為安全Web裝置配置防火牆

目錄

[簡介](#)

[必要條件](#)

[防火牆規則](#)

[參考資料](#)

簡介

本檔案介紹需要開啟以操作Cisco Secure Web Appliance(SWA)的連線埠。

必要條件

傳輸控制通訊協定/網際網路通訊協定(TCP/IP)的一般知識。

瞭解傳輸控制通訊協定(TCP)和使用者資料包通訊協定(UDP)的差異和行為。

防火牆規則

該表列出了為使Cisco SWA正常運行而需要開啟的可能埠。

注意：埠號都是預設值，如果其中任何值已更改，請考慮新值。

預設埠	通訊協定	InBound/Outbound	主機名	目的
20 21	TCP	InBound或 Outbound	AsyncOS管理IP.（入站） FTP伺服器（出站）	用於聚合日誌檔案的檔案傳輸協定(FTP)。 資料埠TCP 1024及更高版本 也必須開啟
22	TCP	InBound	AsyncOS管理IP	安全殼層通訊協定(SSH)存取安全殼層通訊協定(SSH), 日誌檔案的聚合
22	TCP	外界	SSH伺服器	日誌檔案的SSH聚合。

				安全複製協定(SCP)推入日誌伺服器。
25	TCP	外界	簡易郵件傳輸通訊協定(SMTP)伺服器IP	通過電子郵件傳送警報
53	UDP	外界	網域名稱系統(DNS)伺服器	DNS（如果配置為使用網際網路）根伺服器或其他DNS伺服器防火牆之外。 也適用於SenderBase查詢。
8080	TCP	InBound	AsyncOS管理IP地址	對圖形使用者介面(GUI)的超文本傳輸協定(HTTP)訪問
8443	TCP	InBound	AsyncOS管理IP地址	超文字傳輸通訊協定安全存取(HTTP)GUI
80 443	TCP	外界	downloads.ironport.com	McAfee定義
80 443	TCP	外界	updates.ironport.com	AsyncOS升級和McAfee定義
88	TCP和UDP	外界	Kerberos金鑰發佈中心(KDC)/Active Directory網域伺服器	Kerberos驗證
88	UDP	InBound	Kerberos金鑰發佈中心(KDC)/Active Directory網域伺服器	Kerberos驗證
445	TCP	外界	Microsoft SMB	Active Directory身份驗證領域

				（NTLMSSP和基本）
389	TCP和UDP	外界	輕量型目錄存取通訊協定(LDAP)伺服器	LDAP身份驗證
3268	TCP	外界	LDAP全域性目錄(GC)	LDAP GC
636	TCP	外界	使用安全套接字層(SSL)的LDAP	LDAP SSL
3269	TCP	外界	使用SSL的LDAP GC	LDAP GC SSL
135	TCP	InBound & OutBound	端點解析度 — 連線埠對映器 網路登入固定埠	端點解析度
161 162	UDP	外界	簡易網路管理通訊協定(SNMP)伺服器	SNMP查詢
161	UDP	InBound	AsyncOS管理IP	SNMP陷阱
123	UDP	外界	網路時間協定(NTP)伺服器	NTP時間同步
443	TCP	外界	update-manifests.ironport.com	取得最新檔案的清單從更新伺服器 （用於物理硬體）
443	TCP	外界	update-manifests.sco.cisco.com	取得最新檔案的清單從更新伺服器 （用於虛擬硬體）
443	TCP	外界	regsvc.sco.cisco.com est.sco.cisco.com updates-talos.sco.cisco.com updates.ironport.com serviceconfig.talos.cisco.com	Cisco Talos智慧服務 獲取統一資源定位器(URL)類別和信譽資

			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	料。
443	TCP	外界	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com	高級惡意軟體防護(AMP)公共雲
443	TCP	外界	panacea.threatgrid.com panacea.threatgrid.eu	適用於安全惡意軟體分析門戶和整合裝置
80 3128	TCP	InBound	代理使用者端	預設客戶端連線到HTTP/HTTPS代理
80 443	TCP	外界	預設閘道	HTTP和HTTPS代理流量傳出
514	UDP	外界	系統日誌伺服器	用於收集日誌的系統日誌伺服器
990	TCP	外界	cxd.cisco.com	要上傳以下內容的調試日誌： 思科技術協助合作(TAC)收集。 SSL(FTPS)的檔案傳輸通訊協定隱含。
21	TCP	外界	cxd.cisco.com	要上傳以下內容的調試日誌： 由Cisco TAC收集。

				FTPS顯式或FTP
443	TCP	外界	cxd.cisco.com	要上傳以下內容的調試日誌： 由Cisco TAC通過HTTPS收集
22	TCP	外界	cxd.cisco.com	要上傳以下內容的調試日誌： 由Cisco TAC透過SCP和安全檔案傳輸通訊協定(SFTP)收集
22 25（預設） 53 80 443 4766	TCP	外界	s.tunnels.ironport.com	遠端訪問後端
443	TCP	外界	smartreceiver.cisco.com	智慧型授權

參考資料

為AD域和信任配置防火牆 — Windows Server | Microsoft瞭解

安全、Internet訪問和通訊埠(cisco.com)

安全惡意軟體分析所需的IP和埠 — Cisco

客戶檔案上傳至Cisco技術援助中心 — Cisco

有關思科ESA/WSA/SMA上遠端訪問常見問題的技術說明 — Cisco

思科電郵和網路安全(ESA、WSA、SMA)的智慧許可概述和最佳實踐 — 思科

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。