사용자-IP 매핑을 수신하도록 Umbrella VA 구성

목차

소개

이 문서에서는 보안 채널을 통해 사용자-IP 매핑을 수신하도록 Cisco Umbrella Virtual Appliance(VA)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

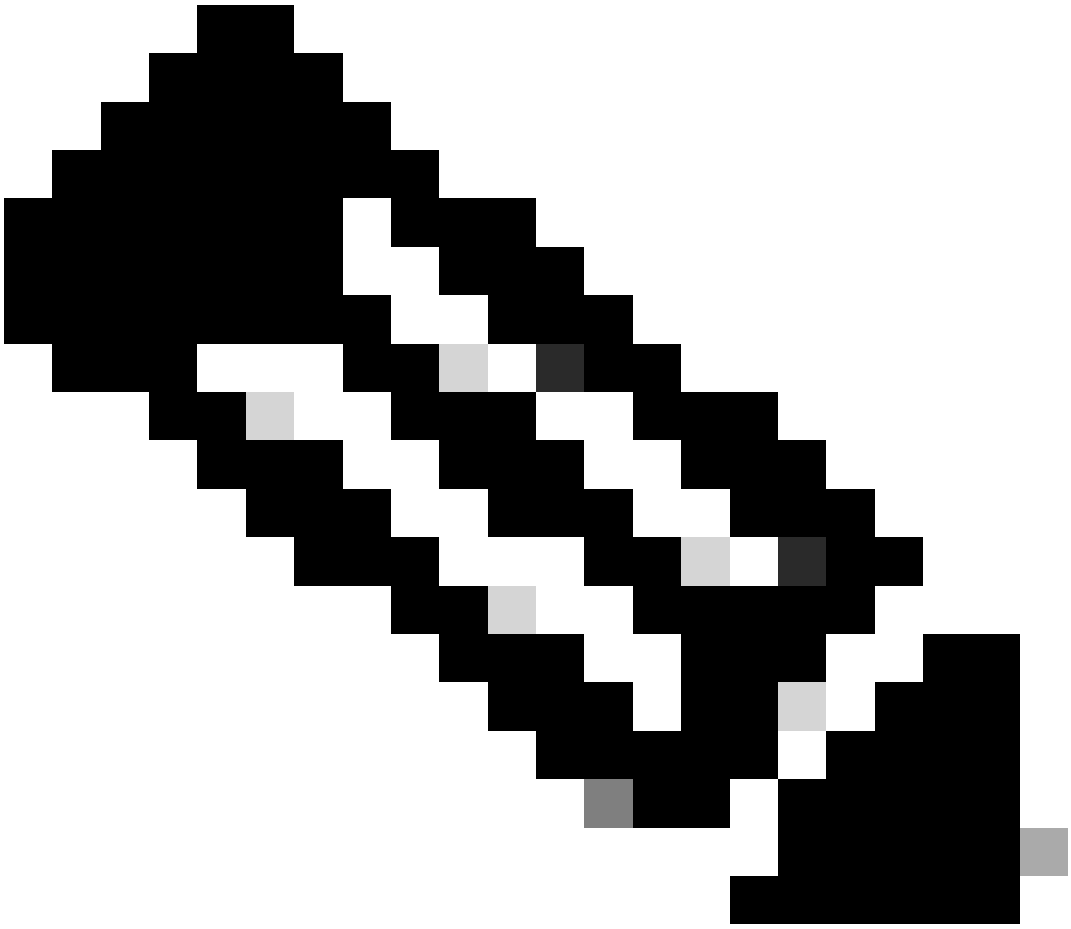
- 개인 키 생성, 인증서 생성, 인증서 서명 및 관리는 Umbrella 구성 요소의 범위를 벗어납니다. 이러한 구성 요소의 외부에서 수행해야 합니다.
- 가상 어플라이언스마다 고유한 CN을 사용하여 인증서를 하나 생성해야 합니다.
- 또한 내부 DNS 서버에 A 레코드를 추가하여 이 Common Name(공용 이름)을 Virtual Appliance의 IP 주소로 지정해야 합니다.
- 가상 어플라이언스의 IP 주소를 변경해야 하는 경우 이 A 레코드도 그에 따라 변경해야 합니다.
- 인증서에 해당하는 FQDN을 Umbrella 대시보드에서 로컬 도메인으로 구성해야 VA에서 이를 로컬 도메인으로 인식합니다.

