New and Changed Information

This chapter lists new and changed content in this document by software release.

New and Changed Information for Security Configuration

This section lists new and changed content in this document by software release.

To find additional information about new features or command changes, see the *Cisco Nexus 1000V Release Notes* and *Cisco Nexus 1000V Command Reference*.

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
802.1X Support	Support for 802.1X feature that defines a client-server-based access control and authentication protocol to restrict unauthorized clients from connecting to a LAN through publicly accessible ports.	5.2(1)SV3(4.1)	Information About 802.1X
Cisco TrustSec Subnet-SGT Mapping	Support for binding SGT to all the host addresses of a specified subnet.	5.2(1)SV3(2.1)	Cisco TrustSec Subnet-SGT Mapping
CTS SXPv3 Protocol Support	Support for Cisco TrustSec SXPv3 protocol.	5.2(1)SV3(2.1)	Cisco TrustSec With SXPv3
Multi-IP per MAC support for IPSG	Multiple IP address attached to a MAC address for packet management.	5.2(1)SV3(2.1)	Information About IP Source Guard
Cisco TrustSec SXP Peer Connection Modes	Cisco Nexus 1000V supports both speaker and listener modes for remote peer connections.	5.2(1)SV3(1.3)	Configuring Cisco TrustSec SXP Peer Connections

Feature	Description	Changed in Release	Where Documented
Port Security	MAC Move Detection and Violation is no longer supported.	5.2(1)SV3(1.1)	Security Violations and Actions
Layer 3 Security	Layer 3 Security (L3Sec) is a framework that secures the internal control plane communications (control and packet traffic) of the Cisco Nexus 1000V in a more robust way than in previous releases.	5.2(1)SV3(1.1)	Configuring Layer 3 Security
Cisco TrustSec 2.0	This feature supports tagging of packets with the Cisco TrustSec command header and SGACL enforcement.	5.2(1)SV3(1.1)	Configuring Cisco TrustSec
Traffic Storm Control	You can implement this feature to control broadcast, multicast, and unknown unicast traffic on ports and to control flooding.	5.2(1)SV3(1.1)	Configuring Traffic Storm Control
SSH	SSH can support IPv6 addresses	5.2(1)SV3(1.1)	Configuring SSH
Telnet	Telnet can support IPv6 addresses.	5.2(1)SV3(1.1)	Configuring Telnet
IPACLs	You can configure IPv6 ACLs	5.2(1)SV3(1.1)	Configuring IP ACLs
Cisco TrustSec	This feature was introduced.	4.2(1)SV2(1.1)	Configuring Cisco TrustSec
Licensing Changes and advanced features	The following features are available as advanced features that require licenses: Cisco TrustSec, DHCP snooping, IP Source Guard, and Dynamic ARP Inspection.	4.2(1)SV2(1.1)	Configuring DHCP Snooping,Configuring Dynamic ARP Inspection,Configuring IP Source Guard
DHCP Enhancements	You can enable source IP-based filtering on the Cisco Nexus 1000V switch.	4.2(1)SV2(1.1)	Configuring DHCP Snooping
ACL Logging	You can log statistics for flows that match the ACL permit or deny conditions to monitor the flows.	4.2(1)SV1 (5.1)	Creating a MAC ACL
UUFB	You can block unknown unicast packets from flooding the forwarding path.	4.2(1)SV1(4a)	Information About UUFB
DHCP Snooping Relay Agent (Option 82)	You can configure DHCP to relay VSM MAC and port information in DHCP packets.	4.2(1)SV1(4)	Configuring DHCP Snooping

Feature	Description	Changed in Release	Where Documented
DHCP Snooping binding table	You can clear DHCP snooping binding table entries for an interface.	4.2(1)SV1(4)	Configuring DHCP Snooping
Enable DHCP	You can enable or disable DHCP globally by using the **feature DHCP** command.	4.2(1)SV1(4)	Configuring DHCP Snooping
Enable SSH server	You can enable or disable the SSH server by using the **feature DHCP** command.	4.2(1)SV1(4)	Configuring SSH
Enable Telnet server	You can enable or disable the Telnet server by using the **feature DHCP** command.	4.2(1)SV1(4)	Configuring Telnet
Disable HTTP Server	You can disable the HTTP server for security purposes.	4.0(4)SV1(4)	Disabling the HTTP Server
VSD	Virtual service domains (VSDs) allow you to classify and separate traffic for network services.	4.0(4)SV1(2)	Chapter 3, "Configuring VSD"
DHCP Snooping	The Dynamic Host Configuration Protocol (DHCP) snooping acts like a firewall between untrusted hosts and trusted DHCP servers.	4.0(4)SV1(2)	Configuring DHCP Snooping
Dynamic ARP Inspection (DAI)	Dynamic ARP-inspection (DAI) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address.	4.0(4)SV1(2)	Configuring Dynamic ARP Inspection
IP Source Guard	IP Source Guard is a per-interface traffic permit filter for IP and MAC addresses.	4.0(4)SV1(2)	Configuring IP Source Guard
Secure Login Enhancement	Support to configure login parameters.	5.2(1)SV3(4.1a)	Secure Login Enhancements