Using Layers in a Network Analysis or Intrusion Policy

Larger organizations with many managed devices may have many intrusion policies and network analysis policies to support the unique needs of different departments, business units or, in some instances, different companies. Configurations in both policy types are contained in building blocks called *layers,* which you can use to efficiently manage multiple policies.

Layers in intrusion and network analysis policies work in essentially the same way. You can create and edit either policy type without consciously using layers. You can modify your policy configurations and, if you have not added user layers to your policy, the system automatically includes your changes in a single configurable layer that is initially named *My Changes*. Optionally, you can also add up to 200 layers where you can configure any combination of settings. You can copy, merge, move, and delete user layers and, most important, share individual user layers with other policies of the same type.

See the following sections for more information:

- Understanding the Layer Stack, page 24-1 describes the user-configurable and built-in layers that comprise a basic policy.
- Managing Layers, page 24-6 explains how to use layers in your policies.

Understanding the Layer Stack

License: Protection

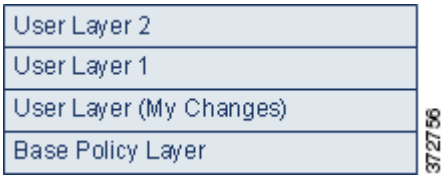
A network analysis or intrusion policy where you do not add layers includes the built-in, read-only base policy layer and a single user-configurable layer that is initially named My Changes. You can copy, merge, move, or delete any user-configurable layer and set any user-configurable layer to be shared by other policies of the same type.

Each policy layer contains complete configurations for either all preprocessors in a network analysis policy or all intrusion rules and advanced settings in an intrusion policy. The lowest, base policy layer includes all the settings from the base policy you selected when you created the policy. A setting in a higher layer takes precedence over the same setting in a lower layer. Features not explicitly set in a layer *inherit* their settings from the next highest layer where they are explicitly set.

The system *flattens* the layers, that is, it applies only the cumulative effect of all settings, when it handles network traffic.

Tip You can create an intrusion or network analysis policy based solely on the default settings in the base policy and, optionally in the case of an intrusion policy, using FireSIGHT rule state recommendations.

The following figure shows an example layer stack that, in addition to the base policy layer and the initial My Changes layer, also includes two additional user-configurable layers, *User Layer 1* and *User Layer 2*. Note in the figure that each user-configurable layer that you add is initially positioned as the highest layer in the stack; thus, User Layer 2 in the figure was added last and is highest in the stack.



Note the following points when working with multiple layers:

- When the highest layer in your policy is a read-only layer, or a shared layer as described in Sharing Layers Between Policies, page 24-10, the system automatically adds a user-configurable layer as the highest layer in your intrusion policy if you do either of the following:
  - modify a rule action (that is, a rule state, event filtering, dynamic state, or alerting) on the intrusion policy Rules page. See Tuning Intrusion Policies Using Rules, page 32-1 for more information.
  - enable, disable, or modify any preprocessor, intrusion rule, or advanced setting.

  All settings in the system-added layer are inherited except for the changes that resulted in the new layer.
- When the highest layer is a shared layer, the system adds a layer when you take either of the following actions:
  - share the highest layer with other policies
  - add a shared layer to your policy
- Regardless of whether you allow rule updates to modify your policy, changes in a rule update never override changes you make in a layer. This is because changes in a rule update are made in the base policy, which determines the default settings in your base policy layer; your changes are always made in a higher layer, so they override any changes that a rule update makes to your base policy. See Importing Rule Updates and Local Rule Files, page 66-15 for more information.

See the following sections for more information:

- Understanding the Base Layer, page 24-2
- Understanding the FireSIGHT Recommendations Layer, page 24-5

Understanding the Base Layer

License: Protection

The base layer, also referred to as the base policy, of an intrusion or network analysis policy defines the default settings for all configurations in the policy, and is the lowest layer in the policy. When you create a new policy and change a setting without adding new layers, the change is stored in the My Changes layer, and overrides—but does not change—the setting in the base policy.

See the following sections for more information:

- Understanding System-Provided Base Policies, page 24-3
- Understanding Custom Base Policies, page 24-3
- Changing the Base Policy, page 24-4
- Allowing Rule Updates to Modify a System-Provided Base Policy, page 24-4

Understanding System-Provided Base Policies

License: Protection

Cisco delivers several pairs of network analysis and intrusion policies with the FireSIGHT System. By using system-provided network analysis and intrusion policies, you can take advantage of the experience of the Cisco Vulnerability Research Team (VRT). For these policies, the VRT sets intrusion and preprocessor rule states, as well as provides the initial configurations for preprocessors and other advanced settings. You can use these system-provided policies as-is, or you can use them as the base for custom policies.

If you use a system-provided policy as your base, importing rule updates may modify settings in your base policy. However, you can configure a custom policy to not automatically make these changes to its system-provided base policy. This allows you to update system-provided base policies manually, on a schedule independent of rule update imports. In either case, changes that a rule update makes to your base policy do not change or override settings in your My Changes or any other layer. For more information, see Allowing Rule Updates to Modify a System-Provided Base Policy, page 24-4.

System-provided intrusion and network analysis policies are similarly named but contain different configurations. For example, the Balanced Security and Connectivity network analysis policy and the Balanced Security and Connectivity intrusion policy work together and can both be updated in intrusion rule updates. For more information, see Understanding the System-Provided Policies, page 23-8.

Understanding Custom Base Policies

License: Protection

If you do not want to use a system-provided policy as the base policy in your network analysis or intrusion policy, you can use a custom policy as your base. You can tune settings in custom policies to inspect traffic in ways that matter most to you so you can improve both the performance of your managed devices and your ability to respond effectively to the events they generate.

You can chain up to five custom policies, with four of the five using one of the other four previously created policies as its base policy; the fifth must use a system-provided policy as its base.

Changes you make to a custom policy that you use as the base for another policy are automatically used as the default settings the of policy that uses the base. Additionally, because all policies have a system-provided policy as the eventual base in a policy chain, importing a rule update may affect your policy even if you use a custom base policy. If the first custom policy in a chain (the one that uses the system-provided policy as its base) allows rule updates to modify its base policy, your policy may be affected. For information on changing this setting, see Allowing Rule Updates to Modify a System-Provided Base Policy, page 24-4.

Regardless of how they are made, changes to your base policy—whether by a rule update or when you modify a custom policy that you use as a base policy—do not change or override settings in your My Changes or any other layer.

Changing the Base Policy

License: Protection

You can select a different base policy for your network analysis or intrusion policy and, optionally, allow rule updates to modify a system-provided base policy, without affecting modifications in higher layers.

To change the base policy:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Information** in the navigation panel.

The Policy Information page appears.

Step 2 Select a base policy from the **Base Policy** drop-down list.

Step 3 Optionally, if you choose a system-provided base policy, click **Manage Base Policy** to specify whether intrusion rule updates can automatically modify your base policy.

For more information, see Allowing Rule Updates to Modify a System-Provided Base Policy, page 24-4.

Step 4 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Allowing Rule Updates to Modify a System-Provided Base Policy

License: Protection

Rule updates that you import provide system-provided policies with modified network analysis preprocessor settings, modified intrusion policy advanced settings, new and updated intrusion rules, and modified states for existing rules. Rule updates can also delete rules and provide new rule categories and default variables. See Importing Rule Updates and Local Rule Files, page 66-15 for more information.

Rule updates always modify system-provided policies with any changes to preprocessors, advanced settings, and rules. Changes to default variables and rule categories are handled at the system level. See Understanding System-Provided Base Policies, page 24-3 for more information.

When you use a system-provided policy as your base policy, you can allow rule updates to modify your base policy which, in this case, is a copy of the system-provided policy. If you allow rule updates to update your base policy, a new rule update makes the same changes in your base policy that it makes to the system-provided policy that you use as your base policy. If you have not modified the corresponding setting, a setting in your base policy determines the setting in your policy. However, rule updates do not override changes you make in your policy.

If you do not allow rule updates to update your base policy, you can manually update your base policy after importing one or more rule updates.

