Ejemplo de Configuración de SSLVPN con Teléfonos IP

Contenido

Introducción

Este documento describe cómo configurar teléfonos IP sobre una VPN de capa de sockets seguros (SSL VPN), también conocida como WebVPN. Con esta solución se utilizan dos Cisco Unified Communications Manager (CallManagers) y tres tipos de certificados. Los CallManagers son:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

Los tipos de certificado son:

- Certificados autofirmados
- Certificados de terceros, como Entrust, Thawte y GoDaddy
- Autoridad certificadora (CA) de Cisco IOS®/Adaptive Security Appliance (ASA)

El concepto clave que se debe entender es que, una vez que se haya completado la configuración en el gateway SSL VPN y CallManager, debe unirse a los teléfonos IP localmente. Esto permite que los teléfonos se unan a CUCM y utilicen la información de VPN y los certificados correctos. Si los teléfonos no están unidos localmente, no pueden encontrar el gateway SSL VPN y no tienen los certificados correctos para completar el intercambio de señales SSL VPN.

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

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM) o Cisco Unified Communications Manager Express (Cisco Unified CME)
- VPN SSL (WebVPN)
- Dispositivo de seguridad adaptable (ASA) de Cisco
- Tipos de certificados, como autofirmados, terceros y autoridades de certificados

Componentes Utilizados

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

- Licencia de ASA Premium.
- Licencia de teléfono VPN de AnyConnect.
  - Para ASA versión 8.0.x, la licencia es AnyConnect para Linksys Phone.
  - Para ASA versión 8.2.x o posterior, la licencia es AnyConnect para Cisco VPN Phone.
- Gateway VPN SSL: ASA 8.0 o posterior (con una licencia de AnyConnect para Cisco VPN Phone), o Cisco IOS Software Release 12.4T o posterior.
  - La versión 12.4T o posterior del software del IOS de Cisco no se soporta formalmente como se documenta en la Guía de Configuración de SSL VPN.
  - En Cisco IOS Software Release 15.0(1)M, el gateway SSL VPN es una función de licencias con recuento de asientos en las plataformas Cisco 880, Cisco 890, Cisco 1900, Cisco 2900 y Cisco 3900. Se requiere una licencia válida para una sesión SSL VPN exitosa.
- CallManager: CUCM 8.0.1 o posterior, o Unified CME 8.5 o posterior.

The information in this document was created from the devices in a specific lab environment. 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

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

Configuración básica de ASA SSL VPN

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

- ASA 8.x: Ejemplo de Configuración de Acceso VPN con AnyConnect VPN Client Usando Certificado Autofirmado
- Configuración de las Conexiones de AnyConnect VPN Client

Una vez finalizada esta configuración, un PC de prueba remoto debe poder conectarse al gateway SSL VPN, conectarse a través de AnyConnect y hacer ping en el CUCM. Asegúrese de que ASA tenga una licencia de AnyConnect para Cisco IP Phone. (Utilice el comando **show ver**.) Tanto el puerto TCP como el puerto UDP 443 deben estar abiertos entre el gateway y el cliente.

Nota: VPN SSL con equilibrio de carga no es compatible con los teléfonos VPN.

CUCM: Configuración de ASA SSL VPN con certificados autofirmados

Refiérase a IP Phone SSL VPN a ASA usando AnyConnect para obtener información más detallada.

El ASA debe tener una licencia para AnyConnect para Cisco VPN Phone. Después de configurar SSL VPN, configure su CUCM para la VPN.

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

   ```
   ciscoasa(config)# crypto ca export trustpoint name identity-certificate
   ```

   Este comando muestra un certificado de identidad codificado por pem al terminal.
2. Copie y pegue el certificado en un editor de texto y guárdelo como archivo .pem. Asegúrese de incluir las líneas BEGIN CERTIFICATE y END CERTIFICATE, o el certificado no se importará correctamente. No modifique el formato del certificado porque esto causará problemas cuando el teléfono intente autenticarse en el ASA.
3. Navegue hasta **Administración de Cisco Unified Operating System > Seguridad > Administración de certificados > Cargar certificado/Cadena de certificados** para cargar el archivo de certificado en la sección GESTIÓN DE CERTIFICADOS de CUCM.
4. Descargue los certificados CallManager.pem, CAPF.pem y Cisco_Manufacturing_CA.pem de la misma área utilizada para cargar los certificados autofirmados del ASA (consulte el Paso 1) y guárdelos en su escritorio.
   1. Por ejemplo, para importar 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 se le pida que copie y pegue el certificado correspondiente para el punto de

confianza, abra el archivo que guardó de CUCM y, a continuación, copie y pegue el certificado codificado en Base64. Asegúrese de incluir las líneas BEGIN CERTIFICATE y END CERTIFICATE (con guiones).
3. Escriba **end** y, a continuación, presione **Return**.
4. Cuando se le pida que acepte el certificado, escriba **yes** y, a continuación, presione **Enter**.
5. Repita los pasos del 1 al 4 para los otros dos certificados (CAPF.pem, Cisco_Manufacturing_CA.pem) desde CUCM.

