ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide

TAC **Document ID: 116497**

Contributed by Michal Garcarz, Cisco TAC Engineer.
Jan 21, 2016

Contents

Introduction

This article describes how to configure Cisco TrustSec (CTS) on the Cisco Secure Adaptive Security Appliance (ASA) and a Cisco Catalyst 3750X Series switch (3750X).

In order to learn the mapping between Security Group Tags (SGTs) and IP addresses, the ASA uses the SGT Exchange Protocol (SXP). Then, Access Control Lists (ACLs) based on SGT are used in order to filter the traffic. The 3750X downloads Role-Based Access Control List (RBACL) policies from the Cisco Identity Services Engine (ISE), and filters traffic based on them. This article details the packet level in order to describe how the communication operates and the expected debugs.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- CTS Components
- CLI Configuration of ASA and Cisco IOS®

Components Used

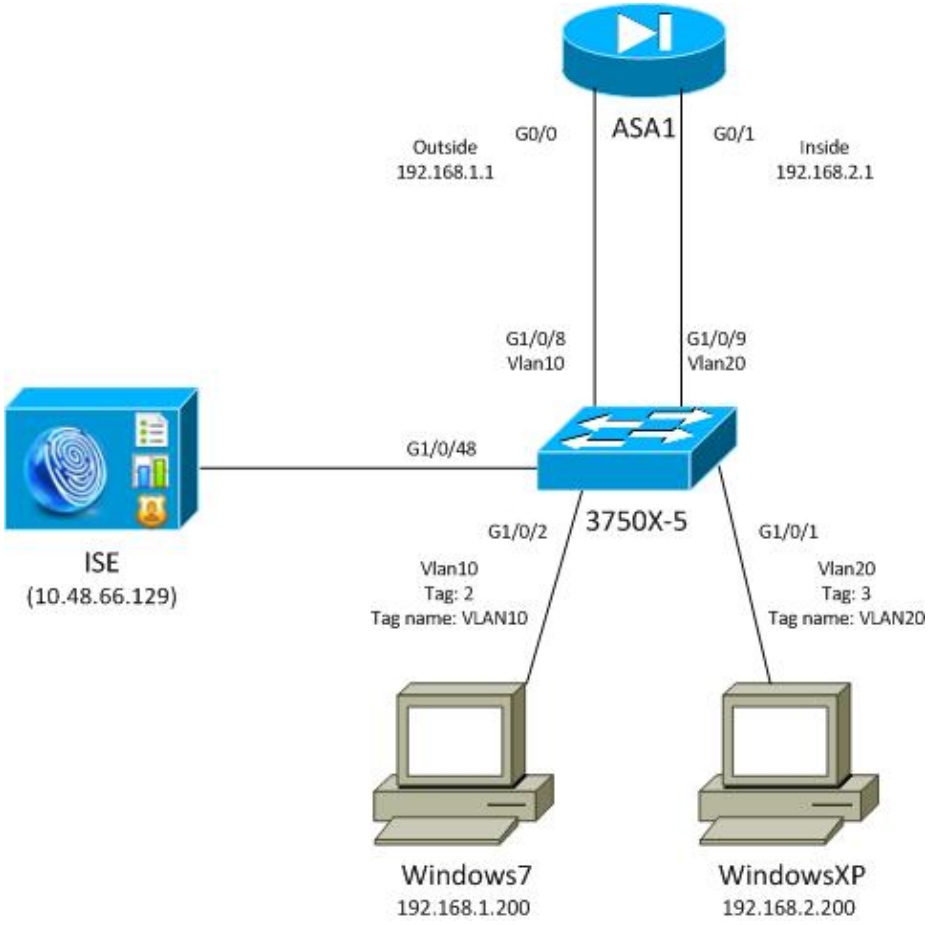
The information in this document is based on these software and hardware versions:

- Cisco ASA software, Versions 9.1 and later
- Microsoft (MS) Windows 7 and MS Windows XP
- Cisco 3750X software, Versions 15.0 and later
- Cisco ISE software, Versions 1.1.4 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram



Traffic Flow

Here is the traffic flow:

- The 3750X is configured on **G1/0/1** and **G1/0/2** for port authentication.
- The ISE is used as the Authentication, Authorization, and Accounting (AAA) server.
- MAC Address Bypass (MAB) is used for authentication for MS Windows 7.
- IEEE 802.1x is used for MS Windows XP in order to demonstrate that it does not matter which authentication method is used.

After successful authentication, the ISE returns the SGT, and the 3750X binds that tag to the authentication session. The switch also learns the IP addresses of both stations with the **ip device tracking** command. The switch then uses SXP in order to send the mapping table between the SGT and the IP address to the ASA. Both MS Windows PCs have a default routing that points to the ASA.

After the ASA receives traffic from the IP address that is mapped to the SGT, it is able to use the ACL based on the SGT. Also, when you use 3750X as a router (default gateway for both MS Windows stations), it is able to filter the traffic based on policies downloaded from the ISE.

Here are the steps for configuration and verification, each of which is detailed in its own section later in the document:

- Port authentication with the **ip device tracking** command on the 3750X
- ISE configuration for authentication, SGT, and Security Group Access Control List (SGACL) policies
- CTS configuration on the ASA and the 3750X
- Protected Access Credential (PAC) provisioning on the 3750X (automatic) and the ASA (manual)
- Environment refresh on the ASA and the 3750X
- Port authentication verification and enforcement on the 3750X
- Policy refresh on the 3750X
- SXP exchange (the ASA as listener, and the 3750X as speaker)
- Traffic filtering on the ASA with SGT ACL
- Traffic filtering on the 3750X with policies downloaded from the ISE

Configurations

Port Authentication with the *ip device tracking* Command on the 3750X

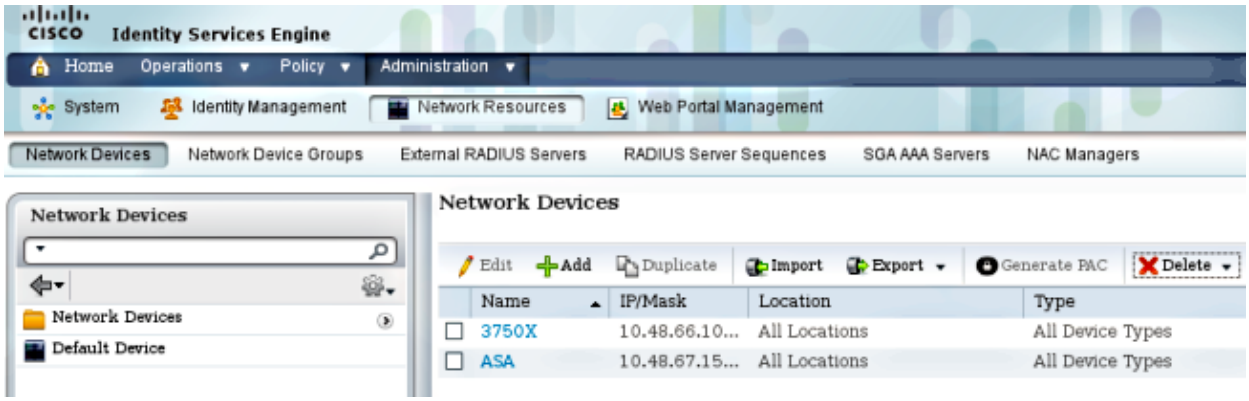
This is the typical configuration for 802.1x or MAB. RADIUS Change of Authorization (CoA) is needed only when you use active notification from the ISE.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

!Radius COA
aaa server radius dynamic-author
 client 10.48.66.129 server-key cisco
 server-key cisco

ip device tracking

interface GigabitEthernet1/0/1
 description windowsxp
 switchport mode access
 authentication order mab dot1x
```

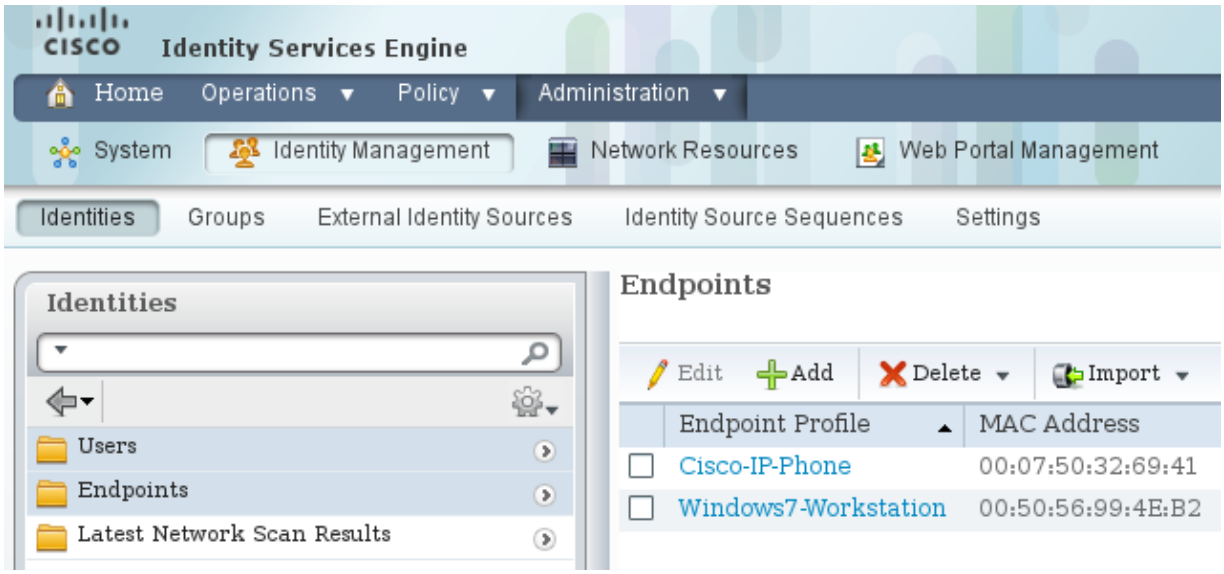
```
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

ISE Configuration for Authentication, SGT, and SGACL Policies

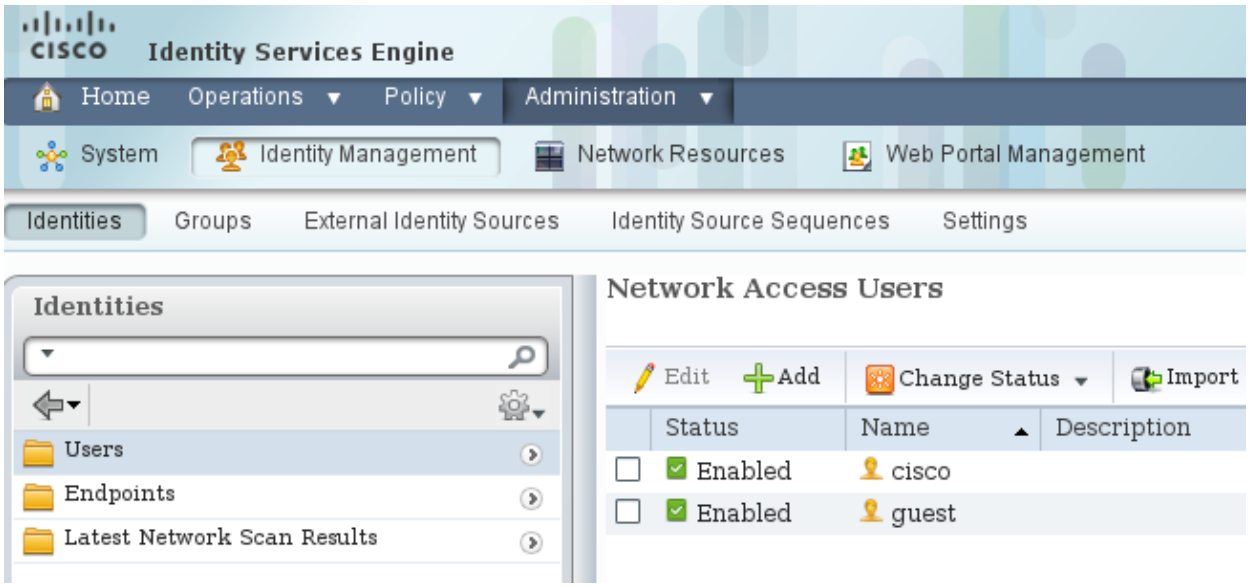
The ISE must have both network devices configured under **Administration > Network Devices**:



For MS Windows 7, which uses MAB authentication, you must create Endpoint Identity (MAC address) under **Administration > Identity Management > Identities > Endpoints**:

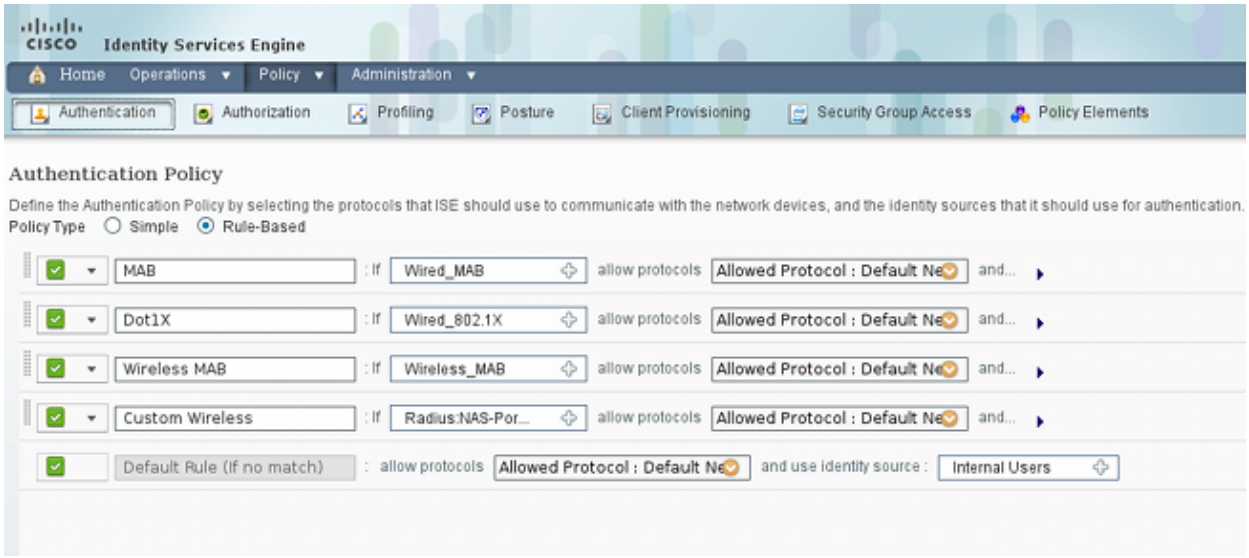


For MS Windows XP, which uses 802.1x authentication, you must create a User Identity (username) under **Administration > Identity Management > Identities > Users**:

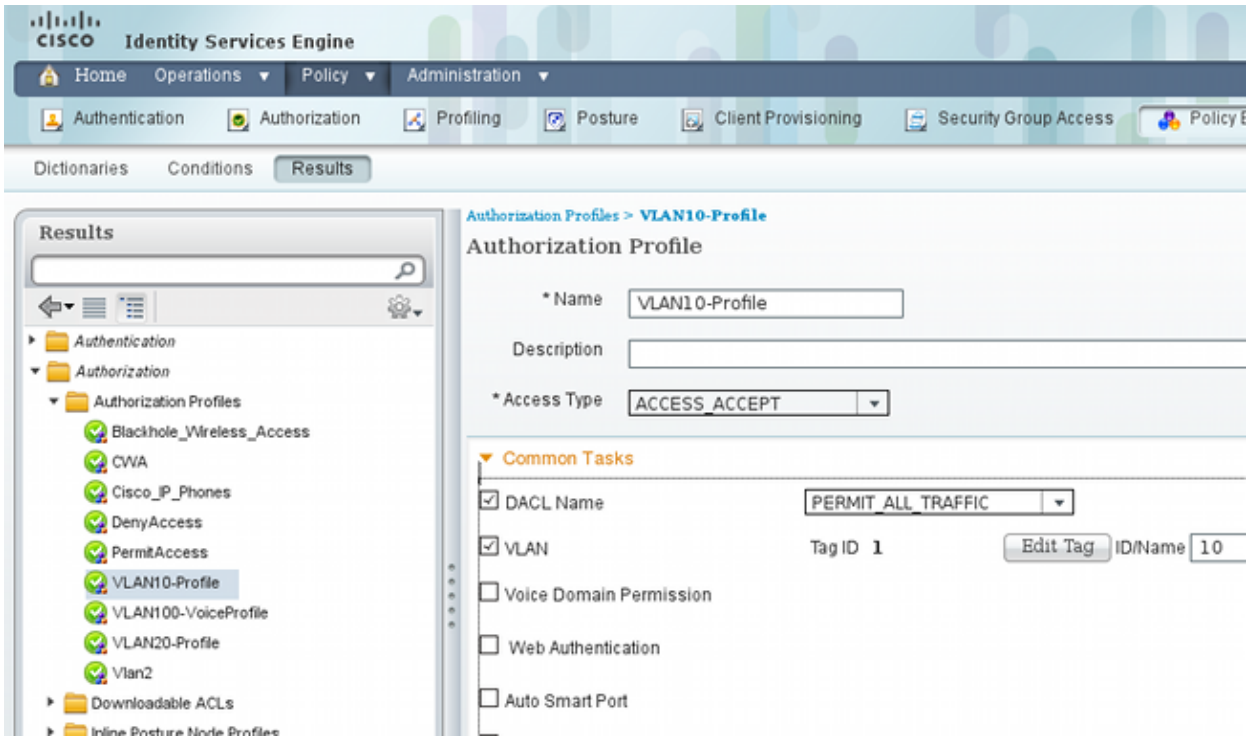


The username **cisco** is used. Configure MS Windows XP for Extensible Authentication Protocol-Protected EAP (EAP-PEAP) with these credentials.

On the ISE, the default authentication policies are used (do not change this). The first is the policy for MAB authentication, and the second is 802.1x:



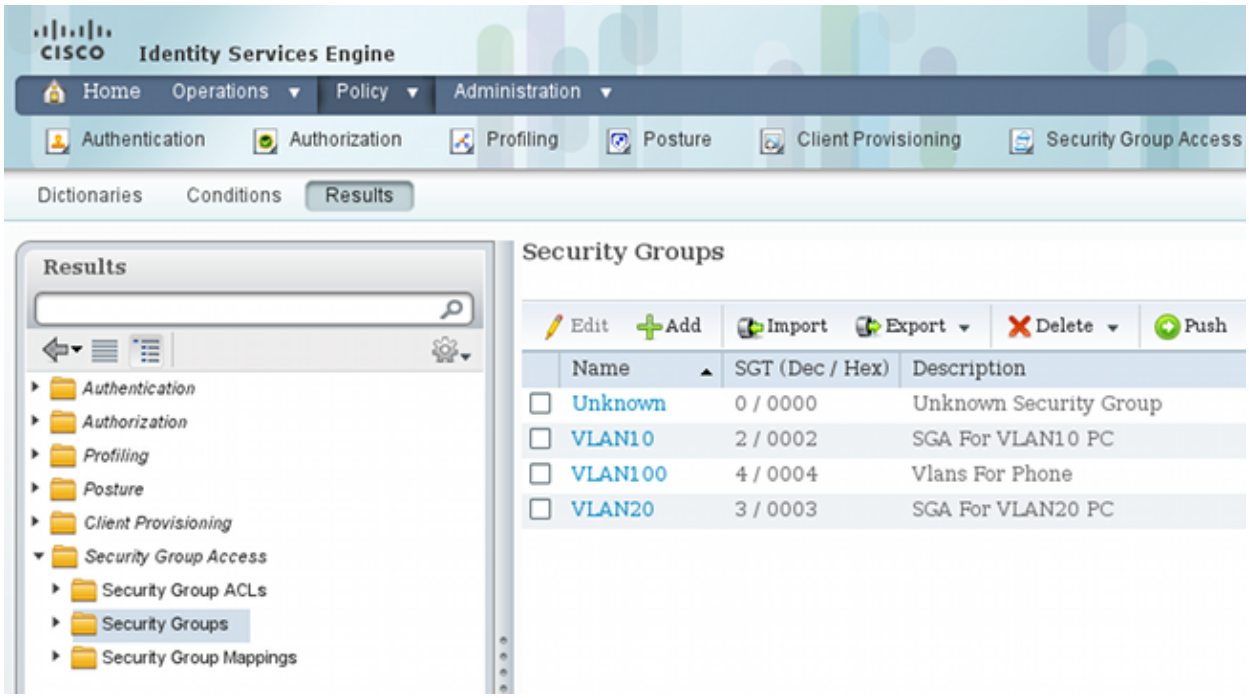
In order to configure authorization policies, you must define authorization profiles under **Policy > Results > Authorization > Authorization Profiles**. The VLAN10-Profile with Downloadable ACL (DACL), which allows for all traffic, is used for the MS Windows 7 profile:



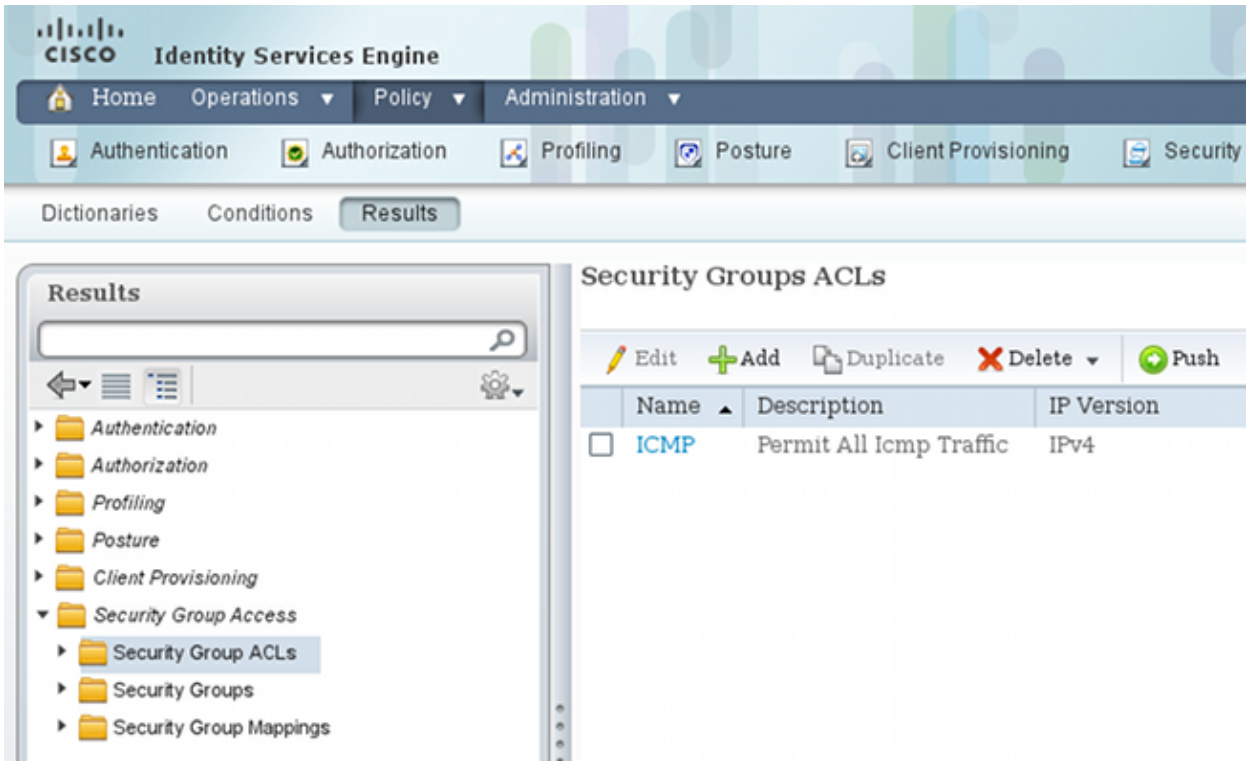
A similar configuration, VLAN20-Profile, is used for MS Windows XP with the exception to VLAN number (20).

In order to configure the SGT groups (tags) on ISE, navigate to **Policy > Results > Security Group Access > Security Groups**.

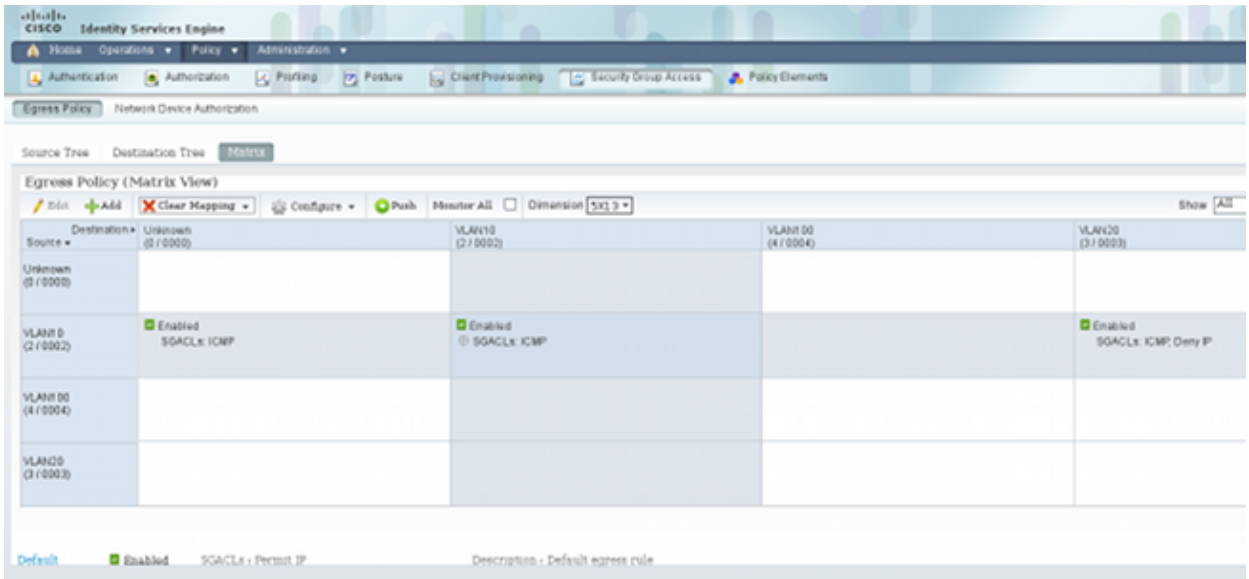
Note: It is not possible to choose a tag number; it is selected automatically by the first free number except 1. You can configure the SGT name only.



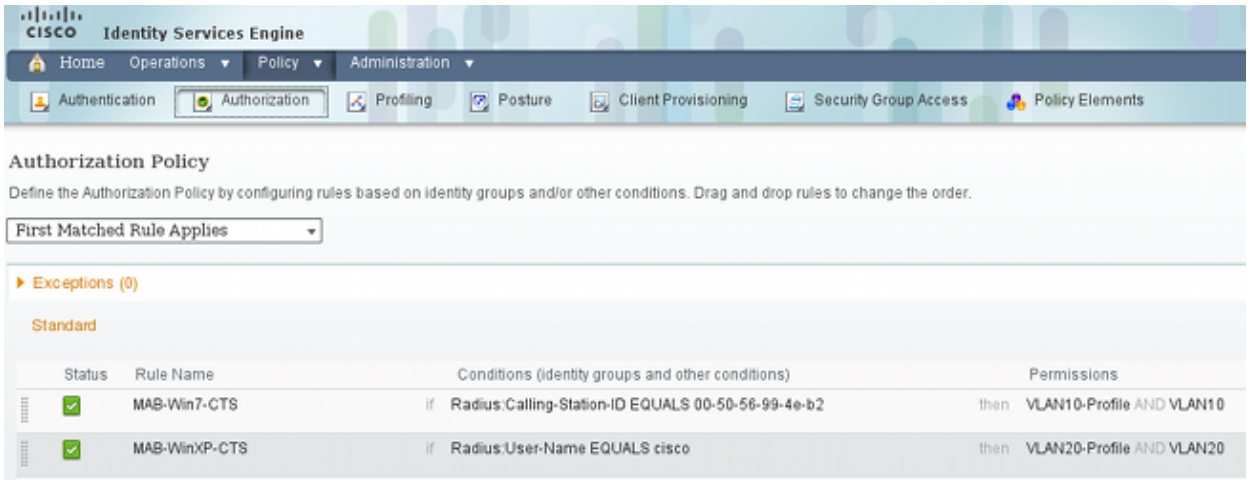
In order to create the SGACL to permit Internet Control Message Protocol (ICMP) traffic, navigate to **Policy > Results > Security Group Access > Security Group ACLs**:



In order to create policies, navigate to **Policy > Security Group Access > Egress Policy**. For traffic between VLAN10 and the unknown VLAN or VLAN10 or VLAN20, the ICMP ACL is used (**permit icmp**):



In order to set authorization rules, navigate to **Policy > Authorization**. For MS Windows 7 (specific MAC address), **VLAN10-Profile** is used, returning VLAN10 and DACL, and the security profile VLAN10 with the SGT named **VLAN10**. For MS Windows XP (specific username), **VLAN20-Profile** is used, returning VLAN 20 and DACL, and the security profile VLAN20 with the SGT named **VLAN20**.



Finish the switch and ASA configuration in order for them to accept the SGT RADIUS attributes.

CTS Configuration on the ASA and the 3750X

You must configure basic CTS settings. On the 3750X, you must indicate from which server policies should be downloaded:

```
aaa authorization network ise group radius
cts authorization list ise
```

On the ASA, only the AAA server is needed along with CTS that points to that server:

```
aaa-server ISE protocol radius
aaa-server ISE (mgmt) host 10.48.66.129
 key *****
cts server-group ISE
```

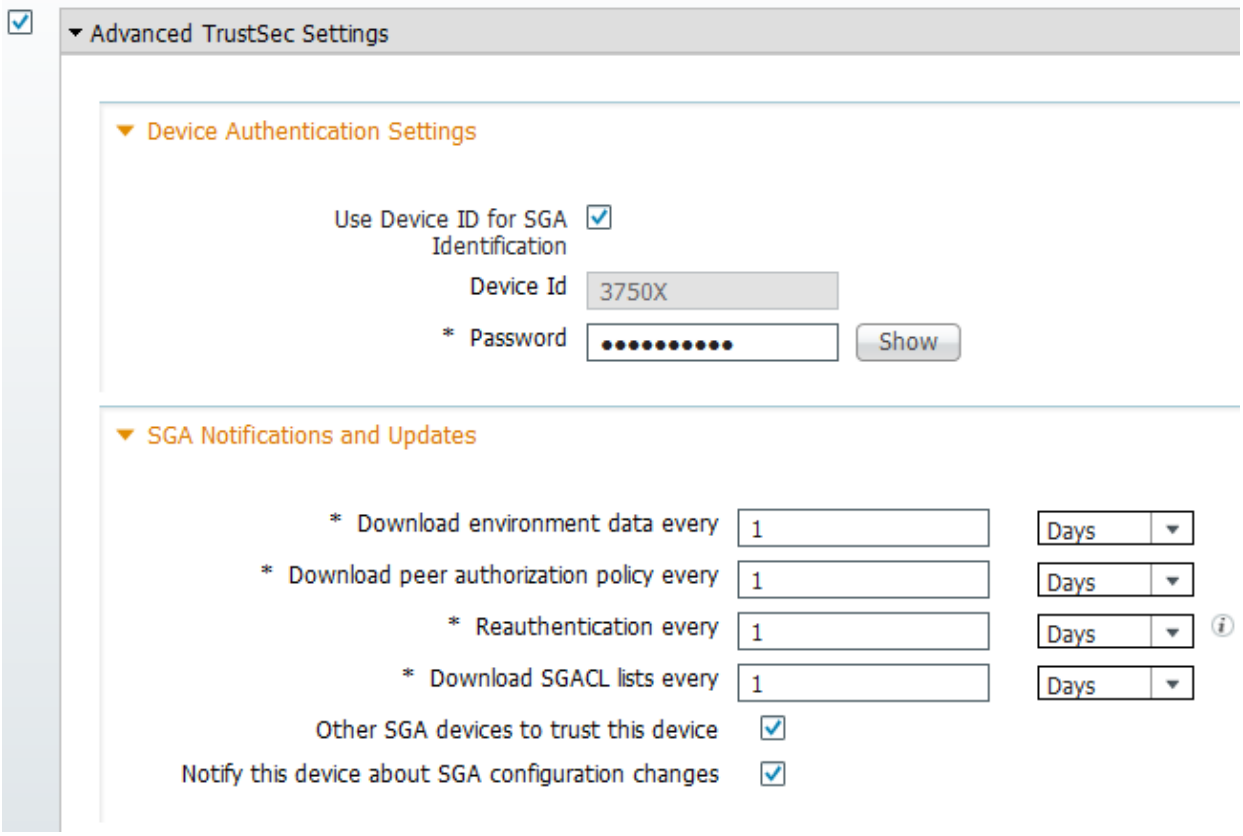
Note: On the 3750X, you must explicitly point to the ISE server with the **group radius** command. This is because the 3750X uses automatic PAC provisioning.

PAC Provisioning on the 3750X (Automatic) and the ASA (Manual)

Each device in the CTS cloud must authenticate to the authentication server (ISE) in order to be trusted by other devices. It uses the Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST) method (RFC 4851) for this. This method requires you to have PAC delivered out-of-band. This process is also called **phase0**, and is not defined in any RFC. PAC for EAP-FAST has a similar role as the certificate for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). PAC is used in order to establish a secure tunnel (phase1), which is needed for authentication in phase2.

PAC Provisioning on the 3750X

The 3750X supports automatic PAC provisioning. A shared password is used on the switch and the ISE in order to download PAC. That password and ID must be configured on the ISE under **Administration > Network Resources > Network Devices**. Select the switch, and expand the **Advanced TrustSec Settings** section in order to configure:



In order to have PAC use these credentials, enter these commands:

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
  AID: C40A15A339286CEAC28A50DBBAC59784
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: C40A15A339286CEAC28A50DBBAC59784
    I-ID: 3750X
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 08:04:40 UTC Sep 25 2013
  PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC59784000600940003
  010094F559DAE0C837D7847F2454CAD7E80B0000001351C8235900093A803D7D427BFB5C6F0FBBDF
  7EDF0818C58FECF97F8BDECF1B115FB0240260ADA8C96A46AA2A64C9EA2DB51E0E886768CA2D133D
  2468D9D33339204BAA7E4CA2DE8E37FF1EB5BCB343408E9847998E301C26DDC6F91711F631A5B4C7
  C2CB09EAB028630A3B22901FE3EF44F66FD019D09D2C46D92283
  Refresh timer is set for 2y24w
```

PAC Provisioning on the ASA

The ASA supports only manual PAC provisioning. This means that you must generate it manually on the ISE (in Network Devices/ASA):

Then the file must be installed (for example, with FTP):

```
bsns-asa5510-17(config)# cts import-pac ftp://ftp:ftp@10.147.25.80/ASA.pac
password ciscocisco
!PAC Imported Successfully

bsns-asa5510-17(config)# show cts pac

  PAC-Info:
    Valid until: Jul 04 2014 13:33:02
    AID:         c40a15a339286ceac28a50dbbac59784
    I-ID:        ASA
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200a8000300010004001 0c40a15a339286ceac28a50dbbac597840006008c000301
    0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
    e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
    c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
    7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

Environment Refresh on the ASA and the 3750X

At this stage, both devices have PAC installed correctly and automatically start to download the ISE environment data. This data is basically tag numbers and their names. In order to trigger an environment refresh on the ASA, enter this command:

```
bsns-asa5510-17# cts refresh environment-data
```

In order to verify it on the ASA (unfortunately you cannot see the specific SGT tags/names, but it is verified later), enter this command:

```
bsns-asa5510-17(config)# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          05:05:16 UTC Apr 14 2007
Env-data expires in:       0:23:56:15 (dd:hr:mm:sec)
Env-data refreshes in:     0:23:46:15 (dd:hr:mm:sec)
```

In order to verify it on 3750X, trigger an environment refresh with this command:

```
bsns-3750-5#cts refresh environment-data
```

In order to verify the results, enter this command:

```
bsns-3750-5#show cts environment-data
```

```
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-01:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
          Status = ALIVE    flag(0x11)
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
          deadtime = 20 secs
Security Group Name Table:
  0001-60 :
    0-47:Unknown
    2-47:VLAN10
    3-47:VLAN20
    4-47:VLAN100
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 05:33:49 UTC Thu Apr 7 2011
Env-data expires in   0:16:46:50 (dd:hr:mm:sec)
Env-data refreshes in 0:16:46:50 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

This shows that all tags and corresponding names are correctly downloaded.

Port Authentication Verification and Enforcement on the 3750X

After the 3750X has the environment data, you must verify that the SGTs are applied to authenticated sessions.

In order to verify if MS Windows 7 is authenticated correctly, enter this command:

```
bsns-3750-5#show authentication sessions interface g1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5699.4eb2
           IP Address:  192.168.1.200
            User-Name:  00-50-56-99-4E-B2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  10
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0002-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A800010000001002B67334C
      Acct Session ID:  0x00000179
               Handle:  0x94000101

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

The output shows that **VLAN10** is used along with the **SGT 0002** and DACL permitting for all traffic.

In order to verify if MS Windows XP is authenticated correctly, enter this command:

```
bsns-3750-5#sh authentication sessions interface g1/0/1
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  20
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0003-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80001000000FE2B67334C
      Acct Session ID:  0x00000177
               Handle:  0x540000FF

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

The output shows that **VLAN 20** is used along with the **SGT 0003** and DACL permitting for all traffic

IP addresses are detected with the **ip device tracking** functionality. The DHCP switch should be configured for **dhcp snooping**. Then, after the snooping DHCP response, it learns the IP address of the client. For a statically-configured IP address (like in this example), the **arp snooping** functionality is used, and a PC must send any packet for the switch to be able to detect its IP address.

For **device tracking**, a hidden command might be needed in order to activate it on ports:

```
bsns-3750-5#ip device tracking interface g1/0/1
bsns-3750-5#ip device tracking interface g1/0/2
bsns-3750-5#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface                STATE
---------------------------------------------------------------------
192.168.1.200   0050.5699.4eb2  10   GigabitEthernet1/0/2     ACTIVE
192.168.2.200   0050.5699.4ea1  20   GigabitEthernet1/0/1     ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:
  Gi1/0/1, Gi1/0/2
```

Policy Refresh on the 3750X

The 3750X (unlike the ASA) can download policies from the ISE. Before it downloads and enforces a policy, you must enable it with these commands:

```
bsns-3750-5(config)#cts role-based enforcement
bsns-3750-5(config)#cts role-based enforcement vlan-list 1-1005,1007-4094
```

If you do not enable it, the policy is downloaded, but not installed and not used for enforcement.

In order to trigger a policy refresh, enter this command:

```
bsns-3750-5#cts refresh policy
Policy refresh in progress
```

In order to verify that the policy is downloaded from the ISE, enter this command:

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 2:VLAN10:
        ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

The output shows that only the necessary part of the policy is downloaded.

In the CTS cloud, the packet contains the SGT of the source host, and **enforcement is made at the destination device**. This means that the packet is forwarded from the source to the last device, which is connected directly to the destination host. That device is the point of enforcement, since it knows the SGTs of its directly-connected hosts, and knows if the incoming packet with a source SGT should be permitted or denied for the specific destination SGT.

This decision is based on policies downloaded from the ISE.

In this scenario, all the policies are downloaded. However, if you clear the MS Windows XP authentication session (SGT=VLAN20), then there is no need for the switch to download any policy (row) that corresponds to VLAN20, because there are no more devices from that SGT connected to the switch.

The Advanced (Troubleshooting) section explains how the 3750X decides which policies should be downloaded with an examination of the packet level.

SXP Exchange (the ASA as Listener, and the 3750X as Speaker)

The ASA does not support SGT. All the frames with SGT are dropped by the ASA. That is why the 3750X cannot send SGT-tagged frames to the ASA. Instead, SXP is used. This protocol allows the ASA to receive information from the switch about mapping between the IP addresses and SGT. With that information, the ASA is able to map IP addresses to SGTs and make a decision based on SGACL.

In order to configure the 3750X as a speaker, enter these commands:

```
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.1 password default mode local
```

In order to configure the ASA as a listener, enter these commands:

```
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 192.168.1.1
cts sxp connection peer 192.168.1.10 password default mode local listener
```

In order to verify that the ASA received the mappings, enter this command:

```
bsns-asa5510-17# show cts sxp sgt-map ipv4 detail
Total number of IP-SGT mappings : 2
Total number of IP-SGT mappings shown: 2

SGT         : 2:VLAN10
IPv4        : 192.168.1.200
Peer IP     : 192.168.1.10
Ins Num     : 1
Status      : Active
Seq Num     : 49

SGT         : 3:VLAN20
IPv4        : 192.168.2.200
Peer IP     : 192.168.1.10
Ins Num     : 1
Status      : Active
Seq Num     : 39
```

Now, when the ASA receives the incoming packet with the source IP address **192.168.1.200**, it is able to treat it as if it comes from **SGT=2**. For the source IP address **192.168.200.2**, it is able to treat it as if it comes from **SGT=3**. The same applies for the destination IP address.

Note: The 3750X must know the IP address of the associated host. This is done by IP device tracking. For a statically-configured IP address on the end host, the switch must receive any packet after authentication. This triggers IP device tracking in order to find its IP address, which triggers an SXP update. When only the SGT is known, it is not sent via SXP.

Traffic Filtering on ASA with SGT ACL

Here is a check of the ASA configuration:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
```

An ACL is created and applied to the inside interface. It allows for all ICMP traffic from **SGT=3** to **SGT=2** (called **VLAN10**):

```
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
access-group inside in interface inside
```

Note: You can use the tag number or tag name.

If you ping from MS Windows XP with a source IP address of **192.168.2.200** (**SGT=3**) to MS Windows 7 with an IP address of **192.168.1.200** (**SGT=2**), the ASA builds a connection:

```
%ASA-6-302020: Built outbound ICMP connection for faddr 192.168.1.200/0
(2:VLAN10) gaddr 192.168.2.200/512 laddr 192.168.2.200/512(3:VLAN20)
```

When you attempt the same with Telnet, the traffic is blocked:

```
Deny tcp src inside:192.168.2.200/2478(3:VLAN20) dst outside:192.168.1.200/23
(2:VLAN10) by access-group "inside"
```

There are more configuration options on the ASA. It is possible to use both a security tag and an IP address for both the source and the destination. This rule allows ICMP echo traffic from **SGT tag = 3** and IP address **192.168.2.200** to the SGT tag named **VLAN10** and the destination host address **192.168.1.200**:

```
access-list inside extended permit icmp security-group tag 3 host 192.168.2.200
security-group name VLAN10 host 192.168.1.200 echo
```

This can also be achieved with object groups:

```
object-group security SGT-VLAN-10
 security-group name VLAN10
object-group security SGT-VLAN-20
 security-group tag 3
object-group network host1
 network-object host 192.168.1.200
object-group network host2
 network-object host 192.168.2.200
object-group service my-icmp-echo
 service-object icmp echo

access-list inside extended permit object-group my-icmp-echo
object-group-security SGT-VLAN-20 object-group host2 object-group-security
SGT-VLAN-10 object-group host1
```

Traffic Filtering on the 3750X with Policies Downloaded from the ISE (RBACL)

It is also possible to define local policies on the switch. However, this example presents policies downloaded from the ISE. Policies defined on the ASA are allowed to use both IP addresses and SGTs (and the username from Active Directory) in one rule. Policies defined on the switch (both local and from the ISE) allow only for SGTs. If you need to use IP addresses in your rules, then filtering on the ASA is recommended.

ICMP traffic between MS Windows XP and MS Windows 7 is tested. For this, you must change the default gateway from the ASA to the 3750X on MS Windows. The 3750X has routing interfaces and is able to route the packets:

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
!
interface Vlan20
 ip address 192.168.2.10 255.255.255.0
```

The policies are already downloaded from the ISE. In order to verify them, enter this command:

```
 bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 2:VLAN10:
        ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Traffic from **VLAN10** (MS Windows 7) to **VLAN20** (MS WindowsXP) is subjected to ICMP-20 ACL, which is downloaded from the ISE:

```
bsns-3750-5#show ip access-lists ICMP-20
Role-based IP access list ICMP-20 (downloaded)
    10 permit icmp
```

In order to verify the ACL, enter this command:

```
bsns-3750-5#show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
  name   = Deny IP-00
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    deny ip

  name   = ICMP-20
  IP protocol version = IPV4
  refcnt = 6
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit icmp

  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
```

In order to verify the SGT mapping to make sure that traffic from both hosts is correctly tagged, enter this command:

```
bsns-3750-5#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.1.200           2       LOCAL
192.168.2.200           3       LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

ICMP from MS Windows 7 (**SGT=2**) to MS Windows XP (**SGT=3**) works fine with ACL ICMP-20. This is verified by checking counters for traffic from **2** to **3** (15 permitted packets):

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted
```

```
2       0       0               0               1695            224
2       2       0               -               0               -

*       *       0               0               133258          132921

2       3       0               0               0               15
```

After you attempt to use the Telnet counter, the denied packets increase (it is not permitted on ICMP-20 ACL):

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               1695            224
2       2       0               -               0               -

*       *       0               0               133281          132969

2       3       0               2               0               15
```

Note: The star (*) character shown in the output is related to all traffic that is not tagged (that column and row is called **unknown** in Matrix on the ISE, and use tag number **0**).

When you have an ACL entry with the log keyword (defined on the ISE), the corresponding packet details and actions taken are logged as in any ACL with the log keyword.

Verify

Refer to the individual configuration sections for verification procedures.

Troubleshoot

PAC Provisioning

Problems might appear when you use automatic PAC provisioning. Remember to use the **pac** keyword for the RADIUS server. Automatic PAC provisioning on the 3750X uses the EAP-FAST method with the Extensible Authentication Protocol with inner method using Microsoft's Challenge Handshake Authentication Protocol (EAP-MSCHAPv2) authentication. When you debug, you see multiple RADIUS messages that are the part of EAP-FAST negotiation used in order to build the secure tunnel, which uses EAP-MSCHAPv2 with the configured ID and password for authentication.

The first RADIUS request uses AAA **service-type=cts-pac-provisioning** in order to notify the ISE that this is a PAC request.

