Configurar Umbrella VA para Receber Mapeamentos User-IP

Contents

Introdução

Este documento descreve como configurar o Cisco Umbrella Virtual Appliance (VA) para receber mapeamentos de IP de usuário em um canal seguro.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- A criação de chave privada, a criação de certificado, a assinatura de certificado e o gerenciamento estão fora do escopo dos componentes do Umbrella. Isso deve ser feito fora desses componentes.
- Você deve criar um certificado com um nome comum exclusivo por dispositivo virtual.
- Você também deve adicionar um registro A em seu servidor DNS interno, apontando esse nome comum para o endereço IP do dispositivo virtual.
- Se o endereço IP de um dispositivo virtual precisar ser alterado, esse registro A também deverá ser alterado de forma correspondente.

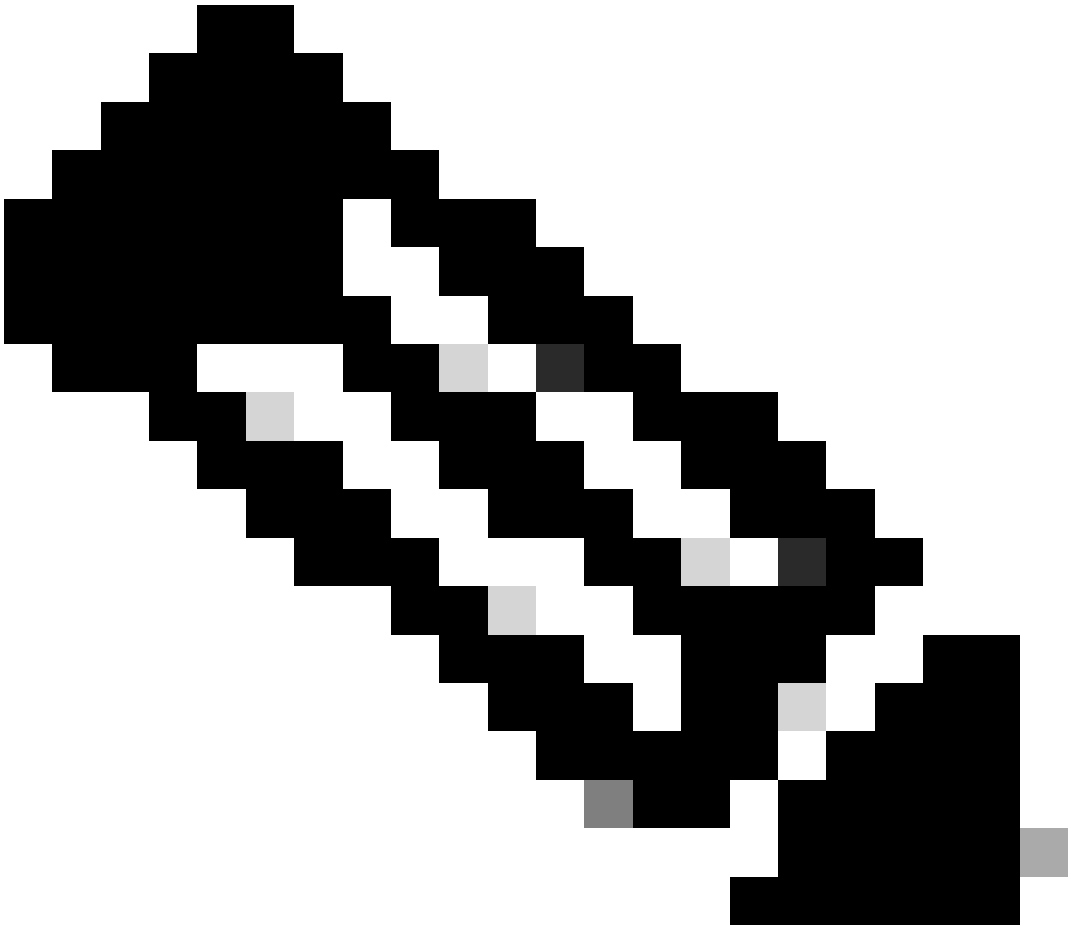
- O FQDN correspondente ao certificado deve ser configurado como um domínio local no painel do Umbrella para que o VA o reconheça como um domínio local.
- A chave privada e os certificados precisam ser criados nos formatos .key e .cer, respectivamente.
- Você pode usar certificados autoassinados ou certificados CA-assinados para esta finalidade.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Virtual Appliance executando a versão 2.7 ou posterior
- O Umbrella AD Connector deve estar executando a versão 1.5 ou posterior
- Os Umbrella Chromebook Clients devem estar executando a versão 1.3.3 ou posterior

---



Note: Se o conector VA ou AD estiver executando versões anteriores, você poderá [abrir]

---

um tíquete de suporte com o Umbrella para atualizá-los para as respectivas versões com suporte.

