計画

Cisco Threat Grid アプライアンスは、出荷前にシスコの製造部門によってインストールされた Threat Grid ソフトウェアを備える Linux サーバです。新しい Threat Grid アプライアンスを受信したら、オンプレミスのネットワーク環境に合わせてセットアップし、設定する必要があります。

この章には、設定前に確認する必要がある環境、ハードウェア、およびネットワーク要件に関する次の情報が含まれています。

対応ブラウザ

Threat Grid は、次のブラウザをサポートしています。

- Google Chrome™
- Mozilla Firefox®

- Apple Safari®

（注） Microsoft Internet Explorer はサポートされません。

環境要件

Threat Grid アプライアンス（v2.7.2 以降）は、Threat Grid M5 アプライアンスサーバ上で展開されます。Threat Grid アプライアンスをセットアップして設定する前に、『*Cisco Threat Grid M5 ハードウェア設置ガイド*』の仕様に従って、電源、ラックスペース、冷却、およびその他の問題に必要な環境要件を満たしていることを確認してください。

ハードウェア要件

管理インターフェイスには、SFP+ フォームファクタが使用されています。Threat Grid アプライアンスをクラスタリングしている場合は、各アプライアンスの Clust インターフェイスに追加の SFP+ モジュールが必要となります。

（注） SFP+ モジュールは、設定ウィザードを実行するセッションで Threat Grid アプライアンスの電源を入れる前に接続する必要があります。

スイッチで使用できる SFP+ ポートがないか、または SFP+ が望ましくなければ、1000Base-T のトランシーバを使用できます（シスコ機器互換のギガビット RJ 45 銅線 SFP トランシーバモジュール Mini -GBIC - 10/100/1000 Base-T 銅線 SFP モジュール）。

図 *1 : Cisco 1000BASE-T* 銅線 *SFP*（*GLC-T*）

サーバにモニタを接続できます。または、Cisco Integrated Management Controller（CIMC）が設定されている場合は、（UCS C220-M3 および C220-M4 サーバ上で）リモート KVMを使用できます。

（注） CIMC は、Threat Grid M5 アプライアンスサーバではサポートされていません。

CISCO UCS Power Calculator は、推定電力を算出するために使用できます。

ネットワーク要件

Threat Grid アプライアンスには次の 3 つのネットワークが必要です。

- **管理**：Threat Grid アプライアンスの設定を行うには、管理ネットワークを設定する必要があります。
  - OpAdmin 管理トラフィック（HTTPS）
  - SSH
  - NFSv4（発信。IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。
- **クリーン**：クリーンネットワークは、インバウンド、Threat Grid アプライアンス（要求）への信頼済みトラフィック（要求）、および Cisco E メール セキュリティ アプライアンスや Web セキュリティアプライアンスなどの統合アプライアンスに使用されます。統合アプライアンスは、クリーンインターフェイスの IP アドレスに接続します。

  （注） Clean network インターフェイスの URL は、OpAdmin portal の設定が完了するまで機能しません。

  以下の制限付きタイプのネットワークトラフィックは、クリーンインターフェイスから発信することができます。
  - リモート syslog 接続
  - Threat Grid アプライアンスによって送信される電子メールメッセージ
  - AMP for Endpoints プライベート クラウド デバイスへの配置更新サービス接続
  - DNS 要求（上記のいずれかに関連）
  - LDAP
- **ダーティ**：「ダーティ」ネットワークは Threat Grid アプライアンス（マルウェアトラフィックを含む）からの発信トラフィックに使用されます。

  （注） 内部ネットワークの評価を保護するために、社内 IP とは異なる専用の外部 IP アドレス（ダーティインターフェイスなど）を使用することをお勧めします。

ネットワーク インターフェイスの設定については、「ネットワーク インターフェイス」を参照してください。

DNS サーバ アクセス

配置更新サービスのルックアップ、リモートの Syslog 接続の解決、および Threat Grid ソフトウェアからの通知に使用されるメール サーバの解決以外の目的に使用される DNS サーバは、ダーティネットワークを介したアクセスが可能になっている必要があります。