Rule updates always delete intrusion rules that VRT deletes, regardless of the rule state in your intrusion policy or whether you allow rule updates to update your base intrusion policy. Until you reapply your changes to network traffic, rules in your currently applied intrusion policies behave as follows:

- Disabled rules remain disabled.
- Rules set to Generate Events continue to generate events when triggered.
- Rules set to Drop and Generate Events continue to generate events and drop offending packets when triggered.

Rule updates do not modify a custom base policy unless both of the following conditions are met:

- You allow rule updates to modify the system-provided base policy of the parent policy, that is, the policy that originated the custom base policy.
- You have not made changes in the parent policy that override the corresponding settings in the parent's base policy.

When both conditions are met, changes in the rule update are passed to the child policy, that is, the policy using the custom base policy, when you save the parent policy.

For example, if a rule update enables a previously disabled intrusion rule, and you have not modified the rule's state in the parent intrusion policy, the modified rule state is passed to the base policy when you save the parent policy.

Likewise, if a rule update modifies a default preprocessor setting and you have not modified the setting in the parent network analysis policy, the modified setting is passed to the base policy when you save the parent policy.

See Changing the Base Policy, page 24-4 for more information.

To allow rule updates to modify a system-provided base policy:

Access: Admin/Intrusion Admin

Step 1 While editing a policy that uses a system-provided policy as its base policy, click **Policy Information** in the navigation panel.

The Policy Information page appears.

Step 2 Click **Manage Base Policy**.

The Base Policy summary page appears.

Step 3 Select or clear the **Update when a new Rule Update is installed** check box.

When you save your policy with the check box cleared and then import a rule update, an **Update Now** button appears on the Base Policy summary page and the status message on the page updates to inform you that the policy is out of date. Optionally, you can click **Update Now** to update your base policy with the changes in the most recently imported rule update.

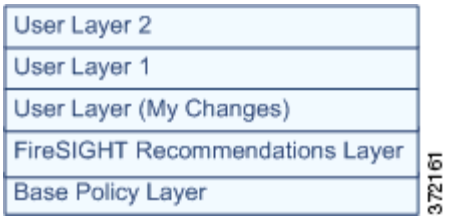
Step 4 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Understanding the FireSIGHT Recommendations Layer

License: Protection

When you generate rule state recommendations in an intrusion policy, you can choose whether to automatically modify rule states based on the recommendations. See Tailoring Intrusion Protection to Your Network Assets, page 33-1for more information.

As seen in the following figure, using recommended rule states adds a read-only, built-in FireSIGHT Recommendations layer immediately above the base layer.



Note that this layer is unique to intrusion policies.

If you subsequently choose not to use recommended rule states, the system removes the FireSIGHT Recommendations layer. You cannot manually delete this layer, but you can add and remove it by choosing to use or not use recommended rule states.

Adding the FireSIGHT Recommendations layer adds a FireSIGHT Recommendations link under Policy Layers in the navigation panel. This link leads you to a read-only view of the FireSIGHT Recommendations layer page where you can access a recommendation-filtered view of the Rules page in read-only mode. See Tuning Intrusion Policies Using Rules, page 32-1 for more information on working with rules on the Rules page.

Using recommended rule states also adds a Rules sublink beneath the FireSIGHT Recommendations link in the navigation panel. The Rules sublink provides access to a read-only display of the Rules page in the FireSIGHT Recommendations layer. Note the following in this view:

- When there is no rule state icon in the state column, the state is inherited from the base policy.
- When there is no rule state icon in the FireSIGHT Recommendations column in this or other Rules page views, there is no recommendation for this rule.

Tip When a rule state is not recommended, the rule's overhead rating was higher than the setting for **Recommendation Threshold (By Rule Overhead)** when recommendations were generated. See Understanding Rule Overhead, page 33-3 for more information.

Managing Layers

License: Protection

The Policy Layers page provides a single-page summary of the complete layer stack for your network analysis or intrusion policy. On this page you can add shared and unshared layers, copy, merge, move, and delete layers, access the summary page for each layer, and access configuration pages for enabled, disabled, and overridden configurations within each layer.

