Host Identity Sources

The following topics provide information on host identity sources:

Overview: Host Data Collection

As the system passively monitors the traffic that travels through your network, it compares specific packet header values and other unique data from network traffic against established definitions (called *fingerprints*) to determine information about the hosts on your network, including:

- the number and types of hosts (including network devices such as bridges, routers, load balancers, and NAT devices)

- basic network topology data, including the number of hops from the discovery point on the network to the hosts

- the operating systems running on the hosts

- applications on the hosts and users associated with these applications

If the system cannot identify a host's operating system, you can create custom client or server fingerprints. The system uses these fingerprints to identify new hosts. You can map fingerprints to systems in the vulnerability database (VDB) to allow the appropriate vulnerability information to be displayed whenever a host is identified using the custom fingerprint.

Note In addition to collecting host data from monitored network traffic, the system can collect host data from exported NetFlow records, and you can actively add host data using Nmap scans and the host input feature.

Requirements and Prerequisites for Host Identity Sources

Model Support

Any.

Supported Domains

Any, with the exception of custom fingerprinting, which is Leaf only.

User Roles

- Admin

- Discovery Admin, except for third-party data and custom mappings.

Determining Which Host Operating Systems the System Can Detect

To learn which exact operating systems the system can fingerprint, view the list of available fingerprints that is shown during the process of creating a custom OS fingerprint.

Procedure

Step 1	Choose **Policies** > **Network Discovery**.
Step 2	Click **Custom Operating Systems**.
Step 3	Click **Create Custom Fingerprint**.
Step 4	View the lists of options in the drop-down lists in the **OS Vulnerability Mappings** section. These options are the operating systems that the system can fingerprint.

What to do next

As needed, see Identifying Host Operating Systems, on page 2.

Identifying Host Operating Systems

If the system does not correctly identify a host's operating system (for example, it shows in the Host Profile as Unknown or is incorrectly identified), try the strategies below.

Procedure

Try one of the following strategies:

- Check the Network Discovery Identity Conflict Settings.

- Create a custom fingerprint for the host.

- Run an Nmap scan against the host.

- Import data into the network map, using the host input feature.

- Manually enter operating system information.

Custom Fingerprinting

The system includes operating system *fingerprints* that the system uses to identify the operating system on each host it detects. However, sometimes the system cannot identify a host operating system or misidentifies it because no fingerprints exist that match the operating system. To correct this problem, you can create a *custom fingerprint,* which provides a pattern of operating system characteristics unique to the unknown or misidentified operating system, to supply the name of the operating system for identification purposes.

If the system cannot match a host's operating system, it cannot identify the vulnerabilities for the host, because the system derives the list of vulnerabilities for each host from its operating system fingerprint. For example, if the system detects a host running Microsoft Windows, the system has a stored Microsoft Windows vulnerability list that it adds to the host profile for that host based on the detected Windows operating system.

As an example, if you have several devices on your network running a new beta version of Microsoft Windows, the system cannot identify that operating system or map vulnerabilities to the hosts. However, knowing that the system has a list of vulnerabilities for Microsoft Windows, you may want to create a custom fingerprint for one of the hosts to help identify the other hosts running the same operating system. You can include a mapping of the vulnerability list for Microsoft Windows in the fingerprint to associate that list with each host that matches the fingerprint.

When you create a custom fingerprint, the Firewall Management Center lists the set of vulnerabilities associated with that fingerprint for any hosts running the same operating system. If the custom fingerprint you create does not have any vulnerabilities mappings in it, the system uses the fingerprint to assign the custom operating system information you provide in the fingerprint. When the system sees new traffic from a previously detected host, the system updates the host with the new fingerprint information. the system also uses the new fingerprint to identify any new hosts with that operating system the first time they are detected.

Before creating a custom fingerprint, you should determine why the host is not being identified correctly to decide whether custom fingerprinting is a viable solution.

You can create two types of fingerprints with the system:

- Client fingerprints, which identify operating systems based on the SYN packet that the host sends when it connects to a TCP application running on another host on the network.

- Server fingerprints, which identify operating systems based on the SYN-ACK packet that the host uses to respond to an incoming connection to a running TCP application.