デフォルトでは、DNS はダーティ インターフェイスを使用します。クリーン インターフェイスは AMP for Endpoints プライベート クラウドの統合に使用されます。AMP for Endpoints プライベート クラウドのホスト名がダーティ インターフェイスに解決できない場合、クリーン インターフェイスを使用する別の DNS サーバを OpAdmin インターフェイスに構成できます。

詳細については、『Cisco Threat Gridアプライアンス管理者ガイド』を参照してください。

NTP サーバ アクセス

NTP サーバはダーティ ネットワークからアクセスできる必要があります。

統合

Threat Grid アプライアンスを他のシスコ製品（E メール セキュリティ アプライアンス、Web セキュリティアプライアンス、AMP for Endpoint プライベートクラウドなど）とともに使用する場合、追加の計画が必要になることがあります。詳細については、『*Cisco Threat Grid アプライアンス管理者ガイド*』を参照してください。

DHCP

DHCP を使用するように設定されたネットワークに接続している場合は、『*Cisco Threat Grid アプライアンス管理者ガイド*』の「DHCPの使用」の項に記載されている手順に従ってください。

ライセンス

Cisco Threat Grid からライセンスとパスワードを受信します。

ライセンスに関して不明な点がある場合は、Threat Grid のサポートにお問い合わせください。

レート制限

API レート制限は、ライセンス契約の条件に基づいて Threat Grid アプライアンス全体に適用されます。API レート制限は API 送信にのみ適用され、手動によるサンプル送信には適用されません。

レート制限はカレンダー日ではなくローリングタイムの時間枠に基づきます。送信制限に達すると、次の API 送信の再試行まで待機する時間を通知するメッセージとともに、429 エラーが返されます。詳細な説明については、Threat Grid Portal UI オンラインヘルプのよくある質問を参照してください。

組織とユーザ

Threat Grid アプライアンスの設定とネットワーク設定を完了したら、Threat Grid の初期組織を作成してユーザアカウントを追加する必要があります。これにより、ユーザはログインして、分析用にマルウェアサンプルの送信を開始できるようになります。この作業では、要件に応じて、複数の組織やユーザ間での計画と調整が必要になる場合があります。

『*Cisco Threat Grid アプライアンス管理者ガイド*』の「新しい組織の作成」の項を参照してください。ユーザの管理の詳細については、Threat Grid Portal のヘルプを参照してください。

変更点（Updates）

Threat Grid アプライアンスの更新をインストールする場合は、事前に初期のアプライアンスセットアップおよび設定手順が**完了している**必要があります。初期設定の完了直後に、更新を確認することをお勧めします（「更新プログラムのインストール」を参照）。

Threat Grid アプライアンスの更新は、ライセンスがインストールされるまでダウンロードできません。また、更新プロセスでは、アプライアンスの初期設定が完了している必要があります。更新は順に行う必要があります。

（注） 更新用に SSH が指定されていることを確認してください。

ユーザ インターフェイス

サーバがネットワークに正常に接続され、電源が入ると、複数のユーザインターフェイスを使用して Threat Grid アプライアンスを設定できるようになります。

（注） LDAP 認証は、TGSH Dialog および OpAdmin で使用できます。RADIUS 認証は、Threat Grid アプリケーション UI（バージョン 2.10 以降）で使用できます。

TGSH ダイアログ

TGSH ダイアログインターフェイスは、ネットワーク インターフェイスの設定に使用します。Threat Grid アプライアンスが正常に起動すると、[TGSH] ダイアログが表示されます。

TGSH ダイアログへの再接続

[TGSH] ダイアログはコンソール上で開いたままになり、アプライアンスにモニタを接続するか、またはリモート KVM 経由で CIMC が設定されている場合は、アクセスできます。

