为安全Web设备配置防火墙

目录

简介

本文档介绍需要打开才能运行思科安全网络设备(SWA)的端口。

先决条件

传输控制协议/Internet协议(TCP/IP)的一般知识。

了解传输控制协议(TCP)和用户数据报协议(UDP)的差异和行为。

防火墙规则

下表列出了为使Cisco SWA正常运行而需要打开的端口。

注意：端口号都是默认值，如果其中任何值已更改，请考虑新值。

默认端口	协议	InBound/Outbound	主机名	目的
20 21	TCP	InBound或 Outbound	AsyncOS管理IP.（入站） FTP服务器（出站）	用于聚合日志文件的文件传输协议(FTP)。 数据端口TCP 1024及更高版本也必须打开
22	TCP	入站	AsyncOS管理IP	安全外壳协议(SSH)访问安全外壳协议(SSH), 日志文件的聚合
22	TCP	出站	SSH服务器	日志文件的SSH聚合。

				安全复制协议(SCP)推送到日志服务器。
25	TCP	出站	简单邮件传输协议(SMTP)服务器IP	通过电子邮件发送警报
53	UDP	出站	域名系统(DNS)服务器	DNS（如果配置为使用互联网）根服务器或其他DNS服务器防火墙外部。 也适用于SenderBase查询。
8080	TCP	入站	AsyncOS管理IP地址	对图形用户界面(GUI)的超文本传输协议(HTTP)访问
8443	TCP	入站	AsyncOS管理IP地址	安全访问GUI的超文本传输协议(HTTP)
80 443	TCP	出站	downloads.ironport.com	McAfee定义
80 443	TCP	出站	updates.ironport.com	AsyncOS升级和McAfee定义
88	TCP和UDP	出站	Kerberos密钥分发中心(KDC)/Active Directory域服务器	Kerberos身份验证
88	UDP	入站	Kerberos密钥分发中心(KDC)/Active Directory域服务器	Kerberos身份验证
445	TCP	出站	Microsoft SMB	Active Directory身份验证领域（NTLMSSP和基本）

389	TCP和UDP	出站	轻量级目录访问协议(LDAP)服务器	LDAP 验证
3268	TCP	出站	LDAP全局目录(GC)	LDAP GC
636	TCP	出站	基于安全套接字层(SSL)的LDAP	LDAP SSL
3269	TCP	出站	基于SSL的LDAP GC	LDAP GC SSL
135	TCP	InBound & OutBound	终端分辨率 — 端口映射器 网络登录固定端口	终端分辨率
161 162	UDP	出站	简单网络管理协议(SNMP)服务器	SNMP查询
161	UDP	入站	AsyncOS管理IP	SNMP 陷阱
123	UDP	出站	网络时间协议(NTP)服务器	NTP时间同步
443	TCP	出站	update-manifests.ironport.com	获取最新文件的列表从更新服务器 （用于物理硬件）
443	TCP	出站	update-manifests.sco.cisco.com	获取最新文件的列表从更新服务器 （对于虚拟硬件）
443	TCP	出站	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	思科Talos智能服务 获取统一资源定位符(URL)类别和信誉数据。

			146.112.63.0/24 146.112.255.0/24 146.112.59.0/24 IPv6 2a04:e4c7:ffff::/48 2a04:e4c7:fffe::/48	
443	TCP	出站	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.am p.cisco.com	高级恶意软件防护(AMP)公共云
443	TCP	出站	panacea.threatgrid.com panacea.threatgrid.eu	用于安全恶意软件分析门户和集成设备
80 3128	TCP	入站	代理客户端	默认客户端连接到HTTP/HTTPS代理
80 443	TCP	出站	默认网关	HTTP和HTTPS代理流量传出
514	UDP	出站	Syslog 服务器	用于收集日志的系统日志服务器
990	TCP	出站	cxd.cisco.com	上传以下调试日志：思科技术支持协作(TAC)收集的数据。 SSL(FTPS)隐式文件传输协议。
21	TCP	出站	cxd.cisco.com	上传以下调试日志：思科TAC收集。 FTPS显式或FTP
443	TCP	出站	cxd.cisco.com	上传以下调试日志：由Cisco TAC通过HTTPS收集

22	TCP	出站	cxd.cisco.com	上传以下调试日志：由Cisco TAC通过SCP和安全文件传输协议(SFTP)收集
22 25 (Default) 53 80 443 4766	TCP	出站	s.tunnels.ironport.com	远程访问后端
443	TCP	出站	smartreceiver.cisco.com	智能许可

参考

为AD域和信任配置防火墙 — Windows Server | Microsoft学习

安全、Internet接入和通信端口(cisco.com)

安全恶意软件分析所需的IP和端口 — 思科

向思科技术支持中心上传客户文件 - 思科

思科ESA/WSA/SMA远程访问常见问题解答技术说明 — 思科

思科电邮与Web安全(ESA、WSA、SMA)智能许可概述和最佳实践 — 思科

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。