

Application detection

Application detection is a process that

- identifies network traffic by application type,
- classifies network traffic to facilitate granular management, and
- enhances security.

Application detection provides administrators visibility into network usage patterns and enhances control over network management and policy enforcement.

- Application detection, on page 1
- Requirements and prerequisites for application detection, on page 7
- Custom application detectors, on page 7
- View or download detector details, on page 16
- Sort the detector list, on page 17
- Filter the detector list, on page 17
- Navigate to other detector pages, on page 19
- Activate and deactivate detectors, on page 19
- Edit custom application detectors, on page 20
- Deleting detectors, on page 21

Application detection

Application detection is a system capability that

- analyzes IP traffic to identify commonly used applications on your network,
- provides application awareness crucial for application control, and
- identifies applications according to characteristics specified in detectors.

Application detection types and sources

The system detects three types of applications:

- *application protocols* such as HTTP and SSH, representing communications between hosts
- *clients* such as web browsers and email clients, representing software running on the host

- *web applications* such as MPEG video and Facebook, representing the content or requested URL for HTTP traffic

The system identifies applications in network traffic according to the characteristics specified in the detector. For example, applications may be identified using ASCII patterns in packet headers. SSL protocol detectors use session information to identify the applications.

Application detectors come from two sources:

- *System-provided detectors* detect web applications, clients, and application protocols based on system software version and VDB. Professional Services can import individual detectors. Release notes provide information on updated detectors.
- *Custom application protocol detectors* are user-created to detect web applications, clients, and application protocols.

Implied application protocol detection, infers the existence of an application protocol based on client detection.

You can identify applications only if they originate from monitored network hosts as defined in your network discovery policy. If an internal host accesses an FTP server at an unmonitored remote site, the system does not identify the application protocol as FTP. However, if a remote or internal host accesses an FTP server on a monitored host, the system can identify the application protocol.

If the system identifies the client used by a monitored host to connect to a non-monitored server, it identifies the client's application protocol. However, it does not add this protocol to the network map. Client sessions must include a response from the server to occur for application detection.

The system characterizes each application that it detects; see Application rule conditions. The system uses these characteristics to create groups of applications, called *application filters*. Application filters are used to perform access control and to constrain search results and data used in reports and dashboard widgets.

You can also supplement application detector data using exported NetFlow records, Nmap active scans, and the host input feature.

Related Topics

Application detectors, on page 2

Application detectors

An application detector is a tool used in network analysis that

- identifies commonly used applications on your network by analyzing traffic patterns,
- provides customizable detection capabilities through different detector types, and
- operates only when active to analyze application traffic.

Application detector types and characteristics

Application detectors identify commonly used applications on your network. Use the Detectors page (**Policies** > **+ Show more** > **Advanced** > **Applications**) to view the detector list and customize detection capabilities.

Modify a detector or change its state (active or inactive) based on its type. The system uses only active detectors to analyze application traffic.

Note

- Cisco-provided detectors may change with system and VDB updates. Refer to the release notes for updates.
- For firepower application identification, we intentionally do not list the ports. The application's associate ports are not reported for any of Cisco's applications because most of the applications are port-agnostic. Our platform's detection capabilities can identify services running at any port in the network.

- *Internal detectors* are a special category of detectors for client, web application, and application protocol traffic. Internal detectors are delivered with system updates and are always on.

  If an application matches internal detectors for client-related activity and no specific client detector exists, it reports a generic client.
- *Client detectors* detect client traffic and are delivered via VDB or system update. These detectors are provided for import by Cisco Professional Services. You can activate and deactivate client detectors. You can export a client detector only if you import it.
- *Web application detectors* detect web applications in HTTP traffic payloads and are delivered via VDB or system update. Web application detectors are always on.
- *Port-based application protocol detectors* use well-known ports to identify network traffic. They are delivered via VDB or system update, or are provided for import by Cisco Professional Services. You can activate and deactivate application protocol detectors, and view a detector definition to use it as the basis for a custom detector.
- *Firepower-based application protocol detectors* analyze network traffic using Firepower application fingerprints and are delivered via VDB or system update. You can activate and deactivate application protocol detectors.
- *Custom application detectors* are pattern-based. They detect patterns in packets from client, web application, or application protocol traffic. You have full control over imported and custom detectors.

Identification of application protocols in the web interface

This table shows how the web interface system identifies application protocols:

Table 1: System identification of application protocols

Identification	Description
Application protocol name	The Firewall Management Center lists the protocol name if it is: • Positively identified by the system • Identified using NetFlow data and a correlation exists in `/etc/sf/services` • Manually identified using the host input feature • Identified by Nmap or an active source

Identification	Description
`pending`	The Firewall Management Center identifies an application protocol as `pending` if the system can neither positively nor negatively identify the application. The system usually needs to collect and analyze more connection data to identify a pending application. In the Application Details and Servers tables and in the host profile, the `pending` status appears only where specific application protocol traffic is detected, not inferred from detected client or web application traffic.
`unknown`	The Firewall Management Center identifies an application protocol as `unknown` if: • the application does not match any of the system's detectors. • the application protocol was identified using NetFlow data, but no port-application protocol correlation exists in `/etc/sf/services`. • Snort has closed the session, but the session still persists in the device. Here, the traffic is allowed to pass through the firewall, but the application is not detected.
blank	All available detected data has been examined, but no application protocol was identified. In the Application Details and Servers tables and in the host profile, the application protocol is left blank for generic client traffic without HTTP connections.

Implied application protocol detection from client detection

Implied application protocol detection is a process that

- occurs when the system can identify the client used by a monitored host to access a non-monitored server,
- allows the Firewall Management Center to infer that the connection uses the application protocol that corresponds with the client, and
- provides application protocol information for connections where monitored hosts access non-monitored servers.

Consequences of implied application protocol detection

This process has these consequences:

- The system does not generate a New TCP Port or New UDP Port event for these servers, preventing their appearance in the Servers table. Additionally, the detection of these application protocols cannot trigger discovery event alerts or correlation rules.
- The application protocol is not associated with a host. Its details cannot be viewed in host profiles, its server identity is not set, and its information is not used in host profile qualifications for traffic profiles or correlation rules. In addition, the system does not associate vulnerabilities with hosts based on this type of detection.

You can trigger correlation events when application protocol information is present in a connection. You can also use the application protocol information in connection logs to create connection trackers and traffic profiles.

Host limits and discovery event logging

The system generates a discovery event when it detects a client, server, or web application, unless the associated host has reached its maximum number of clients, servers, or web applications.

Each host profile displays up to 16 clients, 100 servers, and 100 web applications.

Actions that depend on the detection of clients, servers, or web applications are not affected by this limit. Access control rules set to activate on a server will continue to log connection events.

Special considerations for application detection

Special considerations for application detection are network traffic analysis requirements that

- define specific conditions needed for accurate detection of certain application protocols,
- address limitations in detecting encrypted or proxy-based traffic, and
- establish rules for identifying applications that use referral mechanisms or certificate-based identification.

Application-specific detection requirements

Different applications require specific detection approaches:

- **SFTP**: To detect SFTP traffic, the same rule must also detect SSH.
- **Squid**: The system identifies Squid server traffic when either the system detects a connection from a host on your monitored network to a Squid server where proxy authentication is enabled, or the system detects a connection from a Squid proxy server on your monitored network to a target system, like the the destination server where the client is requesting information or another resource.

The system cannot identify Squid service traffic if:

- proxy authentication is disabled, or
- the Squid proxy server is configured to strip through header fields from its HTTP responses

SSL application detection:

The system uses session information from a Secure Socket Layers (SSL) session to identify the application protocol, client application, or web application in the session.

When the system detects an encrypted connection, it marks that connection as either a generic HTTPS connection or as a specific secure protocols, like SMTPS, when applicable. When the system detects an SSL session, it adds `SSL client` to the **Client** field in connection events for the session. If it identifies a web application for the session, the system generates discovery events for the traffic.

For SSL application traffic, managed devices can also detect the common name from the server certificate and match that against a client or web application from an SSL host pattern. When the system identifies a specific client, it replaces `SSL client` with the name of the client.

Because the SSL application traffic is encrypted, the system can use only information in the certificate for identification, not application data within the encrypted stream. For this reason, SSL host patterns can sometimes only identify the company that authored the application, so SSL applications produced by the same company may have the same identification.

In some instances, such as when an HTTPS session is launched from within an HTTP session, managed devices detect the server name from the client certificate in a client-side packet.

