Using the Network Map

The FireSIGHT System passively collects traffic traveling over the network, decodes the data, and then compares it to established operating system and fingerprints. From this information, the system builds a *network map*, which is a detailed representation of your network.

The network map allows you to use the Defense Center to view your network topology in terms of hosts and network devices (bridges, routers, NAT devices, and load balancers). It is a useful tool for a quick, overall view of your network. The network map also allows you to drill down on associated host attributes, applications, clients, indications of compromised hosts, and vulnerabilities. In other words, you can select different views of the network map to suit the analysis you perform.

You can augment the information your system collects by adding operating system, application, client, protocol, or host attribute information from a third-party application using the host input feature. You can also actively scan hosts in the network map using Nmap and add the scan results to your network map.

You can use the custom topology feature to help you organize and identify subnets in the views of the network map. For example, if each department in your organization uses a different subnet, you can assign familiar labels to those subnets using the custom topology feature.

For more information, see the following sections:

Understanding the Network Map

License: FireSIGHT

Each view of the network map has the same format: a hierarchical tree with expandable categories and sub-categories. When you click a category, it expands to show you the sub-categories beneath it. You can select different views of the network map depending on the kind of analysis you are performing.

The Defense Center gathers data from all security zones where discovery policies are applied (including zones that process data from NetFlow-enabled devices). If multiple devices detect the same network asset, the Defense Center combines the information into a composite representation of the asset.

Although you can configure your network discovery policy to add 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. For more information, see Differences Between NetFlow and FireSIGHT Data, page 45-17.

From any network map, you can view any host's *host profile*, which provides a complete view of all the information collected by the system for that host. The host profile contains general information, such as the host name, operating system, and all associated IP addresses, as well as more specific information including detected protocols, applications, indications of compromise, and clients that are running on the host. The host profile also includes information about the vulnerabilities associated with the host and its detected assets. For more information on host profiles, see Using Host Profiles, page 49-1.

You can delete an item from the network map if you are no longer interested in investigating it. You can delete hosts and applications from the network map; you can also delete or deactivate vulnerabilities. If the system detects activity associated with a deleted host, it re-adds the host to the network map. Similarly, deleted applications are re-added to the applications network map if the system detects a change in the application (for example, if an Apache web server is upgraded to a new version). Vulnerabilities are reactivated on specific hosts if the system detects a change that makes the host vulnerable.

You can also use the network map to deactivate vulnerabilities network-wide, which means that you deem these hosts, which the system has judged to be vulnerable, to be safe from that particular attack or exploit.

Tip If you want to permanently exclude a host or subnet from the network map, modify the network discovery policy. You may wish to exclude load balancers and NAT devices from monitoring. They may create excessive and misleading events, filling the database and overloading the Defense Center. See Understanding Host Data Collection, page 45-2 for more information.

Working with the Hosts Network Map

License: FireSIGHT

Use the hosts network map to view the hosts on your network, organized by subnet in a hierarchical tree, as well as to drill down to the host profiles for specific hosts. This network map view provides a count of all unique hosts detected by the system, regardless of whether the hosts have one IP address or multiple IP addresses.

Although you can configure your 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 hosts added to the network map using NetFlow data, unless you provide it using the host input feature.

By creating a custom topology for your network, you can assign meaningful labels to your subnets, such as department names, that appear in the hosts network map.

You can also view the hosts network map according to the organization you specified in the custom topology; see Working with Custom Network Topologies, page 48-10.

You can delete entire networks, subnets, or individual hosts from the hosts network map. For example, if you know that a host is no longer attached to your network, you can delete it from the network map to simplify your analysis. If the system afterwards detects activity associated with the deleted host, it re-adds the host to the network map. If you want to permanently exclude a host or subnet from the network map, modify the network discovery policy. See Creating a Network Discovery Policy, page 45-22 for more information.

