Secure Router NGFW

Objective

Use this information to install, configure, migrate, verify, and monitor the Secure Router NGFW security-application container.

Feature history: Secure Router NGFW

Objective

Use the feature history to identify the releases that introduce Secure router NGFW and the capabilities included in those releases.

Table 1: Feature history

Feature name	Release information	Description
Secure Router NGFW	Cisco IOS XE Catalyst SD-WAN Release 26.2.1 Cisco Catalyst SD-WAN Manager Release 26.2.1	This feature introduces Secure Router NGFW, a new security-application container for supported Cisco Catalyst 8000 Series Secure Routers. In Cisco IOS XE Catalyst SD-WAN Release 26.2.1 and Cisco Catalyst SD-WAN Manager Release 26.2.1, it provides workflows to install the container and migrate supported settings from V1 Engine to V2 Engine. IPS and IDS retain their existing detection and prevention behavior while using Talos Lightweight Security Package (LSP) content. The release also adds Encrypted Visibility Engine (EVE) for encrypted-flow analysis without payload decryption and Snort ML inspection for supported threats. The V2 Engine replaces the UTD community/subscriber signature-package workflow with independently managed LSP and Vulnerability Database (VDB) packages. LSP provides Talos rules and detectors, while VDB provides application, fingerprint, and enrichment information.

About Secure Router NGFW

Secure Router NGFW is a security application container that provides advanced traffic inspection on supported Cisco Catalyst 8000 Series Secure Routers. It succeeds Unified Threat Defense (UTD) and hosts the security services introduced for the V2 engine.

The Cisco Catalyst SD-WAN Zone-Based Firewall (ZBFW) selects the traffic that requires advanced inspection. The Cisco Catalyst 8000 Series Secure Router diverts that traffic from the data plane to Secure Router NGFW, which inspects the flow and returns a verdict. The device then permits, rejects or blocks the flow and may export any applicable operational data if configured to do so.

Inspection engine

The inspection engine is the set of Secure Router NGFW services that receives traffic diverted from the data plane by ZBFW, applies the configured inspection policy and security content, and returns an inspection verdict. The inspected traffic remains within the device.

Snort 3 is the primary threat-inspection component in Secure Router NGFW. It evaluates selected traffic against the configured threat profile and Talos LSP rules, then returns an permit, alert, reject, or block result for enforcement and reporting.

Cisco SD-WAN Manager uses the term V1 Engine (UTD) and V2 Engine (Secure Router NGFW). SD-WAN Manager can manage a deployment that contains both V1 Engine and V2 Engine devices. An individual device can run only one security application container at a time: either UTD or Secure Router NGFW.

Release 26.2.1 capabilities

This release introduces the following Secure Router NGFW capabilities.

IPS/IDS

IPS/IDS uses Snort rules to detect threats. In IDS mode, matching traffic is permitted and an event is generated. In IPS mode, matching traffic is rejected and an event is generated. Secure Router NGFW provides the same IPS/IDS behavior as UTD but uses the Talos LSP ruleset. IPS/IDS also supports custom signatures and editable signature sets. By enabling the port-scan inspector, Secure Router NGFW can detect attempts to discover open ports and services. Port-scan detection supports Low, Medium, and High sensitivity levels and generates alerts and counters.

Encrypted Visibility Engine

Encrypted Visibility Engine (EVE) analyzes TLS handshake characteristics and VDB fingerprints without decrypting the application payload. Monitor mode adds likely-process and threat-confidence information to connection events. Protect mode can block High or Very High threat-confidence flows, subject to the configured exception rules.

Snort ML

Snort ML is an optional machine-learning inspection module for Snort 3. In this release, it inspects HTTP request headers for potential SQL injection attacks. Snort ML is supported with the Security and Max Detect threat policies. You must enable Snort ML globally for it to take effect in these threat policies.

LSP and VDB

Secure Router NGFW replaces the UTD community/subscriber signature-package workflow with two independently managed content packages. The Lightweight Security Package (LSP) contains Talos Snort rules, detectors, rule groups, and policy metadata. The Vulnerability Database (VDB) contains application, fingerprint, and enrichment information used by EVE and related inspection functions. For SD-WAN Manager-managed SD-WAN and SD-Routing deployments, online LSP and VDB content is obtained through the Cisco Catalyst SD-WAN Self-serve Portal (SSP), rather than downloaded from Cisco.com; Cloud Services must be enabled for this online workflow. LSP and VDB packages remain available on Cisco.com for deployments that are not managed by SD-WAN Manager and for users who manually manage package versions, such as in air-gapped deployments.

