ネットワーク分析ポリシーと侵入ポリシーに対するアクセス コントロールの詳細設定

以下のトピックでは、ネットワーク分析ポリシーと侵入ポリシー用の高度な設定を行う手順を示します。

ネットワーク分析および侵入ポリシーのアクセス コントロールの詳細設定について

アクセス コントロール ポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

（注） Snort 2 は、Threat Defense バージョン 7.7ではサポートされていません。7.7 より前のバージョンでサポートされている Snort 2 機能については、ご使用の Firewall Threat Defense のバージョンに対応する Firewall Management Center のガイドを参照してください。

ネットワーク分析/侵入ポリシーのための高度なアクセス制御の設定の要件と前提条件

Model support

任意

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

トラフィック識別の前に通過するパケットのインスペクション

URLフィルタリング、アプリケーション検出、レート制限、インテリジェントアプリケーションバイパスなどの一部の機能では、接続を確立するとともに、システムが、トラフィックを識別して、そのトラフィックを処理するアクセスコントロールルール（存在する場合）を決定するために、いくつかのパケットを通過させる必要があります。

これらのパケットを検査し、宛先に到達することを防止し、イベントを生成するために、アクセス コントロール ポリシーを明示的に設定する必要があります。

システムが接続を処理する必要があるアクセスコントロールルールまたはデフォルトアクションを識別するとすぐに、接続内の残りのパケットが適宜処理され検査されます。

トラフィック識別の前に通過するパケットを処理するためのベストプラクティス

- アクセス コントロール ポリシーに指定されたデフォルトのアクションは、これらのパケットには適用されません。
- 代わりに、以下のガイドラインを使用して、アクセス コントロール ポリシーの詳細設定で [アクセス コントロール ルールが決定される前に使用される侵入ポリシー（Intrusion Policy used before Access Control rule is determined）] の値を選択します。

- システムによって作成された侵入ポリシーまたはカスタム侵入ポリシーを選択できます。たとえば、[バランスのとれたセキュリティと接続（Balanced Security and Connectivity）] を選択できます。
- パフォーマンス上の理由から、特別な理由がないかぎり、この設定はアクセス コントロール ポリシーに設定されているデフォルトのアクションと一致している必要があります。
- システムが侵入インスペクションを実行しない場合（たとえば、検出専用の導入において）は、[アクティブなルールなし（No Rules Active）] を選択します。システムはこれらの初期パケットのインスペクションを行わず、これらのパケットの通過が許可されます。
- デフォルトでは、この設定は、デフォルトの変数セットを使用します。これが目的に適していることを確認してください。詳細については、変数セットを参照してください。
- 最初に一致したネットワーク分析ルールに関連付けられているネットワーク分析ポリシーが、選択されたポリシーに対してトラフィックを前処理します。ネットワーク分析ルールがない場合、あるいはどのルールも一致しない場合は、デフォルトのネットワーク分析ポリシーが使用されます。

トラフィック識別の前に通過するパケットを処理するためのポリシーの指定

（注） この設定は、デフォルト侵入ポリシーと呼ばれることもあります。（これは、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とは異なります。）

始める前に

これらの設定のベストプラクティスを確認します。トラフィック識別の前に通過するパケットを処理するためのベストプラクティス （2 ページ） を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある **Edit** (✎) をクリックします。

代わりに **View** (👁) が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [アクセス制御ルールが決定される前に使用されている侵入ポリシー（ntrusion Policy used before Access Control rule is determined）] ドロップダウン リストから、侵入ポリシーを選択します。

ユーザーが作成したポリシーを選択した場合は、**Edit** (✎) をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 必要に応じて、[侵入ポリシーの変数セット（Intrusion Policy Variable Set）] ドロップダウン リストから別の変数セットを選択します。変数セットの横にある **Edit** (✎) を選択して、変数セットを作成および編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

変数セット

ネットワーク分析プロファイルの詳細設定

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。トラフィックの前処理は、セキュリティインテリジェンスの照合およびトラフィックの復号の後、侵入ポリシーによるパケットインスペクションの前に行われます。デフォルトでは、システム提供の [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが、デフォルト ネットワーク分析ポリシーです。

ヒント システムによって提供される [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです。複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する

方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

デフォルトのネットワーク分析ポリシーの設定

システムによって作成されたポリシーまたはユーザーが作成したポリシーを選択できます。

（注） プリプロセッサを無効にしているが、システムは有効になっている侵入ルールまたはプリプロセッサルールと照合して前処理されたパケットを評価する必要がある場合、システムはプリプロセッサを自動的に有効にして使用します。しかし、ネットワーク分析ポリシー Web インターフェイスでは無効のままです。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理および侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる**必要があります**。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある **Edit** (✎) をクリックします。

代わりに **View** (👁) が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。

ユーザーが作成したポリシーを選択した場合は、**Edit** (✎) をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

カスタム ポリシーの制限

ネットワーク分析ルール

アクセスコントロールポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワーク トラフィックへの前処理設定を調整できます。

ネットワーク分析ルールには1から番号が付けられます。システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。

ルールには、ゾーン、ネットワーク、VLANタグの条件を追加できます。ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

ネットワーク分析ポリシールール条件

ルール条件を使用すると、ネットワーク分析ポリシーを微調整して、制御するユーザーとネットワークを対象にできます。詳細については、次の項を参照してください。

関連トピック

セキュリティ ゾーン ルール条件
ネットワークルールの条件
VLAN タグ ルールの条件

セキュリティ ゾーン ルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーン

も同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルールの条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレスブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注） アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

VLAN タグ ルールの条件

（注） アクセス ルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

ネットワーク分析ルールの設定

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある **Edit** (✎) をクリックします。

代わりに **View** (👁) が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ヒント
[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックし、既存のカスタム ネットワーク分析ポリシーを表示および編集します。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 追加する条件をクリックして、ルールの条件を設定します。

ステップ 5 [ネットワーク分析（Network Analysis）] をクリックし、このルールに一致するトラフィックの前処理に使用する [ネットワーク分析ポリシー（Network Analysis Policy）] を選択します。

Edit(✎)をクリックして、新しいウィンドウでカスタムポリシーを編集します。システムによって提供されたポリシーは編集できません。

ステップ 6 **[追加（Add）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

ネットワーク分析ルールの管理

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは1つのポリシーにのみ属します。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[侵入ポリシーおよびネットワーク分析ポリシー（Intrusion and Network Analysis Policies）] セクションの横にある**Edit** ( )をクリックします。

代わりに **View** ( ) が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ステップ 3 カスタム ルールを編集します。次の選択肢があります。

- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある**Edit** ( )をクリックします。
- ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある**Delete** ( )をクリックします。

ヒント
ルールを右クリックするとコンテキスト メニューが表示され、新しいネットワーク分析ルールの切り取り、コピー、貼り付け、編集、削除、および追加を実行できます。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

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。