侵入ポリシーとネットワーク分析ポリシーのレイヤ

以下のトピックでは、侵入ポリシーおよびネットワーク分析ポリシーでレイヤ（層）を使用する方法について説明します。

レイヤの基本

多数の管理対象デバイスが存在する大規模な組織では、さまざまな部署や事業部門、場合によってはさまざまな企業の固有のニーズをサポートするために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシータイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシー タイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザー レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は *My Changes* という名前が付けられています）に含められます。また、最大200までレイヤを追加して、それらのレイヤで設定を任意に組み合わせて構成することもできます。ユーザー レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザー レイヤを同じタイプの他のポリシーと共有できます。

ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

ネットワーク分析ポリシーレイヤと侵入ポリシーレイヤの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

レイヤ スタック

レイヤ スタックは、次の各レイヤから構成されています。

ユーザ レイヤ

ユーザ設定可能なレイヤです。ユーザ設定可能なレイヤは、コピー、マージ、移動、または削除を行うことができます。また、任意のユーザ設定可能なレイヤが同じタイプの他のポリシーと共有されるように設定することもできます。このレイヤには、最初にMy Changesという名前が付けられた自動生成されたレイヤが含まれています。

組み込み型レイヤ

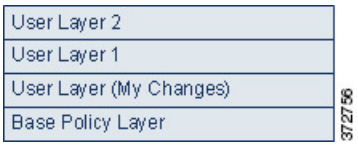
読み取り専用の基本ポリシー レイヤです。このレイヤ内のポリシーは、システムによって提供されるポリシー、または自分で作成したカスタム ポリシーにできます。

ネットワーク分析ポリシーまたは侵入ポリシーには、デフォルトでは基本ポリシー レイヤと My Changes レイヤが含まれています。ユーザ レイヤは必要に応じて追加できます。

各ポリシー レイヤには、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を継承します。システムはレイヤをフラット化します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント 侵入またはネットワークの分析ポリシーは、基本ポリシーのデフォルト設定のみに基づいて作成できます。侵入ポリシーの場合に、モニタ対象ネットワークの特定のニーズに合わせて侵入ポリシーを調整したいときは、Firepower のルール状態の推奨を使用することもできます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤの他に、2 つの追加のユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* も含まれているレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能なレイヤそれぞれがスタックの最上位レイヤとして最初に配置されるため、図内の User Layer 2 が最後に追加されたもので、このスタックの最上位になっていることに注目してください。



ルール更新にポリシーの変更を許可しているかどうかに関わらず、ルール更新での変更は、レイヤで行った変更を上書きしません。これは、ルール更新での変更が、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール更新が基本ポリシーに加えた変更が上書きされます。

基本レイヤ

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更は My Changes レイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

システム提供の基本ポリシー

Firepower システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか提供されています。システム提供のネットワーク分析ポリシーおよび侵入ポリシーを使用して、Talos インテリジェンス グループのエクスペリエンスを活用することができます。これらのポリシーでは、Talos は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよ

び他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタム ポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。ただし、カスタム ポリシーを設定して、これらの変更内容がシステム提供の基本ポリシーに自動的に反映されないようにすることもできます。これにより、ルール更新とは関係ないスケジュールで、システム提供の基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によって My Changes または他のレイヤの設定が変更または上書きされることはありません。

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。

カスタム基本ポリシー

カスタム ポリシーを基本（ベース）として使用することができます。カスタム ポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

別のポリシーのベースとして使用するカスタムポリシー変更すると、変更内容はこのベースを使用するポリシーのデフォルト設定として自動的に使用されます。

また、ポリシーはすべて、システムが提供するポリシーをポリシーチェーンにおける最終的なベースとしているため、たとえカスタム基本ポリシーを使っていても、ルールが更新されればポリシーに影響する可能性があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許可されている場合は、ポリシーが影響を受ける可能性があります。

基本ポリシーがどのように変更されたかに関わらず（ルール更新による変更でも、基本ポリシーとして使用するカスタムポリシーを変更でも）、ユーザーの基本ポリシーに対する変更によって My Changes やその他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーに対するルール更新の影響