Cisco Catalyst SD-WAN Manager integration

Cisco Catalyst SD-WAN Manager orchestrates Secure Router NGFW for supported Cisco Catalyst SD-WAN and SD-Routing deployments. The integration separates policy intent from the selected V1 or V2 inspection engine so mixed deployments can be managed during migration.

Policy and lifecycle management

SD-WAN Manager adds V2 engine configuration while retaining the Advanced Inspection Policy workflow. Administrators can stage Secure Router NGFW images, select the V2 engine and resource profile, deploy IPS/IDS, EVE, and Snort ML configuration, migrate supported UTD configuration, schedule LSP and VDB updates, and remove images or uninstall the container through policy deployment.

IPS signature sets

An IPS signature set is a reusable collection of IPS rules that an administrator selects and customizes for an IPS profile. SD-WAN Manager displays the LSP rules that can be used in editable signature sets. An information marker identifies a rule as V1-only or V2-only; a rule without a marker applies to both engines. During supported V1-to-V2 migration, a V1 IPS signature list is converted to a custom editable signature set and associated with the migrated IPS profile. Global custom signatures are managed separately under Administration > Settings and can be referenced by Secure Router NGFW IPS profiles.

Monitoring integration

SD-WAN Manager provides security-dashboard widgets, Device360 security pages, connection-event fields, update-status views, and real-time operational views for the Secure Router NGFW engine, image version, inspection events, and LSP/VDB state. EVE analytics additionally exposes process and threat-confidence views when the analytics service is onboarded.

Benefits

Compared with UTD, Secure Router NGFW provides the following additional capabilities:

1. Adds encrypted-flow visibility through EVE and Snort ML inspection.

Supported platforms

Objective

Use the supported-platform information to determine the platform family documented for Secure Router NGFW.

Cisco Catalyst 8000 Series Secure Routers.

How Secure Router NGFW works

Summary

These stages describe how Secure Router NGFW inspects a flow:

Workflow

1. Classify: A Cisco Catalyst SD-WAN zone-based firewall rule matches the traffic and selects an Advanced Inspection Policy.
2. Redirect: The Cisco Catalyst 8000 Series Secure Router diverts the selected flow from the data plane to the running Secure Router NGFW container.
3. Inspect: The Advanced Inspection Policy is applied according to how the flow was classified. The Secure Router NGFW inspection engine evaluates the flow using the applicable threat profile, enabled services, and Snort, LSP, and VDB content.
4. Reinject: Secure Router NGFW reinjects the inspected traffic into the data plane along with the inspection verdict.

5. Enforce: The device returns permitted traffic to the datapath or enforces the reject or block verdict.
6. Report: The Cisco Catalyst 8000 Series Secure Router and Secure Router NGFW generate the applicable events, statistics, syslogs, notifications, and SD-WAN Manager telemetry.

How V1 and V2 policy intent is applied

1. Create or reuse the threat-inspection profile and Advanced Inspection Policy intent.
2. Select V1 Engine or V2 Engine for each supported device. One device cannot run both security applications.
3. Configure engine-specific content and settings. V1 uses the UTD signature-package workflow; V2 uses LSP and VDB.
4. Deploy the policy. SD-WAN Manager checks device capability, image availability, and content dependencies before it generates the device configuration.
5. When you migrate from V1 Engine to V2 Engine, review the supported V1-to-V2 configuration conversion. The migration can convert signature schedules and custom-signature configuration, but it does not perform a general in-place container migration.
6. Confirm that the selected container is running and that its configuration and content state are synchronized.

For migration conditions and exclusions, see Migrate NGFW V1 Engine settings to NGFW V2 Engine settings.

Prerequisites

Before you configure Secure Router NGFW, meet these prerequisites:

1. Add the required Secure Router NGFW virtual image to the Cisco Catalyst SD-WAN Manager software repository.
2. From the V2 tab of **Administration** > **Settings** > **Snort Subscriber Signature Package**, enable LSP and VDB updates and configure Cisco cloud, a remote server, or a local upload as the content source.
3. After the compatible Secure Router NGFW image, LSP, and VDB are available, select V2 Engine in the policy for the target device.
4. To use the deeper EVE analytics dashboard and process/threat-confidence visualizations, onboard the analytics service and meet its licensing requirements.
5. Use valid Snort syntax in custom-signature files. Validate custom rules before deployment. Invalid rules are disabled before the configuration is passed to Secure Router NGFW.
6. For online LSP and VDB download, enable Cloud Services and ensure that every SD-WAN Manager node can reach id.cisco.com and ssp.sdwan.cisco.com. A proxy is supported where required. If Cloud Services and the V1 Engine Cisco.com source are enabled before the SD-WAN Manager upgrade, the upgrade enables the V2 online content settings automatically. If Cloud Services is enabled only after the upgrade, enable the V2 settings manually.