To enable SSL application identification, you must create access control rules that monitor responder traffic. Those rules must have either an application condition for the SSL application or URL conditions using the URL from the SSL certificate. For network discovery, the responder IP address does not have to be in the networks to monitor in the network discovery policy; the access control policy configuration determines whether the traffic is identified. To identify detections for SSL applications, you can filter by the `SSL protocol` tag, in the application detectors list or when adding application conditions in access control rules.

Referred web applications:

Web servers sometimes refer traffic to other websites, which are often advertisement servers. To help you understand referred traffic on your network, the system lists the referring web application in the **Web Application** field for the referred sessio eventsn. The VDB contains a list of known referred sites. When the system detects traffic from one of those sites, the referring site is stored with the event for that traffic. For example, if an advertisement accessed via Facebook is actually hosted on Advertising.com, the detected Advertising.com traffic is associated with the Facebook web application. The system can also detect referring URLs in HTTP traffic, such as when a website provides a simple link to another site; in this case, the referring URL appears in the HTTP Referrer event field.

In events, if a referring application exists, it is listed as the web application for the traffic, while the URL is that for the referred site. In the example above, the web application for the connection event for that traffic would be Facebook, but the URL would be Advertising.com. A referred application may appear as the web application if no referring web application is detected, if the host refers to itself, or if there is a chain of referrals. In the dashboard, connection and byte counts for web applications include sessions where the web application is associated with traffic referred by that application.

Note When creating a rule for referred traffic, add a condition for the referred application instead of the referring application. To block Advertising.com traffic referred from Facebook, for example, add an application condition to your access control rule specific to Advertising.com.

Disable application detection in Snort 3

Disable application detection in Snort 3 by removing application rules and related policies that enable application monitoring.

Note Snort 3 is now at parity with Snort 2, with respect to enabling AppID inspection exclusively on particular network subnets that are defined in the Network Discovery policy filters **if** no other configuration in the AC policy requires AppID to monitor all traffic.

Snort 3 always enables application detection for all networks by default.

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control**, click edit policy and delete the application rules.

Step 2 Choose **Policies** > **Security policies** > **Decryption**, click delete to delete the SSL policy.

Step 3 Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**, click delete to delete the network discovery policy.

Step 4 Choose **Policies** > **Security policies** > **Access Control**. Click **Edit** (✎) to the policy you want to edit and then click the **Security Intelligence** > **URLs** tab to delete the URLs Allow or Block list.

Step 5 As you cannot delete default DNS rules, choose **Policies** > **Security policies** > **DNS**, click edit, and uncheck the enabled box to disable the DNS policy.

Step 6 In the access control policy, under the **Advanced** settings, disable the *Enable Threat Intelligence Director* and the *Enable reputation enforcement on DNS traffic* options.

Step 7 Save and deploy the access control policy.

Application detection is disabled in Snort 3, stopping any network monitoring for application identification.

Requirements and prerequisites for application detection

This reference provides the requirements and prerequisites for application detection, including model support, supported domains, and required user roles.

Model support

Any.

Supported domains

Any

User roles

- Administrator
- Discovery Admin

Custom application detectors

A custom application detector is a network monitoring tool that

- provides the system with information needed to identify custom applications on your network
- can be created as a custom web application, client, or application protocol detector, and
- is determined by your selections in the **Protocol**, **Type**, and **Direction** fields.

Custom application detector requirements and limitations

The system detects application protocols in server traffic when client sessions include a responder packet from the server. For UDP traffic, the system designates the server as the source of the responder packet.

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

You can export and import both custom detectors and those provided by Cisco Professional Services. However, you **cannot** export or import any other type of Cisco-provided detectors.

Custom application detector and user-defined application fields

Use these fields to configure custom application detectors and user-defined applications.

Custom application detector fields: general

You should use these fields to configure basic and advanced custom application detectors.

Table 2: General custom application detector fields

Field	Description
Application Protocol	The application protocol you want to detect. This can be a system-provided application or a user-defined application. If you want the application to be available for exemption from active authentication (configured in your identity rules), you should select or create an application protocol with the **`User-Agent Exclusion`** tag.
Description	A description for the application detector.
Name	A name for the application detector.
Detector Type	The type of detector, **`Basic`** or **`Advanced`**. Basic application detectors are created in the web interface as a series of fields. Advanced application detectors are created externally and uploaded as custom .lua files.

Custom application detector fields: detection patterns

Use these fields to configure the detection patterns for basic custom application detectors.

