

Intrusion Prevention System

Table 1: Feature History

Feature Name	Release Information	Description
Snort Engine Version Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature adds support for Snort engine version 3, which is an upgrade from version 2.
Custom IPS Signature Sets	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	With custom IPS signature sets,you can create custom Snort 3 signature sets, override supported rule and rule-group behavior, create custom rules, and add comments for traceability in Cisco SD-WAN Manager.

This feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco Catalyst SD-WAN. It is delivered using a virtual image on Cisco IOS XE Catalyst SD-WAN devices. This feature uses the Snort engine to provide IPS and IDS functionalities.

Snort is an open source network IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks. It can also perform protocol analysis, content searching or matching, and detect a variety of attacks and probes (such as buffer overflows).

- Overview of Intrusion Prevention System, on page 2
- Cisco Catalyst SD-WAN IPS Solution, on page 2
- Configure and Apply IPS or IDS, on page 2
- Modify an Intrusion Prevention or Detection Policy, on page 6
- Delete an Intrusion Prevention or Detection Policy , on page 6
- Monitor Intrusion Prevention Policy, on page 6
- Update IPS Signatures, on page 7
- Update IPS Signatures and Custom Signature Rules, on page 8
- Process Single Stream Large Session (Elephant Flow) by UTD, on page 14
- Configure Intrusion Prevention System for Unified Security Policy, on page 15
- Custom IPS signature sets, on page 17

Overview of Intrusion Prevention System

The IPS feature works in the network intrusion detection and prevention mode that provides IPS or IDS functionalities. In the network intrusion detection and prevention mode, the engine performs the following actions:

- Monitors network traffic and analyzes against a defined rule set.
- Performs attack classification.
- Invokes actions against matched rules.

Based on your requirements, you can enable Snort either in IPS or IDS mode. In IDS mode, the engine inspects the traffic and reports alerts, but does not take any action to prevent attacks. In IPS mode, in addition to intrusion detection, actions are taken to prevent attacks.

IPS the traffic and reports events to Cisco SD-WAN Manager or an external log server (if configured). External third party monitoring tools, which supports Snort logs, can be used for log collection and analysis.

Cisco Catalyst SD-WAN IPS Solution

The Snort IPS solution consists of the following entities:

- Snort sensor: Monitors the traffic to detect anomalies based on the configured security policies (that includes signatures, statistics, protocol analysis, and so on) and sends alert messages to the Alert/Reporting server. The Snort sensor is deployed as a security virtual image on the router.
- Signature store: Hosts the Cisco Talos signature packages that are updated periodically. Cisco SD-WAN Manager periodically downloads signature packages to the Snort sensors. You can modify the time interval to check for and download signature updates in **Administration** > **Settings** > **IPS Signature Update** (in releases through Cisco vManage Release 20.9.1) or **Administration** > **Settings** > **UTD Snort Subscriber Signature** (in releases beginning with Cisco vManage Release 20.10.1).



Note Options for downloading UTD signature packages out of band from Cisco.com and uploading them to Cisco SD-WAN Manager or a remote server and options for custom signatures are available from Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

- Alert/Reporting server: Receives alert events from the Snort sensor. Alert events generated by the Snort sensor can either be sent to Cisco SD-WAN Manager or an external syslog server or to both Cisco SD-WAN Manager and an external syslog server. Cisco SD-WAN Manager events can be viewed in **Monitor** > **Events**. No external log servers are bundled with the IPS solution.

Configure and Apply IPS or IDS

To configure and apply IPS or IDS to a Cisco IOS XE Catalyst SD-WAN device, do the following:

- Before you Begin
- Configure Intrusion Prevention or Detection
- Apply Intrusion Prevention Policy to a Device

Before you Begin

Before you apply an IPS/IDS, URL Filtering, or Advanced Malware Protection policy for the first time, you must Upload the Cisco Security Virtual Image to vManage.

Configure Intrusion Prevention or Detection

To configure Intrusion Prevention or Detection through a security policy, use the Cisco SD-WAN Manager security configuration wizard:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
3. In Add Security Policy, choose a scenario that supports intrusion prevention (**Compliance**, **Direct Cloud Access**, **Direct Internet Access**, or **Custom**).
4. Click **Proceed** to add an Intrusion Prevention policy in the wizard.
5. In the **Add Security Policy** wizard, click **Next** until the **Intrusion Prevention** window displays.
6. Click the **Add Intrusion Prevention Policy** drop-down menu and choose **Create New** to create a new Intrusion Prevention policy. The Intrusion Prevention - Policy Rule Configuration wizard appears.
7. Click **Target VPNs** to add the required number of target service VPNs in the Add Target VPNs wizard.
8. Enter a policy name in the **Policy Name** field.
9. Choose a signature set that defines rules for evaluating traffic from the **Signature Set** drop-down menu. The following options are available. Connectivity provides the least restrictions and the highest performance. Security provides the most restrictions but can affect system performance.
    - **Balanced**: Designed to provide protection without a significant effect on system performance.

      This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 9. It also blocks CVEs published in the last two years and that have the following rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.
    - **Connectivity**: Designed to be less restrictive and provide better performance by imposing fewer rules.

      This signature set blocks vulnerabilities with a CVSS score of 10 and CVEs published in the last two years.
    - **Security**: Designed to provide more protection than Balanced but with an impact on performance.

      This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 8. It also blocks CVEs published in the last three years and that have the following rule categories: Malware CNC, Exploit Kits, SQL Injection, blocked list, and App Detect Rules.

10. Choose mode of operation from the **Inspection Mode** drop-down menu. The following options are available:
    - **Detection**: Choose this option for intrusion detection mode
    - **Protection**: Choose this option for intrusion protection mode

11. (Optional) From **Advanced**, choose one or more existing IPS signature lists or create new ones as needed from the **Signature Whitelist** drop-down menu.

    Choosing an IPS signature list allows the designated IPS signatures to pass through.

    To create a new signature list, do the following:

    a. Click **New Signature List** at the bottom of the drop-down. In **IPS Signature List Name**, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only).

    b. In **IPS Signature**, enter signatures in the format `Generator ID:Signature ID`, separated with commas. You also can use **Import** to add a list from an accessible storage location.

    c. Click **Save**.

    You also can create or manage IPS Signature lists by choosing **Configuration** > **Security**, and then choosing **Lists** from **Custom Options**, and then choosing **Signatures**.

    To remove an IPS Signature list from the **Signature Whitelist** field, click the **X** next to the list name in the field.

12. (Optional) Choose a minimum alert level for syslogs from the **Alert Log Level** drop-down menu. The options are:

    Table 2: Alert Log Levels

Alert Level	Alert	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Info	Informational messages
7	Debug	Debug-level messages

    You must configure the address of the external log server in the Policy Summary page.

13. Click **Save Intrusion Prevention Policy** to add an Intrusion Prevention policy.

14. Click **Next** until the Policy Summary page is displayed

15. Enter Security Policy Name and Security Policy Description in the respective fields.

16. If you set an alert level when configuring the Intrusion Prevention policy, in the Additional Policy Settings section, you must specify the following:
    - External Syslog Server VPN: The syslog server should be reachable from this VPN.
    - Server IP: IP address of the server.
    - Failure Mode: **Open** or **Close**
17. Click **Save Policy** to configure the Security policy.
18. You can edit the existing Intrusion Prevention policy by clicking on **Custom Options** in the right-side panel of the Cisco SD-WAN Manager menu, **Configuration** > **Security** wizard.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.



Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.

   The **Additional Templates** section is displayed.
6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click **…** next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.



Note If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco SD-WAN Manager, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

Modify an Intrusion Prevention or Detection Policy

To modify a intrusion prevention or detection policy, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. In the Security window, click **Custom Options** drop-down menu and choose **Intrusion Prevention**.
3. For the policy you want to modify, click **…** and choose **Edit**.
4. Modify the policy as required and click **Save Intrusion Prevention Policy**.

Delete an Intrusion Prevention or Detection Policy

To delete an intrusion prevention or detection policy, you must first detach the policy from the security policy:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Detach the IPS or IDS policy from the security policy as follows:
   a. For the security policy that contains the IPS or IDS policy, click **...** and choose **Edit**.

      The Policy Summary page is displayed.

   b. Click **Intrusion Prevention**.
   c. For the policy that you want to delete, click **...** and choose **Detach**.
   d. Click **Save Policy Changes**.
3. Delete the IPS or IDS policy as follows:
   a. In the Security screen, click **Custom Options** drop-down menu and choose **Intrusion Prevention**.
   b. For the policy that you want to delete, click **...** and choose **Delete**.

      A dialog box is displayed.

   c. Click **OK**.

Monitor Intrusion Prevention Policy

You can monitor the Intrusion Prevention System (IPS) signature violations by severity and by count using the following steps.

To monitor the Signatures of IPS Configuration on Cisco IOS XE Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. In the left panel, under **Security Monitoring**, Click **Intrusion Prevention**. The Intrusion Prevention wizard displays.
3. Click **By Severity** or **By Count** to designate how you want to display intrusion prevention information.

