가상 어플라이언스 및 AD 커넥터 구축을 위한 보안 Cisco Umbrella

목차

소개

이 문서에서는 Cisco Umbrella Virtual Appliance(VA) 및 Active Directory(AD) Connector 구축과 관련된 모범 사례 및 권장 사항을 설명하여 이러한 구성 요소를 사용하여 발생하는 내부 공격의 위험을 완화합니다.

VA는 강화된 버전의 Ubuntu Linux 20.04를 실행합니다. 고객은 구성 및 문제 해결 목적으로만 액세스가 제한됩니다. 고객은 VA에 추가 소프트웨어나 스크립트를 구축할 수 없습니다.

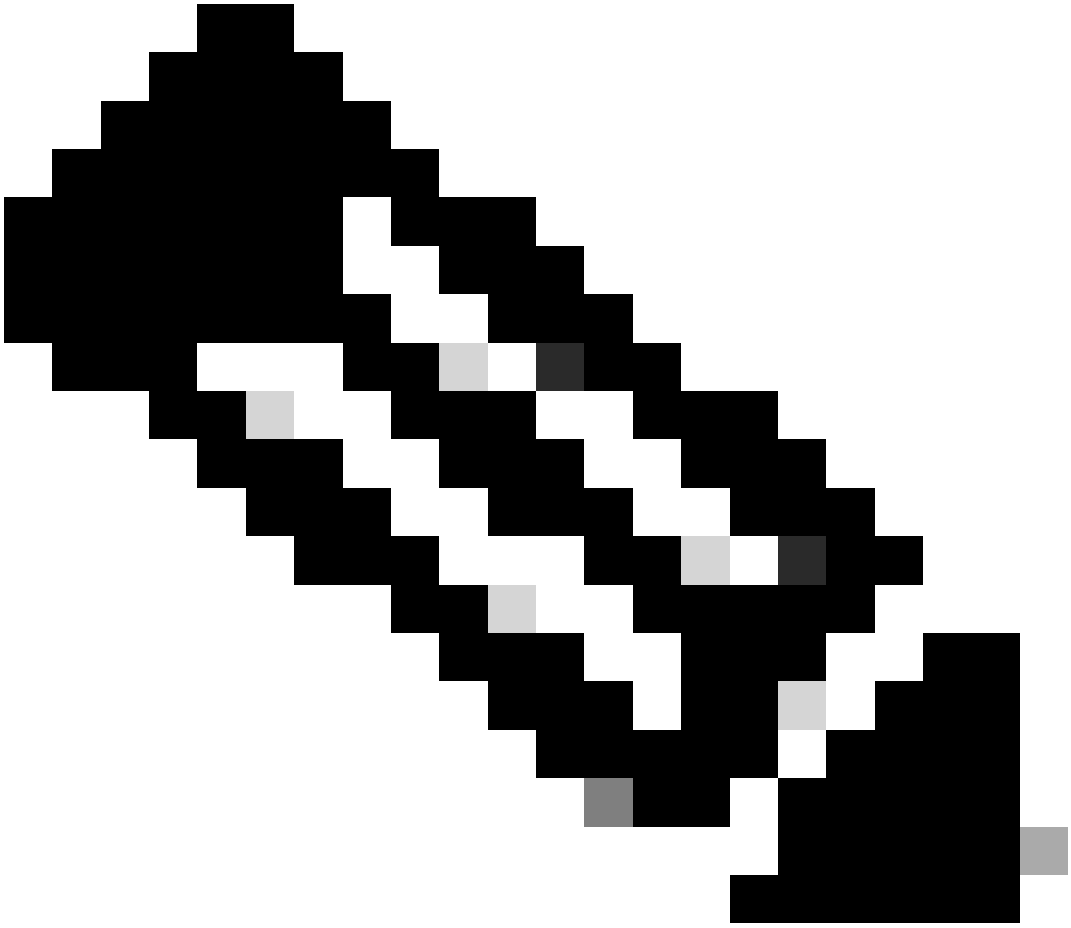
Cisco Umbrella Virtual Appliance

.tar 파일 관리:

- Cisco Umbrella VA(Virtual Appliance) 소프트웨어는 Umbrella Dashboard에서 실제 VA 이미지 및 해당 이미지의 시그니처가 포함된 .tar 파일로 다운로드됩니다.
- VA 이미지의 무결성을 확인하려면 시그니처의 유효성을 검사하는 것이 좋습니다.

포트 구성:

- 기본적으로 구축 시 인바운드 트래픽에 대해 포트 53 및 443만 열려 있습니다.
- Azure, KVM, Nutanix, AWS 또는 GCP에서 VA를 실행하는 경우 포트 22도 기본적으로 활성화되어 VA 구성을 위한 SSH 연결을 허용합니다.
- VMware 및 Hyper-V에서 실행되는 VA의 경우 VA에서 SSH를 활성화하는 명령이 실행되는 경우에만 포트 22가 열립니다.
- VA는 특정 포트/프로토콜을 통해 Umbrella 설명서에서 언급한 대상으로 아웃바운드 쿼리를 수행합니다.
- Cisco Umbrella에서는 VA에서 다른 모든 대상으로 이동하는 트래픽을 차단하도록 방화벽에 규칙을 설정할 것을 권장합니다.



