ASA 和 Catalyst 3750X 系列交换机 TrustSec 配置示例和故障排除指南

目录

简介

本文描述如何在思科安全自适应安全设备(ASA)和Cisco Catalyst 3750X系列交换机(3750X)上配置Cisco TrustSec(CTS)。

为了了解安全组标记(SGT)和IP地址之间的映射，ASA使用SGT交换协议(SXP)。然后，使用基于SGT的访问控制列表(ACL)来过滤流量。3750X从思科身份服务引擎(ISE)下载基于角色的访问控制列表(RBACL)策略，并根据这些策略过滤流量。本文详细介绍数据包级别，以便描述通信运行方式和预期调试。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- CTS组件
- ASA和Cisco IOS®的CLI配置

使用的组件

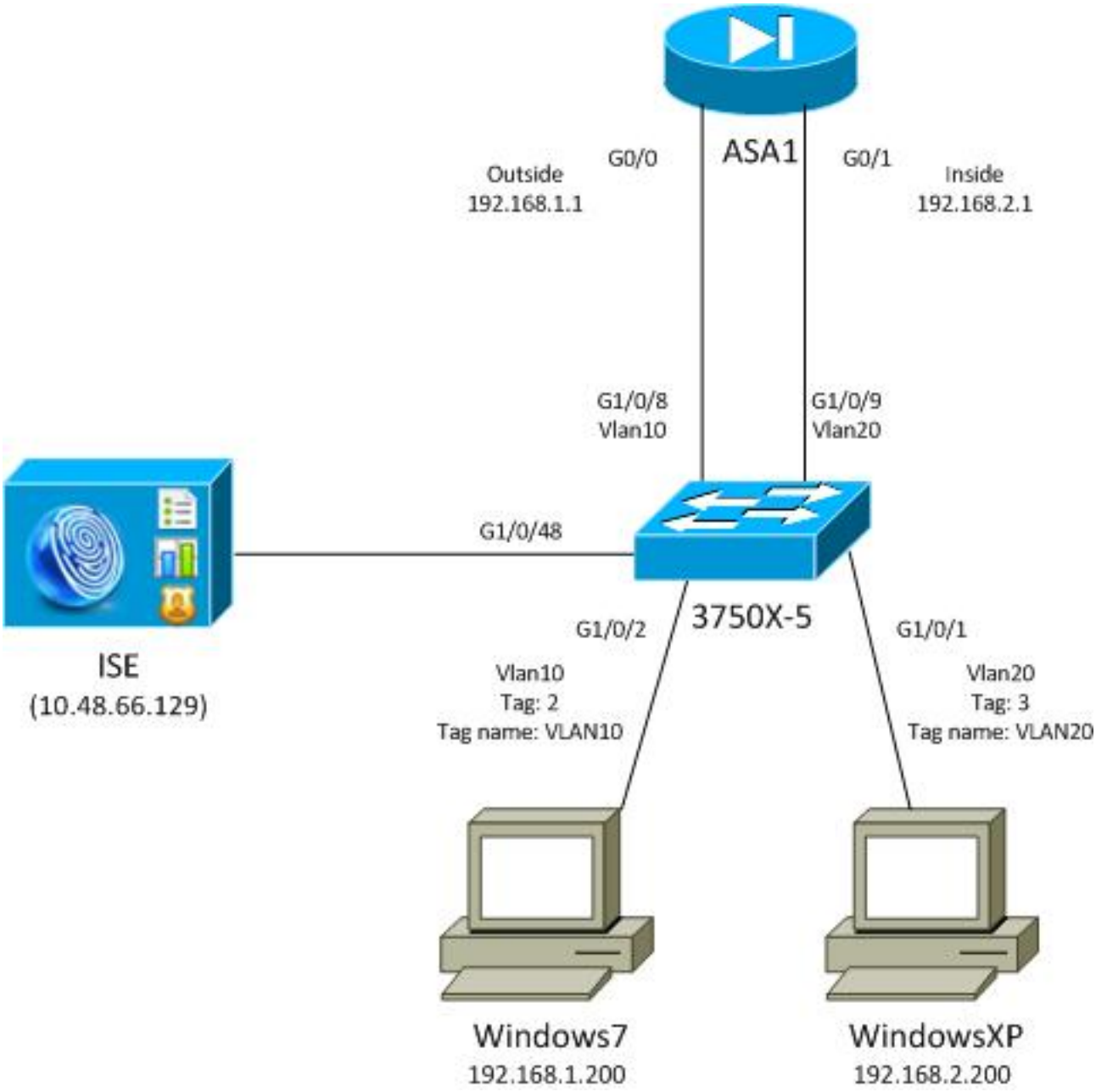
本文档中的信息基于以下软件和硬件版本：

- Cisco ASA软件9.1版及更高版本
- Microsoft(MS)Windows 7和MS Windows XP
- Cisco 3750X软件，版本15.0及更高版本
- Cisco ISE软件1.1.4版及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图



流量传输

以下是流量：

- 3750X配置在**G1/0/1**和**G1/0/2**上，用于端口身份验证。
- ISE用作身份验证、授权和记帐(AAA)服务器。
- MAC地址绕行(MAB)用于MS Windows 7的身份验证。
- IEEE 802.1x用于MS Windows XP，以证明使用哪种身份验证方法无关紧要。

身份验证成功后，ISE返回SGT，3750X将该标记绑定到身份验证会话。交换机还使用**ip device tracking**命令获取两个站点的IP地址。然后，交换机使用SXP将SGT和IP地址之间的映射表发送到ASA。两台MS Windows PC都有指向ASA的默认路由。

ASA收到来自映射到SGT的IP地址的流量后，能够根据SGT使用ACL。此外，当您使用3750X作为路由器（两个MS Windows工作站的默认网关）时，它能够根据从ISE下载的策略过滤流量。

以下是配置和验证步骤，在本文档后面的部分中会详细介绍其中的每个步骤：

- 在3750X上使用ip device tracking命令进行端口身份验证
- 身份验证、SGT和安全组访问控制列表(SGACL)策略的ISE配置
- ASA和3750X上的CTS配置
- 3750X（自动）和ASA（手动）上的保护访问凭证(PAC)调配
- ASA和3750X上的环境更新
- 3750X上的端口身份验证验证和实施
- 3750X上的策略更新
- SXP交换（ASA作为侦听器，3750X作为扬声器）
- 使用SGT ACL在ASA上过滤流量
- 使用从ISE下载的策略在3750X上过滤流量

配置

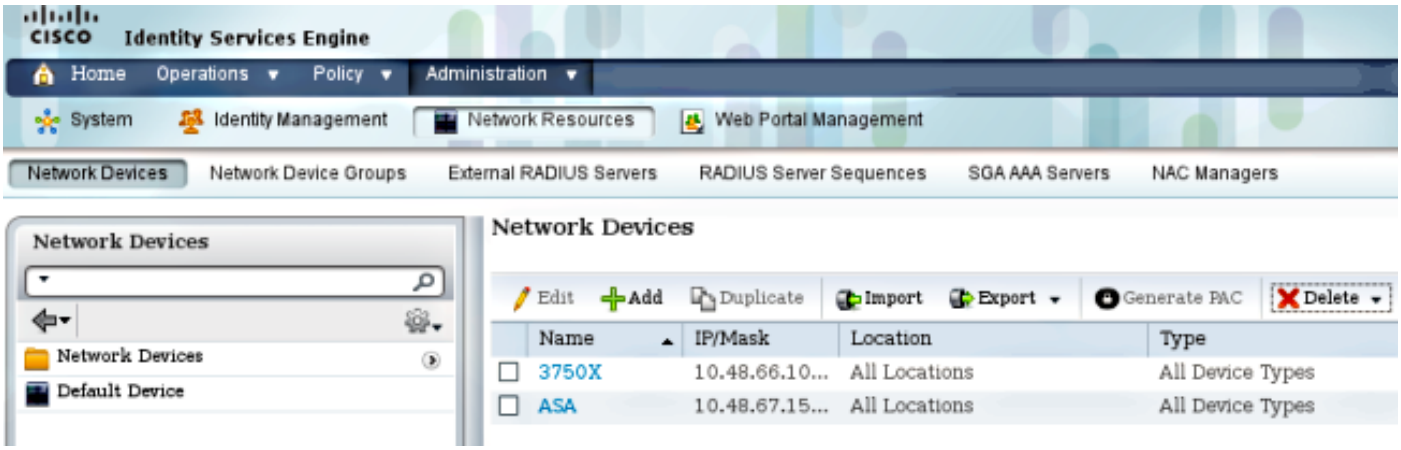
在3750X上使用*ip device tracking*命令进行端口身份验证

这是802.1x或MAB的典型配置。只有当您使用来自ISE的活动通知时，才需要RADIUS授权更改(CoA)。

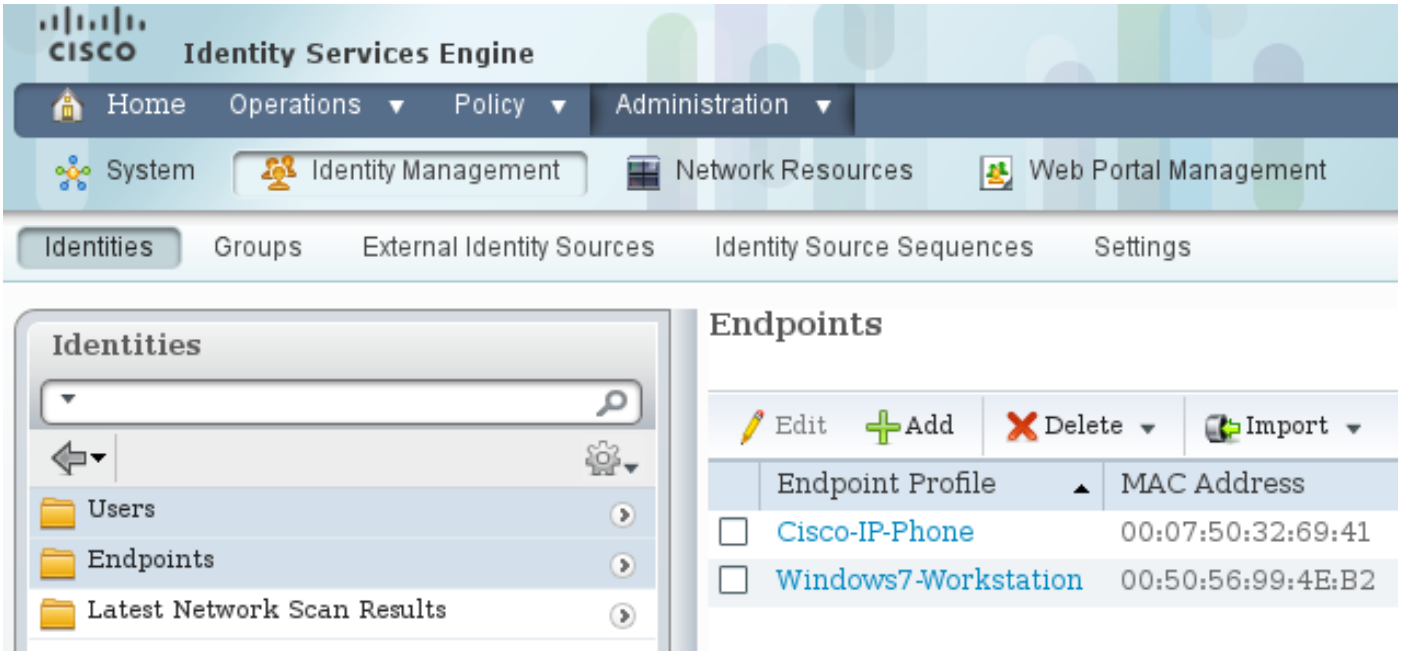
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

!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
```

身份验证、SGT和SGACL策略的ISE配置

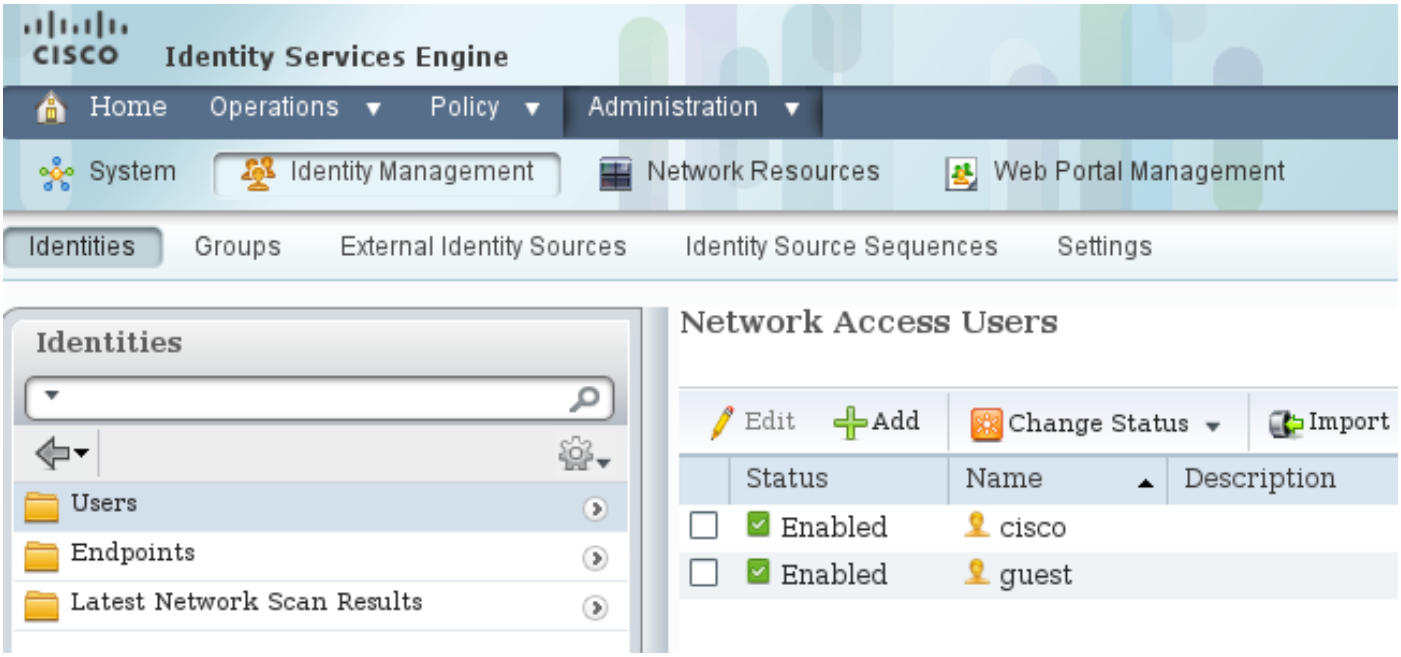
ISE必须在**Administration > Network Devices**下配置两个网络设备：



对于使用MAB身份验证的MS Windows 7，必须在**管理>身份管理>身份>终端**下创建终端身份（MAC地址）：

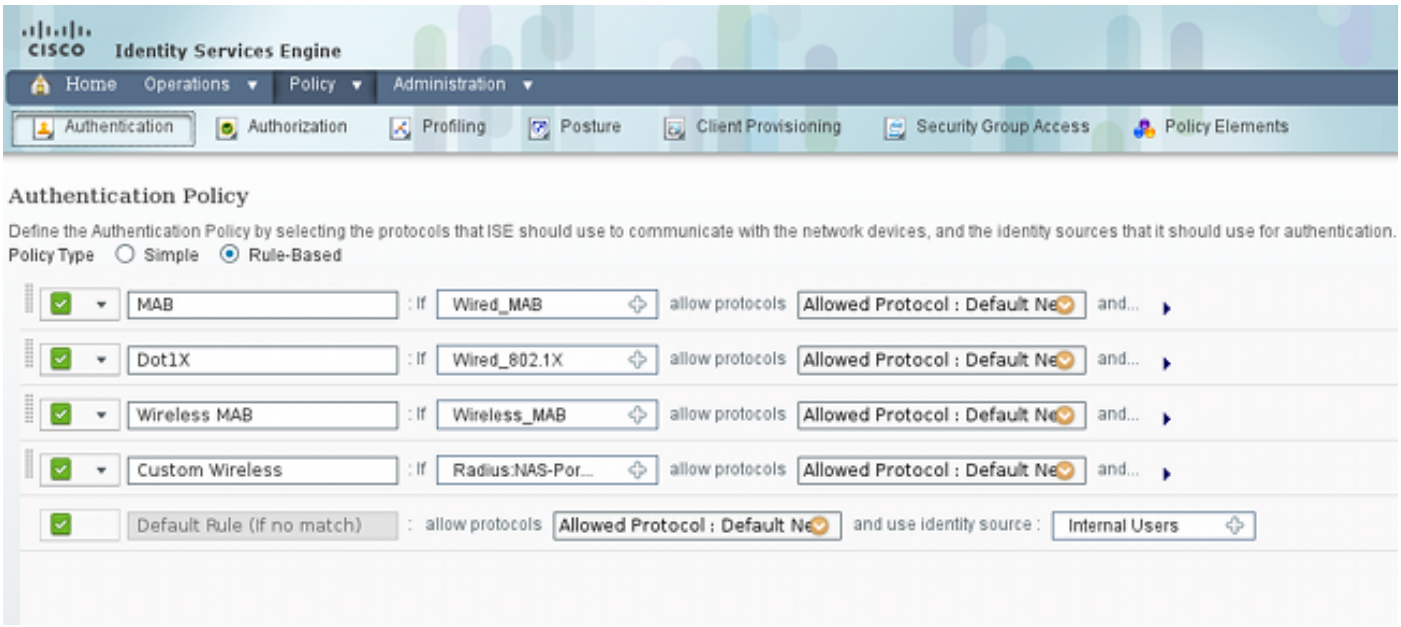


对于使用802.1x身份验证的MS Windows XP，您必须在**Administration > Identity Management > Identities > Users**下创建用户身份（用户名）：

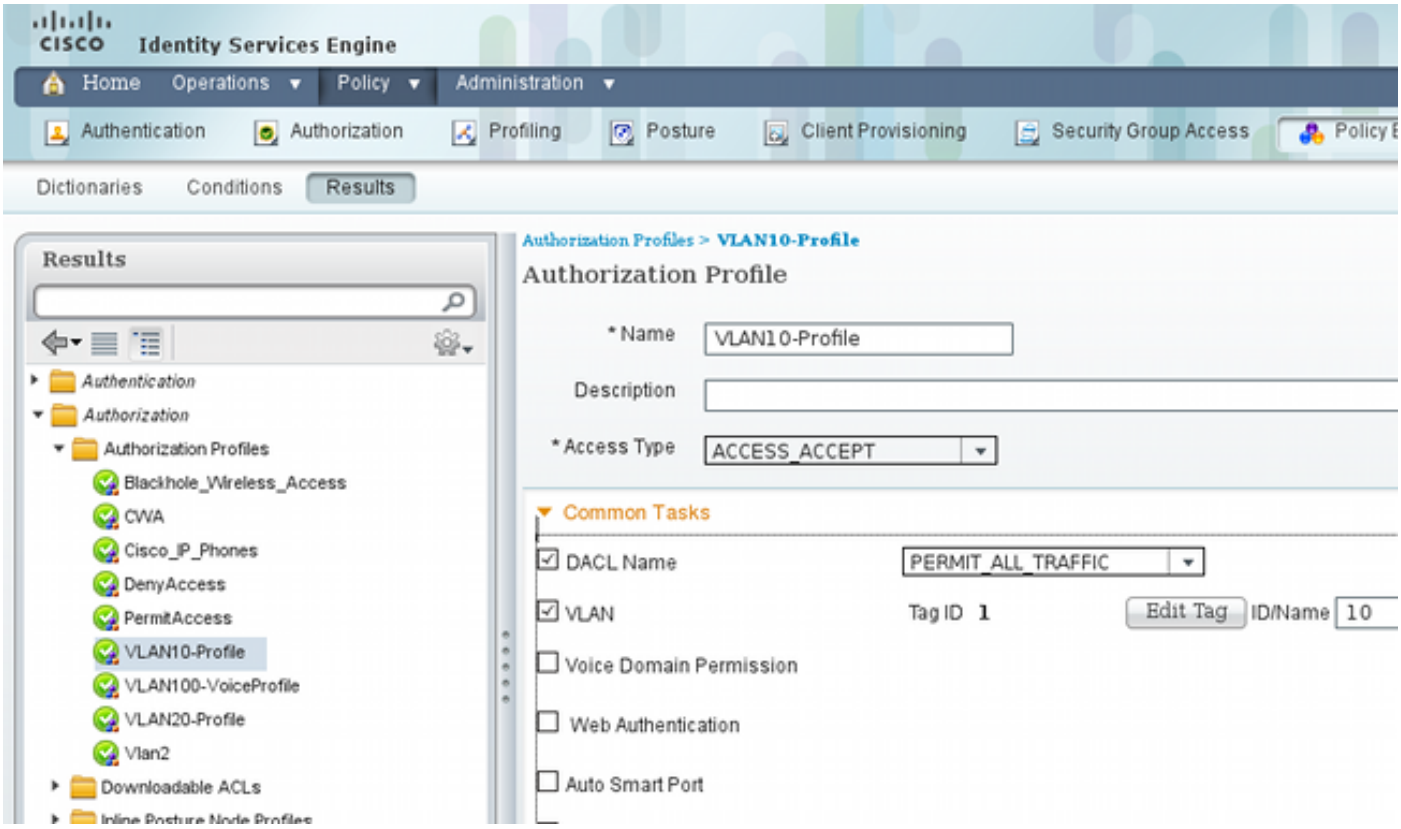


使用用户名**cisco**。使用这些凭证为MS Windows XP配置受可扩展身份验证协议保护的EAP(EAP-PEAP)。

在ISE上，使用默认身份验证策略（请勿更改）。第一个是MAB身份验证策略，第二个是802.1x:



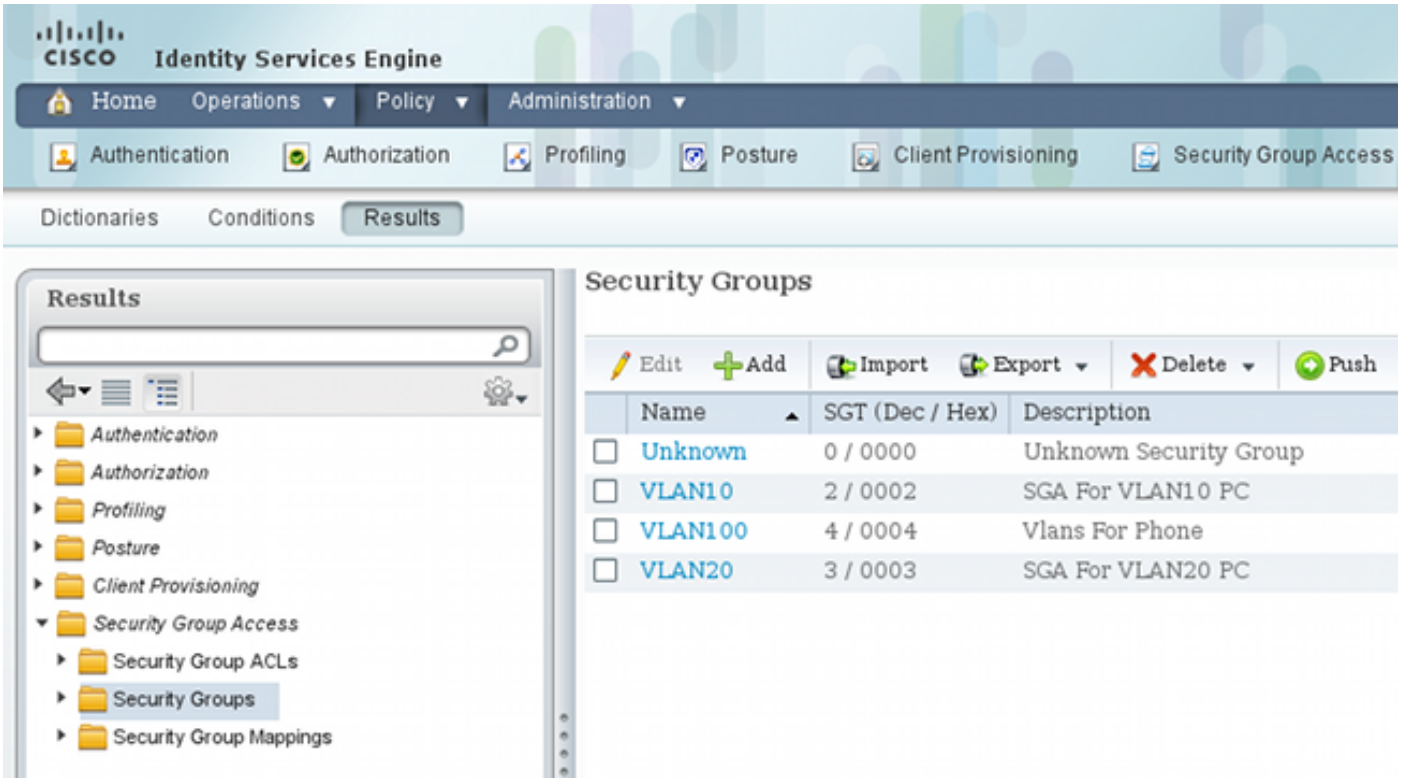
要配置授权策略，必须在**Policy > Results > Authorization > Authorization Profiles**下定义授权配置文件。包含可下载ACL(DACL)的VLAN10-Profile允许所有流量，用于MS Windows 7配置文件：