（注） CIMC は、Threat Grid M5 アプライアンスサーバではサポートされていません。

TGSH ダイアログに再接続するには、ユーザ **threatgrid** を使用して管理 IP アドレスに SSH 接続します。

必要なパスワードは、TGSH ダイアログに最初に表示される、ランダムに生成された初期設定パスワード、または OpAdmin Portal 設定の最初の手順で作成した新しい管理者パスワードのどちらかです。

Threat Grid シェル（tgsh）

Threat Grid シェル（tgsh）は、（estroy-data や forced backup などの）コマンドを実行するために使用される管理者のインターフェイスであり 、専門家による低レベルのデバッグにも使用されます。tgsh にアクセスするには、TGSH ダイアログで [CONSOLE] を選択します。

（注） OpAdmin は Threat Grid ユーザと同じクレデンシャルを使用するため、tgsh を介して行われたパスワードの変更/更新は OpAdmin にも影響します。

注意 tgsh によるネットワーク設定の変更は、Threat Grid サポートによって特に指示された場合を除き、サポートされません。代わりに OpAdmin または TGSH ダイアログを使用する必要があります。

OpAdmin Portal

これは主要な Threat Grid GUI 設定ツールです。ライセンス、電子メールホスト、SSL 証明書など、Threat Grid アプライアンス設定の多くは OpAdmin からのみ実行できます。

Threat Grid Portal

この Threat Grid ユーザ インターフェイス アプリケーションはクラウド サービスとして使用可能で、Threat Grid アプライアンスにもインストールされます。Threat Grid Cloud サービスと、Threat Grid アプライアンスに含まれる Threat Grid Portal との間で通信は行われません。

ネットワーク インターフェイス

使用可能なネットワークインターフェイスを次の表に示します。

インターフェイス	説明
Admin	• 管理ネットワークに接続します。管理ネットワークからの**着信のみ**。 • OpAdmin UI トラフィック • SSH （inbound）for TGSH Dialog • バックアップとクラスタリングのための NFSv4（アウトバウンド) IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。すべてのクラスタ ノードからアクセスできる必要があります。 • 管理ポートは（tgsh シェルから）無効にすることができます。無効になっている場合、クラスタ化されていない Threat Grid アプライアンスは、クリーンポートとダーティポートが接続されている場合のみ正しく動作します。管理UIはクリーンインターフェイスのポート 8443 に表示されます。ポートが無効になっていない場合、管理ポートを抜くと、機能していない（または機能が非常に高い）Threat Grid アプライアンスになります。 （注） 管理インターフェイス用のフォーム ファクタは SFP+ です。「ハードウェア要件」を参照してください。
クラスタ	非管理 SFP+ ポートはクラスタリングに使用されます。 • クラスタリングに必要なクラスタ インターフェイス（任意） • ダイレクト インターコネクトには追加の SFP+ モジュールが必要です。このインターフェイスでは、設定の必要はありません。アドレスが自動的に割り当てられます。

インターフェイス	説明
[クリーン（Clean）]	• クリーンネットワークに接続します。クリーンには、社内ネットワークからアクセスできる必要がありますが、インターネットへの発信アクセスができないようにする必要があります。 • UI および API トラフィック（着信） • サンプルの送信 • SMTP（設定済みメール サーバへの発信接続） • SSH （inbound for TGSH Dialog) • syslog（設定済み syslog サーバへの発信） • ESA/WSA と CSA の統合 • AMP for Endpoints プライベート クラウドの統合 • DNS（オプション） • LDAP（発信） • RADIUS（発信）

