



Firepower Threat Defense のプラットフォーム設定

Firepower Threat Defense デバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、いくつかのデバイス間でその値を共有できます。デバイスごとに異なる設定が必要な場合でも、共有ポリシーを作成し、該当するデバイスにそれを適用する必要があります。

- [ARP インспекションの設定 \(1 ページ\)](#)
- [バナー設定 \(3 ページ\)](#)
- [フラグメントの処理の設定 \(4 ページ\)](#)
- [HTTP の設定 \(5 ページ\)](#)
- [ICMP アクセス ルールの設定 \(7 ページ\)](#)
- [SSL 設定 \(9 ページ\)](#)
- [セキュア シェルの設定 \(13 ページ\)](#)
- [SMTP の設定 \(15 ページ\)](#)
- [SNMP の脅威に対する防御の設定 \(15 ページ\)](#)
- [Syslog の設定 \(22 ページ\)](#)
- [グローバル タイムアウトの設定 \(37 ページ\)](#)
- [脅威に対する防御のための NTP 時刻同期の設定 \(39 ページ\)](#)

ARP インспекションの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インспекションを有効にします。

ARP インспекションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インспекションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インспекションをイネーブルにすると、/Firepower Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、/Firepower Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように /Firepower Threat Defense デバイスを設定できます。



(注) 専用の/診断インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [ARP インспекション (ARP Inspection)] を選択します。

ステップ 3 ARP インспекション テーブルにエントリを追加します。

- a) [追加 (Add)] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集 (Edit)] アイコンをクリックします。
- b) 任意のオプションを選択します。
 - [インспекション有効 (Inspect Enabled)] : 選択されているインターフェイスとゾーンの ARP インспекションを実行します。
 - [フラッディング有効 (Flood Enabled)] : 静的 ARP エントリに一致しない ARP 要求を元のインターフェイスまたは専門の管理インターフェイス以外のすべてのインターフェイスにフラッディングします。これはデフォルトの動作です。

ARP 要求のフラッドイングを選択しない場合、静的 ARP エントリに一致する要求のみが許可されます。

- [セキュリティゾーン (Security Zones)]: 選択されているアクションを実行するインターフェイスを含むゾーンを追加します。ゾーンはスイッチドゾーンにする必要があります。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加 (Add)]をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。

c) [OK] をクリックします。

ステップ 4 [スタティック ARP エントリの追加](#)に従って、静的 ARP エントリを追加します。

ステップ 5 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

バナー設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デバイスの CLI (コマンドラインインターフェイス) に接続するユーザを表示するよう、メッセージを設定できます。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [バナー (Banner)] を選択します。

ステップ 3 バナーを設定します。

以下は、バナーのコツと要件です。

- 使用できる文字は ASCII 文字のみです。回線返品 (Enter を押します) を使用できますが、タブを使用できません。
- デバイスのホスト名またはドメイン名は、**\$(hostname)** 変数と **\$(domain)** 変数を組み込むことによってダイナミックに追加できます。

- バナーに長さの制限はありませんが、バナー メッセージの処理に十分なシステム メモリがない場合、Telnet または SSH セッションは閉じます。
- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。侵入者を招き入れる可能性があるため、「ようこそ」や「お願いします」などの言葉は使用しないでください。次のバナーは、不正アクセスに対する適切な基調を定めます。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

ステップ 4 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

フラグメントの処理の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、Firepower Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、[チェーン (Chain)] を 1 に設定してフラグメントを許可しないようにすることをお勧めします。フラグメント化されたパケットは、サービス妨害 (DoS) 攻撃によく使われます。



- (注) これらの設定は、このポリシーが割り当てられたデバイスのデフォルトになります。インターフェイス構成で [デフォルトフラグメント設定のオーバーライド (Override Default Fragment Setting)] を選択することで、デバイスの特定のインターフェイスでこれらの設定をオーバーライドできます。インターフェイスを編集する際、[詳細 (Advanced)] > [セキュリティ設定 (Security Configuration)] タブでオプションを確認できます。> [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択して、Firepower Threat Defense デバイスを編集し、[インターフェイス (Interfaces)] タブを選択して、インターフェイスのプロパティを編集します。>

手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [フラグメント (Fragment)] を選択します。
- ステップ 3** 次のオプションを設定します。デフォルト設定を使用する場合は、[デフォルトにリセット (Reset to Defaults)] をクリックします。
- [サイズ (ブロック (Size (Block))] : リアセンブルを待機可能な、すべての集成的な接続からのパケットフラグメントの最大数。デフォルトは 200 フラグメントです。
 - [チェーン (フラグメント) (Chain (Fragment))] : 1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。フラグメントを許可しない場合は、このオプションを 1 に設定します。
 - [タイムアウト (秒) (Timeout (Sec))] : フラグメント化されたパケット全体の到着を待機する最大秒数を設定します。デフォルトは 5 秒です。すべてのフラグメントがこの時間内に受信されなかった場合、すべてのフラグメントが破棄されます。
- ステップ 4** [保存 (Save)] をクリックします。
- これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

HTTP の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

HTTPS 接続を Firepower Threat Defense デバイスの複数のインターフェイスに対して許可するには、HTTPS 設定を行います。トラブルシューティングでパケットキャプチャをダウンロードするために、HTTPS を使用できます。

始める前に

- HTTPS の使用で、ホスト IP アドレスを許可するアクセスルールは必要ありません。このセクションの手順に従って、HTTPS アクセスを設定する必要があるだけです。
- 到達可能なインターフェイスにのみ HTTPS を使用できます。HTTPS ホストが外部インターフェイスにある場合は、外部インターフェイスへの直接的な管理接続のみ開始できます。

- デバイスでは、最大 5 つの HTTPS 接続を同時にできます。
- デバイスへの HTTPS 接続に許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクトグループを使用する場合は、ルールに必要なグループがすでに存在することを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してオブジェクトを設定します。
- 物理管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有されます。この設定は、診断論理インターフェイスを使用すると、こちらにのみ適用されます。管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。Firepower Management Center にデバイスを設定し、登録するために使用されます。これには、個別の IP アドレスとスタティック ルーティングがあります。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [HTTP] を選択します。

ステップ 3 [HTTP サーバを有効にする (Enable HTTP server)] をクリックして、HTTPS サーバを有効にします。

ステップ 4 (任意) HTTPS ポートを変更します。デフォルトは 443 です。

ステップ 5 HTTPS 接続を許可する IP アドレスとインターフェイスを指定します。

このテーブルを使用して、HTTPS 接続および HTTPS 接続が許可されているクライアントの IP アドレスを承認するインターフェイスを制限します。個々の IP アドレスではなく、ネットワーク アドレスを使用することができます。

- a) [追加 (Add)] をクリックして新しいルールを追加するか、[編集 (Edit)] アイコンをクリックして既存のルールを編集します。
- b) ルールのプロパティを設定します。
 - [IP アドレス (IP Address)] : HTTPS 接続を許可するホストまたはネットワークを識別するネットワーク オブジェクト。ドロップダウン メニューからオブジェクトを選択するか、または + ボタンをクリックして新しいネットワーク オブジェクトを追加します。
 - [セキュリティゾーン (Security Zones)] : HTTPS 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。

c) [OK] をクリックします。

ステップ 6 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

ICMP アクセス ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- Firepower Threat Defense デバイスは、ブロードキャストアドレス宛での ICMP エコー要求に応答しません。
- Firepower Threat Defense デバイスは、トラフィックが着信するインターフェイス宛での ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセスルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対していずれかの ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージタイプだけを拒否する場合は、残りのメッセージタイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージタイプ (タイプ 3) には常にアクセス許可を付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリが無効化され、IPsec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。

