Cisco Umbrella seguro para implementaciones de appliances virtuales y conectores AD

Contenido

Introducción

Este documento describe las prácticas recomendadas y las recomendaciones sobre las implementaciones de Cisco Umbrella Virtual Appliance (VA) y del conector de Active Directory (AD) para mitigar el riesgo de cualquier ataque interno derivado del uso de estos componentes.

El VA ejecuta una versión reforzada de Ubuntu Linux 20.04. A los clientes se les proporciona acceso restringido solo con fines de configuración y resolución de problemas. Los clientes no pueden implementar ningún software ni guiones adicionales en el dispositivo virtual.

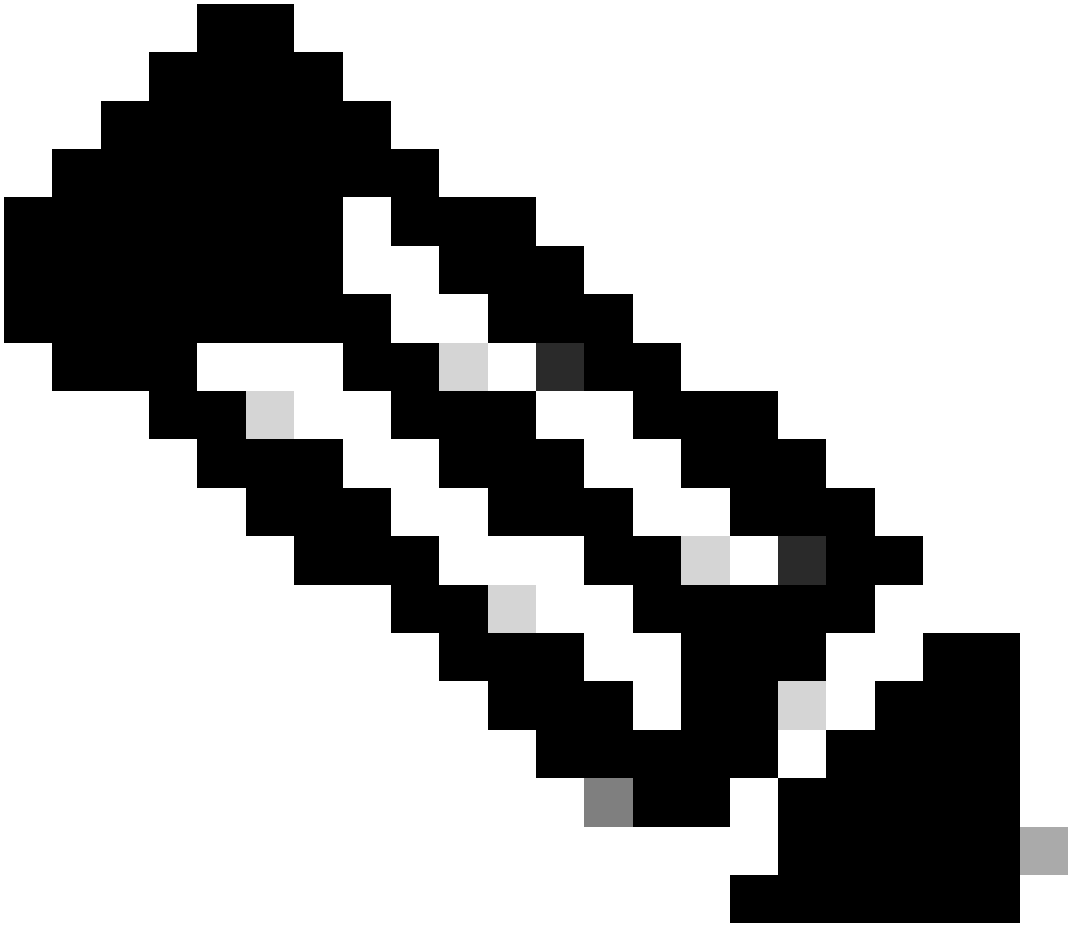
Dispositivo virtual Cisco Umbrella

Administración del archivo .tar:

- El software Cisco Umbrella Virtual Appliance (VA) se descarga del panel de Umbrella como un archivo .tar que contiene la imagen de VA real y una firma para esa imagen.
- Cisco recomienda validar la firma para verificar la integridad de la imagen de AV.

Configuración de puertos:

- De forma predeterminada, tras la implementación, sólo los puertos 53 y 443 están abiertos para el tráfico entrante.
- Si ejecuta el VA en Azure, KVM, Nutanix, AWS o GCP, el puerto 22 también se habilita de forma predeterminada para permitir conexiones SSH para configurar el VA.
- Para los VA que se ejecutan en VMware e Hyper-V, el puerto 22 se abre solamente si el comando para habilitar SSH se ejecuta en el VA.
- El VA realiza consultas salientes sobre puertos/protocolos específicos a los destinos mencionados en la documentación de Umbrella.
- Cisco Umbrella recomienda configurar reglas en su firewall para bloquear el tráfico de sus AV a todos los demás destinos.