Update IPS Signatures

Supported releases: Cisco SD-WAN Release 20.9.1 and earlier releases

IPS uses Cisco TALOS signatures to monitor the network. We recommend that you use the following procedure to download the latest signatures.



Note To download the signatures, Cisco Catalyst SD-WAN Manager requires access to the following domains using port 443:

- api.cisco.com
- cloudsso.cisco.com
- dl.cisco.com
- dl1.cisco.com
- dl2.cisco.com
- dl3.cisco.com
- download-ssc.cisco.com
- softwarecloud.cisco.com
- id.cisco.com
- apix.cisco.com

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** to configure IPS Signature Update.
2. Click on **Edit** to **Enable/Disable** and provide your Cisco.com **Username** and **Password** details to save the Policy details.

Update IPS Signatures and Custom Signature Rules

Table 3: Feature History

Feature Name	Release Information	Description
IPS Custom Signature and Offline Updates	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature lets you download IPS signature packages for the Intrusion Prevention System (IPS) out-of-band from Cisco SD-WAN Manager and upload these packages to Cisco SD-WAN Manager or a remote server. Cisco SD-WAN Manager then distributes these IPS signature packages to the devices on your network. This feature also lets you upload a custom signature rules file to Cisco SD-WAN Manager or a remote server, which Cisco SD-WAN Manager then distributes and appends to the existing IPS signature package rules.

Information About IPS Custom Signature and Offline Updates

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, if Cisco SD-WAN Manager does not have an internet connection, you can download IPS signature packages locally and either upload them directly to Cisco SD-WAN Manager or to a remote server or servers to which your devices have network access. Cisco SD-WAN Manager does not need to have network access to the remote servers. You also can append custom signature rules to the current Cisco TALOS signature rules file. This custom signature rules file can also be uploaded to Cisco SD-WAN Manager or to a remote server or servers to which your devices have network access.

The filename of an IPS signature package has the format shown in this example, where the numbers represent the Snort engine version and the version of the IPS signature package:
UTD-STD-SIGNATURE-29181-105-S.pkg

The first number is the Snort engine version and the second number is the version of the IPS signature package for the Snort engine. In this example, the filename represents the 105th release of the IPS signature package for the 2.9.18.1 Snort engine.

Prerequisites for IPS Custom Signature and Offline Updates

- To download the signatures, Cisco SD-WAN Manager requires access to the following domains using port 443:
  - api.cisco.com
  - cloudsso.cisco.com

- dl.cisco.com
- dl1.cisco.com
- dl2.cisco.com
- dl3.cisco.com
- download-ssc.cisco.com
- softwarecloud.cisco.com
- id.cisco.com
- apix.cisco.com

- If you enable **IPS Signatures** and choose the **Remote Server** or **Local** option, you must download a separate IPS signature package for each Snort engine version that is used in your network.

  You can download the latest IPS signature packages for your Snort engines from the following page. The latest IPS signature package for each Snort engine is shown at the top left corner of this page.

  https://software.cisco.com/download/home/284389362/type/286285292/release/

  To determine the version of the Snort engine or engines that you are using, you can use the **show utd engine standard version** command or check the UTD package filename.

  For example, in the following output of the **show utd engine standard version** command, the Snort engine version number is 2.9.18.1, so you should use the latest 29181 IPS signature package release:

  ```
  Device# show utd engine standard version
  IOS-XE Recommended UTD Version: 1.0.6_SV2.9.18.1_XE17.9
  IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.9$
  ```

  Similarly, in the following UTD package filename, the Snort engine version number is 2.9.18.1, so again you should use the latest 29181 IPS signature package release:

  secapp-utd.17.09.01a.1.0.6_SV**2.9.18.1**_XE17.9.x86_64.tar

- The IPS signature packages are updated approximately every 24 to 72 hours. If you enable **IPS Signatures** and choose the **Remote Server** or **Local** option, we recommend that you check for new IPS signature packages daily to ensure that the IPS signature packages that you are using are up to date.
- If you use an IPS signature package file on a remote sever and the filename that Cisco SD-WAN Manager points to includes the IPS signature package version, you must update the filename that Cisco SD-WAN Manager points to each time a new IPS signature package is uploaded to the remote server, for each Snort engine version used.

Configure IPS Custom Signature and Offline Updates

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

Use the procedure that this section describes to update IPS signatures and custom signature rules.

Before you begin, if you are using a remote server, we recommend that you perform either of the following actions for each Snort engine version that you are using to avoid needing to manually update the path in Cisco SD-WAN Manager each time a new IPS signature package is uploaded to the remote server:

- Remove the signature package version number (keeping the Snort engine version number) from the filename that Cisco SD-WAN Manager points to and override this filename on the remote server each time a new IPS signature package is uploaded for this Snort engine version.

  For example, rename UTD-STD-SIGNATURE-29181-105-S.pkg to UTD-STD-SIGNATURE-29181-S.pkg on the remote server and have Cisco SD-WAN Manager point to this filename. Then override this filename each time a new IPS signature package for the 2.9.18.1 Snort engine is uploaded to the remote server. Perform a similar action for each Snort engine version that is used.

- Use a symbolic link (symlink) on the remote server and update it to point to the latest IPS signature package each time a new IPS signature package is uploaded for a Snort engine version. In this case, have Cisco SD-WAN Manager point to this symbolic link.

- Every time you update the UTD signatures on Cisco IOS XE Catalyst SD-WAN devices, you must update the IPS signature package file on the remote server and on Cisco SD-WAN Manager.

- For a custom signature file, you must login to Cisco SD-WAN Manager and update the custom signature's file attributes, and these attributes are included in the UTD signature package metadata sent to the Cisco IOS XE Catalyst SD-WAN devices. This indicates that the custom signature file on the remote server has been updated and the file needs to be downloaded and applied on the device.

  For example, have a symbolic link called UTD-STD-SIGNATURE-29181-S.pkg that points to UTD-STD-SIGNATURE-29181-105-S.pkg on the remote server and have Cisco Catalyst SD-WAN Manager point to this symbolic link. Then update the file that this symbolic link points to each time a new IPS signature package for the 2.9.18.1 Snort engine is uploaded to the remote server. Perform a similar action for each Snort engine version that is used.

- For every custom signature file, ensure that each rule includes a `classtype` parameter. If a `classtype` is not specified, it will default to a classification value of 0, which may result in alerts being skipped or treated as low priority. By assigning a meaningful classification, you can guarantee that alerts are properly processed and categorized.

  For example:

  ```
  alert tcp any any -> any 20000 (msg:"DNP3 confirm"; dnp3_func: 0; classtype:misc-activity;
   sid:1000000;)
  ```

- UTD IPS signature package update using **Remote Server** option under **Administration** > > **Settings** > **UTD Snort Subscriber Signature** is successful only when the last modified time of signature package on remote server is recent than the last successful update time on UTD package.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** in the **UTD Snort Subscriber Signature** row.
3. In the **IPS Signature Download Interval Hours** and **Minute** fields, enter how often Cisco SD-WAN Manager attempts to download new IPS signature packages from Cisco.com.

   This interval is also used for how often Cisco SD-WAN Manager has the devices attempt to download the latest IPS signature package or packages and custom signature rules file from Cisco SD-WAN Manager or the remote server or servers.

   You can enter an interval from 2 hours to 24 hours. The default interval is 24 hours.
4. To enable the IPS signature package update, enable the **IPS Signatures** option, then click one of the following radio buttons to specify how the IPS signature packages are distributed by Cisco SD-WAN Manager:

- **Cisco.com**: Downloads IPS signature packages to Cisco SD-WAN Manager from Cisco.com, then causes the devices to download the IPS signature packages from Cisco SD-WAN Manager. This option requires that Cisco SD-WAN Manager has an internet connection.

  In the **Username** and **Password** fields, enter your Cisco Connection Online username and password.

- **Remote Server**: Devices download the IPS signature packages from one or more remote servers over a local network connection, not from Cisco SD-WAN Manager. We recommend that you use this option to avoid Cisco SD-WAN Manager scaling issues.

  From the **Select Remote Server** drop-down list, choose a remote server (you can use the **Search** field to find a server), or click **Add Remote Server** to configure a new remote server.

  If you click **Add Remote Server**, perform these actions:

  a. Enter information for this server in the following fields:

Field	Description
Server Name	Name of the server
Server IP/DNS name	IP address or DNS hostname of the server
Select Protocol	Protocol that is used for the Cisco SD-WAN Manager network connection to the server (**FTP**, **HTTP**, or **SCP**)
Port	Port on the server that is used for access to the server
User ID	Username for access to the server
Password	Password for access to the server
Image location prefix:	Path to the folder that contains the IPS signature package
VPN	VPN used for access to the server. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

  b. Click **Add** and choose the server from the **Select Remote Server** drop-down list.

  c. Click the **Remote Server Details** box that appears.

  d. In the **IPS Signature Filename** field, enter the filename of the IPS signature package or the symbolic link to this IPS signature package that is on the remote server.

  e. In the **IPS Signature Snort Version** field, enter the Snort engine version of the IPS signature package.

  f. Click **Add**.

