Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Esempio di rete](#)
[Flusso traffico](#)
[Configurazioni](#)
[Autenticazione delle porte con il comando *ip device tracking* sullo switch 3750X](#)
[Configurazione ISE per criteri di autenticazione, SGT e SGACL](#)
[Configurazione CTS sull'appliance ASA e sullo switch 3750X](#)
[Provisioning delle PAC sullo switch 3750X (automatico) e sull'appliance ASA (manuale)](#)
[Aggiornamento dell'ambiente sull'appliance ASA e sullo switch 3750X](#)
[Verifica e applicazione dell'autenticazione delle porte sullo switch 3750X](#)
[Aggiornamento della policy sullo switch 3750X](#)
[SXP Exchange (ASA come listener e 3750X come altoparlante)](#)
[Filtraggio del traffico sull'appliance ASA con ACL SGT](#)
[Traffic Filtering sullo switch 3750X con policy scaricate dall'ISE (RBACL)](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Provisioning PAC](#)
[Aggiornamento dell'ambiente](#)
[Aggiornamento criteri](#)
[SXP Exchange](#)
[SGACL sull'appliance ASA](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Cisco TrustSec (CTS) su Cisco Secure Adaptive Security Appliance (ASA) e uno switch Cisco Catalyst serie 3750X (3750X).

Per conoscere il mapping tra i tag del gruppo di sicurezza (SGT) e gli indirizzi IP, l'ASA usa il protocollo SGT Exchange Protocol (SXP). Quindi, per filtrare il traffico, vengono utilizzati gli

Access Control Lists (ACL) basati su SGT. Lo switch 3750X scarica le policy RBACL (Role-Based Access Control List) da Cisco Identity Services Engine (ISE) e filtra il traffico in base a esse. In questo documento viene descritto in dettaglio il livello del pacchetto per descrivere il funzionamento della comunicazione e i debug previsti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Componenti CTS
- Configurazione CLI di ASA e Cisco IOS®

Componenti usati

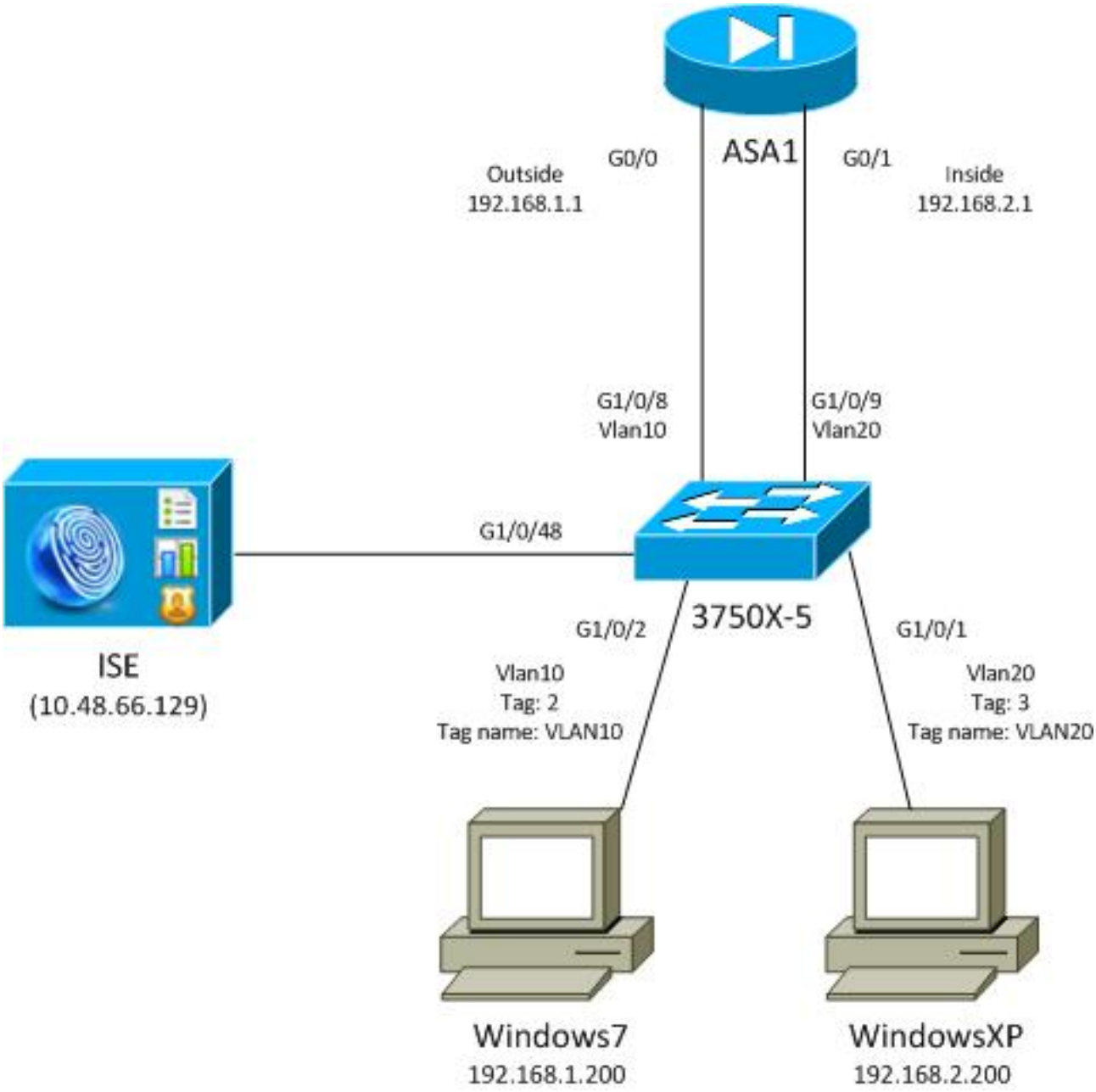
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco ASA, versioni 9.1 e successive
- Microsoft (MS) Windows 7 e MS Windows XP
- Software Cisco 3750X, versioni 15.0 e successive
- Software Cisco ISE, versione 1.1.4 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Flusso traffico

Di seguito viene riportato il flusso del traffico:

- Lo switch 3750X è configurato su **G1/0/1** e **G1/0/2** per l'autenticazione delle porte.
- L'ISE viene usato come server di autenticazione, autorizzazione e accounting (AAA).
- MAC Address Bypass (MAB) viene utilizzato per l'autenticazione per MS Windows 7.
- IEEE 802.1x viene utilizzato per MS Windows XP per dimostrare che non importa quale metodo di autenticazione viene utilizzato.

Una volta completata l'autenticazione, ISE restituisce il SGT e lo switch 3750X associa il tag alla sessione di autenticazione. Lo switch impara anche gli indirizzi IP di entrambe le stazioni con il comando **ip device tracking**. Lo switch usa quindi SXP per inviare la tabella di mapping tra il server SGT e l'indirizzo IP all'appliance ASA. I due PC MS Windows dispongono di un routing predefinito che punta all'ASA.

Dopo aver ricevuto il traffico dall'indirizzo IP mappato al SGT, l'ASA può usare l'ACL basato sul SGT. Inoltre, quando si usa lo switch 3750X come router (gateway predefinito per entrambe le

postazioni di MS Windows), è possibile filtrare il traffico in base ai criteri scaricati dall'ISE.

Di seguito viene riportata la procedura per la configurazione e la verifica, ognuna delle quali viene descritta in dettaglio nella sezione successiva del documento:

- Autenticazione delle porte con il comando **ip device tracking** sullo switch 3750X
- Configurazione ISE per i criteri di autenticazione, SGT e SGACL (Security Group Access Control List)
- Configurazione CTS sull'appliance ASA e sullo switch 3750X
- Provisioning delle credenziali di accesso protetto (PAC) sullo switch 3750X (automatico) e sull'appliance ASA (manuale)
- Aggiornamento dell'ambiente sull'appliance ASA e sullo switch 3750X
- Verifica dell'autenticazione delle porte e applicazione del protocollo 3750X
- Aggiornamento delle policy sullo switch 3750X
- Scambio SXP (ASA come listener e 3750X come speaker)
- Filtraggio del traffico sull'appliance ASA con ACL SGT
- Traffic Filtering sullo switch 3750X con policy scaricate da ISE

Configurazioni

Autenticazione delle porte con il comando *ip device tracking* sullo switch 3750X

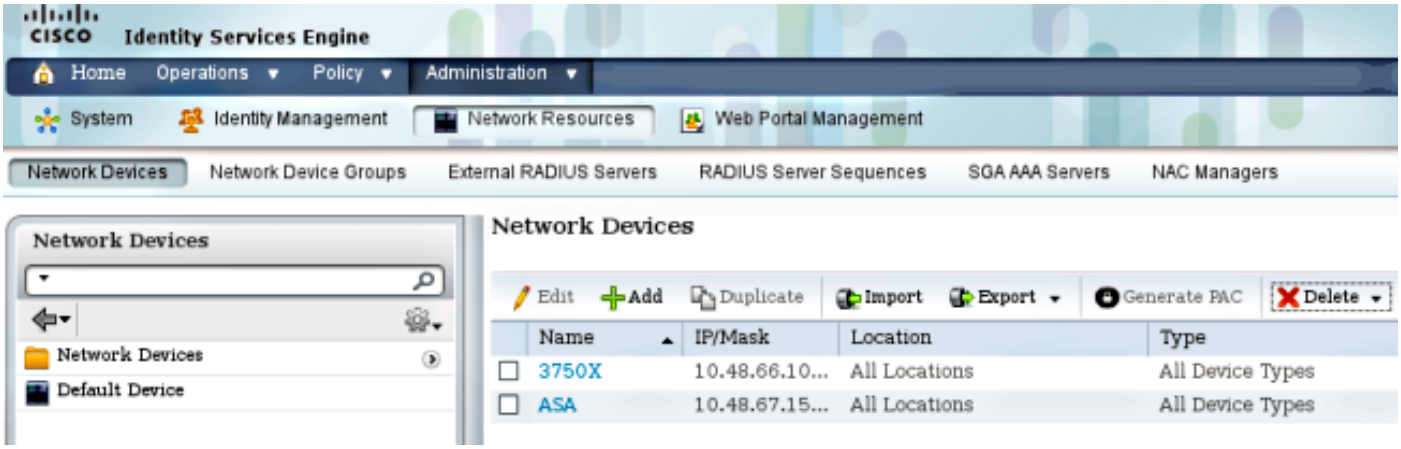
Questa è la configurazione tipica per 802.1x o MAB. RADIUS Change of Authorization (CoA) è richiesto solo quando si utilizza la notifica attiva dall'ISE.

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

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

ip device tracking

interface GigabitEthernet1/0/1
 description windowsxp
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
```

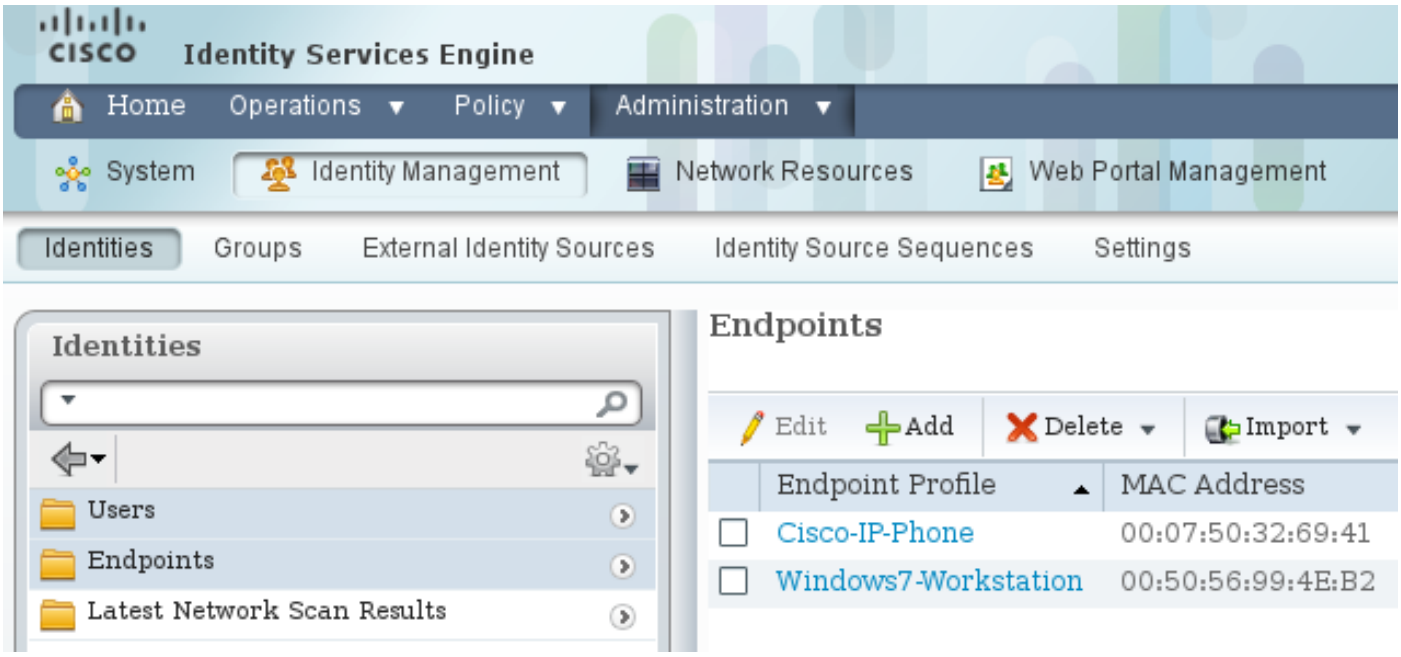
```
spanning-tree portfast

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

Configurazione ISE per criteri di autenticazione, SGT e SGACL

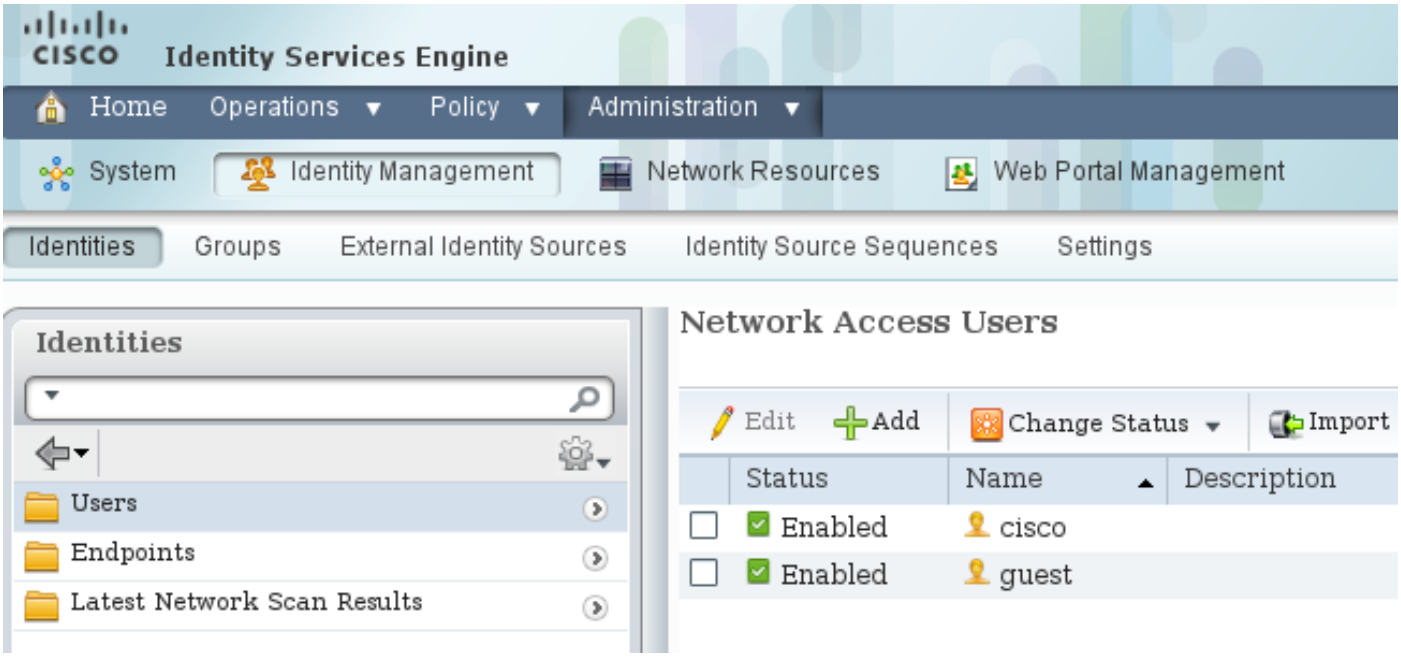
Nell'ISE devono essere configurati entrambi i dispositivi di rete in **Amministrazione > Dispositivi di rete**:



Per MS Windows 7, che utilizza l'autenticazione MAB, è necessario creare l'identità dell'endpoint (indirizzo MAC) in **Amministrazione > Gestione identità > Identità > Endpoint**:

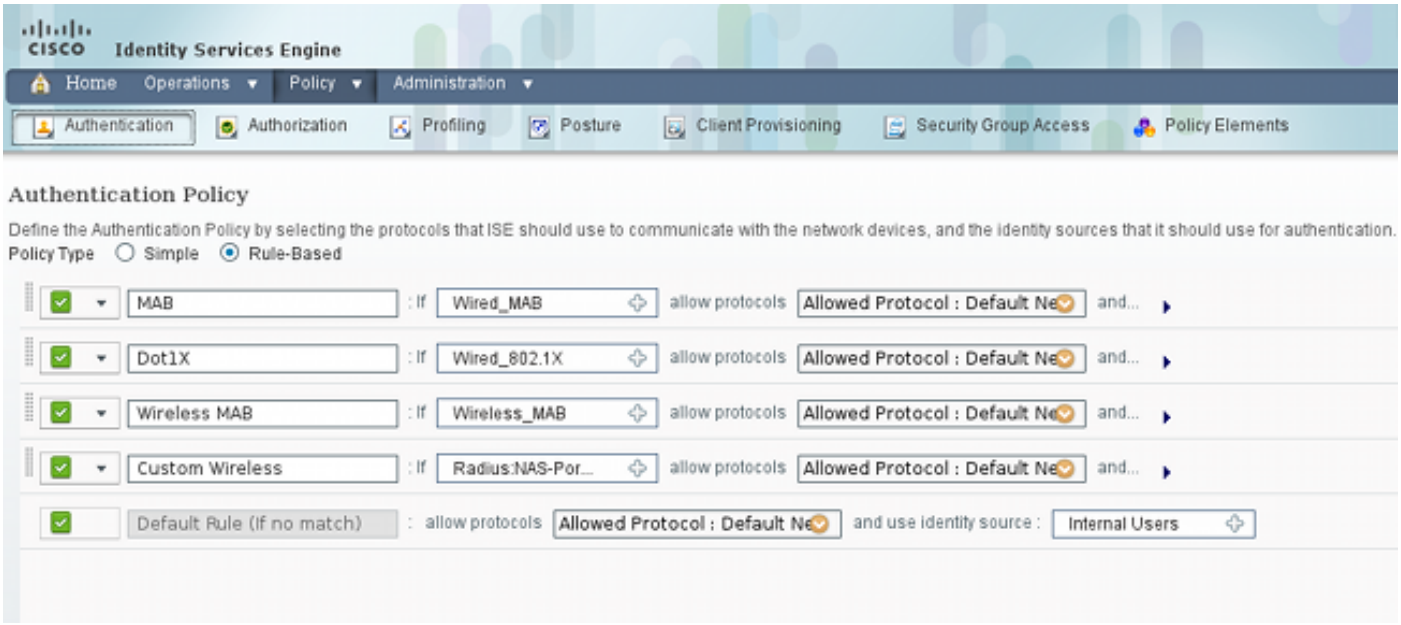


Per MS Windows XP, che utilizza l'autenticazione 802.1x, è necessario creare un'identità utente (nome utente) in **Amministrazione > Gestione identità > Identità > Utenti**:

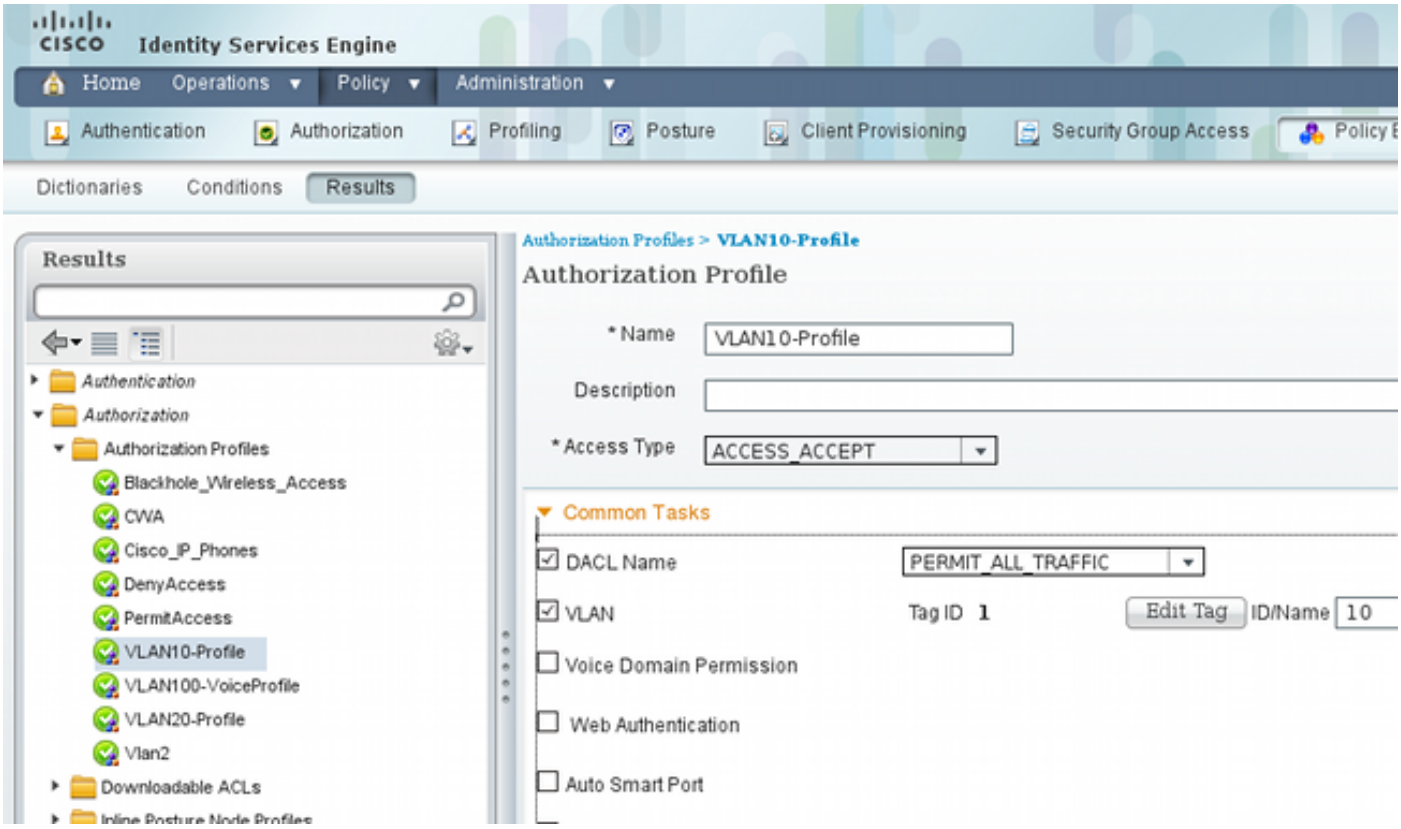


Viene usato il nome utente **cisco**. Configurare MS Windows XP per Extensible Authentication Protocol-Protected EAP (EAP-PEAP) con queste credenziali.

