ASA en Native L2TP-IPSec Android-clientconfiguratievoorbeeld

Inhoud

Inleiding

Layer 2 Tunneling Protocol (L2TP) via IPSec biedt de mogelijkheid om een L2TP VPN-oplossing naast IPSec VPN en firewallservices in één platform te implementeren en beheren. Het primaire voordeel van de configuratie van L2TP via IPSec in een ver toegangsscenario is dat de externe gebruikers toegang kunnen krijgen tot een VPN via een openbaar IP-netwerk zonder een gateway of een specifieke lijn, die externe toegang van vrijwel elke plaats met gewone oude telefoonservice (POTS) mogelijk maakt. Een bijkomend voordeel is dat de enige clientbehoefte voor VPN-toegang het gebruik van Windows met Microsoft Dial-Up Network (DUN) is. Er is geen extra clientsoftware nodig, zoals de Cisco VPN-clientsoftware.

Dit document biedt een voorbeeldconfiguratie voor de native L2TP/IPSec Android-client. Het voert u door alle benodigde opdrachten op een Cisco adaptieve security applicatie (ASA), evenals de stappen die op het Android-apparaat zelf moeten worden gezet.

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 hardwareversies:

- Voor Android L2TP/IPSec is Cisco ASA-softwareversie 8.2.5 of later, versie 8.3.2.12 of hoger, of versie 8.4.1 of hoger vereist.
- ASA ondersteunt Secure Hash Algorithm 2 (SHA2) ondersteuning voor certificeringsmerken voor Microsoft Windows 7 en Android-native VPN-clients wanneer het L2TP/IPSec-protocol wordt gebruikt.
- Zie Cisco ASA 5500 Series configuratiegids met behulp van de CLI, 8.4 en 8.6: L2TP configureren via IPSec: Licentievereisten voor L2TP via IPSec.

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. 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.

Configureren

In dit gedeelte wordt de informatie beschreven die u nodig hebt om de functies te configureren die in dit document worden beschreven.

Het configureren van de L2TP/IPSec-verbinding op de Android

Deze procedure beschrijft hoe u de L2TP/IPSec-verbinding op de Android kunt configureren:

1. Open het menu en kies **Instellingen**.
2. Kies **Draadloos en netwerk** of **draadloze controller**. De beschikbare optie is afhankelijk van uw versie van Android.
3. Kies **VPN-instellingen**.
4. Kies **VPN toevoegen**.
5. Kies **Add L2TP/IPsec PSK VPN**.
6. Kies **VPN-naam** en voer een descriptieve naam in.
7. Kies **VPN-server** en voer een descriptieve naam in.
8. Kies **Stel IPSec vooraf gedeelde toets in**.
9. Schakel **het geheim L2TP uit**.
10. [Optioneel] Stel de IPSec-identificator in als de ASA-tunnelgroepsnaam. Geen enkele instelling betekent dat het in DefaultRAGGroup valt op de ASA.
11. Open het menu en kies **Opslaan**.

Het configureren van de L2TP/IPSec-verbinding op ASA

Dit zijn de vereiste ASA Internet Key Exchange versie 1 (IKEv1) (Internet Security Association en Key Management Protocol [ISAKMP])-beleidsinstellingen die native VPN-clients, geïntegreerd met het besturingssysteem op een eindpunt, in staat stellen een VPN-verbinding met de ASA te maken wanneer L2TP via IPSec-protocol wordt gebruikt:

- IKEv1 fase 1 - Triple Data Encryption Standard (3DES)-encryptie met SHA1-hashmethode
- IPSec fase 2 - 3DES of Advanced Encryption Standard (AES) encryptie met Message Digest 5 (MD5) of SHA-hashmethode
- PPP-verificatie - Password-verificatie Protocol (PAP), Microsoft Challenge Handshake Authentication Protocol, versie 1 (MS-CHAPv1) of MS-CHAPv2 (voorkeursbehandeling)
- Vooraf gedeelde sleutel

  Opmerking: ASA ondersteunt alleen de PPP authenticaties PAP en MS-CHAP (versies 1 en 2) op de lokale database. Het Extensible Authentication Protocol (EAP) en CHAP worden uitgevoerd door proxy-servers. Daarom, als een externe gebruiker tot een tunnelgroep behoort die met de opdrachten **authenticatie-**of **authenticatieschap** wordt ingesteld en als de ASA is ingesteld om de lokale database te gebruiken, kan die gebruiker geen verbinding maken.

  Bovendien ondersteunt Android PAP niet en is LDAP, omdat het lichtgewicht Directory Access Protocol (LDAP) MS-CHAP niet ondersteunt, geen bruikbaar verificatiemechanisme. De enige tijdelijke oplossing is het gebruik van RADIUS. Zie Cisco Bug ID CSCtw58945, "L2TP over IPSec-verbindingen faalt bij ldap-autorisatie en MSV2" voor verdere details over kwesties met MS-CHAP en LDAP.