- **Local**: Uploads IPS signature packages from a local computer to Cisco SD-WAN Manager, then causes the devices to download the IPS signature packages from Cisco SD-WAN Manager.

In the field that appears, click **Choose Files** and choose the IPS signature package, or drag and drop an IPS signature package. Then click **Add**.

5. (Optional) To change the IPS signature filename or Snort engine version for an IPS signature package on a remote server, perform the following actions.

Note If you are overwriting the filename or using a symbolic link for the file that Cisco SD-WAN Manager points to, you do not need to perform this step each time a new IPS signature package is uploaded to the remote server.

   a. Under **IPS Signatures**, click **Remote Server**.
   b. From the **Select Remote Server** drop-down menu, choose the server for which you want to update information.
   c. Click the server in the **Remote Server Details** box that appears.
   d. In the **IPS Signature Filename** field, enter the name of the IPS signature package file that is on the remote server.
   e. In the **IPS Signature Snort Version** field, enter the Snort engine version of the IPS signature package.
   f. Click **Add**.

6. To append custom signature rules to the current IPS signature package, enable **Custom Signature**, then click one of the following radio buttons to specify the location of the custom signature rules file.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, the Snort engine version has been upgraded from version 2 to version 3.

   The custom signature rules file must be a text file that contains rules in the appropriate Snort engine version rule format, be no larger than 1 MB, and have the .txt or .rules extension. Each rule should use the generator ID 1 or no generator ID (which defaults to 1), and the signature ID should be unique and greater than 1000000.

Note Cisco does not provide support for writing custom signatures or resolving issues with custom signatures and may request that you disable custom signatures before troubleshooting an issue.

Note Snort 2 and Snort 3 supported UTD versions cannot be used in combination with custom signatures since the custom signatures rules must either be in Snort 2 or Snort 3 format.

- **Remote Server**: Devices download the custom signature rules file from one or more remote servers over a local network connection, not from Cisco SD-WAN Manager. We recommend this option to optimize memory usage, as it prevents Cisco SD-WAN Manager from storing multiple image files locally.

  From the **Select Remote Server** drop-down list, choose a remote server(you can use the **Search** field to find a server), or click **Add Remote Server** to configure a new remote server.

If you click **Add Remote Server**, perform these actions:

a. Enter information for this server in the configuration fields. These fields are the same as the ones that are described for **Add Remote Server** in Step 4.

b. Click **Add** and choose the server from the **Select Remote Server** drop-down list.

c. Click the **Remote Server Details** box that appears.

d. In the **Custom Signature Filename** field, enter the name of the custom signature rules file that is on the remote server.

e. Click **Add**.

- **Local**: Uploads a custom signature rules file from a local computer to Cisco SD-WAN Manager, then causes the devices to download the custom signature rules file from Cisco SD-WAN Manager.

  In the field that appears, click **Choose Files** and choose the custom signature rules file, or drag and drop the custom signature rules file. Then click **Add**.

7. (Optional) To change the name of the custom signature rules file that is on a remote server, perform the following actions.



Note If you are overwriting the filename or using a symbolic link for the file that Cisco SD-WAN Manager points to, you do not need to perform this step each time a new custom signature rules file is uploaded to the remote server.

a. Under **Custom Signature**, click **Remote Server**.

b. From the **Select Remote Server** drop-down menu, choose the server for which you want to update information.

c. Click the server in the **Remote Server Details** box that appears.

d. In the **Custom Signature Filename** field, enter the name of the custom signature rules file that is on the remote server.

e. Click **Add**.

8. If you are appending custom signature rules to the current IPS signature package, perform these actions to enable custom signatures for a security policy:

a. From the Cisco SD-WAN Manager window, choose **Configuration** > **Security**.

b. Choose **Custom Options** > **Policies/Profiles**.

c. In the left panel, click **Intrusion Prevention**.

d. For the desired policy, click **...** and choose **Edit**.

e. Under the **Advanced** options, enable **Custom Signature Set** for the custom rules to be appended.

Process Single Stream Large Session (Elephant Flow) by UTD

Introduction

This document describes why a single flow cannot consume the entire rated throughput of a Cisco Unified Threat Defense (UTD) deployment.