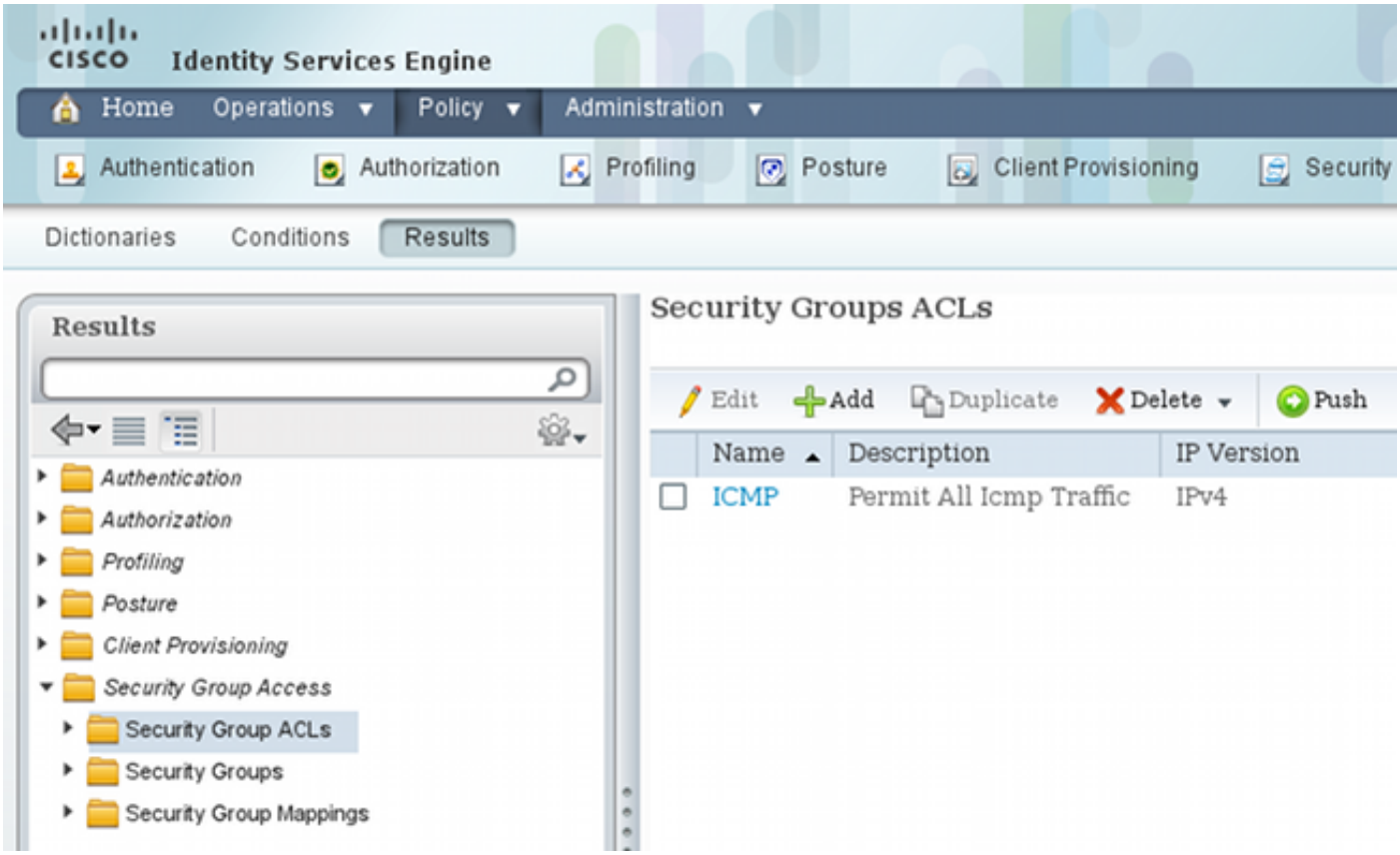
MS Windows XP使用类似的配置VLAN20-Profile，但VLAN编号(20)除外。

要在ISE上配置SGT组（标记），请导航至**策略>结果>安全组访问>安全组**。

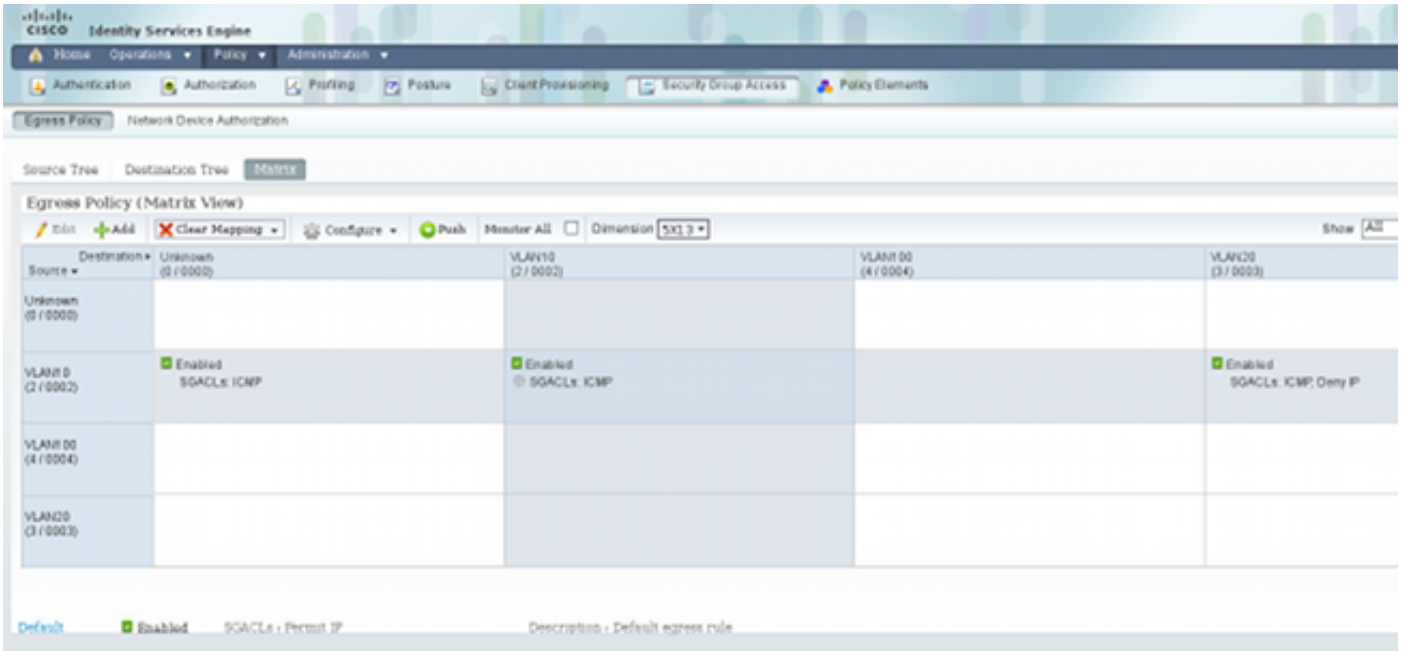
注意：不能选择标签号；它由第一个空闲号码自动选择，但1除外。您只能配置SGT名称。



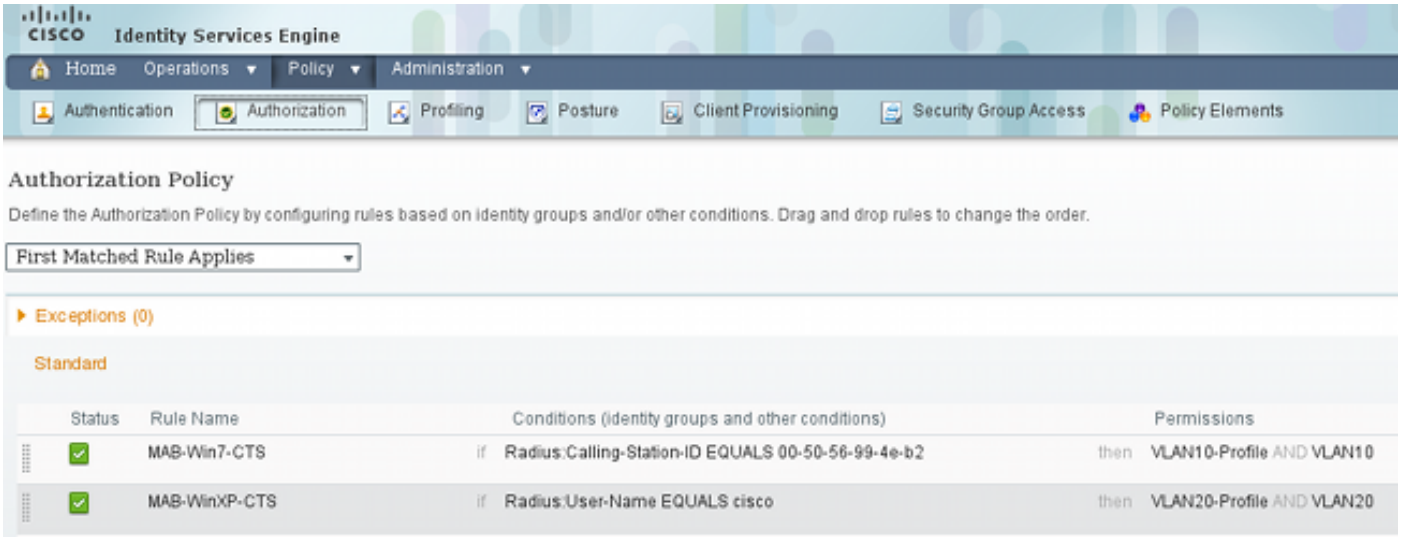
要创建SGACL以允许Internet控制消息协议(ICMP)流量，请导航到**Policy > Results > Security Group Access > Security Group ACLs**:



要创建策略，请导航到**Policy > Security Group Access > Egress Policy**。对于VLAN10与未知VLAN或VLAN10或VLAN20之间的流量，使用ICMP ACL(**permit icmp**):



要设置授权规则，请导航到**Policy > Authorization**。对于MS Windows 7（特定MAC地址），使用**VLAN10-Profile**，返回VLAN10和DACL，以及名为**VLAN10**的SGT的安全配置文件VLAN10。对于MS Windows XP（特定用户名），使用**VLAN20-Profile**，返回VLAN 20和DACL，使用名为**VLAN20**的SGT返回安全配置文件VLAN20。



完成交换机和ASA配置，以便它们接受SGT RADIUS属性。

ASA和3750X上的CTS配置

