ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用

多数の ASA FirePOWER モジュール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、場合によっては異なる企業の固有のニーズに対応するために、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。

侵入ポリシーとネットワーク分析ポリシーのレイヤは、基本的に同じように動作します。どちらのポリシータイプも、レイヤを意識せずに作成したり編集することができます。ポリシーの設定は変更でき、ポリシーにユーザ レイヤを追加していない場合は、1つ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）にその変更が自動的に取り込まれます。必要に応じて、最大200のレイヤを追加できます。それらのレイヤでは、任意の設定項目を組み合わせて設定することができます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要な点は、個々のユーザ レイヤを同じタイプの他のポリシーと共有できることです。

レイヤ スタックについて

ライセンス：Protection

レイヤが追加されていないネットワーク分析ポリシーや侵入ポリシーには、組み込みの読み取り専用の基本ポリシー レイヤと、ユーザが設定可能な単一のレイヤ（最初は「My Changes」という名前が付けられています）が含まれています。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。

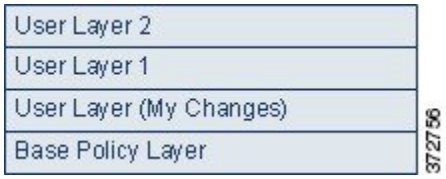
各ポリシー レイヤには、ネットワーク分析ポリシーのすべてのプリプロセッサの全設定、または、侵入ポリシーの侵入ルールと詳細設定がすべて含まれています。最下位の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれています。上位

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に上位のレイヤの設定を継承します。

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。

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 つのユーザが設定可能な追加レイヤ「User Layer 1」と「User Layer 2」を含むレイヤ 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各レイヤは、スタックの最上位のレイヤに配置されていることに注目してください。図の User Layer 2 は、最後に追加され、スタックの最上位にあります。



複数のレイヤを使用する場合は、次の点に注意してください。

- 以下のいずれかを実行する場合、ポリシー内の最上位のレイヤが読み取り専用レイヤであるか、またはポリシー間でのレイヤの共有 （11 ページ）で説明されてる共有レイヤであるときに、ユーザ設定可能なレイヤが最上位のレイヤとして侵入ポリシーに自動的に追加されます。
  - 侵入ポリシーの [Rules] ページでルールのアクション（ルール状態、イベント フィルタリング、動的状態、または警告）を変更する。詳細については、「ルールを使用した侵入ポリシーの調整」を参照してください。
  - プリプロセッサ、侵入ルール、あるいは詳細設定を有効化、無効化、または変更する。

システムによって追加されたレイヤの設定は、新しいレイヤで生じた変更を除いてすべて継承されます。

- 最上位レイヤが共有レイヤの場合、次のいずれかの操作を実行するとレイヤが追加されます。
  - 他のポリシーと最上位レイヤを共有する
  - ポリシーにレイヤを追加する
- ルール アップデートによる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 アップデートによる変更は、ユーザがレイヤで行った変更を上書きしません。これは、ルール アップデートよる変更は、基本ポリシー レイヤのデフォルト設定を決定する基本

ポリシーに対して行われるからです。ユーザによる変更はより上位のレイヤで行われるので、その変更によって、ルール アップデートによる基本ポリシーの変更が上書きされます。詳細については、「ルール更新とローカル ルール ファイルのインポート」を参照してください。

基本レイヤについて

ライセンス：Protection

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変更するのではなく、上書きます。

システムによって提供される基本ポリシーについて

ライセンス：Protection

シスコではASA FirePOWERモジュールで、ネットワーク分析ポリシーと侵入ポリシーのペアを複数提供しています。システムによって提供されるネットワーク分析ポリシーと侵入ポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRTは侵入およびプリプロセッサ ルールの状態を設定し、プリプロセッサと他の詳細設定の初期設定も行います。これらのシステム付属のポリシーはそのまま使用することも、カスタム ポリシーの基本として使用することもできます。

