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、これらの例から製品の使用法は理解できるはずです。

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。
- （Firepower 4100/9300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、設定可能なその他の機能の概要を示します。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お読みください。

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。

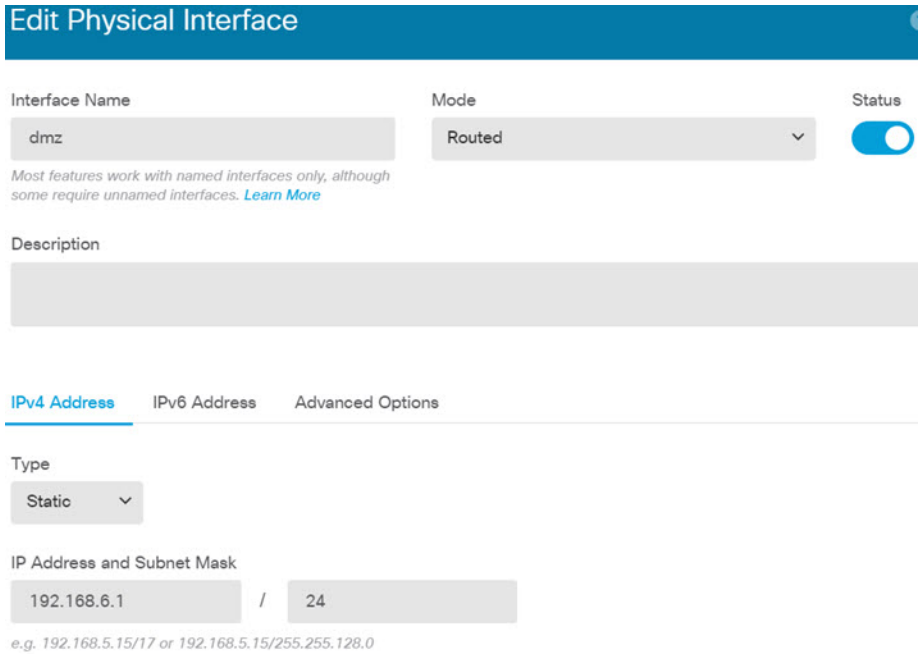
ステップ 2 他のインターフェイスに接続している場合は、[デバイス（Device）] を選択し、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックしてから、インターフェイスのタイプをクリックして、インターフェイスのリストを表示します。

- 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、別のネットワークをホストするようにこれらのインターフェイスを設定できます。

  その他のモデルの場合は、他のインターフェイス用のブリッジグループを作成するか、個別ネットワークを設定するか、またはそれらを組み合わせることができます。
- Firepower 1010 および Secure Firewall 1210/1220 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。

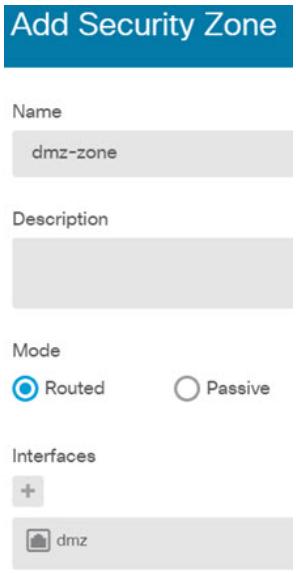
次の例では、Web サーバなどのパブリック アクセスが可能なアセットを配置する「緩衝地帯」（DMZ）として使用されるインターフェイスを設定します。完了したら [保存（Save）] をクリックします。



ステップ 3 新しいインターフェイスを設定した場合は、[オブジェクト（Objects）] を選択してから、目次から [セキュリティゾーン（Security Zones）] を選択します。

必要に応じて新しいゾーンを編集または作成します。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設定するため、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。インターフェイスの設定中はインターフェイスをゾーンに配置できないため、常に、新しいインターフェイスの作成後または既存のインターフェイスの目的の変更後にゾーンオブジェクトを編集する必要があります。

次の例は、DMZ インターフェイス用の新しい DMZ ゾーンを作成する方法を示しています。

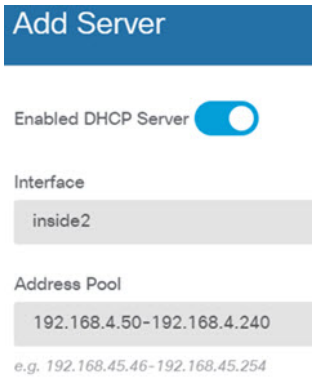


ステップ 4 内部クライアントがDHCPを使用してデバイスからIPアドレスを取得するようにする場合は、[デバイス（Device）] を選択し、次に**[システム設定]** > **[DHCPサーバ]**を選択します。[DHCP サーバ（DHCP Servers）] タブを選択します。

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設定する場合、それらのインターフェイスにDHCPサーバを設定するのが非常に一般的です。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。

次の例は、inside2 インターフェイス上の DHCP サーバをアドレス プール 192.168.4.50-192.168.4.240 を使用して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 any-ipv4（0.0.0.0/0）用で、デフォルトの

IPv6 ルートは any-ipv6（::0/0）用です。使用する IP バージョンごとにルートを作成します。DHCP を使用して外部インターフェイスのアドレスを取得している場合は、必要なデフォルトルートがすでに存在している可能性があります。

このページで定義するルートはデータ インターフェイス専用です。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-gateway 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（ISP からアドレスを取得する必要があります）。このオブジェクトは、[ゲートウェイ（Gateway）] ドロップダウン リストの下部で [新しいネットワークの作成（Create New Network）] をクリックして作成します。

ステップ 6 [ポリシー（Policies）] を選択し、ネットワークのセキュリティ ポリシーを設定します。

デバイス セットアップ ウィザードにより、内部ゾーンと外部ゾーンの間のトラフィック フロー、および外部インターフェイスに向かうすべてのインターフェイスのインターフェイス NAT が有効になります。新しいインターフェイスを設定する場合でも、そのインターフェイスを内部ゾーン オブジェクトに追加するとアクセス制御ルールが自動的に適用されます。

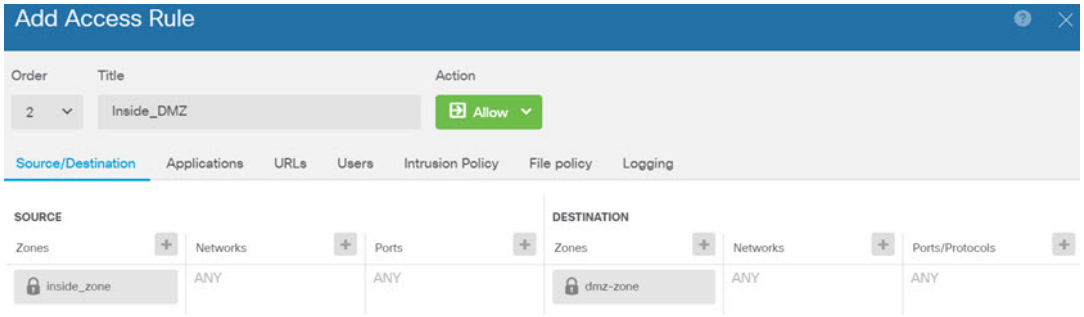
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティ ゾーンを追加する場合は、それらのゾーンとの双方向トラフィックを許可するルールが必要です。これらは最小限の変更です。

さらに、追加のサービスを提供するために他のポリシーを設定し、組織が必要とする結果を取得するために NAT およびアクセス ルールを調整することができます。以下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、接続を復号する必要があります。SSL 復号ポリシーを使用して、どの接続を復号する必要があるか判断します。検査後にシステムが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）]：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）：NAT ポリシーを使用して内部 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します。
- [アクセス制御（Access Control）]：アクセス制御ポリシーを使用してネットワーク上で許可する接続を決定します。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 グループでフィルター処理できます。また、アクセス制御ルールを使用して侵入およびファイル（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ても、侵入ポリシーを編集して特定の侵入ルールを有効または無効にすることができます。

次の例は、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ています。この例では、[接続終了時（At End of Connection）] が選択されている [ロギング（Logging）] 以外のタブではオプションは設定されていません。



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、または [OK] をクリックして、後でタスク リストや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

デバイスの初期セットアップが完了すると、すべての内部トラフィックに対してインターネットまたはその他のアップストリーム ネットワークへのアクセスを許可するアクセス制御ポリシーと、その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ています。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
- 最もヒットしているアクセス制御ルール（ポリシー）

初期アクセス ルールから、トラフィックに関する情報（ポリシー、宛先、セキュリティ ゾーンなど）を取得できます。ただし、ユーザ情報を確認するには、ユーザがユーザ自身を認証（識別）することを要件としたアイデンティティ ポリシーを設定する必要があります。ネットワークで使用されているアプリケーションに関する情報を取得するには、追加の調整が必要です。

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。カテゴリとレピュテーションに関する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 ライセンスを有効に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を設定する必要があります。

アイデンティティポリシーを有効にすると、ネットワークを使用しているユーザや、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（User）] 監視ダッシュボードで確認できます。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。

認証に失敗したユーザは、Web 接続を確立できません。これは、接続のためのユーザ 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、認証失敗ユーザのトラフィックをドロップするアクセス制御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、次に [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のアクティブ認証が要求されると、そのユーザ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。