Sull'ISE, vengono utilizzati i criteri di autenticazione predefiniti (non modificare questa impostazione). Il primo è il criterio per l'autenticazione MAB, il secondo è 802.1x:



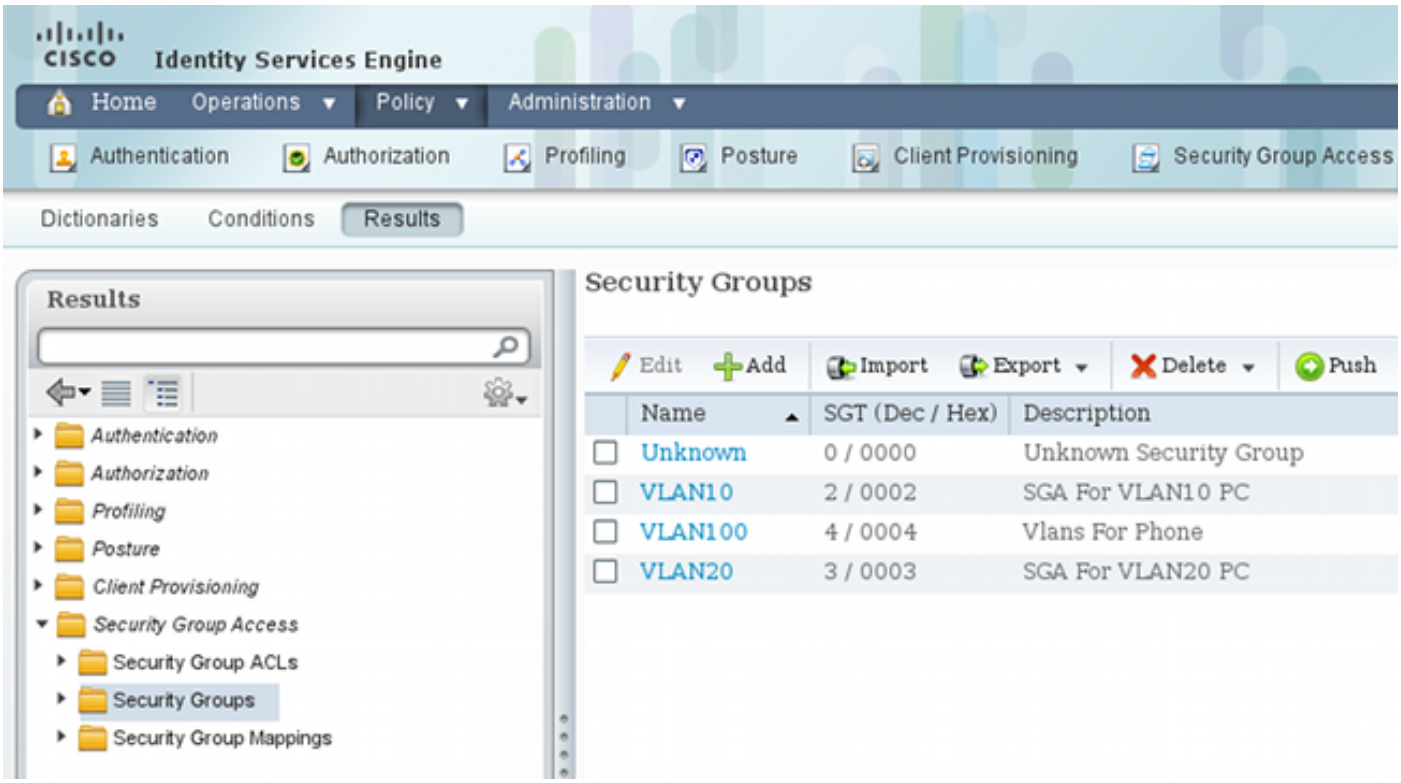
Per configurare i criteri di autorizzazione, è necessario definire i profili di autorizzazione in **Criteri > Risultati > Autorizzazione > Profili di autorizzazione**. Il profilo VLAN10 con ACL scaricabile (DACL), che consente tutto il traffico, è usato per il profilo MS Windows 7:



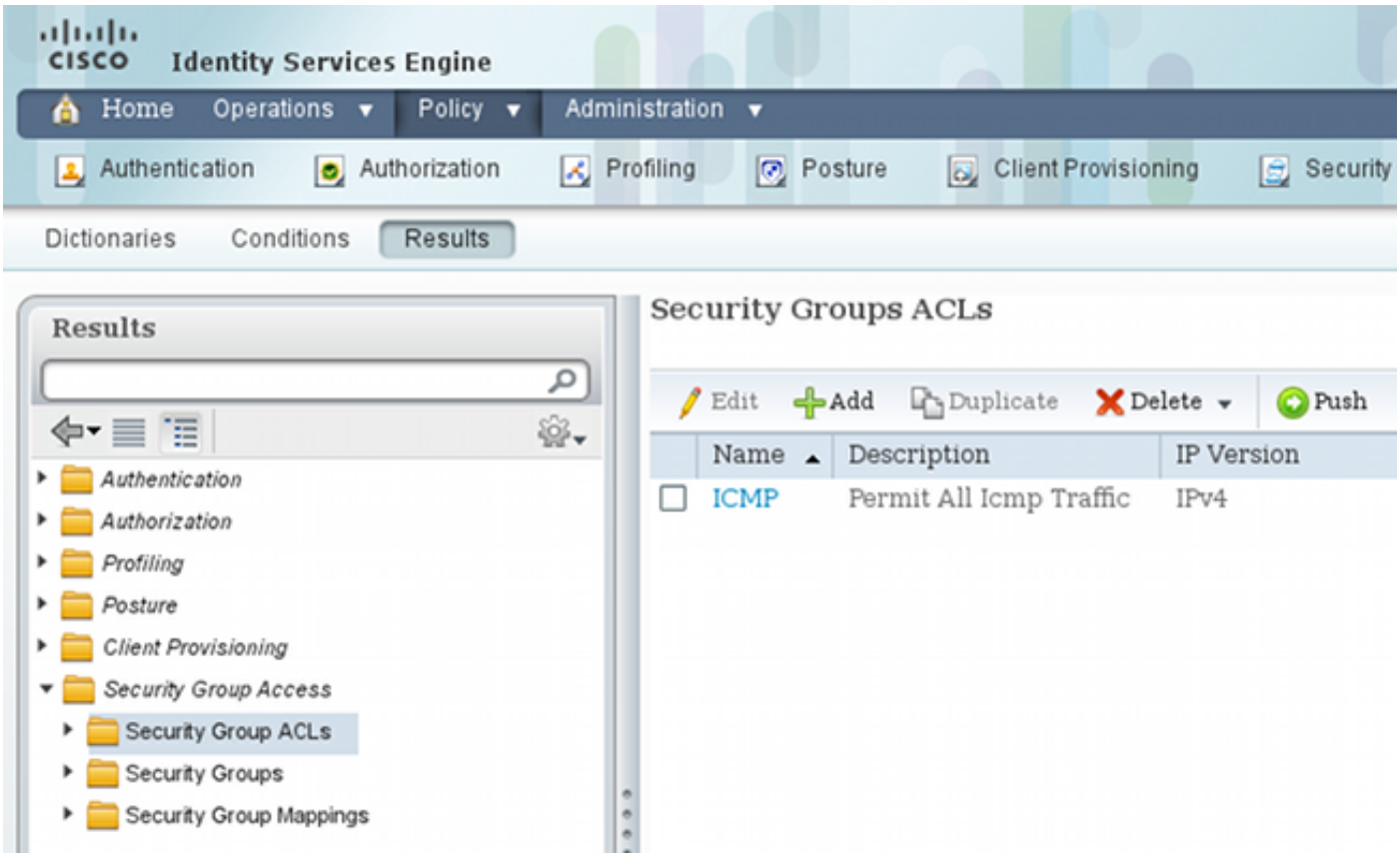
Una configurazione simile, VLAN20-Profile, viene utilizzata per MS Windows XP ad eccezione del numero VLAN (20).