システム付属のポリシーを基本として使用する場合は、ルールアップデートをインポートすると基本ポリシーの設定が変更されます。ただし、カスタムポリシーで、システム付属の基本ポリシーが自動的に変更されないように設定できます。これにより、ルールアップデートのインポートとは別に、スケジュールに基づいて、システム付属の基本ポリシーを手動で変更できます。いずれの場合も、ルールアップデートによって基本ポリシーが変更されても、My Changesや他のレイヤの設定は変更されず、上書きもされません。詳細については、ルールアップデートによるシステム付属基本ポリシーの変更を許可する （4 ページ）を参照してください。

システム付属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いていますが、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。詳細については、システムによって提供されるポリシーについて を参照してください。

カスタム基本ポリシーについて

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーでシステムによって提供されるポリシーを基本ポリシーとして使用しない場合は、カスタムポリシーをベースとして使用できます。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、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。

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。

別のポリシーの基本として使用しているカスタム ポリシーに加えた変更は、それを使用してい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、すべてのポリシーにはポリシー チェーンの最終的なベースとしてシステム付属のポリシーがあるため、カスタム基本ポリシーを使用している場合でも、ルール アップデートをインポートするとポリシーに影響が及びます。チェーンの最初のカスタム ポリシー（システム付属のポリシーを基本として使用しているポリシー）で、ルール アップデートによる基本ポリシーの変更が許可されている場合は、ユーザのポリシーが影響を受ける可能性があります。この設定の変更の詳細については、ルール アップデートによるシステム付属基本ポリシーの変更を許可する （4 ページ）を参照してください。

変更の内容に関係なく、また、ルール アップデートによる変更であるか、基本ポリシーとして使用しているカスタム ポリシーの変更であるかを問わず、ユーザの基本ポリシーに対する変更は、My Changes や他のレイヤの設定を変更せず、上書きもしません。

基本ポリシーの変更

ライセンス：Protection

ネットワーク分析ポリシーや侵入ポリシーに対して別の基本ポリシーを選択できます。または必要に応じて、上位レイヤでの変更に影響を与えることなく、ルール アップデートによってシステム付属の基本ポリシーを変更できます。

基本ポリシーの変更方法：

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

[Policy Information] ページが表示されます。

ステップ 2 [Base Policy] ドロップダウン リストから基本ポリシーを選択します。

ステップ 3 （任意）システム付属の基本ポリシーを選択する場合は、[Manage Base Policy] をクリックして、侵入ルールのアップデートによって基本ポリシーを自動的に変更できるかどうかを指定します。

詳細については、ルール アップデートによるシステム付属基本ポリシーの変更を許可する （4 ページ）を参照してください。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定を参照してください。

ルール アップデートによるシステム付属基本ポリシーの変更を許可する

ライセンス：Protection

インポートするルール更新によって、変更済みのネットワーク分析プリプロセッサの設定、変更済みの侵入ポリシーの詳細設定、新規および更新済みの侵入ルール、および既存ルールの変更済みの状態が、システム提供ポリシーに提供されます。ルール更新では、ルールを削除したり、新しいルール カテゴリとデフォルト変数を提供したりすることもできます。詳細については、「ルール更新とローカル ルール ファイルのインポート」を参照してください。

ルール更新は、プリプロセッサ、詳細設定およびルールの変更とともに、システムによって提供されるポリシーを常に変更します。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。詳細については、「システムによって提供される基本ポリシーについて （3 ページ）」を参照してください。

システム提供のポリシーを基本ポリシーとして使用する場合、ルール更新による基本ポリシー（この場合はシステム提供ポリシーのコピー）の変更を許可できます。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、新しいポリシー内の設定が決定されます。ただし、ユーザがポリシーに加えた変更は、新しいルール アップデートによって上書きされません。

ルール更新で基本ポリシーの更新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 アップデートでは、侵入ポリシー内のルール状態や、ルール アップデートによる基本ポリシーの更新が許可されているかどうかに関係なく、VRT が削除したルールは必ず削除されるので注意してください。ネットワーク トラフィックに変更が再適用されるまで、現在適用されている侵入ポリシー内のルールは次のように動作します。

