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

目錄

簡介

本文描述如何在思科安全自適應安全裝置(ASA)和Cisco Catalyst 3750X系列交換機(3750X)上配置Cisco TrustSec(CTS)。

為了瞭解安全組標籤(SGT)和IP地址之間的對映，ASA使用SGT交換協定(SXP)。接著，會使用基於SGT的存取控制清單(ACL)來過濾流量。3750X從思科身分識別服務引擎(ISE)下載基於角色的存取控制清單(RBACL)策略，並根據這些策略過濾流量。本文詳細介紹資料包級別，以便描述通訊運行方式和預期的調試。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- CTS元件
- ASA和Cisco IOS®的CLI配置

採用元件

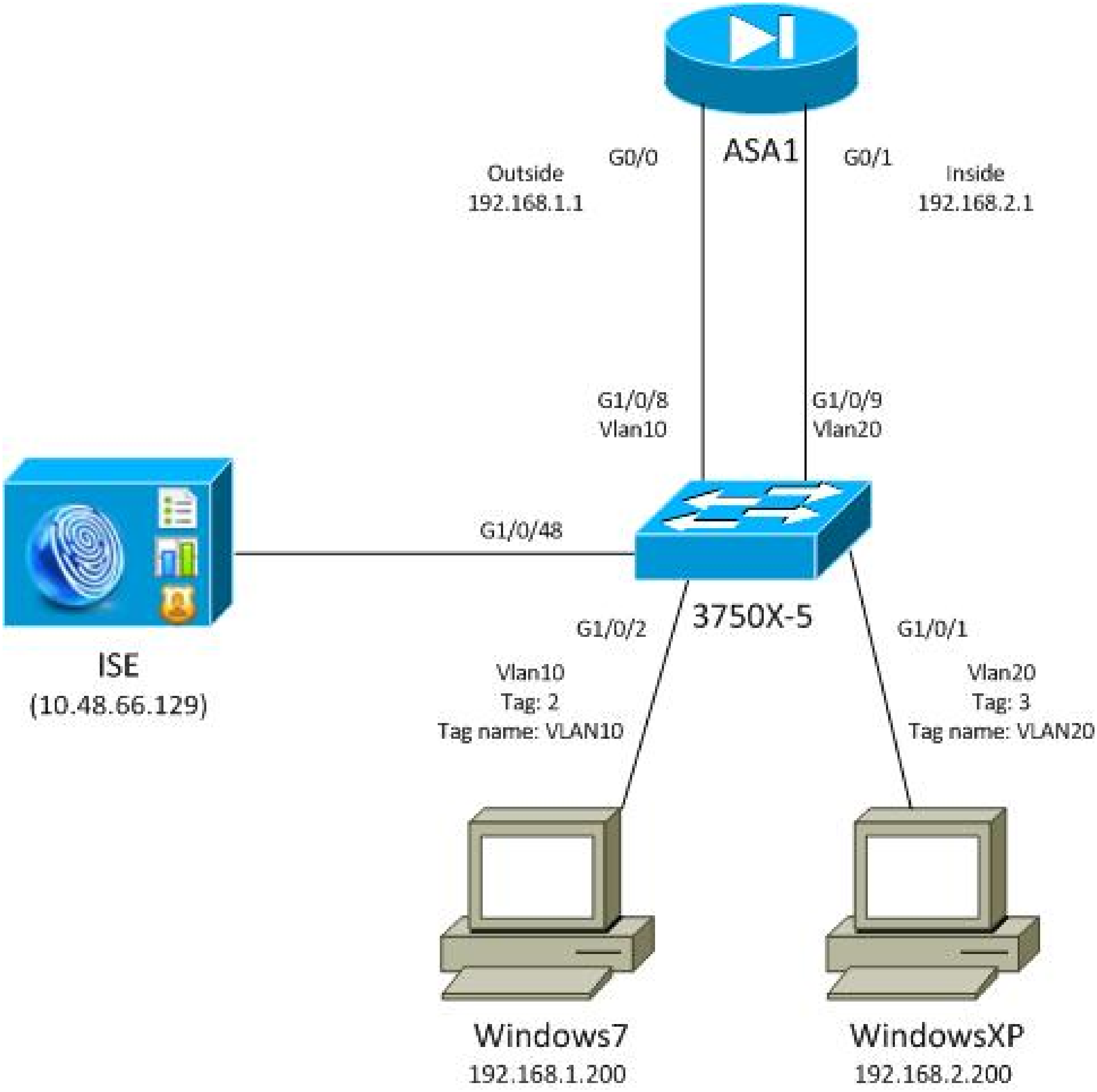
本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表



流量

以下是流量：

- 3750X在**G1/0/1**和**G1/0/2**上配置為埠身份驗證。
- ISE用作身份驗證、授權和記帳(AAA)伺服器。
- MAC Address Bypass(MAB)用於MS Windows 7的身份驗證。
- IEEE 802.1x用於MS Windows XP，以證明使用哪種身份驗證方法無關緊要。

身份驗證成功後，ISE返回SGT，3750X將該標籤繫結到身份驗證會話。交換機還使用**ip device tracking**命令獲取兩個站的IP地址。然後，交換機使用SXP將SGT和IP地址之間的對映表傳送到ASA。兩台MS Windows PC都有指向ASA的預設路由。

ASA收到來自對映到SGT的IP地址的流量後，能夠根據SGT使用ACL。此外，當您使用3750X作為路由器（兩個MS Windows工作站的預設網關）時，它能夠根據從ISE下載的策略過濾流量。

以下是組態和驗證步驟，每個步驟在稍後文檔中各自的部分詳述：

- 在3750X上使用**ip device tracking**命令進行埠身份驗證
- 身份驗證、SGT和安全組訪問控制清單(SGACL)策略的ISE配置
- ASA和3750X上的CTS配置
- 3750X（自動）和ASA上的保護訪問憑證(PAC)調配（手動）
- ASA和3750X上的環境更新
- 3750X上的連線埠驗證驗證和執行
- 3750X上的策略更新
- SXP交換（ASA作為監聽程式，3750X作為揚聲器）
- 在具有SGT ACL的ASA上過濾流量
- 3750X上的流量過濾（從ISE下載策略）