For remote-server or offline deployments, open the V2 tab of **Administration** > **Settings** > **Snort Subscriber Signature Package**, configure the LSP and VDB source separately, and ensure that the server contains packages compatible with the running Secure Router NGFW and Snort versions. A policy can deploy without current V2 content, but signatures and enrichment data will not be updated.

Restrictions

The following restrictions apply to Secure Router NGFW:

1. A device can run only one security application container. UTD and Secure Router NGFW cannot coexist on the same device.
2. The Secure Router NGFW image and Cisco Catalyst IOS XE SD-WAN software image must be a supported combination. After upgrading the device software, use the compatible Secure Router NGFW image.
3. Secure Router NGFW supports the low, medium, and high resource profiles. The UTD-specific cloud and on-box resource-profile variants are not used for Secure Router NGFW.
4. Secure Router NGFW does not include URL filtering or file inspection in 26.2 release.
5. EVE operates globally in 26.2.1 release, not independently per firewall rule.
6. The Now update workflow does not support a remote-server content source. Configure a scheduled update to deliver LSP or VDB packages from a remote server..
7. Snort ML support is limited to HTTP request-header inspection for SQL-injection patterns and to security or max-detect threat policies.

Configure Secure Router NGFW

Use Cisco Catalyst SD-WAN Manager for centralized image staging, V2 policy selection, deployment, content updates, and monitoring. Use autonomous CLI configuration when the device operates without SD-WAN Manager orchestration. Both paths configure the same inspection functions, but the workflows and custom-signature capabilities differ.

Install Secure Router NGFW using Cisco Catalyst SD-WAN Manager

Before you begin

1. Meet the platform, version, resource, access, and repository prerequisites.
2. Decide whether the device uses V1 Engine or V2 Engine. The two containers cannot coexist on the device.
3. Obtain a Secure Router NGFW image that matches the target architecture and Cisco Catalyst IOS XE SD-WAN software release.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software** > **Repository** > **Virtual Images**.

Step 2 Click **Add New Virtual Image**.

Step 3
a) **Choose Remote Server (Preferred).**
b) In **Image File Name**, enter the image filename, including its extension.
c) Optionally, enter an Image description and select one or more values in Add Tags.

d) For **Select service type**, choose **App-Hosting**, and for **Select app type**, choose **Next-Generation Firewall**.
e) In **Enter version**, enter the image version, and for **Select architecture**, choose x86_64.
f) In the Remote Server section, choose the configured server from Remote server name.
g) Optionally, enter the path in Image File Path. To add another server, click Add Remote Server and complete the additional remote-server entry.

Step 4 Stage the required LSP and VDB content before deployment. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Snort Subscriber Signature Package**, select the V2 tab, enable the required packages, select **Now** or **Schedule**, and save the settings.

Step 5 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**, and create or edit the Policy Group for the target device.

Step 6 Create or edit the NGFW policy, select the required Advanced Inspection Profile, and open **Additional Settings**.

Step 7 Under **Security App Hosting**, select **V2 Engine** for **Security Software** and select the required resource profile.

Step 8 Save the policy, preview the generated configuration, and verify that the app-hosting configuration uses the ngfw application ID and the intended resource profile.

Step 9 Deploy the Policy Group and monitor the task until Cisco SD-WAN Manager reports **Success**.

Step 10 In **Maintenance** > **Software Upgrade** > **WAN Edge**, open **Available Services** for the device and confirm that Secure Router NGFW is running. In Cisco SD-WAN Manager, use the NGFW Engine Status and NGFW Version Status real-time operation views to verify the running state and version.

The Policy Group deployment installs and starts Secure Router NGFW on the target Cisco Catalyst 8000 Series Secure Router and applies the inspection configuration. If content updates are enabled, Cisco SD-WAN Manager also starts the applicable LSP and VDB update tasks.