- 無効になっているルールは無効のままになります。
- [Generate Events] に設定されたルールは、トリガーされると引き続きイベントを生成します。
- [Drop and Generate Events] に設定されたルールは、トリガーされると引き続きイベントを生成し、違反パケットをドロップします。

次の両方の条件が満たされていない場合、ルール アップデートはカスタム基本ポリシーを変更しません。

- ルール アップデートによる親ポリシーのシステム付属基本ポリシー（カスタム基本ポリシーの元となるポリシー）の変更が許可されている。
- 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、無効化されていた侵入ルールがルール アップデートによって有効化され、親となる侵入ポリシーのルールの状態がユーザによって変更されていない場合は、親ポリシーの保存時に、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、ルールアップデートによってデフォルトのプリプロセッサ設定が変更され、親となるネットワーク分析ポリシーの設定がユーザによって変更されていない場合は、親ポリシーの保存時に、変更された設定が基本ポリシーに渡されます。

詳細については、「基本ポリシーの変更 （4 ページ）」を参照してください。

ルール アップデートによるシステム付属基本ポリシーの変更を許可するには：

ステップ 1 システム提供のポリシーを基本ポリシーとして使用するポリシーの編集時に、ナビゲーション パネルで [Policy Information] をクリックします。

[Policy Information] ページが表示されます。

ステップ 2 [Manage Base Policy] をクリックします。

[Base Policy summary] ページが表示されます。

ステップ 3 [Update when a new Rule Update is installed] チェック ボックスをオンまたはオフにします。

このチェックボックスをオフにしてポリシーを保存してから、ルールアップデートをインポートすると、[Base Policy] 概要ページに [Update Now] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。必要に応じて、[Update Now] をクリックして、最近インポートしたルール更新内の変更で基本ポリシーを更新できます。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

レイヤの管理

ライセンス：Protection

[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 スタックの概要が 1 ページで表示されます。このページでは、共有レイヤや非共有レイヤを追加したり、レイヤをコピー、マージ、移動、削除したり、各レイヤの概要ページにアクセスすることができます。また、各レイヤ内の設定を有効化、無効化、上書きするための設定ページにもアクセスできます。

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
- どのレイヤが、最も上位の（つまり、効率的な）プリプロセッサまたは詳細設定を含んでいるか（機能名別に表示）
- 侵入ポリシーにおける、レイヤに状態が設定されている侵入ルールの数、および各ルール状態に対して設定されているルールの数。

サマリに表示される各レイヤの機能名は、次のように、レイヤで有効化、無効化、上書き、継承されている設定を示しています。

このページには、すべての有効なプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、および侵入ルール（侵入ポリシーの場合）の実質的な効果の概要も表示されます。

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
下位レイヤから継承される	表示されない

次の表に、[Policy Layers] ページで使用できるアクションを示します。

表 *1*: ネットワーク分析ポリシーおよび侵入ポリシーの設定操作

目的	操作
[ポリシー情報（Policy Information）] ページの表示	[Policy Summary] をクリックします。 [Policy Information] ページで実行できる操作については、ルールを使用した侵入ポリシーの調整および侵入ポリシーについてを参照してください。
レイヤのサマリ ページを表示する	該当するレイヤの行でレイヤ名をクリックするか、またはユーザ レイヤの横にある編集アイコンをクリックします。表示アイコンをクリックして、共有レイヤの読み取り専用サマリ ページにアクセスすることもできます。 レイヤのサマリ ページで実行できる操作については、ポリシー間でのレイヤの共有 （11 ページ）、層のプリプロセッサと詳細の設定 （17 ページ）、およびレイヤでの侵入ルールの設定 （13 ページ）を参照してください。
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へのアクセス	該当するレイヤの行で機能名をクリックします。基本ポリシーと共有レイヤでは、設定ページが読み取り専用であることに注意してください。詳細については、「層のプリプロセッサと詳細の設定 （17 ページ）」を参照してください。
ルール状態のタイプ別にフィルタリングされた、レイヤレベルのルール設定ページにアクセスする	レイヤのサマリで、イベントのドロップおよび生成アイコン（  ）、イベントの生成アイコン（  ）、または無効化アイコン（）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。
ポリシーへのレイヤの追加	レイヤの追加 （8 ページ）を参照してください。
別のポリシーからの共有レイヤの追加	ポリシー間でのレイヤの共有 （11 ページ）を参照してください。
レイヤの名前または説明を変更する	レイヤの名前および説明の変更 （9 ページ）を参照してください。

