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

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。

デフォルトの侵入ポリシー

各アクセス コントロール ポリシーは、システムがトラフィックを検査する方法を正確に決定する前に、デフォルトの侵入ポリシーを使用してそのトラフィックを最初に検査します。これは、場合によってシステムが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）を決定する前に、接続の最初の数パケットを処理し**通過を許可する**必要があるため必要となります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。デフォルトでは、デフォルトの侵入ポリシーでデフォルトの変数セットが使用されます。

システムはクライアントとサーバの間で接続が完全に確立される前にアプリケーションを識別したり URL をフィルタ処理することはできないので、デフォルトの侵入ポリシーは、アプリ

ケーション制御およびURLフィルタリングを実行する場合に特に有用です。たとえば、パケットがアプリケーションまたはURL条件を持つアクセス コントロール ルールのその他のすべての条件に一致する場合、そのパケットと後続のパケットは、接続が確立されてアプリケーションまたはURLの識別が完了するまで通過することを許可されます。通常は3～5パケットです。

システムはこれらの許可されたパケットをデフォルトの侵入ポリシーで検査し、これによってイベントを生成したり、インラインで配置されている場合は、悪意のあるトラフィックをブロックできます。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した後、接続内の残りのパケットが適宜処理され検査されます。

アクセス コントロール ポリシーを作成する場合、そのデフォルトの侵入ポリシーは**最初に**選択したデフォルト アクションによって異なります。アクセス コントロールの初期のデフォルト侵入ポリシーは次のとおりです。

- [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）]（システムによって提供されるポリシー）は、最初に [侵入防御（Intrusion Prevention）] デフォルト アクションを選択した場合のアクセス コントロール ポリシーのデフォルトの侵入ポリシーです。
- 最初に [すべてのトラフィックをブロック（Block all traffic）] または [ネットワーク検出（Network Discovery）] デフォルト アクションを選択した場合、アクセス コントロール ポリシーのデフォルトの侵入ポリシーはNo Rules Activeになります。このオプションを選択すると、前述の許可されたパケットでの侵入インスペクションが無効になりますが、侵入データが必要なければ、パフォーマンスを向上できます。

（注） （たとえば、検出専用の導入において）侵入インスペクションを実行していない場合は、デフォルトの侵入ポリシーとしてNo Rules Activeポリシーを保持してください。

アクセス コントロール ポリシーを作成した後にデフォルトアクションを変更する場合、デフォルトの侵入ポリシーは自動的には変更され**ません**。手動で変更するには、アクセス コントロール ポリシーの詳細オプションを使用します。

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

（注） 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、デフォルトの侵入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。

デフォルトの侵入ポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

⚠

注意 アクセス コントロール ポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセス コントロール ルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

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）] タブをクリックし、[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編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、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、[ベース ポリシーから継承する（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。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）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編集アイコン（）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。設定変更の導入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ブラックリスト登録およびトラフィックの復号化の後、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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

システムによって作成されたポリシーまたはユーザ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）] タブをクリックし、[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編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、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、[ベース ポリシーから継承する（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。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）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。

注意 アクセス コントロール ポリシーによって使用されるネットワーク分析ポリシーの総数を変更すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。現在使用されていないポリシーを追加するか、ネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。

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。設定変更の導入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。

ネットワーク分析ルールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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（Advanced）] タブをクリックし、[ネットワーク分析（Network Analysis）] および [侵入ポリシー（Intrusion Policies）] セクションの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、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、[ベース ポリシーから継承する（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 追加する条件に対応するタブをクリックして、ルールの条件を設定します。ルール条件タイプを参照してください。

ステップ 5 [ネットワーク分析（Network Analysis）] タブをクリックし、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。

編集アイコン（  ）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。

注意 アクセス コントロール ポリシーによって使用されるネットワーク分析ポリシーの総数を変更すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。現在使用されていないポリシーを追加するか、ネットワーク分析ポリシーの最後のインスタンスを削除することで、ネットワーク分析ポリシーの総数を変更します。ネットワーク分析ポリシーは、ネットワーク分析ルールと一緒に使用することもできれば、デフォルトのネットワーク分析ポリシーとして使用することもできます。

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。設定変更の導入を参照してください。

ネットワーク分析ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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（Advanced）] タブをクリックして、[侵入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編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、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、[ベース ポリシーから継承する（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、ルールの横にある編集アイコン（）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、ルールの横にある削除アイコン（）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。設定変更の導入を参照してください。