ルール更新をインポートすると、システム提供の侵入ポリシー、アクセス コントロール ポリシー、ネットワーク分析ポリシーが変更されます。ルール更新には次の要素が含まれる場合があります。

- 変更されたネットワーク分析プリプロセッサの設定
- 変更された侵入ポリシーおよびアクセス コントロール ポリシーの詳細設定
- 新規または更新された侵入ルール
- 既存のルールの変更された状態
- 新しいルール カテゴリとデフォルト変数

ルール更新により、既存のルールがシステム提供のポリシーから削除される場合もあります。

デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。

システム提供のポリシーを侵入またはネットワーク分析の基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステム提供のポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新による基本ポリシーの変更を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新による基本の侵入ポリシーの変更が許可されているかどうかに関係なく、Talos が削除した侵入ルールが常に削除されます。

ネットワーク トラフィックに変更を再展開するまで、現在展開されている侵入ポリシー ルールは次のように動作します。

- 無効になっている侵入ルールは無効のままになります。
- [イベントを生成する（Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー（つまり、カスタム基本ポリシーの起源となるポリシー）を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

基本ポリシーの変更

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 必要な侵入ポリシーの行にある [編集（Edit）]（✎） をクリックします。

ステップ 4 [ベースポリシー（Base Policy）] ドロップダウンリストからベースポリシーを選択します。

ステップ 5 [保存（Save）] 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。

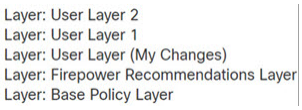
関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

Cisco 推奨レイヤ

侵入ポリシーでルール状態の推奨を生成する場合は、その推奨に基づいてルール状態を自動的に変更するかどうかを選択できます。

下記の図に示すように、推奨されたルール状態を使用すると、侵入ポリシーの基本レイヤのすぐ上に読み取り専用の組み込み Cisco 推奨レイヤが挿入されます。



このレイヤは侵入ポリシー固有のものです。

それ以後、推奨されたルール状態を使用しないことを選択すると、Cisco 推奨レイヤは削除されます。このレイヤは手動で削除できませんが、推奨されるルール状態を使用するかどうかを選択することで、サービスを追加したり削除することができます。

Cisco推奨レイヤを追加すると、ナビゲーションパネルの[ポリシー階層（Policy Layers）]の下に Cisco 推奨リンクが追加されます。このリンクから Cisco 推奨レイヤページの読み取り専用

ビューにアクセスして、[ルール（Rules）]ページの推奨でフィルタリングされたビューを読み取り専用モードで表示できます。

推奨されたルール状態を使用すると、ナビゲーションパネルの Cisco 推奨リンクの下に [ルール（Rules）] サブリンクも追加されます。[ルール（Rules）] サブリンクから、Cisco 推奨レイヤの [ルール（Rules）] ページの読み取り専用画面にアクセスできます。このビューでは次の点に注意してください。

- 状態列にルール状態のアイコンがない場合、状態は基本ポリシーから継承されます。
- このビューまたは他の [ルール（Rules）] ページビューの Cisco 推奨列にルール状態のアイコンがない場合、このルールに対する推奨は存在しません。

関連トピック

ネットワーク資産に応じた侵入防御の調整

レイヤ管理

[ポリシー層（Policy Layers）] ページには、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤスタックの単一ページの概要が示されます。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

[ポリシー層（Policy Layers）] ページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

各レイヤのサマリーにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示

機能の状態	機能名
下位レイヤから継承される	表示されない

最大200のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して[継承（Inherit）]で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルール アクションのアラートは設定されません。

レイヤをポリシーに追加する際は、ユーザが設定可能なレイヤに一意の名前を指定します。その名前は後で変更できます。また、必要に応じて、レイヤを編集する際に表示される説明を追加あるいは変更することもできます。

レイヤはコピーすることも、[ユーザ レイヤ（User Layers）]ページ内での表示位置を上下に移動することもできます。また、初期の My Changes レイヤを含め、ユーザ レイヤを削除することも可能です。次の考慮事項に注意してください。