組態

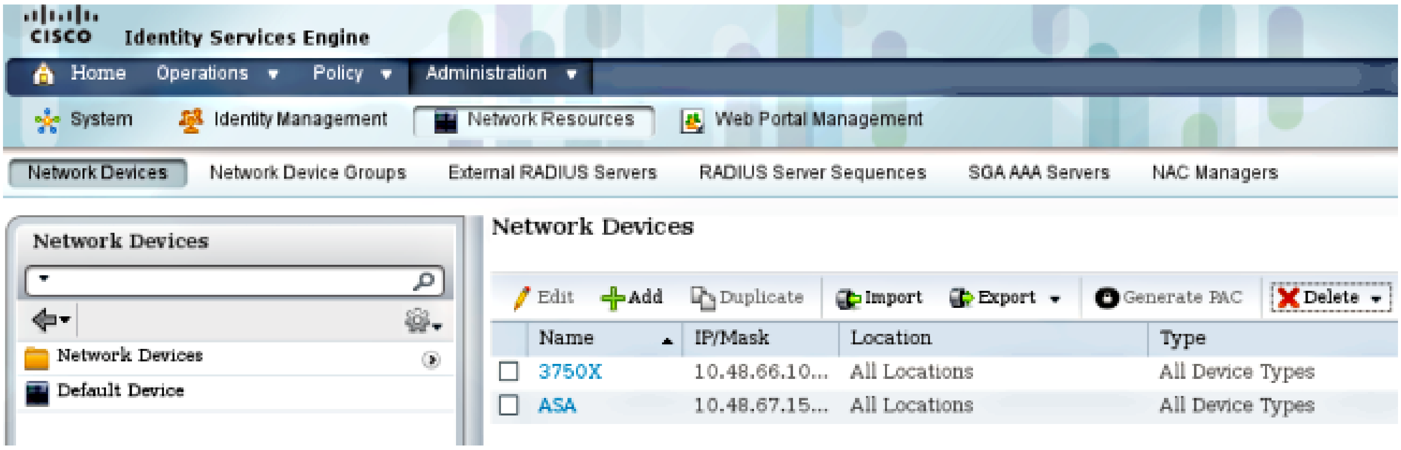
在3750X上使用*ip device tracking*命令進行埠身份驗證

這是802.1x或MAB的典型配置。只有當您使用來自ISE的活動通知時，才需要RADIUS授權更改(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
```

身份驗證、SGT和SGACL策略的ISE配置

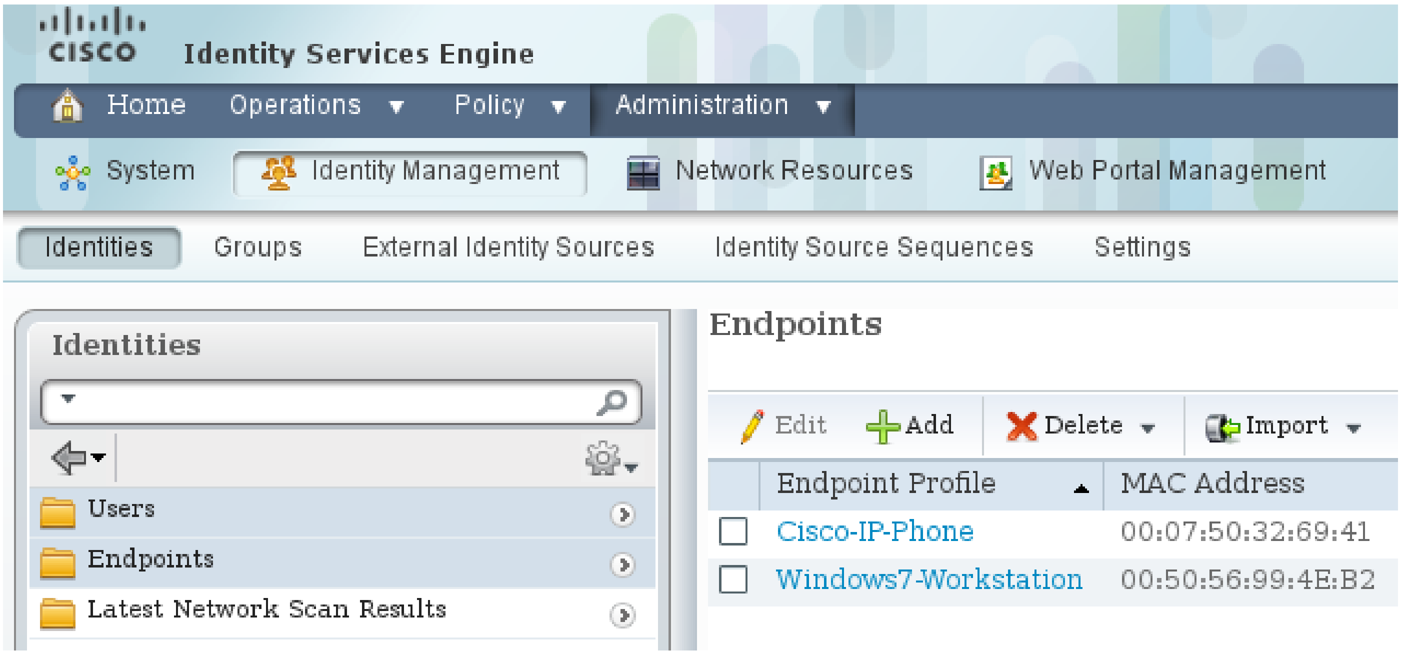
ISE必須在**管理>網路裝置**下配置兩個網路裝置：



Network Devices

	Name ▲	IP/Mask	Location	Type
□	3750X	10.48.66.10...	All Locations	All Device Types
□	ASA	10.48.67.15...	All Locations	All Device Types

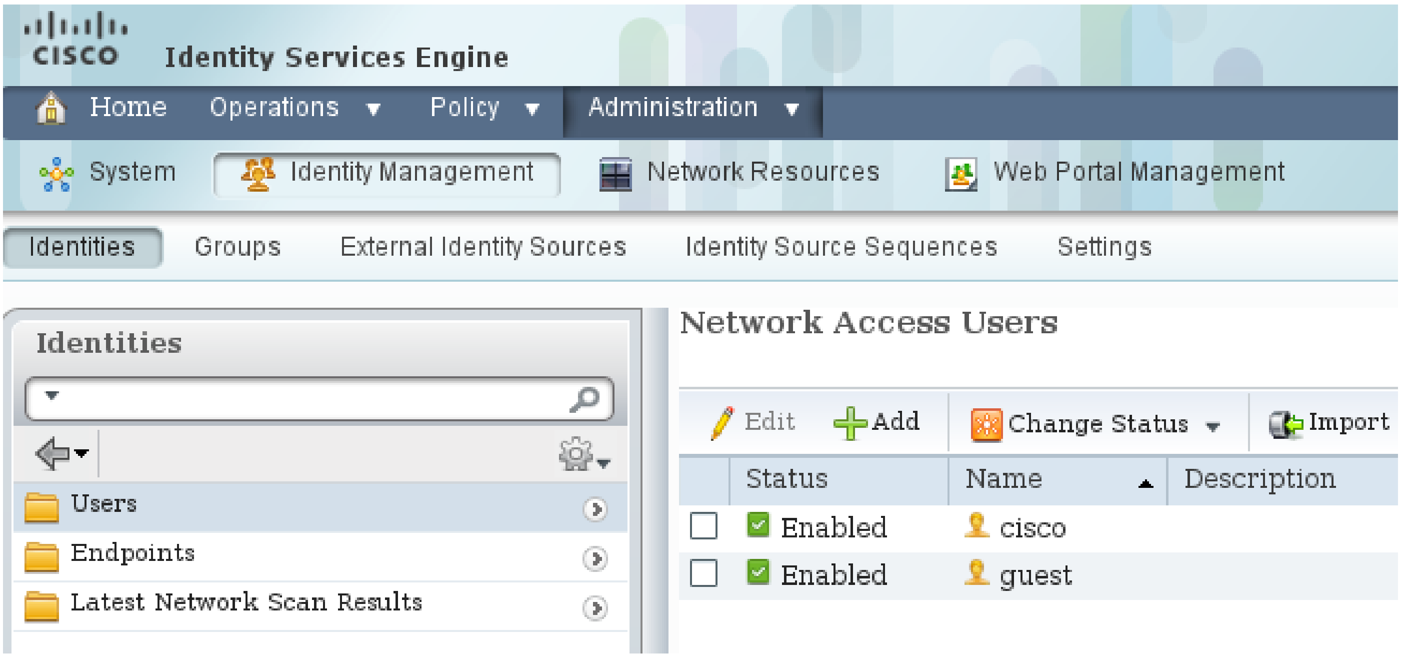
對於使用MAB身份驗證的MS Windows 7，必須在**管理>身份管理>身份>終端**下建立終端身份（MAC地址）：



Endpoints

	Endpoint Profile ▲	MAC Address
□	Cisco-IP-Phone	00:07:50:32:69:41
□	Windows7-Workstation	00:50:56:99:4E:B2

對於使用802.1x身份驗證的MS Windows XP，必須在**管理>身份管理>身份>使用者**下建立使用者身份（使用者名稱）：

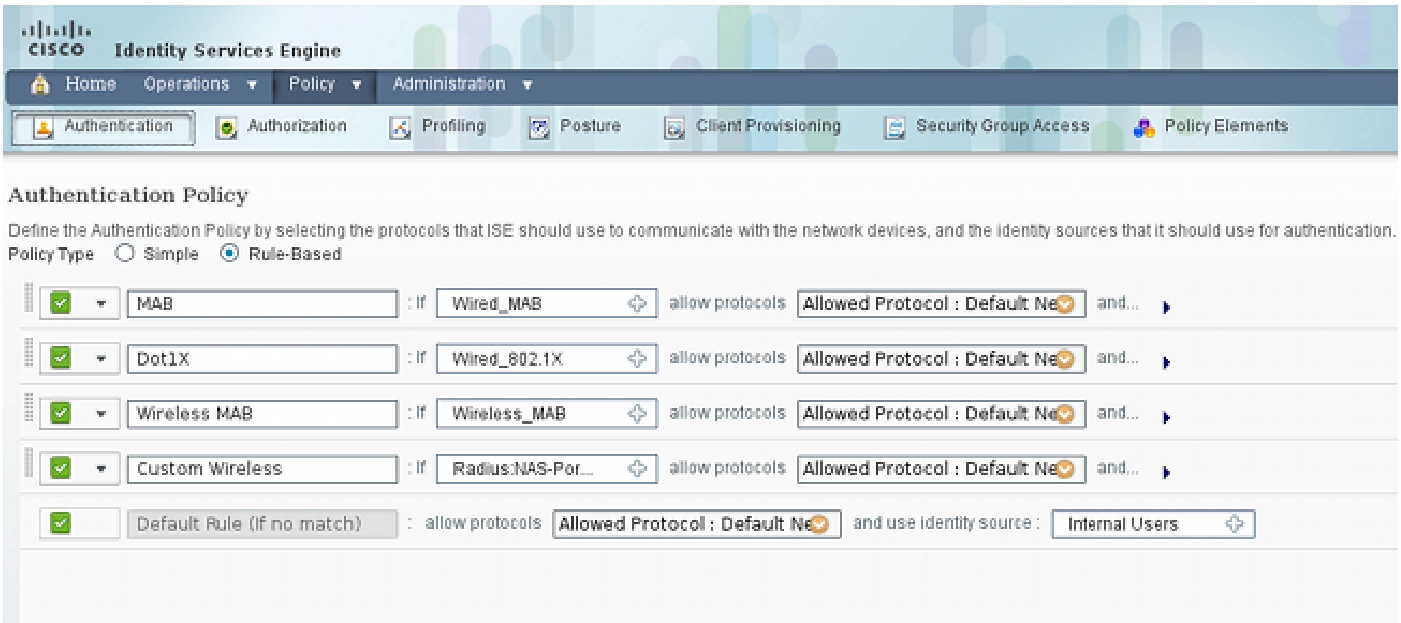


Network Access Users

	Status	Name	Description
□	☑ Enabled	cisco	
□	☑ Enabled	guest	

使用使用者名稱**cisco**。使用以下憑證為MS Windows XP配置可擴展身份驗證協定保護的EAP(EAP-PEAP)。

在ISE上，使用預設身份驗證策略（請勿更改）。第一個是MAB身份驗證的策略，第二個是802.1x:



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Ne and...

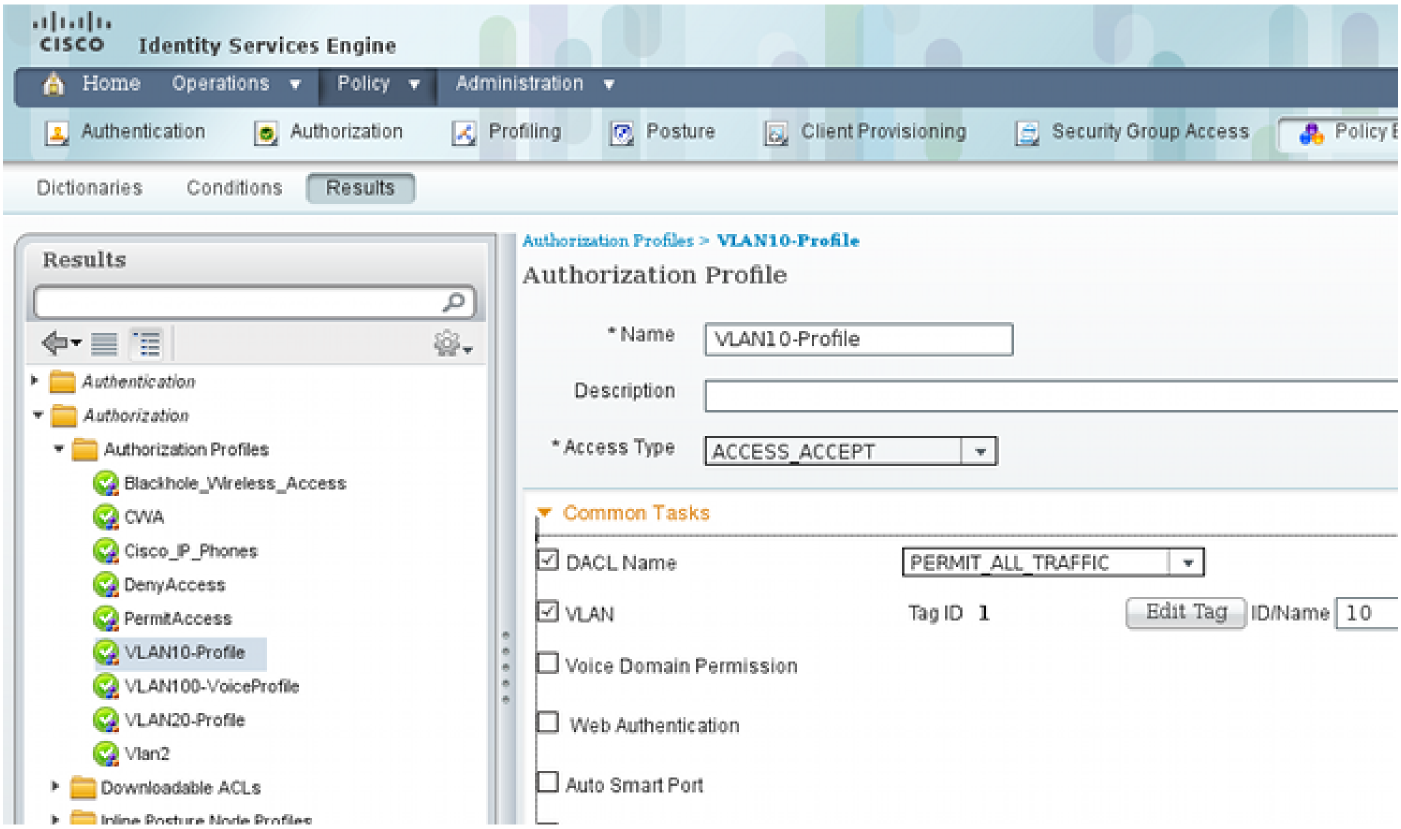
☑ Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Ne and...

☑ Wireless MAB : If Wireless_MAB allow protocols Allowed Protocol : Default Ne and...

☑ Custom Wireless : If Radius:NAS-Por... allow protocols Allowed Protocol : Default Ne and...

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Ne and use identity source : Internal Users

要配置授權策略，必須在**Policy > Results > Authorization > Authorization Profiles**下定義授權配置檔案。帶有可下載ACL(DACL)的VLAN10配置檔案允許所有流量，用於MS Windows 7配置檔案：



