ASA y ejemplo nativo de la configuración del cliente L2TP-IPSec Android

Contenido

Introducción

El Protocolo de tunelización de la capa 2 (L2TP) por IPSec proporciona la capacidad para desplegar y para administrar una solución de VPN L2TP junto al IPSec VPN y los servicios del Firewall en una plataforma única. El beneficio principal de la configuración del L2TP sobre el IPSec en un escenario del Acceso Remoto es que los usuarios remotos pueden acceder un VPN sobre una red IP pública sin un gateway o una línea dedicada, que habilita el Acceso Remoto de virtualmente cualquier lugar con el Servicio telefónico sencillo antiguo (POTS). Un beneficio adicional es que el único requisito del cliente para el acceso VPN es el uso de Windows con el dial-up networking de Microsoft (DUN). No se requiere ningún software de cliente adicional, tal como el software de VPN Client de Cisco.

Este documento proporciona una configuración de muestra para el cliente nativo de Android del L2TP/IPSec. Toma le a través de todos los comandos required necesarios en un dispositivo de seguridad adaptante de Cisco (ASA), así como las medidas de ser adquirido el dispositivo sí mismo de Android.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El L2TP/IPSec de Android requiere la versión de software 8.2.5 de Cisco ASA o más adelante, versión 8.3.2.12 o posterior, o versión 8.4.1 o posterior.
- El ASA soporta el soporte de la firma del certificado del algoritmo de troceo seguro 2 (SHA2) para Microsoft Windows 7 y los clientes VPN Android-nativos cuando se utiliza el protocolo del L2TP/IPSec.
- Vea la guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6: Configurar el L2TP sobre el IPSec: Requisitos para obtener la licencia para el L2TP sobre el IPSec.

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Esta sección describe la información una necesitaría para configurar las características descritas en este documento.

Configure la conexión del L2TP/IPSec en Android

Este procedimiento describe cómo configurar la conexión del L2TP/IPSec en Android:

1. Abra el menú, y elija las **configuraciones**.
2. Elija los **controles de la Tecnología inalámbrica y de la red** o de la **Tecnología inalámbrica**. La opción disponible depende de su versión de Android.
3. Elija las **configuraciones VPN**.
4. Elija **agregan el VPN**.
5. Elija **agregan el PSK VPN L2TP/IPsec**.
6. Elija el **nombre VPN**, y ingrese un nombre descriptivo.
7. Elija al **servidor VPN determinado**, y ingrese un nombre descriptivo.
8. Elija la **clave previamente compartida determinada del IPSec**.
9. Desmarque el **secreto del permiso L2TP**.
10. [Optional] fije el identificador del IPSec como el nombre de grupo de túnel ASA. Ninguna configuración significa que caerá en DefaultRAGroup en el ASA.
11. Abra el menú, y elija la **salvaguardia**.

Configure la conexión del L2TP/IPSec en el ASA

Éstas son la versión requerida 1 (IKEv1) ([ISAKMP] del intercambio de claves de Internet ASA del protocolo internet security association and key management) las configuraciones de la directiva que permiten a los clientes VPN nativos, integradas con el sistema operativo en un punto final,

para hacer una conexión VPN al ASA cuando el L2TP sobre el Protocolo IPSec se utiliza:

- IKEv1 fase 1 - Cifrado del Estándar de triple cifrado de datos (3DES) con el método del hash SHA1
- Fase IPSec 2 - Cifrado 3DES o del Advanced Encryption Standard (AES) con la publicación de mensaje 5 (MD5) o el método del hash SHA
- Autenticación PPP - Versión 1 (MS-CHAPv1) del protocolo password authentication (PAP), del protocolo microsoft challenge handshake authentication, o MS-CHAPv2 (preferido)
- Clave previamente compartida

  Nota: El ASA soporta solamente las autenticaciones PPP PAP y MS-CHAP (versiones 1 y 2) en la base de datos local. El Protocolo de Autenticación Extensible (EAP) y la GRIETA son realizados por los servidores de la autenticación de representación. Por lo tanto, si un usuario remoto pertenece a un grupo de túnel configurado con el EAP-**proxy de la autenticación** o los **comandos chap de la autenticación** y si el ASA se configura para utilizar la base de datos local, ese usuario no podrá conectar.

  Además, Android no soporta el PAP y, porque el Lightweight Directory Access Protocol (LDAP) no soporta el MS-CHAP, el LDAP no es un mecanismo de autenticación viable. La única solución alternativa es utilizar el RADIUS. Vea el Id. de bug Cisco CSCtw58945, "L2TP sobre el fall de las conexiones del IPSec con la autorización del ldap y el mschapv2," para otros detalles en los problemas con el MS-CHAP y el LDAP.