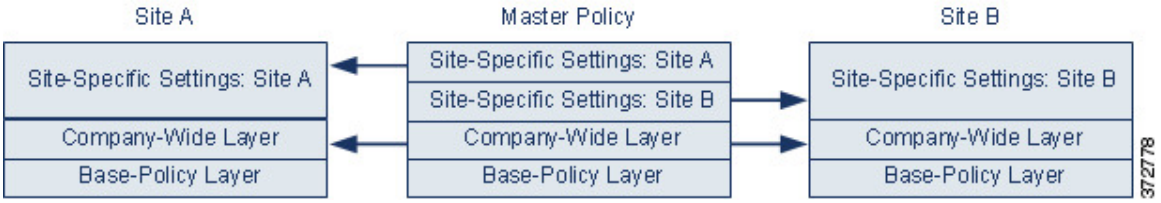
- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、初期状態ではそのレイヤは共有されませんが、必要に応じて、後から共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

ユーザ設定可能なレイヤの直下に、別のユーザ設定可能なレイヤをマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルール、または詳細設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。他のポリシーに追加できる共有可能なレイヤを作成するポリシーでは、共有可能なレイヤのすぐ上に非共有レイヤのある共有可能なレイヤをマージできますが、共有可能なレイヤの直下には非共有レイヤのある共有可能なレイヤをマージすることはできません。別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤとマージすることはできません。

共有レイヤ

共有レイヤとは、あるポリシー内で作成して共有を許可し、別のポリシーに追加されたレイヤのことです。共有可能レイヤとは、共有が許可されているレイヤのことです。

以下の図に示すプライマリポリシーの例では、全社的レイヤと、サイト A およびサイト B に固有のレイヤを作成し、これらのサイト固有のレイヤの共有を許可しています。その上で、これらのサイト固有のレイヤを共有レイヤとしてサイト A とサイト B のポリシーに追加しています。



プライマリポリシーの全社的なレイヤには、サイト A とサイト B に適用される設定が含まれる一方、サイト固有のレイヤには各サイトに固有の設定が含まれています。たとえば、ネットワーク分析ポリシーの場合、サイト A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクションプリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、サイト A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、サイト B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のプライマリポリシーでフラット化された設定値そのものがトラフィックをモニターするのに役立つわけではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー階層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、ネットワーク、さらにはユーザごとにポリシーのレイヤを定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できるように設定できます。共有可能レイヤ内の設定を変更し、変更をコミットすると、そのレイヤを共有するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシーの機能設定のみを変更できます。

別のポリシーに追加しているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

基本ポリシーが共有するレイヤが作成されたカスタムポリシーである場合、ポリシーに共有レイヤを追加することはできません。追加した場合、ポリシーで依存関係が循環することになります。

レイヤの管理

手順

ステップ 1 Snort 2 ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] をクリックします。

ステップ 2 [ポリシー層（Policy Layers）] ページでは、次に示す管理アクションを実行できます。

- 別のポリシーからの共有レイヤの追加：[ユーザーレイヤ（User Layers）] の横にある [共有レイヤの追加（Add Shared Layer）] [追加（Add）] () をクリックし、[共有レイヤの追加（Add Shared Layer）] ドロップダウンリストからレイヤを選択して、[OK] をクリックします。
- 非共有レイヤの追加：[ユーザーレイヤ（User Layers）] の横にあるレイヤの追加[追加（Add）] ()をクリックし、[名前（Name）] を入力して、[OK] をクリックします。
- レイヤの説明の追加または変更：レイヤの横にある[編集（Edit）]（  ）をクリックして、[説明（Description）] を追加または変更します。
- 別のポリシーとのレイヤの共有の許可：レイヤの横にある[編集（Edit）]（  ）をクリックして、[共有（Sharing）] チェックボックスをオフにします。
- レイヤの名前の変更：レイヤの横にある[編集（Edit）]（  ）をクリックして、[名前（Name）] を変更します。
- レイヤのコピー：レイヤの[コピー（Copy）]（  ）をクリックします。
- レイヤの削除：レイヤの[削除（Delete）]（  ）をクリックして、[OK] をクリックします。
- 2 つのレイヤのマージ：2 つのレイヤの上部の**マージ**（  ）をクリックして、[OK] をクリックします。
- レイヤの移動：レイヤサマリ内の任意の空いている場所をクリックし、**位置矢印**が移動するレイヤの上または下の行を指すまでドラッグします。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