Table 3: Detection pattern fields

Field	Description
Direction	The source of the traffic the detector should inspect, **`Client`** or **`Server`**.
Offset	The location in a packet, in bytes from the beginning of the packet payload, where the system should begin the pattern search. Because packet payloads start at byte 0, calculate the offset by subtracting 1 from the number of bytes you want to move forward from the beginning of the packet payload. For example, to look for the pattern in the fifth bit of the packet, type `4` in the **Offset** field.
Pattern	The pattern string associated with the **Type** you selected.
Ports	The port of the traffic the detector should inspect.

Field	Description
Protocol	The protocol you want to detect. Your protocol selection determines whether the **Type** or the **URL** field displays. The protocol (and, in some cases, your subsequent selections in the **Type** and **Direction** fields) determine the type of application detector you create: web application, client, or application protocol.
Type	The type of pattern string you entered. The options you see are determined by the **Protocol** you selected. If you selected **`RTMP`** as the protocol, the **URL** field displays instead of the **Type** field. **Note** If you select **`User Agent`** as the **Type**, the system automatically sets the **Tag** for the application to **`User-Agent Exclusion`**.
URL	Either a full URL or a section of a URL from the swfURL field within the C2 message of a RTMP packet. This field displays instead of the **Type** field when you select **`RTMP`** as the **Protocol**. **Note** The detector assumes that the string you enter is a complete section of the URL. For example, entering **`cisco.com`** would match **`www.cisco.com/support`** and **`www.cisco.com`**, but not **`www.wearecisco.com`**.

Table 4: Application detector types by protocol and configuration

Detector Type	Protocol	Type or Direction
Web Application	HTTP	**Type** is **`Content Type`** or **`URL`**
	RTMP	Any
	SSL	Any
Client	HTTP	**Type** is **`User Agent`**
	SIP	Any
	TCP or UDP	**Direction** is **`Client`**
Application Protocol	TCP or UDP	**Direction** is **`Server`**

Table 5: Pattern string types and characteristics

Type Selection	String Characteristics
`ASCII`	The string is ASCII encoded.
`Common Name`	The string is the value in the commonName field within the server response message.
`Content Type`	The string is the value in the content-type field within the server response header.

Type Selection	String Characteristics
Hex	The string is in hexadecimal notation.
Organizational Unit	The string is the value in the organizationName field within the server response message.
SIP Server	The string is the value in the From field within the message header.
SSL Host	The string is the value in the server_name field within the ClientHello message.
URL	The string is a URL. **Note** The detector assumes that the string you enter is a complete section of the URL. For example, entering **cisco.com** would match **www.cisco.com/support** and **www.cisco.com**, but not **www.wearecisco.com**.
User Agent	The string is the value in the user-agent field within the GET request header. It is also available for the SIP protocol and indicates that the string is the value in the User-Agent field within the SIP message header.

User-defined application fields

Use these fields to configure user-defined applications within basic and advanced custom application detectors.

Table 6: User-defined application configuration fields

Field	Description
Business Relevance	The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally: **Very High**, **High**, **Medium**, **Low**, or **Very Low**. Select the option that best describes the application.
Categories	A general classification for the application that describes its most essential function.
Description	A description for the application.
Name	A name for the application.
Risk	The likelihood that the application is used for purposes that might be against your organization's security policy: **Very High**, **High**, **Medium**, **Low**, or **Very Low**. Select the option that best describes the application.
Tags	One or more predefined tags that provide additional information about the application. If you want an application to be available for exemption from active authentication (configured in your identity rules), you must add the **User-Agent Exclusion** tag to your application.

Configure custom application detectors

Configure custom application detectors to identify specific applications and protocols not covered by the default detectors, enabling more accurate traffic analysis and control.

Configure basic or advanced custom application detectors.

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 Click **Create Custom Detector**, and enter a **Name** and a **Description**.

Step 3 Choose an **Application Protocol** from the application drop-down list.

You have these options:

- If you are creating a detector for an existing application protocol (for example, if you want to detect a particular application protocol on a non-standard port), select the application protocol from the drop-down list.
- If you are creating a detector for a user-defined application, follow the procedure outlined in Create a user-defined application, on page 12.

Step 4 Click **Detector Type** as **Basic** or **Advanced** and click **OK**.

