Beveiligde Cisco-paraplu voor implementatie van virtuele apparaten en AD-connectors

Inhoud

Inleiding

In dit document worden best practices en aanbevelingen beschreven voor de implementaties van Cisco Umbrella Virtual Appliance (VA) en Active Directory (AD) Connector om het risico van interne aanvallen als gevolg van het gebruik van deze componenten te beperken.

De VA draait een geharde versie van Ubuntu Linux 10 .04. Klanten krijgen beperkte toegang voor configuratie- en probleemoplossingsdoeleinden. Klanten kunnen geen extra software of scripts op de VA implementeren.

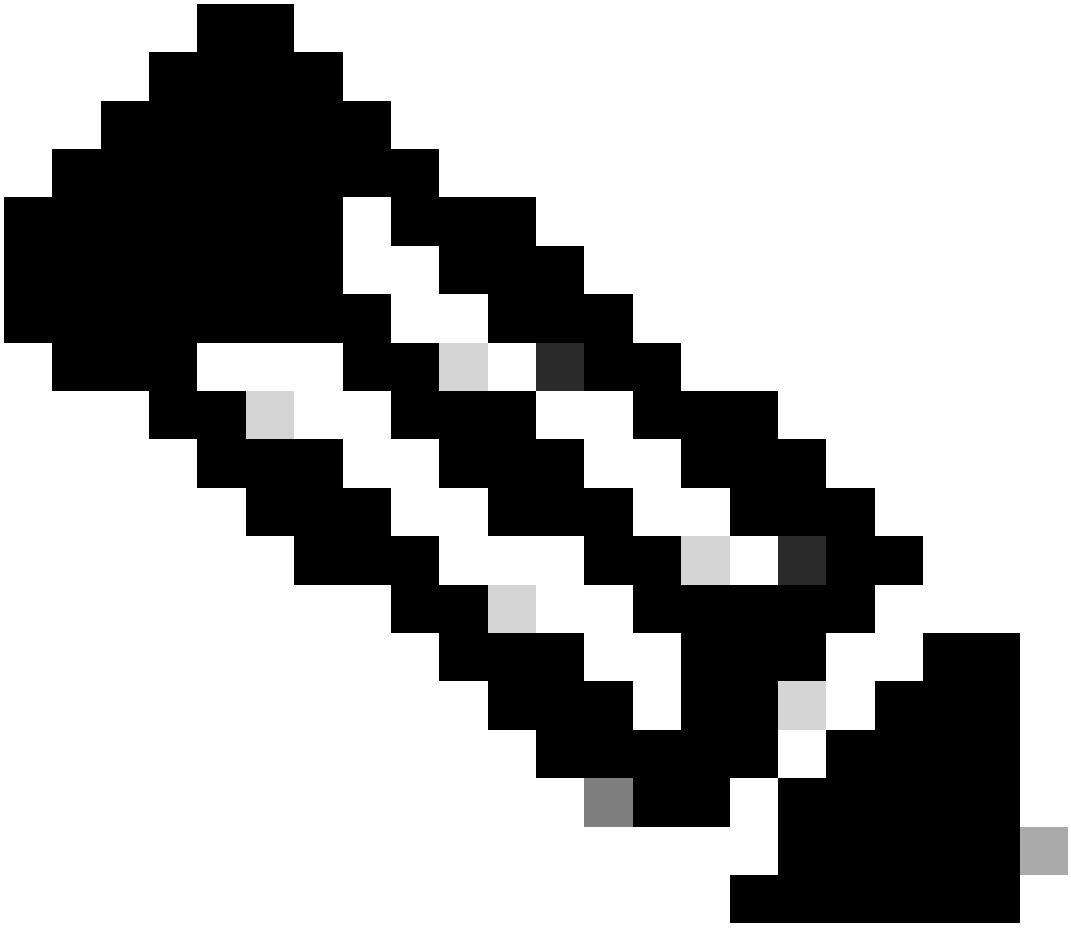
Cisco Umbrella Virtual Appliance

Het .tar-bestand beheren:

- De Cisco Umbrella Virtual Appliance (VA)-software downloadt van het Umbrella Dashboard als een .tar-bestand dat het eigenlijke VA-beeld en een handtekening voor dat beeld bevat.
- Cisco raadt aan de handtekening te valideren om de integriteit van het VA-image te verifiëren.

Poorten configureren:

- Standaard zijn bij implementatie alleen de poorten 53 en 443 geopend voor inkomend verkeer.
- Als u de VA uitvoert op Azure, KVM, Nutanix, AWS of GCP, is poort 22 standaard ook ingeschakeld om SSH-verbindingen toe te staan voor het configureren van de VA.
- Voor VA's die op VMware en Hyper-V worden uitgevoerd, wordt poort 22 alleen geopend als de opdracht om SSH in te schakelen op de VA wordt uitgevoerd.
- De VA doet uitgaande vragen over specifieke havens/protocollen naar de in de overkoepelende documentatie genoemde bestemmingen.
- Cisco Umbrella raadt aan om regels op uw firewall in te stellen om verkeer van uw VA's naar alle andere bestemmingen te blokkeren.