レイヤ間のナビゲーション

手順

ステップ 1 Snort 2 ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] をクリックします。Snort 2 ポリシーにアクセスするには、[ポリシー（Policies）] > [侵入（Intrusion）]

> [侵入ポリシー（Intrusion Policies）] タブ を選択し、編集するポリシーに対して [Snort 2] をクリックします。 > >

ステップ 2 レイヤの移動は、次のいずれかのアクションで実行できます。

- プリプロセッサ ページまたは詳細設定ページにアクセスする：レイヤ レベルのプリプロセッサまたは詳細設定の設定ページにアクセスするには、そのレイヤに対応する行の機能名をクリックします。基本ポリシーおよび共有レイヤでは、設定ページは読み取り専用です。
- ルールページにアクセスする：ルールの状態タイプでフィルタ処理されたレイヤレベルのルール設定ページにアクセスする場合は、レイヤの概要で [イベントのドロップおよび生成（Drop and Generate Events）]、[イベントの生成（Generate Events）]、または [無効化（Disabled）] をクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。
- [ポリシー情報ページ（Policy Information）] ページを表示する：[ポリシー情報ページ（Policy Information）] ページを表示するには、ナビゲーション ウィンドウで [ポリシーの概要（Policy Summary）] をクリックします。
- レイヤの概要ページを表示する：レイヤの概要ページを表示するには、レイヤに対応する行のレイヤ名をクリックするか、ユーザーレイヤの横にある [編集（Edit）]（ ） をクリックします。[表示（View）]（ ） をクリックして、共有レイヤの読み取り専用サマリーページにアクセスすることもできます。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

レイヤでの侵入ルール

レイヤの [ルール（Rules）] ページで個々のレイヤ設定を表示することも、[ルール（Rules）] ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[ルール（Rules）] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[ルール（Rules）] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 *1*: レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [継承（Inherit）] に設定します。侵入ポリシーの [ルール（Rules）] ページは、すべてのルール設定の最終的な効果を示す複合ビューであるため、このページでの作業中にルールの状態を [継承（Inherit）] に設定することはできないことに注意してください。
1	しきい値 SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。
1 つ以上	抑制 レートベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。

たとえば、あるレイヤでルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定し、それよりも上位のレイヤで [無効（Disabled）] に設定した場合、侵入ポリシーの [ルール（Rules）] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[ルール（Rules）] ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレートベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

特定のレイヤの各 [ルール（Rules）] ページの色分けでは、有効状態が上位レイヤ、下位レイヤ、現在のレイヤのどれに該当するのかが次の色で示されます。

- 赤：上位レイヤでの有効状態
- 黄色：下位レイヤでの有効状態
- 陰影なし：現在のレイヤでの有効状態

侵入ポリシーの [ルール（Rules）] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。

レイヤでの侵入ルールの設定

侵入ポリシーでは、すべてのユーザー設定可能なレイヤのルールに対して、ルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [ルール（Rules）] ページの設定を、侵入ポリシーの [ルール（Rules）] ページの設定と同じように追加します。

手順

ステップ 1 Snort 2 侵入ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 変更するポリシー階層を展開します。

ステップ 3 変更するポリシー レイヤのすぐ下にある [ルール（Rules）] をクリックします。

ステップ 4 ルールを使用した侵入ポリシーの調整 に示されている任意の設定を変更します。

ヒント
編集可能なレイヤから個々の設定を削除するには、そのレイヤの [ルール（Rules）] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [Delete] をクリックして [OK] を 2 回クリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

複数のレイヤからのルール設定の削除

侵入ポリシーの複数のレイヤから、特定のタイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。後者の場合、そのレイヤから設定が削除され、設定タイプの削除が停止されます。

共有レイヤまたは基本ポリシーに指定されたタイプの設定があり、ポリシーの最上位レイヤが編集可能である場合は、ルールの残りの設定とルール状態がその編集可能なレイヤにコピーさ