您必须配置基本CTS设置。在3750X上，必须指示应下载哪些服务器策略：

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

在ASA上，仅需要AAA服务器以及指向该服务器的CTS:

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

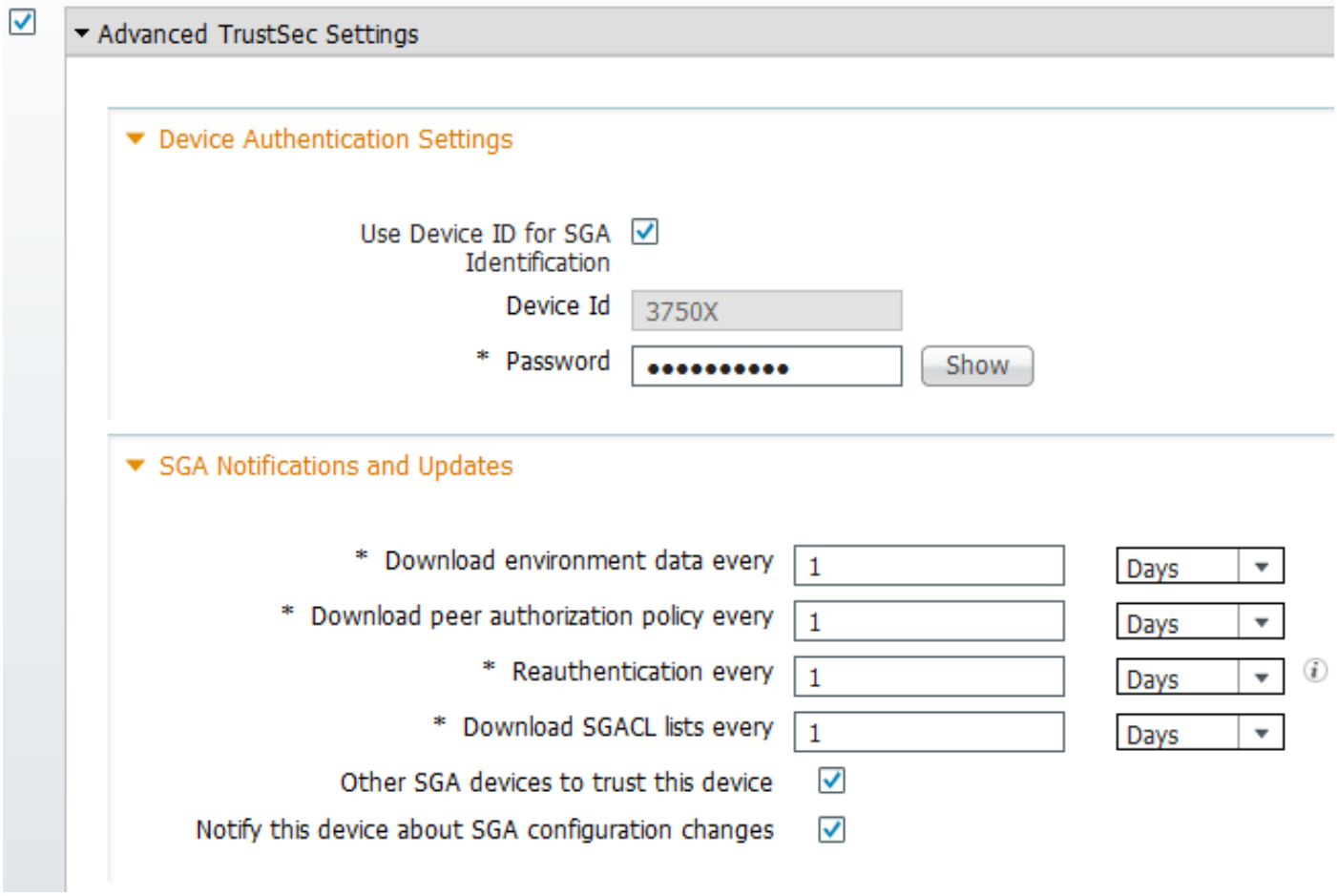
> **注**：在3750X上，必须使用**group radius**命令明确指向**ISE服**务器。这是因为3750X使用自动PAC调配。

3750X（自动）和ASA上的PAC调配（手动）

CTS云中的每台设备都必须通过身份验证服务器(ISE)进行身份验证，才能被其他设备信任。为此，它使用可扩展身份验证协议 — 通过安全协议的灵活身份验证(EAP-FAST)方法(RFC 4851)。此方法要求您在带外提供PAC。此过程也称为**phase0**，它未在任何RFC中定义。EAP-FAST的PAC具有类似于可扩展身份验证协议 — 传输层安全(EAP-TLS)的证书的角色。使用PAC建立安全隧道（第1阶段），在第2阶段进行身份验证时需要该安全隧道。

3750X上的PAC调配

3750X支持自动PAC调配。在交换机和ISE上使用共享密码来下载PAC。必须在ISE上的**Administration > Network Resources > Network Devices**下配置该密码和ID。选择交换机，然后展开**Advanced TrustSec Settings**部分以配置：



要让PAC使用这些凭证，请输入以下命令：