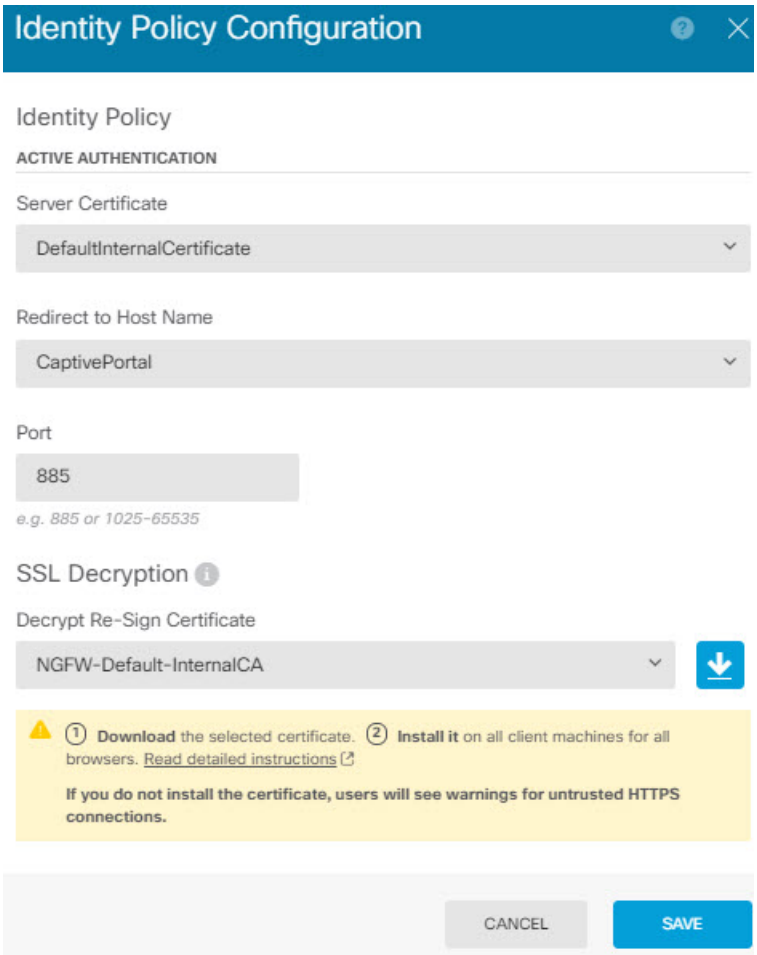
- [ポート（Port）]：キャプティブ ポータル ポート。デフォルトは 885（TCP）です。別のポートを設定する場合は、1025 ～ 65535 の範囲にする必要があります。

- [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 復号ポリシーをまだ有効にしていない場合にのみ、復号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、完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してユーザが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 サーバを更新する必要もあります。そうでない場合は、リダイレクションが完了せず、ユーザは認証できません。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、そのオブジェクトを選択して、サーバ設定手順を省略します。

次のフィールドを入力し、[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。サポートされているタイプは Active Directory のみのため、このフィールドは変更できません。
- [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 と変換されます。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。たとえば、dc=example,dc=com となります。ベース DN の検索方法については、ディレクトリベース 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のある、完全修飾 Active Directory ドメイン名。たとえば、example.com のように指定します。
- [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。LDAPS を暗号化方式に選択している場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザとグループの情報をダウンロードするのに暗号化接続を使用する場合は、適切な方式を [STARTTLS] または [LDAPS] から選択します。

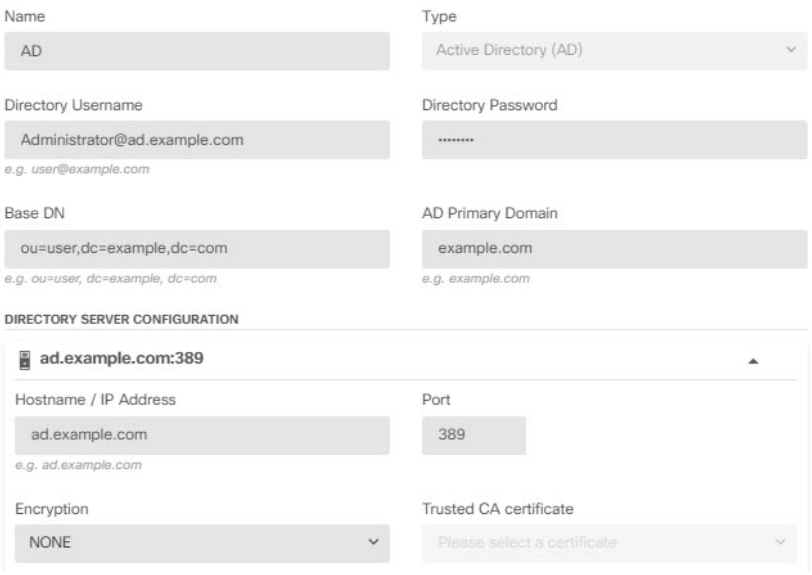
デフォルトは [なし（None）] です。したがって、ユーザとグループ情報はクリアテキストでダウンロードされます。

- [STARTTLS] 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ている最も強力な方式を使用します。ポート 389 を使用します。リモートアクセス VPN 用にレルムを使用する場合は、このオプションが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）]：暗号化方式を選択した場合は、認証局（CA）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している場合、証明書のサーバ名とサーバのホスト名/IP アドレスが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 を使用するが、証明書では ad.example.com が指定されている場合、接続が失敗します。

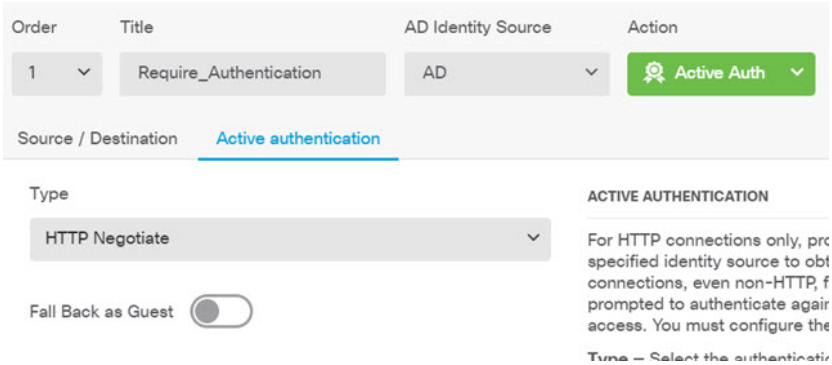
例：

次の図に、ad.example.com サーバの非暗号化接続を作成する例を示します。プライマリドメインは example.com、ディレクトリ ユーザ名は Administrator@ad.example.com です。すべてのユーザと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。

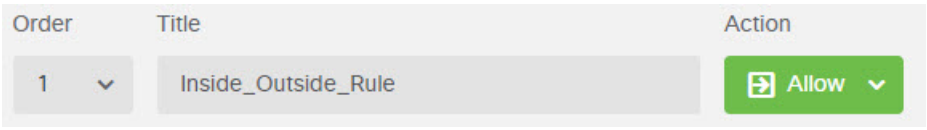
ウィンドウの右上にある [展開（Deploy）] アイコン ボタンに 1 つのドットが表示されています。これは、まだ展開されていない変更があることを示します。ユーザ インターフェイスで変更を行っても、デバイスで変更を設定するには十分ではありません。変更を展開する必要があります。したがって、一連の関連する変更を行ってからそれらの変更を展開します。このように展開することで、部分的に設定された変更がデバイスに反映されるという問題が発生しません。この手順の後半で変更を展開します。

ステップ 2 Inside_Outside_Rule アクセス制御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 ルールが信頼ルールとして作成されます。ただし信頼されているトラフィックは検査されないため、トラフィック一致基準に、ゾーン、IP アドレス、およびポート以外の条件やアプリケーションが含まれていない場合、システムは信頼されているトラフィックの特性の一部（アプリケーションなど）を学習できません。トラフィックを信頼する代わりにトラフィックを許可するようにこのルールを変更すると、システムはトラフィックを完全に検査します。

（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 [アクセス制御（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 ポインタを合わせて編集アイコンと削除アイコンを表示させ、編集アイコン（）をクリックしてルールを開きます。
c) [アクション（Action）] で [許可（Allow）] を選択します。

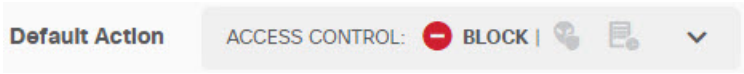


d) [OK] をクリックして変更を保存します。

ステップ 3 アクセス制御ポリシーのデフォルト アクションでロギングを有効にします。

接続ロギングを有効にするアクセス制御ルールに一致する接続の場合にのみ、接続に関する情報がダッシュボードに表示されます。Inside_Outside_Rule によりロギングが有効になりますが、デフォルト アクションではロギングが無効です。したがってダッシュボードには Inside_Outside_Rule の情報だけが表示されており、どのルールにも一致しない接続は反映されません。

a) アクセス制御ポリシー ページの下部にあるデフォルト アクション内の任意の位置をクリックします。



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）]** の順に選択します。

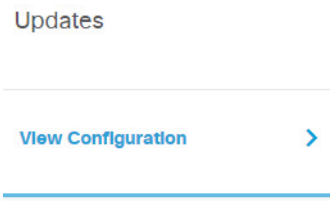
c) [OK] をクリックします。

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。

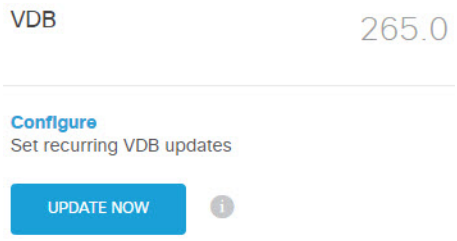
シスコは VDB の更新を定期的にリリースしています。VDB には、接続で使用されているアプリケーションを特定できるアプリケーション検出プログラムが含まれます。VDB は定期的に更新する必要があります。更新を手動でダウンロードするか、定期的なスケジュールを設定できます。次の手順では、スケジュールの設定方法を説明します。デフォルトでは、VDB の更新は無効化されているため、VDB の更新を取得するには操作を実行する必要があります。

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。

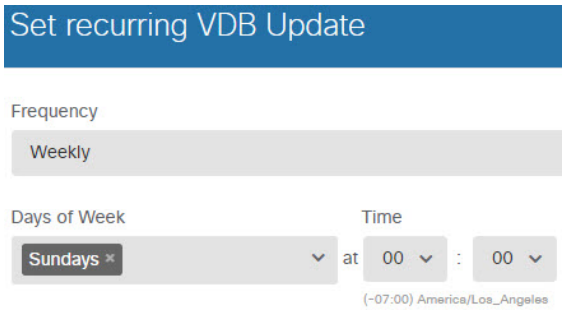


d) 更新スケジュールを定義します。

ネットワークに支障のない時間と頻度を選択します。また、更新をダウンロードした後、システムが自動展開を実行する点にも注意してください。これは、新しい検出プログラム

を有効化するのに必要です。このため、何らかの形で設定をすでに変更して保存した後、まだ展開していない場合は、それも展開する必要があります。

たとえば、次のスケジュールは VDB を 1 週間に 1 回、日曜日の午前 12:00（24 時間表記を使用）に更新します。



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

次のタスク

この時点で、監視ダッシュボードとイベントによりユーザとアプリケーションの情報が表示され始めます。この情報を評価して不適切なパターンを特定し、許容できない使用を制限するための新しいアクセス ルールを作成できます。

侵入とマルウェアに関する情報の収集を開始するには、1 つ以上のアクセス ルールで侵入ポリシーとファイル ポリシーを有効にする必要があります。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。

脅威のブロック方法

侵入ポリシーをアクセス制御ルールに追加することにより、次世代の侵入防御システム（IPS）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、トラ

フィック コンテンツを既知の脅威と比較します。いずれかの接続が監視対象の脅威と一致する場合、システムはその接続をドロップし、こうして攻撃を防止できます。

ネットワーク トラフィックに対して侵入検査を行う前に、他のすべてのトラフィック処理が行われます。侵入ポリシーをアクセス制御ルールに関連付けると、アクセス制御ルールの条件に一致するトラフィックをシステムが通過させる前に、侵入ポリシーを使ってまずトラフィックを検査するようシステムに指示できます。

単にトラフィックを許可するルール上で侵入ポリシーを設定できます。トラフィックを信頼またはブロックするように設定したルールにインスペクションは実行されません。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して、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) [デバイス（Device）] をクリックします。

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。ライセンスが有効になっていることがグループに表示され、ボタンが [無効化（Disable）] ボタンに変わります。

ステップ 2 1 つ以上のアクセス ルール用の侵入ポリシーを選択します。

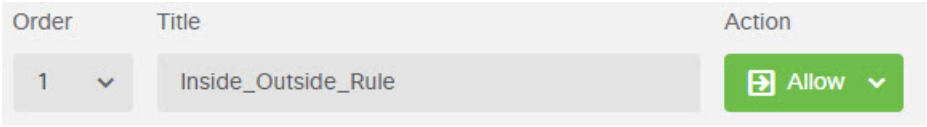
脅威のスキャニング対象となるトラフィックをどのルールで扱うかを決定します。この例では、Inside_Outside_Rule に侵入検査を追加します。

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てい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 ポインタを合わせて編集アイコンと削除アイコンを表示させ、編集アイコン（）をクリックしてルールを開きます。

c) [アクション（Action）] に [許可（Allow ）] をまだ選択していない場合は、これを選択します。

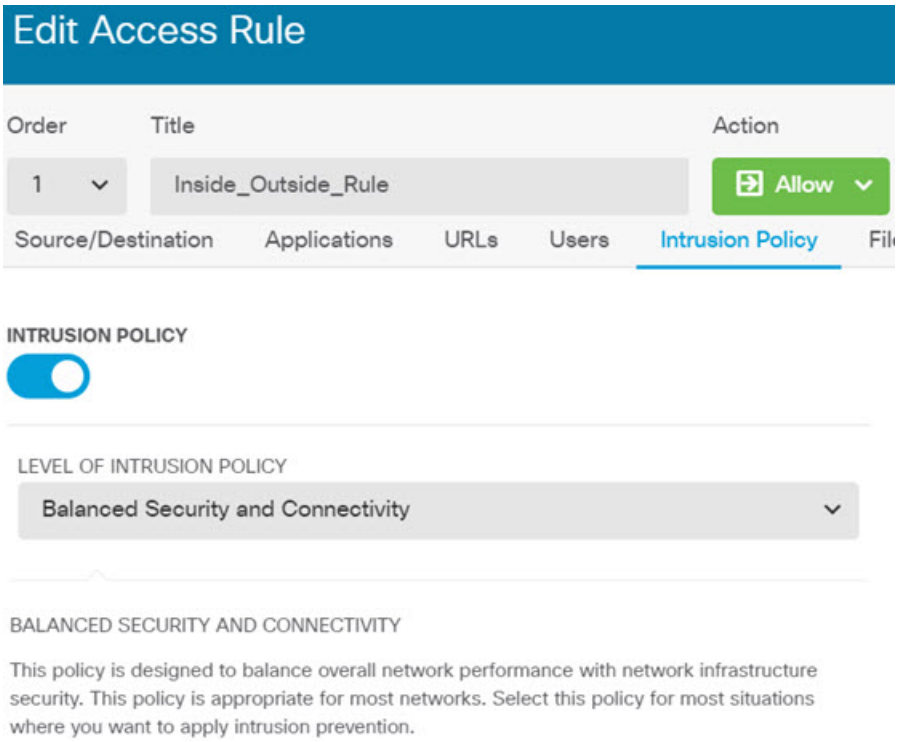


d) [侵入ポリシー（Intrusion Policy）] タブをクリックします。

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。

ほとんどのネットワークでは、[バランスのとれたセキュリティと接続（Balanced Security and Connectivity）] ポリシーが適しています。このポリシーは適度な侵入保護を提供し、過剰にアグレッシブ（ドロップすべきでないトラフィックがドロップされる可能性がある）でもありません。ドロップされるトラフィックが多すぎる場合は、[セキュリティを上回る接続性（Connectivity over Security）] ポリシーを選択することにより、侵入検査を緩和できます。

アグレッシブなセキュリティが必要な場合は、[接続性を上回るセキュリティ（Security over Connectivity）] ポリシーを試してください。[最大検出（Maximum Detection）] ポリシーは、ネットワーク インフラストラクチャ セキュリティをさらに重視したポリシーであり、運用上より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。

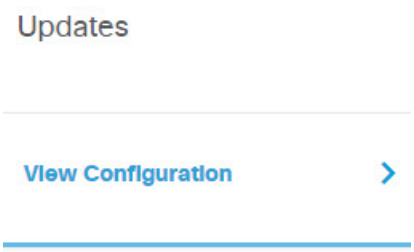
ステップ 3 （オプション）。**[ポリシー（Policies）]**>**[侵入（Intrusion）]**に移動し、歯車アイコンをクリックして、侵入ポリシーの syslog サーバを設定します。

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。

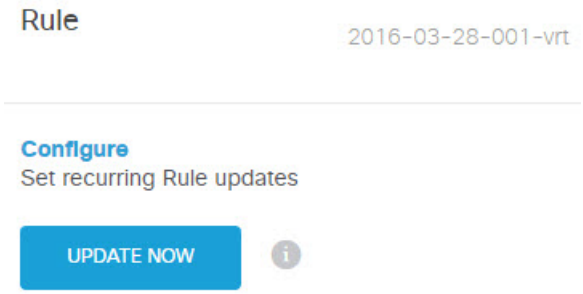
ステップ 4 侵入ルール データベースの更新スケジュールを設定します。

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。接続をドロップすべきかどうかを判断するために、侵入ポリシーでこれが使用されます。ルールデータベースを定期的に更新してください。更新を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。次の手順では、スケジュールの設定方法を説明します。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。



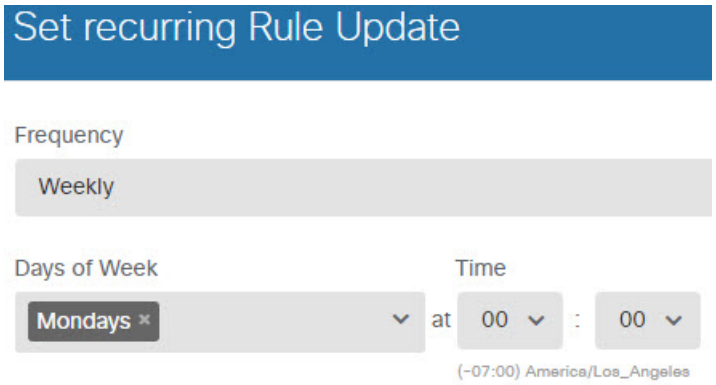
c) [ルール（Rule）] グループで [設定（Configure）] をクリックします。



d) 更新スケジュールを定義します。

ネットワークに支障のない時間と頻度を選択します。また、更新をダウンロードした後、システムが自動展開を実行する点にも注意してください。新しいルールを有効化するには、この操作が必要です。このため、何らかの形で設定をすでに変更して保存した後、まだ展開していない場合は、それも展開する必要があります。

たとえば、次のスケジュールはルール データベースを 1 週間に 1 回、月曜日の午前 12:00（24 時間表記を使用）に更新します。



e) [保存（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。

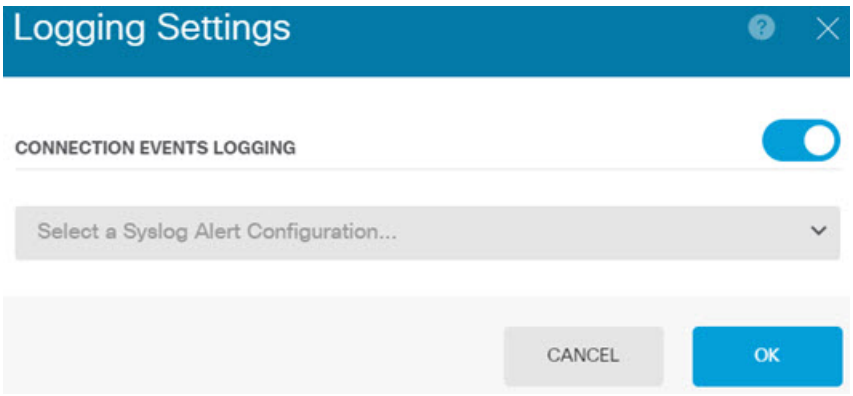
他にも不正 IP アドレスがある場合は、**[+] > [ネットワーク オブジェクト（Network Objects）]** をクリックして、それらのアドレスを含むオブジェクトを追加できます。リストの下部にある [新規ネットワーク オブジェクトの作成（Create New Network Object）] をクリックして、今すぐ追加することもできます。

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) ギア 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を評価するため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の接続はアクセス制御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、または [OK] をクリックして、後でタスク リストや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。

マルウェアのブロック方法

ユーザは、悪意のあるソフトウェア（つまりマルウェア）をインターネットサイトや電子メールなどの通信手段から取り込んでしまうリスクに絶えずさらされています。信頼される Web

サイトでさえ、ハイジャックされて、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、別のソースからのオブジェクトが含まれることがあります。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、しばしば、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。

単にトラフィックを許可するルール上で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。

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) [デバイス（Device）] をクリックします。
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。ライセンスが有効になっていることがグループに表示され、ボタンが [無効化（Disable）] ボタンに変わります。

ステップ 2 1 つ以上のアクセス ルール用のファイル ポリシーを選択します。

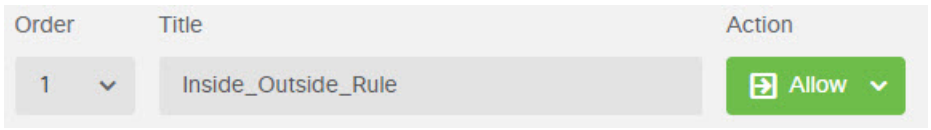
マルウェア スキャニングの対象となるトラフィックをどのルールで扱うかを決定します。この例では、Inside_Outside_Rule にファイル検査を追加します。

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てい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 ポインタを合わせて編集アイコンと削除アイコンを表示させ、編集アイコン（  ）をクリックしてルールを開きます。

c) [アクション（Action）] に [許可（Allow ）] をまだ選択していない場合は、これを選択します。



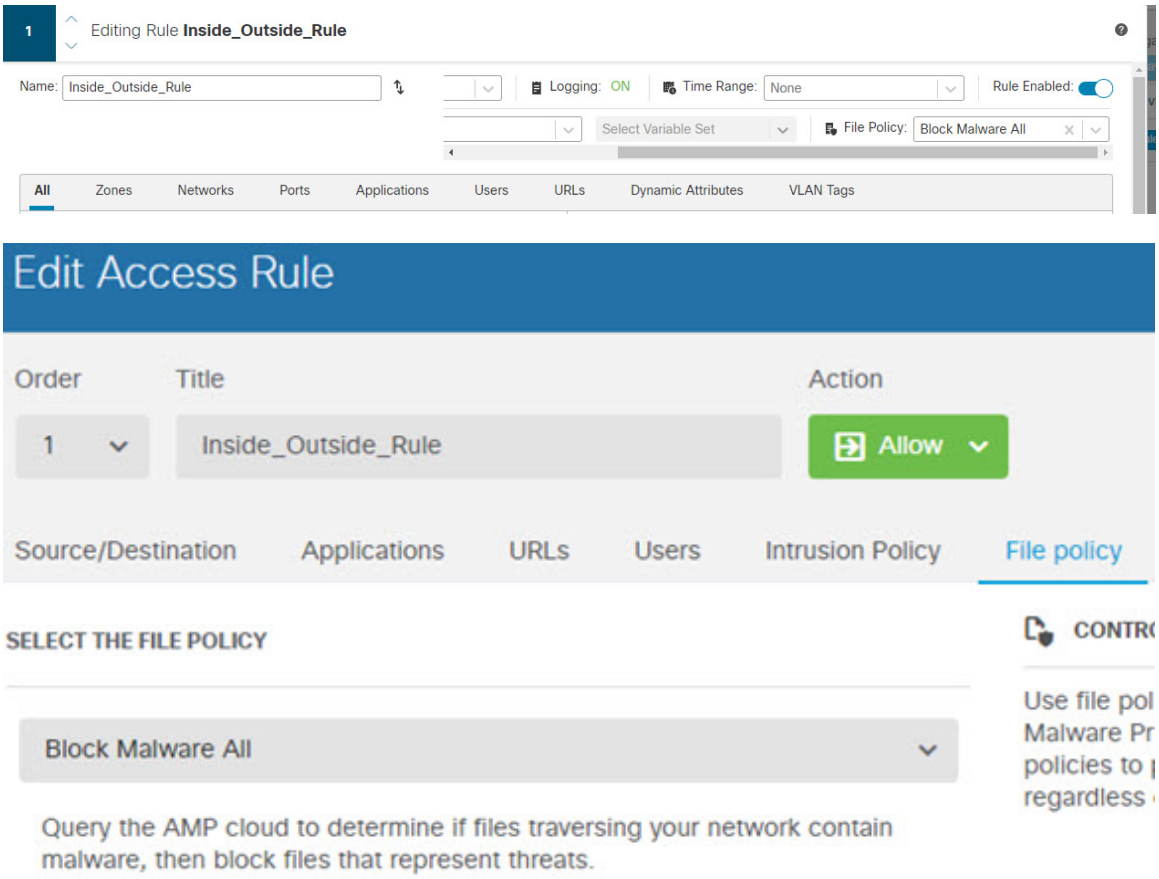
d) [ファイル ポリシー（File Policy）] タブをクリックします。

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。ファイルの評価を適切に確認できた後で、ブロッキング ポリシーに変更できます。

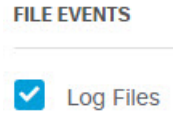
マルウェアをブロックする他のポリシーを使用することもできます。これらのポリシーをファイル制御と組み合わせて、Microsoft Office、Office、PDF ドキュメントのアップロードをブロックできます。つまり、これらのポリシーを使用すると、マルウェアをブロックするだけでなく、これらのファイル タイプがユーザから他のネットワークに送信されるのを防止できます。実際の要件に合う場合は、これらのポリシーを選択できます。

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、[ファイル イベント（File Events）] の下で [ログ ファイル（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常にファイル ロギングが有効になります。イベントやダッシュボードにファイルとマルウェアの情報を表示させるには、ファイル ロギングを有効にする必要があります。



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、または [OK] をクリックして、後でタスク リストや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。この情報を評価して、ファイル伝送に関するセキュリティ上の予防策をネットワークにさらに追加すべきかどうか判断できます。

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。カテゴリ照合の場合は、許可またはブロックするサイトの関連レピュテーションも指定できます。該当するカテゴリとレピュテーションの URL をユーザが参照しようとすると、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 トラフィックを予期されるとおりに制御することが保証されます。さらに、シスコの脅威インテリジェンスは常に更新されて新しい URL が追加され、既存の URL も新しいカテゴリとリスクに更新されるため、システムでは常に最新情報を使用して要求対象のURLがフィルタ処理されます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表す悪意のあるサイトが現れては消えるペースが早すぎて、新しいポリシーを更新して導入するのが間に合わないこともあります。

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 [URL] ライセンスを有効にしていない場合は、有効にします。

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) [デバイス（Device）] をクリックします。
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。ライセンスが有効になっていることがグループに表示され、ボタンが [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 アクセス制御ルールを作成します。

ブロック ルールを作成する前に、まずユーザが表示しているサイトのカテゴリを確認します。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。

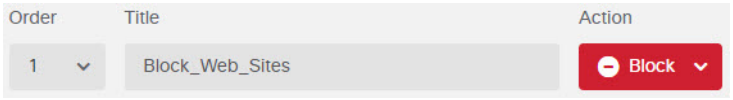
[アクセス コントロール（Access Control）] ポリシーが表示されていることを確認します。

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、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/宛先その他の基準に一致するルールよりも前（上）にこのルールを配置する必要があります。こうしないと、このルールは決して一致しません（各接続はテーブル内で最初に一致する 1 つのルールにのみ一致します）。このルールの場合、同じ [送信元/宛先（Source/Destination）] を、デバイスの初期設定時に作成された Inside_Outside_Rule として使用します。他のルールをすでに作成している場合もあります。アクセス制御の効率を最大にするには、接

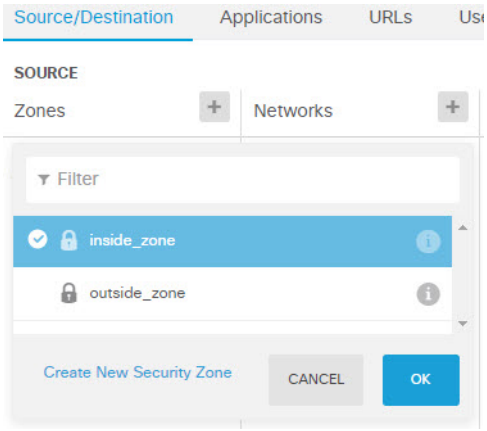
続の許可/ドロップを迅速に決定できるように特定のルールを早く適用するのが最善です。この例では、この目的でルールの順序として [1] を選択します。

- [タイトル（Title）]：ルールに Block_Web_Sites などのわかりやすい名前を付けます。
- [アクション（Action）]：[ブロック（Block）] を選択します。

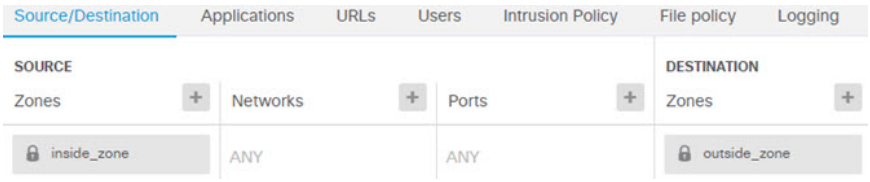


d) [送信元または送信先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の順に [+] をクリックし、inside_zone を選択して、[ゾーン（zones）] ダイアログボックスで [OK] をクリックします。

条件の追加も同じ方法です。[+] をクリックすると表示される小さいダイアログボックスで、追加する項目をクリックします。複数の項目をクリックしたり、選択されている項目をクリックして選択解除したりすることができます。チェック マークは選択されている項目を示します。ただし [OK] ボタンをクリックするまではポリシーには何も追加されません。単純に項目を選択するだけでは十分ではありません。



e) 同じ手法で、**[宛先（Destination）]** > **[ゾーン（Zones）]** に outside_zone を選択します。

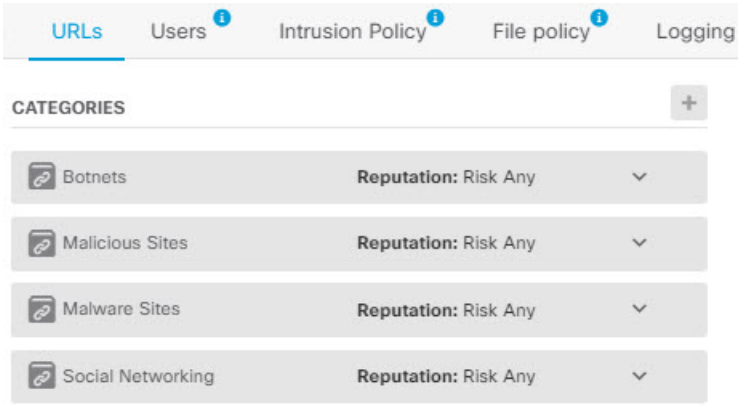


f) [URL] タブをクリックします。

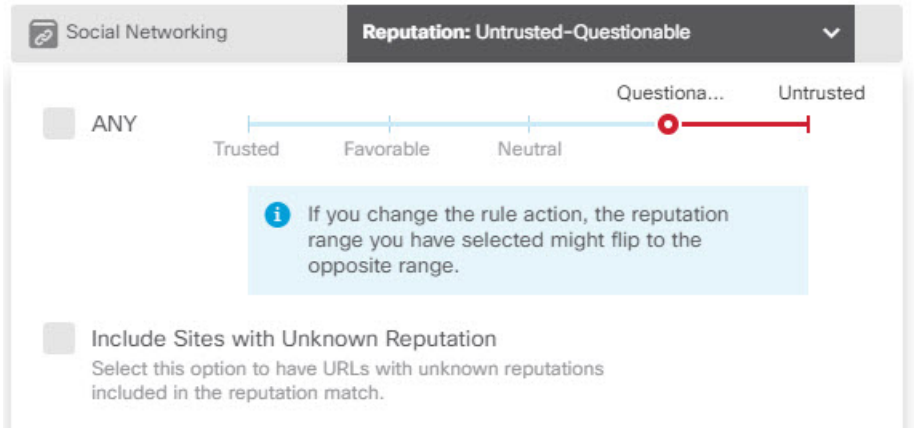
g) [カテゴリ（Categories）] の [+] をクリックし、完全にブロックするカテゴリまたは部分的にブロックするカテゴリを選択します。

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。他にもブロックできる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 スライダの左側に許可されるサイトが示され、右側にブロックされるサイトが示されます。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、ユーザは一般に利用されるソーシャル ネットワーキング サイト（リスクが少ないサイト）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して、許可するカテゴリ内のサイトを選択してブロックできます。

i) カテゴリ リストの左側にある [URL（URLS）] リストの横の [+] をクリックします。

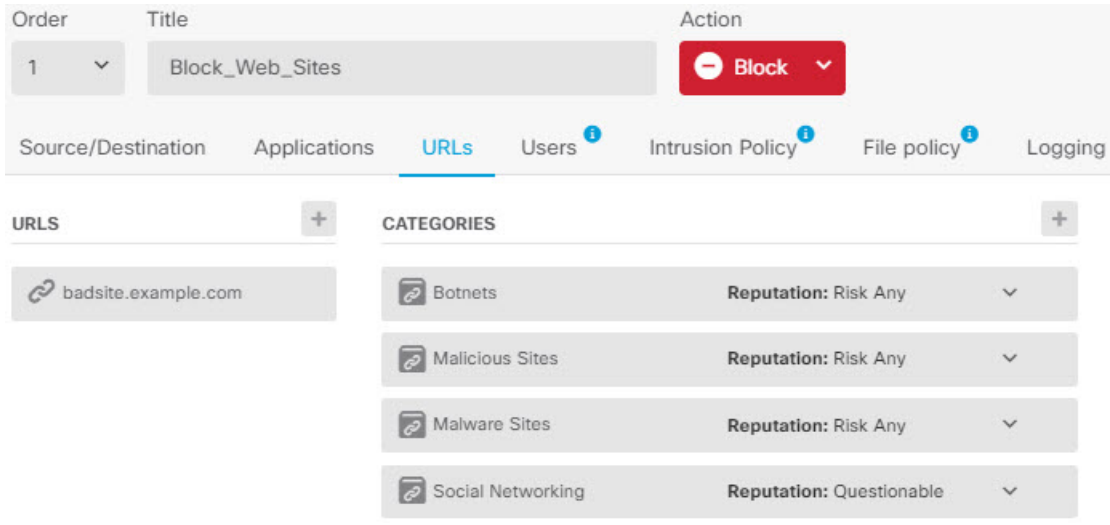
j) ポップアップ ダイアログ ボックスの下部で、[新規URLの作成（Create New URL）] リンクをクリックします。

k) 名前と URL の両方に **badsite.example.com** を入力し、[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 では、URL のプロトコル部分を含めず、サーバ名だけを追加します。

l) 新しいオブジェクトを選択して [OK] をクリックします。

ポリシーの編集中に新しいオブジェクトを追加すると、リストにオブジェクトが追加されます。新しいオブジェクトは自動的には選択されません。



m) [ロギング（Logging）] タブをクリックし、**[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）]** の順に選択します。

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 フィルタリングの設定を指定します。

[URL] ライセンスを有効にすると、Web カテゴリ データベースの更新が自動的に有効になります。通常、データが更新されるのは 1 日に 1 度ですが、システムは 30 分間隔で更新を確認します。何らかの理由でこれらの更新を実行しない場合には、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、または [OK] をクリックして、後でタスク リストや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。

Web サイトのカテゴリと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、ユーザに対して事前に通知することを検討してください。

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 プラットフォームの場合も、あるいは企業ネットワーク内外の伝送として Web プロトコルを使用するリッチ メディア アプリケーションの場合も、Web は企業内でアプリケーションを配信するユビキタス プラットフォームとなりました。

Threat Defense は接続を検査し、使用されているアプリケーションを判別します。これにより、特定の TCP/UDP ポートを対象とするだけではなく、アプリケーションを対象としたアクセス制御ルールを記述することが可能になります。したがって、複数の Web ベース アプリケーションが同じポートを使用する場合でも、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選択して許可またはブロックできることに加えて、種類、カテゴリ、タグ、リスク、ビジネスとの関連性などに基づき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関連性が低いすべてのアプリケーションを識別してブロックするアクセス制御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、システムや脆弱性データベース（VDB）の更新プログラムにより、追加のアプリケーション検出機能を頻繁に更新および追加しています。これにより、リスクの高いアプリケーションをブロックするルールが新しいアプリケーションに自動的に適用され、手動でルールを更新する必要がなくなります。

この事例では、[アノニマイザー/プロキシ（anonymizer/proxy）] カテゴリに属するすべてのアプリケーションをブロックします。

始める前に

この事例では、ネットワーク トラフィックを調べる方法 （7 ページ）にある事例をすでに完了したことを想定しています。前提となる事例では、アプリケーションダッシュボードで分析可能なアプリケーション使用状況に関する情報を収集する方法について説明しました。実際にどんなアプリケーションが使用されているか理解することにより、アプリケーションベースのルールを効率的に設計できます。その事例では、VDB 更新をスケジュールする方法についても説明しました（したがってここでは繰り返し説明しません）。アプリケーションが正しく識別されるように、VDB を定期的に更新してください。

手順

ステップ 1 アプリケーションベースのアクセス制御ルールを作成します。

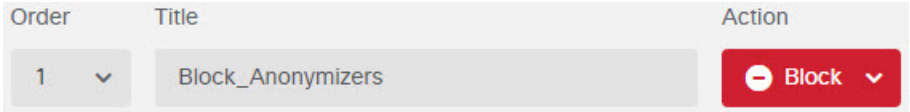
a) メイン メニューで [ポリシー（Policies）] をクリックします。

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

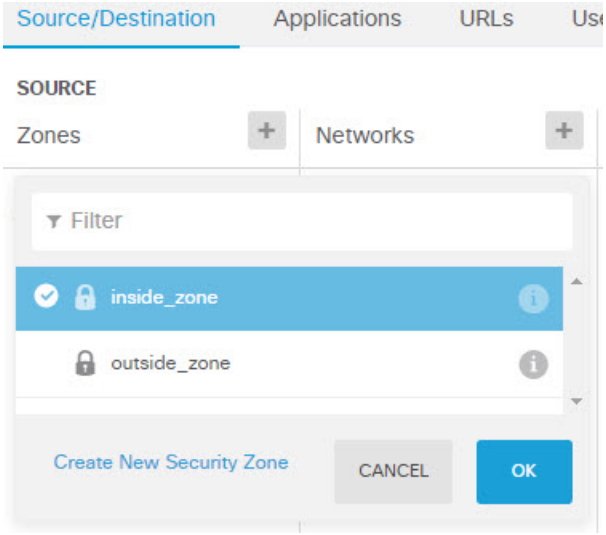
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、アクション を設定します。

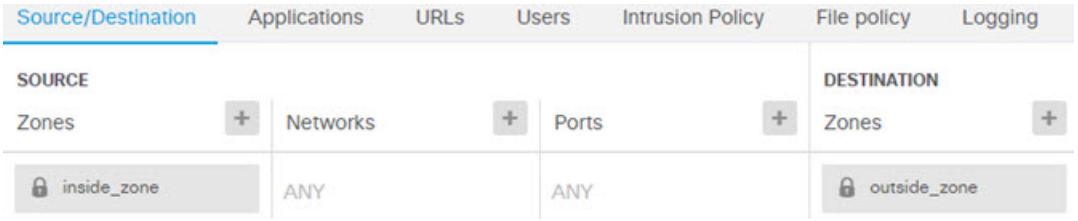
- [順序（Order）]：デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先その他の基準に一致するルールよりも前（上）にこのルールを配置する必要があります。こうしないと、このルールは決して一致しません（各接続はテーブル内で最初に一致する 1 つのルールにのみ一致します）。このルールの場合、同じ [送信元/宛先（Source/Destination）] を、デバイスの初期設定時に作成された Inside_Outside_Rule として使用します。他のルールをすでに作成している場合もあります。アクセス制御の効率を最大にするには、接続の許可/ドロップを迅速に決定できるように特定のルールを早く適用するのが最善です。この例では、この目的で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) [送信元または送信先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の順に [+] をクリックし、inside_zone を選択して、[ゾーン（zones）] ダイアログボックスで [OK] をクリックします。



e) 同じ手法で、**[宛先（Destination）]** > **[ゾーン（Zones）]** に 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。

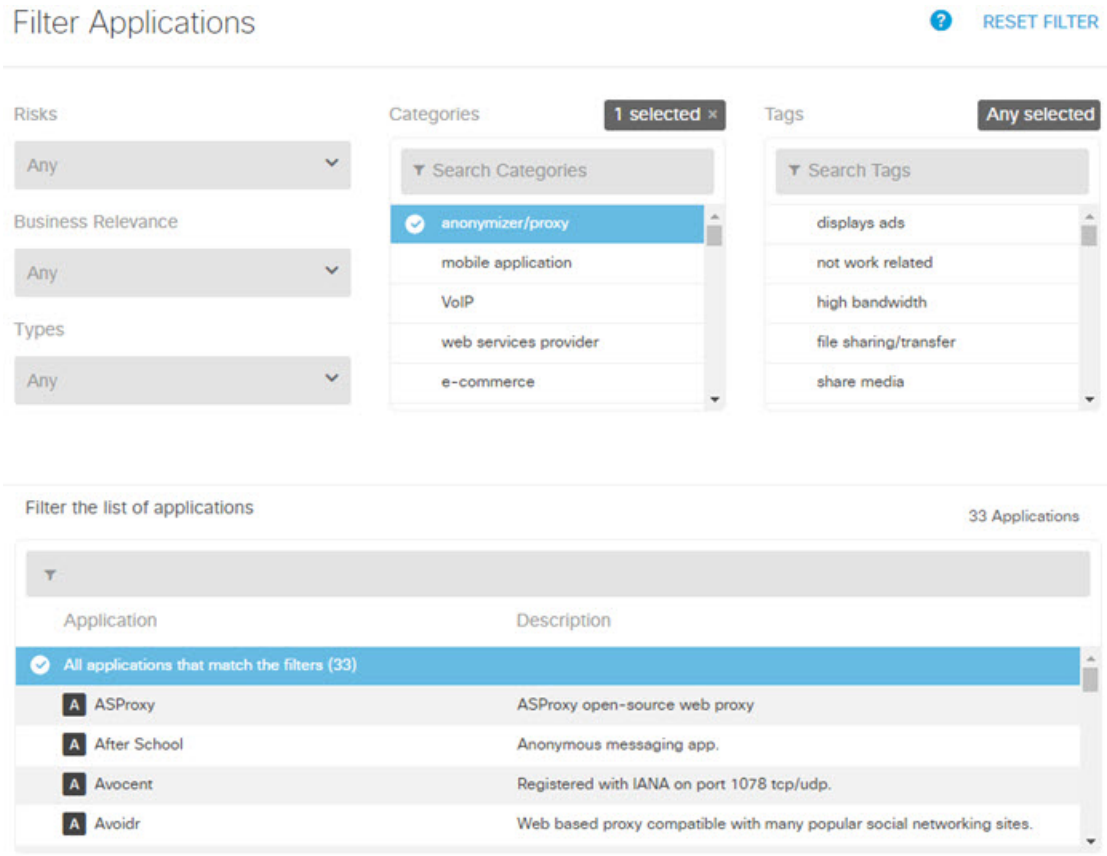
g) [アプリケーション（Applications）] で [+] をクリックしてから、ポップアップ ダイアログボックスの下部にある [高度なフィルタ（Advanced Filter）] リンクをクリックします。

アプリケーション フィルタ オブジェクトを事前に作成してこの [アプリケーション フィルタ（Application Filters）] リストでそれらを選択することもできますが、別の方法として、アクセス制御ルールで基準を直接指定し、オプションでその基準をフィルタ 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関するルールを記述している場合を除き、[高度なフィルタ（Advanced Filter）] ダイアログボックスでアプリケーションを見つけて適切な基準を作成する方が簡単です。

基準を選択すると、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、その基準に一致するアプリケーションが正確に表示されます。作成しようとしているルールは、これらのアプリケーションに適用されます。

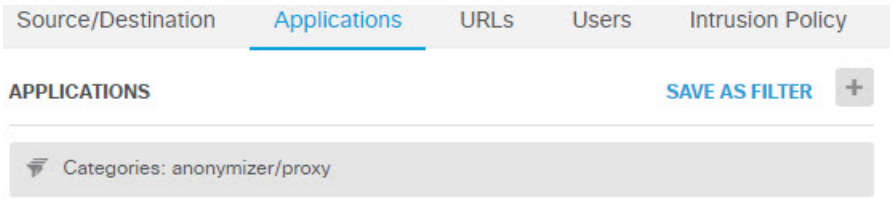
このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、TFPT は非常に高リスクに分類されています。ほとんどの組織は、このアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストは VDB 更新のたびに変更される可能性があることに注意してください。

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（anonymizers/proxies）] を選択します。



h) [高度なフィルタ（Advanced Filter）] ダイアログボックスで [Add（追加）] 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、**[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）]** の順に選択します。

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、または [OK] をクリックして、後でタスク リストや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。

ドロップされた接続があれば、[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（Applications）] ウィジェットにそれが表示されるようになります。ドロップされたアプリケーションだけに注目するには [すべて/拒否/許可（All/Denied/Allowed）] ドロップダウン オプションを使用します。

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。いずれかのユーザがこれらのアプリケーションの使用を試みた場合、アイデンティティ ポリシーが有効で認証が必要になっていれば、接続を試みたユーザとアプリケーションを相関させることができます。

サブネットの追加方法

デバイス上に利用可能なインターフェイスが存在する場合は、それをスイッチ（または別のルータ）に有線接続して別のサブネットにサービスを提供することができます。

さまざまな理由で、サブネットを追加する必要が生じることがあります。この事例では、次の典型的なシナリオを扱います。

- 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 が指定されています。この例では、この物理インターフェイスはネットワーク専用です。別のオプションとして、すでに有線接続されたインターフェイスを使用し、新しいネットワーク用のサブインターフェイスを作成する方法もあります。
- デバイスは DHCP を使用し、アドレス プール 192.168.2.2 ～ 192.168.2.254 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。
- 他の内部ネットワーク、および外部ネットワークに対するネットワーク アクセスは許可されます。外部ネットワークに向かうトラフィックは 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、未使用のインターフェイスがブリッジグループに含まれていないことを想定しています。現在、これがブリッジ グループのメンバーとなっている場合は、ブリッジ グループから削除した後で、この手順を進める必要があります。

始める前に

新しいサブネット用に、ネットワーク ケーブルを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

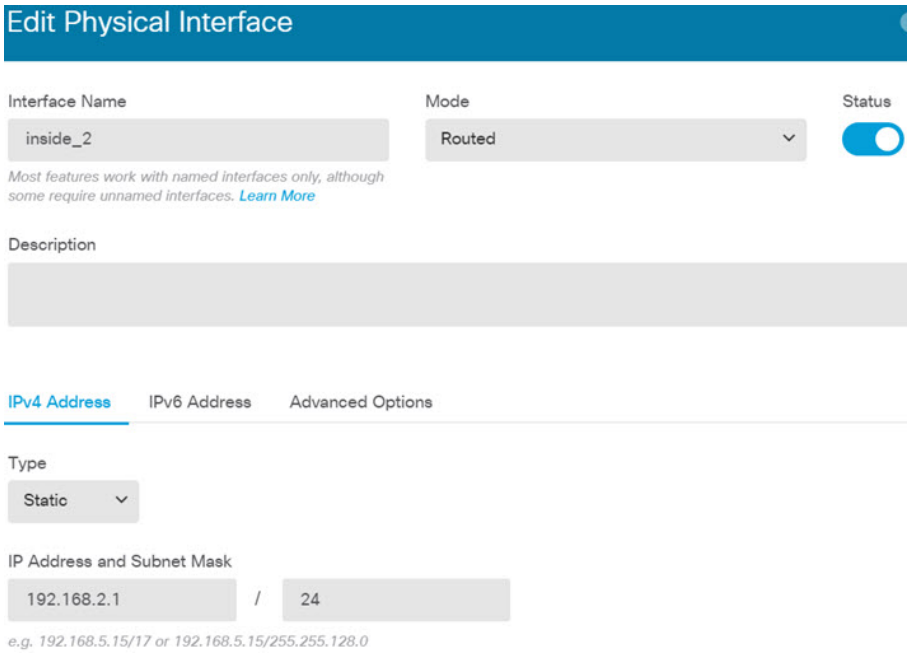
ステップ 1 インターフェイスを設定します。

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) 有線接続したインターフェイスの行の右側にある [アクション（Actions）] セルにマウスポインタを合わせ、編集アイコン（）をクリックします。

c) 基本的なインターフェイス プロパティを設定します。

- [名前（Name）]：インターフェイスの一意の名前。（[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：[種類（Type）] に [静的（Static）] を選択して、「192.168.2.1/24」と入力します。



d) [保存（Save）] をクリックします。

インターフェイスの一覧に、更新されたインターフェイスの状態と設定された 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。

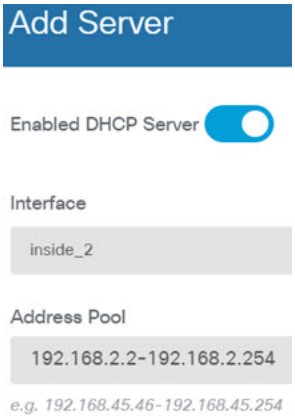
a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) **[システム設定（System Settings）] > [DHCPサーバ（DHCP Server）]** をクリックします。
c) [DHCP サーバ（DHCP Server）] タブをクリックします。

このテーブルには、既存のすべての DHCP サーバが一覧表示されます。デフォルト設定を使用している場合は、この一覧に内部インターフェイス用のものが 1 つ含まれます。

d) テーブルの上の [+] 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 サーバを有効にする]：サーバを有効にするにはこのトグルをクリックします。
- [インターフェイス（Interface）]：DHCP サービスを提供す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提供できるアドレス。「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）、およびブロードキャストアドレス（.255）は含めないでください。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。プールは連続するアドレスから

なる単一の範囲である必要があるため、スタティック アドレスを選択する際にはこの範囲の先頭または末尾から選択します。



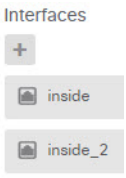
f) [追加（Add）] をクリックします。

#	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

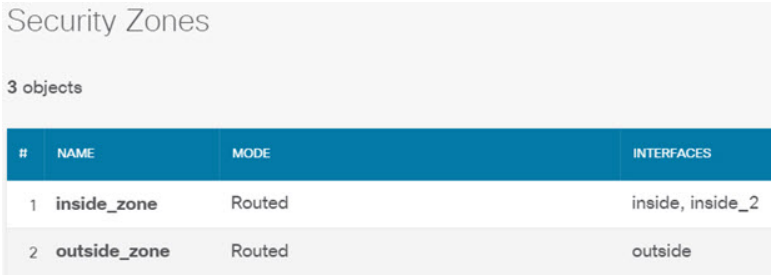
ステップ 3 インターフェイスを内部セキュリティ ゾーンに追加します。

インターフェイスのポリシーを作成するには、インターフェイスが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用のポリシーを作成します。このようにすると、ゾーン内でインターフェイスを追加または削除したときに、インターフェイスに適用されるポリシーが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) コンテンツ テーブルから [セキュリティ ゾーン（Security Zones）] を選択します。
c) [inside_zone（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 ポインタを合わせ、編集アイコン（  ）をクリックします。
d) [インターフェイス（Interfaces）] の下で [+] をクリックし、inside_2 インターフェイスを選択して、インターフェイスの一覧で [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制御ルールを作成します。

どのインターフェイス間でも、トラフィックは自動的には許可されません。必要なトラフィックを許可するためのアクセス制御（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、アクセス制御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た場合です。この例では、デバイス セットアップ ウィザードで設定されるブロック デフォルト アクションを保持しているものと想定します。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済みの場合は、この手順をスキップしてください。

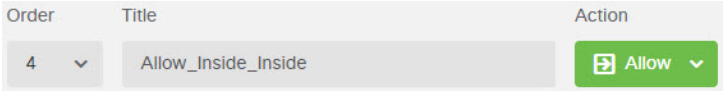
a) メイン メニューで [ポリシー（Policies）] をクリックします。

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

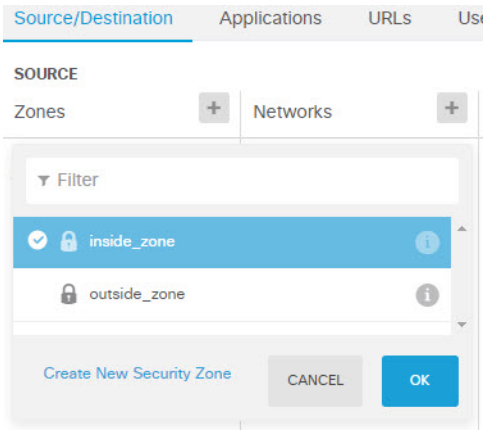
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、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/宛先その他の基準に一致するルールよりも前（上）にこのルールを配置する必要があります。こうしないと、このルールは決して一致しません（各接続はテーブル内で最初に一致する 1 つのルールにのみ一致します）。このルールの場合、一意の送信元/宛先基準を使用しているので、ルールを一覧の最後に追加しても構いません。
- [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。

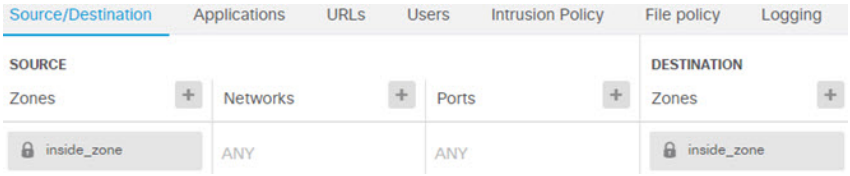


d) [送信元または送信先（Source/Destination）] タブで、**[送信元（Source）]**>**[ゾーン（Zones）]** の順に [+] をクリックし、inside_zone を選択して、[ゾーン（zones）] ダイアログボックスで [OK] をクリックします。



e) 同じ手法で、**[宛先（Destination）]** > **[ゾーン（Zones）]** に 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検査を設定します。

内部インターフェイスは信頼済みゾーンにありますが、ユーザがラップトップをネットワークに接続することがよくあります。したがって、ユーザはそれと知らずに、外部ネットワークや Wi-Fi ホット スポットからネットワーク内部に脅威を持ち込む可能性があります。このため、内部ネットワーク間でやり取りされるトラフィックに対して侵入やマルウェアのスキャンを実行するのが適切でしょう。

次を行うことを検討します。

- [侵入ポリシー（Intrusion Policy）] タブをクリックし、侵入ポリシーを有効化します。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（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、**[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）]** の順に選択します。

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。ロギングにより、ダッシュボードに統計が追加され、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 必要なポリシーが新しいサブネット用に定義されていることを確認します。

インターフェイスを inside_zone セキュリティ ゾーンに追加すると、inside_zone の既存のすべてのポリシーが新しいサブネットに自動的に適用されます。ただし、時間をかけてポリシーを検査し、ポリシーをさらに追加する必要がないことを確認してください。

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るはずです。

- [アクセス制御（Access Control）]：Inside_Outside_Rule は新しいサブネットと外部ネットワークの間のすべてのトラフィックを許可します。前述の事例に従って設定した場合は、ポリシーにより侵入/マルウェア検査も提供されます。新しい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を設定する必要があります。そうしないと、ユーザはインターネットその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向かうインターフェイスに適用され、インターフェイス PAT を適用します。このルールを保持した場合、新しいネットワークから外部に向かうトラフィックには、外部インターフェイスの IP アドレスで一意のポートに変換された IP アドレスが指定されます。外部インターフェイスに向かう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は、この時点でルールを作成する必要があるかもしれません。
- [アイデンティティ（Identity）]：デフォルトのアイデンティティ ポリシーは存在しません。ただし、前述の事例に従って設定した場合は、新しいネットワークの認証を要求するアイデンティティ ポリシーがすでに設定されているはずです。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、または [OK] をクリックして、後でタスク リストや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とイベント ビューアを使用して、ネットワーク使用状況を評価します。

ネットワークでトラフィックを受動的にモニタする方法

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 [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) 以下を設定します。

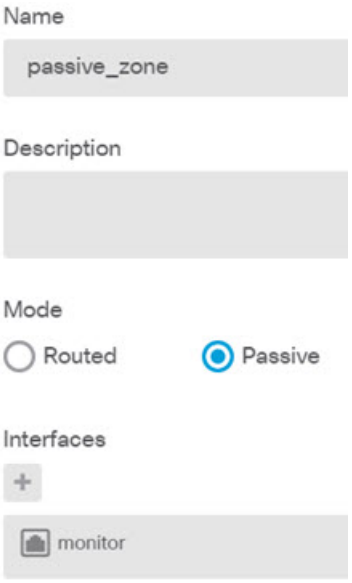
- [インターフェイス名（Interface Name）]：インターフェイスの名前（最大 48 文字）。英字は小文字でなければなりません。たとえば、**monitor** などです。

- [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、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。

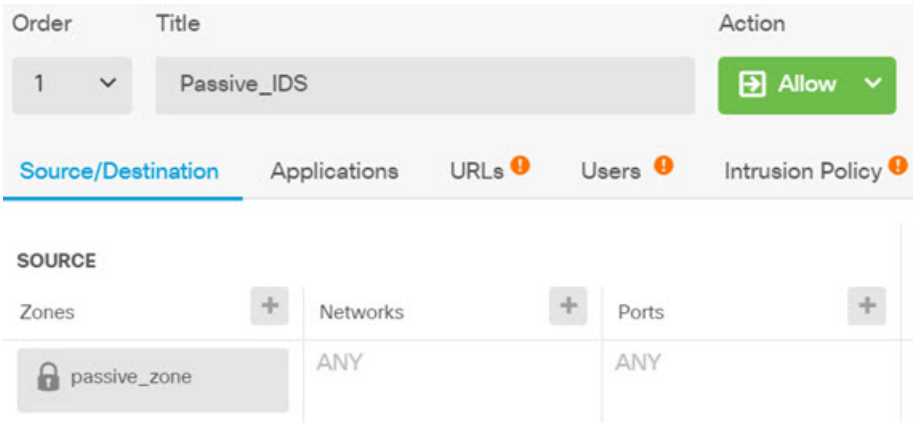
次の使用例では、アクセス制御ルールの主な使用方法について説明します。それらの使用例は、パッシブ インターフェイスにも当てはまります。作成するルールの送信元ゾーンとしてパッシブ セキュリティ ゾーンを選択します。

- 脅威のブロック方法 （15 ページ）
- マルウェアのブロック方法 （21 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）

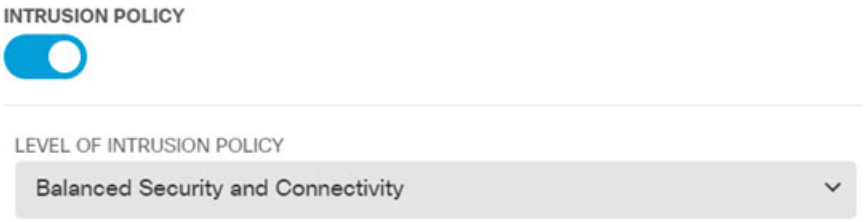
次の手順では、侵入ポリシーを適用して、URL カテゴリ データを収集する 2 つの [許可（Allow）] ルールを作成します。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** の順に選択します。
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) [送信元または宛先（Source/Destination）] タブで、**[送信元（Source）]**>**[ゾーン（Zones）]** の下でパッシブ 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。

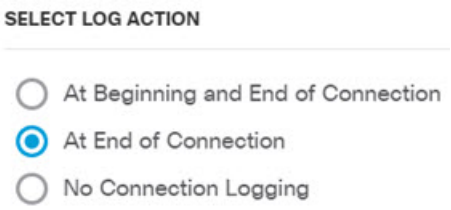
この時点で、評価モードで実行中のルールは次のようになります。



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（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）] タブをクリックして、ロギング オプションで [接続終了時（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。

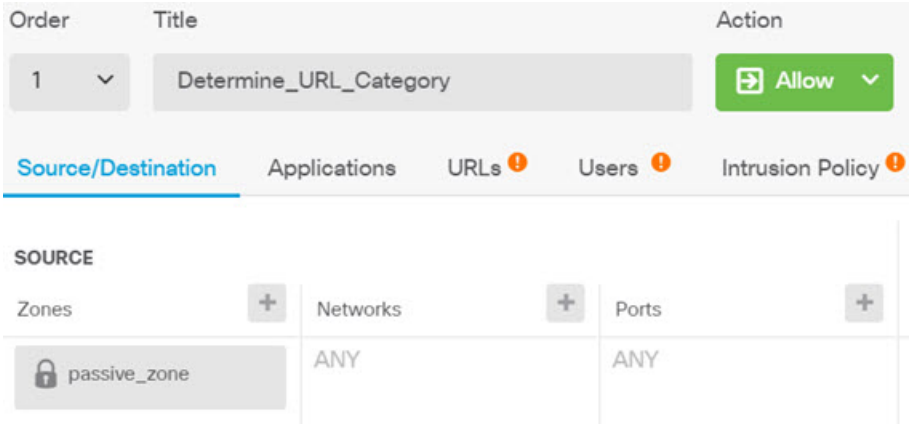
k) ルールの順序として [1] を選択します。これは、前のルール（Passive_IDS）の上に配置されます。（すべてのトラフィックに適用される）ルールの後に配置すると、今作成しているルールは決して一致しません。

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

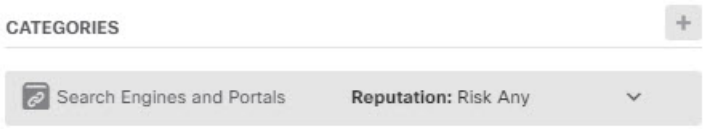
m) [アクション（Action）] として [許可（Allow）] を選択します。

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) [送信元または宛先（Source/Destination）] タブで、**[送信元（Source）]>[ゾーン（Zones）]** の下でパッシブ 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）] タブをクリックして、ロギング オプションで [接続終了時（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。詳細については、脅威のブロック方法 （15 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、または [OK] をクリックして、後でタスク リストや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

ネットワーク アドレス変換（NAT）

IPv4 アドレスの 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のための単一アドレス（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 トラフィックの免除

IPv6 アドレスの 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 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
- リモート アクセス VPN ユーザの外部インターフェイスでインターネット アクセスを実現する方法（ヘアピニング）
- リモート アクセス VPN を使用した外部ネットワークでのディレクトリ サーバの使用法
- 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 トラフィックの免除
- 外部サイト間 VPN ユーザの外部インターフェイスでインターネット アクセスを実現する方法（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

- 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。