For each layer, you can view the following information:

- whether the layer is a built-in, shared user, or unshared user layer
- which layers contain the highest, that is the effective, preprocessor or advanced setting configurations, by feature name
- in an intrusion policy, the number of intrusion rules whose states are set in the layer, and the number of rules set to each rule state.

The feature name in the summary for each layer indicates which configurations are enabled, disabled, overridden, or inherited in the layer, as follows:

When the feature is...	The feature name is...
enabled in the layer	written in plain text
disabled in the layer	struck out
overridden by the configuration in a higher layer	written in italic text
inherited from a lower layer	not present

This page also provides a summary of the net effect of all enabled preprocessors (network analysis) or advanced settings (intrusion) and, for intrusion policies, intrusion rules.

The following table lists the actions available on the Policy Layers page.

Table 24-1 Network Analysis and Intrusion Policy Layer Configuration Actions

To...	You can...
display the Policy Information page	click **Policy Summary**. See Tuning Intrusion Policies Using Rules, page 32-1, Getting Started with Network Analysis Policies, page 26-1, and Getting Started with Intrusion Policies, page 31-1 for information on the actions you can take on the Policy Information page.
display the summary page for a layer	click the layer name in the row for the layer or, alternately, click the edit icon ( ) next to a user layer. You can also click the view icon ( ) to access the read-only summary page for a shared layer. See Sharing Layers Between Policies, page 24-10, Configuring Preprocessors and Advanced Settings in Layers, page 24-15, and Configuring Intrusion Rules in Layers, page 24-12 for information on actions you can take on the summary page for a layer.
access a layer-level preprocessor or advanced setting configuration page	click the feature name in the row for the layer. Note that configuration pages are read-only in the base policy and in shared layers. See Configuring Preprocessors and Advanced Settings in Layers, page 24-15 for more information.
access a layer-level rule configuration page filtered by rule state type	click the icon for drop and generate events ( ), generate events ( ), or disabled ( ) in the summary for the layer. No rules are displayed if the layer contains no rules set to the selected rule state.
add a layer to your policy	see Adding a Layer, page 24-8.
add a shared layer from another policy	see Sharing Layers Between Policies, page 24-10.
change a layer's name or description	see Changing a Layer's Name and Description, page 24-8.
move, copy, or delete a layer	see Moving, Copying, and Deleting Layers, page 24-9.
merge a layer into the next layer beneath it	see Merging Layers, page 24-10.

To use the Policy Layers page:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers summary page appears.

Step 2 You can take any of the actions in the Network Analysis and Intrusion Policy Layer Configuration Actions table.

Step 3 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Adding a Layer

License: Protection

You can add up to 200 layers to a network analysis or intrusion policy. When you add a layer, it appears as the highest layer in your policy. The initial state is Inherit for all features and, in an intrusion policy, no event filtering, dynamic state, or alerting rule actions are set.

To add a layer to your network analysis or intrusion policy:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers page appears.

Step 2 Click the add layer icon ( ) next to User Layers.

The Add Layer pop-up window appears.

Step 3 Type a unique layer **Name** and click **OK**.

The new layer appears as the topmost layer under User Layers.

Step 4 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Changing a Layer's Name and Description

License: Protection

You can change the name of a user-configurable layer in your network analysis or intrusion policy and, optionally, add or modify a description that is visible when you edit the layer.

To change a layer's name and add or modify its description:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers page appears.

Step 2 Click the edit icon ( ) next to the user layer you want to edit.

The summary page for the layer appears.

Step 3 You can take the following actions:

- Modify the layer **Name**.
- Add or modify the layer **Description**.

Step 4 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Moving, Copying, and Deleting Layers

License: Protection

You can copy, move, or delete a user layer in your network analysis or intrusion policy, including the initial My Changes layer. Note the following considerations:

- When you copy a layer, the copy appears as the highest layer.
- Copying a shared layer creates an unshared copy which, optionally, you can then share with other policies.
- You cannot delete a shared layer; a layer with sharing enabled that you have not shared with another policy is not a shared layer.