```
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
```

ASA上的PAC调配

ASA仅支持手动PAC调配。这意味着您必须在ISE上手动生成它（在网络设备/ASA中）：

然后必须安装文件（例如，使用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:
   000200a800030001000400010c40a15a339286ceac28a50dbbac597840006008c000301
   0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
   e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
   c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
   7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

ASA和3750X上的环境更新

在此阶段，两台设备都已正确安装PAC，并自动开始下载ISE环境数据。这些数据基本上是标记编号和它们的名称。要触发ASA上的环境刷新，请输入以下命令：

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

要在ASA上验证它（很遗憾，您看不到特定SGT标记/名称，但稍后会进行验证），请输入以下命令：

```
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)
```

要在3750X上验证它，请使用以下命令触发环境刷新：

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

要验证结果，请输入以下命令：

```
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
```

这表示所有标记和相应的名称都已正确下载。

3750X上的端口身份验证验证和实施

在3750X具有环境数据后，必须验证SGT是否应用于经过身份验证的会话。

要验证MS Windows 7是否正确通过身份验证，请输入以下命令：

```
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
```

输出显示VLAN10与SGT 0002和DACL一起用于所有流量。

要验证MS Windows XP是否正确通过身份验证，请输入以下命令：

```
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
```

输出显示，VLAN 20与SGT 0003和DACL一起用于所有流量

使用ip device tracking功能检测IP地址。DHCP交换机应配置为dhcp snooping。然后，在监听DHCP响应后，它会获取客户端的IP地址。对于静态配置的IP地址（如本例所示），使用arp snooping功能，并且PC必须发送任何数据包才能检测交换机的IP地址。

对于**设备跟踪**，可能需要隐藏命令才能在端口上激活它：

```
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
```

3750X上的策略更新

3750X（与ASA不同）可以从ISE下载策略。在下载和实施策略之前，您必须使用以下命令启用策略：

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

如果未启用该策略，则下载该策略，但不会安装该策略，也不会将其用于实施。

要触发策略刷新，请输入以下命令：

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

要验证是否已从ISE下载策略，请输入以下命令：

```
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
```

输出显示仅下载策略的必要部分。

在CTS云中，数据包包含源主机的SGT，并在目**标设备上进行实施**。这意味着数据包将从源设备转发到最后一台设备，该设备直接连接到目的主机。该设备是实施点，因为它知道其直连主机的SGT，并知道对于特定目标SGT是否应该允许或拒绝具有源SGT的传入数据包。

此决定基于从ISE下载的策略。

在此场景中，所有策略都将被下载。但是，如果清除MS Windows XP身份验证会话(SGT=VLAN20)，则交换机无需下载任何与VLAN20对应的策略（行），因为该SGT中没有更多设备连接到交换机。

高级（故障排除）部分说明3750X如何通过检查数据包级别来决定应下载哪些策略。

SXP Exchange（将ASA用作侦听器，将3750X用作扬声器）

ASA不支持SGT。ASA会丢弃所有带有SGT的帧。因此，3750X无法向ASA发送SGT标记的帧。而是使用SXP。该协议允许ASA从交换机接收有关IP地址与SGT之间映射的信息。借助该信息，ASA能够将IP地址映射到SGT并根据SGACL做出决策。

要将3750X配置为扬声器，请输入以下命令：

```
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
```

要将ASA配置为侦听程序，请输入以下命令：

```
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
```

要验证ASA是否已收到映射，请输入以下命令：

```
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
```

现在，当ASA收到源IP地址为192.168.1.200的传入数据包时，它能够将其视为来自SGT=2的传入数据包。对于源IP地址192.168.200.2，它能够将其视为来自SGT=3。目的IP地址也是如此。

> **注**:3750X必须知道关联主机的IP地址。这是通过IP设备跟踪完成的。对于终端主机上静态配置的IP地址，交换机必须在身份验证后接收任何数据包。这会触发IP设备跟踪以查找其IP地址，从而触发SXP更新。当只有SGT已知时，它不会通过SXP发送。

使用SGT ACL在ASA上过滤流量

以下是对ASA配置的检查：

```
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
```

创建一个ACL并将其应用于内部接口。它允许从SGT=3到SGT=2(称为VLAN10)的所有ICMP流量：

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

注：您可以使用标记编号或标记名称。

如果从源IP地址为**192.168.2.200(SGT=3)的**MS Windows XP ping IP地址为**192.168.1.200(SGT=2)**的MS Windows 7，则ASA会建立连接：

```
%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)
```

当您尝试使用Telnet时，流量会被阻止：

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

ASA上有更多配置选项。源和目标都可以使用安全标记和IP地址。此规则允许从**SGT标记= 3**和IP地址**192.168.2.200**到名为**VLAN10**的SGT标记和目标主机地址**192.168.1.200**的ICMP回应流量：

```
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
```

对象组也可以实现此目的：

```
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
```

使用从ISE下载的策略在3750X上进行流量过滤(RBACL)

也可以在交换机上定义本地策略。但是，此示例展示从ISE下载的策略。允许在ASA上定义的策略在一个规则中使用IP地址和SGT（以及来自Active Directory的用户名）。在交换机上定义的策略（本地和来自ISE）仅允许SGT。如果您需要在规则中使用IP地址，则建议在ASA上进行过滤。

测试MS Windows XP和MS Windows 7之间的ICMP流量。为此，您必须在MS Windows上将默认网关从ASA更改为3750X。3750X具有路由接口，能够路由数据包：

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

已从ISE下载策略。要验证它们，请输入以下命令：

```
 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
```

从VLAN10(MS Windows 7)到VLAN20(MS WindowsXP)的流量受ICMP-20 ACL的制约，ICMP-20 ACL从ISE下载：

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

要验证ACL，请输入以下命令：

```
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
```

要验证SGT映射以确保来自两台主机的流量被正确标记，请输入以下命令：

```
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
```

从MS Windows 7(**SGT=2**)到MS Windows XP(**SGT=3**)的ICMP与ACL ICMP-20配合使用效果良好。通过检查从**2**到**3**（15个允许的数据包）的流量计数器可以验证这一点：

```
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
```

在您尝试使用Telnet计数器后，被拒绝的数据包会增加（ICMP-20 ACL上不允许出现这种情况）：

```
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
```

> **注意**：输出中显示的星号(*)字符与所有未标记的流量相关(该列和行在ISE上的矩阵中称为unknown，并使用标记号**为0**)。

当您拥有带有log关键字的ACL条目（在ISE上定义）时，相应的数据包详细信息和采取的操作会与带有log关键字的任何ACL中记录相同。

验证

有关验证过程，请参阅各个配置部分。

故障排除

PAC调配

使用自动PAC调配时可能出现问题。请记住对RADIUS服务器使用**pac**关键字。3750X上的自动

PAC调配使用可扩展身份验证协议的EAP-FAST方法，内部方法使用Microsoft质询握手身份验证协议(EAP-MSCHAPv2)身份验证。在调试时，您会看到多个RADIUS消息，它们是EAP-FAST协商的一部分，用于构建安全隧道，该隧道使用具有已配置ID和密码的EAP-MSCHAPv2进行身份验证。

第一个RADIUS请求使用AAA **service-type=cts-pac-provisioning**以通知ISE这是一个PAC请求。

```
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.
```

输出末尾的**RADIUS reject**是预期值，因为您已经收到PAC，并且没有执行进一步的身份验证过程。

请记住，与ISE的所有其他通信均需要PAC。但是，如果没有配置，交换机在配置时仍会尝试环境或策略刷新。然后，它不会在RADIUS请求中附加**cts-opaqueue**(PAC)，从而导致失败。

如果您的PAC密钥错误，此错误消息会显示在ISE上：

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

如果PAC密钥错误，您还会看到交换机上的调试(**debug cts provisioning + debug radius**)的以下输出：

```
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
```

如果使用现代**radius server**约定，则会显示：

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

注意：您必须在ISE上使用您在设备身份验证设置**中使用的密码**。

PAC调配成功后，ISE上会显示以下内容：

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)

环境更新

环境刷新用于从ISE获取基本数据，包括SGT编号和名称。数据包级别显示它只有三个RADIUS请求和具有属性的响应。

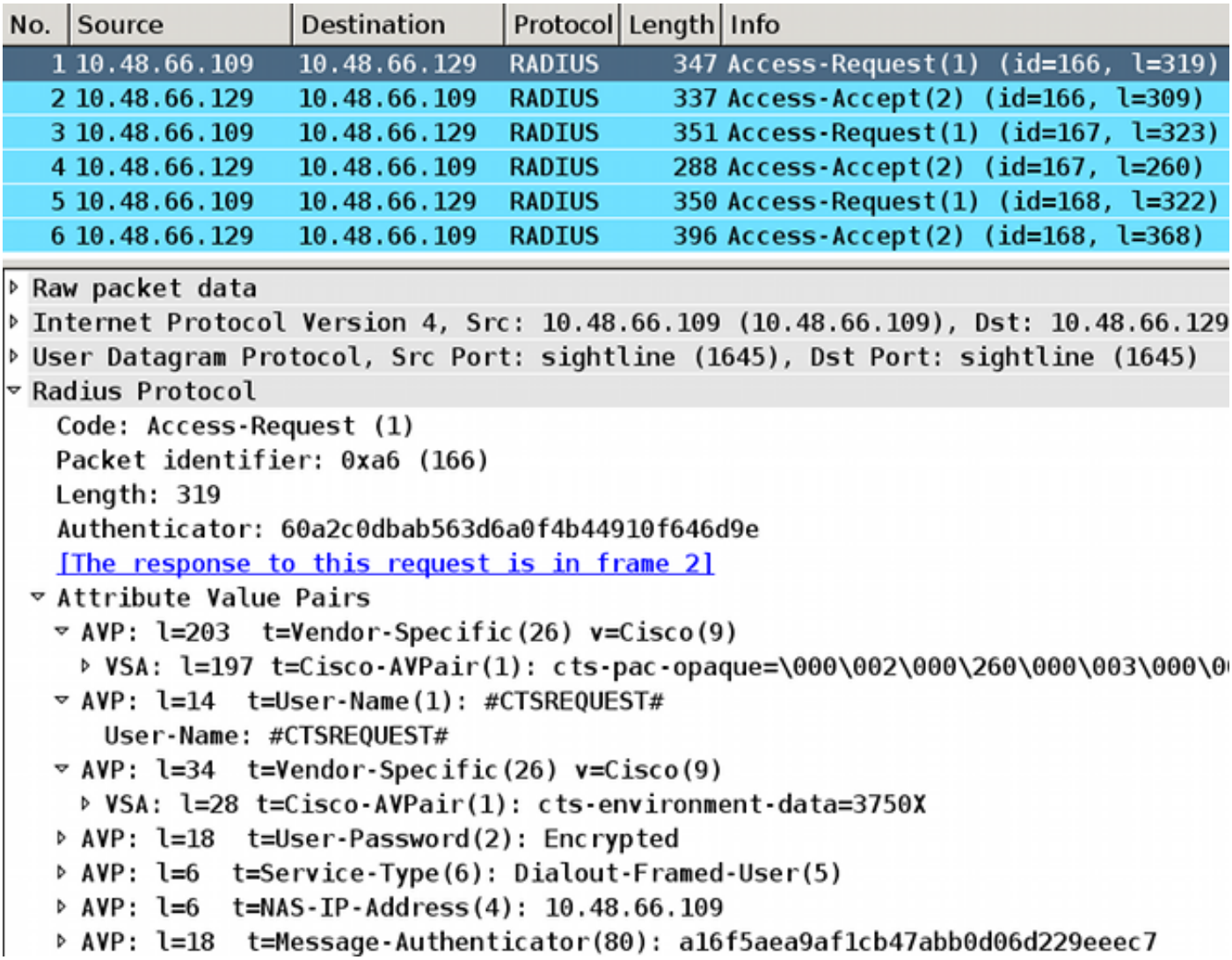
对于第一个请求，交换机收到**CTSServerlist**名称。对于第二个SGT，它会收到该列表的详细信息，对于最后一个SGT，它会收到带有标记和名称的所有SGT:

No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

```
Authenticator: b1672c429de0593417de4315ee0bd40c
[This is a response to a request in frame 5]
[Time from request: 0.008000000 seconds]
▾ Attribute Value Pairs
  ▾ AVP: l=14  t=User-Name(1): #CTSREQUEST#
      User-Name: #CTSREQUEST#
  ▸ AVP: l=40  t=State(24): 52656175746853657373696f6e3a306133303432383130...
  ▸ AVP: l=50  t=Class(25): 434143533a3061333034323831303030303134303353143...
  ▸ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
  ▸ AVP: l=18  t=Message-Authenticator(80): ac8e7b6f0d59da776f0dbf1ffa04baf1
  ▾ AVP: l=39  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=33 t=Cisco-AVPair(1): cts:security-group-table=0001-5
  ▾ AVP: l=46  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=40 t=Cisco-AVPair(1): cts:security-group-info=0-0-00-Unknown
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=ffff-0-00-ANY
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=2-0-00-VLAN10
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=3-0-00-VLAN20
```

此处可以看到默认**SGT 0**和 **ffff**，以及两个自定义：SGT标记2命名为**VLAN10**,SGT标记3命名为**VLAN20**。

注意：由于PAC调配，所有RADIUS请求都包括**cts-pac-opaque**。



No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

在3750X上，您应该看到所有三种RADIUS响应的调试，以及相应的列表、列表详细信息和特定SGT内部列表：

