Ejemplo de Configuración de ASA y L2TP-IPSec Android Client Nativo

Contenido

Introducción

El protocolo de túnel de capa 2 (L2TP) sobre IPSec proporciona la capacidad de implementar y administrar una solución VPN L2TP junto con la VPN IPSec y los servicios de firewall en una única plataforma. La principal ventaja de la configuración de L2TP sobre IPSec en un escenario de acceso remoto es que los usuarios remotos pueden acceder a una VPN a través de una red IP pública sin un gateway o una línea dedicada, lo que permite el acceso remoto desde prácticamente cualquier lugar con un servicio telefónico simple (POTS). Una ventaja adicional es que el único requisito del cliente para el acceso VPN es el uso de Windows con Microsoft Dial-Up Networking (DUN). No se requiere ningún software cliente adicional, como el software cliente Cisco VPN.

Este documento proporciona una configuración de ejemplo para el cliente nativo L2TP/IPSec Android. Le lleva a través de todos los comandos necesarios en un Cisco Adaptive Security Appliance (ASA), así como a través de los pasos que debe seguir el dispositivo Android en sí.

Prerequisites

Requirements

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.

- Android L2TP/IPSec requiere el software Cisco ASA versión 8.2.5 o posterior, versión 8.3.2.12 o posterior, o versión 8.4.1 o posterior.
- ASA es compatible con la firma de certificados de algoritmo hash seguro 2 (SHA2) para Microsoft Windows 7 y clientes VPN nativos de Android cuando se utiliza el protocolo L2TP/IPSec.
- Consulte Guía de Configuración de Cisco ASA 5500 Series con CLI, 8.4 y 8.6: Configuración de L2TP sobre IPSec: Requisitos de licencia para L2TP sobre IPSec.

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Esta sección describe la información que se necesita para configurar las funciones descritas en este documento.

Configure la conexión L2TP/IPSec en el Android

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

1. Abra el menú y elija **Settings**.
2. Elija **Wireless and Network** or **Wireless Controls**. La opción disponible depende de la versión de Android.
3. Elija **VPN Settings**.
4. Elija **Add VPN**.
5. Elija **Add L2TP/IPsec PSK VPN**.
6. Elija **VPN Name** e ingrese un nombre descriptivo.
7. Elija **Set VPN Server** e ingrese un nombre descriptivo.
8. Elija **Set IPSec pre-shared key**.
9. Desmarque **Enable L2TP secret**.
10. [Opcional] Establezca el identificador IPSec como el nombre del grupo de túnel ASA. Ningún valor significa que caerá en DefaultRAGroup en el ASA.
11. Abra el menú y elija **Guardar**.

Configure la conexión L2TP/IPSec en ASA

Estos son los ajustes de política de intercambio de claves de Internet ASA versión 1 (IKEv1) (protocolo ISAKMP [Asociación de seguridad de Internet y protocolo de administración de claves]) necesarios que permiten a los clientes VPN nativos, integrados con el sistema operativo en un terminal, realizar una conexión VPN al ASA cuando se utiliza L2TP sobre el protocolo IPSec:

- Fase 1 de IKEv1: triple cifrado de datos (3DES) con método hash SHA1
- Cifrado IPSec fase 2 - 3DES o estándar de cifrado avanzado (AES) con Message Digest 5 (MD5) o método hash SHA
- Autenticación PPP: protocolo de autenticación de contraseña (PAP), protocolo de autenticación por desafío mutuo de Microsoft versión 1 (MS-CHAPv1) o MS-CHAPv2 (preferido)
- Clave previamente compartida

Nota: El ASA sólo admite las autenticaciones PPP PAP y MS-CHAP (versiones 1 y 2) en la base de datos local. Los servidores de autenticación proxy realizan el protocolo de autenticación extensible (EAP) y el CHAP. Por lo tanto, si un usuario remoto pertenece a un grupo de túnel configurado con los comandos **authentication eap-proxy** o **authentication chap** y si el ASA está configurado para utilizar la base de datos local, ese usuario no podrá conectarse.