Authorization Profiles > VLAN10-Profile

Authorization Profile

* Name	VLAN10-Profile
Description	
* Access Type	ACCESS_ACCEPT

▾ Common Tasks

☑ DACL Name PERMIT_ALL_TRAFFIC

☑ VLAN Tag ID 1 Edit Tag ID/Name 10

☐ Voice Domain Permission

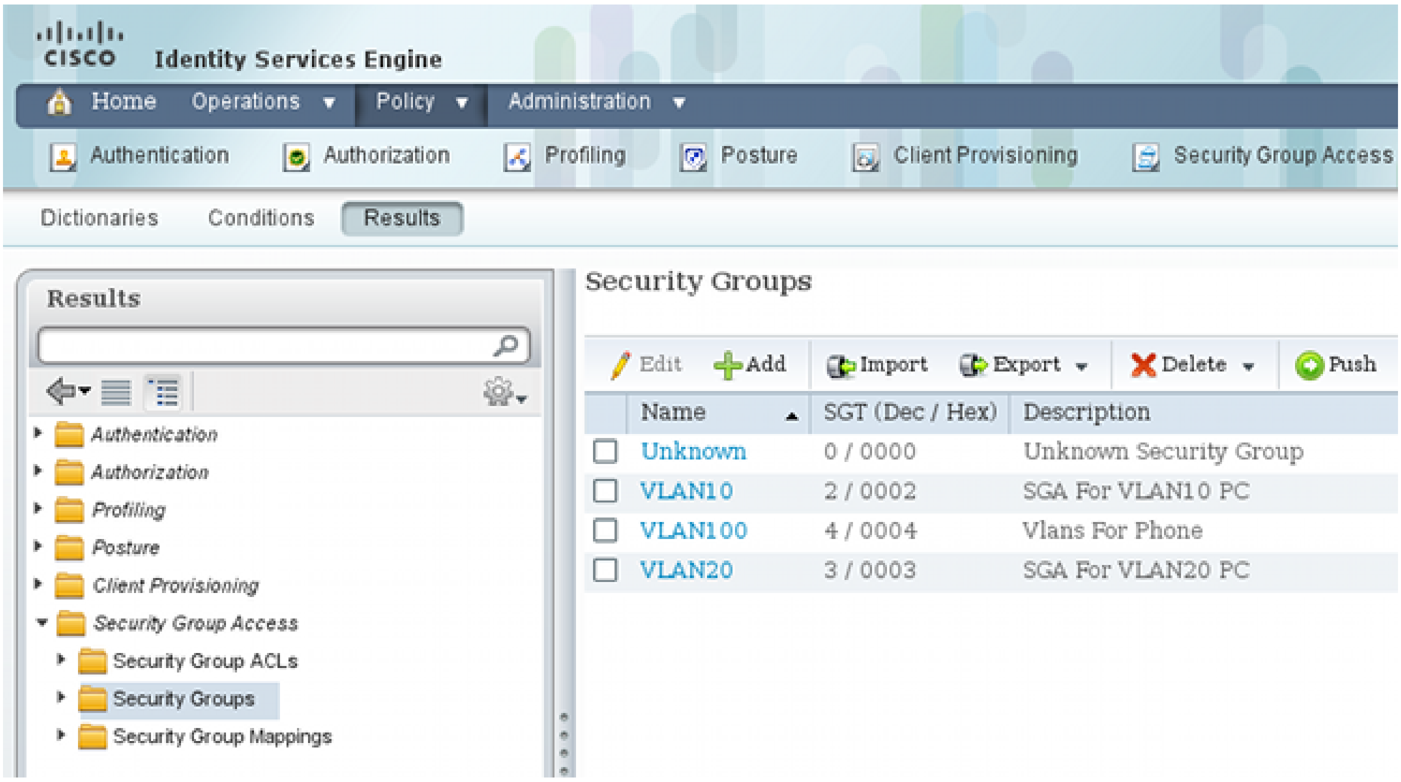
☐ Web Authentication

☐ Auto Smart Port

MS Windows XP使用類似的配置VLAN20-Profile，但VLAN編號(20)除外。

要在ISE上配置SGT組（標籤），請導航到**Policy > Results > Security Group Access > Security Groups**。

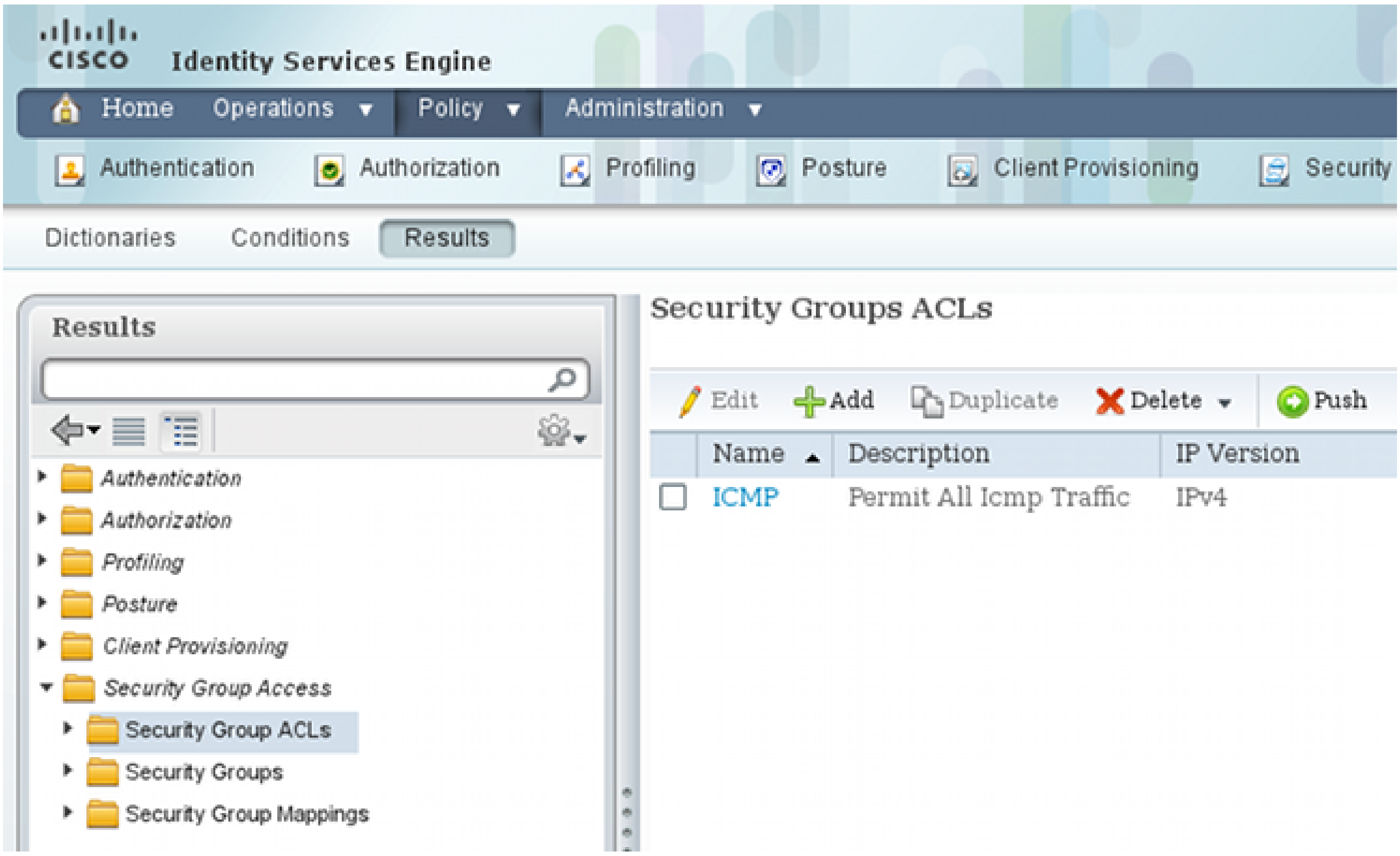
註：不能選擇標籤號；它將自動由除1之外的第一個空閒號選擇。您只能配置SGT名稱。



Security Groups

	Name ▲	SGT (Dec / Hex)	Description
☐	Unknown	0 / 0000	Unknown Security Group
☐	VLAN10	2 / 0002	SGA For VLAN10 PC
☐	VLAN100	4 / 0004	Vlans For Phone
☐	VLAN20	3 / 0003	SGA For VLAN20 PC

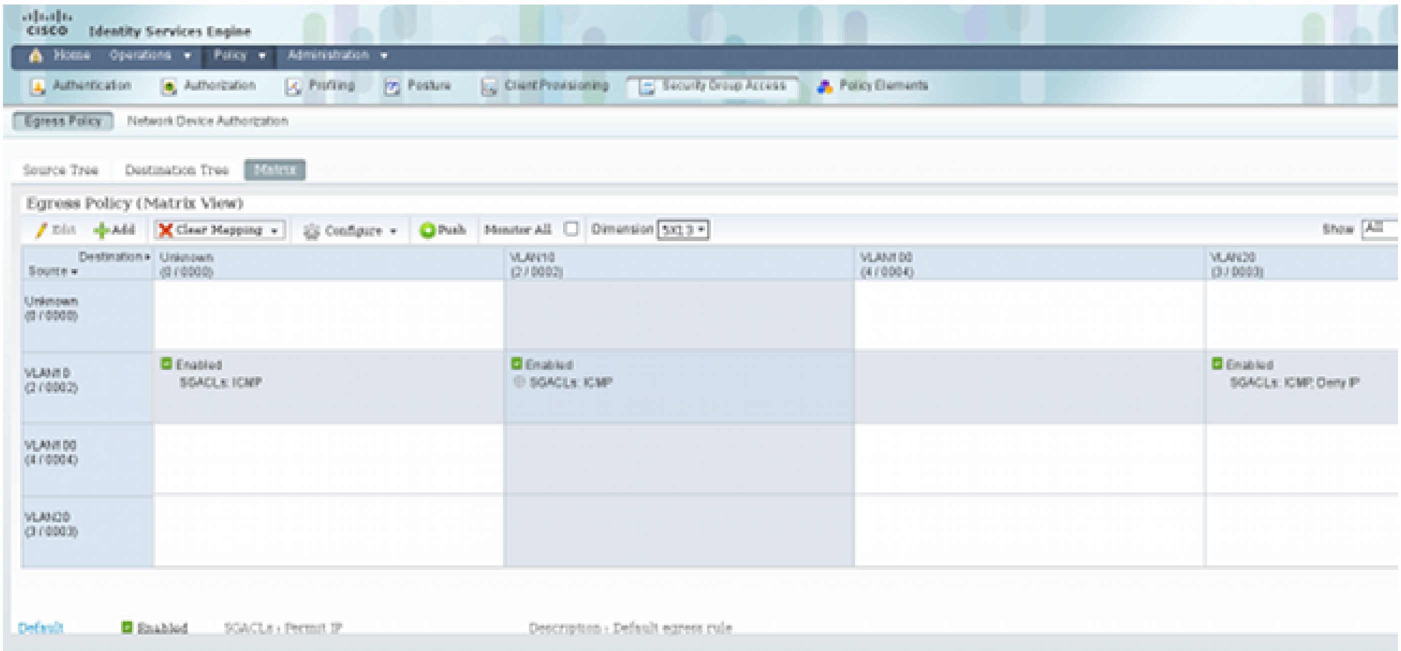
若要建立SGACL以允許網際網路控制訊息通訊協定(ICMP)流量，請導覽至**Policy > Results > Security Group Access > Security Group ACLs**:



Security Groups ACLs

□	Name	Description	IP Version
□	ICMP	Permit All Icmp Traffic	IPv4

要建立策略，請導航到**Policy > Security Group Access > Egress Policy**。對於VLAN10與未知VLAN、VLAN10或VLAN20之間的流量，使用ICMP ACL(**permit icmp**):

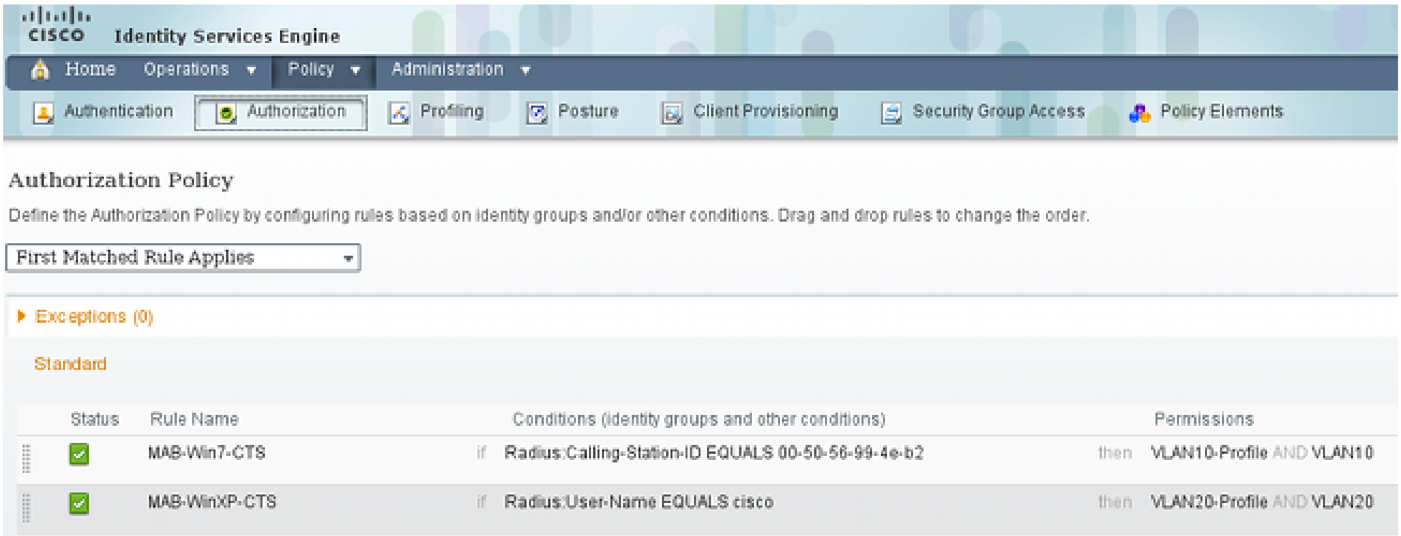


Egress Policy (Matrix View)

Destination ▸ Source ▾	Unknown (0 / 0000)	VLAN10 (2 / 0002)	VLAN100 (4 / 0004)	VLAN20 (3 / 0003)
Unknown (0 / 0000)				
VLAN10 (2 / 0002)	Enabled SGACLs: ICMP	Enabled SGACLs: ICMP		Enabled SGACLs: ICMP, Deny IP
VLAN100 (4 / 0004)				
VLAN20 (3 / 0003)				

Default　Enabled　SGACLs : Permit IP　Description : Default egress rule