> **Note** If both a client and server fingerprint match the same host, the client fingerprint is used.

After creating fingerprints, you must activate them before the system can associate them with hosts.

Related Topics

Managing Fingerprints

After a fingerprint is created and activated, you can edit a fingerprint to make changes or add vulnerability mappings.

Procedure

Step 1	Choose **Policies** > **Network Discovery**.
Step 2	Click **Custom Operating Systems**. If the system is awaiting data to create a fingerprint, it automatically refreshes the page every 10 seconds until the fingerprint is created.
Step 3	Manage your custom fingerprints:

- Activate/Deactivate — Activate or deactivate a fingerprint as described in Activating and Deactivating Fingerprints, on page 4.
- Create — Create fingerprints as described in Creating a Custom Fingerprint for Clients, on page 6 and Creating a Custom Fingerprint for Servers, on page 8.
- Edit — Edit a fingerprint as described in Editing an Active Fingerprint, on page 5 and Editing an Inactive Fingerprint, on page 5.
- Delete — Click **Delete** (🗑) next to the fingerprint you want to delete, and click **OK** to confirm. You can only delete deactivated fingerprints.

Activating and Deactivating Fingerprints

You must activate a custom fingerprint before the system can use it to identify hosts. After the new fingerprint is activated, the system uses it to re-identify previously discovered hosts and discover new hosts.

If you want to stop using a fingerprint, you can deactivate it. Deactivating a fingerprint causes a fingerprint to no longer be used, but allows it to remain on the system. When you deactivate a fingerprint, the operating system is marked as unknown for hosts that use the fingerprint. If the hosts are detected again and match a different active fingerprint, they are then identified by that active fingerprint.

Deleting a fingerprint removes it from the system completely. After deactivating a fingerprint, you can delete it.

Procedure

Step 1   Choose **Policies** > **Network Discovery**.

Step 2   Click **Custom Operating Systems**.

Step 3   Click the slider next to the fingerprint you want to activate or deactivate.

> **Note**
> The activate option is only available if the fingerprint you created is valid. If the slider is not available, try creating the fingerprint again.

Editing an Active Fingerprint

If a fingerprint is *active*, you can modify the fingerprint name, description, custom operating system display, and map additional vulnerabilities to it.

You can modify the fingerprint name, description, custom operating system display, and map additional vulnerabilities to it.

Procedure

Step 1   Choose **Policies** > **Network Discovery**.

Step 2   Click **Custom Operating Systems**

Step 3   Click **Edit** (✐) next to the fingerprint you want to edit.

Step 4   Modify the fingerprint name, description, and custom OS display, if necessary.

Step 5   If you want to delete a vulnerability mapping, click **Delete** next to the mapping in the **Pre-Defined OS Product Maps** section of the page.

Step 6   If you want to add additional operating systems for vulnerability mapping, choose the **Product** and, if applicable, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** and then click **Add OS Definition**.

         The vulnerability mapping is added to the **Pre-Defined OS Product Maps** list.

Step 7   Click **Save**.

Editing an Inactive Fingerprint

If a fingerprint is *inactive*, you can modify all elements of the fingerprint and resubmit it to the Secure Firewall Management Center. This includes all properties you specified when creating the fingerprint, such as fingerprint type, target IP addresses and ports, vulnerability mappings, and so on. When you edit an inactive fingerprint and submit it, it is resubmitted to the system and, if it is a client fingerprint, you must resend traffic to the appliance before activating it. Note that you can choose only a single vulnerability mapping for an inactive fingerprint. After you activate the fingerprint, you can map additional operating systems and versions to its vulnerabilities list.

Procedure

Step 1	Choose **Policies** > **Network Discovery**.
Step 2	Click **Custom Operating Systems**.
Step 3	Click **Edit** ( ) next to the fingerprint you want to edit.
Step 4	Make changes to the fingerprint as necessary:

       • If you are modifying a client fingerprint, see Creating a Custom Fingerprint for Clients, on page 6.

       • If you are modifying a server fingerprint, see Creating a Custom Fingerprint for Servers, on page 8.

Step 5	Click **Save**.

What to do next

• If you modified a client fingerprint, remember to send traffic from the host to the appliance gathering the fingerprint.

