Cisco クラウド Web セキュリティ プロキシへのアプライアンスの接続

この章で説明する内容は、次のとおりです。

クラウドコネクタ モードで機能を設定および使用する方法

クラウドコネクタのサブセットに含まれる機能の使用方法は、注記した点を除き、標準モードと同じです。詳細については、操作モードの比較を参照してください。

このトピックは本書のさまざまな個所と関連し、標準モードとクラウド Web セキュリティコネクタモードの両方に共通する Web セキュリティアプライアンス の主要機能の一部は、それらの個所に記載されています。クラウドへのディレクトリ グループの送信に関する情報およびクラウド コネクタの設定情報を除き、関連情報は本書の他の個所に記載されています。

このトピックには、標準モードでは適用できないクラウド Web セキュリティコネクタの設定に関する情報が含まれています。

本書には、Cisco クラウド Web セキュリティ製品に関する情報は記載されていません。Cisco クラウド Web セキュリティのドキュメントは、

http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html [英語] から入手できます。

クラウド コネクタ モードでの展開

アプライアンスの初期設定時に、クラウド コネクタ モードと標準モードのどちらで展開するかを選択します。必要なライセンスを所有している場合は、現在展開されているアプライアンスでシステム セットアップ ウィザードを標準モードで実行し、これをクラウド コネクタ モードで再展開することもできます。システム セットアップ ウィザードを実行すると、既存の設定は上書きされ、既存のすべてのデータが削除されます。

アプライアンスの展開は標準モードとクラウド セキュリティ モードのどちらにおいても同様ですが、オンサイト Web プロキシ サービスおよびレイヤ 4 トラフィック モニター サービスは、クラウド Web セキュリティ コネクタ モードでは使用できません。

クラウド Web セキュリティ コネクタは、明示的な転送モードまたは透過モードで展開できます。

初期設定後にクラウド コネクタの設定を変更するには、[ネットワーク（Network）] > [クラウド コネクタ（Cloud Connector）] を選択します。

関連項目

- 接続、インストール、設定

クラウド コネクタの設定

始める前に

「仮想アプライアンスでの Web インターフェイスへのアクセスの有効化」を参照してください。

ステップ 1 Web セキュリティアプライアンス の Web インターフェイスにアクセスします。

インターネット ブラウザに Web セキュリティアプライアンス の IPv4 アドレスを入力します。

初めてシステム セットアップ ウィザードを実行するときは、以下のデフォルトの IPv4 アドレスを使用します。

```
https://192.168.42.42:8443
```

または

```
http://192.168.42.42:8080
```

ここで、`192.168.42.42` はデフォルトの IPv4 アドレス、`8080` は、HTTP のデフォルトの管理ポート設定、`8443` は HTTPS のデフォルトの管理ポートです。

ステップ 2 [システム管理（System Administration）] > [システム セットアップ ウィザード（System Setup Wizard）] を選択します。

ステップ 3 ライセンス契約の条項に同意します。

ステップ 4 [セットアップの開始（Begin Setup）] をクリックします。

ステップ 5 システム設定項目を設定します。

設定	説明
デフォルト システム ホスト名（Default System Hostname）	Web セキュリティアプライアンス の完全修飾ホスト名。
DNS サーバー（DNS Server(s)）	ドメイン名サービス ルックアップ用のインターネット ルート DNS サーバー。 DNS の設定も参照してください。
NTP サーバー（NTP Server）	システム クロックと同期させるサーバー。デフォルトは time.ironport.com です。
タイム ゾーン	アプライアンス上にタイム ゾーンを設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプが正確に表示されるようにします。