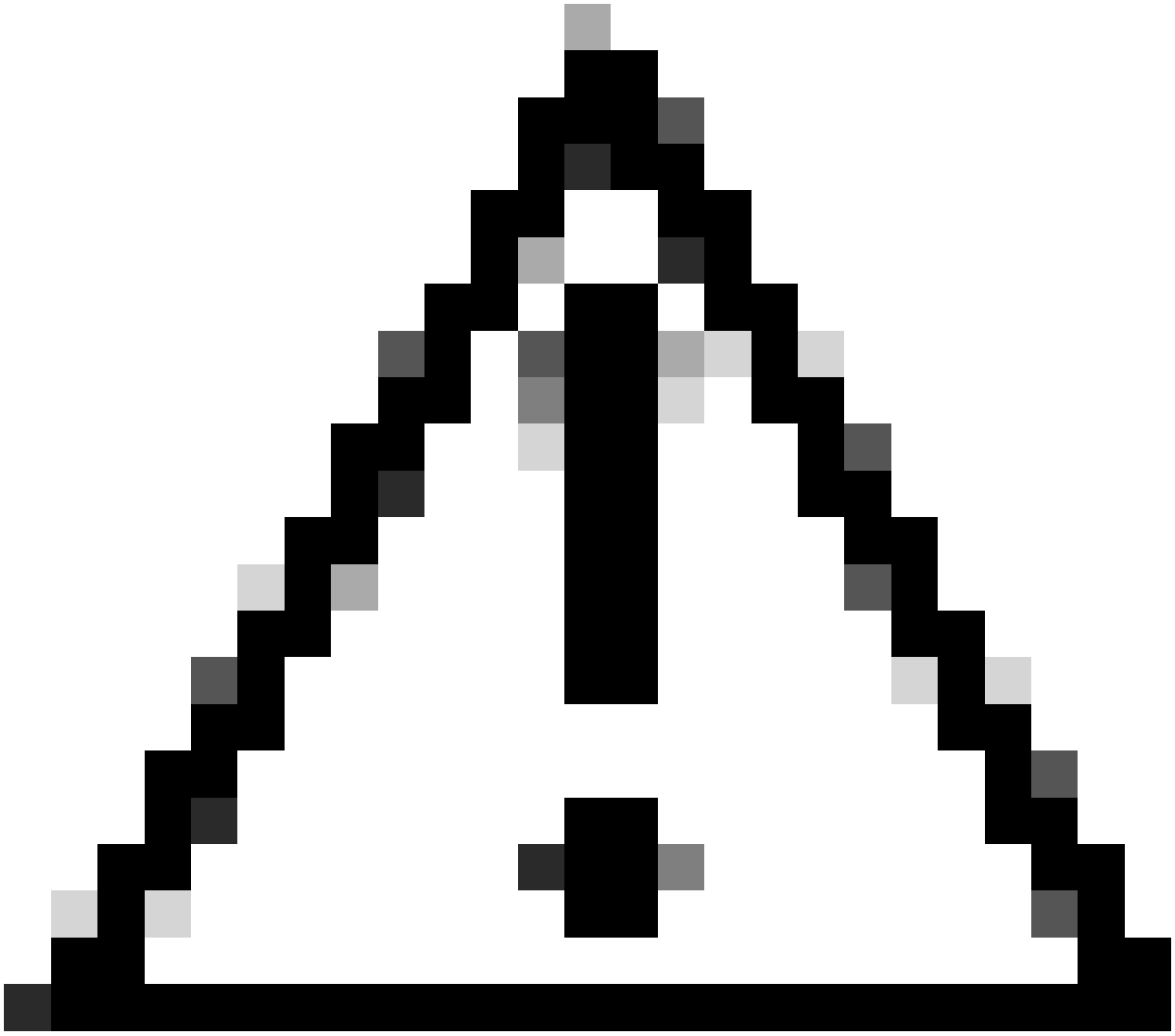
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Os Umbrella Virtual Appliances, executando a versão 2.6 ou anterior, oferecem suporte ao recebimento de mapeamentos de IP de usuário do Umbrella Ative Diretory (AD) Connector e do Umbrella Chromebook Clients somente de forma não criptografada na porta 443. Como resultado, um pré-requisito obrigatório para implantação foi que o AD Connector e o VA ou o Chromebook Clients e o VA se comuniquem somente por uma rede confiável.

