インバウンドおよびアウトバウンド接続

インバウンド接続およびアウトバウンド接続を使用して、他のシスコのアプライアンス、デバイス、およびサービスと通信するように Cisco Secure Malware Analytics アプライアンスを設定できます。暗号化された SSL 接続により、他のアプライアンス（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）が、分析のために潜在的なマルウェアサンプルを Cisco Secure Malware Analytics に送信できるようになります（インバウンド接続）。

また、アウトバウンド接続を介して、配置更新サービスのために Cisco Secure Endpoint プライベートクラウドと通信するように Cisco Secure Malware Analytics アプライアンスを設定できます。

この付録では、インバウンド接続とアウトバウンド接続の両方を設定する手順について説明します。

ESA または WSA の Secure Malware Analytics アプライアンスへの接続

Cisco Secure Malware Analytics アプライアンスと Cisco E メール セキュリティ アプライアンス（ESA）または Web セキュリティアプライアンス（WSA）間の接続は、Cisco Sandbox API（CSA API）によって有効になり、CSA 統合と呼ばれることがよくあります。ESA/WSA アプライアンスは、分析用のサンプルを送信する前に、Secure Malware Analytics アプライアンスに登録する必要があります。

ESA/WSA を Secure Malware Analytics アプライアンスに登録するには、まず ESA/WSA の管理者が、使用中のアプライアンスとネットワーク環境に適した SSL 証明書接続をセットアップする必要があります。

インバウンドおよびアウトバウンド接続

ESA/WSA のマニュアル

ESA/WSA の製品マニュアルで、「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

- 『*Cisco Email Security Appliance User Guides*』
- 『*Cisco Web Security Appliance User Guides*』

（注） これらのマニュアルで、Secure Malware Analytics アプライアンスは、多くの場合「分析サービス」または「プライベートクラウドファイル分析サーバー」と呼ばれています。

インバウンド接続の概要

インバウンド接続を設定する場合、次の作業を実行する必要があります。

（注） Cisco Secure Malware Analyticsは、クラスタまたはスタンドアロンSMAアプライアンスのいずれかと通信できる1つの環境とのみ通信できます。環境がクラスタの場合は、クラスタ内のすべてのノードを追加する必要があります。

- **SSL 証明書のセットアップ**：Secure Malware Analytics アプライアンスの SSL 証明書の SAN（サブジェクト代替名）または CN（共通名）は、ホスト名および ESA/WSA の想定と一致している必要があります。統合先の ESA/WSA との接続を成功させるには、統合先の ESA/WSA が Secure Malware Analytics アプライアンスの識別に使用するものと同じホスト名にする必要があります。

  要件に応じて、Secure Malware Analytics アプライアンスで自己署名 SSL 証明書を再生成する必要があります。その際、[SAN/CN] フィールドには現在のホスト名が入力されます。この証明書を作業環境にダウンロードし、統合先の ESA/WSA にアップロードしてインストールできます。

  あるいは、企業向けの SSL 証明書や市販の SSL 証明書（または手動で生成した証明書）をアップロードして、現在の Secure Malware Analytics アプライアンスの SSL 証明書と置き換えなければならないこともあります。詳細な手順については、SSL 証明書の置き換えを参照してください。

- **接続性の確認**：SSL 証明書の設定が完了したら、次の手順として、ESA/WSA が Secure Malware Analytics アプライアンスと通信できることを確認します。ESA/WSA は、ネットワーク経由で Secure Malware Analytics アプライアンスのクリーン インターフェイスに接続できる必要があります。製品マニュアルの手順に従って、Secure Malware Analytics アプライアンスと ESA/WSA が相互に通信できることを確認します（ESA または WSA の Secure Malware Analytics アプライアンスへの接続を参照）。

- **ESA/WSA ファイル分析の構成の完了**：**ファイル分析セキュリティ** サービスを有効にし、詳細を構成します。

- **Cisco Secure Malware Analytics アプライアンスへの ESA/WSA の登録** ：製品マニュアルに従って設定された ESA/WSA は、Cisco Secure Malware Analytics アプライアンスに自動的に登録されます。接続先デバイスの登録時に、デバイス ID がログイン ID となる新しい Cisco Secure Malware Analytics ユーザーが自動的に作成され、同じ ID に基づく名前を使用して新しい組織が作成されます。管理者は、新しいデバイスユーザーアカウントをアクティブにする必要があります。
- **Cisco Secure Malware Analytics アプライアンスでの新しい ESA/WSA アカウントのアクティブ化** ：ESA/WSA または他の統合が接続され、それ自体が Cisco Secure Malware Analytics アプライアンスに登録されると、新しい Cisco Secure Malware Analytics ユーザー アカウントが自動的に作成されます。ユーザーアカウントの初期ステータスは、非アクティブになっています。Cisco Secure Malware Analytics アプライアンス管理者は、分析用のマルウェア サンプルの送信に使用する前に、デバイス ユーザー アカウントを手動でアクティブにする必要があります。