- 개인 키와 인증서는 각각 .key 및 .cer 형식으로 만들어야 합니다.
- 이 용도로 자체 서명 인증서 또는 CA 서명 인증서를 사용할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 2.7 이상을 실행하는 가상 어플라이언스
- Umbrella AD Connector는 버전 1.5 이상을 실행해야 합니다.
- Umbrella Chromebook 클라이언트는 버전 1.3.3 이상을 실행해야 합니다.



참고: VA 또는 AD 커넥터에서 이전 버전을 실행 중인 경우 Umbrella를 사용하여 지원 티켓을 열어 지원되는 해당 버전으로 업그레이드할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

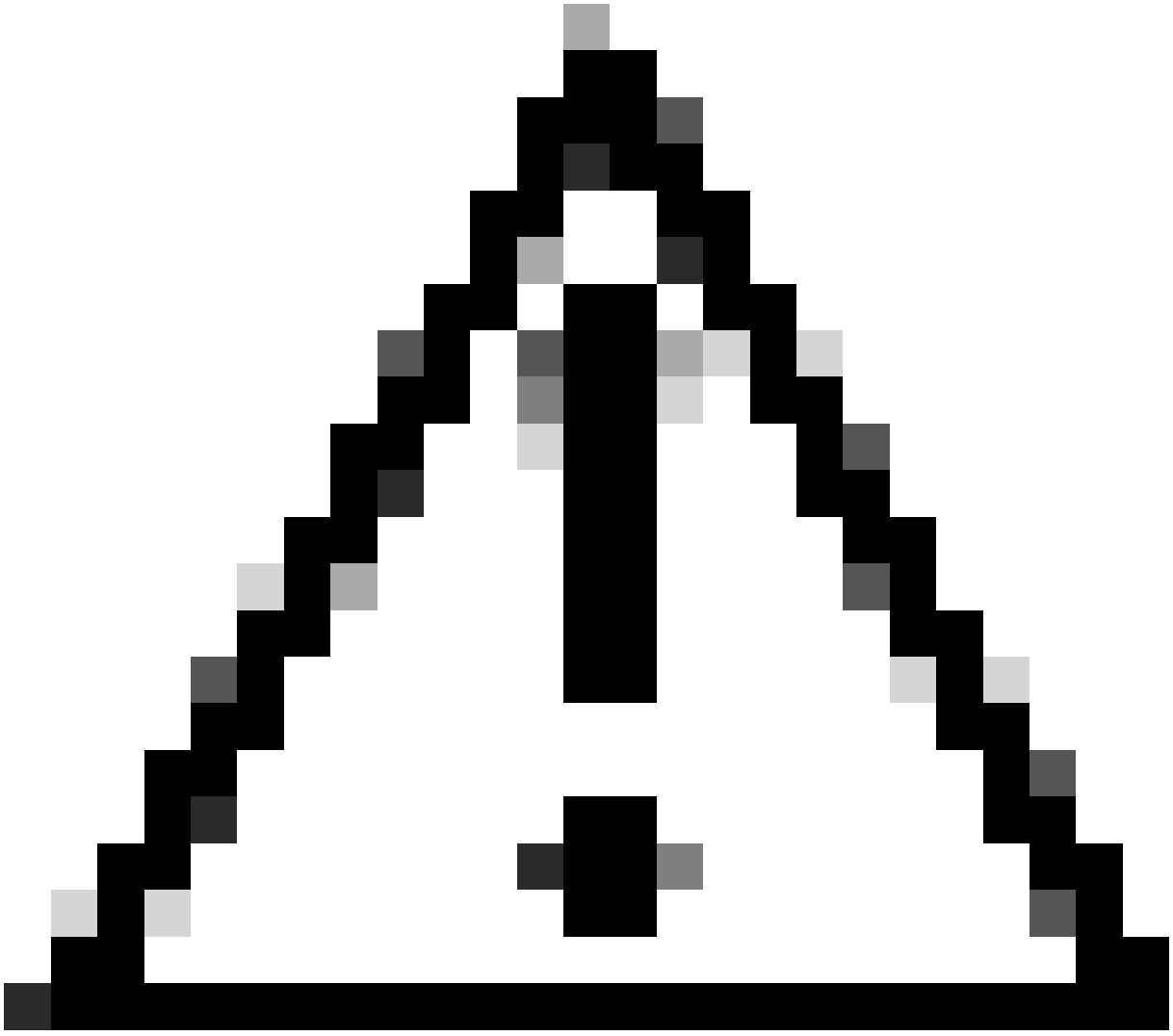
명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

버전 2.6 이상을 실행하는 Umbrella Virtual Appliance는 포트 443의 암호화되지 않은 형식으로만 Umbrella AD(Active Directory) 커넥터 및 Umbrella Chromebook 클라이언트에서 사용자-IP 매핑을 수신할 수 있습니다. 따라서 AD 커넥터와 VA 또는 Chromebook 클라이언트 및 VA가 신뢰할 수 있는 네트워크에서만 통신하는 것이 구축의 필수 전제조건이었습니다.

버전 2.7부터 Umbrella Virtual Appliance는 이제 HTTPS를 통해 AD 커넥터에서 AD 사용자-IP 매핑을 수신할 수 있으며, 마찬가지로 HTTPS를 통해 각 Umbrella Chromebook 클라이언트에서 사용자-IP 매핑을 전송할 수 있습니다.

이 문서에서는 HTTPS 통신을 활성화하는 각 구성 요소의 컨피그레이션 단계에 대해 자세히 설명합니다. 기본적으로 HTTPS 통신은 비활성화되며 AD 커넥터 및 Chromebook 클라이언트는 HTTP를 통해서만 VA와 통신합니다.



주의: 이 기능을 켜면 VA 및 Umbrella AD 커넥터의 CPU 및 메모리 사용률이 증가하고 VA의 DNS 처리량이 감소할 수 있습니다. 따라서 조직의 모든 규정 준수 요구 사항에 의해 의무화된 경우에만 이 기능을 설정하는 것이 좋습니다.

가상 어플라이언스

VA에 개인 키 및 인증서 추가

VA에 개인 키 및 인증서를 추가하려면
1. 텍스트 편집기를 통해 개인 키 파일을 엽니다.

2. 모두를 선택하고 복사한 다음 이 명령에 대한 큰따옴표를 붙여 넣습니다.

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

VA에 인증서 추가

VA에 인증서를 추가하려면
1. 텍스트 편집기를 통해 인증서 파일을 엽니다.

2. 모두 선택하고 복사한 다음 아래 명령에 대한 큰따옴표를 붙여 넣습니다.

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

VA에서 HTTPS 사용

다음 명령을 사용하여 VA에서 HTTPS를 활성화합니다.

```
config va ssl enable
```

HTTPS 사용 확인

다음 명령을 사용하여 HTTPS가 활성화되었는지 확인합니다.

```
config va show
```

이 명령의 출력에는 HTTPS 상태 및 SSL 인증서 세부사항이 포함될 수 있습니다.

출력 예:

```
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
```

VA가 HTTPS를 통해 이벤트 수신을 시작하는 데 최대 20분이 소요될 수 있습니다. config va status 명령을 사용하여 약 20분 후에 확인할 수 있습니다. AD 커넥터 상태는 중간 기간에 노란색(정지됨) 상태이며 VA가 HTTPS를 통해 이벤트를 수신하기 시작하면 녹색 상태로 전환됩니다.

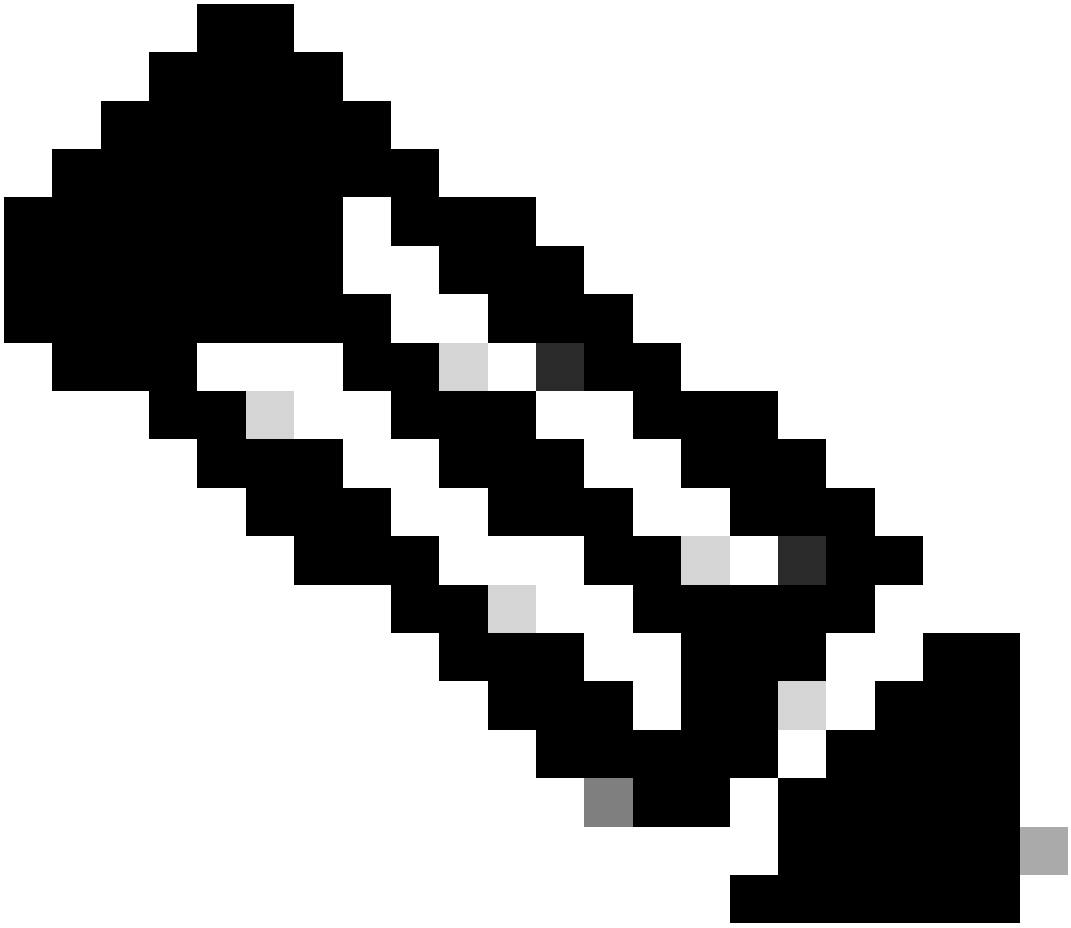
HTTPS를 비활성화하고 HTTP로 되돌리려면 ssl disable을 통해 config 명령을 사용합니다.

HTTPS를 다시 활성화하려면 개인 키와 인증서를 다시 추가한 다음 config va enable 명령을 사용해야 합니다.

액티브 디렉토리

각 VA에 대해 CA 서명 인증서를 사용하는 경우 VA와 동일한 사이트에서 AD Connector를 실행하는 각 시스템에 루트 인증서 및 각 VA 인증서에 대한 CA 인증서 발급이 설치되어 있는지 확인합니다.

각 VA에 자체 서명 인증서를 사용하는 경우 각 VA 인증서가 VA와 동일한 Umbrella 사이트에서 AD Connector를 실행하는 각 시스템에 설치되어 있는지 확인합니다.



참고: AD 커넥터와 동일한 Umbrella 사이트의 VA에 대한 인증서만 AD 커넥터에 설치해야 합니다.

VA가 HTTPS 상태를 Umbrella에 동기화하고 AD 커넥터에 동기화하는 데 최대 20분이 소요될 수 있습니다. 따라서 커넥터가 HTTPS를 통해 VA에 데이터를 전송하기 시작하는 데 최대 20분이 소요될 수 있습니다. 이 기간 동안 전송된 사용자-IP 매핑은 VA에서 폐기됩니다. 따라서 사용자 로그인이 예상되지 않는 다운타임 시간에만 VA의 컨피그레이션을 변경하는 것이 좋습니다.

Umbrella Android 클라이언트

VA에 CA 서명 인증서를 사용하는 경우 루트 인증서와 각 VA 인증서에 대한 CA 인증서 발급이 각 Android 디바이스에 푸시되어 설치되어 있는지 확인합니다.

VA에 자체 서명 인증서를 사용하는 경우 각 VA 인증서가 각 Android 디바이스에 푸시되어 설치되어 있는지 확인합니다.

인증서가 사용 가능해지면 Umbrella Android Client는 이 인증서를 사용하여 VA를 사용하는 HTTPS 채널을 설정할 수 있습니다.

Umbrella Chromebook 클라이언트

VA에 대해 CA 서명 인증서를 사용하는 경우 루트 인증서와 각 VA 인증서에 대한 CA 인증서 발급이 각 Chromebook에 푸시되어 설치되어 있는지 확인합니다.

VA에 자체 서명 인증서를 사용하는 경우 각 VA 인증서가 각 Chromebook에 푸시되어 설치되어 있는지 확인하십시오.

인증서를 사용할 수 있게 되면 Umbrella Chromebook Client에서 이 인증서를 사용하여 VA와의 HTTPS 채널을 설정할 수 있습니다.