A partir da versão 2.7, os Umbrella Virtual Appliances agora podem receber mapeamentos de IP de usuário do AD do AD Connector sobre HTTPS e, da mesma forma, mapeamentos de IP de usuário do GSuite de cada Umbrella Chromebook Client sobre HTTPS.

Este artigo detalha as etapas de configuração em cada componente para ativar a comunicação HTTPS. Por padrão, a comunicação HTTPS é desabilitada e o Conector do AD e os Clientes Chromebook se comunicam com o VA somente por HTTP.



Caution: Ativar esse recurso pode aumentar a utilização da CPU e da memória no VA e no Umbrella AD Connector e pode resultar em uma taxa de transferência de DNS reduzida para o VA. Como resultado, é recomendável ativar esse recurso somente se exigido por qualquer requisito de conformidade para sua organização.

Dispositivo virtual

Adicionar chave privada e certificado ao VA

Para adicionar a chave privada e o certificado ao VA:
1. Abra o arquivo de chave privada através do editor de texto.

2. Selecione tudo, copie e cole entre aspas duplas para este comando:

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

Adicionar certificado ao VA

Para adicionar o certificado ao VA:
1. Abra o arquivo do certificado através do editor de texto.

2. Selecione tudo, copie e cole entre aspas duplas para o comando abaixo:

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

Habilitar HTTPS no VA

Ative o HTTPS no VA usando este comando:

```
config va ssl enable
```

Verificar a habilitação de HTTPS

Verifique se o HTTPS está habilitado usando o comando:

```
config va show
```

A saída desse comando pode incluir o status HTTPS e os detalhes do certificado SSL.

Saída de exemplo:

```
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
```

Pode levar até 20 minutos para que o VA comece a receber eventos por HTTPS. Você pode verificar após cerca de 20 minutos usando o comando `config va status`. O status do Conector AD está no estado amarelo (paralisado) no período intermediário e passa para o estado verde quando o VA começa a receber eventos por HTTPS.

