プラットフォーム設定

Firewall 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。

プラットフォーム設定の概要

プラットフォーム設定ポリシーは、時刻の設定や外部認証など、展開内の他の管理対象デバイスと同様になる可能性の高い、管理対象デバイスの側面を定義する共有の機能またはパラメータのセットです。

共有ポリシーによって同時に複数の管理対象デバイスを設定することができ、これによって展開に一貫性をもたらし、管理の手間を合理化することができます。プラットフォーム設定ポリシーへの変更は、ポリシーを適用したすべての管理対象デバイスに影響します。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

たとえば、組織のセキュリティポリシーではユーザのログイン時にアプライアンスに「無断使用禁止」のメッセージを表示する必要があるとします。プラットフォーム設定を使えば、プラットフォーム設定ポリシー内で一度ログイン バナーを設定するだけで完了します。

また、単一の Firewall Management Center で複数のプラットフォーム設定ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメール リレー ホストを使用する場合や、さまざまなアクセス リストをテストする場合は、単一のポリシーを編集するのではなく、いくつかのプラットフォーム設定ポリシーを作成し、それらを切り替えることができます。

プラットフォーム設定ポリシーの要件と前提条件

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

プラットフォーム設定ポリシーの管理

[プラットフォームの設定（Platform Settings）]ページ（**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]**）を使用して、プラットフォーム設定ポリシーを管理します。このページには、各ポリシーのデバイスのタイプが示されます。[ステータス（Status）]列で、ポリシーのデバイスターゲットが示されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**を選択します。

ステップ 2 既存のポリシーの場合は、ポリシーを [コピー（Copy）] （）、[編集（Edit）]（）、または[削除（Delete）]（） できます。

注意
どのターゲットデバイスでも、最後に展開したポリシーは期限切れであっても削除しないでください。ポリシーを完全に削除する前に、それらのターゲットに別のポリシーを展開するようにしてください。

ステップ 3 新しいポリシーを作成するには、[新しいポリシー（New Policy）] をクリックします。

a) ドロップダウン リストから、デバイス タイプを選択します。

- [Firepower設定（Firepower Settings）]：従来型の管理対象デバイス用の共有ポリシーを作成します。
- [脅威に対する防御設定（Threat Defense Settings）]：Firewall Threat Defenseの管理対象デバイス用の共有ポリシーを作成します。

b) 新しいポリシーの [名前（Name）]、および必要に応じて [説明（Description）] を入力します。

c) 必要に応じて、ポリシーを適用する [使用可能なデバイス（Available Devices）] を選択し、[追加（Add）] をクリック（またはドラッグアンドドロップ）して、選択したデバイスを追加します。 [検索（Search）] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。

d) [保存（Save）] をクリックします。

システムにより、ポリシーが作成され、編集のために開かれます。

ステップ 4 ポリシーのターゲットデバイスを変更するには、編集するプラットフォーム設定ポリシーの横にある [編集（Edit）]（） をクリックします。

a) [ポリシーの割り当て（Policy Assignment）] をクリックします。

b) デバイス、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス（Available Devices）] リストで選択し、[Add] をクリックします。ドラッグアンド ドロップを使用することもできます。

c) デバイスの割り当てを削除するには、[選択されたデバイス（Selected Devices）] リストのデバイス、高可用性ペア、またはデバイスグループの横にある [削除（Delete）]（） をクリックします。

d) **[OK]** をクリックします。

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。

ARP インスペクション

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有効化すると、Firewall 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、Firewall 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Firewall Threat Defense デバイスを設定できます。

（注） 専用のDiagnostic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、Firewall 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）] 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。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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

バナー

デバイスの CLI（コマンド ライン インターフェイス）に接続するユーザーを表示するよう、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、Firewall 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

DNS

ドメイン ネーム システム（DNS）サーバは、IP アドレスのホスト名の解決に使用されます。2つのDNSサーバー設定があり、異なるタイプのトラフィック（データトラフィックと特別な管理トラフィック）に適用されます。データトラフィックには、アクセスコントロールルールやリモートアクセス VPN など、DNS ルックアップが必要な FQDN を使用するサービスが含まれます。特別な管理トラフィックには、構成やデータベースの更新など、管理インターフェイスで発生するトラフィックが含まれます。この手順は、データ DNS サーバーにのみ適用されます。管理 DNS 設定については、CLI コマンドの **configure network dns servers** と **configure network dns searchdomains** を参照してください。

DNS サーバー通信の正しいインターフェイスを決定するために、管理対象デバイスではルーティングルックアップが使用されますが、使用されるルーティングテーブルは、DNSを有効にするインターフェイスによって異なります。詳細については、以下のインターフェイス設定を参照してください。

必要に応じて、複数のDNSサーバーグループを構成し、それらを使用してさまざまなDNSドメインを解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバーを使用するキャッチオールのデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部DNSサーバーを使用する別のグループを構成できます。したがって、組織のドメイン名を使用したFQDNへの接続は、内部 DNS サーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS

サーバーを使用します。これらの解決は、NAT やアクセスコントロールルールなど、データ DNS 解決を使用する機能によって使用されます。

[信頼されたDNSサーバー（Trusted DNS Servers）] タブを使用して、DNS スヌーピング用の信頼された DNS サービスを構成できます。DNS スヌーピングは、アプリケーションドメインを IP にマッピングして、最初のパケットでアプリケーションを検出するために使用されます。信頼された DNS サーバーの構成とは別に、構成済みのサーバーを、DNS グループ、DHCP プール、DHCP リレー、および DHCP クライアントに、信頼された DNS サーバーとして含めることができます。

（注） アプリケーションベースの PBR の場合、信頼された DNS サーバーを構成する必要があります。また、ドメインを解決してアプリケーションを検出できるように、DNS トラフィックがクリアテキスト形式で Firewall Threat Defense を通過するようにする必要があります（暗号化された DNS はサポートされていません）。

始める前に

- 1 つ以上の DNS サーバーグループを作成していることを確認します。詳細については、DNS サーバー グループ オブジェクトの作成を参照してください。
- DNS サーバーに接続するためのインターフェイス オブジェクトが作成されていることを確認します。
- 管理対象デバイスに、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあることを確認します。

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、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 [DNS設定（DNS Settings）] タブをクリックします。

ステップ 4 [Enable DNS name resolution by device] をオンにします。

ステップ 5 DNS サーバーグループを設定します。

a) DNS サーバーグループリストで次のいずれかを実行します。

- グループをリストに追加するには、[追加（Add）]をクリックします。サーバーグループの既存のリスト内に 30 のフィルタドメインが構成されている場合、別のグループを追加することはできません。
- グループの設定を編集するには、グループの横にある [編集（Edit）]（✎） をクリックします。

- グループを削除するには、グループの横にある [削除（Delete）]（）をクリックします。グループを削除しても、DNS サーバー グループ オブジェクトは削除されません。このリストから削除されるだけです。

b) グループを追加または編集するときは、次の設定を構成し、[OK] をクリックします。

- [DNSグループの選択（Select DNS Group）]：既存の DNS サーバー グループ オブジェクトを選択するか、[+] をクリックして新しいオブジェクトを作成します。
- [デフォルトに設定（Make as default）]：このオプションを選択して、このグループをデフォルトのグループにします。他のグループのフィルタに一致しない DNS 解決要求は、このグループのサーバーを使用して解決されます。
- [ドメインのフィルタ処理（Filter Domains）]：デフォルト以外のグループの場合のみ、example.com、example2.com などのドメイン名のカンマ区切りリスト。スペースは使用できません。

  グループは、これらのドメインの DNS 解決にのみ使用されます。この DNS プラットフォーム設定ポリシーに追加されたすべてのグループで、最大 30 の個別のドメインを入力できます。それぞれの名前は最大 127 文字です。

  これらのフィルタドメインは、グループのデフォルトドメイン名とは関係がないことに注意してください。フィルタリストは、デフォルトドメインとは異なる場合があります。

ステップ 6 （任意）[Expiry Entry Timer] と [Poll Timer] の値を分単位で入力します。

これらのオプションは、ネットワークオブジェクトにのみ指定されている FQDN に適用されます。これらは、他の機能で使用される FQDN には適用されません。

- [Expire Entry Timer] は、DNS エントリの最小存続可能時間（TTL）を分単位で指定します。有効期限タイマーがエントリの TTL よりも長い場合、TTL は有効期限エントリ時間値まで増加します。TTL が有効期限タイマーよりも長い場合、有効期限エントリ時間値は無視されます。この場合、TTL に追加の時間は追加されません。有効期限が切れると、DNS ルックアップテーブルからエントリが削除されます。エントリの削除にはテーブルをコンパイルする必要があります。したがって、削除を頻繁に行うとデバイス上の処理負荷が増加する可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です（つまり、すべての解像度の最小 TTL は 1 分です）。指定できる範囲は 1 ～ 65535 分です。

