Configurare Umbrella VA per la ricezione di mapping IP utente

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Panoramica
- Appliance virtuale
  - Aggiungi chiave privata e certificato a VA
  - Aggiungi certificato a VA
  - Abilita HTTPS su VA
  - Verifica abilitazione HTTPS
- Active Directory
- Umbrella Android Client
- Umbrella Chromebook Client
  - Sequenza di configurazione

Introduzione

In questo documento viene descritto come configurare Cisco Umbrella Virtual Appliance (VA) per ricevere i mapping IP degli utenti su un canale sicuro.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- La creazione di chiavi private, la creazione di certificati, la firma e la gestione di certificati non rientrano nell'ambito dei componenti Umbrella. Questa operazione deve essere eseguita all'esterno di questi componenti.
- È necessario creare un certificato con un nome comune univoco per ogni appliance virtuale.
- È inoltre necessario aggiungere un record A nel server DNS interno, che punti il nome comune all'indirizzo IP dell'appliance virtuale.
- Se è necessario modificare l'indirizzo IP di un'appliance virtuale, è necessario modificare anche il record A.

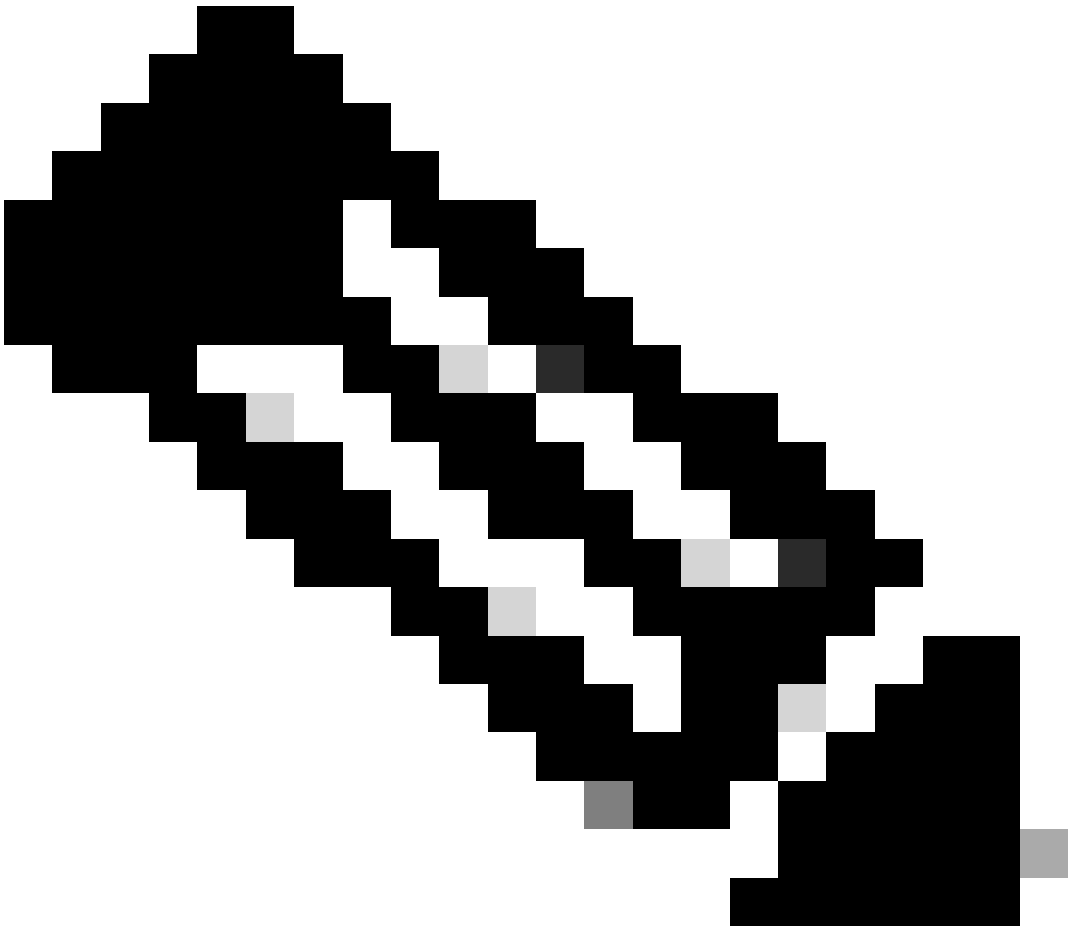
- L'FQDN corrispondente al certificato deve essere configurato come dominio locale nel dashboard Umbrella in modo che il VSA lo riconosca come dominio locale.
- La chiave privata e i certificati devono essere creati rispettivamente nel formato con estensione key e cer.
- A tale scopo, è possibile utilizzare certificati autofirmati o certificati firmati dall'autorità di certificazione.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance virtuale con versione 2.7 o successive
- Umbrella AD Connector deve eseguire la versione 1.5 o successiva
- I client Umbrella Chromebook devono eseguire la versione 1.3.3 o successiva