Step 5 Configure **Detection Patterns** or **Detection Criteria** or **Encrypted Visibility Engine Process Assignments**:

- If you are configuring a basic detector, specify preset **Detection Patterns** as described in Specifying detection patterns in basic detectors, on page 13.
- If you are configuring an advanced detector, specify custom **Detection Criteria** as described in Specify detection criteria in advanced detectors, on page 14.
- If you are configuring an encrypted visibility engine (EVE) detector, specify custom EVE process assignments as described in *Specifying EVE Process Assignments* section in this chapter.



Caution Advanced custom detectors are complex; ensure your knowledge of .lua files is adequate. Incorrect configuration can negatively impact performance or detection.

Step 6 Optionally, use **Packet Captures** to test the new detector as described in Testing a custom application protocol detector, on page 15.

Step 7 Click **Save**.



Note If you include the application in an access control rule, the detector is automatically activated and cannot be deactivated while it's in use.

The custom application detector is created and is ready for activation in access control rules and policies.

What to do next

Activate the detector as described in Activate and deactivate detectors, on page 19.

Related Topics

Custom application detector and user-defined application fields, on page 8

Create a user-defined application

Creating an application protocol detector to identify traffic that is not recognized by default system detectors. Applications, categories, and tags created here can be used in access control rules and application filters.

Caution Creating a user-defined application immediately restarts the Snort process without going through the deploy process. The system warns that continuing will restart the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior.

Before you begin

Begin configuring your custom application protocol detector as described in Configure custom application detectors, on page 11.

Follow these steps to create a user-defined application:

Procedure

Step 1 On the **Create A Custom Application Detector** dialog box, click **Add** (+) next to the **Application** field.

Step 2 Type a **Name**.

Step 3 Type a **Description**.

Step 4 Select a **Business Relevance**.

Step 5 Select a **Risk**.

Step 6 Click **Add** next to Categories to add a category and type a new category name, or select an existing category from the **Categories** drop-down list.

Step 7 Click **Add** next to Tags to add a tag and type a new tag name, or select an existing tag from the **Tags** drop-down list.

Note To associate the customized application detector domain for Policy Based Routing, you must select NSG from the **Tags** list.

Step 8 Click **OK**.

The user-defined application is created and is ready to be configured as part of your custom application protocol detector.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 11. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Custom application detector and user-defined application fields, on page 8

Specifying detection patterns in basic detectors

Configure a custom application protocol detector to search application protocol packet headers for a specific pattern string. You can also configure detectors to search for multiple patterns; requiring the application protocol traffic to match all patterns for positive identification.

Application protocol detectors can search for ASCII or hexadecimal patterns, using any offset.

Before you begin

Configure your custom application protocol detector as described in Configure custom application detectors, on page 11.

Follow these steps to specify detection patterns in basic detectors:

Procedure

Step 1 On the **Create Detector** page, in the **Detection Patterns** section, click **Add**.

Step 2 Choose protocol type from the **Application** drop-down list.

Step 3 Choose pattern type from the **Type** drop-down list.

Step 4 Type a **Pattern** string that matches the **Type** you specified.

Step 5 Optionally, type the **Offset** (in byte).

Step 6 Optionally, to identify application protocol traffic based on the port it uses, type a port from 1 to 65535 in the **Port(s)** field. To use multiple ports, separate them by commas.

Step 7 Click a **Direction**: `Client` or `Server`.

Step 8 Click **OK**.

Tip If you want to delete a pattern, click **Delete** ( ) next to the pattern you want to delete.

The detection pattern is successfully added to your custom application protocol detector configuration.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 11. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Specify detection criteria in advanced detectors, on page 14

Specify detection criteria in advanced detectors

Upload a custom .lua file to specify detection criteria for advanced custom application detectors.



Caution

- Advanced custom detectors are complex and require outside knowledge to construct valid .lua files. Incorrectly configured detectors could have a negative impact on performance or detection capability.
- Do not upload .lua files from untrusted sources.

Custom .lua files contain your custom application detector settings. Creating custom .lua files requires advanced knowledge of the lua programming language and experience with Cisco's C-lua API. Cisco strongly recommends you use these references to prepare .lua files:

- Third-party instruction and reference material for the lua programming language
- The Open Source Detectors Developers Guide: https://www.snort.org/downloads
- OpenAppID Snort community resources: http://blog.snort.org/search/label/openappid



Note The system does not support .lua files that reference system calls or file I/O.