Este procedimiento describe cómo configurar la conexión del L2TP/IPSec en el ASA:

1. Defina un pool de la dirección local o utilice un DHCP-servidor para el dispositivo de seguridad adaptante para afectar un aparato los IP Addresses a los clientes para la directiva del grupo.
2. Cree una grupo-directiva interna. Defina el Tunnel Protocol para ser l2tp-ipsec.Configure un Domain Name Server (DNS) que se utilizará por los clientes.
3. Cree a un nuevo grupo de túnel o modifique los atributos del DefaultRAGroup existente. (El nuevo grupo de túnel A puede ser utilizado si el identificador del IPSec se fija como nombre del grupo en el teléfono; vea el paso 10 para la Configuración del teléfono.)
4. Defina los atributos generales del grupo de túnel se utilizan que. Asocie la directiva del grupo definido a este grupo de túnel.Asocie a la agrupación de direcciones definida que se utilizará por este grupo de túnel.Modifique al grupo de servidor de autenticación si usted quiere utilizar algo con excepción del LOCAL.
5. Defina la clave previamente compartida bajo atributos del IPSec del grupo de túnel que se utilizará.
6. Modifique los atributos PPP del grupo de túnel se utilizan que para solamente utilizar grieta, ms-chap-v1 y ms-chap-v2.
7. Cree una transformación fijada con un tipo de encripción y un tipo de autenticación específicos del Encapsulating Security Payload (ESP).
8. Dé instrucciones el IPSec para utilizar el modo de transporte bastante que el modo túnel.
9. Defina una directiva ISAKMP/IKEv1 usando el cifrado 3DES con el método del hash SHA1.
10. Cree una correspondencia cifrada dinámica, y asocíela a una correspondencia de criptografía.
11. Aplique la correspondencia de criptografía a una interfaz.
12. Habilite el ISAKMP en esa interfaz.

Comandos del archivo de configuración para la compatibilidad ASA

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Este ejemplo muestra los comandos del archivo de configuración que aseguran la compatibilidad ASA con un cliente VPN nativo en cualquier sistema operativo.

ASA 8.2.5 o ejemplo de configuración posterior

```
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 o ejemplo de configuración posterior

```
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Este procedimiento describe cómo configurar la conexión:

1. Abra el menú, y elija las **configuraciones**.
2. Seleccione los **controles de la Tecnología inalámbrica y de la red** o de la **Tecnología inalámbrica**. (La opción disponible depende de su versión de Android.)
3. Seleccione la configuración VPN de la lista.
4. Ingrese su nombre de usuario y contraseña.
5. Selecto **recuerde el nombre de usuario**.
6. Selecto **conecte**.

Este procedimiento describe cómo desconectar:

1. Abra el menú, y elija las **configuraciones**.
2. Seleccione los **controles de la Tecnología inalámbrica y de la red** o de la **Tecnología inalámbrica**. (La opción disponible depende de su versión de Android.)
3. Seleccione la configuración VPN de la lista.
4. Seleccione la **desconexión**.

Utilice estos comandos para confirmar que su conexión trabaja correctamente.

- **muestre el isakmp crypto del funcionamiento** - Para la Versión de ASA 8.2.5
- **muestre el funcionamiento ikev1 crypto** - Para Versión de ASA 8.3.2.12 o más adelante
- **muestre VPN-sessiondb ra-ikev1-ipsec -** Para Versión de ASA 8.3.2.12 o más adelante
- **muestre el telecontrol de VPN-sessiondb -** Para la Versión de ASA 8.2.5

  Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Advertencias conocidas

- Id. de bug Cisco CSCtq21535, “traceback ASA al conectar con el cliente de Android L2TP/IPsec”
- El Id. de bug Cisco CSCtj57256, conexión "L2TP/IPSec de Android no establece al ASA55xx"

- El Id. de bug Cisco CSCtw58945, "L2TP sobre las conexiones del IPSec falla con la autorización y el mschapv2" del ldap

Información Relacionada

- Guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6: Configurar el L2TP sobre el IPSec
- Release Note para las 5500 Series de Cisco ASA, versión 8.4(x)
- Guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, 8.3: Información sobre el NAT
- ASA Pre-8.3 a 8.3 ejemplos de la configuración del NAT
- Soporte Técnico y Documentación - Cisco Systems