Background Information

The result of any bandwidth speed testing website, or the output of any bandwidth measurement tool (for example, iperf) might not exhibit the advertised throughput rating of a Cisco UTD deployment. Similarly, the transfer of a very large file over any transport protocol does not demonstrate the advertised throughput rating of a Cisco UTD deployment. It occurs because the UTD service does not use a single network flow in order to determine its maximum throughput.

Process Traffic by Snort

The underlying detection technology of the UTD service is Snort. A Cisco UTD deployment (router model and UTD resource profile) is rated for a specific rating based on the total throughput of all flows that goes through the UTD container. It is expected that the routers with UTD are deployed on a Corporate network, usually near the border edge and works with thousands of connections.

Depending on the UTD resource profile used, UTD uses load balancing of traffic to a number of different Snort processes. Ideally, the system load balances traffic evenly across all of the Snort processes. Snort needs to be able to provide proper contextual analysis for Next-Generation Firewall (NGFW), Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) inspection. In order to ensure Snort is most effective, all the traffic from a single flow is load balanced to one Snort instance. If all the traffic from a single flow was not balanced to a single Snort instance, the system could be evaded and the traffic would spilt in such a way that a Snort rule might be less likely to match or pieces of a file are not contiguous for AMP inspection. Therefore, the load balancing algorithm is based on the connection information that can uniquely identify a given connection.

Traffic is load balanced to Snort using a 3-tuple algorithm. The datapoints for this algorithm are:

- Source IP
- Destination IP
- VRF

Any traffic with the same source, destination, and VRF are load balanced to the same instance of Snort.

Total Throughput

The total throughput of a UTD deployment is measured based on the aggregate throughput of all the Snort instances that work to their fullest potential. Industry standard practices in order to measure the throughput are for multiple HTTP connections with various object sizes. For example, the Network Security Services (NSS) NGFW test methodology measures total throughput of the device with 44k, 21k, 10k, 4.4k, and 1.7k objects. These translate to a range of average packet sizes from around 1k bytes to 128 bytes because of the other packets involved in the HTTP connection.

Different types of traffic, network protocols, sizes of the packets along with differences in the overall security policy can all impact the observed throughput of the device.

Third Party Tool Test Result

When you test with any speed testing website, or any bandwidth measurement tool, such as, iperf, one large single stream TCP flow is generated. This type of large TCP flow is called an Elephant Flow. An Elephant Flow is a single session, relatively long running network connection that consumes a large or disproportionate amount of bandwidth. This type of flow is assigned to one Snort instance, therefore the test result displays the throughput of single Snort instance, not the aggregate throughput rating of the UTD deployment.

Remediations

Configure a unified security policy so that trusted traffic can be exempted from UTD inspection to avoid any latency during data transfer. For more information about configuring a unified security policy, refer to Unified Security Policy.

Configure Intrusion Prevention System for Unified Security Policy

You can create an intrusion prevention policy specifically for use in a unified security policy. When created, intrusion prevention policy is included in the advanced inspection profile and applied to the unified security policy for implementation on Cisco IOS XE Catalyst SD-WAN devices.

To configure an intrusion prevention system for a unified security policy, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **Intrusion Prevention** in the left pane.
5. Click **Add Intrusion Prevention Policy**, and choose **Create New**.
6. Click **Policy Mode** to enable the unified mode. This implies that you are creating an intrusion prevention policy for use in the unified security policy.

Note Target VPNs are not applicable for the intrusion prevention system used in a unified security policy. The **Policy Mode** can only be set at time of creation and cannot be modified after the policy has been saved.

7. Enter a policy name in the **Policy Name** field.
8. From the **Signature Set** drop-down list, choose a signature set that defines rules for evaluating traffic. The following options are available. **Connectivity** provides the least restrictions and the highest performance. **Security** provides the most restrictions but can affect system performance.
   - **Balanced**: Provides protection without a significant effect on system performance.

     This signature set blocks vulnerabilities with a Common Vulnerability Scoring System (CVSS) score that is greater than or equal to 9. It also blocks (Common Vulnerabilities and Exposures) CVEs published in the last two years and have the following rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.

- **Connectivity**: Less restrictive and provides better performance by imposing fewer rules.

  This signature set blocks vulnerabilities with a CVSS score of 10 and CVEs published in the last two years.

- **Security**: Provides more protection than **Balanced** but with an impact on performance.

  This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 8. It also blocks CVEs published in the last three years and have the following rule categories: Malware CNC, Exploit Kits, SQL Injection, blocked list, and App Detect Rules.

9. From the **Inspection Mode** drop-down list, choose an option:

- **Detection**: Choose this option for intrusion detection mode.
- **Protection**: Choose this option for intrusion protection mode.