---



Nota: Se sul connettore VA o AD sono in esecuzione versioni precedenti, è possibile aprire un ticket di supporto con Umbrella per aggiornarli alle rispettive versioni supportate.

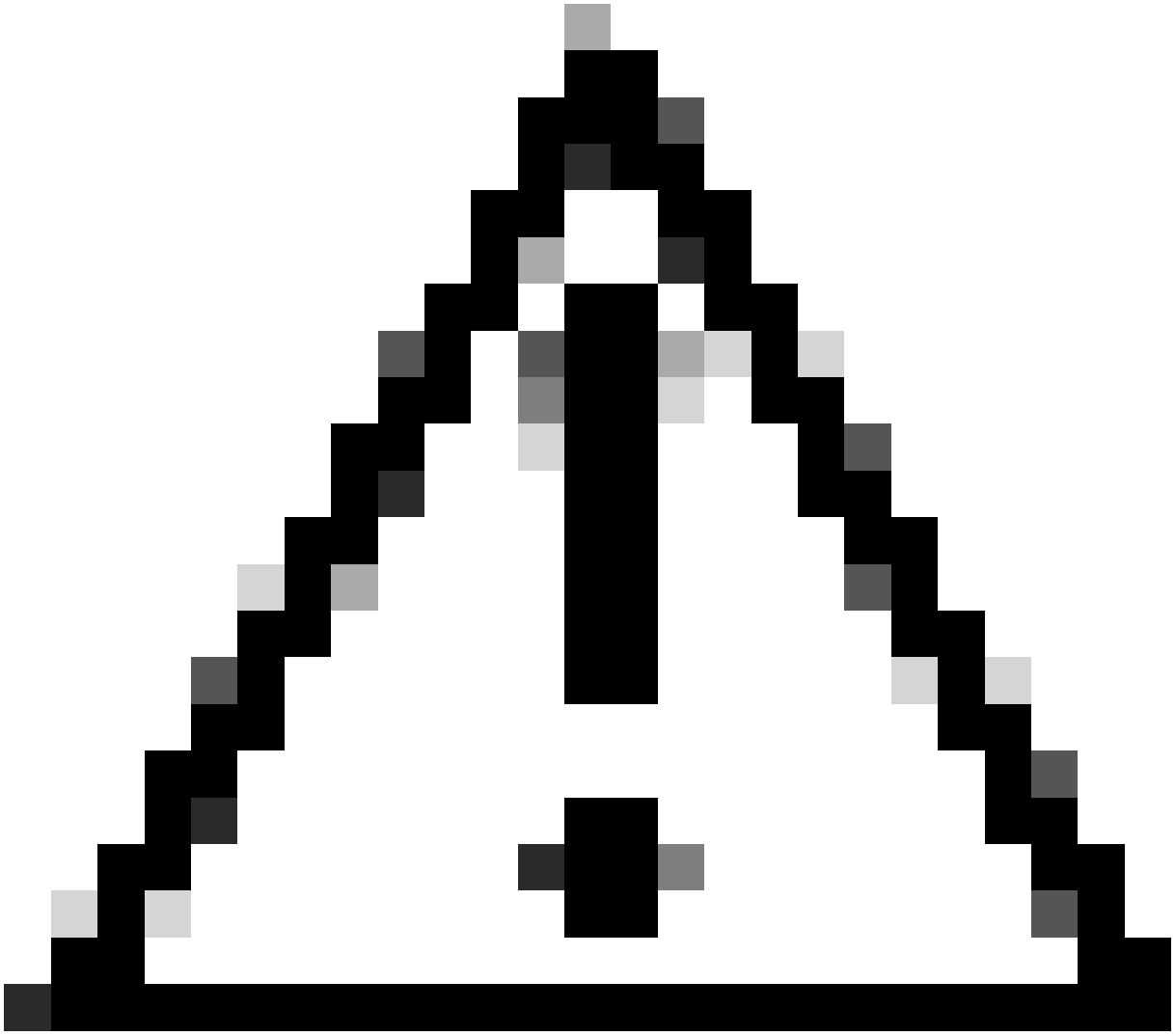
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Umbrella Virtual Appliance, che esegue la versione 2.6 o precedente, supporta la ricezione di mapping IP utente dal connettore Umbrella Active Directory (AD) e dai client Umbrella Chromebook solo in forma non crittografata sulla porta 443. Di conseguenza, un prerequisito obbligatorio per la distribuzione è stato che il connettore AD e i client VA o Chromebook e VA comunicano solo su una rete attendibile.

