Secure NX-OS with Cisco Live Protect

This chapter provides information about the Cisco Live Protect feature that secures NX-OS when NXSecure configuration is enabled. This chapter covers:

Cisco Live Protect

Cisco Live Protect is a security feature that

- protects the control plane of the Cisco network devices,
- requires enabling NXSecure configuration on NX-OS devices, and
- provides comprehensive security observability with real-time security event detection and analysis.

The Cisco NX-OS Release 10.6(1)F introduces the Cisco Live Protect feature to secure NX-OS and provide enhanced security and software integrity assurance for the NX-OS device control plane. Only the monitoring mode is supported in this release.

NXSecure: NXSecure is a security configuration tool for Nexus switches. It protects the control plane from security vulnerabilities. NXSecure uses a technology called extended Berkeley Packet Filter (eBPF) internally to track, detect, and report security events in real time. NXSecure also monitors files, tracks processes, and traces system calls.

Tracing policies: The Cisco Live Protect feature uses tracing policies to provide security observability. These policies are packaged with the NX-OS image.

Monitoring mode: Based on the configured policies, the monitoring mode allows the system to detect and generate log files for each anomaly event.

Event logs: Event logs are generated in the monitoring mode. You can export the event logs using telemetry, if you have configured the correct sensor path for NXSecure.

Guidelines and limitations for Cisco Live Protect

When using Cisco Live Protect, always verify that your platform and features are supported in your software release. Follow these guidelines and limitations to ensure compatibility and avoid unsupported deployments:

- **Platform support**—Starting from Cisco NX-OS Release 10.6(1)F, this feature is
  - supported on Cisco Nexus 9300-FX, -FX2, -FX3, -GX, -GX2, -H1, and -H2R switches with at least 24G RAM.
  - not supported on SiliconOne switches, including Nexus 9800 and N9324C-SE1U.
- **Compatibility with other features**—This feature is not supported with application hosting or AuditD features.

Enable the NXSecure feature for Cisco Live Protect

Follow this step to enable the NXSecure feature:

Procedure

Use the **feature nxsecure** command to enable the NXSecure feature.

Example:

```
switch(config)# feature nxsecure
```

Use the **no** form of this command to disable the NXSecure feature.

The NXSecure feature is enabled; dockerd and NXSecure containers are started.

Verify NXSecure configuration for Cisco Live Protect

To verify the status of the NXSecure configuration for the Cisco Live Protect feature, use the following show commands:

Command	Purpose
show nxsecure status	Displays the status of NXSecure
show nxsecure logfiles	Displays the current set of generated log files
show tech-support nxsecure	Displays debug logs for NXSecure
show telemetry transport sessions	Loops through the telemetry transport sessions and displays information about such sessions

Sample outputs for the verification commands

The sample outputs for the listed show commands are included here for your reference.

- **show nxsecure status**

```
switch# show nxsecure status
Tetragon Agent Status: Running
```

- **show nxsecure logfiles**

```
switch# show nxsecure logfiles
tetragon-2025-03-17T22-17-32.948.log
tetragon-2025-03-17T22-21-59.194.log
tetragon-2025-03-17T22-25-58.694.log
tetragon.log
```

- **show telemetry transport sessions**

```
switch# show telemetry transport sessions
Session Id: 0
Dst Grp Id: 1000
IP Address:Port <ip address>
Transport: EVTLOG
Status: Connected
Last Connected: Tue Jun 24 14:33:32.577 IST
Last Disconnected: Tue Jun 24 14:33:32.570 IST
Tx Error Count: 0
Last Tx Error: None
```

Event logs

An event log is a log file that is

- generated in NXSecure monitoring mode for each security anomaly,
- formatted in JSON, and
- exported using telemetry.

JSON log files: NXSecure generates JSON events and alerts received from kernel programs into log files as plain JSON data. The system is configured to generate up to a maximum of 5 JSON event files. Each file has a size limit of 3MB or a time limit of 120 seconds, whichever occurs first.

Export log files using telemetry: Telemetry transport is used to export the NXSecure log files to a remote HTTPS server. This is possible only when the **path event-nxsecure** sensor type is configured.

Configure telemetry path sensor type

When configuring telemetry, path sensor type is configured. In addition to the existing path sensor types such as event-history and event-monitor, the NX-OS Release 10.6(1)F introduces a new telemetry path sensor type, event-nxsecure. This sensor type is used to export the log files to external receivers. To configure the new **path event-nxsecure** sensor type, use the sample configuration.

For more information about configuring the path sensor type, refer to the *Telemetry* chapter in the appropriate version of the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Sample configuration

```
switch(config)# telemetry
switch(config-telemetry)# certificate /bootflash/server.pem <ip address>
switch(config-telemetry)# destination-group 1
switch(conf-tm-dest)# ip address <ip address> port 8083 protocol HTTP encoding Form-data
switch(conf-tm-dest)# sensor-group 1
switch(conf-tm-sensor)# path event-nxsecure
switch(conf-tm-sensor)# data-source native
switch(conf-tm-sensor)# subscription 1
switch(conf-tm-sub)# dst-grp 1
switch(conf-tm-sub)# snsr-grp 1 sample-interval 0
```