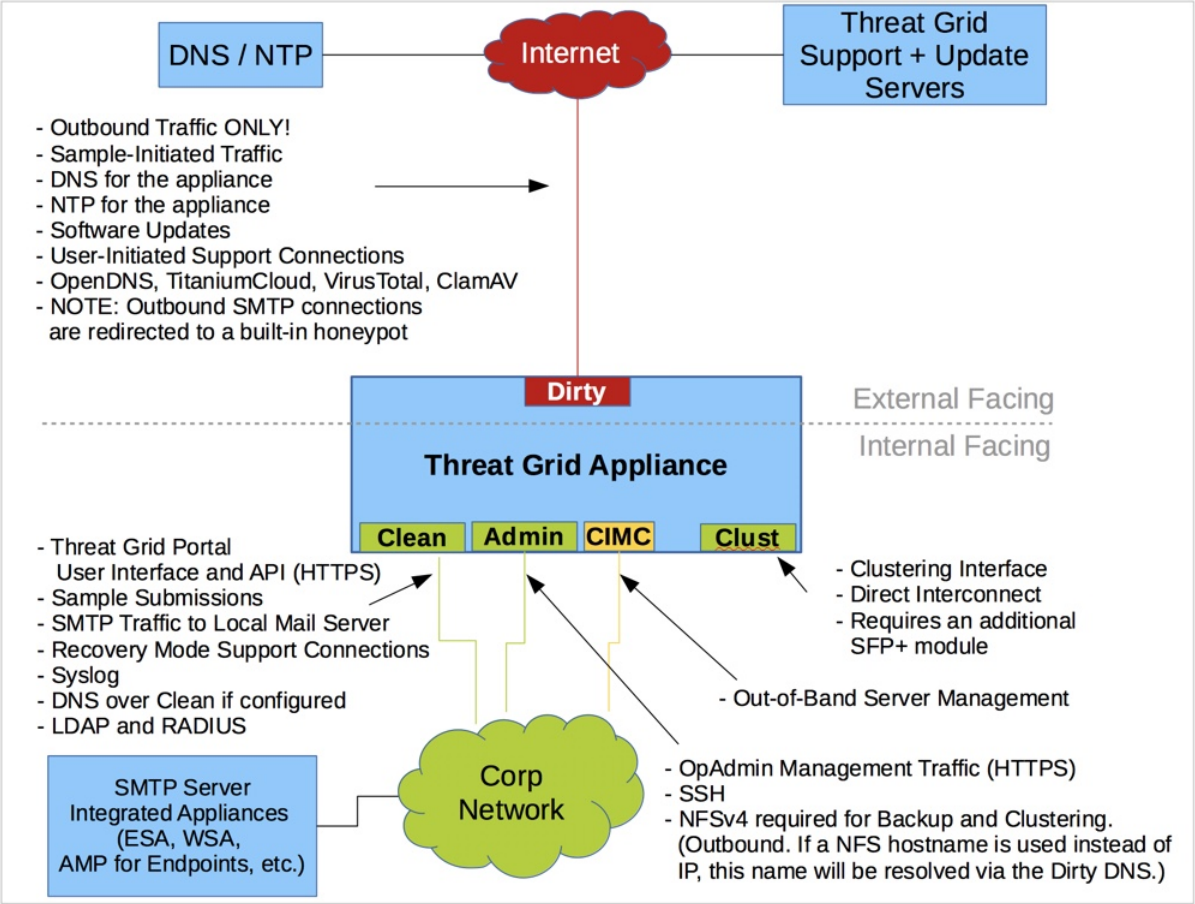
インターフェイス	説明
ダーティ	ダーティネットワークに接続します。インターネットアクセスが必要です。発信のみ。 プライベート IP に送信されるトラフィックは、ネットワーク出口のローカリゼーション ファイアウォールでドロップされるため、ダーティインターフェイスには独自の DNS（プライベート IP）を使用しないようにしてください。 • DNS （注） AMP for Endpoints プライベートクラウドとの統合を設定し、AMP for Endpoints アプライアンスのホスト名がダーティインターフェイスで解決できない場合、クリーンインターフェイスを使用する別の DNS サーバを OpAdmin に設定できます。 • NTP • Updates • 通常の動作モードでのサポートセッション • サポートスナップショット • マルウェアサンプルから開始されたトラフィック • リカバリ モード サポート セッション（発信） • OpenDNS、TitaniumCloud、VirusTotal、ClamAV • SMTP の発信接続が組み込みのハニーポットにリダイレクト （注） ダーティインターフェイスでの IPv4LL アドレス空間（168.254.0.16）の使用はサポートされていません。
CIMC インターフェイス	推奨。Cisco Integrated Management Controller（CIMC）インターフェイスが設定されている場合は、サーバの管理とメンテナンスに使用できます。詳細については、『*Cisco Threat Grid アプライアンス管理者ガイド*』を参照してください。 （注） CIMC は、Threat Grid M5 アプライアンスサーバではサポートされていません。