要設定授權規則，請導航到**Policy > Authorization**。對於MS Windows 7（特定MAC地址），使用**VLAN10-Profile**，返回VLAN10和DACL，以及名為**VLAN10** SGT的安全配置檔案VLAN10。對於MS Windows XP（特定使用者名稱），使用**VLAN20-Profile**，返回VLAN 20和DACL，使用SGT命名為**VLAN20**的安全配置檔案VLAN20。



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	MAB-Win7-CTS	if	Radius:Calling-Station-ID EQUALS 00-50-56-99-4e-b2	then	VLAN10-Profile AND VLAN10
☑	MAB-WinXP-CTS	if	Radius:User-Name EQUALS cisco	then	VLAN20-Profile AND VLAN20

完成交換機和ASA配置，以便它們接受SGT RADIUS屬性。

ASA和3750X上的CTS配置

您必須配置基本CTS設定。在3750X上，必須指明應從哪些伺服器策略下載：

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

在ASA上，僅需要AAA伺服器以及指向該伺服器的CTS:

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

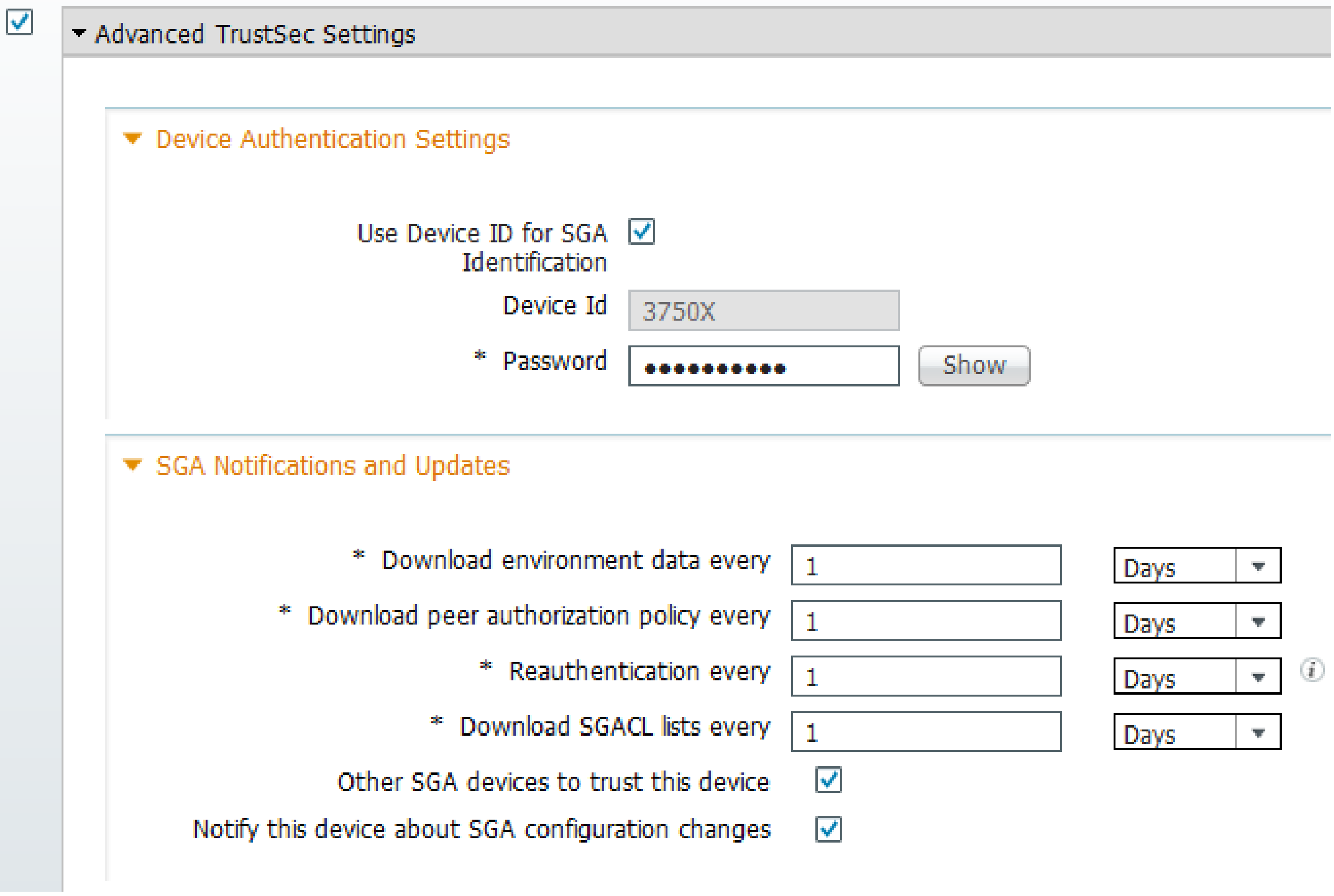
> **註**：在3750X上，必須使用**group radius 命令明確指向ISE伺服器。**這是因為3750X使用自動PAC布建。

3750X和ASA上的PAC調配（自動）（手動）

CTS雲中的每台裝置都必須向身份驗證伺服器(ISE)進行身份驗證，才能被其他裝置信任。為此它使用可擴展身份驗證協定 — 通過安全協定的靈活身份驗證(EAP-FAST)方法(RFC 4851)。此方法要求您在帶外提供PAC。此程式也稱為**phase0**，未在任何RFC中定義。EAP-FAST的PAC與可擴展身份驗證協定 — 傳輸層安全(EAP-TLS)的證書具有類似的角色。PAC用於建立安全通道（第1階段），在第2階段進行身份驗證時需要該通道。

3750X上的PAC布建

3750X支援自動PAC布建。在交換機和ISE上使用共用密碼下載PAC。必須在ISE上的**管理>網路資源>網路裝置**下配置該密碼和ID。選擇交換機，然後展開**Advanced TrustSec Settings**部分以配置：



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for SGA Identification ☑

Device Id: 3750X

* Password: ●●●●●●●●●●● Show

SGA Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Days

Other SGA devices to trust this device ☑

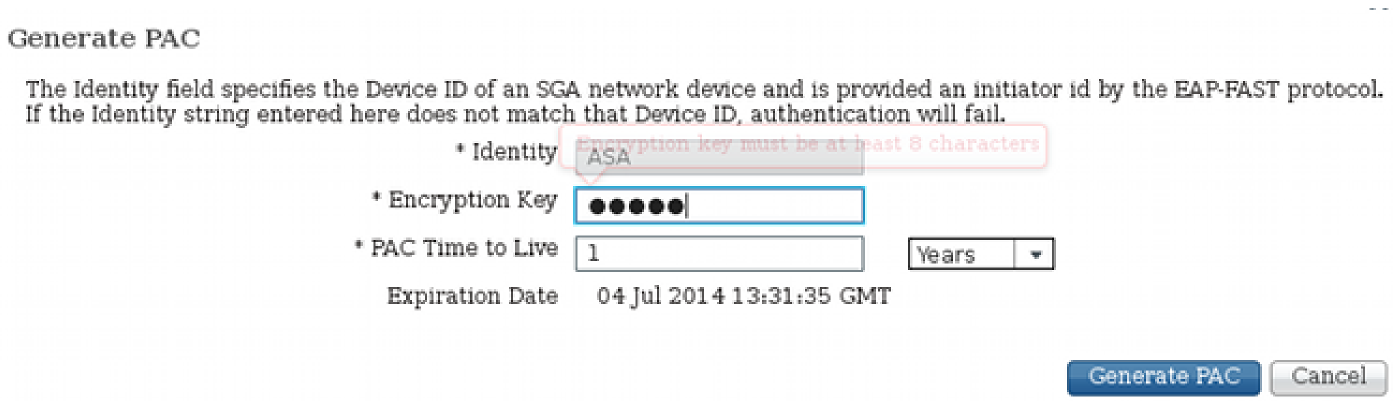
Notify this device about SGA configuration changes ☑

要讓PAC使用這些憑據，請輸入以下命令：