A partire dalla versione 2.7, Umbrella Virtual Appliance può ora ricevere mapping IP utente AD dal connettore AD su HTTPS e, analogamente, mapping IP utente GSuite da ciascun client Umbrella Chromebook su HTTPS.

In questo articolo vengono illustrati in dettaglio i passaggi di configurazione per ogni componente per abilitare la comunicazione HTTPS. Per impostazione predefinita, la comunicazione HTTPS è disabilitata e il connettore AD e i client Chromebook comunicano con VA solo su HTTP.



Attenzione: L'attivazione di questa funzionalità può aumentare l'utilizzo della CPU e della memoria sul VA e sul connettore Umbrella AD e può comportare una riduzione del throughput DNS per il VA. Di conseguenza, si consiglia di attivare questa funzione solo se richiesto da eventuali requisiti di conformità per l'organizzazione.

Appliance virtuale

Aggiungi chiave privata e certificato a VA

Per aggiungere la chiave privata e il certificato alla VA:
1. Aprire il file della chiave privata tramite un editor di testo.

2. Selezionare tutto, copia e incollare tra virgolette doppie per questo comando:

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

Aggiungi certificato a VA

Per aggiungere il certificato al VA:
1. Aprire il file del certificato tramite un editor di testo.

2. Selezionare tutto, copia e incollare tra virgolette doppie per il comando seguente:

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

Abilita HTTPS su VA

Abilitare HTTPS su VA utilizzando questo comando:

```
config va ssl enable
```

Verifica abilitazione HTTPS

Verificare che HTTPS sia abilitato utilizzando il comando:

```
config va show
```

L'output di questo comando può includere lo stato HTTPS e i dettagli del certificato SSL.

Output di esempio:

```
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
```

Possono essere necessari fino a 20 minuti prima che la VA inizi a ricevere eventi tramite HTTPS. È possibile eseguire il controllo dopo circa 20 minuti utilizzando il comando `config va status`. Lo stato del connettore AD è in giallo (bloccato) nel periodo intermedio e passa allo stato verde quando il VA inizia a ricevere eventi tramite HTTPS.