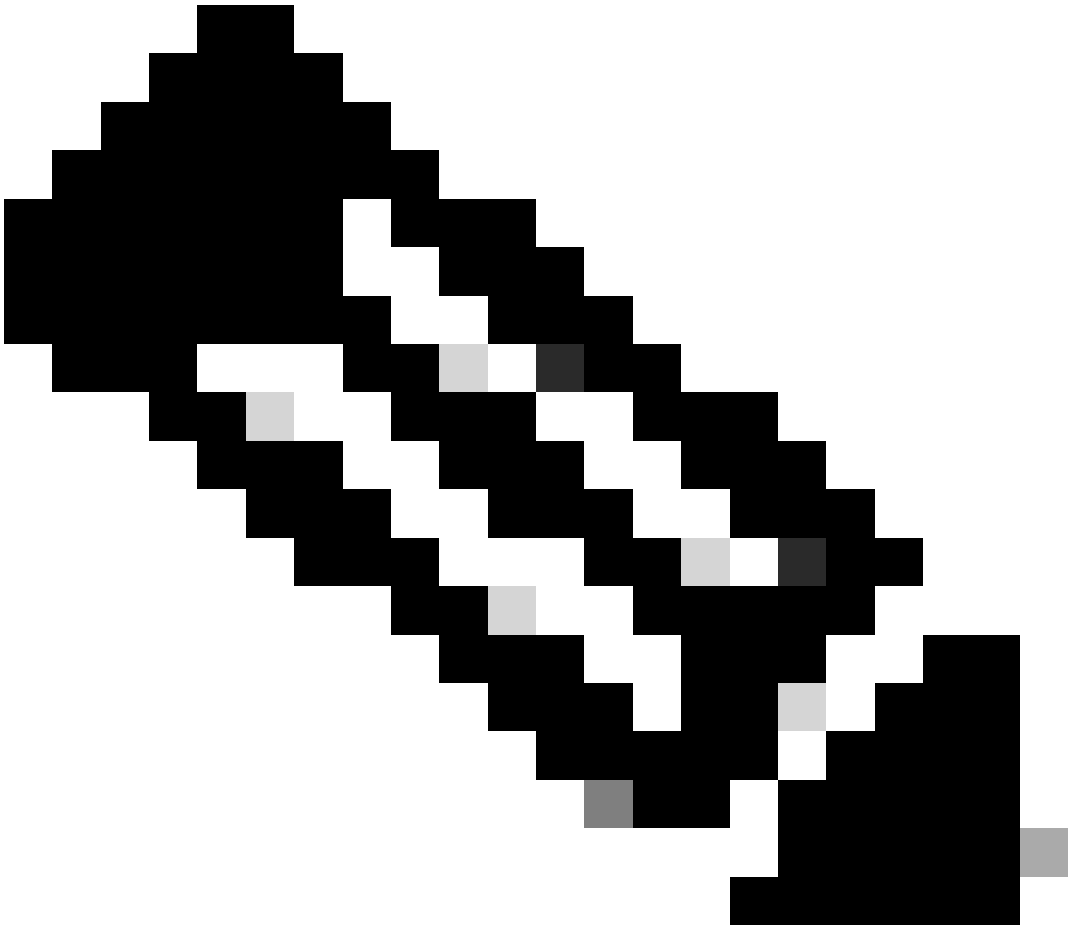
Se desejar desabilitar o HTTPS e reverter para HTTP, use o comando `config va ssl disable`.

Se desejar reabilitar o HTTPS, você deverá adicionar a chave privada e o certificado novamente e usar o comando `config va enable`.

Diretório ativo

Se você estiver usando um certificado assinado por CA para cada VA, verifique se o certificado raiz e os certificados CA emissores para cada certificado VA estão instalados em cada sistema que executa o Conector AD no mesmo site que o VA.

Se você estiver usando um certificado autoassinado para cada VA, verifique se cada certificado VA está instalado em cada sistema que executa o Conector AD no mesmo site do Umbrella que o VA.



> Note: Somente certificados para VAs no mesmo site de guarda-chuva que o Conector AD precisam ser instalados no Conector AD.

Pode levar até 20 minutos para que o VA sincronize o status HTTPS com o Umbrella, que é então

sincronizado com o Conector AD. Como resultado, pode levar até 20 minutos para que o Conector comece a enviar dados para o VA via HTTPS. Qualquer mapeamento user-IP enviado durante esse período é descartado pelo VA. Portanto, é recomendável fazer a alteração de configuração no VA somente durante as horas de inatividade quando não se espera nenhum logon de usuário.

Cliente Umbrella Android

Se você estiver usando certificados assinados por CA para VAs, certifique-se de que o certificado raiz e a emissão de certificados CA para cada certificado VA sejam enviados para e instalados em cada dispositivo Android.

Se você estiver usando certificados autoassinados para VAs, certifique-se de que cada certificado VA seja enviado para e instalado em cada dispositivo Android.

Quando o certificado estiver disponível, o cliente Android Umbrella pode começar a usar esse certificado para configurar um canal HTTPS com o VA.

Cliente de Chromebook Umbrella

Se você estiver usando certificados assinados por CA para VAs, certifique-se de que o certificado raiz e os certificados CA emissores para cada certificado VA sejam enviados para e instalados em cada Chromebook.

Se você estiver usando certificados autoassinados para VAs, certifique-se de que cada certificado VA seja enviado para e instalado em cada Chromebook.

Quando o certificado estiver disponível, o cliente Umbrella Chromebook pode começar a usar esse certificado para configurar um canal HTTPS com o VA.

Para obter mais informações, consulte o artigo Umbrella Chromebook Client: Enviando mapeamentos de IP de usuário por um canal seguro para o Umbrella Virtual Appliance.

