Cisco TrustSec How-To Guide: Server-to-Server Segmentation Using SGA

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

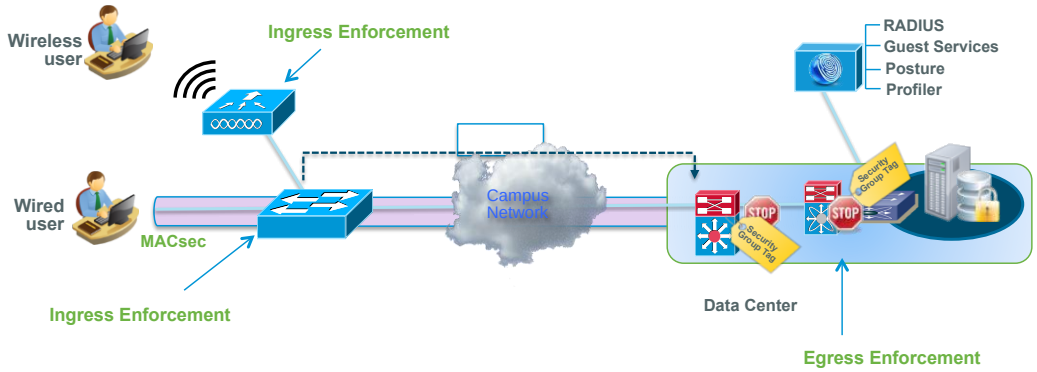
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

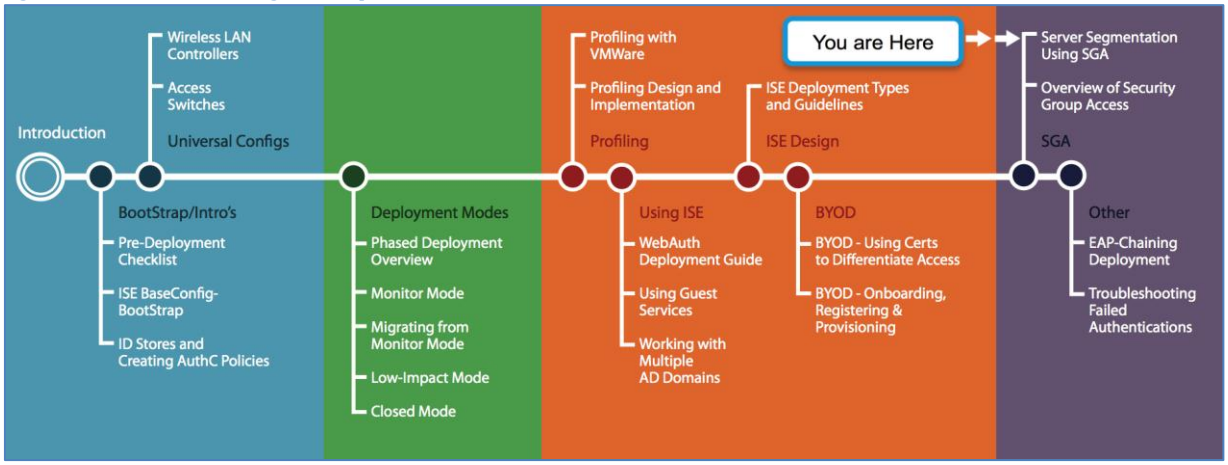


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "TrustSec certified". The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Server Segmentation with SGA

Overview

The goal of this document is to provide the details necessary to configure and test Security Group Tagging (SGT)assignment and Security Group Access Control List (SGACL) enforcement on the Cisco Nexus® 5500 Series Switches with the Cisco Nexus 2000 Fabric Extender. This document provides the Security Group Access (SGA) configuration on the Cisco Nexus 5000 and 2000 Series and for the Cisco Identity Services Engine 1.1 (ISE) for a specific use case: server-to-server segmentation within the data center. There are other use cases depending on the network architecture and features enabled. However, this document focuses specifically on the new ability to filter server-to-server traffic regardless of underlying topology rather than the traditional VLAN segmentation method.

