Secure NX-OS with Live Protect

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

Live Protect

Live Protect is a security feature that

- provides real-time, kernel-level security using eBPF technology through the Tetragon agent embedded in NX-OS,
- enables Common Vulnerabilities and Exposures (CVE) compensating controls and zero-day attack mitigation without software upgrades or reboots, and
- uses NXSecure to manage and activate the feature, configuring Tetragon for monitoring, detection, and logging of security events for enhanced threat visibility and telemetry integration.

While managing data center network infrastructure, security and uptime are non-negotiable. Patch updates for CVEs lead to operational disruptions and unacceptable downtime for critical systems. With Live Protect feature, you can address emerging vulnerabilities immediately by deploying real-time shields that mitigate CVE exploitation. This proactive approach eliminates the need for disruptive patching, emergency maintenance, or urgent code upgrades in your data center. Thus, the Live Protect feature allows you to maintain continuous protection and operational stability.

Note

- The CVEs for which the Live Protect feature provides compensating controls are qualified by beginning with Release 10.6(2)F and future releases post this release.
- When PSIRT identifies a high-profile Threat Protection System (TPS) vulnerability, they notify affected OS teams and publish an advisory. The OS team confirms impact, then collaborates with PSIRT and Tetragon to create and test a shield. Tetragon team checks for the impact and feasibility of providing the mitigation for the CVE. After successful testing, PSIRT updates the security advisory, and the OS team provides the shield to customers.
- For more information, refer to the *Field Advisory Notices for CVEs* .

Key concepts of Live Protect

The Live Protect feature secures NX-OS and provides enhanced security and software integrity assurance for the NX-OS device control plane. A few key concepts of this feature are:

- Extended Berkeley Packet Filter – Also abbreviated as eBPF, is a powerful Linux kernel technology that enables programmable, safe, and efficient kernel extensions for networking, security, and observability, forming the foundation for advanced security and networking features.
- Tetragon – This is an agent developed by Isovalent and embedded in NX-OS. It compiles CVE compensating controls into eBPF policies that run in the kernel, enabling advanced monitoring and enforcement of security policies in real time. It provides protection and security through the Live Protect feature.
- NXSecure – This is the NX-OS security configuration tool that activates and manages Live Protect. When enabled, NXSecure starts the Tetragon agent and related containers on the switch. NXSecure uses eBPF internally to track, detect, and report security events such as file, process, and system call anomalies.

  NXSecure configures and controls the Tetragon agent's operation, which continuously monitors the system for security threats and generates event logs.
- Tracing policies – The Live Protect feature uses tracing policies to provide security observability. These policies are packaged with the NX-OS image.
- Modes – The two modes in Live Protect are:
  - Monitoring mode – Based on the configured policies, the monitoring mode allows the system to detect and generate log files for each anomaly event. Beginning with Release 10.6(1)F, monitoring mode is supported.

    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.
  - Enforce mode – Beginning with Release 10.6(2)F, enforce mode is supported. In enforce mode, Live Protect actively blocks or mitigates detected threats in real time. This mode provides proactive protection by enforcing security policies that prevent exploitation of vulnerabilities such as privilege escalation and control-plane DDoS attacks. Enforcement happens at the kernel level, allowing immediate mitigation without requiring software upgrades, reboots, or downtime.

    The enforce mode uses NXSecure embedded in NX-OS to apply the kernel-level security shields. This enables continuous protection of Nexus 9000 series switches against emerging Common Vulnerabilities and Exposures (CVEs) while maintaining operational stability and uptime.

- Add-on policy packages – This allows you to install additional live protect policies when such policies are available for the current running software version on the switch. Live protect policies would be released either for enforce or monitor mode. Additional commands are available to change the mode between enforce and monitor. You can disable the mode temporarily using a few commands mentioned in Modify the policy mode section. To add or remove Live Protect Policy packages, see Add or remove Live Protect policy packages, on page 6.

Note We recommend to install policies in monitoring mode (default mode) for a short duration and observe the effectiveness of the policy. The show nxsecure policy status command provides the hit counts, which can be used to identify if there are any conflicts with the regular switch functions. If there are no hit counts observed during the normal switch function, the policy can be changed to enforce mode.

In the show output the header tags displayed are `Id`, `Name`, `Package`, `Original`, `Override`, `Current`, and `Hits`. However, in the XML output of the command, the `Original` header tag gets replaced with `Policy` tag.

```
switch# show nxsecure policy status
Id      Name                Package                         Original
 Override   Current  Hits
lp00002 CVE-XXXX-20002-v1   lp00002.CVE-XXXX-20002-v1.lps   monitor
  none      monitor     2
lp00004 CVE-XXXX-20004-v1   lp00004.CVE-XXXX-20004-v1.lps   enforce
  monitor   monitor     0
```

Guidelines and limitations for Live Protect

When using 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

The table depicts the releases in which the Live Protect feature is supported on various Nexus switches.