Note Cisco **strongly** recommends that you do **not** delete network devices from the network map, because the system uses their locations to determine network topology (including generating network hops and TTL values for monitored hosts). Although you cannot delete network devices from the network devices network map, make sure you do not delete them from the hosts network map.

To view the hosts network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map**, then select the **Hosts** tab.

The hosts network map appears, displaying a host count and a list of host IP addresses and MAC addresses. Each address or partial address is a link to the next level.

Step 2 Drill down to the specific IP address or MAC address of the host you want to investigate.

For example, to view a host with the IP address 192.168.40.11, click **192**, then **192.168**, then **192.168.40**, then **192.168.40.11**. When you click **192.168.40.11**, the host profile appears. For more information on host profiles, see Using Host Profiles, page 49-1.

To filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

Step 3 Optionally, to delete a subnet, IP address, or MAC address, click the delete icon ( ) next to the element you want to delete, then confirm that you want to delete the host or subnet.

The host is deleted. If the system rediscovers the host, it re-adds the host to the network map.

Step 4 Optionally, switch between the hosts view and the topology view of the hosts network map:

- To switch to a view of the hosts network map organized by your custom topology, on the hosts view (the default), click **(topology)** at the top of the network map.
- To switch to a view of the hosts network map organized by subnet, on the topology view, click **(hosts)** at the top of the network map.

For information on configuring custom topologies, see Working with Custom Network Topologies, page 48-10.

Working with the Network Devices Network Map

License: FireSIGHT

Use the network devices network map to view the network devices (bridges, routers, NAT devices, and load balancers) that connect one segment of your network to another, as well as to drill down to the host profiles of those network devices. The network devices network map is separated into two sections: IP and MAC. The IP section lists network devices identified by an IP address; the MAC section lists

network devices identified by a MAC address. This network map view also provides a count of all unique network devices detected by the system, regardless of whether the devices have one IP address or multiple IP addresses.

If you create a custom topology for your network, the labels you assign to your subnets appear in the network devices network map.

The methods the system uses to distinguish network devices include:

- the analysis of Cisco Discovery Protocol (CDP) messages, which can identify network devices and their types (Cisco devices only)
- the detection of the Spanning Tree Protocol (STP), which identifies a device as a switch or bridge
- the detection of multiple hosts using the same MAC address, which identifies the MAC address as belonging to a router
- the detection of TTL value changes from the client side, or TTL values that change more frequently than a typical boot time, which identify NAT devices and load balancers

If a network device communicates using CDP, it may have one or more IP addresses. If it communicates using STP, it may only have a MAC address.

You cannot delete network devices from the network map, because the system uses their locations to determine network topology (including generating network hops and TTL values for monitored hosts).

The host profile for a network device has a Systems section rather than an Operating Systems section, which includes a Hardware column that reflects the hardware platform for any mobile devices detected behind the network device. If a value for a hardware platform is listed under Systems, that system represents a mobile device or devices detected behind the network device. Note that mobile devices may or may not have hardware platform information, but hardware platform information is never detected for systems that are not mobile devices.

To view the network devices network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map > Network Devices**.

The network devices network map appears, displaying a count of unique network devices and a list of network device IP addresses and MAC addresses. Each address or partial address is a link to the next level of addresses or to the host profile for an individual host.

Step 2 Drill down to the specific IP address or MAC address of the network device you want to investigate.

The host profile for the network device appears. For more information on host profiles, see Using Host Profiles, page 49-1.

Step 3 Optionally, to filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

Working with the Indications of Compromise Network Map

License: FireSIGHT

Use the indications of compromise (IOC) network map to view the compromised hosts on your network, organized by IOC category. Affected hosts are listed beneath each category.

The system uses data from multiple sources to determine a host's compromised status, including intrusion events, Security Intelligence, and FireAMP.

From the indications of compromise network map, you can view the host profile of each host determined to have been compromised in a specific way. You can also delete (mark as resolved) any IOC category or any specific host, which removes the IOC tag from the relevant hosts. For example, you can delete an IOC category from the network map if you have determined that the issue is addressed and unlikely to recur.