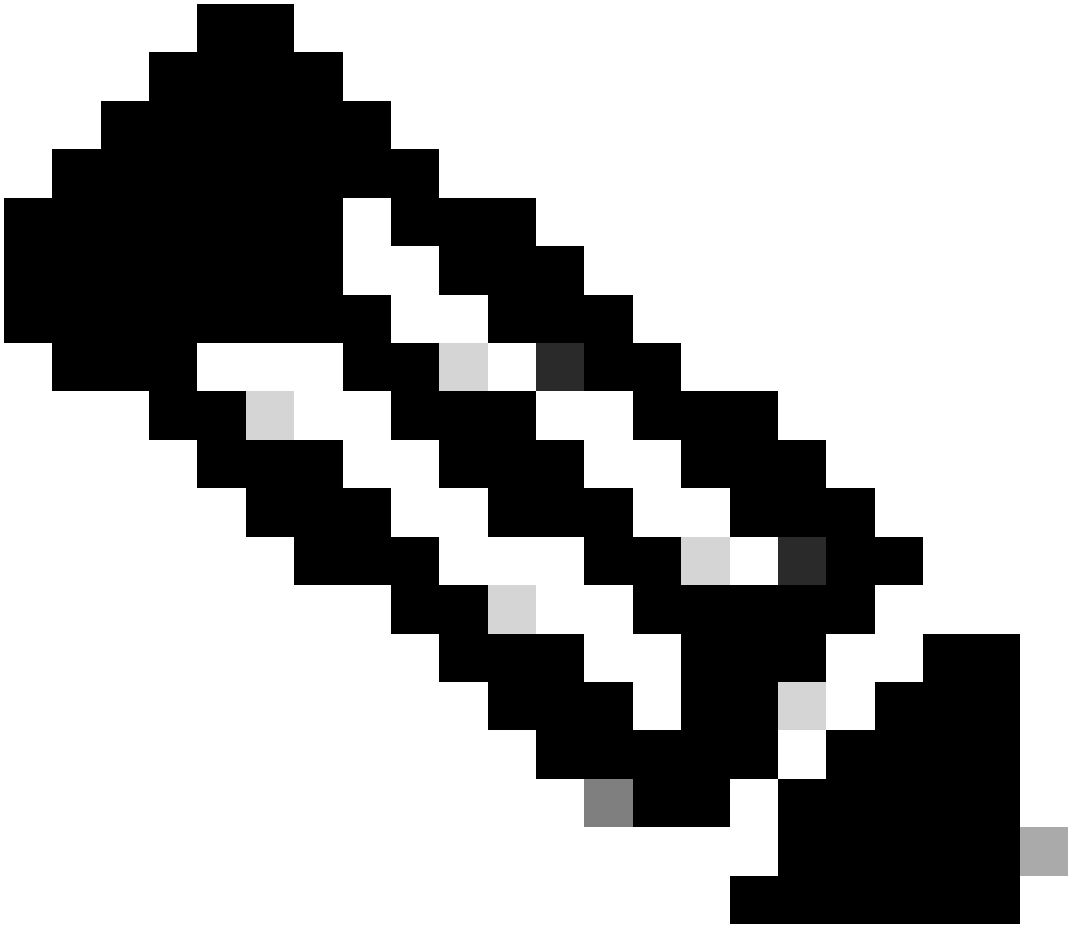
Per disabilitare HTTPS e tornare al protocollo HTTP, usare il comando `config via ssl disable`.

Se si desidera riattivare HTTPS, è necessario aggiungere nuovamente la chiave privata e il certificato e quindi utilizzare il comando `config va enable`.

Active Directory

Se si utilizza un certificato firmato dall'autorità di certificazione per ogni VA, verificare che il certificato radice e i certificati dell'autorità di certificazione emittente per ogni certificato VA siano installati in ogni sistema che esegue il connettore AD nello stesso sito del VA.

Se si utilizza un certificato autofirmato per ogni VA, verificare che ogni certificato VA sia installato in ogni sistema che esegue il connettore AD nello stesso sito Umbrella del VA.



> Nota: Solo i certificati per i VA nello stesso sito Umbrella del connettore AD devono essere installati nel connettore AD.

La sincronizzazione dello stato HTTPS con Umbrella può richiedere fino a 20 minuti e viene quindi sincronizzata con il connettore AD. Di conseguenza, il connettore può impiegare fino a 20 minuti

per iniziare a inviare dati al VA su HTTPS. Qualsiasi mapping utente-IP inviato durante questo periodo viene ignorato dal VSA. Si consiglia pertanto di apportare la modifica alla configurazione sulla VA solo durante le ore di inattività quando non è previsto alcun accesso utente.

Umbrella Android Client

Se si utilizzano certificati firmati dall'autorità di certificazione per i dispositivi Android, verificare che il certificato radice e i certificati dell'autorità di certificazione emittente per ogni certificato di autorità di certificazione siano stati sottoposti a push e installati in ogni dispositivo Android.

Se si utilizzano certificati autofirmati per i dispositivi Android, verificare che ogni certificato VA sia installato e sottoposto a push in ogni dispositivo Android.

Una volta che il certificato è disponibile, il client Umbrella Android può iniziare a utilizzare questo certificato per configurare un canale HTTPS con VA.

Umbrella Chromebook Client

Se si utilizzano certificati firmati dall'autorità di certificazione (CA) per i VNA, verificare che il certificato radice e i certificati dell'autorità di certificazione emittente per ogni certificato VSA siano stati inseriti e installati in ogni Chromebook.

Se si utilizzano certificati autofirmati per i VSA, assicurarsi che ogni certificato VSA sia inserito e installato in ogni Chromebook.

Una volta che il certificato è disponibile, il client Umbrella Chromebook può iniziare a utilizzare questo certificato per configurare un canale HTTPS con VA.

Per ulteriori informazioni, fare riferimento all'articolo Umbrella Chromebook Client: Invio di mapping IP utente tramite un canale sicuro a Umbrella Virtual Appliance.

