomainName e alla password ricevute dal client.
11. Il servizio LNS duplica un accesso virtuale da un modello virtuale specificato nella

configurazione VPDN. Il server LNS accetta le opzioni LCP ricevute dal LAC e autentica il client localmente o contattando il server AAA.

12. L'LNS invia una risposta CHAP al client.
13. Viene eseguita la fase IPCP (IP Control Protocol), quindi viene installato il router: la sessione PPP è attiva e in esecuzione tra il client e l'LNS. Il LAC inoltra semplicemente i frame PPP. I frame PPP vengono tunneling tra il LAC e l'LNS.

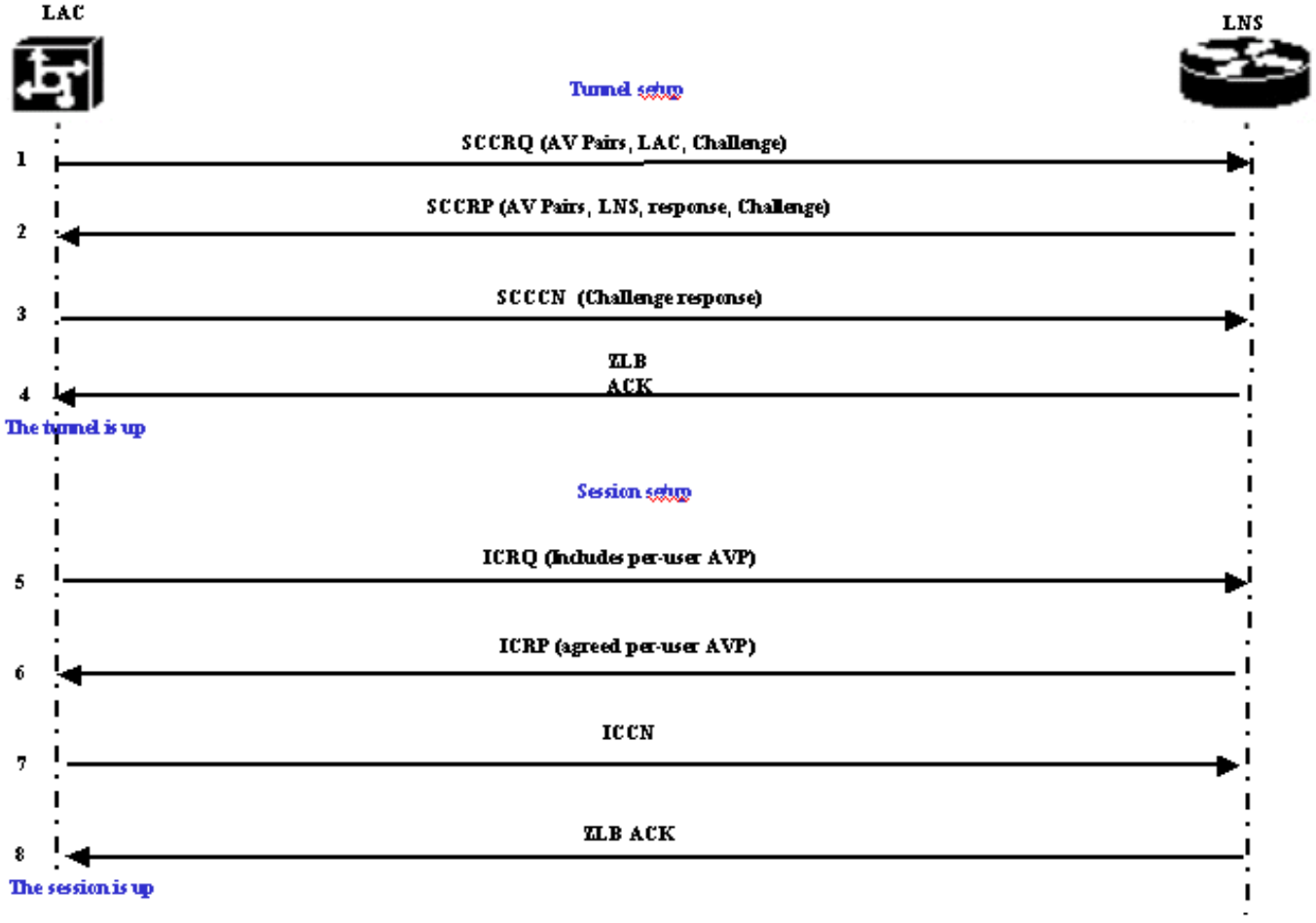
Protocolli di tunneling

Un tunnel VPDN può essere generato utilizzando l'inoltro di livello 2 (L2F) o il protocollo L2TP (Layer-2 Tunneling Protocol).