  7.0 以前を実行しているシステムでは、有効期限が実際に TTL に追加されることに注意してください。最小値は指定されません。

- [Poll Timer] では、ネットワークオブジェクトに定義されている FQDN を解決するために、デバイスが DNS サーバー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。

ステップ 7 すべてのインターフェイスまたは特定のインターフェイスで DNS ルックアップを有効にします。これらの選択は、使用されるルーティングテーブルにも影響します。

インターフェイスで DNS ルックアップを有効にすることは、ルックアップの送信元インターフェイスを指定することとは異なるので注意してください。Firewall Threat Defense は、常にルートルックアップを使用して送信元インターフェイスを決定します。専用の管理インターフェイス以外の管理専用インターフェイスは使用できません。

- [インターフェイスの選択なし（No interfaces selected）]：管理インターフェイスと管理専用インターフェイスを含む、すべてのインターフェイスで DNS ルックアップを有効にします。Firewall Threat Defense はデータルーティングテーブルのみチェックし、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックします。
- [特定のインターフェイスが選択されました（Specific interfaces selected）] ただし [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/management interface also）] オプションはなし：指定したインターフェイスで DNS ルックアップを有効にします。Firewall Threat Defense はデータルーティングテーブルのみチェックします。
- [特定のインターフェイスが選択されました（Specific interfaces selected）] に加えて [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/management interface also）] オプション：指定したインターフェイスと [診断（Diagnostic）] インターフェイスで DNS ルックアップを有効にします。Firewall Threat Defense はデータルーティングテーブルをチェックし、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックします。
- [Enable DNS Lookup via diagnostic interface also] オプションのみ：[診断（Diagnostic）] で DNS ルックアップを有効にします。Firewall Threat Defense は、管理専用ルーティングテーブルのみチェックします。[Devices] > [Device Management] > [edit device] > [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 信頼された DNS サーバーを構成するには、[信頼されたDNSサーバー（Trusted DNS Servers）] タブをクリックします。

ステップ 9 デフォルトでは、DHCP プール、DHCP リレー、DHCP クライアント、または DNS サーバーグループで構成されている既存の DNS サーバーは、信頼された DNS サーバーとして含まれています。それらのいずれかを除外する場合は、該当するチェックボックスをオフにします。

ステップ 10 信頼された DNS サーバーを追加するには、[DNSサーバーの指定（Specify DNS Servers）] で [編集（Edit）] をクリックします。

ステップ 11 [DNSサーバーの選択（Select DNS Servers）] ダイアログボックスで、信頼された DNS サーバーとしてホストオブジェクトを選択するか、信頼された DNS サーバーの IP アドレスを直接指定します。

a) 既存のホストオブジェクトを選択するには、[使用可能なホストオブジェクト（Available Host Objects）] で必要なホストオブジェクトを選択し、[追加（Add）] をクリックしてそれを [選択済みDNSサーバー（Selected DNS Servers）] に含めます。ホストオブジェクトの追加については、ネットワーク オブジェクトの作成を参照してください。

b) 信頼された DNS サーバーの IP アドレス（IPv4 または IPv6）を直接指定するには、所定のテキストフィールドにアドレスを入力し、[追加（Add）] をクリックして、[選択済みDNSサーバー（Selected DNS Servers）] に追加します。

c) [保存（Save）] をクリックします。追加された DNS サーバーは、[信頼されたDNSサーバー（Trusted DNS Servers）] ページに表示されます。

（注）
最大で 12 の DNS サーバーを設定できます。

ステップ 12 （オプション）ホスト名または IP アドレスを使用して、追加された DNS サーバーを検索するには、[DNSサーバーの指定（Specify DNS Servers）] の下の検索フィールドを使用します。

ステップ 13 [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。

外部認証

（注） このタスクを実行するには、管理者特権が必要です。

管理ユーザーの外部認証を有効にすると、Firewall Threat Defense により外部認証オブジェクトで指定された LDAP または RADIUS サーバーを使用してユーザー 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、Firewall Management Center および Firewall Threat Defense デバイスで使用できます。同じオブジェクトを Firewall Management Center とデバイス間で共有することも、別々のオブジェクトを作成することもできます。Firewall Threat Defense は RADIUS サーバーでのユーザーの定義をサポートしますが、Firewall Management Center では外部認証オブジェクトのユーザー リストを事前定義する必要があることに注意してください。Firewall Threat Defense 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 サーバーでユーザーを定義する場合は Firewall Threat Defense と Firewall Management Center に個別のオブジェクトを作成する必要があります。

（注） タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（LDAP の場合は 1 ー 30 秒、RADIUS の場合は 1 ー 300 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense 外部認証設定が機能しません。

デバイスへの外部認証オブジェクトの割り当て

Firewall Management Center では、**[システム（System）] > [ユーザー（Users）] > [外部認証（External Authentication）]** 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、Firewall Management Center の使用にのみ影響します。管理対象デバイスを使用する場合は、有効にする必要はありません。Firewall Threat Defense 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、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。オブジェクトを共有していない場合でも、Firewall Threat Defense と Firewall Management Center の両方が LDAP サーバーに到達できることを確認します。Firewall Management Center は、ユーザーリストを取得してデバイスにダウンロードするために必要です。

Firewall Threat Defense サポート対象フィールド

Firewall Threat Defense 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 Firewall Management Center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、Firewall Threat Defense 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、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Configure External Authentication for the Firewall Management Center*」を参照してください。

ユーザー名

ユーザー名は 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** ユーザーを追加することはできません。外部ユーザーは、Firewall Management Center 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。内部ユーザーは、Firewall Management Center 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 内部ユーザーとして同じユーザー名がコマンドを使用して設定されていた場合は、Firewall Threat Defense は最初にその内部ユーザーのパスワードをチェックし、それが失敗した場合はAAAサーバーをチェックします。後から外部ユーザーと同じ名前の内部ユーザーを追加できないことに注意してください。既存の内部ユーザーしかサポートされません。RADIUS サーバーで定義されているユーザーの場合は、内部ユーザーの権限レベルと同じに設定してください。そうしないと、外部ユーザー パスワードを使用してログインできません。

Privilege Level

LDAP ユーザーには常に Config 権限があります。RADIUS ユーザーは、Config ユーザーまたは Basic ユーザー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、Shellの確保 （21 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ユーザーに次の動作を通知し、適切に動作するようにします。
  - 外部ユーザーが初めてログインすると、Firewall Threat Defenseは必要な構造体を作成しますが、ユーザー 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.」
  - ユーザーのService-Type属性がRADIUSサーバーで定義されていないか、正しく設定されていない場合、RADIUSで定義されたユーザーを認証に使用すると、次のようなメッセージがユーザーに表示されます。「Your username is not defined with a service type that is valid for this system. You are not authorized to access the system?」

    場合により、失敗メッセージを表示する前でも、SSHクライアントは失敗したSSH接続のCLIウィンドウを閉じます。したがって、ユーザーのService-Type属性がRADIUSサーバーで正しく定義されていることを確認してください。
  - 同様に、最後のログイン以降にユーザーのService-Type認証が変更された場合、ユーザーを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.）」

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、Firewall Threat Defense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 [外部認証サーバーの管理（Manage External Authentication Server）] リンクをクリックします。

[システム（System）] > **[ユーザー（Users）]** > **[外部認証（External Authentication）]**をクリックして、[外部認証（External Authentication）] 画面を開くこともできます。

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）
証明書を使用して 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）[ユーザー名テンプレート（User Name Template）]：Firewall Threat Defense 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（1 ー 30 秒）を入力します。デフォルトは 30 です。

  （注）
  タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense 外部認証設定が機能しません。

i) （任意）ユーザー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、[CLIアクセス属性（CLI 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ーを取得するには、[CLIアクセス属性（CLI Access Attribute）] フィールドに `sAMAccountName` と入力します。

j) [CLIアクセスフィルタ（CLI 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 サーバー上の名前は、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 サーバーで後からユーザーを追加または削除する場合は、ユーザー 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）] > [ユーザー（Users）] > [外部認証（External Authentication）]** を選択します。

b) LDAP サーバーの横にある [更新（Refresh）]（ ） をクリックします。

ユーザー 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 サーバー上のユーザーを定義します。

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。これらのユーザーは、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。これらのユーザーは **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。