れます。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

（注） 共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。

手順

ステップ 1 Snort 2 侵入ポリシーの編集中に、ナビゲーションパネルの [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。Snort 2 ポリシーにアクセスするには、[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policies）] タブ を選択し、編集するポリシーに対して [Snort 2] をクリックします。 > >

ヒント
また、任意のレイヤの [ルール（Rules）] ページでレイヤのドロップダウンリストから [ポリシー（Policy）] を選択するか、[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] をクリックすることもできます。

ステップ 2 複数の設定を削除するルールを選択します。

- 特定の選択（Choose specific）：特定のルールを選択するには、各ルールの横にあるチェックボックスをオンにします。
- すべて選択（Choose all）：現在のリストのルールをすべて選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 3 次のいずれかのオプションを選択します。

- **[イベントのフィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）]**
- **[イベントのフィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）]**
- **[動的状態（Dynamic State）] > [レート ベースのルール状態の削除（Remove Rate-Based Rule States）]**
- **[アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）]**

（注）
共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

カスタム基本ポリシーからのルール変更の受け入れ

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合、および
- 基本ポリシーとして使用する他のカスタム ポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

手順

ステップ 1 Snort 2 侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開します。

ステップ 2 [個人用の変更（My Changes）] を展開します。

ステップ 3 [個人用の変更（My Changes）] のすぐ下にある [ルール（Rules）] リンクをクリックします。

ステップ 4 設定を受け入れるルールを選択します。次の選択肢があります。

- [特定ルールの選択（Choose specific rules）]：特定のルールを選択するには、各ルールの横にあるチェックボックスをチェックします。
- [すべてのルールを選択（Choose all rules）]：現在のリストのすべてのルールを選択する場合は、列の最上部にあるチェックボックスをチェックします。

ステップ 5 [ルール状態（Rule State）] ドロップダウン リストから、[継承（Inherit）] を選択します。

ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

レイヤでのプリプロセッサと詳細設定

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [設定（Settings）] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [詳細設定（Advanced Settings）] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[設定（Settings）] ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。ナビゲーション パネルの [ポリシー層（Policy Layers）] の下のレイヤの名前を選択することによって、別のレイヤのサマリー ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能の設定ページへのサブリンクがナビゲーションパネルのレイヤの名前の下に表示され、[編集（Edit）]（）がそのレイヤのサマリーページの機能の横に表示されます。レイヤで機能を無効にしたり、[継承（Inherit）] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態（有効または無効）を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [継承（Inherit）] に設定します。[設定（Settings）] または [詳細設定（Advanced Settings）] ページで操作するときには、[継承（Inherit）] の選択項目は使用できないことに注意してください。また、現在有効にされている機能を継承すると、ナビゲーション パネルではその機能のサブリンクが表示されなくなり、設定ページではその機能の編集アイコンが表示されなくなることにも注意してください。

システムは、機能が有効にされている最上位レイヤの設定を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤでネットワーク分析 DCE/RPC プリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

各レイヤのサマリページは次のようにカラーコード化されており、有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤのいずれにあるかが示されます。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定（Settings）] および [詳細設定（Advanced Settings）] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラーコーディングを使用しません。

層のプリプロセッサと詳細の設定

手順

ステップ 1 Snort 2 ポリシーの編集中に、ナビゲーションパネルで [ポリシー層（Policy Layers）] を展開し、変更するレイヤの名前をクリックします。

ステップ 2 次の選択肢があります。

- 層の名前を変更します。
- 説明を追加または変更します。
- [共有（Sharing）] チェックボックスをオンまたはオフにして、層を別のポリシーと共有できるようにするかどうかを指定します。
- 有効にしたプリプロセッサ/詳細設定の設定ページにアクセスするには、[編集（Edit）]（）または機能のサブリンクをクリックします。
- 現在の層のプリプロセッサ/詳細設定を無効にするには、機能の横にある [無効化（Disabled）] をクリックします。
- 現在の層のプリプロセッサ/詳細設定を有効にするには、機能の横にある [有効化（Enabled）] をクリックします。
- 現在の層の下にある最上位レイヤの設定からプリプロセッサ/詳細設定の状態および構成を継承するには、[継承（Inherit）] をクリックします。

ステップ 3 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

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。