FirePOWER Threat Defenseの使用例

ここでは、FirePOWER Threat Defenseで Firepower Device Manager を使用して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を完了し、その初期設定を維持していることを前提としています。初期設定を変更している場合でも、これらの例を参照することは、製品の使用方法を理解する上で役立つはずです。

ネットワーク トラフィックを調べる方法

デバイスの初期設定を完了すると、インターネットまたはその他のアップストリーム ネットワークへのすべての内部トラフィック アクセスを許可するアクセス コントロール ポリシーと、他のトラフィックすべてをブロックするデフォルトアクションが設定されます。付加的な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の状況を知ることは有益です。

ネットワーク トラフィックの分析には、FirePOWER デバイス マネージャのモニタリング機能を利用できます。FirePOWERデバイスマネージャのレポートは、次の質問の答えを得るのに役立ちます。

- 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

- 最も多く適用されているアクセス コントロール ルール（ポリシー）

最初のアクセスルールは、ポリシー、接続先、セキュリティゾーンを含むトラフィックに関するいくらかの情報を提供できます。しかし、ユーザ情報を取得するには、ユーザ自身を認証（特定）するよう求め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、いくらかの付加的な調整が必要です。

次の手順で、FirePOWER Threat Defenseデバイスがトラフックをモニタするように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） この手順は、ユーザが参照するサイトの Web サイト カテゴリとレピュテーションについて理解する手がかりにはならないため、Web カテゴリ ダッシュボードで有意義な情報を得ることはできません。カテゴリおよびレピュテーション 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行して、URL ライセンスを有効にする必要があります。この情報を取得するには、許容されるカテゴリ（[金融サービス（Financial Services）] など）へのアクセスを許可する新しいアクセス コントロール ルールを追加し、このルールをアクセス コントロール ポリシーの最初のルールにします。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。

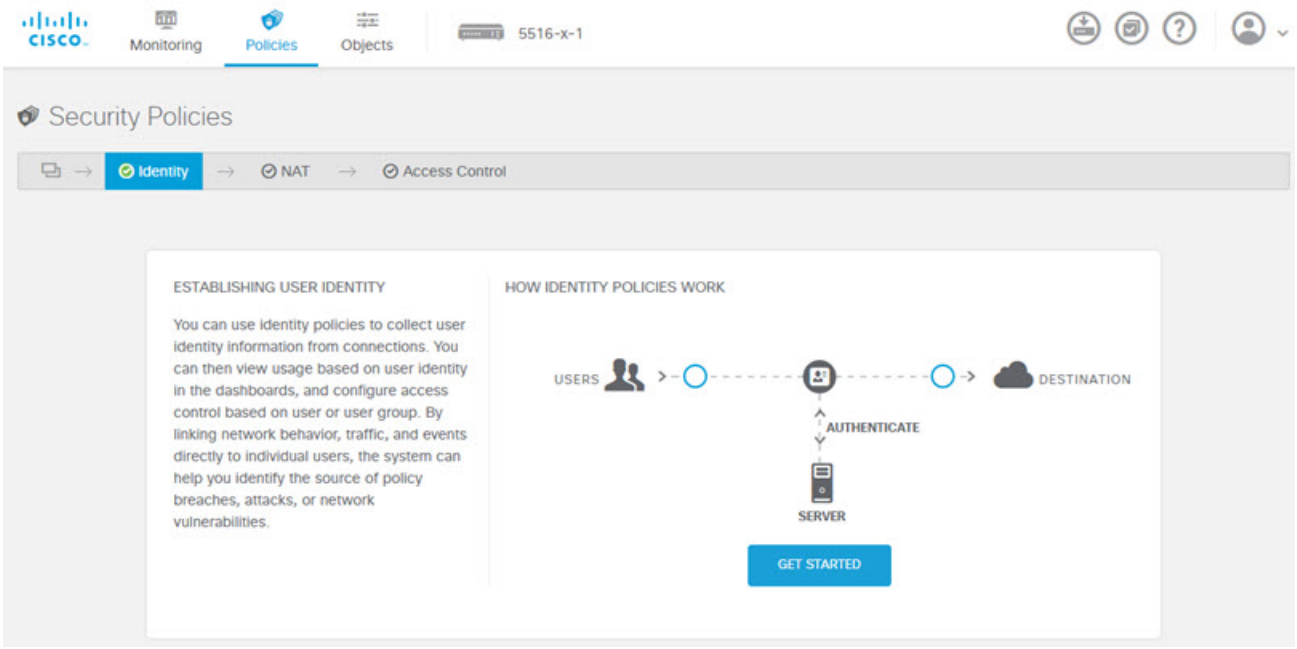
手順

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 ポリシーを有効にすることにより、だれがネットワークを使用しているか、使用されているリソースは何かに関する情報を収集できます。この情報は、ユーザ監視ダッシュボードで入手できます。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使用できます。

ユーザは、HTTP 接続のために Web ブラウザを使用する際に認証されます。

認証に失敗したユーザが Web 接続を阻止されることはありません。これは、単に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）]をクリックしてから、[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、初期状態では無効になっています。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、使用中のワークステーションの IP アドレスにユーザを関連付けます。その後、システムは、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特定します。



b) [開始（Get Started）]ボタンをクリックして、必要な要素を設定するウィザードを開始します。

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。

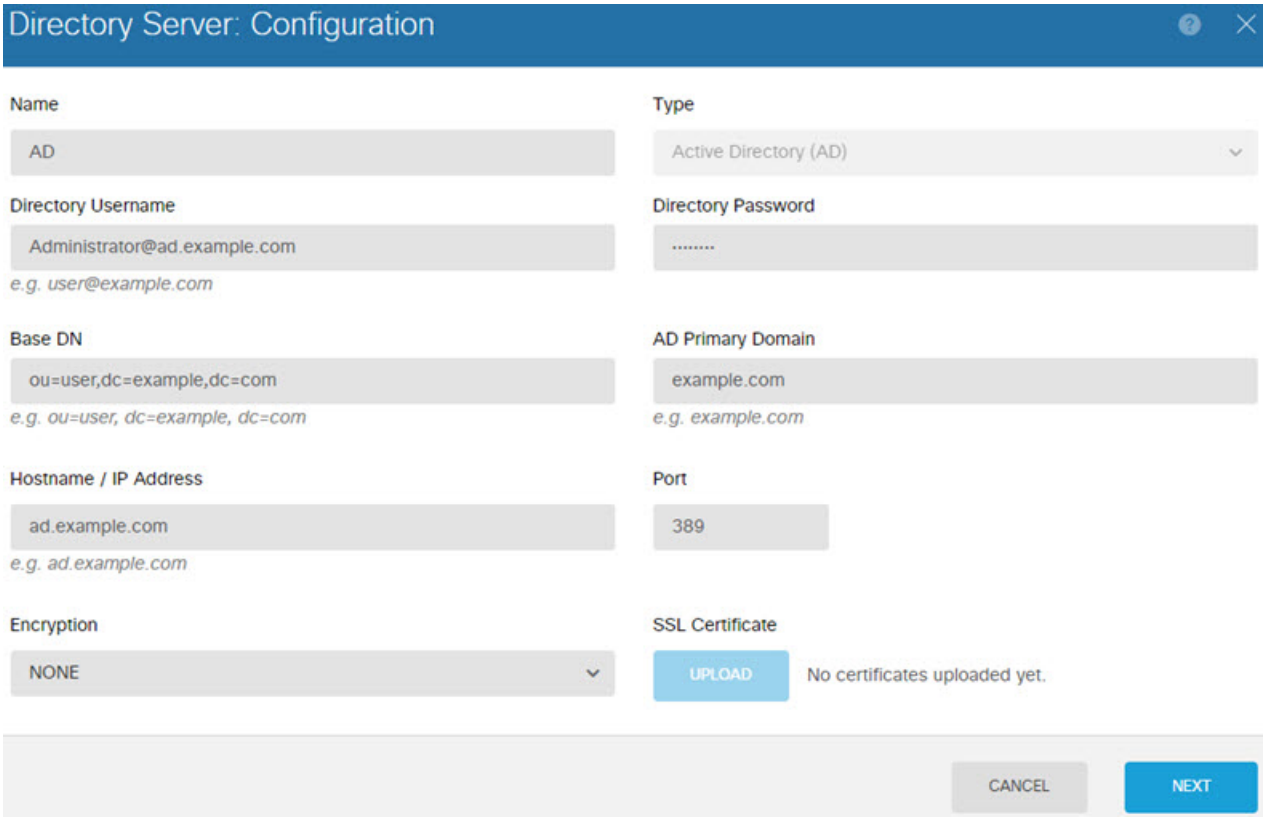
- 名前（Name）：ディレクトリ レルムの名前。
- タイプ（Type）：ディレクトリ サーバのタイプ。Active Directory が唯一サポートされているタイプであり、このフィールドは変更できません。
- ディレクトリ ユーザ名（Directory Username）、ディレクトリ パスワード（Directory Password）：取得するユーザ情報に対する適切な権限を持つユーザの識別ユーザ名とパスワード。たとえば、admin@ad.example.com。
- ベース DN（Base DN）：ユーザおよびグループ情報を検索またはクエリするためのディレクトリ ツリー、つまり、ユーザとグループの共通の親。たとえば、dc=example、dc=com。ベース DN の検索方法の詳細については、ディレクトリ ベースの DN の決定を参照してください。
- AD プライマリ ドメイン（AD Primary Domain）：デバイスが参加する必要のある完全修飾 Active Directory ドメイン名。たとえば、example.com。
- ホスト名/IP アドレス（Hostname/IP Address）：ディレクトリ サーバのホスト名または IP アドレス。サーバへの暗号化された接続を使用している場合は、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されるポート番号。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された接続を使用するには、目的の方式 [STARTTLS] または [LDAPS] を選択します。デフォ