Configure IPS or IDS using Cisco Catalyst SD-WAN Manager

Before you begin

1. Stage a compatible LSP for the Snort version in the Secure Router NGFW image.
2. Enable the V2 engine settings in **Administration** > **Settings** > **Snort Subscriber Signature Package**.

Procedure

Step 1 From the Cisco Catalyst SD-WAN Manager menu, choose **Configuration** > **Policy Groups and open Objects & Profiles**.

Step 2 Create or edit an **Intrusion Prevention Profile**.

Step 3 Enter the profile name and select the required **Signature Set**.

Step 4 For **Inspection Mode**, select **Prevention** for IPS behavior or **Detection** for IDS behavior. Select the required Alerts Log Level, and save the profile.

Step 5 Create or edit an **Advanced Inspection Profile**, select the intrusion-prevention profile, and save the profile.

Step 6 Return to the Policy Group, create or edit the NGFW policy, and configure a firewall rule with the **Inspect** action.

Step 7 Select the Advanced Inspection Profile at the firewall-rule level or in the policy-level **Additional Settings**, according to the required traffic scope.

Step 8 In **Additional Settings** > **Security App Hosting**, select **V2 Engine** for **Security Software**. Confirm that the required LSP is enabled if Cisco Catalyst SD-WAN Manager displays a package warning.

Step 9 Save the policy, preview the generated configuration, and confirm that the Advanced Inspection Profile references the intended intrusion-prevention profile and that the app-hosting application ID is **`ngfw`**.

Step 10 Deploy the Policy Group and monitor the task until Cisco SD-WAN Manager reports Success.

The Cisco Catalyst SD-WAN zone-based firewall redirects matching traffic to Secure Router NGFW. IDS allows matching traffic and generates an event; IPS enforces the Snort verdict and generates an event.

Configure EVE using Cisco Catalyst SD-WAN Manager

Before you begin

1. Stage a compatible VDB.
2. Decide whether EVE should monitor traffic or protect the device from High or Very High threat-confidence flows.
3. Create the required EVE exception rules and exception list if protect mode must allow specific processes or IPv4/IPv6 source or destination prefixes.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** open **Objects & Profiles**.

Step 2 If required, create an E**VE Exception List**, add one or more **EVE Exception Rules**, and define the process name and supported IPv4 or IPv6 source or destination match criteria.

Step 3 Return to the Policy Group, create or edit the NGFW policy, and open **Additional Settings**.

Step 4 Under **Security App Hosting**, select **V2 Engine** for **Security Software**.

Step 5 Under **Security Profile**, enable **Encrypted Visibility Engine**.

Step 6 Select **Monitor** to identify client processes and report encrypted-flow information without blocking traffic, or select **Protect** to enforce the configured threat-confidence threshold.

Step 7 If you select **Protect**, select **High** or **Very High** as the blocking threshold and select the EVE exception list when required.

Step 8 To generate connection-event data, enable **Unified Logging** in the policy additional settings and enable **Log Events** on each inspected firewall rule for which flow logs are required.

Step 9 Save the policy, preview the generated configuration, and confirm the EVE mode, threshold, exception-list reference, V2 engine selection, and logging configuration.

Step 10 Deploy the Policy Group and monitor the task until Cisco SD-WAN Manager reports **Success**.

EVE globally evaluates selected encrypted flows without decrypting the application payload. Monitor mode adds process and threat-confidence information to connection events. Protect mode blocks flows at the configured threshold unless an exception rule allows the flow.

Configure Snort ML using Cisco Catalyst SD-WAN Manager

Before you begin

1. Use a security or max-detect threat policy.
2. Stage a compatible LSP and select V2 Engine for the target device.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** and open **Objects & Profiles**.

Step 2 Create or edit an **Intrusion Prevention Profile**.

Step 3 Select **Prevention** as the inspection mode, select **Security** or **Max Detect** as the signature set, configure the alert logging level, and save the profile.

Step 4 Create or edit an **Advanced Inspection Profile**, select the intrusion-prevention profile, and save the profile.

Step 5 Return to the Policy Group, edit the NGFW policy, attach the Advanced Inspection Profile to the traffic that requires inspection, and open **Additional Settings**.

Step 6 Under **Security App Hosting**, select **V2 Engine** for **Security Software**.

Step 7 Under **Security** Profile, enable **Snort ML**.

Step 8 Save the policy, preview the generated configuration, and confirm the V2 engine selection, Snort ML enablement, threat profile, and Advanced Inspection Profile references.

Step 9 Deploy the Policy Group and monitor the task until Cisco SD-WAN Manager reports Success.