Per configurare i gruppi SGT (tag) su ISE, selezionare **Policy > Results > Security Group Access > Security Groups** (Criteri > Risultati > Accesso al gruppo di sicurezza > Gruppi di sicurezza).

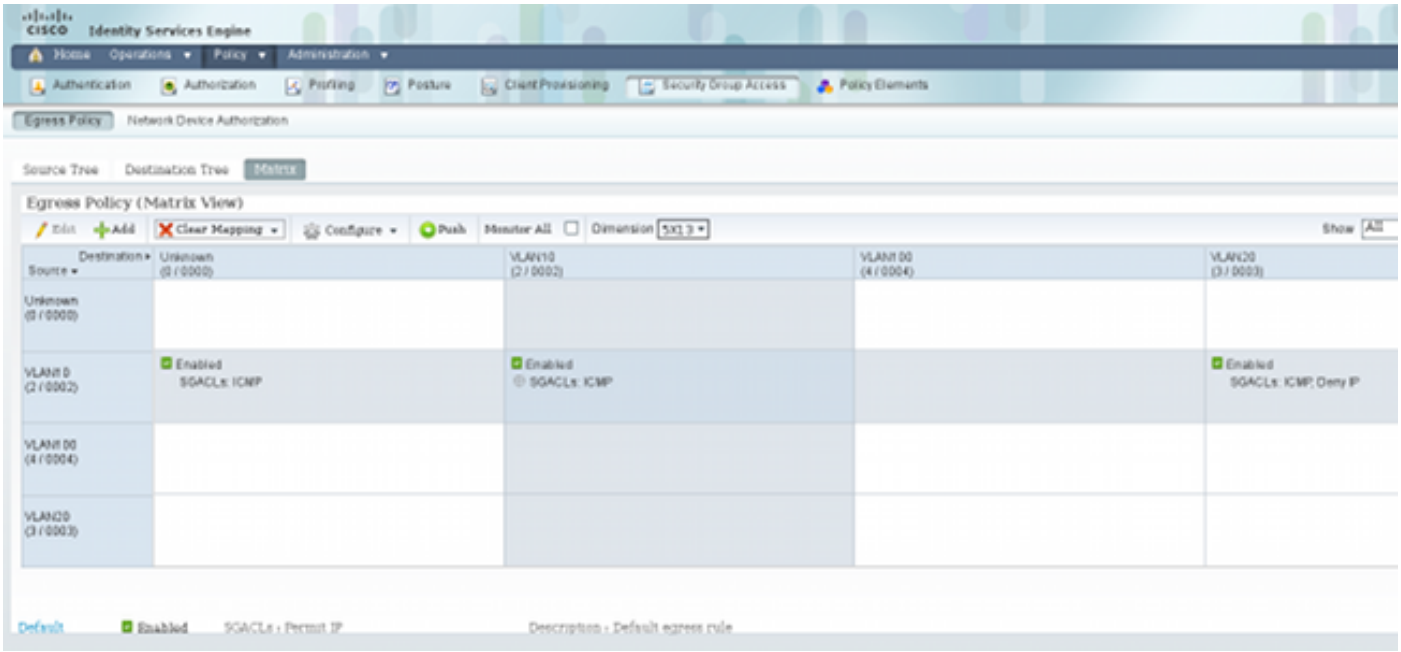
> **Nota**: non è possibile scegliere un numero di cartellino; viene selezionato automaticamente dal primo numero libero ad eccezione di 1. È possibile configurare solo il nome SGT.



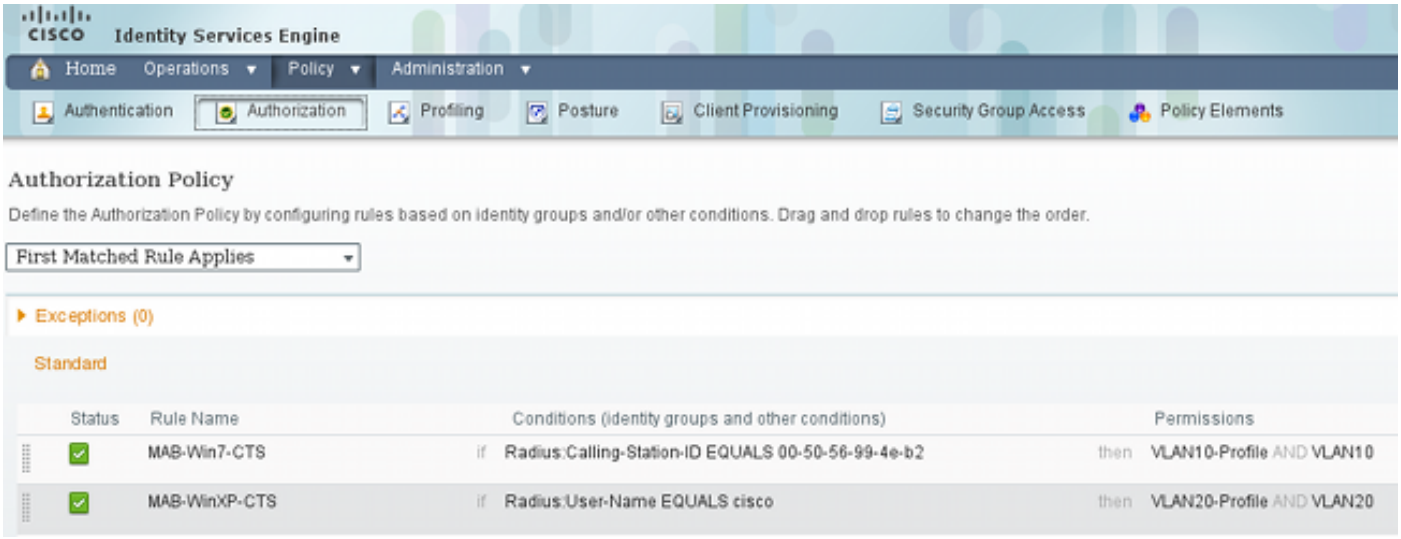
Per creare il SGACL in modo da consentire il traffico ICMP (Internet Control Message Protocol), selezionare **Criteri > Risultati > Accesso al gruppo di sicurezza > ACL del gruppo di sicurezza**:



Per creare i criteri, selezionare **Criteri > Accesso al gruppo di sicurezza > Criteri in uscita**. Per il traffico tra la VLAN10 e la VLAN sconosciuta o la VLAN10 o la VLAN20, viene usato l'ACL ICMP (**permettere l'icmp**):



Per impostare le regole di autorizzazione, passare a **Criterio > Autorizzazione**. Per MS Windows 7 (indirizzo MAC specifico), viene utilizzato **VLAN10-Profile** che restituisce VLAN10 e DACL e il profilo di sicurezza VLAN10 con SGT denominato **VLAN10**. Per MS Windows XP (nome utente specifico), viene utilizzato **VLAN20-Profile** che restituisce VLAN 20 e DACL e il profilo di sicurezza VLAN20 con SGT denominato **VLAN20**.



Completare la configurazione dello switch e dell'ASA in modo che accettino gli attributi SGT RADIUS.