Opmerking: Alle HTTPS-communicatie van/naar de VA gebeurt alleen via TLS 1.2. Oudere protocollen worden niet gebruikt.

Wachtwoorden beheren:

- De eerste aanmelding op de VA vereist een wachtwoordwijziging.
- Cisco raadt aan het wachtwoord op de VA periodiek te draaien na deze eerste wachtwoordwijziging.

DNS-aanvallen beperken:

- Om het risico van een interne Denial of Service-aanval op de DNS-service die op de VA wordt uitgevoerd, te beperken, kunt u per-IP snelheidslimieten configureren voor de DNS op de VA.
- Dit is niet standaard ingeschakeld en moet expliciet worden geconfigureerd met behulp van de instructies die zijn beschreven in de overkoepelende documentatie.

VA's via SNMP controleren:

- Als u uw VA's via SNMP bewaakt, raadt Cisco Umbrella het gebruik van SNMPv3 met verificatie en codering aan.
- Instructies hiervoor staan in de overkoepelende documentatie.
- Zodra u de SNMP-bewaking inschakelt, wordt poort 161 op de VA geopend voor inkomend verkeer.
- U kunt verschillende kenmerken controleren, zoals de CPU, belasting en geheugen op de VA via SNMP.

De Cisco AD-integratie met VA's gebruiken:

- Als u de VA's gebruikt met de Cisco Umbrella Active Directory-integratie, is het de beste manier om de duur van de gebruikerscache op de VA af te stemmen (of aan te passen) op uw DHCP-leasetijd.
- Raadpleeg de instructies in de documentatie Virtual Appliance: Tuning User Case Settings. Dit minimaliseert het risico op onjuiste gebruikersattributies.

Controlelogboekregistratie configureren:

- De VA houdt een auditlogboek bij van alle configuratiewijzigingen die op de VA zijn uitgevoerd.
- U kunt de externe logboekregistratie van dit controlelog configureren voor een syslog-server volgens de instructies in de overkoepelende documentatie.

VA's configureren:

- Per Umbrella-site moeten ten minste twee VA's worden geconfigureerd en het IP-adres van deze twee VA's kan als de DNS-servers naar eindpunten worden gedistribueerd.
- Voor extra redundantie kunt u Anycast-adressering configureren op de VA. Hierdoor kunnen meerdere VA's één Anycast-adres delen.
- U kunt dus effectief meerdere VA's implementeren terwijl u nog steeds slechts twee DNS-server-IP's naar elk eindpunt distribueert. Als een VA mislukt, zorgt Anycast ervoor dat de DNS-query's worden gerouteerd naar de andere VA die dezelfde Anycast IP deelt.
- Lees meer over de stappen voor het configureren van Anycast op de VA.

De Cisco Umbrella Active Directory-connector configureren

Een aangepaste accountnaam maken:

- Een van de beste praktijken voor de Cisco Umbrella AD Connector is om een aangepaste accountnaam te gebruiken in plaats van de standaard OpenDNS_Connector.
- Deze account kan worden gemaakt voordat de connector wordt geïmplementeerd en de vereiste machtigingen worden verleend.
- De accountnaam moet worden opgegeven als onderdeel van de installatie van de connector.

LDAPS configureren met de AD-connector:

- De Umbrella AD Connector probeert gebruikersgroepinformatie op te halen via LDAPS