To copy, move, or delete a layer:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers page appears.

Step 2 You can take the following actions:

- To copy a layer, click the copy icon ( ) for the layer you want to copy.

  The page refreshes and a copy of the layer appears as the highest layer.
- To move a layer up or down within the User Layers page area, click any open area in the layer summary and drag until the position arrow ( ) points to a line above or below a layer where you want to move the layer.

  The screen refreshes and the layer appears in the new location.
- To delete a layer, click the delete icon ( ) for the layer you want to delete, then click **OK**

  The page refreshes and the layer is deleted.

Step 3 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Merging Layers

License: Protection

You can merge a user-configurable layer in your network analysis or intrusion policy with the next user layer beneath it. A merged layer retains all settings that were unique to either layer, and accepts the settings from the higher layer if both layers included settings for the same preprocessor, intrusion rule, or advanced setting. The merged layer retains the name of the lower layer.

In the policy where you create a shared layer that you add to other policies, you can merge an unshared layer immediately above the shared layer with the shared layer, but you cannot merge the shared layer with an unshared layer beneath it.

In a policy where you add a shared layer that you created in another policy, you can merge the shared layer into an unshared layer immediately beneath it and the resulting layer is no longer shared; you cannot merge an unshared layer into a shared layer beneath it.

To merge a user layer with a user layer beneath it:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers page appears.

Step 2 Click the merge icon ( ) in the upper of the two layers, then click **OK**.

The page refreshes and the layer is merged with the layer beneath it.

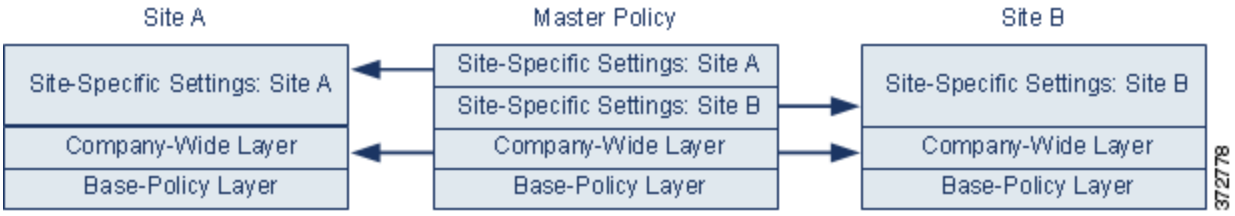
Step 3 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Sharing Layers Between Policies

License: Protection

You can share a user-configurable layer with other policies of the same type (intrusion or network analysis). When you modify a configuration within a shared layer and then commit your changes, the system updates all policies that use the shared layer and provides you with a list of all affected policies. You can only modify shared layer feature configurations in the policy where you created the layer.

The following figure shows an example master policy that serves as the source for site-specific policies.



The master policy in the figure includes a company-wide layer with settings applicable to the policies at Site A and Site B. It also includes site-specific layers for each policy. For example, in the case of a network analysis policy Site A might not have web servers on the monitored network and would not require the protection or processing overhead of the HTTP Inspect preprocessor, but both sites would

likely require TCP stream preprocessing. You could enable TCP stream processing in the company-wide layer that you share with both sites, disable the HTTP Inspect preprocessor in the site-specific layer that you share with Site A, and enable the HTTP Inspect preprocessor in the site-specific layer that you share with Site B. By editing configurations in a higher layer in the site-specific policies, you could also further tune the policy for each site if necessary with any configuration adjustments.

It is unlikely that the flattened net settings in the example master policy would be useful for monitoring traffic, but the time saved in configuring and updating the site-specific policies makes this a useful application of policy layers.

Many other layer configurations are possible. For example, you could define policy layers by company, by department, by network, or even by user. In the case of an intrusion policy, you could also include advanced settings in one layer and rule settings in another.

Tip You cannot add a shared layer to a policy when your base policy is a custom policy where the layer you want to share was created. When you attempt to save your changes, an error message indicates that the policy includes a circular dependency. See Understanding Custom Base Policies, page 24-3 for more information.