ルトは [なし（None）]で、ユーザおよびグループ情報はクリア テキストで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て、ディレクトリ サーバによってサポートされている最強の方式を使用します。ポート 389 を使用します。
- [LDAPS]には、LDAP over SSL が必要です。ポート 636 を使用します。

- SSL証明書（SSL Certificate）：暗号化方式を選択する場合は、システムとディレクトリ サーバ間の信頼できる接続を有効にするため、CA 証明書をアップロードします。証明書を使用して認証している場合は、証明書のサーバ名がサーバのホスト名/IP アドレスと一致している必要があります。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、次のイメージは、ad.example.com サーバへの非暗号化接続を作成する方法を示しています。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。すべてのユーザ情報とグループ情報は、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) アクティブ認証キャプティブ ポータルを設定します。
最も簡単なオプションは、すべてのフィールドをそのままにして[保存（Save）]をクリックすることです。アクティブ認証のデフォルト ポートを設定した場合、ユーザは、自分のユーザ名とパスワードを提供するために信頼する必要のある自己署名証明書を取得します。そうなることが予想されることと、ユーザは証明書を承認する必要があることをユーザに知らせてください。

とはいえ、ブラウザがすでに信頼した証明書をアップロードすることが理想的です。証明書が存在する場合、その証明書を使用するには、次のフィールドに入力します。

- サーバ証明書（Server Certificate）：アクティブ認証時にユーザに提供される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。証明書を貼り付けるか、または[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、ユーザ認証時に自己署名証明書を提供します。
- 証明書キー（Certificate Key）：サーバ証明書のキー。キーを貼り付けるか、または[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 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は、1025 ～ 65535 の範囲内にする必要があります。

f) [Save]をクリックします。
これにより、セットアップ ウィザードが実行されます。次に、アクティブ認証を必要とする特定の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、[+] ボタンをクリックします。

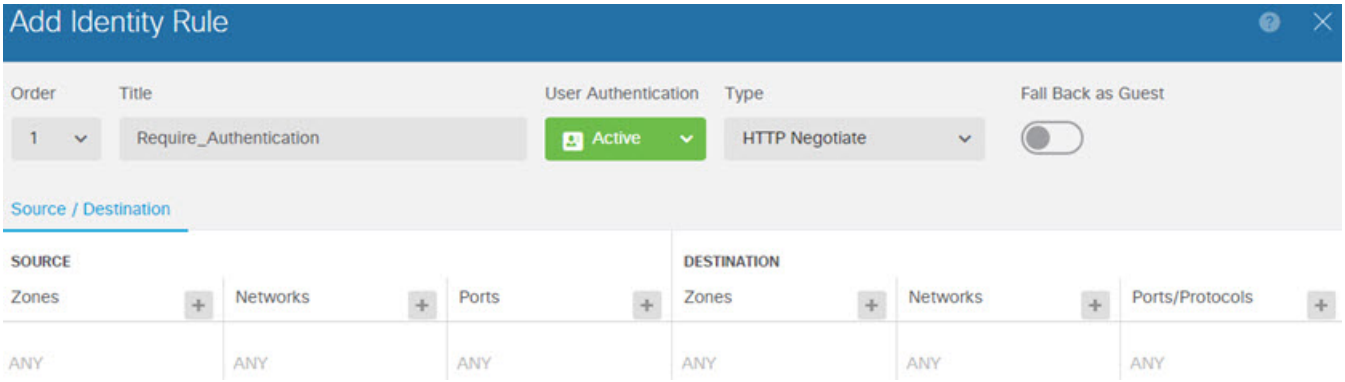
h) アイデンティティ ルールのプロパティを入力します。
すべてにユーザに認証を要求する場合、次の設定を使用できます。

- [名前（Name）]：任意の名前。Require_Authenticationなど。
- [ユーザ認証（User Authentication）]：[アクティブ（Active）]がすでに選択されている必要があります。変更しないでください。
- [タイプ（Type）]：[HTTPネゴシエート（HTTP Negotiate）]を選択します。これは、ブラウザとディレクトリ サーバが、まずNTLM、次にHTTPベーシックの順序で、最も強力な認証プロトコルをネゴシエートすることを許可します。

  （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ネゴシエートの場合は、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は、DNSサーバも更新して、アクティブな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必要があります。そうしないと、リダイレクションが完了できず、ユーザは認証できません。認証が実行されない場合、または認証を実行しない場合には、DNSサーバを更新して、他の認証方法の1つを選択します。

- [送信元/接続先（Source/Destination）]：すべてのフィールドをデフォルトから[任意（Any）]にします。

トラフィックを一層制限された設定にすることがふさわしいと判断する場合、ポリシーを制限することもできます。とはいえ、アクティブ認証はHTTPトラフィックのみで試行されるため、非HTTPトラフィックが送信元/接続先条件に一致するかどうか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。



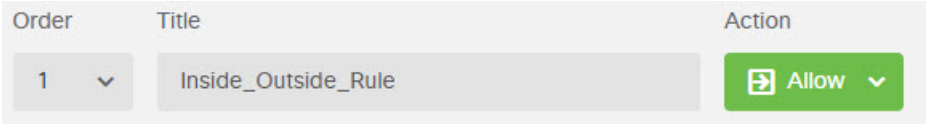
i) [OK]をクリックしてルールを追加します。
ウィンドウ右上の[展開（Deploy）]アイコンボタンにはドットが表示されます。これは、展開されていない変更があることを示しています。ユーザインターフェイスでの変更だけでは、変更がデバイスに設定されないため、変更を展開する必要があります。そのため、部分的に設定された一連の変更がデバイス上で実行されるという潜在的な問題に直面せずにすむよう、変更を展開する前に関係する一連の変更を作成することができます。このプロシージャの後の手順で変更を展開します。

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[許可する（Allow）]に変更します。
Inside_Outside_Ruleアクセス ルールは、信頼済みのルールとして作成されます。ただし、信頼済みのトラフィックのインスペクションは実行されないため、トラフィックの一致条件に、アプリケーションや、ゾーン、IPアドレス、ポート以外の他の条件が含まれていない場合、システムは、信頼済みのトラフィックの特性の一部（アプリケーションなど）について把握することができません。トラフィックを信頼するのではなく、トラフィックを許可するようにルールを変更すると、システムは、トラフィックのインスペクションを完全に実行します。

（注） （ASA 5506-Xモデル）Inside_Inside_Ruleを[信頼する（Trust）]から[許可する（Allow）]に変更することも検討してください。このルールは、内部インターフェイス間のトラフィックを対象とします。

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。

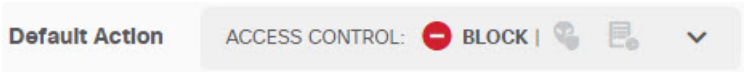
b) Inside_Outside_Rule の右側の [アクション（Actions）]セルにマウスオーバーして編集項目を表示してからアイコンを削除し、編集アイコン（）をクリックしてルールを開きます。
c) [アクション（Action）]の [許可する（Allow）] を選択します。



d) [OK]をクリックして変更を保存します。

ステップ 3 アクセス コントロール ポリシーのデフォルト アクションでのロギングを有効にします。
ダッシュボードには、接続が、接続ロギングを有効にするアクセス コントロール ルールに一致する場合にのみ、接続に関する情報が表示されます。Inside_Outside_Rule はロギングを有効にしますが、デフォルト アクションはロギングを無効にしています。したがって、ダッシュボードには Inside_Outside_Rule の情報のみが表示され、ルールに一致しない接続は反映されません。

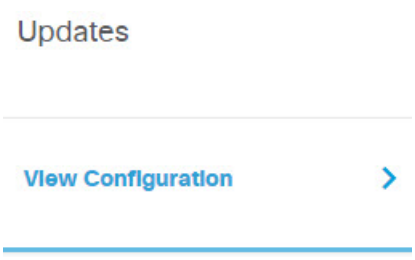
a) アクセス コントロール ポリシーのページ下部にあるデフォルト アクションの部分をクリックします。