```
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調配

ASA僅支援手動PAC調配。這意味著您必須在ISE上手動生成它（在網路裝置/ASA中）：



Generate PAC

The Identity field specifies the Device ID of an SGA network device and is provided an initiator id by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication will fail.

* Identity: ASA

Encryption key must be at least 8 characters

* Encryption Key: ●●●●●

* PAC Time to Live: 1 Years ▾

Expiration Date: 04 Jul 2014 13:31:35 GMT

然後必須安裝檔案（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:
   000200a80003000100040010c40a15a339286ceac28a50dbbac597840006008c000301
   0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
   e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
   c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
   7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

ASA和3750X上的環境更新

在這個階段，兩台裝置都已正確安裝PAC並自動開始下載ISE環境資料。這些資料基本上是標籤號及其名稱。要觸發ASA上的環境刷新，請輸入以下命令：

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

要在ASA上驗證它（很遺憾，您看不到特定的SGT標籤/名稱，但稍後會驗證它），請輸入以下命令：

```
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)
```

若要在3750X上驗證它，請使用以下命令觸發環境刷新：

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

若要驗證結果，請輸入以下命令：

```
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
```

這顯示已正確下載所有標籤和相應的名稱。

3750X上的連線埠驗證和執行

在3750X具有環境資料後，必須驗證SGT是否應用於已驗證的作業階段。

要驗證MS Windows 7是否正確通過身份驗證，請輸入以下命令：

```
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:  C0A80001000001002B67334C
     Acct Session ID:  0x00000179
              Handle:  0x94000101
```

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

輸出顯示，**VLAN10**與**SGT 0002**和DACL一起用於所有流量。

要驗證MS Windows XP是否正確通過身份驗證，請輸入以下命令：

```
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
```

輸出顯示，**VLAN 20**與**SGT 0003**和DACL一起用於所有流量

使用ip裝置跟蹤**功能檢測IP**地址。DHCP交換機應配置為**dhcp snooping**。接著，在監聽DHCP響應後，它獲取客戶端的IP地址。對於靜態配置的IP地址（如本例所示），會使用**arp snooping**功能，並且PC必須傳送任何資料包才能檢測交換機的IP地址。

對於**裝置跟蹤**，可能需要隱藏命令以在埠上啟用它：

```
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（與ASA不同）可以從ISE下載策略。在下載和實施策略之前，您必須使用以下命令啟用該策略：

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

如果未啟用該功能，則系統將下載該策略，但不會安裝該策略並且不會將其用於實施。

要觸發策略刷新，請輸入以下命令：

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

要驗證是否從ISE下載策略，請輸入以下命令：

```
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
```

輸出顯示，只下載了策略的必要部分。

在CTS雲中，資料包包含源主機的SGT，並在目**的地裝置上實施**。這表示封包從來源轉送到最後一個裝置，而最後裝置直接連線到目的地主機。該裝置是實施點，因為它知道其直連主機的SGT，並知道對於特定目標SGT，應允許還是拒絕包含源SGT的傳入資料包。

此決定基於從ISE下載的策略。

在此場景中，所有策略都將被下載。但是，如果清除MS Windows XP身份驗證會話(SGT=VLAN20)，則交換機無需下載任何與VLAN20對應的策略（行），因為該SGT中沒有更多裝置連線到交換機。

高級（疑難排解）部分說明3750X如何通過檢查封包層級來決定下載哪些原則。

SXP Exchange（ASA作為監聽程式，3750X作為揚聲器）

ASA不支援SGT。ASA丟棄所有具有SGT的幀。因此，3750X無法將SGT標籤的幀傳送到ASA。而是使用SXP。此協定允許ASA從交換機接收有關IP地址與SGT之間對映的資訊。藉助該資訊，ASA能夠將IP地址對映到SGT並根據SGACL做出決策。

若要將3750X配置為揚聲器，請輸入以下命令：

```
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
```

要將ASA配置為監聽程式，請輸入以下命令：

```
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
```

要驗證ASA是否已收到對映，請輸入以下命令：

```
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
```

現在，當ASA收到源IP地址為**192.168.1.200**的傳入資料包時，可以將其視為來自**SGT=2的資料包**。對於源IP地址**192.168.200.2**，它能夠將其視為來自**SGT=3**。這同樣適用於目的IP地址。

> **註**:3750X必須知道關聯主機的IP地址。這是通過IP裝置跟蹤完成的。對於終端主機上靜態配置的IP地址，交換機必須在身份驗證後接收任何資料包。這將觸發IP裝置跟蹤以查詢其IP地址，從而觸發SXP更新。如果只有SGT是已知的，則不會通過SXP傳送。

使用SGT ACL的ASA上的流量過濾

以下是對ASA配置的檢查：

```
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
```

ACL即會建立並應用到內部介面。允許從**SGT=3**到**SGT=2**(稱為**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
```

注意：您可以使用標籤編號或標籤名稱。

如果從源IP地址為**192.168.2.200**(**SGT=3**)的MS Windows XP對IP地址為**192.168.1.200**(**SGT=2**)的MS Windows 7執行ping，ASA將建立連線：

```
%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)
```