To share a layer with other policies, you must do the following:

- Enable sharing on the layer summary page of the layer you want to share.
- Add the shared layer on the Policy Layers page of the policy where you want to share it.

You cannot disable sharing for a layer that is in use in another policy; you must first delete the layer from the other policy or delete the other policy.

To enable or disable sharing a layer with other policies:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers page appears.

Step 2 Click the edit icon ( ) next to the layer you want to share with other policies.

The summary page for the layer appears.

Step 3 Select (enable) or clear (disable) the **Sharing** check box.

Step 4 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

To add a shared layer to your policy:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, click **Policy Layers** in the navigation panel.

The Policy Layers page appears.

Step 2 Click the add shared layer icon ( ) next to User Layers.

The Add Shared Layer pop-up window appears.

Step 3 Select the shared layer you want to add from the Add Shared Layer drop-down list, then click **OK**.

The Policy Layers summary page appears and the shared layer you selected appears as the highest layer in your policy.

If there are no shared layers in any other policies, no drop-down list appears; click **OK** or **Cancel** on the pop-up window to return to the Policy Layers summary page.

Step 4 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Configuring Intrusion Rules in Layers

License: Protection

In an intrusion policy, you can set the rule state, event filtering, dynamic state, alerting, and rule comments for a rule in any user-configurable layer. After accessing the layer where you want to make your changes, you add settings on the Rules page for the layer the same as you would on the intrusion policy Rules page; see Tuning Intrusion Policies Using Rules, page 32-1.

You can view individual layer settings on the Rules page for the layer, or view the net effect of all settings on the policy view of the Rules page. When you modify rule settings on the policy view of the Rules page, you are modifying the highest user-configurable layer in the policy. You can switch to another layer using the layer drop-down list on any Rules page.

The following table describes the effects of configuring the same type of setting in multiple layers.

Table 24-2 Layer Rule Settings

You can set...	Of this setting type...	To...
one	rule state	override a rule state set for the rule in a lower layer, and ignore all thresholds, suppressions, rate-based rule states, and alerts for that rule configured in lower layers. See Setting Rule States, page 32-20 for more information. If you want a rule to inherit its state from the base policy or a lower layer, set the rule state to Inherit. Note that when you are working on the intrusion policy Rules page, you cannot set a rule state to Inherit. Note also that rule state settings are color-coded when you view them on the Rules page for a specific layer: rules whose effective state is set in a lower layer are highlighted in yellow; rules whose effective state is set in a higher layer are highlighted in red; rules whose effective state is set in the current layer are not highlighted. Because the intrusion policy Rules page is a composite view of the net effect of all rule settings, rule states are not color-coded on this page.
one	threshold SNMP alert	override a setting of the same type for the rule in a lower layer. Note that setting a threshold overwrites any existing threshold for the rule in the layer. See Configuring Event Thresholding, page 32-22 and Adding SNMP Alerts, page 32-33 for more information.

Table 24-2 Layer Rule Settings (continued)

You can set...	Of this setting type...	To...
one or more	suppression rate-based rule state	cumulatively combine settings of the same type for each selected rule down to the first layer where a rule state is set for the rule. Settings below the layer where a rule state is set are ignored. See Configuring Suppression Per Intrusion Policy, page 32-27 and Adding Dynamic Rule States, page 32-29 for more information.
one or more	comment	add a comment to a rule. Comments are rule-specific, not policy- or layer-specific. You can add one or more comments to a rule in any layer. See Adding a Rule Comment for a Rule, page 32-9 for more information.

For example, if you set a rule state to Drop and Generate Events in one layer and to Disabled in a higher layer, the intrusion policy Rules page shows that the rule is disabled.

In another example, if you set a source-based suppression for a rule to 192.168.1.1 in one layer, and you also set a destination-based suppression for the rule to 192.168.1.2 in another layer, the Rules page shows that the cumulative effect is to suppress events for the source address 192.168.1.1 and the destination address 192.168.1.2. Note that suppression and rate-based rule state settings cumulatively combine settings of the same type for each selected rule down to the first layer where a rule state is set for the rule. Settings below the layer where a rule state is set are ignored.

