Configure Firewall for Secure Web Appliance

Contents

Introduction

This document describes ports that are needed to be open for operation of Cisco Secure Web Appliance (SWA).

Prerequisites

General Knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP).

Understand Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) differences and behaviours.

Firewall Rules

The table lists possible ports that are needed to be opened for the proper operation of Cisco SWA.

Note: Port numbers are all default values, if any of them have been changed, consider the new value.

Default port	Protocol	InBound/OutBound	Host name	Purpose
20 21	TCP	InBound or OutBound	AsyncOS Management IP. (inbound) FTP server (outbound)	File Transfer Protocol (FTP) for aggregation of log files. Data ports TCP 1024 and higher must also be open
22	TCP	InBound	AsyncOS Management IP	Secure Shell Protocol (SSH) access to the Secure Shell Protocol (SSH), Aggregation of log files

22	TCP	OutBound	SSH Server	SSH aggregation of log files. Secure copy protocol (SCP) push to log server.
25	TCP	OutBound	Simple Mail Transfer Protocol (SMTP) server IP	Send alerts via Email
53	UDP	OutBound	Domain Name System (DNS) servers	DNS if configured to use Internet root servers or other DNS servers outside the firewall. Also for SenderBase queries.
8080	TCP	InBound	AsyncOS Management IP address	Hypertext Transfer Protocol (HTTP) access to the Graphical User Interface (GUI)
8443	TCP	InBound	AsyncOS Management IP address	Hypertext Transfer Protocol Secure (HTTPs) access to GUI
80 443	TCP	OutBound	downloads.ironport.com	McAfee definitions
80 443	TCP	OutBound	updates.ironport.com	AsyncOS upgrades and McAfee definitions
88	TCP & UDP	OutBound	Kerberos Key Distribution	Kerberos

			Center (KDC) / Active Directory Domain Server	Authentication
88	UDP	InBound	Kerberos Key Distribution Center (KDC) / Active Directory Domain Server	Kerberos Authentication
445	TCP	OutBound	Microsoft SMB	Active Directory authentication realm (NTLMSSP and Basic)
389	TCP & UDP	OutBound	Lightweight Directory Access Protocol (LDAP) Server	LDAP Authentication
3268	TCP	OutBound	LDAP Global Catalog (GC)	LDAP GC
636	TCP	OutBound	LDAP over Secure Sockets Layer (SSL)	LDAP SSL
3269	TCP	OutBound	LDAP GC over SSL	LDAP GC SSL
135	TCP	InBound & OutBound	End-point resolution - Port Mapper Net Log-on fixed port	End-point Resolution
161 162	UDP	OutBound	Simple Network Management Protocol (SNMP) Server	SNMP Queries
161	UDP	InBound	AsyncOS Management IP	SNMP Traps
123	UDP	OutBound	Network Time Protocol (NTP) server	NTP time synchronization
443	TCP	OutBound	update-manifests.ironport.com	Obtain the list of the latest files from the update server (for physical

				hardware)
443	TCP	OutBound	update-manifests.sco.cisco.com	Obtain the list of the latest files from the update server (for virtual 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 Obtain Uniform Resource Locator (URL) category and reputation data.
443	TCP	OutBound	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com	Advance Malware Protection (AMP) Public Cloud
443	TCP	OutBound	panacea.threatgrid.com panacea.threatgrid.eu	For Secure Malware Analytics Portal and Integrated Devices
80 3128	TCP	InBound	Proxy Clients	Default Clients connectivity to HTTP/HTTPS Proxy
80 443	TCP	OutBound	Default gateway	HTTP and HTTPS Proxy Traffic Out

514	UDP	OutBound	Syslog server	Syslog server to collect logs
990	TCP	OutBound	cxd.cisco.com	To upload the debug logs that are collected by Cisco Technical Assistance Collaborative (TAC). File Transfer Protocol of SSL (FTPS) Implicit.
21	TCP	OutBound	cxd.cisco.com	To upload the debug logs that are collected by Cisco TAC. FTPS Explicit or FTP
443	TCP	OutBound	cxd.cisco.com	To upload the debug logs that are collected by Cisco TAC over HTTPS
22	TCP	OutBound	cxd.cisco.com	To upload the debug logs that are collected by Cisco TAC over SCP and Secure File Transfer Protocol (SFTP)
22 25 (Default) 53 80 443 4766	TCP	OutBound	s.tunnels.ironport.com	Remote access to backend

443	TCP	OutBound	smartreceiver.cisco.com	smart licensing

References

Configure firewall for AD domain and trusts - Windows Server | Microsoft Learn

Security, Internet Access, and Communication Ports (cisco.com)

Required IP and Ports for Secure Malware Analytics - Cisco

Customer File Uploads to Cisco Technical Assistance Center - Cisco

Technote on FAQ for Remote Access on Cisco ESA/WSA/SMA - Cisco

Smart Licensing Overview and Best Practices for Cisco Email and Web Security (ESA, WSA, SMA) - Cisco