Creating a Custom Fingerprint for Clients

Client fingerprints identify operating systems based on the SYN packet a host sends when it connects to a TCP application running on another host on the network.

If the Firewall Management Center does not have direct contact with monitored hosts, you can specify a device that is managed by the Firewall Management Center and is closest to the host you intend to fingerprint when specifying client fingerprint properties.

Before you begin the fingerprinting process, obtain the following information about the host you want to fingerprint:

• The number of network hops between the host and the Firewall Management Center or the device you use to obtain the fingerprint. (Cisco strongly recommends that you directly connect the Firewall Management Center or the device to the same subnet that the host is connected to.)

• The network interface (on the Firewall Management Center or the device) that is connected to the network where the host resides.

• The actual operating system vendor, product, and version of the host.

• Access to the host in order to generate client traffic.

Procedure

Step 1	Choose **Policies** > **Network Discovery**.
Step 2	Click **Custom Operating Systems**.
Step 3	Click **Create Custom Fingerprint**.

Step 4   From the **Device** drop-down list, choose the Firewall Management Center or the device that you want to use to collect the fingerprint.

Step 5   Enter a **Fingerprint Name**.

Step 6   Enter a **Fingerprint Description**.

Step 7   From the **Fingerprint Type** list, choose **Client**.

Step 8   In the **Target IP Address** field, enter an IP address of the host you want to fingerprint.

Note that the fingerprint will only be based on traffic to and from the host IP address you specify, not any of the host's other IP addresses (if it has any).

Step 9   In the **Target Distance** field, enter the number of network hops between the host and the device that you chose earlier to collect the fingerprint.

Caution
This must be the actual number of physical network hops to the host, which may or may not be the same as the number of hops detected by the system.

Step 10   From the **Interface** list, choose the network interface that is connected to the network segment where the host resides.

Note
Use the management interface or any other available network interfaces that is configured as the sensing interface on your device to perform fingerprint collection. If you do not know which interface is the sensing interface on your device, refer to the *Installation Guide* for the specific model you are using to fingerprint.

Step 11   If you want to display custom information in the host profile for fingerprinted hosts (or if the host you want to fingerprint does not reside in the **OS Vulnerability Mappings** section), choose **Use Custom OS Display** and provide the values you want to display for the following:

- In the **Vendor String** field, enter the operating system's vendor name. For example, the vendor for Microsoft Windows would be Microsoft.

- In the **Product String** field, enter the operating system's product name. For example, the product name for Microsoft Windows 2000 would be Windows.

- In the **Version String** field, enter the operating system's version number. For example, the version number for Microsoft Windows 2000 would be 2000.

Step 12   In the OS Vulnerability Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping.

You must specify **Vendor** and **Product** values in this section if you want to use the fingerprint to identify vulnerabilities for matching hosts or if you do not assign custom operating system display information.

To map vulnerabilities for all versions of an operating system, specify only the **Vendor** and **Product** values.

Note
Not all options in the **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** drop-down lists may apply to the operating system you choose. In addition, if no definition appears in a list that matches the operating system you want to fingerprint, you can leave these values empty. Be aware that if you do not create any OS vulnerability mappings in a fingerprint, the system cannot use the fingerprint to assign a vulnerabilities list with hosts identified by the fingerprint.

Example:

If you want your custom fingerprint to assign the list of vulnerabilities from Redhat Linux 9 to matching hosts, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the major version.

Example:

To add all versions of the Palm OS, you would choose **PalmSource, Inc.** from the **Vendor** list, **Palm OS** from the **Product** list, and leave all other lists at their default settings.

Step 13   Click **Create**.

The status briefly shows `New`, then switches to `Pending`, where it remains until traffic is seen for the fingerprint. Once traffic is seen, it switches to `Ready`.

The Custom Fingerprint status page refreshes every ten seconds until it receives data from the host in question.

Step 14   Using the IP address you specified as the target IP address, access the host you are trying to fingerprint and initiate a TCP connection to the appliance.

To create an accurate fingerprint, traffic **must** be seen by the appliance collecting the fingerprint. If you are connected through a switch, traffic to a system other than the appliance may not be seen by the system.