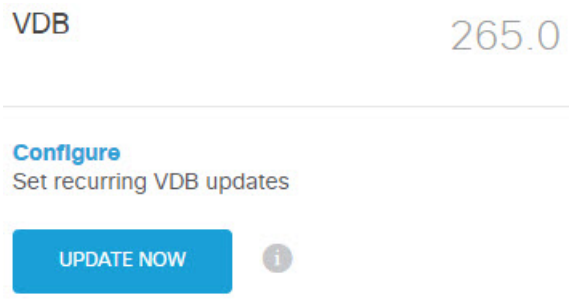
b) [ログ アクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）] を選択します。
c) [OK]をクリックします。

ステップ 4 脆弱性データベース（VDB）の更新スケジュールを設定します。
シスコは、接続に使用するアプリケーションを特定できるアプリケーション ディテクタを含む VDB に定期的に更新を提供します。VDB は定期的に更新する必要があります。手動で更新をダウンロードすることもできれば、定期的なスケジュールを設定することもできます。次に、スケジュールを設定する方法を示します。デフォルトでは、VDB 更新が無効になっているため、更新された VDB を取得するアクションを実行する必要があります。

a) デバイスをクリックします。
b) [更新（Updates）] グループの [設定の表示（View Configuration）]をクリックします。

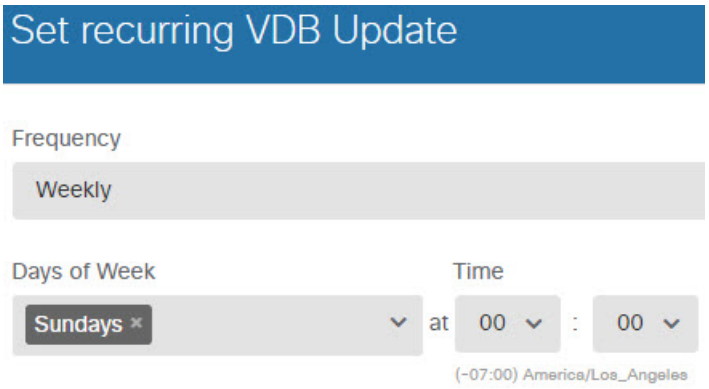


c) [VDB] グループの [設定（Configure）]をクリックします。



d) 更新スケジュールを定義します。
ネットワークを阻害しない時間と頻度を選択します。また、更新のダウンロード後に、システムが更新を自動展開することに留意してください。これは新しいディテクタを有効にするために必要です。したがって、実行し保存したもののまだ展開していなかったいずれの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、毎週日曜日の AM 12:00（24 時間表記を使用）に VDB データベースを更新します。

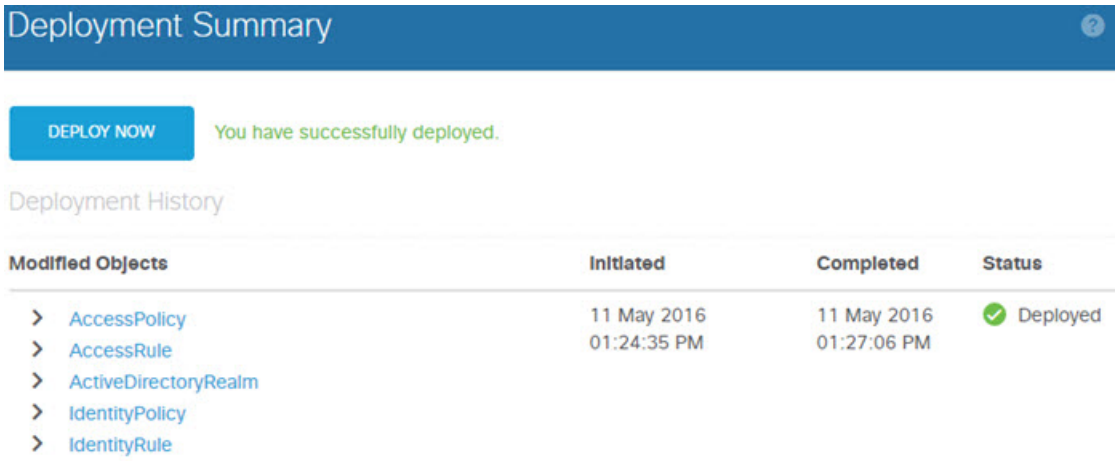


e) [保存（Save）]をクリックします。

ステップ 5 変更を保存します。

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

b) [すぐに展開する（Deploy Now）]ボタンをクリックして、展開が完了するまで待機します。
展開の概要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）] になる必要があります。



次の作業

この時点で、監視ダッシュボードとイベントに、ユーザとアプリケーションについての情報が表示され始める必要があります。望ましくないパターンの情報を評価し、許容されない使用を制約する新しいアクセス ルールを作成することができます。

侵入とマルウェアに関する情報の収集を開始する場合、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。これらの機能のライセンスを有効にする必要もあります。

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

脅威をブロックする方法

アクセス コントロール ルールに侵入ポリシーを追加することで、次世代侵入防御システム（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て、トラフィックの内容と既知の脅威を比較します。ある接続と監視中の脅威が一致する場合、システムはその接続をドロップすることにより攻撃を阻止します。

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、侵入ポリシーを使っ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。

侵入ポリシーの設定に使用できるルールは、トラフィックを[許可する（allow）]ルールのみです。インスペクションは、ルールがトラフィックを[信頼する（trust）]または[ブロックする（block）]ように設定されていると実行されません。さらに、デフォルト アクションが[許可する（allow）]になっている場合、侵入ポリシーをデフォルト アクションの一部として設定できます。

FirePOWER システムには複数の侵入ポリシーが付属しています。これらのポリシーは、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

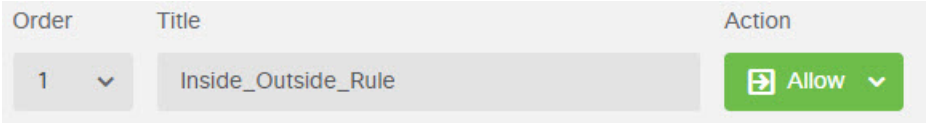
ステップ 1 まだ有効にしていない場合には、[脅威（Threat）]ライセンスを有効にします。
侵入ポリシーを使用するには、[脅威（Threat）] ライセンスを有効にする必要があります。現在評価ライセンスを使用している場合、このライセンスの評価版が有効になっています。デバイスが登録済みの場合、必要なライセンスを購入して、そのライセンスを Cisco.com の Smart Software Manager のアカウントに追加する必要があります。

a) デバイスをクリックします。
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) [脅威（Threat）]グループで [有効にする（Enable）] をクリックします。
システムは、ユーザのアカウントでライセンスを登録するか、必要に応じて評価ライセンスを有効にします。グループの表示は、ライセンスが有効になり、ボタンが [無効にする（Disable）] ボタンに変更されている必要があります。

ステップ 2 1 つ以上のアクセス ルールに対して侵入ポリシーを選択します。
脅威をスキャンするトラフィックを対象とするルールを決定します。この例では、侵入インスペクションを Inside_Outside_Rule に追加します。ASA 5506-X モデルの場合、Inside_Inside_Rule にも追加できます。

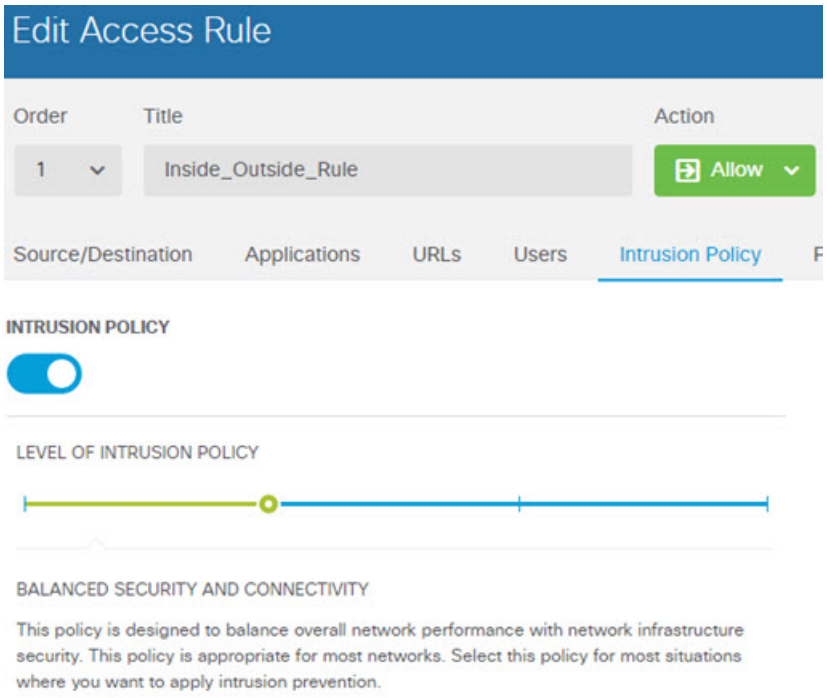
a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されていることを確認します。
b) Inside_Outside_Rule の右側の [アクション（Actions）]セルにマウスオーバーして編集項目を表示してからアイコンを削除し、編集アイコン（ ）をクリックしてルールを開きます。
c) まだ実行していない場合、[アクション（Action）]を [許可する（Allow）] を選択します。



