SSLVPN con el ejemplo de configuración de los Teléfonos IP

Contenido

Introducción

Este documento describe cómo configurar los Teléfonos IP sobre Secure Sockets Layer VPN (SSL VPN), también conocido como WebVPN. Utilizan a dos administradores de las Comunicaciones unificadas de Cisco (CallManageres) y a tres tipos de Certificados con esta solución. Los CallManageres son:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM)
- Cisco Unified Communications Manager Express (CME unificado Cisco)

Los tipos de certificado son:

- Certificados autofirmados
- Los Certificados de tercera persona, por ejemplo confían, Thawte, y GoDaddy
- Certificate Authority (CA) del dispositivo de seguridad del Cisco IOS ®/Adaptive (ASA)

El concepto fundamental a entender es que, una vez la configuración en el gateway de VPN SSL y el CallManager están completados, usted debe unirse a los Teléfonos IP localmente. Esto permite a los teléfonos para unirse al CUCM y para utilizar la información de VPN y los Certificados correctos. Si los teléfonos no se unen a localmente, no pueden encontrar el gateway de VPN SSL y no tienen los Certificados correctos para completar el apretón de manos SSL VPN.

La mayoría de las configuraciones comunes son CUCM/Unified CME con los certificados autofirmados ASA y los certificados autofirmados del Cisco IOS. Por lo tanto, son las más fáciles de configurar.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM) o Cisco Unified Communications Manager Express (CME unificado Cisco)
- SSL VPN (WebVPN)
- Dispositivo de seguridad adaptante de Cisco (ASA)
- Tipos de certificado, tales como uno mismo-firmado, de tercera persona, y autoridades de certificación

Componentes Utilizados

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

- Licencia del premio ASA.
- Licencia del teléfono de AnyConnect VPN.
  - Para la versión 8.0.x ASA, la licencia es AnyConnect para el teléfono de Linksys.
  - Para la versión 8.2.x ASA o más adelante, la licencia es AnyConnect para el teléfono del Cisco VPN.
- Gateway de VPN SSL: ASA 8.0 o más adelante (con un AnyConnect para la licencia del teléfono del Cisco VPN), o Cisco IOS Software Release 12.4T o Posterior.
  - El Cisco IOS Software Release 12.4T o Posterior no se soporta formalmente como se documenta en la guía de configuración VPN SSL.
  - En el Cisco IOS Software Release 15.0(1)M, el gateway de VPN SSL es una característica Seat-contada de la autorización en Cisco 880, Cisco 890, Cisco 1900, el Cisco 2900, y Cisco 3900 Plataformas. Una licencia válida se requiere para una sesión de VPN acertada SSL.
- CallManager: CUCM 8.0.1 o más adelante, o CME unificado 8.5 o más adelante.

La información que contiene este documento se creó a partir de los dispositivos en 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

Notas:

Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

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.

Configuración VPN básica ASA SSL

La configuración VPN básica ASA SSL se describe en estos documentos:

- ASA 8.x: Acceso VPN con el cliente VPN de AnyConnect que usa el ejemplo de configuración del certificado autofirmado
- Configurar las conexiones de cliente VPN de AnyConnect

Una vez que esta configuración es completa, una prueba remota PC debe poder conectar con el gateway de VPN SSL, conecta vía AnyConnect, y hace ping el CUCM. Asegúrese que el ASA tenga un AnyConnect para la licencia del Cisco IP Phone. (Utilice el **comando show ver**.) El puerto 443 TCP y UDP debe estar abierto entre el gateway y el cliente.

Nota: La carga balanceada SSL VPN no se soporta para los teléfonos VPN.

CUCM: ASA SSL VPN con la configuración de los certificados autofirmados

Refiera al teléfono del IP SSL VPN al ASA usando AnyConnect para más información detallada.

El ASA debe tener una licencia para AnyConnect para el teléfono del Cisco VPN. Después de que usted configure el SSL VPN, usted entonces configura su CUCM para el VPN.

1. Utilice este comando para exportar el certificado autofirmado del ASA:

   `ciscoasa(config)# crypto ca export trustpoint name identity-certificate` Este comando visualiza un certificado de identidad PEM-codificado a la terminal.
2. La copia y pega el certificado a un editor de textos, y lo salva como archivo del .pem. Esté seguro de incluir las líneas del CERTIFICADO del COMENZAR y del CERTIFICADO del EXTREMO, o el certificado no importará correctamente. No modifique el formato del certificado porque esto causará los problemas cuando el teléfono intenta autenticar al ASA.
3. Navegue a **Cisco unificó el Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración del sistema operativo > el certificado/la Cadena de certificados de la carga** para cargar el archivo de certificado a la sección de administración de certificados del CUCM.
4. Descargue los Certificados CallManager.pem, CAPF.pem, y Cisco_Manufacturing_CA.pem de la misma área usada para cargar los certificados autofirmados del ASA (véase el paso 1), y sálvelos a su escritorio.
   1. Por ejemplo, para importar el CallManager.pem al ASA, utilice estos comandos:

      ```
      ciscoasa(config)# crypto ca trustpoint certificate-name
      ciscoasa(config-ca-trustpoint)# enrollment terminal
      ```

```
ciscoasa(config)# crypto ca authenticate certificate-name
```

2. Cuando a le indican que copie y pegue el certificado correspondiente para el trustpoint, abra el archivo que usted guardó del CUCM, después de la copia y pegue el certificado codificado en base64. Esté seguro de incluir el CERTIFICADO del COMENZAR y el CERTIFICADO del EXTREMO alinea (con los guiones).
3. **El extremo del** tipo, entonces presiona la **vuelta**.
4. Cuando se le pregunte para validar el certificado, teclee **sí**, entonces Presione ENTER.
5. Relance los pasos 1 a 4 para los otros dos Certificados (CAPF.pem, Cisco_Manufacturing_CA.pem) del CUCM.