To modify rules in a layer:

Access: Admin/Intrusion Admin

Step 1 While editing your intrusion policy, expand **Policy Layers** in the navigation panel and expand the policy layer you want to modify.

Step 2 Click **Rules** immediately beneath the policy layer you want to modify.

The Rules page for the layer appears.

You can modify any of the settings in the Layer Rule Settings table. See Tuning Intrusion Policies Using Rules, page 32-1 for more information on configuring intrusion rules.

To delete an individual setting from an editable layer, double-click the rule message on the Rules page for the layer to display rule details. Click **Delete** next to the setting you want to delete, then click **OK** twice.

Step 3 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Removing Multi-Layer Rule Settings

License: Protection

You can select one or more rules on the intrusion policy Rules page and then simultaneously remove a specific type of event filter, dynamic state, or alerting from multiple layers in your intrusion policy.

The system removes the setting type downward through each layer where it is set until it removes all the settings or encounters a layer where a rule state is set for the rule. If it encounters a layer where a rule state is set, it removes the setting from that layer and stops removing the setting type.

When the system encounters the setting type in a shared layer or in the base policy, and if the highest layer in the policy is editable, the system copies the remaining settings and rule state for the rule to that editable layer. Otherwise, if the highest layer in the policy is a shared layer, the system creates a new editable layer above the shared layer and copies the remaining settings and rule state for the rule to that editable layer.

Note Removing rule settings derived from a shared layer or the base policy causes any changes to this rule from lower layers or the base policy to be ignored. To stop ignoring changes from lower layers or the base policy, set the rule state to **Inherit** on the summary page for the topmost layer. See Setting Rule States, page 32-20 for more information.

To remove rule settings in multiple layers:

Access: Admin/Intrusion Admin

Step 1 While editing your intrusion policy, click **Rules** immediately beneath Policy Information in the navigation panel.

Tip You can also select **Policy** from the layer drop-down list on the Rules page for any layer, or select **Manage Rules** on the Policy Information page.

The intrusion policy Rules page appears.

Step 2 Select the rule or rules from which you want to remove multiple settings. You have the following options:

- To select a specific rule, select the check box next to the rule.
- To select all the rules in the current list, select the check box at the top of the column.

See Understanding Rule Filtering in an Intrusion Policy, page 32-10 and Setting a Rule Filter in an Intrusion Policy, page 32-18 for information on locating rules.

Step 3 You have the following options:

- To remove all thresholds for a rule, select **Event Filtering > Remove Thresholds**.
- To remove all suppression for a rule, select **Event Filtering > Remove Suppressions**.
- To remove all rate-based rule states for a rule, select **Dynamic State > Remove Rate-Based Rule States**.
- To remove all SNMP alert settings for a rule, select **Alerting > Remove SNMP Alerts**.

A confirmation pop-up window appears.

Note Removing rule settings derived from a shared layer or the base policy causes any changes to this rule from lower layers or the base policy to be ignored. To stop ignoring changes from lower layers or the base policy, set the rule state to **Inherit** on the summary page for the topmost layer. See Setting Rule States, page 32-20 for more information.

Step 4 Click **OK**.

The system removes the selected setting and copies the remaining settings for the rule to the highest editable layer in the policy. See the introduction to this procedure for conditions that affect how the system copies the remaining settings.

Step 5 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Accepting Rule Changes from a Custom Base Policy

License: Protection

When a custom network analysis or intrusion policy where you have not added layers uses another custom policy as its base policy, you must set a rule to inherit its rule state if:

- you delete an event filter, dynamic state, or SNMP alert set for the rule in the base policy, and
- you want the rule to accept subsequent changes that you make to it in the other custom policy that you use as your base policy

The following procedure explains how to accomplish this. See Removing Multi-Layer Rule Settings, page 24-13 to accept settings for these rules in a policy where you have added layers.

To accept rule changes in a policy where you have not added layers:

Access: Admin/Intrusion Admin

Step 1 While editing your intrusion policy, expand the **Policy Layers** link in the navigation panel, then expand the **My Changes** link.

