Firepower Threat Defense のプラットフォーム設定

FTD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 インスペクションの設定

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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 インスペクションをイネーブルにします。

ARPインスペクションによって、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 インスペク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 インスペク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。

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、FTD ポリシーを作成または編集します。

ステップ 2 [ARP インスペクション（ARP Inspection）] を選択します。

ステップ 3 ARP インスペクション 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。

- [インスペクション有効（Inspect Enabled）]：選択されているインターフェイスとゾーンの ARP インスペク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 要求のフラッディ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。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にのみ、これらのルールがデバイスに適用されます。

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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

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、FTD 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ので、「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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

DNS 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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower Threat Defense	任意	Access Admin Administrator Network Admin

DNS 解決の設定では、データ インターフェイスおよび診断インターフェイスの DNS を設定できます。また、DNS サーバに接続するための変数も設定できます。

始める前に

DNS サーバ グループを作成していることを確認します。この説明については、DNS サーバ グループ オブジェクトの作成 を参照してください。

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 [DNS] をクリックします。

ステップ 3 [デバイスによるDNS名前解決を有効にする（Enable DNS name resolution by device）] チェックボックスを選択します。

ステップ 4 作成済みの [DNS サーバ グループ（DNS Server Group）] を選択します。

ステップ 5 （オプション）[有効期限エントリ タイマー（Expiry Entry Timer）] と [ポール タイマー（Poll Timer）] の値を分単位で入力します。

- 有効期限エントリ タイマーでは、存続可能時間（TTL）経過後に、DNS ルックアップ テーブルから解決済み FQDN の IP アドレスを削除するまでの制限時間を指定します。エントリを削除するとテーブルの再コンパイルが必要になるため、頻繁に削除するとデバイスの処理負荷が増えることがあります。この設定は事実上 TTL を延長します。
- ポール タイマーでは、ネットワーク オブジェクト グループに定義されている FQDN を解決するために、デバイスが DNS サーバにクエリを行うまでの制限時間を指定します。FQDN は、ポール タイマーの期限切れ、または解決された IP エントリの TTL の期限切れのいずれかが発生すると定期的に解決されます。

（注） FQDN 解決の最初のインスタンスは、FQDN オブジェクトがアクセス コントロール ポリシーに展開された場合に発生します。

ステップ 6 （オプション）使用可能リストから必要なインターフェイス オブジェクトを選択し、[追加（Add）] を選択して、[選択済みインターフェイス オブジェクト（Selected Interface Objects）] リストに追加します。

インターフェイスを指定せず、診断インターフェイスで DNS ルックアップを有効にしない場合（次の手順を参照）、FTD はルーティング テーブルを使用してインターフェイスを決定します。一致しない場合は、管理ルーティング テーブルが使用されます。

ステップ 7 （オプション）[診断インターフェイス経由の DNS ルックアップも有効にする（Enable DNS Lookup via diagnostic interface also）] チェックボックスを選択します。

有効になっている場合、Firepower Threat Defense は、選択したデータ インターフェイスと診断インターフェイスの両方を DNS 解決に使用します。**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（edit device）] > [インターフェイス（Interfaces）]** ページで診断インターフェイスの IP アドレスを設定してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

アクセス制御ルールの FQDN オブジェクトを使用するには、アクセス制御ルールに割り当て可能な FQDN ネットワーク オブジェクトを作成します。手順については、ネットワーク オブジェクトの作成を参照してください。

SSH の外部認証の設定

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	管理者

管理ユーザの外部認証を有効にすると、FTD により外部認証オブジェクトで指定された LDAP または RADIUS サーバを使用してユーザ クレデンシャルが検証されます。

外部認証オブジェクトの共有

外部認証オブジェクトは、FMC、7000 および 8000 シリーズ、および FTD デバイスで使用できます。すべてのアプライアンス/デバイス タイプで同じオブジェクトを共有することも、別々のオブジェクトを作成することもできます。FTD は RADIUS サーバでのユーザの定義をサポートしますが、他のプラットフォームでは外部認証オブジェクトのユーザ リストを事前に認証する必要があります。FTD には事前に定義されているリスト方式を使用できますが、RADIUS サーバでユーザを定義する場合は FTD とその他のプラットフォームに個別のオブジェクトを作成する必要があります。