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にしてから、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、安全性の小さいものから大きいものへの順序で表示されます。[バランスのとれた安全性と接続性（Balanced Security and Connectivity）]は、ほとんどのネットワークに適しています。ユーザがドロップすることを望まないトラフィックをドロップする可能性のある過度に積極的な防御機能ではなく、適度な侵入防御機能を提供します。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、[安全性よりも接続性を優先する（Connectivity over Security）]ポリシーを選択することにより、侵入インスペクションを緩和できます。

セキュリティに関して積極的である必要がある場合には、[接続性よりも安全性を優先する（Security over Connectivity）]ポリシーを試行します。[最大限検出する（Maximum Detection）]ポリシーは、ネットワークインフラストラクチャのセキュリティにさらに重点を置いており、運用上の影響が一層大きくなる可能性があります。

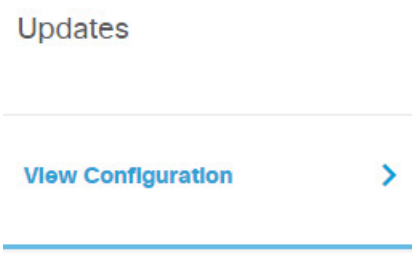


f) [OK]をクリックして変更を保存します。

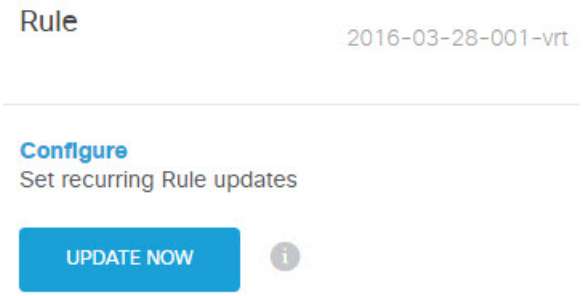
ステップ 3 侵入ルール データベースの更新スケジュールを設定します。
シスコは、接続をドロップするかどうかを判断するために侵入ポリシーによって使用される侵入ルールデータベースの更新を定期的にリリースします。ルールデータベースを定期的に更新する必要があります。手動で更新をダウンロードすることもできれば、定期的なスケジュールを設定

することもできます。次に、スケジュールを設定する方法を示します。デフォルトでは、データベース更新が無効になっているため、更新されたルールを取得するアクションを実行する必要があります。

a) デバイスをクリックします。
b) [更新（Updates）] グループの [設定の表示（View Configuration）]をクリックします。

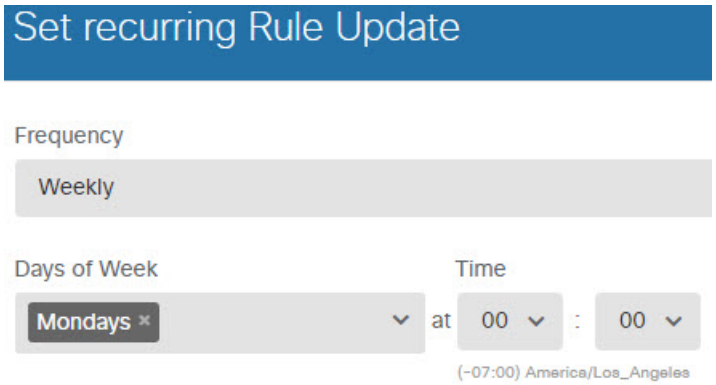


c) [ルール（Rule）] グループの [設定（Configure）]をクリックします。



d) 更新スケジュールを定義します。
ネットワークを阻害しない時間と頻度を選択します。また、更新のダウンロード後に、システムが更新を自動展開することに留意してください。これは新しいルールを有効にするために必要です。したがって、実行し保存したもののまだ展開していなかったいずれの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、毎週月曜日の AM 12:00（24 時間表記を使用）にルールデータベースを更新します。



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 [変更を展開する（Deploy Changes）]アイコンをクリックします。

b) [すぐに展開する（Deploy Now）]ボタンをクリックして、展開が完了するまで待機します。展開の概要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）] になる必要があります。

次の作業

この時点で、監視ダッシュボードとイベントが開始され、何らかの侵入が確認された場合、攻撃者、ターゲット、脅威に関する情報が表示されるようになる必要があります。この情報を評価して、ネットワークにより多くのセキュリティ対策が必要かどうか、または侵入ポリシーのレベルを下げる必要があるかどうかを判断できます。

マルウェアをブロックする方法

ユーザは、悪意のあるソフトウェアや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他の通信方法で取得するリスクに常にさらされています。信頼される 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 用 Advanced Malware Protection（FirePOWER 用 AMP）を使用してマルウェアを検出するファイル 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 用 AMPは、AMP クラウドを使用して、ネットワーク トラフィックで検出されたマルウェアの疑いのあるファイルの性質を把握します。管理インターフェイスには、AMP クラウドに到達し、マルウェア ルックアップを実行するためのインターネットへのパスが必要です。デバイスは、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、AMP クラウドにファイルの性質について問い合わせます。想定される性質には、[クリーン（clean）]、[マルウェア（malware）]、または [不明（unknown）]（明確に判定できない）が含まれます。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、接続されている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。

ファイル ポリシーの設定に使用できるルールは、トラフィックを [許可する（allow）]ルールのみです。インスペクションは、ルールがトラフィックを [信頼する（trust）]または [ブロックする（block）] ように設定されていると実行されません。

手順

ステップ 1 まだ有効にしていない場合には、[マルウェア（Malware）]ライセンスを有効にします。
マルウェアの制御にファイル ポリシーを使用するには、[マルウェア（Malware）] 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、このライセンスの評価版が有効になっています。デバイスが登録済みの場合、必要なライセンスを購入して、そのライセンスを Cisco.com の Smart Software Manager のアカウントに追加する必要があります。

a) デバイスをクリックします。

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（Malware）]グループで [有効にする（Enable）] をクリックします。
システムは、ユーザのアカウントでライセンスを登録するか、必要に応じて評価ライセンスを有効にします。グループの表示は、ライセンスが有効になり、ボタンが [無効にする（Disable）] ボタンに変更されている必要があります。

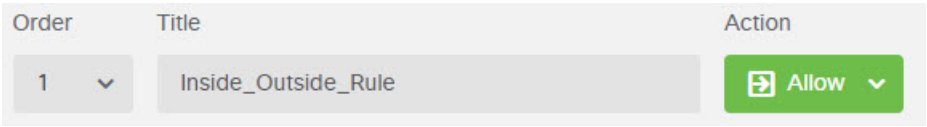
ステップ 2 1 つ以上のアクセス ルールに対してファイル ポリシーを選択します。

マルウェアをスキャンするトラフィックを対象とするルールを決定します。この例では、ファイル インスペクションを Inside_Outside_Rule に追加します。ASA 5506-X モデルの場合、Inside_Inside_Rule にも追加できます。

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

b) Inside_Outside_Rule の右側の [アクション（Actions）]セルにマウスオーバーして編集項目を表示してからアイコンを削除し、編集アイコン（）をクリックしてルールを開きます。

c) まだ実行していない場合、[アクション（Action）]を [許可する（Allow）] を選択します。

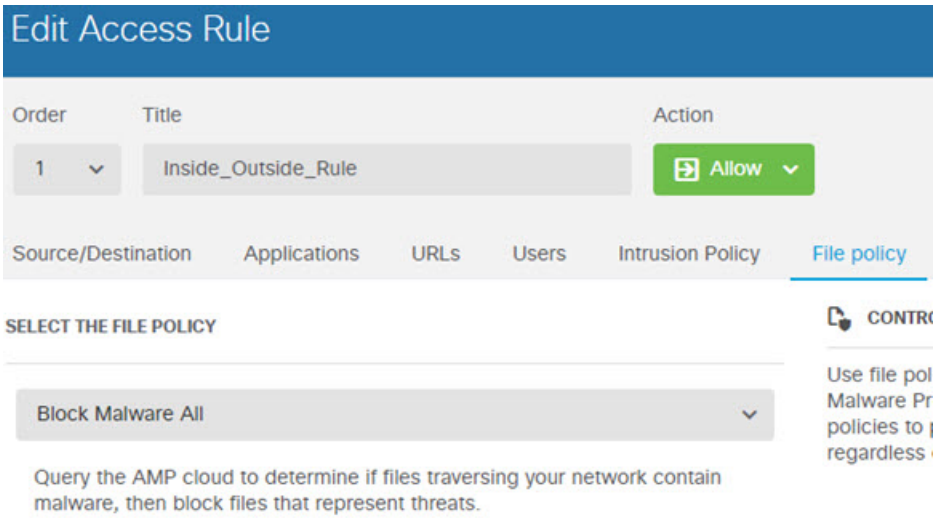


d) [ファイル ポリシー（File Policy）]タブをクリックします。

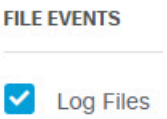
e) 使用するファイル ポリシーをクリックします。
マルウェアとみなされたすべてのファイルをドロップする [すべてのマルウェアをブロックする（Block Malware All）]と、ファイルの性質を判断するために AMP クラウドに問い合わるもののブロックはしない [クラウドですべてをルックアップする（Cloud Lookup All）]のどちらを選択するかが主要な選択事項です。最初にファイルの評価方法を確認するには、クラウドルックアップを使用します。ファイルの評価方法に納得した後で、ブロッキング ポリシーに切り替えることもできます。

