Firewall für sichere Web-Appliance konfigurieren

Inhalt

Einleitung

In diesem Dokument werden die Ports beschrieben, die für den Betrieb der Cisco Secure Web Appliance (SWA) offen sein müssen.

Voraussetzungen

Allgemeine Kenntnisse des Transmission Control Protocol/Internet Protocol (TCP/IP).

Kenntnis der Unterschiede und Verhaltensweisen beim Transmission Control Protocol (TCP) und User Datagram Protocol (UDP)

Firewall-Regeln

In der Tabelle sind mögliche Ports aufgeführt, die zum ordnungsgemäßen Betrieb der Cisco SWA geöffnet werden müssen.

> **Hinweis**: Portnummern sind alle Standardwerte. Wenn eine dieser Werte geändert wurde, berücksichtigen Sie den neuen Wert.

Standard-Port	**Protokolle**	**Ein-/Ausgehend**	**Host-Name**	**Zweck**
20 21	TCP	InBound oder OutBound	AsyncOS Management-IP (eingehend) FTP-Server (ausgehend)	File Transfer Protocol (FTP) für die Aggregation von Protokolldateien. Datenports TCP 1024 und höher muss auch offen sein
22	TCP	InBound	AsyncOS Management-IP	Zugang zum Secure Shell Protocol (SSH), Aggregation von Protokolldateien

22	TCP	OutBound	SSH-Server	SSH-Aggregation von Protokolldateien. Secure Copy Protocol (SCP)-Push an Protokollserver.
25	TCP	OutBound	Simple Mail Transfer Protocol (SMTP) Server-IP	Benachrichtigungen per E-Mail senden
53	UDP	OutBound	DNS-Server (Domain Name System)	DNS, falls für die Verwendung des Internets konfiguriert Stammserver oder andere DNS-Server außerhalb der Firewall. Auch für SenderBase-Abfragen.
8080	TCP	InBound	AsyncOS Management-IP-Adresse	Hypertext Transfer Protocol (HTTP)-Zugriff auf die grafische Benutzeroberfläche (GUI)
8443	TCP	InBound	AsyncOS Management-IP-Adresse	HTTP-Zugriff (Hypertext Transfer Protocol Secure) auf GUI
80 443	TCP	OutBound	downloads.ironport.com	McAfee-Definitionen
80 443	TCP	OutBound	updates.ironport.com	AsyncOS-Upgrades und McAfee-Definitionen
88	TCP und UDP	OutBound	Kerberos Key Distribution Center (KDC)/Active Directory-Domänenserver	Kerberos-Authentifizierung

88	UDP	InBound	Kerberos Key Distribution Center (KDC)/Active Directory-Domänenserver	Kerberos-Authentifizierung
389	TCP und UDP	OutBound	LDAP-Server (Lightweight Directory Access Protocol)	LDAP-Authentifizierung
3268	TCP	OutBound	Globaler LDAP-Katalog (GC)	LDAP-GC
636	TCP	OutBound	LDAP über Secure Sockets Layer (SSL)	LDAP-SSL
3269	TCP	OutBound	LDAP GC über SSL	LDAP-GC-SSL
135	TCP	InBound und OutBound	Endpunktauflösung - Port Mapper Fester Net Log-on-Port	Endpunktauflösung
161 162	UDP	OutBound	Simple Network Management Protocol (SNMP)-Server	SNMP-Abfragen
161	UDP	InBound	AsyncOS Management-IP	SNMP-Traps
123	UDP	OutBound	Network Time Protocol (NTP)-Server	NTP-Zeitsynchronisierung
443	TCP	OutBound	update-manifests.ironport.com	Abrufen der Liste der neuesten Dateien vom Update-Server (für physische Hardware)
443	TCP	OutBound	update-manifests.sco.cisco.com	Abrufen der Liste der neuesten Dateien vom Update-Server (für virtuelle Hardware)

443	TCP	OutBound	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 Abrufen von URL-Kategorie- und Reputationsdaten
443	TCP	OutBound	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com	Advanced Malware Protection (AMP) Public Cloud
443	TCP	OutBound	panacea.threatgrid.com panacea.bedrohgrid.eu	Für Secure Malware Analytics-Portal und integrierte Geräte
80 3128	TCP	InBound	Proxy-Clients	Verbindung der Standard-Clients mit dem HTTP/HTTPS-Proxy
80 443	TCP	OutBound	Default gateway (Standardgateway)	HTTP- und HTTPS-Proxy-Datenverkehr ausgehend
514	UDP	OutBound	Syslog-Server	Syslog-Server zum Erfassen von Protokollen
990	TCP	OutBound	cxd.cisco.com	So laden Sie die Debug-Protokolle hoch, die erfasst vom Cisco Technical Assistance Collaborative (TAC). File Transfer Protocol über SSL (FTPS)

				implizit.
21	TCP	OutBound	cxd.cisco.com	So laden Sie die Debug-Protokolle hoch, die vom Cisco TAC abgeholt. FTPS Explizit oder FTP
443	TCP	OutBound	cxd.cisco.com	So laden Sie die Debug-Protokolle hoch, die erfasst von Cisco TAC über HTTPS
22	TCP	OutBound	cxd.cisco.com	So laden Sie die Debug-Protokolle hoch, die vom Cisco TAC über SCP und Secure File Transfer Protocol (SFTP) erfasst
22 25 (Standard) 53 80 443 4766	TCP	OutBound	s.tunnels.ironport.com	Remote-Zugriff auf das Backend
443	TCP	OutBound	smartreceiver.cisco.com	smart licensing

Referenzen

Konfigurieren der Firewall für die AD-Domäne und Vertrauenswürdigkeit - Windows Server | Microsoft - Lernen

Sicherheits-, Internetzugriffs- und Kommunikationsports (cisco.com)

Erforderliche IP-Adressen und Ports für sichere Malwareanalysen - Cisco

Kundendateien werden an das Cisco Technical Assistance Center (TAC) hochgeladen

Technische Informationen zu FAQs für Remote-Zugriff auf Cisco ESA/WSA/SMA - Cisco

Smart Licensing - Überblick und Best Practices für Cisco Email und Web Security (ESA, WSA, SMA) - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.