Además, Android no admite PAP y, como el protocolo ligero de acceso a directorios (LDAP) no admite MS-CHAP, LDAP no es un mecanismo de autenticación viable. La única solución alternativa es utilizar RADIUS. Consulte Cisco Bug ID CSCtw58945, "L2TP sobre conexiones IPSec fallan con la autorización ldap y mschapv2," para obtener más detalles sobre problemas con MS-CHAP y LDAP.

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

1. Defina un conjunto de direcciones local o utilice un servidor dhcp para el dispositivo de seguridad adaptable para asignar direcciones IP a los clientes para la política de grupo.
2. Cree una política de grupo interna. Defina el protocolo de túnel como l2tp-ipsec.Configure un servidor de nombres de dominio (DNS) que utilizarán los clientes.
3. Cree un nuevo grupo de túnel o modifique los atributos del DefaultRAGroup existente. (Se puede utilizar un nuevo grupo de túnel si el identificador IPSec se establece como nombre de grupo en el teléfono; consulte el paso 10 para ver la configuración del teléfono.)
4. Defina los atributos generales del grupo de túnel que se utilizan. Asigne la política de grupo definida a este grupo de túnel.Asigne el conjunto de direcciones definido que utilizará este grupo de túnel.Modifique el grupo de servidor de autenticación si desea utilizar algo que no sea LOCAL.
5. Defina la clave previamente compartida bajo los atributos IPSec del grupo de túnel que se utilizará.
6. Modifique los atributos PPP del grupo de túnel que se utilizan para que sólo se utilicen chap, ms-chap-v1 y ms-chap-v2.
7. Cree un conjunto de transformación con un tipo de cifrado y de autenticación de carga útil de seguridad de encapsulación (ESP) específico.
8. Indique IPSec que utilice el modo de transporte en lugar del modo de túnel.
9. Defina una política ISAKMP/IKEv1 usando cifrado 3DES con el método hash SHA1.
10. Cree un mapa criptográfico dinámico y asígnelo a un mapa criptográfico.
11. Aplique el mapa criptográfico a una interfaz.
12. Habilite ISAKMP en esa interfaz.

Comandos de 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 garantizan la compatibilidad de ASA con un cliente VPN nativo en cualquier sistema operativo.

Ejemplo de Configuración de ASA 8.2.5 o 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
```

Ejemplo de Configuración de ASA 8.3.2.12 o 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 **Settings**.
2. Seleccione **Wireless and Network** or **Wireless Controls**. (La opción disponible depende de la versión de Android.)
3. Seleccione la configuración VPN de la lista.
4. Ingrese su nombre de usuario y contraseña.
5. Seleccione **Recordar nombre de usuario**.
6. Seleccione **Connect**.

Este procedimiento describe cómo desconectar:

1. Abra el menú y elija **Settings**.
2. Seleccione **Wireless and Network** or **Wireless Controls**. (La opción disponible depende de la versión de Android.)
3. Seleccione la configuración VPN de la lista.
4. Seleccione **Disconnect**.

Utilice estos comandos para confirmar que su conexión funciona correctamente.

- **show run crypto isakmp** - Para ASA versión 8.2.5
- **show run crypto ikev1** - Para ASA versión 8.3.2.12 o posterior
- **show vpn-sessiondb ra-ikev1-ipsec -** Para ASA versión 8.3.2.12 o posterior
- **show vpn-sessiondb remote -** Para ASA versión 8.2.5

  Nota: La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Advertencias conocidas

- Id. de error de Cisco CSCtq21535, "Seguimiento de ASA al conectarse con cliente Android L2TP/IPsec"
- Id. de error de Cisco CSCtj57256, "La conexión L2TP/IPSec de Android no se establece en el ASA55xx"

- Id. de error de Cisco CSCtw58945, "L2TP sobre conexiones IPSec fallan con autorización ldap y mschapv2"

Información Relacionada

- Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6: Configuración de L2TP sobre IPsec
- Notas de la versión de Cisco ASA serie 5500, versión 8.4(x)
- Guía de configuración de Cisco ASA serie 5500 con la CLI, 8.3: Información sobre NAT
- Ejemplos de Configuración de NAT de ASA Pre-8.3 a 8.3
- Soporte Técnico y Documentación - Cisco Systems