デバイスへの外部認証オブジェクトの割り当て

FMC では、**[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** タブで外部認証オブジェクトを直接有効にします。この設定は、FMC の使用にのみ影響し、管理対象デバイスを使用する場合には、このタブで有効にする必要はありません。7000 および 8000 シリーズ および FTD のデバイスでは、デバイスに展開するプラットフォーム設定で外部認証オブジェクトを有効にする必要があります。FTD、では、ポリシーごとにアクティブ化できる外部認証オブジェクトは 1 つのみです。CAC 認証を有効にした LDAP オブジェクトは、CLI アクセスでも使用することはできません。

FTD サポート対象フィールド

FTD SSH アクセスでは、外部認証オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを他のデバイス タイプにも使用する場合は、それらのフィールドが使用されます。この手順は、FTD でサポートされているフィールドのみを対象とします。その他のフィールドについては、外部認証の設定を参照してください。

ユーザ名

ユーザ名は Linux で有効な名前で、かつ、小文字のみである必要があり、英数文字とピリオド（.）およびハイフン（-）を使用できます。アットマーク（@）やスラッシュ（/）など、その他の特殊文字はサポートされていません。外部認証に **admin** ユーザを追加することはできません。外部ユーザは、FMC で（外部認証オブジェクトの一部として）追加することしかできません。CLI では追加できません。内部ユーザは、FMC ではなく、CLI でしか追加できないことに注意してください。

configure user add 内部ユーザとして同じユーザ名がコマンドを使用して設定されていた場合は、FTD は最初にその内部ユーザのパスワードをチェックし、それが失敗した場合は AAA サーバをチェックします。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。RADIUS サーバで定義されているユーザの場合は、内部ユーザの権限レベルと同じに設定してください。そうしないと、外部ユーザ パスワードを使用してログインできません。

Privilege Level

LDAP ユーザには常に Config 権限があります。RADIUS ユーザは、Config ユーザまたは Basic ユーザとして定義できます。

始める前に

- SSHアクセスは管理インターフェイス上でデフォルトで有効になります。データインターフェイス上で SSH アクセスを有効にするには、セキュア シェルの設定 （19 ページ）を参照してください。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。
- RADIUS ユーザに次の動作を通知し、適切に動作するようにします。
  - 外部ユーザが初めてログインすると、FTD は必要な構造体を作成しますが、ユーザセッションを同時に作成することはできません。ユーザがセッションを開始するには、再度認証する必要があるだけです。ユーザには次のようなメッセージが表示されます。「New external username identified. Please log in again to start a session.」
  - 同様に、最後のログイン以降に Service-Type で定義したユーザの認証が変更された場合は、ユーザは再認証する必要があります。ユーザには次のようなメッセージが表示されます。「Your authorization privilege has changed. セッションを開始するにはもう一度ログインしてください。（Please log in again to start a session.）」

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、FTD ポリシーを作成または編集します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 [外部認証サーバの管理（Manage External Authentication Server）] リンクをクリックします。

新しいブラウザタブで、**[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** 画面が開きます。

ステップ 4 LDAP 認証オブジェクトを設定します。

a) [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。
b) [認証方式（Authentication Method）] を [LDAP] に設定します。
c) [名前（Name）] とオプションの [説明（Description）] を入力します。
d) ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。
e) [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

（注） 証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

f) （任意） [ポート（Port）] をデフォルトから変更します。
g) （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。
h) [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。

- [ベースDN（Base DN）]：アクセスする LDAP ディレクトリのベース識別名を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。

- （オプション）[基本フィルタ（Base Filter）]：たとえば、ディレクトリ ツリー内のユーザ オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。
- [ユーザ名（User Name）]：LDAP サーバを参照するために十分なクレデンシャルを持つユーザの識別名を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。
- [パスワード（Password）] と [パスワードの確認（Confirm Password）]：ユーザのパスワードを入力して確認します。
- （オプション）[詳細オプションを表示（Show Advanced Options）]：次の詳細オプションを設定します。
  - **[暗号化（Encryption）]**：**[なし（None）]**、**[TLS]**、または **[SSL]** をクリックします。