```
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)
```

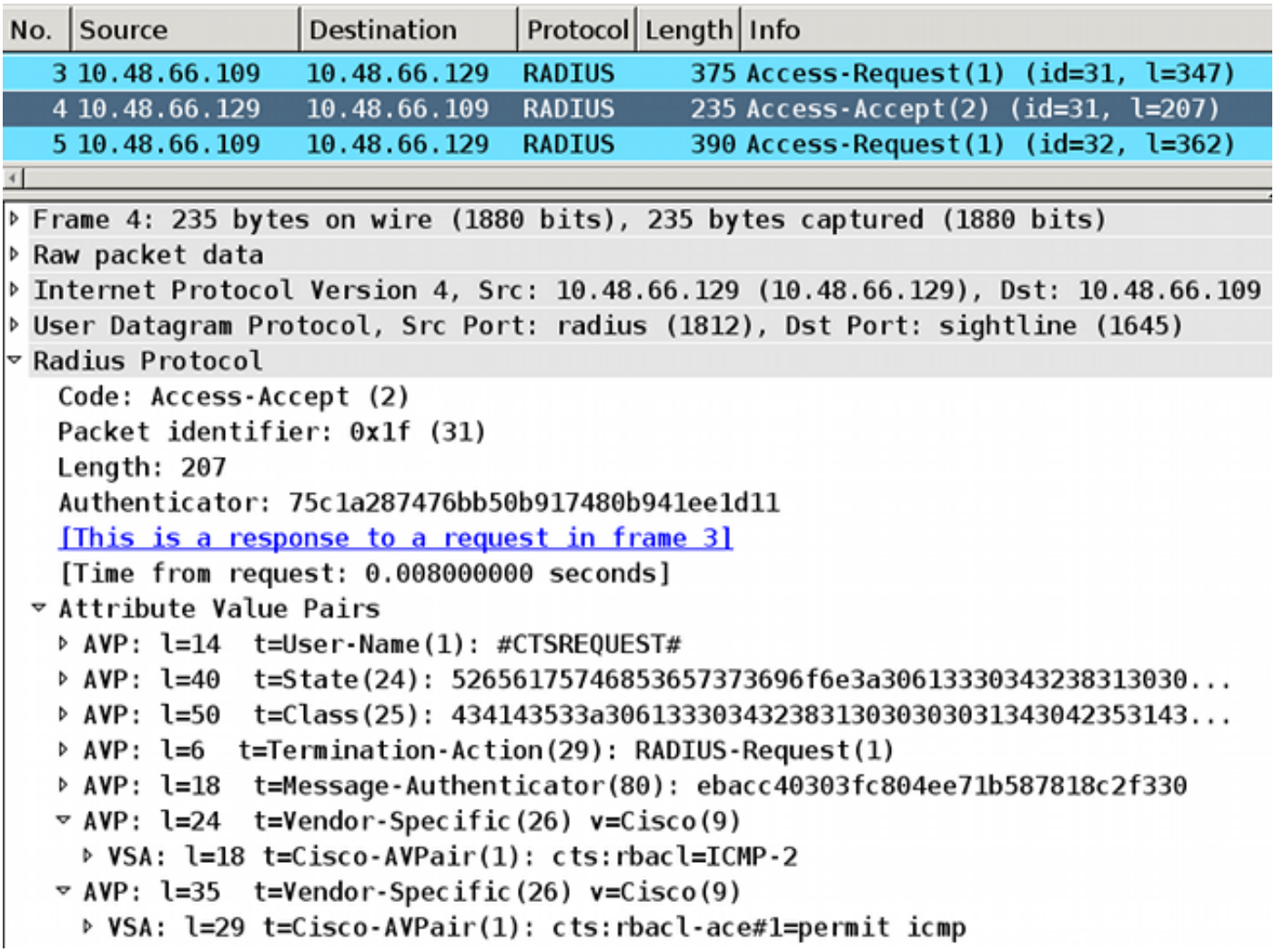
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: 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
```

策略刷新

只有交换机支持策略刷新。它类似于环境更新。这些只是RADIUS请求和接受。

交换机要求输入默认列表中的所有ACL。然后，对于每个不是最新（或不存在）的ACL，它会发送另一个请求以获取详细信息。

以下是请求ICMP-20 ACL时的响应示例：



请记住，您必须配置**cts role-based enforcement**才能实施该ACL。

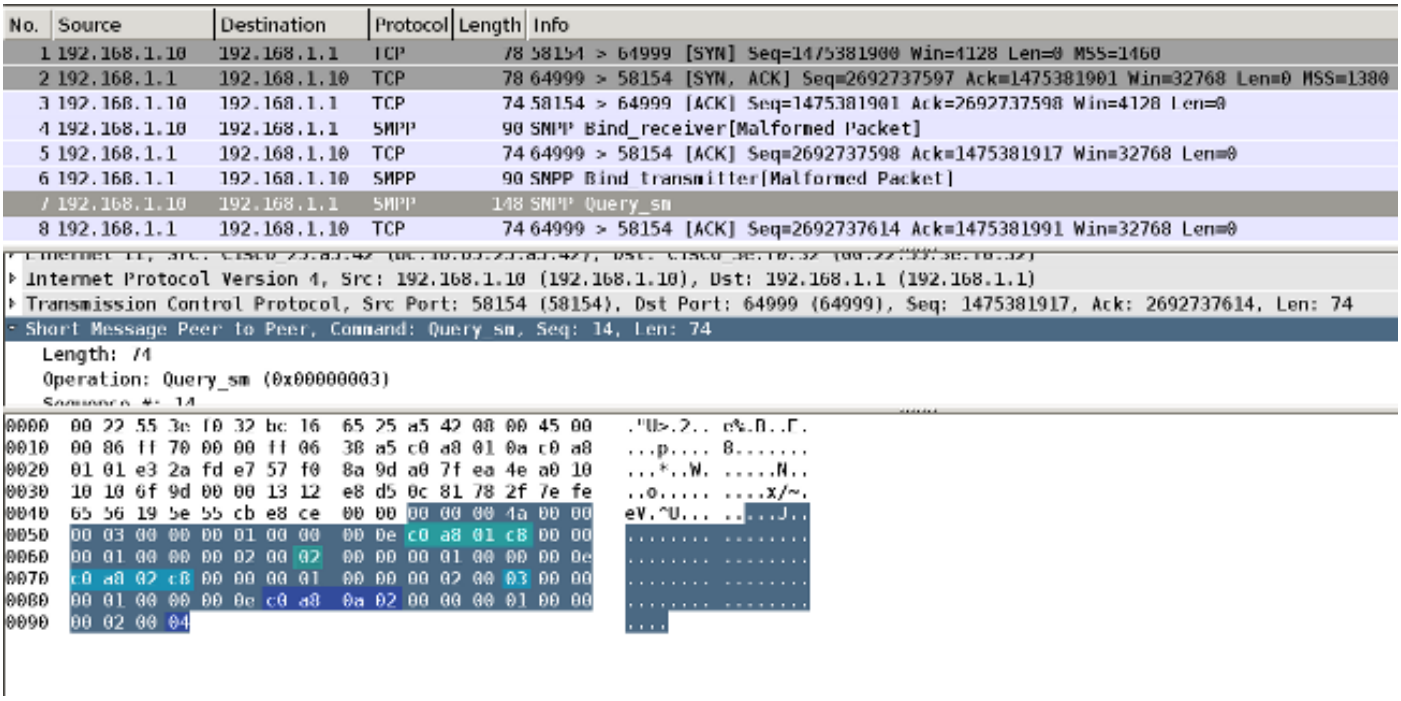
调试指示是否发生更改（基于gen ID）。如果需要，您可以卸载旧策略，并安装新策略。这包括ASIC编程（硬件支持）。

```
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交换

SXP更新由查找设备IP地址的IP设备跟踪代码触发。然后，使用短消息对等设备(SMPP)协议发送更新。它使用**TCP选项19**进行身份验证，该选项与边界网关协议(BGP)相同。SMPP负载未加密。Wireshark没有适用于SMPP负载的正确解码器，但很容易找到其中的数据：



- 第一个c0 a8 01 c8是192.168.1.200，并且带有标记2。
- 第二个c0 a8 02 c8是192.168.2.200,带有标记3。
- 第三个c0 a8 0a 02是192.168.10.2，具有tag 4(此标记用于测试电话SGT=4)

在IP设备跟踪找到MS Windows 7的IP地址后，在3750X上进行了以下调试：

```
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
```

以下是ASA上的相应调试：

```
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.
```

为了查看ASA上的更多调试，您可以启用调试详细级别：

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

ASA上的SGACL

在ASA正确安装SXP收到的SGT映射后，安全组ACL应该可以正常工作。当映射遇到问题时，请输入：

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

带有security-group的ACL与IP地址或用户身份的ACL的工作方式完全相同。日志可揭示问题，以及所命中的ACL的确切条目。

以下是从MS Windows XP到MS Windows 7的ping，表明Packet Tracer工作正常：

```
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>
```

相关信息

- 适用于3750的Cisco TrustSec配置指南
- 适用于ASA 9.1的思科TrustSec配置指南
- Cisco TrustSec部署和路线图
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。