Cisco Secure Email Cloud Gateway と脅威防御の統合

この章は、次の項で構成されています。

Threat Defense Connector の概要

Threat Defense Connector クライアントは、Secure Email Cloud Gateway を Secure Email Threat Defense に接続して、高度なフィッシングとスプーフィングのメッセージをスキャンします。クラウドベースの高度な脅威スキャンを実行する機能は、組織が次のことを実行するために役立ちます。

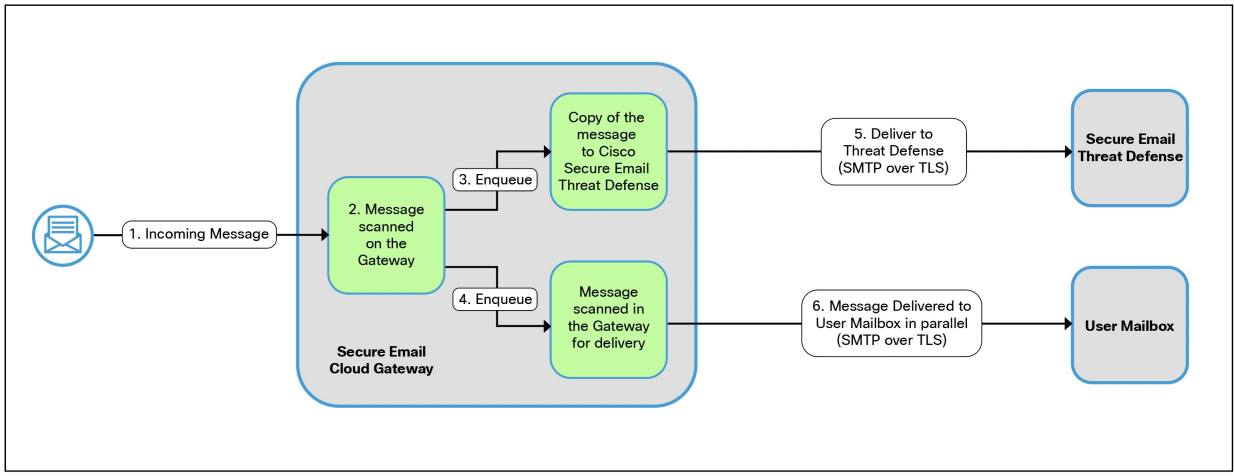
- 高度なフィッシングおよびスプーフィング ソリューションを入手する
- 常に変化するフィッシングの問題に対して、これまでよりはるかに迅速にセキュリティソリューションを利用する

Threat Defense Connector を設定すると、Cisco Secure Email Cloud Gateway は実際のメッセージのコピーを添付ファイルとして Threat Defense ポータルのメッセージ受信アドレスにジャーナル形式で送信します。

メッセージが Cisco Secure Email Cloud Gateway のすべてのスキャンエンジンによってスキャンされ、メッセージが安全に配信されると、メッセージは複製されます。メッセージのコピーはキューに入れられ、RFC 822 形式の添付ファイルとして Cisco Secure Email Threat Defense に送信され、高度なスキャンが実行されます。元のメッセージは元の受信者に配信されます。

Email Cloud Gateway は、SMTP カンバセーションの Cisco Secure Email Threat Defense で必要とされる最小の TLS 1.2 を使用して、標準の SMTP インターフェイスを介して高度な脅威スキャンを目的とした電子メールを送信します。Threat Defense はメッセージをスキャンし、ユーザーのメールボックスに最初に配信されたメッセージに対して適切な修復アクションが実行されます。

図 *1 : Threat Defense Connector* の概要



関連項目

- Threat Defense Conncetor を使用するように電子メールゲートウェイを設定する方法 （2 ページ）

Threat Defense Conncetor を使用するように電子メールゲートウェイを設定する方法

次の手順を順番に実行します。

手順	操作手順	詳細情報
ステップ 1	（Cisco Secure Email Threat Defense 上）Cisco Secure Email Cloud Gateway からの電子メールを受信するように Cisco Secure Email Threat Defense ポータルを設定します。	『Cisco Secure Email Threat Defense User Guide』の「Set up Secure Email Threat Defense」
ステップ 2	Cisco Secure Email Threat Defense ポータルからメッセージ受信アドレスを取得します。	『Cisco Secure Email Threat Defense User Guide』。
ステップ 3	Cisco Secure Email Cloud Gateway で Threat Defense Connector を有効にして設定します。	Email Cloud Gateway での Threat Defense Connector の有効化 (4 ページ)