始める前に

ルールに必要なオブジェクトがすでに存在していることを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、オブジェクトを設定します。> 任意のホストまたはネットワークを定義するネットワークオブジェクトまたはグループ、あるいは制御する ICMP メッセージタイプを定義するポート オブジェクトが必要です。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [ICMP] を選択します。

ステップ 3 ICMP ルールを設定します。

- a) [追加 (Add)] をクリックして新しいルールを追加するか、[編集 (Edit)] アイコンをクリックして既存のルールを編集します。
- b) ルールのプロパティを設定します。
 - [アクション (Action)] : 一致するトラフィックを許可または拒否 (ドロップ) するかどうかを指定します。
 - [ICMP サービス (ICMP Service)] : ICMP メッセージタイプを識別するポート オブジェクト。
 - [ネットワーク (Network)] : アクセスを制御しているホストまたはネットワークを識別するネットワーク オブジェクトまたはグループ。
 - [セキュリティゾーン (Security Zones)] : 保護しているインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。
- c) [OK] をクリックします。

ステップ 4 (オプション) ICMPv4 到達不能メッセージをレート制限します。

- [レート制限 (Rate Limit)] : 到達不能メッセージのレート制限を、1 秒あたり 1 ~ 100 の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
- [バースト サイズ (Burst Size)] : バースト レートを 1 ~ 10 の範囲で設定します。現在、この値はシステムによって使用されていません。

ステップ 5 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

SSL 設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート コンプライアンス	該当なし	Firepower Threat Defense	リーフのみ	Admin

始める前に

完全にライセンス供与されたバージョンの Firepower Management Center を実行していることを確認する必要があります。評価モードで Firepower Management Center を実行している場合は、[SSL 設定 (SSL Settings)] タブは無効になります。また、ライセンス供与された Firepower Management Center のバージョンがエクスポートのコンプライアンス基準を満たしていない場合、[SSL 設定 (SSL Settings)] タブは無効になります。SSL でリモート アクセス VPN を使用している場合、スマートアカウントで強力な暗号化機能が有効になっている必要があります。詳細については、[スマート ライセンスのタイプと制約事項](#)を参照してください。

手順

-
- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [SSL] を選択します。
- ステップ 3** エントリを、[SSL 設定の追加 (Add SSL Configuration)] テーブルに追加します。
- [追加 (Add)] をクリックして新しいエントリを作成するか、エントリがすでにある場合は、[編集 (Edit)] アイコンをクリックします。
 - ドロップダウンリストから必要なセキュリティ設定を選択します。
 - [プロトコルバージョン (Protocol Version)] : リモート アクセス VPN セッションを設定するときに使用する TLS プロトコルを指定します。
 - [セキュリティレベル (Security Level)] : SSL で設定するセキュリティポジショニングのタイプを指定します。
- ステップ 4** 選択するプロトコルバージョンに基づく [使用可能なアルゴリズム (Available Algorithms)] を選択し、[追加 (Add)] をクリックして選択したプロトコルに含めます。詳細については、次を参照してください。[SSL 設定について \(10 ページ\)](#)
- アルゴリズムは、選択するプロトコルバージョンに基づいてリストされます。それぞれのセキュリティプロトコルは、セキュリティレベルの設定の一意のアルゴリズムを識別します。
- ステップ 5** [OK] をクリックして変更を保存します。
-

次のタスク

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。

SSL 設定について

Firepower Threat Defense デバイスでは、セキュアソケットレイヤ (SSL) プロトコルと Transport Layer Security (TLS) を使用して、リモートクライアントからのリモートアクセス VPN のセキュアメッセージ伝送をサポートします。[SSL 設定 (SSL Settings)] ウィンドウでは、SSL でのリモート VPN アクセス中に、ネゴシエートとメッセージ伝送に使用される SSL バージョンと暗号化アルゴリズムを設定できます。

SSL 設定は、次の場所で構成します。

[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] > [SSL]

フィールド

[最小 SSL バージョン サーバ (Minimum SSL Version Server)] : Firepower Threat Defense デバイスがサーバとして動作するとき使用する最小バージョンの SSL/TLS プロトコルを指定します。たとえば、リモートアクセス VPN ゲートウェイとして機能する場合があります。ドロップダウンリストからプロトコルバージョンを選択します。

TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1 (以降) をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1 (以降) をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2 (以降) をネゴシエートします。

[Diffie-Hellman グループ (Diffie-Hellmann Group)] : ドロップダウンリストからグループを選択します。使用可能なオプションは、[Group1] (768 ビット絶対値)、[Group2] (1024 ビット絶対値)、[Group5] (1536 ビット絶対値)、[Group14] (2048 ビット絶対値、224 ビット素数位数)、および [Group24] (2048 ビット絶対値、256 ビット素数位数) です。デフォルト値は [Group1] です。

[楕円曲線 Diffie-Hellman グループ (Elliptical Curve Diffie-Hellman Group)] : ドロップダウンリストからグループを選択します。使用可能なオプションは、[Group19] (256 ビット EC)、[Group20] (384 ビット EC)、および [Group21] (521 ビット EC) です。デフォルト値は [Group19] です。

TLSv1.2 では、次の暗号方式のサポートが追加されています。

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384

- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256



(注) 優先度が最も高いのは ECDSA 暗号方式と DHE 暗号方式です。

Firepower Threat Defense デバイスでサポートしたいプロトコルバージョン、セキュリティレベル、および暗号アルゴリズムを指定するために、SSL 設定テーブルを使用できます。

[プロトコルバージョン (Protocol Version)] : Firepower Threat Defense デバイスでサポートされ、SSL 接続に使用されるプロトコルバージョンを一覧表示します。利用可能なプロトコルバージョンは次のとおりです。

- デフォルト
- TLSV1
- TLSV1.1
- TLSV1.2
- DTLSv1

[セキュリティレベル (Security Level)] : Firepower Threat Defense デバイスでサポートされ、SSL 接続に使用される暗号セキュリティレベルを一覧表示します。次のいずれかのオプションを選択します。

[すべて (All)] : NULL-SHA を含めたすべての暗号方式。

[低 (Low)] : NULL-SHA を除くすべての暗号方式。

[中 (Medium)] : NULL-SHA、DES-CBC-SHA、RC4-SHA、および RC4-MD5 を除くすべての暗号方式を含む (これがデフォルトです)。

[FIPS] : NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号方式を含む。

[高(High)] : SHA-2 暗号を使用する AES-256 のみを含み、TLS バージョン 1.2 およびデフォルトバージョンに適用される。

[カスタム (Custom)] : [暗号アルゴリズム/カスタム文字列 (Cipher Algorithms/Custom String)] ボックスで指定する1つ以上の暗号方式を含む。このオプションでは、OpenSSL暗号定義文字列を使用して暗号スイートを詳細に管理できます。

[暗号アルゴリズム/カスタム文字列 (Cipher Algorithms/Custom String)] : Firepower Threat Defense デバイスでサポートされ、SSL接続に使用される暗号アルゴリズムを一覧表示します。OpenSSLを使用した暗号の詳細については、<https://www.openssl.org/docs/apps/ciphers.html> を参照してください。 <https://www.openssl.org/docs/apps/ciphers.html>

