Access Control Using Security Group Firewall

Introduction

Traditional firewalls perform access control based on predefined IP addresses, source and destination ports, and protocol types. However, with businesses reaching outside the traditional boundaries of the enterprise and with a workforce that is continuously mobile, security solutions must be able to allow access to resources from anywhere, at any time. Firewall administrators are facing challenges managing and maintaining access rules based on source and destination IP addresses that are always changing in this dynamic landscape.

To remove the dependency on IP, Cisco® Security Group Firewall (SGFW) takes a next-generation approach to filtering decisions by allowing access rules and security policies to be based on security groupings built from a combination of attributes, such as role, device type, location, time of day, and/or posture.

For example, a security group named “Mobile Sales” could represent all salespersons in an organization that are using a mobile device to access network resources. Likewise, a security group named “Engineering Servers” could represent data center servers that are for engineering use only. SGFW allows the administrator to then define a rule to deny traffic between several Mobile Sales users and several Engineering Servers. Representing users and devices with security groups makes access control easier to manage, maintain, and scale.

Security Group Firewall Overview

The benefits of using security groups to define policy are best described with the basic firewall example shown in Figure 1. In the example, firewall object groups, such as “MA,” are used to logically group a list of subnets based on location. The access rules are divided into three sets. The first set of rules, in black, permits communication between three source objects and three destination objects. The second set of rules, in blue, shows the additions necessary if just one new source object is added. The third set of rules, in red, shows the additions required when one new destination object is added. As you can see, the list of rules grows longer and more complex as objects are added.

Figure 1. Traditional Firewall Rules

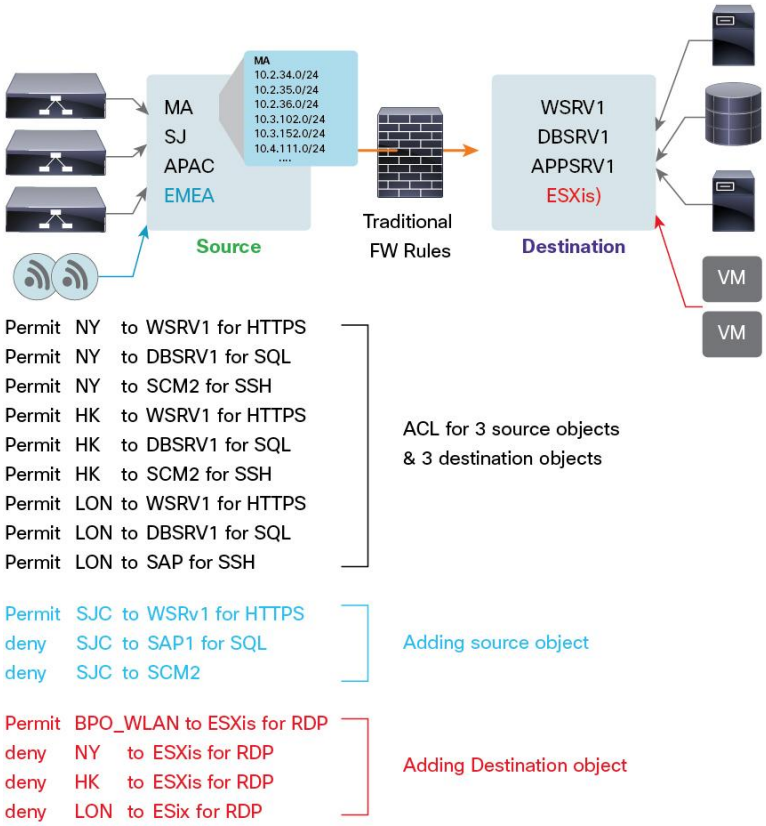
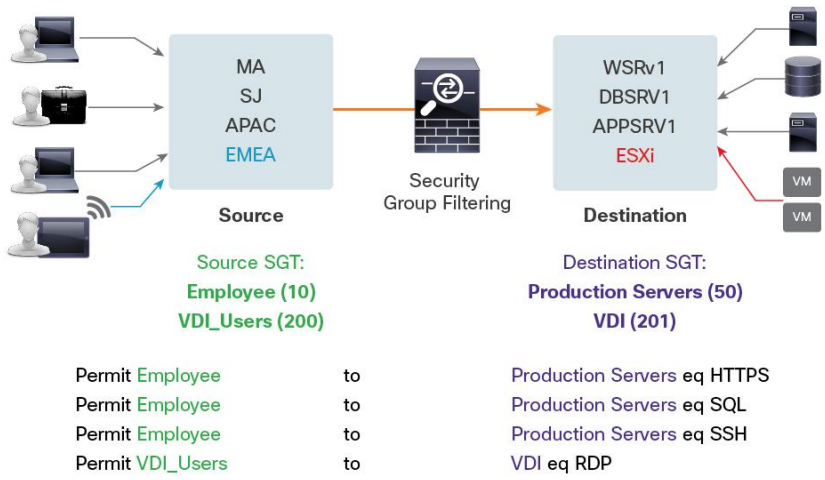


Figure 2 shows how the same type of access is defined in a Security Group Firewall (SGFW).

Figure 2. Security Group Firewall



Rather than defining access rules by networks or static IPs, access is governed by user or device group memberships. By using these member roles, the addition of a new user or server requires no change to the existing rules - the administrator just needs to add the user or server to the role.

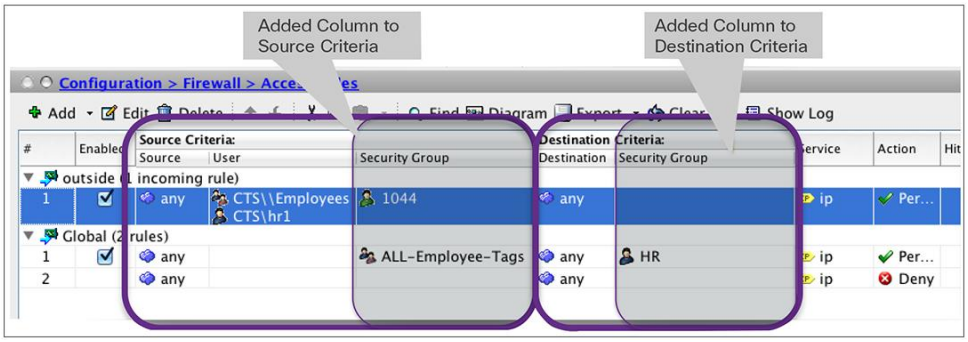
With SGFW:

- It takes less operational effort and is faster to deploy new services.
- Policy stays with user/server group regardless of location or topology.
- Access is simple to define, manage, and audit.

Security Group Firewall on the ASA

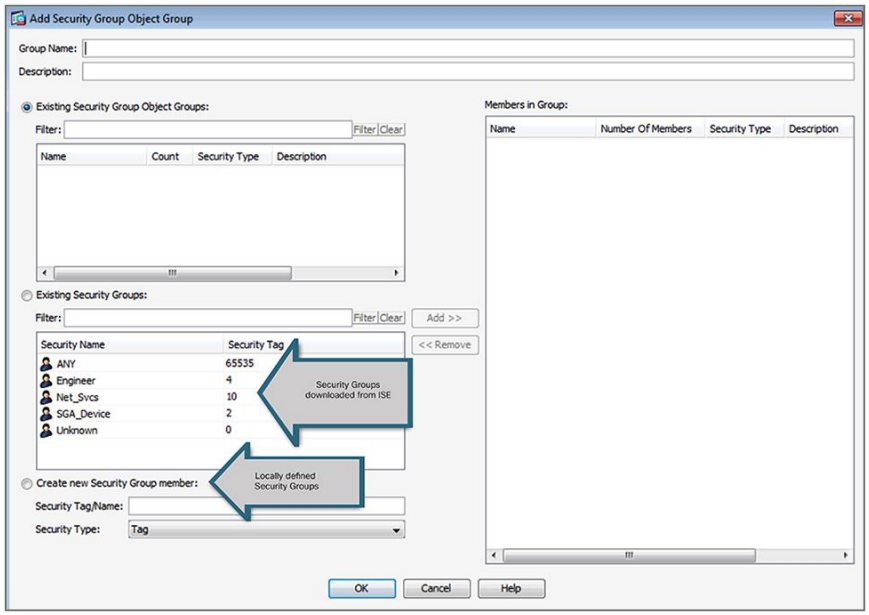
Beginning with Cisco ASA Software Release 9.0.1, the ASA firewall gains SGFW functionality. Policy in the firewall has been expanded to include source and destination security groups in the decision. As you can see in Figure 3, there is a new Security Group column in the Source Criteria and Destination Criteria sections.

Figure 3. Access Rules with Security Groups



A security group can either be locally defined on the ASA firewall or can be configured on the Identity Services Engine (ISE). Figure 4 shows the process on the ASA firewall.