Nota: Todas las comunicaciones HTTPS hacia/desde el VA ocurren solamente sobre TLS 1.2. No se utilizan protocolos más antiguos.

Administración de contraseñas:

- El inicio de sesión inicial en el dispositivo virtual requiere un cambio de contraseña.
- Cisco recomienda rotar periódicamente la contraseña en el dispositivo virtual después de este cambio de contraseña inicial.

Mitigación de ataques DNS:

- Para mitigar el riesgo de un ataque interno de denegación de servicio en el servicio DNS que se ejecuta en el VA, puede configurar límites de velocidad por IP para el DNS en el VA.
- Esta opción no está activada de forma predeterminada y debe configurarse de forma explícita siguiendo las instrucciones que se describen en la documentación de Umbrella.

Monitoreo de VAs sobre SNMP:

- Si supervisa los dispositivos virtuales a través de SNMP, Cisco Umbrella recomienda utilizar SNMPv3 con autenticación y cifrado.
- En la documentación de Umbrella se incluyen instrucciones para el mismo.
- Una vez que habilita el monitoreo SNMP, el puerto 161 en el VA se abre para el tráfico entrante.
- Puede monitorear varios atributos como la CPU, la carga y la memoria en el VA a través de SNMP.

Uso de la integración de Cisco AD con las AV:

- Si utiliza los VA con la integración de Cisco Umbrella Active Directory, se recomienda ajustar (o ajustar) la duración de la caché del usuario en el VA para que coincida con el tiempo de concesión de DHCP.
- Consulte las instrucciones del dispositivo virtual: Ajustando la documentación de Configuración de efectivo del usuario. Esto minimiza el riesgo de que las atribuciones del usuario sean incorrectas.

Configuración del registro de auditoría:

- El VA mantiene un registro de auditoría de todos los cambios de configuración ejecutados en el VA.
- Puede configurar el registro remoto de este registro de auditoría en un servidor syslog según las instrucciones de la documentación de Umbrella.

Configuración de VA:

- Se deben configurar al menos dos AV por sitio de Umbrella y la dirección IP de estas dos AV se puede distribuir como servidores DNS a los terminales.
- Para obtener una redundancia adicional, puede configurar el direccionamiento de difusión ilimitada en el dispositivo virtual. Esto permite que varios dispositivos virtuales compartan una sola dirección de difusión de contenido.
- De manera eficaz, puede implementar varios AV mientras sigue distribuyendo solo dos IP de servidor DNS en cada terminal. Si falla cualquier VA, Anycast garantiza que las consultas DNS se enruten al otro VA que comparte la misma IP Anycast.
- Más información sobre los pasos para configurar Anycast en el dispositivo virtual.

Configuración de Cisco Umbrella Active Directory Connector

Creación de un nombre de cuenta personalizado:

- Una de las prácticas recomendadas para Cisco Umbrella AD Connector es utilizar un nombre de cuenta personalizado en lugar del OpenDNS_Connector predeterminado.
- Esta cuenta se puede crear antes de la implementación del conector y se le conceden los permisos necesarios.
- Es necesario especificar el nombre de cuenta como parte de la instalación del conector.

Configuración de LDAPS con el Conector AD:

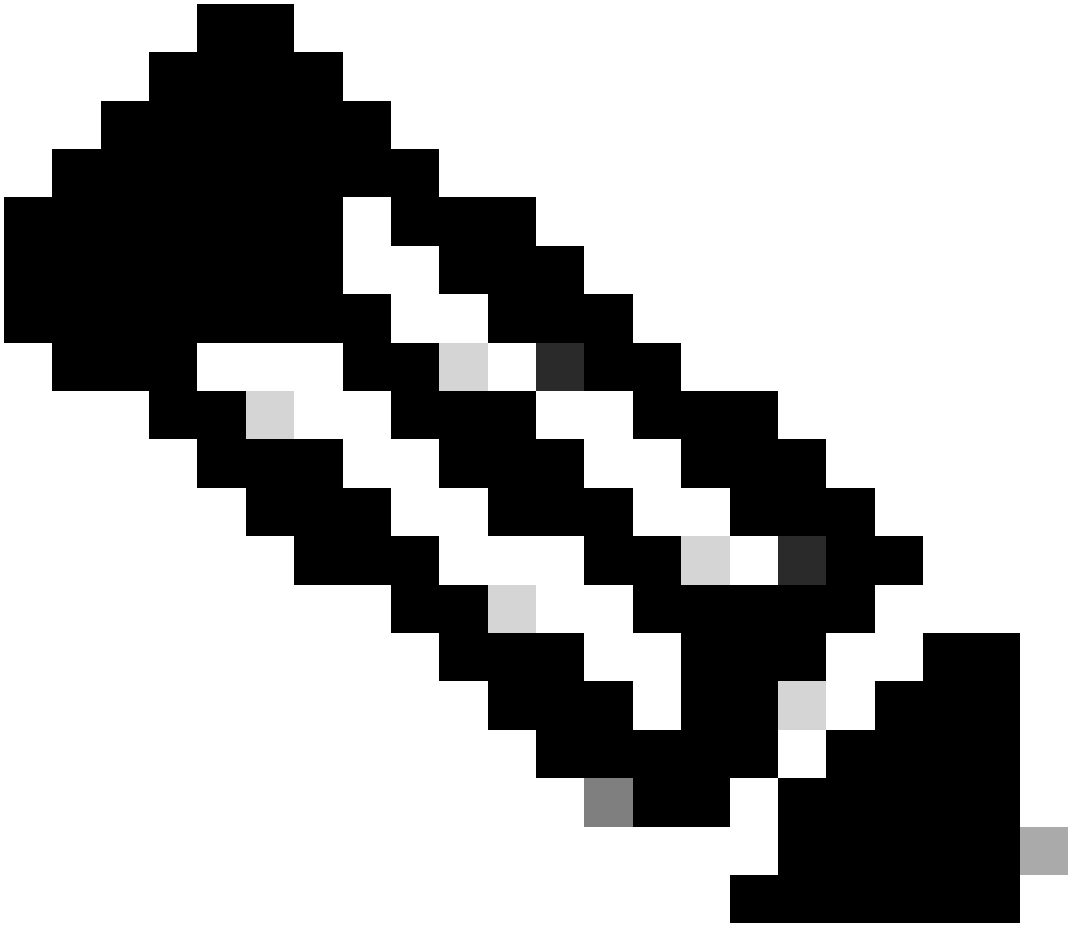
- El conector de Umbrella AD intenta recuperar la información del grupo de usuarios sobre LDAPS (datos transmitidos a través de un canal seguro), a falta de lo cual cambia a LDAP sobre Kerberos (cifrado de nivel de paquete) o a LDAP sobre NTLM (solo autenticación, sin cifrado) en ese orden.
- Cisco Umbrella recomienda configurar LDAPS en los controladores de dominio para que el conector pueda recuperar esta información a través de un canal cifrado.

Administración del archivo .ldif:

- El conector, de forma predeterminada, almacena los detalles de los usuarios y grupos recuperados de los controladores de dominio en un archivo .ldif localmente.
- Dado que puede tratarse de información confidencial almacenada en texto sin formato, puede restringir el acceso al servidor que ejecuta el conector.
- También puede optar por no almacenar los archivos .ldif localmente en el momento de la instalación.

Configuración de puertos:

- Dado que el conector es un servicio de Windows, no habilita ni deshabilita ningún puerto en el equipo host. Cisco Umbrella recomienda ejecutar el servicio Cisco Umbrella AD Connector en un servidor Windows dedicado.
- Al igual que el VA, el conector realiza consultas salientes sobre puertos/protocolos específicos a los destinos mencionados en la documentación de Umbrella. Cisco Umbrella recomienda configurar reglas en el firewall para bloquear el tráfico desde los conectores a todos los demás destinos.



Nota: Toda la comunicación HTTPS hacia/desde el conector ocurre solamente sobre TLS 1.2. No se utilizan protocolos más antiguos.

Administración de la contraseña del conector:

- Cisco recomienda girar la contraseña del conector periódicamente.
- Esto se puede hacer cambiando la contraseña de la cuenta del conector en Active Directory y luego actualizando la contraseña usando la herramienta "PasswordManager" en la carpeta del conector.

Recibiendo mapeos IP de usuario:

- De forma predeterminada, el conector comunica la IP privada.
- AD envía asignaciones de usuario al VA sobre texto sin formato.
- Puede optar por configurar el dispositivo virtual y el conector para que se comuniquen a través de un canal cifrado según las instrucciones que se describen en este artículo de la base de conocimientos.

Administración de certificados:

- La gestión y revocación de certificados están fuera del alcance del VA y usted es responsable de garantizar que el certificado/cadena de certificados más reciente esté presente en el VA y el conector, según corresponda.
- Configurar un canal cifrado para esta comunicación afecta al rendimiento del dispositivo virtual y del conector.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).