Creating Traffic Profiles

A traffic profile is just that—a profile of the traffic on your network, based on connection data collected over a time span that you specify. You can use connection data collected by your devices, the connection data exported by any or all of your NetFlow-enabled devices, or both.

After you create a traffic profile, you can detect abnormal network traffic by evaluating new traffic against your profile, which presumably represents normal network traffic.

Keep in mind that the FireSIGHT System uses connection data to create traffic profiles and trigger correlation rules based on traffic profile changes. You cannot include connections that you do not log to the Defense Center database in traffic profiles. The system uses only end-of-connection data to populate connection summaries (see Understanding Connection Summaries, page 39-3), which the system then uses to create connection graphs and traffic profiles. Therefore, if you want to create and use traffic profiles, make sure you log connection events at the end of connections.

The time span used to collect data to build your traffic profile is called the profiling time window (PTW). The PTW is a sliding window; that is, if your PTW is one week (the default), your traffic profile includes connection data collected over the last week. You can change the PTW to be as short as an hour or as long as several weeks.

When you first activate a traffic profile, it collects and evaluates connection data according to the criteria you have set, for a learning period equal in time to the PTW. The Defense Center does not evaluate rules you have written against the traffic profile until the learning period is complete.

You can create profiles using all the traffic on a monitored network segment, or you can create more targeted profiles using criteria based on the data in the connection events. For example, you could set the profile conditions so that the traffic profile only collects data where the detected session uses a specific port, protocol, or application. Or, you could add a host profile qualification to the traffic profile to collect data only for hosts that exhibit a host criticality of high.

Finally, when you create a traffic profile, you can specify inactive periods—periods in which connection data do not affect profile statistics and rules written against the profile do not trigger. You can also change how often the traffic profile aggregates and calculates statistics on collected connection data.

The following graphic shows a traffic profile with a PTW of one day and a sampling rate of five minutes.
After you create and activate a traffic profile and its learning period is complete, you can create correlation rules that trigger when you detect anomalous traffic. For example, you could write a rule that triggers if the amount of data traversing your network (measured in packets, KBytes, or number of connections) suddenly spikes to three standard deviations above the mean amount of traffic, which could indicate an attack or other security policy violation. Then, you could include that rule in a correlation policy to alert you of the traffic spike or to perform a remediation in response. For information on using traffic profiles to detect abnormal network traffic, see Creating Rules for Correlation Policies, page 51-2.

You create traffic profiles on the Traffic Profiles page. The slider icon next to each profile indicates whether the profile is active. If you want to base a correlation rule on a traffic profile change, you must activate the profile. If the slider icon is blue with a check mark, the profile is active. If it is gray with an x, the profile is inactive. For more information, see Activating and Deactivating Traffic Profiles, page 53-8.

The progress bar shows the status of the traffic profile’s learning period. When the progress bar reaches 100%, correlation rules written against the profile will trigger.

Tip
You can sort traffic profiles by state (active versus inactive) or alphabetically by name using the Sort by drop-down list.

For more information, see:
- Providing Basic Profile Information, page 53-3
- Specifying Traffic Profile Conditions, page 53-3
- Adding a Host Profile Qualification, page 53-5
Providing Basic Profile Information

License: FireSIGHT

When you create a traffic profile, you must give it a name and, optionally, a short description.

To begin creating a traffic profile:
Access: Admin/Discovery Admin

Step 1 Select Policies > Correlation, then click Traffic Profiles. The Traffic Profiles page appears.

Step 2 Click New Profile. The Create Profile page appears.

Step 3 In the Profile Name field, type a name of up to 255 characters for the new traffic profile.

Step 4 In the Profile Description field, type a short description of up to 255 characters of the new traffic profile.

Step 5 Continue with Specifying Traffic Profile Conditions.