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

または、外部認証オブジェクトにユーザーを事前定義できます（ステップ 6.j （16 ページ）を参照）。Firewall Threat Defense に対して Service-Type 属性メソッドを使用しているときに Firewall Threat Defense および Firewall Management Center に同じ RADIUS サーバーを使用するには、同じ RADIUS サーバーを識別する外部認証オブジェクトを 2 つ作成します。一方のオブジェクトには事前に定義した [CLIアクセスフィルタ（CLI Access Filter）] ユーザーを含め（Firewall Management Center で使用）、もう一方のオブジェクトの [CLIアクセスフィルタ（CLI Access Filter）] は空のままにします（Firewall Threat Defense で使用）。

b) Firewall Management Center 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）
証明書を使用して 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）RADIUS 定義ユーザーを使用する代わりに、[CLIアクセスフィルタ（CLI Access Filter）] の下で、[管理者CLIアクセスユーザーリスト（Administrator CLI Access User List）] フィールドに、カンマ区切りのユーザー名のリストを入力します。たとえば、**`jchrichton, aerynsun, rygel`** と入力します。

Firewall Threat Defense で [CLIアクセスフィルタ（CLI Access Filter）] メソッドを使用すると、Firewall Threat Defense およびその他のプラットフォームタイプで同一の外部認証オブジェクトを使用できます。RADIUS 定義ユーザーを使用する場合は、[CLIアクセスフィルタ（CLI Access Filter）] を空のままにする必要があります。

これらのユーザー名が RADIUS サーバーのユーザー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 サーバーでユーザー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）]** に戻ります。

ステップ 8 [更新（Refresh）]（  ）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、このウィンドウにサーバー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 [有効なスライダ（Slider enabled）]（  ）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。

フラグメント設定

デフォルトでは、Firewall 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）]** 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、Firewall 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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [フラグメント設定（Fragment Settings）] 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

HTTP

HTTPS サーバーを有効にして、アプリケーション ロードバランサを使用する AWS 上の Firewall Threat Defense Virtual など、クラウドロードバランサのヘルスチェックメカニズムを提供できます。

Firewall Threat Defense での HTTPS のその他の用途はサポートされていません。たとえば、Firewall Threat Defense 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。

この設定は、管理専用として設定したものも含め、データインターフェイスにのみ適用されます。専用管理インターフェイスには適用されません。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とは分離されています。Firewall 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。

始める前に

- 同じ TCP ポートに関して、同じインターフェイスに HTTPS と Cisco Secure Client の AnyConnect VPN モジュール 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。

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、Firewall 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サーバーを有効にする（Enable HTTP Server）] チェックボックスをオンにして HTTP サーバーを有効にします。

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

ステップ 5 HTTP 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。

このテーブルを使用して、HTTP 接続および HTTP 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）] 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）]：HTTP 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またはグループ。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 [+] 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）]**：HTTP 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、**[選択したセキュリティゾーン（Selected Security Zones）]** 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

ICMP

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。

- Firewall Threat Defense 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。
- Firewall Threat Defense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）]** を選択して、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、Firewall 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）] 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。ゾーンにないインターフェイスでは、**[選択したセキュリティゾーン（Selected Security Zones）]** 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 （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。この数の応答は送信されますが、それ以降の応答は、レート制限に達するまで送信されません。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

Shellの確保

外部インターフェイスなどのデータインターフェイスでFirewall Management Centerアクセスを有効にした場合は、この手順に従ってそのインターフェイスで SSH を有効にする必要があります。ここでは、Firewall Threat Defense で 1 つ以上のデータインターフェイスに対して SSH 接続を有効にする方法について説明します。 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。

Firewall Threat Defense は、OpenSSH に基づく CiscoSSH スタックを使用します。CiscoSSH は、FIPSの順守と、シスコおよびオープンソースコミュニティからの更新を含む定期的な更新をサポートします。

（注） SSH は管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。

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Firewall 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 アクセスリストを構成するには Cisco Secure Firewall Threat Defense コマンドリファレンス 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を開始できます。

SSH は、次の暗号およびキー交換をサポートしています。

- 暗号化：aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr
- 完全性：hmac-sha2-256
- キー交換：dh-group14-sha256

（注） SSH を使用した CLI へのログイン試行が 3 回連続して失敗すると、デバイスの SSH 接続は終了します。

始める前に

- SSH 内部ユーザーは、**configure user add** コマンドを使用して CLI でのみ設定できます。を参照してくださいCLI での内部ユーザーの追加。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザーが存在します。LDAP または RADIUS 上の外部ユーザーは、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。外部認証 （10 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。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。

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、Firewall 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 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）]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 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またはグループ。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 [+] 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。ゾーンにないインターフェイスでは、**[選択したセキュリティゾーン（Selected Security Zones）]** 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

SMTP サーバー

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 サーバーのホスト 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、Firewall 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 サーバーの IP アドレス（Primary Server IP Address）]、およびオプションで、[セカンダリ サーバーの 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、**[展開（Deploy）] > [展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

SNMP

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ー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ー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ーと、DES（廃止）、3DES、AES256、AES192、および AES128 による暗号化をサポートします。

（注） DES オプションは廃止されました。展開に、DES 暗号化を使用する SNMP v3 ユーザーが含まれていて、そのユーザーが 6.5 より前のバージョンを使用して作成された場合、それらのユーザーを 6.6 以前を実行する Firewall Threat Defense で引き続き使用できます。ただし、これらのユーザーを編集した後も DES 暗号化を維持したり、DES 暗号化を使用する新しいユーザーを作成したりすることはできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、DES 暗号化を使用するプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。

（注） SNMP 構成は、ルーテッドインターフェイスと診断インターフェイスのみをサポートします。

（注） 外部 SNMP サーバー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、Firewall 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 サーバーを有効にする（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 Firewall 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 ユーザーの追加 （32 ページ）。

ステップ 5 SNMP ホストの追加 （35 ページ）。

ステップ 6 SNMP トラップの設定 （37 ページ）。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

SNMP について

SNMP は、ネットワークデバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコルスイートの一部です。Firewall Threat Defense は、SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。Firewall Threat Defense のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワークデバイスを監視できます。Firewall Threat Defense は GET 要求の発行を通じて SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように Firewall Threat Defense を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIB は定義の集合であり、Firewall Threat Defenseは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

SNMP エージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクが稼働状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *1 : SNMP* の用語

用語	説明
エージェント	Secure Firewall Threat Defenseで稼働する SNMP サーバー。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。

用語	説明
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニターすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIB は、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMP イベントのモニターやデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニターおよび表示される情報の源をユーザーに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。 **coldStart**：coldStart トラップは、SNMP の設定後に SNMP エージェントが起動したときに発生します。このトラップは、システムの再起動後にエージェントが起動したときにも発生します。 （注） クラスタノードと HA ノードの場合、リロード後、インターフェイスのリブート時間が 5 分（プリセットしきい値）を超えると、トラップはドロップされます。クラスタおよび HA ノードが正常に再起動すると、他のすべてのトラップが想定どおりに送信されます。 **snmp-server enable traps snmp coldstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

MIB およびトラップ

MIB は、標準またはエンタープライズ固有です。標準 MIB はインターネット技術特別調査委員会（IETF）によって作成され、さまざまな Request for Comment（RFC）に記載されています。トラップは、ネットワークデバイスで発生する重要なイベント（多くの場合、エラーまたは障害）を報告します。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、ASA 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することもできます。

http://www.ietf.org/

SNMP オブジェクトナビゲータを参照し、次の場所から Cisco MIB、トラップ、および OID を検索してください。

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

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

MIB でサポートされるテーブルおよびオブジェクト

以下に、指定された MIB でサポートされるテーブルおよびオブジェクトを示します。

リモートアクセス VPN のポーリング

表 *2 : CISCO-REMOTE-ACCESS-MONITOR-MIB*

カウンタ	OID	説明
アクティブセッション（Active Sessions）	crasNumSessions（1.3.6.1.4.1.9.9.392.1.3.1）	現在アクティブなセッションの数。
ユーザー	crasNumUsers（1.3.6.1.4.1.9.9.392.1.3.3）	アクティブなセッションを持つユーザーの数。
ピークセッション数（Peak Sessions）	crasNumPeakSessions（1.3.6.1.4.1.9.9.392.1.3.41）	システムが起動してからのピーク RA セッションの数。

サイト間 VPN トンネルのポーリング

表 *3 : CISCO-REMOTE-ACCESS-MONITOR-MIB*

カウンタ	OID	説明
LAN 間セッション（LAN to LAN Sessions）	crasL2LNumSessions（1.3.6.1.4.1.9.9.392.1.3.29）	現在アクティブなLAN間セッションの数。
ピーク LAN 間セッション（Peak LAN to LAN Sessions）	crasL2LPeakConcurrentSessions（1.3.6.1.4.1.9.9.392.1.3.31）	システムが起動してからのピーク同時 LAN 間セッションの数。

接続のポーリング

表 *4 : CISCO-FIREWALL-MIB*

カウンタ	OID	説明
Active Connections	cfwConnectionActive （1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6）	ファイアウォール全体で現在使用されている接続の数。
Peak Connections	cfwConnectionPeak （1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7）	システムが起動してからの、一度に使用された接続の最大数。
1 秒あたりの接続数（Connections Per Second）	cfwConnectionPerSecond （1.3.6.1.4.1.9.9.147.1.2.2.3）	ファイアウォールでの現在の 1 秒あたりの接続数。
1 秒あたりのピーク接続数（Peak Connections Per Second）	cfwConnectionPerSecondPeak （1.3.6.1.4.1.9.9.147.1.2.2.4）	システムが起動してからの、ファイアウォールでの 1 秒あたりの最大接続数。

NAT 変換のポーリング

表 *5 : CISCO-NAT-EXT-MIB*

カウンタ	OID	説明
アクティブな変換（Active Translations）	cneAddrTranslationNumActive （1.3.6.1.4.1.9.9.532.1.1.1.1）	NATデバイスで現在使用可能なアドレス変換エントリの総数。これは、スタティックアドレス変換メカニズムとダイナミックアドレス変換メカニズムの両方から作成された変換エントリの合計を示しています。

カウンタ	OID	説明
ピークアクティブ変換（Peak Active Translations）	cneAddrTranslationNumPeak （1.3.6.1.4.1.9.9.532.1.1.1.2）	システムが起動してから、一度にアクティブになったアドレス変換エントリの最大数。これは、システムの起動以降に一度にアクティブになったアドレス変換エントリの高水準点を示しています。 このオブジェクトには、スタティックアドレス変換メカニズムとダイナミックアドレス変換メカニズムの両方から作成された変換エントリが含まれます。

ルーティング テーブル エントリのポーリング

表 *6 : IP-FORWARD-MIB*

カウンタ	OID	説明
アクティブな変換（Active Translations）	inetCidrRouteNumber （1.3.6.1.2.1.4.24.6）	現在の有効な inetCidrRouteTable エントリの総数。

インターフェイス デュプレックス ステータスのポーリング

表 *7 : CISCO-IF-EXTENSION-MIB*

カウンタ	OID	説明
デュプレックスステータス（Duplex Status）	cieIfDuplexCfgStatus （1.3.6.1.4.1.9.9.276.1.1.2.1.20）	このオブジェクトは、特定のインターフェイスで設定されたデュプレックスステータスを示します。
検出されたデュプレックスステータス（Detected Duplex Status）	cieIfDuplexDetectStatus （1.3.6.1.4.1.9.9.276.1.1.2.1.21）	このオブジェクトは、特定のインターフェイスで検出されたデュプレックスステータスを示します。

Snort 3 侵入イベントレートのポーリング

表 *8 : CISCO-UNIFIED-FIREWALL-MIB*

カウンタ	OID	説明
Snort 3 侵入イベントレート（Snort 3 Intrusion Event Rate）	cufwAaicIntrusionEvtRate（1.3.6.1.4.1.9.9.491.1.5.3.2.1）	このファイアウォールで Snort によって記録された侵入イベントのレート（過去 300 秒間の平均値）。

BGP ピアフラップトラップ通知

表 *9 : BGP4-MIB*

カウンタ	OID	説明
BGP ピアフラップ（BGP Peer-flap）	bgpBackwardTransition（1.3.6.1.4.1.9.9.491.1.5.3.2.1）	BGPBackwardTransition イベントは、BGP FSM が大きい番号が付いた状態から小さい番号が付いた状態に移行した場合に生成されます。

CPU 使用率ポーリング

表 *10 : CISCO-PROCESS-MIB*

カウンタ	OID	説明
CPU Total Utilization	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	過去 1 分間のシステムプロセスの合計 CPU 使用率。

カウンタ	OID	説明
個々の CPU コア使用率	cpmCPUTotal1minRev の関連パラメータと値 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 ～ 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	過去 1 分間の個々の CPU コア使用率の値。「n」はコアの数を表します。 例： • 3.6.1.4.1.9.9.109.1.1.1.1.7(n+2) - 集約システム CPU 使用率（この値は、シングルコンテキストモードの 3.6.1.4.1.9.9.109.1.1.1.1.7.1 のシステム CPU 使用率と同じです）。 • 3.6.1.4.1.9.9.109.1.1.1.1.7(n+3) - Snort 平均 CPU 使用率（すべての snort インスタンスの合計値） • 3.6.1.4.1.9.9.109.1.1.1.1.7(n+4) - システムプロセス平均 %（「Sysproc」コアの平均）

（注） CPU のモニタリング（hrProcessorTable および hrNetworkTable）に関連する SNMP OID 1.3.6.1.2.1.25.3.3 および 1.3.6.1.2.1.25.3.4 は、ASA FirePOWER では削除されています。デバイスの CPU 正常性の詳細情報は、デバイスマネージャを介してのみ、表示およびモニタリングできます。

SNMPv3 ユーザーの追加

（注） SNMPv3 でのみユーザーを作成できます。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ーのみをサポートすることに注意してください。

SNMPユーザーには、ユーザー名、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。

（注） クラスタリングまたは高可用性でSNMPv3を使用する場合、最初のクラスタ形成後に新しいクラスタユニットを追加するか、高可用性ユニットを交換すると、SNMPv3ユーザーは新しいユニットに複製されません。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいユニットに強制的にレプリケートする必要があります。

認証アルゴリズムのオプション

認証アルゴリズムのオプションはMD5（廃止、6.5より前のみ）、SHA、SHA224、SHA256、およびSHA384です。

（注） MD5 オプションは廃止されました。展開に、6.5 より前のバージョンを使用して作成されたMD5認証アルゴリズムを使用するSNMP v3ユーザーが含まれている場合、6.7以前のバージョンを実行する FTD でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 認証アルゴリズムを保持したり、MD5 認証アルゴリズムを使用して新しいユーザーを作成したりすることはできません。管理センターでバージョン 7.0 以降を実行している Threat Defense を管理している場合、MD5認証アルゴリズムを使用するプラットフォーム設定ポリシーをそれらの Threat Defense に展開すると失敗します。

暗号化アルゴリズムのオプションはDES（廃止、6.5より前のみ）、3DES、AES256、AES192、およびAES128です。

（注） DES オプションは廃止されました。6.5 より前のバージョンを使用して作成されたDES暗号化を使用するSNMP v3ユーザーが展開に含まれている場合は、6.7以前のバージョンを実行するThreat Defense でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集した後も DES 暗号化を維持したり、DES 暗号化を使用する新しいユーザーを作成したりすることはできません。管理センターでバージョン 7.0 以降を実行している Threat Defense を管理している場合、DES 暗号化を使用するプラットフォーム設定ポリシーをそれらの Threat Defense に展開すると失敗します。

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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SNMP]** > **[ユーザー（Users）]** 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 リストからユーザー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 [ユーザー名（Username）] フィールドに SNMP ユーザーの名前を入力します。このユーザー名は 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**：Firewall 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**：Firewall 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、SHA、SHA224、SHA256、SHA384 のうち、使用する認証タイプを選択します。

（注）
MD5 オプションは廃止されました。展開に、6.5 より前のバージョンを使用して作成された MD5 認証アルゴリズムを使用する SNMP v3 ユーザーが含まれている場合、6.7 以前のバージョンを実行する FTD でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 認証アルゴリズムを保持したり、MD5 認証アルゴリズムを使用して新しいユーザーを作成したりすることはできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、MD5 認証アルゴリズムを使用するプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。

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 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。

（注）
DES オプションは廃止されました。6.5 より前のバージョンを使用して作成された DES 暗号化を使用する SNMP v3 ユーザーが展開に含まれている場合は、6.7 以前のバージョンを実行する Firewall Threat Defense でそれらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集した後も DES 暗号化を維持したり、DES 暗号化を使用する新しいユーザーを作成したりすることはできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、DES 暗号化を使用するプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。

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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

SNMP ホストの追加

[ホスト（Host）] 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、Firewall 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。

最大 8,192 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。

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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SNMP]** > **[ホスト（Hosts）]** 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）[ユーザー名（User Name）] ドロップダウン リストから設定した SNMP ユーザーのユーザー名を選択します。

（注）
SNMP ホストごとに 23 人までの SNMP ユーザー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 サーバーを有効にする（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 [次でアクセス可能（Reachable By）] オプションで、デバイスと SNMP 管理ステーションの間の通信インターフェイスタイプを選択します。デバイスの管理インターフェイスまたは使用可能なセキュリティゾーン/名前付きインターフェイスのいずれかを選択できます。

- **デバイスの管理インターフェイス**：デバイスと SNMP 管理ステーション間の通信は、管理インターフェイスを介して行われます。
  - SNMPv3 ポーリングにこのインターフェイスを選択すると、設定されたすべての SNMPv3 ユーザーがポーリングを許可され、ステップ 6（36 ページ）で選択したユーザーに制限されません。ここでは、SNMPv3 ホストからの SNMPv1 および SNMPv2c は許可されていません。
  - SNMPv1 および SNMPv2c ポーリングにこのインターフェイスを選択すると、ポーリングはステップ 5（36 ページ）で選択したバージョンにまったく制限されません。
- **セキュリティゾーンまたは名前付きインターフェイス**：デバイスと SNMP 管理ステーション間の通信は、セキュリティゾーンまたはインターフェイスを介して行われます。
  - [使用可能なゾーン（Available Zones）] フィールドでゾーンを検索します。
  - [選択したゾーン/インターフェイス（Selected Zones/Interfaces）] リストに、デバイスが管理ステーションと通信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。

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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

SNMP トラップの設定

[SNMP トラップ（SNMP Traps）] を使用して、Firewall 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 Firewall 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。

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、Firewall Threat Defense 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。

SNMP Object Navigator

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

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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SNMP] > [SNMP トラップ（SNMP Traps）]** をクリックして、Firewall 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。

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、Firewall Threat Defense 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、シビラティ（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 （60 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。
- [CPU上昇しきい値（CPU Rising Threshold）]：この通知は、設定された期間の CPU 使用率の上昇が、事前定義されたしきい値を超えた場合に生成されます。CPU 上昇しきい値通知を有効にするには、このオプションをオンにします。
  - [割合（Percentage）]：上限しきい値通知のデフォルト値は 70% です。範囲は 10 ～ 94% です。クリティカルしきい値は、95% にハードコードされています。

- [期間（Period）]：デフォルトのモニタリング期間は1分です。範囲は1～60分です。

- [メモリ上昇しきい値（Memory Rising Threshold）]：この通知は、メモリ使用率の上昇が事前定義されたしきい値を超え、使用可能なメモリが減少している場合に生成されます。メモリ上昇しきい値通知を有効にするには、このオプションをオンにします。
  - [割合（Percentage）]：上限しきい値通知のデフォルト値は 70% です。範囲は 50 ～ 95% です。

- [フェールオーバー（Failover）]：この通知は、CISCO-UNIFIED-FIREWALL-MIB によってレポートされたフェールオーバー状態に変化があった場合に生成されます。

- [クラスタ（Cluster）]：この通知は、CISCO-UNIFIED-FIREWALL-MIB によってレポートされたクラスタの正常性に変化があった場合に生成されます。

- [ピアフラップ（Peer Flap）]：この通知は、BGP ルートフラッピングが発生した場合に生成されます。これは、BGP システムが、ネットワークの到達可能性情報をアドバタイズするために過剰な数の更新メッセージを送信する状況です。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

SSL

（注） このタスクを実行するには、管理者権限があり、リーフドメインに属している必要があります。

完全にライセンス供与されたバージョンの Secure Firewall 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 Secure Firewall Management Center を実行している場合は、[SSL 設定（SSL Settings）] は無効になります。また、ライセンス供与された Secure Firewall 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）] 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、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*License Types and Restrictions*」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、Firewall 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）] 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、SSL 設定について （41 ページ）を参照してください。

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

[展開（Deploy）] > [展開（Deployment）] を選択し、[展開（Deploy）] をクリックして、割り当てられたデバイスにポリシーを展開します。

SSL 設定について

Firewall Threat Defense デバイスでは、セキュ 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。

（注） セキュリティ認証（UCAPL、CC、または FIPS）準拠モードで動作するように Firewall Management Center と Firewall Threat Defense が構成されていても、Firewall Management Center はサポートされていない暗号の構成を許可します。たとえば、FIPS 対応モードでは、Management Center は FIPS に準拠していない DH グループ 5 の構成を許可します。ただし、非準拠の暗号が使用されるため、VPN トンネルはネゴシエートしません。

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

[Minimum SSL Version Server]：Firewall Threat Defense デバイスがサーバー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。

[TLSバージョン（TLS Version）]：ドロップダウンリストから、次のいずれかの TLS 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。
TLSV1.3	SSLv2 クライアントの hello を受け入れ、TLSv1.3（以降）をネゴシエートします。

（注） リモートアクセス VPN の TLS 1.3 には、Cisco Secure Client バージョン 5.0 以降が必要です。

[DTLSバージョン（DTLS Version）]：選択した TLS バージョンに基づいて、ドロップダウンリストから DTLS バージョンを選択します。デフォルトでは、DTLSv1 は Firewall Threat Defense デバイスで設定されており、要件に応じて DTLS バージョンを選択できます。

（注） TLS プロトコルのバージョンが、選択した DTLS プロトコルバージョン以上であることを確認します。TLS プロトコルバージョンでは、次の DTLS バージョンがサポートされています。

TLS V1	DTLSv1
TLSV1.1	DTLSv1

TLSV1.2	DTLSv1、DTLSv 1.2
TLSV1.3	DTLSv1、DTLSv 1.2

[Diffie-Hellman グループ（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、[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。

TLSv1.3 では、次の暗号方式のサポートが追加されています。

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

Secure Firewall 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）]：Secure Firewall 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
- TLSV1.3
- DTLSv1
- DTLSv1.2

[セキュリティ レベル（Security Level）]：Firewall 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。

評価ライセンスを使用しているFirewall Threat Defenseデバイスがある場合、デフォルトではセキュリティレベルが低くなります。Firewall Threat Defense スマートライセンスでは、デフォルトのセキュリティレベルは[高（High）]です。次のオプションのいずれかを選択して、必要なセキュリティレベルを設定できます。

- [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、DES-CBC3-SHA、TLS_CHACHA20_POLY1305_SHA256 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。
- [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。

[Cipher Algorithms/Custom String]：Firewall 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

Firewall 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

Syslog

Firewall 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。また、一部のセキュリティ イベントを syslog サーバー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、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。

表 *11* : のシステム ログ *Secure Firewall 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 サーバー、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、Secure Firewall 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 Secure Firewall 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**
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、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「About Sending Syslog Messages for Security Events」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）]
（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、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Configurations Supporting Alert Responses*」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、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Creating a Syslog Alert Response*」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）]

複数の syslog サーバーを設定し、各サーバー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。

重要度レベル

次の表に、syslog メッセージのシビラティ（重大度）の一覧を示します。

表 *12 : Syslog*メッセージのシビラティ（重大度）

レベル番号	重要度	説明
0	**致命的**	システムが使用不可能です。
1	**Alert**（警告）	すぐに措置する必要があります。
2	**深刻**	深刻な状況です。
3	**エラー**	エラー状態です。
4	**warning**	注意状態。
5	**Notification**（通告）	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。 問題をデバッグするときに、このレベルで一時的にのみログに記録します。このログレベルでは、非常に多くのメッセージが生成される可能性があるため、システムパフォーマンスに影響を与える可能性があります。

（注） ASA および Firewall 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、Firewall 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 Firewall 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 *13 : syslog* メッセージの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	ユーザ認証	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
—	ボットネット トラフィック フィルタ	338
bridge	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
citrix	Citrix クライアント	723
—	クラスタリング	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	セキュアなデスクトップ	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 コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	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 アドレスの割り当て	735
ips	侵入防御システム	400、401、420

クラス	定義	Syslog メッセージ ID 番号
—	IPv6	325
—	ライセンシング	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ための NAC 設定	732
—	NAT および PAT	305
—	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
—	Phone Proxy	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120
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

クラス	定義	Syslog メッセージ ID 番号
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
tag-switching	サービス タグ スイッチング	779
transactional-rule-engine-tre	トランザクション ルール エンジン	780
uc-ims	UC-IMS	339
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 セキュアクライアント	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 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

- Firewall Management Center をプライマリ syslog サーバーとして設定しないでください。Firewall Management Center は、いくつかの syslog をログに記録できます。ただし、特に複数のセンサーが使用され、すべてのセンサーから syslog が送信される場合、すべてのセンサーの接続イベントから送信される大量の情報を格納するのに十分なストレージのプロビジョニングはありません。
- 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。
- syslog サーバーは、ファイアウォールシステムの syslog-ng プロセスに基づいて動作します。SecureWorks の *scwx.conf* ファイルなどの外部設定ファイルは使用しないでください。このようなファイルは、デバイスと互換性がありません。これらを使用すると、解析エラーが発生し、最終的に syslog-ng プロセスが失敗します。
- Firewall 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、Firewall 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。
- トランスポートプロトコルとして TCP を使用する場合、メッセージが失われないように syslog サーバーへの接続が 4 つ開きます。syslog サーバーを使用して非常に多数のデバイスからメッセージを収集する場合、接続オーバーヘッドの合計がサーバーに対して大きすぎる場合は、代わりに UDP を使用します。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバー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、Firewall 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。すべてのシビラティ（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 サーバー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。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。
- Firewall 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。

- TCP ロギングホストがダウンすると、接続ステータスが *[*接続済み（*Connected*）*]* から *[*接続されていない（*Not connected*）*]* に変わるまで約 6 分かかります。ロギングは TCP を使用してチャネルステートを検出します。それまでは、ロギングはチャネルを介してログを送信します。この間に、**show log**を実行すると、出力に TCP ロギングホストが接続済みであると表示されます。TCP チャネルが閉じられると、TCP ロギング ホストの状態は *[*接続されていません（*Not connected*）*]* に更新されます。

Firewall Threat Defense デバイスの syslog ロギングの設定

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 Firewall Threat Defense 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 Firewall Threat Defense プラットフォームの設定 （54 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 （51 ページ）で要件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、Firewall 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）] をクリックしてロギングを有効にし、FTP サーバーの設定を指定し、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 （54 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）] 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 （57 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）] 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 （58 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）] 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 （59 ページ）を参照してください。

ステップ 7 [レート制限（Rate Limit）] 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シビラティ（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 （60 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、サーバーを 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 （61 ページ）を参照してください。

ステップ 9 [Syslogサーバー（Syslog Servers）] をクリックして、ロギング接続先として指定される Syslog サーバーの 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 サーバーの設定 （63 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 Firewall Threat Defense 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 サーバー（Syslog Servers）] タブ：
  - [Syslog サーバーを追加（Add Syslog Server）] 形式（および設定済みサーバーのリスト）のすべてのオプション

ロギングの有効化および基本設定の構成

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し、基本設定を構成します。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 サーバー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 Firewall Threat Defense 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 Firewall Threat Defense プラットフォームの設定 （54 ページ）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、Firewall 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）]：Firewall 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）：Firewall 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。

  EMBLEM syslog フォーマットは、RFC 3164 および RFC 5424 の標準に基づいて構築されたシスコ固有の規則です。したがって、EMBLEM が有効になっている場合、syslog メッセージは、<PRI> フィールドの後にコロン（:）を出力します。これは RFC 5424 フォーマットとは対照的です。

  （注）
  RFC5424 形式の syslog メッセージには、通常、プライオリティ値（PRI）が表示されます。ただし、Firewall Management Center では、管理対象 Firewall Threat Defense デバイスの syslog メッセージに PRI 値を表示する場合、EMBLEM 形式を有効にしてください。また、EMBLEM フォーマットの syslog メッセージにデバイス ID は表示されません。

- 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 711001 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。範囲は4096～52428800です。

ステップ 4 （任意）Firewall Management Center への syslog メッセージロギングを設定します。

a) **[（Cisco Secure Firewall Management Center へのロギングを有効化（Enable Logging to Secure Firewall Management Center）]** 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。

b) [ログレベル（Logging Level）] ドロップダウンリストから、ロギングメッセージの syslog セキュリティレベルを選択します。

- VPN メッセージのロギングレベルは、デフォルトで [エラー（Errors）] に設定されます。

  VPN トラブルシューティング syslog により、Firewall Management Center に過度の負荷がかかる場合があります。そのため、このオプションを有効にするには注意が必要です。また、サイト間 VPN またはリモートアクセス VPN を設定してデバイスを設定すると、VPN syslog はデフォルトで自動的に Management Center に送信されます。特に複数のデバイスが関係する RAVPN の場合は、Firewall Management Center への syslog の過剰なフローを制限するために、ログレベルを [エラー（Error）] 以上に制限することをお勧めします。

レベルについては、重要度レベル （47 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、サーバーにログ バッファの内容を保存するには、FTP サーバーを設定します。FTP サーバー情報を指定します。

- FTP サーバーバッファラップ（FTP Server Buffer Wrap）：バッファの内容が上書きされる前にFTPサーバーに保存するには、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 サーバーの 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 サーバー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 サーバーへのユーザー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、サーバーにログ 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（キロバイト単位）。範囲は、4 ～ 8044176 KB 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 KB です。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

ロギング接続先の有効化

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 Firewall Threat Defense プラットフォームの設定 （54 ページ）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、Firewall 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。

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。

- [シビラティ（重大度）によるフィルタ（Filter on severity）]：シビラティ（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）]ページで作成します。
- [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シビラティ（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 （48 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

電子メール アドレスへの syslog メッセージの送信

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 Firewall Threat Defense プラットフォームの設定 （54 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 （54 ページ）
- ロギングの宛先として電子メールを設定します

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、Firewall 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、重要度レベル（47 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

カスタム イベント リストの作成

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、シビラティ（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、シビラティ（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）] 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）] 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 Firewall Threat Defense プラットフォームの設定 （54 ページ）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、Firewall 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) シビラティ（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、[シビラティ（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 （48 ページ） を参照してください。

レベルについては、重要度レベル （47 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）] 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 （48 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）] 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 （57 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートは、シビラティ（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 Firewall Threat Defense プラットフォームの設定 （54 ページ） 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、Firewall 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 シビラティ（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）]** > **[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）：レートを制限するシビラティ（重大度）レベル。レベルについては、重要度レベル （47 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）]** > **[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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

Syslog 設定

一般的な Syslog 設定を設定して、Syslog サーバーに送信される 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、メッセージのシビラティ（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。Cisco Secure Firewall Management Center アドミニストレーション ガイド の「セキュリティイベントの *syslog* メッセージに適用する *Threat Defense* プラットフォームの設定」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、Firewall 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 サーバーのシステム 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。メッセージにファシリティ値を含める必要がある場合は、Cisco Secure Firewall Management Center アドミニストレーション ガイド の「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 5424 syslog 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シビラティ（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）] 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、新しいシビラティ（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、シビラティ（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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

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。

Syslog サーバーの設定

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 サーバーを設定するには、次の手順を実行します。

この syslog サーバーに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させる場合は、セキュリティイベントの syslog メッセージに適用する Firewall Threat Defense プラットフォームの設定 （54 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 （51 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。

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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [Syslog] > [Syslog サーバー（Syslog Server）] > を選択します。

ステップ 3 [TCP syslogサーバーがダウンしているときにユーザートラフィックの通過を許可する（推奨）（Allow user traffic to pass when TCP syslog server is down (Recommended)）] 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サーバー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。

（注）

- このオプションは、デフォルトで有効です。必要な場合を除き、デバイスが外部TCP syslogサーバーに到達できない場合は、脅威防御デバイスを介した接続を許可することをお勧めします。
- Firewall Management Center バージョン 6.2.x 以前で [TCP syslogサーバーがダウンしているときにユーザートラフィックの通過を許可する（Allow user traffic to pass when TCP syslog server is down）] オプションが無効になっている場合、このオプションはバージョン 6.3 以降にアップグレードした後も無効状態になります。手動で有効にしてください。
- このオプションが無効で、デバイスに複数のTCP syslogサーバーが設定されている場合、少なくとも1つのサーバーが脅威防御デバイスから到達可能であれば、ユーザートラフィックの通過が許可されます。そのため、無効化オプションは、デバイスに設定されているTCP syslog サーバーに到達できない場合にのみ適用されます。デバイスは、デバイスを介して拒否されたトラフィックの根本原因を説明する次の syslog を生成します。

```
%FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. New
connections are denied based on logging permit-hostdown policy
```

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 サーバーがビジー状態の場合に 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）。

メッセージが指定されたキューのサイズを超えると、メッセージは破棄され、syslog が失われます。最適なキューサイズを決定するには、使用可能なブロックメモリを特定する必要があります。**show blocks** コマンドを使用して、現在のメモリ使用率を確認します。コマンドと属性の詳細については、『*Cisco Secure Firewall ASA Series Command Reference Guide*』を参照してください。さらにサポートが必要な場合は、Cisco TAC にお問い合わせください。

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

a) [IP アドレス（IP Address）] ドロップダウン リストで、Syslog サーバーの 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、Firewall Threat Defense デバイスと Syslog サーバー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 です。TCP 用にポート 1470 を手動で設定する必要があります。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）。

EMBLEM syslog フォーマットは、RFC 3164 および RFC 5424 の標準に基づいて構築されたシスコ固有の規則です。したがって、EMBLEM が有効になっている場合、syslog メッセージは、<PRI> フィールドの後にコロン（:）を出力します。

（注）
RFC5424 形式の syslog メッセージには、通常、プライオリティ値（PRI）が表示されます。ただし、Firewall Management Centerでは、Cisco EMBLEM 形式でのロギングを有効にした場合にのみ、管理対象 Firewall Threat Defense の syslog メッセージに PRI 値が表示されます。また、EMBLEM フォーマットの syslog メッセージにデバイス ID は表示されません。

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、デバイスとサーバーの間の接続を 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、プロトコルとして TCP を選択し、1025 ～ 65535 の範囲のポート値を選択する必要があります。また、**[Devices]** > **[Certificates]** ページで、syslog サーバー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、Firewall Threat Defense デバイスから syslog サーバー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を許可します。デバイス管理インターフェイスでは、[Enable Secure Syslog] オプションはサポートされていません。

e) Syslog サーバーと通信するための [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。

- [Device Management Interface]：管理インターフェイスから syslog を送信します。Snort イベントで Syslog を設定する場合は、このオプションを使用することをお勧めします。

  （注）
  [Device Management Interface] オプションでは、[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。

重要
Firewall Threat Defense データプレーン（Lina）の syslog メッセージは、診断インターフェイスを介して送信できません。データプレーンの syslog メッセージを送信するように、他のインターフェイスまたは管理インターフェイス（Br1/Management0）を設定します。

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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

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。

タイムアウト

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、Firewall 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。FIN と FIN-ACK の両方が検出された場合、接続はハーフクローズ状態と見なされます。FIN のみが検出された場合は、通常の接続タイムアウトが適用されます。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。

  Sun RPC ベースの接続では、親接続が削除またはタイムアウトされると、新しい子接続が親子接続の一部と見なされないことがあるため、システムで設定されているポリシーまたはルールに従って新しい接続が評価される可能性があります。親接続がタイムアウトになると、既存の子接続はタイムアウトの設定値になるまで有効です。
- [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）]：同じネットワークへの複数のルートが存在し、それぞれメトリックが異なる場合、システム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。このタイマーは、仮想トンネルインターフェイス（VTI）を介した接続には適用されません。VTI を介した接続がスタックした場合は、手動でクリアする必要があります。
- [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）]：ARP テーブルを再構築する間隔の秒数（60 ～ 4,294,967）。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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

時刻の同期

Network Time Protocol（NTP）サーバーを使用して、デバイスのクロック設定を同期します。Firewall Management Center と同じ NTP サーバーを使用するように、Firewall Management Center によって管理されるすべての Firewall Threat Defense を設定することをお勧めします。Firewall Threat Defense は、設定された NTP サーバーから時刻を直接取得します。Firewall Threat Defense の設定済み NTP サーバーが何らかの理由で到達できない場合は、その時刻を Firewall Management Center と同期します。

デバイスは NTPv4 をサポートします。

（注） Firepower 4100/9300 シャーシに Firewall Threat Defense 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 Firewall Management Center には、同じ NTP サーバーを使用する必要があります。

始める前に

- 組織に Firewall Threat Defense からアクセスできる 1 台以上の NTP サーバーがある場合は、Firewall Management Center 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 サーバーを使用します。
- Firewall Management Center の 1 つまたは複数の NTP サーバーを設定する場合に [認証されたNTPサーバーのみを使用する（Use the authenticated NTP server only）] を選択すると、デバイスでは、Firewall Management Center を使用して認証するように設定された 1 つまたは複数の NTP サーバーのみが使用されます。（管理対象デバイスは、Firewall Management Center と同じ NTP サーバーを使用しますが、その NTP 接続では認証を使用しません）。
- デバイスが NTP サーバーに到達できない場合または組織に NTP サーバーがない場合は、次の手順で説明するように、[ディフェンスセンターの NTP 使用（Via NTP from Defense Center）] オプションを使用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、Firewall 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。

- [ディフェンスセンターの NTP 使用（Via NTP from Defense Center）]：（デフォルト）。管理対象デバイスは、Firewall Management Center 用に設定された NTP サーバー（認証されたNTPサーバーを除く）から時刻を取得し、それらのサーバーと時刻を直接同期します。ただし、次のいずれかに該当する場合、管理対象デバイスは Firewall Management Center と時刻を同期します。
  - Firewall Management Center の NTP サーバーに、デバイスからアクセスできない。
  - Firewall Management Center には、認証されていないサーバーはありません。
- [Via NTP from]：Firewall Management Center がネットワーク上の NTP サーバーを使用している場合は、このオプションを選択して、[System] > [Configuration] > [Time Synchronization] で指定した NTP サーバーと同じ完全修飾 DNS 名（ntp.example.com など）か IPv4 または IPv6 アドレスを入力します。NTP サーバーに到達できない場合は、Firewall Management Center が NTP サーバーとして機能します。

複数の NTP サーバーが設定されている場合、デバイスは、RFC で定義されている基準に基づいて適切と見なされる NTP サーバーを使用します。したがって、特定の NTP サーバーの [使用中（Being used）] のステータスは、そのサーバーがデバイスによって現在使用されていることを示します。

ステップ 4 [保存（Save）] をクリックします。

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。

タイムゾーン

デフォルトでは、システムは UTC タイムゾーンを使用します。デバイスに別のタイムゾーンを指定するには、次の手順を実行します。

指定したタイムゾーンは、この機能をサポートするポリシーの時間ベースのポリシーアプリケーションにのみ使用されます。

（注） 時間ベースの ACL は、Firewall Management Center 7.0 以降の Snort 3 でもサポートされています。

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、Firewall Threat Defense ポリシーを作成または編集します。

[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[タイムゾーン（Time Zone）] ページからタイムゾーンオブジェクトを作成することもできます。

ステップ 2 [+] をクリックして、新しいタイムゾーンオブジェクトを作成します。

ステップ 3 タイムゾーンを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

- 時間範囲オブジェクトを作成して、アクセス制御およびプレフィルタールールで適用可能な時間範囲を選択し、正しいタイムゾーンに関連付けられているデバイスに親ポリシーを割り当てます。
- 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。

UCAPL/CC コンプライアンス

この設定と、Firewall Management Center で有効にする方法の詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイド を参照 してください。

⚠

注意 この設定を有効にした後に無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードから解除する必要がある場合は、再イメージ化する必要があります。

始める前に

- Secure Firewall Threat Defense デバイスは評価ライセンスを使用できません。輸出管理機能を有効にするには、Smart Software Manager アカウントを有効にする必要があります。
- Secure Firewall Threat Defense デバイスはルーテッド モードで展開する必要があります。
- このタスクを実行するには、管理者ユーザーである必要があります。
- Firewall Threat Defense デバイスが高可用性の場合、セキュリティ認定準拠モードは変更できません。高可用性ペアを形成する前に、セキュリティ認定準拠モードを変更してください。

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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [UCAPL/CC コンプライアンス（UCAPL/CC Compliance）] をクリックします。

ステップ 3 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2 つの選択肢があります。

- [コモン クライテリア（Common Criteria）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [CC] を選択します。
- [Unified 機能承認製品リスト（Unified Capabilities Approved Products List）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [UCAPL] 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、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更を展開するまで、変更は有効ではありません。

パフォーマンス プロファイル

パフォーマンスプロファイルにより、デバイスの CPU コアがデータプレーン（Lina）と Snort の 2 つのメインシステムプロセスに割り当てられる方法が決定されます。データプレーンは、VPN 接続、ルーティング、およびその他の基本的なレイヤ 3/4 処理を処理します。Snort は、侵入とマルウェアの防止、URL フィルタリング、アプリケーション フィルタリング、および

詳細なパケットインスペクションを必要とするその他の機能を含む、高度なインスペクションを提供します。

基本機能と高度な機能をバランスよく使用する場合は、パフォーマンスプロファイルを変更しないでください。システムは、それらのプロセスにコアをバランスよく割り当てるように設計されています。割り当ては、ハードウェアモデルによって異なります。

ただし、デバイスを主に VPN や、侵入などの高度な検査に使用する場合は、パフォーマンスプロファイルを変更して、頻繁に使用される機能に多くのコアが割り当てられるようにすることができます。これにより、システムのパフォーマンスが向上する可能性があります。

始める前に

- これらの設定は、リリース 7.3 以降を実行しているシステムにのみ適用されます。
- パフォーマンスプロファイルは、次のデバイスタイプでサポートされています。
  - Firepower 4100/9300
  - Secure Firewall Threat Defense Virtual
- パフォーマンスプロファイルの変更は、クラスタまたは高可用性グループ内のユニット、またはマルチインスタンス用に設定されたユニットではサポートされません。スタンドアロンデバイス以外にプロファイルを割り当てると、展開はブロックされます。
- コア割り当ての最小数は2です。コアは、選択したパフォーマンスプロファイルに基づいて偶数単位で割り当てられます。

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、Firewall Threat Defense ポリシーを作成または編集します。