10. (Optional) From **Advanced**, choose one or more existing IPS signature lists or create new ones, as needed, from the **Signature Whitelist** drop-down list.

Choosing an IPS signature list allows the designated IPS signatures to pass through.

To create a new signature list, do the following:

a. Click **New Signature List** at the bottom of the drop-down list.

b. In the **IPS Signature List Name** field, enter a list name of up to 32 characters (letters, numbers, hyphens, and underscores only).

c. In the **IPS Signature**, enter signatures in the format `Generator ID:Signature ID`, separated by commas. You also can click **Import** to add a list from an accessible storage location.

d. Click **Save**.

You also can create or manage IPS Signature lists by choosing **Configuration** > **Security** in the left pane, choosing **Lists** from **Custom Options** at the top-right corner of the window, and then choosing **Signatures** in the left pane.

To remove an IPS Signature list from the **Signature Whitelist** field, click **X** next to the corresponding list name.

11. (Optional) Click **Alert Log Level**, and choose one of the following options:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

You configure the address of the external log server in the **Policy Summary** page.

12. Click **Save Intrusion Prevention Policy**.

Custom IPS signature sets

Custom Intrusion Prevention System (IPS) signature sets are user-created collections of Snort 3 threat-detection rules in Cisco Catalyst SD-WAN Manager. A custom signature set enables you to tailor IPS behavior by selecting a basesignature set, overriding supported rule or rule-group behavior, creating custom rules from supported existing rules, and adding comments for traceability.

A custom IPS signature set is different from an IPS signature package. An IPS signature package is a Cisco Talos signature file that Cisco Catalyst SD-WAN Manager downloads or uploads and distributes to devices. A custom IPS signature set defines how the available Snort 3 rules are selected and applied.

- Createsignature sets tailored to specific security needs and network environments.
- Overridethe default actions of supported IPS rules.
- Applysecurity-level overrides to supported rule categories or rule groups.
- Createcustom rules by duplicating supported existing rules

Create and apply custom IPS rules

Create custom IPS rules by duplicating and modifying supported existing rules. Custom rules are global objects that canbe reused across multiple signature sets. Deploy policies that include custom IPS signature sets through Policy Groups to enforce the security policy consistently across the SD-WAN network.

From SD-WAN Manager 26.2.x, the action labels shown in Cisco SD-WAN Manager and in Catalyst NGFW device threat events may differ. Cisco SD-WAN Manager displays custom IPS signature set actions as **Alert**, **Drop**, and **Disable**, while threat events from the corresponding device-side actions are **Block** or **Reject**.

Custom IPS policy levels

The information provided below is based on guidelines from Cisco Talos and is intended for advisory purposes only.

- Connectivity: This policy prioritizes device performance over strict security controls. It enables deployment with minimal false positives while maintaining full rated performance in most network environments. It focuses on detecting the most common and prevalent threats.

  Criteria

  - CVSS score = 10
  - CVE published within the past 2 years.

- Balanced: This default policy balances security effectiveness and device performance. It provides strong threat blocking capability with relatively high performance, making it suitable for initial deployments.

  Criteria:

  - CVSS score $\geq$ 9
  - CVE published within the past 2 years.

- Includes MALWARE-CNC, EXPLOIT-KIT, SQL Injection, and Blacklist rules.
- Includes all rules from the Connectivity policy.

- Security: This policy prioritizes maximum protection for environments with high security requirements and lower bandwidth needs. It tolerates higher false positives and supports strict application control and restricted network usage without disrupting network operations.

  Criteria:

  - CVSS score ≥ 8
  - CVE published within the past 3 years.
  - Includes MALWARE-CNC, EXPLOIT-KIT, SQL Injection, Blacklist, and App-detect rules.
  - Includes all rules from the Connectivity and Balanced policies.

- Maximum Detection: This policy supports testing environments and does not optimize for performance. It accepts higher false positives and broad detection coverage.

  Criteria:

  - Provides coverage required for field testing.
  - Includes all rules from the Security, Balanced, and Connectivity policies.
  - Includes all active rules with SID above 10000 unless specified otherwise.

Benefits of custom IPS signature sets

CustomIPS signature sets provide the following benefits:

- Custom signature-set creation: Create IPS signature sets tailored to specific security needs and network environments.
- Rule-action overrides: Changethe default action of an individual supported IPS rule within a signature set.
- Rule-group overrides: Apply a security level to a supported rule category or rule group to manage related rules consistently.
- Custom rule creation: Duplicate supported existing rules and modify the copies for organization-specific requirements.
- Reusable rules: Reuse custom rules across multiple custom signature sets.
- Comments: Add comments to rules for traceability and compliance auditing.
- Consistent enforcement: Deploy policies containing custom signature sets through Policy Groups.