ネットワーク インターフェイスの設定図

このセクションでは、Threat Grid アプライアンスの最も論理的で推奨される設定について説明します。ただし、お客様によってインターフェイス設定は異なります。ネットワーク要件に応

じて、ダーティインターフェイスを内部に接続するか、適切なネットワークセキュリティ対策を講じてクリーンインターフェイスを外部に接続するかを決定できます。

図 *2:* ネットワークインターフェイス設定図



（注） Threat Grid アプライアンス（v 2.7.2 以降）では、**enable_clean_interface** オプションは使用できますが、デフォルトでは無効になっています。このオプション（設定を適用して再起動した後）により、割り当てられたクリーン IP のポート 8443 の管理インターフェースにアクセスできます。

ファイアウォール ルール

ここでは、推奨されるファイアウォールルールについて説明します。

（注） ポート 22 および 19791 のダーティインターフェイス上で制限付きの発信ポリシーを実装すると、経時的な更新の追跡が必要となり、ファイアウォールの維持等により多くの時間がかかる可能性があります。

（注） ダーティインターフェイスでの IPv4LL アドレス空間（168.254.0.16）の使用はサポートされていません。

ダーティインターフェイスによる発信

送信元	宛先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	インターネット	ANY	ANY	許可（Allow）	サンプルからの発信トラフィックを許可します。（正確な結果を取得するには、指定されたポートやプロトコルにかかわらず、マルウェアからコマンド アンド コントロール サーバへのアクセスが許可されている必要があります。）

ダーティ インターフェイスによる着信

送信元	宛先	プロトコル	ポート	操作	コメント
ANY	ダーティインターネット	ANY	ANY	拒否（Deny）	すべての着信接続を拒否します。

クリーン インターフェイスによる発信

送信元	宛先	プロトコル	ポート	操作	コメント
クリーンインターフェイス	SMTP サーバ	TCP	25	許可（Allow）	アプライアンスはクリーン インターフェイスを使用して、設定済みメールサーバへの SMTP 接続を開始します

クリーンインターフェイスによる発信（任意）

送信元	宛先	プロトコル	ポート	操作	コメント
クリーンインターフェイス	企業の DNS サーバ	TCP/UDP	53	許可（Allow）	任意。クリーン DNS が設定されている場合のみ必須。
クリーンインターフェイス	AMP プライベート クラウド	TCP	443	許可（Allow）	任意。AMP for Endpoints プライベートクラウド統合が使用されている場合のみ必須。
クリーンインターフェイス	Syslog サーバ	UDP	514	許可（Allow）	syslog メッセージと Threat Grid 通知を受信するようにサーバへの接続を許可。
クリーンインターフェイス	LDAP サーバ	TCP/UDP	389	許可（Allow）	任意。LDAP が設定されている場合のみ必須。
クリーンインターフェイス	LDAP サーバ	TCP	636	許可（Allow）	任意。LDAP が設定されている場合のみ必須。
クリーンインターフェイス	RADIUS サーバ	DTLS	2083	許可	Threat Grid アプリケーション UI（Face）へのログインを許可します。任意。RADIUS が設定されている場合のみ必須。