インバウンド接続の構成

ESA/WSA 間の接続は、Cisco Secure Malware Analytics アプライアンスから見れば受信になり、CSA API を使用します。

（注） 実行する必要のあるタスクの詳細については、ESA および WSA 製品のマニュアルを参照してください。

手順

ステップ 1 Cisco Secure Malware Analytics アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして構成します。

ステップ 2 更新を確認し、必要に応じてインストールします。

ステップ 3 ESA/WSA を通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 4 Cisco Secure Malware Analytics アプライアンス SSL 証明書 SAN または CN は、現在のホスト名と ESA/WSA の想定と一致する必要があります。自己署名 SSL 証明書を展開する場合は、（Cisco Secure Malware Analytics アプリケーションのクリーンインターフェイスで）新しい SSL 証明書を生成し、必要に応じてデフォルトと置き換え、ダウンロードして ESA/WSA にインストールします（「SSL 証明書の置き換え」を参照）。

（注）
Cisco Secure Malware Analytics アプライアンスのホスト名が SAN または CN になっている証明書を生成してください（Cisco Secure Malware Analytics アプライアンスのデフォルトの証明書は機能しません）。IP アドレスではなく、ホスト名を使用します。

ステップ 5 ESA/WSA は、ネットワーク経由で Secure Malware Analytics アプライアンスのクリーン インターフェイスに接続できることを確認します。

ステップ 6 Cisco Secure Malware Analytics アプライアンスとの統合用に ESA/WSA を構成します。詳細な手順については、ESA/WSA 製品のマニュアルを参照してください。

ステップ 7 変更を送信し、保存します。

Cisco Secure Malware Analytics アプライアンスへの ESA/WSA の登録は、ファイル分析の設定を送信すると自動的に実行されます。

ステップ 8 Cisco Secure Malware Analytics アプライアンスで新しいデバイスユーザーアカウントをアクティブ化します。

a) Cisco Secure Malware Analytics ポータル UI に管理者としてログインします。
b) **[管理（Administration）**] タブをクリックし、**[ユーザーの管理（Manage Users）]** を選択して [**ユーザー（Users）]** ページを開きます。
c) ユーザー名をクリックして、デバイス ユーザ アカウントの [ユーザーの詳細（User Details）] ページを開きます（探すために検索を使用する必要がある場合があります）。
d) ユーザー ステータスは現在 **非アクティブ**です。 **[現用系（Active）]** をクリックして、新しいアカウントをアクティブ化します。
e) 確認ダイアログで、アクションを確認します。

ESA/WSA は、Cisco Secure Malware Analytics アプライアンスとの接続を開始できるようになりました。

Cisco Secure Endpoint プライベートクラウドを Cisco Secure Malware Analytics アプライアンスに接続

Cisco Secure Malware Analytics アプライアンスは、配置更新サービス用の Cisco Secure Endpoint プライベートクラウドとの統合をアウトバウンド接続としてサポートします。

（注） 特に新しいアプライアンスを設定する場合は、Cisco Secure Malware Analytics アプライアンス配置更新サービスと Cisco Secure Endpoint プライベートクラウドの統合の設定タスクを、指定された順序に従ってデバイスで実行する必要があります。すでにセットアップして設定されているアプライアンスを統合する場合は、順序はそれほど重要ではありません。

実行するタスクの詳細については、Cisco Secure Endpoint プライベートクラウドのマニュアルを参照してください。

手順

ステップ 1 Cisco Secure Malware Analytics アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして設定します。更新を確認し、必要に応じてインストールします。

ステップ 2 Cisco Secure Endpoints プライベートクラウドを通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 3 Cisco Secure Malware Analytics アプライアンス管理 UI で、**[設定（Configuration）]** タブをクリックし、**[SSL]**を選択します。

ステップ 4 必要に応じて、クリーンインターフェイスで SSL 証明書を再生成してデフォルトの証明書を置き換え、そのコピーを作成して Cisco Secure Endpoint プライベートクラウド デバイスにインストールする（詳細については、「SSL 証明書の再生成」 を参照）。