Example:

Access the web interface of the Firewall Management Center from the host you want to fingerprint or SSH into the Firewall Management Center from the host. If you are using SSH, use the command below, where localIPv6address is the IPv6 address specified in step 7 that is currently assigned to the host and DCmanagementIPv6address is the management IPv6 address of the Firewall Management Center. The Custom Fingerprint page should then reload with a "Ready" status.

```
ssh -b localIPv6address DCmanagementIPv6address
```

What to do next

• Activate the fingerprint as described in .

Creating a Custom Fingerprint for Servers

Server fingerprints identify operating systems based on the SYN-ACK packet that the host uses to respond to an incoming connection to a running TCP application. Before you begin, you should obtain the following information about the host you want to fingerprint:

• The number of network hops between the host and the appliance you use to obtain the fingerprint. Cisco strongly recommends that you directly connect an unused interface on the appliance to the same subnet that the host is connected to.

• The network interface (on the appliance) that is connected to the network where the host resides.

• The actual operating system vendor, product, and version of the host.

• An IP address that is not currently in use and is authorized on the network where the host is located.

Tip   If the Firewall Management Center does not have direct contact with monitored hosts, you can specify a managed device that is closest to the host you intend to fingerprint when specifying server fingerprint properties.

Procedure

Step 1	Choose **Policies** > **Network Discovery**.
Step 2	Click **Custom Operating Systems**.
Step 3	Click **Create Custom Fingerprint**.
Step 4	From the **Device** list, choose the Firewall Management Center or the managed device that you want to use to collect the fingerprint.
Step 5	Enter a **Fingerprint Name**.
Step 6	Enter a **Fingerprint Description**.
Step 7	From the **Fingerprint Type** list, choose **Server** to display the server fingerprinting options.
Step 8	In the **Target IP Address** field, enter an IP address of the host you want to fingerprint.

Note that the fingerprint will only be based on traffic to and from the host IP address you specify, not any of the host's other IP addresses (if it has any).

Caution
You can capture IPv6 fingerprints only with appliances running Version 5.2 and later.

Step 9	In the **Target Distance** field, enter the number of network hops between the host and the device that you chose earlier to collect the fingerprint.

Caution
This must be the actual number of physical network hops to the host, which may or may not be the same as the number of hops detected by the system.

Step 10	From the **Interface** list, choose the network interface that is connected to the network segment where the host resides.

Caution
Cisco recommends that you do **not** use the sensing interface on a managed device for fingerprinting for several reasons. First, fingerprinting does not work if the sensing interface is on a span port. Also, if you use the sensing interface on a device, the device stops monitoring the network for the amount of time it takes to collect the fingerprint. You can, however, use the management interface or any other available network interfaces to perform fingerprint collection. If you do not know which interface is the sensing interface on your device, refer to the *Installation Guide* for the specific model you are using to fingerprint.

Step 11	Click **Get Active Ports**.
Step 12	In the **Server Port** field, enter the port that you want the device chose to collect the fingerprint to initiate contact with, or choose a port from the **Get Active Ports** drop-down list.

You can use any server port that you know is open on the host (for instance, 80 if the host is running a web server).

Step 13	In the **Source IP Address** field, enter an IP address that should be used to attempt to communicate with the host.

You should use a source IP address that is authorized for use on the network but is not currently being used, for example, a DHCP pool address that is currently not in use. This prevents you from temporarily knocking another host offline while you create the fingerprint.

You should exclude that IP address from monitoring in your network discovery policy while you create the fingerprint. Otherwise, the network map and discovery event views will be cluttered with inaccurate information about the host represented by that IP address.

Step 14   In the **Source Subnet Mask** field, enter the subnet mask for the IP address you are using.

Step 15   If the **Source Gateway** field appears, enter the default gateway IP address that should be used to establish a route to the host.

Step 16   If you want to display custom information in the host profile for fingerprinted hosts or if the fingerprint name you want to use does not exist in the OS Definition section, choose **Use Custom OS Display** in the Custom OS Display section.

Provide the values you want to appear in host profiles for the following:

- In the **Vendor String** field, enter the operating system's vendor name. For example, the vendor for Microsoft Windows would be Microsoft.