- L2F è stato introdotto da Cisco nella RFC (Request For Comments) 2341 ed è utilizzato anche per inoltrare sessioni PPP per Multilink PPP Multicassis.
- L2TP, introdotto nella RFC 2661, combina il meglio del protocollo Cisco L2F e del protocollo PPTP (Microsoft Point-to-Point Tunneling Protocol). Inoltre, L2F supporta solo la VPDN chiamata in ingresso, mentre L2TP supporta sia la VPDN chiamata in ingresso che quella chiamata in uscita.

Entrambi i protocolli usano la porta UDP 1701 per costruire un tunnel attraverso una rete IP e inoltrare i frame del livello di collegamento. Per L2TP, la configurazione del tunneling di una sessione PPP è costituita da due passaggi:

1. Creazione di un tunnel tra il LAC e il LNS. Questa fase ha luogo solo quando non vi è alcun tunnel attivo tra i due dispositivi.
2. Stabilire una sessione tra il LAC e il LNS.



Il LAC decide che il tunnel deve essere avviato tra il LAC e il LNS.

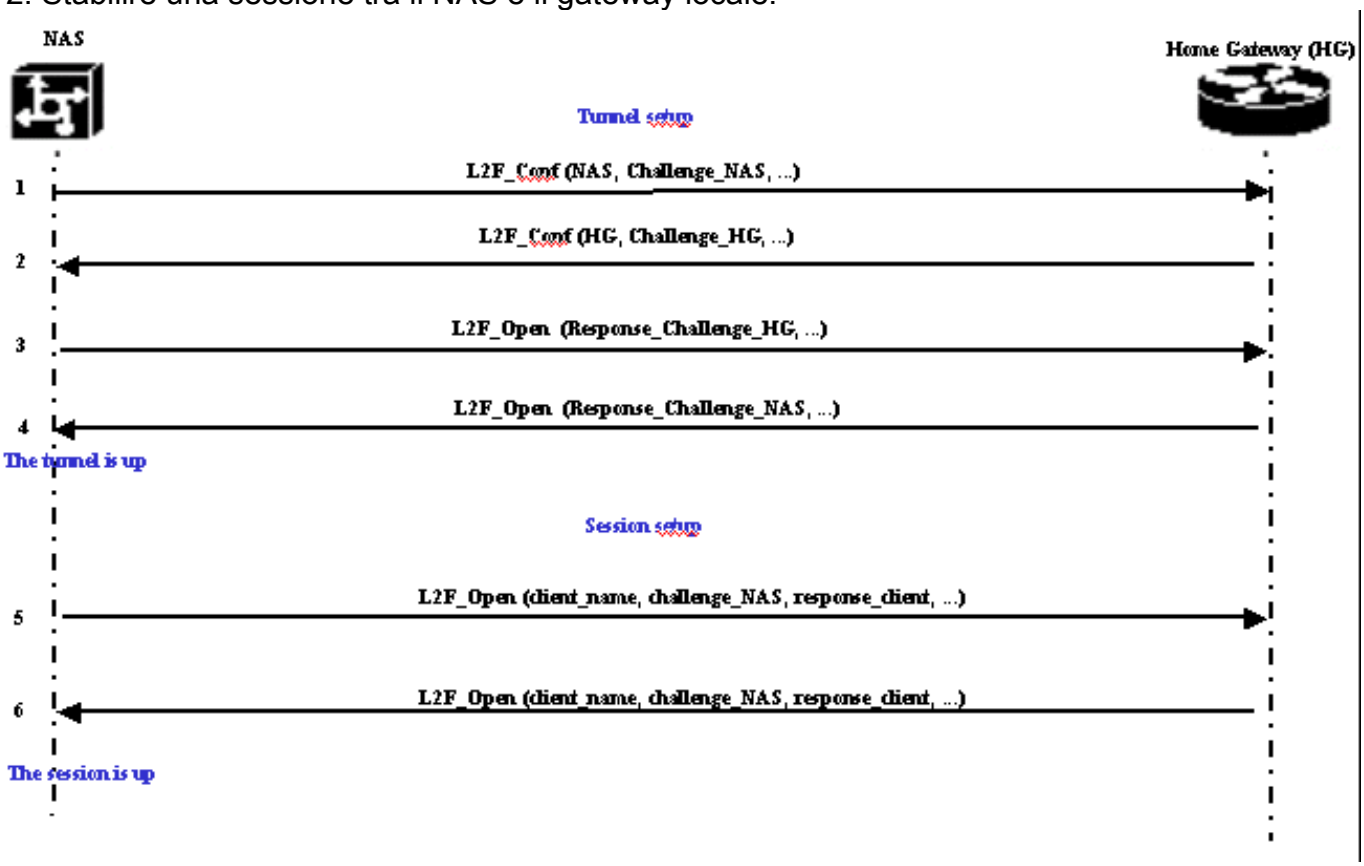
1. Il LAC invia un messaggio Start-Control-Connection-Request (SCCRQ). In questo messaggio sono incluse una richiesta CHAP e coppie di dispositivi AV.
2. L'LNS risponde con un SCCRP (Start-Control-Connection-Reply). Una sfida CHAP, la risposta alla sfida del LAC e le coppie AV sono incluse in questo messaggio.
3. Il LAC invia un messaggio Start-Control-Connection-Connected (SCCN). La risposta CHAP è inclusa in questo messaggio.
4. L'LNS risponde con un riconoscimento corpo di lunghezza zero (ZLB ACK). Tale menzione può figurare in un altro messaggio. Il tunnel è attivo.
5. Il LAC invia una richiesta di chiamata in arrivo (ICRQ) all'LNS.
6. L'LNS risponde con un messaggio ICRP (Incoming-Call-Reply).
7. Il LAC invia un messaggio Incoming-Call-Connected (ICCN).
8. L'LNS risponde con un ACK ZLB. Tale menzione può figurare anche in un altro messaggio.
9. Sessione attiva.

