



## Firepower Threat Defense の使用例

ここでは、Firepower Device Manager を使用して、Firepower Threat Defense で実行する共通のタスクについていくつか説明します。これらの使用例は、デバイス設定ウィザードが完了しており、この初期設定が保持されていることを前提としています。初期設定を変更した場合でも、これらの例を使用して、製品の使用方法を理解できます。

- [Firepower Device Manager でデバイスを設定する方法 \(1 ページ\)](#)
- [ネットワークトラフィックを調べる方法 \(6 ページ\)](#)
- [脅威をブロックする方法 \(15 ページ\)](#)
- [マルウェアをブロックする方法 \(22 ページ\)](#)
- [アクセプタブルユースポリシー \(URL フィルタリング\) の実装方法 \(26 ページ\)](#)
- [アプリケーションの使用を制御する方法 \(31 ページ\)](#)
- [サブネットを追加する方法 \(35 ページ\)](#)
- [その他の例 \(42 ページ\)](#)

## Firepower Device Manager でデバイスを設定する方法

セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- (ASA 5506-X および ISA 3000 を除く)。外部インターフェイスと内部インターフェイス。その他のデータインターフェイスは設定されません。
- (ASA 5506-X、ISA 3000 のみ)。外部インターフェイスと、他のすべてのデータのインターフェイスが含まれる内部ブリッジグループ。
- 内部インターフェイスおよび外部インターフェイスのセキュリティゾーン。
- 内部から外部へのトラフィックをすべて信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスまたはブリッジグループで実行されている DHCP サーバ。

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

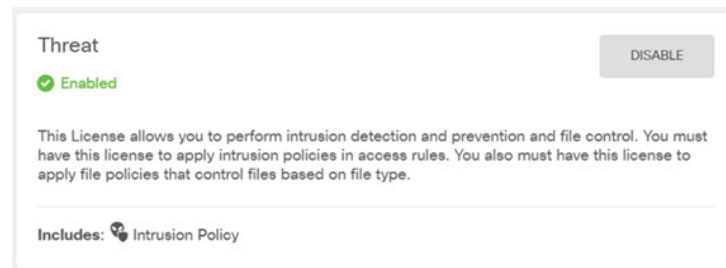
## 手順

**ステップ 1** [デバイス (Device)] を選択し、[スマートライセンス (Smart License)] グループで [設定の表示 (View Configuration)] をクリックします。

使用するオプションのライセンス ([脅威 (Threat)], [マルウェア (Malware)], [URL]) でそれぞれ [有効化 (Enable)] をクリックします。必要かどうかわからない場合は、各ライセンスの説明を確認します。

登録していない場合は、このページから登録できます。[Request Register] をクリックして、説明に従います。評価ライセンスの有効期限が切れる前に登録してください。

たとえば、有効な脅威ライセンスは次のようになります。



**ステップ 2** 他のインターフェイスに接続している場合は、[デバイス (Device)] を選択し、[インターフェイス (Interfaces)] サマリーにあるリンクをクリック。

- ASA 5506-X および ISA 3000 は外部以外のすべてのデータ インターフェイスが含まれるブリッジグループが事前に設定された状態で出荷されるため、これらのインターフェイスを設定する必要はありません。ブリッジグループを分割する場合は、ブリッジグループを編集して個別に扱うインターフェイスを除去できます。その後、別々のネットワークをホストするインターフェイスとしてそれらを設定できます。

他のモデルでは、他のインターフェイスのブリッジグループを作成、別々のネットワークを設定、または両方の組み合わせを設定できます。

各インターフェイスの編集アイコン (🔗) をクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバなどのパブリックアクセス可能な資産を配置する「非武装地帯」(DMZ) として使用するためのインターフェイスを構成します。完了したら [保存 (Save)] をクリックします。

## Edit Physical Interface

Interface Name Status

dmz

Description

---

[IPv4 Address](#) [IPv6 Address](#) [Advanced Options](#)

Type

Static

IP Address and Subnet Mask

192.168.6.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

**ステップ 3** 新しいインターフェイスを構成する場合は、[オブジェクト (Objects)] を選択し、目次から [セキュリティゾーン (Security Zones)] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後は常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZ インターフェイスのために新しい DMZ ゾーンを作成する方法を示します。

## Add Security Zone

Name

dmz-zone

Description

Interfaces

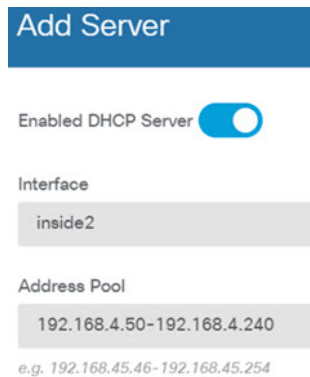
dmz

**ステップ 4** 内部クライアントが DHCP を使用してデバイスから IP アドレスを取得するようにする場合は、[デバイス (Device)]、次に [システム設定 (System Settings)] > [DHCP サーバ (DHCP Server)] を選択します。[DHCP サーバ (DHCP Servers)] タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバがありますが、アドレス プールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバをセットアップするのがごく一般的です。各内部インターフェイスのサーバおよびアドレス プールを設定するには、[+] をクリックします。

クライアントに対して提供される WINS および DNS リストを [設定 (Configuration)] タブで調整することもできます。

次の例では、アドレス プールの 192.168.4.50 ~ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバを設定する方法を示しています。



**ステップ 5** [[デバイス (Device)]] を選択し、次に [設定の表示 (View Configuration)] (または [最初のスタティックルートの作成 (Create First Static Route)]) を [ルーティング (Routing)] グループでクリックし、デフォルト ルートを設定します。

デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4 (0.0.0.0/0)、デフォルトの IPv6 ルートは任意の ipv6 (::0/0) です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

このページで定義したルートは、データインターフェイス用のみです。管理インターフェイスには影響しません。管理ゲートウェイは [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです (アドレスは ISP から取得する必要があります)。[ゲートウェイ (Gateway)] の下部の [新しいネットワークを作成する (Create New Network)] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A list of networks with a '+' icon to add more. The current list contains 'any-ipv4'.

**ステップ 6** [ポリシー (Policies)] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間でのトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーンオブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

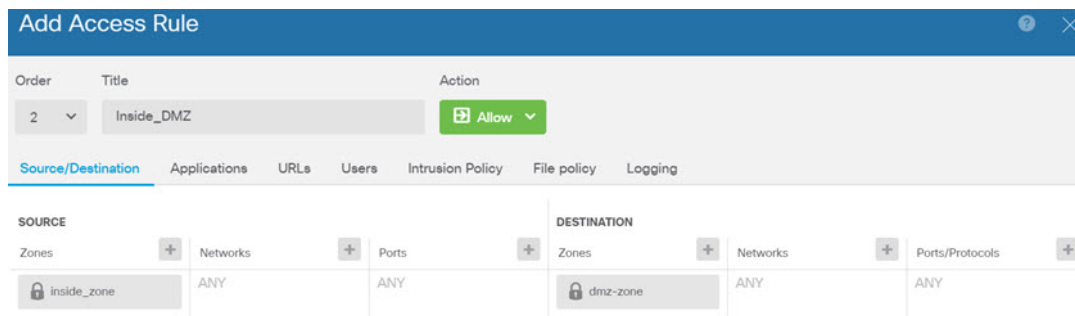
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

- [SSL復号 (SSL Decryption)] : 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ (Identity)] : 個々のユーザにネットワーク アクティビティを関連付ける、またはユーザまたはユーザ グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティ ポリシーを使用します。
- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。

- [NAT] (ネットワーク アドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御 (Access Control) ]: ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル (マルウェア) ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [侵入 (Intrusion) ]: 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーン間のトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection) ] が選択されている場合、[ロギング (Logging) ] を除いて他のいずれのタブでもオプションは設定されません。



**ステップ7** 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes) ] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now) ] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed) ] になります。

## ネットワークトラフィックを調べる方法

デバイスの初期設定を完了すると、インターネットまたはその他のアップストリーム ネットワークへのすべての内部トラフィックアクセスを許可するアクセスコントロールポリシーと、他のすべてのトラフィックをブロックするデフォルトアクションが設定されます。追加のアクセスコントロールルールを作成する前に、ネットワークで実際に発生しているトラフィックを調べると役立ちます。

Firepower Device Manager のモニタリング機能を使用して、ネットワークトラフィックを分析できます。Firepower Device Manager のレポートの内容は、次のとおりです。

- ネットワークの用途
- 最も多くネットワークを使用しているユーザ
- ユーザの接続先
- ユーザが使用しているデバイス
- ヒット数が最も多いアクセスコントロールルール（ポリシー）

初期のアクセスルールでは、ポリシー、宛先、セキュリティゾーンなどのトラフィックについての情報が明らかになります。しかし、ユーザ情報を取得するには、ユーザを認証（識別）する必要があるアイデンティティポリシーの設定が必要です。ネットワークで使用されるアプリケーションの情報を取得するには、追加でいくつかの調整を行う必要があります。

次の手順で、トラフィックをモニタするように Firepower Threat Defense デバイスを設定する方法を説明し、設定ポリシーおよびモニタリングポリシーのエンドツーエンドプロセスの概要を示します。



- (注) この手順では、ユーザがアクセスしたサイトの Web サイトカテゴリとレピュテーションの情報は取得されないため、URL カテゴリダッシュボードに有用な情報は表示されません。カテゴリおよびレピュテーションのデータを取得するには、カテゴリベースの URL フィルタリングを実装し、URL ライセンスを有効化する必要があります。この情報のみ取得する場合は、許可するカテゴリ（金融サービスなど）へのアクセスを許可する新規のアクセス制御ルールを追加して、アクセス制御ポリシーで最初のルールに設定できます。URL フィルタリングの実装の詳細については、[アクセプタブルユースポリシー（URL フィルタリング）の実装方法（26 ページ）](#) を参照してください。

## 手順

- ステップ 1** ユーザの動作を調べるには、接続に関連付けられているユーザを識別するアイデンティティポリシーの設定が必要です。

アイデンティティポリシーを有効化すると、ネットワークを使用するユーザおよびそのユーザが使用しているリソースに関する情報を収集できます。この情報は、ユーザの監視ダッシュボードに表示されます。ユーザ情報は、イベントビューアに表示される接続イベントにも表示されます。

ユーザは、HTTP 接続に Web ブラウザを使用する場合にのみ認証されます。

ユーザが認証に失敗した場合でも、そのユーザは Web 接続を確立することはできます。これは、単に、接続に関するユーザのアイデンティティ情報がないことを意味します。必要に応じて、認証に失敗したユーザのトラフィックをドロップするアクセスコントロールルールを作成できます。

- a) メインメニューで、[ポリシー (Policies)] をクリックして、[アイデンティティ (Identity)] をクリックします。

アイデンティティポリシーは、最初は無効化されています。アイデンティティポリシーはアクティブディレクトリサーバを使用してユーザを認証し、ユーザが使用しているワークステーションの IP アドレスとユーザを関連付けます。その後、システムはその IP アドレスのトラフィックをユーザのトラフィックとして識別します。

- b) [アイデンティティポリシーの有効化 (Enable Identity Policy)] をクリックします。

このアクションで [アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログボックスが開きます。

- c) [レルムサーバ (Realm Server)] をクリックしてドロップダウンリストを開き、[新規アイデンティティレルムの作成 (Create New Identity Realm)] を選択します。

レルムサーバオブジェクトをすでに作成している場合は、それを選択して、サーバの設定手順をスキップします。

- d) 次のフィールドに入力して、[OK] をクリックします。

- [名前 (Name)] : ディレクトリレルムの名前。
- [タイプ (Type)] : ディレクトリサーバのタイプ。サポートされるタイプは **Active Directory** のみで、このフィールドを変更することはできません。
- [ディレクトリユーザ名 (Directory Username)]、[ディレクトリパスワード (Directory Password)] : 取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は **Administrator@example.com** (Administrator だけでなく) などの完全修飾名である必要があります。

(注) この情報から `ldap-login-dn` と `ldap-login-password` が生成されます。たとえば、**Administrator@example.com** は `cn=adminisntrator,cn=users,dc=example,dc=com` に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN (Base DN)] : ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリツリー。(dc=example,dc=com など)。ベース DN の検索の詳細については、[ディレクトリベースの DN の決定](#) を参照してください。
- [ADプライマリドメイン (AD Primary Domain)] : デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。(example.com など)。
- [ホスト名/IPアドレス (Hostname/IP Address)] : ディレクトリサーバのホスト名または IP アドレス。サーバへの暗号化された接続を使用する場合、IP アドレスではなく完全修飾ドメイン名を入力する必要があります。



- [ポート (Port) ] : サーバとの通信に使用するポート番号。デフォルトは389です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化 (Encryption) ] : ユーザおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法 ([STARTTLS] または [LDAPS]) を選択します。デフォルトでは [なし (None) ] になっており、ユーザおよびグループの情報がクリアテキストでダウンロードされます。
  - [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリサーバでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモートアクセス VPN にレルムを使用する場合はサポートされません。
  - [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。
- [信頼できるCA証明書 (Trusted CA Certificate) ] : 暗号化方式を選択する場合、認証局 (CA) の証明書をアップロードして、システムとディレクトリサーバの間で信頼できる接続を有効化します。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス (Hostname/IP Address) ] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

**例 :**

たとえば、次のイメージには、ad.example.com サーバの暗号化されていない接続の作成方法が示されています。プライマリドメインは example.com で、ディレクトリユーザ名は Administrator@ad.example.com です。すべてのユーザおよびグループの情報は、識別名 (DN) ou=user,dc=example,dc=com の下にあります。

<b>Name</b>	<b>Type</b>
AD	Active Directory (AD) ▼
<b>Directory Username</b>	<b>Directory Password</b>
Administrator@ad.example.com	.....
<i>e.g. user@example.com</i>	
<b>Base DN</b>	<b>AD Primary Domain</b>
ou=user,dc=example,dc=com	example.com
<i>e.g. ou=user, dc=example, dc=com</i>	<i>e.g. example.com</i>

## Directory Server Configuration

<b>Hostname / IP Address</b>	<b>Port</b>
ad.example.com	389
<i>e.g. ad.example.com</i>	
<b>Encryption</b>	<b>Trusted CA certificate</b>
NONE ▼	Please select a certificate ▼

- e) [アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログボックスの [レルムサーバ (Realm Server)] リストで、作成したレルムサーバを選択します。
- f) [アイデンティティポリシーの設定 (Identity Policy Configuration)] ダイアログボックスで、アクティブ認証のキャプティブポータル設定を行います。

アイデンティティルールにユーザのアクティブ認証が必要な場合、ユーザは接続されているインターフェイスのキャプティブポータルポートにリダイレクトされ、その後、認証を要求されます。

- [サーバ証明書 (Server Certificate)] : アクティブ認証時にユーザに提示する内部証明書を選択します。事前定義された自己署名の DefaultInternalCertificate を選択するか、[新規内部証明書の作成 (Create New Internal Certificate)] をクリックして、ブラウザが信頼している証明書をアップロードできます。

ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

- [ポート (Port)] : キャプティブポータルポート。デフォルトは885 (TCP) です。別のポートを設定する場合は、1025 ~ 65535 の範囲にする必要があります。

例 :

[アイデンティティポリシーの設定 (Identity Policy Configuration) ] ダイアログは、次のようになります。

Identity Policy Configuration

Realm Server

AD

ACTIVE AUTHENTICATION

Server Certificate

DefaultInternalCertificate

Port

885

e.g. 885 or 1025-65535

CANCEL SAVE

- g) [保存 (Save) ] をクリックします。
- 次に、アクティブ認証に必要なルールを作成します。
- h) [アイデンティティルールの作成 (Create Identity Rule) ] ボタンをクリックするか、[+] ボタンをクリックします。
- i) アイデンティティルールのプロパティを入力します。
- 全員を認証する必要があることを前提として、次の設定を使用できます。
- [名前 (Name) ] : 任意の選択 (Require\_Authentication など) 。
  - [ユーザ認証 (User Authentication) ] : [アクティブ (Active) ] が選択されているため、そのままにします。
  - [タイプ (Type) ] : [HTTP ネゴシエート (HTTP Negotiate) ] を選択します。これにより、ブラウザおよびディレクトリサーバは最も強力な認証プロトコルを、NTLM、HTTP ベーシックの順にネゴシエートできます。

(注) HTTP Basic、HTTP 応答ページ、および NTLM 認証方式では、ユーザはインターフェイスの IP アドレスを使用してキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してリダイレクトされます。HTTP ネゴシエートを使用する場合、アクティブ認証を必要としているすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバを更新する必要があります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。DNS サーバを更新できない、または更新を望まない場合は、その他の認証方式のいずれかを選択します。

- [送信元/宛先 (Source/Destination) ]: すべてのフィールドをデフォルトの [すべて (Any) ] のままにします。

より制限されているトラフィックに合わせて、ポリシーに制約を加えることができます。ただし、アクティブ認証は HTTP トラフィックに対してのみ試行されるため、非 HTTP トラフィックが送信元/宛先条件に一致していることは重要ではありません。アイデンティティポリシーのプロパティの詳細については、[アイデンティティルールの設定](#)を参照してください。

Order	Title	User Authentication	Type	Fall Back as Guest
1	Require_Authentication	Active	HTTP Negotiate	<input type="checkbox"/>

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ANY	ANY	ANY	ANY	ANY

- j) [OK] をクリックしてルールを追加します。

ウィンドウの右上を見ると、[展開 (Deploy) ] アイコン ボタンにドットが表示されていることがあります。これは、展開されていない変更があることを示します。ユーザインターフェイスを変更するだけでは、デバイスに変更を設定するには不十分です。変更を展開する必要があります。部分的に設定された変更がデバイスで実行される潜在的な問題を避けるために、一連の関連する変更を加えてから変更を展開できます。この手順で、後から変更を展開します。



**ステップ 2** Inside\_Outside\_Rule アクセス コントロール ルールのアクションを [許可 (Allow) ] に変更します。

Inside\_Outside\_Rule アクセスルールは、信頼できるルールとして作成されます。ただし、信頼できるトラフィックのインスペクションは実行されないため、トラフィック一致基準にアプリ

ケーションやその他の条件（ゾーン、IPアドレス、およびポートを除く）が含まれない場合、システムは信頼できるトラフィックの一部の特性（アプリケーションなど）を学習できません。信頼できるトラフィックではなく許可にルールを変更すると、システムはすべてのトラフィックのインスペクションを実行します。

(注) (ASA 5506-X、ISA 3000)。また、`Inside_Inside_Rule` を [信頼性 (Trust)] から [許可 (Allow)] に変更することも検討してください。このルールは、内部インターフェイス間を移動するトラフィックに対応しています。

- [ポリシー (Policies)] ページの [アクセスコントロール (Access Control)] をクリックします。
- `Inside_Outside_Rule` 行の右側にある [アクション (Actions)] セルにマウスを合わせると、[編集 (edit)] アイコンと [削除 (delete)] アイコンが表示されます。ルールを開くには、[編集 (edit)] アイコン (🔗) をクリックします。
- [アクション (Action)] の [許可 (Allow)] を選択します。

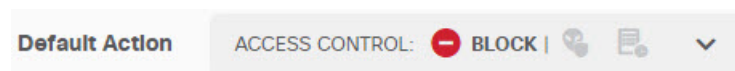
Order	Title	Action
1	<code>Inside_Outside_Rule</code>	🔗 Allow

- [OK] をクリックして変更を保存します。

### ステップ3 アクセスコントロールポリシーのデフォルトアクションでロギングを有効化します。

接続のロギングが有効なアクセスコントロールルールと接続が一致する場合にのみ、ダッシュボードに接続情報が表示されます。`Inside_Outside_Rule` ではロギングが有効ですが、デフォルトアクションのロギングは無効化されています。そのため、ダッシュボードには `Inside_Outside_Rule` の情報のみが表示され、ルールと一致しない接続は反映されません。

- アクセスコントロールポリシー ページの下部のデフォルトアクションで、任意の場所をクリックします。



- [ログアクションの選択 (Select Log Action)] > [接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。
- [OK] をクリックします。

### ステップ4 脆弱性データベース (VDB) の更新スケジュールを設定します。

シスコはVDBの更新を定期的にリリースしています。これには、接続で使用されるアプリケーションを特定できるアプリケーションディテクタが含まれています。定期的にVDBを更新する必要があります。更新を手動でダウンロードするか、または定期的なスケジュールを設定できます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、VDBの更新は無効化されているため、VDBの更新を取得するには操作を実行する必要があります。

- [the name of the device in the menu] をクリックします。[デバイス (Device)]
- [更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックします。

## Updates

[View Configuration](#) >

- c) [VDB] グループで [設定 (Configure)] をクリックします。

VDB 265.0

**Configure**  
Set recurring VDB updates

UPDATE NOW

- d) 更新スケジュールを定義します。

ネットワークを妨害しない時間および頻度を選択します。また、更新をダウンロードすると、システムが自動的に展開することも理解しておいてください。これは、新しいディテクタを有効化するために必要です。そのため、実行して保存したが、展開していない設定変更も展開されます。

たとえば、次のスケジュールでは、VDB が週に 1 回、日曜日の午前 0:00 (24 時間方式を使用) に更新されます。

## Set recurring VDB Update

Frequency

Weekly

Days of Week

Sundays \*

Time

at 00 : 00

(-07:00) America/Los\_Angeles

- e) [保存 (Save)] をクリックします。

### ステップ 5 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックして、展開が完了するまで待ちます。

展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

## Deployment Summary

DEPLOY NOW

You have successfully deployed.

### Deployment History

Modified Objects	Initiated	Completed	Status
> AccessPolicy	11 May 2016	11 May 2016	✔ Deployed
> AccessRule	01:24:35 PM	01:27:06 PM	
> ActiveDirectoryRealm			
> IdentityPolicy			
> IdentityRule			

### 次のタスク

この時点から、監視ダッシュボードおよびイベントにユーザおよびアプリケーションの情報が表示されます。望ましくないパターンがないかこの情報を評価し、許容できない使用を制限するための新しいアクセスルールを展開できます。

侵入およびマルウェアに関する情報の収集を開始する場合、1つまたは複数のアクセスルールで侵入ポリシーとファイルポリシーの有効化が必要です。また、これらの機能のライセンスも有効化する必要があります。

URL カテゴリに関する情報の収集を開始するには、URL フィルタリングを実装する必要があります。

## 脅威をブロックする方法

侵入ポリシーをアクセスコントロールルールに追加することによって、次世代侵入防御システム (IPS) のフィルタリングを実装できます。侵入ポリシーはネットワークトラフィックを分析して、トラフィックの内容を既知の脅威と比較します。接続がモニタリング中の脅威と一致した場合、システムはその接続をドロップして攻撃を阻止します。

その他すべてのトラフィックの処理は、ネットワークトラフィックに侵入の形跡がないかどうかを調べる前に実行されます。侵入ポリシーをアクセスコントロールルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシーを使用してトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可 (allow)] するルールに侵入ポリシーを設定できます。インスペクションは、トラフィックを [信頼 (trust)] または [ブロック (block)] するよう設定されたルールでは実行されません。また、デフォルトアクションが [許可 (allow)] の場合、デフォルトアクションの一部として侵入ポリシーを設定できます。

Firepower システムには複数の侵入ポリシーが付属しています。これらのポリシーは Cisco Talos Intelligence Group (Talos) によって設計されており、侵入ルール、プリプロセッサルール状態、詳細設定が設定されています。

潜在的な侵入を許可するトラフィックの検査に加え、セキュリティインテリジェンスポリシーを使用することで、既知の不正 IP アドレスとのすべてのトラフィック、または既知の不正 URL へのすべてのトラフィックを先制的にブロックできます。

## 手順

**ステップ 1** まだ有効化していない場合は、[脅威 (Threat)] ライセンスを有効化します。

侵入ポリシーおよびセキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device)]
- b) [スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。



- c) [脅威 (Threat)] グループで [有効化 (Enable)] をクリックします。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化 (Disable)] ボタンに変わります。



**ステップ 2** 1 つまたは複数のアクセスルールの侵入ポリシーを選択します。

脅威がないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside\_Outside\_Rule に侵入インスペクションを追加します。ASA 5506-X モデルでは、Inside\_Inside\_Rule に追加することもできます。

- a) メインメニューで [ポリシー (Policies)] をクリックします。

[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。



- b) Inside\_Outside\_Rule 行の右側にある [アクション (Actions)] セルにマウスを合わせると、[編集 (edit)] アイコンと [削除 (delete)] アイコンが表示されます。ルールを開くには、[編集 (edit)] アイコン (🔗) をクリックします。
- c) まだ選択していない場合は、[アクション (Action)] の [許可 (Allow)] を選択します。

Order	Title	Action
1	Inside_Outside_Rule	🔗 Allow

- d) [侵入ポリシー (Intrusion Policy)] タブをクリックします。
- e) [侵入ポリシー (Intrusion Policy)] トグルをクリックしてから、侵入ポリシーを選択します。

ポリシーは、安全性の低いものから高いものへの順で表示されています。[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)] ポリシーは、ほとんどのネットワークに適しています。ドロップしたくないトラフィックをドロップする可能性がある、過度に強力な防御ではなく、侵入に対する適切な防御を実現します。ドロップされるトラフィックが多すぎると判断した場合は、[セキュリティより接続を優先する (Connectivity over Security)] ポリシーを選択することによって侵入インスペクションを緩和できます。

セキュリティを強力にする必要がある場合は、[接続性よりもセキュリティを優先 (Security over Connectivity)] ポリシーを試します。[最大検出 (Maximum Detection)] ポリシーでは、ネットワークインフラストラクチャのセキュリティがよりいっそう重視され、動作にさらに大きな影響を及ぼす可能性があります。

### Edit Access Rule

Order	Title	Action
1	Inside_Outside_Rule	🔗 Allow

Source/Destination   Applications   URLs   Users   **Intrusion Policy**   File

---

**INTRUSION POLICY**

---

LEVEL OF INTRUSION POLICY

Balanced Security and Connectivity

---

**BALANCED SECURITY AND CONNECTIVITY**

This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.

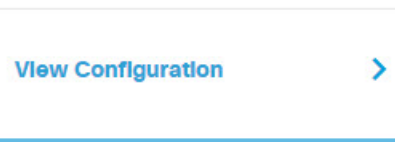
f) [OK] をクリックして変更を保存します。

**ステップ 3** 侵入ルール データベースの更新スケジュールを設定します。

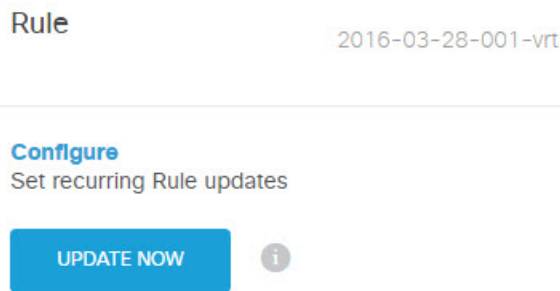
シスコは、接続をドロップするかどうかを決定する侵入ポリシーで使用される、侵入ルール データベースの更新を定期的にリリースしています。ルールデータベースは定期的に更新する必要があります。更新は手動でダウンロードするか、定期的なスケジュールを設定できます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、データベースの更新は無効化されているため、更新されたルールを取得するには操作が必要です。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device) ]
- b) [更新 (Updates) ] グループで [設定の表示 (View Configuration) ] をクリックします。

### Updates



- c) [ルール (Rule) ] グループで [設定 (Configure) ] をクリックします。



- d) 更新スケジュールを定義します。

ネットワークを妨害しない時間および頻度を選択します。また、更新をダウンロードすると、システムが自動的に展開することも理解しておいてください。これは、新しいルールを有効化するために必要です。そのため、実行して保存したが、展開していない設定変更も展開されます。

たとえば、次のスケジュールでは、ルール データベースが週に 1 回、月曜日の午前 0:00 (24 時間方式を使用) に更新されます。

Set recurring Rule Update

Frequency

Weekly

Days of Week

Mondays \*

Time

at 00 : 00

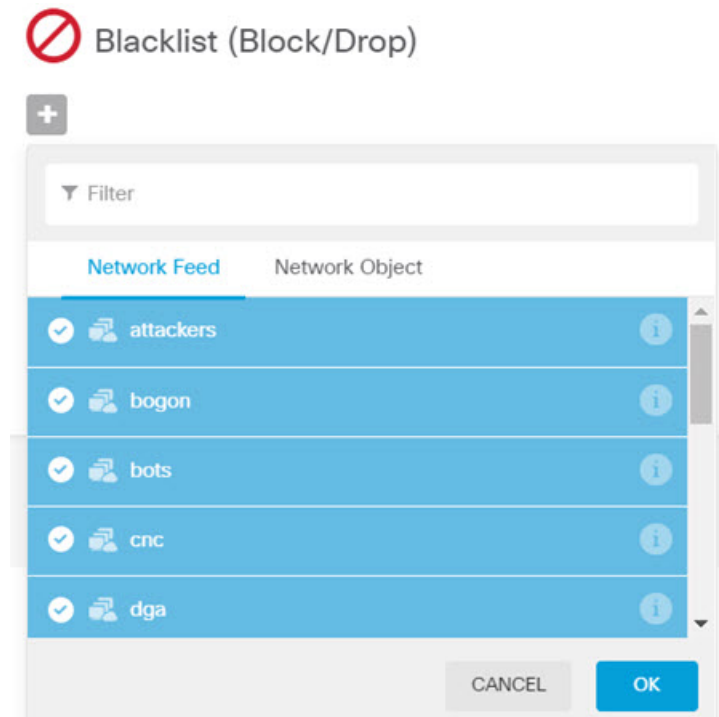
(-07:00) America/Los\_Angeles

e) [保存 (Save) ]をクリックします。

**ステップ 4** 既知の不正ホストやサイトとの接続を先制的にドロップするためのセキュリティインテリジェンス ポリシーを設定します。

セキュリティインテリジェンスを使用して、脅威だとわかっているホストやサイトとの接続をブロックすることで、接続ごとに脅威を特定するためのディープ パケット インスペクションに必要な時間を節約できます。セキュリティインテリジェンスにより、不必要なトラフィックを早期にブロックして、実際に関心があるトラフィックの処理により多くのシステム時間を残すことができます。

- a) [デバイス (Device) ]をクリックし、[更新 (Updates) ]グループで[設定の表示 (View Configuration) ]をクリックします。
- b) [セキュリティインテリジェンスフィード (Security Intelligence Feeds) ]グループで[今すぐ更新 (Update Now) ]をクリックします。
- c) または、[設定 (Configure) ] をクリックして、フィードの定期更新を設定します。デフォルトの[毎時 (Hourly) ]はほとんどのネットワークに適していますが、必要に応じて頻度を減らすことができます。
- d) [ポリシー (Policies) ]をクリックして、[セキュリティインテリジェンス (Security Intelligence) ]ポリシーをクリックします。
- e) ポリシーをまだ有効化していない場合は、[セキュリティインテリジェンスの有効化 (Enable Security Intelligence) ]をクリックします。
- f) [ネットワーク (Network) ]タブで、[ブラックリスト (Blacklist) ]の下にある[+] をクリックして、[ネットワークフィード (Network Feeds) ]タブにあるすべてのフィードを選択します。フィードの横にある[i] ボタンをクリックして、各フィードの説明を確認できます。



フィードが存在しないというメッセージが表示される場合は、後でもう一度試してください。フィードのダウンロードはまだ完了していません。この問題が解決しない場合は、管理 IP アドレスとインターネット間にパスがあることを確認してください。

- g) [OK] をクリックして、選択したフィードを追加します。

他にも不正 IP アドレスがある場合は、[+] > [ネットワークオブジェクト (Network Objects)] をクリックして、それらのアドレスを含むオブジェクトを追加できます。リストの下部にある [新規ネットワークオブジェクトの作成 (Create New Network Object)] をクリックして、すぐに追加することもできます。

- h) [URL] タブをクリックし、[ブラックリスト (Blacklist)] の下にある [+] > [URL フィード (URL Feeds)] をクリックして、すべての URL フィードを選択します。[OK] をクリックして、それらをブラックリストに追加します。

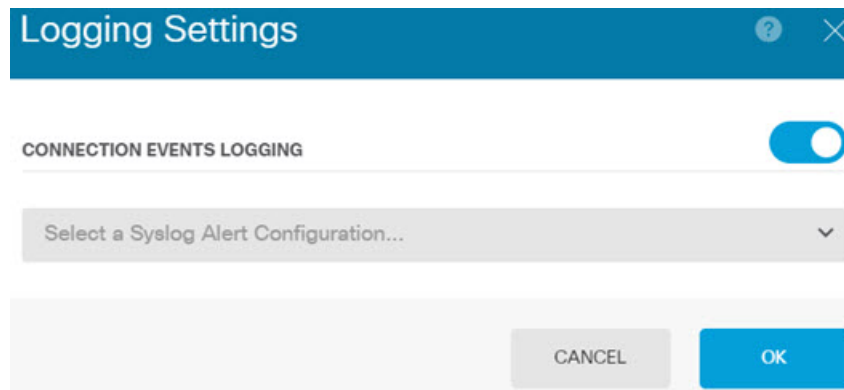
ネットワークリストと同様に、独自の URL オブジェクトをブラックリストに追加して、フィードに含まれていないその他のサイトをブロックできます。[+] > [URL オブジェクト (URL Objects)] をクリックします。リストの最後にある [新規 URL オブジェクトの作成 (Create New URL Object)] をクリックして、新しいオブジェクトを追加できます。

## Blacklist (Block/Drop)



- i) [歯車 (gear) ]アイコンをクリックし、[接続イベントロギング (Connection Events Logging) ]を有効にして、一致した接続のセキュリティインテリジェンスイベントをポリシーが生成できるようにします。[OK] をクリックして変更を保存します。

接続ロギングを有効にしない場合、ポリシーが予想どおりに機能しているかどうかの評価に使用するためのデータを得られません。外部 syslog サーバを定義している場合は、ここで選択することで、そのサーバにもイベントを送信できます。



- j) 必要に応じて、各タブの [ブロックしない (Do Not Block) ] リストにネットワーク オブジェクトまたは URL オブジェクトを追加して、ブラックリストに対する例外を作成できます。

[ブロックしない (Do Not Block) ] リストは、ホワイトリストではなく、例外リストです。例外リストにあるアドレスや URL がブラックリストにも表示されている場合、そのアドレスや URL の接続はアクセスコントロールポリシーの通過を許可されます。フィードはこのようにしてブロックできますが、後で必要なアドレスやサイトがブロックされていることに気付いた場合は、例外リストを使用して、フィードを完全に削除することなく、そのブロックをオーバーライドできます。その後、それらの接続はアクセス制御、および侵入ポリシー (設定されている場合) によって評価される点に注意してください。

したがって、接続に脅威が含まれている場合は、侵入検査中に特定されてブロックされます。

[アクセスおよびSIルール (Access and SI Rules)] ダッシュボード、およびイベントビューアのセキュリティインテリジェンスビューアを使用して、ポリシーによって実際にドロップされているトラフィックを特定し、[ブロックしない (Do Not Block)] リストにアドレスや URL を追加する必要があるかどうかを決めます。

#### ステップ 5 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

#### 次のタスク

この時点から、侵入が特定された場合は、監視ダッシュボードおよびイベントに攻撃者、ターゲット、および脅威に関する情報が表示されます。この情報を評価して、ネットワークにさらにセキュリティ対策が必要かどうか、または使用中の侵入ポリシーのレベルを下げる必要があるかどうかを決定できます。

セキュリティインテリジェンスの場合、[アクセスおよびSIルール (Access and SI Rules)] ダッシュボードでポリシーのヒット数を確認できます。セキュリティインテリジェンス イベントはイベントビューアでも確認できます。セキュリティインテリジェンスのブロック数は侵入の脅威情報には反映されません。これは、検査する前にトラフィックがブロックされるためです。

## マルウェアをブロックする方法

ユーザは、インターネットサイトまたは電子メールなどのその他の通信方法から、悪意のあるソフトウェア (マルウェア) を取得する危険に常にさらされています。信頼できる Web サイトでも、乗っ取られて、無警戒なユーザにマルウェアを配布することがあります。Web ページには、別の送信元からのオブジェクトを含めることができます。このオブジェクトには、イメージ、実行可能ファイル、Javascript、広告などがあります。改ざんされた Web サイトには頻繁に、外部の送信元でホストされているオブジェクトが組み込まれます。真のセキュリティとは、最初の要求だけではなく、各オブジェクトを個別に調べることです。

Firepower の高度なマルウェア防御 (AMP for Firepower) を使用してマルウェアを検出するには、ファイルポリシーを使用します。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

AMP for Firepower は AMP クラウドを使用して、ネットワーク トラフィックで検出された潜在的なマルウェアの性質を取得します。AMP クラウドにアクセスし、マルウェア ルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドに問い合わせます。可能性のある性質は、[クリーン (clean)]、[マルウェア (malware)]、または [不明 (unknown)] (明確な判定を下せない) になります。AMP クラウドに到達できない場合、性質は [不明 (unknown)] になります。

ファイルポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、接続時にファイルのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可 (allow)] するルールにファイル ポリシーを設定できます。インスペクションは、トラフィックを [信頼 (trust)] または [ブロック (block)] するよう設定されたルールでは実行されません。

## 手順

**ステップ 1** まだ有効化していない場合は、[マルウェア (Malware)] ライセンスを有効化します。

マルウェア制御にファイル ポリシーを使用するには、マルウェア ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

- [the name of the device in the menu] をクリックします。[デバイス (Device)]
- [スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。



- [マルウェア (Malware)] グループで [有効化 (Enable)] をクリックします。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化 (Disable)] ボタンに変わります。



**ステップ 2** 1 つまたは複数のアクセス ルールのファイル ポリシーを選択します。

マルウェアがないかスキャンされるトラフィックに対応するルールを決定します。この例では、`Inside_Outside_Rule` にファイルインスペクションを追加します。ASA 5506-X モデルでは、`Inside_Inside_Rule` に追加することもできます。

- a) メインメニューで [ポリシー (Policies)] をクリックします。  
[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。
- b) `Inside_Outside_Rule` 行の右側にある [アクション (Actions)] セルにマウスを合わせると、[編集 (edit)] アイコンと [削除 (delete)] アイコンが表示されます。ルールを開くには、[編集 (edit)] アイコン (🔍) をクリックします。
- c) まだ選択していない場合は、[アクション (Action)] の [許可 (Allow)] を選択します。

Order	Title	Action
1	Inside_Outside_Rule	Allow

- d) [ファイルポリシー (File Policy)] タブをクリックします。
- e) 使用するファイルポリシーをクリックします。

主な選択は、マルウェアと見なされるすべてのファイルをドロップする [マルウェアをすべてブロック (Block Malware All)]、または AMP クラウドにクエリしてファイルの性質を判断するがブロックはしない [クラウドをすべてルックアップ (Cloud Lookup All)] です。ファイルがどのように評価されるかを確認する場合は、クラウドルックアップを使用します。ファイルが評価される方法に納得したら、後でブロッキングポリシーに切り替えることができます。

他にも、マルウェアをブロックするために使用できるポリシーがあります。これらのポリシーは、ファイル制御や Microsoft Office、または Office および PDF ドキュメントのアップロードのブロックと関連しています。つまり、これらのポリシーを使用すると、マルウェアがブロックされるだけでなく、ユーザはこれらのファイルタイプを他のネットワークに送信できなくなります。ニーズに合う場合は、これらのポリシーを選択できます。

この例では、[マルウェアをすべてブロック (Block Malware All)] を選択します。



The screenshot displays the 'Edit Access Rule' interface. At the top, the rule title is 'Inside\_Outside\_Rule' and the action is 'Allow'. Below this, there are tabs for 'Source/Destination', 'Applications', 'URLs', 'Users', 'Intrusion Policy', and 'File policy'. The 'File policy' tab is active, showing a dropdown menu set to 'Block Malware All'. A descriptive text below the dropdown states: 'Query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.'

- f) [ロギング (Logging) ] タブをクリックして、[ファイルイベント (File Events) ] の下にある [ファイルのロギング (Log Files) ] が選択されていることを確認します。

デフォルトでは、ファイルポリシーを選択するとファイルロギングは有効化されます。イベントおよびダッシュボードにファイルおよびマルウェア情報を表示するには、ファイルロギングを有効化が必要です。

#### FILE EVENTS

Log Files

- g) [OK] をクリックして変更を保存します。

### ステップ 3 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes) ] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now) ] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスクステータスが [展開済み (Deployed) ] になります。

### 次のタスク

この時点から、ファイルまたはマルウェアが送信される場合に、監視ダッシュボードおよびイベントにファイルタイプやファイルおよびマルウェアのイベントに関する情報が表示されます。この情報を評価し、ファイルの送信に関してネットワークにさらにセキュリティ対策が必要かどうかを決定できます。

# アクセプタブルユース ポリシー (URL フィルタリング) の実装方法

ネットワークのアクセプタブルユース ポリシーを設定できます。アクセプタブルユース ポリシーは、組織で適切とされるネットワークアクティビティと、不適切とされるアクティビティを区別します。通常、これらのポリシーはインターネットの使用に注目し、生産性の維持、法的責任の回避（敵対的でない作業場所の維持など）、Web トラフィックの制御を目的としています。

URL フィルタリングを使用して、アクセス ポリシーと共にアクセプタブルユース ポリシーを定義できます。広範なカテゴリ（ジャンルなど）でフィルタリングできるため、ブロックする Web サイトを個別に識別する必要はありません。カテゴリの照合では、サイトの関連レピュテーションを指定して、許可またはブロックすることもできます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と出没する可能性があります。

次の手順で、URL フィルタリングを使用してアクセプタブルユース ポリシーを実装する方法について説明します。この例では、複数のカテゴリのあらゆるレピュテーションのサイト、高リスクのソーシャルネットワーキングサイト、および未分類サイトである `badsite.example.com` をブロックします。

## 手順

**ステップ 1** まだ有効化していない場合は、[URL] ライセンスを有効化します。

URL カテゴリとレピュテーションの情報を使用する場合、またはこれらの情報をダッシュボードとイベントに表示する場合には、URL ライセンスを有効にする必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device) ]
- b) [スマートライセンス (Smart License) ] グループの [設定の表示 (View Configuration) ] をクリックします。



- c) [URLライセンス (URL License) ]グループの [有効化 (Enable) ]をクリックします。
- 必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化 (Disable) ] ボタンに変わります。



## ステップ2 URL フィルタリングのアクセス コントロール ルールを作成します。

ブロッキングルールの作成前に、ユーザがアクセスしているサイトのカテゴリを最初に確認できます。その場合、許可するカテゴリ (金融サービスなど) に [許可 (Allow) ] アクションを設定したルールを作成できます。すべての Web 接続のインスペクションを実行して、URL がこのカテゴリに属しているかどうかを判断する必要があるため、金融サービスサービス以外のサイトのカテゴリ情報も取得します。

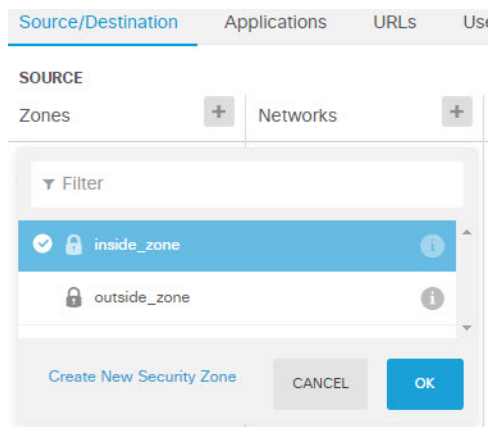
ただし、ブロック対象とすることがすでに判明している URL カテゴリが存在する場合があります。ブロッキングポリシーでもインスペクションが強制されるため、ブロックされるカテゴリだけでなく、ブロックされないカテゴリへの接続に関するカテゴリ情報も取得します。

- a) メインメニューで [ポリシー (Policies) ] をクリックします。
- [アクセスコントロール (Access Control) ] ポリシーが表示されることを確認します。
- b) [+] をクリックして新しいルールを追加します。
- c) 順序、タイトル、およびアクションを設定します。
- [順序 (Order) ] : デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの1つのみです)。このルールでは、デバイスの初期設定時に作成した Inside\_Outside\_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセスコントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。
  - [タイトル (Title) ] : ルールに Block\_Web\_Sites などの意味のある名前を付けます。
  - [アクション (Action) ] : [ブロック (Block) ] を選択します。

Order	Title	Action
1	Block_Web_Sites	Block

- d) [送信元/接続先 (Source/Destination) ] タブで、[送信元 (Source) ] > [ゾーン (Zones) ] の [+] をクリックし、[inside\_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。

条件の追加も同じ方法です。 [+] をクリックすると小さいダイアログボックスが開くため、追加する項目をクリックします。複数の項目をクリックできます。選択した項目をクリックすると選択が解除されます。チェックマークは、選択済みの項目を示します。ただし、 [OK (OK) ] ボタンをクリックするまでポリシーには何も追加されません。項目を選択するだけでは不十分です。

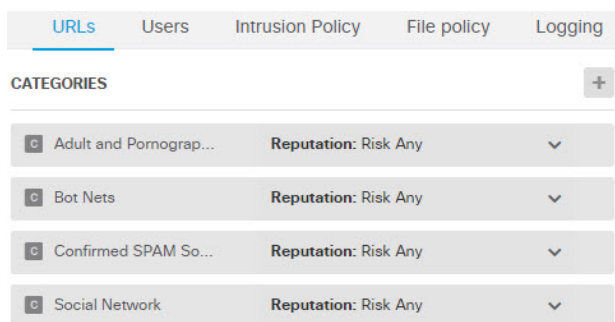


- e) 同じ技術を使用して、[接続先 (Destination) ] > [ゾーン (Zones) ] で [outside\_zone] を選択します。

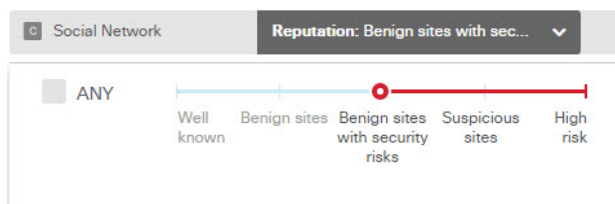
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
<p><b>SOURCE</b></p> <p>Zones <input type="button" value="+"/> Networks <input type="button" value="+"/></p> <p>inside_zone</p>						
					<p><b>DESTINATION</b></p> <p>Zones <input type="button" value="+"/></p> <p>outside_zone</p>	

- f) [URLs] タブをクリックします。
- g) [カテゴリ (Categories) ] の [+] をクリックして、完全または部分的にブロックするカテゴリを選択します。

この例では、[アダルトおよびポルノ (Adult and Pornography) ]、[ボットネット (Bot Nets) ]、[確認済みのスパム送信元 (Confirmed SPAM Sources) ]、および[ソーシャルネットワーク (Social Network) ] を選択します。ブロックすることが必要な可能性が高い追加カテゴリがあります。



- h) レピュテーションに影響されるブロッキングを [ソーシャルネットワーク (Social Network)] カテゴリに実装するには、そのカテゴリの [レピュテーション: すべてのリスク (Reputation: Risk Any)] をクリックして、[すべて (Any)] の選択を解除してからスライダを [セキュリティリスクがある無害なサイト (Benign sites with security risks)] に移動します。閉じるには、スライダをクリックします。



レピュテーションスライダの左側は許可されるサイトを示し、右側はブロックされるサイトを示します。この場合、レピュテーションが [疑わしいサイト (Suspicious Sites)] と [高リスク (High Risk)] の範囲内にあるソーシャル ネットワーキング サイトのみがブロックされます。したがって、ユーザは、リスクの少ない、一般的に使用されるソーシャル ネットワーキング サイトにはアクセスできます。

レピュテーションを使用すると、別の方法で許可したカテゴリ内のサイトを選択的にブロックできます。

- i) カテゴリ リストの左側にある [URLS] リストの横の [+] をクリックします。
- j) ポップアップダイアログボックスの下部で、[新規URLの作成 (Create New URL)] リンクをクリックします。
- k) 名前と URL の両方に「badsite.example.com」と入力して、[追加 (Add)]、[OK] の順にクリックしてオブジェクトを作成します。

オブジェクトに URL と同じ名前を付けるか、またはオブジェクトに別の名前を付けることができます。URL には、URL のプロトコル部分を含めず、サーバ名のみを追加します。

- l) 新規オブジェクトを選択して、[OK] をクリックします。

ポリシーの編集時に新規オブジェクトを追加するだけで、リストにオブジェクトが追加されます。新規オブジェクトは、自動的に選択されません。

Order	Title	Action
1	Block_Web_Sites	Block

Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging				
<table border="1"> <thead> <tr> <th>URLS</th> <th>CATEGORIES</th> </tr> </thead> <tbody> <tr> <td>badsite.example.com</td> <td> <ul style="list-style-type: none"> <li>Adult and Pornograp... Reputation: Risk Any</li> <li>Bot Nets Reputation: Risk Any</li> <li>Confirmed SPAM So... Reputation: Risk Any</li> <li>Social Network Reputation: Benign sites with sec...</li> </ul> </td> </tr> </tbody> </table>							URLS	CATEGORIES	badsite.example.com	<ul style="list-style-type: none"> <li>Adult and Pornograp... Reputation: Risk Any</li> <li>Bot Nets Reputation: Risk Any</li> <li>Confirmed SPAM So... Reputation: Risk Any</li> <li>Social Network Reputation: Benign sites with sec...</li> </ul>
URLS	CATEGORIES									
badsite.example.com	<ul style="list-style-type: none"> <li>Adult and Pornograp... Reputation: Risk Any</li> <li>Bot Nets Reputation: Risk Any</li> <li>Confirmed SPAM So... Reputation: Risk Any</li> <li>Social Network Reputation: Benign sites with sec...</li> </ul>									

- m) [ロギング (Logging) ] タブをクリックして、[ログアクションの選択 (Select Log Action) ] > [接続の開始時と終了時 (At Beginning and End of Connection) ] を選択します。

Web カテゴリ ダッシュボードおよび接続イベントにカテゴリおよびレピュテーションの情報を表示するには、ロギングを有効化する必要があります。

- n) [OK] をクリックしてルールを保存します。

### ステップ 3 (オプション) URL フィルタリングを設定します。

URL ライセンスが有効化されている場合、システムは Web カテゴリ データベースへの更新を自動的に有効化します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。何らかの理由で更新を希望しない場合は、更新をオフにできます。

また、分類されていない URL を分析のためにシスコに送信するよう選択することもできます。したがって、インストールされている URL データベースにはサイトのカテゴリがなく、Cisco CSI にカテゴリが含まれていることがあります。Cisco CSI からカテゴリとレピュテーションが返されると、カテゴリベースのルールを URL 要求に正しく適用できます。メモリ制限により

インストールされる URL データベースが小さいローエンドのシステムでは、このオプションを選択することが重要です。

- a) [the name of the device in the menu] をクリックします。[デバイス (Device) ]
- b) [システム設定 (System Settings) ]>[トラフィック設定 (Traffic Settings) ]>[URLフィルタリングの設定 (URL Filtering Preferences) ] をクリックします。
- c) [未知のURL用Cisco CSIのクエリー (Query Cisco CSI for Unknown URLs) ] を選択します。
- d) [保存 (Save) ] をクリックします。

#### ステップ 4 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes) ] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now) ] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed) ] になります。

#### 次のタスク

この時点で、URL カテゴリとレピュテーション、およびドロップされた接続に関する情報が監視ダッシュボードとイベントに表示され始めます。この情報を評価して、URL フィルタリングによって好ましくないサイトのみがドロップされているかどうか、または特定カテゴリのレピュテーション設定を緩和する必要があるかどうかを判断できます。

分類およびレピュテーションに基づいて Web サイトへのアクセスをブロックすることを、ユーザーに事前に通知することについて検討します。

## アプリケーションの使用を制御する方法

ブラウザ ベースのアプリケーション プラットフォームか、企業ネットワークの内部および外部で転送として Web プロトコルを使用するリッチ メディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになっています。

Firepower Threat Defense では、接続のインスペクションを実行して、使用するアプリケーションを決定します。これにより、特定の TCP/UDP ポートをターゲットにするのではなく、アプリケーションをターゲットとしたアクセスコントロールルールを記述できるようになります。したがって、Web ベース アプリケーションが同じポートを使用していても、それらを選択的にブロックまたは許可できます。

特定のアプリケーションを許可またはブロックするよう選択できますが、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性に基づいてルールを記述することもできます。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロック

する、アクセスコントロールルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとする、セッションがブロックされます。

シスコは、システムおよび脆弱性データベース (VDB) の更新を通じて頻繁にアプリケーションディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

この使用例では、[アノマイザー/プロキシ (anonymizer/proxy)] カテゴリに属するアプリケーションをブロックします。

### 始める前に

この使用例では、使用例 [ネットワークトラフィックを調べる方法 \(6 ページ\)](#) を完了していることを前提としています。その使用例では、[アプリケーション (Applications)] ダッシュボードで分析できる、アプリケーションの使用状況に関する情報を取得する方法について説明しています。実際に使用されているアプリケーションを理解することで、効率的なアプリケーションベースのルールを設計できます。また、その使用例では、VDB の更新をスケジュールする方法についても説明しています (ここでは繰り返しません)。アプリケーションを正しく識別できるように、定期的に VDB を更新してください。

### 手順

#### ステップ 1 アプリケーションベースのアクセスコントロールルールを作成します。

- a) メインメニューで [ポリシー (Policies)] をクリックします。

[アクセスコントロール (Access Control)] ポリシーが表示されることを確認します。

- b) [+] をクリックして新しいルールを追加します。
- c) 順序、タイトル、およびアクションを設定します。

- [順序 (Order)] : デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです)。このルールでは、デバイスの初期設定時に作成した `Inside_Outside_Rule` と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセスコントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。

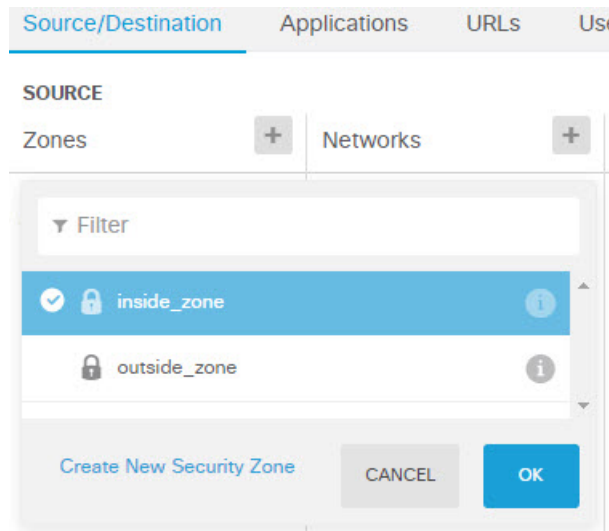
- [タイトル (Title)] : ルールに `Block_Anonymizers` などの意味のある名前を付けます。

- [アクション (Action)] : [ブロック (Block)] を選択します。



Order	Title	Action
1	Block_Anonymizers	Block

- d) [送信元/接続先 (Source/Destination) ] タブで、[送信元 (Source) ]>[ゾーン (Zones) ] の [+] をクリックし、[inside\_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。



- e) 同じ技術を使用して、[接続先 (Destination) ]>[ゾーン (Zones) ] で [outside\_zone] を選択します。

Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
<p><b>SOURCE</b></p> <p>Zones + Networks +</p> <p>inside_zone ANY ANY</p>						<p><b>DESTINATION</b></p> <p>Zones +</p> <p>outside_zone</p>

- f) [アプリケーション (Applications) ] タブをクリックします。  
 g) [アプリケーション (Applications) ] の [+] をクリックして、ポップアップダイアログボックスの下部にある [高度なフィルタ (Advanced Filter) ] リンクをクリックします。

事前にアプリケーションフィルタオブジェクトを作成して、ここの [アプリケーションフィルタ (Application Filters) ] リストで選択できますが、アクセスコントロールルールで条件を直接指定して、オプションで条件をフィルタオブジェクトとして保存することもできます。単一のアプリケーションにルールを記述していない場合は、[高度なフィルタ (Advanced Filter) ] ダイアログボックスを使用して、より簡単にアプリケーションを検索して適切な条件を生成できます。

条件を選択すると、ダイアログボックスの下部にある [アプリケーション (Applications) ] リストが更新され、条件に一致するアプリケーションが表示されます。記述したルールは、これらのアプリケーションに適用されます。

このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、Facebook および TFPT は非常に高リスクに分類されています。ほとんどの組織は、これらのアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストは VDB の更新で変更できることを覚えておいてください。

この例では、[カテゴリ (Categories)] リストから匿名化/プロキシを選択します。

Filter Applications ? RESET FILTER

Risks: Any

Business Relevance: Any

Types: Any

Categories: 1 selected ×

- Search Categories
- anonymizer/proxy
- mobile application
- VoIP
- web services provider
- e-commerce

Tags: Any selected

- Search Tags
- displays ads
- not work related
- high bandwidth
- file sharing/transfer
- share media

---

Filter the list of applications 33 Applications

Application	Description
<input checked="" type="checkbox"/> All applications that match the filters (33)	
<input type="checkbox"/> ASProxy	ASProxy open-source web proxy
<input type="checkbox"/> After School	Anonymous messaging app.
<input type="checkbox"/> Avocent	Registered with IANA on port 1078 tcp/udp.
<input type="checkbox"/> Avoidr	Web based proxy compatible with many popular social networking sites.

- h) [高度なフィルタ (Advanced Filters)] ダイアログボックスで、[追加 (Add)] をクリックします。

フィルタが追加され、[アプリケーション (Applications)] タブに表示されます。

Source/Destination **Applications** URLs Users Intrusion Policy

APPLICATIONS SAVE AS FILTER +

Categories: anonymizer/proxy

- i) [ロギング (Logging)] タブをクリックして、[ログアクションの選択 (Select Log Action)] > [接続の開始時と終了時 (At Beginning and End of Connection)] を選択します。

このルールによってブロックされる接続の情報を取得するには、ロギングを有効化する必要があります。

- j) [OK] をクリックしてルールを保存します。

**ステップ 2** 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now)] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み (Deployed)] になります。

**ステップ 3** [モニタリング (Monitoring)] をクリックして、結果を評価します。

これで、[ネットワークの概要 (Network Overview)] ダッシュボードのアプリケーション ウィジェットにドロップされた接続が表示されます。[すべて (All)]/[拒否 (Denied)]/[許可 (Allowed)] ドロップダウン オプションを使用して、ドロップされたアプリケーションのみに焦点を当てます。

アプリケーションに関する情報は、[Webアプリケーション (Web Applications)] ダッシュボードで検索することもできます。[アプリケーション (Applications)] ダッシュボードにプロトコル関連の結果が表示されます。これらのアプリケーションを使用しようとするユーザがいる場合、アイデンティティポリシーが有効で認証が必要なことを前提として、接続を試行しているユーザとアプリケーションを関連付けることができます。

## サブネットを追加する方法

デバイスに使用可能なインターフェイスがある場合、スイッチ（または別のルータ）に接続して、別のサブネットにサービスを提供できます。

サブネットを追加する潜在的な理由は多数あります。この使用例では、次の一般的なシナリオに対処します。

- サブネットは、プライベート ネットワーク 192.168.2.0/24 を使用する内部ネットワークです。
- ネットワークのインターフェイスには、スタティック アドレス 192.168.2.1 があります。この例では、物理インターフェイスはこのネットワーク専用です。別の方法では、すでに接続されているインターフェイスを使用して、新しいネットワークのサブインターフェイスを作成します。

- デバイスは、DHCPを使用してネットワーク上のワークステーションにアドレスを提供します。アドレスプールとして 192.168.2.2 ~ 192.168.2.254 を使用します。
- 他の内部ネットワークおよび外部ネットワークへのネットワークアクセスは、許可されません。外部ネットワークに移動するトラフィックでは、NAT を使用してパブリックアドレスを取得します。



(注) この例では、ブリッジグループに未使用のインターフェイスは含まれていないことを前提としています。現在、未使用のインターフェイスがブリッジグループメンバーである場合、次の手順に進む前にこれをブリッジグループから削除する必要があります。

#### 始める前に

ネットワークケーブルを新しいサブネットのインターフェイスおよびスイッチに物理的に接続します。

#### 手順

**ステップ1** インターフェイスを設定します。

- a) [デバイス (Device)] をクリックしてから、[インターフェイス (Interface)] サマリーにあるリンクをクリックします。
- b) 接続しているインターフェイスの行の右側にある [アクション (Actions)] セルにマウスを合わせて、[編集 (edit)] アイコン (🔧) をクリックします。
- c) 基本的なインターフェイスのプロパティを設定します。
  - [名前 (Name)] : インターフェイスに固有の名前 ([Inside\_2] など)。
  - [ステータス (Status)] : ステータストグルをクリックして、インターフェイスを有効化します。
  - [IPv4アドレス (IPv4 Address)] タブ : [タイプ (Type)] に [スタティック (Static)] を選択して、[192.168.2.1/24] を入力します。

### Edit Physical Interface

Interface Name:  Status:

Description:

IPv4 Address IPv6 Address Advanced Options

Type:  IP Address and Subnet Mask:  /

- d) [保存 (Save) ] をクリックします。

インターフェイス リストに、更新されたインターフェイス ステータスと設定された IP アドレスが表示されます。

GigabitEthernet1/3	inside_2	<input checked="" type="checkbox"/>	192.168.2.1	STATIC
--------------------	----------	-------------------------------------	-------------	--------

## ステップ 2 インターフェイスの DHCP サーバを設定します。

- [the name of the device in the menu] をクリックします。[デバイス (Device) ]
- [システム設定 (System Settings) ] > [DHCPサーバ (DHCP Server) ] をクリックします。
- [DHCPサーバ (DHCP Servers) ] タブをクリックします。

表に、既存の DHCP サーバが表示されます。デフォルト設定を使用している場合、リストには内部インターフェイスのいずれかが含まれます。

- 表の上部の [+] をクリックします。
- サーバのプロパティを設定します。
  - [DHCPサーバの有効化 (Enable DHCP Server) ] : このトグルをクリックして、サーバを有効化します。
  - [インターフェイス (Interface) ] : DHCP サービスを提供しているインターフェイスを選択します。この例では、inside\_2 を選択します。
  - [アドレスプール (Address Pool) ] : サーバがネットワーク上のデバイスに供給できるアドレス。192.168.2.2 ~ 192.168.2.254 を入力します。ネットワークアドレス (.0) 、インターフェイスアドレス (.1) 、またはブロードキャストアドレス (.255) が含まれないようにしてください。また、ネットワーク上のデバイスにスタティックアドレスが必要な場合は、プールからそれらのアドレスを除外します。プールは単一の連続したアドレスである必要があるため、範囲の最初または最後からスタティックアドレスを選択します。

**Add Server**

Enabled DHCP Server

Interface

inside\_2

Address Pool

192.168.2.2-192.168.2.254

*e.g. 192.168.45.46-192.168.45.254*

- f) [追加 (Add)] をクリックします。

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

### ステップ3 内部セキュリティゾーンにインターフェイスを追加します。

インターフェイスにポリシーを記述するには、インターフェイスはセキュリティゾーンに属している必要があります。セキュリティゾーンのポリシーを記述します。そのため、ゾーンでインターフェイスを追加および削除すると、インターフェイスに適用されたポリシーは自動的に変更されます。

- メインメニューで[オブジェクト (Objects)] をクリックします。
- オブジェクトの目次から、[セキュリティゾーン (Security Zones)] を選択します。
- [inside\_zone] オブジェクトの行の右側にある[アクション (Actions)] セルにマウスを合わせて、[編集 (edit)] アイコン (🔗) をクリックします。
- [インターフェイス (Interfaces)] の下にある[+] をクリックして、inside\_2 インターフェイスを選択し、インターフェイスリストで[OK] をクリックします。

Interfaces

+

🔗 inside

🔗 inside\_2

- e) [保存 (Save)] をクリックします。

Security Zones		
2 objects		
#	NAME	INTERFACES
1	inside_zone	inside, inside_2
2	outside_zone	outside

**ステップ 4** 内部ネットワーク間のトラフィックを許可するアクセス コントロール ルールを作成します。

トラフィックは、すべてのインターフェイス間で自動的に許可されません。希望のトラフィックを許可するには、アクセスコントロールルールを作成する必要があります。唯一の例外は、アクセスコントロールルールのデフォルトアクションでトラフィックを許可している場合です。この例では、デバイスのセットアップウィザードで設定したブロックのデフォルトアクションを保持していることを前提としています。したがって、内部インターフェイス間のトラフィックを許可するルールを作成する必要があります。このようなルールをすでに作成している場合は、この手順をスキップします。

a) メインメニューで [ポリシー (Policies) ] をクリックします。

[アクセスコントロール (Access Control) ] ポリシーが表示されることを確認します。

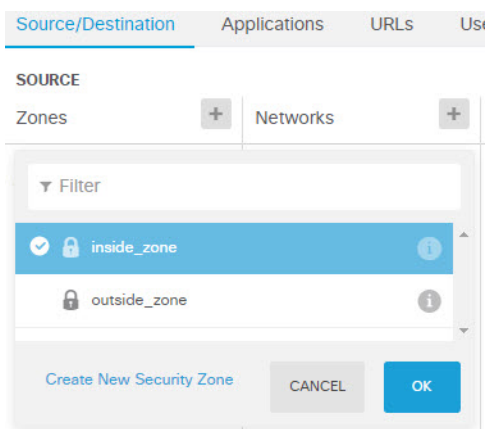
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

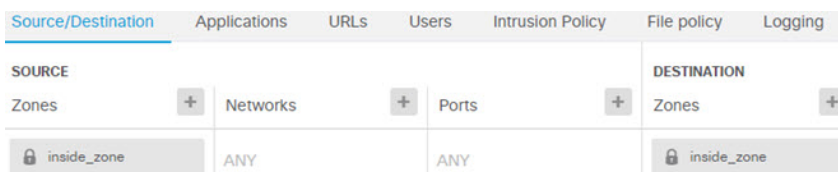
- [順序 (Order) ] : デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前 (上位) にこのルールを配置する必要があります。そうしなければ、ルールは照合されません (接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです)。このルールでは、一意の送信元/宛先条件を使用するため、リストの最後にルールを追加できます。
- [タイトル (Title) ] : ルールに Allow\_Inside\_Inside などの意味のある名前を付けます。
- [アクション (Action) ] : [許可 (Allow) ] を選択します。

Order	Title	Action
4	Allow_Inside_Inside	Allow

d) [送信元/宛先 (Source/Destination) ] タブで、[送信元 (Source) ] > [ゾーン (Zones) ] の [+] をクリックし、[inside\_zone] を選択してからゾーンのダイアログボックスで [OK] をクリックします。



- e) 同じ方法で、**[宛先 (Destination)]** > **[Zones (ゾーン)]** の **[inside\_zone]** を選択します。  
送信元および宛先に同じゾーンを選択するには、セキュリティゾーンに2つ以上のインターフェイスが含まれている必要があります。



- f) (オプション) 侵入およびマルウェアのインスペクションを設定します。  
内部インターフェイスは信頼できるゾーン内にありますが、一般的に、ユーザはラップトップをネットワークに接続します。そのため、ユーザは、外部ネットワークまたは Wi-Fi ホットスポットからネットワーク内に、知らないうちに脅威を持ち込んでいます。したがって、内部ネットワーク間を移動するトラフィックに侵入やマルウェアの形跡がないかスキャンが必要な場合があります。  
次の操作の実行を検討します。
- **[侵入ポリシー (Intrusion Policy)]** タブをクリックして侵入ポリシーを有効化し、スライダを使用して **[バランスのとれたセキュリティと接続性 (Balanced Security and Connectivity)]** ポリシーを選択します。
  - **[ファイルポリシー (File Policy)]** タブをクリックして、**[すべてのマルウェアをブロックする (Block Malware All)]** ポリシーを選択します。
- g) **[ロギング (Logging)]** タブをクリックして、**[ログアクションの選択 (Select Log Action)]** > **[接続の開始時および終了時 (At Beginning and End of Connection)]** を選択します。  
このルールに一致する接続に関する情報を取得するには、ロギングを有効化する必要があります。ロギングによってダッシュボードにスタティックが追加され、イベントビューアにイベントが表示されます。
- h) **[OK]** をクリックしてルールを保存します。

**ステップ 5** 新規サブネットに必要なポリシーが定義されていることを確認します。



inside\_zone セキュリティゾーンにインターフェイスを追加することによって、inside\_zone の既存のポリシーが自動的に新規サブネットに適用されます。ただし、ポリシーのインスペクションには時間がかかるため、ポリシーの追加が必要ないことを確認します。

デバイスの初期設定を完了すると、次のポリシーがすでに適用されています。

- [アクセスコントロール (Access Control) ] : Inside\_Outside\_Rule は、新規サブネットと外部ネットワーク間のすべてのトラフィックを許可します。以前の使用例に従っている場合、ポリシーによって侵入およびマルウェアのインスペクションも提供されます。新規ネットワークと外部ネットワークの間の一部のトラフィックを許可するルールが必要です。このルールがなければ、ユーザはインターネットや他の外部ネットワークにアクセスできません。
- [NAT] : InsideOutsideNATrule は、外部インターフェイスに対するすべてのインターフェイスに適用され、インターフェイス PAT が適用されます。このルールを守っている場合、新規ネットワークから外部に移動するトラフィックの IP アドレスは、外部インターフェイスの IP アドレスの一意のポートに変換されます。すべてのインターフェイスまたは inside\_zone インターフェイスに適用されるルールがない場合、外部インターフェイスに移動するときに新しいルールの作成が必要になる場合があります。
- [アイデンティティ (Identity) ] : デフォルトのアイデンティティポリシーはありません。ただし、以前の使用例に従っている場合、新規ネットワークの認証に必要なアイデンティティポリシーがある可能性があります。適用されるアイデンティティポリシーがなく、新規ネットワークのユーザベース情報が必要な場合は、新しいポリシーを作成します。

#### ステップ 6 変更を保存します。

- a) Web ページの右上にある [変更の展開 (Deploy Changes) ] アイコンをクリックします。



- b) [今すぐ展開 (Deploy Now) ] ボタンをクリックします。

展開が完了するまで待機します。展開のサマリーに変更が正常に展開されたことが示され、ジョブのタスクステータスが [展開済み (Deployed) ] になります。

---

#### 次のタスク

新規サブネットのワークステーションが DHCP を使用して IP アドレスを取得していることと、そのワークステーションが他の内部ネットワークおよび外部ネットワークに到達できることを確認します。監視ダッシュボードおよびイベントビューアを使用して、ネットワークの使用状況を評価します。

## その他の例

使用例の章の例に加えて、特定のサービスについて説明している一部の章で設定例が示されています。場合によっては次の例が役立つ可能性があります。

### Network Address Translation (NAT)

#### IPv4 アドレス用の NAT

- 内部 Web サーバへのアクセスの提供 (スタティック自動 NAT)
- FTP、HTTP、および SMTP の単一アドレス (ポート変換を設定したスタティック自動 NAT)
- 宛先に応じて異なる変換 (ダイナミック手動 PAT)
- 宛先アドレスおよびポートに応じて異なる変換 (ダイナミック手動 PAT)
- DNS 応答修正：外部の DNS サーバ
- DNS 応答修正：ホスト ネットワーク上の DNS サーバ
- NAT からのサイト間 VPN トラフィックの除外

#### IPv6 アドレス用の NAT

- NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット
- NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク
- NAT66 の例：ネットワーク間のスタティック変換
- NAT66 の例：シンプルな IPv6 インターフェイス PAT
- DNS 64 応答修正

#### リモート アクセス仮想プライベート ネットワーク (RA VPN)

- 外部インターフェイスでリモート アクセス VPN ユーザにインターネットアクセスを提供する方法 (ヘア ピニング)
- リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバを使用する方法

#### サイト間仮想プライベート ネットワーク (VPN)

- NAT からのサイト間 VPN トラフィックの除外
- 外部インターフェイスで外部のサイト間 VPN ユーザにインターネットアクセスを提供する方法 (ヘア ピニング)

### SSL/TLS の復号

- 例：ネットワークからの古い SSL/TLS バージョンのブロック

### FlexConfig ポリシー（FlexConfig Policy）

- グローバル デフォルト インспекションを有効/無効にする方法
- FlexConfig の変更を元に戻す方法
- 一意のトラフィック クラスのインспекションを有効にする方法