Specifying Traffic Profile Conditions

License: FireSIGHT

Profile conditions constrain the kinds of connection data you want the traffic profile to track. A simple traffic profile that profiles all the traffic on a monitored network segment has no conditions. In contrast, traffic profiles can be complex, with multiple nested conditions.

For example, the traffic profile conditions in the following graphic collects HTTP connections on the 10.4.x.x subnet.
You build traffic profile conditions in the **Profile Conditions** section of the Create Profile page. See **Understanding Condition-Building Mechanics**, page 53-9 for information on building conditions. Also, the syntax you can use to build conditions is fully described in **Syntax for Traffic Profile Conditions**, page 53-4.

**Tip**

If you want to use the settings from an existing traffic profile, click **Copy Settings** and, in the pop-up window, select the traffic profile you want to use and click **Load**.

### Syntax for Traffic Profile Conditions

**License:** FireSIGHT

The following table describes how to build a traffic profile condition.

Keep in mind that NetFlow records do not contain information about which host in the connection is the initiator and which is the responder. When the system processes NetFlow records, it uses an algorithm to determine this information based on the ports each host is using, and whether those ports are well-known. For more information, see **Differences Between NetFlow and FireSIGHT Data**, page 45-17.

The information available for a traffic profile depends on several factors, including the detection method, the logging method, and event type. For more information, see **Information Available in Connection and Security Intelligence Events**, page 39-11.

**Table 53-1 Syntax for Profile Conditions**

<table>
<thead>
<tr>
<th>If you specify...</th>
<th>Select an operator, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Protocol</td>
<td>Select an application protocol name from the drop-down list of available protocols.</td>
</tr>
<tr>
<td>Application Protocol Category</td>
<td>Select an application protocol category name from the drop-down list of available categories.</td>
</tr>
<tr>
<td>Client</td>
<td>Select a client name from the drop-down list of available clients.</td>
</tr>
<tr>
<td>Client Category</td>
<td>Select a client category name from the drop-down list of available categories.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Specify in the traffic profile whether you want to use connection data collected by your Cisco devices or by NetFlow-enabled devices. If you do not specify a connection type, the traffic profile includes both.</td>
</tr>
<tr>
<td>Destination Country or Source Country</td>
<td>Select a country from the drop-down list of available countries. This represents the country associated with a source or destination IP address identified in network traffic.</td>
</tr>
<tr>
<td>Initiator IP, Responder IP, or...</td>
<td>Use a specific IP address or CIDR notation to specify a range of IP addresses. See <strong>Specifying IP Addresses in Searches</strong>, page 60-6 for a description of the syntax allowed for IP addresses. Note, however, that you <strong>cannot</strong> use the local or remote keywords to specify IP addresses that are or are not in the networks you are monitoring.</td>
</tr>
<tr>
<td>NetFlow Device</td>
<td>Select the NetFlow-enabled device whose data you want to use to create the traffic profile. If you did not add any NetFlow-enabled devices to your deployment (using the local configuration), the NetFlow Device drop-down list is blank.</td>
</tr>
<tr>
<td>Responder Port/ICMP Code</td>
<td>Type the port number or ICMP code.</td>
</tr>
</tbody>
</table>
Chapter 53   Creating Traffic Profiles

Adding a Host Profile Qualification

**License:** FireSIGHT

You can constrain any traffic profile with information from the host profile of the tracked hosts. This constraint is called a *host profile qualification*. For example, as shown in the following graphic, you could collect connection data only for hosts that are assigned a host criticality of **high**.

To use a host profile qualification, the host must exist in the database and the host profile property you want to use as a qualification must already be included in the host profile. For example, if you configure a correlation policy rule to trigger when an intrusion event is generated on a host running Windows, the rule only triggers if the host is already identified as Windows when the intrusion event is generated.

To add a host profile qualification:

**Access:** Admin/Discovery Admin

---

**Step 1**

On the Create Profile page, click **Add Host Profile Qualification**.

The Host Profile Qualification section appears.

**Step 2**

Build the host profile qualification’s conditions.

