

必要なIPおよびファイアウォールルールのセキュアマルウェア分析の設定

内容

[概要](#)

[問題](#)

[環境](#)

[解決方法](#)

[Cisco Secure Malware Analytics アプライアンス](#)

[管理インターフェイス](#)

[クリーンインターフェイス](#)

[Dirtyインターフェイス](#)

[Dirtyインターフェイス発信](#)

[Dirtyインターフェイス着信](#)

[セキュアマルウェア分析クラウド](#)

[米国\(US\)クラウド](#)

[欧州\(EU\)クラウド](#)

[カナダ\(CA\)クラウド](#)

[オーストラリア\(AU\)クラウド](#)

[インド\(IN\)クラウド](#)

[関連コンテンツ](#)

概要

このドキュメントでは、Cisco Secure Malware Analytics (クラウドおよびアプライアンス) に必要なホスト名、IPアドレス、およびポートについて説明します。

問題

Cisco Secure Malware Analyticsでは、特定のホスト名、IPアドレス、およびポートへの発信および着信接続が必要です。これらのフローがブロックされると、ポータルアクセス、アップデート、ライセンス、リモートサポート、統合などの機能が失敗する可能性があります。

環境

 注：最初にこのドキュメントを参照してください。他のサービス用の追加のIPとポートが記



載されています。

[Threat Gridに必要なIPとポート](#)

このドキュメントには、アプライアンスのバージョンに基づくその他のサービス用の追加IPおよびポートが含まれています。

インストールおよびアップグレードガイドのドキュメント「[Threat Gridアプライアンスインストールガイド](#)」を参照してください。

解決方法

デバイスへのアップストリームのファイアウォールのファイアウォールルール：

*IPは公開時点で正しく機能していました。nslookupを使用してローカルに、これらがまだ正しいことを確認してください。

Cisco Secure Malware Analytics アプライアンス

管理インターフェイス

送信元	宛先	プロトコル	ポート	方向	アクション	注意事項
ANY	管理インターフェイス	TCP	22	IN	プライベート ネットワーク間で	SSH
ANY	管理インターフェイス	TCP	80/443	IN	プライベート ネットワーク間で	管理GUIインターフェイスへのアクセスを許可します。
管理インターフェイス	NFSサーバーIP	TCP	2049	OUT	プライベート ネットワーク間で	* NFSバックアップまたはクラスタリング機能を使用するには、開いている必要があります。

クリーンインターフェイス

送信元	宛先	プロトコル	ポート	方向	アクション	注意事項
ANY	クリーンインターフェイス	TCP	80/443	IN	プライベート ネットワーク間で	Clean GUIインターフェイスへのアクセスを許可します。
ANY	クリーンインターフェイス	TCP	8443	IN	プライベート ネットワーク間で	* クリーン機能よりもAdminを使用するには、開いている必要があります。
ANY	クリーンインターフェイス	TCP	9443	IN	プライベート ネットワーク間で	* サンプルのグローブボックス機能を使用するには、開いている必要があります。
クリーンインターフェイス	設定された電子メールリレーサーバ	TCP	25	OUT	許可	アプライアンスは、de cleanインターフェイスを使用して、設定されたメールサーバへのSMTP接続を開始します。
クリーンインターフェイス	Clean DNSサーバの設定	TCP/UDP	53	OUT	プライベート ネットワーク間で	* オプション。Clean DNSが設定されている場合のみ必要。
クリーンインターフェイス	設定されたSyslogサーバ	TCP/UDP	514	OUT	プライベート ネットワーク間で	SyslogメッセージおよびThreat Grid通知を受信するように指定されたサーバへの接続を許可します。
クリーンインターフェイス	LDAP サーバ	TCP/UDP	389/636	OUT	プライベート ネットワーク間で	* オプション。LDAPが設定されている場合にのみ必要。

Dirtyインターフェイス

Dirtyインターフェイス発信

送信元	宛先	プロ トコ ル	ポー ト	アク ショ ン	注記
Dirtyイン ターフェ イス	イン ター ネット	ANY	ANY	プ ラ イ ベ ー ト ネ ッ ト ワ ー ク 間 で	サンプルからの発信トラフィックを許可します。オプションでシスコデータセンターを通じてプロキシします。(正確な結果を得るためには、マルウェアが使用するように設計されたポートとプロトコルを使用して、コマンドおよびコントロールサーバにアクセスできる必要があります)。

Dirtyインターフェイス着信

送信元	宛先		プロトコル	ポート	アクション	注記
ANY	ダーティインターネット		ANY	ANY	拒否	すべての着信接続を拒否します。

送信元	宛先	プロトコル	ポート	アクション	注記
Dirtyインターフェイス	インターネット	TCP	22	プライベートネットワーク間で	アップデート、サポートスナップショット、およびライセンスサービス
Dirtyインターフェイス	インターネット	TCP/UDP	53	プライベートネットワーク間で	発信DNSを許可します。
Dirtyインターフェイス	インターネット	UDP	123	プライベートネットワーク間で	発信NTPを許可します。

Dirtyインターフェイス	インターネット	TCP	19791	プライベートネットワーク間で	Secure Malware Analyticsサポートへの接続を許可
Dirtyインターフェイス	シスコの傘	TCP	443	プライベートネットワーク間で	サードパーティの検出およびエンリッチメントサービスと接続します。
Dirtyインターフェイス	ウイルス合計	TCP	443	プライベートネットワーク間で	サードパーティの検出およびエンリッチメントサービスと接続します。
Dirtyインターフェイス	チタンクラウド	TCP	443	プライベートネットワーク間で	サードパーティの検出およびエンリッチメントサービスと接続します。