Cisco Secure Email Cloud Gateway からメッセージを受信するための Threat Defense ポータルの設定

電子メール管理者は、Cisco Secure Email Cloud Gateway からメッセージを受信するように Cisco Secure Email Threat Defense を設定する必要があります。詳細については、『Secure Email Threat Defense User Guide』の「Set up Secure Email Threat Defense」の章を参照してください。

メッセージ受信アドレスの取得

メッセージ受信アドレスは、Cisco Secure Email Threat Defense セットアップページに表示されます。初期設定後にジャーナルアドレスを見つける必要がある場合は、[アカウントの詳細（Account Details）]セクションの [設定（Settings）]（歯車アイコン）>[管理（Administration）] > [ビジネス（Business）] ページで見つけることができます。詳細については、「Cisco Secure Email Threat Defense FAQ」を参照してください。

Email Cloud Gateway での Threat Defense Connector の有効化

始める前に

Cisco Secure Email Threat Defense からメッセージ受信アドレスを受信していることを確認します。また、このドメインと受信者アドレスへのメール配信が許可されていることを確認します。

（注） メール配信にカスタムSMTPルートを使用する場合は、メッセージ受信アドレスドメインへの配信に DNS を使用していることを確認します。たとえば、SMTP ルートのドメインに「USEDNS」を使用します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Threat Defense Connector] をクリックします。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 [Threat Defense Connector の有効化（Enable Threat Defense Connector）] チェックボックスをオンにします。

ステップ 4 Email Threat Defense ポータルから取得したメッセージ受信アドレスを入力します。

ステップ 5 [送信（Submit）] をクリックし、変更をコミットします。

Email Cloud Gateway での Threat Defense Connector の無効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Threat Defense Connector] をクリックします。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [Threat Defense Connector の有効化（Enable Threat Defense Connector）] チェックボックスをオフにします。

ステップ 4 [送信（Submit）] をクリックし、変更をコミットします。

Threat Defense Connector およびクラスタ

中央管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで Threat Defense Connector を有効にできます。

（注） マシンレベルで Threat Defense Connector を無効にすると、グループレベルとクラスタレベルでも無効になります。

Threat Defense Connector レポートのモニタリング

Threat Defense Connector の高度なスキャンレポートを表示するには、Cisco Secure Threat Defense ポータルにログインする必要があります。詳細については、『Cisco Secure Email Threat Defense User Guide』を参照してください。

[モニタ（Monitor）]>[配信ステータス（Delivery Status）] で、送信メールの配信ステータスを表示できます。[配信ステータス（Delivery Status）] ページは、特定の受信者ドメインに関する電子メール動作のモニタリング情報を提供します。Threat Defense Connector が有効になっている場合、**.tdc.queue** 宛先ドメインの下のメッセージ受信アドレスへのメールの配信ステータスを表示できます。

関連項目

- [送信処理ステータス（Delivery Status）] ページ

ログの表示

Threat Defense Connector の情報は、プレフィックス「TDC」を付けてメールログに投稿されます。

Threat Defense Connector ログエントリの例

- メッセージの配信失敗 - TLS エラー （5 ページ）

メッセージの配信失敗 - TLS エラー

この例のログは、Threat Defense と通信する際の TLS エラーのために配信されなかったメッセージを示しています。

```
17 Aug 2022 05:52:04 (GMT +00:00) Message 3 queued for delivery.
17 Aug 2022 05:52:04 (GMT +00:00) (DCID O) Delivery started for message 3 to
astra_victim@astra-cs.com.
17 Aug 2022 05:52:04 (GMT +00:00) (CID O) Delivery details: Message 3 sent to astra
```

```
victim@astra-cs.com
17 Aug 2022 05:52:04 (GMT +00:00) Incoming connection (ICID 3) lost.
17 Aug 2022 05:52:04 (GMT +00:00) Message 3 to astra_victim@astra-cs.com received remote
 SMTP response "/dev/null'
17 Aug 2022 05:52:04 (GMT +00:00) TDC: Message 4 delivery failed to Cisco Secure Email
Threat Defense: TLS Error.
```

ソリューション

このエラーをさらに調査して修正するには、Cisco Technical Assistance Center（TAC）に連絡してください。

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。