Firepower Threat Defense デバイスでは、サポートされる暗号方式の優先度が次のように指定されています。

TLSv1.2 のみでサポートされる暗号方式

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 または TLSv1.2 でサポートされない暗号方式

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

セキュア シェルの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Firepower Threat Defense デバイスの 1 つ以上のインターフェイスへの SSH 接続を許可するには、セキュア シェル設定を行います。

始める前に

- SSH は診断インターフェイスに対してサポートされていません。
- SSH ローカルユーザは、**configure user add** コマンドを使用して CLI でのみ設定できます。デフォルトでは、初期設定時にパスワードを設定した **Admin** ユーザが存在します。
- SSH トラフィックでは、設定または CLI で設定されたスタティック ルートではなく、通常のルーティング設定が使用されます。
- SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。
- SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。
- デバイスでは、最大 5 つの同時 SSH 接続を許可できます。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。手順の一部としてオブジェクトを追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールに必要なグループがすでに存在することを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してオブジェクトを設定します。



(注) システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [セキュア シェル (Secure Shell)] を選択します。

ステップ 3 (オプション) SSH アクセスの制限を変更します。

- [SSH バージョン (SSH Version)] : デフォルトでは、ユーザは SSH バージョン 1 および 2 を使用して接続できます。これらのバージョンの 1 つのみにアクセスを制限できます。たとえば SSH バージョン 2 のみをサポートする場合は、**2** を選択します。
- [タイムアウト (Timeout)] : システムがセッションを切断するまでに SSH セッションがアイドル状態を維持する時間の長さ。タイムアウトは 1 ~ 60 分に設定します。デフォルトは 5 分です。
- [セキュア コピーを有効にする (Enable Secure Copy)] : デバイスのセキュア コピー (SCP) サーバを有効にするかどうか。これにより、デバイスはデバイスとの間でファイルを転送するための SCP サーバとして機能できます。SSH を使用したセキュリティ アプライアンスへのアクセスを許可されるクライアントだけが、セキュア コピー接続を確立できます。SCP には、SSH バージョン 2 が必要です。

ステップ 4 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH 接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワークアドレスを使用できます。

- a) [追加 (Add)] をクリックして新しいルールを追加するか、[編集 (Edit)] アイコンをクリックして既存のルールを編集します。
- b) 次のルールプロパティを設定します。
 - [IP アドレス (IP Address)] : SSH 接続を許可するホストまたはネットワークを特定するネットワーク オブジェクト。オブジェクトをドロップダウンメニューから選択するか、または + ボタンをクリックして新しいネットワーク オブジェクトを追加します。
 - [セキュリティゾーン (Security Zones)] : SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンに存在しないインターフェイスの場合は、[選択されたセキュリティゾーン (Selected Security Zone)] リストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。これらのルールは、デバイスに選択したインターフェイスまたはゾーンが含まれている場合にのみ適用されます。
- c) [OK] をクリックします。

ステップ 5 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

SMTP の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Syslog 設定で電子メールアラートを設定する場合は、SMTP サーバを指定する必要があります。Syslog で設定する送信元電子メールアドレスは、SMTP サーバの有効なアカウントである必要があります。

始める前に

プライマリおよびセカンダリ SMTP サーバのホストアドレスを定義するネットワークオブジェクトが存在することを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択してオブジェクトを定義します。または、ポリシーの編集時にオブジェクトを作成することもできます。

手順

- ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2 [SMTP サーバ (SMTP Server)] をクリックします。
- ステップ 3 [プライマリ サーバの IP アドレス (Primary Server IP Address)]、およびオプションで、[セカンダリ サーバの IP アドレス (Secondary Server IP Address)] を特定するネットワークオブジェクトを選択します。
- ステップ 4 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

SNMP の脅威に対する防御の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

簡易ネットワーク管理プロトコル (SNMP) は、PC またはワークステーションで実行されているネットワーク管理ステーションが、スイッチ、ルータ、セキュリティアプライアンスなどのさまざまなタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。[SNMP] ページを使用して、SNMP 管理ステーションによってモニタされるようにファイアウォール デバイスを設定できます。

簡易ネットワーク管理プロトコル (SNMP) は、集中管理する場所からのネットワークデバイスのモニタリングをイネーブルにします。Cisco セキュリティアプライアンスでは、SNMP バージョン 1、2c、および 3 を使用したネットワークモニタリングに加えて、トラップおよび SNMP 読み取りアクセスがサポートされます。SNMP 書き込みアクセスはサポートされません。

SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。



(注) 外部 SNMP サーバでアラートを作成するには、[ポリシー (Policies)] > [アクション (Action)] > [アラート (Alerts)] にアクセスします。 > >

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [SNMP] を選択します。

ステップ 3 SNMP を有効にし、基本オプションを設定します。

- [SNMP サーバを有効にする (Enable SNMP Servers)] : 設定された SNMP ホストに SNMP 情報を提供するかどうかを指定します。このオプションの選択を解除すると、設定情報を保持したまま、SNMP モニタリングをディセーブルにできます。
- [コミュニティストリングの表示 (Read Community String)]、[確認 (Confirm)] : SNMP 管理ステーションが Firepower Threat Defense デバイスに要求を送信する際に使用するパスワードを入力します。SNMP コミュニティストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティ デバイスでは、このパスワードを使用して、着信 SNMP 要求が有効かどうかを判断します。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。
- [システム管理者名 (System Administrator Name)] : デバイス管理者またはその他の担当者の名前を入力します。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [場所 (Location)] : このセキュリティ デバイスの場所を入力します (Building 42, Sector 54 など)。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
- [ポート (Port)] : 着信要求が受け入れられる UDP ポートを入力します。デフォルトは 161 です。

ステップ 4 (SNMPv3 のみ) [SNMPv3 ユーザの追加 \(17 ページ\)](#)。

ステップ 5 [SNMP ホストの追加 \(19 ページ\)](#)。

ステップ6 **SNMP** トラップの設定 (20 ページ)。

ステップ7 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

SNMPv3 ユーザの追加



(注) SNMPv3 でのみユーザを作成できます。以下の手順は、SNMPv1 または SNMPv2c には適用されません。

SNMPv3 は読み取り専用ユーザのみをサポートすることに注意してください。

SNMP ユーザには、ユーザ名、認証パスワード、暗号化パスワードおよび使用する認証アルゴリズムと暗号化アルゴリズムが指定されています。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES と AES128 です。

手順

- ステップ1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ2 目次の [SNMP] をクリックして、[ユーザ (User)] タブをクリックします。
- ステップ3 [追加 (Add)] をクリックします。
- ステップ4 [セキュリティ レベル (Security Level)] ドロップダウン リストからユーザに適したセキュリティ レベルを選択します。
 - **Auth** : 認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
 - **No Auth** : 認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
 - **Priv** : 認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。
- ステップ5 [ユーザ名 (Username)] フィールドに SNMP ユーザの名前を入力します。このユーザ名は 32 文字以下であることが必要です。
- ステップ6 [暗号化パスワードタイプ (Encryption Password Type)] ドロップダウン リストから使用するパスワードのタイプを選択します。
 - **Clear text** : Firepower Threat Defense デバイスは、デバイスへの導入時を待ってパスワードを暗号化します。

- **Encrypted** : Firepower Threat Defense デバイスは、暗号化を済ませたパスワードを直接展開します。

ステップ 7 [認証アルゴリズム タイプ (Auth Algorithm Type)] ドロップダウン リストから MD5 または SHA のうち、使用する認証タイプを選択します。

ステップ 8 認証に使用するパスワードを、[認証パスワード (Authentication Password)] フィールドに入力します。暗号化パスワードタイプに [暗号化 (Encrypted)] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。

