Cisco TrustSec How-To Guide: Segmenting Clients and Servers in the Data Center Using the Cisco Nexus 1000V Series Switches

Guide

Contents

Introduction

The goal of this guide is to provide you with the basic configurations required to test the features of Cisco TrustSec® technology in the 4.2(1)SV2(1.1) release of the Cisco Nexus® 1000V Series Switches. This guide will provide you with the configuration details for the Cisco® Identity Services Engine, Cisco ASA 5500 Adaptive Security Appliance, Cisco CiscoNexus 7000, and Cisco Nexus 1000V platforms. Once you are familiar with the concepts of Cisco TrustSec, you should be able to refer to the Cisco Secure Access how-to guides and expand your pilot environment to include platforms running Cisco IOS® Software. Examples include Cisco Catalyst® 6000, Catalyst 4000, and Catalyst 3000 Series Switches, and Cisco Wireless LAN Controllers.

In this document you will learn the necessary steps to enable data center segmentation. The data center segmentation includes, but is not limited to, server-server segmentation between both physical and virtual servers. The campus-to-data center segmentation includes, but is not limited to, users accessing data center resources either directly from the campus or through a virtual desktop environment. While there are multiple ways to enforce such polices, we will primarily focus on the use of Security Group Access Control Lists (SGACLs) and Security Group Firewalling (SGFW).

After readingthis guide, you should be able to:

- Configure basic TrustSec-based classification of end users and devices in the campus access layer as well as classification for servers and virtual desktop infrastructure (VDI) sessions within the data centers
- Demonstrate and test SGACL enforcement on the Cisco Nexus 7000 Series Switch by propagating SGT information from the Cisco Nexus 1000V
- Demonstrate and test SGFW on the Cisco ASA 5500 Adaptive Security Appliance
- Understand how Cisco Nexus 1000V interacts with the VMware vCenter and VMview components
- Configure each component in the Cisco TrustSec solution to build a strong access control and policy enforcement environment

Cisco TrustSec Overview

Cisco TrustSec uses the device and user identity information, as well as other attributes acquired during authentication and access layer handling, for classifying, or coloring the packets as they enter the network. This is called Cisco Secure Access. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network or communicating the tag to other elements using a control plane protocol called Security Group eXchange Protocol (SXP). These two transport mechanisms for the tag allow for the user or device to be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by helping to enable the endpoint device to act upon the SGT to filter traffic consistently, regardless of the underlying IP topology.

For additional information about Cisco TrustSec, see http://www.cisco.com/go/trustsec.

Additionally, specific design and implementation guidance is available for implementing the basic TrustSec functions (802.1X, MAB, WebAuth) that are a baseline for testing SGFW.

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html.

Topology Overview

Figure 1 shows a simple reference topology of the TrustSec solution. Since the scope of this document is limited to the TrustSec features on the Cisco Nexus 1000V platform, other components of the solution have been intentionally omitted. It is assumed that the user is already familiar with the other components of the solution. Please refer to the following links for additional information:

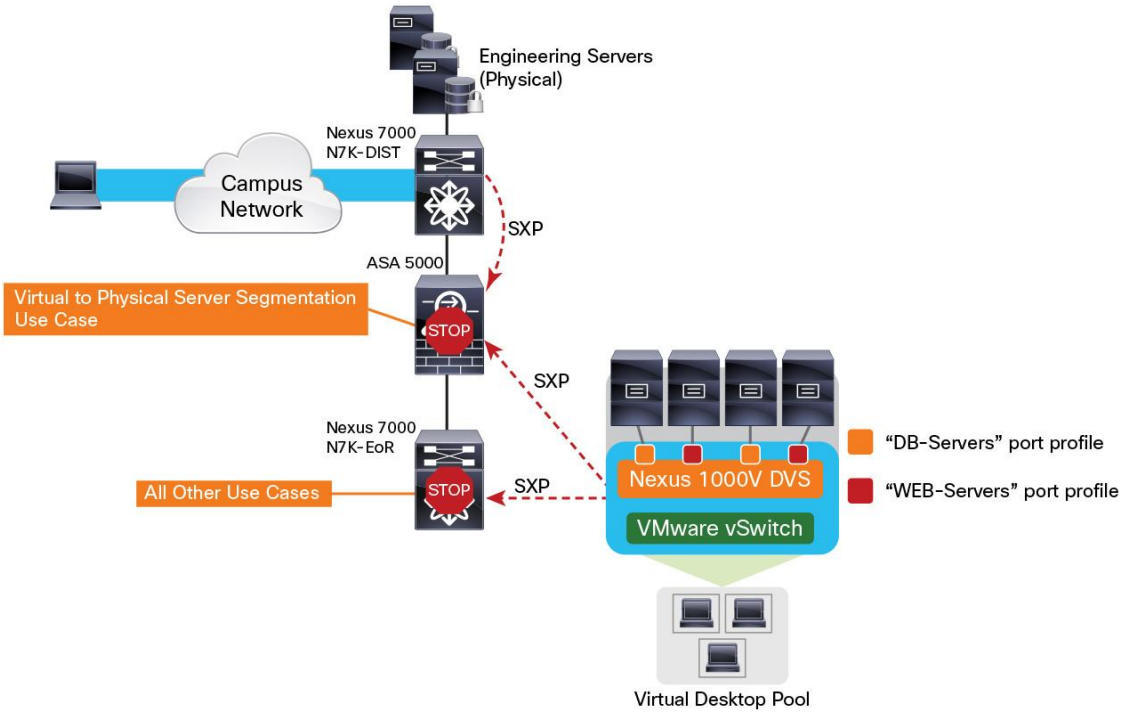
TrustSec 3.0 product bulletin: http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html.

TrustSec3.0 how-to guides:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html.

For the scope of this document the topology includes two instances of a Cisco Nexus 7000 Switch (distribution and end of row), the Cisco Adaptive Security Appliance, and the Cisco Nexus 1000V. The topology also consists of the Cisco Identity Services Engine, a Microsoft Active Directory environment, and a VMware View virtual desktop environment built on the Cisco UCS® platform running VMware ESXi 5.1. There are also a number of virtual and physical servers used to highlight the segmentation capabilities as each use case is outlined.

A number of SXP connections are setup between the various network devices to allow the flow of SGT tags. The use of SGACL enforcement on the Nexus 7000 end-of-row switch and security group firewalling on the Cisco ASA will be highlighted. Since the Nexus 1000V currently supports SGT Exchange Protocol (SXP) speaker mode only, the SXP connection design and choice of enforcement points are designed specifically for the purpose of this document.

Figure 1. Reference Topology of the TrustSec Solution



The reference topology consists of several components. Table 1 outlines required components, and Table 2 details optional ones.

Table 1. Required Topology Components

Platform (Supervisor)	TrustSec Feature	Version	Requirement
Cisco Nexus 1000V	SXP	Cisco NX-OS Software 4.2(1)SV2(1.1)	Required; Cisco Nexus 1000V sends SXP information to the upstream TrustSec-aware device
Cisco Nexus 7000	SXP, SGT assignment, SGACL	Cisco NX-OS Software 5.2(4), 6.1(1) or later release image required	Required as an enforcement point for data center segmentation use case
Cisco ASA 5500 Adaptive Security Appliance	SGFW, SXP	Cisco ASA 9.0.1, Adaptive Security Device Manager (ASDM) 7.0(1); SGFW functionality is required	Mandatory as an enforcement point for campus-to-data center use case as well as data center segmentation use case
Cisco ISE 1.1.x	Policy manager	1.1.1	Required
VMware vCenter		ESXi5.x	Virtual infrastructure manager (required)
Web SVMware View		VMview 5.1	VDI manager (optional)
Microsoft Server		Server 2003, Server 2008	AD, DHCP, DNS, CA
Cisco Unified Computing Servers™		Cisco UCS B-Series blade servers and UCS C-Series rack servers	Servers to run ESXi on

Table 2. Optional Components

Platform (Supervisor)	TrustSec Feature	OS Version	Requirement
Cisco Catalyst 4900 Series Switch	SXP	Cisco IOS Software 15.0(2)SG2 Release or later	Optional as access switch for campus-to-data center use case
Cisco Catalyst 4500E Switch with Supervisor 6L-E or 6-E	SXP	Cisco IOS Software Release 15.0(2)SG2 or later	Optional as access switch for campus-to-data center use case
Cisco Catalyst 4500E Switch with Supervisor 7L-E or 7-E	SXP	Cisco IOS Software Release 3.2.1SG or later	Optional as access switch for campus-to-data center use case
Cisco Catalyst 3750 or 3560 Series Switches	SXP	Cisco IOS Software Release 12.2 (53) SE or later; IP Base image required	Optional as access switch for campus-to-data center use case
Cisco Wireless LAN Controller	SXP	Cisco Software Release 7.2 or later	Optional as access switch for campus-to-data center use case

The Cisco TrustSec architecture is based on several key features described in Table 3.

Table 3. Features of Cisco TrustSec Architecture

Feature	Description
Secure Access	Cisco Secure Access is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually the process takes place at an access layer switch. Successful authentication and authorization in the process results in SGT assignment for the user or device.
Security Group Tag (SGT)	SGT is a 16-bit single label indicating the classification of a source in the TrustSec domain, appended to an Ethernet frame or IP packet. There are several methods in which to assign SGT to network entities, such as in an authorization process of successful 802.1X authentication or MAC Authentication Bypass. A SGT can be assigned statically to a particular IP address or to a switch interface.
Security Association Protocol	Security Association Protocol (SAP) for IEEE 802.1AE-based link encryption.
SGT Exchange Protocol	SGT Exchange Protocol (SXP) for IP to SGT mapping.
Security Group Firewall	Security Group Firewalling (SGFW) for firewall traffic enforcement.

Use Case Overview

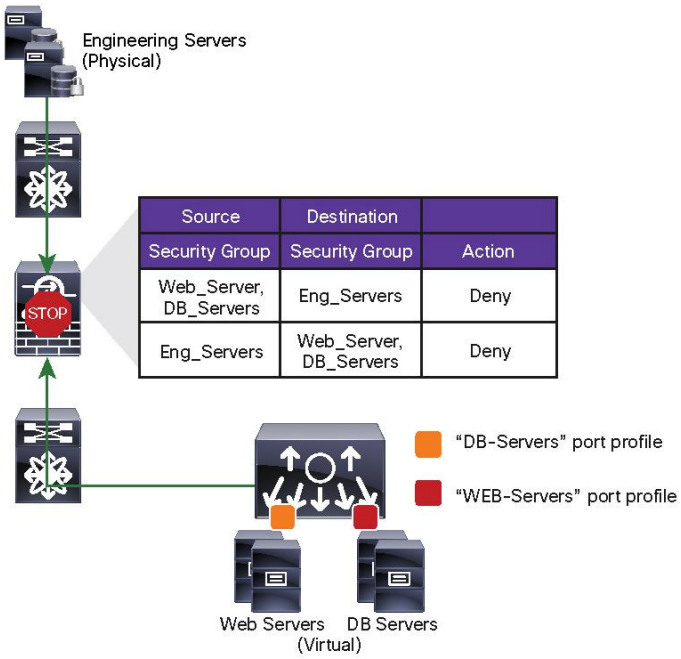
Data-Center Segmentation

This use case will cover the following types of segmentation:

1. Virtual server - physical server segmentation using SGFW (Figure 2).

   For this use case, we will deny all network traffic between the engineering server connected to the Cisco Nexus 7000 distribution switch and the virtual servers hosted behind the Cisco Nexus 7000 end-of-row switch. While SGFW is the chosen enforcement device, it is also possible to use SGACLs on the Nexus 7000 platforms. The Cisco ASA will receive the IP-SGT mapping for all the servers from the Cisco Nexus 7000 distribution switch and the Cisco Nexus 1000V using SXP.

