Virtual Private Networks en Internet Key Exchange voor Cisco VPN 5000 Concentrator Series

Inhoud

Inleiding

Internet Key Exchange (IKE) is een standaardmethode die wordt gebruikt om beveiligde, gewaarmerkte communicatie te regelen. Cisco VPN 5000 Concentrator gebruikt IKE om IPSec-tunnels in te stellen. Deze IPSec-tunnels zijn de ruggengraat van dit product.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VPN 5000 Series Concentrator

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

IKE-taken

IKE behandelt deze taken:

- Verificatie
- Sessieonderhandeling
- Sleutel
- IPsec-tunnelonderhandeling en -configuratie

Verificatie

Verificatie is de belangrijkste taak die IKE uitvoert en is de meest gecompliceerde. Telkens als je iets onderhandelt, is het belangrijk om te weten met wie je onderhandelt. IKE kan een van meerdere methoden gebruiken om onderhandelingspartijen aan elkaar te authentiseren.

- **Shared key** - IKE gebruikt een hashing-techniek om ervoor te zorgen dat alleen iemand met dezelfde toets de IKE-pakketten kan verzenden.
- **Digital Signature Standard (DSS) of Rivest, Shamir, Adelman (RSA) digitale handtekeningen** - IKE gebruikt cryptografie met digitale handtekeningen van een openbare sleutel om te controleren of elke partij is wie zij claimen te zijn.
- **RSA-encryptie** - IKE gebruikt een van twee methoden om genoeg van de onderhandeling te versleutelen om te verzekeren dat alleen een partij met de juiste privé-sleutel de onderhandelingen kan voortzetten.

Sessieonderhandeling
Tijdens sessieonderhandelingen stelt IKE partijen in staat te onderhandelen over de wijze waarop zij authenticatie zullen uitvoeren en hoe zij toekomstige onderhandelingen zullen beschermen (dat wil zeggen, onderhandelingen met IPSec-tunnels). Over deze punten wordt onderhandeld:

- **Verificatiemethode** - Dit is een van de methoden die in de sectie Verificatie van dit document worden vermeld.
- **Key exchange algoritme** - Dit is een wiskundige techniek voor het veilig uitwisselen van cryptografische sleutels via een openbaar medium (Diffie-Hellman). De toetsen worden gebruikt voor encryptie- en pakketkenmerkende algoritmen.
- **Encryption algoritme** - Data Encryption Standard (DES) of Triple Data Encryption Standard (3DES).
- **Packet signatuur** - Message Digest 5 (MD5) en Secure Hash Algorithm 1 (SHA-1).

Sleutel

IKE gebruikt de methode voor het uitwisselen van sleutel via onderhandelingen (zie het gedeelte Sessieonderhandeling van dit document) om genoeg stukjes cryptografisch materiaal te maken om toekomstige transacties veilig te stellen. Deze methode garandeert dat elke IKE-sessie wordt beschermd met een nieuwe, beveiligde set toetsen.

Verificatie, sessieonderhandeling en belangrijke uitwisseling vormen fase één van een IKE-onderhandeling. Voor een VPN 5000 Concentrator, worden deze eigenschappen in de sectie van het **IKE Beleid** door het sleutelwoord van de Bescherming gevormd. Dit sleutelwoord is een etiket dat drie stukken heeft: algoritme voor verificatie, encryptie algoritme en algoritme voor sleuteluitwisseling. De stukken worden van elkaar gescheiden door een underscore. Het etiket MD5_DES_G1 betekent gebruik MD5 voor IKE-pakketverificatie, gebruik DES voor IKE-pakketencryptie en gebruik Diffie-Hellman groep 1 voor belangrijke uitwisseling. Raadpleeg voor meer informatie het configureren van het IKE-beleid voor IPSec-tunnelbeveiliging.