5. Configure el CUCM para las configuraciones de VPN correctas, como se describe en CUCM IPphone VPN config.pdf.

Nota: El gateway VPN configurado en CUCM debe coincidir con la URL configurada en el gateway VPN. Si el gateway y la URL no coinciden, el teléfono no puede resolver la dirección y no verá ninguna depuración en el gateway VPN.

- En CUCM: La URL del gateway VPN 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
```

- Puede utilizar estos comandos en el Administrador adaptable de dispositivos de seguridad (ASDM) o en el perfil de conexión.

CUCM: Configuración de ASA SSL VPN con certificados de terceros

Esta configuración es muy similar a la descrita en CUCM: Sección Configuración de ASA SSLVPN con Certificados Autofirmados, excepto que está utilizando certificados de terceros. Configure SSL VPN en el ASA con certificados de terceros como se describe en ASA 8.x Instalación Manual de Certificados de Proveedores de Terceros para su Uso con el Ejemplo de Configuración de WebVPN.

Nota: Debe copiar la cadena completa de certificados del ASA en CUCM e incluir todos los certificados intermedios y raíz. Si CUCM no incluye la cadena completa, los teléfonos no tienen los certificados necesarios para la autenticación y fallarán el intercambio de señales VPN SSL.

Configuración básica de VPN SSL de IOS

Nota: Los teléfonos IP se designan como no soportados en IOS SSL VPN; las configuraciones se realizan con el mejor esfuerzo.

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

- Ejemplo de Configuración de SSL VPN Client (SVC) en IOS con SDM
- Ejemplo de Configuración de AnyConnect VPN Client on IOS Router with IOS Zone Based

Policy Firewall

Una vez finalizada esta configuración, un PC de prueba remoto debe poder conectarse al gateway SSL VPN, conectarse a través de AnyConnect y hacer ping en el CUCM. En Cisco IOS 15.0 y posteriores, debe tener una licencia SSL VPN válida para completar esta tarea. Tanto el puerto TCP como el puerto UDP 443 deben estar abiertos entre el gateway y el cliente.

CUCM: Configuración de VPN SSL de IOS con certificados autofirmados

Esta configuración es similar a la descrita en CUCM: ASA SSLVPN con configuración de certificados de terceros y CUCM: Secciones de Configuración de ASA SSLVPN con Certificados Autofirmados. Las diferencias son:

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

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

2. Utilice estos comandos para importar los certificados de CUCM:

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

La configuración de contexto de WebVPN debe mostrar este texto:

```
gateway webvpn_gateway domain VPNPhone
```

Configure el CUCM como se describe en CUCM: sección Configuración de SSLVPN ASA con Certificados Autofirmados.

CUCM: Configuración de VPN SSL de IOS con certificados de terceros

Esta configuración es similar a la descrita en CUCM: sección Configuración de SSLVPN ASA con Certificados Autofirmados. Configure su WebVPN con un certificado de terceros.

> **Nota:** Debe copiar la cadena completa de certificados WebVPN en CUCM e incluir todos los certificados intermedios y raíz. Si CUCM no incluye la cadena completa, los teléfonos no tienen los certificados necesarios para la autenticación y fallarán el intercambio de señales VPN SSL.

Unified CME: VPN SSL ASA/Router con Certificados Autofirmados/Configuración de Certificados de Terceros

La configuración de Unified CME es similar a la de CUCM; por ejemplo, las configuraciones de extremo de WebVPN son las mismas. La única diferencia significativa son las configuraciones del agente de llamadas de Unified CME. Configure el grupo VPN y la política VPN para Unified CME como se describe en Configuración de SSL VPN Client para teléfonos IP SCCP.

Nota: Unified CME admite solo el protocolo Skinny Call Control Protocol (SCCP) y no el protocolo de inicio de sesión (SIP) para teléfonos VPN.

Nota: No es necesario exportar los certificados de Unified CME al ASA o al router. Solo es necesario exportar los certificados desde el gateway WebVPN de ASA o router a Unified CME.

Para exportar los certificados desde el gateway WebVPN, consulte la sección ASA/router. Si utiliza un certificado de terceros, debe incluir la cadena completa de certificados. Para importar los certificados a Unified CME, utilice el mismo método utilizado para importar certificados a un router:

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

Configuración de teléfonos IP UC 520 con SSL VPN

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

- Dado que el teléfono IP UC 520 es el CallManager y el gateway WebVPN, no es necesario configurar los certificados entre ambos.
- Configure el WebVPN en un router como lo haría normalmente con certificados autofirmados o certificados de terceros.
- El teléfono IP UC 520 tiene un cliente WebVPN integrado y puede configurarlo del mismo modo que si fuera un PC normal para conectarse a WebVPN. Introduzca la puerta de enlace y, a continuación, la combinación nombre de usuario/contraseña.
- El teléfono IP UC 520 es compatible con los teléfonos Cisco Small Business IP Phone SPA 525G.

Verificación

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

Troubleshoot

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