警告：リストされたIPアドレスは2023年5月29日以降もアクティブなままです。

送信元	宛先	プロトコル	ポート	方向	ホスト名	詳細
Dirtyインターフェイス	63.97.201.96 63.162.55.96	TCP	19791	OUT	rash.threatgrid.com	リモートサポート/アプリケーションサポートモード
Dirtyインターフェイス	63.97.201.97 63.162.55.97	TCP	22	OUT	appliance-updates.threatgrid.com	自動サポート診断アップロードに使用されます。  注：ソフトウェアバージョン 1.2+が必要
Dirtyインターフェイス	63.97.201.98 63.162.55.98	TCP	22	OUT	support-snapshots.threatgrid.com	自動サポート診断アップロードに使用されます。 

						注：ソフトウェアバージョン1.2+が必要
Dirtyインターフェイス	63.97.201.99 63.162.55.99	TCP	22	OUT	appliance-licensing.threatgrid.com	ライセンス管理

セキュアマルウェア分析クラウド

米国(US)クラウド

アクセスURL:<https://panacea.threatgrid.com>

ホスト名	IP	ポート	詳細
panacea.threatgrid.com	IPv4 63.97.201.67 63.162.55.67 IPv6 : 2602:811:9007:6::61 2602:811:900b:6::6e	443	Secure Malware Analyticsポータルと統合デバイス(ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4:200.194.241.35 IPv6 : 2602:811:900f:6::6e	443	Sample Interactionウィンドウ
glovebox.rcn.threatgrid.com	IPv4	443	Sample Interactionウィンドウ

	63.97.201.67 IPv6 : 2602:811:9007:6::61		
glovebox.scl.threatgrid.com	IPv4 63.162.55.67 IPv6 : 2602:811:900b:6::6e	443	Sample Interactionウィンドウ
fmc.api.threatgrid.com	IPv4 63.97.201.67 63.162.55.67 IPv6 : 2602:811:9007:6::61 2602:811:900b:6::6e	443	FMC/FTDファイル分析サービス

欧州(EU)クラウド

アクセスURL:<https://panacea.threatgrid.eu>

ホスト名	IP	ポート	詳細
panacea.threatgrid.eu (日本)	IPv4 62.67.214.195 200.194.242.35 200.194.245.35 IPv6 : 2602:811:9006:6::6e	443	Secure Malware Analyticsポータルと統合デバイス(ESA/WSA/FTD/ODNS/Meraki)

	2602:811:900c:6::6e		
グローブボックス .muc.threatgrid.eu	IPv4 62.67.214.195 200.194.245.35 IPv6 : 2602:811:900c:6::6e	3	Sample Interactionウィンドウ
グローブボックス .fam.threatgrid.eu	IPv4 200.194.242.35 IPv6 : 2602:811:9006:6::6e	443	Sample Interactionウィンドウ
fmc.api.threatgrid.eu (欧州)	IPv4 62.67.214.195 200.194.242.35 200.194.245.35 IPv6 : 2602:811:9006:6::6e 2602:811:900c:6::6e	443	FMC/FTDFile分析サービス

古いIP 89.167.128.132は廃止されました。これらのIPでファイアウォールルールを更新してください。

カナダ(CA)クラウド

アクセスURL:<https://panacea.threatgrid.ca>

ホスト名	IP	ポート	詳細
------	----	-----	----

panacea.threatgrid.ca (すべてのバージョン)	IPv4 200.194.240.35 IPv6 : 2602:811:900d:6::6e	443	Secure Malware Analyticsポータルと統合デバイス (ESA/WSA/FTD/ODNS/Meraki)
globebox.kam.threatgrid.ca	IPv4 200.194.240.35 IPv6 : 2602:811:900d:6::6e	443	Sample Interactionウィンドウ
fmc.api.threatgrid.ca (すべてのバージョンのFMCを含む)	IPv4 200.194.240.35 IPv6 : 2602:811:900d:6::6e	443	FMC/FTDファイル分析サービス

オーストラリア(AU)クラウド

アクセスURL:<https://panacea.threatgrid.com.au>

ホスト名	IP	ポート	詳細
panacea.threatgrid.com.au	IPv4 200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e	443	Secure Malware Analyticsポータルと統合デバイス (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	IPv4	443	Sample Interactionウィンドウ

	200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e		
fmc.api.threatgrid.com.au	IPv4 200.194.246.35 200.194.247.35 IPv6 : 2602:811:900e:6::6e 2602:811:9003:6::6e	443	FMC/FTDファイル分析サービス

インド(IN)クラウド

アクセスURL:<https://panacea.threatgrid.in>

ホスト名	IP	ポート	詳細
panacea.threatgrid.in (日本での対応時期未定)	IPv4 200.194.244.35 IPv6 : 2602:811:9001:6::6e	443	Secure Malware Analyticsポータルと統合デバイス (ESA/WSA/FTD/ODNS/Meraki)
グローブボックス bom.threatgrid.in	IPv4 200.194.244.35 IPv6 : 2602:811:9001:6::6e	443	Sample Interactionウィンドウ

fmc.api.threatgrid.com.in	IPv4 200.194.244.35 IPv6 : 2602:811:9001:6::6e	443	FMC/FTDファイル分析サービス
---	---	-----	-------------------

アプライアンスなど、Cisco Secure Malware Analyticsのその他の要件については、次の記事を参照してください。

関連コンテンツ

最新の要件については、を参照してください。

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。