Lab 3-3: Configuring Security Features

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will log into your VDC and configure the Cisco Nexus 7000 Switch to support the data security requirements in the design. After completing this activity, you will be able to meet these objectives:

- Configure and verify access control lists using atomic programming
- Configure port security on the Cisco Nexus 7000 Switch and verify that the configuration has been applied as per the design requirements
- Configure traffic storm control on the Cisco Nexus 7000 Switch and verify that the configuration has been applied as per the design requirements
- Configure 802.1ae data encryption on the Cisco Nexus 7000 Switch

Command List

The table describes the commands that are used in this activity.

Command	Description
absolute start *time date* [end *time date*]	This command creates an absolute rule that is in effect beginning at the time and date that are specified after the start keyword.
configure session *name*	This command creates a configuration session and enters session configuration mode.
Commit	This command validates the configuration changes that are made in the current session and applies valid changes to the device.
feature port-security	This command enables port security globally.
ip access-group access-list {in | out}	This command applies an IPv4 or IPv6 ACL to the Layer 3 interface for traffic flowing in the direction specified.
ip access-list *name*	This command creates the IP ACL and enters IP ACL configuration mode.
object-group ip address *name*	This command creates the IPv4 address object group.
object-group ip port *name*	This command creates the protocol port object group.
periodic *list-of-weekdays time* to *time*	This command creates a periodic rule that is in effect on the days that are specified by the list-of-weekdays argument between and including the specified start and end times.
periodic *weekday time to [weekday] time*	This command creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.
resequence ip access-list	This command assigns sequence numbers to the rules contained in the ACL.
show configuration session	This command displays the contents of the session.
show interface [ethernet *slot/port* | port-channel	This command displays the traffic storm

Command	Description
number] counters storm-control	control configuration for the interfaces.
show ip access-lists	This command displays the IPv4 ACL configuration.
show port-security interface	This command displays the port security status of a specific interface.
show running-config aclmgr	This command displays ACL configuration, including all time ranges.
storm-control {broadcast | multicast | unicast} level *percentage*	This command configures traffic storm control for traffic on the interface.
switchport port-security	This command enables port security on the interface.
switchport port-security maximum *number*	This command configures the maximum number of MAC addresses that can be learned or statically configured for the current interface.
time-range *name*	This command creates the time range.
verify	This command verifies the configuration as a whole, which is based on the existing hardware and software configuration and resources.

Task 0: Lab Preparation

In this task, you will perform the steps necessary to get ready for performing the Tasks in this lab.

Activity Procedure

Complete these steps:

Step 1 Before you can perform this lab you will need a Student Server and a Pod Number assigned to you. Your instructor should provide to you the following information:

- Student Server Name or IP Address
- Student Server Username
- Student Server Password
- Pod Number
- Peer Pod Number

Step 2 From your personal/work computer use the Remote Desktop Connection (RDC) application to log in to your assigned Student Server. Refer to *Accessing the NterOne Lab Equipment* for detailed instructions regarding how to use RDC to connect to your Student Server.

Step 3 From your Student Server desktop use the PuTTY application to open SSH sessions to each of the devices in the following table.

Device Name	Device Description	IP Address	Username	Password
vdcP*	Your Pod Nexus 7004 VDC	10.0.0.8P*	admin	Nterone179
vdcQ*	Your Peer Pod Nexus 7004 VDC	10.0.0.8Q*	admin	Nterone179
N5K-A	Nexus 5548UP Switch	10.0.0.78	admin	Nterone179
N5K-B	Nexus 5548UP Switch	10.0.0.79	admin	Nterone179

*Note	Replace “P” with your Pod Number for this lab and replace “Q” with your Peer Pod Number.

Step 4 Perform a configuration rollback on your Pod VDC to the checkpoint named “baseline”. Use the “best-effort” option.

```
vdcP# rollback running-config checkpoint baseline best-effort
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch

Rollback completed successfully.
```

Step 5 If any VLANs other than VLAN 1 are still on your Pod VDC, delete them.

Step 6 Reconfigure all interfaces as trunk switchorts and ensure that are operational.

```
vdcP# config
Enter configuration commands, one per line.  End with CNTL/Z.
vdcP(config)# interface ethernet 3/A-D
vdcP(config-if-range)# switchport
vdcP(config-if-range)# switchport mode trunk
vdcP(config-if-range)# no shutdown
```

Step 7 Enable the SVI feature and configure interface VLAN P0 with the IP address 172.16.1P.7P/24 (P is your Pod number).

```
vdcP(config)# feature interface-vlan
vdcP(config)# interface vlan P0
vdcP(config-if)# ip address 172.16.1P.7P/24
vdcP(config-if)# no shutdown
vdcP(config-if)# vlan P0
```

Step 8 On N5K-X configure interface Ethernet 1/a as a trunk to the VDC interface Ethernet 3/A.

```
N5K-X# config
Enter configuration commands, one per line.  End with CNTL/Z.
N5K-X(config)# interface ethernet 1/a
N5K-X(config-if)# speed 1000
N5K-X(config-if)# switchport mode trunk
N5K-X(config-if)# no shutdown
```

Step 9 Create interface VLAN P0 and assign the IP address 172.16.1P.5P/24.

```
N5K-X(config-if)# feature interface-vlan
N5K-X(config)# interface vlan P0
N5K-X(config-if)# ip address 172.16.1P.5P/24
N5K-X(config-if)# no shutdown
N5K-X(config-if)# vlan P0
```

Step 10 Verify that you can ping between the two SVIs you just created.

```
N5K-X(config-if)# ping 172.16.1P.7P
PING 172.16.P1.7P (172.16.1P.7P) from 172.16.P1.5P: 56 data bytes
64 bytes from 172.16.1P.7P: icmp_seq=0 ttl=254 time=1.226 ms
64 bytes from 172.16.1P.7P: icmp_seq=1 ttl=254 time=0.878 ms
64 bytes from 172.16.1P.7P: icmp_seq=2 ttl=254 time=0.844 ms
64 bytes from 172.16.1P.7P: icmp_seq=3 ttl=254 time=7.094 ms
64 bytes from 172.16.1P.7P: icmp_seq=4 ttl=254 time=9.605 ms

--- 172.16.1P.7P ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.844/3.929/9.605 ms
```

Activity Verification

You have completed this activity when you have achieved these goals:

- You have made a successful connection to your Student Server.
- You have successfully used PuTTY to connect to the devices in the table above.

- You rolled back the running configuration to the state at checkpoint “baseline” on your Pod VDC.
- You have connectivity between the SVI’s on your N5K and your VDC.

Task 1: Configuring ACLs

In this task, you will configure and verify ACLs using atomic programming.

Activity Procedure

Complete these steps:

Step 11 From within your VDC, enter the session using the configure session command. Name your session ACL-CHECK and create two object groups, one named RemSupport (includes host 172.16.1P.5P and host 172.16.1Q.5Q) and the other named RemTerminal (permits Telnet and SSH).

```
vdcP# configure session ACL-CHECK
Config Session started, Session ID is 1
Enter configuration commands, one per line.    End with CNTL/Z.
vdcP(config-s)# object-group ip address RemSupport
vdcP(config-s-ipaddr-ogroup)# host 172.16.1P.5P
vdcP(config-s-ipaddr-ogroup)# host 172.16.1Q.5Q
vdcP(config-s-ipaddr-ogroup)# exit
vdcP(config-s)# object-group ip port RemTerminal
vdcP(config-s-port-ogroup)# eq 22
vdcP(config-s-port-ogroup)# eq 23
```

Step 12 View the configuration session.

```
vdcP(config-s-port-ogroup)# show configuration session

config session ACL-CHECK
0001   object-group ip address RemSupport
0002   host 172.16.1P.5P
0003   host 172.16.1Q.5Q
0004   object-group ip port RemTerminal
0005   eq 22
0006   eq 23
Number of active configuration sessions = 1
vdcP(config-s-port-ogroup)# exit
```

Step 13 Configure the time range: absolute starting from 8:00 a.m. (0800) 1 January 2013 and periodic for working time (from 8:00 a.m. [0800] to 11:00 p.m. [2300]) and weekends. If necessary, adjust the times to ensure that you are in the correct time range (show clock command on the Cisco Nexus 7000 VDC).

```
vdcP(config-s)show clock
15:15:49.052 UTC Tue Nov 29 2011
vdcP(config-s)# time-range RemSupportVPN
vdcP(config-s-time-range)# absolute start 8:00:00 1 January 2013
vdcP(config-s-time-range)# periodic Monday Tuesday Wednesday Thursday Friday
8:00:00 to 23:00:00
vdcP(config-s-time-range)# exit
```

Step 14 Create an IP access list named TermAccess.

```
vdcP(config-s)# ip access-list TermAccess
```

Step 15 Configure the IP access list TermAccess to permit access from your Pod and the peer Windows servers to SVI 10. Use the object groups named RemSupport and RemTerminal that were created in Step 1 with the time range RemSupportVPN that was created in Step 3.

```
vdcP(config-s-acl)# statistics
```

```
vdcP(config-s-acl)# permit tcp addrgroup RemSupport host 172.16.1P.7P portgroup
RemTerminal time-range RemSupportVPN
vdcP(config-s-acl)# deny ip any any
```

Step 16 Assign the IP access list to an SVI P0 interface within your Pod VDC in the ingress direction.

```
vdcP(config-s)# interface vlan P0
vdcP(config-s-if)# ip access-group TermAccess in
```

Step 17 View the configuration session.

```
vdcP(config-s-if)# show configuration session

0001  object-group ip address RemSupport
0002  host 172.16.1P.5P
0003  host 172.16.1Q.5Q
0004  object-group ip port RemTerminal
0005  eq 22
0006  eq 23
0007  time-range RemSupportVPN
0008  absolute start 8:0:0 1 January 2013
0009  periodic Monday Tuesday Wednesday Thursday Friday 8:0:0 to 23:0:0
0010  ip access-list TermAccess
0011  statistics
0012  permit tcp addrgroup RemSupport host 172.16.1P.7P portgroup RemTerminal
time-range RemSupportVPN
0013  deny ip any any
0014  interface VlanP0
0015  ip access-group TermAccess in

Number of active configuration sessions = 1
```

Step 18 Verify the configuration session ACL-CHECK.

```
vdcP(config-s-if)# verify
Verification Successful
```

Step 19 If the operation in the previous was successful, then commit the session to the running configuration.

```
vdcP(config-s)# commit
Commit Successful
```

Q1) Ping the VDC VLAN P0 SVI from N5K-X. Was the ping successful? Why?

Q2) Try SSH to your VDC VLAN P0 SVI from N5K-X (ssh admin@172.16.1P.5P). Was SSH successful?

Step 20 Issue a show running-config aclmgr command.

```
vdcP# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sun Mar      6 08:12:31 2011

version 5.2(1)
object-group ip address RemSupport
10 host 172.16.1P.5P
20 host 172.16.1Q.5Q
object-group ip port RemTerminal
10 eq 22
```

```
20 eq 23
ip access-list TermAccess
  statistics per-entry
  10 permit tcp addrgroup RemSupport 172.16.1P.7P/32 portgroup RemTerminal time-
range RemSupportVPN
  20 deny ip any any

interface VlanP0
ip access-group TermAccess in
time-range RemSupportVPN
10 absolute start 8:00:00 1 January 2013
20 periodic Monday Tuesday Wednesday Thursday Friday 8:00:00 to 23:00:00
```

Step 21 View the IP access list TermAccess.

```
vdcP# show access-lists

IP access list TermAccess
        statistics per-entry
        10 permit tcp addrgroup RemSupport 172.16.1P.7P/32 portgroup RemTerminal
time-range RemSupportVPN
        20 deny ip any any [match=4]

vdcP# show access-lists expanded

IP access list TermAccess
statistics per-entry
10 permit tcp 172.16.1P.5P/32 172.16.1P.7P/32 eq 22 time-range RemSupportVPN
10 permit tcp 172.16.1P.5P/32 172.16.1P.7P/32 eq telnet time-range RemSupportVPN
10 permit tcp 172.16.1Q.5Q/32 172.16.1Q.7Q/32 eq 22 time-range RemSupportVPN
10 permit tcp 172.16.1Q.5Q/32 172.16.1Q.7Q/32 eq telnet time-range RemSupportVPN
20 deny ip any any [match=4]
```

Step 22 Check that the access list TermAccess is applied to interface VLAN P0.

```
vdcP# show access-lists summary
IPV4 ACL TermAccess
        Total ACEs Configured: 2
        Configured on interfaces:
                VlanP0 - ingress (Router ACL)
        Active on interfaces:
                VlanP0 - ingress (Router ACL)
```

Step 23 Permit the following IP hosts between sequence numbers 5 and 8.

- 192.168.150.10
- 192.168.160.10
- 192.168.165.55
- 192.168.179.35

```
vdcP# config
Enter configuration commands, one per line.   End with CNTL/Z.
vdcP(config)# ip access-list TermAccess
vdcP(config-acl)# 5 permit ip host 192.168.150.10 any
vdcP(config-acl)# 6 permit ip host 192.168.160.10 any
vdcP(config-acl)# 7 permit ip host 192.168.165.55 any
vdcP(config-acl)# 8 permit ip host 192.168.179.35 any
```

Step 24 View the IP access list TermAccess.

```
vdcP(config-acl)# show access-lists TermAccess

IP access list TermAccess
statistics per-entry
5 permit ip 192.168.150.10/32 any
```

```
6 permit ip 192.168.160.10/32 any
7 permit ip 192.168.165.55/32 any
8 permit ip 192.168.179.35/32 any
10 permit tcp addrgroup RemSupport 172.16.1P.7P/32 portgroup RemTerminal time-
range RemSupportVPN
20 deny ip any any [match=4]
```

Step 25 Use the resequence command to change the sequence numbers and the step increment.

```
vdcP(config)# resequence ip access-list TermAccess 10 20
```

Step 26 View the IP access list.

```
vdcP(config)# show access-lists TermAccess

IP access list TermAccess
IP access list TermAccess
statistics per-entry
10 permit ip 192.168.150.10/32 any [match=0]
30 permit ip 192.168.160.10/32 any [match=0]
50 permit ip 192.168.165.55/32 any [match=0]
70 permit ip 192.168.179.35/32 any [match=0]
90 permit tcp addrgroup RemSupport 172.16.1P.7P/32 portgroup RemTerminal time-
rang
e RemSupportVPN
110 deny ip any any [match=4]
```

Activity Verification

You have completed this task when you attain these results:

- You have used the show commands to verify the ACL configuration.
- You have logged into the Windows host and generated some traffic, and then verified that the traffic that should be denied has been denied.

Task 2: Configuring Port Security

In this task, you will configure port security on the Cisco Nexus 7000 Switch and verify that the configuration has been applied as per the design requirements.

Activity Procedure

Complete these steps:

Step 27 Enable the port security feature.

```
vdcP(config)# feature port-security
```

Step 28 Verify that the port security feature is enabled.

```
vdcP(config)# show feature | include port
eth_port_sec          1         enabled
```

Step 29 Enable port security on Ethernet interface that is connected to your opposite N5K, which is interface Ethernet 3/B.

```
vdcP(config)# interface ethernet 3/B
vdcP(config-if)# switchport port-security
```

Step 30 Verify the port security configuration.

```
vdcP(config-if)# show port-security interface ethernet 3/B
Port Security              : Enabled
Port Status                : Secure UP
```

```
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Security violation count   : 0
```

Step 31 Check the interface MAC address table.

```
vdcP(config-if)# show mac address-table interface ethernet 3/B
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
```

Step 32 Configure two static MAC addresses.

```
vdcP(config-if)# switchport port-security mac-address 00C0.0000.0001
vdcP(config-if)# switchport port-security mac-address 00C0.0000.0002
ERROR: Maximum value reached, MAC address cannot be configured
```

Step 33 Vertify the staus of the port security on this interface.

```
vdcP(config-if)# show port-security interface ethernet 3/B
Port Security              : Enabled
Port Status                : Secure UP
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Security violation count   : 0
```

Step 34 Check the interface MAC address table.

```
vdcP(config-if)# show mac address-table interface ethernet 3/B
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
* 1        00c0.0000.0001    static       -       T    T  Eth3/B
```

Step 35 Remove port security from the interface and any configured MAC address.

```
vdcP(config-if)# no switchport port-security
vdcP(config-if)# no switchport port-security mac-address 00C0.0000.0001
```

Step 36 Check the interface MAC address table on the interface.

```
vdcP(config-if)# show mac address-table interface ethernet 3/B
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
```

Step 37 Disable the port security feature.

```
vdcP(config-if)# no feature port-security
```

Activity Verification

You have completed this task when you attain these results:

- You have used the show commands to verify that port security is configured.

Task 3: Configuring Traffic Storm Control

In this task, you will configure traffic storm control on the Cisco Nexus 7000 Switch and verify that the configuration has been applied as per the design requirements.

Activity Procedure

Complete these steps:

Step 38 Configure the broadcast traffic storm control limits to 50 percent on interface Ethernet 3/A.

```
vdcP(config)# interface ethernet 3/A
vdcP(config-if)# storm-control broadcast level 50
```

Step 39 Verify the traffic storm control parameters.

```
vdcP(config-if)# show interface ethernet 3/A counters storm-control

--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth3/A           100.00          100.00           50.00                       0
```

Step 40 Configure the multicast traffic storm control limits to 30 percent on interface Ethernet 3/A:

```
vdcP(config-if)# storm-control multicast level 30
```

Step 41 Verify the traffic storm control parameters.

```
vdcP(config-if)# show interface ethernet 3/A counters storm-control

--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth3/A           100.00           30.00           30.00                       0
```

Step 42 Configure the unicast traffic storm control limits to 75 percent on interface Ethernet 3/A.

```
vdcP(config-if)# storm-control unicast level 75
```

Step 43 Verify the traffic storm control parameters.

```
--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth3/A            75.00           75.00           75.00                       0
```

Note Only one suppression level is shared by all three suppression modes. As an example, if you set the broadcast level to 30 and set the multicast level to 40, both levels are enabled and set to 40.

Activity Verification

You have completed this task when you attain these results:

- You have used the show commands to verify that storm control is enabled.

Task 4: Configuring 802.1ae Data Encryption

In this task, you will configure 802.1ae data encryption on the Cisco Nexus 7000 Switch and verify that the configuration has been applied as per the design requirements.

Activity Procedure

Complete these steps:

Step 44 Enable the dot1x feature on your Pod VDC.

```
vdcP(config)# feature dot1x
```

Step 45 Enable the CTS feature on your Pod VDC.

```
vdcP(config)# feature cts
```

Step 46 Configure the Ethernet interface 3/D in your VDC that is connected to the peer VDC to use CTS in manual mode.

```
vdcP(config)# interface ethernet 3/D
vdcP(config-if)# cts manual
```

Step 47 Configure the SAP PMK and the cryptography mode to use. Use the 32-bit key **Nterone179**.

```
vdcP(config-if-cts-manual)# sap pmk Nterone179 modelist gcm-enc
```

Step 48 Check the CTS status on the interface.

```
vdcP(config-if)# show cts interface ethernet 3/D
CTS Information for Interface Ethernet3/D:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              Unknown
    Authentication Status:  CTS_AUTHC_INIT
      Peer Identity:
      Peer is:              Unknown in manual mode
      802.1X role:          CTS_ROLE_UNKNOWN
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_INIT
      PEER SGT:             0
      Peer SGT assignment:  Not Trusted
    SAP Status:             CTS_SAP_INIT
      Configured pairwise ciphers:
      Replay protection:
      Replay protection mode:
      Selected cipher:
    Propagate SGT: Enabled
```

Step 49 Restart the interface.

```
vdcP(config-if-cts-manual)# shutdown
vdcP(config-if)# no shutdown
```

Step 50 Check the CTS status on the interface (after the peer Pod completes this step).

```
vdcP(config-if)# show cts interface ethernet 3/D
CTS Information for Interface Ethernet3/D:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
```

```
Authentication Status:  CTS_AUTHC_SKIPPED_CONFIG
  Peer Identity:
  Peer is:              Unknown in manual mode
  802.1X role:          CTS_ROLE_UNKNOWN
  Last Re-Authentication:
Authorization Status:   CTS_AUTHZ_SKIPPED_CONFIG
  PEER SGT:             0
  Peer SGT assignment:  Not Trusted
SAP Status:             CTS_SAP_SUCCESS
  Configured pairwise ciphers: GCM_ENCRYPT
  Replay protection: Enabled
  Replay protection mode: Strict
  Selected cipher: GCM_ENCRYPT
  Current receive SPI: sci:6f61b861b0000 an:0
  Current transmit SPI: sci:6f61b86170000 an:0
Propagate SGT: Enabled
```

Activity Verification

You have completed this task when you attain these results:

- You have used the show commands to verify that 802.1ae data encryption is enabled.