ステップ 6 アプライアンス モードの [クラウド Web セキュリティ コネクタ（Cloud Web Security Connector）] を選択します。

ステップ 7 クラウド コネクタの設定項目を設定します。

設定	説明
クラウド Web セキュリティ プロキシ サーバー（Cloud Web Security Proxy Servers）	クラウド プロキシ サーバー（CPS）のアドレス（例：proxy1743.scansafe.net）。
失敗のハンドリング（Failure Handling）	AsyncOS がクラウド Web セキュリティ プロキシへの接続に失敗した場合、インターネットに [直接接続（Connect directly）] するか、[要求をドロップ（Drop requests）] します。
Cloud Web Security 認証スキーム（Cloud Web Security Authorization Scheme）	トランザクションを認証する方式： • Web セキュリティアプライアンス の一般向け IPv4 アドレス • 各トランザクションに含まれている認証キー。Cisco Cloud Web Security Portal 内で認証キーを生成できます。

ステップ 8 ネットワーク インターフェイスおよび配線を設定します。

設定	説明
イーサネット ポート（Ethernet Port）	M1 インターフェイスを管理トラフィック専用として設定する場合は、データ トラフィック用の P1 インターフェイスを設定する必要があります。ただし、管理トラフィックとデータ トラフィックの両方をM1インターフェイスとして使用する場合でも、P1 インターフェイスを設定できます。
[IPアドレス（IP Address）]	Web セキュリティアプライアンス を管理するために使用する IPv4 アドレス。
ネットワーク マスク（Network Mask）	このネットワーク インターフェイス上の Web セキュリティアプライアンス を管理する際に使用するネットワークマスク。
ホスト名（Hostname）	このネットワーク インターフェイス上の Web セキュリティアプライアンス を管理する際に使用するホスト名。

ステップ 9 管理およびデータ トラフィックのルートを設定します。

設定	説明
デフォルト ゲートウェイ（Default Gateway）	管理インターフェイスやデータ インターフェイスを通過するトラフィックに使用するデフォルトのゲートウェイの IPv4 アドレス。
名前（Name）	スタティック ルートの識別に使用する名前。
内部ネットワーク（Internal Network）	このルートのネットワーク上の宛先の IPv4 アドレス。
内部ゲートウェイ（Internal Gateway）	このルートのゲートウェイの IPv4 アドレス。ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。

ステップ 10 透過的接続の設定項目を設定します。

（注） デフォルトでは、クラウドコネクタはトランスペアレントモードで展開され、レイヤ4スイッチまたは WCCP バージョン 2 ルータと接続する必要があります。

設定	説明
レイヤ 4 スイッチ（Layer-4 Switch） または デバイスなし（No Device）	• Web セキュリティアプライアンス はレイヤ 4 スイッチに接続されます。 または • 明示的な転送モードでクラウド コネクタを展開します。

設定	説明
WCCP v2 ルータ（WCCP v2 Router）	Web セキュリティアプライアンス は WCCP バージョン 2 対応ルータに接続されます。 注：パスフレーズは任意であり、7 文字以内の文字を含めることができます。

ステップ 11 管理設定項目を設定します。

設定	説明
管理者パスフレーズ（Administrator Passphrase）	Web セキュリティアプライアンス にアクセスするためのパスフレーズ。パスフレーズは 6 文字以上にする必要があります。
システム アラート メールの送信先（Email system alerts to）	アプライアンスによって送信されるアラートの宛先メール アドレス。
SMTP リレー ホスト経由で電子メールを送信（Send Email via SMTP Relay Host）	（任意）AsyncOS がシステムによって生成された電子メール メッセージの送信に使用する SMTP リレー ホストのホスト名またはアドレス。 デフォルトの SMTP リレー ホストは、MX レコードにリストされているメール サーバーです。 デフォルトのポート番号は 25 です。
オートサポート（AutoSupport）	アプライアンスは、シスコ カスタマー サポートにシステム アラートと毎週のステータス レポートを送信できます。

ステップ 12 レビューしてインストールします。

a) インストールを確認します。
b) 前に戻って変更する場合は、[前へ（Previous）] をクリックします。
c) 入力した情報を使って続行する場合は、[この設定をインストール（Install This Configuration）] をクリックします。

