Virtual Private Network e Internet Key Exchange per Cisco VPN serie 5000 Concentrator

Sommario

Introduzione

IKE (Internet Key Exchange) è un metodo standard utilizzato per organizzare comunicazioni autenticate protette. Cisco VPN 5000 Concentrator utilizza il protocollo IKE per configurare i tunnel IPSec. Questi tunnel IPSec sono la backbone di questo prodotto.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- VPN serie 5000 Concentrator

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.

Attività IKE

IKE gestisce le seguenti attività:

- Autenticazione
- Negoziazione sessione
- Scambio chiave
- Negoziazione e configurazione tunnel IPSec

Autenticazione

L'autenticazione è l'attività più importante eseguita da IKE ed è la più complessa. Ogni volta che si negozia qualcosa, è importante sapere con chi si negozia. IKE può utilizzare uno dei diversi metodi disponibili per autenticare le parti della negoziazione.

- **Chiave condivisa**: IKE utilizza una tecnica di hashing per garantire che solo un utente che possiede la stessa chiave possa inviare i pacchetti IKE.
- **Firme digitali DSS (Digital Signature Standard) o Rivest, Shamir, Adelman (RSA)** - IKE utilizza la crittografia della firma digitale a chiave pubblica per verificare che ogni parte sia quella che dichiara di essere.
- **Crittografia RSA**: IKE utilizza uno dei due metodi disponibili per crittografare una parte della negoziazione sufficiente a garantire che solo una parte con la chiave privata corretta possa continuare la negoziazione.

Negoziazione sessione
Durante la negoziazione delle sessioni, IKE consente alle parti di negoziare le modalità di autenticazione e di protezione di eventuali negoziazioni future, ovvero la negoziazione del tunnel IPSec. Questi elementi sono negoziati:

- **Metodo di autenticazione**: uno dei metodi elencati nella sezione Autenticazione di questo documento.
- **Algoritmo di scambio chiave**: tecnica matematica per lo scambio sicuro di chiavi crittografiche su un supporto pubblico (Diffie-Hellman). Le chiavi vengono utilizzate negli algoritmi di crittografia e firma dei pacchetti.
- **Algoritmo di crittografia** - DES (Data Encryption Standard) o 3DES (Triple Data Encryption Standard).
- **Algoritmo di firma del pacchetto** - Message Digest 5 (MD5) e Secure Hash Algorithm 1 (SHA-1).

Scambio chiave

IKE utilizza il metodo di scambio delle chiavi negoziato (vedere la sezione Negoziazione delle sessioni di questo documento) per creare un numero di bit di materiale per le chiavi crittografiche sufficiente a proteggere le transazioni future. Questo metodo garantisce che ogni sessione IKE sia protetta con un nuovo set di chiavi protetto.

L'autenticazione, la negoziazione di sessioni e lo scambio di chiavi costituiscono la prima fase di una negoziazione IKE. Per un concentratore VPN 5000, queste proprietà vengono configurate nella sezione **Criteri IKE** tramite la parola chiave Protection. Questa parola chiave è un'etichetta composta da tre parti: algoritmo di autenticazione, algoritmo di crittografia e algoritmo di scambio chiavi. I pezzi sono separati da un carattere di sottolineatura. L'etichetta MD5_DES_G1 indica che è necessario utilizzare MD5 per l'autenticazione dei pacchetti IKE, DES per la crittografia dei pacchetti IKE e Diffie-Hellman Group 1 per lo scambio di chiavi. Per ulteriori informazioni, vedere Configurazione dei criteri IKE per la protezione del tunnel IPSec.

Negoziazione e configurazione tunnel IPSec

Dopo aver completato la negoziazione di un metodo sicuro per lo scambio di informazioni (fase uno), IKE viene utilizzato per negoziare un tunnel IPSec. Questa operazione viene eseguita utilizzando la fase due di IKE. In questo scambio, IKE crea nuovo materiale per le chiavi da utilizzare per il tunnel IPSec (utilizzando i tasti di fase uno IKE come base o eseguendo un nuovo scambio di chiavi). Vengono inoltre negoziati gli algoritmi di crittografia e autenticazione per il tunnel.

I tunnel IPSec vengono configurati utilizzando la sezione VPN Group (in precedenza denominata client STEP (Secure Tunnel Establishment Protocol) per i tunnel client VPN e la sezione Tunnel Partner per i tunnel LAN-LAN. Nella sezione **Utenti VPN** viene memorizzato il metodo di autenticazione per ogni utente. Per ulteriori informazioni, vedere Configurazione dei criteri IKE per la sicurezza del tunnel IPSec.

Estensioni VPN 5000 Concentrator IKE

- **RADIUS** - IKE non supporta l'autenticazione RADIUS. L'autenticazione RADIUS viene eseguita in uno scambio speciale di informazioni che ha luogo dopo il primo pacchetto IKE inviato dal client VPN. Se è richiesto il protocollo PAP (Password Authentication Protocol), è necessario un segreto di autenticazione RADIUS speciale. Per ulteriori informazioni, fare riferimento alla documentazione di NoCHAP e PAPAuthSecret in Configurazione dei criteri IKE per la sicurezza del tunnel IPSec. L'autenticazione RADIUS è autenticata e crittografata. Lo scambio PAP è protetto da PAPAuthSecret. Tuttavia, poiché esiste un solo segreto per l'intero pacchetto IntraPort, la protezione è minima quanto quella offerta da qualsiasi password condivisa.
- **SecurID** - IKE non supporta attualmente l'autenticazione SecurID. L'autenticazione SecurID viene eseguita in uno speciale scambio di informazioni tra la fase uno e la fase due. Questo scambio è completamente protetto dalla Security Association (SA) IKE negoziata nella prima fase.
- **STAMP (Secure Tunnel Access Management Protocol)**: le connessioni client VPN scambiano informazioni con IntraPort durante il processo IKE. Informazioni come se fosse possibile salvare segreti, quali reti IP tunnel o se tunnel il traffico IPX (Internetwork Packet Exchange) vengono inviate in payload privati durante gli ultimi due pacchetti IKE. Questi payload vengono inviati solo ai client VPN compatibili.

ISAKMP e Oakley

Il protocollo ISAKMP (Internet Security Association and Key Management Protocol) è un

linguaggio utilizzato per condurre negoziazioni in Internet, ad esempio tramite il protocollo IP. Oakley è un metodo per lo scambio autenticato di materiale contenente chiavi crittografiche. IKE raggruppa i due dispositivi in un unico pacchetto che consente di configurare connessioni sicure su Internet non protetto.

STEP e STAMP

STEP (Secure Tunnel Establishment Protocol) è il nome precedente del sistema VPN. Nei giorni precedenti a IKE è stato utilizzato STAMP per negoziare le connessioni IPSec. Le versioni del client VPN precedenti alla 3.0 utilizzano STAMP per stabilire una connessione con IntraPort.

Informazioni correlate

- Cisco VPN serie 5000 concentrator: annuncio di fine vendita
- Configurazione di un tunnel da router a VPN serie 5000 concentrator da LAN a LAN
- Cisco VPN 5000 Concentrator - Pagina di supporto dei prodotti
- Pagina di supporto dei prodotti Cisco VPN 5000 Client
- Negoziazione IPSec/supporto tecnologia protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems