New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 7000 Series NX-OS Security Command Reference*. The latest version of this document is available at the following Cisco website:
http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html

To check for additional information about this Cisco NX-OS Release, see the Cisco NX-OS Release Notes available at the following Cisco website:
http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

The following table summarizes the new and changed features for the *Cisco Nexus 7000 Series NX-OS Security Command Reference* and tells you where they are documented.

Table 1 New and Changed Information

Feature	Description	Changed in Release
Port Group Modifier	Added the **portgroup-modifier** keyword and the *modifier* argument to the **hardware rate-limiter** command.	6.2(12)
Control Plane Policing	Added the **unicast rpf-failure** keywords to the **match (class-name)** command.	6.2(10)
Cisco TrustSec	Added F3 Module support for the **propagate-sgt** command.	6.2(10)
ACL TCAM bank mapping	Added the **show hardware access-list feature-combo** command.	6.2(10)
Cisco TrustSec	Added the **cts refresh environment-data** command.	6.2(2)
Cisco TrustSec	Enabled the **cts sgt** and **policy** commands to accept decimal values.	6.2(2)
Cisco TrustSec	Added the **left-zero-padded, display encrypt** and **encrypted** *encrypted_pmk* keywords and argument to the **sap pmk** command.	6.2(2)
Cisco TrustSec	Added the **show cts capability interface** command.	6.2(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
Cisco TrustSec	Added the **brief** keyword to the **show cts interface** command.	6.2(2)
Cisco TrustSec	Added the **show cts role-based sgt vlan command.**	6.2(2)
Cisco TrustSec	Added the **show cts sap pmk** command.	6.2(2)
Cisco TrustSec	Added the **summary**, **sxp peer** *peer-ipv4-addr*, **vlan** *vlan-id*, and **vrf** *vrf-name* keywords and arguments to the **show cts role-based sgt-map command.**	6.2(2)
Control Plane Policing	Added the **show policy-map interface control-plane command.**	6.2(2)
DHCP	Added the **ipv6 dhcp relay** command.	6.2(2)
DHCP	Added the **show ipv6 dhcp relay** command.	6.2(2)
DHCP	Added the **show ipv6 dhcp relay statistics** command.	6.2(2)
DHCP	Added the **ipv6 dhcp relay address** command.	6.2(2)
DHCP	Added the **clear ip dhcp relay statistics** command.	6.2(2)
DHCP	Added the **clear ipv6 dhcp relay statistics** command.	6.2(2)
DHCP	Added the **show ip dhcp relay statistics** command.	6.2(2)
IP ACLs	Added the *hardware access-list resource feature bank-mapping command.*	6.2(2)
IP ACL	Added the **show system internal access-list feature bank-class map** command.	6.2(2)
Rate Limits	Added the **glean-fast** keyword to the **hardware rate-limiter, show hardware rate-limiter, and clear hardware rate-limiter commands.**	6.2(2)
TACACS+	Added the single-connection keyword to the tacacs-server host command.	6.2(2)
VLAN ACLs	Added the **hardware access-list allow deny ace** command.	6.1(3)
VACL capture for M2 modules	Added support for M2 Series module. Changed the usage guideline for the **hardware access-list capture** command.	6.1(1)
show cts interface	Added the new output for **show cts interface** command for M2 Series modules for 40/100G links.	6.1(1)
Cisco TrustSec authentication	Added F1 and F2 Series modules support for cts dot1x command.	6.0

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
Cisco TrustSec authentication	Added F1 and F2 Series modules support for replay protection command.	6.0
Cisco TrustSec authentication	Added F1 and F2 Series modules support for **sap pmk** command.	6.0
ACL capture	Added the ability to configure ACL capture in order to selectively monitor traffic on an interface or VLAN. Also, added support for ACL capture on M1 Series modules.	5.2(1)
AES password encryption	Added the ability to support the AES password encryption.	5.2(1)
Control Plane policy	Added the ability to change or reapply the default CoPP policy without rerunning the setup utility.	5.2(1)
	Changed the CoPP best practice policy to read-only CoPP and added the ability to copy the policy in order to modify it.	5.2(1)
	Added the **show copp profile** and **show copp diff profile** commands to display the details of the CoPP best practice policy and the difference between the applied default policy and the latest or previous policy, respectively.	5.2(1)
	Added the **show running-config aclmgr** and **show startup-config aclmgr** commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.	5.2(1)
DHCP enhancements	Added support for DHCP smart relay.	5.2(1)
	Added subnet broadcast support for DHCP relay agent.	5.2(1)
Pause frame encryption	Added the ability to support pause frame encryption and decryption on interfaces.	5.2(1)
Control Plane policy	Added the ability to specify the threshold value for Control Plane Policing (CoPP)) map-dropped packets and generate a syslog if the drop count exceeds the configured threshold.	5.1(1)
SCP and SFTP servers	Added the ability to configure SCP and SFTP servers on the Cisco NX-OS device in order to copy files to and from a remote device by using the following commands: • feature scp-server • feature sftp-server	5.1(1)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
User roles	Added the ability to display the syntax of the commands that the network-admin and network-operator roles can use by executing the following commands: • show cli syntax roles network-admin • show cli syntax roles network-operator	5.1(1)
Rate limit	Added the ability to configure rate limits for packets that reach the supervisor module and to log a system message if the rate limit is exceeded. The following commands were introduced with this feature: • rate-limit • show system internal pktmgr internal control sw-rate-limit	5.1(1)
RSA key size range	Beginning in Cisco NX-OS Release 5.1, the RSA key size range can be from 1024 to 2048 bits.	5.1(1)
AAA accounting	Added the **logflash** keyword to the following command to clear the accounting log stored in the logflash for the current VDC: • clear accounting log	5.0(2)
AAA authentication	Added the **fallback error local** keyword to the following commands to support fallback to local authentication for the console or default login if remote authentication is configured and all AAA servers are unreachable: • aaa authentication login console • aaa authentication login default	5.0(2)
AAA authorization	Deprecated the **none** keyword in the following commands: • **aaa authorization commands default** • aaa authorization config-commands default Added the following command to configure the default AAA authorization method for TACACS+ or LDAP servers: • aaa authorization **ssh-certificate** default Added the following command to configure LDAP or local authorization with the SSH public key as the default AAA authorization method for LDAP servers: • aaa authorization **ssh-publickey** default	5.0(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
CHAP authentication	Added the following commands to support CHAP authentication: • aaa authentication login chap enable • **show aaa authentication login**	5.0(2)
DHCP snooping	Added or changed the following commands to support virtual routing and forwarding instances (VRFs): • **ip dhcp relay address** • **ip dhcp relay information option vpn** • **show dhcp relay address** • **show ip dhcp relay** Added the following command to enable DHCP to use Cisco proprietary numbers 150, 152, and 151 for the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions: • **ip dhcp relay sub-option type cisco** Added the following command to support DHCP snooping: • **ip dhcp packet strict-validation**	5.0(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
LDAP authentication	Changed the following commands to support LDAP server groups: • aaa authentication login console • aaa authentication login default Added the following command to support the creation of an LDAP server group: • **aaa group server ldap** Added the following command to configure LDAP authentication to use the bind or compare method: • **authentication** {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]} Added the following command to clear LDAP server statistics: • clear ldap-server **statistics** Added the following command to support sending a search query to the LDAP server: • **CRLLookup** Added the following command to enable LDAP users to log in only if the user profile lists the subject-DN of the user certificate as authorized for login: • **enable Cert-DN-match** Added the following command to enable group validation for an LDAP server group: • **enable user-server-group** Added the following command to enable LDAP: • feature ldap Added the following command to configure the deadtime interval for all LDAP servers: • ldap-server deadtime Added the following command to configure LDAP server host parameters: • ldap-server host Added the following command to configure a global LDAP server port through which clients initiate TCP connections: • ldap-server port	5.0(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
LDAP (continued)	Added the following command to configure the global timeout interval for LDAP servers: • **ldap-server timeout** Added the following command to configure an LDAP search map: • ldap search-map Changed the following command to add support for LDAP server groups: • server Added the following command to display information about the configured LDAP attribute maps: • show ldap-search-map Added the following command to display the LDAP server configuration: • show ldap-server Added the following command to display the LDAP server group configuration: • show ldap-server groups Added the following command to display the LDAP server statistics: • show ldap-server **statistics** Added the following command to display LDAP server information in the running configuration: • show running-config ldap Added the following command to display LDAP server information in the startup configuration: • **show startup-config ldap** Added the following command to configure the trusted certificate in order to send a search query to the LDAP server: • **trustedCert attribute-name** Changed the following command to add support for LDAP server groups: • use-vrf Added the following command to configure the certificate DN match in order to send a search query to the LDAP server: • **user-certdn-match attribute-name**	5.0(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
LDAP (continued)	Added the following command to configure the public key match in order to send a search query to the LDAP server: • **user-pubkey-match attribute-name** Added the following command to configure the user-switchgroup in order to send a search query to the LDAP server: • **user-switch-bind attribute-name** Added the following command to configure the user profile in order to send a search query to the LDAP server: • **userprofile attribute-name**	5.0(2)
PKI	Added the following command to specify the cert-store to be used for certificate authentication: • **crypto ca lookup** {**local** | **remote** | **both**} Added the following command to configure the refresh time to update the certificate revocation list (CRL) from the remote cert-store: • **crypto ca remote ldap crl-refresh-tim**e Added the following command to configure the LDAP server group: • **crypto ca remote ldap server-group** Added the following command to support the creation of a filter map: • **crypto certificatemap mapname** Added the following command to configure a certificate mapping filter for the SSH protocol: • crypto cert ssh-authorize Added the following command to configure certificate mapping filters within the filter map: • **filter** Added the following command to display the cert-store configuration: • show crypto ca certstore Added the following command to display the remote cert-store configuration: • **show crypto ca remote-certstore**	5.0(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
PKI (continued)	Added the following command to display the certificate mapping filters: • show crypto certificatemap Added the following command to display the mapping filters configured for SSH authentication: • show crypto ssh-auth-map	5.0(2)
RADIUS	Added the following command to monitor the availability of all RADIUS servers without having to configure the test parameters for each server individually: • radius-server **test**	5.0(2)
Rate limiting	Added the **l2pt** keyword to the following command to clear rate-limit statistics for Layer 2 Tunnel Protocol (L2TP) packets: • **clear hardware rate-limiter** Added the **l2pt** keyword to the following command to configure rate limits for L2TP packets: • hardware rate-limiter Added the **l2pt** keyword to the following command to display rate limit statistics for L2TP packets: • show rate-limiter	5.0(2)
RBACL	Added the following command to clear RBACL statistics: • **clear cts role-based counters** Added the following command to enable RBACL statistics: • **cts role-based counters enable** Added the **log** keyword to the following commands in support of RBACL logging: • deny • permit Added the following command to display the configuration status of RBACL statistics and list the statistics for all RBACL policies: • show cts role-based counters	5.0(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
SSH	Added the following command to configure the maximum number of times that a user can attempt to log in to an SSH session: • ssh **login-attempts** Added the following command to display the public key for the specified user: • **show username** *username* **keypair**	5.0(2)
TACACS+	Added the following command to enable a user to move to a higher privilege level after being prompted for a secret password: • **enable** *level* Added the following command to enable a secret password for a specific privilege level: • **enable secret** Added the following command to enable the cumulative privilege of roles for command authorization on TACACS+ servers: • feature privilege Added the **priv-***n keyword to the following command to* specify the privilege level when creating or modifying a user role or privilege role: • role name Added the following command to show the current privilege level, username, and status of cumulative privilege support: • show privileg**e** Added the following command to monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually: • **tacacs**-server **test** Added the **keypair** and **priv-lvl** keywords to the following command for use when creating a user account in a virtual device context (VDC): • **username** *user-id*	5.0(2)
AAA MSCHAP V2 authentication	Added the **mschapv2** keyword to the **aaa authentication login default** and **show authentication** commands.	4.2(1)
AAA accounting log	Added the **last-index** and **start-seqnum** keywords to the **show accounting log** command.	4.2(1)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
802.1x authentication	Added the **dot1x pae authenticator** command.	4.2(1)
RADIUS statistics	Added the **clear radius-server statistics** command.	4.2(1)
TACACS+ statistics	Added the **clear tacacs-server statistics** command.	4.2(1)
TACACS+ command authorization	Added the following commands to support TACACS+ command authorication: • **aaa test authorization command-type** • **show aaa authorization** • **tacacs-server authorization command login default** • **tacacs-server authorization config-command login default** • **terminal verify-only**	4.2(1)
Port Security	Changed the following commands to support support port security on port-channel interfaces: • **clear port-security** • **switchport port-security** • **switchport port-security aging time** • **switchport port-security aging type** • **switchport port-security mac-address** • **switchport port-security mac-address sticky** • **switchport port-security maximum** • **switchport port-security violation**	4.2(1)
IP ACLs	Added the **fragments** command to support optimization of fragment handling during IP ACL processing.	4.2(1)
MAC ACLs	Added or changed the following commands to support MAC packet classification: • **ip port access-group** • **ipv6 port traffic-filter** • **mac packet-classify**	4.2(1)
Atomic ACL updates	Changed the **hardware access-list update** command to indicate that, in Cisco NX-OS Release 4.1(4) and later, it is available in the default virtual device context (VDC) only..	4.1(4)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
Cisco TrustSec SXP passwords	Changed the **cts sxp default password** and **cts sxp connection peer** commands to allow encrypted passwords.	4.1(3)
Hardware commands	Added the **hardware access-list update** and **hardware rate-limit** commands and deprecated the **platform access-list update** and **platform rate-limit** commands.	4.1(2)
Access-list resource pooling	Added the **hardware access-list resource-pooling** command.	4.1(2)
SSH	Added the **feature ssh** command and deprecated the **ssh server enable** command.	4.1(2)
Telnet	Added the **feature telnet** command and deprecated the **telnet server enable** command.	4.1(2)
IPv6 ACLs	Added and changed commands to support IPv6 ACLs, including the **ipv6 access-list**, **permit (IPVv6)**, **deny (IPv6)**, **ipv6 traffic-filter**, and **ipv6 port traffic-filter** commands.	4.1(2)
Packet length filtering	Added the **packet-length** keyword to the **deny (IPv4)** and **permit (IPv4)** commands. The **permit (IPVv6)** and **deny (IPv6)** commands also support the **packet-length** keyword.	4.1(2)
RADIUS	Added **radius abort**, **radius commit**, **radius distribute**, and **show radius** commands for CFS distribution of the RADIUS configuration.	4.1(2)
TACACS+	Added **tacacs+ abort**, **tacacs+ commit**, **tacacs+ distribute**, and **show tacacs+** commands for CFS distribution of the TACACS+ configuration.	4.1(2)
User roles	Added **role abort**, **role commit**, and **role distribute** commands for CFS distribution of the user role configuration. Also, added the **pending** and **pending-diff** keywords to the **show role** command.	4.1(2)
AAA	Added the **aaa authentication login ascii-authentication** and **show aaa authentication login ascii-authentication** commands to support enabling ASCII authentication on TACACS+ servers.	4.1(2)
Public Key Infrastructure (PKI)	Added command to support PKI, including **crypto ca trustpoints**, **crypto ca authenticate**, and **crypto ca crl request command**.	4.1(2)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release
RADIUS and TACACS+ server groups	Added the **ip radius source-interface**, **ip tacacs source-interface**, and **source-interface** commands to configure source interfaces for RADIUS or TACACS+ server groups.	4.1(2)
Default user roles for AAA authentication of remote users	Added the **aaa user default-role** and **show aaa default-user role** commands.	4.0(3)
VLAN ACL capture	Removed the **capture** keyword from the **action** command. Capture of traffic forwarded by a VLAN ACL is not supported in Cisco NX-OS Release 4.0.	4.0(3)
Rate limits	Added the **port-security** key word to the **clear hardware rate-limit**, **platform rate-limit**, and **clear hardware rate-limit** commands.	4.0(3)
IPv6 packet policing in control plane class maps	Added IPv6 support to the **match (class-map)** command.	4.0(3)
Password-strength checking	Added the **password strength-check** and **show password strength-check** commands.	4.0(3)
Cisco TrustSec	Added the **propagate-sgt** command.	4.0(3)
Telnet for IPv6	Added the **telnet6** command.	4.0(2)
Control plane policing (CoPP) configuration status information	Added the **show copp status** command.	4.0(2)