Prerequisites for custom IPS signature packages

Beforeyou create a custom IPS signature set:

- Ensure that the Cisco IOS XE Catalyst SD-WAN device runs Release 17.18.1a or later.

- Ensure that Cisco SD-WAN Manager runs Release 20.18.1 or later.
- Ensure that the UTD image is Release 17.18.1 or later and is installed on at least one supported device.
- From Cisco SD-WAN Manager, choose **Administration** > **Settings** > **UTD Snort Subscriber Signature** and enable IPS signatures.
- Perform a UTD signature update. IPS rules appear in Cisco SD-WAN Manager only after a UTD image is installed on at least one device and the signatures are populated.
- If the download from Cisco.com fails, use a supported Local or Remote Server option and upload the appropriate IPS signature package.

Restrictions for custom IPS signature sets

- OnlySnort 3 IPS signature sets can be edited.
- System-defined rules and rule groups cannot be rewritten directly. Use rule actions, group overrides, or the supported duplication workflow.
- Only rules with Generator ID (GID) 1 can be duplicated.
- When you duplicate a Cisco Talos intrusion rule, assign a unique Signature ID (SID) greater than 1000000.
- Changes to a deployed custom signature set synchronize to the device at the next UTD signature-update interval.

Create and manage custom IPS signature sets

Use the following procedures to create, inspect, modify, and deploy a custom IPS signature set.



Note The Cisco SD-WAN Manager label **Group of Interest** is now **Objects and Profiles**.

Procedure

Step 1 Create a custom IPS signature set

a) From Cisco Catalyst SD-WAN Manager, choose **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**.
b) Select **Signature Set**, and click **Add Signature Set**.
c) Enter a unique name for the signature set.
d) Choose a **Base Signature Set**: Connectivity, Balanced, Security, Max-Detect, No-Rules-Active, or an available custom signature set. Modifications and updates from the selected base signature set apply to the new signature set.
e) Click **Save**.

Step 2 Manage a custom IPS signature set

Click the edit icon next to the signature set that you want to modify. If you change the signature-set name or base policy, deploy the policy group to apply the change. If a deployed custom signature set is modified, the change synchronizes to

the device at the next UTD signature-update interval. Check the timer under **Administration** > **Settings** > **UTD Snort Subscriber Signature**.

Step 3 View the base policy

Use the Base Policy tab to view the rules and actions inherited from the selected base signature set. Filter rules with the search field or Rule Action filter.

Step 4 Configure group overrides

On the Group Overrides tab, select a rule category or rule group and set its security level to Connectivity, Balanced, Security, Max-Detect, or Disable. To remove an override, select the applicable revert control and choose Revert to default.

Step 5 Configure rule overrides

On the Rule Overrides tab, locate a rule by using the search field or Rule Action filter. Change the action of a supported rule to Drop, Alert, Rewrite, or Disable. To undo an override, select the applicable revert control and choose Revert to default.

Step 6 Duplicate an intrusion rule

a) On the Rule Overrides tab, click the ellipsis (...) for a supported rule and choose **Duplicate**.
b) Assign a unique ID to the custom rule. For a duplicated Cisco Talos rule, use a unique SID greater than 1000000.
c) Add the custom rule to an existing custom rule group, or create a local rule group. Local rule groups appear under Group Overrides.
d) Modify the duplicated rule as required, and click **Create New**.

You can duplicate only rules with GID 1. The Duplicate option is unavailable for rules with other GID values.

Step 7 Add a comment

On the Rule Overrides tab, select the rule, click the ellipsis (...), add a comment that describes the change, and save the comment.

Step 8 Save and deploy the signature set

Click **Save**. If the custom signature set is associated with a deployed policy group, deploy or update the policy group as required. Rule changes synchronize according to the configured UTD signature-update interval.

Step 9 Troubleshoot missing IPS rules

If Cisco Catalyst SD-WAN Manager displays **No Rule Available** after you select **Edit Signature Set**, populate the IPS signatures manually:

a) Choose **Administration** > **Settings** > **UTD Snort Subscriber Signature**.
b) Under **IPS Signature**, choose **Local** from **Download From**.
c) Upload a UTD signature set. Version 3.3.5.0 or later is required. The upload can take several minutes.
d) Save the settings and verify that signature rules are available for editing.
e) Return **Download From** to its previous value, if appropriate, and save the settings.