

Firewall voor beveiligde web applicatie configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Firewallregels](#)

[Referenties](#)

Inleiding

Dit document beschrijft poorten die open moeten zijn voor gebruik van Cisco Secure Web Applicatie (SWA).

Voorwaarden

Algemene kennis van TCP/IP (Transmission Control Protocol/Internet Protocol).

Begrijp verschillen en gedrag in Transmission Control Protocol (TCP) en User Datagram Protocol (UDP).

Firewallregels

De tabel vermeldt mogelijke poorten die moeten worden geopend voor een juiste werking van Cisco SWA.

Opmerking: poortnummers zijn alle standaardwaarden. Als een van deze waarden is gewijzigd, overweeg dan de nieuwe waarde.

Standaard poort	Protocol	In-/uitgaand	Hostnaam	Doel
20 21	TCP	In- of uitgaand	AsyncOS-beheer voor IP. (inkomend) FTP-server (uitgaand)	File Transfer Protocol (FTP) voor aggregatie van logbestanden. Gegevenspoorten TCP 1024 en hoger moet ook open zijn
22	TCP	ingebonden	AsyncOS-beheer voor IP	toegang tot het Secure Shell-protocol (SSH) (Secure Shell Protocol) (SSH); Aggregatie van logbestanden

22	TCP	Uitgaand	SSH-server	SSH-aggregatie van logbestanden. Secure Copy Protocol (SCP) - push naar logserver.
25	TCP	Uitgaand	Simple Mail Transfer Protocol (SMTP)-server IP	Verzend berichten via e-mail
53	UDP	Uitgaand	Domain Name System-servers (DNS)	DNS indien geconfigureerd voor gebruik van internet basisservers of andere DNS-servers buiten de firewall. Ook voor SenderBase-vragen.
8080	TCP	ingebonden	AsyncOS-beheer voor IP-adres	HTTP-toegang (Hypertext Transfer Protocol) tot de grafische gebruikersinterface (GUI)
8443	TCP	ingebonden	AsyncOS-beheer voor IP-adres	Toegang tot GUI met Hypertext Transfer Protocol Secure (HTTP)
80 443	TCP	Uitgaand	downloads.ironport.com	McAfee-definities
80 443	TCP	Uitgaand	updates.ironport.com	AsyncOS-upgrades en McAfee-definities
88	TCP- EN UDP- protocollen	Uitgaand	Kerberos Key Distribution Center (KDC) / Active Directory-domeinserver	Kerberos-verificatie
88	UDP	ingebonden	Kerberos Key Distribution	Kerberos-verificatie

			Center (KDC) / Active Directory-domeinserver	
389	TCP- EN UDP- protocollen	Uitgaand	Lichtgewicht Directory Access Protocol (LDAP)-server	LDAP-verificatie
3268	TCP	Uitgaand	LDAP Global Catalog (GC)	LDAP GC
636	TCP	Uitgaand	LDAP over Secure Sockets Layer (SSL)	LDAP SSL
3269	TCP	Uitgaand	LDAP GC via SSL	LDAP GC-SSL
135	TCP	InBound & OutBound	End-point resolutie - poortadapter Net Log-on vaste poort	Eindpuntresolutie
161 162	UDP	Uitgaand	Simple Network Management Protocol (SNMP)-server	SNMP-vragen
161	UDP	ingebonden	AsyncOS-beheer voor IP	SNMP-traps
123	UDP	Uitgaand	Network Time Protocol (NTP)- server	NTP- tijdsynchronisatie
443	TCP	Uitgaand	update-manifests.ironport.com	Verkrijg de lijst van de recentste bestanden vanaf de updateserver (voor fysieke hardware)
443	TCP	Uitgaand	update-manifests.sco.cisco.com	Verkrijg de lijst van de recentste bestanden vanaf de updateserver (voor virtuele hardware)
443	TCP	Uitgaand	regsvc.sco.cisco.com	Cisco Talos

			<p>est.sco.cisco.com updates-talos.sco.cisco.com updates.ironport.com serviceconfig.talos.cisco.com grpc.talos.cisco.com</p> <p>IPv4 146.112.62.0/24 146.112.63.0/24 146.112.255.0/24 146.112.59.0/24</p> <p>IPv6-server 2a04:e4c7:fff: 00/48 2a04:e4c7:fff: 00/48</p>	<p>Intelligence-services</p> <p>Verkrijg de Uniform Resource Locator (URL) categorie en reputatiegegevens.</p>
443	TCP	Uitgaand	<p>cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com</p>	<p>Advanced Malware Protection (AMP), openbare cloud</p>
443	TCP	Uitgaand	<p>panacea.threatgrid.com panacea.bedreiggrid.eu</p>	<p>Voor Secure Malware Analytics-portal en geïntegreerde apparaten</p>
80 3128	TCP	ingebonden	<p>Proxyclients</p>	<p>Standaard Clients verbinding met HTTP/HTTPS proxy</p>
80 443	TCP	Uitgaand	<p>Standaardgateway</p>	<p>HTTP- en HTTPS-proxyverkeer naar buiten</p>
514	UDP	Uitgaand	<p>Syslog-server</p>	<p>Syslog-server om logbestanden te verzamelen</p>
990	TCP	Uitgaand	<p>cxd.cisco.com</p>	<p>Om de debug-logbestanden te uploaden die verzameld door Cisco Technical Assistance Collaborative (TAC).</p> <p>File Transfer Protocol of SSL (FTPS) Impliciet.</p>

21	TCP	Uitgaand	cxd.cisco.com	Om de debug-logbestanden te uploaden die verzameld door Cisco TAC. FTPS expliciet voor FTP
443	TCP	Uitgaand	cxd.cisco.com	Om de debug-logbestanden te uploaden die verzameld door Cisco TAC via HTTPS
22	TCP	Uitgaand	cxd.cisco.com	Om de debug-logbestanden te uploaden die verzameld door Cisco TAC via SCP en Secure File Transfer Protocol (SFTP)
22 25 (standaard) 53 80 443 4766	TCP	Uitgaand	s.tunnels.ironport.com	Externe toegang tot backend
443	TCP	Uitgaand	smartreceiver.cisco.com	smart licensing

Referenties

[Firewall voor AD domein en trusts configureren - Windows Server | Microsoft Learn](#)

[Beveiligings-, internettoegang- en communicatiepoorten \(cisco.com\)](#)

[Vereiste IP en poorten voor Secure Malware Analytics - Cisco](#)

[Uploaden van klantbestanden naar Cisco Technical Assistance Center - Cisco](#)

[TechNotes over veelgestelde vragen voor toegang op afstand via Cisco ESA/WSA/SMA - Cisco](#)

[Smart Licensing - Overzicht en beste praktijken voor Cisco Email Security en Web Security \(ESA, WSA,](#)

[SMA\) - Cisco](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.