Table of Contents

Use Cases

RETAIL: SEGMENTATION FOR PCI COMPLIANCE

Business Problem

A retail chain is required to comply with Payment Card Industry (PCI) standards where all devices that process

When the user first accesses the network, they authenticate. The switch or the WLC authenticates the user by using Cisco ISE, and the user is assigned a tag. The switch or WLC tags (with the SGT) the traffic from this user. The policy is enforced, based on the SGT, in the data center with an SGACL on the DC router or with an SGFW on the DC firewall.

Providing Di□erentiated Access to Data Center Resources Based on the User and Location

Figure 9

Deployment Details

Tech Tip

After you have finished software installation, you should check the release notes to see if there are patches available to apply that are appropriate for the requirements of your organization. After you download any required patches, you can automatically distribute and apply them to all nodes by navigating to Administration > System > Maintenance, selecting Patch Management, and following the instructions.

Step 12: In the Location list, choose a location. You can create a new location by clicking on the gear icon in the upper right corner and selecting Create New Network Device Group.

Step 13: In the Parent list, choose the parent device group.

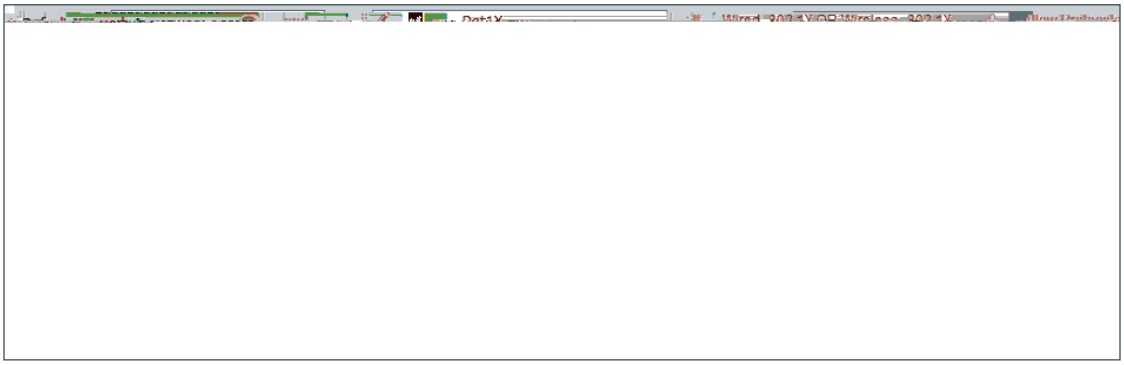
Step 14: Enter a name and (optionally) description, and then click

Step 3:

Step 4: Enter the RADIUS shared secret, and then click Save. The default network device configuration is now saved.

Procedure 9 Configure Cisco ISE to use Active Directory

Step 4: Click Done, and then click Save.



Procedure 11

Deployment Details

Step 4: Click

Step 3:

```
 key [radius key]
aaa group server radius ISE_GROUP
 server name ise-3
 server name ise-4

aaa authentication dot1x default group ISE_GROUP
aaa authorization network default group ISE_GROUP
aaa authorization confguration default group ISE_GROUP
aaa accounting dot1x default start-stop group ISE_GROUP

radius-server vsa send accounting
```

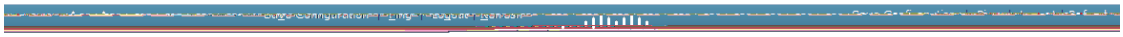
Step 5: Connect to the console of each access switch, and configure all host access ports on each. These commands should not be configured on infrastructure-facing ports, such as uplinks.

```
interface range [interface type] [port number]-[port number]
 ip access-group PreAuth in
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Tech Tip

On the Catalyst 3650/3850, there is a caveat where TrustSec inline tagging is incompatible with IP Source Guard (ip verify source). If you plan on using inline tagging, you need to disable IP Source Guard on the access port. This will be resolved in a future software release.

Step 14: Example on a WLC:



Assigning SGTs to Servers

1. Enable TrustSec on NX-OS switches
2. Con□gure IP-to-SGT binding on the NX-OS switch
3. Con□gure IP-to-SGT binding in ISE

Con□guring SGT Propagation

1. Con□gure SXP on IOS devices
2. Con□gure SXP on WLCs
3. Con□gure SXP on ISE
4. Con□gure SXP on Cisco ASA
5. Con□gure SXP in NX-OS
6. Con□gure inline tagging in IOS switches
7. Con□gure inline tagging in NX-OS switches
8. Con□gure inline tagging on the Nexus 1000v with port pro□les
9. Enable SXP on ISR
10. Enable inline tagging on the ISR
11. Enable inline tagging over DMVPN
12. Enable inline tagging over GET VPN

Figure 12 Propagation using inline tagging

```
cts sxp default password [password]
cts sxp connection peer 10.4.63.2 password default mode local speaker
cts sxp connection peer 10.4.15.5 password default mode local listener
cts sxp connection peer 10.4.15.6 password default mode local listener
```

Step 2: Verify the SXP connection.

```
D1-6807-VSS#show cts sxp connection
 S0 1  s0 1 Tf-s n2nabledr



10.4.15254r
```

```
Connection inst# : 9
TCP conn fd      : 2
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 9:16:54:20 (dd:hr:mm:sec)

---------------------------------------------
Peer IP          : 10.4.63.3
Source IP        : 10.4.15.254
Conn status      : Off
Conn version     : 4
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: none
Duration since last state change: 0:00:01:57 (dd:hr:mm:sec)


Total num of SXP Connections = 3
```

Step 7:

Step 5: Click Save.

Step 14: In the Version list, choose V4.

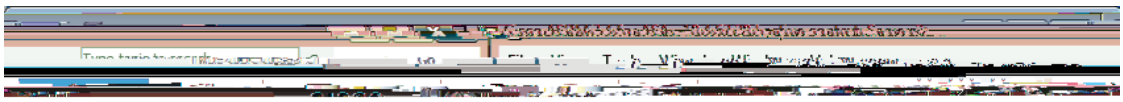
Tech Tip

SXP negotiates the version to use between devices and selects the highest version available. Selecting SXP V4 ensures that the device negotiates the highest version it supports.

Step 15: Click

Step 10: For Accounting Mode, select Simultaneous, and then click OK.

Step 32: Click Apply.



Tech Tip

Step 3: Verify the inline configuration. You'll see that TrustSec is in manual mode and that authorization was successful, using the SGT configured in the port profile.

As an example:

```
RS15-4331#show tunnel endpoints tunnel 20
 Tunnel20 running in multi-GRE/IP mode

 Endpoint transport 172.18.140.20 Refcount 3 Base 0x7F3F8C7D3AC0 Create Time 00:04:07
   overlay 10.6.38.1 Refcount 2 Parent 0x7F3F8C7D3AC0 Create Time 00:04:07
   Tunnel Subblocks:
      Tunnel TrustSec:
CTS-SGT:2 )(         ock 20)Tjnhrp-sb(        ocks:)NHRP sks:ec:
  D( .111  oveWE2-INET1-4451-/TT1 1 Tf0 Tw (show tunnel endpoints tunnel 20)TjTT0 1 Tf0 -2 TD( Tunn
```

```
KGS: Disabled
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): expired
Anti-Replay(Time Based) : 20 sec interval
tag method : cts sgt
alg key size: 32 (bytes)
sig key size: 20 (bytes)
encaps: ENCAPS_TUNNEL
```

Enabling Enforcement in the DC

1.

Step 8: In the Existing Security Group section, locate the user group you want to con□gure (example: **Research_Users**), and then click Add

Appendix A: Product List

IDENTITY MANAGEMENT

Appendix A: Product List

LAN DISTRIBUTION LAYER

Appendix A: Product List

Appendix A: Product List

WAN REMOTE SITE

Please use the feedback form to send comments and suggestions about this guide.