참고: VA와의 모든 HTTPS 통신은 TLS 1.2를 통해서만 이루어집니다. 이전 프로토콜은 사용되지 않습니다.

비밀번호 관리:

- VA의 초기 로그인에는 비밀번호 변경이 필요합니다.
- Cisco에서는 이러한 초기 비밀번호 변경 후 VA에서 주기적으로 비밀번호를 순환하는 것을 권장합니다.

DNS 공격 완화:

- VA에서 실행 중인 DNS 서비스에 대한 내부 서비스 거부 공격의 위험을 완화하려면 VA에서 DNS에 대한 IP당 속도 제한을 구성할 수 있습니다.
- 이 기능은 기본적으로 활성화되어 있지 않으며 Umbrella 설명서에 설명된 지침을 사용하여 명시적으로 구성해야 합니다.

SNMP를 통한 VA 모니터링:

- SNMP를 통해 VA를 모니터링하는 경우 Cisco Umbrella에서는 인증 및 암호화와 함께 SNMPv3를 사용할 것을 권장합니다.
- 이에 대한 지침은 Umbrella 문서에 나와 있습니다.
- SNMP 모니터링을 활성화하면 VA의 포트 161이 인바운드 트래픽에 대해 열립니다.
- SNMP를 통해 VA에서 CPU, 로드 및 메모리와 같은 다양한 특성을 모니터링할 수 있습니다.

Cisco AD와 VA의 통합 사용:

- Cisco Umbrella Active Directory 통합과 함께 VA를 사용하는 경우 VA의 사용자 캐시 기간을 DHCP 임대 시간에 맞게 조정(또는 조정)하는 것이 좋습니다.
- 가상 어플라이언스의 지침을 참조하십시오. 사용자 캐시 설정 조정 설명서 이렇게 하면 잘못된 사용자 속성의 위험을 최소화할 수 있습니다.

감사 로깅 구성:

- VA는 VA에서 실행된 모든 컨피그레이션 변경의 감사 로그를 유지 관리합니다.
- Umbrella 설명서의 지침에 따라 syslog 서버에 대한 이 감사 로그의 원격 로깅을 구성할 수 있습니다.

VA 구성:

- Umbrella 사이트당 최소 2개의 VA를 구성해야 하며, 이 2개의 VA의 IP 주소를 DNS 서버로 엔드포인트에 배포할 수 있습니다.
- 추가적인 이중화를 위해 VA에서 애니캐스트 주소 지정을 구성할 수 있습니다. 이렇게 하면 여러 VA가 단일 Anycast 주소를 공유할 수 있습니다.
- 따라서 여러 VA를 구축하는 동시에 각 엔드포인트에 DNS 서버 IP를 두 개만 배포할 수 있습니다. VA에 장애가 발생하면 Anycast는 DNS 쿼리가 동일한 Anycast IP를 공유하는 다른 VA로 라우팅되도록 합니다.
- VA에서 Anycast를 구성하는 단계에 대해 자세히 알아보십시오.

Cisco Umbrella Active Directory 커넥터 구성

사용자 지정 계정 이름 만들기:

- Cisco Umbrella AD Connector의 모범 사례 중 하나는 기본 OpenDNS_Connector 대신 사용자 지정 계정 이름을 사용하는 것입니다.
- 이 계정은 커넥터 배포 전에 만들고 필요한 권한을 부여할 수 있습니다.
- 계정 이름은 커넥터 설치의 일부로 지정해야 합니다.

AD 커넥터로 LDAPS 구성:

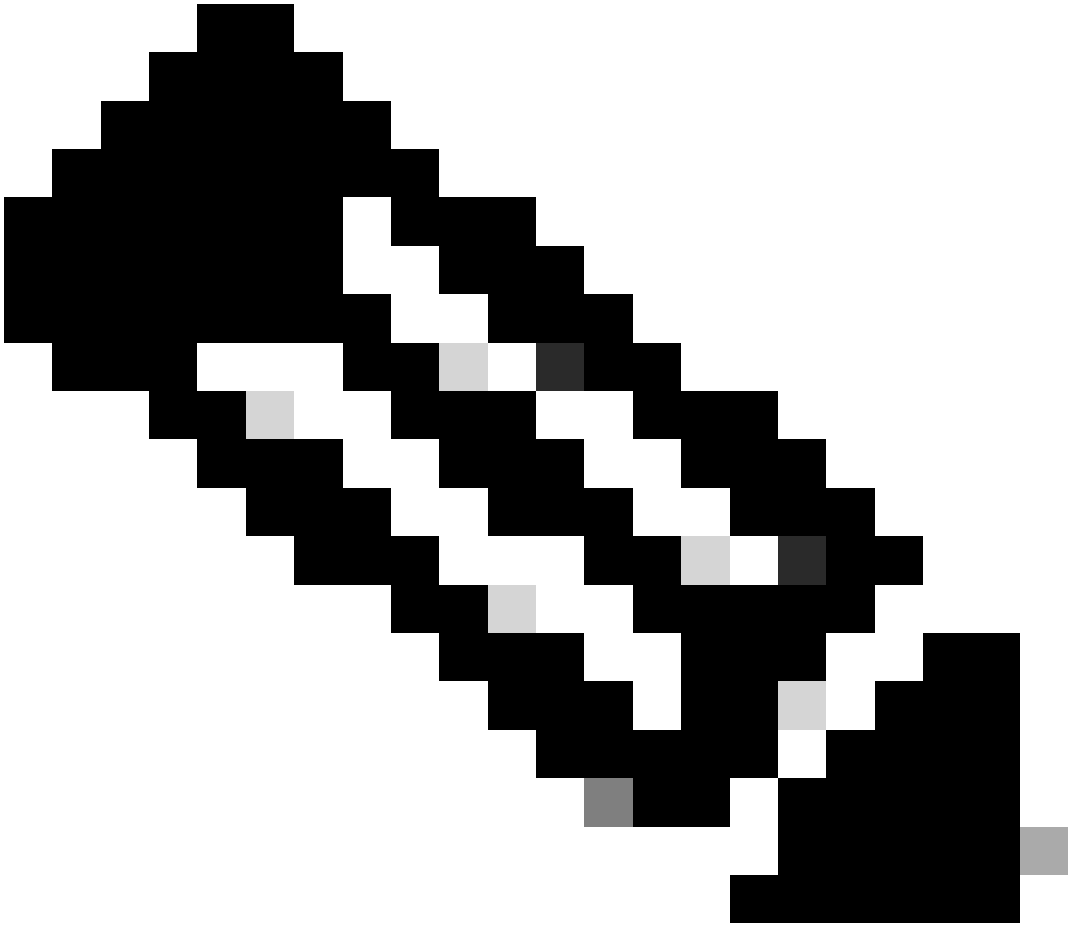
- Umbrella AD Connector는 LDAPS(보안 채널을 통해 전송된 데이터)를 통해 사용자 그룹 정보를 검색하려고 시도하지만, 이 순서대로 Kerberos를 통한 LDAP(패킷 레벨 암호화) 또는 NTLM을 통한 LDAP(인증만 수행, 암호화 없음)로 전환되지 않습니다.
- Cisco Umbrella에서는 커넥터가 암호화된 채널을 통해 이 정보를 검색할 수 있도록 도메인 컨트롤러에 LDAPS를 설정할 것을 권장합니다.

.ldif 파일 관리:

- 기본적으로 커넥터는 도메인 컨트롤러에서 검색된 사용자 및 그룹의 세부 정보를 로컬로 .ldif 파일에 저장합니다.
- 이 정보는 일반 텍스트로 저장되는 중요한 정보일 수 있으므로 커넥터를 실행하는 서버에 대한 액세스를 제한할 수 있습니다.
- 또는 설치 시 .ldif 파일을 로컬에 저장하지 않도록 선택할 수 있습니다.

포트 구성:

- 커넥터는 Windows 서비스이므로 호스트 시스템에서 어떤 포트도 활성화/비활성화하지 않습니다. Cisco Umbrella는 전용 Windows 서버에서 Cisco Umbrella AD Connector 서비스를 실행할 것을 권장합니다.
- VA와 마찬가지로, 커넥터는 특정 포트/프로토콜을 통해 Umbrella 설명서에서 언급한 대상으로 아웃바운드 [쿼리를 수행합니다](). Cisco Umbrella는 커넥터에서 다른 모든 대상으로 이동하는 트래픽을 차단하기 위해 방화벽에 규칙을 설정할 것을 권장합니다.



참고: 커넥터와 주고받는 모든 HTTPS 통신은 TLS 1.2를 통해서만 이루어집니다. 이전 프로토콜은 사용되지 않습니다.

커넥터 비밀번호 관리:

- 커넥터 비밀번호를 주기적으로 회전하는 것이 좋습니다.
- Active Directory에서 커넥터 계정 암호를 변경한 다음 커넥터 폴더의 "PasswordManager" 도구를 사용하여 암호를 업데이트하면 이 작업을 수행할 수 있습니다.

사용자-IP 매핑 수신:

- 기본적으로 커넥터는 프라이빗 IP를 통신합니다.
- AD는 일반 텍스트를 통해 VA에 사용자 매핑을 전송합니다.
- 이 Knowledge Base 문서에 설명된 지침에 따라 암호화된 채널을 통해 통신하도록 VA 및 커넥터를 구성할 수 있습니다.

인증서 관리:

- 인증서 관리 및 취소는 VA의 범위를 벗어납니다. 그리고 사용자는 최신 인증서/인증서 체인이 VA 및 커넥터에 있는지 확인할 책임이 있습니다.
- 이 통신에 암호화된 채널을 설정하면 VA 및 커넥터의 성능이 영향을 받습니다.

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.