Sequenza di configurazione

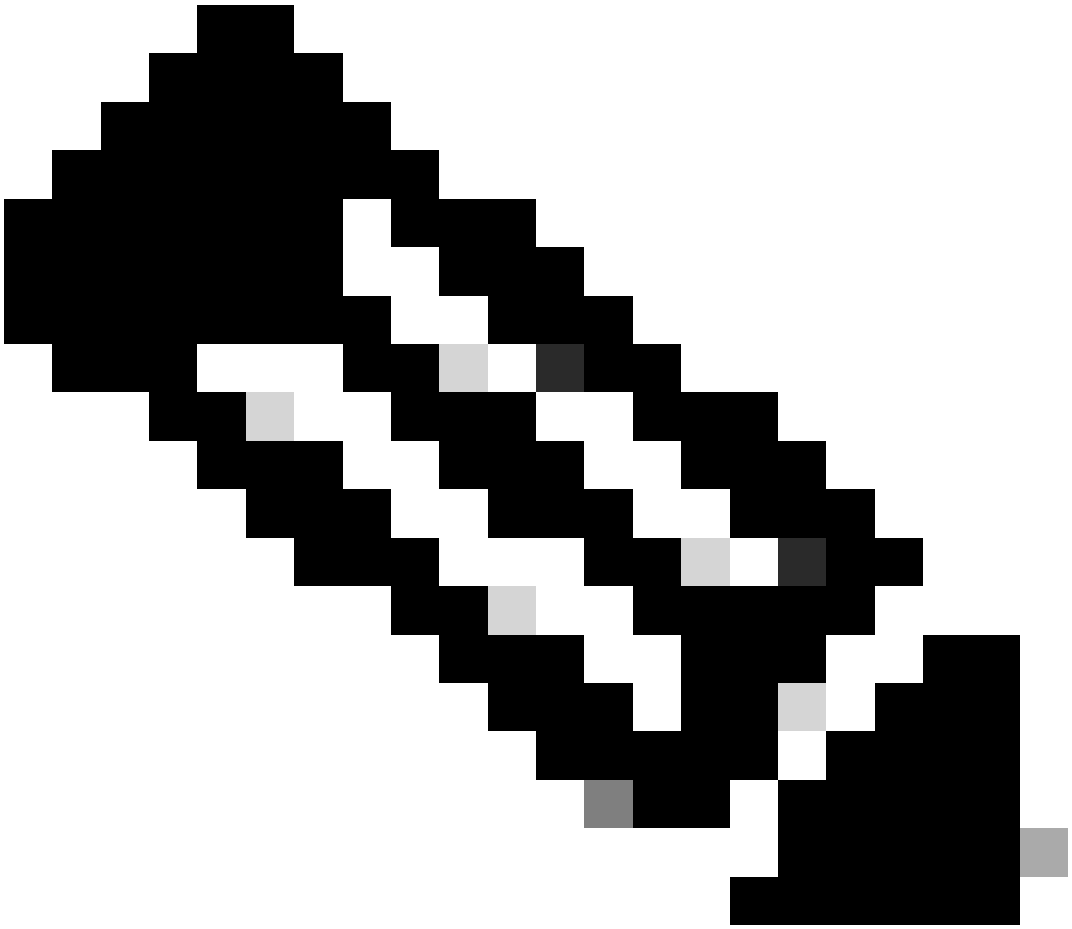
Dopo aver abilitato HTTPS sulla VA, la VA non accetta i mapping IP utente inviati in testo normale su HTTP. Di conseguenza, tutti gli accessi utente inviati tramite HTTP vengono eliminati e l'attribuzione delle richieste DNS da parte di questi utenti non è disponibile. Si consiglia pertanto di configurare i seguenti componenti nell'ordine indicato:

1. Creare il certificato e la chiave privata per ogni VA in base a un certificato autofirmato o firmato da un'autorità di certificazione.

2. Aggiungere rispettivamente il certificato e la chiave privata a ogni VA.

3. Verificare che il certificato radice e i certificati padre intermedi per ogni certificato VA (o certificato autofirmato VA) siano installati in ogni sistema che esegue il connettore AD nello stesso sito del VA e in ogni Chromebook.

4. Durante le ore di inattività, abilitare HTTPS su VA.



Nota: Il certificato sulla VA deve essere sostituito prima di scadere e i certificati principali intermedi devono essere installati sui client Active Directory Connector e Umbrella Chromebook. In caso contrario, i client AD Connector e Umbrella Chromebook non sono in grado di comunicare con VA.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).