Configuración de Umbrella VA para recibir asignaciones de IP de usuario

Contenido

Introducción

Este documento describe cómo configurar Cisco Umbrella Virtual Appliance (VA) para recibir asignaciones de IP de usuario a través de un canal seguro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- La creación de claves privadas, la creación de certificados, la firma de certificados y la administración están fuera del alcance de los componentes de Umbrella. Esto debe hacerse fuera de estos componentes.
- Debe crear un certificado con un nombre común único por dispositivo virtual.
- También debe agregar un registro A en el servidor DNS interno, señalando este nombre común a la dirección IP del dispositivo virtual.
- Si es necesario cambiar la dirección IP de un dispositivo virtual, este registro A también debe cambiarse en consecuencia.

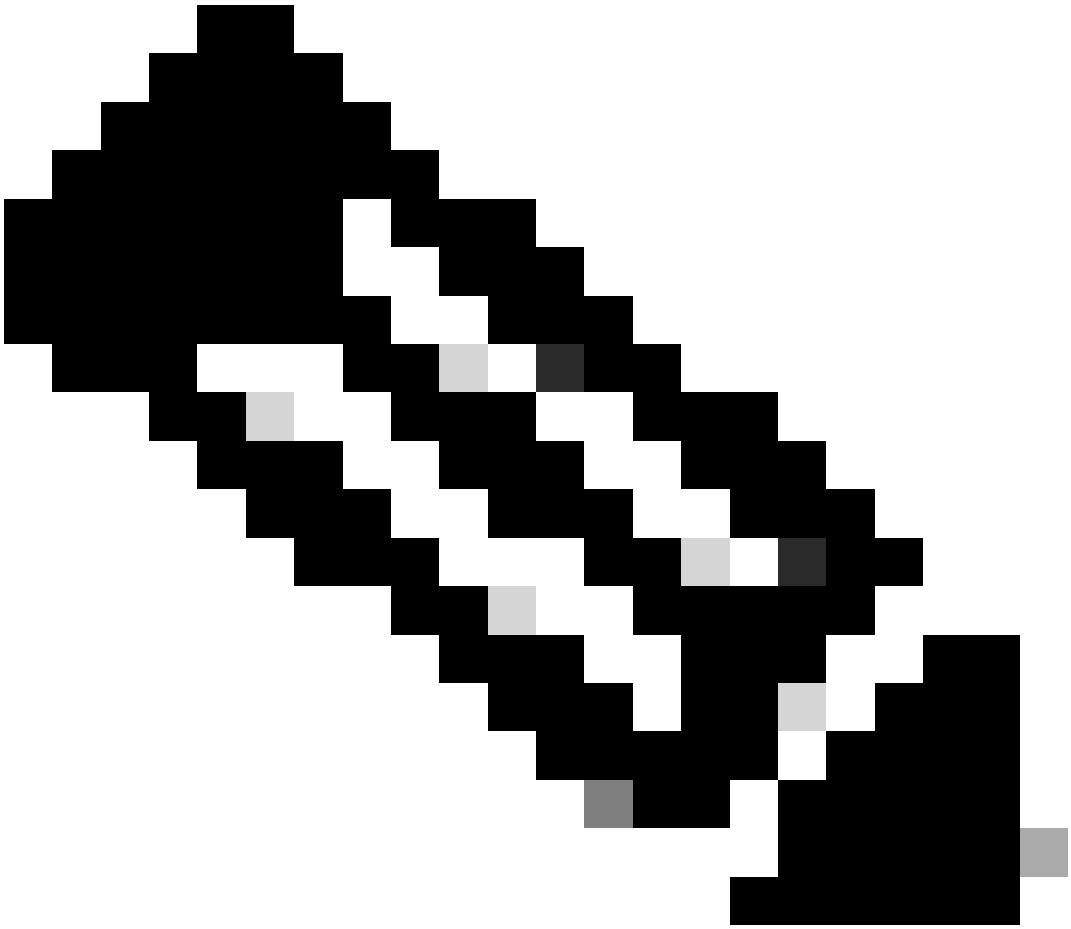
- El FQDN correspondiente al certificado debe configurarse como dominio local en el panel de Umbrella para que el VA lo reconozca como dominio local.
- La clave privada y los certificados deben crearse en los formatos .key y .cer respectivamente.
- Puede utilizar certificados autofirmados o certificados firmados por CA para este fin.