當您嘗試使用Telnet時，流量會遭到封鎖：

```
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上有更多配置選項。源和目標都可以同時使用安全標籤和IP地址。此規則允許從**SGT標籤= 3**和IP地址**192.168.2.200**到名為**VLAN10**的SGT標籤和目標主機地址**192.168.1.200**的ICMP回應流量：

```
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
```

目標組也可以實現此目的：

```
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
```

使用從ISE下載的策略在3750X上進行流量過濾(RBACL)

也可以在交換機上定義本地策略。但是，此示例顯示從ISE下載的策略。允許在ASA上定義的策略在一個規則中使用IP地址和SGT（以及來自Active Directory的使用者名稱）。交換機上定義的策略（本地和從ISE）僅允許SGT。如果您需要在規則中使用IP地址，則建議在ASA上進行過濾。

在MS Windows XP和MS Windows 7之間測試ICMP流量。為此，您必須在MS Windows上將預設網關從ASA更改為3750X。3750X具有路由介面，並能夠路由封包：

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

策略已經從ISE下載。若要驗證它們，請輸入以下命令：

```
 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
```

從**VLAN10(MS Windows 7)到VLAN20**(MS WindowsXP)的流量會受到ICMP-20 ACL的制約，該流量從ISE下載：

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

若要確認ACL，請輸入以下命令：

```
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
```

要驗證SGT對映以確保來自兩台主機的流量標籤正確，請輸入以下命令：

```
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
```

從MS Windows 7(**SGT=2**)到MS Windows XP(**SGT=3**)的ICMP與ACL ICMP-20搭配使用效果良好。檢查從**2**到**3**（15個允許的資料包）的流量的計數器可以驗證這一點：

```
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
```

嘗試使用Telnet計數器後，遭到拒絕的封包會增加（ICMP-20 ACL上不允許）：

```
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
```

> **註**意：輸出中顯示的星號(*)字元與所有未標籤的流量相關(該列和行在ISE上的矩陣中稱為**unknown，並使用標籤號號0**)。

如果您的ACL條目帶有log關鍵字（在ISE上定義），則對應的資料包詳細資訊和採取的操作將記錄為任何ACL帶有log關鍵字。

驗證

有關驗證過程，請參閱各個配置部分。

疑難排解

PAC布建

使用自動PAC調配時可能出現問題。請記得對RADIUS伺服器使用**pac**關鍵字。3750X上的自動

PAC設定使用EAP-FAST方法和可擴展身份驗證協定，內部方法使用Microsoft質詢握手身份驗證協定(EAP-MSCHAPv2)身份驗證。進行調試時，您會看到多個RADIUS消息，它們是EAP-FAST協商的一部分，用於構建安全隧道，該隧道使用具有已配置ID和密碼的EAP-MSCHAPv2進行身份驗證。

第一個RADIUS請求使用AAA **service-type=cts-pac-provisioning**通知ISE這是一個PAC請求。

```
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.
```

輸出結尾應該有**RADIUS reject**，因為您已經收到PAC，並且沒有執行進一步的身份驗證過程。

請記住，與ISE的所有其他通訊均需要PAC。但是，如果您沒有配置環境或策略，交換機在配置時仍會嘗試刷新環境或策略。接下來，它不會在RADIUS要求中附加**cts-opaqueue**(PAC)，這將會導致失敗。

如果您的PAC金鑰錯誤，ISE上將顯示以下錯誤消息：

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

如果PAC金鑰錯誤，您也會在交換器上看到偵錯(**debug cts provisioning + debug radius**)的以下輸出：

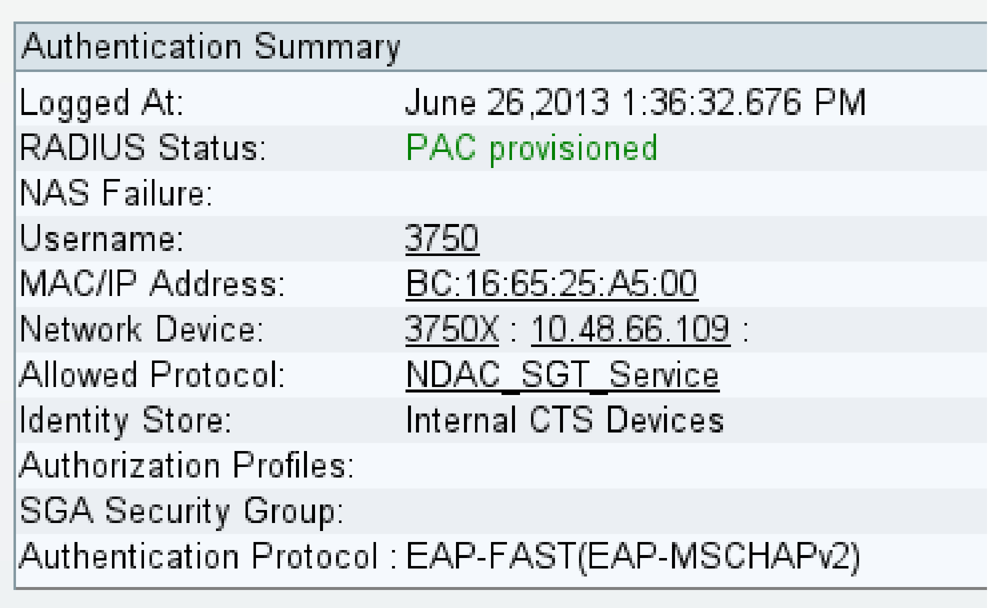
```
Apr 20 10:07:11.768: CTS-provisioning: Sending EAP Response/Identity t
Apr 20 10:07:15.325: RADIUS(0000024B): Request timed out!
Apr 20 10:07:15.325: RADIUS: No response from (10.62.84.224:1645,1646) for
id 1645/37
```

如果您使用現代**radius server**慣例，將會顯示：

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

注意：您必須在ISE上使用在裝置身份驗證設定中使用**的相同密碼。**

PAC調配成功後，ISE上將顯示以下內容：



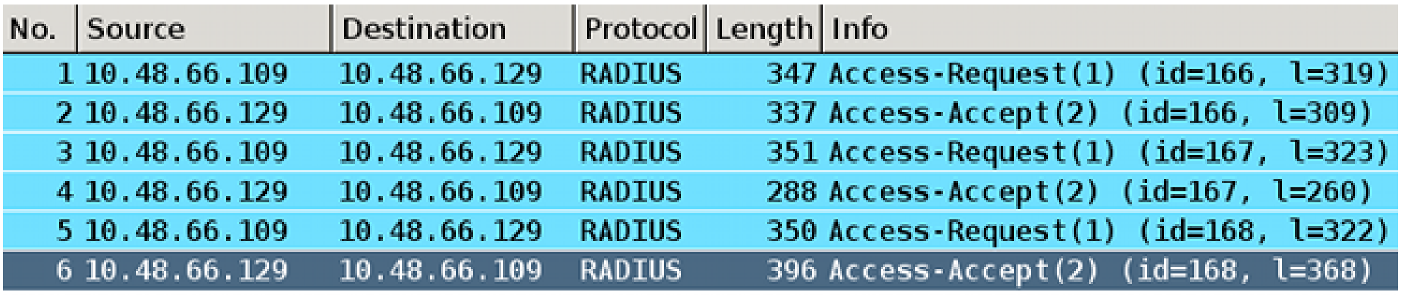
Authentication Summary

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)

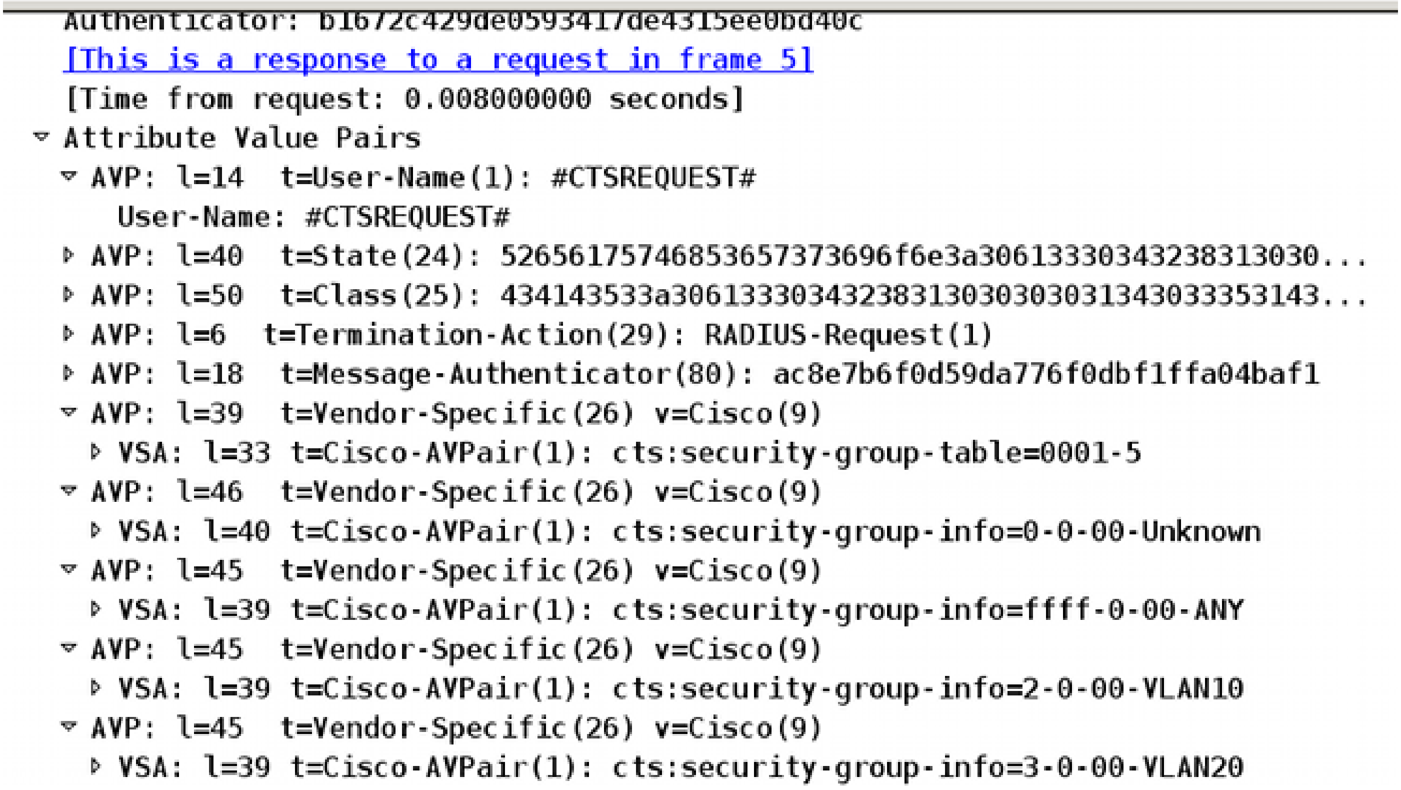
環境刷新

環境刷新用於從ISE獲取基本資料，包括SGT編號和名稱。封包層級顯示只有三個RADIUS要求和帶屬性的回應。

對於第一個請求，交換機收到**CTSServerlist**名稱。對於第二個，它接收該清單的詳細資訊；對於最後一個清單，它接收帶有標籤和名稱的所有SGT:



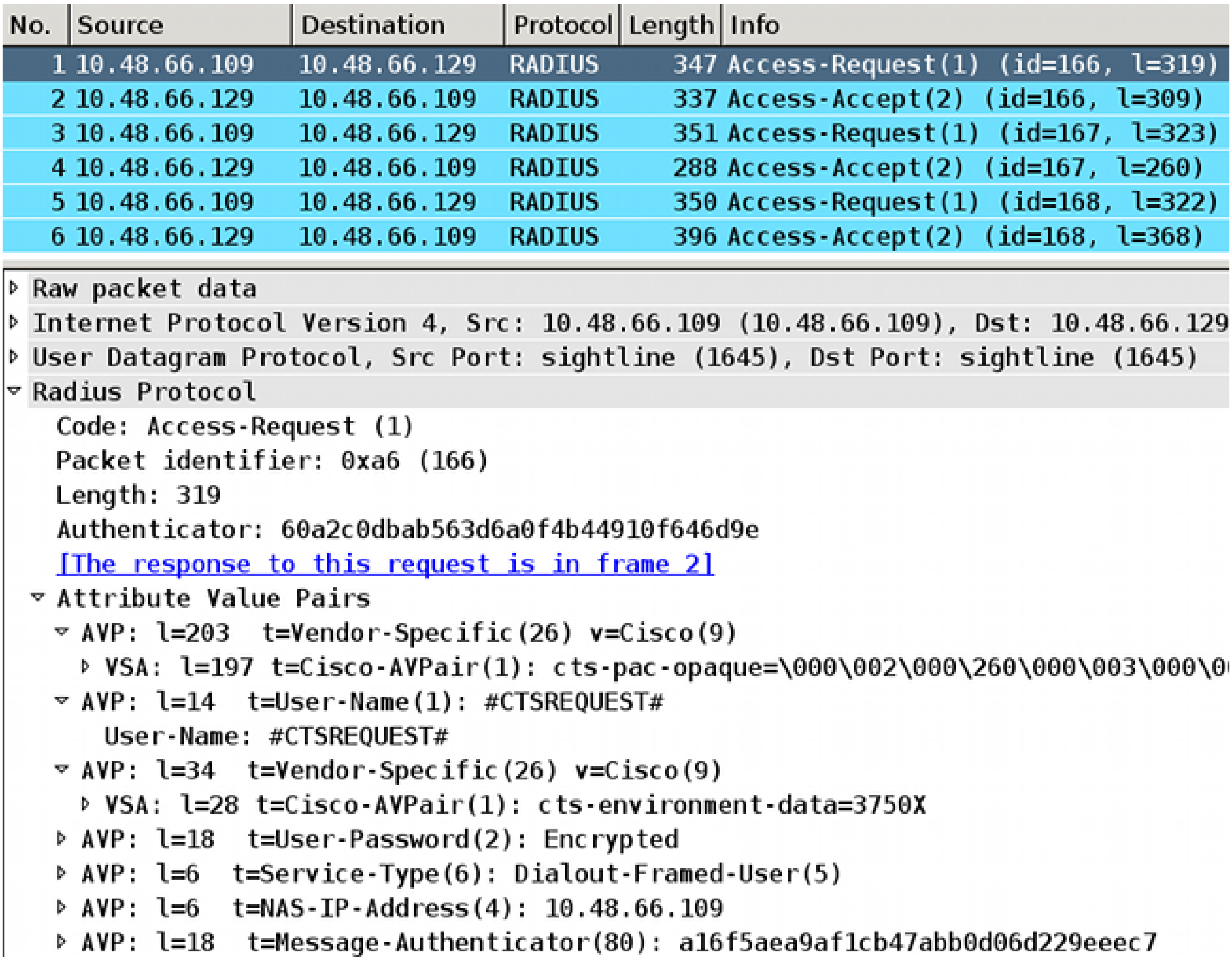
```
No. Source        Destination   Protocol Length Info
  1 10.48.66.109  10.48.66.129  RADIUS      347 Access-Request(1) (id=166, l=319)
  2 10.48.66.129  10.48.66.109  RADIUS      337 Access-Accept(2) (id=166, l=309)
  3 10.48.66.109  10.48.66.129  RADIUS      351 Access-Request(1) (id=167, l=323)
  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): 5265617574685365737369 6f6e3a30613330343238313030...
  ▹ AVP: l=50  t=Class(25): 434143533a30613330343238313030303031343033353143...
  ▹ 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
```

此處您會看到預設的**SGT 0**、 **ffff**以及兩個自訂定義：SGT標籤2命名為**VLAN10**,SGT標籤3命名為**VLAN20**。

注意：由於PAC調配，所有RADIUS請求都包括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)