目的	操作
レイヤを移動、コピー、または削除する	レイヤの移動、コピー、削除 （9 ページ）を参照してください。
すぐ下のレイヤとのレイヤのマージ	レイヤのマージ （10 ページ）を参照してください。

[Policy Layers] ページの使用方法：

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

[Policy Layers] サマリ ページが表示されます。

ステップ 2 表「ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定操作」のいずれかの操作を実行できます。#unique_328 unique_328_Connect_42_Table （7 ページ）

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

レイヤの追加

ライセンス：Protection

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、そのレイヤがポリシーの最上位レイヤとして表示されます。すべての機能の初期状態が継承され、侵入ポリシーでは、イベント フィルタリング、動的状態、アラート ルール アクションは設定されません。

ネットワーク分析ポリシーまたは侵入ポリシーへのレイヤの追加方法：

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

[Policy Layers] ページが表示されます。

ステップ 2 ユーザ レイヤの横にあるレイヤの追加アイコン（  ）をクリックします。

[Add Layer] ポップアップ ウィンドウが表示されます。

ステップ 3 [Name] に一意のレイヤ名を入力し、[OK] をクリックします。

新しいレイヤが、ユーザ レイヤの最上位のレイヤとして表示されます。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

レイヤの名前および説明の変更

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーのユーザ設定可能レイヤの名前は変更できます。必要に応じて、レイヤの編集時に表示される説明を追加または変更することもできます。

レイヤ名の変更方法および説明の追加/変更方法：

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

[Policy Layers] ページが表示されます。

ステップ 2 編集するユーザ レイヤの横にある編集アイコンをクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3 次の操作を実行できます。

- レイヤの**名前**の変更
- レイヤの**説明**の追加または変更

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

レイヤの移動、コピー、削除

ライセンス：Protection

初期の My Changes レイヤを含め、ネットワーク分析ポリシーまたは侵入ポリシーのユーザ レイヤはコピー、移動、削除することができます。以下の点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、非共有のコピーが作成されます。このコピーは、必要に応じて他のポリシーと共有できます。
- 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が他のポリシーと共有されていない場合、そのレイヤは共有レイヤではありません。

レイヤのコピー、移動、削除方法：

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

[Policy Layers] ページが表示されます。

ステップ 2 次の操作を実行できます。

- レイヤをコピーするには、コピーするレイヤのコピー アイコンをクリックします。

ページが更新され、レイヤのコピーが最上位のレイヤとして表示されます。

- [User Layers] ページ領域内でレイヤを上下に移動するには、レイヤ サマリ内の任意の空領域をクリックし、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。

画面が更新され、レイヤが新しい場所に表示されます。

- レイヤを削除するには、削除するレイヤの削除アイコンをクリックし、[OK] をクリックします。

ページが更新され、レイヤは削除されます。

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

レイヤのマージ

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤを、その下にある次のユーザ レイヤとマージできます。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の設定が含まれている場合は、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。

ポリシーで共有レイヤを作成して他のポリシーに追加する場合、作成元のポリシーでは、その共有レイヤをすぐ上の非共有レイヤとマージできますが、下の非共有レイヤとマージすることはできません。

ポリシーで共有レイヤを作成して他のポリシーに追加する場合、追加先のポリシーでは、その共有レイヤをすぐ下の非共有レイヤとマージできますが、マージ後のレイヤは共有されなくなります。共有レイヤを上の非共有レイヤとマージすることはできません。