Marking a host or IOC category resolved from the network map does not remove it from your network. A resolved host or IOC category reappears in the network map if your system newly detects information that triggers that IOC.

To view the indications of compromise network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map > Indications of Compromise**.

The indications of compromise network map appears.

Step 2 Click the specific IOC category you want to investigate.

For example, if you want to view hosts on which malware was detected, click **Malware Detected**.

To filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

Step 3 Drill down to a specific IP address under the IOC category you selected. Each address or partial address is a link to the next level.

The host profile of the compromised host appears with the indications of compromise section expanded. For more information about the IOC section of the host profile, see Working with Indications of Compromise in the Host Profile, page 49-8.

Step 4 Optionally, to mark any IOC category, compromised host, or group of compromised hosts resolved, click the delete icon ( ) next to the element you want to resolve, then confirm that you want to resolve it.

The category or host is resolved (IOC tags removed). If the IOC is triggered again, it is re-added to the network map.

Working with the Mobile Devices Network Map

License: FireSIGHT

Use the mobile devices network map to view mobile devices attached to your network, and to drill down to the host profiles for those devices. This network map view also provides a count of all unique mobile devices detected by the system, regardless of whether the devices have one IP address or multiple IP addresses.

The methods the system uses to distinguish mobile devices include:

- analysis of user agent strings in HTTP traffic from the mobile device's mobile browser
- monitoring of HTTP traffic of specific mobile applications

If you create a custom topology for your network, the labels you assign to your subnets appear in the mobile devices network map.

To view the mobile devices network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map**, then select the **Mobile Devices** tab.

The mobile devices network map appears, displaying a count of unique mobile devices and a list of mobile device IP addresses. Each address or partial address is a link to the next level.

Step 2 Drill down to the specific IP address of the mobile device you want to investigate.

For example, to view a device with the IP address 10.11.40.11, click **10**, then **10.11**, then **10.11.40**, then **10.11.40.11**. When you click **10.11.40.11**, the host profile appears. For more information on host profiles, see Using Host Profiles, page 49-1.

To filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

Step 3 Optionally, to delete a subnet or IP address, click the delete icon ( ) next to the element you want to delete, then confirm that you want to delete the device or subnet.

The device is deleted. If the system rediscovers the device, it re-adds the device to the network map.

Working with the Applications Network Map

License: FireSIGHT

Use the applications network map to view the applications on your network, organized in a hierarchical tree by application name, vendor, version, and finally by the hosts running each application.

The applications that the system detects may change with system software and VDB updates, and also if you import any add-on detectors. The release notes or advisory text for each system or VDB update contains information on any new and updated detectors. For a comprehensive up-to-date list of detectors, see either of the following Support Sites:

- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

From the applications network map, you can view the host profile of each host that runs a specific application as well as delete any application category, any application running on all hosts, or any application running on a specific host. For example, you can delete an application from the network map if you know it is disabled on the host and you want to make sure the system does not use it for impact level qualification.

Deleting an application from the network map does not remove it from your network. A deleted application reappears in the network map if your system detects a change in the application (for example, if an Apache web server is upgraded to a new version) or if you restart your system's discovery function.

Depending on what you delete, the behavior differs:

- If you delete an application category, the application category is removed from the network map. All applications that reside beneath the category are removed from any host profile that contains the applications.

  For example, if you delete **http**, all applications identified as **http** are removed from all host profiles and **http** no longer appears in the applications view of the network map.
- If you delete a specific application, vendor, or version, the affected application is removed from the network map and from any host profiles that contain it.

For example, if you expand the **http** category and delete **Apache**, all applications listed as Apache with any version listed beneath Apache are removed from any host profiles that contain them. Similarly, if instead of deleting **Apache**, you delete a specific version (**1.3.17**, for example), only the version you selected will be deleted from affected host profiles.

- If you delete a specific IP address, the IP address is removed from the application list and the application itself is removed from the host profile of the IP address you selected.