This document will explain how to:

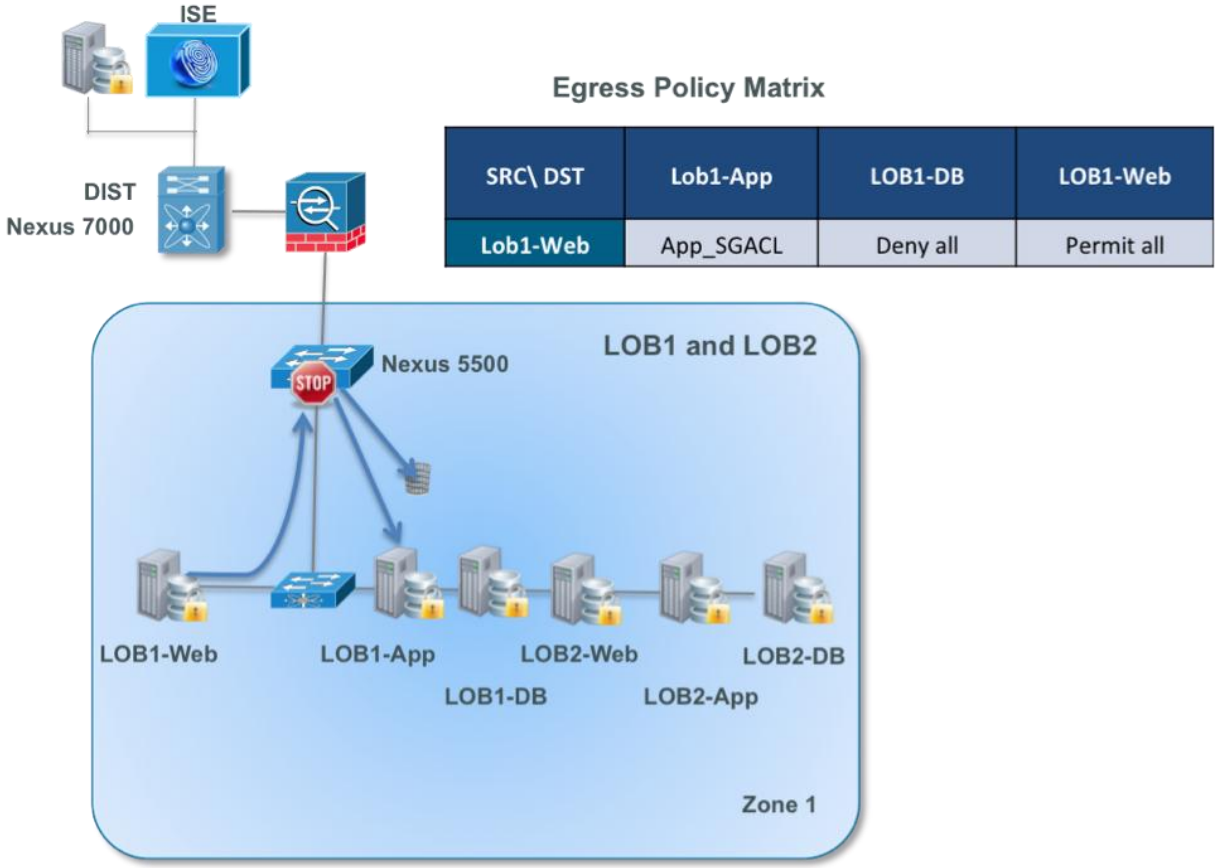
1. Configure the Cisco Nexus 5000 Series to receive policies from ISE
2. Demonstrate and test server-to-server traffic enforcement by using SGTs and SGACLs
3. Configure the Cisco Nexus 5000 Series to build strong access control and policy enforcement environment
4. Understand how to troubleshoot Security Group Access

Architecture

Figure 3 shows the reference topology used for describing how to configure the Cisco Nexus 5000 and 2000 Series in a Cisco TrustSec environment. Figure 3 shows an example topology for the TrustSec Software Version 2.1 solution. For illustrative purposes, we've created lines of business (LOBs in the figure) that have built three-tiered web models in Zone 1 of their data center. These lines of business have a web server, an application server, and a database server. These servers will be used to show combined enforcement solution the Cisco Nexus 5000 Series and 2000 Series in all of the security zones.

This guide will illustrate how to filter intra-server traffic irrespective of the underlying topology within Zone 1.

Figure 3 Architecture Used in This How-To Guide



In the diagram, all these servers are on the same VLAN to illustrate that there is no need for any type of traffic engineering to enforce policy. The servers are assigned a SGT and the Cisco Nexus 5000 Series will filter traffic communications between the various servers. Per the sample egress policy matrix, traffic will flow as follows:

1) Traffic from LOB1-Web to LOB1-App is filtered based on the rules within the App_SGACL SGACL.

2) Traffic from LOB1-Web to LOB1-DB will be dropped.

3) Traffic from LOB1-Web to itself is permitted.