5. Configure el CUCM para las configuraciones VPN correctas, según lo descrito en CUCM IPphone VPN config.pdf.

   Nota: El gateway de VPN configurado en el CUCM debe hacer juego el URL que se configura en el gateway de VPN. Si el gateway y el URL no hacen juego, el teléfono no puede resolver el direccionamiento, y usted no verá ninguna debugs en el gateway de VPN.

- En el CUCM: El gateway de VPN URL es https://192.168.1.1/VPNPhone
- En el ASA, utilice estos comandos:

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- Usted puede utilizar estos comandos en el Administrador de dispositivos de seguridad adaptante (ASDM) o bajo perfil de la conexión.

CUCM: ASA SSL VPN con la configuración de tercera persona de los Certificados

Esta configuración es muy similar a la configuración descrita en CUCM: El ASA SSLVPN con la sección de configuración de los certificados autofirmados, salvo que usted están utilizando los Certificados de tercera persona. Configure SSL VPN en el ASA con los Certificados de tercera persona como descrito en ASA 8.x instale manualmente los Certificados del vendedor de las de otras compañías para el uso con el ejemplo de configuración del WebVPN.

Nota: Usted debe copiar la Cadena de certificados llena del ASA al CUCM e incluir todo el intermedio y certificados raíz. Si el CUCM no incluye el encadenamiento lleno, los teléfonos no tienen los Certificados necesarios a autenticar y fallarán el apretón de manos SSL VPN.

Configuración VPN básica IOS SSL

Nota: Los Teléfonos IP se señalan como no soportado en IOS SSL VPN; las configuraciones están en mejor esfuerzo solamente.

La configuración VPN básica del Cisco IOS SSL se describe en estos documentos:

- **Ejemplo de Configuración de SSL VPN Client (SVC) en IOS con SDM**
- El cliente VPN de AnyConnect en el router IOS con la zona IOS basó el ejemplo de la

configuración de escudo de protección de la directiva

Una vez que esta configuración es completa, una prueba remota PC debe poder conectar con el gateway de VPN SSL, conecta vía AnyConnect, y hace ping el CUCM. En el Cisco IOS 15.0 y posterior, usted debe tener una licencia válida SSL VPN de completar esta tarea. El puerto 443 TCP y UDP debe estar abierto entre el gateway y el cliente.

CUCM: IOS SSL VPN con la configuración de los certificados autofirmados

Esta configuración es similar a la configuración descrita en CUCM: ASA SSLVPN con la configuración de tercera persona de los Certificados y CUCM: ASA SSLVPN con las secciones de configuración de los certificados autofirmados. Las diferencias son:

1. Utilice este comando para exportar el certificado autofirmado del router:

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. Utilice estos comandos para importar los Certificados CUCM:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

La configuración del contexto del WebVPN debe mostrar este texto:

```
gateway webvpn_gateway domain VPNPhone
```

Configure el CUCM según lo descrito en CUCM: ASA SSLVPN con la sección de configuración de los certificados autofirmados.

CUCM: IOS SSL VPN con la configuración de tercera persona de los Certificados

Esta configuración es similar a la configuración descrita en CUCM: ASA SSLVPN con la sección de configuración de los certificados autofirmados. Configure su WebVPN con un certificado de tercera persona.

> Nota: Usted debe copiar la Cadena de certificados llena del WebVPN al CUCM e incluir todo el intermedio y certificados raíz. Si el CUCM no incluye el encadenamiento lleno, los teléfonos no tienen los Certificados necesarios a autenticar y fallarán el apretón de manos SSL VPN.

CME unificado: ASA/Router SSL VPN con los certificados autofirmados/la configuración de tercera persona de los Certificados

La configuración para el CME unificado es similar a las configuraciones del CUCM; por ejemplo, las configuraciones del punto final del WebVPN son lo mismo. La única diferencia significativa es las configuraciones del agente unificado de la llamada CME. Configure el grupo VPN y la política del VPN para el CME unificado según lo descrito en configurar al cliente VPN SSL para los Teléfonos IP del SCCP.

> Nota: El CME unificado soporta solamente el Skinny Call Control Protocol (SCCP) y no

soporta el Session Initiation Protocol (SIP) para los teléfonos VPN.

Nota: No hay necesidad de exportar los Certificados del CME unificado al ASA o al router. Usted necesita solamente exportar los Certificados del ASA o el gateway del WebVPN del router al CME unificado.

Para exportar los Certificados del gateway del WebVPN, refiera a la sección ASA/router. Si usted está utilizando un certificado de tercera persona, usted debe incluir la Cadena de certificados llena. Para importar los Certificados al CME unificado, utilice el mismo método según lo utilizado a los Certificados de importación en un router:

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

Teléfonos IP UC 520 con la configuración VPN SSL

El teléfono del IP modelo UC 520 de las 500 Series de las Comunicaciones unificadas de Cisco es muy diferente de las configuraciones CUCM y CME.

- Puesto que el teléfono del IP UC 520 es el CallManager y el gateway del WebVPN, no hay necesidad de configurar los Certificados entre los dos.
- Configure el WebVPN en un router como usted normalmente con los certificados autofirmados o los Certificados de tercera persona.
- El teléfono del IP UC 520 tiene construido en el cliente del WebVPN, y usted puede configurarlo apenas pues usted un PC normal conectaría con el WebVPN. Ingrese el gateway, entonces la Combinación de nombre de usuario/contraseña.
- El teléfono del IP UC 520 es compatible con los teléfonos del teléfono del IP SPA 525G de la Pequeña empresa de Cisco.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.