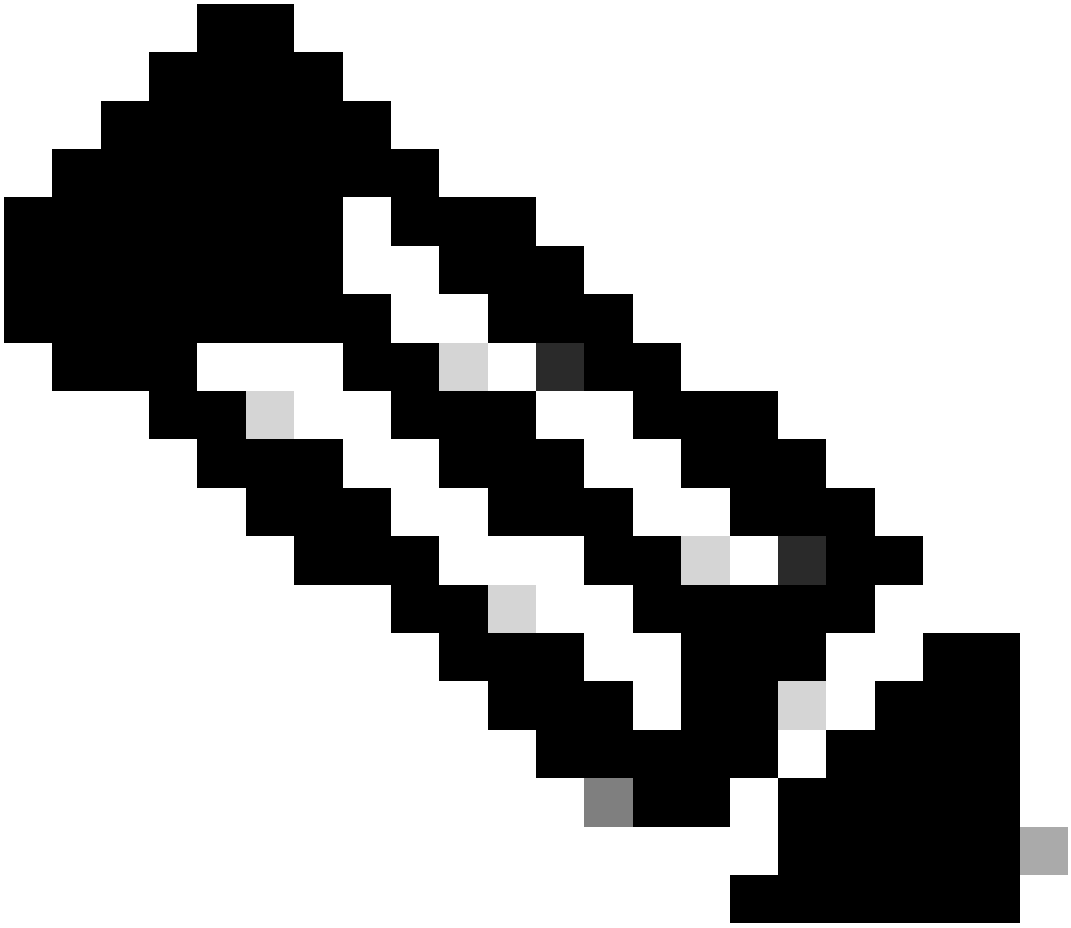
(gegevens die via een beveiligd kanaal worden verzonden), waardoor het niet in die volgorde naar LDAP over Kerberos (codering op pakketniveau) of LDAP over NTLM (alleen verificatie, geen codering) switches.
- Cisco Umbrella raadt aan om LDAPS op uw domeincontrollers in te stellen, zodat de connector deze informatie via een gecodeerd kanaal kan ophalen.

Het .ldif-bestand beheren:

- De connector slaat de gegevens van de gebruikers en groepen die zijn opgehaald van de domeincontrollers standaard lokaal op in een .ldif-bestand.
- Aangezien dit gevoelige informatie kan zijn die is opgeslagen in platte tekst, kunt u de toegang beperken tot de server waarop de connector wordt uitgevoerd.
- U kunt er ook voor kiezen om tijdens de installatie de .ldif-bestanden niet lokaal op te slaan.

Poorten configureren:

- Omdat de connector een Windows-service is, worden er geen poorten op het hostsysteem in- of uitgeschakeld. Cisco Umbrella raadt u aan de Cisco Umbrella AD Connector-service uit te voeren op een speciale Windows-server.
- Net als bij de VA voert de connector uitgaande vragen uit over specifieke poorten/protocollen naar de bestemmingen die in de overkoepelende documentatie worden vermeld. Cisco Umbrella raadt aan om regels op uw firewall in te stellen om verkeer van uw connectors naar alle andere bestemmingen te blokkeren.



Opmerking: Alle HTTPS-communicatie van/naar de connector vindt alleen plaats via TLS 1.2. Oudere protocollen worden niet gebruikt.

Het verbindingswachtwoord beheren:

- Cisco raadt aan het verbindingswachtwoord periodiek te draaien.
- Dit kan worden gedaan door het wachtwoord van de connectoraccount in Active Directory te wijzigen en vervolgens het wachtwoord bij te werken met het gereedschap "PasswordManager" in de connectormap.

IP-toewijzingen van de gebruiker ontvangen:

- De connector communiceert standaard privé-IP.
- AD verzendt gebruikerstoewijzingen naar de VA via platte tekst.
- U kunt ervoor kiezen om de VA- en connector te configureren voor communicatie via een gecodeerd kanaal volgens de instructies die in dit Knowledge Base-artikel zijn beschreven.

Certificaatbeheer:

- Certificaatbeheer en intrekking vallen buiten het bereik van de VA en u bent verantwoordelijk voor het waarborgen dat de nieuwste certificaatketen aanwezig is op de VA en de connector, indien relevant.
- Het instellen van een gecodeerd kanaal voor deze communicatie heeft invloed op de prestaties van de VA en de connector.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.