You can create a single, simple condition, or you can create more elaborate constructs by combining and nesting conditions. See [Understanding Condition-Building Mechanics](#), page 53-9 for information building conditions.

The syntax you can use to build conditions is described in [Syntax for Host Profile Qualifications](#), page 53-6.

---

**Tip**

To remove a host profile qualification, click **Remove Host Profile Qualification**.

---

### Table 53-1 Syntax for Profile Conditions (continued)

<table>
<thead>
<tr>
<th>If you specify...</th>
<th>Select an operator, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Intelligence Category</td>
<td>Select a Security Intelligence category name from the drop-down list of available categories. To use a Security Intelligence category for a traffic profile condition, that category must be set to <strong>Monitor</strong> instead of <strong>Block</strong> in the Security Intelligence section of your access control policy. For more information, see <a href="#">Building the Security Intelligence Whitelist and Blacklist</a>, page 13-3.</td>
</tr>
<tr>
<td>SSL Encrypted Session</td>
<td>Select <strong>Successfully Decrypted</strong>.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Type <strong>TCP</strong> or <strong>UDP</strong> as the transport protocol.</td>
</tr>
<tr>
<td>Web Application</td>
<td>Select a web application name from the drop-down list of available web applications.</td>
</tr>
<tr>
<td>Web Application Category</td>
<td>Select a web application category name from the drop-down list of available categories.</td>
</tr>
</tbody>
</table>
Adding a Host Profile Qualification

Syntax for Host Profile Qualifications

License: FireSIGHT

When you build a host profile qualification condition, you must first select the host you want to use to constrain your traffic profile. You can select either Responder Host or Initiator Host. After you select the host role, continue building your host profile qualification condition, as described in the Syntax for Host Profile Qualifications table.

Although you can configure the network discovery policy to add hosts to the network map based on data exported by NetFlow-enabled devices, the available information about these hosts is limited. For example, there is no operating system data available for these hosts, unless you provide it using the host input feature. In addition, if your traffic profile uses connection data exported by NetFlow-enabled devices, keep in mind that NetFlow records do not contain information about which host in the connection is the initiator and which is the responder. When the system processes NetFlow records, it uses an algorithm to determine this information based on the ports each host is using, and whether those ports are well-known. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

To match against implied or generic clients, create a host profile qualification based on the application protocol used by the server responding to the client. When the client list on a host that acts as the initiator or source of a connection includes an application protocol name followed by client, that client may actually be an implied client. In other words, the system reports that client based on server response traffic that uses the application protocol for that client, not on detected client traffic.

For example, if the system reports HTTPS client as a client on a host, create a host profile qualification for Responder Host where Application Protocol is set to HTTPS, because HTTPS client is reported as a generic client based on the HTTPS server response traffic sent by the responder or destination host.

Table 53-2 Syntax for Host Profile Qualifications

<table>
<thead>
<tr>
<th>If you specify...</th>
<th>Select an operator, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Type</td>
<td>Select one or more host types from the drop-down list. You can choose between a normal host or one of several types of network device.</td>
</tr>
<tr>
<td>NETBIOS Name</td>
<td>Type the NetBIOS name of the host.</td>
</tr>
<tr>
<td>Operating System &gt; OS Vendor</td>
<td>Select one or more operating system vendor names from the drop-down list.</td>
</tr>
<tr>
<td>Operating System &gt; OS Name</td>
<td>Select one or more operating system names from the drop-down list.</td>
</tr>
<tr>
<td>Operating System &gt; OS Version</td>
<td>Select one or more operating system versions from the drop-down list.</td>
</tr>
<tr>
<td>Network Protocol</td>
<td>Type the network protocol number as listed in <a href="http://www.iana.org/assignments/ethernet-numbers">http://www.iana.org/assignments/ethernet-numbers</a>.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Type the name or number of the transport protocol as listed in <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a>.</td>
</tr>
<tr>
<td>Host Criticality</td>
<td>Select the host criticality from the list that appears. You can select None, Low, Medium, or High. For more information on host criticality, see Working with the Predefined Host Attributes, page 49-30.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Type the VLAN ID number of the host.</td>
</tr>
<tr>
<td>Application Protocol</td>
<td>Select an application protocol from the drop-down list.</td>
</tr>
</tbody>
</table>
Chapter 53      Creating Traffic Profiles