```
▷ Raw packet data
▷ Internet Protocol Version 4, Src: 10.48.66.109 (10.48.66.109), Dst: 10.48.66.129
▷ User Datagram Protocol, Src Port: sightline (1645), Dst Port: sightline (1645)
▽ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xa6 (166)
    Length: 319
    Authenticator: 60a2c0dbab563d6a0f4b44910f646d9e
    [The response to this request is in frame 2]
  ▽ Attribute Value Pairs
    ▽ AVP: l=203  t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=197 t=Cisco-AVPair(1): cts-pac-opaque=\000\002\000\260\000\003\000\0
    ▽ AVP: l=14  t=User-Name(1): #CTSREQUEST#
        User-Name: #CTSREQUEST#
    ▽ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=28 t=Cisco-AVPair(1): cts-environment-data=3750X
    ▷ AVP: l=18  t=User-Password(2): Encrypted
    ▷ AVP: l=6  t=Service-Type(6): Dialout-Framed-User(5)
    ▷ AVP: l=6  t=NAS-IP-Address(4): 10.48.66.109
    ▷ AVP: l=18  t=Message-Authenticator(80): a16f5aea9af1cb47abb0d06d229eeec7
```

在3750X上，您應該會看到所有三種RADIUS回應的偵錯，以及對應的清單、清單詳細資訊和特定的SGT-inside清單：

```
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)
```

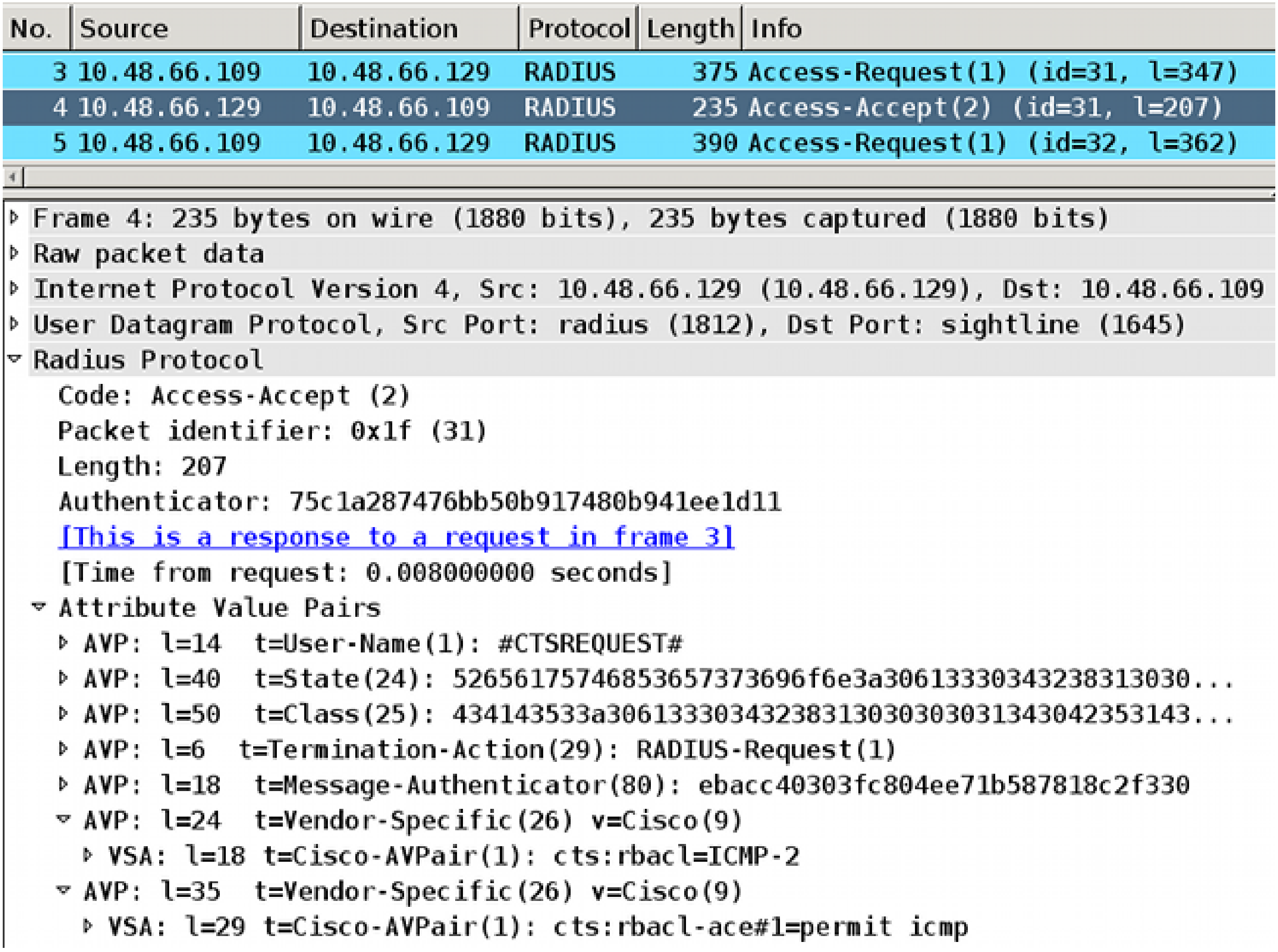
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: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

只有交換機支援策略刷新。它類似於環境刷新。這些只是RADIUS請求和接受。

交換器會要求取得預設清單中的所有ACL。然後，對於每個不是最新的（或不存在）的ACL，它會傳送另一個請求以獲取詳細資訊。

以下是您要求ICMP-20 ACL時的回應範例：



No.	Source	Destination	Protocol	Length	Info
3	10.48.66.109	10.48.66.129	RADIUS	375	Access-Request(1) (id=31, l=347)
4	10.48.66.129	10.48.66.109	RADIUS	235	Access-Accept(2) (id=31, l=207)
5	10.48.66.109	10.48.66.129	RADIUS	390	Access-Request(1) (id=32, l=362)