Configurazione CTS sull'appliance ASA e sullo switch 3750X

Ènecessario configurare le impostazioni CTS di base. Sullo switch 3750X è necessario indicare da quali criteri server scaricare:

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

Sull'appliance ASA, solo il server AAA è richiesto insieme al protocollo CTS che punta a quel server:

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

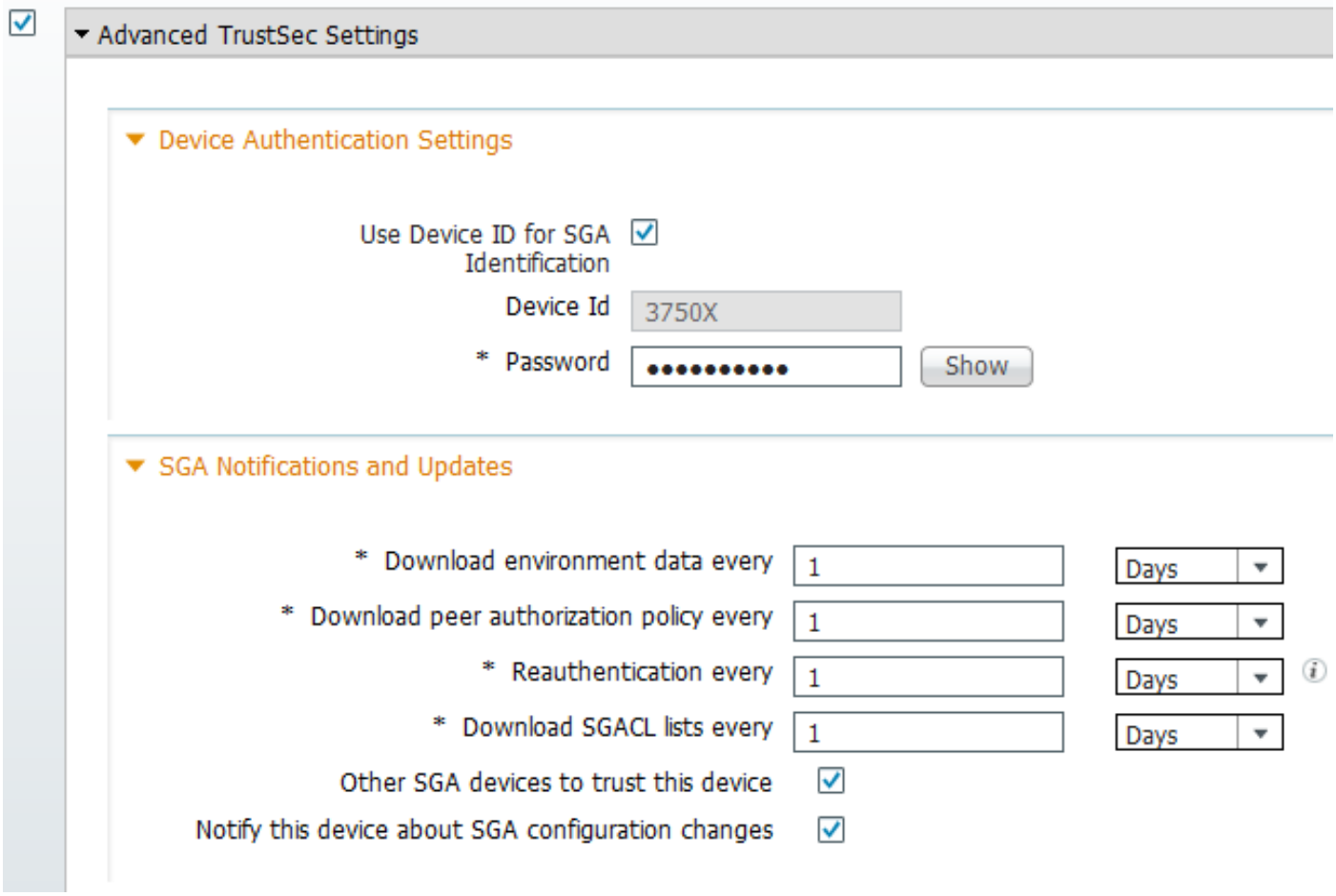
> **Nota**: sullo switch 3750X, è necessario puntare esplicitamente al server ISE con il comando **group radius**. Infatti, lo switch 3750X utilizza la preparazione automatica della PAC.

Provisioning delle PAC sullo switch 3750X (automatico) e sull'appliance ASA (manuale)

Ogni dispositivo nel cloud CTS deve eseguire l'autenticazione al server di autenticazione (ISE) per poter essere considerato attendibile da altri dispositivi. Per questo scopo, viene utilizzato il metodo di autenticazione flessibile EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Protocol) (RFC 4851). Questo metodo richiede la consegna fuori banda della PAC. Questo processo viene anche denominato **fase0** e non è definito in alcuna RFC. Il PAC per EAP-FAST ha un ruolo simile al certificato per EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). La PAC viene usata per stabilire un tunnel sicuro (fase 1), necessario per l'autenticazione nella fase 2.

Provisioning PAC su 3750X

Lo switch 3750X supporta la preparazione automatica della PAC. Sullo switch e sull'ISE viene usata una password condivisa per scaricare la PAC. La password e l'ID devono essere configurati sull'ISE in **Amministrazione > Risorse di rete > Dispositivi di rete**. Selezionare lo switch ed espandere la sezione **Advanced TrustSec Settings** per configurare:



Per fare in modo che la PAC utilizzi queste credenziali, immettere i seguenti comandi:

```
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
```

Provisioning delle PAC sull'appliance ASA

L'ASA supporta solo la preparazione manuale della PAC. Ciò significa che deve essere generata manualmente sull'ISE (in Network Devices/ASA):

Quindi, il file deve essere installato (ad esempio, con 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
```

Aggiornamento dell'ambiente sull'appliance ASA e sullo switch 3750X

In questa fase, entrambi i dispositivi hanno installato correttamente la PAC e iniziano automaticamente a scaricare i dati dell'ambiente ISE. Questi dati sono fondamentalmente numeri di tag e i loro nomi. Per attivare l'aggiornamento di un ambiente sull'appliance ASA, immettere questo comando:

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

Per verificarlo sull'appliance ASA (purtroppo non è possibile visualizzare i tag/nomi SGT specifici, ma è possibile verificarlo in un secondo momento), immettere questo comando:

```
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)
```

Per verificarlo su 3750X, attivare un aggiornamento dell'ambiente con questo comando:

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

Per verificare i risultati, immettere questo comando:

```
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
```

In questo modo, tutti i tag e i nomi corrispondenti vengono scaricati correttamente.

Verifica e applicazione dell'autenticazione delle porte sullo switch 3750X

Dopo che lo switch 3750X ha ricevuto i dati di ambiente, è necessario verificare che i SGT vengano applicati alle sessioni autenticate.

Per verificare se MS Windows 7 è autenticato correttamente, immettere questo comando:

```
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
```

L'output mostrato come la **VLAN10** venga usata insieme all'**SGT 0002** e al DACL, consentendo di tutto il traffico.

Per verificare se MS Windows XP è autenticato correttamente, immettere questo comando:

```
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
```

L'output mostrato come la **VLAN 20** venga usata insieme all'**SGT 003** e al DACL, consentendo tutto il traffico

gli indirizzi IP vengono rilevati con la funzionalità **ip device tracking**. Lo switch DHCP deve essere configurato per lo **snooping dhcp**. Quindi, dopo la risposta DHCP di snooping, viene appreso l'indirizzo IP del client. Per un indirizzo IP configurato in modo statico (come nell'esempio), viene utilizzata la funzionalità di **snooping arp** e il PC deve inviare qualsiasi pacchetto affinché lo switch possa rilevare il proprio indirizzo IP.

Per il **rilevamento dei dispositivi**, potrebbe essere necessario un comando nascosto per attivarlo sulle porte:

```
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
```

Aggiornamento della policy sullo switch 3750X

A differenza dell'ASA, lo switch 3750X può scaricare le policy dall'ISE. Prima di scaricare e applicare un criterio, è necessario attivarlo con i seguenti comandi:

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

Se non viene attivato, il criterio verrà scaricato, ma non installato e non utilizzato per l'imposizione.

Per attivare un aggiornamento dei criteri, immettere questo comando:

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

Per verificare che la policy sia stata scaricata dall'ISE, immettere questo comando:

```
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
```

L'output mostra che viene scaricata solo la parte necessaria del criterio.

Nel cloud CTS, il pacchetto contiene il SGT dell'host di origine e **l'imposizione viene eseguita sul dispositivo di destinazione**. In questo modo, il pacchetto viene inoltrato dall'origine all'ultimo dispositivo, collegato direttamente all'host di destinazione. Il dispositivo è il punto di applicazione, in quanto conosce le SGT dei suoi host con connessione diretta e sa se il pacchetto in entrata con una SGT di origine deve essere autorizzato o rifiutato per la SGT di destinazione specifica.

Questa decisione è basata sulle policy scaricate dall'ISE.

In questo scenario vengono scaricati tutti i criteri. Tuttavia, se si cancella la sessione di autenticazione di MS Windows XP (SGT=VLAN20), non sarà necessario che lo switch scarichi i criteri (riga) che corrispondono alla VLAN20, in quanto non vi sono più dispositivi del SGT collegati allo switch.

La sezione Avanzate (Risoluzione dei problemi) spiega in che modo lo switch 3750X decide quali criteri scaricare con un esame del livello del pacchetto.

SXP Exchange (ASA come listener e 3750X come altoparlante)

L'ASA non supporta il protocollo SGT. Tutti i frame con SGT vengono scartati dall'ASA. Ecco perché lo switch 3750X non può inviare frame con tag SGT all'appliance ASA. Viene invece utilizzato SXP. Questo protocollo consente all'ASA di ricevere informazioni dallo switch sul mapping tra gli indirizzi IP e il protocollo SGT. Con queste informazioni, l'ASA è in grado di mappare gli indirizzi IP alle SGT e di prendere una decisione basata sul SGACL.

Per configurare lo switch 3750X come altoparlante, immettere questi comandi:

```
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
```

Per configurare l'ASA come listener, immettere i seguenti comandi:

```
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
```

Per verificare che l'ASA abbia ricevuto i mapping, immettere questo comando:

```
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
```

Ora, quando l'ASA riceve il pacchetto in arrivo con l'indirizzo IP di origine **192.168.1.200**, è in grado di gestirlo come se provenga da **SGT=2**. Per l'indirizzo IP di origine **192.168.200.2**, è in grado di trattarlo come se provenisse da **SGT=3**. Lo stesso vale per l'indirizzo IP di destinazione.

> **Nota**: lo switch 3750X deve conoscere l'indirizzo IP dell'host associato. Questa operazione viene eseguita mediante il rilevamento dei dispositivi IP. Per un indirizzo IP configurato in modo statico sull'host finale, lo switch deve ricevere qualsiasi pacchetto dopo l'autenticazione. In questo modo viene attivato il rilevamento del dispositivo IP per individuare l'indirizzo IP, attivando così un aggiornamento SXP. Quando è nota solo la SGT, non viene inviata tramite SXP.

Filtraggio del traffico sull'appliance ASA con ACL SGT

Di seguito è riportato un controllo della configurazione dell'ASA:

```
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
```

Viene creato un ACL che viene applicato all'interfaccia interna. Consente tutto il traffico ICMP da **SGT=3** a **SGT=2** (chiamata **VLAN10**):

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

Nota: è possibile utilizzare il numero o il nome del tag.

Se si esegue il ping tra MS Windows XP con indirizzo IP di origine **192.168.2.200** (**SGT=3**) e MS Windows 7 con indirizzo IP **192.168.1.200** (**SGT=2**), l'ASA crea una connessione:

```
%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)
```

Quando si tenta di eseguire la stessa operazione con Telnet, il traffico viene bloccato:

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

L'appliance ASA offre più opzioni di configurazione. È possibile utilizzare sia un tag di protezione che un indirizzo IP sia per l'origine che per la destinazione. Questa regola consente il traffico echo ICMP tra il tag **SGT = 3** e l'indirizzo IP **192.168.2.200** e il tag SGT **VLAN10** e l'indirizzo host di destinazione **192.168.1.200**:

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

Ciò è possibile anche con i gruppi di oggetti:

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

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

Traffic Filtering sullo switch 3750X con policy scaricate dall'ISE (RBACL)

Inoltre, è possibile definire delle policy locali sullo switch. Tuttavia, nell'esempio vengono presentate le policy scaricate dall'ISE. I criteri definiti sull'appliance ASA possono utilizzare sia indirizzi IP che SGT (e il nome utente da Active Directory) in un'unica regola. Le policy definite sullo switch (sia locale che dall'ISE) consentono solo le SGT. Se si desidera utilizzare gli indirizzi IP nelle regole, si consiglia di filtrare l'appliance ASA.

Viene verificato il traffico ICMP tra MS Windows XP e MS Windows 7. Per questo motivo, è necessario modificare il gateway predefinito dall'ASA allo switch 3750X su MS Windows. Lo switch 3750X ha interfacce di routing ed è in grado di indirizzare i pacchetti:

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

Le policy sono già state scaricate dall'ISE. Per verificarle, immettere questo comando:

```
 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
```

Il traffico tra la VLAN10 (MS Windows 7) e la VLAN20 (MS Windows XP) è soggetto all'ACL ICMP-20, scaricato dall'ISE:

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

Per verificare l'ACL, immettere questo comando:

```
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
```

Per verificare il mapping SGT per accertarsi che il traffico proveniente da entrambi gli host sia contrassegnato correttamente, immettere questo comando:

```
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
```

Il protocollo ICMP da MS Windows 7 (**SGT=2**) a MS Windows XP (**SGT=3**) funziona correttamente con ACL ICMP-20. Ciò viene verificato controllando i contatori per il traffico da **2** a **3** (15 pacchetti consentiti):

```
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
```

Dopo aver tentato di utilizzare il contatore Telnet, i pacchetti negati aumentano (ciò non è consentito sugli ACL ICMP-20):

```
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
```

> **Nota**: il carattere asterisco (*) mostrato nell'output è relativo a tutto il traffico senza tag (la colonna e la riga sono chiamate **sconosciute** in Matrix sull'ISE, e usano il tag numero **0**).

Se si ha una voce ACL con la parola chiave log (definita sull'ISE), i dettagli del pacchetto corrispondente e le azioni intraprese vengono registrati come in qualsiasi ACL con la parola chiave log.

Verifica

Per le procedure di verifica, consultare le singole sezioni relative alla configurazione.

Risoluzione dei problemi

Provisioning PAC

Quando si utilizza la preparazione automatica delle credenziali di accesso protette possono verificarsi dei problemi. Ricordarsi di utilizzare la parola chiave **pac** per il server RADIUS. La preparazione automatica della PAC sullo switch 3750X utilizza il metodo EAP-FAST con il protocollo EAP-MSCHAPv2 (Extensible Authentication Protocol) e il metodo interno con l'autenticazione EAP-MSCHAPv2 (Challenge Handshake Authentication Protocol) di Microsoft. Quando si esegue il debug, vengono visualizzati più messaggi RADIUS che fanno parte della negoziazione EAP-FAST utilizzata per creare il tunnel protetto, che utilizza EAP-MSCHAPv2 con l'ID e la password configurati per l'autenticazione.

La prima richiesta RADIUS utilizza AAA **service-type=cts-pac-provisioning** per notificare all'ISE che si tratta di una richiesta PAC.

```
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.
```

Il **rifiuto RADIUS** alla fine dell'output è previsto perché è già stata ricevuta la PAC e non è stato seguito da un ulteriore processo di autenticazione.

Ricorda che la PAC è richiesta per tutte le altre comunicazioni con l'ISE. In caso contrario, lo switch tenta comunque di aggiornare l'ambiente o le policy quando è configurato. Quindi, non collega **ct-opaqueue** (PAC) nelle richieste RADIUS, il che provoca gli errori.

Se il codice PAC è errato, questo messaggio di errore viene visualizzato sull'ISE:

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

Inoltre, se la chiave PAC è errata, sullo switch viene visualizzato questo output del comando **debug** (**debug cts provisioning + debug radius**):