マルウェアをブロックする使用可能な他のポリシーもあります。これらのポリシーは、Microsoft Office、または Office および PDF ドキュメントのアップロードをブロックするファイル制御と併用されます。つまり、これらのポリシーは、マルウェアをブロックするだけでなく、ユーザが他のネットワークにこれらのファイルタイプを送信することを防止します。必要に応じて、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）] 下の [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 ポリシーを選択した場合にはいつでもファイル ロギングが有効になります。イベントとダッシュボードのファイルとマルウェア情報を取得するには、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 [変更を展開する（Deploy Changes）]アイコンをクリックします。

b) [すぐに展開する（Deploy Now）]ボタンをクリックして、展開が完了するまで待機します。
展開の概要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）] になる必要があります。

次の作業

この時点で、ダッシュボードおよびイベントの監視が開始され、ファイルまたはマルウェアが送信された場合には、ファイル タイプ、ファイル イベントおよびマルウェア イベントに関する情報が表示される必要があります。この情報を評価して、ネットワークが送信に関連したセキュリティ対策をさらに必要とするかどうかを判断できます。

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。カテゴリを一致させるため、サイトの相対的な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、シスコの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。例として、いくつかのカテゴリの任意の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、badsite.example.com をブロックします。

手順

ステップ 1 まだ有効にしていない場合には、[URL]ライセンスを有効にします。
Web カテゴリとレピュテーション情報を使用したり、ダッシュボードとイベントの情報を表示したりするには、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、このライセンスの評価版が有効になっています。デバイスが登録済みの場合、必要なライセンスを購入して、そのライセンスを Cisco.com の Smart Software Manager のアカウントに追加する必要があります。

a) デバイスをクリックします。
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 ライセンス]グループで [有効にする（Enable）] をクリックします。
システムは、ユーザのアカウントでライセンスを登録するか、必要に応じて評価ライセンスを有効にします。グループの表示は、ライセンスが有効になり、ボタンが [無効にする（Disable）] ボタンに変更されている必要があります。

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 ルールを作成する前に、ユーザが閲覧しているサイトのカテゴリを最初に確認したいと思うかも知れません。その場合、許容されるカテゴリ（[金融サービス（Financial Services）] など）の [許可する（Allow）] アクションでルールを作成できます。すべての Web 接続を確認して URL がこのカテゴリに属しているかどうか判断する必要があるため、[金融サービス（Financial Services）] ではないサイトのカテゴリ情報を取得します。

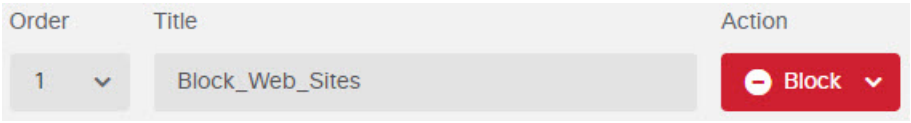
しかし、ブロックするつもりであることをすでに知っている Web カテゴリも存在します。ブロッキング ポリシーはインスペクションを強制するため、ユーザは、ブロックされたカテゴリだけではなく、ブロックされなかったテゴリへの接続に関する情報も取得します。

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。

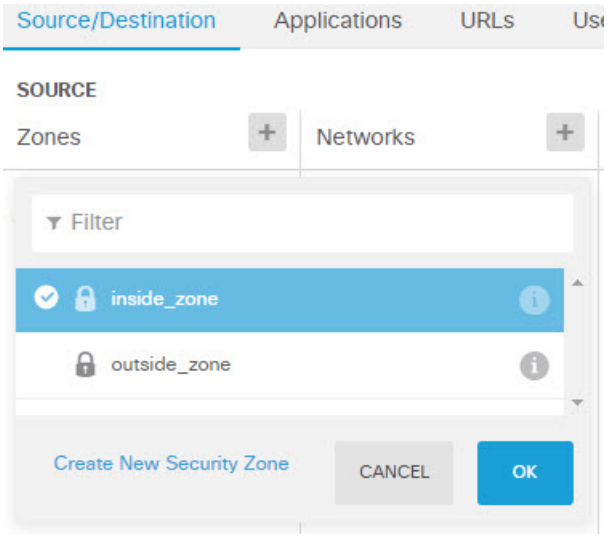
b) [+]をクリックして新しいルールを追加します。

c) 順序、タイトル、アクションを設定します。

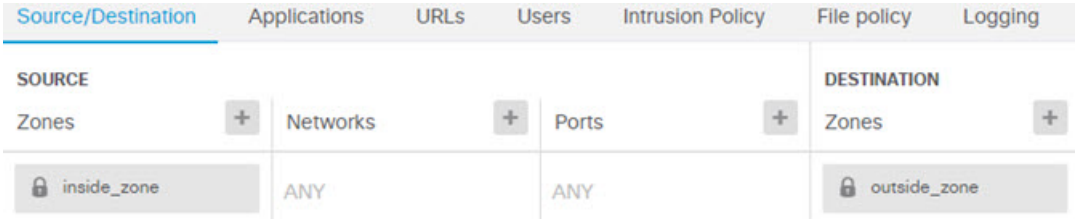
- [順序（Order）] : デフォルトでは、アクセス コントロール ポリシーの末尾に新しいルールを追加します。ただしこのルールは、同じ送信元/接続先その他の条件に一致するルールの前（上）に配置する必要があります。そうしないと、このルールはどの接続とも一致しなくなります（1 つの接続は 1 つのルール、つまりテーブル内で一致する最初のルールのみと一致します）。このルールの場合、デバイスの初期設定時に作成された Inside_Outside_Rule と同じ送信元/接続先を使用します。すでに他のルールが作成されている場合もあります。アクセス コントロールの効率を最大化するため、早期に特定のルールを作成して、接続を許可するか、またはドロップするかの決定を最大限迅速化することが最善です。例として、ルールの順序に [1]を選択します。
- [タイトル（Title）] : ルールに意味のある名前を付けます（Block_Web_Sites など）。
- [アクション（Action）] : [ブロックする（Block）] を選択します。



d) [送信元/接続先（Source/Destination）]タブで、[送信元（Source）]>[ゾーン（Zones）]の[+]をクリックし、[inside_zone]を選択してから、ゾーンのダイアログボックスで[OK]をクリックします。
どの条件を追加しても、同じ方法で動作します。[+]をクリックすると開く小さな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することができ、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された項目を示します。しかし、[OK]ボタンをクリックしない限り、何もポリシーに追加されません。項目を選択するたけでは十分ではありません。

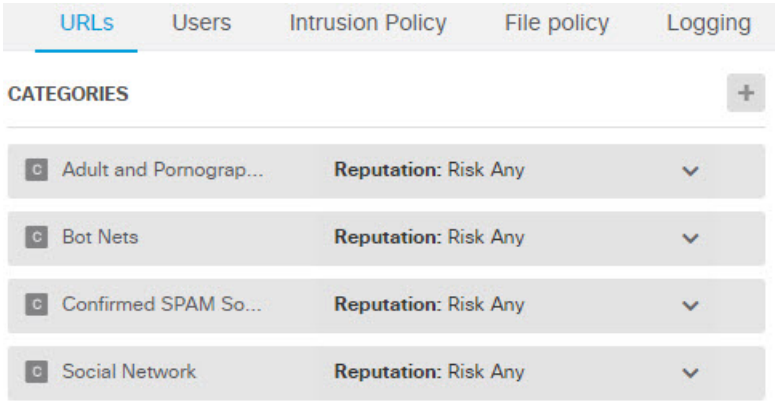


e) 同じ技術を使用して、[接続先（Destination）]>[ゾーン（Zones）]で[outside_zone]を選択します。

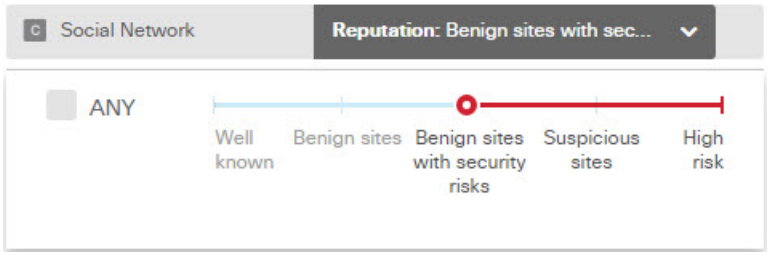


f) [URL]タブをクリックします。
g) [カテゴリ（Categories）]の[+]をクリックして、完全にまたは一部をブロックするカテゴリを選択します。

例として、[成人向けおよびポルノ（Adult and Pornography）]、[ボットネット（Bot Nets）]、[確認済みスパム ソース（Confirmed SPAM Sources）]、[ソーシャル ネットワーク（Social Network）] を選択します。ブロックする可能性の高い付加的なカテゴリもあります。



h) [ソーシャル ネットワーク（Social Network）] カテゴリのレピュテーション依存ブロッキングを実装するには、このカテゴリの [レピュテーション：すべてのリスク（Reputation: Risk Any）] をクリックし、[すべて（Any）] を解除してから、スライダを [セキュリティ リスクのある無害なサイト（Benign sites with security risks）]に移動します。スライダから離れた部分をクリックしてスライダを閉じます。



