Configurar firewall para dispositivo seguro da Web

Contents

[Introdução](#)
[Pré-requisitos](#)
[Regras de firewall](#)
[Referências](#)

Introdução

Este documento descreve as portas que precisam ser abertas para a operação do Cisco Secure Web Appliance (SWA).

Pré-requisitos

Conhecimento Geral do Protocolo TCP/IP.

Entender as diferenças e os comportamentos do Protocolo de Controle de Transmissão (TCP - Transmission Control Protocol) e do Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol).

Regras de firewall

A tabela lista as portas possíveis que precisam ser abertas para a operação adequada do Cisco SWA.

> **Observação**: os números de porta são valores padrão; se algum deles tiver sido alterado, considere o novo valor.

Porta padrão	Protocolo	Entrada/SaídaLigação	Nome do host	Propósito
20 21	TCP	InBound ou OutBound	AsyncOS Management IP (IP de gerenciamento AsyncOS). (entrada) Servidor FTP (saída)	File Transfer Protocol (FTP) para agregação de arquivos de log. Portas de dados TCP 1024 e superior também deve ser aberto
22	TCP	Entrada	IP de gerenciamento AsyncOS	Acesso ao protocolo

				Secure Shell (SSH) ao protocolo Secure Shell (SSH), Agregação de arquivos de log
22	TCP	Saída	Servidor SSH	Agregação SSH de arquivos de log. Envio do protocolo SCP (Secure Copy Protocol) para o servidor de registro.
25	TCP	Saída	IP do servidor SMTP (Simple Mail Transfer Protocol)	Enviar alertas por e-mail
53	UDP	Saída	Servidores DNS (Domain Name System)	DNS, se configurado para usar a Internet servidores raiz ou outros servidores DNS fora do firewall. Também para consultas SenderBase.
8080	TCP	Entrada	Endereço IP de gerenciamento AsyncOS	Acesso ao protocolo HTTP à interface gráfica do usuário (GUI)

8443	TCP	Entrada	Endereço IP de gerenciamento AsyncOS	Acesso seguro ao Hypertext Transfer Protocol (HTTPs) à GUI
80 443	TCP	Saída	downloads.ironport.com	Definições da McAfee
80 443	TCP	Saída	updates.ironport.com	Atualizações AsyncOS e definições McAfee
88	TCP e UDP	Saída	Centro de Distribuição de Chaves Kerberos (KDC) / Servidor de Domínio do Ative Diretory	Autenticação Kerberos
88	UDP	Entrada	Centro de Distribuição de Chaves Kerberos (KDC) / Servidor de Domínio do Ative Diretory	Autenticação Kerberos
389	TCP e UDP	Saída	Servidor Lightweight Diretory Access Protocol (LDAP)	Autenticação LDAP
3268	TCP	Saída	Catálogo global LDAP (GC)	LDAP GC
636	TCP	Saída	LDAP sobre SSL (Secure Sockets Layer)	SSL LDAP
3269	TCP	Saída	LDAP GC sobre SSL	LDAP GC SSL
135	TCP	LigaçãoEntrada eSaída	Resolução de ponto final - Mapeador de portas Porta fixa de Logon de Rede	Resolução de ponto final

161 162	UDP	Saída	Servidor SNMP (Simple Network Management Protocol)	Consultas SNMP
161	UDP	Entrada	IP de gerenciamento AsyncOS	Armadilhas de SNMP
123	UDP	Saída	Servidor Network Time Protocol (NTP)	Sincronização de tempo NTP
443	TCP	Saída	update-manifests.ironport.com	Obter a lista dos arquivos mais recentes a partir do servidor de atualização (para hardware físico)
443	TCP	Saída	update-manifests.sco.cisco.com	Obter a lista dos arquivos mais recentes a partir do servidor de atualização (para hardware virtual)
443	TCP	Saída	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	Serviços de inteligência Cisco Talos Obtenha a categoria Uniform Resource Locator (URL) e os dados de reputação.

443	TCP	Saída	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.cisco.com	Nuvem pública de proteção avançada contra malware (AMP)
443	TCP	Saída	panacea.threatgrid.com panacea.threatgrid.eu	Para Secure Malware Analytics Portal e dispositivos integrados
80 3128	TCP	Entrada	Clientes Proxy	Conectividade de Clientes Padrão com Proxy HTTP/HTTPS
80 443	TCP	Saída	Gateway padrão	Tráfego de saída de proxy HTTP e HTTPS
514	UDP	Saída	Servidor Syslog	Servidor syslog para coletar logs
990	TCP	Saída	cxd.cisco.com	Para carregar os logs de depuração que estão coletados pelo Cisco Technical Assistance Collaborative (TAC). File Transfer Protocol of SSL (FTPS) implícito.
21	TCP	Saída	cxd.cisco.com	Para carregar

				os logs de depuração que estão coletados pelo Cisco TAC. FTP ou FTPS explícito
443	TCP	Saída	cxd.cisco.com	Para carregar os logs de depuração que estão coletado pelo Cisco TAC sobre HTTPS
22	TCP	Saída	cxd.cisco.com	Para carregar os logs de depuração que estão coletado pelo Cisco TAC sobre SCP e SFTP (Secure File Transfer Protocol)
22 25 (Padrão) 53 80 443 4766	TCP	Saída	s.tunnels.ironport.com	Acesso remoto ao back-end
443	TCP	Saída	smartreceiver.cisco.com	smart licensing

Referências

Configurar firewall para domínio e relações de confiança do AD - Windows Server | Aprendizado da Microsoft

Portas de segurança, acesso à Internet e comunicação (cisco.com)

IP e portas necessários para análise segura de malware - Cisco

Carregamentos de arquivo do cliente no Technical Assistance Center - Cisco

Nota técnica sobre perguntas frequentes sobre acesso remoto no Cisco ESA/WSA/SMA - Cisco

Visão geral do Smart Licensing e práticas recomendadas para Cisco Email and Web Security (ESA, WSA, SMA) - Cisco

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.