Setting Profile Options

Table 53-2 Syntax for Host Profile Qualifications (continued)

<table>
<thead>
<tr>
<th>If you specify...</th>
<th>Select an operator, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Protocol &gt; Application Port</td>
<td>Type the application protocol port number.</td>
</tr>
<tr>
<td>Application Protocol &gt; Protocol</td>
<td>Select the protocol from the drop-down list.</td>
</tr>
<tr>
<td>Client &gt; Client</td>
<td>Select a client from the drop-down list.</td>
</tr>
<tr>
<td>Client &gt; Client Version</td>
<td>Type the client version.</td>
</tr>
<tr>
<td>Web Application</td>
<td>Select a client from the drop-down list.</td>
</tr>
<tr>
<td>MAC Address &gt; MAC Address</td>
<td>Type all or part of the MAC address of the host.</td>
</tr>
<tr>
<td>MAC Address &gt; MAC Type</td>
<td>Select whether the MAC type is ARP/DHCP Detected.</td>
</tr>
<tr>
<td></td>
<td>That is, select whether the system positively identified the MAC address as belonging to the</td>
</tr>
<tr>
<td></td>
<td>host (is ARP/DHCP Detected), whether the system is seeing many hosts with that MAC address</td>
</tr>
<tr>
<td></td>
<td>because, for example, there is a router between the device and the host (is not ARP/DHCP</td>
</tr>
<tr>
<td></td>
<td>Detected), or whether the MAC type is irrelevant (is any).</td>
</tr>
<tr>
<td>MAC Vendor</td>
<td>Type all or part of the MAC vendor of hardware used by the host.</td>
</tr>
<tr>
<td>any available host attribute, including</td>
<td>Specify the appropriate value, which depends on the type of host attribute you select:</td>
</tr>
<tr>
<td>the default compliance white list host</td>
<td>• If the host attribute type is Integer, enter an integer value in the range defined for the</td>
</tr>
<tr>
<td>attribute</td>
<td>attribute.</td>
</tr>
<tr>
<td></td>
<td>• If the host attribute type is Text, and enter a text value.</td>
</tr>
<tr>
<td></td>
<td>• If the host attribute type is List, select a valid list string from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• If the host attribute type is URL, enter a URL value.</td>
</tr>
<tr>
<td></td>
<td>For more information on host attributes, see Working with User-Defined Host Attributes,</td>
</tr>
<tr>
<td></td>
<td>page 49-31.</td>
</tr>
</tbody>
</table>

Tip

Your PTW should include at least 100 data points.

Setting Profile Options

License: FireSIGHT

The profiling time window (PTW) is the sliding time window, equal in length to the learning period, that the FireSIGHT System uses to calculate statistics for the traffic profile. The default PTW is one week, but you can change it to be as short as an hour or as long as several weeks.

Also, traffic profiles are based on aggregated connection data. By default, traffic profiles generate statistics on connection events generated by the system over five-minute intervals. However, you can set this sampling rate anywhere between the default five minutes and one hour.

Keep in mind that you should set your PTW and sampling rate so that your traffic profiles contain enough data to be statistically meaningful. For example, a PTW of one day with a sampling rate of one hour would only contain 24 data points, which may not be enough for accurate analysis of network traffic patterns.