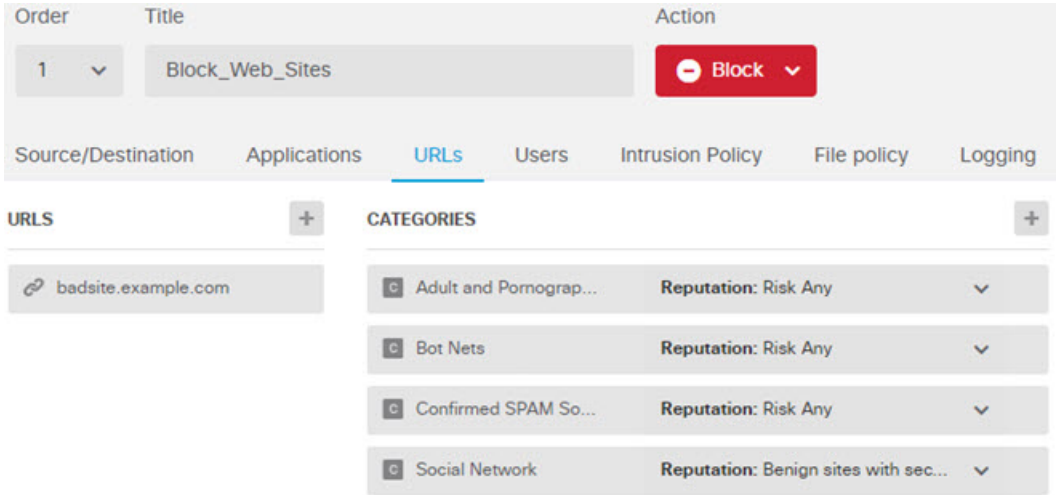
レピュテーション スライダの左側は許可されるサイトを、右側はブロックされるサイトを示します。この例では、[疑わしいサイト（Suspicious Sites）] と [高リスク（High Risk）] の範囲内のレピュテーションを持つソーシャル ネットワーキング サイトのみがブロックされます。このようにして、ユーザは、一般的に使用されているソーシャル ネットワーキング サイトにアクセスすることができます。

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的にブロックすることもできます。

i) カテゴリ一覧左の [URL（URLS）]一覧横の [+] 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、[新しい 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]と入力してから、[追加（Add）][OK] をクリックしてオブジェクトを作成します。

オブジェクトを URL と同じ名前にすることもできますし、オブジェクトに別の名前を指定することもできます。URL には、URL のプロトコル部分を含めずに、サーバ名のみを追加してください。

l) 新しいオブジェクトを選択してから、[OK]をクリックします。
ポリシーの編集時に新しいオブジェクトを追加すると、そのオブジェクトは一覧に追加されます。新しいオブジェクトは自動的に選択されません。



m) [ロギング（Logging）]タブをクリックして、[ログ アクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）] を選択します。
Web カテゴリ ダッシュボードと接続イベントにカテゴリおよびレピュテーション情報を取得するには、ロギングを有効にする必要があります。

n) [OK]をクリックしてルールを保存します。

ステップ 3 （オプション）URL フィルタリングを設定します。

URL ライセンスを有効にすると、システムは、Web カテゴリ データベースに対する更新を自動的に有効にします。システムは 30 分ごとに更新をチェックしますが、データは通常 1 日ごとに更新されます。何らかの理由で更新を必要としない場合には、更新を無効にすることもできます。

分析のために、シスコに分類されていないURLを選択し送信することもできます。そうすると、ユーザがカテゴリとレピュテーションのない新しいサイトに移動した場合、シスコはそのサイトを評価し、分類し、レピュテーションを付与し、将来の更新に含めることができます。サイトへのその後のアクセスは、新しい情報に基づいて許可されるか、またはブロックされる場合があります。

a) デバイスをクリックします。
b) [システム設定（System Settings）] > [トラフィック設定（Traffic Settings）] > [URL フィルタリングの設定（URL Filtering Preferences）] をクリックします。
c) [未知の URL 用 Cisco CSI のクエリ（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 [変更を展開する（Deploy Changes）]アイコンをクリックします。

b) [すぐに展開する（Deploy Now）]ボタンをクリックして、展開が完了するまで待機します。展開の概要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）] になる必要があります。

次の作業

この時点で、監視ダッシュボードとイベントに、Web カテゴリおよびレピュテーション、ドロップされた接続についての情報が表示されるようになる必要があります。この情報を評価して、URL フィルタリングで好ましくないサイトがドロップされているかどうか、または特定の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前に、ユーザ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か、または企業ネットワークの内部および外部での転送に 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りました。

FirePOWER Threat Defenseは、接続のインスペクションを実行して、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 ポートや UDP ポートではなく、アプリケーショ

ンを対象とするアクセス コントロール ルールを記述することが可能になります。そのため、同じポートを使用している場合でも、Web ベース アプリケーションを選択的にブロックまたは許可することができます。

許可またはブロックする特定のアプリケーションを選択することもできますが、タイプ、カテゴリ、タグ、リスク、あるい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を更新し追加します。したがって、リスクの高いアプリケーションをブロックするルールは、新しいアプリケーションに自動的に適用され、ルールを手動で更新する必要はありません。

この使用例では、[アノニマイザー/プロキシ（anonymizer/proxy）]カテゴリに属するすべての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）が完了済みであることを前提としています。その使用例は、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情報を収集する方法を説明しています。どのようなアプリケーションが実際に使用されているかを理解することは、有効なアプリケーションベースのルールを設計するのに役立つ場合があります。さらにこの使用例は、ここでは繰り返されないVDB 更新スケジュールの作成方法についても説明しています。VDBが定期的に更新され、アプリケーションが正しく特定されることを確認してください。

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。

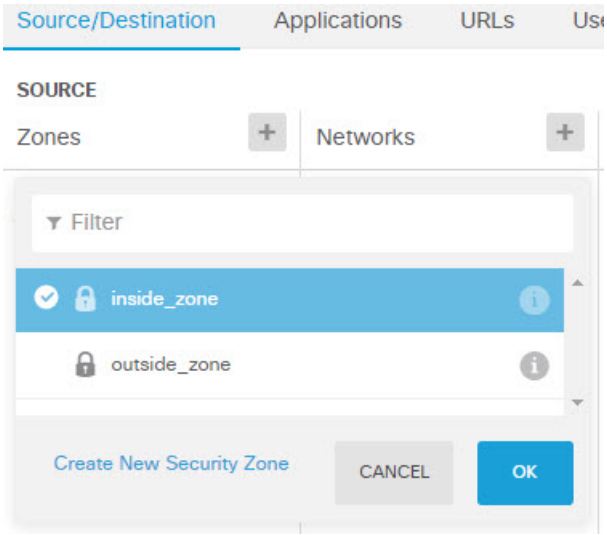
a) メイン メニューで [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されていることを確認します。

b) [+]をクリックして新しいルールを追加します。

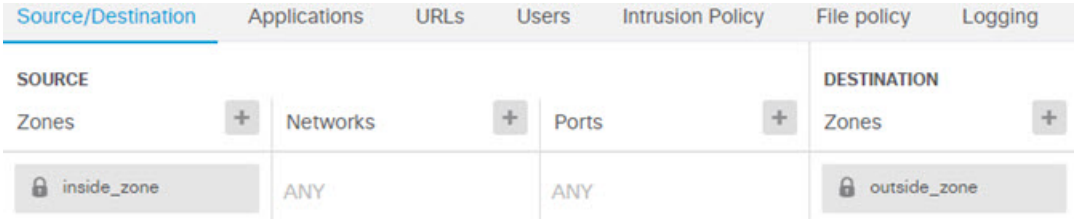
c) 順序、タイトル、アクションを設定します。

- [順序（Order）]：デフォルトでは、アクセス コントロール ポリシーの末尾に新しいルールを追加します。ただしこのルールは、同じ送信元/接続先その他の条件に一致するルールの前（上）に配置する必要があります。そうしないと、このルールはどの接続とも一致しなくなります（1 つの接続は 1 つのルール、つまりテーブル内で一致する最初のルールのみと一致します）。このルールの場合、デバイスの初期設定時に作成された Inside_Outside_Rule と同じ送信元/接続先を使用します。すでに他のルールが作成されている場合もあります。アクセス コントロールの効率を最大化するため、早期に特定のルールを作成して、接続を許可するか、またはドロップするかの決定を最大限迅速化することが最善です。例として、ルールの順序に [1]を選択します。
- [タイトル（Title）]：ルールに意味のある名前を付けます（Block_Anonymizers など）。
- [アクション（Action）]：[ブロックする（Block）] を選択します。