Nota: i messaggi sopra riportati, utilizzati per aprire un tunnel o una sessione, includono coppie di valori di attributo (AVP) definite nella RFC 2661. Descrivono proprietà e informazioni (ad esempio Bearercap, hostname, vendor name e window size). Alcune coppie AV sono obbligatorie mentre altre sono facoltative.

Nota: un ID tunnel viene usato per multiplex e demultiplex dei tunnel tra il LAC e il LNS. Un ID di sessione viene utilizzato per identificare una particolare sessione con il tunnel.

Per L2F, la configurazione per il tunneling di una sessione PPP è la stessa di L2TP. Esso comporta:

1. Creazione di un tunnel tra il NAS e il gateway locale. Questa fase ha luogo solo quando non vi è alcun tunnel attivo tra i due dispositivi.
2. Stabilire una sessione tra il NAS e il gateway locale.



Il NAS decide che un tunnel deve essere avviato dal NAS al gateway principale.

1. Il NAS invia un L2F_Conf al gateway locale. In questo messaggio è inclusa una richiesta CHAP.
2. Il gateway locale risponde con un L2F_Conf. In questo messaggio è inclusa una richiesta CHAP.
3. Il NAS invia un messaggio L2F_Open. In questo messaggio è inclusa la risposta CHAP della richiesta di verifica del gateway principale.
4. Il gateway locale risponde con un L2F_Open. In questo messaggio è inclusa la risposta CHAP della sfida NAS. Il tunnel è attivo.
5. Il NAS invia un L2F_Open al gateway principale. Il pacchetto include il nome utente del client (nome_client), la richiesta CHAP inviata dal server NAS al client (challenge_NAS) e la relativa risposta (response_client).
6. Il gateway locale, restituendo l'elemento L2F_OPEN, accetta il client. Il traffico tra il client e il gateway principale è ora libero di scorrere in entrambe le direzioni.

Nota: un tunnel è identificato da un CLID (ID client). L'ID multiplex (MID) identifica una particolare connessione all'interno del tunnel.

Configurazione della VPDN

Per informazioni sulla configurazione della VPDN, consultare il manuale Configurazione delle reti private virtuali e andare alla sezione sulla configurazione della VPN.

Informazioni correlate

- Pagine di supporto per la tecnologia di composizione e accesso
- Documentazione e supporto tecnico – Cisco Systems