- In the **Product String** field, enter the operating system's product name. For example, the product name for Microsoft Windows 2000 would be Windows.

- In the **Version String** field, enter the operating system's version number. For example, the version number for Microsoft Windows 2000 would be 2000.

Step 17   In the OS Vulnerability Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping.

You must specify a Vendor and Product name in this section if you want to use the fingerprint to identify vulnerabilities for matching hosts or if you do not assign custom operating system display information.

To map vulnerabilities for all versions of an operating system, specify only the vendor and product name.

Note

Not all options in the **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** drop-down lists may apply to the operating system you choose. In addition, if no definition appears in a list that matches the operating system you want to fingerprint, you can leave these values empty. Be aware that if you do not create any OS vulnerability mappings in a fingerprint, the system cannot use the fingerprint to assign a vulnerabilities list with hosts identified by the fingerprint.

Example:

If you want your custom fingerprint to assign the list of vulnerabilities from Redhat Linux 9 to matching hosts, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

Example:

To add all versions of the Palm OS, you would choose **PalmSource, Inc.** from the **Vendor** list, **Palm OS** from the **Product** list, and leave all other lists at their default settings.

Step 18   Click **Create**.
The Custom Fingerprint status page refreshes every ten seconds and should reload with a "Ready" status.

Note

If the target system stops responding during the fingerprinting process, the status shows an `ERROR: No Response` message. If you see this message, submit the fingerprint again. Wait three to five minutes (the time

period may vary depending on the target system), click **Edit** ( ) to access the Custom Fingerprint page, and then click **Create**.

What to do next

- Activate the fingerprint as described in Activating and Deactivating Fingerprints, on page 4.

Host Input Data

You can augment the network map by importing network map data from third parties. You can also use the host input feature by modifying operating system or application identities or deleting application protocols, protocols, host attributes, or clients using the web interface.

The system may reconcile data from multiple sources to determine the current identity of an operating system or application.

All data except third-party vulnerabilities is discarded when the affected host is removed from the network map. For more information on setting up scripts or import files, see the *Firepower System Host Input API Guide*.

To include imported data in impact correlations, you must map the data to the operating system and application definitions in the database.

Requirements for Using Third-Party Data

You can import discovery data from third-party systems on your network. However, to enable features where intrusion and discovery data are used together, such as Cisco recommendations, adaptive profile updates, or impact assessment, you should map as many elements of it as possible to corresponding definitions. Consider the following requirements for using third-party data:

- If you have a third-party system that has specific data on your network assets, you can import that data using the host input feature. However, because third parties may name the products differently, you must map the third-party vendor, product, and versions to the corresponding Cisco product definition. After you map the products, you must enable vulnerability mappings for impact assessment in the Firewall Management Center configuration to allow impact correlation. For versionless or vendorless application protocols, you need to map vulnerabilities for the application protocols in the Firewall Management Center configuration.

- If you import patch information from a third party and you want to mark all vulnerabilities fixed by that patch as invalid, you must map the third-party fix name to a fix definition in the database. All vulnerabilities addressed by the fix will then be removed from hosts where you add that fix.

- If you import operating system and application protocol vulnerabilities from a third party and you want to use them for impact correlation, you must map the third-party vulnerability identification string to vulnerabilities in the database. Note that although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot import and map third-party client vulnerabilities. After the vulnerabilities are mapped, you must enable third-party vulnerability mappings for impact assessment in the Firewall Management Center configuration. To cause application protocols without vendor or

version information to map to vulnerabilities, an administrative user must also map vulnerabilities for the applications in the Firewall Management Center configuration.

• If you import application data and you want to use that data for impact correlation, you must map the vendor string for each application protocol to the corresponding Cisco application protocol definition.

Related Topics

Third-Party Product Mappings

When you add data from third parties to the network map through the user input feature, you must map the vendor, product, and version names used by the third party to the Cisco product definitions. Mapping the products to Cisco definitions assigns vulnerabilities based on those definitions.

Similarly, if you are importing patch information from a third party, such as a patch management product, you must map the name for the fix to the appropriate vendor and product and the corresponding fix in the database.