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



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



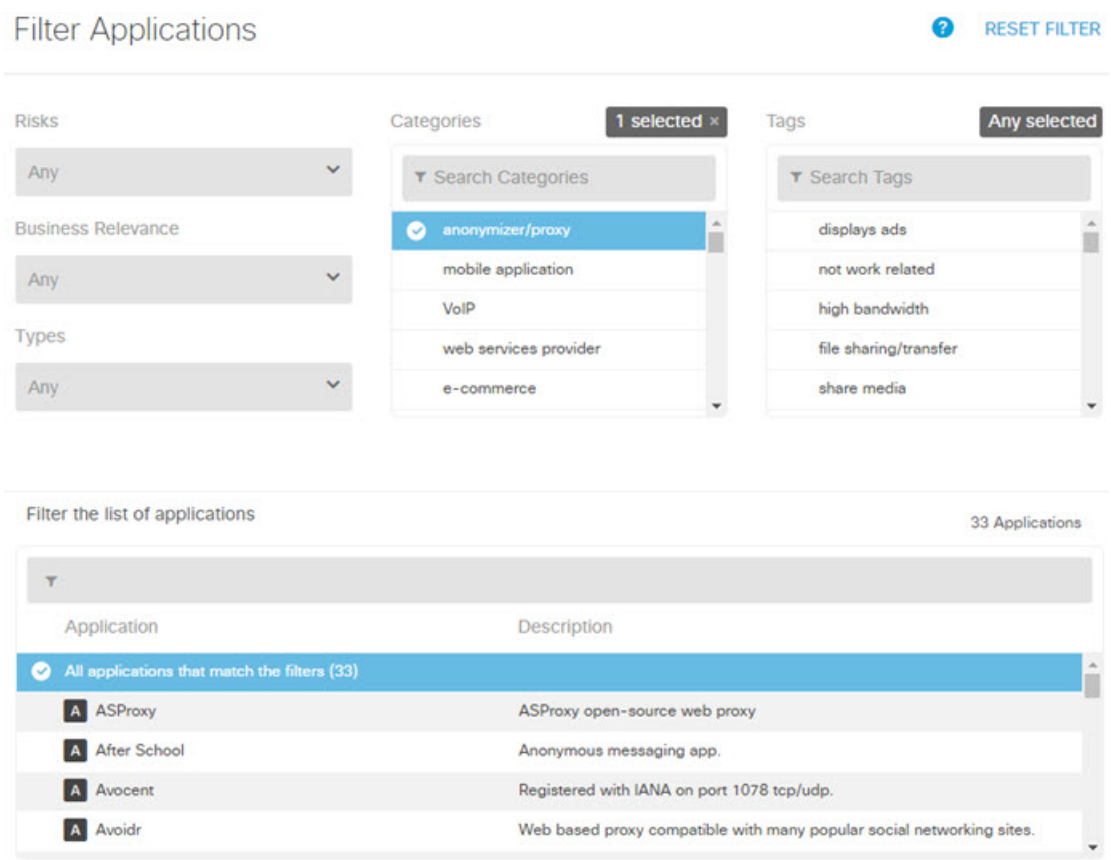
f) [アプリケーション（Applications）]タブをクリックします。

g) [アプリケーション（Applications）]の[+]をクリックしてから、ポップアップ ダイアログボックスの下部にある[詳細フィルタ（Advanced Filter）]リンクをクリックします。
前もってアプリケーション フィルタ オブジェクトを作成しておき、ここでアプリケーション フィルタ リストに対して適用することも可能ですが、アクセス コントロール ルールで直接条件を指定して、その条件をフィルタ 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対してルールを記述する場合でない限り、[詳細フィルタ（Advanced Filter）]ダイアログボックスを使用してアプリケーションを選択し、適切な条件を構築する方が簡単です。

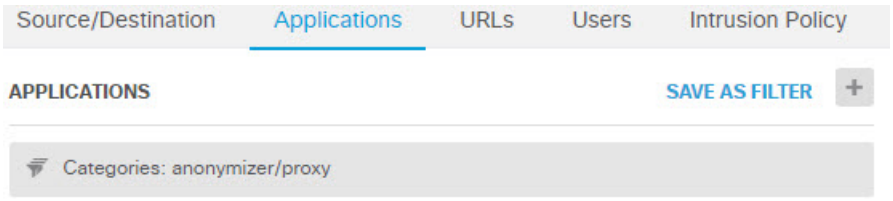
条件を選択すると、ダイアログボックス下のアプリケーションリストが更新され、どのアプリケーションが選択した条件と一致するかが表示されます。記述中のルールは、これらのアプリケーションに適用されます。

このリストを注意深く参照してください。たとえば、非常にリスクの高いアプリケーションすべてをブロックしたいと思うかもしれません。しかし、このルール記述の場合、Facebook と TFPT は非常にリスクが高いアプリケーションとして分類されます。ほとんどの組織は、これらのアプリケーションをブロックしたいとは考えません。時間をかけてさまざまなフィルタ条件を試行し、どのアプリケーションが選択に一致するかを確認してください。これらのリストは、すべての VDB 更新で変更される場合があることに留意してください。

例として、[カテゴリ（Categories）] リストからアノニマイザーまたはプロキシを選択します。



h) [詳細フィルタ（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 [アプリケーション（Applications）] タブに追加され、表示されます。



i) [ロギング（Logging）]タブをクリックして、[ログ アクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）] を選択します。
このルールによってブロックされるすべての接続についての情報を取得するには、ロギングを有効に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 [変更を展開する（Deploy Changes）]アイコンをクリックします。

b) [すぐに展開する（Deploy Now）]ボタンをクリックして、展開が完了するまで待機します。
展開の概要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）] になる必要があります。

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。
[ネットワークの概要（Network Overview）]ダッシュボードに、アプリケーション ウィジェットでドロップされた接続が表示される場合があります。[すべて/拒否済み/許可済み（All/Denied/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にフォーカスします。

[アプリケーション（Applications）] ダッシュボードには、これらの結果も表示されます。あるユーザがこれらのアプリケーションを使用しようとする場合、アイデンティティ ポリシーが有効になっており認証が必要であると仮定すると、アプリケーションと接続を試行するそのユーザを関連付ける必要があります。

サブネットの追加方法

デバイスで使用可能なインターフェイスがあれば、それをスイッチ（または別のルータ）に配線して、異なる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理由は数多くあります。この使用例では、次の一般的なシナリオについて説明します。

- サブネットは、プライベート ネットワーク 192.168.2.0/24 を使用してい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、ネットワークには物理インターフェイスが使用されています。別のオプションとして、すでに配線済みのインターフェイスを使用して、新しいネットワーク向けのサブインターフェイスを作成することができます。
- デバイスは、192.168.2.2 ～ 192.168.2.254 をアドレス プールとして使用し、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。
- 他の内部ネットワークと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向かうトラフィックは、パブリック アドレスを取得するために NAT を使用します。

（注） この例では、未使用のインターフェイスがブリッジ グループの一部ではないと仮定します。もし現在ブリッジグループのメンバーであるならば、この手順を進める前に、ブリッジグループから削除する必要があります。

はじめる前に

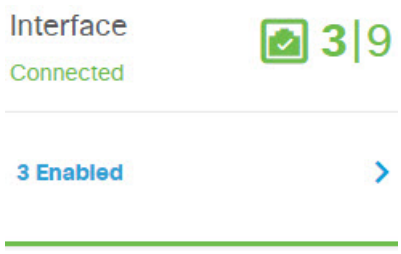
ネットワーク ケーブルを、新しいサブネットのインターフェイスとスイッチに物理的に接続します。

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。

b) [インターフェイス（Interfaces）]グループで、有効なインターフェイスの数を表示するリンクをクリックします。
有効なインターフェイス数とデバイス上のインターフェイスの合計数（モデルによって異なる）を比較した概要が表示されます。この例では、9 つのうち 3 つのインターフェイスが有効になっています。

