セキュアWebアプライアンス用のファイアウォールの設定

内容

はじめに

このドキュメントでは、Cisco Secure Web Appliance(SWA)の動作のために開く必要があるポートについて説明します。

前提条件

Transmission Control Protocol/Internet Protocol（TCP/IP；伝送制御プロトコル/インターネットプロトコル）に関する一般知識。

伝送制御プロトコル(TCP)とユーザデータグラムプロトコル(UDP)の相違点と動作について理解する。

Firewall Rules

次の表に、Cisco SWAを正しく動作させるために開く必要があるポートを示します。

注：ポート番号はすべてデフォルト値です。変更されている場合は、新しい値を検討してください。

デフォルトポート	プロトコル	インバウンド/アウトバウンド	ホスト名	目的
20 21	TCP	着信または発信	AsyncOS管理IP。（インバウンド） FTPサーバ（アウトバウンド）	ログファイルを集約するためのファイル転送プロトコル(FTP)。 データポートTCP 1024以上 また、オープンになっている必要があります

22	TCP	Inbound	AsyncOS管理IP	セキュアシェルプロトコル(SSH)へのSSHアクセス ログファイルの集約
22	TCP	Outbound	SSHサーバ	ログファイルのSSH集約。 Secure Copy Protocol(SCP)を口グサーバにプッシュします。
25	TCP	Outbound	シンプルメール転送プロトコル(SMTP)サーバIP	電子メールによるアラートの送信
53	UDP	Outbound	ドメインネームシステム(DNS)サーバ	DNS（インターネットを使用するように設定されている場合） ルートサーバまたは他のDNSサーバ ファイアウォールの外側にあります SenderBaseクエリの場合も同様です。
8080	TCP	Inbound	AsyncOS管理IPアドレス	グラフィカルユーザインターフェイス(GUI)へのハイパーテキスト転送プロトコル(HTTP)アクセス
8443	TCP	Inbound	AsyncOS管理IPアドレス	GUIへのHypertext Transfer Protocol Secure(HTTPs)アクセス
80 443	TCP	Outbound	downloads.ironport.com	McAfee定義

80 443	TCP	Outbound	updates.ironport.com	AsyncOSのアップグレードとMcAfeeの定義
88	TCPおよびUDP	Outbound	Kerberosキー配布センター(KDC)/Active Directoryドメインサーバ	Kerberos 認証
88	UDP	Inbound	Kerberosキー配布センター(KDC)/Active Directoryドメインサーバ	Kerberos 認証
445	TCP	Outbound	Microsoft SMB	Active Directory認証レルム （NTLMSSPおよびBasic）
389	TCPおよびUDP	Outbound	Lightweight Directory Access Protocol(LDAP)サーバ	[LDAP Authentication]
3268	TCP	Outbound	LDAPグローバルカタログ(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	インバウンドとアウトバウンド	エンドポイント解決 – ポートマッパー Net Log-on固定ポート	エンドポイントの解決
161 162	UDP	Outbound	簡易ネットワーク管理プロトコル(SNMP)サーバ	SNMPクエリー
161	UDP	Inbound	AsyncOS管理IP	SNMP トラップ

123	UDP	Outbound	ネットワークタイムプロトコル(NTP)サーバ	NTP時刻の同期
443	TCP	Outbound	update-manifests.ironport.com	最新ファイルのリストを取得するアップデートサーバから （物理ハードウェア用）
443	TCP	Outbound	update-manifests.sco.cisco.com	最新ファイルのリストを取得するアップデートサーバから （仮想ハードウェア用）
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インテリジェンスサービス Uniform Resource Locator(URL)カテゴリおよびレピュテーションデータを取得します。
443	TCP	Outbound	cloud-sa.amp.cisco.com cloud-sa.amp.sourcefire.com cloud-sa.eu.am p.cisco.com	高度なマルウェア防御(AMP)パブリッククラウド
443	TCP	Outbound	panacea.threatgrid.com panacea.threatgrid.eu	Secure Malware Analyticsポータルおよび統合デバイス向け

80 3128	TCP	Inbound	プロキシクライアント	HTTP/HTTPSプロキシへのデフォルトクライアント接続
80 443	TCP	Outbound	デフォルト ゲートウェイ	発信HTTPおよびHTTPSプロキシトラフィック
514	UDP	Outbound	Syslog サーバー	ログを収集するsyslogサーバ
990	TCP	Outbound	cxd.cisco.com	次のデバッグログをアップロードします。 Cisco Technical Assistance Collaborative(TAC)によって収集されます。 SSL を使ったファイル転送プロトコル（FTPS）暗黙モード.
21	TCP	Outbound	cxd.cisco.com	次のデバッグログをアップロードします。 Cisco TACが収集します。 FTPS ExplicitまたはFTP
443	TCP	Outbound	cxd.cisco.com	次のデバッグログをアップロードします。 HTTPS経由でCisco TACによって収集される
22	TCP	Outbound	cxd.cisco.com	次のデバッグログを

				アップロードします。 scpおよびSecure File Transfer Protocol(SFTP)経由でCisco TACが収集
22 25（デフォルト） 53 80 443 4766	TCP	Outbound	s.tunnels.ironport.com	バックエンドへのリモートアクセス
443	TCP	Outbound	smartreceiver.cisco.com	smart licensing

参考資料

ADドメインと信頼のファイアウォールを構成する – Windows Server | Microsoftラーニング

セキュリティ、インターネットアクセス、および通信ポート(cisco.com)

セキュアなマルウェア分析に必要なIPおよびポート – シスコ

Cisco Technical Assistance Center にファイルをアップロードする方法 - Cisco

Cisco ESA/WSA/SMAのリモートアクセスに関するFAQに関するテクニカルノート：シスコ

Cisco Email & Webセキュリティ(ESA、WSA、SMA)のスマートライセンスの概要とベストプラクティス – シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。