    （注） ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

  - [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。
  - （未使用）[ユーザ名テンプレート（User Name Template）]：FTD では使用されていません。
  - [タイムアウト（Timeout）]：バックアップ接続にロールオーバーするまでの秒数を入力します。デフォルトは 30 です。

i) （任意） ユーザ識別タイプ以外のシェル アクセス属性を使用する場合は、[シェルアクセス属性（Shell Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で `sAMAccountName` シェル アクセス属性を使用してシェル アクセス ユーザを取得するには、[シェル アクセス属性（Shell Access Attribute）] フィールドに `sAMAccountName` と入力します。

j) [シェルアクセスフィルタ（Shell Access Filter）] を設定します。

次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] を選択します。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

LDAP サーバ上の名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

k) [保存（Save）] をクリックします。

ステップ 5 LDAP の場合、LDAP サーバで後からユーザを追加または削除する場合は、ユーザ リストを更新し、プラットフォーム設定を再展開する必要があります。

a) **[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** を選択します。

b) LDAP サーバの横にある[Refresh] アイコン（）をクリックします。

ユーザ リストが変更された場合は、デバイスの設定変更を展開するように促すメッセージが表示されます。Firepower Threat Defense のプラットフォーム設定には、「*x* 台の対象デバイスで古くなっている」ことも表示されます。

c) 設定変更を展開します。設定変更の展開を参照してください。

ステップ 6 RADIUS 認証オブジェクトを設定します。

a) Service-Type 属性を使用して RADIUS サーバ上のユーザを定義します。

次に、Service-Type 属性でサポートされている値を示します。

- Administrator (6)：CLI への config アクセス認証を提供します。これらのユーザは、CLI ですべてのコマンドを使用できます。
- NAS Prompt (7) または 6 以外のレベル：CLI への基本的なアクセス認証を提供します。これらのユーザは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

または、外部認証オブジェクトにユーザを事前定義できます（ステップ 6.j （10 ページ） を参照）。

名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

b) FMC で [外部認証オブジェクトの追加（Add External Authentication Object）] をクリックします。

c) [認証方式（Authentication Method）] を [RADIUS] に設定します。

d) [名前（Name）] とオプションの [説明（Description）] を入力します。

e) [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

（注） 証明書を使用し、TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

f) （任意）[ポート（Port）] をデフォルトから変更します。

g) [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

h) （任意）[バックアップサーバ（Backup Server）] パラメータを入力します。

i) [RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

- [タイムアウト（秒）（Timeout (Seconds)）]：バックアップ接続にロールオーバーするまでの秒数を入力します。デフォルトは 30 です。
- [再試行（Retries）]：バックアップ接続にロールオーバーする前にプライマリ サーバ接続を試行する回数を入力します。デフォルトは 3 です。

j) （オプション）外部認証オブジェクトにユーザ名を事前に定義する場合は、[シェルアクセス フィルタ（Shell Access Filter）] の [管理者シェル アクセス ユーザ リスト（Administrator Shell Access User List）] にカンマ区切りのユーザ名のリストを入力します。たとえば、**`jchrichton, aerynsun, rygel`** と入力します。

これらのユーザ名が RADIUS サーバのユーザ名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

（注） RADIUS サーバでユーザのみを定義する場合は、このセクションを空のままにしておく必要があります。

k) [保存（Save）] をクリックします。

ステップ 7 **[デバイス（Devices）]** > > **[プラットフォーム設定（Platform Settings）]** > **[外部認証（External Authentication）]** タブに戻ります。

ステップ 8 [Refresh] アイコン（）をクリックして、新しく追加したオブジェクトを表示します。

LDAP の場合は、SSL 暗号化または TLS 暗号化を指定するときに、その接続用の証明書をアップロードする必要があります。アップロードしない場合は、このタブにサーバがリストされません。

ステップ 9 使用する外部認証オブジェクトの横にあるスライダ（）をクリックします。有効にできるのは、1 つのオブジェクトのみです。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 設定変更を展開します。設定変更の展開を参照してください。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

デフォルトでは、FTD 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、FTD 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。 >

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、FTD 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、すべての集合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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