The Snort ML module examines supported HTTP request-header traffic and can generate an intrusion event for a detected SQL-injection pattern.

Migrate V1 Engine settings to V2 Engine settings

Before you begin

1. Add a compatible Secure Router NGFW image to **Maintenance** > **Software Repository** > **Virtual Images**.
2. Ensure that a compatible LSP is available in Cisco SD-WAN Manager. Policy migration cannot continue if the required LSP is unavailable.
3. Review the V1 content source and Cloud Services state before upgrading SD-WAN Manager. When V1 uses Cisco.com and Cloud Services is already enabled, the upgrade enables V2 online LSP/VDB settings. If Cloud Services is enabled after the upgrade, enable the V2 settings manually. Remote-server and local-file deployments require a separate V2 source.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** and select the Policy Group that currently uses V1 Engine.

Step 2 Start the available V1-to-V2 migration action for the Policy Group.

Step 3 Review the affected intrusion-prevention profiles and the precheck results. Resolve a missing-LSP or unsupported-profile error before continuing.

Step 4 Review the proposed conversion of supported V1 profile settings to V2 settings. The migration does not change the Advanced Inspection Profiles themselves.

Step 5 Review content-setting conversion. For Cisco.com with Cloud Services enabled, confirm that LSP and VDB are enabled. For a remote-server or local-file V1 source, configure the V2 LSP and VDB settings separately.

Step 6 Review the migrated editable signature set and its IPS-profile association. The migration converts a supported V1 IPS signature list to a custom editable signature set. Review any global custom-signature settings and associated remote or local files separately, and configure the required V2 online access because legacy Cisco.com credentials are not migrated.

Step 7 Review the converted update schedule.

Step 8 Confirm the migration and wait for Cisco SD-WAN Manager to report that the policy profiles were migrated successfully.

Step 9 Preview the Policy Group configuration, select **V2 Engine** (Secure Router NGFW) for the applicable devices, and deploy the Policy Group.

Step 10 Monitor the deployment while Cisco SD-WAN Manager removes UTD, installs Secure Router NGFW, applies the V2 configuration, and verifies the container state. If installation fails, confirm that the configuration rolls back and UTD is restored.

The selected Policy Group uses the migrated V2 policy intent and deploys Secure Router NGFW. Switching the container type is a Policy Group deployment operation; **Virtual Image Actions** > **Upgrade Virtual Image** cannot switch a device directly from UTD to Secure Router NGFW.

Upgrade the Secure Router NGFW container using Cisco Catalyst SD-WAN Manager

Before you begin

1. Add a compatible Secure Router NGFW image to **Maintenance** > **Software Repository** > **Virtual Images**.
2. Confirm that the device already runs V2 Engine. The virtual-image upgrade workflow does not migrate V1 Engine to V2 Engine.

Procedure

Step 1 From the Cisco Catalyst SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** > **WAN Edge**.

Step 2 Select the device and choose **Virtual Image Actions** > **Upgrade Virtual Image**.

Step 3 Select the compatible Secure Router NGFW image and version, start the upgrade, and wait until SD-WAN Manager reports Success.

Step 4 Confirm that the image version is downloaded and available for activation.

Step 5 Choose Activate Virtual Image and wait until SD-WAN Manager reports Success.

Step 6 Use Available Services and the NGFW Engine Status and NGFW Version Status real-time operation views to verify that the expected Secure Router NGFW version is running.

The selected Cisco Catalyst 8000 Series Secure Router runs the activated Secure Router NGFW image version.

The app-hosting upgrade command is not supported for Secure Router NGFW.

Delete a Secure Router NGFW image from a device

Procedure

	Command or Action	Purpose
Step 1	From the Cisco Catalyst SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** > **WAN Edge**.	
Step 2	Select the target device and choose **Virtual Image Actions** > **Delete Virtual Image**.	
Step 3	Select the downloaded Secure Router NGFW image version and confirm the deletion.	
Step 4	Monitor the task until Cisco Catalyst SD-WAN Manager reports Success.	
Step 5	Verify that the downloaded version is no longer available on the device. The running Secure Router NGFW container is not uninstalled by this operation.	

Uninstall the Secure Router NGFW container

Procedure

Step 1 From the Cisco Catalyst SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.

Step 2 Edit the Policy Group attached to the target device.

Step 3 Remove the intrusion-prevention profile or NGFW policy configuration that causes the Policy Group to install the Secure Router NGFW application.