  For example, if you expand **http**, **Apache**, **1.3.17 (Win32)**, and then delete **172.16.1.50:80/tcp**, the Apache 1.3.17 (Win32) application is deleted from the host profile of IP address 172.16.1.50.

To view the applications network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map > Applications**.

The applications network map appears.

Step 2 Drill down to the specific application you want to investigate.

For example, if you want to view a specific type of web server like Apache, click **http**, then click **Apache**, and then click the version of the Apache web server you want to view.

To filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

Step 3 Click a specific IP address under the application you selected.

The host profile of the host running the application appears with the applications section expanded. For more information about the applications section of the host profile, see Working with Servers in the Host Profile, page 49-15.

Step 4 Optionally, to delete any application category, any application running on all hosts, or any application running on a specific host, click the delete icon () next to the element you want to delete, then confirm that you want to delete it.

The application is deleted. If the system rediscovers the application, it is re-added to the network map.

Working with the Vulnerabilities Network Map

License: FireSIGHT

Use the vulnerabilities network map to view the vulnerabilities that the system has detected on your network, organized by legacy vulnerability ID (SVID), Bugtraq ID, CVE ID, or Snort ID. The vulnerabilities are arranged by identification number, with affected hosts listed beneath each vulnerability.

From the vulnerabilities network map, you can view the details of specific vulnerabilities; you can also view the host profile of any host subject to a specific vulnerability. This can help you evaluate the threat posed by that vulnerability to specific affected hosts.

If you deem that a specific vulnerability is not applicable to the hosts on your network (for example, you have applied a patch), you can deactivate the vulnerability. Deactivated vulnerabilities still appear on the network map, but the IP addresses of their previously affected hosts appear in gray italics. The host

profiles for those hosts show deactivated vulnerabilities as invalid, though you can manually mark them as valid for individual hosts; see Setting Vulnerabilities for Individual Hosts, page 49-30 for more information.

If there is an identity conflict for an application or operating system on a host, the system lists the vulnerabilities for both potential identities. When the identity conflict is resolved, the vulnerabilities remain associated with the current identity. For more information, see Understanding Current Identities, page 46-5 and Understanding Identity Conflicts, page 46-6.

By default, the vulnerability network map displays the vulnerabilities of a detected application only if the packet contains the application's vendor and version. However, you can configure the system to list the vulnerabilities for applications lacking vendor and version data by enabling the vulnerability mapping setting for the application in the system policy. For information on setting the vulnerability mapping for an application, see Mapping Vulnerabilities for Servers, page 63-30.

The numbers next to a vulnerability ID (or range of vulnerability IDs) represent two counts:

- The first number is a count of non-unique hosts that are affected by a vulnerability or vulnerabilities. If a host is affected by more than one vulnerability, it is counted multiple times. Therefore, it is possible for the count to be higher than the number of hosts on your network. Deactivating a vulnerability decrements this count by the number of hosts that are potentially affected by the vulnerability. If you have not deactivated any vulnerabilities for any of the potentially affected hosts for a vulnerability or range of vulnerabilities, this count is not displayed.
- The second number is a similar count of the total number of non-unique hosts that the system has determined are *potentially* affected by a vulnerability or vulnerabilities.

Deactivating a vulnerability renders it inactive only for the hosts you designate. You can deactivate a vulnerability for all hosts that have been judged vulnerable or for a specified individual vulnerable host. If the system subsequently detects the vulnerability on a host where it has not been deactivated (for example, on a new host in the network map), the system activates the vulnerability for that host. You have to explicitly deactivate the newly discovered vulnerability. Also, if the system detects an operating system or application change for a host, it may reactivate associated deactivated vulnerabilities.

To view the vulnerabilities network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map > Vulnerabilities**.

The vulnerabilities network map appears.

Step 2 From the **Type** drop-down list, select the class of vulnerability you want to view. By default, vulnerabilities are displayed by legacy vulnerability ID (SVID).