```
▷ Frame 4: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
▷ Raw packet data
▷ Internet Protocol Version 4, Src: 10.48.66.129 (10.48.66.129), Dst: 10.48.66.109
▷ User Datagram Protocol, Src Port: radius (1812), Dst Port: sightline (1645)
▽ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1f (31)
    Length: 207
    Authenticator: 75c1a287476bb50b917480b941ee1d11
    [This is a response to a request in frame 3]
    [Time from request: 0.008000000 seconds]
  ▽ Attribute Value Pairs
    ▷ AVP: l=14  t=User-Name(1): #CTSREQUEST#
    ▷ AVP: l=40  t=State(24): 526561757468536573736f6e3a30613330343238313030...
    ▷ AVP: l=50  t=Class(25): 434143533a3061333034323831303030303134304235143...
    ▷ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
    ▷ AVP: l=18  t=Message-Authenticator(80): ebacc40303fc804ee71b587818c2f330
    ▽ AVP: l=24  t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=18 t=Cisco-AVPair(1): cts:rbacl=ICMP-2
    ▽ AVP: l=35  t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=29 t=Cisco-AVPair(1): cts:rbacl-ace#1=permit icmp
```

請記住，您必須配置**cts role-based enforcement**才能強制實施該ACL。

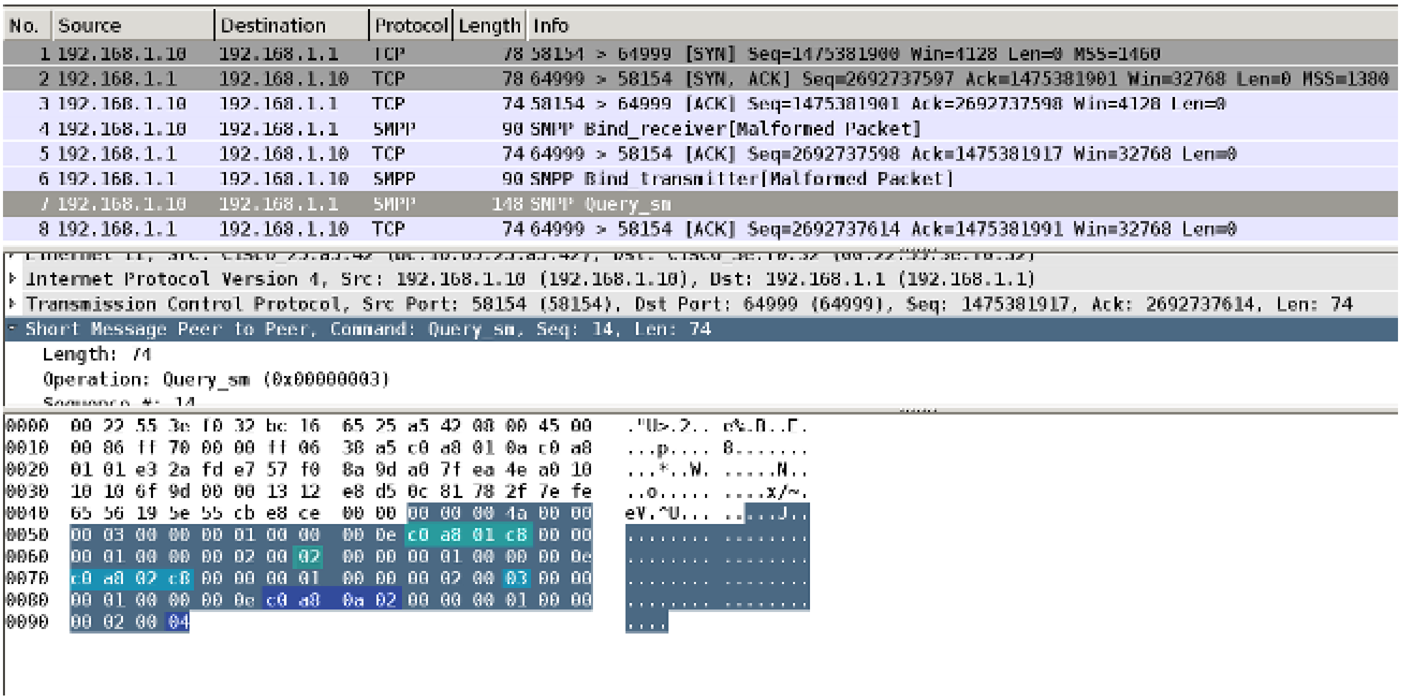
調試指示是否存在更改（基於代ID）。如果需要，可以解除安裝舊策略，然後安裝新策略。這包括ASIC程式設計（硬體支援）。

```
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

SXP更新由查詢裝置IP地址的IP裝置跟蹤代碼觸發。接著，使用短訊息對等(SMPP)通訊協定來傳送更新。它使用**TCP選項19**進行驗證，這與邊界閘道通訊協定(BGP)相同。SMPP負載未加密。Wireshark沒有用於SMPP負載的合適解碼器，但很容易找到其中的資料：



```
No. Source        Destination   Protocol Length Info
  1 192.168.1.10  192.168.1.1   TCP      78 58154 > 64999 [SYN] Seq=1475381900 Win=4128 Len=0 MSS=1460
  2 192.168.1.1   192.168.1.10  TCP      78 64999 > 58154 [SYN, ACK] Seq=2692737597 Ack=1475381901 Win=32768 Len=0 MSS=1380
  3 192.168.1.10  192.168.1.1   TCP      74 58154 > 64999 [ACK] Seq=1475381901 Ack=2692737598 Win=4128 Len=0
  4 192.168.1.10  192.168.1.1   SMPP     90 SMPP Bind_receiver[Malformed Packet]
  5 192.168.1.1   192.168.1.10  TCP      74 64999 > 58154 [ACK] Seq=2692737598 Ack=1475381917 Win=32768 Len=0
  6 192.168.1.1   192.168.1.10  SMPP     90 SMPP Bind_transmitter[Malformed Packet]
  7 192.168.1.10  192.168.1.1   SMPP    148 SMPP Query_sm
  8 192.168.1.1   192.168.1.10  TCP      74 64999 > 58154 [ACK] Seq=2692737614 Ack=1475381991 Win=32768 Len=0
```

```
▸ Internet Protocol Version 4, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.1 (192.168.1.1)
▸ Transmission Control Protocol, Src Port: 58154 (58154), Dst Port: 64999 (64999), Seq: 1475381917, Ack: 2692737614, Len: 74
▾ Short Message Peer to Peer, Command: Query_sm, Seq: 14, Len: 74
    Length: 74
    Operation: Query_sm (0x00000003)
    Sequence #: 14
```

```
0000  00 22 55 3e f0 32 bc 16  65 25 a5 42 08 00 45 00   ."U>.2.. e%.B..E.
0010  00 86 ff 70 00 00 ff 06  38 a5 c0 a8 01 0a c0 a8   ...p.... 8.......
0020  01 01 e3 2a fd e7 57 f0  8a 9d a0 7f ea 4e a0 10   ...*..W. .....N..
0030  10 10 6f 9d 00 00 13 12  e8 d5 0c 81 78 2f 7e fe   ..o..... ....x/~.
0040  65 56 19 5e 55 cb e8 ce  00 00 00 00 00 4a 00 00   eV.^U... .....J..
0050  00 03 00 00 00 01 00 00  00 0e c0 a8 01 c8 00 00   ........ ........
0060  00 01 00 00 00 02 00 02  00 00 00 01 00 00 00 0e   ........ ........
0070  c0 a8 02 c8 00 00 00 01  00 00 00 02 00 03 00 00   ........ ........
0080  00 01 00 00 00 0e c0 a8  0a 02 00 00 00 01 00 00   ........ ........
0090  00 02 00 04                                        ....
```

- 第一個c0 a8 01 c8是192.168.1.200，並帶有**標籤**2。
- 第二個c0 a8 02 c8是192.168.2.200，帶有**標籤**3。
- 第三個c0 a8 0a 02是192.168.10.2，具有tag 4(這個用於測試電話SGT=4)

在IP裝置跟蹤找到MS Windows 7的IP地址後，在3750X上進行了一些調試：

```
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上的相應調試：

```
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.
```

為了檢視ASA上的更多調試，您可以啟用調試詳細級別：

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

ASA上的SGACL

在ASA正確安裝SXP接收的SGT對映後，安全組ACL應該可以正常工作。當對映遇到問題時，請輸入：

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

帶有security-group的ACL的工作方式與用於IP地址或使用者身份的ACL的工作方式完全相同。日誌可揭示問題，以及所命中的ACL的確切條目。

以下是從MS Windows XP到MS Windows 7的ping命令，該命令顯示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>
```

相關資訊

- Cisco TrustSec 3750配置指南
- 適用於ASA 9.1的Cisco TrustSec配置指南
- Cisco TrustSec部署和路線圖
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。