Your PTW should include at least 100 data points.
You can also set up inactive periods in traffic profile. For example, consider a network infrastructure where all the workstations are backed up at midnight every night. The backup takes about 30 minutes and spikes the network traffic. In that case, you might want to set up a recurring inactive period for your traffic profile to coincide with the scheduled backups. During inactive periods, the traffic profile collects data (so you can see the traffic on the traffic profile graphs), but that data is not used when calculating profile statistics. You can set up inactive periods to recur daily, weekly, or monthly. Inactive periods can be as short as five minutes or as long as one hour. Traffic profile graphs plotted over time show inactive periods as a shaded region.

To set profile options:

Access: Admin/Discovery Admin

<table>
<thead>
<tr>
<th>Table 53-3</th>
<th>Profile Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to...</td>
<td>You can...</td>
</tr>
<tr>
<td>change the profiling time window</td>
<td>in the Profiling Time Window field, type the number of hours, days, or weeks. Then choose hour(s), day(s), or week(s) from the drop-down list.</td>
</tr>
<tr>
<td>change the sampling rate</td>
<td>select the rate from the Sampling Rate drop-down list.</td>
</tr>
<tr>
<td>add an inactive period</td>
<td>click Add Inactive Period. Then, using the drop-down lists, specify when and how often you want the traffic profile to refrain from collecting data.</td>
</tr>
<tr>
<td>delete an inactive period</td>
<td>click Delete next to the inactive period you want to delete.</td>
</tr>
</tbody>
</table>

Saving a Traffic Profile

License: FireSIGHT

Use the following procedure to save a traffic profile.

To save a traffic profile:

Access: Admin/Discovery Admin

Step 1

You have two options:

- To save the profile without activating it, click Save.
- To save the profile and start collecting data immediately, click Save & Activate.

Activating and Deactivating Traffic Profiles

License: FireSIGHT

When you want it to begin profiling the traffic on a monitored network segment, you must activate a traffic profile.
Deactivate a profile when you want it to stop collecting and evaluating connection data. Rules written against deactivated traffic profiles do not trigger. In addition, deactivating a traffic profile deletes all data collected and aggregated by the profile. If you later reactivate a deactivated traffic profile, you must wait the length of its PTW before rules written against it will trigger.

**To activate or deactivate a traffic profile:**

**Access:** Admin/Discovery Admin

---

**Step 1**

Select **Policies > Correlation**, then click **Traffic Profiles**.

The Traffic Profiles page appears.

**Step 2**

You have two options:

- To activate an inactive traffic profile, click **Activate** next to the profile.
- To deactivate an active traffic profile, click **Deactivate** next to the profile. Confirm that you want to deactivate the profile by clicking **OK**.

---

**Editing a Traffic Profile**

**License:** FireSIGHT

You cannot substantially edit an active traffic profile; if the traffic profile is active you can only change its name and description. To edit a traffic profile’s conditions options, you must first deactivate it. Note that deactivating a traffic profile deletes all the data it has collected.

For more information on activating and deactivating traffic profiles, see *Activating and Deactivating Traffic Profiles*, page 53-8.

**To edit a traffic profile:**

**Access:** Admin/Discovery Admin

---

**Step 1**

Select **Policies > Correlation**, then click **Traffic Profiles**.

The Traffic Profiles page appears.

**Step 2**

Next to the traffic profile you want to edit, click **Edit**.

The Create Profile page appears.

**Step 3**

Make changes to the profile and click **Save**.

Your profile is updated.

---

**Understanding Condition-Building Mechanics**

**License:** FireSIGHT

You build traffic profiles by specifying the conditions they use to collect data. You can create either simple conditions or more elaborate constructs with nested conditions.
For example, if you want to create a traffic profile that collects data for your entire monitored network segment, you can create a very simple profile with no conditions, as shown in the following graphic.

If you wanted to constrain the profile and collect data only for the 10.4.x.x network, you can add a single condition, as shown in the following graphic.

But the following traffic profile, which collects HTTP activity on the 10.4.x.x network and the 192.168.x.x network, has three conditions, with the last constituting a complex condition.