HTTPS 接続を FTD 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

- Firepower Management Center を使用して FTD を管理する場合は、FTD に対する HTTPS アクセスがパケット キャプチャ ファイルの表示にしか使用されません。FTD は、この管理モードでの設定用の Web インターフェイスを備えていません。
- HTTPS ローカル ユーザは、CLI で **configure user add** コマンドを使用することによってのみ設定できます。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。AAA 外部認証はサポートされません。
- 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間で共有されます。この設定は、使用されている診断論理インターフェイスまたはその他のデータ インターフェイス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。これは、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。
- 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。
- 同じ TCP ポートに関して、同じインターフェイスに HTTPS と AnyConnect リモート アクセス SSL VPN の両方を設定することはできません。たとえば、外部インターフェイスにリモート アクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。同じインターフェイスに両方の機能を設定する必要がある場合は、別々のポートを使用します。たとえば、ポート 4443 で HTTPS を開きます。

- 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。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、ルールで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） システム提供の **any** ネットワーク オブジェクト グループは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

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、FTD 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）]：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。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）]：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。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にのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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 アドレス宛ての 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ての 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 any 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）の権限を常に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 ディスカバリがディセーブルになり、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。

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、FTD 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) 次のルール 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。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にのみ、これらのルールがデバイスに適用されます。
c) [OK] をクリックします。

ステップ 4 （任意）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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	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。

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。

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) 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 （16 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に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です。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 暗号および DHE 暗号です。

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。

[All]：NULL-SHA を含むすべての暗号。

[Low]：NULL-SHA を除くすべての暗号。

[Medium]：NULL-SHA、DES-CBC-SHA、RC4-SHA、および RC4-MD5 を除くすべての暗号（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。

[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。

[Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

FTD デバイス上で 1 つ以上のデータ インターフェイスへの SSH 接続を許可するには、セキュア シェル設定を構成します。 SSH は診断論理インターフェイスに対してサポートされません。物理的な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

間で共有できます。SSH は管理論理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

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。これは、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。データインターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザ リストを共有します。その他の設定は個別に設定されます。データ インターフェイスでは、この画面を使用して SSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセス リストを設定するには『Firepower Threat Defense Command Reference』の **configure ssh-access-list** コマンドを参照してください。スタティック ルートを設定するには、**configure network static-routes** コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルト ルートを設定します。

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。

（注） すべてのアプライアンスでは、SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

始める前に

- SSH 内部ユーザは、**configure user add** コマンドを使用して CLI でのみ設定できます。CLI での内部ユーザの追加を参照してください。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。LDAP または RADIUS 上の外部ユーザは、プラットフォーム設定で [外部認証（External Authentication）] を設定することによっても設定できます。SSH の外部認証の設定 （5 ページ）を参照してください。
- 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、ルールで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。

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、FTD 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 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。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にのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

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、FTD 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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。 > >

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、FTD 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 FTD 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。スペースと特殊文字は使用できません。
- [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 （23 ページ）。

ステップ 5 SNMP ホストの追加 （25 ページ）。

ステップ 6 SNMP トラップの設定 （27 ページ）。

ステップ 7 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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。

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、FTD 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**：FTD 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**：FTD 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（Encrpted）] 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（Encrpted）] 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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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、FTD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。

最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。

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ネットワーク オブジェクトには、IPv6 ホスト、IPv4 ホスト、IPv4 範囲および IPv4 サブネット アドレスが含まれます。

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、FTD 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）] フィールドに、有効な Ipv6 ホストまたは IPv4 ホストを入力するか、SNMP 管理ステーションのホストアドレスを定義するネットワーク オブジェクトを選択します。

IP アドレスには、IPv6 ホスト、IPv4 ホスト、IPv4 範囲または IPv4 サブネットを使用できます。

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。

（注） SNMP ホストの IP アドレスが IPv4 範囲または IPv4 サブネットのいずれかである場合、[ポーリング（Poll）] と [トラップ（Trap）] の両方ではなく、いずれかを設定できます。

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。ゾーン内に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、デバイスでホストが設定されます。

（注） インターフェイスの IP アドレスが、ステップ 4 （25 ページ） の SNMP ホストに定義されている IP アドレスの値と競合しないことを確認します。