Deze procedure beschrijft hoe u de L2TP/IPSec-verbinding op de ASA kunt configureren:

1. Defineer een lokale adrepool of gebruik een dhcp-server voor het adaptieve security apparaat om IP-adressen aan de klanten voor het groepsbeleid toe te wijzen.
2. Creëer een intern groepsbeleid. Defineert het tunnelprotocol om l2tp-ipsec te zijn.Configureer een domeinnaamserver (DNS) die door de clients wordt gebruikt.
3. Maak een nieuwe tunnelgroep of wijzig de eigenschappen van de bestaande DefaultRAGgroup. (Een nieuwe tunnelgroep kan worden gebruikt als de IPSec identifier wordt ingesteld als groepsnaam op de telefoon; zie stap 10 voor de telefoonconfiguratie.)
4. Defineert de algemene eigenschappen van de tunnelgroep die worden gebruikt. Stel het gedefinieerde groepsbeleid in op deze tunnelgroep.Stel de gedefinieerde adrestoewijzing in die door deze tunnelgroep moet worden gebruikt.Wijzig de authenticatieserver groep als u iets anders wilt gebruiken dan LOKAAL.
5. Defineer de vooraf gedeelde toets onder de IPSec-eigenschappen van de te gebruiken tunnelgroep.
6. Wijzig de PPP eigenschappen van de tunnelgroep die worden gebruikt zodat alleen kettingen, ms-chap-v1 en ms-chap-v2 worden gebruikt.
7. Maak een transformatie set met een specifiek ingekapseld security payload-encryptie (ESP) en een verificatietype.
8. Selecteer IPSec om transportmodus in plaats van tunnelmodus te gebruiken.
9. Defineer een beleid ISAKMP/IKEv1 met behulp van 3DES-encryptie met een SHA1-hashmethode.
10. Maak een dynamische crypto kaart, en breng het naar een crypto kaart.
11. Pas de crypto kaart op een interface toe.
12. Laat ISAKMP op die interface staan.

Configuratiebestandsopdrachten voor ASA-compatibiliteit

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Dit voorbeeld toont de opdrachten van het configuratiebestand die ASA compatibiliteit met een native VPN-client op een besturingssysteem waarborgen.

ASA 8.2.5 of hoger configuratievoorbeeld

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

ASA 8.3.2.12 of hoger configuratievoorbeeld

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
```

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

In deze procedure wordt beschreven hoe u de aansluiting kunt opzetten:

1. Open het menu en kies **Instellingen**.
2. Selecteer **Draadloos en Netwerk** of **draadloze knoppen**. (De beschikbare optie is afhankelijk van uw versie van Android.)
3. Selecteer de VPN-configuratie in de lijst.
4. Voer uw gebruikersnaam en wachtwoord in.
5. Selecteer **Gebruikersnaam onthouden**.
6. Selecteer **Connect**.

In deze procedure wordt beschreven hoe de verbinding wordt verbroken:

1. Open het menu en kies **Instellingen**.
2. Selecteer **Draadloos en Netwerk** of **draadloze knoppen**. (De beschikbare optie is afhankelijk van uw versie van Android.)
3. Selecteer de VPN-configuratie in de lijst.
4. Selecteer **Koppelen los**.

Gebruik deze opdrachten om te bevestigen dat de verbinding goed werkt.

- **Show run crypto isakmp** - Voor ASA versie 8.2.5
- **run crypto ikev1** - Voor ASA versie 8.3.2.12 of hoger
- **toon VPN-sessiondb ra-ikev1-ipsec -** voor ASA versie 8.3.2.12 of hoger
- **toon VPN-sessiondb op afstand -** voor ASA versie 8.2.5

> **Opmerking:** De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

gekende Caveats

- Cisco bug-ID CSCtq21535, "ASA-traceerbaarheid bij verbinding met Android L2TP/IPsec-client"
- Cisco bug-ID CSCtj57256, "L2TP/IPSec-verbinding van Android heeft geen beveiliging tegen de ASA55xx"

- Cisco bug-ID CSCtw58945, "L2TP via IPSec-verbindingen niet bij SAP-autorisatie en MSV2"

Gerelateerde informatie

- Cisco ASA 5500 Series configuratiegids met behulp van de CLI, 8.4 en 8.6: L2TP configureren via IPsec
- Releaseopmerkingen van Cisco ASA 5500 Series, versie 8.4(x)
- Cisco ASA 5500 Series configuratiegids met behulp van de CLI, 8.3: Informatie over NAT
- ASA Pre-8.3 tot 8.3 NAT-configuratievoorbeelden
- Technische ondersteuning en documentatie – Cisco Systems