Step 3 Drill down to the specific vulnerability you want to investigate.

To filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

The vulnerability details appear. For details on the information provided, see Viewing Vulnerability Details, page 49-27.

In addition, on the network map, the Defense Center displays the IP addresses of affected hosts. You can click any IP address to display the host profile for that host.

Step 4 Optionally, deactivate the vulnerability:

- To deactivate the vulnerability for all hosts affected by the vulnerability, click the delete icon () next to the vulnerability number.

- To deactivate the vulnerability for an individual host, click the delete icon ( ) next to the host's IP address.

The vulnerability is deactivated. The applicable hosts' IP addresses appear in gray italics in the network map. In addition, host profiles for those hosts show deactivated vulnerabilities as invalid.

Tip See Setting Vulnerabilities for Individual Hosts, page 49-30 for more information on reactivating vulnerabilities.

Working with the Host Attributes Network Map

License: FireSIGHT

Use the host attributes network map to view the hosts on your network organized by their host attributes. When you select the host attribute you want to use to organize your hosts, the Defense Center lists the possible values for that attribute in the network map and groups hosts based on their assigned values. You can also view the host profile of any host assigned a specific host attribute value.

The host attributes network map can organize hosts based on user-defined host attributes. For any of these attributes, the network map displays hosts that do not have a value assigned as Unassigned.

For more information, see Working with User-Defined Host Attributes, page 49-31.

In addition, the host attributes network map can organize hosts based on the host attributes that correspond to any compliance white lists you have created. Each compliance white list that you create automatically creates a host attribute with the same name as the white list.

Possible white list host attribute values are:

- `Compliant`, for hosts that are compliant with the white list
- `Non-Compliant`, for hosts that violate the white list
- `Not Evaluated`, for hosts that are not valid targets of the white list or have not been evaluated for any reason

For more information on compliance white lists, see Using the FireSIGHT System as a Compliance Tool, page 52-1.

Note You cannot organize hosts using predefined host attributes, such as host criticality, on the host attributes network map.

To view the host attributes network map:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Hosts > Network Map > Host Attributes**.

The host attributes network map appears.

Step 2 From the **Attribute** drop-down list, select a host attribute.

The Defense Center lists the values for the host attribute and indicates, in parentheses, the number of hosts assigned that value.

To filter by IP or MAC addresses, type an address in the search field. To clear the search, click the clear icon (✖).

Step 3 Click any host attribute value to view hosts assigned the value.

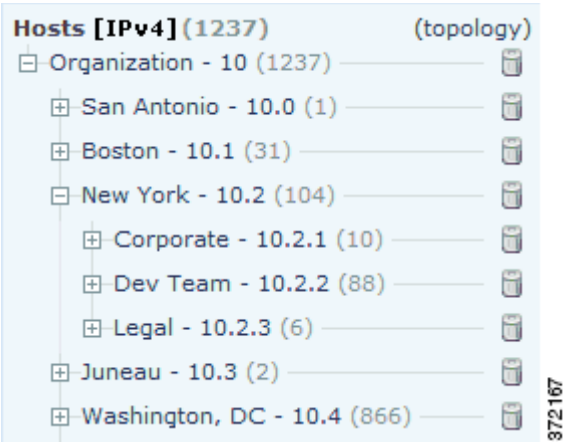
Step 4 Click a host IP address to view the host profile for that host.

Working with Custom Network Topologies

License: FireSIGHT

Use the custom topology feature to help you organize and identify subnets in your hosts and network devices network maps.

For example, if each department within your organization uses a different subnet, you can label those subnets using the custom topology feature. Then, when you view the hosts or network devices network map, the labels you assign to your subnets appear, as shown in the following graphic.



You can also view the hosts network map according to the organization you specified in the custom topology.

For more information about the hosts and network devices network maps, see Working with the Hosts Network Map, page 48-2 and Working with the Network Devices Network Map, page 48-3.