Mapping Third-Party Products

If you import data from a third party, you must map the Cisco product to the third-party name to assign vulnerabilities and perform impact correlation using that data. Mapping the product associates Cisco vulnerability information with the third-party product name, which allows the system to perform impact correlation using that data.

If you import data using the host input import feature, you can also use the AddScanResult function to map third-party products to operating system and application vulnerabilities during the import.

For example, if you import data from a third party that lists Apache Tomcat as an application and you know it is version 6 of that product, you could add a third-party map where:

• **Vendor Name** is set to `Apache`.

• **Product Name** is set to `Tomcat`.

• **Apache** is chosen from the **Vendor** drop-down list.

• **Tomcat** is chosen from the **Product** drop-down list.

• **6** is chosen from the **Version** drop-down list

This mapping would cause any vulnerabilities for Apache Tomcat 6 to be assigned to hosts with an application listing for Apache Tomcat.

Note that for versionless or vendorless applications, you must map vulnerabilities for the application types in the Secure Firewall Management Center configuration. Although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot import and map third-party client vulnerabilities.

Tip If you have already created a third-party mapping on another Secure Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported mapping to suit your needs.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **User Third-Party Mappings**.

Step 3 You have two choices:

- Create — To create a new map set, click **Create Product Map Set**.
- Edit — To edit an existing map set, click **Edit** (✐) next to the map set you want to modify. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Mapping Set Name**.

Step 5 Enter a **Description**.

Step 6 You have two choices:

- Create — To map a third-party product, click **Add Product Map**.
- Edit — To edit an existing third-party product map, **Edit** (✐) next to the map set you want to modify. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 7 Enter the **Vendor String** used by the third-party product.

Step 8 Enter the **Product String** used by the third-party product.

Step 9 Enter the **Version String** used by the third-party product.

Step 10 In the Product Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping from the **Vendor**, **Product**, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** fields.

Example:

If you want a host running a product whose name consists of third-party strings to use the vulnerabilities from Red Hat Linux 9, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

Step 11 Click **Save**.

Mapping Third-Party Product Fixes

If you map a fix name to a particular set of fixes in the database, you can then import data from a third-party patch management application and apply the fix to a set of hosts. When the fix name is imported to a host, the system marks all vulnerabilities addressed by the fix as invalid for that host.

Procedure

Step 1	Choose **Policies** > **Application Detectors**.
Step 2	Click **User Third-Party Mappings**.
Step 3	You have two choices:

- Create — To create a new map set, click **Create Product Map Set**.
- Edit — To edit an existing map set, click **Edit** (✏️) next to the map set you want to modify. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4	Enter a **Mapping Set Name**.
Step 5	Enter a **Description**.
Step 6	You have two choices:

- Create — To map a third-party product, click **Add Fix Map.**
- Edit — To edit an existing third-party product map, click **Edit** (✏️) next to it. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 7	Enter the name of the fix you want to map in the **Third-Party Fix Name** field.
Step 8	In the **Product Mappings** section, choose the operating system, product, and versions you want to use for fix mapping from the following fields:

- **Vendor**
- **Product**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **Build**
- **Patch**
- **Extension**

Example:

If you want your mapping to assign the fixes from Red Hat Linux 9 to hosts where the patch is applied, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

Step 9	Click **Save** to save the fix map.

Mapping Third-Party Vulnerabilities

To add vulnerability information from a third party to the VDB, you must map the third-party identification string for each imported vulnerability to any existing SVID, Bugtraq, or SID. After you create a mapping for the vulnerability, the mapping works for all vulnerabilities imported to hosts in the network map and allows impact correlation for those vulnerabilities.

You must enable impact correlation for third-party vulnerabilities to allow correlation to occur. For versionless or vendorless applications, you must also map vulnerabilities for the application types in the Secure Firewall Management Center configuration.

Although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot use third-party client vulnerabilities for impact assessment.

Tip If you have already created a third-party mapping on another Secure Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported mapping to suit your needs.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **User Third-Party Mappings**.

Step 3 You have two choices:

- Create — To create a new vulnerability set, click **Create Vulnerability Map Set**.
- Edit — To edit an existing vulnerability set, click **Edit** (✎) next to the vulnerability set. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Click **Add Vulnerability Map**.

