Configurer le pare-feu pour l'appliance Web sécurisée

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Règles de pare-feu](#)

[Autres informations utiles](#)

Introduction

Ce document décrit les ports qui doivent être ouverts pour le fonctionnement de Cisco Secure Web Appliance (SWA)

Conditions préalables

Une connaissance générale du protocole TCP/IP (Transmission Control Protocol/Internet Protocol) est recommandée.

Comprendre les différences et les comportements des protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

Règles de pare-feu

Le tableau répertorie les ports possibles qui doivent être ouverts pour que Cisco SWA fonctionne correctement.

Remarque : Les numéros de port sont tous des valeurs par défaut. Si l'une d'entre elles a été modifiée, utilisez la valeur de port mise à jour.

Port par défaut	Protocol	Entrant/Sortant	Nom de domaine complet (FQDN)	Objectif

20 21	TCP	EntrantLié ou SortantLié	IP de gestion AsyncOS (entrant) Serveur FTP (sortant)	Protocole FTP (File Transfer Protocol) pour l'agrégation des fichiers journaux. Ports de données TCP 1024 et supérieurs doit également être ouvert
22	TCP	Entrant	IP de gestion AsyncOS	accès SSH (Secure Shell Protocol) au protocole SSH (Secure Shell Protocol), Agrégation des fichiers journaux
22	TCP	Sortant	Serveur SSH	Agrégation SSH des fichiers journaux. Diffusion SCP (Secure Copy Protocol) vers le serveur de journalisation.
25	TCP	Sortant	Adresse IP du serveur SMTP (Simple Mail Transfer Protocol)	Envoyer des alertes par e-mail
53	UDP	Sortant	Serveurs DNS (Domain Name System)	DNS si configuré pour utiliser Internet Serveurs racine ou autres serveurs DNS en dehors du pare-feu. Également pour les requêtes SenderBase.
8080	TCP	Entrant	Adresse IP de gestion	Accès HTTP

			AsyncOS	(Hypertext Transfer Protocol) à l'interface graphique utilisateur (GUI)
8443	TCP	Entrant	Adresse IP de gestion AsyncOS	Accès HTTPS (Hypertext Transfer Protocol Secure) à l'interface utilisateur graphique
80 443	TCP	Sortant	downloads.ironport.com	Définitions McAfee
80 443	TCP	Sortant	updates.ironport.com	Mises à niveau AsyncOS et définitions McAfee
88	TCP et UDP	Sortant	Centre de distribution de clés Kerberos (KDC) / serveur de domaine Active Directory	Authentification Kerberos
88	UDP	Entrant	Centre de distribution de clés Kerberos (KDC) / serveur de domaine Active Directory	Authentification Kerberos
445	TCP	Sortant	Microsoft PME	Domaine d'authentification Active Directory (NTLMSSP et Basic)
389	TCP et UDP	Sortant	Serveur LDAP (Lightweight Directory Access Protocol)	Authentification LDAP
3268	TCP	Sortant	Catalogue global LDAP (GC)	catalogue global LDAP
636	TCP	Sortant	LDAP sur SSL (Secure Sockets Layer)	SSL LDAP

3269	TCP	Sortant	LDAP GC sur SSL	SSL du catalogue global LDAP
135	TCP	EntrantLié et sortantLié	Résolution des points d'extrémité - Mappeur de ports Port fixe de connexion réseau	Résolution des points d'extrémité
161 162	UDP	Sortant	Serveur SNMP (Simple Network Management Protocol)	Requêtes SNMP
161	UDP	Entrant	IP de gestion AsyncOS	Déroutements SNMP
123	UDP	Sortant	Serveur NTP (Network Time Protocol)	Synchronisation de l'heure NTP
443	TCP	Sortant	update-manifests.ironport.com	Obtenir la liste des derniers fichiers à partir du serveur de mise à jour (pour le matériel physique)
443	TCP	Sortant	update-manifests.sco.cisco.com	Obtenir la liste des derniers fichiers à partir du serveur de mise à jour (pour le matériel virtuel)
443	TCP	Sortant	regsvc.sco.cisco.com est.sco.cisco.com updates-talos.sco.cisco.com updates.ironport.com serviceconfig.talos.cisco.com grpc.talos.cisco.com	Cisco Talos Intelligence Services Obtenir la catégorie Uniform Resource Locator (URL) et les

			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	données de réputation.
443	TCP	Sortant	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com api.amp.cisco.com api.amp.sourcefire.com	Cloud public AMP (Advanced Malware Protection)
443	TCP	Sortant	AMÉRIQUE api-sse.cisco.com mx01.sse.itd.cisco.com dex.sse.itd.cisco.com EUROPE api.eu.sse.itd.cisco.com mx01.eu.sse.itd.cisco.com dex.eu.sse.itd.cisco.com ASIE/PACIFIQUE api.apj.sse.itd.cisco.com mx01.apj.sse.itd.cisco.com dex.apj.sse.itd.cisco.com	Services cloud Cisco sur l'appliance Web sécurisée. Les URL requises sont différentes selon la région Serveurs cloud sécurisés.
443	TCP	Sortant	panacea.threatgrid.com panacea.threat.eu	Pour le portail Secure Malware Analytics et les périphériques intégrés
80 3128	TCP	Entrant	Clients proxy	Connectivité client par défaut au proxy HTTP/HTTPS
80 443	TCP	Sortant	Passerelle par défaut	Trafic sortant du proxy HTTP et

				HTTPS
514	UDP	Sortant	Syslog Server (Serveur de journal système)	Serveur Syslog pour collecter les journaux
990	TCP	Sortant	cxd.cisco.com	Pour télécharger les journaux de débogage qui sont collectées par le centre d'assistance technique collaboratif (TAC) de Cisco. Protocole de transfert de fichier de SSL (FTPS) implicite.
21	TCP	Sortant	cxd.cisco.com	Pour télécharger les journaux de débogage qui sont collectées par le TAC Cisco. FTPS Explicit ou FTP
443	TCP	Sortant	cxd.cisco.com	Pour télécharger les journaux de débogage qui sont collectés par le TAC Cisco sur HTTPS
22	TCP	Sortant	cxd.cisco.com	Pour télécharger les journaux de débogage qui sont collectées par le TAC Cisco sur SCP et le protocole SFTP (Secure File Transfer Protocol)

22 25 (par défaut) 53 80 443 4766	TCP	Sortant	s.tunnels.ironport.com	Accès à distance au service principal
443	TCP	Sortant	smartreceiver.cisco.com	Licences Smart

Autres informations utiles

- Configurer le pare-feu pour le domaine Active Directory et les approbations - Windows Server | Microsoft Learn
- Ports de sécurité, d'accès à Internet et de communication - Cisco
- IP et ports requis pour l'analyse sécurisée des programmes malveillants - Cisco
- Téléversement de fichiers des clients au Cisco Technical Assistance Center (TAC, Centre d’assistance technique de Cisco) – Cisco
- Note technique sur les questions fréquentes relatives à l'accès à distance sur Cisco ESA/WSA/SMA - Cisco
- Présentation des licences Smart et meilleures pratiques pour la sécurité de la messagerie électronique et du web Cisco (ESA, WSA, SMA) - Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.