Step 4 Preview the generated configuration and confirm that the Secure Router NGFW app-hosting configuration is removed.

Step 5 Deploy the Policy Group and monitor the task until SD-WAN Manager reports Success.

Step 6 In **Maintenance** > **Software Upgrade** > **WAN Edge**, open Available Services for the device and verify that Secure Router NGFW is absent. In SD-WAN Manager, use the NGFW Engine Status and NGFW Version Status real-time operation views to confirm that the Secure Router NGFW service and version are no longer reported for the device.

Deleting a repository image or a downloaded device image does not uninstall the running container. **Reload Services** restarts a service, and **Reset Services** reinstalls a service; neither operation is the Policy Group uninstall workflow.

What to do next

For SD-WAN Manager monitoring workflows, see Monitor Secure Router NGFW using SD-WAN Manager.

Configure Secure Router NGFW using the CLI

Before you begin

1. Obtain privileged access to a supported Cisco Catalyst 8000 Series Secure Router.
2. Install and activate a compatible Secure Router NGFW image.
3. Configure the required service-plane resources.
4. Make compatible LSP and VDB packages available through the autonomous update source.

Procedure

Configure the platform for the service-plane-heavy resource allocation.

```
Device(config)# platform resource service-plane-heavy
```

Configure IPS or IDS using the CLI

Procedure

Step 1 Create the threat-inspection profile.

```
Device(config)# threat-inspection profile <profile-name>
```

Step 2 Select prevention for IPS behavior or detection for IDS behavior, select the Talos policy posture, and configure the logging level.

```
Device(config-profile)# threat { prevention | detection }
Device(config-profile)# policy { connectivity | balanced | security | max-detect | no-rules-active
}
Device(config-profile)# logging level { alert | crit | debug | emerg | err | info | notice | warning
 }
```

Step 3 If required, attach a validated profile-specific custom-signature group.

```
Device(config-profile)# custom-signature profile <custom-profile-name>
```

Step 4 Create the Advanced Inspection Policy and attach the threat-inspection profile.

```
Device(config)# policy <aip-name>
Device(config-policy)# threat-inspection profile <profile-name>
```

Step 5 Attach the Advanced Inspection Policy to the unified security firewall inspection path that selects the required traffic.

Step 6 Confirm that the running configuration contains the firewall policy, Advanced Inspection Policy, threat-inspection profile, and Secure Router NGFW application configuration.

```
Device# show running-config | section ngfw
Device# show ngfw engine config
```

Configure EVE using the CLI

Procedure

Step 1 Enter the Secure Router NGFW global encrypted-visibility configuration mode.

```
Device(config)# ngfw global
Device(config-ngfw)# encrypted-visibility
```

Step 2 Select monitor or protect mode.

```
Device(config-encrypted-visibility)# policy-mode { monitor | protect }
```

Step 3 For protect mode, select the blocking threshold and attach an exception list when required.

```
Device(config-encrypted-visibility)# block-threat-confidence-level { very-high | high }
Device(config-encrypted-visibility)# block-exempt-rule-list <exception-list-name>
```

Step 4 Create the exception list and add the required process and address match criteria.

```
Device(config)# encrypted-visibility exempt-rule-list <exception-list-name>
Device(config-exception-list)# exempt-rule <rule-name>
Device(config-exception-rule)# process-name <process-name>
Device(config-exception-rule)# source-ipv4 prefix <ipv4-prefix>
Device(config-exception-rule)# destination-ipv4 prefix <ipv4-prefix>
```

Step 5 If connection-event monitoring is required, enable unified logging and flow-event logging for the inspected traffic.

Step 6 Confirm that the running configuration and Secure Router NGFW engine configuration show the same EVE mode, threshold, and exception-list reference.

```
Device# show running-config | section ngfw
Device# show ngfw engine config
```

The source model also includes IPv4/IPv6 object-group and IPv6 prefix variants.

Configure Snort ML using the CLI

Procedure

Step 1 Enable Snort ML globally.

```
Device(config)# ngfw global
Device(config-ngfw)# threat-inspection snort-ml
```

Step 2 Create a prevention profile that uses the security or max-detect posture and configure the logging level.

```
Device(config)# threat-inspection profile <profile-name>
Device(config-profile)# threat prevention
Device(config-profile)# policy { security | max-detect }
Device(config-profile)# logging level err
```

Step 3 Create or reuse an Advanced Inspection Policy, attach the threat-inspection profile, and attach that policy to the unified security firewall inspection path.