次のタスク

関連項目

- セキュア データの漏洩防止 （8 ページ）
- ネットワーク インターフェイス
- TCP/IP トラフィック ルートの設定
- トランスペアレント リダイレクションの設定

- アラートの管理
- SMTP リレー ホストの設定

クラウドのディレクトリ グループの使用による Web アクセスの制御

Cisco クラウド Web セキュリティを使用して、ディレクトリ グループに基づいてアクセスを制御できます。Cisco クラウド Web セキュリティへのトラフィックがクラウドコネクタモードの Web セキュリティアプライアンス を介してルーティングされている場合、Cisco クラウド Web セキュリティは、グループベースのクラウドポリシーを適用できるように、クラウドコネクタからトランザクションと共にディレクトリグループ情報を受け取る必要があります。

始める前に

Web セキュリティアプライアンス の設定に認証レルムを追加します。

ステップ 1 [ネットワーク（Network）] > [クラウドコネクタ（Cloud Connector）] に移動します。
ステップ 2 [クラウドポリシーディレクトリ グループ（Cloud Policy Directory Groups）] 領域で、[グループの編集（Edit Groups）] をクリックします。
ステップ 3 Cisco クラウド Web セキュリティ内で作成したクラウド ポリシーの対象となる [ユーザー グループ（User Groups）] と [マシン グループ（Machine Groups）] を選択します。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [完了（Done）] をクリックして、変更を確定します。

次のタスク

関連情報

- 認証レルム

クラウド プロキシ サーバーのバイパス

クラウド ルーティング ポリシーを使用すると、以下の特性に基づいて、Web トラフィックを Cisco クラウド Web セキュリティ プロキシにルーティングしたり、インターネットに直接ルーティングできたりします。

- **識別プロファイル**
- プロキシ ポート（Proxy Port）
- Subnet
- URL カテゴリ

- ユーザー エージェント

クラウド コネクタ モードでクラウド ルーティング ポリシーを作成するプロセスは、標準モードを使用してルーティング ポリシーを作成するプロセスと同じです。

関連項目

- ポリシーの作成

クラウド コネクタ モードでの FTP および HTTPS の部分的サポート

クラウドコネクタモードの Web セキュリティアプライアンス では、FTP および HTTPS が完全にはサポートされていません。

FTP

FTP はクラウド コネクタではサポートされません。アプライアンスがクラウド コネクタ用に設定されている場合、AsyncOS はネイティブ FTP トラフィックをドロップします。

FTP over HTTP はクラウド コネクタ モードでサポートされます。

HTTPS

クラウド コネクタは復号をサポートしていません。復号せずに HTTPS トラフィックを渡します。

クラウド コネクタは復号をサポートしていないため、通常、AsyncOS は HTTPS トラフィックのクライアント ヘッダー情報にアクセスできません。したがって、通常、AsyncOS は暗号化されたヘッダー情報に依存するルーティング ポリシーを適用できません。これは、透過的 HTTPS トランザクションでよくあることです。たとえば、透過的 HTTPS トランザクションの場合、AsyncOS は HTTPS クライアント ヘッダー内のポート番号にアクセスできないため、ポート番号に基づいてルーティング ポリシーを照合できません。この場合、AsyncOS はデフォルトのルーティング ポリシーを使用します。

明示的な HTTPS トランザクションの場合は 2 つの例外があります。AsyncOS は、明示的 HTTPS トランザクションの以下の情報にアクセスできます。

- URL
- 宛先ポート番号

明示的 HTTPS トランザクションの場合は、URL またはポート番号に基づいてルーティング ポリシーを照合できます。

セキュア データの漏洩防止

[ネットワーク（Network）] > [外部 DLP サーバー（External DLP Servers）] で、クラウド コネクタを外部のデータ漏洩防止サーバーと統合できます。