クリーン インターフェイスによる着信

送信元	宛先	プロトコル	ポート	操作	コメント
ユーザ サブネット	クリーン インターフェイス	TCP	22	許可（Allow）	TGSH ダイアログへの SSH 接続を許可します。
ユーザ サブネット	クリーン インターフェイス	TCP	80	許可（Allow）	アプライアンスの API と Threat Grid ユーザ インターフェイス。これは HTTPS TCP/443 にリダイレクトします。
ユーザ サブネット	クリーン インターフェイス	TCP	443	許可（Allow）	アプライアンスの API と Threat Grid ユーザ インターフェイス。
ユーザ サブネット	クリーン インターフェイス	TCP	9443	許可	Threat Grid UI Glovebox への接続を許可します。

管理インターフェイスによる発信（任意）

以下は、設定されるサービスの内容に依存します。

送信元	宛先	プロトコル	ポート	操作	コメント
管理インターフェイス	NFSv4 サーバ	TCP	2049	許可（Allow）	任意。Threat Grid アプライアンスが NFSv4 共有にバックアップを送信するように設定されている場合のみ必須。

管理インターフェイスによる着信

送信元	宛先	プロトコル	ポート	操作	コメント
管理サブネット	管理インターフェイス	TCP	22	許可（Allow）	[TGSH] ダイアログへの SSH 接続を許可します。
管理サブネット	管理インターフェイス	TCP	80	許可（Allow）	OpAdmin Portal インターフェイスへのアクセスを許可します。これは HTTPS TCP/443 にリダイレクトします。
管理サブネット	管理インターフェイス	TCP	443	許可（Allow）	OpAdmin Portal インターフェイスへのアクセスを許可します。

シスコ未検証/導入が推奨されるダーティ インターフェイス

送信元	宛先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	インターネット	TCP	22	許可（Allow）	更新、サポートスナップショット、ライセンスのサービス。
ダーティインターフェイス	インターネット	TCP/UDP	53	許可（Allow）	発信 DNS を許可。
ダーティインターフェイス	インターネット	UDP	123	許可（Allow）	発信 NTP を許可します。
ダーティインターフェイス	インターネット	TCP	19791	許可（Allow）	Threat Grid サポートへの接続を許可します。

送信元	宛先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	Cisco Umbrella	TCP	443	許可（Allow）	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結合します。
ダーティインターフェイス	VirusTotal	TCP	443	許可（Allow）	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結合します。
ダーティインターフェイス	TitaniumCloud	TCP	443	許可（Allow）	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結合します。

ログイン名とパスワード（デフォルト）

デフォルトのログイン名とパスワードを次の表に示します。

ユーザ（User）	ログイン/パスワード
OpAdmin およびシェルユーザ	最初の Threat Grid/TGSH ダイアログでランダムに生成されたパスワードを使用し、次に OpAdmin 設定ワークフローの最初の手順で入力した新しいパスワードを使用します。 パスワードを紛失した場合は、『*Cisco Threat Grid アプライアンス管理者ガイド*』の「管理者パスワードのリセット」の項を参照してください。
Threat Grid Web ポータル UI 管理者	Login: **admin** Password：最初の OpAdmin パスワードを使用して初期化します。その後、独立した状態になります。
CIMC	Login: **admin** Password: **password**

設定と構成の概要

このドキュメントでは、次のセットアップおよび初期設定の手順を説明します。

- 初期ネットワーク設定
- OpAdmin Portal の設定

- 更新のインストール
- アプライアンスのセットアップのテスト

『*Threat Grid* アプライアンス管理者ガイド』に記載されているとおり、OpAdmin Portal で、（ライセンスのインストール、電子メールサーバ、SSL 証明書などの）残りの管理設定タスクを完了します。

初期設定手順を完了するには約 1 時間かかります。