Figure 4. Security Group on ASA Firewall



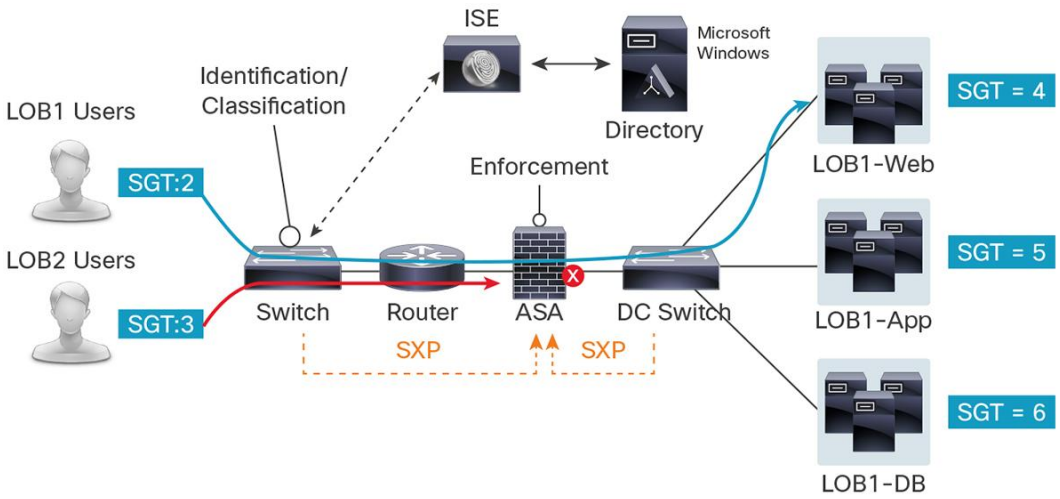
There are added benefits when configuring security groups on ISE, including:

- **Increased visibility:** Apply context (combination of AD group membership, device type via profiling, location, time, and/or access method) to rules.
- **Ease of deployment:** Dynamically assign Security Group Tags to users/devices as they authenticate through ISE at the access layer.
- **Central management:** Security groups defined on ISE are applicable to Cisco TrustSec® aware network devices (switches, routers, firewalls), not just the ASA firewall.

Deployment Scenarios

Controlling Campus to Data Center Traffic Overview

Figure 5. Campus to Data Center Example



LOB1 and LOB2 users are classified based on their context. The users are assigned a security group tag (SGT) that represents their unique classification. The switch will then bind the endpoint IP address to the SGT, and communicate this binding information to enforcement points (in this case, the ASA firewall). The data center servers can be classified via SGTs as well. With data center servers, the SGT to IP address binding is configured manually on the data center switch. The data center switch communicates this binding table to the ASA firewall via SGT Exchange Protocol over TCP (SXP). In this way you can define ASA firewall policy using both source and destination security groups. The ASA firewall maintains the source IP address to the SGT binding table via SXP so that the ASA firewall can filter traffic from a specific source IP address based on SGT.

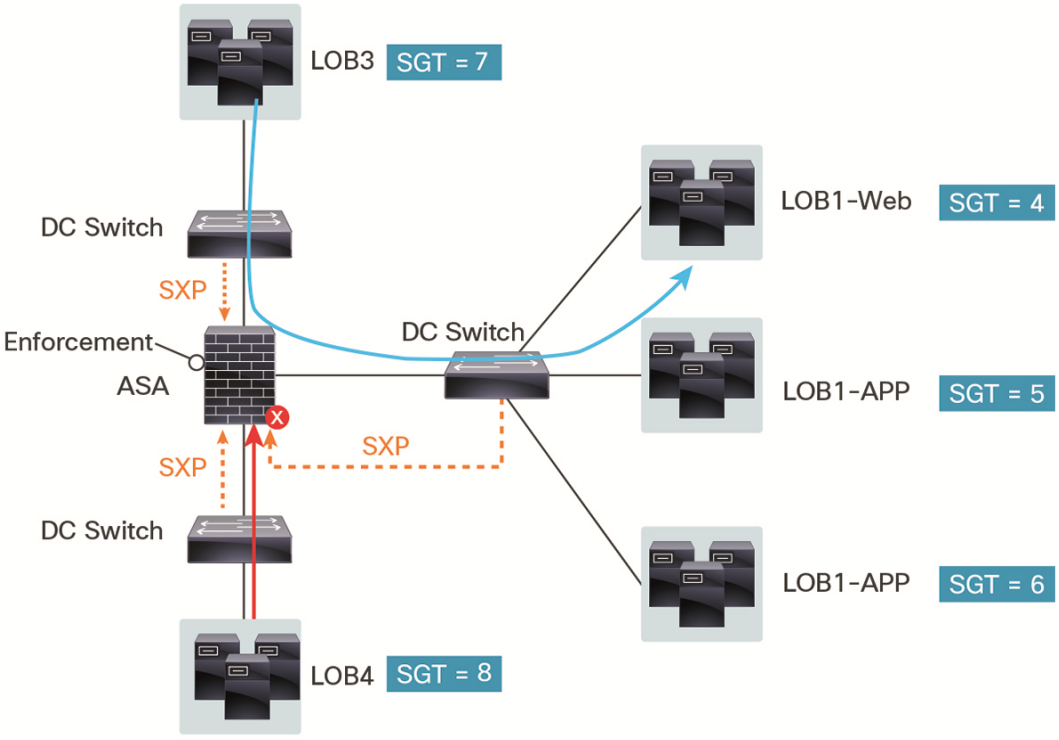
Server-to-Server Data Center Classification and Enforcement

The second use case is that the ASA firewall will be providing firewall services between the servers using security groups within the data center. Instead of using the IP addresses of servers to segment traffic from one server group to others, security groups can be used to logically group those servers based on function and policy, then filter traffic between servers. Using security groups on the ASA firewall dramatically simplifies and automates security policy maintenance and operation - an operator does not need to take care of individual server IP addresses in their policy. They need to assign a server IP address to a specific security group. When a server IP address changes (e.g., decommission of server), the server IP address to security group can simply be removed from policy.

The ASA firewall filters traffic between different LOBs as they are grouped into logical interfaces (ASA interfaces). SGT/DGT-based filtering is used between Interface-Inside and Interface-LOB3, but communication will fall back to SGT/IP- or IP/DGT-based filtering between Interface-Inside and Interface-LOB4. Sample policies for this interface-to-interface communications are included.

Figure 6 shows how SGFW will be implemented between interfaces. This specific example shows how ASA SGFW will allow LOB3 to speak to LOB1_Web, but deny access to LOB2 and other LOB1 servers, since LOB1 and LOB2 are in the same security context and would not have policy applied to their communications by the ASA SGFW. The "Server Segmentation Using SGA" Cisco TrustSec 2.1 guide outlines the permissions that would be in place for those LOB communications.

Figure 6. Data Center Interface-to-Interface SGFW



SXP Compatibility and Caveats

NAT

NAT cannot be used for SXP peer communication. SXP conveys IP→SGT mappings to enforcement points in the network. If the access layer switch belongs to a different NAT domain than the enforcing point, the IP→SGT map it uploads will be meaningless and an IP→SGT database lookup on the enforcement device will yield nothing. This means it will not be possible to apply identity-based (security-group-aware) ACLs on the enforcement device.

“Through the box” SXP

Through-the-box transit SXP connections will break if NAT is caused by TCP sequence number randomization and TCP option 19 stripping. In order to allow these connections, the following configuration is necessary:

```
class bypass
                set connection random-sequence-number disable
                set connection advanced-options sxp-tcp-map
tcp-map sxp-tcp-map
                tcp-options range 19 19 allow
```

Multi-Context Mode

Both single-context and multi-context modes are supported. Each context maintains its own configurations, databases, credentials, and environment data.

Firewall Mode

Both routed and transparent modes are supported. In transparent mode, each user context typically has an inside interface, an outside interface, and a management interface. We can assign an IP address to the management interface, or the inside and outside interfaces can be grouped into a bridge-group virtual interface (BVI) and we can assign an IP address to the BVI. This IP address should be used in the SXP communication with peer devices.

High Availability

Both active-standby and active-active modes are supported. When a standby unit takes over as active, security-group-based policies can be seamlessly enforced through information synchronized from the previously active unit. The new active unit will then establish SXP connections and refresh its IP-SGT bindings. The environment data and the security group table will also be refreshed. Detailed SGA HA considerations are included in the Appendix.

Clustering

Clustering is supported. The master unit will contact ISE and obtain environment data, which is then replicated to all units in the cluster via reliable messaging. Security-group-based policies are replicated as part of the configuration sync. The master unit establishes SXP connections and learns IP-SGT mappings. This SXP mapping database is replicated to all units. Thus security-group-based policies can be enforced on the slave units. Detailed SGA HA considerations are included in the Appendix.

SXP Scalability Considerations

The number of SXP connections and IP-SGT mappings varies per platform. Please refer to Table 1.

Table 1. SXP Connections and IP-SGT Mappings

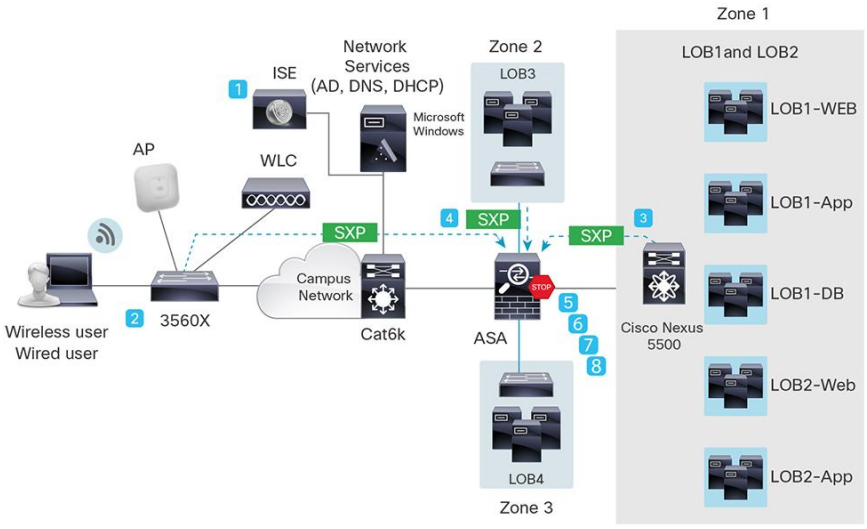
ASA Platform	SXP Connections	IP-SGT Mappings
ASA5505	10	250
ASA5510	25	1000
ASA5520	50	2500
ASA5540	100	5000
ASA5550	150	7500
ASA5580-20	250	10,000
ASA5580-40	500	20,000
ASA5585-SSP10	150	18,750

ASA Platform	SXP Connections	IP-SGT Mappings
ASA5585-SSP20	250	25,000
ASA5585-SSP40	500	50,000
ASA5585-SSP60	1000	100,000

Configuration

Figure 7 shows [[complete sentence]].

Figure 7. SGFW Configuration Flow



0. Assumption: ISE and switches are configured for baseline Cisco TrustSec (802.1X, MAB, WebAuth) on access layer device; Cisco Catalyst® 3560-X.
1. Configure security groups in ISE 1.1.1 and SGT assignment.
2. Configure SXP connection Catalyst 3560-X switch to exchange IP-to-SGT binding table for campus to data center use case.
3. Configure SXP connection Interface-Inside-Nexus® 5500 to exchange IP-to-SGT binding table for data center server to server use case.
4. Configure SXP connection Interface-LOB3-Catalyst 3750 to exchange IP-to-SGT binding table for data center server to server use case.
5. Configure ISE and ASA to communicate SGT Name/Number Table:
   a. Configure ASA firewall as an SGA device in ISE.
   b. Create/export SGA PAC from ISE to file.
   c. Import SGA PAC into ASDM from file and validate SGT Name/Number Table download.
6. Configure the ASA firewall for SXP to campus and data center access switches:
   a. Configure SXP connection between ASA firewall and campus Catalyst 3560-X to exchange IP-to-SGT binding table for campus to data center use case.
   b. Configure SXP connection between ASA firewall and the Interface-Inside-Nexus 5500 to exchange IP-to-SGT binding table for data center server to server use case.

c. Configure SXP connection between ASA firewall and the Interface-LOB3-Catalyst 3750 to exchange IP-to-SGT binding table for data center server to server use case.

7. Configure Cisco ASA SGFW policy via ASDM. Since this guide is intended to be an optional companion guide for Cisco Nexus 5500 SGT/SGACL filtering, the example policies synchronize basic connectivity policy between the ISE and the ASDM/ASA SGFW policy. Example policies are included in configuration examples.
8. Validate that Cisco ASA SGFW policies are being invoked via syslog monitoring and policy hit count.

Configuring Security Groups

In this section, we will configure the security groups in ISE 1.1.1 that are used as examples in this guide. The following groups will be created:

- **LOB1_Users:** Users in Line of Business 1 that are fully compliant with corporate software policy
- **LOB1_Users_Noncompliant:** A user in Line of Business 1 who is not compliant with corporate software policy
- **LOB2_Users:** Users in Line of Business 2 that are fully compliant with corporate software policy
- **LOB2_Users_Noncompliant:** A user in Line of Business 2 who is not compliant with corporate software policy
- **SGA_Device:** Networking devices that support SGT/SGACL
- **Network_Services:** Servers that are used for basic networking like Active Directory, ISE, DHCP, DNS
- **LOB1-Web:** Line of Business 1 Web Servers
- **LOB1-App:** Line of Business 1 Application Servers
- **LOB1-DB:** Line of Business 1 Database Servers
- **LOB2-Web:** Line of Business 2 Web Servers
- **LOB2-App:** Line of Business 2 Application Servers
- **LOB2-DB:** Line of Business 2 Database Servers
- **LOB3_Srv:** Line of Business 3 Servers

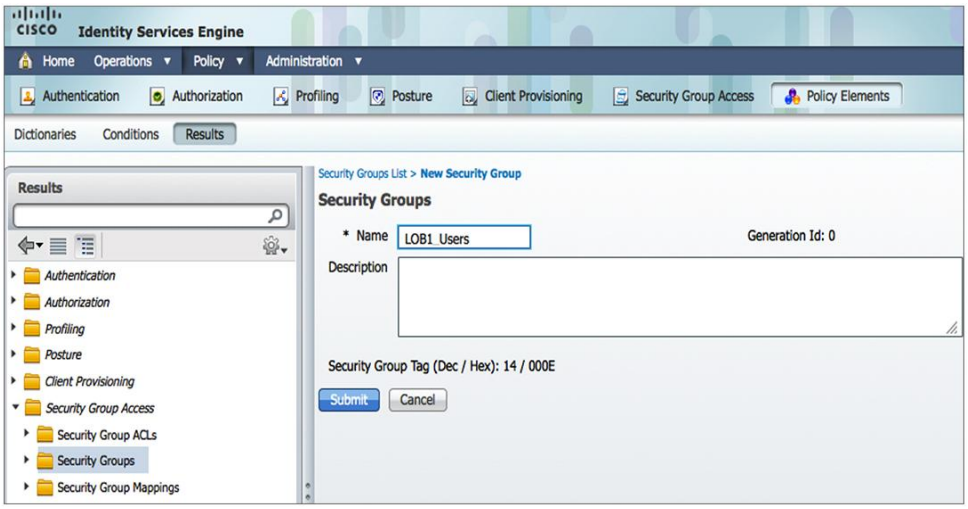
LOB4 servers will be handled via IP/network objects. They will not have an SGT associated with them, as an example of coexistence and migration from pure IP classification environments to hybrid IP and SGT classification environments.

In this document, the policy that dictates what users and servers are able to talk to one another is handled by the ASA SGFW. The notable exception to this is that LOB1 and LOB2 are in the same security interface and would not have policy applied to their communications by the ASA SGFW. Instead, please refer to the "Server Segmentation Using SGA" document.

Step 1. In the web browser, navigate to **Policy → Policy Elements → Results →Security Group Access → Security Groups** (Figure 8)

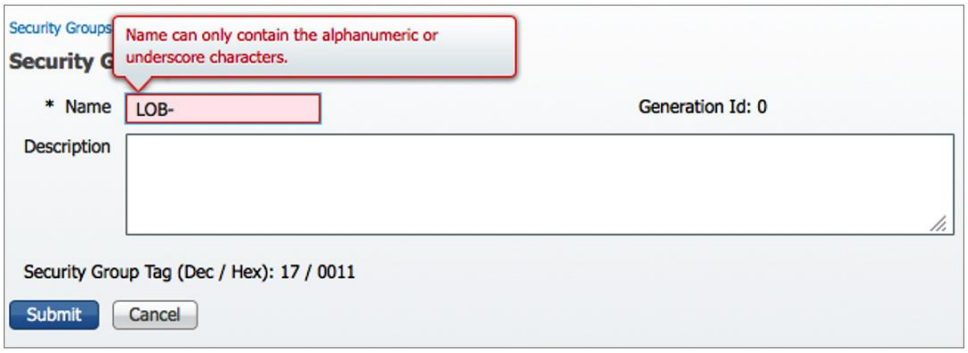
Step 2. Click Add button to add one of the example SGTs to the ISE 1.1 server

Figure 8. Creating a Security Group Tag



Troubleshooting: If there is an error in creating the SGT, you should look at the error message from ISE and try again. Typically the issue is a reversed character in the SGT name. ISE should indicate if an invalid character is being used. See Figure 9 for an example.

Figure 9. Invalid SGT Name Error



Procedure 1 SGT Assignment for Users/Devices

Step 1. Navigate to **Policy→Authorization**

Step 2. Create a new authorization policy for LOB1_Users or edit an existing LOB1_Users policy

Step 3. Under the authorization rule condition, match the Active Directory group “LOB1_Users”

Step 4. Use the authorization rule permissions select the Security Group Lob1_Users-SGT

Step 5. Repeat for all relevant SGTs that you want to use to classify users/devices (for example, LOB2_Users and the addition of posture attributes for LOB1_Users_noncompliant and LOB2_Users_noncompliant if desired)

Step 6. Figure 10 shows an example of SGT assignment in ISE and the CLI. In this example, LOB1_Users_SGT= 14/0x00E. The SGT assignment is highlighted in yellow in the CLI block in Figure 11

Figure 10. SGT Assignment in Authorization Rule Table

Figure 11. Successful User Authentication and SGT Assignment (ISE)


```
3560X#show authentication session interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  0010.1864.e5be
           IP Address:  10.1.10.101
            User-Name:  lob1comp
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
                  SGT:  000e-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A01300200000B16FFBF631B
      Acct Session ID:  0x00000BD2
              Handle:  0x59000B17

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run
```

Procedure 2 Configure SXP on Catalyst 3560-X

Configure SXP on the Catalyst 3560-X to communicate IP to SGT bindings from the campus/access layer to the ASA firewall. The 3560-X is the SXP speaker.

Step 1. Type the following commands on the 3560-X

```
3560X#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
3560X(config)#cts sxp enable
3560X(config)#cts sxp default password cisco123
3560X(config)#cts sxp connection peer 10.2.50.2 source 10.1.48.2 password default
mode peer listener
```

Step 2. Verify the SXP configuration

```
3560X#show cts sxp connections
 SXP              : Enabled
 Default Password : Set
 Default Source IP: 10.1.48.2
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------
Peer IP          : 10.2.50.2
Source IP        : 10.1.48.2
Conn status      : Pending_On
Conn version     : 2
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: default SXP password
Duration since last state change: 0:00:00:04 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

At this point, the SXP connection will be shown as Pending_On or Off since the ASA firewall has not been configured. Once Step 6a is accomplished, you should see the following output:

```
3560X#show cts sxp connections
 SXP              : Enabled
 Default Password : Set
 Default Source IP: 10.1.48.2
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------
Peer IP          : 10.2.50.2
Source IP        : 10.1.48.2
Conn status      : On
Conn version     : 2
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: default SXP password
Duration since last state change: 0:00:00:04 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

If the SXP connection fails to establish, there are several primary configuration tasks that you should verify on both sides of the SXP connection. Verify the following:

- Source interface is specified
- Default password is specified
- The role is specified properly for SXP. Each SXP connection is unidirectional and should be specified as a clear “speaker” and a clear “listener.” In this guide, the switches are always the speakers and the ASA firewall is always the listener.

Procedure 3 Configure SXP on the Nexus 5500

LOB1 and LOB2 servers are behind the Nexus 5500. In order for the ASA firewall to enforce traffic to these servers via SGTs, SXP must be configured.

Step 1. Configure the following commands on the Nexus 5500

```
nexus5k(config)# feature dot1x
nexus5k(config)# feature cts
# the above two commands are requirements to turn on SGTs on NX-OS
nexus5k(config)# cts role-based sgt-map 10.1.101.100 8
nexus5k(config)# cts sxp enable
nexus5k(config)# cts sxp default password cisco123
nexus5k(config)# cts sxp connection peer 10.2.50.2 source 10.1.97.2 password
default mode listener
nexus5k(config)# exit
```

Step 2. Verify the SXP configuration

```
nexus5k# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
10.2.50.2       default          listener       speaker         deleting
```

At this point, the SXP connection will be shown as Pending_On or deleting since the ASA firewall has not been configured. Once Step 6b is accomplished, you should see the following output:

```
nexus5k# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
10.2.50.2       default         listener        speaker         connected Duration
since last state change: 0:00:00:04 (dd:hr:mm:sec)



Total num of SXP Connections = 1
```

If the SXP connection fails to establish, there are several primary configuration tasks that you should verify on both sides of the SXP connection. Verify

- Source interface is specified
- Default password is specified

- The role is specified properly for SXP. Each SXP connection is unidirectional and should be specified as a clear “speaker” and a clear “listener.” With the NX-OS CLI for SXP peers, the “mode” always refers to the peer’s “mode.” So in this step, it is referring to the ASA firewall’s mode in the example CLI. In this guide, the switches are always the speakers and the ASA firewall is always the listener.

Procedure 4 Configure SXP on the Catalyst 3750 (LOB3)

To communicate IP/SGT bindings from the Catalyst 3750 to the Cisco ASA firewall, we need to configure an SXP connection. We are aso simplifying this guide by statically defining IP/SGT bindings in the data center.

Step 1. Enter the following commands on the Catalyst 3750

```
LOB3-3K#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
LOB3-3K(config)#cts role-based sgt-map 10.3.50.100 sgt 18
LOB3-3K(config)#cts sxp enable
LOB3-3K(config)#cts sxp default password cisco123
LOB3-3K(config)#cts sxp connection peer 10.3.50.2 source 10.3.50.3 password default
mode peer listener
LOB3-3K(config)#exit
```

Step 2. Verify the SXP connection

```
LOB3-3K#show cts sxp connections
 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------
Peer IP          : 10.3.50.2
Source IP        : 10.3.50.3
Conn status      : Off
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: default SXP password
Duration since last state change: 0:00:00:36 (dd:hr:mm:sec)
```

At this point, the SXP connection will be shown as Pending_On or Off since the ASA firewall has not been configured. Once Step 6c is accomplished, you should see the following output:

```
LOB3-3K#show cts sxp connections
 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP          : 10.3.50.2
Source IP        : 10.3.50.3
Conn status      : On
Local mode       : SXP Speaker
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:00:10 (dd:hr:mm:sec)
```

If the SXP connection fails to establish, there are several primary configuration tasks that you should verify on both sides of the SXP connection. Verify

- Source interface is specified
- Default password is specified
- The role is specified properly for SXP. Each SXP connection is unidirectional and should be specified as a clear “speaker” and a clear “listener.” In this guide, the switches are always the speakers and the ASA firewall is always the listener.

Procedure 5 Configure ASA as an SGA device in ISE

Step 1. Navigate to **Administration→Network→Resources→Network Devices**

Step 2. Click “Add”

Step 3. In the Network Devices screen (Figure 12), fill in the “Name” text box

Note: Match the hostname on the CLI/ASDM of the ASA firewall 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. Under “Password,” enter the shared secret used for SGA communications. This will match the RADIUS shared secret in the ASDM/ASA definitions so please note it.

Step 6. Click Save

The only consideration is to make sure you match the hostname on the CLI of the ASA firewall with the “Identity” text box. The identity being used is “ciscoasa”. See Figures 12 and 13.

Figure 12. ASA SGA Device Definition - Part 1

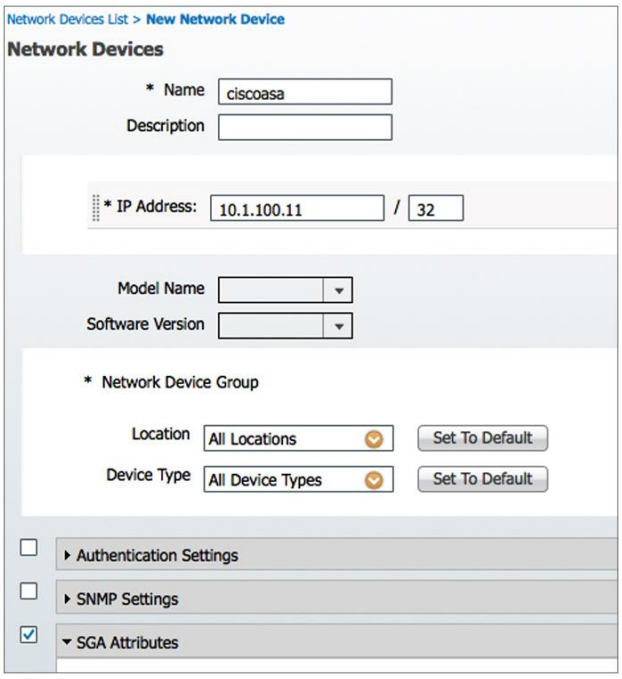
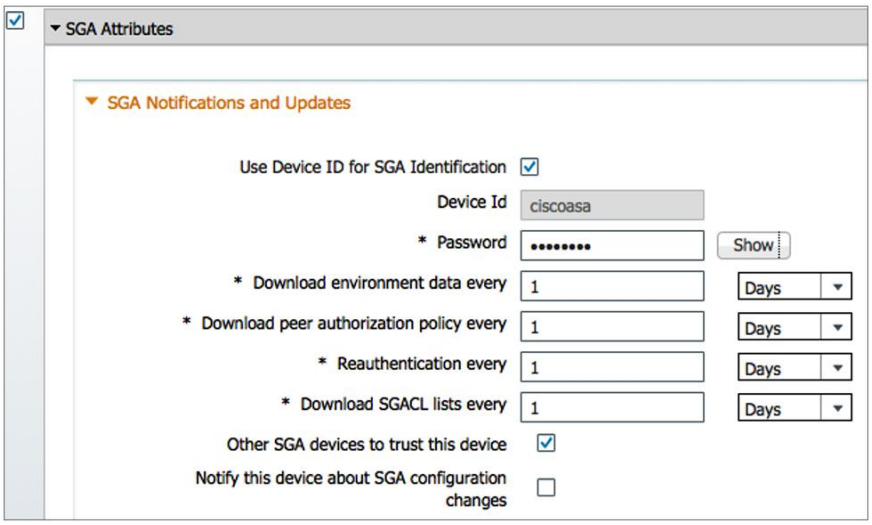


Figure 13. ASA SGA Device Definition - Part 2



Procedure 6 Create/Export SGA PAC from ISE to File

There are two ways to create and export and SGA PAC in ISE for the ASA firewall (Figures 14 and 15).

Option 1: Generate the PAC out of a generic EAP-FAST Settings panel.

Step 1. Navigate to Administration→System→Settings→Protocols→EAP-FAST→Generate PAC

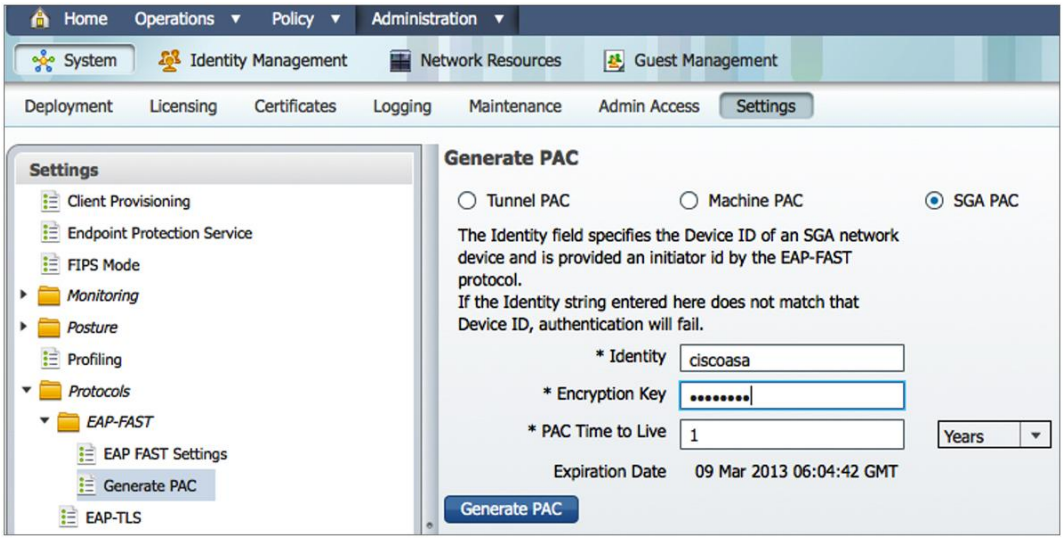
Step 2. Click “SGA PAC”

Step 3. Fill in the text boxes for “Identity,” “Encryption Key,” and “PAC Time to Live”

Step 4. Generate the PAC and save the file

Note: Make sure you match the hostname on the CLI of the ASA firewall with the “Identity” text box. In this guide, the identity being used is “ciscoasa”. See Figure 14.

Figure 14. Out of Band PAC Creation



Option 2: Creates a PAC from within the Network Devices configuration screen

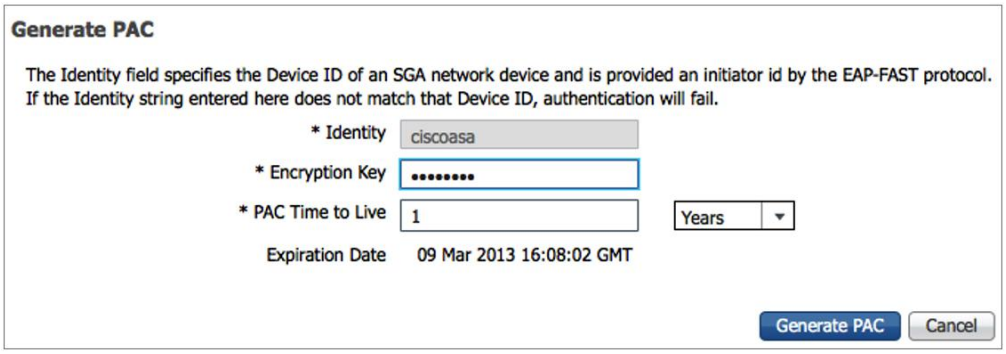
Step 1. Navigate to **Administration→Network Resources→Network Devices**

Step 2. Scroll to the bottom of the Network Device screen, expand the “Out of Band PAC (OOB) SGA PAC” section, and click “Generate PAC”

Step 3. Fill in the text boxes for “Identity,” “Encryption Key,” and “PAC Time to Live”

Step 4. Generate the PAC and save file

Figure 15. SGA PAC Provisioning from Network Devices Screen



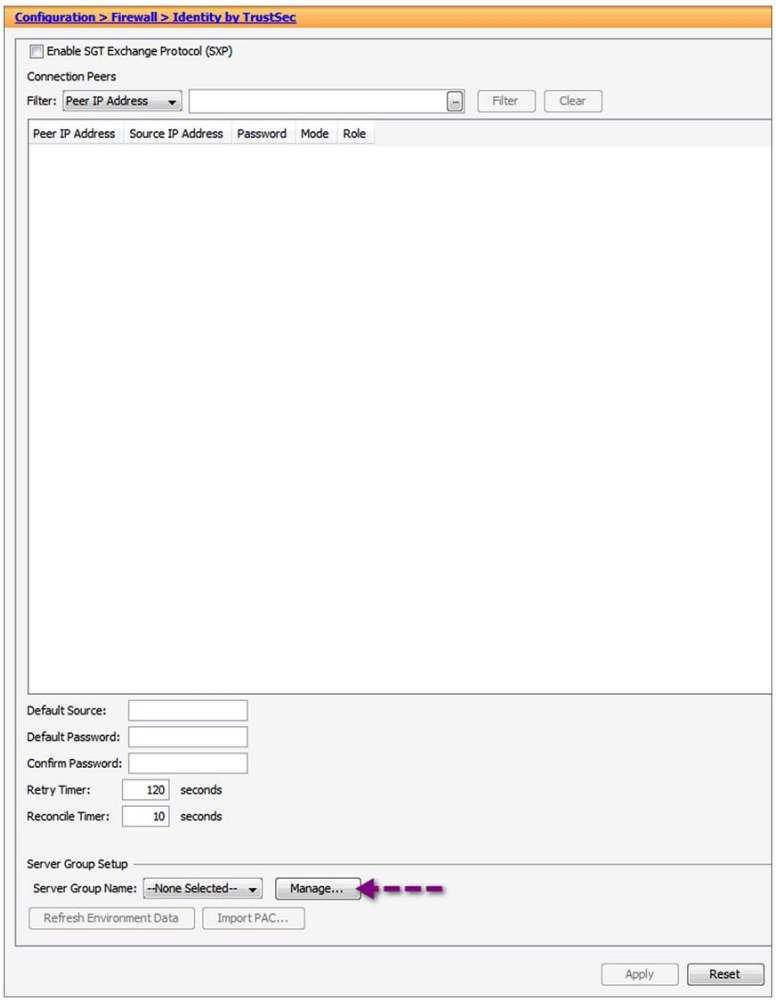
Procedure 7 Import SGA PAC File into ASDM/ASA

In the previous procedure, you generated a PAC file. This file must be installed on the ASA firewall. Once the PAC is installed, the ASA firewall will communicate securely to ISE to retrieve the environment data (security group name list).

Step 1. In ASDM, navigate to Configuration‣Firewall‣Identity by TrustSec

Step 2. In the “Server Group Setup” area, click “Manage”

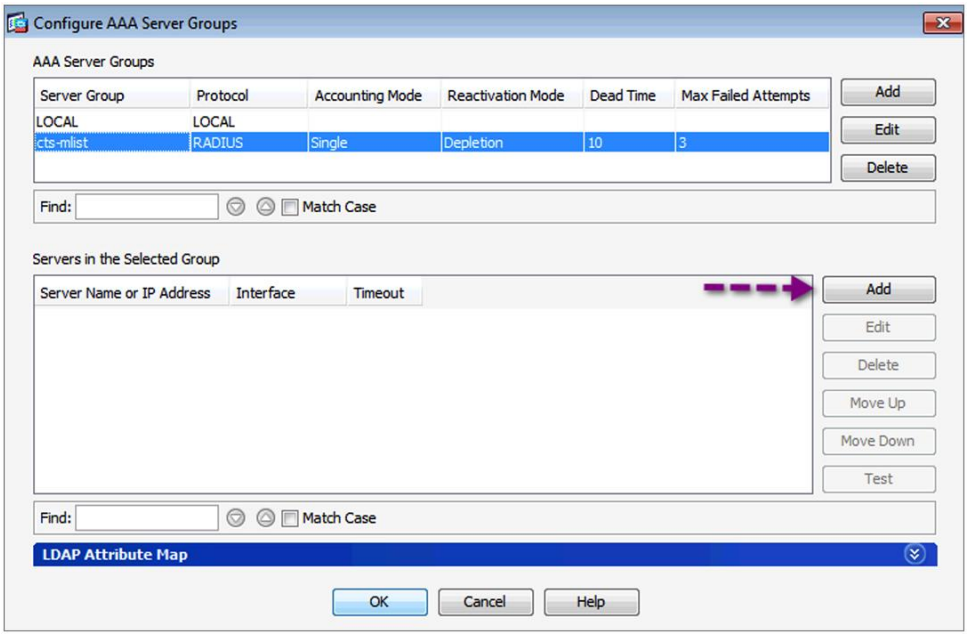
Figure 16. Import PAC



Step 3. In the pop-up form, enter “cts-mlist” in the text box for AAA Server Group

Step 4. Highlight cts-mlist in the AAA Server Groups list, then go to the “Servers in the Selected Group” box and select “Add”

Figure 17. Configure AAA Server Groups

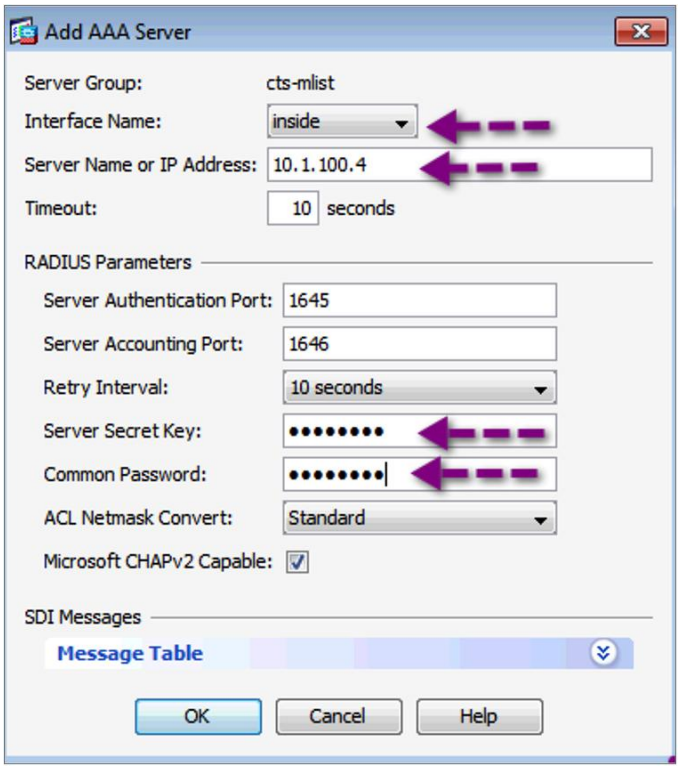


Step 5. Fill in the following terms in the panel. Select the best interface to route to the ISE server ("inside" for this example)

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

Figure 18. AAA Server Configuration

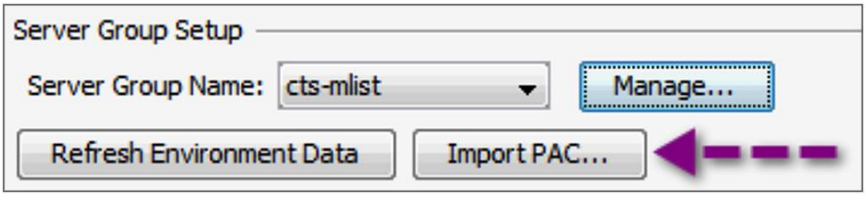


Step 8. Click “OK” for the “Add AAA Server” panel

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

Step 10. Select “Import PAC”

Figure 19. Import PAC



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

Step 12. Validate the PAC is successfully imported

```
sga-asa# show cts pac

  PAC-Info:
    Valid until: Sep 22 2013 20:24:24
    AID:         2e01c4bc2c5506bc4dda00b3f931439e
    I-ID:        ASA
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200a800030001000400102e01c4bc2c5506bc4dda00b3f931439e0006008c000301
    0058014e038d96f68abea4c4a657e8c9d200000013505ad79300093a80957cb4c20f38
    3a529f3dfb98df84ff4c92caa0d055ccedf60322e5d640e0bea4e951553cbe16695619
    892cd6d06b1138ae944ec97faa7c368b1a3fd0958b1474dea545b2d79487d888125b52
    2150b99e8d464f7726988810d933c94ffcc8d128c90b7edc4dd50087b6e7c524
```

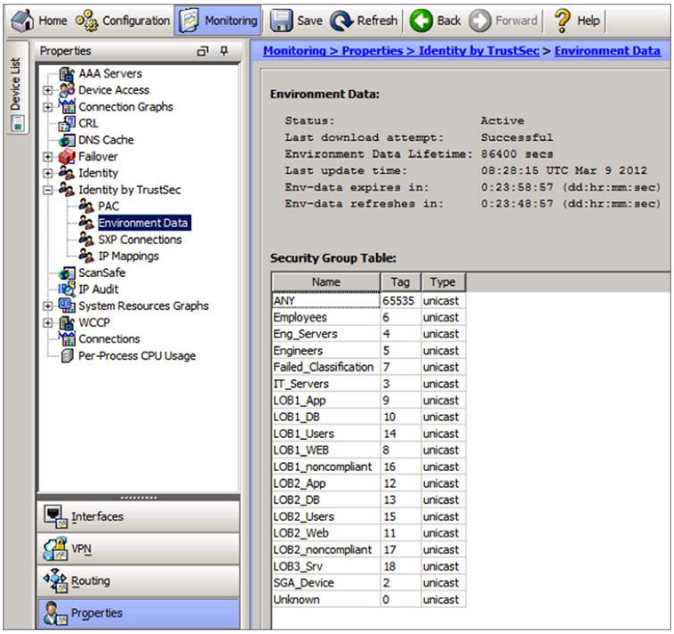
Step 13. Now that the PAC is imported, validate that the communication between the ASA firewall and ISE is successful

```
sga-asa# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          11:31:42 UTC Oct 8 2012
Env-data expires in:       0:23:31:56 (dd:hr:mm:sec)
Env-data refreshes in:     0:23:21:56 (dd:hr:mm:sec)
```

Procedure 8 Verify the SGT Name/Number Table Download Is Successful

Step 1. In ADSM, navigate to Monitoring→ Firewall→Identity by TrustSec→Environmental Data

Figure 20. SGT Name/Number Download from ISE



Via the CLI:

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

Security Group Table:
Valid until: 08:28:15 UTC Mar 10 2012
Showing 19 of 19 entries

SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
Employees                             6     unicast
Eng_Servers                           4     unicast
Engineers                             5     unicast
Failed_Classification                 7     unicast
IT_Servers                            3     unicast
LOB1_App                              9     unicast
LOB1_DB                              10     unicast
LOB1_Users                           14     unicast
LOB1_WEB                              8     unicast
LOB1_noncompliant                    16     unicast
LOB2_App                             12     unicast
```

LOB2_DB	13	unicast
LOB2_Users	15	unicast
LOB2_Web	11	unicast
LOB2_noncompliant	17	unicast
LOB3_Srv	18	unicast
SGA_Device	2	unicast
Unknown	0	unicast

Note: If the SGT Name/Number table does not download, the issue is with the PAC export from ISE or the PAC import into ASDM. This typically results in the error of "Bad Opaque PAC Data" in ISE Menu: Operations > Authentication

Another option is the ASA firewall is not communicating to ISE on the proper IP address and ISE can't service the SGA environmental download request. If that occurs you will see "Unknown SGA Device" in ISE Menu: Operations > Authentication

Procedure 9 Configure the ASA/ASDM for SXP to the Campus and Data Center Access Switches

You have already configured peer SXP connections from the switches to the ASA firewall. Since the ASA firewall is the point of enforcement, it should be configured as the listener - the receiver of all IP-SGT mappings from the different switches.

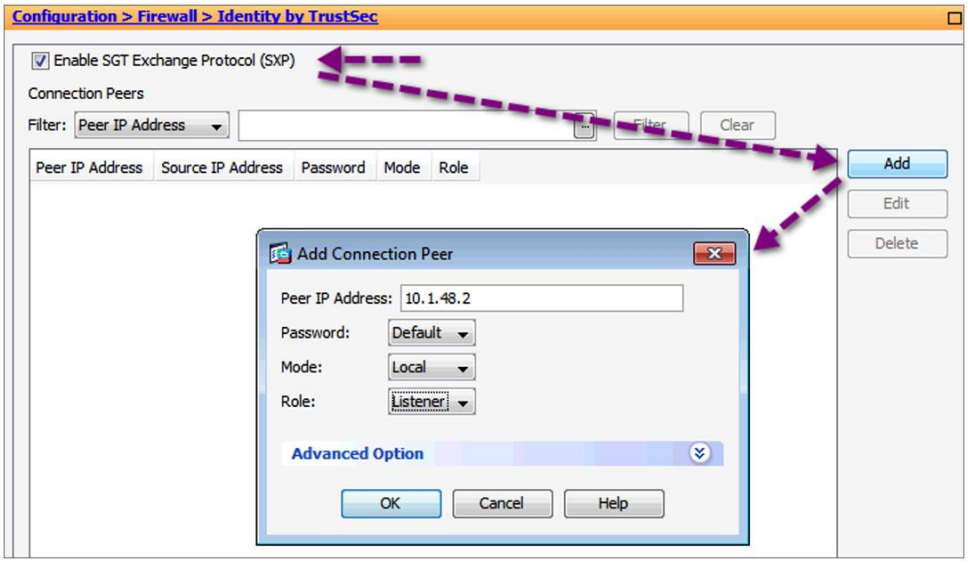
Step 1. In ASDM, navigate to Configuration‣Firewall‣Identity by TrustSec

Step 2. Check "Enable SGT Exchange Protocol (SXP)"

Step 3. Under "Connection Peers," click "Add"

Step 4. Define the 3560-X IP address. Under the "Role" drop-down, and select "Listener"

Figure 21. SXP Configuration



Step 5. Click "OK"

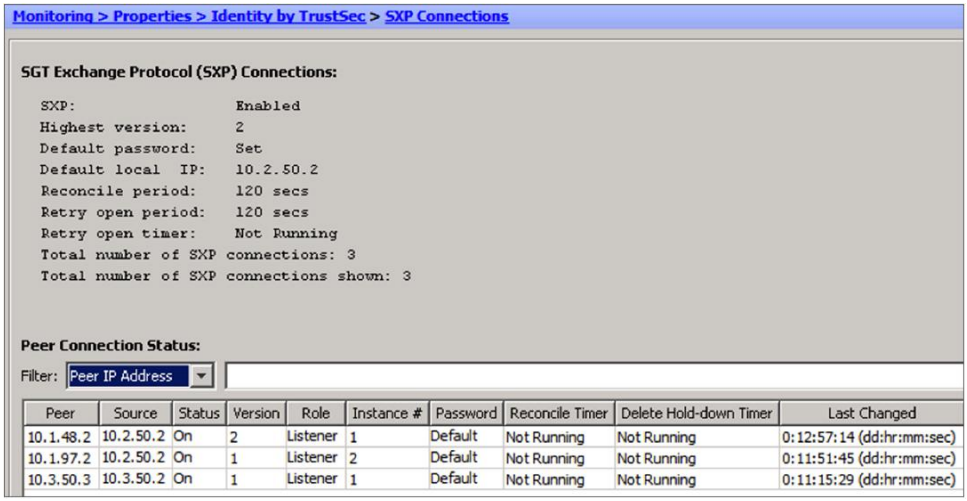
Step 6. Repeat the process for the inside interface of the Nexus 5500

Step 7. Repeat the process for the LOB3 Catalyst 3750

Note: Select “Advanced Options” and enter the LOB3 interface IP address “10.3.50.2”. The reason for this new entry is that the SXP peer must be peered to the closest ASA interface rather than an interface that would require the packet to go through the ASA firewall and hairpin.

Step 8. Validate that all SXP connections are up by navigating to Monitoring‧ Firewall‧Identity by TrustSec ‧SXP Connections

Figure 22. ASA/ASDM SXP Monitoring in ASA/ASDM



Via CLI:

```
Sga-asa# show cts sxp connections brief
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local  IP  : 10.2.50.2
Reconcile period   : 120 secs
Retry open period  : 120 secs
Retry open timer   : Not Running
Total number of SXP connections: 3
Total number of SXP connections shown: 3
-----------------------------------------------------------------------------
Peer IP          Local IP         Conn Status       Duration (dd:hr:mm:sec)
-----------------------------------------------------------------------------
10.1.48.2        10.2.50.2        On                0:12:54:51
10.1.97.2        10.2.50.2        On                0:11:49:22
10.3.50.3        10.3.50.2        On                0:11:13:06
```

If the SXP connection is not moving to the connection state of “On,” there are typically several items to check.

1. Validate that the SXP role is a speaker -> listener model properly on each platform. In this guide’s examples, the switches are always the speakers and the ASA firewall is always a listener.
2. Make sure that the “source address” on the speaker and the “peer IP” on the listener match.
3. Validate that all connections are using the default SXP password, and that the SXP password is configured.

Procedure 10 Configure the Cisco SGFW Policy via ASDM

Now you’re ready to configure firewall policies

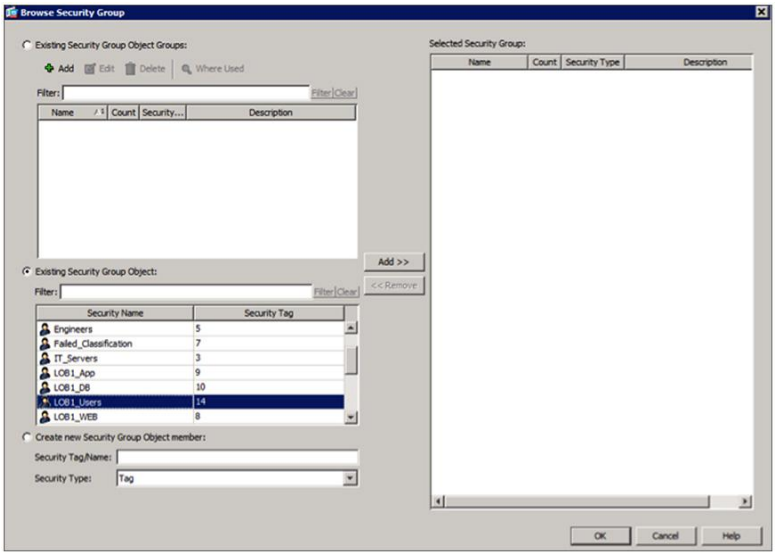
Step 1. In ASDM, navigate to Configuration→Firewall→Access Rules

Step 2. Select the “outside” interface and right click to “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 to the bottom list of SGT Names/Numbers from ISE and select “LOB1_Users.” Click the “Add >>” button in the middle of the page

Figure 23. Assigning a SGT to a Source Criteria in ASDM



Step 5. Click “OK” to return to the “Add Access Rule” dialogue

Step 6. Repeat Steps 2 and 3 for the “Destination Criteria” and use “LOB_Web” for the destination

Step 7. For simplicity, 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 firewall

Step 10. Repeat Step 1 through 8 for the combinations of SGT/DGT and SGT/IP shown in Table 2

Table 2. Access Rules

Source Group	Destination Group	Permissions
LOB1_Users	LOB1_Web	Permit
LOB2_Users	LOB2_Web	Permit
LOB3_Srv	LOB1_Web	Permit
LOB4_Srv	LOB2_Web	Permit
Any	Any	Deny

Figure 24. Campus to DC SGFW Access Rule

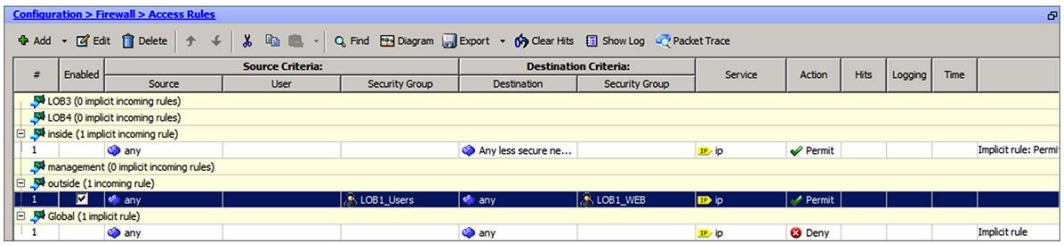
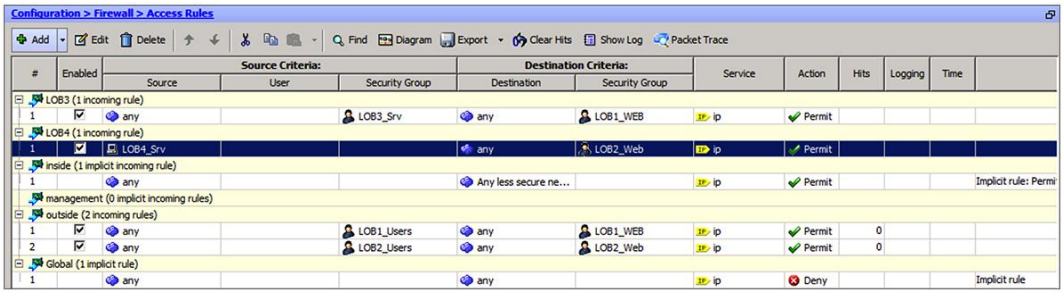


Figure 25. Data Center to DC SGFW Access Rule



Via CLI:

```
sga-asa# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list outside_access_in; 2 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip security-group name
LOB1_Users(tag=14) any security-group name LOB1_WEB(tag=8) any (hitcnt=0)
0xd17a2343
access-list outside_access_in line 2 extended permit ip security-group name
LOB2_Users(tag=15) any security-group name LOB2_Web(tag=11) any (hitcnt=0)
0xe5e79b06
access-list LOB4_access_in; 1 elements; name hash: 0x95a06370
access-list LOB4_access_in line 1 extended permit ip object LOB4_Srv security-group
name LOB2_Web(tag=11) any 0x81550d9c
  access-list LOB4_access_in line 1 extended permit ip host 10.4.50.100 security-
group name LOB2_Web(tag=11) any (hitcnt=0) 0x81550d9c
access-list LOB3_access_in; 1 elements; name hash: 0xd5b169a9
access-list LOB3_access_in line 1 extended permit ip security-group name
LOB3_Srv(tag=18) any security-group name LOB1_WEB(tag=8) any (hitcnt=0) 0xa5dc144b
```

Procedure 11 Validate Cisco ASA SGFW Policies

Validate the SGFW policies that have been created.

Step 1. In ASDM, navigate to Home

Step 2. Expand the “Latest ASDM Syslog Messages” to be able to see the logs

Step 3. Log in as LOB1_User. Ping or web browse the LOB1_Web device. This should result in an ACL hit on the CLI. You should see the TCP or ICMP setup messages for the permit.

Step 4. Log in as LOB2_User. Ping or web browse the LOB1_Web device. This should result in syslog showing denies. Ping or web browse the LOB2_Web device. This should result in an ACL hit on the CLI. You should see the TCP or ICMP setup messages for the permit.

Step 5. Access the LOB3_web server and ping or web browse the LOB2_Web device. This should result in a syslog with denies.

Figure 26. Syslog Denies Based on SGT/DGT Matching in ASDM

Via CLI:

```
sga-asa# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list outside_access_in; 2 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip security-group name
LOB1_Users(tag=14) any security-group name LOB1_WEB(tag=8) any (hitcnt=7)
0xd17a2343
access-list outside_access_in line 2 extended permit ip security-group name
LOB2_Users(tag=15) any security-group name LOB2_Web(tag=11) any (hitcnt=2)
0xe5e79b06
access-list LOB4_access_in; 1 elements; name hash: 0x95a06370
access-list LOB4_access_in line 1 extended permit ip object LOB4_Srv security-group
name LOB2_Web(tag=11) any 0x81550d9c
  access-list LOB4_access_in line 1 extended permit ip host 10.4.50.100 security-
group name LOB2_Web(tag=11) any (hitcnt=0) 0x81550d9c
access-list LOB3_access_in; 1 elements; name hash: 0xd5b169a9
access-list LOB3_access_in line 1 extended permit ip security-group name
LOB3_Srv(tag=18) any security-group name LOB1_WEB(tag=8) any (hitcnt=0) 0xa5dc144b
```

Appendix

The following information is synced from active to standby or from master to slaves, respectively:

- PAC data obtained from ISE. This includes the expiration time.
- The Security Group Table.
- The environment data expiration time. This is derived by the ASA from the TTL value that is received when the environment data is downloaded.

HA Overview

In a failover scenario, when the active unit receives an update on its mapping database, it will sync the update to the mapping database on the standby unit. The mapping database on the standby unit will decide (following the same logic as in the active unit) whether or not to populate this update to the IP-SGT manager on the standby unit. And the IP-SGT manager on the standby unit will decide (following the same logic as in the primary unit) whether or not to populate this update to the data path database.

Upon failover, when the standby unit becomes active, it will attempt to “re-establish” the connections with its peers. These connections are brand new connections as the connection database does not have their records (empty). The new active unit will also start a global HA reconciliation timer. When new mappings are learnt from peers, the new mappings will be compared with the old mappings. If the same mapping is learnt from the same peer, the old mapping will be overwritten. After the HA reconciliation time expires, the remaining old mappings will be deleted. In most cases, the new mappings learnt from the peers within the HA reconciliation period will be the same as the old mappings. They will not be populated to the IP-SGT manager, and hence, not populated to the data path database. Therefore, the impact to the data path is minimal.

For the case of manual failover, the active and standby units have the same copy of mappings from SXP. Therefore, bulk sync between the active unit and the standby unit is not needed after the failover. In a failover scenario, if an active unit crashes, the standby unit will take over as the new active unit, and will establish SXP connections and perform reconciliation of the mapping database as explained above. When the crashed unit comes back up again and assumes standby status, it will request bulk sync from the unit that is currently active. Subsequent updates to the database will be synced via incremental updates.

If the standby unit crashes and comes back up again, its SXP mapping database will be empty and the unit will request bulk sync from the active unit. Subsequently, any new mappings learnt on the active unit will be synced individually to the standby unit.

In the case of consecutive crashes, if the mapping database replication isn’t complete, down time would be expected before re-learning on the new active unit is complete. This should happen rarely.

HA Considerations

As the PAC is imported to the active unit, it will be replicated to the standby unit. However, PAC expiration monitoring and the actual import operation are only supported on the active unit. Likewise, the active unit is responsible for tracking the expiration of CTS environment data and for retrieving the environment data and security group table from ISE. In the event of a failover, the new active unit will resume responsibility for environment data retrieval.

Additionally, the security group table and the associated policies are replicated from the active unit to the standby unit. So when the standby unit takes over as active, these policies can readily be enforced. When the new active unit downloads the security group table from ISE, changes, if any, will be reflected in policies and appropriate rules. Any changes in the security group table will be replicated to the standby via incremental sync so appropriate policy changes can happen on the standby as well.

Clustering Background: Layer 2 and Layer 3 Modes

In Layer 2 mode, all units in the cluster share the same IP and MAC addresses. In Layer 3 mode, each unit in the cluster has its own IP and MAC address to communicate to the external world as a standalone unit.

In Layer 2 mode, to-the-box SXP traffic will be directed to the master unit. In Layer 3 mode, to-the-box SXP traffic will be directed to the master unit if the peer device is configured to talk with the system IP address of the cluster; from-the-box SXP traffic binds to this system IP address too. This ensures that all SXP connections are established through the master unit. Any SXP connection attempt to anything other than the system IP will fail.

Clustering Overview

The PAC import operation and PAC expiration monitoring will only be supported on the master cluster device. As the PAC is imported, it will be replicated to all of the slave devices. If a new master device is elected, it will resume responsibility for PAC import processing and PAC expiration monitoring based on the expiration time that is carried in the PAC. Likewise, the master cluster device is responsible for tracking the expiration of CTS environment data and for retrieving the environment data and security group table from the ISE. If a new master device is elected, the new master will resume responsibility for automatic and manual environment data retrieval.

SXP connections will always be established on the master unit. The master unit will maintain both the SXP connection database and SXP mapping database. Similar to a failover scenario, the SXP mapping database will be replicated to all slave units so security-group-based policies can be enforced on all slave units. The SXP connection database will not be replicated.

In a failover scenario, non-reliable but sequenced LU messaging will be used to sync the SXP mapping database. If the active unit crashes and the standby unit takes over, the replicated database will be used for the transient time until the new active unit establishes SXP connections and re-learns the mappings. In contrast, all slave units need to be able to enforce security-group-based policies: A consistent view of the mapping database is required across all slave units. Hence, reliable messaging will be used for the sync.

Clustering Considerations

Security-group-based policies are replicated to all slave units as part of the configuration sync. As mentioned earlier, the environment data is replicated to slave units, so security group tags or names configured in policies can be resolved via the security group table and appropriate rules can be configured. Additionally, the SXP mapping database will be replicated to all units in the cluster, thus security-group-based policies can be enforced on all slave units. Note that changes in the SXP mapping database and the security group table will be replicated to the slave units via incremental updates.

When the owner of a connection fails, the first slave unit (“slave A”) that receives a packet on the connection will query the director to find the backup owner. The backup owner will be contacted, which will then transfer all LU updates to slave A. Slave A will reconstruct the connection and assume ownership. In the current HA model, security group tags aren’t sent in LU updates; when the new owner constructs the connection, the tags corresponding to the source and destination IP addresses will be looked up and security-group-based policies can be enforced.

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 C07-729794-00 10/13