(注) パスワードの長さは、選択した認証アルゴリズムによって異なります。すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリアテキスト (Clear Text)] を選択した場合、[確認 (Confirm)] フィールドにパスワードをもう一度入力してください。

ステップ 9 [暗号化タイプ (Encryption Type)] ドロップダウン リストで、AES128、AES192、AES256、3DES、DES の中から使用する暗号化タイプを選択します。

(注) AES または 3DES 暗号化を使用するには、デバイスに適切なライセンスをインストールしておく必要があります。

ステップ 10 [暗号化パスワード (Encryption Password)] フィールドに暗号化で使用するパスワードを入力します。暗号化パスワードタイプに [暗号化 (Encrypted)] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。暗号化を行う場合のパスワードの長さは選択された暗号化のタイプにより異なります。パスワードの長さは次のとおりです (各 xx は 1 つのオクテットを示します) 。

- AES 128 では 16 オクテットとする必要があります
- AES 192 では 24 オクテットとする必要があります
- AES 256 では 32 オクテットとする必要があります
- 3DES では 32 オクテットとする必要があります
- DES の長さはさまざまです。

(注) すべてのパスワードの長さを 256 文字以下とする必要があります。

暗号化パスワードタイプに [クリアテキスト (Clear Text)] を選択した場合、[確認 (Confirm)] フィールドにパスワードをもう一度入力してください。

ステップ 11 [OK] をクリックします。

ステップ 12 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

SNMP ホストの追加

[ホスト (Host)] タブを使用して、[SNMP] ページにある [SNMP ホスト (SNMP Hosts)] テーブルのエントリを追加または編集します。これらのエントリは、Firepower Threat Defense デバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

始める前に

SNMP 管理ステーションを定義するネットワークオブジェクトが存在することを確認します。[デバイス (Device)] > [オブジェクト管理 (Object Management)] を選択し、ネットワークオブジェクトを設定します。 >



(注) サポートされているのは IPv4 アドレスだけです。

手順

- ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2 目次の [SNMP] をクリックして、[ホスト (Hosts)] タブをクリックします。
- ステップ 3 [追加 (Add)] をクリックします。
- ステップ 4 [IP アドレス (IP Address)] フィールドで、SNMP 管理ステーションのホストアドレスを決定するネットワークオブジェクトを選択します。
- ステップ 5 [SNMP バージョン (SNMP Version)] ドロップダウンリストから、適切な SNMP バージョンを選択します。
- ステップ 6 (SNMPv3 のみ) [ユーザ名 (User Name)] ドロップダウンリストから設定した SNMP ユーザのユーザ名を選択します。

(注) SNMP ホストごとに 23 人までの SNMP ユーザを関連付けることができます。
- ステップ 7 (SNMPv1、2c のみ) [Read コミュニティストリング (Read Community String)] フィールドに、デバイスの読み取りアクセスのためにすでに設定してあるコミュニティストリングを入力します。確認のためにこの文字列を再入力します。

(注) この文字列は、この SNMP ステーションで使用されている文字列が [SNMP サーバを有効にする (Enable SNMP Server)] セクションに定義済みのものと異なる場合のみ必須です。
- ステップ 8 デバイスと SNMP 管理ステーションの間の通信タイプを選択します。両方のタイプを選択できます。
 - [ポーリング (Poll)] : 管理ステーションは定期的にデバイスに情報を要求します。
 - [トラップ (Trap)] : デバイスは、イベント発生時にこれをトラップし、管理ステーションに送信します。

- ステップ 9** [ポート (Port)]フィールドに、SNMPホストのUDPポート番号を入力します。デフォルト値は162です。有効な範囲は1～65535です。
- ステップ 10** [追加 (Add)]をクリックし、このSNMP管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。
- ステップ 11** [ゾーン/インターフェイス (Zones/Interfaces)]リストに、デバイスが管理ステーションとの通信を行うインターフェイスが含まれたゾーンを追加します。ゾーン内がないインターフェイスの場合は、[選択したゾーン/インターフェイス (Selected Zone/Interface)]リストの下のフィールドにインターフェイス名を入力し、[追加 (Add)]をクリックします。デバイスに選択されたインターフェイスやゾーンが含まれる場合のみデバイスにホストが設定されます。
- ステップ 12** [OK] をクリックします。
- ステップ 13** [保存 (Save)] をクリックします。
- これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

SNMP トラップの設定

[SNMP トラップ] タブを使用して、Firepower Threat Defense デバイスの SNMP トラップ (イベント通知) を設定します。トラップは参照とは異なります。トラップは、生成されるリンクアップイベント、リンクダウンイベント、Syslog イベントなど、特定のイベントに対する Firepower Threat Defense デバイスから管理ステーションへの割り込み「コメント」です。デバイスの SNMP オブジェクト ID (OID) は、デバイスから送信される SNMP イベントトラップに表示されます。

一部のトラップは、特定のハードウェアモデルに適用できません。これらのトラップは、これらのモデルの1つのポリシーを適用すると無視されます。たとえば、すべてのモデルに現場交換可能ユニットがあるわけではありません。そのため、[現場交換可能ユニット挿入/削除 (Field Replaceable Unit Insert/Delete)] トラップはこれらのモデルで設定されません。

手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** 目次の [SNMP] をクリックし、[SNMP トラップ (SNMP Traps)] タブをクリックして、Firepower Threat Defense デバイスの SNMP トラップ (イベント通知) を設定します。
- ステップ 3** 適切な [Enable Traps] オプションを選択します。いずれかまたは両方のオプションを選択できます。
- [すべての SNMP トラップを有効にする (Enable All SNMP Traps)] にマークを付けて、連続する 4 セクションですべてのトラップを素早く選択します。
 - [すべての Syslog トラップを有効にする (Enable All Syslog Traps)] にマークを付けて、トラップ関連の Syslog メッセージの伝送を有効にします。

ステップ 4 [標準 (Standard)] セクションのイベント通知トラップは、既存のポリシーでは、デフォルトで有効になっています。

- [認証 (Authentication)] : 未認可の SNMP アクセス。この認証エラーは、間違ったコミュニティストリングが付いたパケットによって発生します。
- [リンクアップ (Link Up)] : 通知に示されているとおり、デバイスの通信リンクの1つが使用可能になりました。
- [リンクダウン (Link Down)] : 通知に示されているとおり、デバイスの通信リンクの1つにエラーが発生しました。
- [コールドスタート (Cold Start)] : デバイスが自動で再初期化しているときに、その設定またはプロトコル エンティティの実装が変更されることがあります。
- [ウォームスタート (Warm Start)] : デバイスが自動で再初期化しているときに、その設定またはプロトコル エンティティの実装が変更されることはありません。

ステップ 5 [エンティティ MIB (Entity MIB)] セクションで好きなイベント通知トラップを選択します。

- [現場交換可能ユニット挿入 (Field Replaceable Unit Insert)] : 示されているとおり、現場交換可能ユニット (FRU) が挿入されました (FRU には電源装置、ファン、プロセッサモジュール、インターフェイス モジュールなどの組み立て部品が含まれます)。
- [現場交換可能ユニット除外 (Field Replaceable Unit Remove)] : 通知に示されているとおり、現場交換可能ユニット (FRU) が取り外されました。
- [設定変更 (Configuration Change)] : 通知に示されているとおり、ハードウェアに変更がありました。