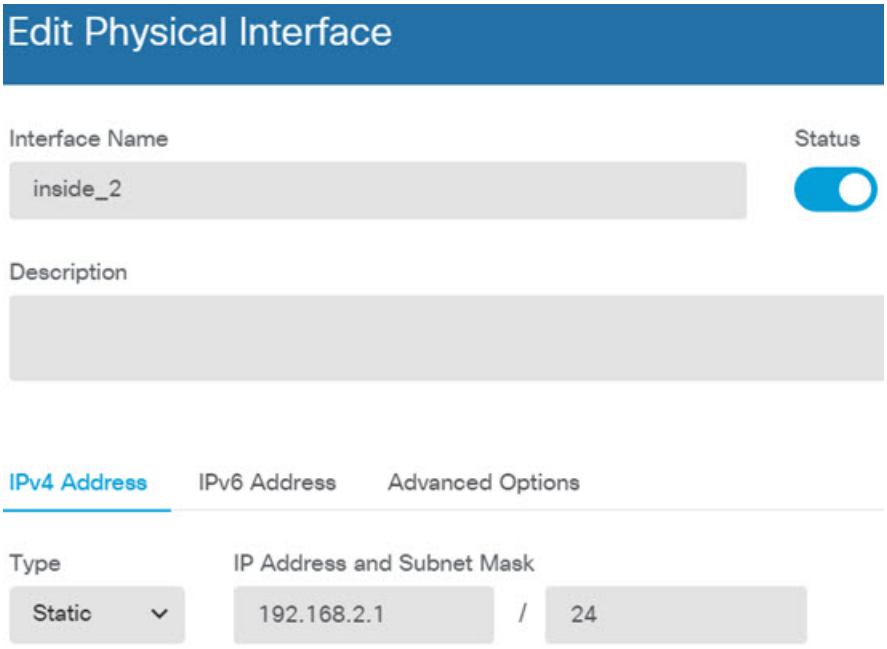


c) 配線したインターフェイスの行の右側にある [アクション（Actions）]セルの上にカーソルを移動し、編集アイコン（ ）をクリックします。

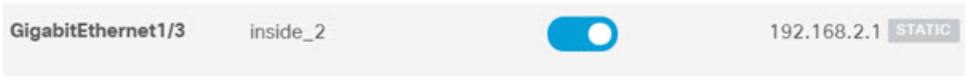
d) 基本的なインターフェイスのプロパティを設定します。

- [名前（Name）]そのインターフェイスに固有の名前です。この例では、inside_2です。

- [ステータス（Status）]：インターフェイスを有効にするには、ステータス トグルをクリックします。
- [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、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 リストには、更新されたインターフェイスのステータスと設定された IP アドレスが表示されます。

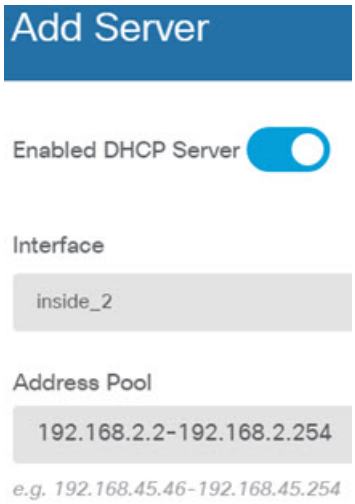


ステップ 2 インターフェイス向けに DHCP サーバを設定します。

a) デバイス。
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。
表に既存の DHCP サーバが表示されます。デフォルト設定を使用している場合、リストには内部インターフェイス向けにのサーバが 1 つ含まれています。
d) 表の上にある [+]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（Enable DHCP Server）]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）、ブロードキャスト アドレス（.255）が含まれていないことを確認します。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、これらのアドレスをプールから除外します。プールは単一の連続した一連のアドレスである必要があるため、最初または最後の範囲からスタティック アドレスを選択します。



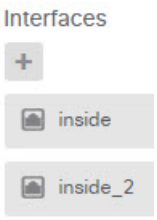
f) [追加（Add）]をクリックします。

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

ステップ 3 セキュリティ ゾーンにインターフェイスを追加します。
インターフェイスのポリシーを記述するには、その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 ゾーンのために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、自動的にインターフェイスに適用されたポリシーが変更されます。

a) メイン メニューの [オブジェクト（Objects）]をクリックします。
b) オブジェクトの目次から [セキュリティ ゾーン（Security Zones）]を選択します。
c) [inside_zone]オブジェクトの行の右側にある [アクション（Actions）] セルの上にカーソルを移動し、編集アイコン（ ）をクリックします。

d) [インターフェイス（Interfaces）]の下の [+] 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 リストで [OK] をクリックします。



e) [保存（Save）] をクリックします。

ステップ 4 内部ネットワーク間でのトラフィックを許可するアクセス コントロール ルールを作成します。トラフィックはすべてのインターフェイス間で自動的に許可されるわけではありません。必要な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する場合です。この例では、デバイスのセットアップ ウィザードで設定するブロックのデフォルト アクションを保持したと仮定します。そのため、内部インターフェイス間で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。すでにこのようなルールを作成している場合、この手順をスキップします。

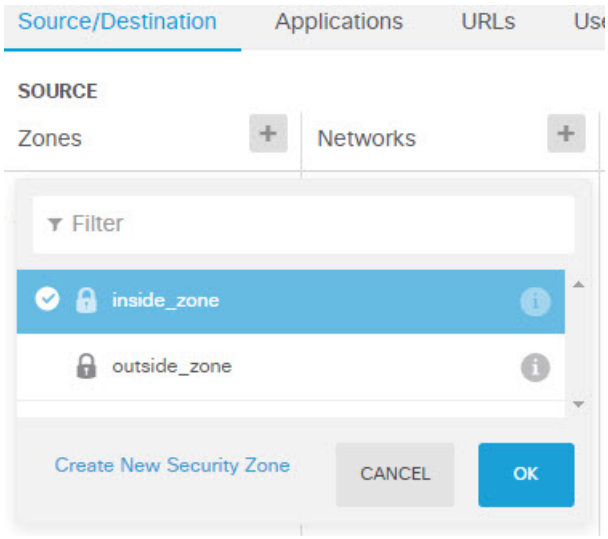
a) メイン メニューの [ポリシー（Policies）]をクリックします。
[アクセス コントロール（Access Control）]ポリシーが表示されていることを確認します。

b) [+]をクリックして新しいロールを追加します。

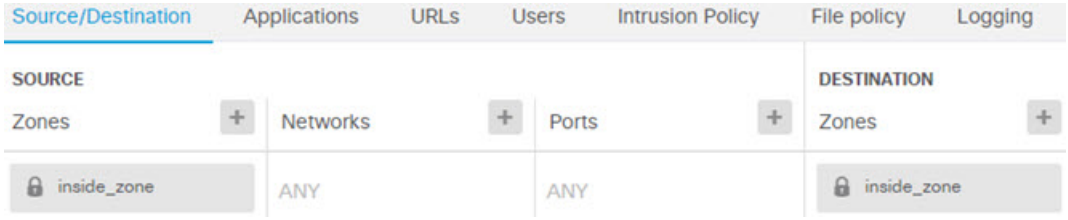
c) 順序、タイトル、およびアクションを設定します。

- [順序（Order）] : デフォルトでは、アクセス コントロール ポリシーの最後に新しいルールが追加されます。ただし、このルールは同じ送信元/接続先およびその他の条件に一致するルールの前に配置する必要があります。そうでない場合、ルールはいつまでも一致しなくなります（1 つの接続で一致するのは 1 つのルールのみであり、それは表中で一致する最初のルールです）。このルールでは、固有の送信元/接続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は容認できます。
- [タイトル（Title）] : ルールに Allow_Inside_Inside などのわかりやすい名前を付けます。
- [アクション（Action）] : [許可（Allow）] を選択します。

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



e) 同じ方法を使用して、宛先[接続先（Destination）]>[ゾーン（Zones）]に[inside_zone]を選択します。
送信元と接続先に同じゾーンを選択するには、セキュリティ ゾーンに少なくとも2つ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された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は一般的にあります。そのため、ユーザは知らずに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脅威をもたらす可能性があります。したがって、内部ネットワーク間で伝送されるトラフィックに対して、侵入およびマルウェアをスキャンすることができます。

次を行うことを検討します。

- [侵入ポリシー（Intrusion Policies）]タブをクリックして侵入ポリシーを有効にし、スライダを使用して[分散型の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、[マルウェアをすべてブロック（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 アクションを選択（Select Log Action）]>[接続の開始時と終了時（At Beginning and End of Connection）]を選択します。
このルールに一致するすべての接続についての情報を取得するには、ロギングを有効にする必要があります。ロギングを行うと、ダッシュボードに統計情報が追加されるだけでなく、イベント ビューアにイベントも表示されます。

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に定義されたことを確認します。
inside_zone セキュリティ ゾーンへインターフェイスを追加すると、inside_zone のすべての既存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、念のためポリシーのインスペクションを実行して、追加のポリシーが必要でないことを確認してください。

デバイスの初期設定が完了したら、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 コントロール（Access Control）]：Inside_Outside_Rule は新しい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する必要があります。前の使用例に従うと、このポリシーでは侵入およびマルウェアのインスペクションも行います。新しいネットワークと外部ネットワーク間の幾つか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。そうでないと、ユーザがインターネットまたは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 を適用します。このルールを保持した場合、外部に向かう新しいネットワークからのトラフィックは、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た IP アドレスを持つことになります。すべてのインターフェイス（または外部インターフェイスに向かう場合は inside_zone インターフェイス）に適用されるルールがない場合、もう 1 つルールを作成する必要があります。
- [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た場合、新しいネットワークの認証をすでに必要とするアイデンティティ ポリシーが存在す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、新しいネットワーク向けのユーザ ベースの情報が必要な場合は、ルールをもう 1 つ作成します。

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、展開が完了するまで待機します。

展開の概要には変更が正常に展開されたことが表示され、ジョブのタスク ステータスは [展開済み（Deployed）] となります。

次の作業

新しい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、および内部ネットワークと外部ネットワークに相互に到達できることを確認します。ネットワークの使用状況を評価するには、モニタリング ダッシュボードとイベント ビューアを使用します。