ユーザ レイヤをその下のユーザ レイヤとマージする方法：

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

[Policy Layers] ページが表示されます。

ステップ 2 2 つのレイヤの上部にあるマージ アイコン（）をクリックし、[OK] をクリックします。

ページが更新され、レイヤがその下のレイヤとマージされます。

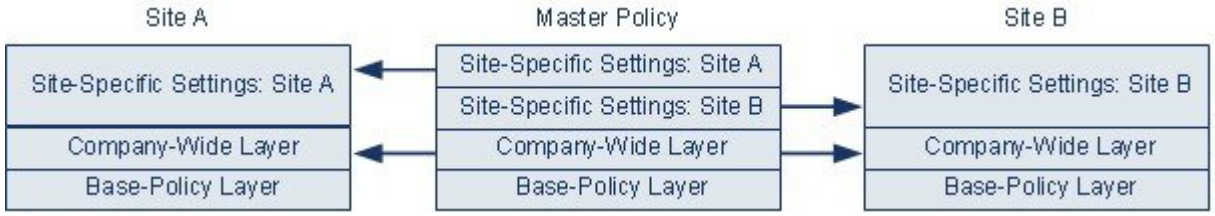
ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

ポリシー間でのレイヤの共有

ライセンス：Protection

ユーザ設定可能なレイヤは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）と共有できます。共有レイヤ内の設定を変更し、変更を確定すると、共有レイヤを使用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表示されます。レイヤを作成したポリシーでのみ、共有レイヤの機能設定を変更できます。

次の図は、サイト固有のポリシーのソースとして機能するマスターポリシーの例を示しています。



図内のマスター ポリシーには、Site A と Site B のポリシーに適用可能な設定を持つ全社的レイヤが含まれています。また、各ポリシーのサイト固有のレイヤも含まれています。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。

この例のマスター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、またはネットワーク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。

ヒント 基本ポリシーが共有対象のレイヤが作成されたカスタム ポリシーである場合は、ポリシーに共有レイヤを追加できません。変更を保存しようとすると、ポリシーに循環依存関係が含まれていることを示すエラー メッセージが表示されます。詳細については、「カスタム基本ポリシーについて （3 ページ）」を参照してください。

他のポリシーとレイヤを共有するには、次の手順を実行します。

- 共有するレイヤのサマリ ページで共有を有効にします。
- レイヤを共有するポリシーの [Policy Layers] ページに、共有するレイヤを追加します。

ポリシー間でのレイヤの共有

別のポリシーで使用されているレイヤの共有を無効にすることはできません。まずその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。

他のポリシーとのレイヤ共有を有効化/無効化する方法：

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

[Policy Layers] ページが表示されます。

ステップ 2 他のポリシーと共有するレイヤの横にある編集アイコンをクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3 [Sharing] チェックボックスをオン（有効）またはオフ（無効）にします。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。

詳細については、競合の解決とポリシー変更の確定を参照してください。

ポリシーへの共有レイヤの追加方法：

ステップ 5 ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 6 [Add Shared Layer] ドロップダウンリストから追加する共有レイヤを選択し、[OK] をクリックします。

[Policy Layers] サマリ ページが表示され、選択した共有レイヤがポリシー内の最上位レイヤとして表示されます。

その他のポリシーに共有レイヤがない場合、ドロップダウンリストは表示されません。ポップアップ ウィンドウで [OK] または [Cancel] をクリックすると、[Policy Layers] サマリ ページに戻ります。

ステップ 7 ユーザ レイヤの横にある共有レイヤ追加アイコン（  ）をクリックします。

[Add Shared Layer] ポップアップ ウィンドウが表示されます。

ステップ 8 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。

詳細については、競合の解決とポリシー変更の確定 を参照してください。

レイヤでの侵入ルールの設定

ライセンス：Protection

侵入ポリシーでは、すべてのユーザ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、侵入ポリシーの [Rules] ページでの操作と同様に、そのレイヤの [Rules] ページに設定を追加します（ルールを使用した侵入ポリシーの調整を参照）。