ステップ 6 [リソース (Resource)] セクションで好きなイベント通知トラップを選択します。

- [接続制限到達 (Connection Limit Reached)] : このトラップは、設定した接続制限に達したため、接続試行が拒否されたことを示します。

ステップ 7 [その他 (Other)] セクションで好きなイベント通知トラップを選択します。

- [NAT パケット破棄 (NAT Packet Discard)] : IP パケットが NAT 機能により廃棄されると、この通知が生成されます。ネットワーク アドレス変換の使用可能なアドレスまたはポートが、設定したしきい値を下回りました。

ステップ 8 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

Syslog の設定

Firepower Threat Defense デバイスのシステム ロギング (syslog) を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。ここでは、ロギングとその設定方法について説明します。

Syslog について

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログ用の保護された長期ストレージを提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

Firepower Threat Defense では、syslog を 2 つの場所で構成できます。

- [プラットフォーム設定 (Platform Settings)]: この syslog 設定では、データプレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバ、NAT などの機能が含まれます。データプレーンの syslog メッセージには番号が付けられており、ASA ソフトウェアを実行しているデバイスで生成されるものと同じです。しかし、Firepower Threat Defense は、必ずしも ASA ソフトウェアで使用可能なすべてのメッセージタイプを生成するとは限りません。これらのメッセージの詳細については、『[Cisco ASA Series Syslog Messages](#)』を参照してください。この構成については、次のトピックで説明します。
- [アラート応答 (Alert Responses)]: この syslog 設定では、[アラート応答のサポート設定](#) で説明されているように、アクセス制御ルール、侵入ルール、およびその他のアドバンスド サービスに関するアラートが生成されます。これらのメッセージには番号が付けられていません。このタイプの syslog の設定については、[Syslog アラート応答の作成](#) を参照してください。

複数の syslog サーバを設定し、各サーバに送信されるメッセージとイベントを制御できます。また、コンソール、電子メール、内部バッファなどの異なる宛先を構成することもできます。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。

表 1: syslog メッセージの重大度

レベル番号	重大度	説明
[0]	緊急	システムが使用不可能な状態です。
1	アラート	すぐに措置する必要があります。
2	重大	深刻な状況です。
3	error	エラー状態です。
4	警告	警告状態です。
5	通知	正常ですが、注意を必要とする状況です。
[6]	情報	情報メッセージです。
7	デバッグ	デバッグ メッセージです。



(注) /Firepower Threat Defense は、重大度 0 (緊急) の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、/Firepower Threat Defense デバイスを設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージクラス (機能エリアと同等)

これらの基準は、出力先を設定するときに指定可能なメッセージリストを作成して、カスタマイズできます。あるいは、メッセージリストとは無関係に、特定のメッセージクラスを各タイプの出力先に送信するように /Firepower Threat Defense デバイスを設定することもできます。

syslog メッセージクラス

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージクラスを指定するメッセージリストを作成します。

syslog メッセージクラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc (VPN クライアント) クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ~ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネルグループ、Username はローカルデータベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモートアクセスクライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージクラスと各クラスのメッセージ ID の範囲をリストします。

表 2: セージクラスおよび関連するメッセージ ID 番号

クラス	定義 (Definition)	メッセージ ID 番号
auth	ユーザ認証	109、113
ブリッジ	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
config	コマンドインターフェイス	111、112、208、308
電子メール (e-mail)	電子メール プロキシ	719
ha	フェールオーバー (ハイ アベイラビリティ)	101、102、103、104、105、210、311、709
ids	侵入検知システム	400、401、415
ip	IP スタック	209、215、313、317、408
np	ネットワークプロセッサ	319
ospf	OSPF ルーティング	318、409、503、613

クラス	定義 (Definition)	メッセージ ID 番号
rip	RIP ルーティング	107、312
rm	Resource Manager	321
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
webvpn	Web ベースの VPN	716

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

- IPv6 がサポートされます。Syslog は、TCP または UDP を使用して送信できます。
- syslog 送信用に設定されたインターフェイスが有効であること、IPv6 対応であること、および syslog サーバが指定インターフェイス経由で到達できることを確認します。
- Ipv6 を介したセキュア ロギングはサポートされていません。

その他のガイドライン

- syslog サーバでは、syslogd というサーバプログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。

- /Firepower Threat Defense デバイスが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、/Firepower Threat Defense デバイスはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。
 - 2つの異なるリストまたはクラスを異なる syslog サーバまたは同じ場所に割り当てることはできません。
 - 最大 16 台の syslog サーバを設定できます。
 - syslog サーバは、/Firepower Threat Defense デバイス 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、313004、および 313005 の生成を抑制します。
 - syslog の UDP 接続の数は、ハードウェアプラットフォームの CPU の数と、設定する syslog サーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定する syslog サーバの数を乗算した値と同じになります。たとえば各 syslog サーバでは次のようになります。
 - Firepower 4110 では最大 22 の UDP syslog 接続が可能です。
 - Firepower 4120 では最大 46 の UDP syslog 接続が可能です。
- これは予期されている動作です。グローバル UDP 接続アイドルタイムアウトはこれらのセッションに適用され、デフォルトは2分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。
- /Firepower Threat Defense デバイスが TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。

Syslog 設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Syslog の設定を行うには、以下の手順を実行します。

手順

- ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2 目次の [Syslog] をクリックします。
- ステップ 3 [ロギング設定 (Logging Setup)] タブをクリックしてロギングを有効にし、FTP サーバの設定を指定し、フラッシュの使用を指定します。詳細については、次を参照してください。 [ロギングの有効化および基本設定の構成 \(27 ページ\)](#)
- ステップ 4 [ロギング接続先 (Logging Destinations)] タブをクリックして、特定の接続先へのロギングを有効にし、メッセージ重要度、イベント クラスまたはカスタム イベント リストでフィルタリングを指定します。詳細については、次を参照してください。 [ロギング接続先の有効化 \(29 ページ\)](#)
- ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。
- ステップ 5 [電子メール設定 (E-mail Setup)] タブをクリックして、Syslog メッセージを電子メールとして送信する際に、その送信元アドレスとして使用する電子メールアドレスを指定します。詳細については、次を参照してください。 [電子メールアドレスへの syslog メッセージの送信 \(30 ページ\)](#)
- ステップ 6 [イベントリスト (Events List)] タブをクリックして、イベントクラス、重要度、イベント ID を含むカスタム イベント リストを定義します。詳細については、次を参照してください。 [カスタム イベント リストの作成 \(31 ページ\)](#)
- ステップ 7 [レート制限 (Rate Limit)] タブをクリックして、設定されているすべての宛先に送信されるメッセージの量を指定し、レート制限を割り当てるメッセージの重大度を定義します。詳細については、次を参照してください。 [Syslog メッセージの生成レートの制限 \(33 ページ\)](#)
- ステップ 8 [Syslog 設定 (Syslog Settings)] タブをクリックして、サーバを Syslog 接続先として設定するために、ロギング機能を指定し、タイムスタンプの包含を有効にし、他の設定を有効にします。詳細については、次を参照してください。 [Syslog 設定 \(34 ページ\)](#)
- ステップ 9 [Syslog サーバ (Syslog Servers)] タブをクリックして、ロギング接続先として指定される Syslog サーバの IP アドレス、使用されているプロトコル、形式、およびセキュリティゾーンを指定します。詳細については、次を参照してください。 [Syslog サーバの設定 \(35 ページ\)](#)

