Configurare il firewall per Secure Web Appliance

Sommario

Introduzione

In questo documento vengono descritte le porte che devono essere aperte per il funzionamento di Cisco Secure Web Appliance (SWA).

Prerequisiti

Conoscenze generali di TCP/IP (Transmission Control Protocol/Internet Protocol).

Comprendere le differenze e i comportamenti tra i protocolli TCP (Transmission Control Protocol) e UDP (User Datagram Protocol).

Regole firewall

Nella tabella vengono elencate le porte possibili che devono essere aperte per il corretto funzionamento di Cisco SWA.

Nota: i numeri di porta sono valori predefiniti. Se sono stati modificati, considerare il nuovo valore.

Porta predefinita	Protocollo	InBound/OutBound	Nome host	Scopo
20 21	TCP	InBound o OutBound	IP di gestione AsyncOS. (in entrata) Server FTP (in uscita)	Protocollo FTP (File Transfer Protocol) per l'aggregazione dei file di registro. Porte dati TCP 1024 e versioni successive deve inoltre essere aperto
22	TCP	InBound	IP gestione AsyncOS	accesso SSH (Secure Shell Protocol) al protocollo SSH

				(Secure Shell Protocol), Aggregazione dei file di log
22	TCP	Uscita	Server SSH	Aggregazione SSH dei file di log. Push del protocollo SCP (Secure Copy Protocol) nel server di registro.
25	TCP	Uscita	IP server SMTP (Simple Mail Transfer Protocol)	Invia avvisi tramite posta elettronica
53	UDP	Uscita	Server DNS (Domain Name System)	DNS se configurato per l'utilizzo di Internet server radice o altri server DNS fuori dal firewall. Anche per le query SenderBase.
8080	TCP	InBound	Indirizzo IP gestione AsyncOS	Accesso HTTP (Hypertext Transfer Protocol) all'interfaccia utente grafica
8443	TCP	InBound	Indirizzo IP gestione AsyncOS	Accesso HTTP (Hypertext Transfer Protocol Secure) alla GUI
80	TCP	Uscita	downloads.ironport.com	Definizioni

443				McAfee
80 443	TCP	Uscita	updates.ironport.com	Aggiornamenti AsyncOS e definizioni McAfee
88	TCP E UDP	Uscita	Centro distribuzione chiavi Kerberos (KDC) / Server di dominio Active Directory	Autenticazione Kerberos
88	UDP	InBound	Centro distribuzione chiavi Kerberos (KDC) / Server di dominio Active Directory	Autenticazione Kerberos
389	TCP E UDP	Uscita	Server LDAP (Lightweight Directory Access Protocol)	Autenticazione LDAP
3268	TCP	Uscita	Catalogo globale LDAP (GC)	GC LDAP
636	TCP	Uscita	LDAP su SSL (Secure Sockets Layer)	SSL LDAP
3269	TCP	Uscita	GC LDAP su SSL	SSL GC LDAP
135	TCP	InBound e OutBound	Risoluzione del punto finale - Port Mapper Porta fissa di accesso rete	Risoluzione del punto finale
161 162	UDP	Uscita	Server SNMP (Simple Network Management Protocol)	Query SNMP
161	UDP	InBound	IP gestione AsyncOS	Trap SNMP
123	UDP	Uscita	Server Network Time Protocol (NTP)	Sincronizzazione ora NTP

443	TCP	Uscita	update-manifests.ironport.com	Ottenere l'elenco dei file più recenti dal server di aggiornamento (per hardware fisico)
443	TCP	Uscita	update-manifests.sco.cisco.com	Ottenere l'elenco dei file più recenti dal server di aggiornamento (per hardware virtuale)
443	TCP	Uscita	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: 1000/48	Cisco Talos Intelligence Services Ottenere la categoria URL (Uniform Resource Locator) e i dati sulla reputazione.
443	TCP	Uscita	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com	Advanced Malware Protection (AMP) Public Cloud
443	TCP	Uscita	panacea.threatgrid.com panacea.threat.eu	Per il portale di analisi sicura dei malware e i dispositivi integrati
80	TCP	InBound	Client Proxy	Connettività

3128				predefinita dei client al proxy HTTP/HTTPS
80 443	TCP	Uscita	Gateway predefinito	Traffico proxy HTTP e HTTPS in uscita
514	UDP	Uscita	Server Syslog	Server Syslog per la raccolta dei log
990	TCP	Uscita	cxd.cisco.com	Per caricare i log di debug raccolti da Cisco Technical Assistance Collaborative (TAC). FTPS (File Transfer Protocol of SSL) Implicit.
21	TCP	Uscita	cxd.cisco.com	Per caricare i log di debug raccolti da Cisco TAC. FTPS Explicit o FTP
443	TCP	Uscita	cxd.cisco.com	Per caricare i log di debug raccolti da Cisco TAC su HTTPS
22	TCP	Uscita	cxd.cisco.com	Per caricare i log di debug raccolti da Cisco TAC over SCP e Secure File Transfer Protocol (SFTP)

22 25 (Predefinito) 53 80 443 4766	TCP	Uscita	s.tunnels.ironport.com	Accesso remoto al back-end
443	TCP	Uscita	smartreceiver.cisco.com	licenze smart

Riferimenti

Configurare il firewall per il dominio Active Directory e i trust - Windows Server | Microsoft Learn

Porte di sicurezza, accesso a Internet e di comunicazione (cisco.com)

IP e porte necessarie per Secure Malware Analytics - Cisco

Caricamento di file die clienti su Cisco Technical Assistance Center - Cisco

Nota tecnica sulle domande frequenti (FAQ) sull'accesso remoto su Cisco ESA/WSA/SMA - Cisco

Panoramica delle licenze Smart e best practice per Cisco Email and Web Security (ESA, WSA, SMA) - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).