```
bsns-3750-5#debug cts provisioning events
bsns-3750-5#debug cts provisioning packets

*Mar  1 09:55:11.997: CTS-provisioning: New session socket: src=
10.48.66.109:57516 dst=10.48.66.129:1645
*Mar  1 09:55:11.997: CTS-provisioning: Sending EAP Response/Identity to
10.48.66.129
*Mar  1 09:55:11.997: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: Received RADIUS challenge from
```

```
10.48.66.129.
*Mar  1 09:55:12.006: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.006: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.006: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.106: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.115: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.744: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.744: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.744: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.853: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.853: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.853: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.853: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.861: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.861: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.861: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.861: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.886: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.886: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.886: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.895: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.895: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.903: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.920: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.920: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.920: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.970: CTS-pac-refresh: PAC C40A15A339286CEAC28A50DBBAC59784
refresh timer has been set for 20y30w
*Mar  1 09:55:12.970: CTS-provisioning: Ignoring key data.
*Mar  1 09:55:12.979: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.979: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.979: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: Received RADIUS reject from 10.48.66.129.
*Mar  1 09:55:12.995: CTS-provisioning: Successfully obtained PAC for A-ID
c40a15a339286ceac28a50dbbac59784
*Mar  1 09:55:12.995: CTS-provisioning: cts_provi_server_cleanup: 10.48.66.129
*Mar  1 09:55:12.995: CTS-provisioning: work complete, process terminating.
```

The **RADIUS reject** at the end of the output is expected since you already received PAC, and did not follow with a further authentication process.

Remember that PAC is required for all other communication with the ISE. But, if you do not have it, the switch still attempts an environment or policy refresh when it is configured. Then, it does not attach **cts-opaqueue** (PAC) in the RADIUS Requests, which causes the failures.

If your PAC key is wrong, this error message displays on the ISE:

```
The Message-Authenticator RADIUS attribute is invalid
```

You also see this output from debugs (**debug cts provisioning + debug radius**) on the switch if your PAC key is wrong:

```
Apr 20 10:07:11.768: CTS-provisioning: Sending EAP Response/Identity t
Apr 20 10:07:15.325: RADIUS(0000024B): Request timed out!
Apr 20 10:07:15.325: RADIUS: No response from (10.62.84.224:1645,1646) for
id 1645/37
```

If you use the modern **radius server** convention, this displays:

```
radius server KRK-ISE
 address ipv4 10.62.84.224 auth-port 1645 acct-port 1646
 pac key CISCO
```

Note: You must use the same password on the ISE that you used in the **Device Authentication Settings**.

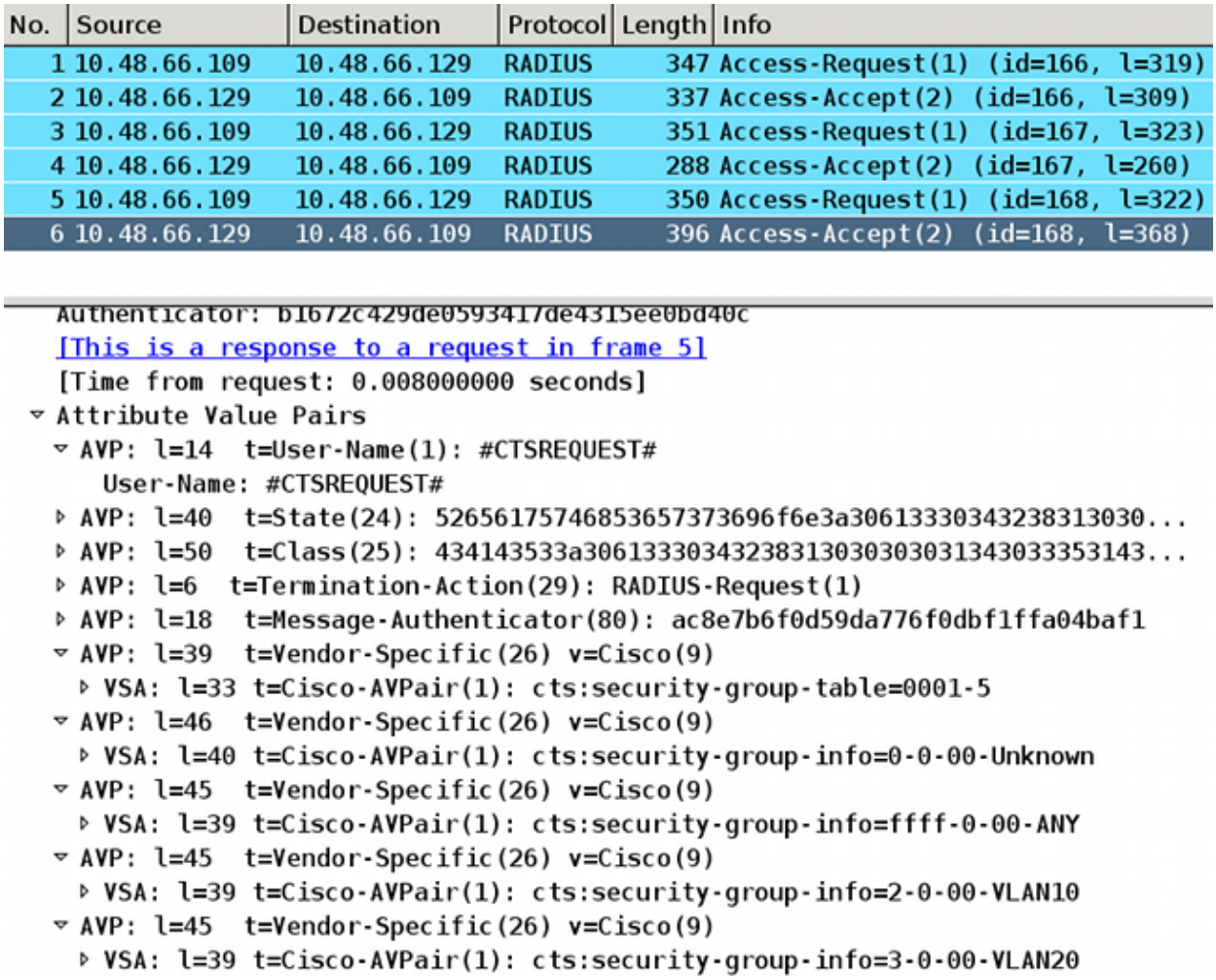
After successful PAC provisioning, this displays on the ISE:

Authentication Summary	
Logged At:	June 26,2013 1:36:32.676 PM
RADIUS Status:	PAC provisioned
NAS Failure:	
Username:	3750
MAC/IP Address:	BC:16:65:25:A5:00
Network Device:	3750X : 10.48.66.109 :
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Environment Refresh

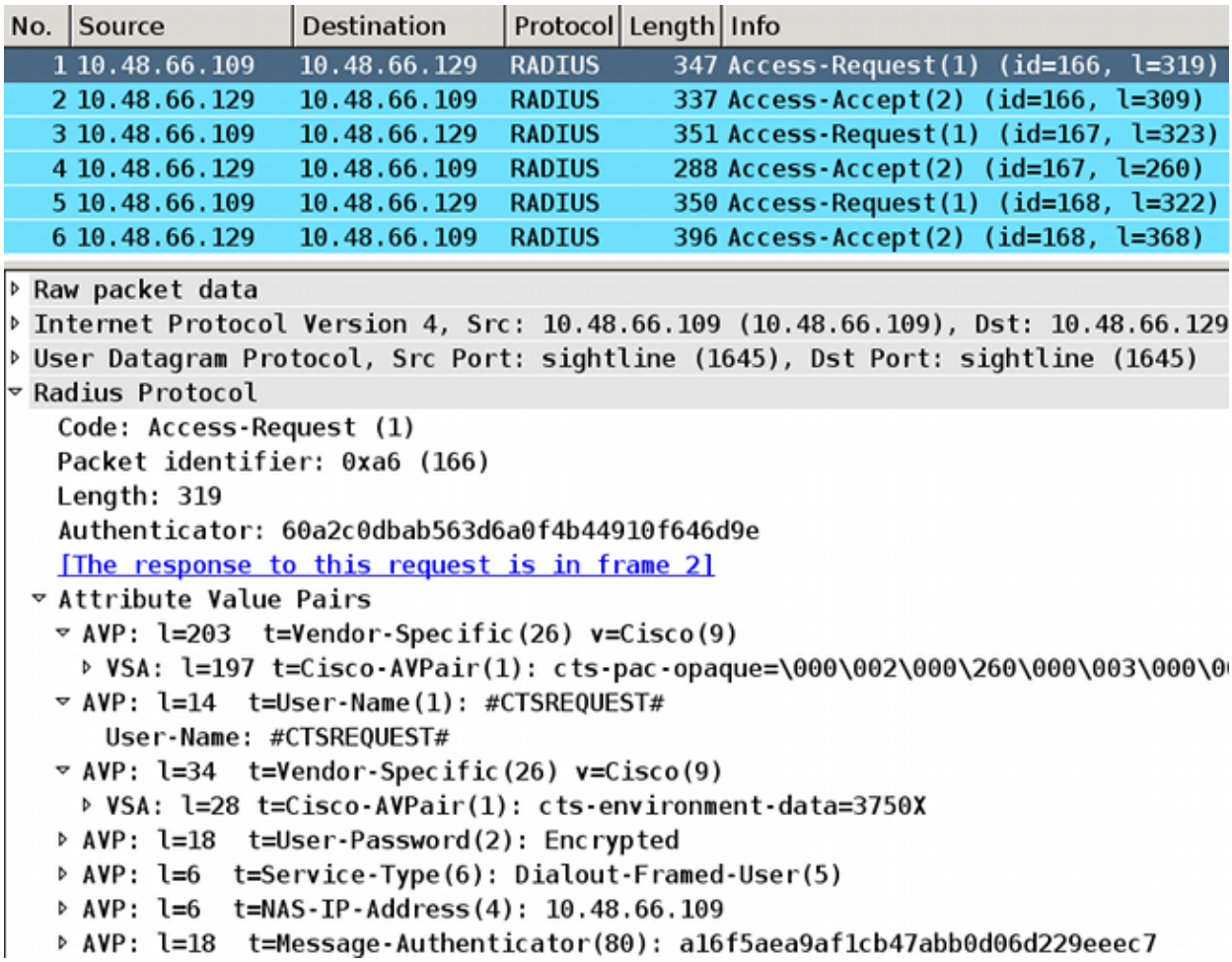
The environment refresh is used in order to obtain basic data from the ISE, which includes the SGT number and name. The packet level shows that it is only three RADIUS requests and responses with attributes.

For the first request, the switch receives **CTSServerlist** name. For the second one, it receives the details for that list, and for the last one, it receives all the SGTs with tags and names:



Here you see the default **SGT 0**, **ffff**, and also two custom-defined: SGT tag 2 is named **VLAN10** and SGT tag 3 is named **VLAN20**.

Note: All RADIUS requests include **cts-pac-opaque** as a result of PAC provisioning.



On the 3750X, you should see debugs for all three RADIUS responses and the corresponding lists, list details, and the specific SGT-inside list:

```
bsns-3750-5#debug cts environment-data all

*Mar  1 10:05:07.454: CTS env-data&colon; cleanup mcast SGT table
*Mar  1 10:05:18.057: CTS env-data&colon; Force environment-data refresh
*Mar  1 10:05:18.057: CTS env-data&colon; download transport-type =
CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057:     cts_env_data START: during state env_data_complete,
got event 0(env_data_request)
*Mar  1 10:05:18.057: @@@ cts_env_data START: env_data_complete ->
env_data_waiting_rsp
*Mar  1 10:05:18.057: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: cts_env_data_is_complete: FALSE, req(x0), rec(x0),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)AAA req(x7C3DF10)
*Mar  1 10:05:18.057: cts_aaa_attr_add: AAA req(0x7C3DF10)
*Mar  1 10:05:18.057:   username = #CTSREQUEST#
*Mar  1 10:05:18.057:   cts-environment-data = 3750X
*Mar  1 10:05:18.057: cts_aaa_req_send: AAA req(0x7C3DF10) successfully sent to AAA.
*Mar  1 10:05:18.083: cts_aaa_callback: (CTS env-data)AAA req(0x7C3DF10)
response success
*Mar  1 10:05:18.083:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.083:   AAA attr: server-list = CTSServerList1-0001.
```

```
*Mar  1 10:05:18.083:   AAA attr: security-group-tag = 0000-00.
*Mar  1 10:05:18.083:   AAA attr: environment-data-expiry = 86400.
*Mar  1 10:05:18.083:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.083: CTS env-data&colon; Receiving AAA attributes
  CTS_AAA_SLIST
    slist name(CTSServerList1) received in 1st Access-Accept
    slist name(CTSServerList1) created
  CTS_AAA_SECURITY_GROUP_TAG - SGT = unicast-unknown-00
  CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
  CTS_AAA_SGT_NAME_LIST
    table(0001) received in 1st Access-Accept
    old name(), gen()
    new name(0001), gen(50)
  CTS_AAA_DATA_END
*Mar  1 10:05:18.083:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.083: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.083: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.083: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.083: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.083: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)AAA req(x792FFD0)
*Mar  1 10:05:18.083: cts_aaa_attr_add: AAA req(0x792FFD0)
*Mar  1 10:05:18.091:   username = #CTSREQUEST#
*Mar  1 10:05:18.091:   cts-server-list = CTSServerList1
*Mar  1 10:05:18.091: cts_aaa_req_send: AAA req(0x792FFD0) successfully sent to AAA.
*Mar  1 10:05:18.099: cts_aaa_callback: (CTS env-data)AAA req(0x792FFD0)
response success
*Mar  1 10:05:18.099:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.099:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.099:   AAA attr: server = c40a15a339286ceac28a50dbbac59784:
10.48.66.129:1812.
*Mar  1 10:05:18.099: CTS env-data&colon; Receiving AAA attributes
  CTS_AAA_SLIST
    2nd Access-Accept slist name(CTSServerList1), gen(0001)
  CTS_AAA_SERVERS
    server (c40a15a339286ceac28a50dbbac59784:10.48.66.129:1812) added
  CTS_AAA_DATA_END
*Mar  1 10:05:18.099:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.099: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.099: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.099: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: env_data_request_action: state = WAITING_RESPONSE
```

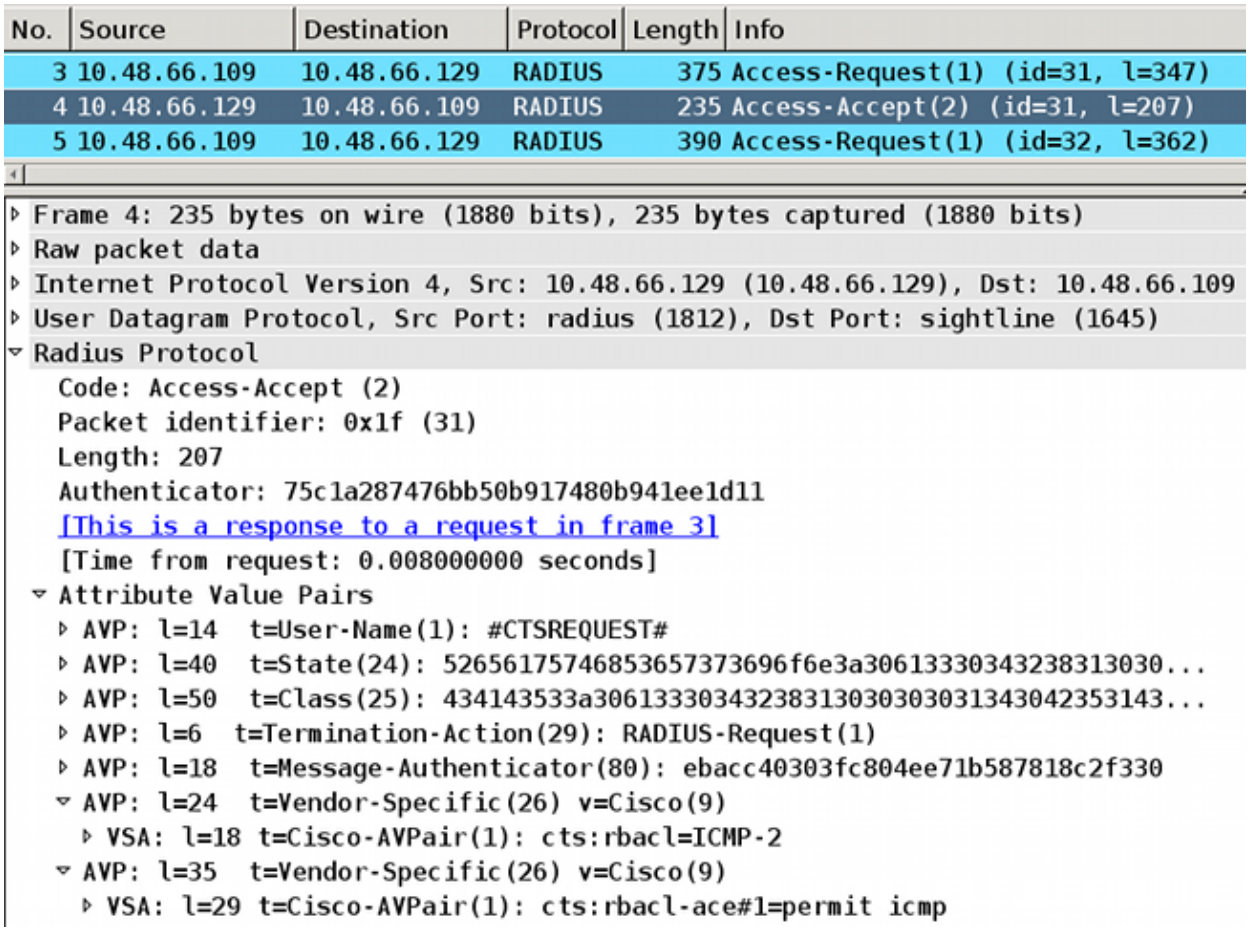
```
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)Using private server group
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)AAA req(x7A6C4AC)
*Mar  1 10:05:18.099: cts_aaa_attr_add: AAA req(0x7A6C4AC)
*Mar  1 10:05:18.099:   username = #CTSREQUEST#
*Mar  1 10:05:18.099:   cts-security-group-table = 0001
*Mar  1 10:05:18.099: cts_aaa_req_send: AAA req(0x7A6C4AC) successfully sent to AAA.
*Mar  1 10:05:18.108: cts_aaa_callback: (CTS env-data)AAA req(0x7A6C4AC)
response success
*Mar  1 10:05:18.108:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.108:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 0-0-00-Unknown.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = ffff-0-00-ANY.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 2-0-00-VLAN10.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 3-0-00-VLAN20.
*Mar  1 10:05:18.108:  CTS env-data&colon; Receiving AAA attributes
  CTS_AAA_SGT_NAME_LIST
    table(0001) received in 2nd Access-Accept
    old name(0001), gen(50)
    new name(0001), gen(50)
  CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-unknown-00
   flag (128) server name (Unknown) added
   name (0001), request (1), receive (1)
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-default-00
   flag (128) server name (ANY) added
   name (0001), request (1), receive (1)
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 2-00
   flag (128) server name (VLAN10) added
   name (0001), request (1), receive (1)
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 3-00
   flag (128) server name (VLAN20) added
   name (0001), request (1), receive (1)
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_DATA_END
*Mar  1 10:05:18.108:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.108: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.108: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.108: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.116: cts_env_data_is_complete: TRUE, req(x2085), rec(x2C87),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.116:     cts_env_data ASSESSING: during state env_data_assessing,
got event 4(env_data_complete)
*Mar  1 10:05:18.116: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_complete
*Mar  1 10:05:18.116: env_data_complete_enter: state = COMPLETE
*Mar  1 10:05:18.116: env_data_install_action: state = COMPLETE
```

Policy Refresh

The policy refresh is supported only on the switch. It is similar to the environment refresh. These are simply RADIUS Requests and Accepts.

The switch asks for all the ACLs within the default list. Then, for each ACL that is not up-to-date (or does not exist), it sends another request to obtain the details.

Here is an example response when you ask for ICMP-20 ACL:



Remember that you must have **cts role-based enforcement** configured in order to enforce that ACL.

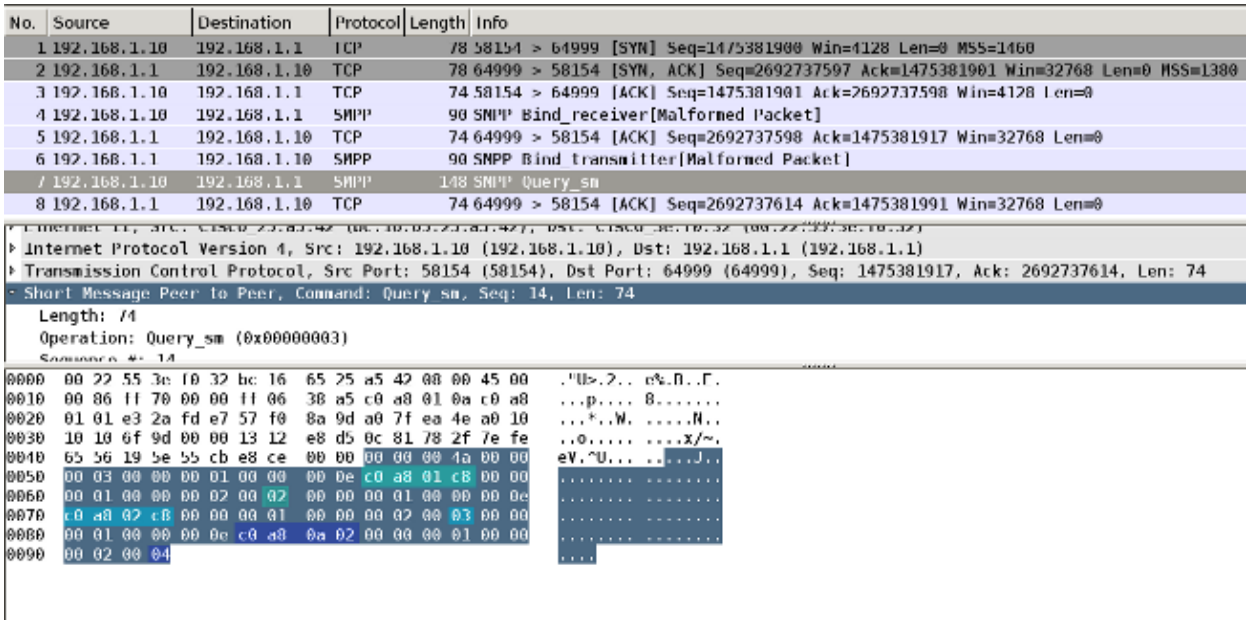
Debugs indicate if there are changes (based on gen ID). If so, you can uninstall the old policy if needed, and install a new one. This includes ASIC programming (hardware support).