자세한 내용은 Umbrella Chromebook 클라이언트 문서를 참조하십시오. 보안 채널을 통해 Umbrella Virtual Appliance로 사용자-IP 매핑 전송

컨피그레이션 시퀀스

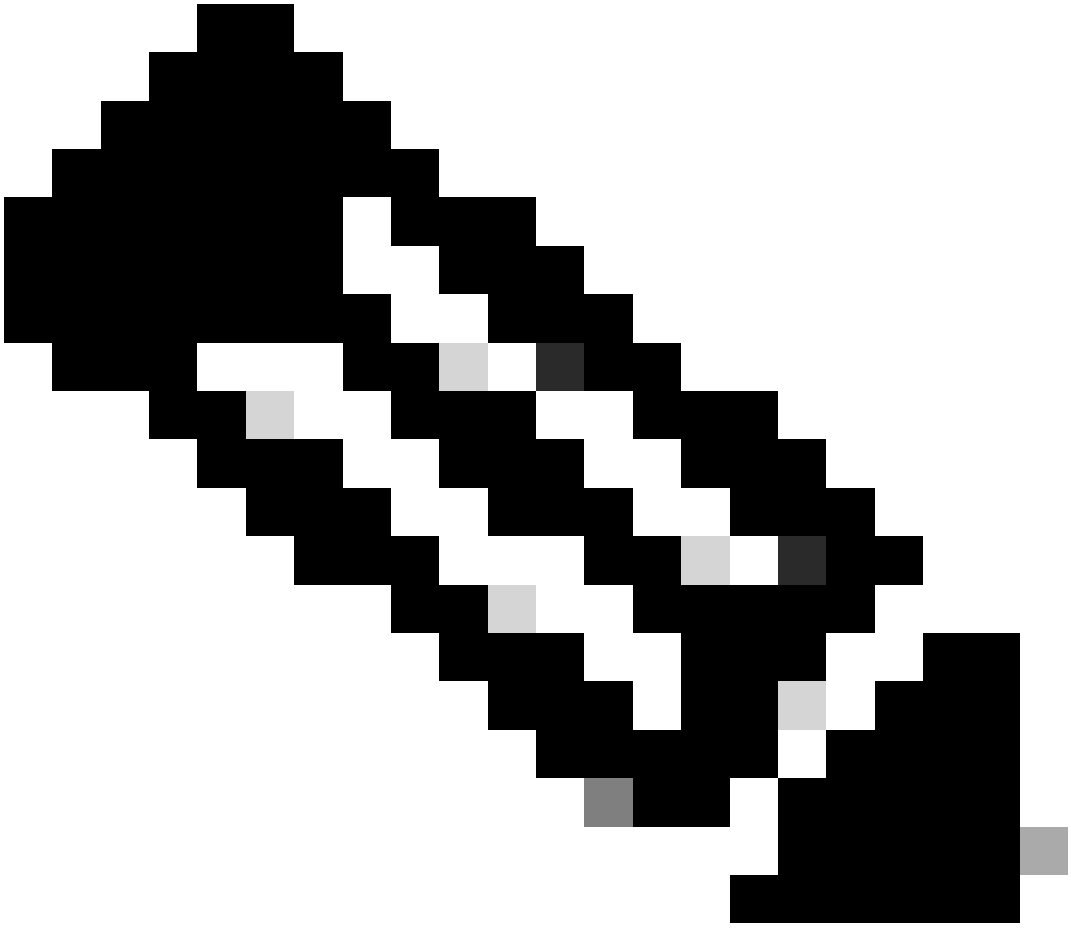
VA에서 HTTPS가 활성화되면 VA는 HTTP를 통해 일반 텍스트로 전송된 사용자 IP 매핑을 수락하지 않습니다. 그 결과 HTTP를 통해 전송된 사용자 로그인은 폐기되며 이러한 사용자의 DNS 요청에 대한 사용자 속성은 사용할 수 없습니다. 따라서 다음 순서대로 이러한 구성 요소를 구성하는 것이 좋습니다.

1. CA 서명 또는 자체 서명 인증서를 기반으로 각 VA에 대한 인증서 및 개인 키를 생성합니다.

2. 각 VA에 인증서와 개인 키를 각각 추가합니다.

3. 각 VA 인증서(또는 VA 자체 서명 인증서)의 루트 인증서 및 중간 상위 인증서가 VA와 동일한 사이트에서 AD Connector를 실행하는 각 시스템 및 각 Chromebook에 설치되어 있는지 확인합니다.

4. 다운타임 시간 중에 VA에서 HTTPS를 활성화합니다.



참고: 만료되기 전에 VA의 인증서를 교체해야 하며, 중간 상위 및 루트 인증서를 AD 커넥터 및 Umbrella Chromebook 클라이언트에 설치해야 합니다. 이렇게 하지 않으면 AD 커넥터와 Umbrella Chromebook 클라이언트가 VA와 통신할 수 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.