Switches	Release	Note
Nexus 9300-FX, FX2, FX3, GX, GX2, H1, and H2R switches	10.6(1)F	Live Protect is su 24G RAM.
Nexus 9500-R and 9800 switches	NA	Live Protect is n
N9324C-SE1U and N9348Y2C6D-SE1U Smart Switches; Silicon One TORs such as N9336C-SE1, N9364E-SG2-Q, N9396T12C-SE1, and N9396Y12C-SE1 switches; N9K-C9408 Cloudscale switch	10.6(2)F **Note** N9324C-SE1U is not supported in 10.6(1)F	Live Protect is su 24G RAM.
N9164E-NS4-O switch	10.6(2n)	NA

Compatibility with other features

This feature is not supported with application hosting , dockerbox, configuration replace, or auditD features.

Impact on CPU

There is negligible impact on CPU.

Licensing

Beginning with Release 10.6(2)F, the Live Protect feature requires an NXOS_ESSENTIALS license.

Command usability

The command help string for nxsecure policy add or remove command works in Exec mode, but not in config mode.

Downgrade

If you have enabled the nxsecure feature and then downgrade from Release 10.6(2)F to 10.6(1)F, we recommend that you perform these commands after the downgrade:

1. **no feature nxsecure**
2. **feature app-hosting**
3. **no feature app-hosting**

Then, verify using the **show app-hosting details** command.

Release-specific information

- Beginning with NX-OS Release 10.6(1)F, only monitoring mode is supported.
- Beginning with NX-OS Release 10.6(2)F, enforce mode is also supported.

Enable the NXSecure feature for Live Protect

In NX-OS, Live Protect feature is implemented as feature nxsecure, so enable this feature on the switch.

Before you begin

- Ensure that you have a minimum of 2G of free space in bootflash before enabling nxsecure.

  Verify the free space using the **dir | include free** command.

```
switch# dir | include free
59822419968 bytes free
switch#
```

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, and NXSecure containers are brought up on the Apphosting Framework.

Verify NXSecure configuration for Live Protect

To verify the status of the NXSecure configuration for the Live Protect feature, use the required 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
```

Add or remove Live Protect policy packages

Use this procedure to add or remove new policy packages on the switch.

Procedure

Step 1 (Optional) Use the **nxsecure policy add** <*package*> command to add new policy package file to the switch.

Example:

Step 2 (Optional) Use the **nxsecure policy remove** <*package*> command to remove an existing policy package on the switch.

Example:

Step 3 (Optional) Use the **show nxsecure packages** command to verify the packages.

Example:

The chosen Live Protect policy package is added to or removed from the switch, and you can verify the current packages installed.

Verify policy status for Live Protect

To verify the status of the policies for the Live Protect feature, use the following show commands:

Command	Purpose
show nxsecure policy status	Displays the status of NXSecure policies

Modify the policy mode

You can disable, monitor, or enforce a policy at a granular level in executive mode. Note that you must define the monitor or enforce action for each policy.

Procedure

Step 1 To disable a particular policy that you enabled, promote a particular policy defined as monitor to enforce, or override a particular policy originally defined as enforce, use the **nxsecure policy-id <policy-id>** [**disable** | **enforce** | **monitor**] command.

Example:

```
switch# nxsecure policy-id lp000002 disable
```

- **disable**—disables the policy
- **enforce**—places the selected policy in enforce mode

- **monitor**—places the selected policy in monitor mode

Step 2 To verify the mode change, use the **show nxsecure policy status** command.

Example:

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.

Sample event log

Events related to enforced and monitoring policies can be viewed through the event logs. Here is a sample output.

```
{
  "event": {
    "process_exec": {
      "process": {
        "exec_id": "c3dpdGNoOjk1MjYyOTUwNjc2MDo5NjA0",
        "pid": 9604,
        "uid": 0,
        "cwd": "/bootflash/home/admin",
        "binary": "/usr/bin/tcpdump",
        "arguments": "-i eth0",
        "flags": "execve clone",
        "start_time": "2025-11-25T20:17:04.338471126Z",
        "auid": 2002,
        "parent_exec_id": "c3dpdGNoOjk0MzMwOTk1NzEwMDo4OTYw”,
  "parent": {
        "exec_id": "c3dpdGNoOjk0MzMwOTk1NzEwMDo4OTYw",
        "pid": 8960,
        "uid": 0,
        "cwd": "/bootflash/home/admin",
        "binary": "/bin/bash",
        "flags": "execve clone",
        "start_time": "2025-11-25T20:16:55.018922031Z",
        "auid": 2002,
        "parent_exec_id": "c3dpdGNoOjk0MzI5NzYyNjczMjo4OTU4",
}
```

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.

```
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
```