ステップ 12 [OK] をクリックします。

ステップ 13 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

SNMP トラップの設定

[SNMP トラップ] タブを使用して、FTD 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 FTD 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。

SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、FTD ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードできます。

http://www.ietf.org/

次の場所から Cisco MIB、トラップ、および OID の完全なリストを参照してください。

ftp://ftp.cisco.com/pub/mibs/

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

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、FTD 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、FTD 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。

a) [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。

b) [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。

（注） SNMP トラップはリアルタイムに近いことが期待されるため、FTD からの他の通知メッセージよりも優先順位が高いです。すべての SNMP トラップまたは syslog トラップを有効にすると、SNMP プロセスがエージェントとネットワーク内で過剰にリソースを消費し、システムがハングアップする可能性があります。システムの遅延、未完了の要求、またはタイムアウトが発生した場合は、SNMP トラップと syslog トラップを選択して有効にすることができます。また、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。たとえば、212 で始まる syslog メッセージ ID はすべて、SNMP クラスに関連しています。syslog メッセージの生成レートの制限 （43 ページ）を参照してください。

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 **[Save（保存）]** をクリックします。

これで、[Deploy]をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

Syslog の設定概要

FTD 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。また、一部のセキュリティ イベントを syslog サーバに送信することもできます。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。中央の 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、シンプル 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、保護された長期的な保存場所をログに提供します。ログは、ルーチン 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。

表 *1* : のシステム ログ *Firepower Threat Defense*

関連ログ	詳細	設定
デバイスとシステム ヘルス、ネットワーク構成	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。ただし、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、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html の『*Cisco Firepower Threat Defense 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。	**プラットフォームの設定**

関連ログ	詳細	設定
（バージョン 6.3 以降を実行しているデバイス） セキュリティ イベント	この syslog の設定では、ファイルとマルウェア、接続、セキュリティ インテリジェンス、および侵入イベントのアラートが生成されます。詳細については、セキュリティ イベントの syslog メッセージの送信についておよびサブトピックを参照してください。	アクセス コントロール ポリシーの [プラットフォーム設定（Platform Settings）] と [ロギング（Logging）] タブ
（すべてのデバイス） ポリシー、ルール、およびイベント	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。	アクセス コントロール ポリシーの [アラート応答（Alert Responses）] と [ロギング（Logging）] タブ

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 *2: 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。
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	**エラー**	エラー状態です。
4	**警告**	警告状態。
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（emergencies）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

  （これは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

- 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）

  （これは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

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。

（メッセージ リストは、接続および侵入イベントなどのセキュリティ イベントの syslog メッセージには適用されません。）

syslog メッセージ クラス

（注） このトピックは、セキュリティ イベント（接続、侵入など）のメッセージには適用されません。

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 *3 : syslog* メッセージ クラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロールの EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336

クラス	定義	Syslog メッセージ ID 番号
電子メール	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブラック リスト、ホワイト リスト、およびグレー リスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120

クラス	定義	Syslog メッセージ ID 番号
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
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
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
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

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 上でのセキュア ロギングはサポートされません。

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 サーバまたは同じロケーション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。

FTD デバイスの syslog ロギングの設定

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

ヒント　セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

Syslog の設定を行うには、以下の手順を実行します。

始める前に

ロギングのガイドライン （35 ページ）で要件を参照してください。

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、FTD 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、ロギングの有効化および基本設定の構成 （38 ページ）を参照してください。

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、ロギング接続先の有効化 （39 ページ）を参照してください。

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、電子メール アドレスへの syslog メッセージの送信 （41 ページ）を参照してください。

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、カスタム イベント リストの作成 （42 ページ）を参照してください。

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、syslog メッセージの生成レートの制限 （43 ページ）を参照してください。

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、Syslog 設定 （44 ページ）を参照してください。

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、Syslog サーバの設定 （46 ページ）を参照してください。

セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定

「セキュリティ イベント」には、接続、セキュリティ インテリジェンス、侵入、ファイルとマルウェアのイベントが含まれます。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense設定（Threat Defense Settings）] > [Syslog] ページとそのタブの syslog 設定の一部はセキュリティ イベントの syslog メッセージに適用されますが、多くの場合は、システム ヘルスとネットワークに関連するイベントのメッセージに適用されるだけです。