ロギングの有効化および基本設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

データ プレーン イベントの syslog メッセージを生成するには、システムでロギングを有効にする必要があります。

また、ローカルバッファがいっぱいになると、フラッシュまたはFTPサーバ上のアーカイブを保存場所として設定することもできます。ログデータは保存後に操作できます。たとえば、特定タイプのsyslogメッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

次の手順では、基本的な syslog 設定の一部について説明します。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [syslog] > [ロギングの設定 (Logging Setup)] を選択します。

ステップ 3 ロギングを有効にし、基本のロギング設定を構成します。

- [ロギングの有効化 (Enable Logging)] : Firepower Threat Defense デバイスのデータ プレーンシステム ロギングをオンにします。
- フェールオーバースタンバイユニットでのロギングの有効化 (Enable Logging on the Failover Standby Unit) : Firepower Threat Defense デバイスのスタンバイのロギングをオンにします。
- EMBLEM 形式での syslog の送信 (Send syslogs in EMBLEM format) : すべてのロギング宛先に対して、EMBLEM形式のロギングを有効にします。EMBLEMを有効にする場合は、UDPプロトコルを使用してsyslogメッセージをパブリッシュする必要があります。EMBLEMはTCPと互換性がありません。
- デバッグメッセージを syslog として送信 (Send debug messages as syslogs) : すべてのデバッグトレース出力を syslog にリダイレクトします。このオプションが有効になっている場合、syslog メッセージはコンソールに表示されません。したがって、デバッグメッセージを表示するには、コンソールでロギングを有効にし、デバッグ syslog メッセージ番号とログレベルの宛先として設定する必要があります。使用される syslog メッセージ番号は 711011 です。この syslog のデフォルトログレベルは [デバッグ (debug)] です。
- 内部バッファのメモリ サイズ (Memory Size of Internal Buffer) : ロギングバッファが有効の場合に syslog メッセージが保存される内部バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。指定できる範囲は 4096 ~ 52428800 です。

ステップ 4 (オプション) [FMC へのロギングを有効化 (Enable Logging to FMC)] チェックボックスをオンにして、VPN ロギングを有効にします。[ログレベル (Logging Level)] ドロップダウンリストから、VPN メッセージの syslog セキュリティ レベルを選択します。

レベルについては、[重大度 \(22 ページ\)](#) を参照してください。

ステップ 5 (オプション) バッファが上書きされる前に、サーバにログバッファの内容を保存するには、FTP サーバを設定します。FTP サーバ情報を指定します。

- FTP サーババッファラップ (FTP Server Buffer Wrap) : バッファの内容が上書きされる前に FTP サーバに保存するには、このボックスをオンにし、次のフィールドに必要な宛先情報を入力します。FTP 設定を削除するには、このオプションを選択解除します。
- IP アドレス (IP Address) : FTP サーバの IP アドレスを含むホストネットワークオブジェクトを選択します。
- ユーザ名 (User Name) : FTP サーバに接続するときに使用するユーザ名を入力します。
- パス (Path) : バッファの内容を保存するパスを FTP ルートからの相対で入力します。
- パスワードの確認 (Password Confirm) : FTP サーバへのユーザ名の認証に使用されるパスワードを入力および確認します。

ステップ 6 (オプション) バッファが上書きされる前に、サーバにログバッファの内容を保存するには、フラッシュ サイズを指定します。

- フラッシュ (Flash) : バッファの内容が上書きされる前にフラッシュ メモリに保存するには、このチェックボックスをオンにします。
- ロギングに使用する最大フラッシュ (KB) (Maximum flash to be used by logging (KB)) : フラッシュ メモリ内でロギングに使用される最大領域を指定します (KB)。範囲は、4 ~ 8044176 バイトです。
- 保持する最小空き領域 (KB) (Minimum free space to be preserved (KB)) : フラッシュ メモリに保持する最小空き領域を指定します (KB)。範囲は、0 ~ 8044176 バイトです。

ステップ 7 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

ロギング接続先の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ロギング接続先を有効にして、その接続先でメッセージを表示可能にする必要があります。接続先を有効にするとき、その接続先に適用するメッセージフィルタも指定する必要があります。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [Syslog] > [ロギング接続先 (Logging Destinations)] を選択します。 >

- ステップ 3** 接続先を有効にし、ロギング フィルタを適用するか、または既存の接続先を編集するには、[追加 (Add)] をクリックします。
- ステップ 4** [ロギング接続先 (Logging Destinations)] ダイアログボックスで、接続先を選択し、接続先で使用するフィルタを設定します。
- [ロギング接続先 (Logging Destination)] ドロップダウンリストで、有効にする接続先を選択します。コンソール、メール、内部バッファ、SNMPトラップ、SSHセッション、Syslog サーバのそれぞれの接続先に各自のフィルタを作成できます。

(注) コンソールおよび SSH セッション ロギングは、診断 CLI でのみ機能します。
system support diagnostic-cli を入力します。
 - [イベントクラス (Event Class)] で、テーブルに表示されていないすべてのクラスに適用するフィルタを選択します。

次のフィルタを設定できます。

 - [重大度によるフィルタ (Filter on severity)] : 重大度のレベルを選択します。設定したレベル以上のメッセージが接続先に送られます。
 - [イベントリスト使用 (Use Event List)] : フィルタを定義するイベントリストを選択します。このイベントリストは [イベントリスト (Event Lists)] タブで作成します。
 - [ロギング無効 (Disable Logging)] : この接続先へのメッセージ送信を停止します。
 - イベントクラスごとのフィルタを作成するには、[追加 (Add)] をクリックして新しいフィルタを作成するか、既存のフィルタを編集し、そのクラスでのメッセージを制限するイベントクラスと重大度レベルを選択します。[OK] をクリックして、フィルタを保存します。

イベントクラスの説明については、[syslog メッセージクラス \(23 ページ\)](#) を参照してください。
 - [OK] をクリックします。
- ステップ 5** [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

電子メールアドレスへの syslog メッセージの送信

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

電子メールとして送信される syslog メッセージの受信者リストを設定できます。

始める前に

- SMTP サーバのプラットフォーム設定ページで SMTP サーバを設定します
- [ロギングの有効化および基本設定の構成](#) (27 ページ)
- [ロギング接続先の有効化](#)

手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [電子メールの設定 (Email Setup)] を選択します。
- ステップ 3** 電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メールアドレスを指定します。
- ステップ 4** [追加 (Add)] をクリックして、指定した syslog メッセージの受信者の新しい電子メールアドレスを入力します。
- ステップ 5** その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウンリストから選択します。
- 宛先の電子メールアドレスに対して適用される syslog メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。レベルについては、[重大度](#) (22 ページ) を参照してください。
- ステップ 6** [OK] をクリックします。
- ステップ 7** [保存 (Save)] をクリックします。
- これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

カスタム イベント リストの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

イベントリストは、ロギング接続先に適用して接続先に送信するメッセージを制御できるカスタムフィルタです。通常、重大度のみに基づいて接続先へのメッセージをフィルタリングしますが、イベントリストを使用して、イベントクラス、重大度、およびメッセージ識別子 (ID) の組み合わせに基づいて送信されるメッセージを微調整できます。

カスタム イベントリストの作成は、2 段階のプロセスです。[イベントリスト (Event Lists)] タブでカスタム リストを作成し、イベントリストを使用して、[宛先のロギング (Logging Destinations)] タブで各種宛先のロギング フィルタを定義します。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [Syslog] > [イベント リスト (Events List)] を選択します。