Cisco ISE Configuration

It is important to note that Security Group Access (SGA) used to be known as Cisco Trusted Security (CTS). The commands on many devices continue to follow the 'CTS' moniker, so the two acronyms (CTS & SGA) can be used interchangeably.

Procedure 1 Configuring Security Groups

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

- SGT_Devices: Networking devices that support SGT/SGACL
- Network_Services: Servers that are used for basic networking like Active Directory, ISE, Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS)
- LOB1-Web: Line of Business 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

Step 1 Navigate to Policy → Policy Elements → Results → Security Group Access → Security Groups.

Step 2 Click the Add button.

Step 3 Create a security group from the above list and click Save (Figure 4)

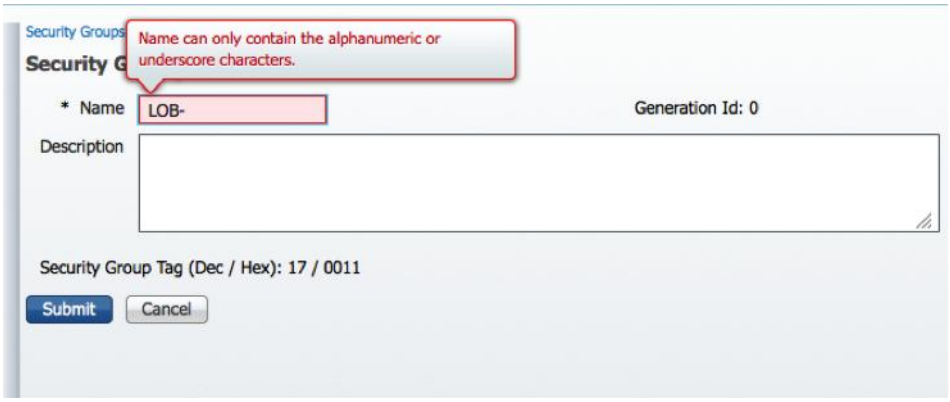
Step 4 Repeat Step 3.

Figure 4 LOB1_App Security Group

Note: SGT values are auto-generated.

Troubleshooting Tip: If there is an error in creating the SGT, you should look at the error message from ISE and try again. Typically an invalid character was typed. See Figure 5 for an example.

Figure 5 Typical Error in Creating the SGT



Procedure 2 Configure the Cisco Nexus 5000 Series as an SGA Device

Step 1 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. Make sure this name matches with the hostname of the Cisco Nexus 5000 Series. This name is used to validate the SGT Name Table download requests.

Step 4 Fill in the IP Address of the Cisco Nexus 5000 Series interface with the best route to ISE.

Step 5 Select the SGA Attributes checkbox. This expands the SGT attributes of the Network Device definition. If the Name you entered in Step 3 matches the hostname of the Cisco Nexus 5000 Series, select the option Use Device ID for SGA Identification".

Step 6 Enter the shared secret used for SGA communication in the Password field. This will match the RADIUS shared secret in the Cisco Nexus 5000 Series definitions so please note it.

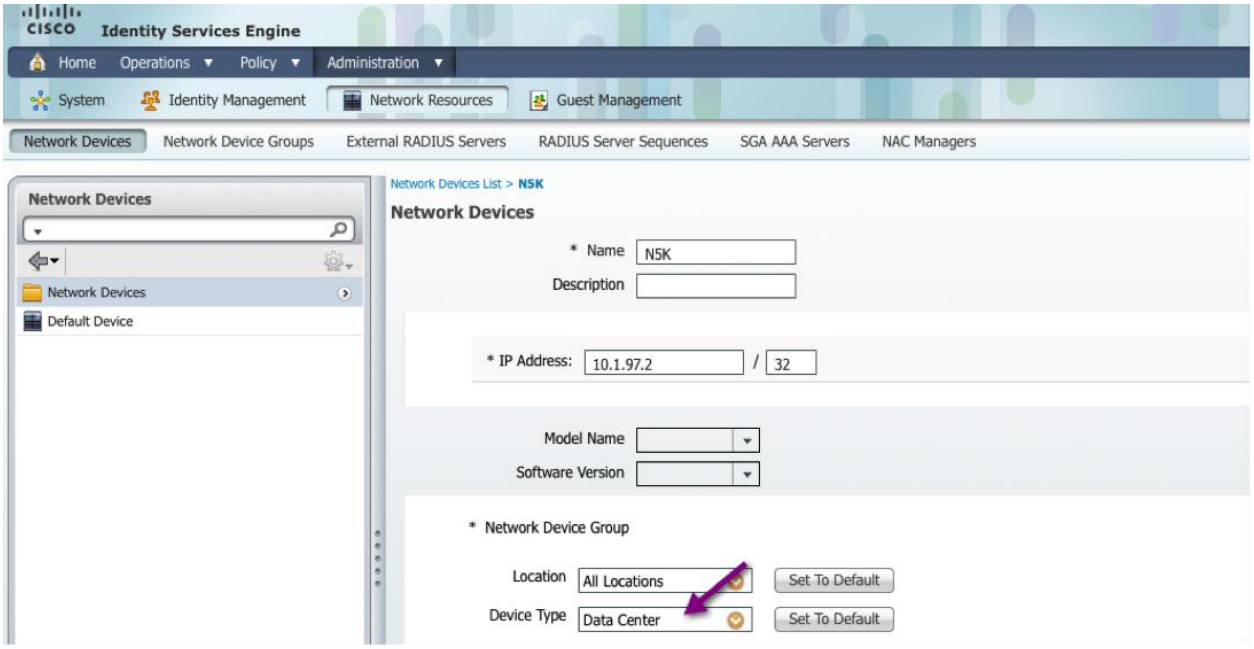
Procedure 3 Configure Network Device Authentication

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

Step 2 Click ADD, and fill in the IP Address (Figure 6).

Best Practice: Add the Cisco Nexus 5000 Series to a Network Device Group. This grouping will greatly simplify rule set creation later. The example in Figure 6 uses Data Center as the device group.

Figure 6 Setting the IP Address and Network Device Group



Step 3 Fill in the Authentication Settings and SGA Attributes, and click Submit (Figures 7 and 8).

Figure 7 NAD Authentication Settings

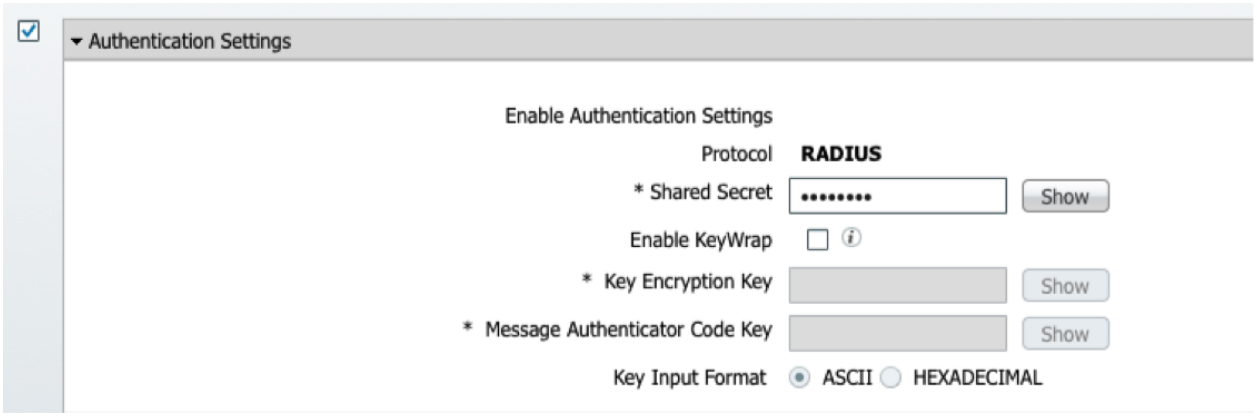
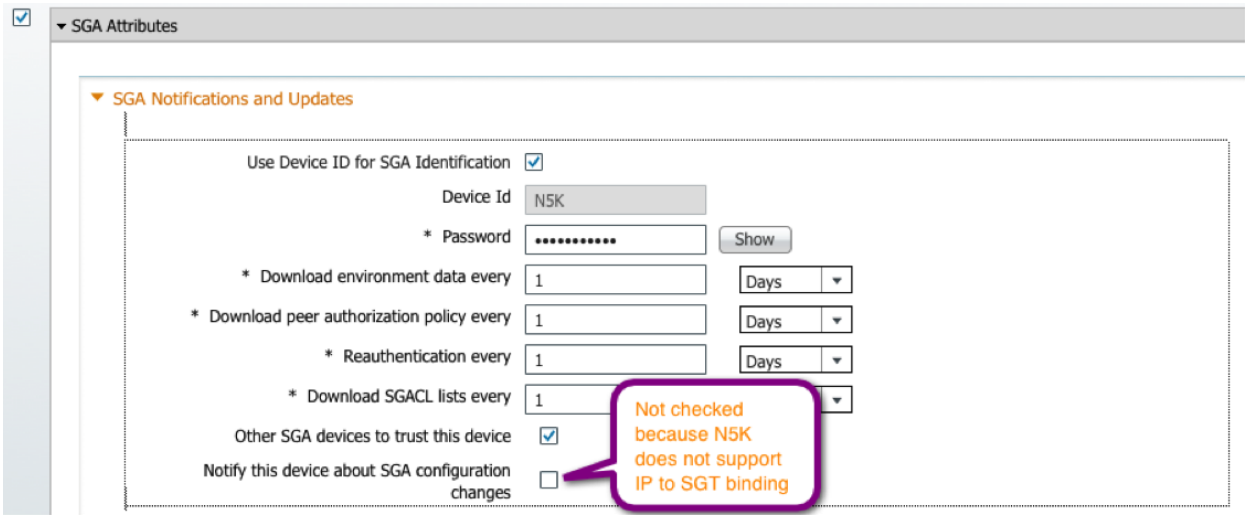


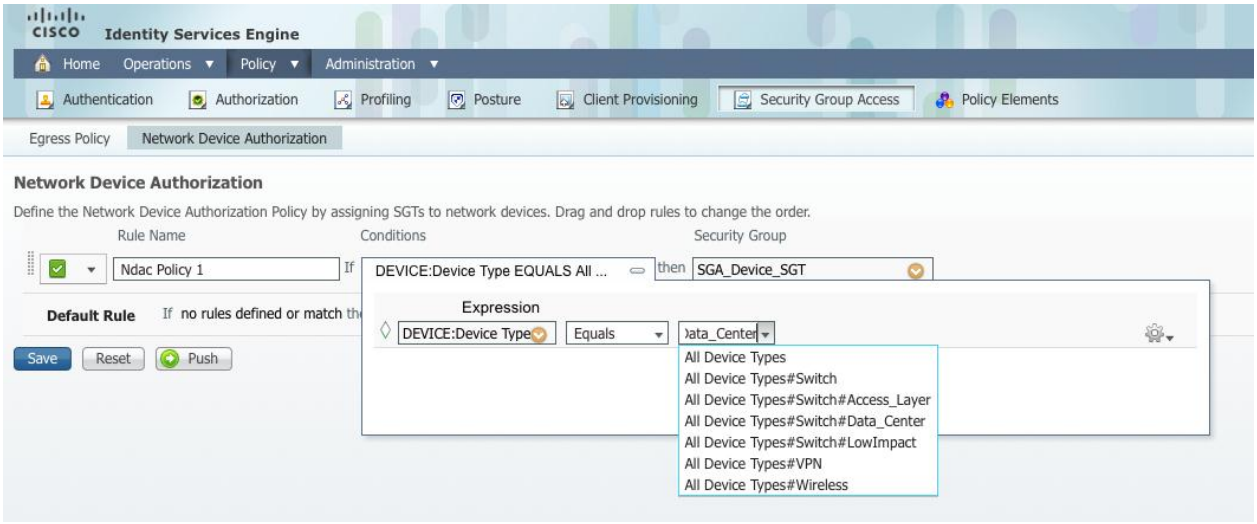
Figure 8 NAD SGA Attributes



Step 4 Navigate to Policy → Security Group Access → Network Device Authorization.

Step 5 Click the Actions tab, choose new row above, and create a rule to assign the SGT_Devices tag to the Cisco Nexus 5000 Series (Figure 9).

Figure 9 Network Device Authorization Policy



Procedure 4 Configure SGACLs

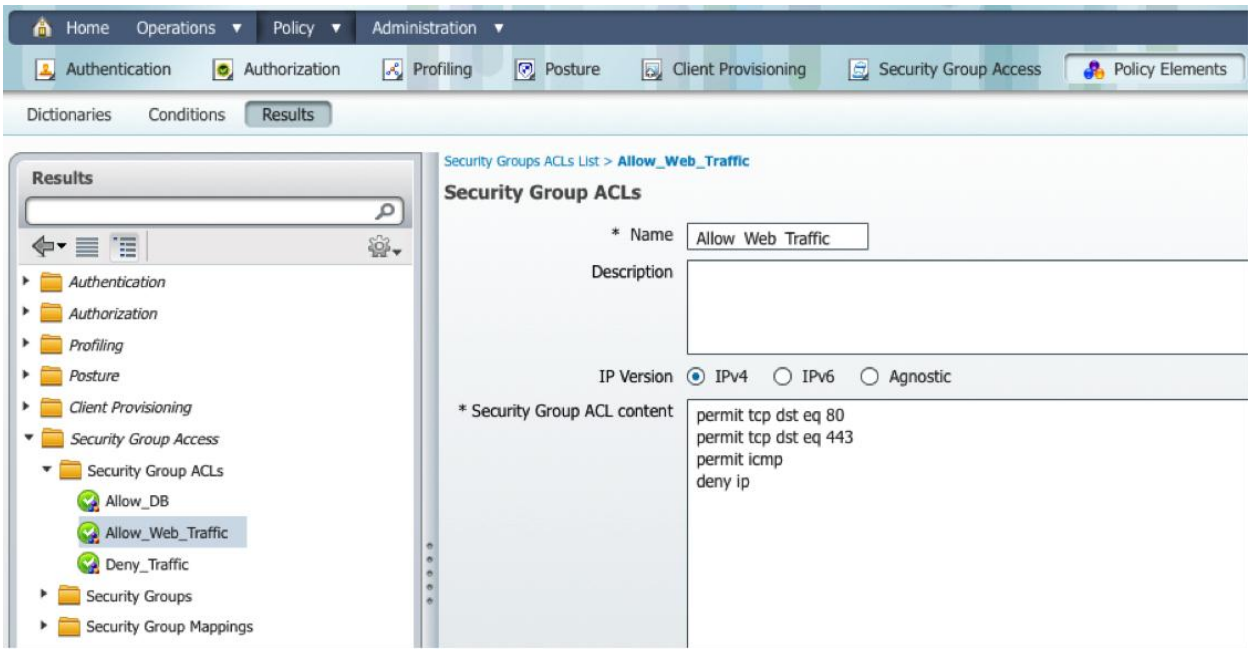
In this section, you will define traffic rules in the form of SGACLs. These will be downloaded to the Cisco Nexus 5000 Series for policy enforcement.

Step 1 Navigate to Policy→Policy Elements→Results→Security Group Access→Security Group ACLs.

Step 2 Create traffic rules, as shown in the example in Figure 10.

Note: Syntax verification is not supported.

Figure 10 Configuring SGACLs



Procedure 5 Configure Egress Policies

In this procedure, using the SGACLs you just created, you will define the traffic filtering policies between each data center server.

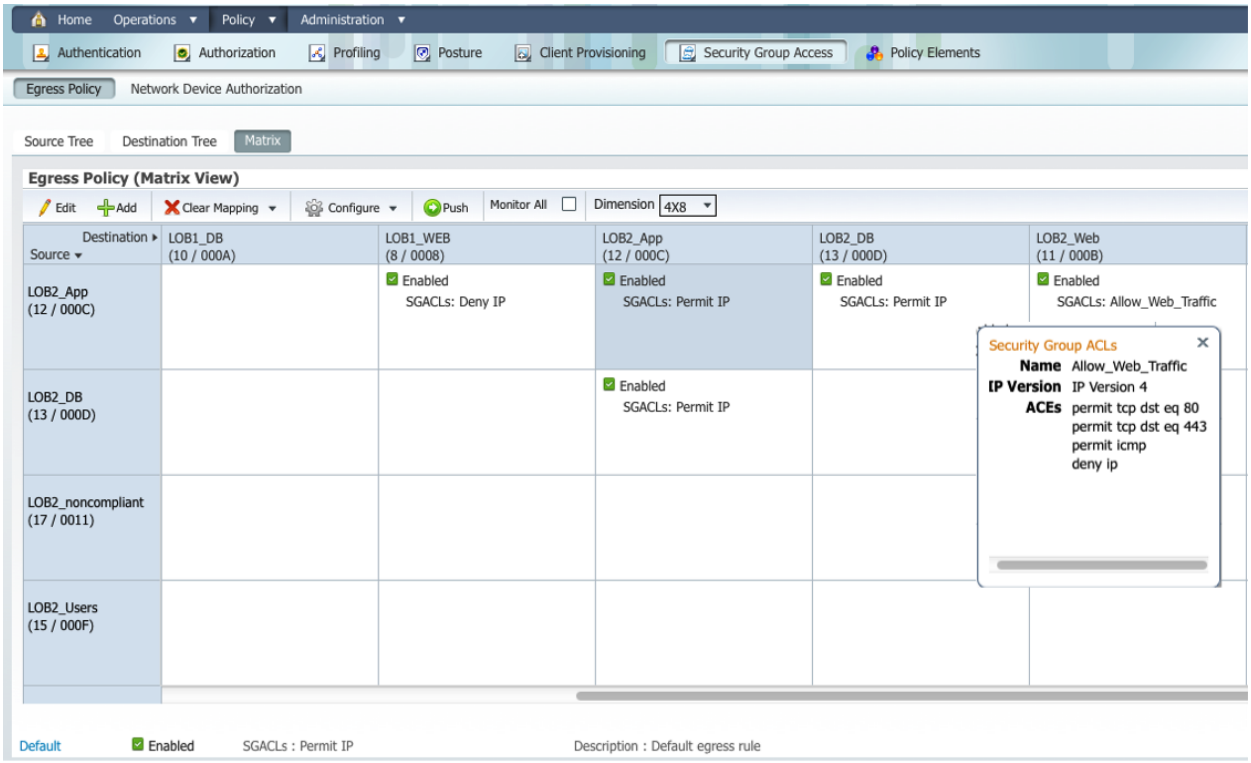
Step 1 Policy → Security Group Access → Egress Policy.

Step 2 Assign SGACLs following the example policy matrix in Figure 11.

Note: The Tree View or Matrix View is a matter of personal preference. Use the filters and/or scroll bars to tune your view.

Best Practice: The default egress rule is to permit traffic

Figure 11 Configuring Egress Policies



Cisco Nexus 5000 Series Configuration

This section configures the RADIUS server between the Cisco Nexus 5000 Series and ISE. Based on the configuration you will complete in Procedure 2, Cisco ISE will authenticate and download the policy to the Cisco Nexus 5000 Series.

Procedure 1 Configure AAA

Step 1 Define Cisco ISE as the RADIUS server, as follows:

```
Radius-server host <ISE IP Address> key 0 <key> pac authentication accounting
```

Step 2 Define the RADIUS server group, as follows:

```
aaa group server radius <group name>
server <ISE IP Address>
use-vrf default
```

Procedure 2 Configure Cisco Nexus 5000 Series to Download Policy

Step 1 Configure the 5000 Series to download the policy, as follows:

```
cts device id <match device name configured on ISE> password <password>
aaa authentication cts default group sga-radius
aaa authorization cts default group sga-radius
```

Procedure 3 Validate Policy Download

Here are the commands used for policy download validation:

```
nexus5k# sho cts
CTS Global Configuration
================================
  CTS support           : enabled
  CTS device identity   : N5K
  SGT                   : 2
  CTS caching support   : disabled

nexus5k# sho cts environment
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        : Thu Mar  8 18:45:59 2012

  Server List             : CTSServerList1
     AID:00f0c9afe1054674dc44c18baf9f86cb IP:10.1.100.4 Port:1812

nexus5K(config)# sho cts pac
PAC Info :
================================
  PAC Type            : Trustsec
  AID                 : d6b526a1b6b1d05104007b17d6a7fb95
```

```
  I-ID                : N5K
  AID Info            : ISE11FCS
  Credential Lifetime : Wed Jun 27 19:25:29 2012

  PAC Opaque          : 000200a80003000100040010d6b526a1b6b1d05104007b17d6a7fb95
0006008c000301006d242d71fa94910a6e8e918e4e9612020000000014f738e8800093a80bbb053d5
e6ee43d0989d1deec14f2beee346a5894d14fe063fbfbefe471d4abc7f822ef68aed5b78a88f123d
c536c265b93f8bd8688bb266bd49908f757ab79116a33e2d622d58294cb2f1907154cc1eff8edcf3
f5c207006dff0d846712803f2218618c0eaf083259b6d167
```

Note: The policy has been downloaded at this point. However, because the SGT mappings have not been defined on the Cisco Nexus 5000 Series, only the default policy is shown, as shown in the following.

```
nexus5k# show cts role-based policy
sgt:any
dgt:any rbacl:Permit IP
        permit ip
```

Note: If the policies fail to download, check the password values for RADIUS and the device-id.

On Cisco ISE, a password mismatch between the switch and ISE looks like this: 11036 The Message-Authenticator RADIUS attribute is invalid.

On Cisco ISE, a device-id mismatch looks like this: Authentication failed: 22056 Subject not found in the applicable identity store(s).

Cisco Nexus 2000 Series Configuration

It is important to note that Security Group Access (SGA) used to be known as Cisco Trusted Security (CTS). The commands on many devices continue to follow the 'CTS' moniker, so the two acronyms (CTS & SGA) can be used interchangeably.

Procedure 1 Configure the Local CTS Configuration

In this section, SGT values are assigned to the port. The server is assigned the SGT value of the port that it is connected port. Currently, the Cisco Nexus 5000 Series does not support IP-to-SGT mapping.

Step 1 Supply local configuration for CTS parameters. This command **must** be enabled for ALL ports.

```
nexus5k(config-if-range)# int e100/1/1-48
nexus5k(config-if-range)# cts manual
```

Step 2 Disable SGT propagation since the peer device is a server, not a SGA device:

```
N5K(config-if-cts-manual)# no propagate-sgt
```

Step 3 Enter into interface-configuration mode for each interface individually (in other words, exit out of the interface range). Assign the SGT value of the server connected to the port. Repeat this step to assign all SGTs.

```
nexus5k(config-if-cts-manual)# int e100/1/1
nexus5k(config-if-cts-manual)# policy static sgt <hex value>
```

Step 4 To apply the change, you must bounce the port (i.e.: issue a shut command followed by a no shut command) for all the Cisco Nexus 2000 Series Fabric Extender (FEX) ports. Note that this is required to apply the configuration.

```
nexus5k(config-if-cts-manual)# shut
nexus5k(config-if-cts-manual)# no shut
```

Step 5 Validate that CTS is enabled, as follows:

```
nexus5k(config-if)# sho cts interface e100/1/1
CTS Information for Interface Ethernet100/1/1:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SKIPPED_CONFIG
```

```
  Peer Identity:
  Peer is:              Unknown in manual mode
  802.1X role:          CTS_ROLE_UNKNOWN
  Last Re-Authentication:
Authorization Status:   CTS_AUTHZ_SKIPPED_CONFIG
  PEER SGT:             12
  Peer SGT assignment:  Not Trusted
SAP Status:             CTS_SAP_SKIPPED_CONFIG
  Configured pairwise ciphers:
  Replay protection:
  Replay protection mode:
  Selected cipher:
  Current receive SPI:
  Current transmit SPI:
Propagate SGT: Disabled
```

Note:

If the FEX port is configured with a nonexistent SGT value, the error is: 11304 Could not retrieve requested Security Group Tag

If all interfaces do not have the same "trust mode" and "propagate-sgt" configuration, the error is: Interface going error-disabled. CTS config should be consistent across all the interfaces with same FEX ID

When removing a command, remove the command on ALL interfaces; otherwise, the port will be err-disabled.

Best Practice: Reference the Egress Policy Table/Matrix on ISE. Its quite common to incorrectly enter the hex value or to incorrectly map the SGT to the wrong server group.

Procedure 2 Enable Policy Enforcement

Step 1 Enable policy enforcement on server VLANs, as follows:

```
nexus5k(config)# vlan 101
nexus5k(config-vlan)# cts role-based enforcement
nexus5k(config-vlan)# exit ← This is required to apply this command
```

Step 2 Verify the enforcement policy, as follows:

```
nexus5k(config)# sho platform fwm info vlan 101 | inc cts
vlan 1.101: pi vlan cts_en: 1
or
nexus5k(config)# sho cts role-based enable
vlan:101
```

Procedure 3 Refresh the SGACL policies

Step 1 Enable role-based counters to view role-based access control list (RBACL) statistics:

```
nexus5k(config)# cts role-based counter enable
```

Step 2 Now re-download the SGACL policies:

```
nexus5k(config)# cts refresh role-based-policy
nexus5k(config)# sho cts role-based policy

sgt:12
dgt:8   rbacl:Deny IP
        deny ip

sgt:12
dgt:11  rbacl:Allow_Web_Traffic
        permit tcp dst eq 80
```

```
        permit tcp dst eq 443
        permit icmp
        deny ip

sgt:12
dgt:12  rbacl:Permit IP
        permit ip

sgt:13
dgt:12  rbacl:Permit IP
        permit ip

sgt:any
dgt:any rbacl:Permit IP
        permit ip
```

Other useful commands:

```
nexus5k(config)# sho cts role-based access-list
rbacl:Allow_Web_Traffic
        permit tcp dst eq 80
        permit tcp dst eq 443
        permit icmp
        deny ip
rbacl:Deny IP
        deny ip
rbacl:Permit IP
        permit ip

nexus5k(config)# sho cts role-based counters

RBACL policy counters enabled
Counters last cleared: 03/10/2012 at 02:27:24 PM
rbacl:Allow_Web_Traffic
        permit tcp dst eq 80                            [0]
        permit tcp dst eq 443                           [0]
        permit icmp                                     [0]
        deny ip                                         [0]
rbacl:Deny IP
        deny ip                                         [0]
rbacl:Permit IP
        permit ip                                       [74]
```

Appendix A: References

Cisco TrustSec System:

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

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html