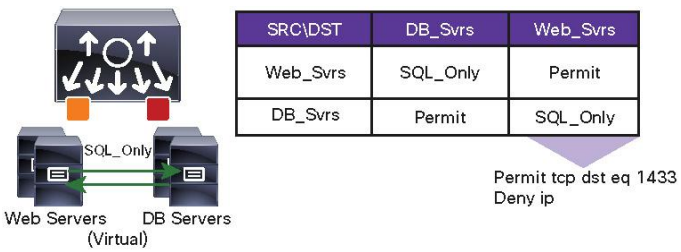
Figure 2. Physical Server Segmentation Using SGFW



2. Virtual server - virtual server segmentation using SGACL enforcement on the Cisco Nexus 7000 end-of-row switch (Figure 3).

   For this use case, we will allow only SQL traffic between the web and database servers. This is done by applying a SGACL on the Cisco Nexus 7000 end-of-row switch. The Cisco Nexus 1000V will assign the SGTs defined as a part of the port-profiles and notify the Cisco Nexus 7000 end-of-row switch of the IP-SGT mappings through SXP.

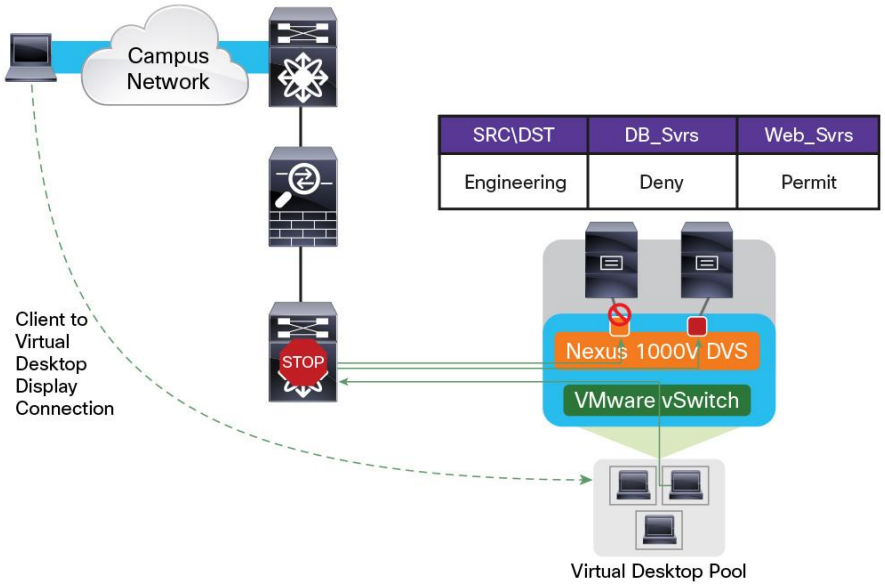
Figure 3. Virtual Server Segmentation Using SGACL Enforcement



3. VDI client to server segmentation (Figure 4)

   For this use case, we will allow users to access the web servers from the hosted virtual desktop pools. However, we will not allow users to access the database servers. We will use SGACL-based enforcement on the Cisco Nexus 7000 end-of-row switch. The Cisco Nexus 1000V will assign the SGTs defined as a part of the port-profiles and notify the Cisco Nexus 7000 end-of-row switch of the IP-SGT mappings using SXP.

Figure 4. VDI Client to Server Segmentation



Campus to Data Center Segmentation

The implementation of campus to datacenter segmentation builds upon the segmentation use cases already covered in this guide. Once you have completed the server-to-SGT mapping, the next step is to enable your network for dynamic SGT assignment at the access layer. This can be achieved by enabling user authentication mechanisms like 802.1X, MAB or WebAuth. This is covered in great detail in the TrustSec how-to guides: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html.

Configuration

In this section we will cover the configurations of Cisco ISE 1.1, Nexus 7000 switches, Nexus 1000V, and Cisco ASA.

It is assumed that the reader is familiar with the:

1. Installation and setup of Cisco Identity Services Engine
2. Installation and setup of Cisco Nexus 1000V
3. Installation and setup of Windows Active Directory services, VMware View, and VMware vCenter

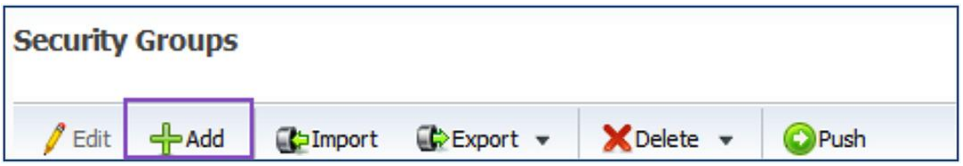
Configure Cisco ISE 1.1 for Security Group Access

In this section we will define Security Group tags for the different groups of servers and users. We will also define the related SGACL polices.

Procedure 1 Creating Security Group Tags in ISE 1.1

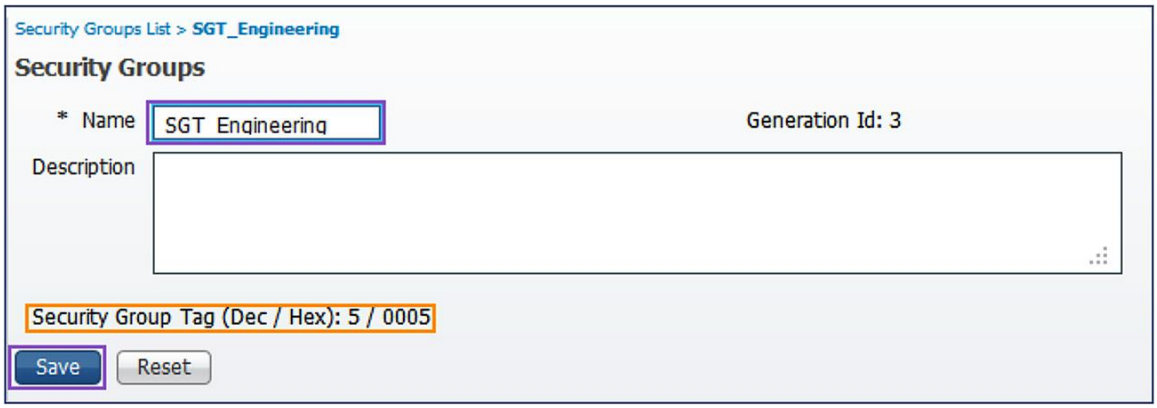
Step 1. From the ISE dashboard, navigate to **Policy → Policy Elements → Results → Security Group Access → Security Groups.**

Step 2. Click on **Add** to create a new Security Group.



Step 3. Create a security group for the engineering team called **SGT_Engineering** and hit **Save**.

Note: The SGT value is auto-generated by ISE. In this case, the SGT value for the engineering group is 5. This value may be different on your setup.



Step 4. Repeat steps 1-3 to create Security Groups for web servers and database servers. The SGT values used in this guide are listed in Table 4.

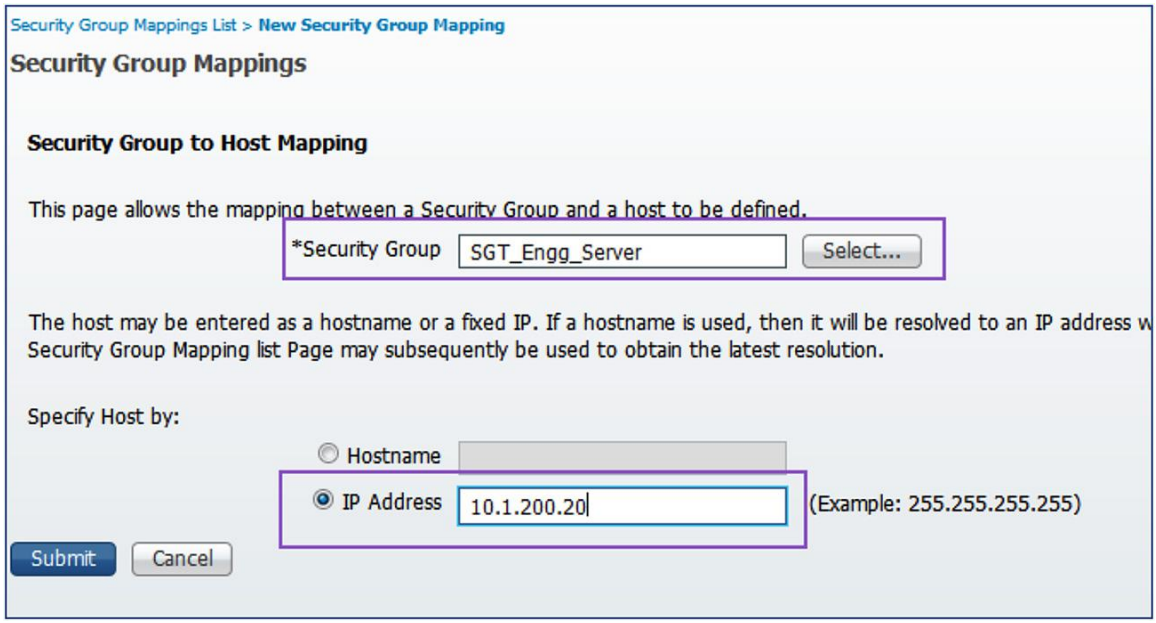
Table 4. Security Group Tag values

Security Group Name	Security Group Tag
SGT_Engineering	5
SGT_DB_Server	10
SGT_WEB_Server	12
SGT_Eng_Server	4

Procedure 2 Creating Manual IP-SGT Mappings

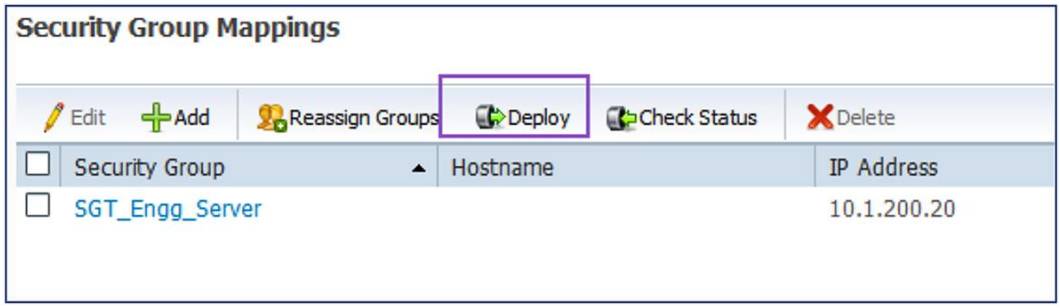
Step 1. From the ISE dashboard, navigate to **Policy → Policy Elements → Results → Security Group Access → Security Group Mappings** and click **Add**.

Define a security group mapping for the physical server connected to the Cisco Nexus 7000 distribution switch.



Step 2. Hit **Submit**.

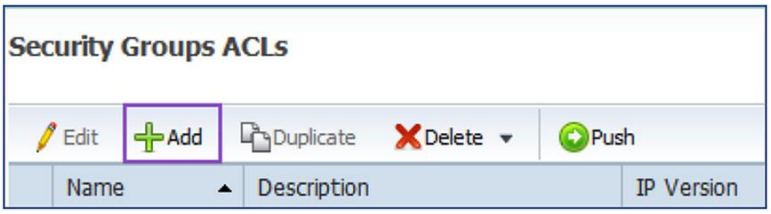
Step 3. Once you have completed the configuration of the Cisco Nexus 7000 Switches, come back to this screen and hit the deploy button to push out the IP-SGT mappings.



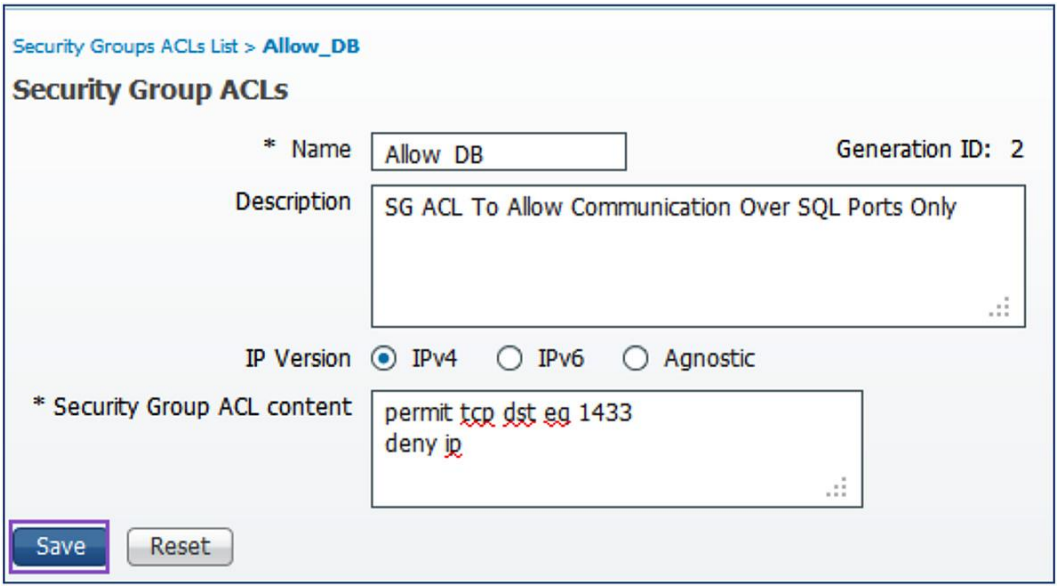
Procedure 3 Creating Security Group-Based ACLs on ISE (SGACLs)

Step 1. From the ISE dashboard, navigate to **Policy → Policy Elements → Results → Security Group Access → Security Group ACLs**.

Step 2. Click on **Add** to create a new SGACL.



Step 3. Create an **Allow_DB** SGACL to allow communication over SQL ports only. Hit **Save.**



Step 4. Repeat steps 1-3 to create an **Allow_WEB** SGACL

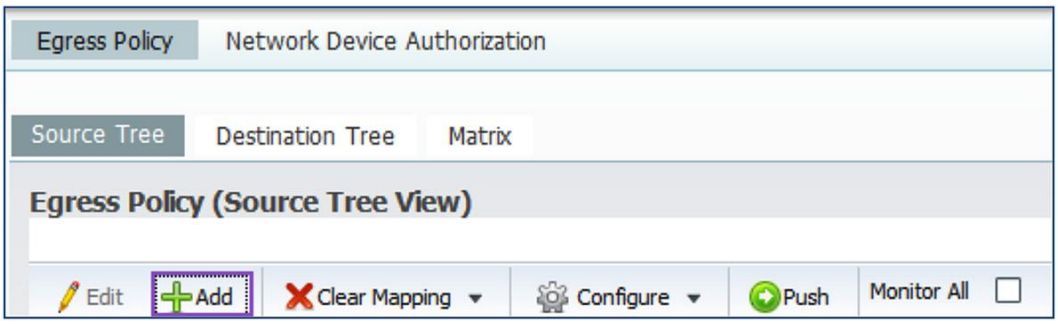
Table 5. SGACL to Allow Web Access Only

Allow_WEB
permittcpdsteq 80
permittcpdst port 443
permiticmp
denyip

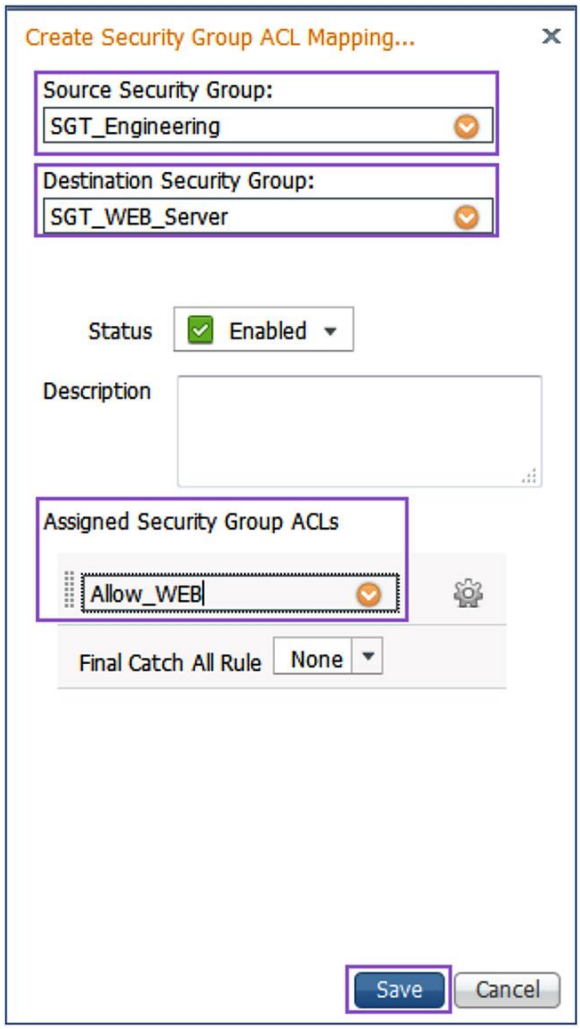
Procedure 4 Defining the Egress Policy Based on SGACL

Step 1. From the ISE dashboard, navigate to **Policy → Security Group Access → Egress Policy**.

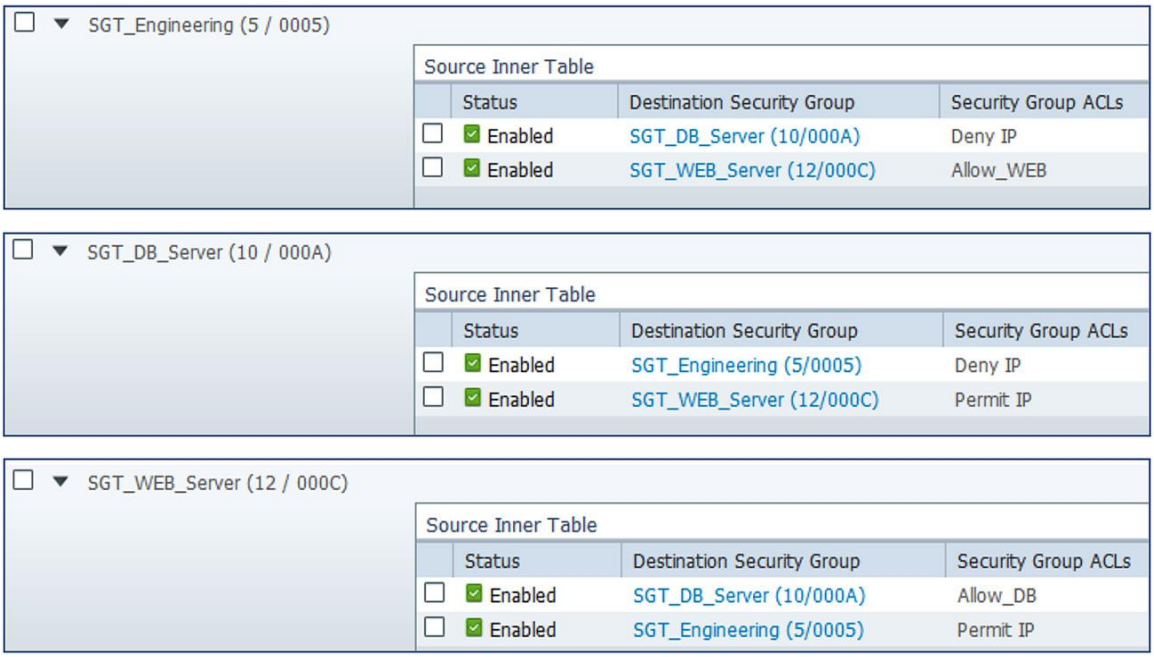
Step 2. Click on **Add** under the **Source Tree** view.



Step 3. Create an egress policy defining the level of access engineering has to the web servers. We set the **Source Security Group to SGT_Engineering**. The Destination Security Group is set to **SGT_WEB_Server**. Select the **Allow_WEB SGACL**. For cases where you would like to permit or deny all traffic, you could use the final option to define either a "Permit IP" or "Deny IP" rule.



Step 4. Follow Steps 2-3 to create additional egress policies.



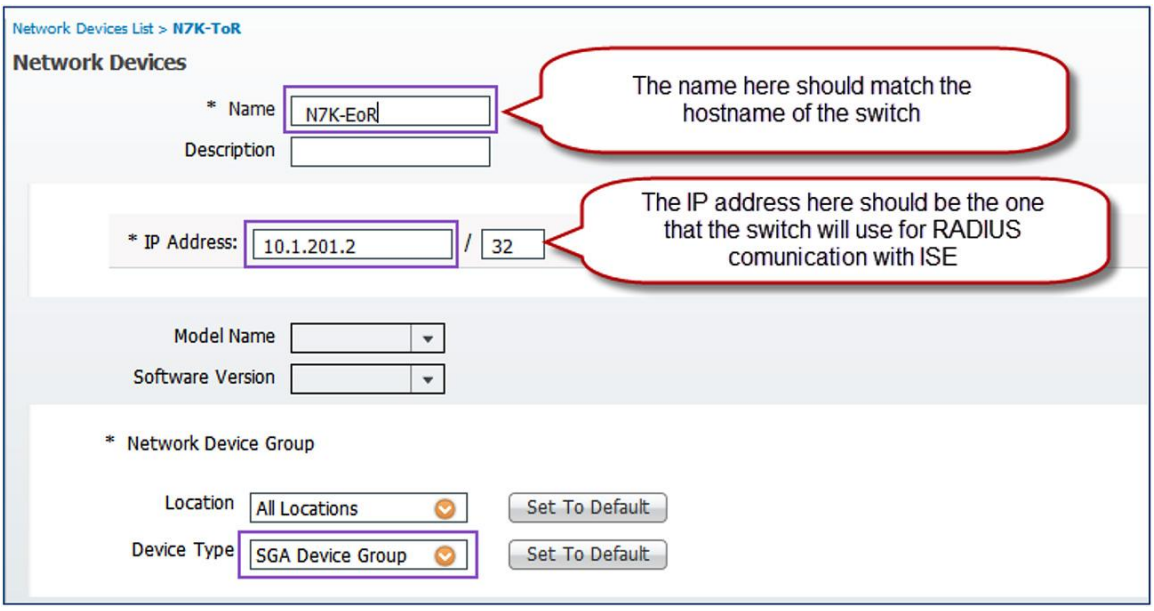
Procedure 5 Adding a Network Access Device to ISE

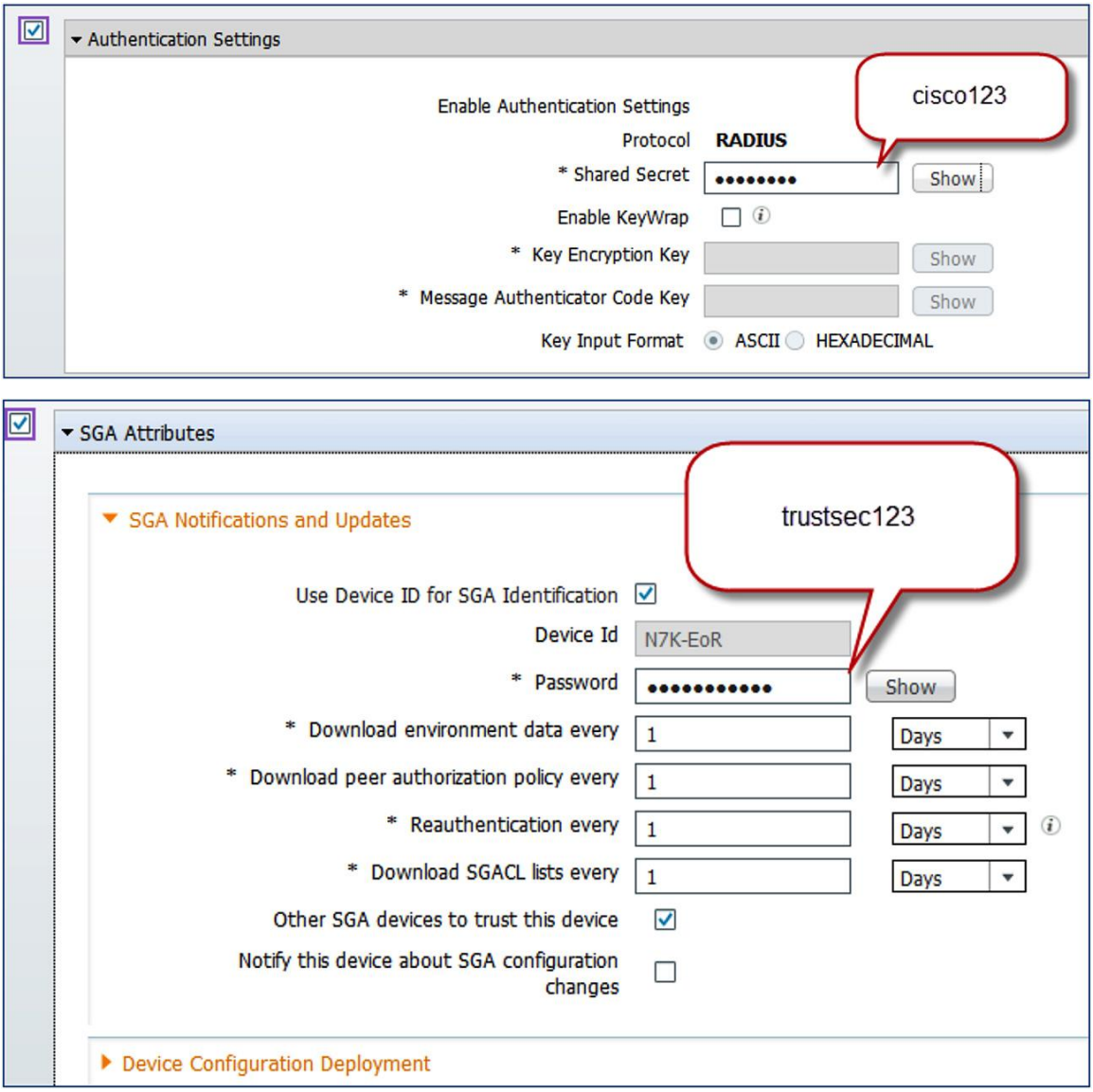
In this section, we will define a list of network devices that will use ISE to process RADIUS requests and receive access policy from ISE. For the purpose of this document, the Cisco Nexus 7000 Switch will be the network device used.

Step 1. From the ISE dashboard, navigate to **Administration → Network Resources → Network Devices**.

Step 2. Click on **Add** and fill in the details for the Cisco **Nexus 7000 end-of-row switch**.

Step 3. Repeat the steps and add the Cisco **Nexus 7000 distribution switch**.





Configuring the Cisco Nexus 7000 End-of-Row Switch

Procedure 1 Enable RADIUS and Related Configurations

Step 1. Type in the following commands.

```
feature dot1x
radius-server host 10.1.100.3 key 7 fewhg123 pac authentication accounting
aaa authentication dot1x default group ise-radius
aaa accounting dot1x default group ise-radius
aaa authorization cts default group ise-radius
ip radius source-interface Vlan201
```

Note: fewhg123 is the encrypted version of cisco123, the shared secret value used while adding the Nexus 7000 to ISE.

Procedure 2 Enable CTS, SXP, and SGACL-Based Enforcement

Step 2. Enable CTS using the following commands.

```
feature cts
cts device-id N7K-EoR password 7 wnyxlszh123
```

Note: The device-id N7K-ToR should exactly match the name used while adding the network device to ISE. Also, wnyxlszh123 is the encrypted version of trustsec123, the password used for SGA notification and updates configuration.

Step 3. Enable SXP and define SXP peer connections using the following commands.

```
cts sxp enable
cts sxp default password 7 fewhg123
cts sxp connection peer 10.1.201.3 source 10.1.201.2 password default mode
speaker
```

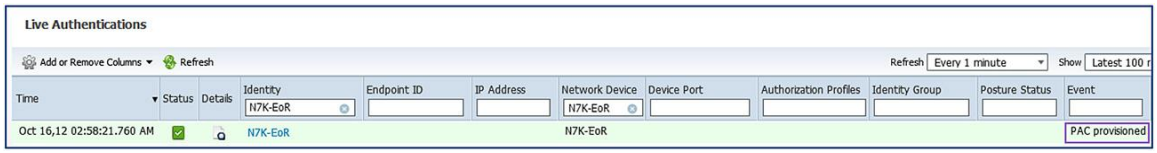
The ctssxp connection is used to define SXP peer connections. For the purpose of this document, we will establish an SXP peer relationship between the Nexus 1000V (10.1.201.3) and the Cisco Nexus 7000 (10.1.201.2). The ctssxp default password command sets the default password value to be used for all SXP connections. In this case, the password value is set to cisco123 (encrypted as fewhg123).

Step 4. Enable the Cisco Nexus 7000 to begin enforcing policies based on security group tags using the following command.

```
cts role-based enforcement
```

Procedure 3 Verify ISE and Nexus 7000 End-of-Row Connectivity

Step 1. From the ISE dashboard, navigate to **Operations → Authentications** and look for a message indicating that the PAC has been provisioned to the Cisco Nexus 7000.



Step 2. On the Cisco Nexus 7000, type the following commands for the correct output.

```
N7K-EoR# show cts environment-data
CTS Environment Data
================================
  Current State           : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
  Last Status             : CTS_ENV_SUCCESS
  Local Device SGT        : 0x0002
  Transport Type          : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache  : FALSE
  Env Data Lifetime       : 86400 seconds after last update
  Last Update Time        : Tue Oct 16 07:47:46 2012

  Server List             : CTSServerList1
     AID:fcb3077b3fd73ae45e0cef38447641c9 IP:10.1.100.3 Port:1812
```

```
N7K-EoR# show cts pacs
PAC Info :
================================
  PAC Type            : Trustsec
  AID                 : fcb3077b3fd73ae45e0cef38447641c9
  I-ID                : N7K-ToR
  AID Info            : ISE
  Credential Lifetime : Mon Jan 14 02:58:21 2013

  PAC Opaque          : 000200b00003000100040010fcb3077b3fd73ae45e0cef38447641c9
00060094000301004e1b0535f50c1626be8112a9339832ca00000013507c704b00093a8069494074
177b846d3da36aa7c7f3d01ddedbe07d77ec70ccaa9146d903718fad483d960a1426acdc6542ba0f
81e052ee5ad28a2e336206b4704e10dd4de54477de745e4aa1422ef605f13826ebe24c202a9fb253
321b1696830ddc66890cf6dccaa907a4eb5885c20250ad9e2d1ff16707e21bbd
```

Note: Repeat the above steps to configure the Nexus 7000 distribution switch. Once you have completed the configuration, remember to deploy the manually-defined IP-SGT mappings from ISE.

Configure the Cisco Nexus 1000V Switch

Procedure 4 License Configuration

The Advance Edition license is necessary for TrustSec functionality on the Cisco Nexus 1000V.

Step 1. Follow the license installation instructions located here: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_4/license/configuration/guide/n1000v_license_2install_cfg.html.

Step 2. Step 2 From the command line interface (CLI), type the following command:

```
svd switch edition advanced
```

Procedure 5 Configuring and Mapping Port-Profiles to VMs

In this section we will configure port-profiles for the web server, database servers, and the virtual desktop clients. Port-profiles include the security group tag value. The port-profiles will be mapped to the virtual interfaces of each of the machines using VMware vCenter. Once the appropriate port-profile is mapped to the VM, every time the VM is powered up, the Cisco Nexus 1000V applies the appropriate port-profile and informs the upstream Cisco Nexus 7000 of the IP to SGT mapping using SXP. Once the Cisco Nexus 7000 learns of the new IP-SGT mappings, it queries ISE for the associated SGACLs, which it then uses for the SGT-based enforcement.

Step 1. Configure port-profiles. Use the following commands to define port-profiles with SGT mappings for the various VMs. Since these port-profiles are going to be applied to VM virtual interfaces, we define them as type **vethernet**.

```
port-profile type vethernet DB-Servers
  vmware port-group
  switchport mode access
  switchport access vlan 202
cts sgt 10
  no shutdown
  state enabled
```

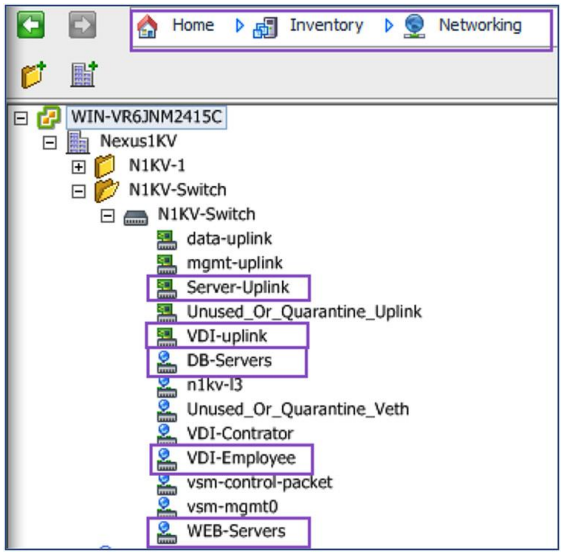
```
port-profile type vethernet WEB-Servers
  vmware port-group
  switchport mode access
  switchport access vlan 202
cts sgt 12
  no shutdown
  state enabled
```

```
port-profile type vethernet VDI-Employee
  vmware port-group
  switchport mode access
  switchport access vlan 203
cts sgt 5
  no shutdown
  state enabled
```

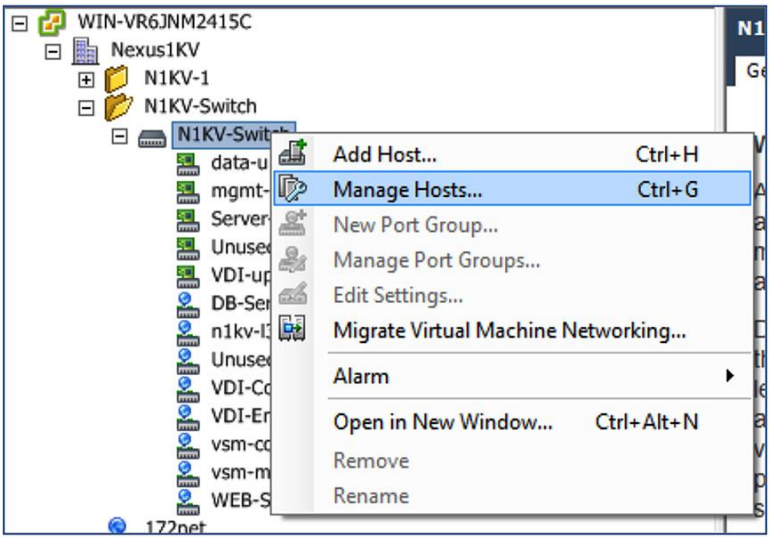
Step 2. Define the port-profiles for the physical interfaces that will carry the VM data traffic. For the purpose of this document, we will configure the uplink interfaces as access ports. All the traffic from the servers will be carried over VLAN 202 and traffic from the VDI clients will be carried over VLAN 203. Since these port-profiles will be applied to physical interfaces, we define them as type **ethernet**.

```
port-profile type ethernet VDI-uplink
  vmware port-group
  switchport mode access
  switchport access vlan 203
  no shutdown
  state enabled

port-profile type ethernet Server-Uplink
  vmware port-group
  switchport mode access
  switchport access vlan 202
  no shutdown
  state enabled
```

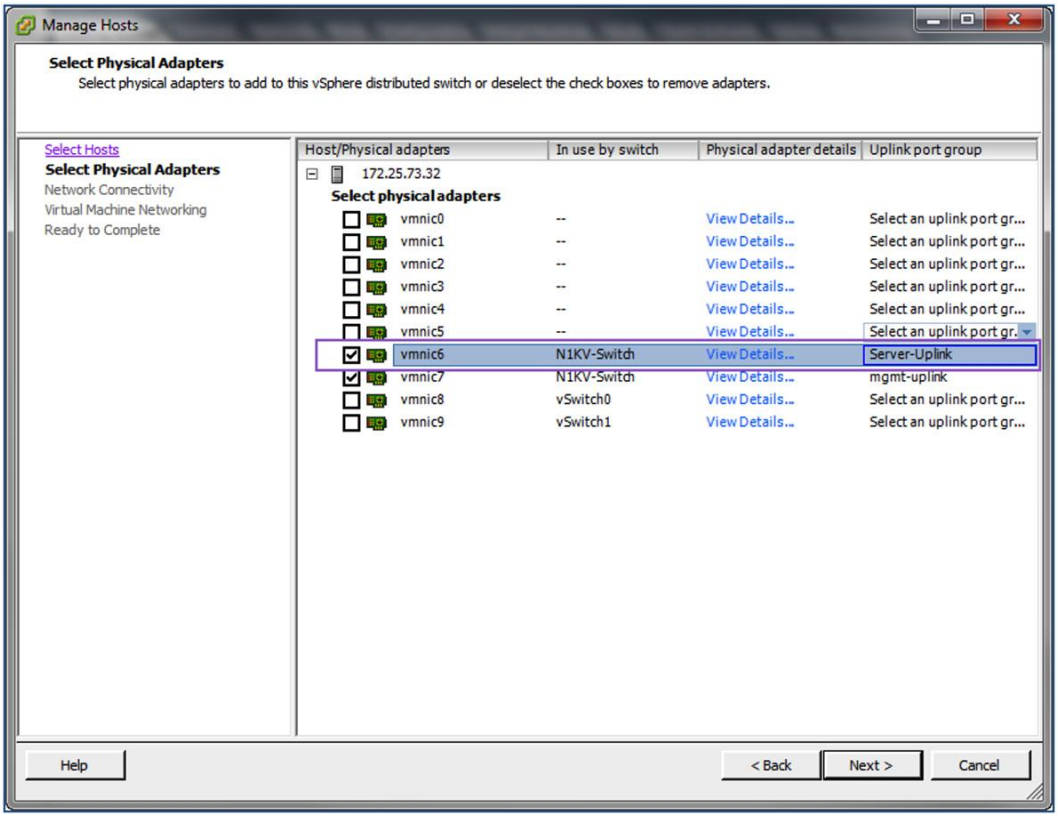
Step 3. Verify that the port-profiles are now available in vCenter. Log into vCenter and navigate to **Home → Inventory → Networking**. You should see the newly created port-profiles available.



Step 4. Now assign the various port-profiles to the appropriate interfaces. Right-click on your Cisco Nexus 1000V Switch in vCenter and choose the manage hosts options.

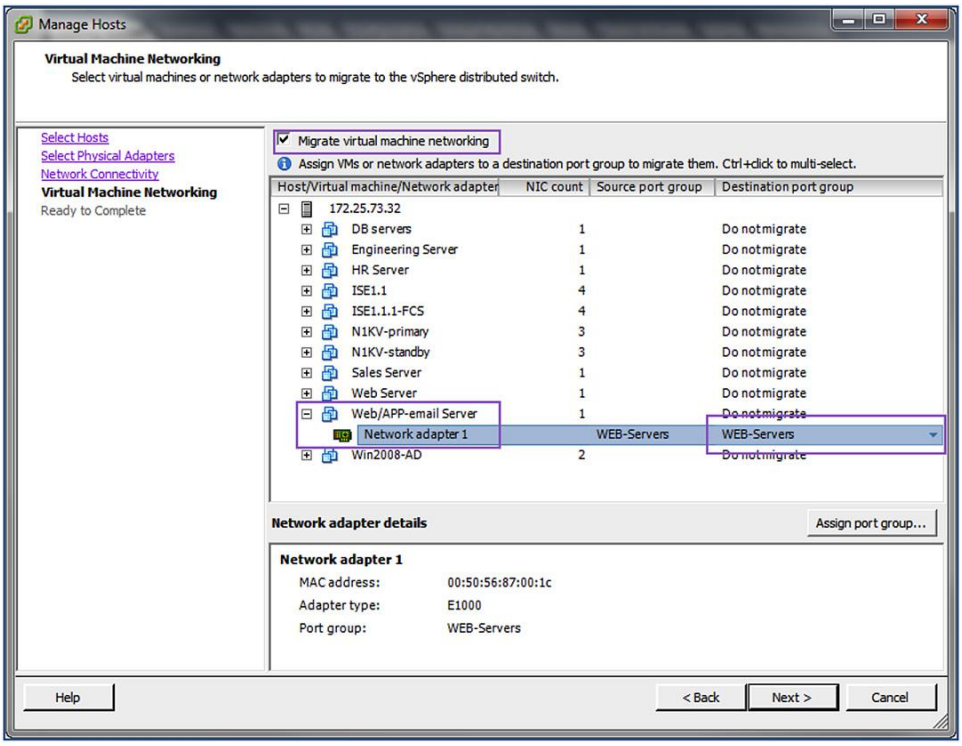


Step 5. Next, choose the host and map the physical interface to the uplink port-profiles. In this case, vmnic6 has been chosen as the physical uplink interface to carry traffic from the servers.

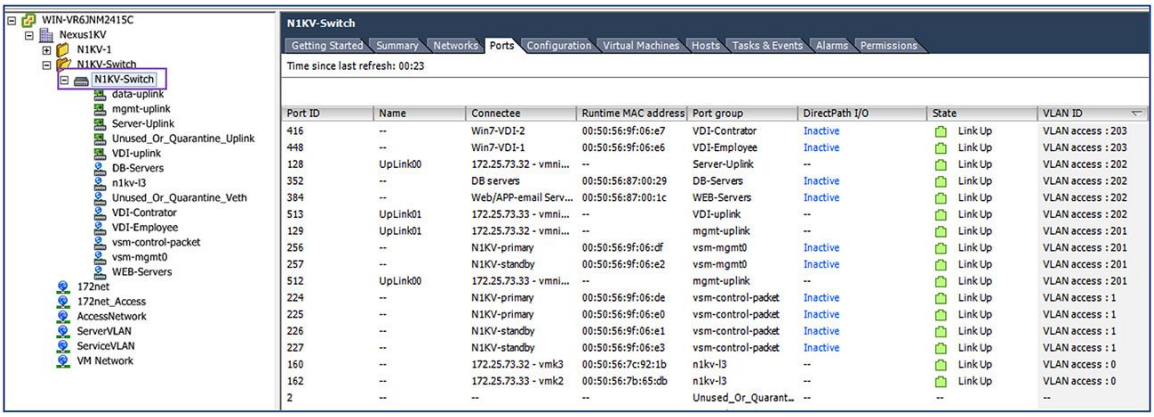


Step 6. Click **Next**. You will be given the option to select ports for distributed switch connectivity. Assuming you have already completed this step during the Cisco Nexus 1000V installation, no changes will be made here. Click **Next** again.

Step 7. You will now have the option to migrate the VM to the new port-profiles. Once you are done mapping the VMs to the appropriate port-profiles, hit **Next** and then **Finish**.



Step 8. Repeat the previous steps to map port-profiles for the VDI clients and the physical interface that will carry the VDI traffic. Once you have completed the configuration, you can verify settings in vCenter.



Step 9. On the Cisco Nexus 1000V Switch you can use the following commands for verification.

```
N1KV-Switch# show int brief

--------------------------------------------------------------------------------
Port      VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0     --           up     10.1.201.3                              1000     1500
```

```
--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/7        202     eth  access up      none                       1000
Eth3/8        201     eth  access up      none                       1000
Eth4/7        203     eth  access up      none                       1000
Eth4/8        201     eth  access up      none                       1000

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                   Speed  Protocol
Interface
--------------------------------------------------------------------------------
Po1          1     eth  pvlan  down    No operational members      auto(I)  none
Po2          1     eth  pvlan  down    No operational members      auto(I)  none

--------------------------------------------------------------------------------
Vethernet     VLAN    Type Mode   Status  Reason                   Speed
--------------------------------------------------------------------------------
Veth1         201     virt access up      none                       auto
Veth2         1       virt access up      none                       auto
Veth3         201     virt access up      none                       auto
Veth4         1       virt access up      none                       auto
Veth5         202     virt access up      none                       auto
Veth6         202     virt access up      none                       auto
Veth7         1       virt access up      none                       auto
Veth8         201     virt access up      none                       auto
Veth9         1       virt access up      none                       auto
Veth11        203     virt access up      none                       auto
Veth12        203     virt access up      none                       auto
Veth13        201     virt access up      none                       auto
Veth128       1       virt access down    nonParticipating           auto

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
control0 --           up     --                                      1000     1500
```

```
N1KV-Switch# show interface virtual

--------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
--------------------------------------------------------------------------------
Veth1       vmk3           VMware VMkernel          3   172.25.73.32
Veth2       Net Adapter 1  N1KV-active              3   172.25.73.32
Veth3       Net Adapter 2  N1KV-active              3   172.25.73.32
Veth4       Net Adapter 3  N1KV-active              3   172.25.73.32
Veth5       Net Adapter 1  DB servers               3   172.25.73.32
Veth6       Net Adapter 1  Email Server             3   172.25.73.32
Veth7       Net Adapter 1  N1KV-standby             3   172.25.73.32
Veth8       Net Adapter 2  N1KV-standby             3   172.25.73.32
Veth9       Net Adapter 3  N1KV-standby             3   172.25.73.32
Veth11      Net Adapter 1  Win7-VDI-1               4   172.25.73.33
Veth12      Net Adapter 1  Win7-VDI-2               4   172.25.73.33
Veth13      vmk2           VMware VMkernel          4   172.25.73.33
```

Procedure 6 Configuring SXP on the Nexus 1000V Switch

In this section, we will enable SXP on the Cisco Nexus 1000V Switch. We will also configure it as an SXP speaker so it can communicate SGT-IP mappings to the Cisco Nexus 7000 Switch.

Step 1. Use the following commands to enable and configure CTS on the Cisco Nexus 1000V Switch.

```
feature CTS
cts device tracking
cts interface delete-hold 60
```

Note: If you cannot enable the ***feature CTS*** command, use the ***svs switch edition advanced*** command first.

Step 2. Next, configure SXP on the Cisco Nexus 1000V Switch using the following commands.

```
cts sxp enable
cts sxp default password 7 fewhg123
cts sxp connection peer 10.1.201.2 source 10.1.201.3 password default mode
listener vrf management
```

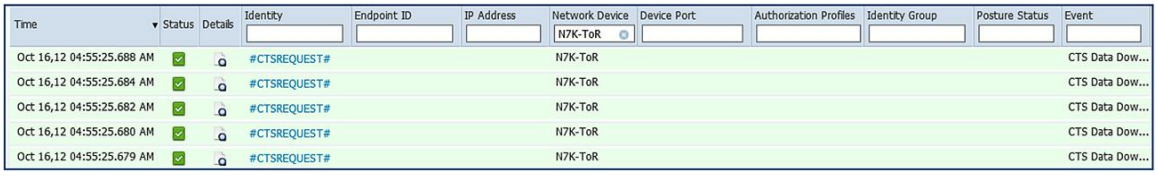
Step 3. The SXP connection to the Cisco Nexus 7000 Switch should now be connected. Verify it using the following command.

```
N1KV-Switch# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
10.1.201.2      management      listener        speaker         connected

N7K-EoR# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
10.1.201.3      default         speaker         listener        connected
```

Step 4. If the VMs are powered up and the port-profiles are being used, the Cisco Nexus 1000V Switch will be aware of the SGT mappings. The IP SGT mapping will also be shared with the Cisco Nexus 7000 Switch. Verify it using the following commands.

```
N1KV-Switch# show cts role-based sgt-map
IP ADDRESS          SGT             VRF/VLAN        SGT CONFIGURATION
10.1.202.10         10              vlan:202        Learned on interface:Vethernet5
10.1.202.20         12              vlan:202        Learned on interface:Vethernet6
10.1.203.10         5               vlan:203        Learned on
interface:Vethernet11
10.1.203.20         13              vlan:203        Learned on
interface:Vethernet12


N7K-EoR# show cts role-based sgt-map
IP ADDRESS          SGT             VRF/VLAN        SGT CONFIGURATION
10.1.202.10         10              vrf:1           Learned from SXP
peer:10.1.201.3
10.1.202.20         12              vrf:1           Learned from SXP
peer:10.1.201.3
10.1.203.10         5               vrf:1           Learned from SXP
peer:10.1.201.3
10.1.203.20         13              vrf:1           Learned from SXP
peer:10.1.201.3
```

Step 5. Since the Cisco Nexus 7000 Switch has learned the SGT-IP mappings, it will query ISE and download policies for each tag it knows. You will see multiple CTS requests in the ISE Live authentication log.



Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
						N7K-ToR					
Oct 16,12 04:55:25.688 AM	✓		#CTSREQUEST#			N7K-ToR					CTS Data Dow...
Oct 16,12 04:55:25.684 AM	✓		#CTSREQUEST#			N7K-ToR					CTS Data Dow...
Oct 16,12 04:55:25.682 AM	✓		#CTSREQUEST#			N7K-ToR					CTS Data Dow...
Oct 16,12 04:55:25.680 AM	✓		#CTSREQUEST#			N7K-ToR					CTS Data Dow...
Oct 16,12 04:55:25.679 AM	✓		#CTSREQUEST#			N7K-ToR					CTS Data Dow...

Step 6. Verify the successful download of policies on the Cisco Nexus 7000 Switch using the following commands.

```
N7K-EoR# show cts role-based policy

sgt:5
dgt:10  rbacl:Deny IP
        deny ip

sgt:5
dgt:12  rbacl:Allow_WEB
        permit tcp dst eq 80
        permit tcp dst eq 443
        permit icmp
        deny ip

sgt:7
dgt:10  rbacl:Permit IP
        permit ip

sgt:8
dgt:10  rbacl:Permit IP
        permit ip

sgt:10
dgt:5   rbacl:Deny IP
        deny ip

.
.
.
```

Step 7. The enforcement of SGACLs can be tracked using the commands below.

```
N7K-EoR(config)# cts role-based counters enable

N7K-EoR# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: 10/16/2012 at 12:12:02 PM

sgt:5 dgt:10    [2]
rbacl:Deny IP
        deny ip [2]

sgt:5 dgt:12    [3]
rbacl:Allow_WEB
        permit tcp dst eq 80    [0]
        permit tcp dst eq 443   [0]
        permit icmp     [3]
        deny ip [0]

sgt:7 dgt:10    [0]
rbacl:Permit IP
        permit ip       [0]

sgt:8 dgt:10    [0]
rbacl:Permit IP
        permit ip       [0]

sgt:10 dgt:5    [6]
rbacl:Deny IP
        deny ip [6]

sgt:10 dgt:12   [0]
rbacl:Permit IP
        permit ip       [0]

sgt:12 dgt:5    [3]
rbacl:Permit IP
        permit ip       [3]
```

Configure the Cisco ASA 5500 Adaptive Security Appliance

Procedure 7 Adding the Cisco ASA to ISE as a NAD and Generating a PAC

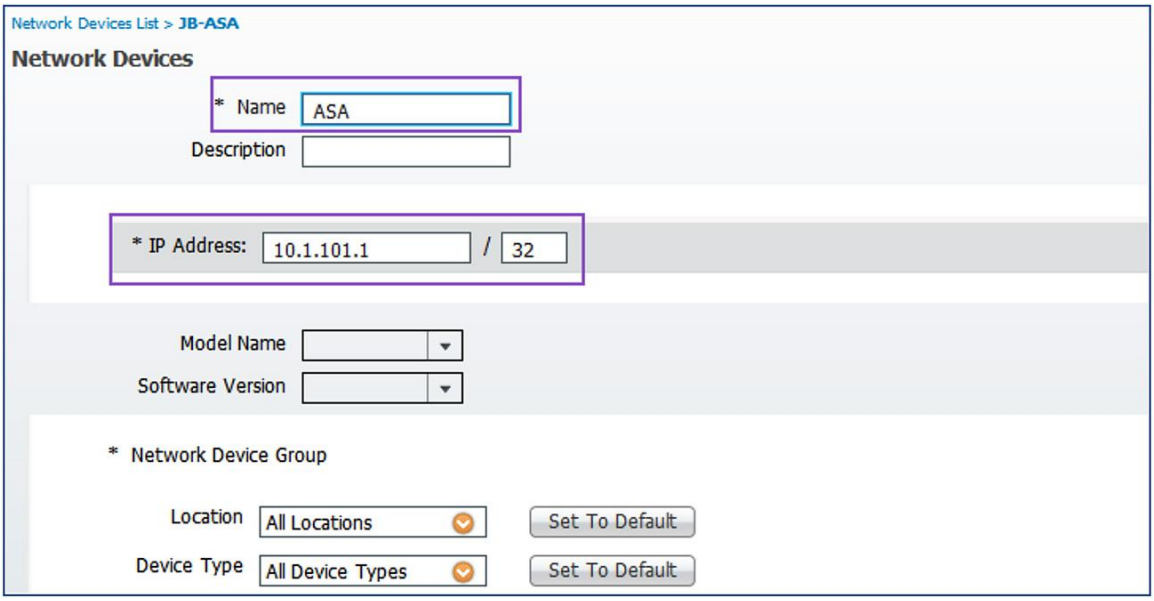
Step 1. From the ISE dashboard, navigate to **Administration → Network Resources → Network Devices**.

Step 2. Click the Add **button**.

Step 3. In the Network Devices screen fill in the text boxes for **Name**.

Note: Match the hostname on the CLI or Cisco Adaptive Security Device Manager (ASDM) of the ASA with this name. This name is used to validate the SGT Name Table download requests.

Step 4. Fill in the **IP Address** of the ASA interface with the best route to ISE.



Step 5. Select the **SGA Attributes** checkbox. This expands the SGA attributes of the Network Device definition. Select **Use Device ID for SGA Identification** if the **Name** above matches the hostname in the CLI or ASDM of the ASA.

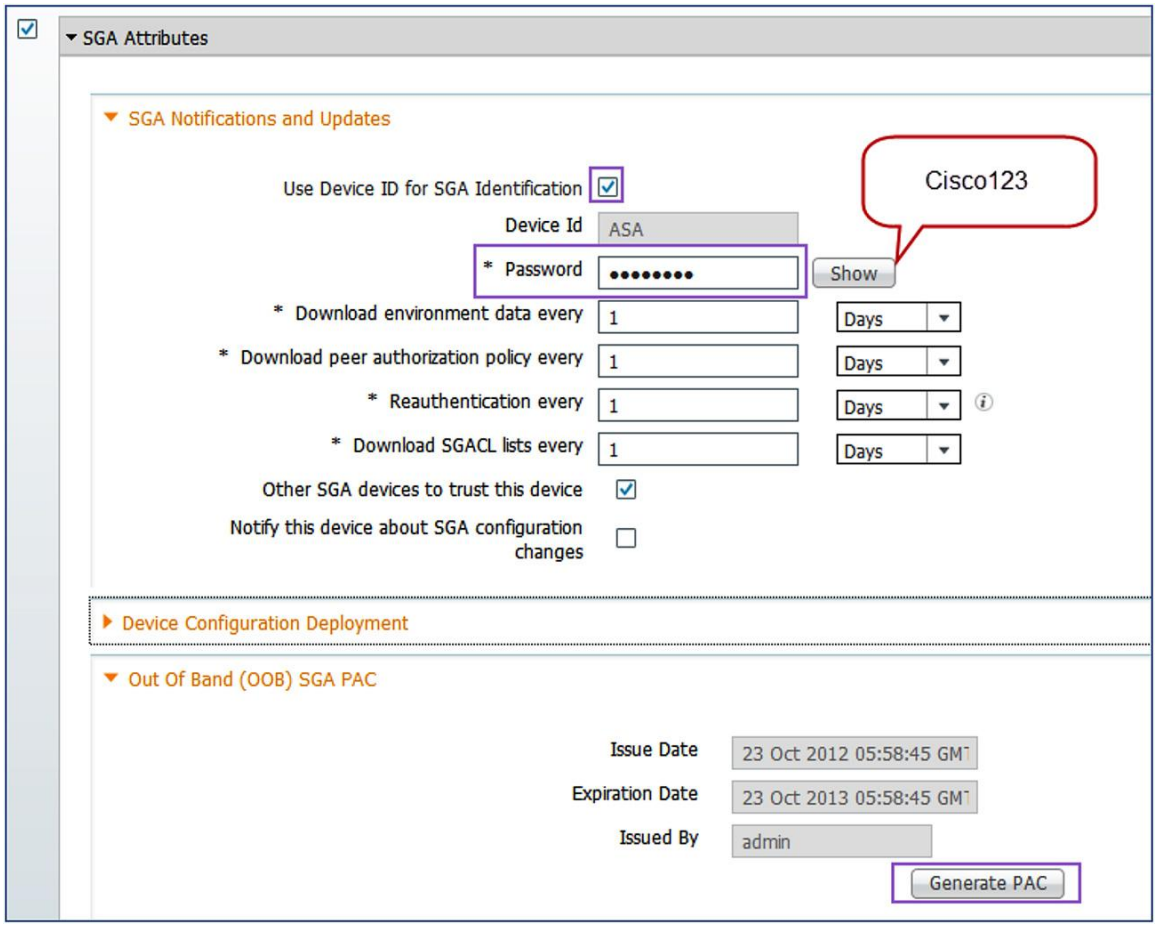
Step 6. Enter the shared secret used for SGA communications in **Password**. This will match the RADIUS shared secret in the ASDM and ASA definitions.

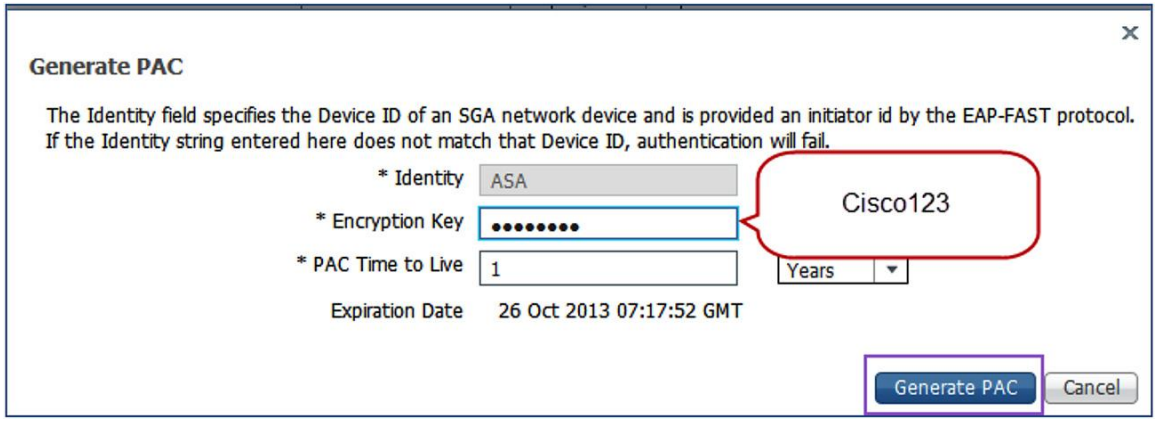
Step 7. Scroll to the bottom of the Network Device screen, expand the **Out of Band PAC (OOB) SGA PAC** section, and click the button, **Generate PAC**.

Step 8. Fill in the text boxes for **Identity**, **Encryption Key**, and **PAC Time to Live**.

Step 9. Generate the PAC and save the file.

Step 10. Click **Save**.





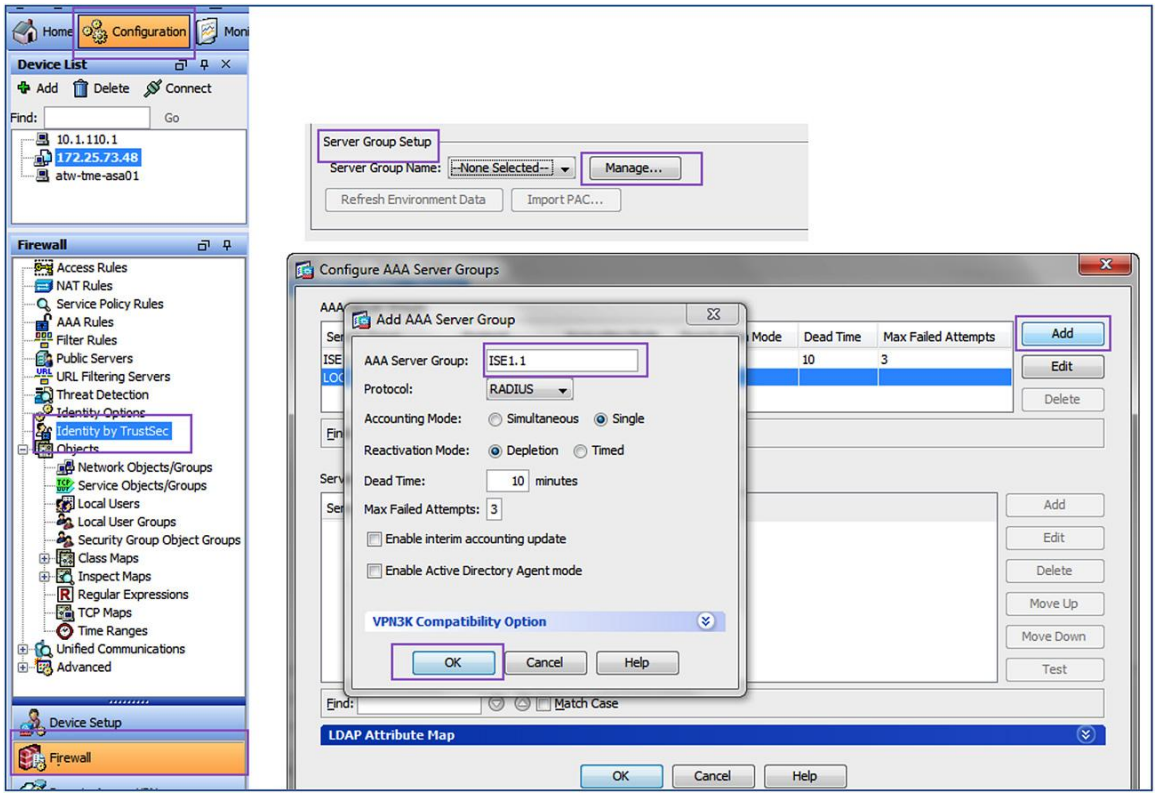
Procedure 8 Add ISE as a RADIUS server and Import PAC using ASDM

Step 1. Navigate in the ASDM to **Configuration → Firewall → Identity by TrustSec**.

Step 2. Click the **Manage** button in the **Server Group Setup** area.

Step 3. Under AAA Server Groups click the **Add** button.

Step 4. In pop-up form fill in the text box for AAA Server Group with **ISE1.1** and click **OK**.

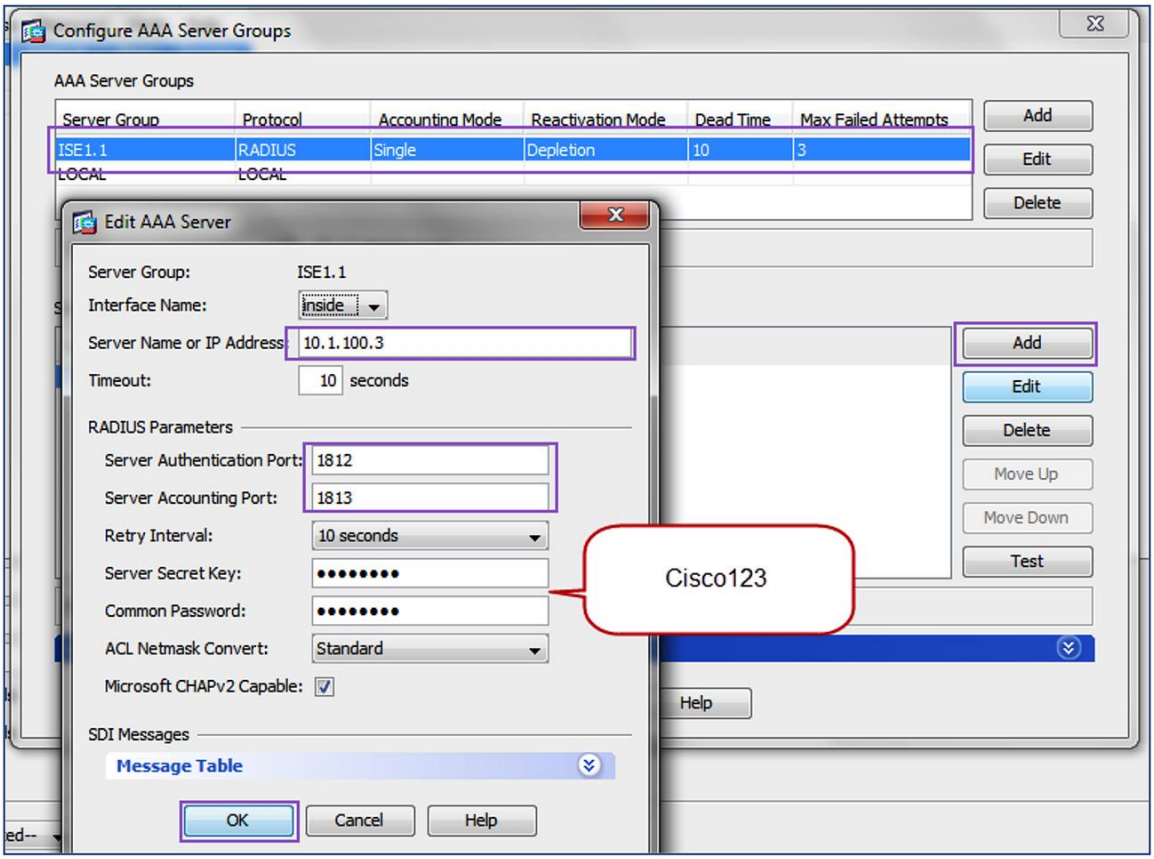


Step 5. Highlight ISE 1.1 in **AAA Server Groups** list, then go to the **Servers** in the selected group box and select **Add**.

Step 6. Define the Server **Name or IP address** of the ISE server.

Step 7. Define the **Server Secret Key** and the **Common Password** in the panel. This should match the shared secret key used earlier to define the ASA in ISE.

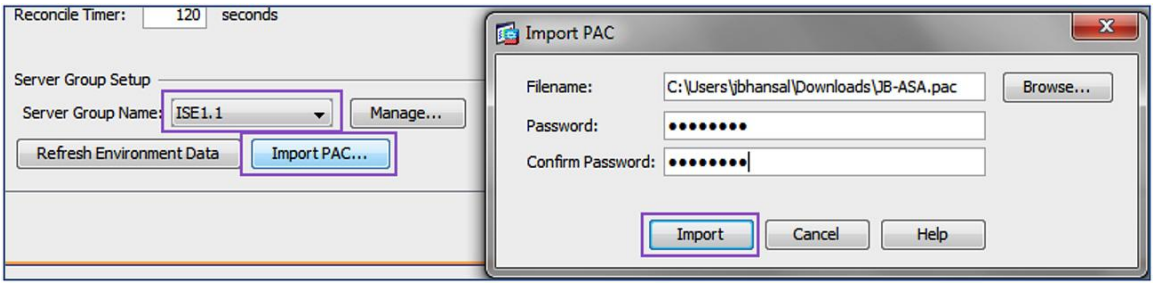
Step 8. Click **OK** for the **Add AAA Server** panel.



Step 9. Click **OK** for the **Configure AAA Server Groups** panel.

Step 10. Select **Import PAC**.

Step 11. Select the SGA PAC file from the previous steps. Enter or confirm the password that was referred to as **Encryption Key** in the ISE SGA PAC creation.



Step 12. Verify that the PAC information has been successfully imported.

```
ASA# show cts pac

  PAC-Info:
    Valid until: Oct 23 2013 05:58:45
    AID:         fcb3077b3fd73ae45e0cef38447641c9
```

```
    I-ID:        JB-ASA
    A-ID-Info:   ISE
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b000030001000400010fcb3077b3fd73ae45e0cef38447641c900060094000301
    004abb7d1f18620591b2eda99927ce2006000000135085aacb00093a8014f446f86b97
    e2279581984fb08ff08ceba93836783d73c7a7c576560373ea0fa5db3f199c4c3cce9b
    7ddfade9d8d6e3172032a61fd8d4602fc6043f199e83be12c1b4d839d73c2c9839ac02
    d02b3840c94f124163eb46ef6e88b981e868fa8598d3a04e3902398eeaf2527608d833
    bc95c099f0
```

```
ASA# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          20:51:27 UTC Oct 25 2012
Env-data expires in:       0:21:28:07 (dd:hr:mm:sec)
Env-data refreshes in:     0:21:18:07 (dd:hr:mm:sec)
```

Step 13. Verify the successful download of the SGT Table using the ASA CLI. This can also be verified from ASDM by navigating to **Monitoring →Firewall →Identity by TrustSec → Environmental Data**.

```
ASA# show cts environment-data sg-table

Security Group Table:
Valid until: 20:51:27 UTC Oct 26 2012
Showing 14 of 14 entries

SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
SGT_DB_Server                        10     unicast
SGT_Device                            2     unicast
SGT_Engg_Server                       4     unicast
SGT_WEB_Server                       12     unicast
Unknown                               0     unicast
```

Procedure 9 Configure SXP on the Cisco ASA

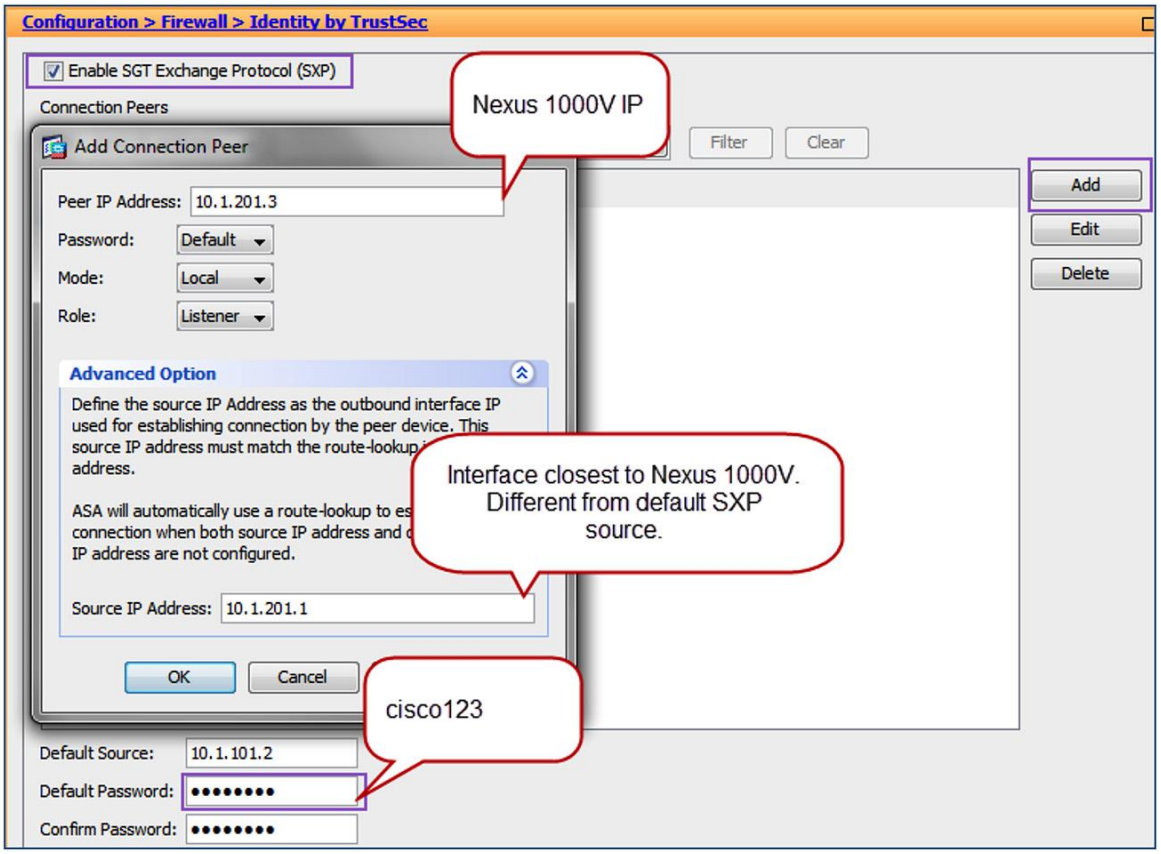
Step 1. On the ASDM, navigate to **Configuration → Firewall → Identity by TrustSec**.

Step 2. Click the checkbox for **Enable SGT Exchange Protocol (SXP)**.

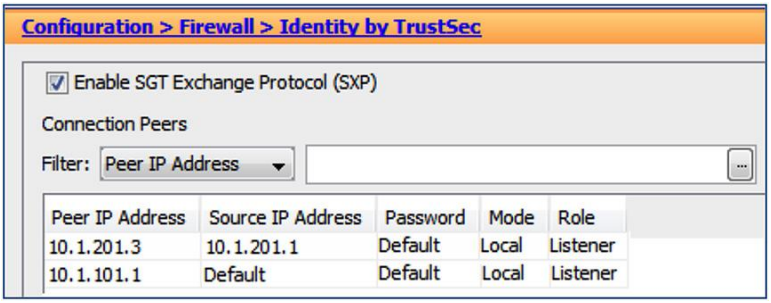
Step 3. Click the **Add** button under **Connection Peers**.

Step 4. Define the Cisco Nexus 1000V IP address, and set the **Mode** as **Local** and **Role** as **Listener**.

Step 5. Click **OK**.



Step 6. Repeat the process for the Cisco Nexus 7000. You should have two SXP peers defined now.



Step 7. Define the Cisco ASA as an SXP peer on the Cisco Nexus 1000V and the Cisco Nexus 7000 using the commands below.

```
N1KV-Switcth(config)#cts sxp connection peer 10.1.201.1 source 10.1.201.3
password default mode listener vrf management



N7K-DIST(config)#cts sxp connection peer 10.1.101.2 source 10.1.101.1 password
default mode listener
```

Step 8. Verify that both SXP connections have been established from the Cisco ASA CLI using the commands below. You can also verify from ASDM by navigating to **Monitoring → Properties → Identity by TrustSec → SXP Connections**.

```
ASA# show cts sxp connections brief
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local  IP  : 10.1.101.2
Reconcile period   : 120 secs
Retry open period  : 120 secs
Retry open timer   : Not Running
Total number of SXP connections: 2
Total number of SXP connections shown: 2
-------------------------------------------------------------------------------
Peer IP          Local IP         Conn Status       Duration (dd:hr:mm:sec)
-------------------------------------------------------------------------------
10.1.101.1       10.1.101.2       On                1:14:54:46
10.1.201.3       10.1.201.1       On                3:09:38:19
```

Procedure 10 Configure the SGFW policy through ASDM

Step 1. From the ASDM dashboard, navigate to **Configuration → Firewall → Access Rules**.

Step 2. Select the **Inside** interface and right-click **Add Access Rule**.

Step 3. Under **Source Criteria** select the **Security Group** inspector box. This brings up a **Browse Security Group** dialogue.

Step 4. Scroll the bottom list of SGT names and numbers from ISE and select the **SGT_WEB_Server**. Select the **Add** button in the middle of the page. Similarly, add the **SGT_DB_Server**.

Step 5. Select **OK** to return to the **Add Access Rule** dialogue.

Step 6. Repeat steps 4 and 5 for the **Destination Criteria** and use the **SGT_Engg_Server** for the destination.

Step 7. For simplicity of setup leave the destination service of **ip** for this example.

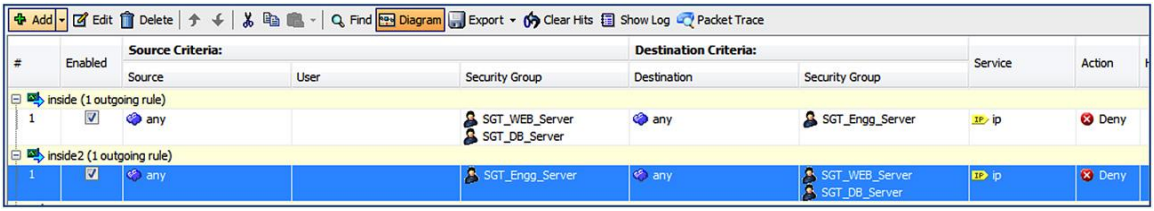
Step 8. Click **OK** to finish the access rule.

Step 9. Click **Apply** to add this configuration to the ASA.

Step 10. Repeat steps 1-9 for the combinations of SGT/DGT and SGT/IP shown below.

Step 11. Example SGFW Access Rules Goals.

Source Group	Destination Group/IP	Permission
SGT_WEB_Server, SGT_DB_Server	SGT_Engg_Server	Deny
SGT_Engg_Server	SGT_WEB_Server, SGT_DB_Server	Deny



Step 12. Verify enforcement of the SGFW rules.

```
ASA# show access-list
---OUTPUT MODIFIED---


  access-list inside_access_out line 1 extended deny ip security-group name
SGT_
WEB_Server(tag=12) any4 security-group name SGT_Engg_Server(tag=4) any4
(hitcnt=                                                              28628)
0xd0de40a1
```

For More Information

Cisco TrustSec How-To Guides: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html.

Cisco ISE 1.1.1 User Guide: http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_admin.html.

Cisco Nexus 1000V Series: http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html.

Cisco Nexus 7000 Series: http://www.cisco.com/en/US/products/ps9402/tsd_products_support_series_home.html.

VMware View 5.1: http://www.vmware.com/support/pubs/view_pubs.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-728628-00 06/13