ステップ 3 イベント リストを設定します。

- a) [追加 (Add)] をクリックして新規リストを追加したり、既存のリストを編集したりします。
- b) [名前 (Name)] フィールドにイベントリストの名前を入力します。スペースは使用できません。
- c) 重大度またはイベントクラスに基づいてメッセージを識別するには、[重大度/イベントクラス (Severity/Event Class)] タブを選択して、項目を追加または編集します。

使用可能なクラスの詳細については、[syslog メッセージクラス \(23 ページ\)](#) を参照してください。

レベルについては、[重大度 \(22 ページ\)](#) を参照してください。

特定のイベントクラスは、トランスペアレント モードのデバイスには適用されません。そのようなオプションが設定された場合、オプションは無視され、展開されません。

- d) メッセージ ID を指定してメッセージを識別するには、[メッセージ ID (Message ID)] タブを選択し、ID を追加または編集します。

ハイフンを使用して ID 範囲を入力できます (たとえば、100000-200000)。ID は 6 桁の数字です。最初の 3 桁が機能にどのようにマップされるかについては、[syslog メッセージクラス \(23 ページ\)](#) を参照してください。

特定のメッセージ番号については、『[Cisco ASA Series Syslog Messages](#)』を参照してください。

- e) [OK] をクリックして、イベントリストを保存します。

ステップ 4 [ロギング接続先 (Logging Destinations)] タブをクリックし、フィルタを使用する必要がある接続先を追加または編集します。

[ロギング接続先の有効化 \(29 ページ\)](#) を参照してください。

ステップ 5 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

Syslog メッセージの生成レートの制限

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

syslog メッセージの生成レートは、重大度レベルまたはメッセージ ID によって制限できます。ロギングレベルごと、および Syslog メッセージ ID ごとに個別の制限を指定できます。設定が競合する場合は、Syslog メッセージ ID の制限が優先されます。

手順

- ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
 - ステップ 2 [Syslog] > [レート制限 (Rate Limit)] を選択します。
 - ステップ 3 重大度レベルによりメッセージの生成を制限するには、[ログレベル (Logging Level)] タブで [追加 (Add)] をクリックして、次のオプションを設定します。
 - ログレベル (Logging Level) : レートを制限する重大度レベル。レベルについては、[重大度 \(22 ページ\)](#) を参照してください。
 - メッセージ数 (Number of messages) : 指定した時間内に許容される指定したタイプのメッセージの最大数。
 - 間隔 (Interval) : レート制限カウンタがリセットされるまでの秒数。
 - ステップ 4 [OK] をクリックします。
 - ステップ 5 syslog のメッセージ ID によりメッセージの生成を制限するには、[Syslog レベル (Syslog Level)] タブで [追加 (Add)] をクリックし、次のオプションを設定します。
 - [Syslog ID] : レートを制限する syslog のメッセージ ID。特定のメッセージ番号については、『[Cisco ASA Series Syslog Messages](#)』を参照してください。
 - メッセージ数 (Number of messages) : 指定した時間内に許容される指定したタイプのメッセージの最大数。
 - 間隔 (Interval) : レート制限カウンタがリセットされるまでの秒数。
 - ステップ 6 [OK] をクリックします。
 - ステップ 7 [保存 (Save)] をクリックします。
- これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

Syslog 設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

一般的な Syslog 設定を設定して、Syslog サーバに送信される Syslog メッセージに含めるファシリティコードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [Syslog 設定 (Syslog Settings)] を選択します。 >
- ステップ 3** ファイルメッセージのベースとして使用する Syslog サーバのシステムログ機能を、[ファシリティ (Facility)] ドロップダウンリストから選択します。

デフォルトは LOCAL4(20) です。これは UNIX システムで最も可能性の高いコードです。ただし、ネットワーク デバイス間では使用可能なファシリティが共用されているため、システムログではこの値を変更しなければならない場合があります。
- ステップ 4** [タイムスタンプを各 Syslog メッセージで有効にする (Enable timestamp on each syslog message)] チェックボックスをオンにして、メッセージ生成日時を Syslog メッセージに含めます。
- ステップ 5** デバイス識別子を Syslog メッセージに追加する場合は (これはメッセージの先頭に配置されます) 、[Syslog デバイス ID を有効にする (Enable Syslog Device ID)] チェックボックスをオンにし、ID のタイプを選択します。
 - [インターフェイス (Interface)] : アプライアンスがメッセージの送信に使用するインターフェイスに関係なく、選択されたインターフェイスの IP アドレスを使用します。インターフェイスを識別するセキュリティゾーンを選択します。ゾーンは、単一のインターフェイスにマッピングされる必要があります。
 - [ユーザー定義 ID (User Defined ID)] : 選択したテキスト文字列を使用します (最大 16 文字) 。
 - [ホスト名 (Host Name)] : デバイスのホスト名を使用します。
- ステップ 6** [Syslog Message] テーブルを使用して、特定の Syslog メッセージのデフォルト設定を変更します。デフォルト設定を変更する場合にだけ、このテーブルでルールを設定する必要があります。メッセージに割り当てられている重大度を変更したり、メッセージの生成を無効にしたりできます。

デフォルトでは、NetFlow が有効になり、エント리는テーブルに表示されます。

- a) NetFlow が原因で冗長している Syslog メッセージを抑制するには、[ネットワーク同等 Syslog (Netflow Equivalent Syslogs)] を選択します。
- これにより、メッセージが抑止されたメッセージとしてテーブルに追加されます。
- (注) これらの同等の Syslog メッセージがすでにテーブルにある場合、既存のルールは上書きされません。
- b) ルールを追加するには、[追加 (Add)] ボタンをクリックします。
- c) 設定変更するメッセージ番号を [Syslog ID] ドロップダウンリストから選択し、新しい重大度を [ロギングレベル (Logging Level)] ドロップダウンリストから選択するか、または [抑制 (Suppressed)] を選択してメッセージの生成を無効にします。通常は、重大度レベルの変更やメッセージのディセーブル化は行いませんが、必要に応じて両方のフィールドを変更できます。
- d) [OK] をクリックしてテーブルにルールを追加します。

ステップ 7 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

Syslog サーバの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

データプレーンから生成されたメッセージを処理するように syslog サーバを設定するには、次の手順を実行します。

アクセスコントロールルールなど、接続やその他のイベントのために syslog サーバを設定するには、[Syslog アラート応答の作成](#) を参照してください。

手順

- ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。
- ステップ 2** [Syslog] > [Syslog サーバ (Syslog Server)] > を選択します。
- ステップ 3** [TCP syslog サーバのダウン時ユーザトラフィックの通過を許可 (Allow user traffic to pass when TCP syslog server is down)] チェックボックスをオンにして、TCP プロトコルを使用する Syslog サーバがダウンしている場合にトラフィックを許可するようにします。

ステップ 4 [メッセージキュー サイズ (メッセージ) (Message queue size (messages))] フィールドに、Syslogサーバが取り込み中の場合に、Syslogメッセージをセキュリティアプライアンスに保存するキューのサイズを入力します。最小件数は1件です。デフォルトは512です。無制限の数のメッセージをキューに入れる場合は、0を指定します (使用可能なブロックメモリによって制限されます)。

ステップ 5 [追加 (Add)] をクリックして、新しい Syslog サーバを追加します。

- a) [IP アドレス (IP Address)] ドロップダウンリストで、Syslog サーバの IP アドレスを含むネットワーク ホスト オブジェクトを選択します。
- b) プロトコル (TCP または UDP) を選択し、Firepower Threat Defense デバイスと Syslog サーバの間の通信のポート番号を入力します。