Sequência de configuração

Quando o HTTPS é habilitado no VA, o VA não aceita mapeamentos de IP de usuário enviados em texto sem formatação sobre HTTP. Como resultado, todos os logons de usuário enviados por HTTP são descartados e a atribuição de usuário para solicitações DNS desses usuários não está disponível. Portanto, é recomendável configurar esses componentes nesta ordem:

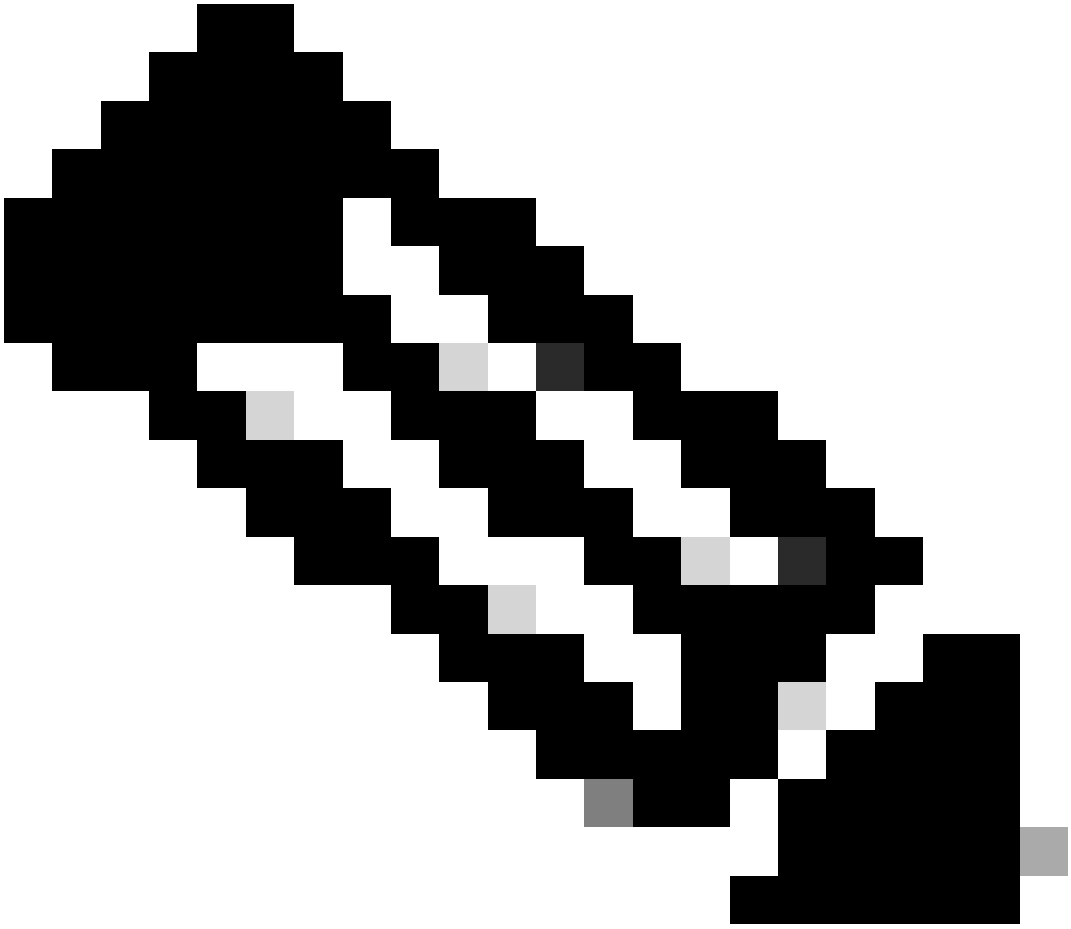
1. Crie o certificado e a chave privada para cada VA com base em um certificado assinado pela CA ou autoassinado.

2. Adicione o certificado e a chave privada a cada VA, respectivamente.

3. Verifique se o certificado raiz e os certificados pai intermediários para cada certificado VA (ou certificado autoassinado VA) estão instalados em cada sistema que executa o Conector AD no

mesmo site que o VA e em cada Chromebook.

4. Durante as horas de inatividade, habilite o HTTPS no VA.



Note: O certificado no VA deve ser substituído antes de expirar, e os certificados pai e raiz intermediários devem ser instalados no AD Connector e nos Umbrella Chromebook Clients. Se isso não for feito, o AD Connector e os Umbrella Chromebook Clients não poderão se comunicar com o VA.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.