The syntax you can use within conditions varies depending on the element you are creating, but the mechanics are the same. For more information, see:

- Building a Single Condition, page 53-11
- Adding and Linking Conditions, page 53-13
- Using Multiple Values in a Condition, page 53-15
Building a Single Condition

License: FireSIGHT

Most conditions have three parts: a category, an operator, and a value. Some conditions are more complex and contain several categories, each of which may have their own operators and values.

For example, the following traffic profile collects information on the 10.4.x.x network. The category of the condition is **Initiator/Responder IP**, the operator is **is in**, and the value is **10.4.0.0/16**.

The following steps explain how to build this traffic profile condition.

**To build a single condition:**

**Access:** Admin/Discovery Admin

---

**Step 1** Select **Policies > Correlation**, then click **Traffic Profiles**.

The Traffic Profiles page appears.

**Step 2** Click **New Profile**.

The Create Profile page appears.

**Step 3** Under **Profile Conditions**, begin building the profile’s single condition by selecting **Initiator/Responder IP** from the first (category) drop-down list.

**Step 4** Select **is in** from the second (operator) drop-down list.

**Tip** When the category represents an IP address, choosing **is in** or **is not in** as the operator allows you to specify whether the IP address is in or is not in a range of IP addresses, as expressed in CIDR notation. For information on using CIDR notation in the FireSIGHT System, see [IP Address Conventions, page 1-22](#).

**Step 5** Type **10.4.0.0/16** in the text field.

In contrast, the following host profile qualification is more complex; it constrains a traffic profile such that it collects connection data only if the responding host in the detected connection is running a version of Microsoft Windows...
The following steps explain how to build this host profile qualification.

**To build this host profile qualification:**

**Access:** Admin/Discovery Admin

---

**Step 1**
Select *Policies > Correlation*, then click *Traffic Profiles*.

The Traffic Profiles page appears.

**Step 2**
Click *New Profile*.

The Create Profile page appears.

**Step 3**
Click *Add Host Profile Qualification*.

**Step 4**
Under *Host Profile Qualification*, in the first condition, specify the host whose information you want to collect.

In this example, select *Responder Host* because we only want information on responding hosts in a connection.

**Step 5**
Begin specifying the details of the operating system of the host by choosing the *Operating System* category.

Three subcategories appear: *OS Vendor*, *OS Name*, and *OS Version*.

**Step 6**
To specify that the host can be running any version of Microsoft Windows, use the same operator for all three subcategories: *is*.

**Step 7**
Finally, specify the values for the subcategories.

Select *Microsoft* as the value for *OS Vendor*, *Windows* as the value for *OS Name*, and leave *any* as the value for *OS Version*.

Note that the categories you can choose from depend on whether you are building traffic profile conditions or a host profile qualification. In addition, a condition’s available operators depend on the category you choose. Finally, the syntax you can use to specify a condition’s value depends on the category and operator. Sometimes you must type the value in a text field. Other times, you can pick a value from a drop-down list.

---

Note
Where the condition syntax allows you to pick a value from a drop-down list, you can often use multiple values from the list. For more information, see *Using Multiple Values in a Condition*, page 53-15.

For information on the syntax for building traffic profile conditions and host profile qualifications, see:
Adding and Linking Conditions

License: FireSIGHT

You can create simple traffic profile conditions and host profile qualifications, or you can create more elaborate constructs by combining and nesting conditions.

When your construct includes more than one condition, you must link them with an **AND** or an **OR** operator. Conditions on the same level are evaluated together:

- The **AND** operator requires that all conditions on the level it controls must be met.
- The **OR** operator requires that at least one of the conditions on the level it controls must be met.

For example, the following traffic profile contains two conditions linked by **AND**. This means that the traffic profile collects connection data only if both conditions are true. In this example, it collects HTTP connections for all hosts with IP addresses in the 10.4.x.x subnet.

In contrast, the following traffic profile, which collects connection data for HTTP activity in either the 10.4.x.x network or the 192.168.x.x network, has three conditions, with the last constituting a complex condition.