Componentes Utilizados

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

- Dispositivo virtual que ejecuta la versión 2.7 o posterior
- Umbrella AD Connector debe ejecutar la versión 1.5 o posterior
- Los clientes de Umbrella Chromebook deben ejecutar la versión 1.3.3 o superior

---



Nota: Si su VA o conector de AD están ejecutando versiones anteriores, puede [abrir un]

---

ticket de soporte con Umbrella para que se actualicen a las respectivas versiones compatibles.

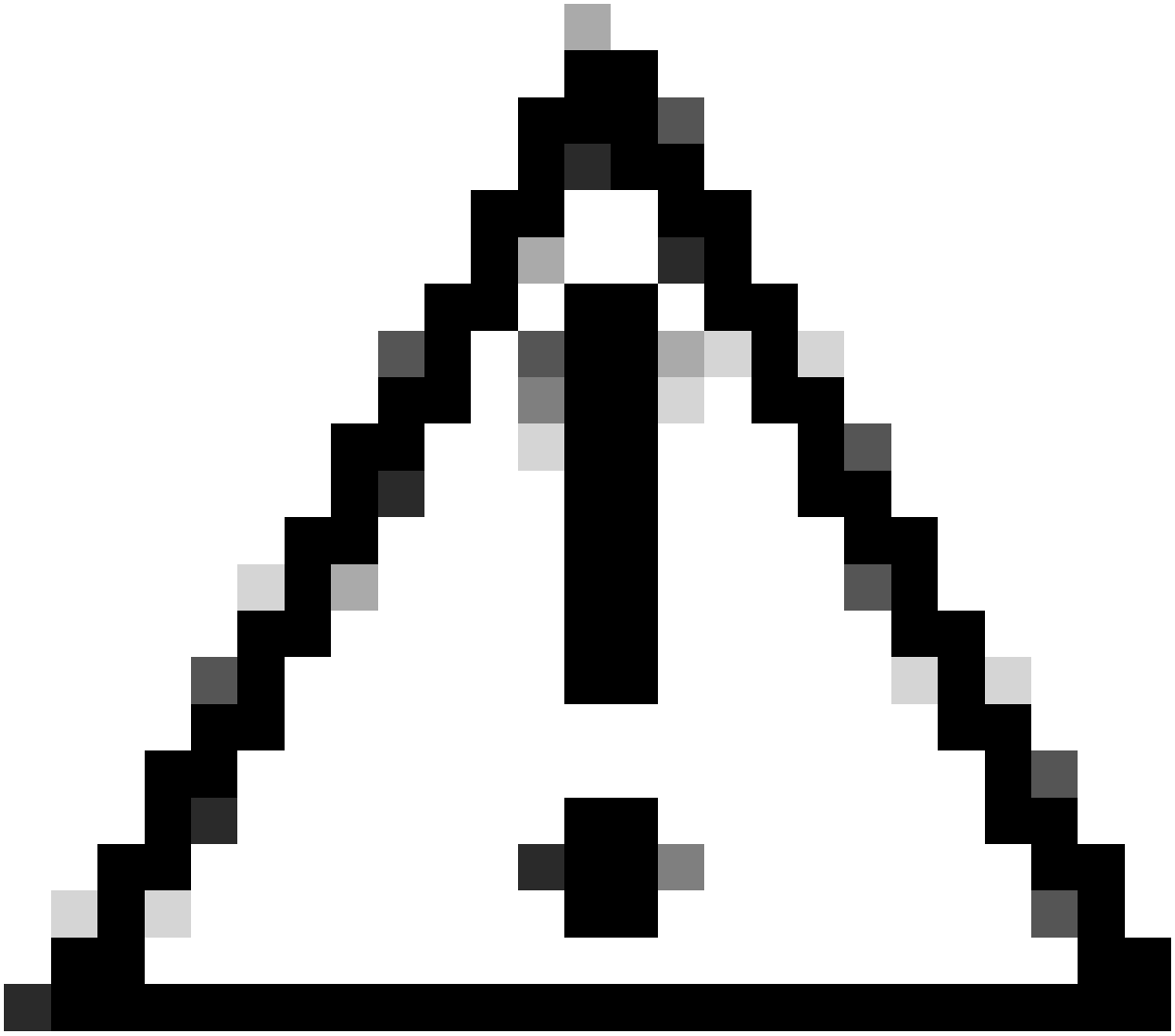
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Los dispositivos virtuales Umbrella, que ejecutan la versión 2.6 o anterior, admiten la recepción de asignaciones de IP de usuario desde el conector de Active Directory (AD) de Umbrella y los clientes de Chromebook de Umbrella sólo de forma no cifrada en el puerto 443. Como resultado, un requisito obligatorio para la implementación ha sido que el conector de AD y los clientes de VA o Chromebook y VA se comuniquen únicamente a través de una red de confianza.

A partir de la versión 2.7, los dispositivos virtuales de Umbrella ahora pueden recibir asignaciones de IP de usuario de AD del conector de AD sobre HTTPS, y de manera similar asignaciones de IP de usuario de GSuite de cada cliente de Umbrella Chromebook sobre HTTPS.

En este artículo se detallan los pasos de configuración de cada componente para habilitar la comunicación HTTPS. De forma predeterminada, la comunicación HTTPS está deshabilitada y el conector AD y los clientes de Chromebook se comunican con el dispositivo virtual a través de HTTP únicamente.



Precaución: Si activa esta función, puede aumentar la utilización de la CPU y la memoria en el VA y el conector Umbrella AD, y puede reducir el rendimiento de DNS del VA. Como resultado, se recomienda activar esta función solo si así lo exigen los requisitos de conformidad de su organización.

Dispositivo virtual

Agregar clave privada y certificado al dispositivo virtual

Para agregar la clave privada y el certificado al dispositivo virtual:
1. Abra el archivo de clave privada a través del editor de texto.

2. Seleccione todo, copie y pegue las comillas dobles de este comando:

```
config va ssl key "paste the contents of the .key file here"
```

Agregar certificado al dispositivo virtual

Para agregar el certificado al dispositivo virtual:
1. Abra el archivo del certificado a través del editor de texto.

2. Seleccione todo, copie y pegue las comillas dobles del siguiente comando:

```
config va ssl cert "paste the contents of the .crt file here"
```

Activar HTTPS en el dispositivo virtual

Habilite HTTPS en el dispositivo virtual mediante este comando:

```
config va ssl enable
```

Verificar habilitación de HTTPS

Verifique que HTTPS esté habilitado mediante el comando:

```
config va show
```

La salida de este comando puede incluir el estado HTTPS así como los detalles del certificado SSL.

Ejemplo de salida:

```
HTTPS status : enabled
SSL Certificate Start Time : 2024-04-16 16:11:08
SSL Certificate Expiry Time : 2025-04-16 16:11:08
Issuer : C = US, ST = MASSACHUSETTS, L = BOSTON, O = CISCOSUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

El dispositivo virtual puede tardar hasta 20 minutos en comenzar a recibir eventos a través de HTTPS. Puede verificar después de aproximadamente 20 minutos usando el comando `config va status`. El estado del conector de AD se muestra en amarillo (estancado) en el período intermedio y pasa al estado verde una vez que el VA comienza a recibir eventos a través de HTTPS.

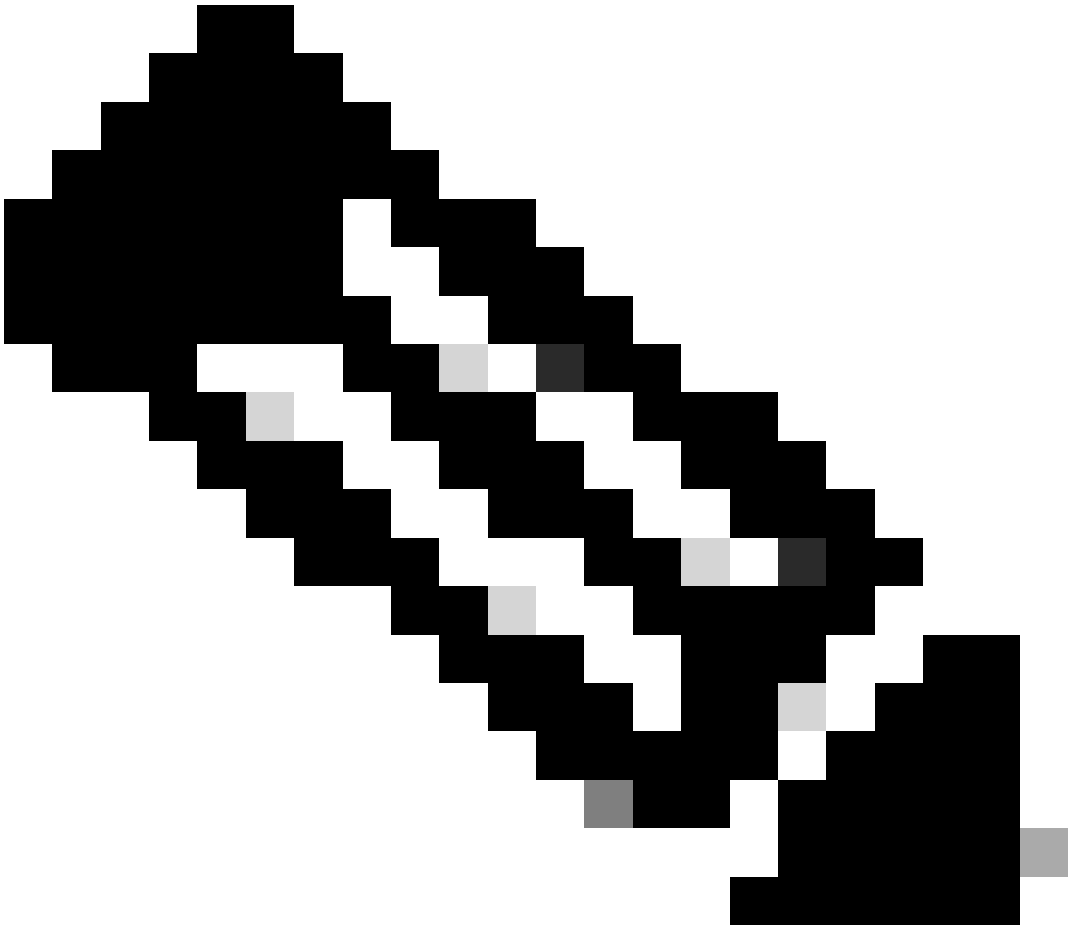
Si desea inhabilitar HTTPS y volver a HTTP, utilice el comando `config vía ssl disable`.

Si desea volver a habilitar HTTPS, debe agregar la clave privada y el certificado nuevamente y luego utilizar el comando `config va enable`.

Directorio activo

Si utiliza un certificado firmado por CA para cada VA, asegúrese de que el certificado raíz y los certificados de CA emisores para cada certificado de VA estén instalados en cada sistema que ejecute el conector de AD en el mismo sitio que el VA.

Si utiliza un certificado autofirmado para cada VA, asegúrese de que cada certificado de VA está instalado en cada sistema que ejecuta el conector de AD en el mismo sitio de Umbrella que el VA.



Nota: Solo los certificados para las AV en el mismo sitio de Umbrella que el conector AD deben instalarse en el conector AD.

El VA puede tardar hasta 20 minutos en sincronizar el estado HTTPS con Umbrella, que luego se sincroniza con el conector AD. Como resultado, el conector puede tardar hasta 20 minutos en comenzar a enviar datos al dispositivo virtual a través de HTTPS. El VA descarta cualquier asignación de IP de usuario enviada durante este período. Por lo tanto, se recomienda realizar el cambio de configuración en el VA solo durante las horas de inactividad cuando no se esperan inicios de sesión de usuario.

Cliente Android Umbrella

Si está utilizando certificados firmados por CA para los VA, asegúrese de que el certificado raíz y los certificados de CA emisores para cada certificado de VA se insertan e instalan en cada dispositivo Android.

Si utiliza certificados autofirmados para dispositivos virtuales, asegúrese de que cada certificado de dispositivo virtual se envía e instala en cada dispositivo Android.

Una vez que el certificado está disponible, el cliente Umbrella Android puede comenzar a usar este certificado para configurar un canal HTTPS con el VA.

Cliente de Chromebook de Umbrella

Si utiliza certificados firmados por CA para los VA, asegúrese de que el certificado raíz y los certificados de CA emisores de cada certificado de VA se insertan e instalan en cada Chromebook.

Si utiliza certificados autofirmados para los VA, asegúrese de que cada certificado de VA se envía e instala en cada Chromebook.

Una vez que el certificado está disponible, el cliente Umbrella Chromebook puede comenzar a usar este certificado para configurar un canal HTTPS con el VA.

Para obtener más información, consulte el artículo Umbrella Chromebook Client: Envío de asignaciones de IP de usuario a través de un canal seguro al dispositivo virtual Umbrella.

Secuencia de configuración

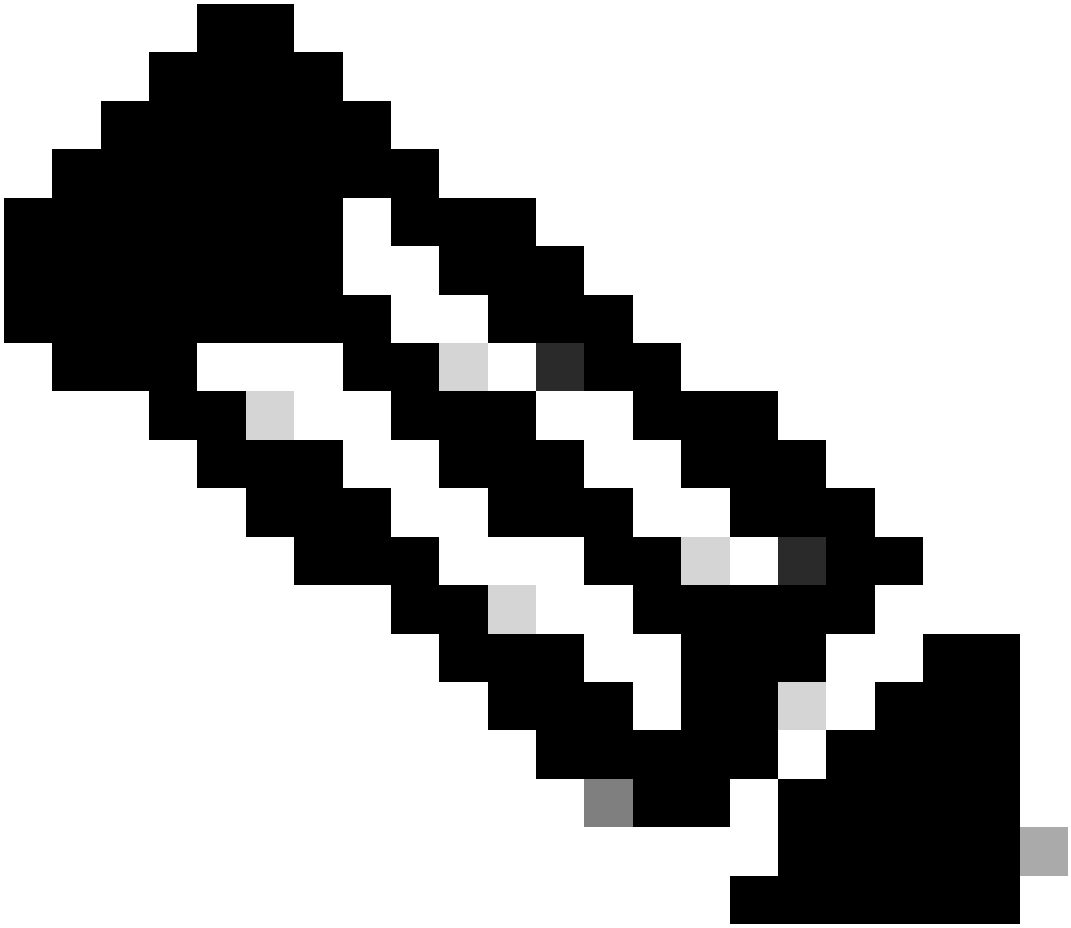
Una vez que HTTPS está habilitado en el dispositivo virtual, el dispositivo virtual no acepta asignaciones de IP de usuario enviadas en texto sin formato a través de HTTP. Como resultado, se descartan todos los inicios de sesión de usuario enviados a través de HTTP y no está disponible la atribución de usuario para solicitudes DNS de estos usuarios. Por lo tanto, se recomienda configurar estos componentes en este orden:

1. Cree el certificado y la clave privada para cada VA basándose en un certificado firmado o autofirmado por la CA.

2. Añada el certificado y la clave privada a cada AV, respectivamente.

3. Asegúrese de que el certificado raíz y los certificados primarios intermedios para cada certificado de VA (o certificado autofirmado de VA) estén instalados en cada sistema que ejecute el conector de AD en el mismo sitio que el VA, y en cada Chromebook.

4. Durante las horas de inactividad, active HTTPS en el dispositivo virtual.



Nota: El certificado en el VA debe ser reemplazado antes de que caduque, y los certificados raíz y primarios intermedios deben ser instalados en el conector AD y los clientes de Umbrella Chromebook. Si esto no se hace, los clientes de AD Connector y Umbrella Chromebook no pueden comunicarse con el VA.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).