IPsec-tunnelonderhandeling en -configuratie

Nadat IKE over een veilige methode voor het uitwisselen van informatie heeft onderhandeld (fase één), wordt IKE gebruikt om te onderhandelen over een IPSec-tunnel. Dit wordt bereikt met IKE fase twee. In deze uitwisseling creëert IKE vers sluitingsmateriaal voor de IPSec-tunnel om te gebruiken (ofwel door de IKE fase 1 toetsen als basis te gebruiken of door een nieuwe sleuteluitwisseling uit te voeren). Er wordt ook onderhandeld over de encryptie- en authenticatiealgoritmen voor deze tunnel.

IPSec-tunnels worden geconfigureerd met behulp van de VPN-groep (voorheen de Secure Tunnel Protocol (STEP-client) voor VPN-clienttunnels en de Tunnel partner-sectie voor LAN-naar-LAN tunnels. Het gedeelte **VPN-gebruikers** is de locatie waar de verificatiemethode voor elke gebruiker is opgeslagen. Deze secties zijn gedocumenteerd in het configureren van het IKE-beleid voor IPSec Tunnel security.

VPN 5000 Concentrator IKE-uitbreidingen

- **RADIUS** - IKE heeft geen ondersteuning voor RADIUS-verificatie. RADIUS-verificatie wordt uitgevoerd in een speciale informatie-uitwisseling die plaatsvindt na het eerste IKE-pakket van de VPN-client. Als Password Authentication Protocol (PAP) vereist is, wordt een speciaal RADIUS-verificatiegeheim vereist. Raadpleeg voor meer informatie de documentatie bij NoCHAP en PAPAuthSecret in het configureren van het IKE-beleid voor IPSec Tunnel security. RADIUS-verificatie is authentiek en versleuteld. De PAP-uitwisseling wordt beschermd door het PAPAuthSecret. Er is echter maar één geheim voor de gehele IntraPort-serie, zodat de bescherming net zo zwak is als ieder gedeeld wachtwoord.
- **SecurID** - IKE biedt momenteel geen ondersteuning voor SecurID-verificatie. SecurID - verificatie wordt uitgevoerd in een speciale uitwisseling van informatie tussen fase één en fase twee. Deze uitwisseling wordt volledig beschermd door de IKE Security Association (SA) die in fase één onderhandeld heeft.
- **Secure Tunnel Access Management Protocol (STAMP)** - VPN-clientverbindingen wisselen informatie uit met IntraPort tijdens het IKE-proces. Informatie zoals als het al goed is om geheimen op te slaan, welke IP netwerken om te tunnel, of of om het verkeer van de Uitwisseling van de Internetwork (IPX) te tunnen, in privé lading tijdens de laatste twee pakketten IKE wordt verzonden. Deze payloads worden alleen naar compatibele VPN-clients verzonden.

ISAKMP en Oakley

De Internet Security Association en Key Management Protocol (ISAKMP) is een taal die wordt

gebruikt om onderhandelingen over het internet te voeren (bijvoorbeeld via het IP-protocol). Oakley is een methode voor het uitvoeren van een gewaarmerkte uitwisseling van cryptografisch belangrijk materiaal. IKE brengt de twee samen in één pakket, waardoor veilige verbindingen kunnen worden opgezet over het onveilige internet.

STAP en STAMP

Secure Tunnel Format Protocol (STEP) is de vorige naam van het VPN-systeem. In de pre-IKE dagen werd STAMP gebruikt om te onderhandelen over IPSec-verbindingen. De VPN-clientversies eerder dan 3.0 gebruiken STAMP om een verbinding met een IntraPort-adapter op te zetten.

Gerelateerde informatie

- Cisco VPN 5000 Series Concentrators end-of-sale aankondiging
- Een router-to-VPN 5000 Series Concentrator LAN-to-LAN tunnellijnen configureren
- Productondersteuningspagina voor Cisco VPN 5000 Concentrator
- Cisco VPN 5000 pagina voor clientproductondersteuning
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems