Firepower Threat Defenseの使用例

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

- ネットワーク トラフィックを調べる方法，1 ページ
- 脅威をブロックする方法，9 ページ
- マルウェアをブロックする方法，13 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，17 ページ
- アプリケーションの使用を制御する方法，22 ページ
- サブネットを追加する方法，26 ページ

ネットワーク トラフィックを調べる方法

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

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

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

初期のアクセスルールでは、ポリシー、宛先、セキュリティゾーンなどのトラフィックについての情報が明らかになります。しかし、ユーザ情報を取得するには、ユーザを認証（識別）する必要があるアイデンティティ ポリシーを設定する必要があります。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、トラフックをモニタするように Firepower Threat Defenseデバイスを設定する方法を説明し、設定ポリシーおよびモニタリングポリシーのエンドツーエンドプロセスの概要を示します。

（注） この手順では、ユーザがアクセスしたサイトの Web サイト カテゴリおよびレピュテーションに関する情報は提供されないため、Web カテゴリ ダッシュボードに有意義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。この情報のみを取得する場合は、許容するカテゴリ（金融サービスなど）へのアクセスを許可する新規のアクセス 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することができます。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, （17 ページ）を参照してください。

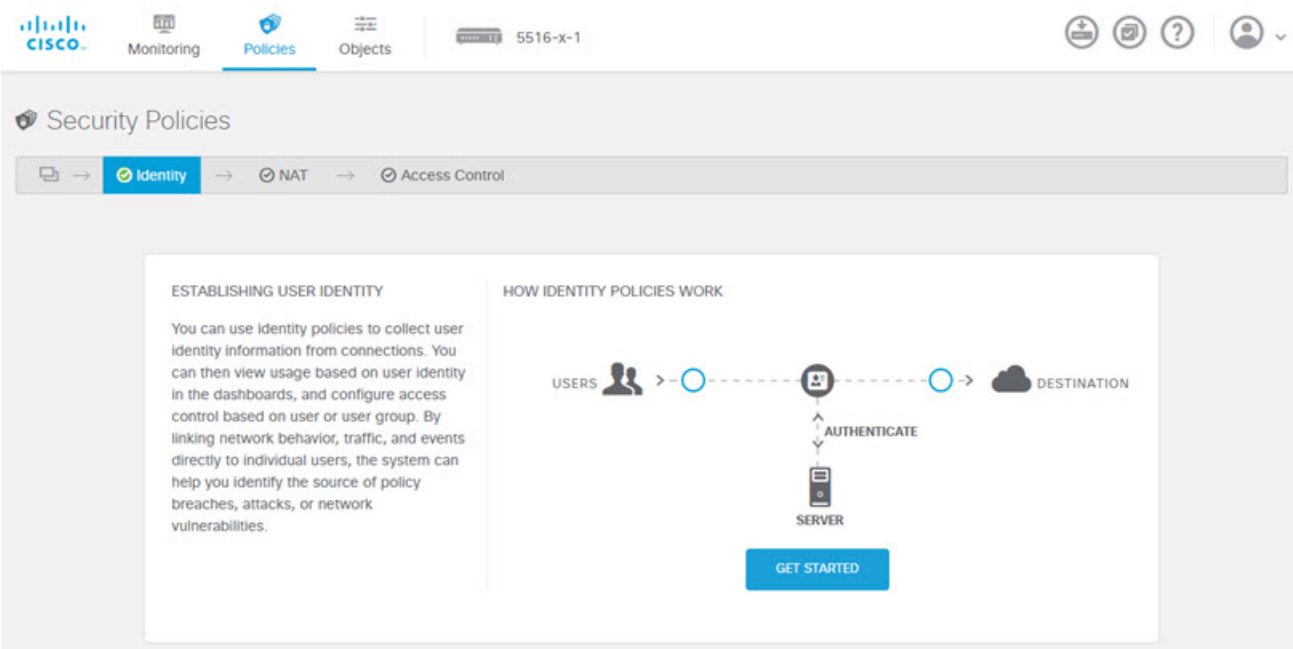
手順

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

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

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

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



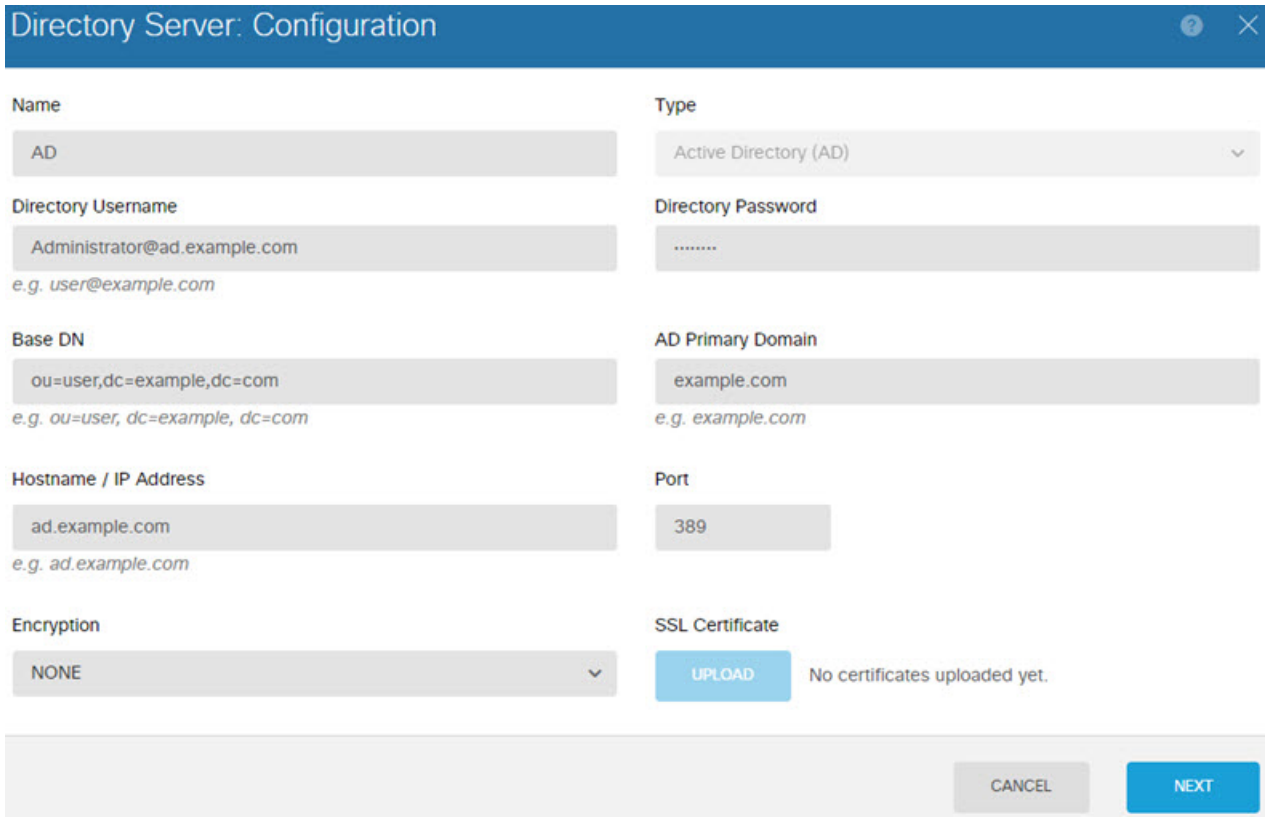
b) [スタート（Get Started）] ボタンをクリックし、ウィザードを起動して必要な要素を設定します。

c) アクティブ ディレクトリ サーバを特定します。
次の情報を入力します。

- [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。Active Directory がサポートされている唯一のタイプであり、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適切な権限を持っているユーザの識別用のユーザ名とパスワード。たとえば、admin@ad.example.com などです。
- [ベース DN（Base DN）] : ユーザおよびグループの共通の親である、ユーザおよびグループ情報を検索、または問い合わせるためのディレクトリ ツリー。たとえば、dc=example,dc=com などです。ベース DN の検索についての詳細は、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 などです。
- [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。サーバへ暗号化接続を使用している場合、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情報をダウンロードするために暗号化接続を使用するには、希望する方法、STARTTLS または LDAPSを選択します。デフォルトは [なし（None）]であり、ユーザおよびグループ情報はクリア テキストにダウンロードされることを意味します。
  - 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。
  - LDAPSでは LDAP over SSL が必要です。ポート 636 を使用します。
- [SSL 証明書（SSL Certificate）]：暗号化方式を選択したら、CA 証明書をアップロードしてシステムとディレクトリ サーバ間の信頼されてい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、証明書内で ad.example.com を使用した場合は、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。



d) [Next]をクリックします。

e) アクティブ認証のキャプティブ ポータルを設定します。
最もシンプルな方法は、すべてのフィールドをそのままにして[保存（Save）]をクリックします。アクティブ認証のデフォルトポートを設定します。ユーザは、ユーザ名とパスワードを提供するための信頼に必要な自己署名証明書を取得します。証明書を受け入れるようユーザに伝えます。

ただし、理想としては、ブラウザが信頼している証明書をアップロードします。証明書を持っている場合は、次のフィールドに入力して使用します。

- [サーバ証明書（Server Certificate）]：アクティブ認証の間にユーザに表示する CA 証明書。証明書は PEM または DER 形式の X509 証明書である必要があります。証明書に貼り付けるか、[証明書のアップロード（Upload Certificate）]をクリックして証明書ファイルを選択します。デフォルトでは、ユーザ認証時の自己署名証明書が表示されます。
- [証明書キー（Certificate Key）]：サーバ証明書のキー。キーに貼り付けるか、[キーのアップロード（Upload Key）]をクリックしてキー ファイルを選択します。
- [ポート（Port）]：キャプティブ ポータルのポート。デフォルトは 885（TCP）です。異なるポートを設定する場合、1025 ～ 65535 の範囲内とする必要があります。

f) [保存（Save）]をクリックします。
これで、セットアップ ウィザードが終了します。次に、アクティブ認証に必要なアイデンティティ ルールを作成します。

g) [アイデンティティ ルールの作成（Create Identity Rule）]ボタンをクリックするか、または [+] ボタンをクリックします。

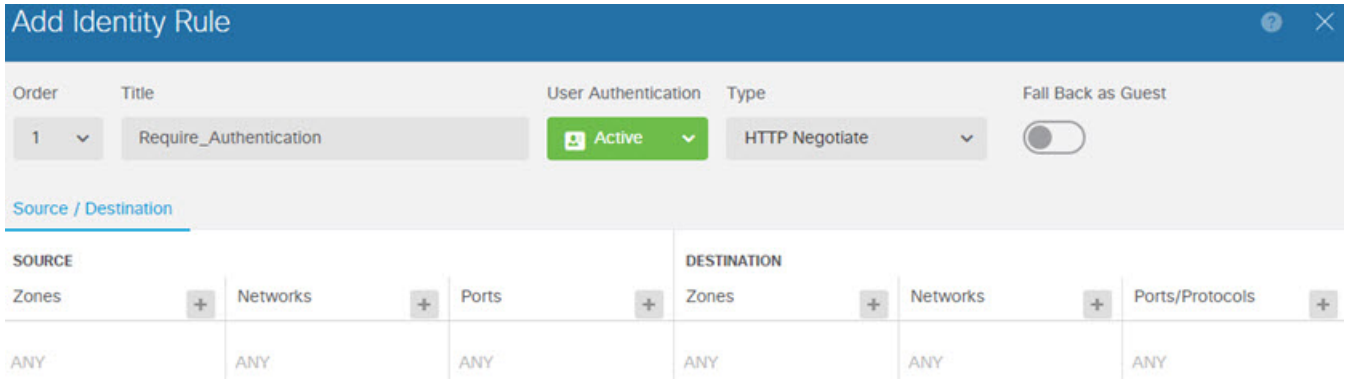
h) アイデンティティ ルールのプロパティを入力します。
全員を認証する必要があることを前提として、次の設定を使用できます。

- [名前（Name）]：任意の選択（Require_Authenticationなど）。
- [ユーザ認証（UserAuthentication）]：[アクティブ（Active）] が選択されているため、そのままにします。
- [タイプ（Type）]：[HTTPネゴシエート（HTTP Negotiate）]を選択します。これにより、ブラウザおよびディレクトリ サーバは最も強力な認証プロトコルを、NTLM、HTTPベーシックの順にネゴシエートできます。

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

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

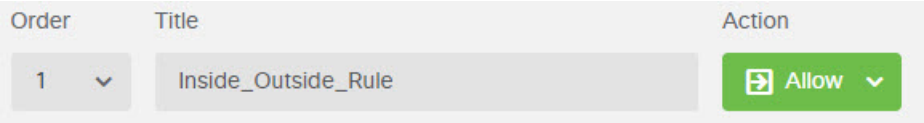
より制限されているトラフィックに合わせて、ポリシーに制約を加えることができます。ただし、アクティブ認証はHTTPトラフィックに対してのみ試行されるため、非HTTPトラフィックが送信元/宛先条件に一致していることは重要ではありません。アイデンティティ ポリシーのプロパティの詳細については、アイデンティティ ルールの設定を参照してください。



i) [OK（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。

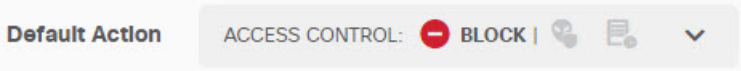
a) [ポリシー（Policies）]ページの[アクセス コントロール（Access Control）]をクリックします。
b) Inside_Outside_Rule行の右側にある[アクション（Actions）]セルにマウスを合わせると、編集アイコンと削除アイコンが表示されます。ルールを開くには、編集アイコン（）をクリックします。
c) [アクション（Action）]の[許可（Allow）]を選択します。



d) [OK（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。

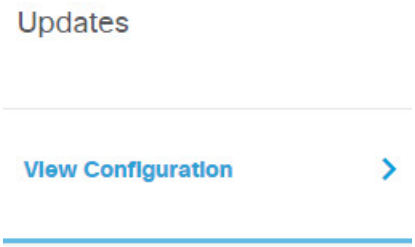
a) アクセス コントロール ポリシー ページの下部のデフォルト アクションで、任意の場所をクリックします。



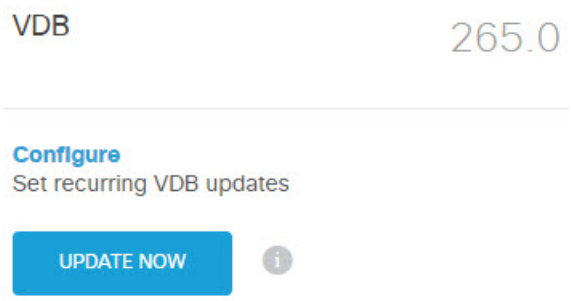
b) [ログ アクションの選択（Select Log Action）＞[接続の開始時および終了時（At Beginning and End of Connection）] を選択します。
c) [OK]をクリックします。

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することができます。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) [デバイス（Device）]メニューのデバイス名をクリックします。
b) [更新（Updates）] グループで [設定の表示（View Configuration）] をクリックします。

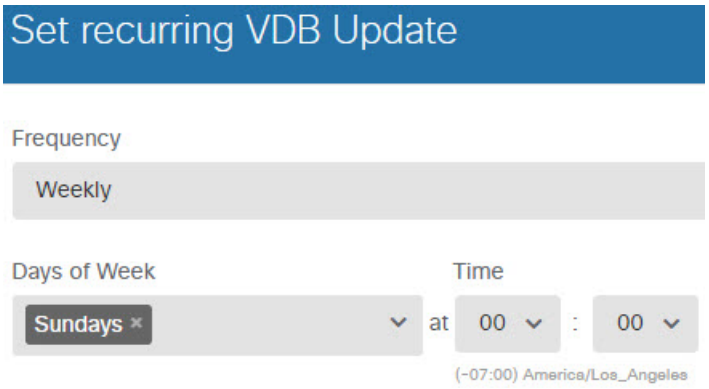


c) [VDB（VDB）] グループで [設定（Configure）]をクリックします。



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、実行して保存したけれども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。

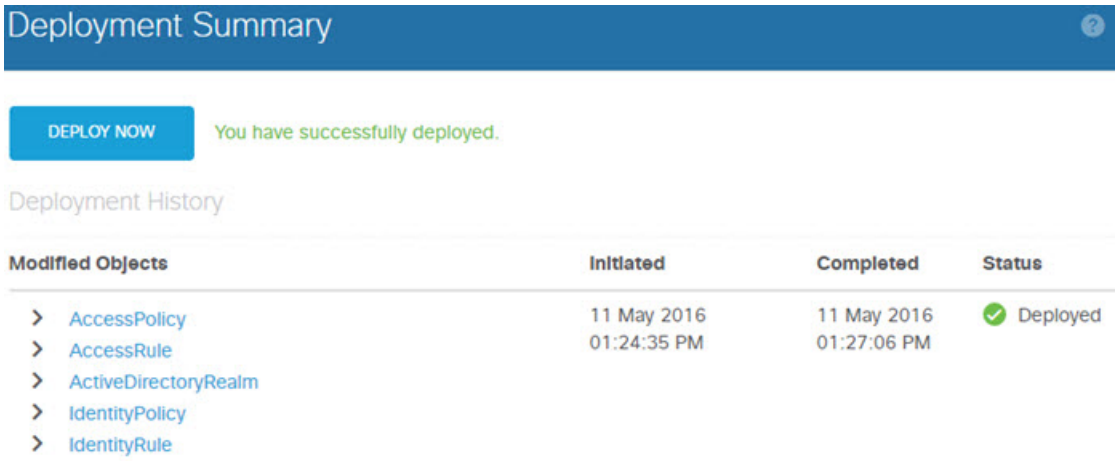


e) [保存（Save）]をクリックします。

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）]をクリックします。

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。



次の作業

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 ルールを展開することができます。

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 ポリシーを有効化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。

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

脅威をブロックする方法

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

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

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

Firepower システムでは、複数の侵入ポリシーが提供されています。これらのポリシーは、侵入ルールとプリプロセッサルールの状態を設定し、詳細設定を構成する Cisco Talos Security Intelligence and Research Group によって設計されています。

手順

ステップ 1 まだ有効化していない場合は、[脅威（Threat）]ライセンスを有効化します。
侵入ポリシーを使用するには、脅威ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイスアイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイスダッシュボードが開きます。

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。

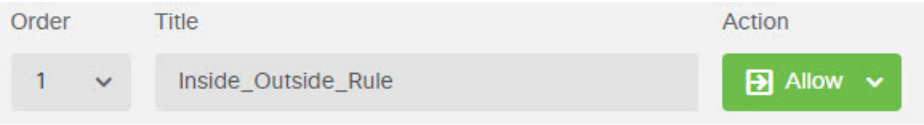
c) [脅威（Threat）]グループで [有効化（Enable）] をクリックします。
必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは[無効化（Disable）]ボタンに変わります。

ステップ 2 1 つまたは複数のアクセス ルールの侵入ポリシーを選択します。
脅威がないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule に侵入インスペクションを追加します。

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、編集アイコンと削除アイコンが表示されます。ルールを開くには、編集アイコン（）をクリックします。

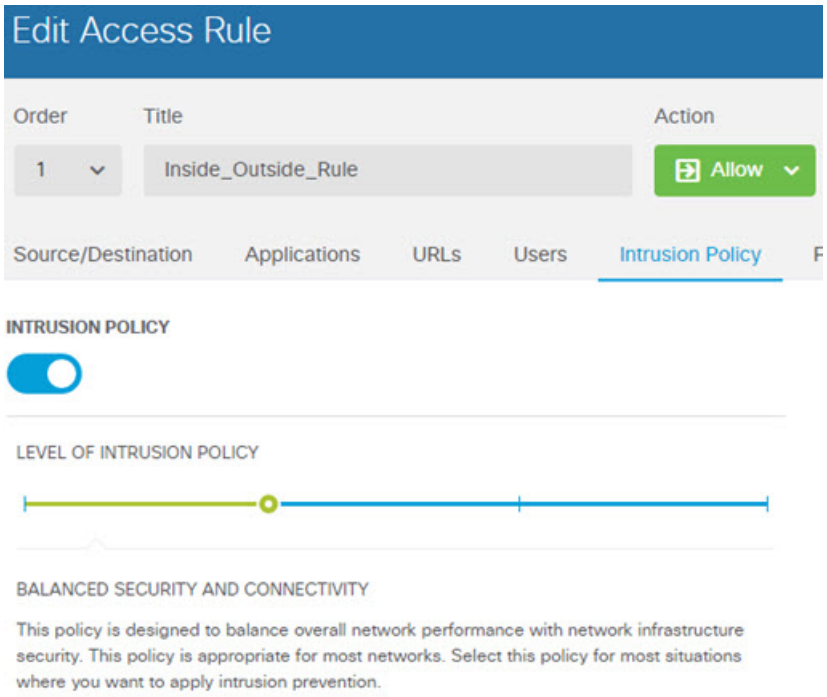
c) まだ選択していない場合は、[アクション（Action）]の [許可（Allow）] を選択します。



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有効化してから、スライダで侵入ポリシーのレベルを選択します。
ポリシーは、安全性の低いものから高いものへの順で表示されています。[セキュリティと接続のバランスをとる（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することができます。

セキュリティを強力にする必要がある場合は、[接続よりセキュリティを優先する（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。

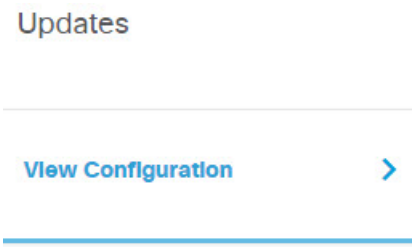


f) [OK（OK）]をクリックして変更を保存します。

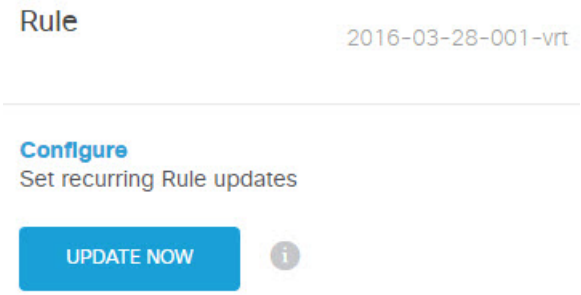
ステップ 3 侵入ルール データベースの更新スケジュールを設定します。
シスコは、接続をドロップするかどうかを決定する侵入ポリシーで使用される、侵入ルール データベースの更新を定期的にリリースしています。定期的にルール データベースを更新する必要があります。更新を手動でダウンロードするか、または定期的なスケジュールを設定することができます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、データベースの更新は無効化されているため、更新されたルールを取得するには操作を実行する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。

b) [更新（Updates）] グループで [設定の表示（View Configuration）]をクリックします。

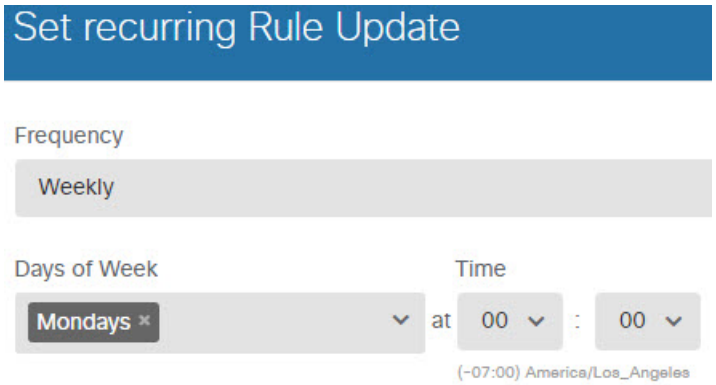


c) [ルール（Rule）] グループで [設定（Configure）]をクリックします。



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、実行して保存したけれども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) [保存（Save）] をクリックします。

ステップ 4 変更を保存します。

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

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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。

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、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、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。

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

Firepower の AMP では、AMP クラウドを使用してネットワーク トラフィックで検出される可能性のあるマルウェアの性質を取得します。AMP クラウドに到達してマルウェア ルックアップを実行するには、管理インターフェイスにインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドにクエリーします。可能性のある性質は、[クリーン（clean）]、[マルウェア（malware）]、または [不明（unknown）]（明確な判定を下せない）になります。 AMP クラウドに到達できない場合、性質は [不明（unknown）]になります。

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

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

手順

ステップ 1 まだ有効化していない場合は、[マルウェア（Malware）]ライセンスを有効化します。
マルウェア制御にファイルポリシーを使用するには、マルウェア ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイスアイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイスダッシュボードが開きます。

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。

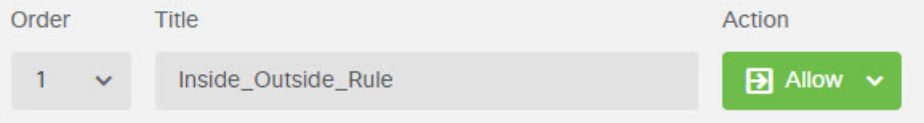
c) [マルウェア（Malware）]グループで [有効化（Enable）] をクリックします。
必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化（Disable）] ボタンに変わります。

ステップ 2 1 つまたは複数のアクセス ルールのファイル ポリシーを選択します。
マルウェアがないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule にファイル インスペクションを追加します。

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、編集アイコンと削除アイコンが表示されます。ルールを開くには、編集アイコン（）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。

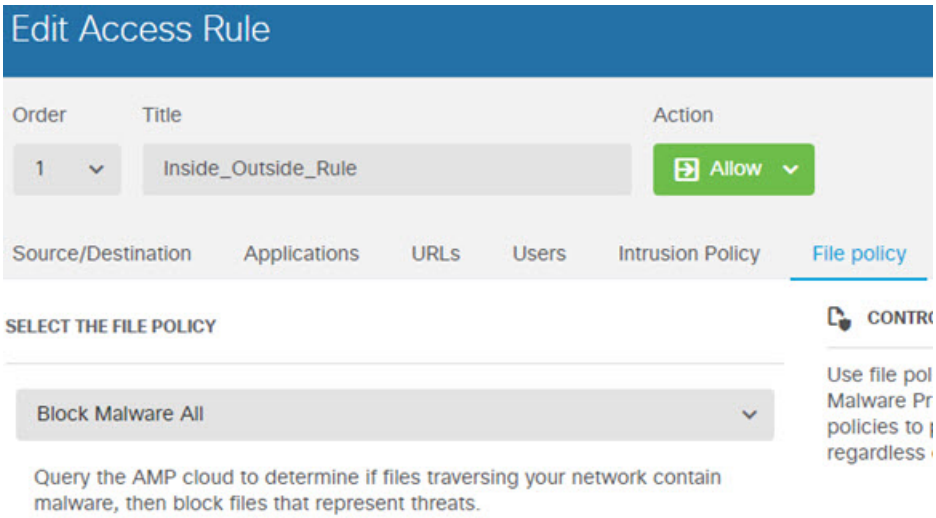


d) [ファイル ポリシー（File Policy）]タブをクリックします。

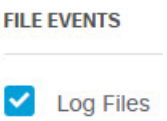
e) 使用するファイル ポリシーをクリックします。
主な選択は、マルウェアと見なされるすべてのファイルをドロップする [すべてのマルウェアをブロックする（Block Malware All）]、または AMP クラウドにクエリーしてファイルの性質を判断するけれどもブロックはしない [すべてのクラウド ルックアップを実行する（Cloud Lookup All）] です。ファイルがどのように評価されるかを確認する場合は、クラウド ルックアップを使用します。ファイルが評価される方法に納得したら、後でブロッキング ポリシーに切り替えることができます。

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、[すべてのマルウェアをブロックする（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 [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 ロギングを有効化する必要があります。



g) [OK（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）]をクリックします。

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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現れては消え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（URL）]ライセンスを有効化します。
Web カテゴリおよびレピュテーションの情報を使用するには、またはダッシュボードおよびイベントで情報を表示するには、URL ライセンスを有効化する必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイスアイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイスダッシュボードが開きます。

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

ステップ 2 URL フィルタリングのアクセス コントロール ルールを作成します。
ブロッキング ルールの作成前に、ユーザがアクセスしているサイトのカテゴリを最初に確認できます。その場合、許可するカテゴリ（金融サービスなど）に[許可（Allow）]アクションを設定したルールを作成できます。すべての Web 接続のインスペクションを実行して、URL がこのカテゴリに属しているかどうかを判断する必要があるため、金融サービス以外のサイトのカテゴリ情報も取得します。

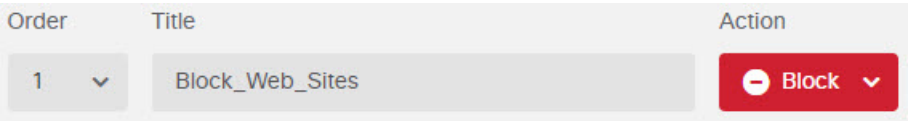
しかし、ブロックする必要があるとすでにわかっている Web カテゴリもあります。ブロッキング ポリシーでもインスペクションが強制されるため、ブロックされるカテゴリだけでなく、ブロックされないカテゴリへの接続に関するカテゴリ情報も取得します。

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。

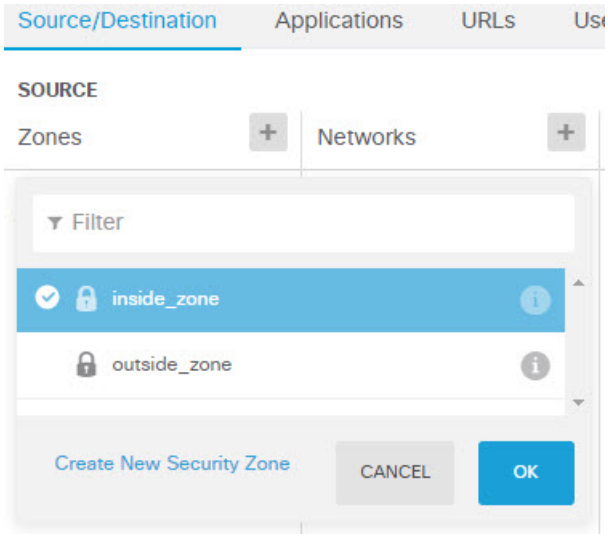
b) [+]をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

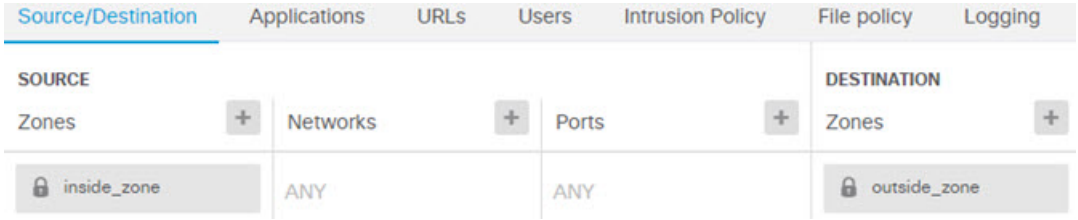
- [順序（Order）] : デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセス コントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを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/宛先（Source/Destination）] タブで、[送信元（Source）> [ゾーン（Zones）] の [+] をクリックし、[inside_zone（inside_zone）] を選択してからゾーンのダイアログ ボックスで [OK（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。

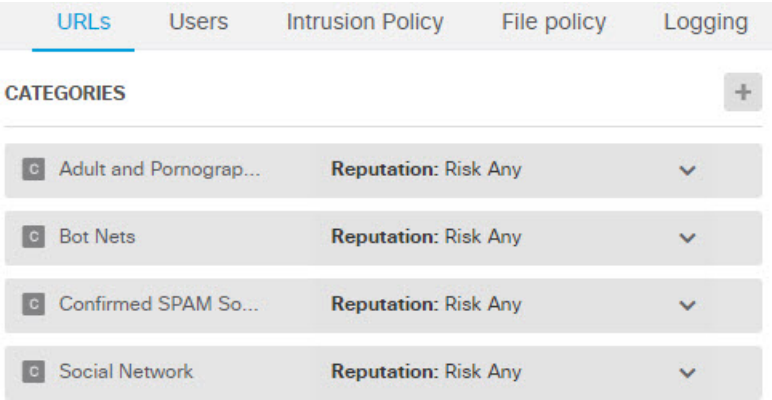


e) 同じ方法で、[宛先（Destination）] > [Zones（ゾーン）] の [outside_zone（outside_zone）] を選択します。

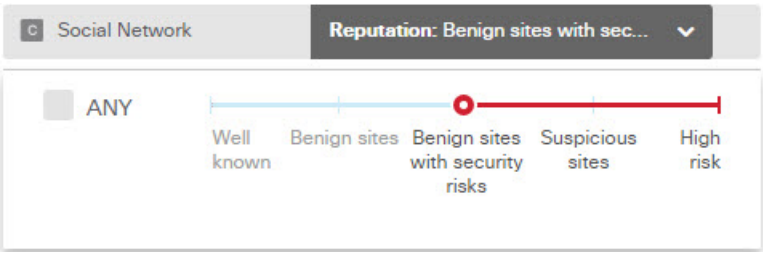


f) [URL（URLs）]タブをクリックします。
g) [カテゴリ（Categories）]の [+] をクリックして、完全または部分的にブロックするカテゴリを選択します。
この例では、[アダルトおよびポルノ（Adult and Pornography）]、[ボット ネット（Bot Nets）]、[確認済みのスパム送信元（Confirmed SPAM Sources）]、および [ソーシャル ネットワーク

（Social Network）] を選択します。ブロックすることが必要な可能性が高い追加カテゴリがあります。



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

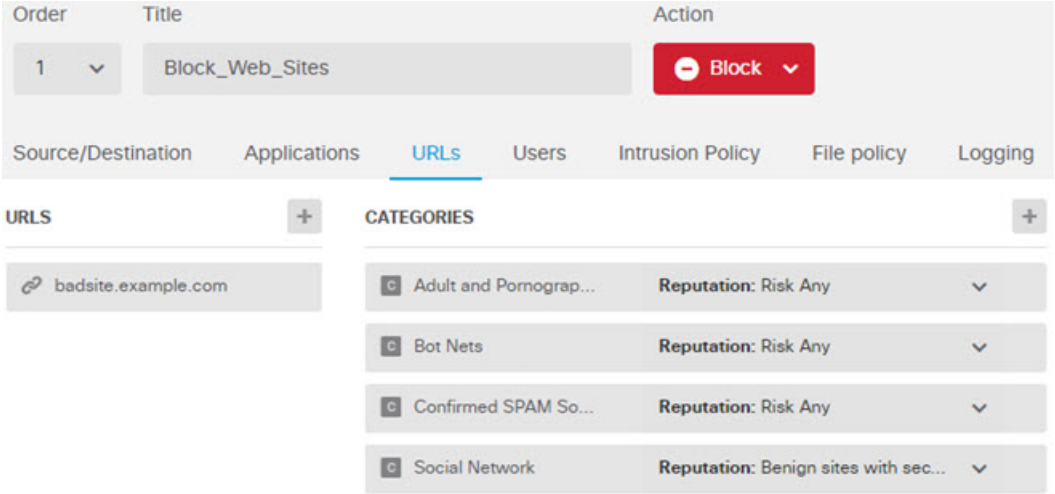


レピュテーション スライダの左側は許可されるサイトを示し、右側はブロックされるサイトを示します。この場合、レピュテーションが [疑わしいサイト（Suspicious Sites）] と [高リスク（High Risk）] の範囲内にあるソーシャル ネットワーキング サイトのみがブロックされます。したがって、ユーザは、リスクの少ない、一般的に使用されるソーシャル ネットワーキング サイトにはアクセスできます。

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

i) カテゴリ リストの左側にある [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」と入力して、[追加（Add）]、[OK（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（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）] > [接続の開始時および終了時（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（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、更新をオフにすることができます。

また、分類されていないURLを分析のためにシスコに送信するよう選択することもできます。これによって、ユーザがカテゴリおよびレピュテーションのない新しいサイトにアクセスすると、シスコはサイトを評価して分類し、レピュテーションを指定し、今後の更新に含めることができます。その後、新しい情報に基づいて、今後のサイトへのアクセスを許可またはブロックすることができます。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
b) [システム設定（System Settings）] > [トラフィック設定（Traffic Settings）] > [クラウド設定）Cloud Preferences] をクリックします。
c) [未知の URL 用 Cisco CSI のクエリー（Query Cisco CSI for Unknown URLs）]を選択します。
d) [保存（Save）]をクリックします。

ステップ 4 変更を保存します。

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

b) [今すぐ展開（Deploy Now）] ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

この時点から、監視ダッシュボードおよびイベントに Web カテゴリとレピュテーションに関する情報とドロップされた接続が表示されます。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、または企業ネットワークの内部および外部で転送として Web プロトコルを使用するリッチメディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになっています。

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

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。ユーザがそれらのアプリケーションの 1 つ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。

はじめる前に

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, （1 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

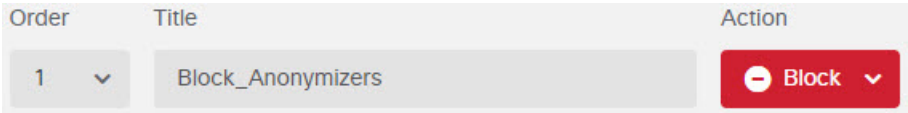
ステップ 1 アプリケーションベースのアクセス コントロール ルールを作成します。

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。

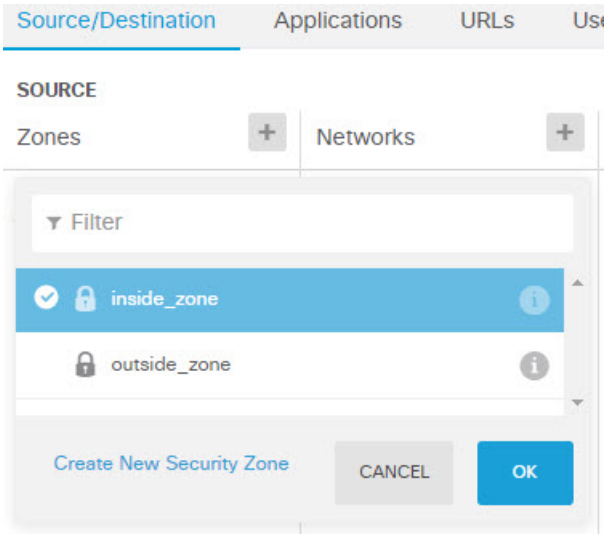
b) [+]をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

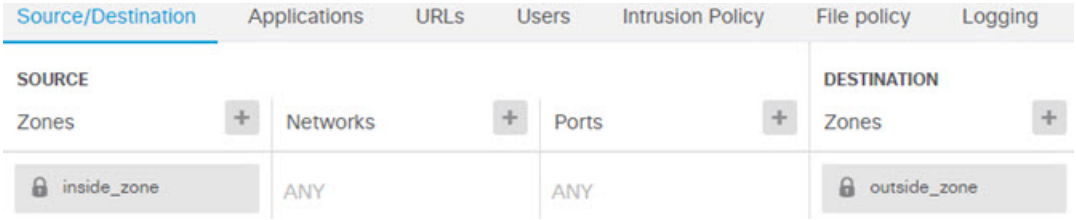
- [順序（Order）] : デフォルトで、新しいルールはアクセスコントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセス コントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅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



e) 同じ方法で、[宛先（Destination）]＞[Zones（ゾーン）] の [outside_zone（outside_zone）] を選択します。



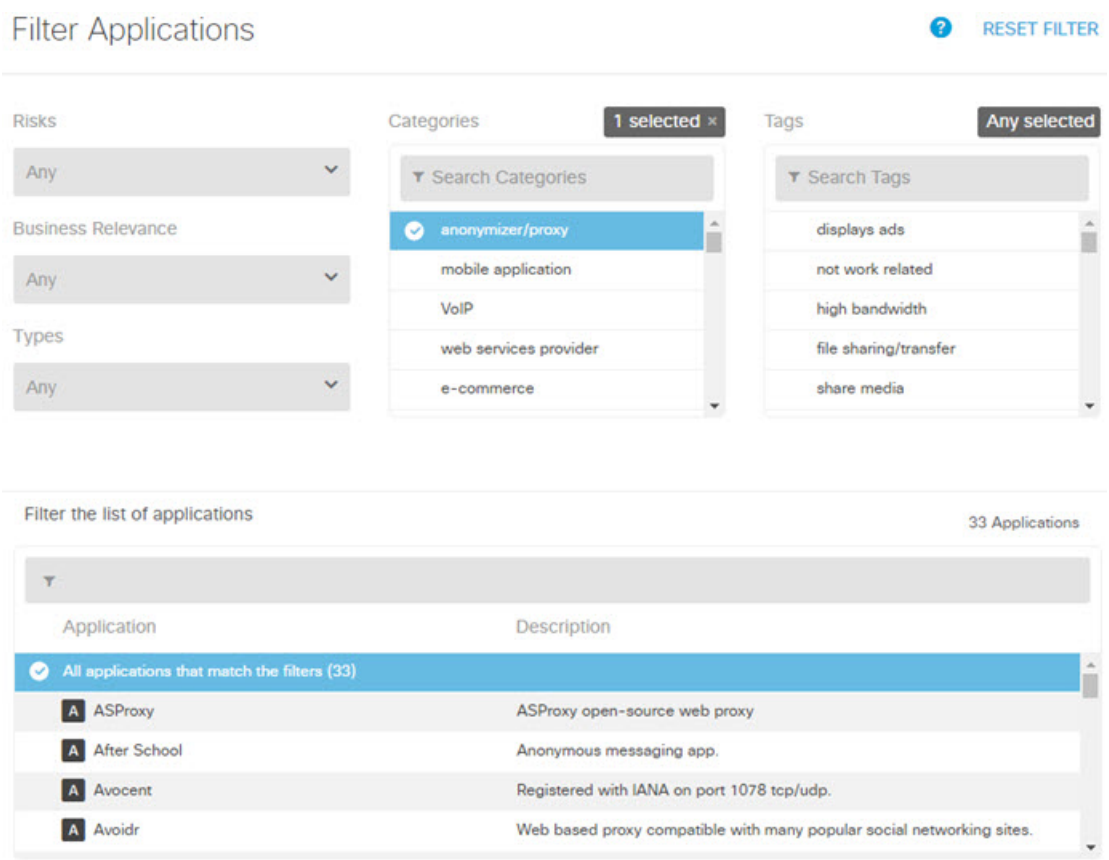
f) [アプリケーション（Applications）]タブをクリックします。

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することができます。

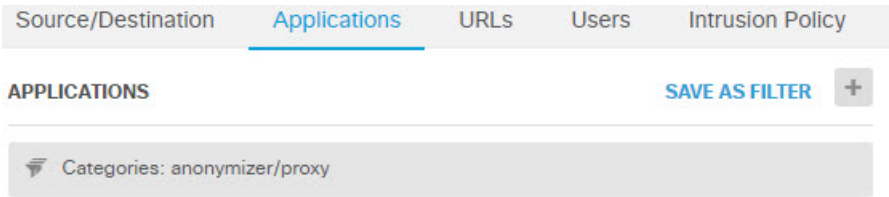
条件を選択すると、ダイアログ ボックスの下部にある [アプリケーション（Applications）] リストが更新され、条件に一致するアプリケーションが表示されます。記述したルールは、これらのアプリケーションに適用されます。

このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、Facebook および TFPT は非常に高リスクに分類されています。ほとんどの組織が、これらのアプリケーションをブロックすることは希望しません。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）] > [接続の開始時および終了時（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（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）]をクリックします。

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

ステップ 3 [モニタリング（Monitoring）]をクリックして、結果を評価します。
これで、[ネットワークの概要（Network Overview）] ダッシュボードのアプリケーション ウィジェットにドロップされた接続が表示されます。[すべて（All）]/[拒否（Denied）]/[許可（Allowed）] ドロップダウン オプションを使用して、ドロップされたアプリケーションのみに焦点を当てます。

[アプリケーション（Applications）]ダッシュボードにも、これら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することができます。

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。

はじめる前に

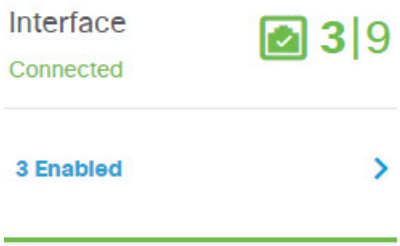
ネットワーク ケーブルを新しいサブネットのインターフェイスおよびスイッチに物理的に接続します。

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）]メニューのデバイス名をクリックします。
メニューには、デバイスのホスト名がラベル付けされたデバイスアイコンが表示されます。たとえば、次のリンクでは「5516-x-1」という名前のデバイスのデバイスダッシュボードが開きます。

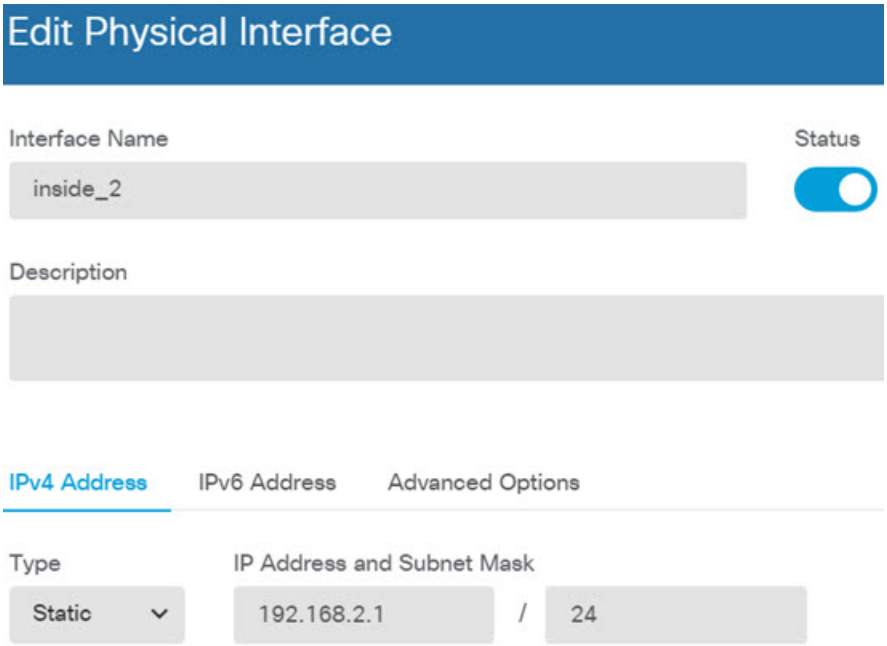
b) 有効なインターフェイスの数を示す[インターフェイス（Interfaces）]グループで、リンクをクリックします。
デバイス上のインターフェイスの合計数に対する有効なインターフェイスの数の概要が示されます。これは、モデルごとに異なります。この例では、9 個のうち 3 個のインターフェイスが有効です。



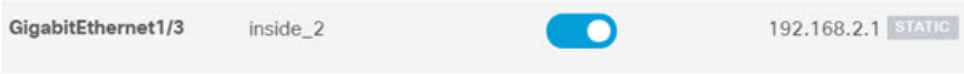
c) 接続しているインターフェイスの行の右側にある[アクション（Actions）]セルにマウスを合わせて、編集アイコン（）をクリックします。
d) 基本的なインターフェイスのプロパティを設定します。

- [名前（Name）]：インターフェイスに固有の名前（inside_2 など）。

- [ステータス（Status）]：ステータストグルをクリックして、インターフェイスを有効化します。
- [IPv4 アドレス（IPv4 Address）]タブ：[タイプ（Type）] に [スタティック（Static）] を選択して、192.168.2.1/24 を入力します。



e) [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。

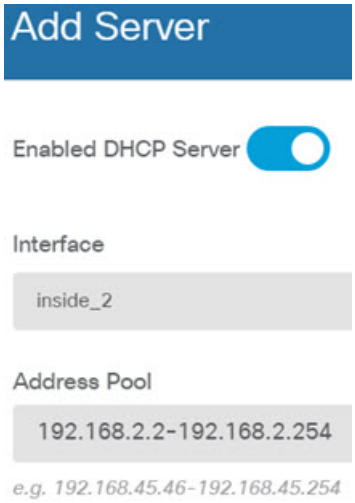


ステップ 2 インターフェイスの DHCP サーバを設定します。

a) [デバイス（Device）]メニューのデバイス名をクリックします。
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 サーバの表までスクロール ダウンして、表の上部の [+]をクリックします。
d) 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（AddressPool）]：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。



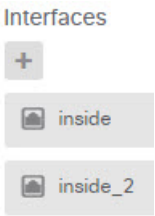
e) [追加（Add）]をクリックします。

#	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（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（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。

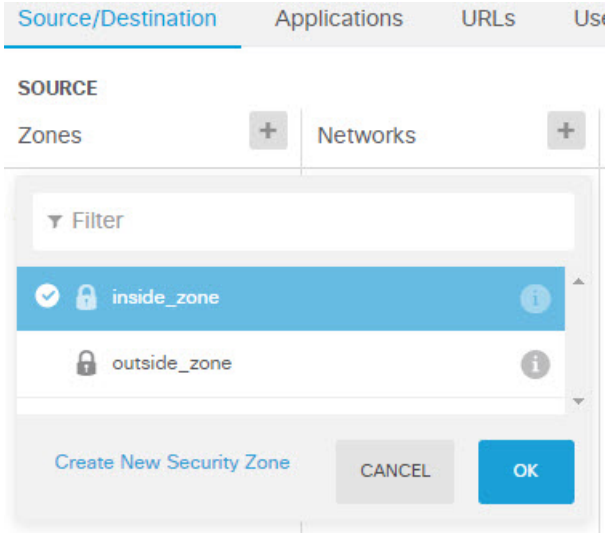
a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されることを確認します。

b) [+]をクリックして新しいルールを追加します。

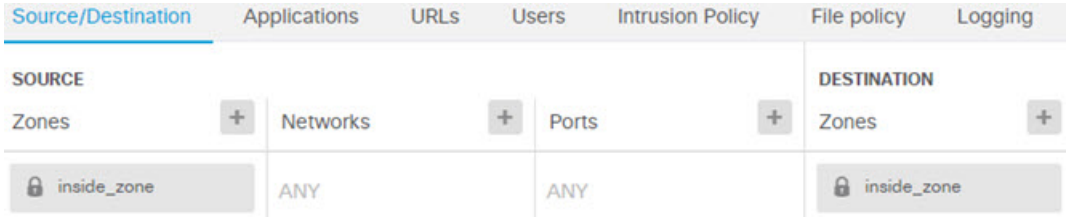
c) 順序、タイトル、およびアクションを設定します。

- [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）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することができます。
- [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/宛先（Source/Destination）]タブで、[送信元（Source）＞[ゾーン（Zones）] の [+] をクリックし、[inside_zone（inside_zone）] を選択してからゾーンのダイアログ ボックスで [OK（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（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する必要がある場合があります。

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 [セキュリティと接続のバランスをとる（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（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（AccessControl）] : 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（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）]をクリックします。

b) [今すぐ展開（Deploy Now）]ボタンをクリックして、展開が完了するまで待ちます。
展開のサマリに変更が正常に展開されたことが示され、ジョブのタスク ステータスが [展開済み（Deployed）] になります。

次の作業

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。