ステップ 2 [パフォーマンスプロファイル（Performance Profile）] を選択します。

ステップ 3 プロファイルを選択します。

- [デフォルト（Default）]：これは推奨設定であり、VPNと侵入検査の両方を設定する場合に最適なオプションです。
- [プレフィルタfastpathによるVPNヘビー（VPN Heavy with prefilter fastpath）]：デバイスを主にVPNエンドポイントまたはヘッドエンドとして使用し、プレフィルタポリシーでVPNトラフィックの fastpath のルールを設定する場合は、このオプションを選択して、CPU コアの大部分をデータプレーンに割り当てることができます。90%をデータプレーン、10%を Snort に割り当てます。
- [検査によるVPNヘビー（VPN Heavy with inspection）]：デバイスを主に VPN エンドポイントまたはヘッドエンドとして使用するが、プレフィルタポリシーを使用して VPN トラフィックの fastpath を実行しない場合は、このオプションを選択して、CPU コアの大部分をデータプレーンに割り当てることができます。このオプションは、Snort を使用した侵

入検査、URLフィルタ処理などの高度な機能をネットワーク内の別のデバイスに任せることを前提としています。60% をデータプレーン、40% を Snort に割り当てます。

- [IPSヘビー（IPS Heavy）]：VPN を設定しないが、侵入防御のためにデバイスを使用する場合は、このオプションを選択して、CPU コアの大部分を Snort プロセスに割り当てることができます。30% をデータプレーン、70% を Snort に割り当てます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーを展開します。

ステップ 6 展開が完了したら、影響を受ける各デバイスを再起動して、新しいコアの割り当てを行えるようにする必要があります。

プラットフォーム設定の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
CPU コア割り当てのパフォーマンスプロファイル。	7.3.0	7.3.0	データプレーンと Snort に割り当てられたシステムコアの割合を調整して、システムパフォーマンスを調整できます。この調整は、VPN と侵入ポリシーの相対的な使用に基づいています。両方を使用する場合は、コア割り当てをデフォルト値のままにします。システムを主に VPN（侵入ポリシー適用なし）または IPS（VPN 設定なし）として使用する場合、コア割り当てをデータプレーン（VPN の場合）または Snort（侵入インスペクションの場合）にスキューできます。 [パフォーマンスプロファイル（Performance Profile）] ページがプラットフォーム設定ポリシーに追加されました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
リモートアクセスVPNの TLS 1.3。	7.3.0	7.3.0	TLS 1.3 を使用して、リモートアクセス VPN 接続を暗号化できます。 デバイスがリモートアクセスVPNサーバーとして機能する場合、Threat Defense プラットフォーム設定を使用して、そのデバイスでは TLS 1.3 プロトコルを使用する必要があることを指定します。 TLS 1.3 では、次の暗号方式のサポートが追加されています。 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 この機能には、Cisco Secure Client バージョン 5.0 以降が必要です。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[新しいポリシー（New Policy）]** > **[Threat Defense 設定の追加/編集（Add/Edit Threat Defense Settings）]** > **[SSL]** > **[TLS バージョン（TLS Version）]**
DNS要求を解決するための複数の DNS サーバーグループ。	7.2.0	7.2.0	クライアントシステムからのDNS要求を解決するために、複数のDNSグループを設定できます。これらの DNS サーバー グループを使用して、さまざまな DNS ドメインの要求を解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバーを使用するキャッチオールのデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部 DNS サーバーを使用する別のグループを構成できます。したがって、組織のドメイン名を使用したFQDNへの接続は、内部DNSサーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS サーバーを使用します。 **[プラットフォーム設定（Platform Settings）]** > **[DNS]**ページを変更しました。
HTTP、ICMP、およびSSHプラットフォーム設定のネットワークオブジェクトのサポート。	7.1.0	7.1.0	Threat Defense プラットフォーム設定ポリシーで IP アドレスを設定するときに、ホストまたはネットワークのネットワークオブジェクトを含むネットワーク オブジェクト グループを使用できるようになりました。 サポートされているプラットフォーム： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
信頼された DNS サーバの指定のサポート。	7.1.0	7.1.0	直接インターネットアクセスの使用中にアドレス解決のために信頼できる DNS サーバを指定するオプションが導入されました。 直接インターネットアクセスの設定時に、信頼された DNS サーバーを設定するための新しいタブ（**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** > **[DNS]** > **[信頼されたDNSサーバー（Trusted DNS Servers）]**）を追加しました。 サポートされているプラットフォーム： Firewall Threat Defense
SNMPv3 ユーザーの MD5認証アルゴリズムまたは DES 暗号化を使用するプラットフォーム設定は、バージョン 7.0 以降を実行している Firewall Threat Defense デバイスに展開できません。	7.0.0	7.0.0	バージョン 6.5 では、Firewall Threat Defense における SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化が廃止されました。展開に、6.4 以前のバージョンを使用して作成された MD5 認証アルゴリズムまたは DES 暗号化を使用する SNMPv3 ユーザーが含まれている場合、バージョン 6.7 以前を実行している Firewall Threat Defense デバイスでは、それらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 または DES の設定を保持することはできません。また、MD5 または DES の設定を使用して新しいユーザーを作成することもできません。Firewall Management Center でバージョン 7.0 以降を実行している Firewall Threat Defense を管理している場合、MD5 認証アルゴリズムまたは DES 暗号化を使用する SNMP v3 ユーザーを持つプラットフォーム設定ポリシーをそれらの Firewall Threat Defense に展開すると失敗します。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** > **[ホスト（Host）]** サポートされているプラットフォーム： Firewall Threat Defense
SNMPv3 ユーザーの認証アルゴリズムの SHA224 または SHA384 を指定します。	7.0.0	7.0.0	SNMPv3 ユーザーの認証アルゴリズムとして、SHA224 または SHA384 を選択できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** > **[ユーザー（Users）]** サポートされているプラットフォーム： Firewall Threat Defense
デバイスのタイムゾーンを指定します。	6.6.0	6.6.0	時間ベースのポリシーの適用で使用する、管理対象デバイスのローカルタイムゾーンを指定します。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[タイムゾーン（Time Zone）]** サポートされているプラットフォーム： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SNMP 通信の管理インターフェイスを指定します。	6.6.0	6.6.0	デバイスとSNMP管理ステーションの間の通信に管理インターフェイスを選択できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ホスト（Host）]** サポートされているプラットフォーム： Firewall Threat Defense
SNMPv3 ユーザーの認証アルゴリズムの SHA256 を指定します。	6.6.0	6.6.0	SNMPv3 ユーザーの認証アルゴリズムとして、SHA256 を選択できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）]** サポートされているプラットフォーム： Firewall Threat Defense
Firewall Threat Defense における SNMPv3 ユーザー向けの DES 暗号化と MD5 認証アルゴリズムは廃止されました。	6.5.0	いずれか	Firewall Threat Defense デバイスでは、SNMPv3 ユーザーに MD5 認証アルゴリズムまたはDES暗号化を使用しないことを推奨します。これらのオプションは廃止されているためです。展開に、6.4 以前のバージョンを使用して作成された MD5 認証アルゴリズムまたは DES 暗号化を使用する SNMPv3 ユーザーが含まれている場合、それらのユーザーを引き続き使用できます。ただし、これらのユーザーを編集して MD5 または DES の設定を保持することはできません。また、MD5 またはDES の設定を使用して新しいユーザーを作成することもできません。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）]** サポートされているプラットフォーム： Firewall Threat Defense
TCP syslog サーバーがダウンしているときにユーザートラフィックの通過を許可します。	6.3.0	6.3.0	デバイスが外部 TCP syslog サーバーに到達できない場合は、Threat Defense デバイスを介した接続を許可することを推奨します。[プラットフォーム設定（Platform Settings）] の [TCP syslogサーバーがダウンしているときにユーザートラフィックの通過を許可する（有効にすることを推奨）（Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)）] オプションはデフォルトで有効になっています。
SSH ログイン失敗の制限数。	6.3.0	6.3.0	ユーザーが 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	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SSH用の外部認証が追加されました。	6.2.3	6.2.3	LDAP または RADIUS認証を使用して Firewall Threat Defense への SSH の外部認証を設定できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（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： Firewall Threat Defense
UC/APPL 準拠モードのサポート。	6.2.1	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。 新規/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
リモートアクセスVPNの SSL 設定。	6.2.1	6.2.1	Firewall Threat Defense デバイスでは、セキュ 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 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。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SSL]** サポートされているプラットフォーム： Firewall Threat Defense
SSH および HTML 用の外部認証は削除されました。	6.1.0	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。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（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： Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firepower Threat Defense のサポート。	6.0.1	6.0.1	この機能が導入されました。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** サポートされているプラットフォーム： Firewall Threat Defense

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