Before you begin

- Begin configuring your custom application protocol detector as described in Configure custom application detectors, on page 11.
- Prepare to create a valid .lua file by downloading and studying the .lua files for comparable detectors. For more information about downloading detector files, refer to View or download detector details, on page 16.
- Create a valid .lua file that contains your custom application detector settings.

Follow these steps to specify detection criteria in advanced detectors:

Procedure

Step 1 On the **Create Detector** page for an advanced custom application detector, in the **Detection Criteria** section, click **Add**.

Step 2 Click **Browse...** to navigate to the `.lua` file and upload it.

Step 3 Click **OK**.

The .lua file is uploaded and the detection criteria are specified for your advanced custom application detector.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 11. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Specifying detection patterns in basic detectors, on page 13

Specifying EVE process assignments

Configure custom application detectors to map processes detected by the encrypted visibility engine (EVE) to applications.

Before you begin

Configure your custom application protocol detector as described in the relevant section on Configure custom application detectors, on page 11.

Follow these steps to specify EVE process assignments:

Procedure

Step 1 On the Create Detector page, in the Encrypted Visibility Engine Process Assignments section, click **Add**.

Step 2 Enter the **Process Name** and **Minimum Process Confidence** value.



Note You can enter text in the **Process Name** field, and this is case-sensitive. The value should match the exact process name detected by EVE. The **Minimum Process Confidence** value ranges from 0 to 100. This is the number displayed in the **Encrypted Visibility Process Confidence Score** field in Connection Events.

For information about the **Encrypted Visibility Process Confidence Score** field, refer to the section *Connection and Security Intelligence Event Fields* in the Cisco Firepower Management Center Administration Guide.

Step 3 Click **Save**.

Step 4 In the Application Detector listing page, activate the detector that you created. For more information, refer to Activate and deactivate detectors, on page 19. When you activate the detector, the system pushes the detector files to all the FTDs registered on the Firewall Management Center.

Your EVE process assignments are set for your custom application detector, effectively mapping processes to the specified applications.

What to do next

Continue the configuration of your custom application protocol detector as described in Configure custom application detectors, on page 11 to enable system traffic analysis.

Testing a custom application protocol detector

Test a custom application protocol detector against packet capture (pcap) files to verify that the detector accurately identifies the intended application traffic before deploying it in your network environment.

If you have a packet capture (pcap) file that contains packets with traffic from the application protocol you want to detect, test it using a custom application protocol detector. Use a simple pcap file free of unnecessary traffic.

Pcap files must be 256 KB or smaller. If you test your detector with a larger pcap file, the Firewall Management Center automatically truncates it and tests the incomplete file. You must fix the unresolved checksums in a pcap before using the file to test a detector.

Before you begin

Configure your custom application protocol detector as described in Configure custom application detectors, on page 11.

Follow these steps to test a custom application protocol detector:

Procedure

Step 1 On the Create Detector page, in the **Packet Captures** section, click **Add**.

Step 2 Browse to the pcap file in the pop-up window and click **OK**.

Step 3 Click **Evaluate** next to the pcap file to test your detector against the contents of the pcap file. The system displays a message shwoing if the test was successful.

Step 4 Optionally, repeat steps 1 to 3 to test the detector against additional pcap files.

Tip To delete a pcap file, click **Delete** ( ) next to the file you want to delete.

The system evaluates your custom application protocol detector against the chosen pcap files and displays test results indicating the detector's success in identifying traffic.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 11. You must save and activate the detector before the system can use it to analyze traffic.

View or download detector details

Use the detectors list to view details for all application detectors and to download details for custom application detectors, supporting network security analysis and configuration management.

Procedure

Step 1 To view application detector details, choose from the available options:

- Refer to the *Cisco Firepower Application Detector Reference* for the relevant VDB version at https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html

- **a.** Select **Policies** > **+ Show more** > **Advanced** > **Applications**.
- **b.** Filter the list to find a particular detector.
- **c.** Click **Information**( )

Step 2 To download detector details for a custom application detector, click **Download** ( ).

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have the necessary permissions.

You can access application detector information either through the reference documentation or the management interface and download custom detector details.

Sort the detector list

Organize detectors in a specific order to make them easier to locate and manage by sorting the detector list.

By default, the Detectors page lists detectors alphabetically by name. An up or down arrow placed next to a column heading shows the sort direction.

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 Click the appropriate column heading.

The detector list is sorted according to the selected column, with an arrow indicator showing the sort direction.