関連項目

- 機密データの漏洩防止

グループ名、ユーザー名、IP アドレスの表示

設定したグループ名、ユーザー名、IP アドレスを表示するには、whoami.scansafe.net にアクセスします。

クラウド コネクタ ログへの登録

クラウド コネクタ ログには、認証されたユーザーやグループ、クラウド ヘッダー、認証キーなど、クラウド コネクタの問題のトラブルシューティングに役立つ情報が含まれています。

ステップ 1 [システム管理（System Administration）] > [ログ サブスクリプション（Log Subsctiptions）] に移動します。
ステップ 2 [ログタイプ（Log Type）] メニューから [クラウドコネクタログ（Cloud Connector Logs）] を選択します
ステップ 3 [ログ名（Log Name）] フィールドに名前を入力します。
ステップ 4 ログ レベルを設定します。
ステップ 5 変更を [実行（Submit）] して [確定する（Commit）] します。

次のタスク

関連項目

- ログによるシステム アクティビティのモニター

クラウド Web セキュリティ コネクタの使用による識別プロファイルと認証

クラウド Web セキュリティ コネクタは、基本認証および NTLM をサポートしています。また、特定の宛先に対して認証をバイパスできます。

クラウド コネクタ モードで Active Directory レルムを使用すると、トランザクション要求を特定のマシンから発信された要求として識別できます。マシン ID サービスは標準モードでは使用できません。

2 つの例外を除き、認証は Web セキュリティアプライアンス 全体で同様に機能します。標準構成であるかクラウドコネクタ構成であるかは問いません。次に例外を示します。

- マシン ID サービスは標準モードでは使用できません。
- アプライアンスがクラウド コネクタ モードに設定されている場合、AsyncOS は Kerberos をサポートしません。

（注） ユーザー エージェントまたは宛先 URL に基づく識別プロファイルは、HTTPS トラフィックに対応していません。

関連項目

- ポリシーの適用に対するマシンの識別 （9 ページ）
- 未認証ユーザーのゲスト アクセス （10 ページ）
- ポリシーの適用に対するエンドユーザーの分類
- エンドユーザー クレデンシャルの取得の概要

ポリシーの適用に対するマシンの識別

マシン ID サービスを有効にすると、AsyncOS は、認証済みユーザーや IP アドレスなどの識別子ではなく、トランザクション要求を実行したマシンに基づいてポリシーを適用できるようになります。AsyncOS は NetBIOS を使用してマシン ID を取得します。

（注） マシン ID サービスは Active Directory レルムを介してのみ使用できることに注意してください。Active Directory レルムが設定されていない場合、このサービスはディセーブルになります。

ステップ 1 [ネットワーク（Network）] > [マシンIDサービス（Machine ID Service）] を選択します。

ステップ 2 [設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3 マシン ID の設定項目を設定します。

設定	説明
マシン ID の NetBIOS の有効化（Enable NetBIOS for Machine Identification）	マシン ID サービスをイネーブルにする場合に選択します。
レルム	トランザクション要求を開始しているマシンの識別に使用する Active Directory レルム。
失敗のハンドリング（Failure Handling）	AsyncOS がマシンを識別できない場合に、トランザクションをドロップするか、ポリシーの照合を続行するかを指定します。

ステップ 4 変更を [実行（Submit）] して [確定する（Commit）] します。

未認証ユーザーのゲスト アクセス

クラウドコネクタモードで、未認証ユーザーにゲストアクセスを提供するように Web セキュリティアプライアンス が設定されている場合、AsyncOS は __GUEST_GROUP__ グループにゲストユーザーを割り当て、その情報を Cisco クラウド Web セキュリティに送信します。未認証ユーザーにゲスト アクセスを提供するには、ID を使用します。これらのゲスト ユーザーを制御するには、Cisco クラウド Web セキュリティ ポリシーを使用します。

関連項目

- 認証失敗後のゲスト アクセスの許可

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。