Step 4 Confirm the global Snort ML enablement and active threat profile in the running and engine configurations.

```
Device# show running-config | section ngfw
Device# show ngfw engine config
Device# show ngfw engine statistics internal
```

What to do next

Verify the running container, content versions, configuration synchronization, and traffic verdict.

Update LSP and VDB packages

LSP and VDB updates are a separate workflow from policy deployment and container-image upgrade.

1. **LSP** contains Talos Snort rules, rule groups, base policies, and related metadata. LSP compatibility depends on the Snort version in the Secure Router NGFW image.
2. **VDB** supplies fingerprint and dynamic metadata used by EVE and related inspection or event functions. The SD-WAN Manager design uses one current VDB independent of the Snort version.

Configure Cisco Catalyst SD-WAN Manager update timing

Procedure

Step 1 From the Cisco Catalyst SD-WAN Manager menu, choose **Administration** > **Settings** > **Snort Subscriber Signature Package**, and select **V2 engine**.

Step 2 Enable LSP, VDB, or both and select Cisco cloud, local upload, or remote server as supported by the timing option.

Step 3 Select **Now** for eligible local or Cisco-cloud content. SD-WAN Manager stages the content and sends newer eligible packages to running V2 devices.

Step 4 Select **Schedule** for periodic deployment. Configure an interval from 2 through 24 hours, a daily time, or a weekly day and time. If you select **Site Time**, SD-WAN Manager starts the update for devices in each site at the configured local time for that site. If you select **Manager Time**, all sites receive the update at the configured SD-WAN Manager time. You can also select another supported time zone.

Step 5 Save the settings and verify the package rows, source, version, and update task.

Verify Secure Router NGFW

Objective

Use these checks and commands to confirm that Secure Router NGFW and its configured inspection functions operate as intended.

Before you begin

1. Deploy the container, policy, and content settings.
2. Allow the Secure Router NGFW control and inspection processes, Snort process, and content installation to reach their operational states.
3. Prepare an approved benign IPS test signature or EICAR-style trigger and an authorized EVE test flow.

Verify the container and configuration

1. Cisco Catalyst SD-WAN Manager, confirm that the deployment task reports the expected image, policy, and package results.
2. Confirm the app-hosting state and resource allocation.

```
Device# show app-hosting detail appid ngfw
Device# show app-hosting resource
```

3. Confirm the Secure Router NGFW version, engine status, configuration synchronization, and content state.

```
Device# show ngfw version
Device# show ngfw engine status
Device# show ngfw engine config
Device# show ngfw engine status update
```

Verify IPS and IDS

1. Generate the approved IPS/IDS test traffic.
2. Correlate the Cisco Catalyst SD-WAN zone-based firewall rule, Advanced Inspection Policy, threat signature, connection identifier, event, and verdict.
3. Verify that IDS permits the test flow and produces an intrusion event.
4. Verify that IPS rejects or blocks the test flow and produces an intrusion event.
5. Review the applicable events and statistics.

```
Device# show ngfw engine events
Device# show ngfw engine statistics
```

Verify EVE

1. Generate an authorized encrypted test flow.
2. Confirm that the connection event contains the expected process name, process confidence, threat-confidence level, and threat score.
3. In monitor mode, verify that EVE reports the flow without blocking it.
4. In protect mode, verify the expected block or exception-allow behavior.
5. Confirm that the Mercury counters increase.

```
Device# show ngfw engine config
Device# show ngfw engine statistics internal
```

Verify Snort ML

1. Generate only the implementation-owner-approved HTTP test traffic in a controlled lab.
2. Confirm that the snort_ml and snort_ml_engine counters increase.
3. Confirm that Secure Router NGFW generates the expected Snort ML intrusion event.

```
Device# show ngfw engine statistics internal
Device# show ngfw engine events
```

Verify LSP and VDB

1. Confirm the installed LSP and VDB versions and operational state.

```
Device# show ngfw engine status update type lsp
Device# show ngfw engine status update type vdb
Device# show ngfw operational update lsp
Device# show ngfw operational update vdb
```

2. Confirm that the LSP is compatible with the Snort version in the running Secure Router NGFW image.

Result

Successful verification shows that the container and inspection processes are operational, the Cisco Catalyst 8000 Series Secure Router and Secure Router NGFW use synchronized configuration, compatible LSP/VDB content is active, and approved traffic produces the expected IDS, IPS, EVE, or Snort ML evidence.