Filter the detector list

Use filters to narrow down the detector list. Focus on specific types of detectors or detector characteristics relevant to your analysis or configuration needs.

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 Expand one of the filter groups described in Filter groups for the detector list, on page 18 and select the check box next to a filter. To select all filters in a group, right-click the group name and select **Check All**.

Step 3 If you want to remove a filter, click **Remove** ( ) in the name of the filter in the **Filters** field or disable the filter in the filter list. To remove all filters in a group, right-click the group name and select **Uncheck All**.

Step 4 If you want to remove all filters, click **Clear all** next to the list of filters applied to the detectors.

The system updates the detector list displaying only those detectors that match your selected criteria.

Filter groups for the detector list

You can use several filter groups, separately or in combination, to filter the list of detectors.

Name

Locate detectors using string-matching in names or descriptions. All alphanumeric and special characters are allowed.

Custom filter

Locates detectors using custom filters set up on the object management page.

Author

Filter detectors based on their creator, such as:

- Individual user: Custom detectors created or imported by a user
- Cisco: All detectors provided by Cisco, *except* imported add-on detectors (you are the author for any detector that you import)
- **Any User**: Detectors not provided by Cisco.

State

Filters detectors based on their status, either **Active** or **Inactive**.

Type

Filters detectors by type, as described in Application detectors, on page 2.

Protocol

Identifies detectors based on the inspected traffic protocol.

Category

Finds detectors based on the application categories they target.

Tag

Locates detectors by the tags assigned to applications.

Risk

Filters detectors based on the application risk levels: **Very High**, **High**, **Medium**, **Low**, and **Very Low**.

Business relevance

Filters detectors according to the business relevance of applications: **Very High**, **High**, **Medium**, **Low**, and **Very Low**.

Navigate to other detector pages

Detector pages display large amounts of data across multiple pages. Use the navigation controls to move efficiently between pages.

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 If you want to view the next page, click **Right Arrow** ( ).

Step 3 If you want to view the previous page, click **Left Arrow** ( ).

Step 4 If you want to view a different page, type the page number and press Enter.

Step 5 If you want to jump to the last page, click **Right End Arrow** ( ).

Step 6 If you want to jump to the first page, click **Left End Arrow** ( ).

You can now navigate efficiently between detector pages using the available navigation controls.

Activate and deactivate detectors

Activate detectors to analyze network traffic or deactivate unused detectors to improve performance.

You must activate a detector before you can use it to analyze network traffic. By default, all Cisco-provided detectors are activated.

You can activate multiple application detectors for each port to enhance detection.

If you include an application in an access control rule in a policy and that policy is deployed without an active detector for that application, one or more detectors automatically activate. You cannot deactivate a detector while an application is in use in a deployed policy if doing so leaves no active detectors for that application.

Tip For improved performance, deactivate any application protocol, client, or web application detectors you do not intend to use.

Caution Activating or deactivating a system or custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior.

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 Click the slider next to the detector you want to activate or deactivate. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Note Some application detectors are required by other detectors. If you deactivate one of these detectors, a warning appears to indicate that the detectors that depend on it are also disabled.

The detector activation status changes immediately. When you activate or deactivate a system or custom application detector, the Snort process automatically restarts.

Edit custom application detectors

Use this procedure to modify the custom application detectors already configured in your system.

Before you begin

Follow these steps to edit custom application detectors:

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 Click **Edit** (✎) next to the detector 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 3 Make changes to the detector as described in Configure custom application detectors, on page 11.

Step 4 Choose an appropriate saving options based on the state of the detector:

- To save an inactive detector, click **Save**.
- To save an inactive detector as a new, inactive detector, click **Save as New**.
- To save an active detector and immediately start using it, click **Save and Reactivate**.

Caution Saving and reactivating a custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing will restart the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior.

- To save an active detector as a new, inactive detector, click **Save as New**.

The custom application detector is modified and saved based on your selected option.

Deleting detectors

You can delete custom detectors as well as individually imported add-on detectors provided by Cisco Professional Services. You cannot delete any of the other Cisco-provided detectors, though you can deactivate many of them.

Note While a detector is in use in a deployed policy, you cannot delete the detector.

Caution Deleting an activated custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior.

Procedure

Step 1 Select **Policies** > **+ Show more** > **Advanced** > **Applications**.

Step 2 Click **Delete** ( ) next to the detector you want to delete. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Click **OK**.