Configuración del firewall para el dispositivo web seguro

Contenido

Introducción

Este documento describe los puertos que deben estar abiertos para el funcionamiento de Cisco Secure Web Appliance (SWA).

Prerequisites

Conocimiento general del protocolo de control de transmisión/protocolo de Internet (TCP/IP).

Comprender las diferencias y comportamientos del protocolo de control de transmisión (TCP) y del protocolo de datagramas de usuario (UDP).

Reglas de firewall

La tabla enumera los puertos posibles que se necesitan abrir para el funcionamiento correcto de Cisco SWA.

Nota: Los números de puerto son todos valores por defecto; si se ha modificado alguno de ellos, tenga en cuenta el nuevo valor.

Puerto predeterminado	Protocolo	InBound/OutBound	Nombre del host	Propósito
20 21	TCP	InBound o OutBound	IP de administración de AsyncOS (entrante) servidor FTP (saliente)	Protocolo de transferencia de archivos (FTP) para agregar archivos de registro. Puertos de datos TCP

				1024 y superiores también debe estar abierto
22	TCP	Entrantes	IP de administración AsyncOS	Acceso mediante el protocolo Secure Shell (SSH) al protocolo Secure Shell (SSH), Agregación de archivos de registro
22	TCP	Salientes	Servidor SSH	Agregación SSH de archivos de registro. Transferencia de protocolo de copia segura (SCP) al servidor de registro.
25	TCP	Salientes	IP de servidor de protocolo simple de transferencia de correo (SMTP)	Enviar alertas por correo electrónico
53	UDP	Salientes	Servidores del Sistema de nombres de dominio (DNS)	DNS si se configura para utilizar Internet servidores raíz u otros servidores DNS fuera del firewall. También para consultas de

				SenderBase.
8080	TCP	Entrantes	Dirección IP de administración de AsyncOS	Acceso mediante el protocolo de transferencia de hipertexto (HTTP) a la interfaz gráfica de usuario (GUI)
8443	TCP	Entrantes	Dirección IP de administración de AsyncOS	Acceso seguro al protocolo de transferencia de hipertexto (HTTP) a la interfaz gráfica de usuario
80 443	TCP	Salientes	downloads.ironport.com	Definiciones de McAfee
80 443	TCP	Salientes	updates.ironport.com	Actualizaciones de AsyncOS y definiciones de McAfee
88	TCP y UDP	Salientes	Centro de distribución de claves Kerberos (KDC) / Servidor de dominio de Active Directory	Autenticación Kerberos
88	UDP	Entrantes	Centro de distribución de claves Kerberos (KDC) / Servidor de dominio de Active Directory	Autenticación Kerberos
445	TCP	Salientes	Microsoft SMB	Dominio de autenticación de Active

				Directory (NTLMSSP y Basic)
389	TCP y UDP	Salientes	Servidor LDAP (protocolo ligero de acceso a directorios)	Autenticación LDAP
3268	TCP	Salientes	Catálogo global de LDAP (GC)	LDAP GC
636	TCP	Salientes	LDAP sobre capa de conexión segura (SSL)	SSL LDAP
3269	TCP	Salientes	LDAP GC sobre SSL	LDAP GC SSL
135	TCP	InBound y OutBound	Resolución de terminales: mapeo de puertos Puerto fijo de Net Log-on	Resolución de terminal
161 162	UDP	Salientes	Servidor con protocolo simple de administración de red (SNMP)	Consultas SNMP
161	UDP	Entrantes	IP de administración AsyncOS	Trampas del protocolo SNMP
123	UDP	Salientes	Servidor de protocolo de tiempo de la red (NTP)	sincronización de hora NTP
443	TCP	Salientes	update-manifests.ironport.com	Obtener la lista de los archivos más recientes desde el servidor de actualización (para hardware físico)

443	TCP	Salientes	update-manifests.sco.cisco.com	Obtener la lista de los archivos más recientes desde el servidor de actualización (para hardware virtual)
443	TCP	Salientes	regsvc.sco.cisco.com est.sco.cisco.com updates-talos.sco.cisco.com updates.ironport.com serviceconfig.talos.cisco.com grpc.talos.cisco.com IPv4 146.112.62.0/24 146.112.63.0/24 146.112.255.0/24 146.112.59.0/24 IPv6 2a04:e4c7:ffff::/48 2a04:e4c7:fffe::/48	Cisco Talos Intelligence Services Obtenga datos de reputación y categoría de Localizador uniforme de recursos (URL).
443	TCP	Salientes	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com	Nube pública de protección frente a malware avanzado (AMP)
443	TCP	Salientes	panacea.threatgrid.com panacea.threatgrid.eu	Para Secure Malware Analytics Portal y dispositivos integrados
80 3128	TCP	Entrantes	Clientes proxy	Conectividad predeterminada de clientes con proxy

				HTTP/HTTPS
80 443	TCP	Salientes	Gateway predeterminado	Tráfico de salida de proxy HTTP y HTTPS
514	UDP	Salientes	servidor Syslog	Servidor Syslog para recopilar registros
990	TCP	Salientes	cxd.cisco.com	Para cargar los registros de depuración que son recopilado por el equipo de colaboración de asistencia técnica de Cisco (TAC). Protocolo de transferencia de archivo de SSL (FTPS) implícito.
21	TCP	Salientes	cxd.cisco.com	Para cargar los registros de depuración que son recopilados por el TAC de Cisco. FTPS explícito o FTP
443	TCP	Salientes	cxd.cisco.com	Para cargar los registros de depuración que son recopilado por

				Cisco TAC a través de HTTPS
22	TCP	Salientes	cxd.cisco.com	Para cargar los registros de depuración que son recopilado por el TAC de Cisco a través de SCP y el protocolo de transferencia de archivos segura (SFTP)
22 25 (Default) 53 80 443 4766	TCP	Salientes	s.tunnels.ironport.com	Acceso remoto al backend
443	TCP	Salientes	smartreceiver.cisco.com	Licencias inteligentes

Referencias

Configurar el firewall para el dominio y las confianzas de AD: Windows Server | Microsoft Learn

Seguridad, acceso a Internet y puertos de comunicación (cisco.com)

IP y puertos necesarios para el análisis seguro de malware - Cisco

Cargas de archivos del cliente al Centro de Asistencia Técnica de Cisco - Cisco

Nota técnica sobre preguntas frecuentes sobre acceso remoto en Cisco ESA/WSA/SMA - Cisco

Descripción general de las licencias inteligentes y prácticas recomendadas para Cisco Email and Web Security (ESA, WSA, SMA) - Cisco

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).