Logically, the above traffic profile is evaluated as follows:
To add a single condition:

**Access:** Admin/Discovery Admin

**Step 1**
To add a single condition, click **Add condition** above the current condition.

A new condition is added to the same logical level as the current set of conditions. By default, it is linked to the conditions on its level with the **OR** operator, though you can change the operator to **AND**.

For example, if you add a simple condition to the following host profile qualification:

<table>
<thead>
<tr>
<th>Where...</th>
<th>Is the condition that states...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Application Protocol Name is HTTP</td>
</tr>
<tr>
<td>B</td>
<td>IP Address is in 10.4.0.0/16</td>
</tr>
<tr>
<td>C</td>
<td>IP Address is in 192.168.0.0/16</td>
</tr>
</tbody>
</table>

The result is:

**To add a complex condition:**

**Access:** Admin/Discovery Admin

**Step 1**
Click **Add complex condition** above the current condition.

A complex condition is added below the current set of conditions. The complex condition comprises two subconditions, which are linked to each other with the opposite operator from the one used to link the conditions on the level above it.

For example, if you add a complex condition to the following host profile qualification:
Chapter 53      Creating Traffic Profiles

Understanding Condition-Building Mechanics

To link conditions:

Access: Admin/Discovery Admin

Step 1
Use the drop-down list to the left of a set of conditions:

- To require that all conditions on the level that the operator controls are met, select **AND**.
- To require that only one of the conditions on the level that the operator controls is met, select **OR**.

Using Multiple Values in a Condition

License: FireSIGHT

When you are building a condition, and the condition syntax allows you to pick a value from a drop-down list, you can often use multiple values from the list. For example, if you want to add a host profile qualification to a traffic profile that requires that a host be running some flavor of UNIX, instead of constructing multiple conditions linked with the OR operator, use the following procedure.

To include multiple values in one condition:

Access: Admin/Discovery Admin

Step 1
Build a condition, choosing **is in** or **is not in** as the operator.

The drop-down list changes to a text field.

Step 2
Click anywhere in the text field or on the **Edit** link.

A pop-up window appears.
Step 3  Under Available, use Ctrl or Shift while clicking to select multiple values. You can also click and drag to select multiple adjacent values.

Step 4  Click the right arrow (>) to move the selected entries to Selected.

Step 5  Click OK.

Your selections appear in the value field of your condition on the Create Profile page.

Viewing Traffic Profiles

License: FireSIGHT

Because traffic profiles are based on connection data, you can view graphs of traffic profiles. The following graphic shows a traffic profile with a PTW of one week, a sampling rate of five minutes, and a daily half-hour inactive period from midnight to 12:30 AM.

You can perform almost all the same actions on traffic profile graphs that you can perform on connection data graphs. However, because traffic profiles are based on aggregated data (connection summaries), you cannot examine the individual connection events on which the graphs are based. In other words, you cannot drill down to a connection data table view from a traffic profile graph. See Viewing Connection and Security Intelligence Data, page 39-14 for more information. In addition, traffic profiles appear as detached graphs. For more information, see Detaching Connection Graphs, page 39-26.

In addition, traffic profile graphs plotted over time show the mean (average) y-axis value as a bold horizontal line. Graphs over time also plot the values of the first four standard deviations above and below the mean, assuming that network traffic is distributed normally. By default, these statistics are
calculated over the PTW, but if you alter the time settings for a graph, the Defense Center recalculates the statistics. Rules written against traffic profile statistics, however, are always evaluated against the statistics for the PTW.

To view a traffic profile graph for a traffic profile:

Access: Admin/Discovery Admin

---

**Step 1**
Select Policies > Correlation, then click Traffic Profiles. The Traffic Profiles page appears.

**Step 2**
Next to the traffic profile for which you want to view the graph, click the graph icon ( ). The graph for the traffic profile appears in a separate browser window.