For more information, see the following sections:

Creating Custom Topologies

License: FireSIGHT

To create a custom topology, you must specify its networks. You can do this using any or all of three strategies:

- by importing the Cisco-discovered topology, which adds networks using a "best guess" at how your network is deployed based on the hosts and network devices the system has detected
- by importing networks from a network discovery policy, which adds the networks that you configured the FireSIGHT System to monitor in a network discovery policy
- by adding networks to your topology manually, if the other two methods create an inaccurate or incomplete representation of your deployment

You must save and activate the topology before using it with the network map.

To create a custom topology:

Access: Admin/Discovery Admin

Step 1 Select **Policies > Network Discovery**, then click **Custom Topology**.

The Custom Topology page appears.

Step 2 Click **Create Topology**.

The Create Topology page appears.

Step 3 Provide basic topology information, such as the topology name and description.

See Providing Basic Topology Information, page 48-12.

Step 4 Add networks to your topology. You can use any or all of the following strategies:

- To add networks to your topology by importing the Cisco-discovered topology, follow the procedure in Importing a Discovered Topology, page 48-12.
- To add networks to your topology by importing them from a network discovery policy, follow the procedure in see Importing Networks from a Network Discovery Policy, page 48-13.
- To add networks to your topology manually, follow the procedure in Manually Adding Networks to Your Custom Topology, page 48-13.

Step 5 Refine your topology:

- To remove a network from your custom topology, click **Delete** next to the network you want to remove.
- To rename a network, click **Rename** next to the network. In the pop-up window that appears, type the new name in the **Name** field and click **Rename**. This name labels the network in the network map.

Step 6 Click **Save**.

The topology is saved.

Note You must activate the topology before you can use it in the network map. For more information, see Managing Custom Topologies, page 48-14.

Providing Basic Topology Information

License: FireSIGHT

You must give each custom topology a name, and, optionally, a short description.

To provide basic topology information:

Access: Admin

Step 1 On the Edit Topology page, in the **Name** field, type a name for the topology.

Step 2 Optionally, in the **Description** field, type a description for the topology.

Step 3 Optionally, continue with the procedures in the following sections, depending on how you want to build your custom topology:

- Importing a Discovered Topology, page 48-12
- Importing Networks from a Network Discovery Policy, page 48-13
- Manually Adding Networks to Your Custom Topology, page 48-13

Importing a Discovered Topology

License: FireSIGHT

One way you can add networks to your custom topology is to import the topology discovered by your FireSIGHT System. This discovered topology is the system's "best guess" at how your network is deployed based on the hosts and network devices it has detected.

To import a discovered topology:

Access: Admin

Step 1 On the Edit Topology page, click **Import Discovered Topology**.

Step 2 The discovered networks populate the page.

Step 3 Optionally, continue with the procedures in the following sections, depending on how you want to build your custom topology:

- Importing a Discovered Topology, page 48-12
- Importing Networks from a Network Discovery Policy, page 48-13
- Manually Adding Networks to Your Custom Topology, page 48-13

Importing Networks from a Network Discovery Policy

License: FireSIGHT

One way you can add networks to your custom topology is to import the networks that you configured the FireSIGHT System to monitor in a network discovery policy; see Creating a Network Discovery Policy, page 45-22.

To import networks from a network discovery policy:

Access: Admin

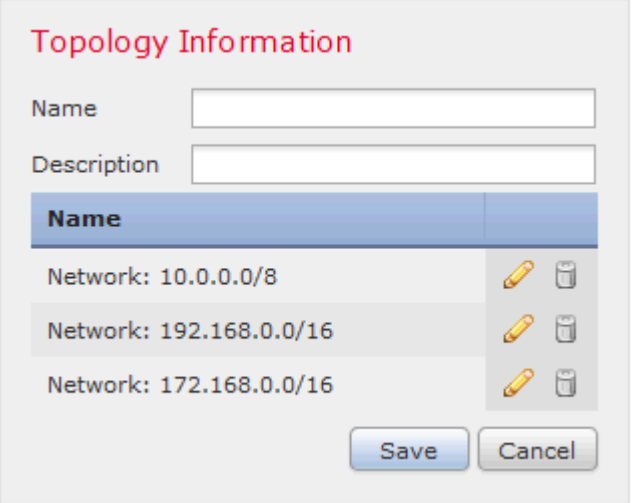
Step 1 On the Edit Topology page, click **Import Policy Networks**.

