Revised: September 2, 2026

Security for Network Mode

Security features

This article outlines the supported security features, their functions, and associated limitations for the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches. The features cover access control, control-plane protection, traffic filtering, link security, security protocols, traffic storm control, and Live Protect. Use the related articles for configuration requirements and feature-specific limitations.

Security features are a collection of integrated tools, protocols, and policies designed to safeguard network systems and data by mitigating threats, preventing unauthorized access, and ensuring data integrity.

Security concepts and relationships

Security features protect the switch, its links, and the traffic that crosses supported interfaces. Select a control according to the asset being protected and the point where the traffic is evaluated.

Table 1: Security terminology

Term	Definition	Relationship
Control plane	The CPU-facing part of the switch that processes control and management traffic.	CoPP protects it by controlling traffic rates sent to the CPU.
IP ACL	An ordered set of permit and deny rules for IP traffic.	Evaluates packet fields at supported interfaces or routing boundaries.
MACsec	Layer 2 link encryption and integrity protection.	Protects traffic between adjacent devices on a supported Ethernet link.
DHCP relay	A service that forwards DHCP messages between subnets.	Connects clients to a trusted, remote address-allocation service.
Traffic storm control	A Layer 2 control that limits excessive broadcast, multicast, and unknown-unicast traffic.	Monitors traffic against a configured threshold and drops excess traffic to reduce flooding.
Live Protect	A kernel-level security feature that uses eBPF technology through the Tetragon agent.	Uses NXSecure to monitor security events and mitigate supported vulnerabilities.

Network security and access control protocols

Network security and access control protocols encompass a variety of mechanisms and technologies designed to regulate and secure access to network resources. Key protocols and concepts include:

Authentication, authorization, and accounting

Authentication, Authorization, and Accounting (AAA) is an architectural framework that uses protocols such as RADIUS and TACACS+ to manage user access and permissions in a modular and consistent manner.

Beginning with NX-OS Release 10.6(2)F, AAA is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information on AAA, refer to Configuring AAA.

- **Remote Authentication Dial-In User Service (RADIUS)** is a client/server protocol used within AAA to provide centralized authentication and authorization for network access.

  Beginning with NX-OS Release 10.6(2)F, RADIUS is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

  For more information on RADIUS, refer to Configuring RADIUS.

- **Terminal Access Controller Access-Control System Plus (TACACS+)** is a security protocol implemented through AAA that provides centralized validation of users, with separate and modular authentication, authorization, and accounting facilities.

  Beginning with NX-OS Release 10.6(2)F, TACACS+ is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

  For more information on TACACS+, refer to Configuring TACACS+.

Secure Shell

Secure Shell (SSH) is a protocol used to establish secure, encrypted connections to network devices, often used for secure remote management and access.

Beginning with NX-OS Release 10.6(2)F, SSH is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information on SSH, refer to Configuring SSH and Telnet.

IP Access Control List

An IP Access Control List (IP ACL) is an ordered set of rules that filters network traffic by specifying conditions based on IP packet information, such as source and destination IP addresses and protocol type, to determine whether a packet is permitted or denied.

Beginning with NX-OS Release 10.6(2)F, the smart switches support PACL, RACL on Layer 3 interfaces, Layer 3 port-channel interfaces, subinterfaces, and SVIs, and PBR ACL.

For information on IP ACLs, refer to Configure IP ACLs.

ACL limitations

- The **mac packet-classify** command is not supported.
- Each TCAM slice supports 7136 entries for RACL or PACL. The N9324C-SE1U and N9348Y2C6D-SE1U Smart switches have two slices.

ACL supported features

- PACL
- RACL on L3 interfaces, L3 Port-channel interfaces, subinterfaces, and SVI interfaces
- PBR ACL

DHCP relay

Dynamic Host Configuration Protocol (DHCP) relay is a feature that enhances network control by centralizing IP address allocation, which enables consistent policy enforcement and aids in the prevention of rogue DHCP servers by forwarding client requests exclusively to trusted, remote servers.

Beginning with NX-OS Release 10.6(2)F, DHCP relay is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For information on DHCP relay, refer to Configuring DHCP.

DHCP relay limitations

When a DHCP relay is configured on a switch and a RACL is also applied, the RACL will drop unicast DHCP relay traffic. This occurs because RACLs and other security policies have a higher priority in the processing order than control plane traffic, such as DHCP relay.

Control Plane Policing

Control Plane Policing (CoPP) is a security feature that protects a network device's control plane from Denial of Service (DoS) attacks by applying a policy map to limit the rate of traffic destined for the CPU, ensuring network stability and reachability.

A custom CoPP policy is an administrator-defined ruleset that tailors the protection of a device's control plane by classifying specific traffic types and applying unique rate limits to meet a network's particular security and operational requirements.

Beginning with NX-OS Release 10.6(2)F, custom CoPP is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For information on CoPP, refer to Configure Control Plane Policing.

CoPP limitations

- Policer rates are specified in packets per second (PPS).
- Destination IP-based access-list matching is not supported in Custom CoPP.
- User-defined MAC access lists are not supported; only built-in MAC ACLs can be used.
- A maximum of 28 class maps can be configured under a Custom CoPP policy.
- Custom CoPP supports maximum 360 IPv4 (uni-dimensional) and 180 IPv6 (uni-dimensional) TCAM entries.
- The CoPP Consistency Checker is not supported for Custom CoPP.
- Zero Committed Information Rate (CIR) is not supported. If zero CIR is configured, the hardware sets it to the minimum possible value.
- On N9324C-SE1U switches, the **clear copp statistics** command clears the CoPP statistics for all policers, except for the **hardware rate-limiter** policers.

MACsec

Media Access Control Security (MACsec) is an IEEE 802.1AE security standard that provides confidentiality and data integrity for Ethernet links by encrypting traffic at Layer 2 on a hop-by-hop basis.

Beginning with NX-OS Release 10.6(2)F, MACsec and Secure Key Integration Protocol (SKIP) are supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For information on MACsec, refer to Configure MACsec.

MACsec limitations

- On Cisco N9324C-SE1U switch, MACsec is supported on all 24 QSFP28 ports.
- On Cisco N9348Y2C6D-SE1U switch, MACsec is supported on all 48 SFP28, 6 QSFP-DD, and 2 QSP28 ports.
- The MACsec SecY statistics do not support any statistical information related to egress Secure Association (SA) counters. Egress statistical data always displays as zero.
- For EAPOL configuration, ensure the following requirements are met:
  - The EAPOL MAC address must be in the range 0180.C200.0000 to 0180.C200.00FF (the last byte can be from 0x00 to 0xFF) and the EtherType can be any value between 0x600 and 0xFFFF.
  - Any MAC address is allowed when the EtherType is set to the default value 0x888E.
  - The broadcast MAC address can be used with any EtherType value in the range 0x600 to 0xFFFF.

Traffic storm control

Traffic storm control is a Layer 2 security feature designed to prevent network disruption caused by excessive broadcast, multicast, or unicast traffic flooding a LAN port. It works by monitoring incoming traffic over a 3.9-millisecond interval and comparing the traffic level against a configured threshold, which is a percentage of the port's total available bandwidth. When the traffic exceeds this threshold during the interval, the feature drops the excessive traffic until the interval ends.

Beginning with NX-OS Release 10.6(2)F, traffic storm control is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches with a one-level threshold (1R2C).

For more information on Traffic Storm Control, refer to Configuring Traffic Storm Control.

Traffic storm control guidelines and limitations

- Supports only one-level threshold (1R2C).
- Do not support two-level threshold (2R3C).
- Do not support PPS.
- Supported interfaces are Layer 2 ports, including physical, breakout, and port-channel interfaces.
- These commands are deprecated on N9300 Series smart switches:
  - **system storm control multi-threshold**
  - **storm-control multi unicast** {**level1** *level-value %* | **level2** *level-value %*}
  - **storm-control multi action1 trap action2 shutdown**

Live protect

Live Protect is a security feature embedded in NX-OS that provides real-time, kernel-level protection using eBPF technology through the Tetragon agent. It enables compensating controls for Common Vulnerabilities and Exposures (CVEs) and mitigates zero-day attacks without requiring software upgrades or system reboots. The feature is managed and activated via NXSecure, which configures Tetragon for continuous monitoring, detection, and logging of security events, enhancing threat visibility and telemetry integration.

Beginning with NX-OS Release 10.6(2)F, Live Protect is supported on the N9324C-SE1U and N9348Y2C6D-SE1U Smart switches.

For more information on Live Protect, refer to Live Protect.

Live Protect guidelines and limitations

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.

Compatibility with other features

The Live Protect feature is not supported with application hosting, dockerbox, configuration replace, or auditD features.

Impact on CPU

There is negligible impact on CPU.

Licensing

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.

Supported modes

- Monitoring mode
- Enforce mode

Release-specific information

Beginning with NX-OS Release 10.6(3)F, the Live protect feature is enhanced, and the enhancements are

- policy mode can now be specified while adding policy to the switch
- syslog is supported now, and
- a new show command is introduced to display the log history for a particular policy.