UDP のデフォルト ポートは 514、TCP のデフォルト ポートは 1470 です。有効な非デフォルトのポート値は、どちらのプロトコルでも 1025 ~ 65535 です。

- c) [Cisco EMBLEM 形式でのログ メッセージ (UDP のみ) (Log messages in Cisco EMBLEM format (UDP only))] チェックボックスをオンにして、Cisco の EMBLEM 形式でメッセージをログに記録するかどうかを指定します (プロトコルとして UDP が選択されている場合に限る)。
- d) [セキュア Syslog を有効にする (Enable Secure Syslog)] チェックボックスをオンにして、デバイスとサーバの間の接続を TCP の SSL/TLS を使用して暗号化します。

このオプションを使用するには、TCP をプロトコルとして選択する必要があります。また、[デバイス (Devices)] > [証明書 (Certificates)] ページで、Syslog サーバとの通信に必要な証明書をアップロードする必要があります。 >最後に、Firepower Threat Defense デバイスから syslog サーバに証明書をアップロードして、セキュアな関係を完成させ、トラフィックの復号化を許可します。

- e) Syslog サーバとの通信に使用するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、[選択されたゾーン/インターフェイス (Selected Zones/Interface)] リストの下のフィールドにインターフェイス名を入力し、[追加 (Add)] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときのみ、これらのルールがデバイスに適用されます。

(注) Syslog サーバが物理管理インターフェイスに接続されたネットワーク上にある場合は、そのインターフェイスの名前を [選択したセキュリティ ゾーン (Selected Security Zones)] リストの下の [インターフェイス名 (Interface Name)] フィールドに入力し、[追加 (Add)] をクリックする必要があります。また、診断インターフェイスにこの名前 (まだ設定されていない場合) と IP アドレスを設定する必要があります ([デバイス管理 (Device Management)] ページからデバイスを編集し、[インターフェイス (Interfaces)] タブを選択します)。管理/診断インターフェイスの詳細については、[診断インターフェイス](#) を参照してください。

- f) [OK] をクリックします。

ステップ 6 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

グローバル タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

さまざまなプロトコルの接続スロットと変換スロットのグローバルアイドルタイムアウト期間を設定できます。指定したアイドル時間の間スロットが使用されなかった場合、リソースはフリープールに戻されます。

また、デバイスのコンソールセッションでタイムアウトを設定できます。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [タイムアウト (Timeouts)] を選択します。

ステップ 3 変更するタイムアウトを設定します。

任意の設定で、[カスタム (Custom)] を選択して自分の値を定義し、[デフォルト (Default)] を選択してシステムのデフォルト値に戻します。ほとんどの場合、最大タイムアウトは 1193 時間です。

[無効 (Disable)] を選択して、タイムアウトを無効にできます。

- [コンソールタイムアウト (Console Timeout)] : コンソールへの接続が閉じられるまでのアイドル時間。範囲は、5 ~ 1440 分です。デフォルトは 0 で、セッションがタイムアウトしないことを示します。値を変更すると、既存のコンソールセッションで古いタイムアウト値が使用されます。新しい値は新しい接続にのみ適用されます。
- [変換スロット (Translation Slot (xlate))] : NAT 変換スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。
- [接続 (Connection (Conn))] : 接続スロットが解放されるまでのアイドル時間。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [ハーフクローズ (Half-Closed)] : TCP ハーフクローズ接続を閉じるまでのアイドル時間。最小値は 30 秒です。デフォルト値は 10 分です。

- [UDP] : UDP 接続を閉じるまでのアイドル時間。この期間は1分以上にする必要があります。デフォルトは2分です。
- [ICMP] : 全般的なICMP状態が終了するまでのアイドル時間。デフォルト（かつ最小値）は2秒です。
- [RPC/Sun RPC] : SunRPC スロットが解放されるまでのアイドル時間。この期間は1分以上にする必要があります。デフォルト値は10分です。
- [H.225] : H.225 シグナリング接続を閉じるまでのアイドル時間。デフォルトは1時間です。すべての呼び出しがクリアされた後に接続をすぐにクローズするには、タイムアウト値を1秒（0:0:1）にすることを推奨します。
- [H.323] : H.245（TCP）およびH.323（UDP）メディア接続が終了するまでのアイドル時間。デフォルト（かつ最小値）は5分です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続はH.323（RTP および RTCP）メディア接続とアイドルタイムアウトを共有します。
- [SIP] : SIP シグナリングポート接続を閉じるまでのアイドル時間。この期間は5分以上にする必要があります。デフォルトは30分です。
- [SIP メディア（SIP Media）] : SIP メディアポート接続を閉じるまでのアイドル時間。この期間は1分以上にする必要があります。デフォルトは2分です。SIP メディアタイマーは、SIP UDP メディアパケットを使用するSIP RTP/RTCPで、UDP非アクティブタイムアウトの代わりに使用されます。
- [SIP 接続解除（SIP Disconnect）] : CANCELメッセージまたはBYEメッセージで200 OKを受信しなかった場合に、SIPセッションを削除するまでのアイドル時間を0:0:1～0:10:0の範囲で指定します。デフォルトは、2分（0:2:0）です。
- [SIP インバイト（SIP Invite）] : 暫定応答のピンホールとメディアxlateを閉じるまでのアイドル時間（0:1:0～00:30:0）。デフォルトは、3分（0:3:0）です。
- [SIP 暫定メディア（SIP Provisional Media）] : SIP 暫定メディア接続のタイムアウト値（1～30分）。デフォルトは2分です。
- [フローティング接続（Floating Connection）] : 同じネットワークへの複数のルートが存在しており、それぞれメトリックが異なる場合、ASAは接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは0です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を0:0:30～1193:0:0の間で設定します。
- [Xlate PAT] : PAT変換スロットが解放されるまでのアイドル時間で、0:0:30～0:5:0の間です。デフォルトは30秒です。前の接続がアップストリームデバイスで引き続き開いている可能性があるため、開放されたPATポートを使用する新しい接続を上流に位置するルータが拒否する場合、このタイムアウトを増やすことができます。

- [TCP プロキシ リアセンブリ (TCP Proxy Reassembly)] : 再構築のためバッファ内で待機しているパケットをドロップするまでのアイドルタイムアウト (0:0:10 ~ 1193:0:0) 。デフォルトは、1分 (0:1:0) です。
- [ARP タイムアウト (ARP Timeout)] : (トランスペアレント モードのみ) 。ARP テーブルを再構築する間隔の秒数 (60 ~ 4294967) 。デフォルトは 14,400 秒 (4 時間) です。

ステップ 4 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

脅威に対する防御のための NTP 時刻同期の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

Network Time Protocol (NTP) を使用して、デバイスのクロック設定を同期します。デフォルトでは、デバイスは Firepower Management Center サーバを NTP サーバとして使用しますが、別の NTP サーバを設定することができます。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower Threat Defense ポリシーを作成または編集します。

ステップ 2 [時間の同期化 (Time Synchronization)] を選択します。

ステップ 3 次のいずれかのクロック オプションを設定します。

- [デフェンス センターの NTP 使用 (Via NTP from Defense Center)] : Firepower Management Center サーバを NTP サーバとして使用します。これがデフォルトです。
- [その他の NTP 使用 (Via NTP from)] : 別の NTP サーバの完全修飾 DNS 名 (ntp.example.com など) または IP アドレスを入力します。複数のアドレスを入力する場合は、各アドレスをカンマで区切ります (例 : ntp1.example.com, ntp2.example.com) 。

ステップ 4 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

脅威に対する防御のための NTP 時刻同期の設定