ステップ 5 Cisco Secure Endpoint プライベート クラウド デバイスで統合を設定するために必要な次の情報を取得します。

- **ホスト名**：**[Configuration] > [Hostname]** をクリックし、ホスト名をメモします。
- **API キー**：Cisco Secure Malware Analytics ポータルの **[ユーザーの詳細（User Details）]** ページから **API キー** をコピーします（**[管理（Administration）]** タブをクリックし、[ユーザーの **管理（Manage Users**）] を選択してから、統合ユーザーアカウントに移動して、**[ユーザーの詳細（User Details）]** ページで API キーを見つけます）。

（注）
この手順を実行するには管理者ユーザーでなければならないというわけではありません。Cisco Secure Malware Analytics アプライアンスで、この目的のために特別にユーザーを作成することも可能です。

ステップ 6 Cisco Secure Malware Analytics アプライアンスとの統合用に Cisco Secure Endpoint プライベート クラウド デバイスを設定する。詳細な手順については、ESA/WSA 製品のマニュアルを参照してください。この設定により、AMP が Cisco Secure Malware Analytics アプライアンスと通信できるようになります。これで、Cisco Secure Malware Analytics にサンプルを送信できるようになりました。

ステップ 7 残りの手順を実行して、処理結果を Cisco Secure Malware Analytics アプライアンスに通知するように廃棄更新サービスを設定します（詳細については、「Secure Endpoint プライベートクラウド」のユーザーマニュアルを参照してください）。

a) 必要に応じて、DNS を設定します。「DNS の構成」を参照してください。
b) 統合先のデバイスを信頼できるように、Cisco Secure Endpoint プライベートクラウド SSL 証明書を Cisco Secure Endpoint アプライアンスにダウンロードするかコピーして貼り付けます。「CA 証明書」を参照してください。
c) Cisco Secure Malware Analytics ポータル UI で、AMP 処理更新サービスの URL とログイン情報を指定し、**[追加（Add）]** をクリックします（配置更新の配信サービスの管理」を参照）。

配置更新の配信サービスの管理

Cisco Secure Malware Analytics ポータルで、Cisco Secure Endpoint Private Cloud アプライアンス統合の Disposition Update Syndication Service を管理できます。URL は、[**Disposition Update Syndication Service**] ページで追加、編集、削除できます。

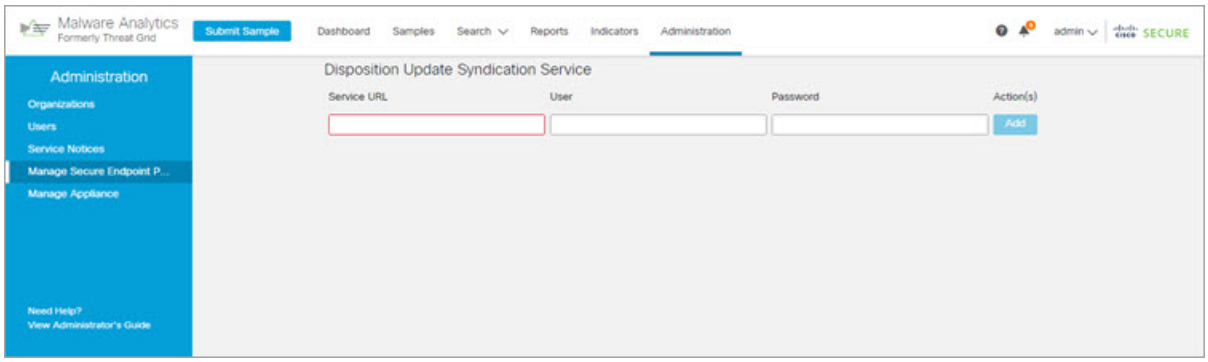
インバウンドおよびアウトバウンド接続

（注） Cisco Secure Endpoint プライベートクラウド アプライアンス統合の詳細については、 Cisco Secure Endpoint プライベート クラウドを Cisco Secure Malware Analytics アプライアンスに接続を参照してください。

手順

ステップ 1 Cisco Secure Malware Analytics ポータルで、**[管理（Administration）]** タブをクリックし、**[Secure Endpoint プライベートクラウドとの統合の管理（Manage Secure Endpoint Private Cloud Integration）]** を選択して **[Disposition Update Syndication Service]** ページを開きます。

図 *1*: 配置更新の配信サービス



ステップ 2 次の情報を入力します。

- **Service URL** - Cisco Secure Endpoint プライベート クラウド URL。
- **[User]**：管理者ユーザー名。
- **パスワード** - Cisco Secure Endpoint 構成ポータルにより提供されたパスワード。

ステップ 3 **[追加（Add）]** をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。