レイヤの [Rules] ページで個々の設定を表示することも、[Rules] ページのポリシー ビューですべての設定の実質的な効果を表示することもできます。[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。[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 *2*: 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。詳細については、「ルール状態の設定」を参照してください。 基本ポリシーまたは下位レイヤのルール状態をルールに継承させる場合は、ルール状態を [Inherit] に設定します。ただし、侵入ポリシーの [Rules] ページで作業している場合は、ルール状態を [Inherit] に設定できません。 特定のレイヤの [Rules]ページでルール状態を表示すると、ルール状態が色分け表示されます。有効状態が下位レイヤで設定されているルールは黄色で、上位レイヤで設定されているルールは赤色で強調表示されます。有効状態が現在のレイヤで設定されているルールは強調表示されません。侵入ポリシーの [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。
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。詳細については、イベントしきい値の設定およびSNMPアラートの追加を参照してください。

設定可能なレイヤ数	設定の種類	目的
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。詳細については、侵入ポリシーごとの抑制の設定および動的ルール状態の追加を参照してください。
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。詳細については、「動的ルール状態の追加」を参照してください。

たとえば、あるレイヤでルール状態を [Drop and Generate Events] に設定し、それよりも上位のレイヤで [Disabled] に設定した場合、侵入ポリシーの [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、[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。

レイヤでのルールの変更方法：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] を展開し、変更するポリシー レイヤを展開します。

ステップ 2 変更するポリシー レイヤのすぐ下にある [Rules] をクリックします。

レイヤの [Rules] ページが表示されます。

表「レイヤ ルールの設定」のいずれかの設定を変更できます。#unique_330 unique_330_Connect_42_Table（13 ページ）侵入ルールの設定の詳細については、ルールを使用した侵入ポリシーの調整を参照してください。

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 [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 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

マルチレイヤ ルールの設定の削除

ライセンス：Protection

侵入ポリシーの [Rules] ページで 1 つ以上のルールを選択して、侵入ポリシーの複数のレイヤから特定タイプのイベント 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、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。レイヤにルール状態が設定されている場合は、レイヤからその設定が削除され、その設定タイプの削除は中止されます。

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。詳細については、「ルール状態の設定」を参照してください。

複数のレイヤのルール設定を削除する方法：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Information] のすぐ下にある [Rules] をクリックします。

ヒント また、任意のレイヤの [Rules] ページでレイヤのドロップダウン リストから [Policy] を選択するか、[Policy Information] ページの [Manage Rules] を選択することもできます。

侵入ポリシーの [Rules] ページが表示されます。

ステップ 2 複数の設定を削除するルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタ処理についておよび侵入ポリシー内のルール フィルタの設定を参照してください。

ステップ 3 次の選択肢があります。

- ルールのすべてのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] を選択します。
- ルールのすべての抑制を削除するには、[Event Filtering] > [Remove Suppressions] を選択します。

- ルールのレートベースのルール状態をすべて削除するには、[Dynamic State] > [Remove Rate-Based Rule States] の順に選択します。
- ルールのすべての SNMP アラート設定を削除するには、[Alerting] > [Remove SNMP Alerts] を選択します。

確認ポップアップ ウィンドウが表示されます。

（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。詳細については、「ルール状態の設定」を参照してください。

ステップ 4 [OK] をクリックします。

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。システムが残りの設定をコピーする方法に影響を与える条件については、この手順の概要を参照してください。

ステップ 5 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

カスタム基本ポリシーからのルール変更の受け入れ

ライセンス：Protection

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で、ベースポリシーとして別のカスタム ポリシーを使用するときは、以下の場合に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 ルールに対するイベント フィルタ、動的状態、または SNMP アラートを削除する。および
- 基本ポリシーとして使用している他のカスタム ポリシーで、ルールに対して加える以降の変更をルールが受け入れるようにする

次の手順は、これを完了させる方法を示しています。階層を追加したポリシーでこれらのルールの設定を受け入れるには、マルチレイヤ ルールの設定の削除 （15 ページ）を参照してください。

レイヤを追加しなかったポリシー内でのルール変更を受け入れるには：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] リンクを展開し、[My Changes] を展開します。

