ベストプラクティス：Threat Defense の使用例

ここでは、Device Manager を使用して 脅威に対する防御 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。

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。

- 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。
- （Firepower 4100/9300）事前に設定されたデータインターフェイスはありません。
- （ISA 3000）ブリッジグループには 2 つの内部インターフェイスと 2 つの外部インターフェイスが含まれています。セットアップを完了するには、BVI1 の IP アドレスを手動で設定する必要があります。
- （Firepower 4100/9300 を除く）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。

- （Firepower 4100/9300 を除く）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。 ISA 3000 の場合、内部から外部、および外部から内部へのすべてのトラフィックを許可するアクセスルールがあります。
- （Firepower 4100/9300 および ISA 3000 を除く）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 アドレスの固有ポートに変換するインターフェイス NAT ルール。
- （Firepower 4100/9300 および ISA 3000 を除く）内部インターフェイスで実行されている DHCP サーバー。

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、[スマートラインセンス（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ライセンス（IPS 、マルウェア防御、URL）ごとに [有効化（Enable）] をクリックします。セットアップ中にデバイスを登録した場合は、必要な RA VPN ライセンスも有効にできます。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。**[Register Device]** 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。

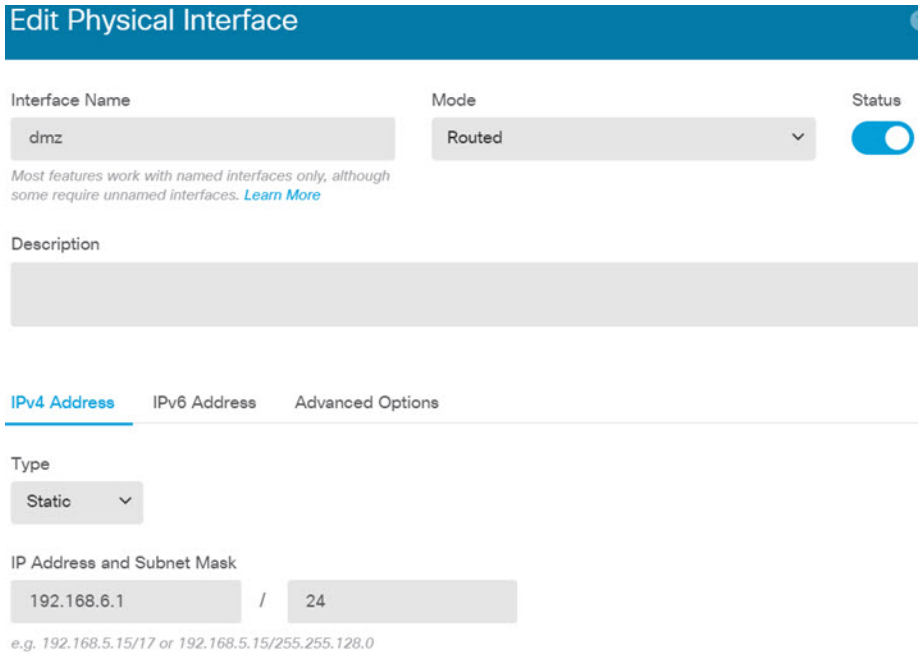
ステップ 2 他のインターフェイスに接続している場合は、[デバイス（Device）] を選択し、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックしてから、インターフェイスのタイプをクリックして、インターフェイスのリストを表示します。

- Firepower 4100/9300 では、名前、IP アドレス、またはセキュリティゾーンを使用して事前に設定されているデータインターフェイスがないため、使用するインターフェイスを有効にして設定する必要があります。
- ISA 3000 は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。ただし、BVI の IP アドレスを手動で設定する必要があります。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。
- Firepower 1010 の場合、Ethernet1/1（外部）以外のインターフェイスはすべて、VLAN1（内部）に割り当てられたアクセスモードのスイッチポートです。スイッチポートをファイアウォールポートに変更することができます。それには、新しい VLAN インターフェイスを追加してスイッチポートを割り当てます。または、トランクモードのスイッチポートを設定します。

各インターフェイスの[編集（Edit）]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。

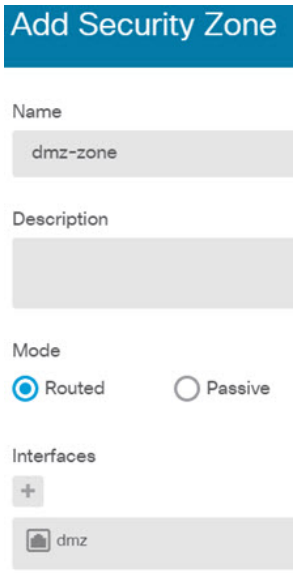
次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。完了したら[保存（Save）]をクリックします。



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には常にゾーン 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。

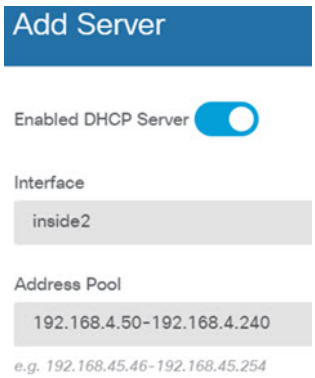


ステップ 4 内部クライアントがDHCPを使用してデバイスからIPアドレスを取得するようにする場合は、[デバイス（Device）] を選択し、次に **[システム設定（System Settings）]** > **[DHCPサーバー（DHCP Server）]** を選択します。[DHCPサーバー（DHCP Servers）] タブを選択します。

すでに内部インターフェイス用に構成されているDHCPサーバーがありますが、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サーバー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ー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 サーバー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）]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。

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。

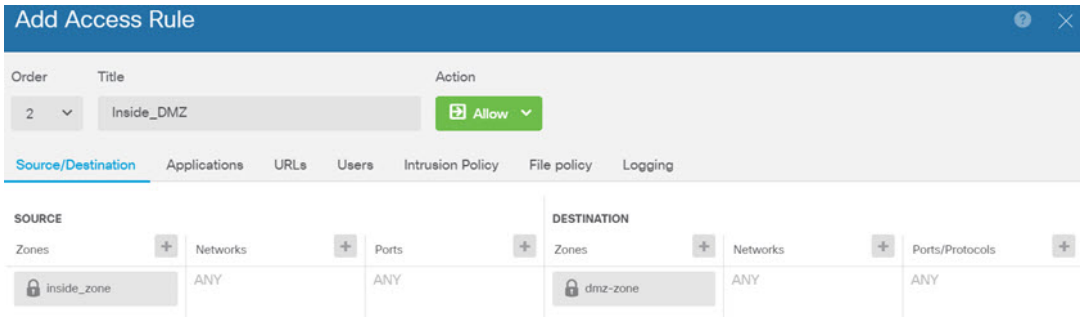
さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

- [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）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー 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ー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）]：セキュリティ インテリジェンス ポリシーを使用して、選択されている IP アドレスまたは URL との接続をすぐにドロップします。既知の不正なサイトをブロックすれば、アクセス制御ポリシーでそれらを考慮する必要がなくなります。シスコでは、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、ユーザーまたはユーザー 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 ゾーンの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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

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。以下の質問の回答には Device Manager のレポートが役立ちます。

- 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 脅威に対する防御 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、許容するカテゴリ（金融など）へのアクセスを許可する新規のアクセスコントロールルールを追加して、アクセス コントロール 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 （25 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。

この例では、ユーザアイデンティティを取得するためにアクティブ認証を実装します。アクティブ認証を使用すると、デバイスからユーザ名とパスワードを求められます。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。アクティブ認証を使用している場合、アイデンティティポリシーは Active Directory 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 アドレスをユーザに関連付けます。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。

c) [アイデンティティルールの作成（Create Identity Rule）] ボタンまたは [+] ボタンをクリックして、アクティブ認証を義務付けるルールを作成します。

この例では、すべての人に認証を義務付けていると仮定しています。

d) ルールの [名前（Name）] を入力します。Require_Authentication など、任意の名前を選択できます。

e) [送信元または宛先（Source/Destination）] タブをデフォルトのままにします。これは、[任意（Any）] 基準に適用されます。

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、を参照してください。アイデンティティ ルールの設定

f) [アクション（Action）] で [アクティブ認証（Active Auth）] を選択します。

いくつか未定義の設定があるため、アイデンティティポリシーの設定が行われていないと仮定して、[アイデンティティポリシー設定（Identity Policy Configuration）] ダイアログボックスが開きます。

g) アクティブ認証に必要な [キャプティブ ポータル（Captive Portal）] の設定と [SSL復号（SSL Decryption）] の設定を行います。

アイデンティティルールによりユーザーのアクティブ認証が要求されると、そのユーザーはキャプティブポータルポートにリダイレクトされ、認証を求められます。キャプティブポータルにはSSL復号化ルールが必要です。このルールは、システムによって自動的に生成されますが、SSL 復号化ルールに使用する証明書は選択する必要があります。

- [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。

- [ホスト名にリダイレクト（Redirect to Host Name）]：アクティブな認証要求のキャプティブポータルとして使用するインターフェイスの完全修飾ホスト名を定義するネットワークオブジェクトを選択します。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。

  FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。

  アイデンティティルールによりユーザーのアクティブ認証が要求されているが、リダイレクト FQDN を指定していない場合、ユーザーは、接続されているインターフェイス上のキャプティブポータルポートにリダイレクトされます。

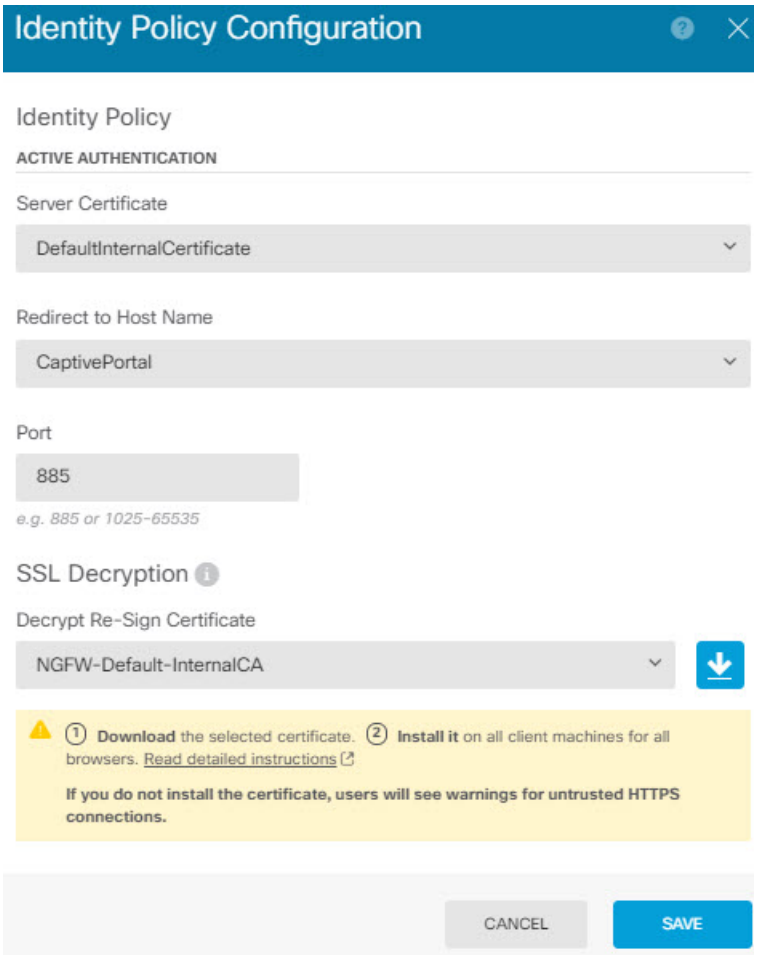
- [ポート（Port）]：キャプティブ ポータル ポート。デフォルトは、885（TCP）です。別のポートを設定する場合は、1025 ～ 65535 の範囲にする必要があります。

- [再署名証明書の復号（Decrypt Re-Sign Certificate）]：再署名証明書での復号を実装するルールに使用する内部 CA 証明書を選択します。事前定義済みの NGFW-Default-InternalCA 証明書（デフォルト）か、作成またはアップロードした証明書を使用できます。証明書がまだ存在しない場合は、[Create Internal CA] をクリックして作成します。SSL 復号化ポリシーをまだ有効にしていない場合にのみ、復号化再署名証明書の入力が求められます。

  クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（  ）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロードも参照してください。

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。



h) [保存（Save）] をクリックしてアクティブ認証の設定を保存します。

[アクティブ認証（Active Authentication）] タブが [アクション（Action）] 設定の下に表示されます。

i) [アクティブ認証（Active Authentication）] タブで、[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） [ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザーが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。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用する場合は、アクティブ認証が必要な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 サーバーを更新する必要もあります。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。認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。 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。

j) [ADアイデンティティソース（AD Identity Source）] で [新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。

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。

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、昇格されたユーザ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 などの完全修飾名である必要があります（Administrator だけでなく）。

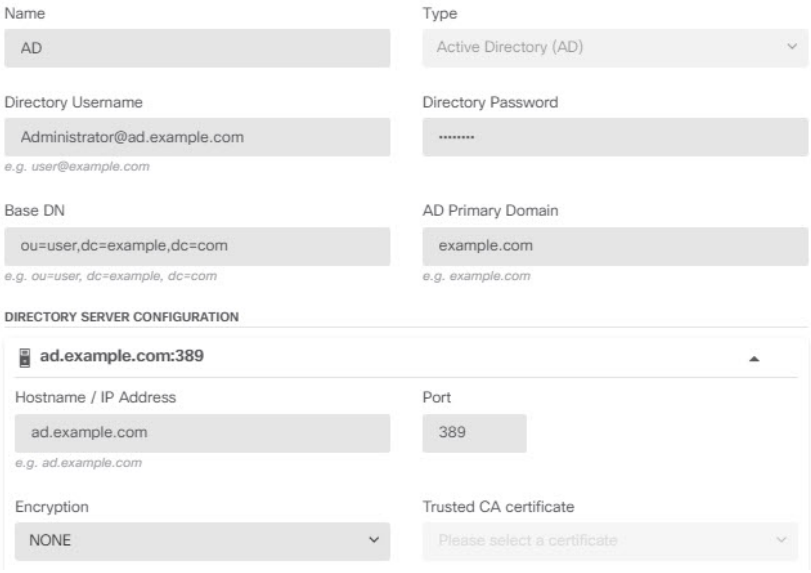
  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=adminisntrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [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。例、example.com。

- [ホスト名または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。サーバに対して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 サーバ間の信頼できる接続を有効にします。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。

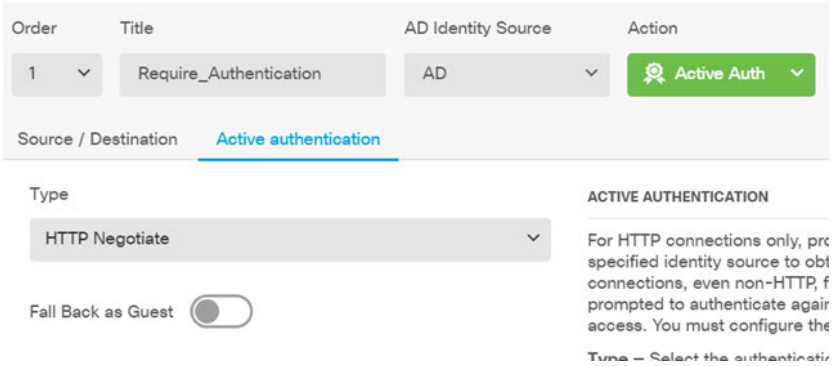
例：

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。



k) [ADアイデンティティソース（AD Identity Source）] で、作成したオブジェクトを選択します。

ルールは次のようになります。



l) [OK] をクリックしてルールを追加します。

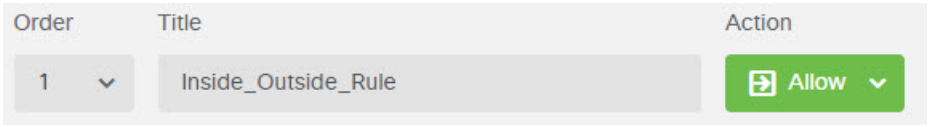
ウィンドウの右上を見ると、[展開（Deploy）] アイコン ボタンにドットが表示されていることがあります。これは、展開されていない変更があることを示します。ユーザインターフェイスを変更するだけでは、デバイスに変更を設定するには不十分です。変更を展開する必要があります。部分的に設定された変更がデバイスで実行される潜在的な問題を避けるために、一連の関連する変更を加えてから変更を展開できます。この手順で、後から変更を展開します。

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）　（ISA 3000）。また、Outside_Inside_Rule、Inside_Inside_Rule および Outside_Outside_Rule を [Trust] から [Allow] に変更することも検討してください。

a) [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。
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) [アクション（Action）] の [許可（Allow）] を選択します。

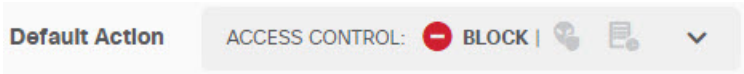


d) [OK] をクリックして変更を保存します。

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。

a) 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。

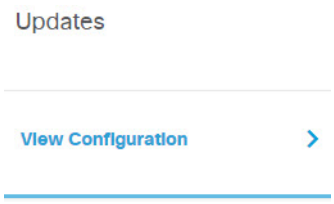


b) **[ログアクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）]** を選択します。
c) [OK] をクリックします。

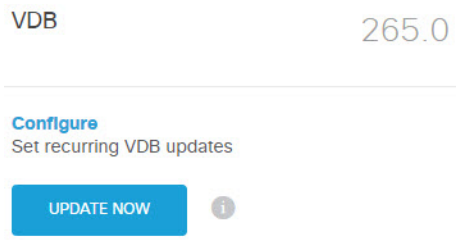
ステップ 4 脆弱性データベース（VDB）の更新スケジュールを設定します。

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。

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。



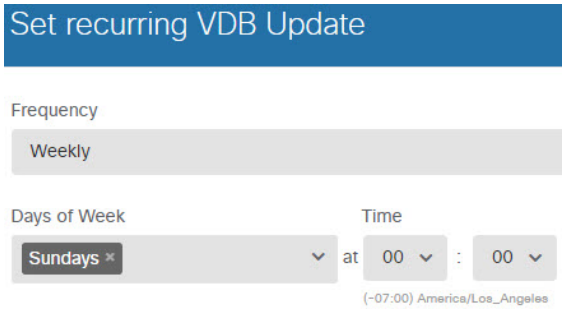
c) [VDB] グループで [設定（Configure）] をクリックします。



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。



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ます。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

侵入ポリシーは 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。Snort 3 をインスペクションエンジンとして使用している場合は、Talos ポリシーに基づき、独自のカスタムポリシーを作成できます。

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、IPS ライセンスを有効化します。

侵入ポリシーとセキュリティインテリジェンスを使用するには、IPS 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) **IPS** 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。

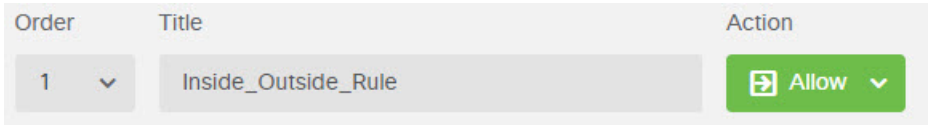
ステップ 2 1 つまたは複数のアクセス ルールの侵入ポリシーを選択します。

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。

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。

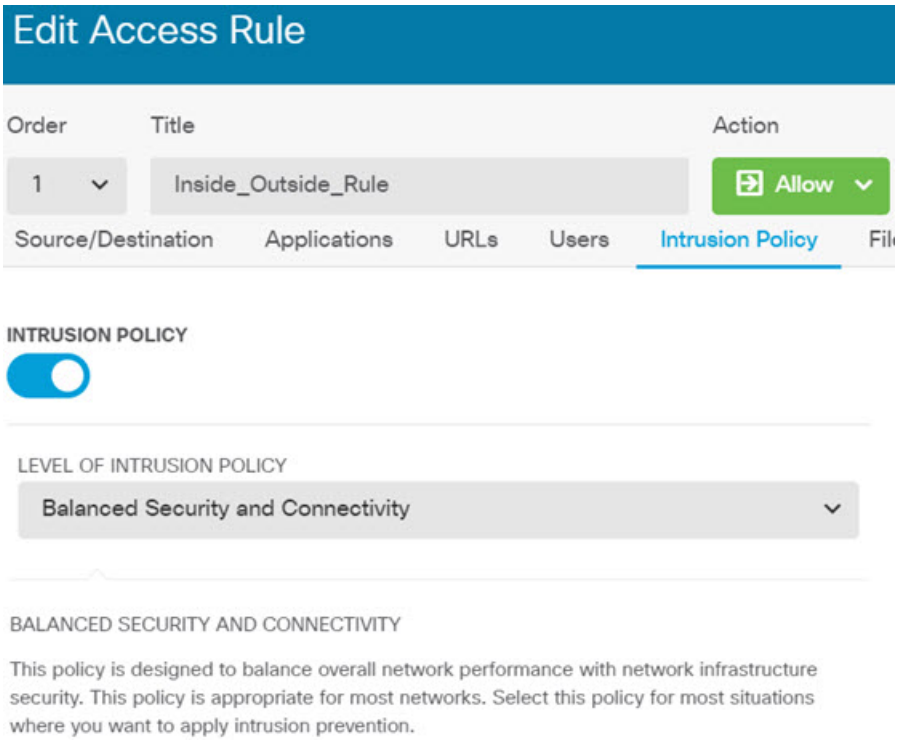


d) [侵入ポリシー（Intrusion Policy）] タブをクリックします。
e) [侵入ポリシー（Intrusion Policy）] トグルをクリックしてから、侵入ポリシーを選択します。

[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。



f) [OK] をクリックして変更を保存します。

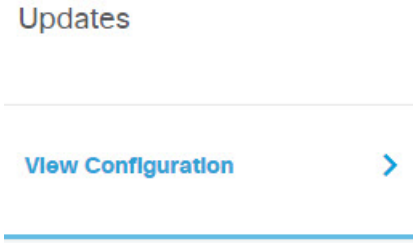
ステップ 3 （任意）**[ポリシー（Policies）]**>**[侵入（Intrusion）]**に移動し、歯車アイコンをクリックして、侵入ポリシーの syslog サーバを設定します。

侵入イベントは、アクセスコントロールルール用に設定されたsyslogサーバを使用しません。

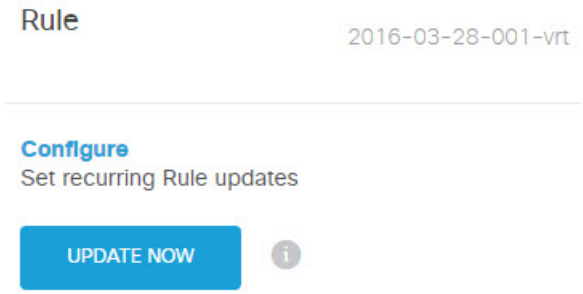
ステップ 4 侵入ルール データベースの更新スケジュールを設定します。

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、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。



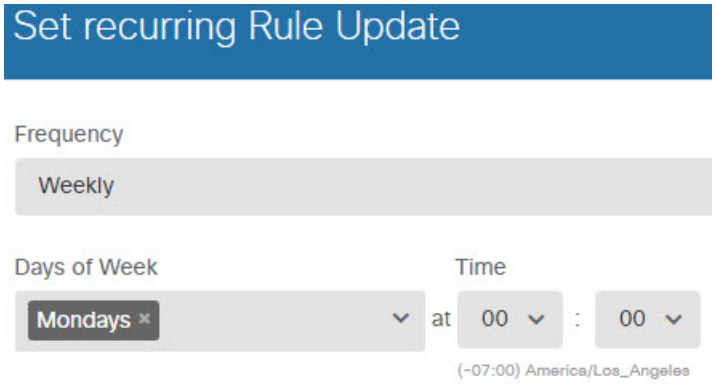
c) [ルール（Rule）] グループで [設定（Configure）] をクリックします。



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。



e) [Save] をクリックします。

ステップ 5 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/ドロップリストの [+] 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。

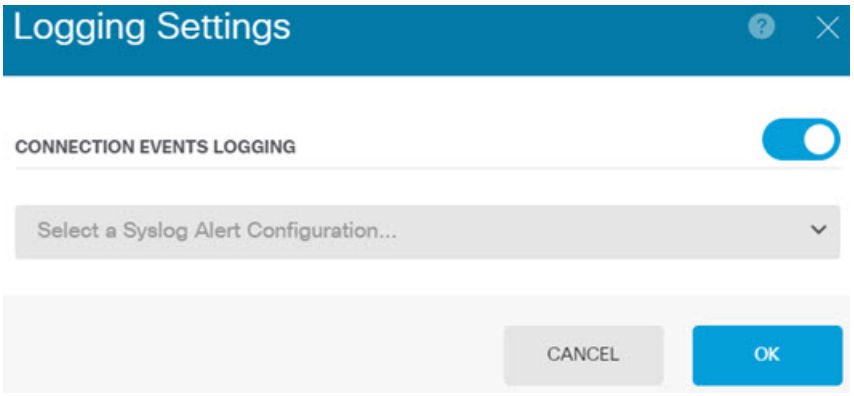
   他にも不正 IP アドレスがある場合は、**[+] > [ネットワークオブジェクト（Network Objects）]** をクリックして、それらのアドレスを含むオブジェクトを追加できます。リストの下部にある [新規ネットワークオブジェクトの作成（Create New Network Object）] をクリックして、すぐに追加することもできます。

h) [URL] タブをクリックし、ブラック/ドロップリストの **[+] > [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、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。

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、ブロ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がブロ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 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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

マルウェア防御を使用してマルウェアを検出するために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。

マルウェア防御は Secure Malware Analytics Cloud 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。Secure Malware Analytics Cloud 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 Secure Malware Analytics Cloud 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。 Secure Malware Analytics Cloud 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、マルウェア防御 および IPS ライセンスを有効化します。

ファイルポリシーを使用するには、侵入ポリシーに必要なIPS ライセンスに加えて、マルウェア防御 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、それらの

評価ライセンスを有効にします。デバイスを登録している場合は、必要なライセンスを購入して、それらを 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) **マルウェア防御** グループで [有効化（Enable）] をクリックし、**IPS** グループでも [有効化（Enable）] をクリックします（まだ有効化されていない場合）。

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。

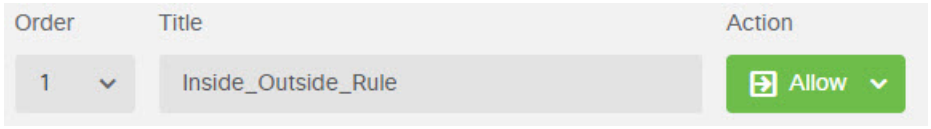
ステップ 2 1 つまたは複数のアクセス ルールのファイル ポリシーを選択します。

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。

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。

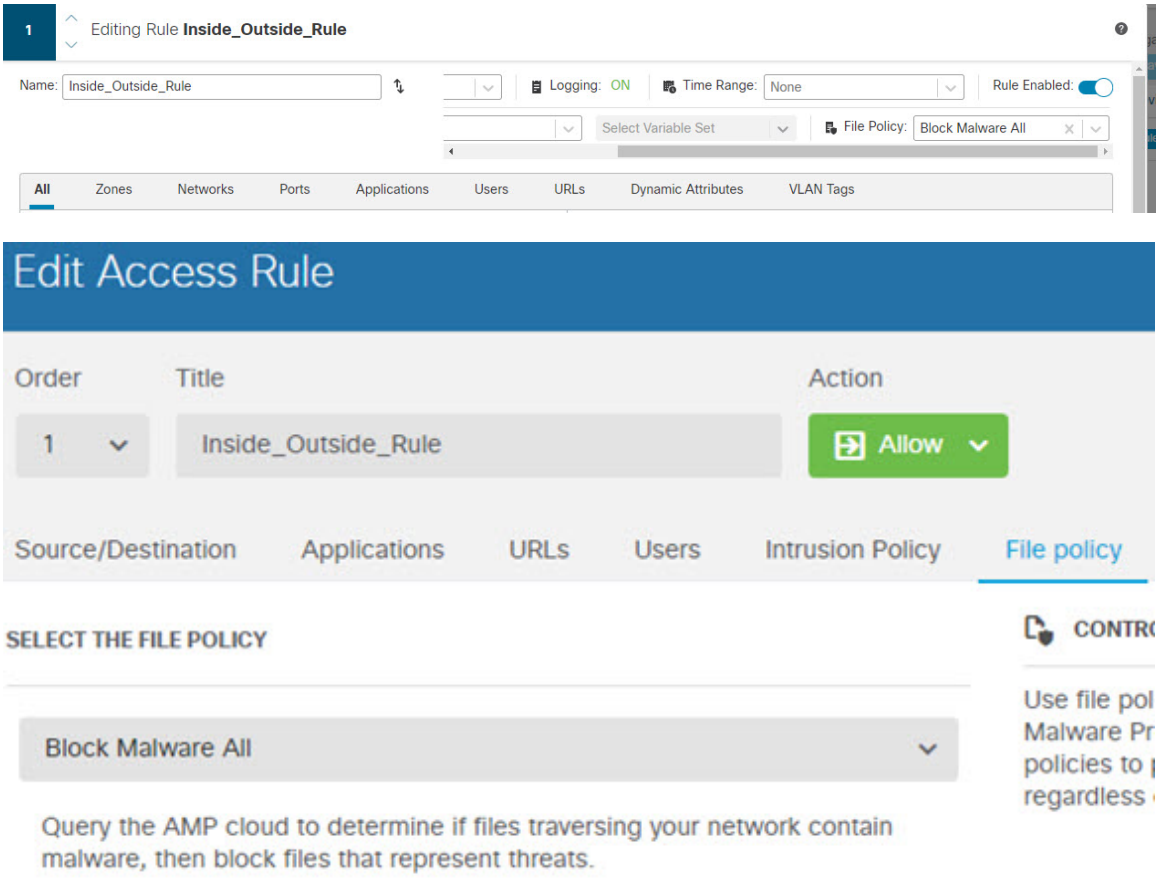


d) [ファイルポリシー（File Policy）] タブをクリックします。
e) 使用するファイル ポリシーをクリックします。

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 Secure Malware Analytics Cloud 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。

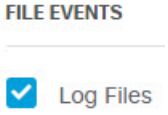
他にも、マルウェアをブロックするために使用できるポリシーがあります。これらのポリシーは、ファイル制御やMicrosoft Office、またはOfficeおよびPDFドキュメントのアップロードのブロックと関連しています。つまり、これらのポリシーを使用すると、マルウェアがブロックされるだけでなく、ユーザはこれらのファイルタイプを他のネットワークに送信できなくなります。ニーズに合う場合は、これらのポリシーを選択できます。

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。



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。



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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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（ギャンブルなど）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]** 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（金融など）に [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。

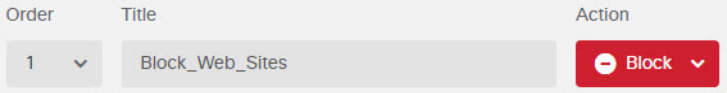
[アクセスコントロール（Access Control）] ポリシーが表示されることを確認します。

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

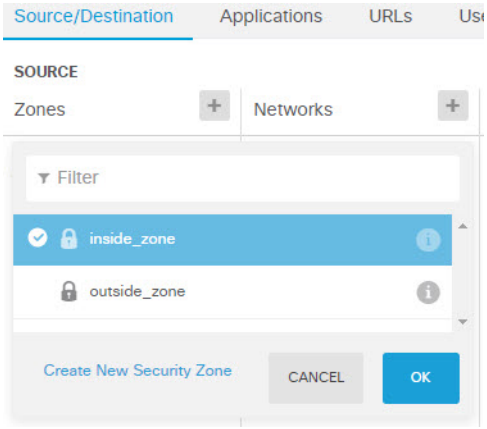
の 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセス コントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。

- [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。

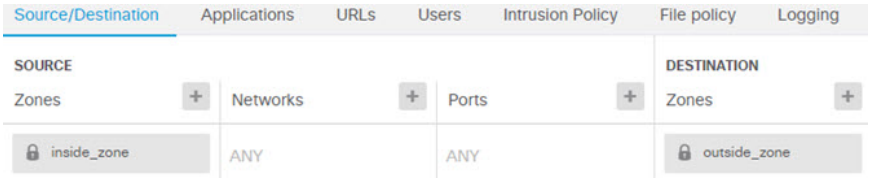


d) [送信元/接続先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。

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。



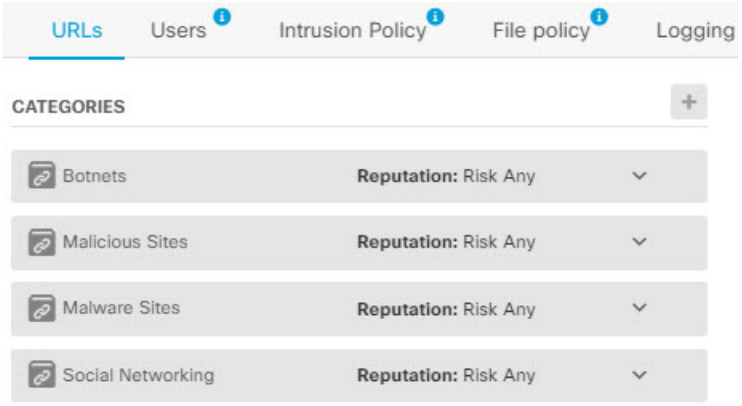
e) 同じ技術を使用して、**[接続先（Destination）]** > **[ゾーン（Zones）]** で [outside_zone] を選択します。



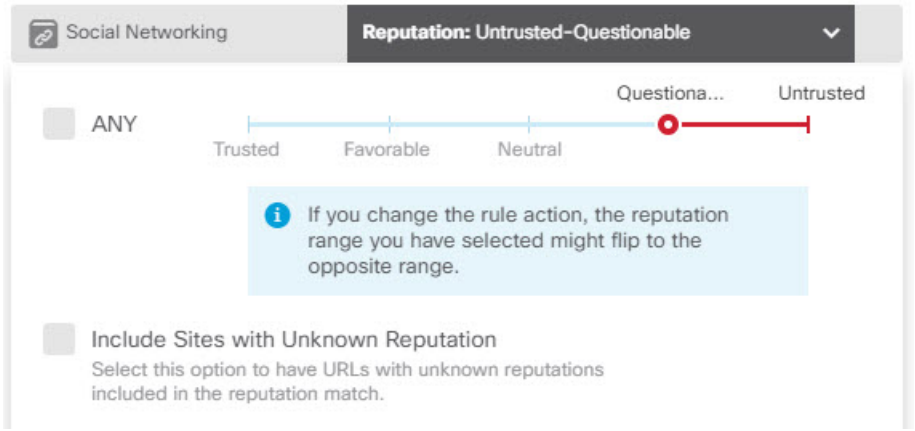
f) [URLs] タブをクリックします。

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、ボットネット、悪意のあるサイト、マルウェアサイト、およびソーシャルネットワーキングを選択します。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。ブロックしたいサイトがわかっていても、そのカテゴリがわからない場合は、[URL to Check] フィールドに URL を入力し、[Go] をクリックします。ルックアップ結果を示す Web サイトが表示されます。



h) レピュテーションに影響されるブロッキングを [Social Networking] カテゴリに実装するには、そのカテゴリの [Reputation: Risk Any] をクリックして、[Any] の選択を解除してからスライダを [Questionable] 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 [Questionable] と [Untrusted] 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。

レピュテーションが不明な URL をレピュテーション一致に含めるには、[レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] オプションを選択します。通常、新しいサイトは評価されていません。また、その他の理由でサイトのレピュテーションが不明である（または判断できない）場合もあります。

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。

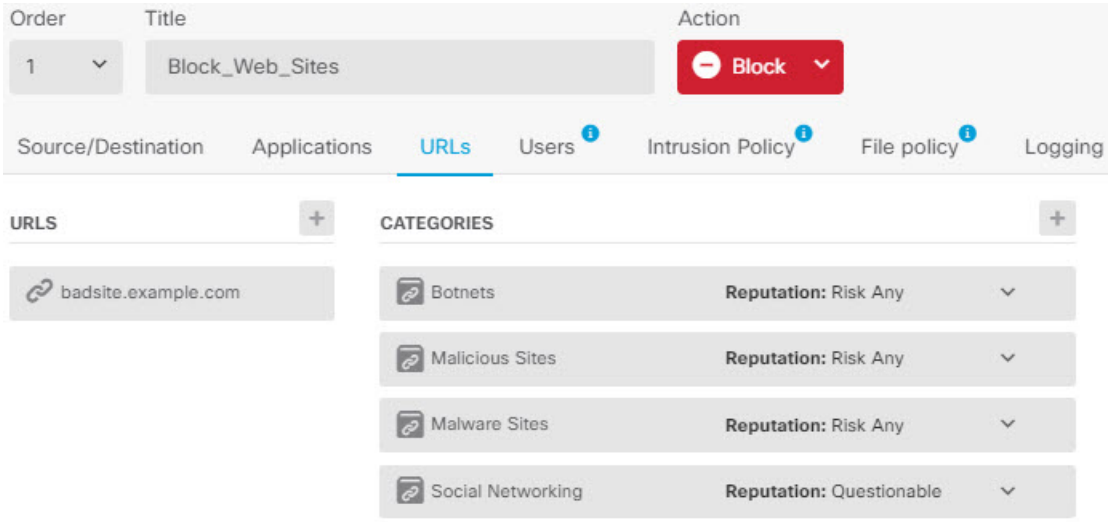
j) ポップアップ ダイアログ ボックスの下部で、[新規URLの作成（Create New URL）] リンクをクリックします。

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。



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。

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) [URL クエリ ソース（URL Query Source）] で、推奨オプションの [ローカル データベースと Cisco Cloud（Local Database and Cisco Cloud）] を選択します。

インストールされている URL データベースにサイトのカテゴリがない場合、Cisco Cloud にカテゴリが含まれている可能性があります。クラウド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。

あるいは、ルックアップをローカル データベースまたは Cisco Cloud に制限できます。

d) 妥当な [URL 存続可能時間（URL Time to Live）]（24 時間など）を選択します。
e) [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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

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と、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、[アノニマイザー/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 （7 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。

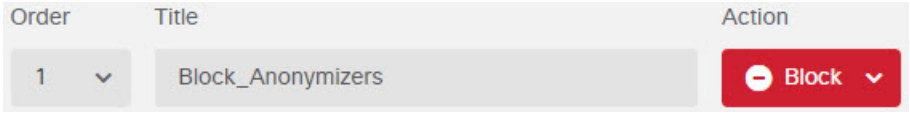
a) メイン メニューで [ポリシー（Policies）] をクリックします。

[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。

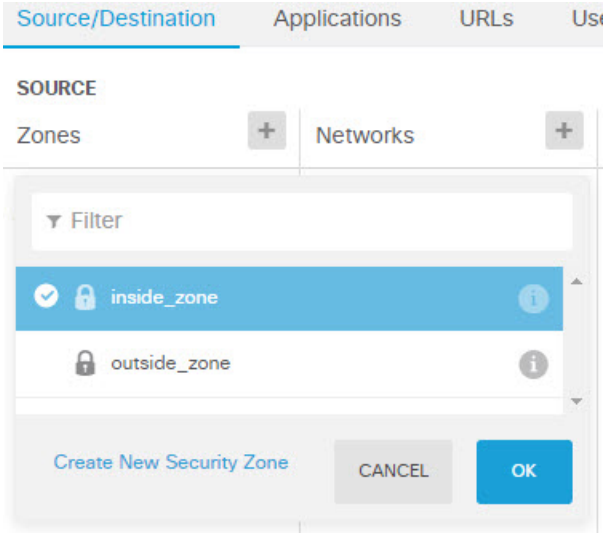
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

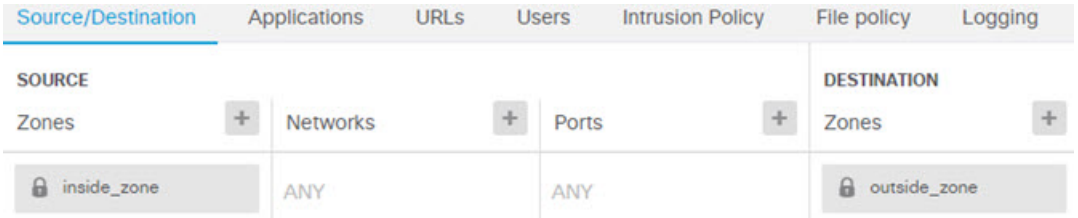
- [順序（Order）]：デフォルトで、新しいルールはアクセスコントロールポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上位）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセスコントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決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



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。



f) [アプリケーション（Applications）] タブをクリックします。

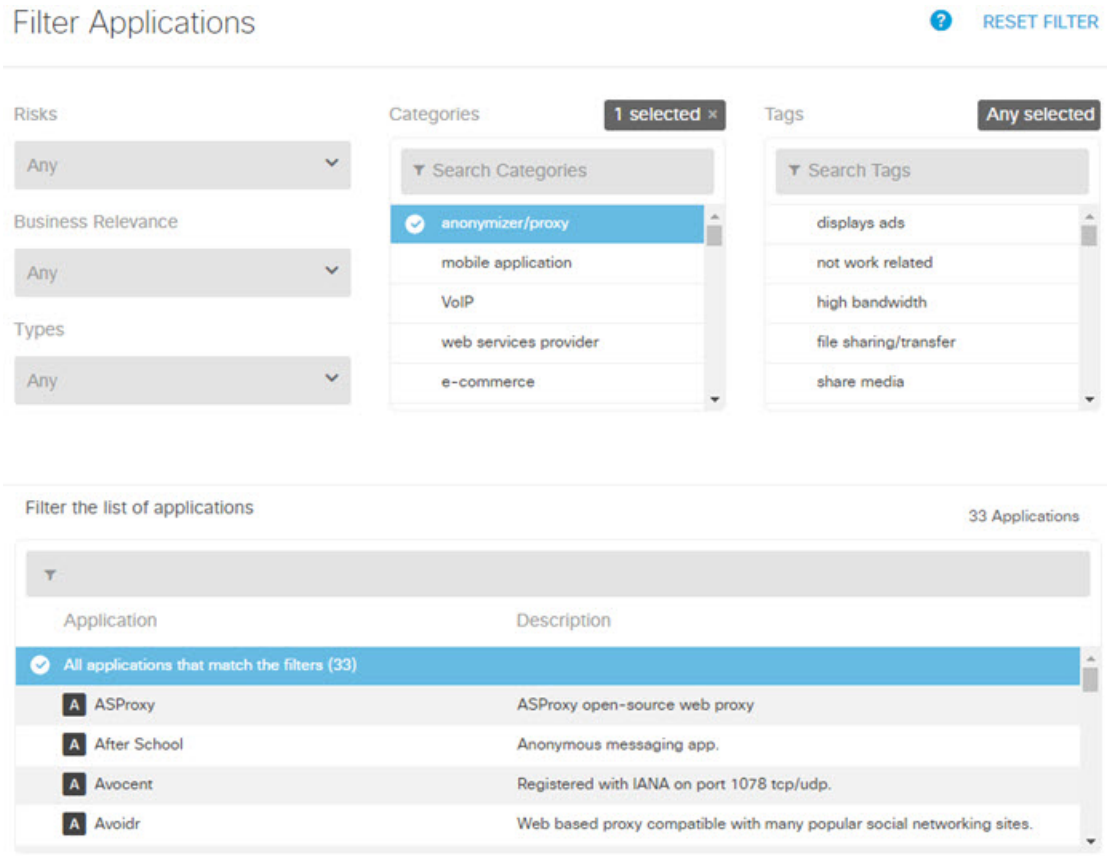
g) [アプリケーション（Applications）] の [+] をクリックして、ポップアップ ダイアログ ボックスの下部にある [高度なフィルタ（Advanced Filter）] リンクをクリックします。

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。

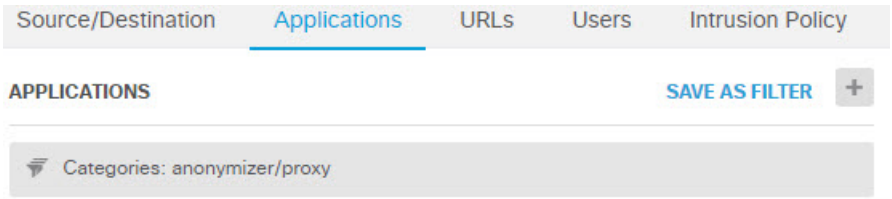
このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、TFPT は非常に高リスクに分類されています。ほとんどの組織は、このアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストは VDB の更新で変更できることを覚えておいてください。

この例では、[カテゴリ（Categories）] リストからアノニマイザー/プロキシを選択します。



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。



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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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、許可されます。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

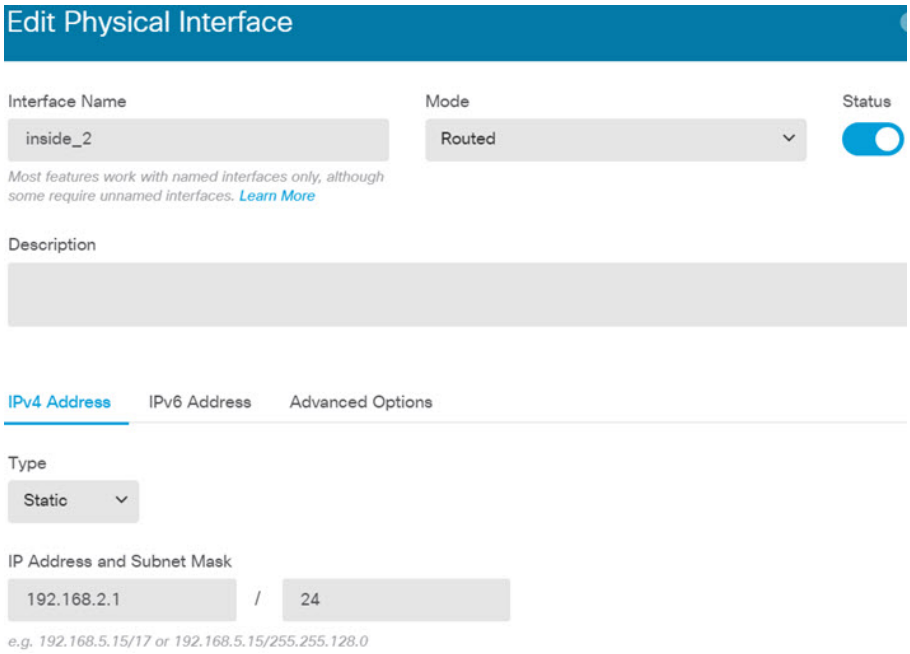
ステップ 1 インターフェイスを設定します。

a) [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、次にインターフェイスタイプをクリックして、インターフェイスのリストを表示します。

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）。
- [モード（Mode）]：[ルーテッド（Routed）] を選択します。
- [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。



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。

ステップ 2 インターフェイスの DHCP サーバを設定します。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]

b) **[システム設定（System Settings）]** > **[DHCPサーバ（DHCP Server）]** をクリックします。

c) [DHCPサーバ（DHCP Servers）] タブをクリックします。

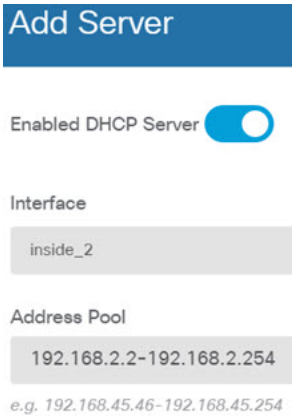
表に、既存の DHCP サーバが表示されます。デフォルト設定を使用している場合、リストには内部インターフェイスのいずれかが含まれます。

d) 表の上部の [+] をクリックします。

e) 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。



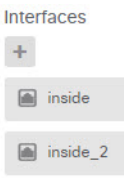
f) [追加（Add）] をクリックします。

#	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

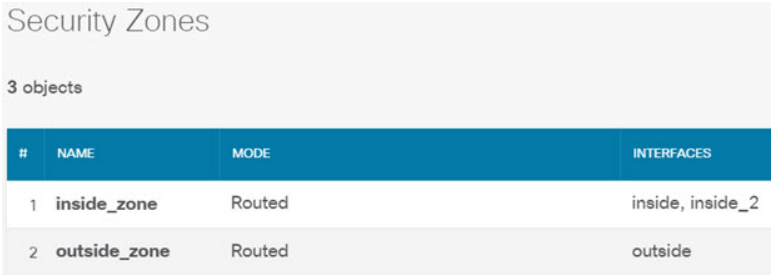
ステップ 3 内部セキュリティ ゾーンにインターフェイスを追加します。

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。

a) メイン メニューで [オブジェクト（Objects）] をクリックします。
b) 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。
c) [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。
d) [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。



e) [保存（Save）] をクリックします。



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は許可されません。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。

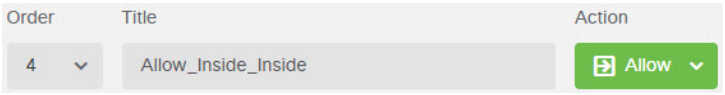
a) メイン メニューで [ポリシー（Policies）] をクリックします。

[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。

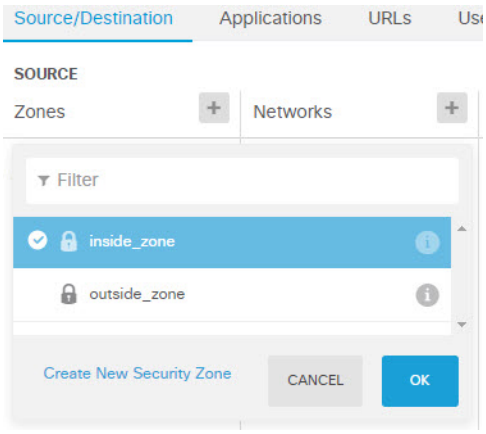
b) [+] をクリックして新しいルールを追加します。

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。

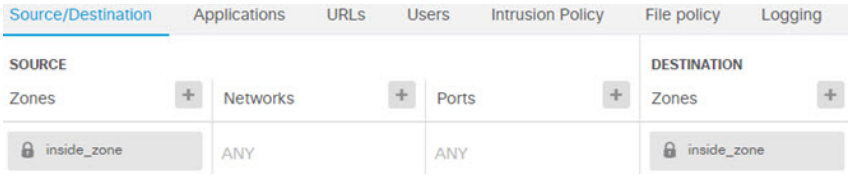


d) [送信元/接続先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。



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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

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。

ネットワーク上のトラフィックをパッシブにモニタする方法

脅威に対する防御デバイスは通常、アクティブなファイアウォールおよびIPS（侵入防御システム）セキュリティデバイスとして展開されます。デバイスの中核的機能は、ネットワークに対するアクティブな保護を提供し、不必要な接続や脅威を排除することにあります。

ただし、システムはパッシブモードで展開することもでき、その場合、デバイスは監視対象のスイッチポート上のトラフィックだけを分析します。このモードは、主にデモやテスト目的で使用されます。そうすることで、デバイスをアクティブなファイアウォールとして展開する前にそのデバイスに慣れることができます。パッシブ展開を使用すると、ネットワーク上に現れる脅威の種類（ユーザが参照している URL カテゴリなど）をモニタできます。

パッシブモードは、通常はデモやテスト目的で使用しますが、防御のないIDS（侵入検知システム）など、必要なサービスが提供される場合は、実稼働環境でパッシブモードを使用することもできます。パッシブ インターフェイスをアクティブなファイアウォールのルーテッド インターフェイスと混在させることで、組織が必要とする的確なサービスの組み合わせを提供できます。

次の手順では、限られた数のスイッチポートからのトラフィックを分析するために、システムをパッシブに展開する方法を説明します。

（注） この例は、ハードウェア 脅威に対する防御 デバイス向けです。Threat Defense Virtual にパッシブモードを使用することもできますが、ネットワークの設定は異なります。詳細は、Threat Defense Virtual パッシブインターフェイスの VLAN の設定を参照してください。それ以外の場合、Threat Defense Virtual にはこの手順が適用されます。

始める前に

次の手順は、内部インターフェイスと外部インターフェイスに接続し、デバイスの初期セットアップ ウィザードが完了していることを前提としています。パッシブ展開の場合でも、システムデータベースの更新をダウンロードするためにインターネットに接続する必要があります。また、Device Manager を開くために管理インターフェイスにも接続できる必要があります。これは、内部ポートまたは管理ポートへの直接接続を介して可能です。

この例では、**[ポリシー（Policies）]** > **[侵入（Intrusion）]**ページで、侵入ポリシーの syslog を有効にしていることも前提としています。

手順

ステップ 1 スイッチ ポートを SPAN（スイッチド ポート アナライザ）ポートとして設定し、送信元インターフェイスのモニタリング セッションを設定します。

次の例では、Cisco Nexus 5000 シリーズ スイッチの 2 つの送信元インターフェイスに SPAN ポートとモニタリング セッションを設定します。異なる種類のスイッチを使用している場合は、必要なコマンドが異なることがあります。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

確認するには、次の手順に従います。

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ 2 脅威に対する防御 インターフェイスをスイッチの SPAN ポートに接続します。

脅威に対する防御デバイス上の現在未使用のポートを選択することをお勧めします。スイッチの設定例に基づいて、スイッチのイーサネット 1/48 にケーブルを接続します。これはモニタリング セッションの宛先インターフェイスです。

ステップ 3 脅威に対する防御 インターフェイスをパッシブモードで設定します。

a) [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、[インターフェイス（Interfaces）] または [EtherChannel（EtherChannels）] をクリックします。

b) 編集する物理インターフェイスまたは EtherChannel の編集アイコン（  ）をクリックします。

現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブ インターフェイスに変換する場合は、最初にセキュリティ ゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

d) 次を設定します。

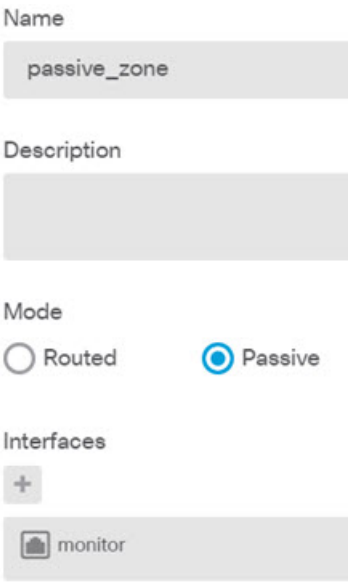
- [インターフェイス名（Interface Name）]：最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、**monitor** などです。

- [モード（Mode）]：[パッシブ（Passive）] を選択します。

e) [OK] をクリックします。

ステップ 4 インターフェイスのパッシブ セキュリティ ゾーンを作成します。

a) [オブジェクト（Objects）] を選択し、次に目次から [セキュリティ ゾーン（Security Zones）] を選択します。
b) [+] ボタンをクリックします。
c) オブジェクトの名前を入力し、任意で説明を入力します。例、**passive_zone**。
d) [モード（Mode）] で [パッシブ（Passive）] を選択します。
e) [+] をクリックして、パッシブ インターフェイスを選択します。



f) [OK] をクリックします。

ステップ 5 パッシブ セキュリティ ゾーン用の 1 つ以上のアクセス制御ルールを設定します。

作成するルールの数と種類は、収集する情報によって異なります。たとえば、IDS（侵入検知システム）としてシステムを設定する場合は、割り当てられた侵入ポリシーを設定した [許可（Allow）] ルールが少なくとも 1 つは必要です。URL カテゴリ データを収集する場合は、URL カテゴリの仕様を含むルールが少なくとも 1 つは必要です。

[ブロック（Block）] ルールを作成して、ルーテッド インターフェイスでアクティブにブロックされる接続を確認できます。インターフェイスがパッシブなので、それらの接続は実際にはブロックされませんが、システムによるネットワーク上のトラフィックの調整方法は明確に確認できます。

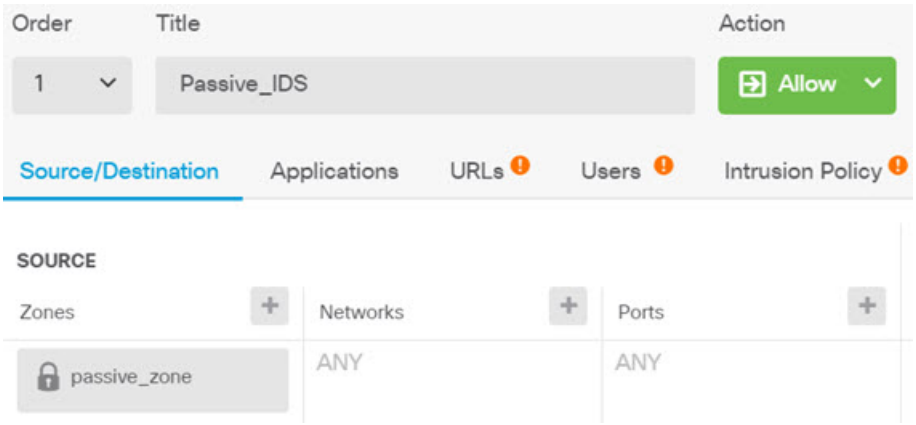
次の使用例では、アクセス制御ルールの主な使用方法について説明します。それらの使用例は、パッシブ インターフェイスにも当てはまります。作成するルールの送信元ゾーンとしてパッシブ セキュリティ ゾーンを選択します。

- 脅威をブロックする方法 （16 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 （25 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）

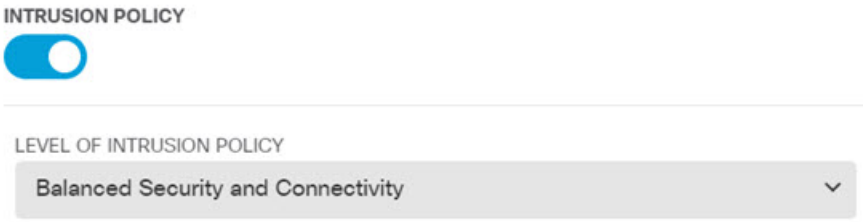
次の手順では、侵入ポリシーを適用して、URL カテゴリ データを収集する 2 つの [許可（Allow）] ルールを作成します。

a) **[ポリシー（Policies）]** > **[アクセス コントロール（Access Control）]** を選択します。
b) [+] をクリックして、すべてのトラフィックを許可するが、侵入ポリシーを適用するルールを追加します。
c) ルールの順序として **1** を選択します。このルールはデフォルトのルールよりも具体的ですが、デフォルトのルールとはオーバーラップしません。カスタム ルールがすでにある場合は適切な位置を選択し、パッシブ インターフェイス向けのトラフィックが代わりにそれらのルールと一致しないようにします。
d) ルールの名前、**Passive_IDS** などを入力します。
e) [アクション（Action）] として [許可（Allow）] を選択します。
f) [送信元/宛先（Source/Destination）] タブの **[送信元（Source）]** > **[ゾーン（Zones）]** でパッシブ ゾーンを選択します。このタブの他の設定は変更しないでください。

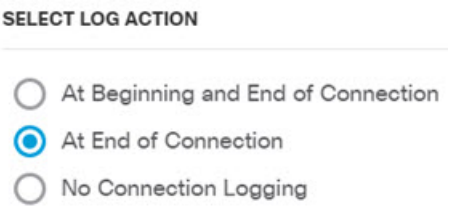
この時点で、評価モードで実行中のルールは次のようになります。



g) [侵入ポリシー（Intrusion Policy）] タブをクリックし、スライダをクリックして [オン（On）] にして、ほとんどのネットワークに推奨される [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーなどの侵入ポリシーを選択します。



h) [ロギング（Logging）] タブをクリックし、ロギング オプションで [接続の終了時（At End of Connection）] を選択します。



i) [OK] をクリックします。

j) [+] をクリックして、URL およびすべての HTTP 要求のカテゴリを判断するためにシステムがディープ インスペクションを実行する必要があるルールを追加します。

このルールにより、ダッシュボードでURLカテゴリ情報を確認できるようになります。処理時間を短縮し、パフォーマンスを向上させるために、URLカテゴリ条件を指定する少なくとも1つのアクセス制御ルールが存在する場合にのみシステムはURLカテゴリを判断します。

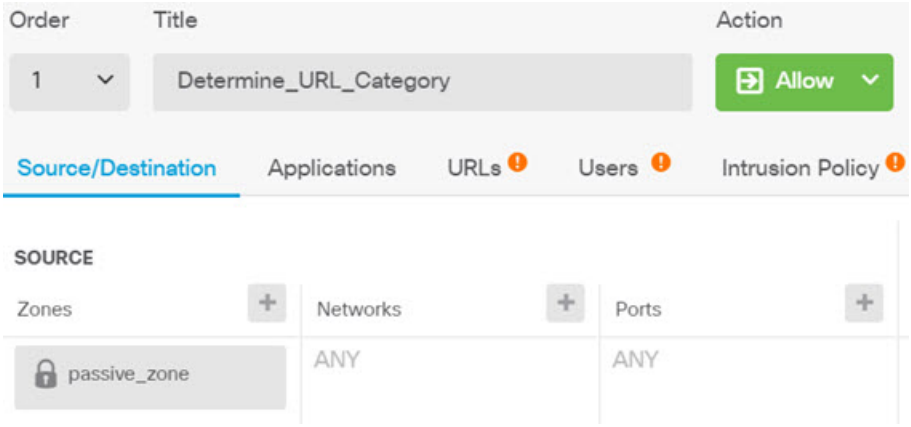
k) ルールの順序として **1** を選択します。これは、前のルール（Passive_IDS）の上に配置されます。（すべてのトラフィックに適用される）ルールの後に配置すると、今作成しているルールは決して一致しません。

l) ルールの名前、**Determine_URL_Category** などを入力します。

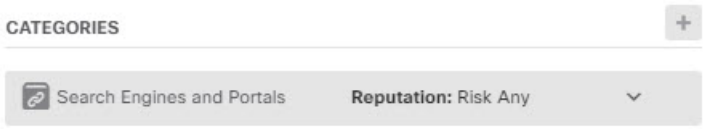
m) [アクション（Action）] として [許可（Allow）] を選択します。

または、[ブロック（Block）] を選択できます。いずれのアクションでも、このルールの目的が達成されます。

n) [送信元/宛先（Source/Destination）] タブの **[送信元（Source）] > [ゾーン（Zones）]** でパッシブ ゾーンを選択します。このタブの他の設定は変更しないでください。



o) [URL（URLs）] タブをクリックし、[カテゴリ（Categories）] 見出しの横にある [+] をクリックして、いずれかのカテゴリを選択します。たとえば、**[Search Engines and Portals]** を選択します。必要に応じて、レピュテーション レベルを選択するか、デフォルトの [任意（Any）] のままにします。



p) [侵入ポリシー（Intrusion Policy）] タブをクリックし、スライダをクリックして [オン（On）] にして、最初のルールに選択したのと同じ侵入ポリシーを選択します。

q) [ロギング（Logging）] タブをクリックし、ロギング オプションで [接続の終了時（At End of Connection）] を選択します。

ただし、アクションとして [ブロック（Block）] を選択した場合は、[接続の開始時と終了時（At Beginning and End of Connection）] を選択します。ブロックされた接続自体は終了しないため、接続の開始時にのみログ情報を取得できます。

r) [OK] をクリックします。

ステップ 6 （オプション）その他のセキュリティ ポリシーを設定します。

次のセキュリティポリシーも設定して、トラフィックにどのような影響を与えるかを確認できます。

- [アイデンティティ（Identity）]：ユーザ情報を収集します。アイデンティティ ポリシーにルールを設定して、送信元 IP アドレスに関連付けられているユーザが確実に特定されるようにできます。パッシブ インターフェイスのアイデンティティ ポリシーの実装プロセスは、ルーテッド インターフェイスのプロセスと同じです。ネットワーク トラフィックを調べる方法 （7 ページ）で説明されている使用例を参照してください。
- [セキュリティインテリジェンス（Security Intelligence）]：既知の不正な IP アドレスと URL をブロックします。詳細は、脅威をブロックする方法 （16 ページ）を参照してください。

（注） パッシブインターフェイス上のすべての暗号化されたトラフィックは復号不可として分類されるため、SSL 復号化ルールは無効になり、パッシブインターフェイスには適用されません。

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するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 8 監視ダッシュボードを使用して、ネットワーク経由で到達するトラフィックや脅威の種類を分析します。脅威に対する防御デバイスに不要な接続をアクティブにドロップさせる場合は、デバイスを再展開して、監視対象ネットワークに対するファイアウォール保護を提供するアクティブなルーテッド インターフェイスを設定できます。

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。

アクセス制御

- Trustsec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法

Network Address Translation（NAT）

IPv4 アドレス用の NAT

- 内部 Web サーバー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 サーバー
- DNS 応答修正：ホスト ネットワーク上の DNS サーバー
- 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）

- RADIUS 認可変更の実装方法
- Duo LDAP を使用した二要素認証の設定方法
- 外部インターフェイスでリモート アクセス VPN ユーザーにインターネット 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 サーバーを使用する方法
- グループによって RA VPN アクセスを制御する方法
- 異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法
- セキュアクライアント のアイコンとロゴをカスタマイズする方法

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 ユーザーにインターネット アクセスを提供する方法（ヘア ピニング）
- サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

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 インスペクションを有効/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 クラスのインスペクションを有効にする方法

仮想ルーティング

- 重複するアドレス空間を持つ複数の仮想ルータへのインターネットアクセスを提供する方法

- 複数の仮想ルータを介して遠隔サーバーにルーティングする方法
- 異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法
- サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

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。