セキュリティ イベントの syslog メッセージには、次の設定が適用されます。

- [ロギング セットアップ（Logging Setup）] タブ：
  - **EMBLEM 形式で syslog を送信**
- [Syslog 設定（Syslog Settings）] タブ：
  - **syslog メッセージのタイムスタンプを有効化**
  - **タイムスタンプ形式**
  - **Enable Syslog Device ID**
- [Syslog サーバ（Syslog Servers）] タブ：
  - [Syslog サーバを追加（Add Syslog Server）] 形式（および設定済みサーバのリスト）のすべてのオプション

セキュリティ イベント syslog メッセージングを設定するためのベストプラクティスも参照してください。

ロギングの有効化および基本設定の構成

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

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、FTD 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 （30 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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

ヒント　セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

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、FTD 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。

a) [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。

b) [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。

c) 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 （31 ページ） を参照してください。

d) [OK] をクリックします。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

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 （38 ページ）
- ロギング接続先の有効化

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、FTD 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 [Add] をクリックして、指定した syslog メッセージの受信者の電子メール 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 （30 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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

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、FTD 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 （31 ページ） を参照してください。

レベルについては、重大度 （30 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 （31 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 （39 ページ）を参照してください。

ステップ 5 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

ヒント セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、ほとんどの FTD プラットフォーム設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

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、FTD 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 （30 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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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。

セキュリティ イベント（接続イベントや侵入イベントなど）に関する syslog メッセージを送信するようにデバイスを設定すると、このページの一部の設定がこれらのメッセージに適用されません。セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）を参照してください。

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、FTD 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。

通常、ファシリティの値はセキュリティ イベントとは関係ありません。ファシリティの値をメッセージに含める必要がある場合は、セキュリティ イベントの syslog メッセージのファシリティを参照してください。

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 syslog メッセージの [タイムスタンプの形式（Timestamp Format）] を選択します。

- [レガシー（Legacy）]（MMM dd yyyy HH:mm:ss）形式は、syslog メッセージのデフォルト形式です。

  このタイムスタンプ形式を選択すると、メッセージには常に UTC であるタイム ゾーンが表示されません。

- [RFC 5424]（yyyy-MM-ddTHH:mm:ssZ）は RFC 5425 形式で指定されている ISO 8601 タイムスタンプ形式を使用します。

  RFC 5424 形式を選択すると、「Z」が各スタンプの末尾に追加され、タイムスタンプが UTC タイム ゾーンを使用していることを示します。

ステップ 6 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 7 [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、エントリはテーブルに表示されます。

a) NetFlow が原因で冗長している Syslog メッセージを抑制にするには、[ネットフロー同等 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 8 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

関連トピック

セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

システム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。

（バージョン 6.3 以降を実行しているデバイスの場合）この syslog サーバが接続イベントや侵入イベントなどのセキュリティ イベントを受信する場合は、セキュリティ イベントの syslog メッセージに適用する FTD プラットフォームの設定 （37 ページ）も参照してください。

始める前に

- ロギングのガイドライン （35 ページ）で要件を参照してください。
- デバイスからネットワーク上の syslog コレクタに到達できることを確認します。

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、FTD 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 は高速で、TCP よりもデバイス上のリソースが減少します。

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。

（注） 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。デバイス管理インターフェイスでは、[セキュア Syslog を有効にする（Enable Secure Syslog）] オプションはサポートされていません。

e) Syslog サーバと通信するための [デバイス管理インターフェイス（Device Management Interface）] または [セキュリティ ゾーンまたは名前付きインターフェイス（Security Zones or Named Interfaces）] を選択します。

- [デバイス管理インターフェイス（Device Management Interface）]：このオプションは、バージョン 6.3 以降の Firepower Threat Defense デバイスにのみ適用されます。

  （注） [デバイス管理インターフェイス（Device Management Interface）] オプションでは、[セキュア Syslog を有効にする（Enable Secure Syslog）] オプションをサポートされていません。

- [セキュリティ ゾーンまたは名前付きインターフェイス（Security Zones or Named Interfaces）]：[使用可能ゾーン（Available Zones）] のリストからインターフェイスを選択して、[追加（Add）] をクリックします。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）] ページでデバイス設定を編集し、[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。