ステップ 2 [My Changes] のすぐ下にある [Rules] リンクをクリックします。

My Changes レイヤの [Rules] ページが表示されます。

ステップ 3 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。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタ処理についておよび侵入ポリシー内のルール フィルタの設定を参照してください。

ステップ 4 [Rule State] ドロップダウン リストから、[Inherit] を選択します。

ステップ 5 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。

層のプリプロセッサと詳細の設定

ライセンス：Protection

ネットワーク分析ポリシーでのプリプロセッサの設定および侵入ポリシーでの詳細設定の設定と同様の方法を使用します。ネットワーク分析の [Settings] ページでプリプロセッサを有効化/無効化したり、侵入ポリシーの [Advanced Settings] ページで侵入ポリシーの詳細設定を有効化/無効化することができます。これらのページには、すべての関連機能の有効状態の概要も表示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤで無効になっており、そのレイヤよりも上位のレイヤで有効になっている場合、[Settings] ページではそのプリプロセッサが有効であると表示されます。このページで加えられる変更は、ポリシーの最上位のレイヤに表示されます。

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、レイヤの名前と説明を変更したり、同じタイプの他のポリシーとレイヤを共有するかどうかを設定できます。詳細については、ポリシー間でのレイヤの共有 （11 ページ）を参照してください。ナビゲーション パネルの [Policy Layers] の下にある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 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、ナビゲーション パネルのレイヤ名の下にその機能の設定ページへのサブリンクが表示され、レイヤのサマリ ページの機能の横に編集アイコンが表示されます。これらは、レイヤで機能を無効化するか、[Inherit] に設定すると表示されなくなります。

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、下位レイヤでこの機能の状態と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、基本ポリシーまたは下位レイヤの状態と設定を継承させる場合は、状態を [Inherit] に設定します。[Settings or Advanced Settings] ページで作業するときは、[Inherit] の選択が表示されません。

各レイヤのサマリ ページは次のように色分けされており、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：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
- 強調表示なし：有効な設定は現在のレイヤにあります

[Settings] および [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、これらのページでは有効な設定の位置を示すためのカラー コーディングは使用されません。

システムでは、設定が有効になっている最も上位のレイヤの設定が使用されます。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、ネットワーク分析 DCE/RPC プリプロセッサをあるレイヤで有効にして変更し、それよりも上位のレイヤでは有効にするが、変更しない場合は、上位レイヤのデフォルト設定が使用されます。

次の表に、ユーザ設定可能なレイヤのサマリ ページで実行できる操作を示します。

表 *3:* レイヤのサマリ ページの操作

目的	操作
レイヤの名前または説明の変更	[名前（Name）] または [説明（Description）] の新しい値を入力します。
他の侵入ポリシーとのレイヤの共有	[他のポリシーによるこのレイヤの使用を許可（Allow this layer to be used by other policies）] を選択します。 詳細については、「ポリシー間でのレイヤの共有 （11 ページ）」 を参照してください。
現在のレイヤのプリプロセッサ/詳細設定を有効化/無効化する	機能の横にある [Enabled] または [Disabled] をクリックします。 有効にすると、ナビゲーション パネルのレイヤ名の下に設定ページへのサブリンクが表示され、サマリ ページの機能の横に編集アイコンが表示されます。 無効にすると、サブリンクと編集アイコンが削除されます。
現在のレイヤの下にある最も上位のレイヤの設定から、プリプロセッサ/詳細設定の状態と設定を継承する	[Inherit] をクリックします。 ページが更新され、機能が有効だった場合は、ナビゲーション パネルの機能のサブリンクおよび編集アイコンが表示されなくなります。
有効なプリプロセッサ/詳細設定の設定ページにアクセスする	編集アイコンまたは機能のサブリンクをクリックして、現在の設定を変更します。 Back Orifice プリプロセッサに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。

ユーザ レイヤのプリプロセッサ/詳細設定を変更する方法：

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

レイヤのサマリ ページが表示されます。

ステップ 2 表「レイヤのサマリ ページの操作」のいずれかの操作を実行できます。

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 を参照してください。