Step 2 Click the **Rules** link immediately beneath My Changes.

The Rules page for the My Changes layer appears.

Step 3 Select the rule or rules whose settings you want to accept. You have the following options:

- To select a specific rule, select the check box next to the rule.
- To select all the rules in the current list, select the check box at the top of the column.

See Understanding Rule Filtering in an Intrusion Policy, page 32-10 and Setting a Rule Filter in an Intrusion Policy, page 32-18 for information on locating rules.

Step 4 Select **Inherit** from the **Rule State** drop-down list.

Step 5 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Configuring Preprocessors and Advanced Settings in Layers

License: Protection

You use similar mechanisms to configure preprocessors in a network analysis policy and advanced settings in an intrusion policy. You can enable and disable preprocessors on the network analysis Settings page and intrusion policy advanced settings on the intrusion policy Advanced Settings page. These pages also provide summaries of the effective states for all relevant features. For example, if the network analysis SSL preprocessor is disabled in one layer and enabled in a higher layer, the Settings page shows it as enabled. Changes made on these pages appear in the top layer of the policy.

You can also enable or disable preprocessors or advanced settings and access their configuration pages on the summary page for a user-configurable layer. On this page you can modify the layer name and description and configure whether to share the layer with other policies of the same type; see Sharing Layers Between Policies, page 24-10 for more information. You can switch to the summary page for another layer by selecting the layer name beneath **Policy Layers** in the navigation panel.

When you enable a preprocessor or advanced setting, a sublink to the configuration page for that feature appears beneath the layer name in the navigation panel, and an edit icon ( ) appears next to the feature on the summary page for the layer; these disappear when you disable the feature in the layer or set it to Inherit.

Setting the state (enabled or disabled) for a preprocessor or advanced setting overrides the state and configuration settings for that feature in lower layers. If you want a preprocessor or advanced setting to inherit its state and configuration from the base policy or a lower layer, set it to **Inherit**. Note that the Inherit selection is not available when you are working in the Settings or Advanced Settings page.

Color-coding on each layer summary page indicates as follows whether the effective configuration is in a higher, lower, or the current layer:

- red - the effective configuration is in a higher layer
- yellow - the effective configuration is in a lower layer
- unshaded - the effective configuration is in the current layer

Because the Settings and Advanced Settings pages are composite views of all relevant settings, these page do not use color coding to indicate the positions of effective configurations.

The system uses the configuration in the highest layer where the feature is enabled. Unless you explicitly modify the configuration, the system uses the default configuration. For example, if you enable and modify the network analysis DCE/RPC preprocessor in one layer, and you also enable but do not modify it in a higher layer, the system uses the default configuration in the higher layer.

The following table describes the actions available on the summary page for user-configurable layers.

Table 24-3 Layer Summary Page Actions

To...	You can...
modify the layer name or description	type a new value for **Name** or **Description**.
share the layer with other intrusion policies	select **Allow this layer to be used by other policies**. See Sharing Layers Between Policies, page 24-10 for more information.
enable or disable a preprocessor/advanced setting in the current layer	click **Enabled** or **Disabled** next to the feature. When you enable, a sublink to the configuration page appears beneath the layer name in the navigation panel, and an edit icon ( ) appears on the summary page next to the feature. Disabling removes the sublink and edit icon.
inherit the preprocessor/advanced setting state and configuration from the settings in the highest layer below the current layer	click **Inherit**. The page refreshes and, if the feature was enabled, the feature sublink in the navigation panel and the edit icon no longer appear.
access the configuration page for an enabled preprocessor/advanced setting	click the edit icon ( ) or the feature sublink to modify the current configuration. Note that the Back Orifice preprocessor has no user-configurable options.

To modify preprocessors/advanced settings in a user layer:

Access: Admin/Intrusion Admin

Step 1 While editing your policy, expand **Policy Layers** in the navigation panel, then click the name of the layer you want to modify.

The summary page for the layer appears.

Step 2 You can take any of the actions in the Layer Summary Page Actions table.

Step 3 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.