Step 5 Enter the third-party identification for the vulnerability in the **Vulnerability ID** field.

Step 6 Enter a **Vulnerability Description**.

Step 7 Optionally:

- Enter a Snort ID in the **Snort Vulnerability ID Mappings** field.
- Enter a legacy vulnerability ID in the **SVID Mappings** field.
- Enter a Bugtraq identification number in the **Bugtraq Vulnerability ID Mappings** field.

Step 8 Click **Add**.

Related Topics

Enabling Network Discovery Vulnerability Impact Assessment

Custom Product Mappings

You can use product mappings to ensure that servers input by a third party are associated with the appropriate Cisco definitions. After you define and activate the product mapping, all servers or clients on monitored hosts that have the mapped vendor strings use the custom product mappings. For this reason, you may want to map vulnerabilities for all servers in the network map with a particular vendor string instead of explicitly setting the vendor, product, and version for the server.

Creating Custom Product Mappings

If the system cannot map a server to a vendor and product in the VDB, you can manually create the mapping. When you activate a custom product mapping, the system maps vulnerabilities for the specified vendor and product to all servers in the network map where that vendor string occurs.

Note Custom product mappings apply to all occurrences of an application protocol, regardless of the source of the application data (such as Nmap, the host input feature, or the system itself). However, if third-party vulnerability mappings for data imported using the host input feature conflicts with the mappings you set through a custom product mapping, the third-party vulnerability mapping overrides the custom product mapping and uses the third-party vulnerability mapping settings when the input occurs.

You create lists of product mappings and then enable or disable use of several mappings at once by activating or deactivating each list. When you specify a vendor to map to, the system updates the list of products to include only those made by that vendor.

After you create a custom product mapping, you must activate the custom product mapping list. After you activate a list of custom product mappings, the system updates all servers with occurrences of the specified vendor strings. For data imported through the host input feature, vulnerabilities update unless you have already explicitly set the product mappings for this server.

If, for example, your company modifies the banner for your Apache Tomcat web servers to read `Internal Web Server`, you can map the vendor string `Internal Web Server` to the vendor **Apache** and the product **Tomcat**, then activate the list containing that mapping, all hosts where a server labeled `Internal Web Server` occurs have the vulnerabilities for Apache Tomcat in the database.

Tip You can use this feature to map vulnerabilities to local intrusion rules by mapping the SID for the rule to another vulnerability.

Procedure

Step 1	Choose **Policies** > **Application Detectors**.
Step 2	Click **Custom Product Mappings**
Step 3	Click **Create Custom Product Mapping List**.
Step 4	Enter a **Custom Product Mapping List Name**.
Step 5	Click **Add Vendor String**.
Step 6	In the **Vendor String** field, enter the vendor string that identifies the applications that should map to the chosen vendor and product values.
Step 7	Choose the vendor you want to map to from the **Vendor** drop-down list.
Step 8	Choose the product you want to map to from the **Product** drop-down list.
Step 9	Click **Add** to add the mapped vendor string to the list.
Step 10	Optionally, repeat steps 4 to 8 as needed to add additional vendor string mappings to the list.
Step 11	Click **Save**.

What to do next

- Activate the custom product mapping list. For more information, see .

Editing Custom Product Mapping Lists

You can modify existing custom product mapping lists by adding or removing vendor strings or changing the list name.

Procedure

Step 1	Choose **Policies** > **Application Detectors**.
Step 2	Click **Custom Product Mappings**.
Step 3	Click **Edit** ( ) next to the product mapping list you want to edit.
	If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
Step 4	Make changes to the list as described in .
Step 5	When you finish, click **Save**.

Activating and Deactivating Custom Product Mappings

You can enable or disable use of an entire list of custom product mappings at once. After you activate a custom product mapping list, each mapping on that list applies to all applications with the specified vendor string, whether detected by managed devices or imported through the host input feature.

Procedure

Step 1	Choose **Policies** > **Application Detectors**.
Step 2	Click **Custom Product Mappings**.
Step 3	Click the slider next to the custom product mapping list to activate or deactivate it.
	If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.