（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）] をクリックします。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）] ページでデバイス設定を編集し、[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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin 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、リソースは空いている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。

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、FTD 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。最小は 30 秒です。デフォルトは 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（および最小）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（および最小）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（0:0:1 ～ 00:10:0）。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）]：1 つのネットワークに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（0:0:30～ 0:5:0）。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アップストリーム 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 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 **[Save（保存）]** をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

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数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin Access Admin Network Admin

Network Time Protocol（NTP）サーバを使用して、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、可能な場合は別の NTP サーバを設定する必要があります。

（注） Firepower 4100/9300 シャーシに FTD を導入する場合は、スマート ライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように、Firepower 4100/9300 シャーシで NTP を設定する必要があります。Firepower 4100/9300 シャーシと Firepower Management Center には、同じ NTP サーバを使用する必要があります。

始める前に

- 組織に FTD からアクセスできる 1 台以上の NTP サーバがある場合は、FMC の [System] > [Configuration] ページで、時刻の同期用に設定したデバイスと同じ NTP サーバを使用します。指定した値をコピーします。

- デバイスが NTP サーバにアクセスできない場合、または組織に NTP サーバがない場合は、Firepower Management Center を NTP サーバとして使用するように設定する必要があります。ネットワーク NTP サーバにアクセスせずに時刻を同期を参照してください。

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、FTD ポリシーを作成または編集します。

ステップ 2 [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。

- [Defense CenterのNTPを使用（Via NTP from Defense Center）]：Firepower Management Center サーバを NTP サーバとして使用します（この機能を提供するように設定している場合）。これはデフォルトです。
- [Via NTP from]：Firepower Management Center がネットワーク上の NTP サーバを使用している場合は、このオプションを選択し、FMC の [System] > [Configuration] > [Time Synchronization] で指定した NTP サーバと同じ完全修飾 DNS 名（ntp.example.com など）または IP アドレスを入力します。

ステップ 4 **[Save（保存）]** をクリックします。

次のタスク

- ポリシーがデバイスに割り当てられていることを確認します。プラットフォーム設定ポリシーのターゲット デバイスの設定を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。
- Firepower システムに従来型デバイスが含まれている場合は、そのデバイスの時刻の同期を設定します。従来型デバイスの時刻を NTP サーバに同期を参照してください。

Firepower Threat Defense プラットフォーム設定の履歴

機能	バージョン	詳細
SSH ログイン失敗の制限数	6.3	ユーザがSSH経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスはSSHセッションを終了します。

機能	バージョン	詳細
SSH 用に追加された外部認証	6.2.3	LDAP または RADIUS を使用して、Firepower Threat Defense への SSH アクセス用に外部認証を設定できるようになりました。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォームの設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされているプラットフォーム：Firepower Threat Defense
UC/APPL 準拠モードのサポート	6.2.1	セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティモードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [UC/APPL準拠（UC/APPL Compliance）]** サポートされているプラットフォーム：すべてのデバイス

機能	バージョン	詳細
リモート アクセス VPN の SSL 設定	6.2.1	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 接続のセキュア メッセージ伝送をサポートします。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。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォーム設定（Platform）] > [SSL]** サポートされているプラットフォーム：Firepower Threat Defense
SSH および HTML 用の外部認証が削除	6.1.0	統合管理アクセスをサポートするための変更により、データ インターフェイスに対する SSH および HTML ではローカル ユーザのみがサポートされます。また、論理診断インターフェイスに対する SSH は使用できなくなりました。代わりに、（同じ物理ポートを共有する）論理管理インターフェイスに対する SSH を使用できます。以前は、診断およびデータ インターフェイスに対する SSH および HTML アクセスでは外部認証のみがサポートされていましたが、管理インターフェイスに対してはローカル ユーザのみがサポートされていました。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォームの設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされているプラットフォーム：Firepower Threat Defense

機能	バージョン	詳細
Firepower Threat Defense のサポート	6.0.1	この機能が導入されました。 新しい/変更された画面： **[Devices] > [Platform Settings]** サポートされているプラットフォーム：Firepower Threat Defense