A pop-up window appears.

Step 2 From the drop-down list, choose the network discovery policy you want to use and click **Load**.

Step 3 The monitored networks in your network discovery policy populate the page.

For example, if you configured your network discovery policy to monitor the 10.0.0.0/8, 192.168.0.0/16, and 172.12.0.0/16 networks, those networks appear on the page.



Step 4 To add networks from a different network discovery policy, repeat steps 1 and 2.

Step 5 Optionally, follow the procedures in the following sections, depending on how you want to build your custom topology:

- Importing a Discovered Topology, page 48-12
- Manually Adding Networks to Your Custom Topology, page 48-13

Manually Adding Networks to Your Custom Topology

License: FireSIGHT

If importing the Cisco-discovered topology and importing networks from your network discovery policy creates an inaccurate or incomplete representation of your network deployment, you can add networks to your custom topology manually.

To add a network to a custom topology manually:

Access: Admin

Step 1 On the Edit Topology page, click **Add Network**.

A pop-up window appears.

Step 2 Optionally, name the network by typing a name in the **Name** field.

This name labels the networks in the hosts and network devices network maps after you activate the topology.

For more information, see Working with the Hosts Network Map, page 48-2 and Working with the Network Devices Network Map, page 48-3.

Step 3 In the **IP Address** and **Netmask** fields, enter the IP address and network mask (in CIDR notation) that represent the network you want to add to your topology.

For information on using CIDR notation in the FireSIGHT System, see IP Address Conventions, page 1-22.

Step 4 Click **Add**.

The network is added to your topology.

Step 5 To add additional networks to your topology, repeat steps 1 through 4.

Tip To delete a network from your topology, click **Delete** next to the network you want to delete, and confirm that you want to delete the network, as well as all links to the network.

Step 6 Optionally, follow the procedures in the following sections, depending on how you want to build your custom topology:

- Importing a Discovered Topology, page 48-12
- Importing Networks from a Network Discovery Policy, page 48-13

Managing Custom Topologies

License: FireSIGHT

Use the Custom Topology page to manage custom topologies. You can create, modify, and delete topologies.

A topology's status appears with its name. If the light bulb icon next to the policy name is lit, the topology is active and affects your network map. If it is dark, the topology is inactive. Only one custom topology can be active at any time. If you have created multiple topologies, activating one automatically deactivates the currently active topology.

Use the following procedures to either activate or deactivate a custom topology, modify a topology, or delete a topology.

If you delete the active topology, your changes take effect immediately; that is, your network map no longer displays your custom topology.

To activate or deactivate a custom topology:

Access: Admin

Step 1 Select **Policies > Network Discovery > Custom Topology**.

The Custom Topology page appears.

Step 2 You have two options:

- To **activate** a topology, click **Activate** next to the policy.
- To **deactivate** a topology, click **Deactivate** next to the policy.

To modify a custom topology:

Access: Admin

Step 1 Select **Policies > Network Discovery > Custom Topology**.

The Custom Topology page appears.

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

The Edit Topology page appears. See Creating Custom Topologies, page 48-11 for information on the various configurations you can change.

Step 3 Make changes as needed and click **Save**.

The topology is changed. If the topology is active, the changes you made take effect in the network map immediately.

To delete a custom topology:

Access: Admin

Step 1 Select **Policies > Network Discovery > Custom Topology**.

The Custom Topology page appears.

Step 2 Click **Delete** next to the topology you want to delete. If the topology is active, confirm that you want to delete it.

The topology is deleted.