Monitor Secure Router NGFW using Cisco Catalyst SD-WAN Manager

Objective

Use these monitoring checks to review Secure Router NGFW status, events, security functions, and content updates in Cisco Catalyst SD-WAN Manager.

Monitor the Secure Router NGFW container

1. In Cisco SD-WAN Manager, open the monitoring page for the target device.
2. Open the NGFW Engine Status real-time operation view.
3. Verify that the Secure Router NGFW engine and its control, inspection, and Snort processes are operational.
4. Open the NGFW Version Status real-time operation view.
5. Verify the running Secure Router NGFW version and configuration-synchronization status.

Monitor IPS and IDS

1. Open the Security dashboard and review the firewall-rule counter and intrusion-prevention widgets.
2. Open Device360 and review the Firewall and Intrusion Prevention pages for the target device.

3. Review intrusion events for the signature GID:SID, severity, action, policy, five-tuple, and connection identifier.
4. Correlate the event with the Cisco Catalyst SD-WAN zone-based firewall rule, Advanced Inspection Policy, threat profile, and final IDS or IPS verdict.
5. Confirm that IDS allows and reports the flow and that IPS rejects or blocks and reports the flow, as intended.

For port-scan monitoring, review the configured sensitivity, scan type, protocol, source and destination information, alerts, and scan counters.

Monitor EVE

1. Enable Unified Logging and rule-level Log Events for inspected traffic, then open Connection Events in SD-WAN Manager. EVE data is added to the connection-end event; connection-start and connection-end logging must be available for the selected flow.
2. Review the process name, process confidence, threat-confidence level, threat score, action, and exception result for the selected flow.
3. Confirm that EVE monitor mode enriches the event without blocking the flow.
4. Confirm that EVE protect mode blocks a High or Very High threat-confidence flow unless an exception rule allows it.

On the Security dashboard, review Encrypted Visibility Engine Processes and Encrypted Visibility Threat Confidence. Filter by site and time range, and use the dashboard link to open Traffic Logs with the process, device, site, and time context prefilled.

The absence of EVE dashboard data does not prove that EVE is disabled. EVE processing is global, while unified logging, event filtering, export, and SD-WAN Manager ingestion use separate controls.

Monitor Snort ML

1. Open the Security dashboard or the Device360 Intrusion Prevention page for the target device.
2. Review the Snort ML intrusion event and confirm the expected GID:SID, policy, action or result, device, and connection details.

Monitor LSP and VDB updates

Use the **NGFW LSP Update Status** and **NGFW VDB Update Status** real-time operation views in SD-WAN Manager.

Confirm the content version, source, installation date, hash where available, and last-update result.

Monitor Secure Router NGFW using the CLI

Objective

Use these commands and checks to review Secure Router NGFW status, events, counters, and content updates from the CLI.

Monitor the Secure Router NGFW container using the CLI

Use the following commands to verify the container, resource allocation, running version, configuration, process state, and utilization.

```
Device# show app-hosting detail appid ngfw
Device# show app-hosting resource
Device# show ngfw version
Device# show ngfw engine config
Device# show ngfw engine status
Device# show ngfw engine utilization
Device# show ngfw operational engine
```

Monitor IPS and IDS using the CLI

Use the following commands to review intrusion events and engine and DAQ counters.

```
Device# show ngfw engine events
Device# show ngfw engine statistics
Device# show ngfw engine statistics daq
```

Monitor EVE using the CLI

1. Review the Mercury counters in the internal engine statistics and confirm that the applicable packet, fingerprint, and threat counters increase.

   ```
   Device# show running-config | section ngfw
   Device# show ngfw engine config
   Device# show ngfw engine statistics internal
   ```

Monitor Snort ML using the CLI

1. Generate only the implementation-owner-approved HTTP test traffic in a controlled lab.
2. Review snort_ml and snort_ml_engine counters in the internal engine statistics.
3. Confirm that uri_alerts, uri_bytes, or the applicable ML-engine counters increase.
4. Review the intrusion event and confirm the expected Snort ML GID:SID, policy, result, and connection details.

   ```
   Device# show ngfw engine statistics internal
   Device# show ngfw engine events
   ```

Monitor LSP and VDB updates using the CLI

Use the following commands to verify LSP and VDB update state and operational status.

```
Device# show ngfw engine status update
Device# show ngfw engine status update type lsp
Device# show ngfw engine status update type vdb
Device# show ngfw operational update lsp
Device# show ngfw operational update vdb
```