```
bsns-3750-5#debug cts all

Mar 30 02:39:37.151:  CTS authz entry: peer(Unknown-2) Receiving AAA attributes
    rcv rbacl list: flags: req(81)rcv(0)wait(80)prev(0)install(880)
     - SGT = 2-01:VLAN10
     - SGT = 2-01:VLAN10
    current arg_cnt=8, expected_num_args=11
    3rd Access-Accept rbacl received name(ICMP), gen(20)
    received_policyp->sgt(2-01:VLAN10)
    existing sgt_policy(73FFDB4) sgt(2-01:VLAN10)
    RBACL name(ICMP-20)flag(40000000) already exists
   acl_listp(740266C) old_acl_infop(0),exist_rbacl_type(0)
  CTS_AAA_AUTHORIZATION_EXPIRY = 86400.
  CTS_AAA_DATA_END

Mar 30 02:39:37.176: cts_authz_entry_complete_action: Policy download complete -
peer(Unknown-2) SGT(2-01:VLAN10) status(RBACL-POLICY SUCCEEDED)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV6
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(C0000000)
```

```
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV4
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(40000000)

Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV6
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(C0000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Waiting for more RBM callback
for remaining IP version(40000000) RBACL policy(73FFDB4) for SGT(2-01:VLAN10)
flag(41400001)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb:
Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV4
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(40000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Program RBACL policy(73FFDB4)
for SGT(2-01:VLAN10) flag(41400001) success
```

SXP Exchange

The SXP update is triggered by the IP device-tracking code that finds the IP address of the device. Then, Short Message Peer-to-Peer (SMPP) protocol is used in order to send the updates. It uses **TCP option 19** for authentication, which is the same as Border Gateway Protocol (BGP). The SMPP payload is not encrypted. Wireshark does not have a proper decoder for the SMPP payload, but it is easy to find data inside it:



- The first one, **c0 a8 01 c8**, is **192.168.1.200** and has **tag 2**.
- The second one, **c0 a8 02 c8**, is **192.168.2.200** and has **tag 3**.
- The third one, **c0 a8 0a 02,** is **192.168.10.2** and has **tag 4** (this one was used in order to test phone **SGT=4**)

Here are some debugs on the 3750X after IP device tracking finds the IP address of MS Windows 7:

```
bsns-3750-5#debug cts sxp message
bsns-3750-5#debug cts sxp internal
bsns-3750-5#debug cts sxp conn
bsns-3750-5#debug cts sxp mdb
bsns-3750-5#debug cts sxp error

Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_message_event = CTS_SXPMSG_REQUEST
Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_request  CTS_SXPMSG_REQ_CONN_NVGEN
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_process_request boolean set
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_send_request set boolean after
Apr  7 00:40:05.418: CTS-SXP-CONN:is_cts_sxp_rf_active
Apr  7 00:40:05.418: CTS-SXP-MDB:sxp_export_ipsgt_change 192.168.1.200/32 add 1
```

Here are the corresponding debugs on the ASA:

```
bsns-asa5510-17# debug cts sxp all

%ASA-7-776018: CTS SXP: Binding 192.168.1.200->2:VLAN10 from peer 192.168.1.10
(instance 1) added in SXP database.
%ASA-7-776019: CTS SXP: Binding 192.168.1.200->2:VLAN10 added. Update binding
manager.
%ASA-6-776251: CTS SGT-MAP: Binding 192.168.1.200->2:VLAN10 from SXP added to
binding manager.
%ASA-7-776014: CTS SXP: SXP received binding forwarding request (add) binding
192.168.1.200->2:VLAN10.
```

In order to see more debugs on the ASA, you can enable the debugging verbosity level:

```
bsns-asa5510-17# debug cts condition level detail
debug cts condition level detail is enable
```

SGACL on the ASA

After the ASA correctly installs the SGT mappings received by SXP, the security-groups ACL should work fine. When you encounter problems with the mapping, enter:

```
bsns-asa5510-17# debug cts sgt-map
```

The ACL with the security-group works exactly the same as it does for the IP address or the user identity. The logs reveal problems, and the exact entry of the ACL that was hit.

Here is a ping from MS Windows XP to MS Windows 7 that shows that packet tracer works correctly:

```
bsns-asa5510-17# packet-tracer input inside icmp 192.168.2.200 8 0 192.168.1.200
detailed
<output ommitted>

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xaaf2ae80, priority=13, domain=permit, deny=false
```

```
        hits=185, user_data=0xaa2f5040, cs_id=0x0, use_real_addr, flags=0x0,
protocol=1
        src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=3:VLAN20
        dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=2:VLAN10, dscp=0x0
        input_ifc=inside, output_ifc=any

<output ommitted>
```

Related Information

- **Cisco TrustSec Configuration Guide for 3750**
- **Cisco TrustSec Configuration Guide for ASA 9.1**
- **Cisco TrustSec Deployment and RoadMap**
- **Technical Support & Documentation - Cisco Systems**

Updated: Jan 21, 2016 Document ID: 116497