```
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
```

Se si utilizza la convenzione moderna del **server radius**, viene visualizzato quanto segue:

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

> **Nota**: è necessario usare la stessa password sull'ISE usata nelle **impostazioni di autenticazione** del **dispositivo**.

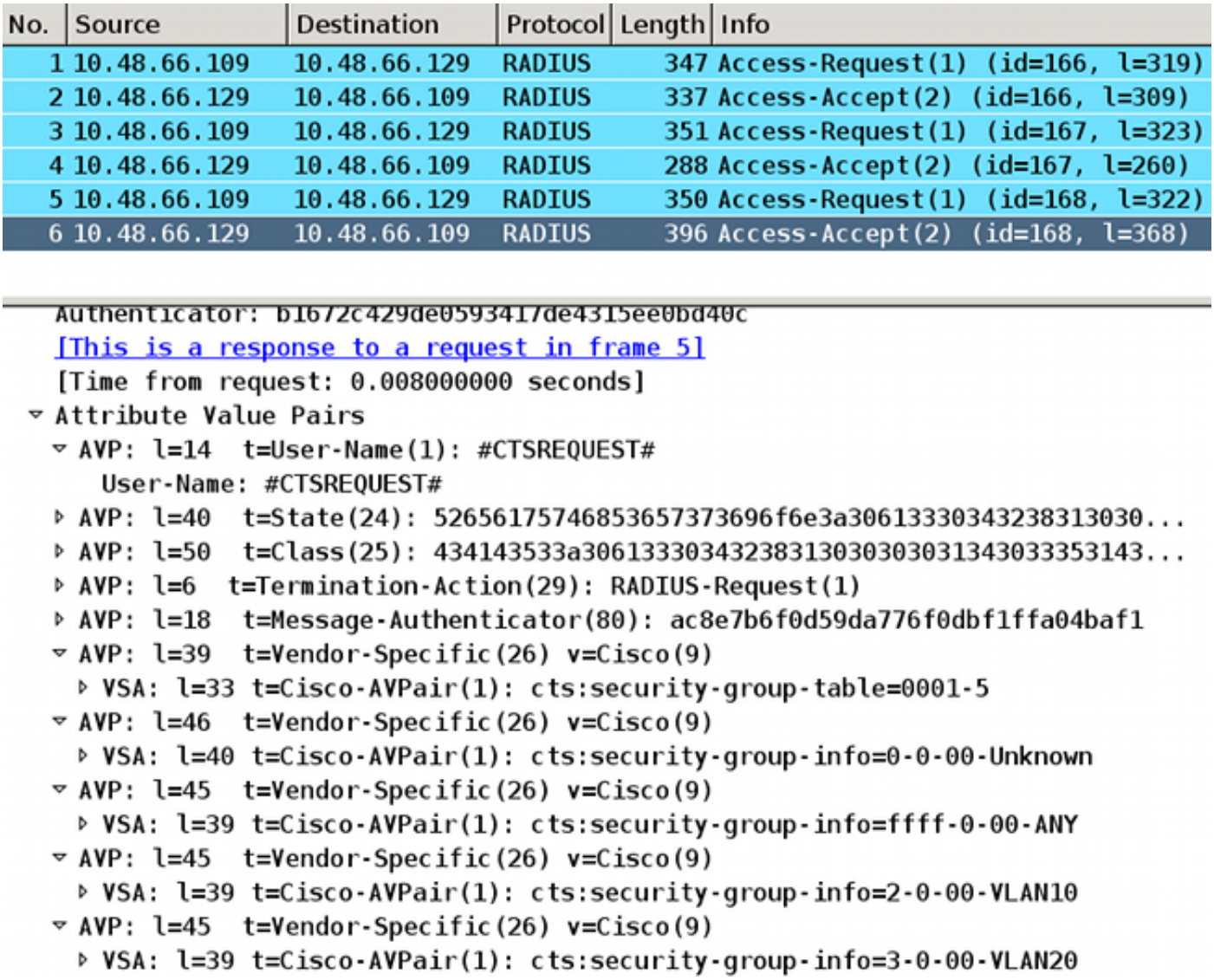
Una volta completata correttamente la preparazione della PAC, questo viene visualizzato sull'ISE:

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

Aggiornamento dell'ambiente

L'aggiornamento dell'ambiente viene utilizzato per ottenere i dati di base dall'ISE, che include il numero e il nome SGT. Il livello di pacchetto indica che sono solo tre le richieste RADIUS e le risposte con attributi.

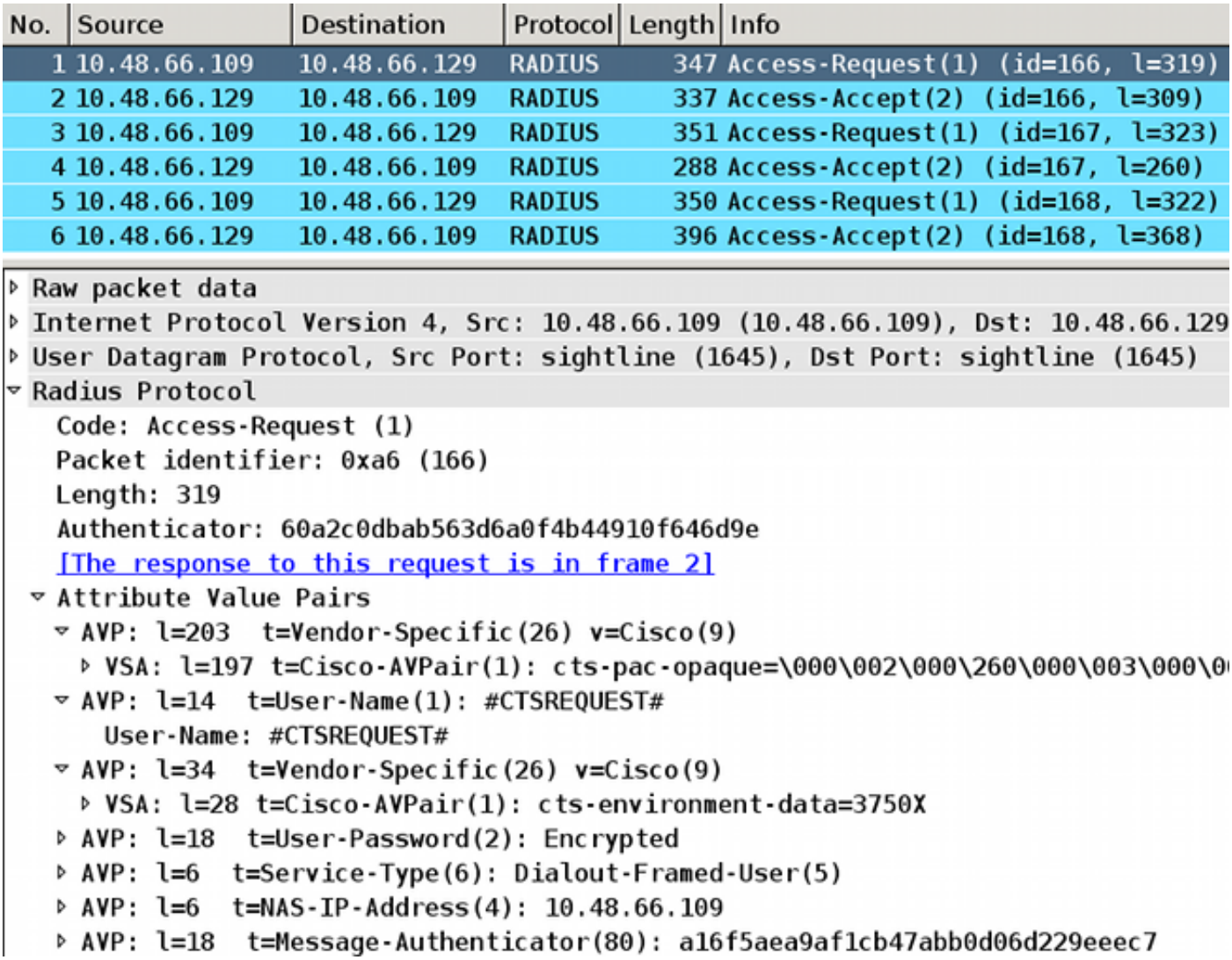
Per la prima richiesta, lo switch riceve il nome **CTSServerlist**. Per il secondo, riceve i dettagli per quell'elenco, e per l'ultimo, riceve tutte le SGT con tag e nomi:



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)

In questa schermata vengono visualizzati il valore predefinito **SGT 0**, **ffff** e due configurazioni personalizzate: SGT tag 2 è denominato **VLAN10** e SGT tag 3 è denominato **VLAN20**.

Nota: tutte le richieste RADIUS includono **ct-pac-opaque** come risultato della preparazione della PAC.



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)

Sullo switch 3750X vengono visualizzati i debug di tutte e tre le risposte RADIUS e degli elenchi corrispondenti, i dettagli dell'elenco e l'elenco SGT-inside specifico:

```
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)
```

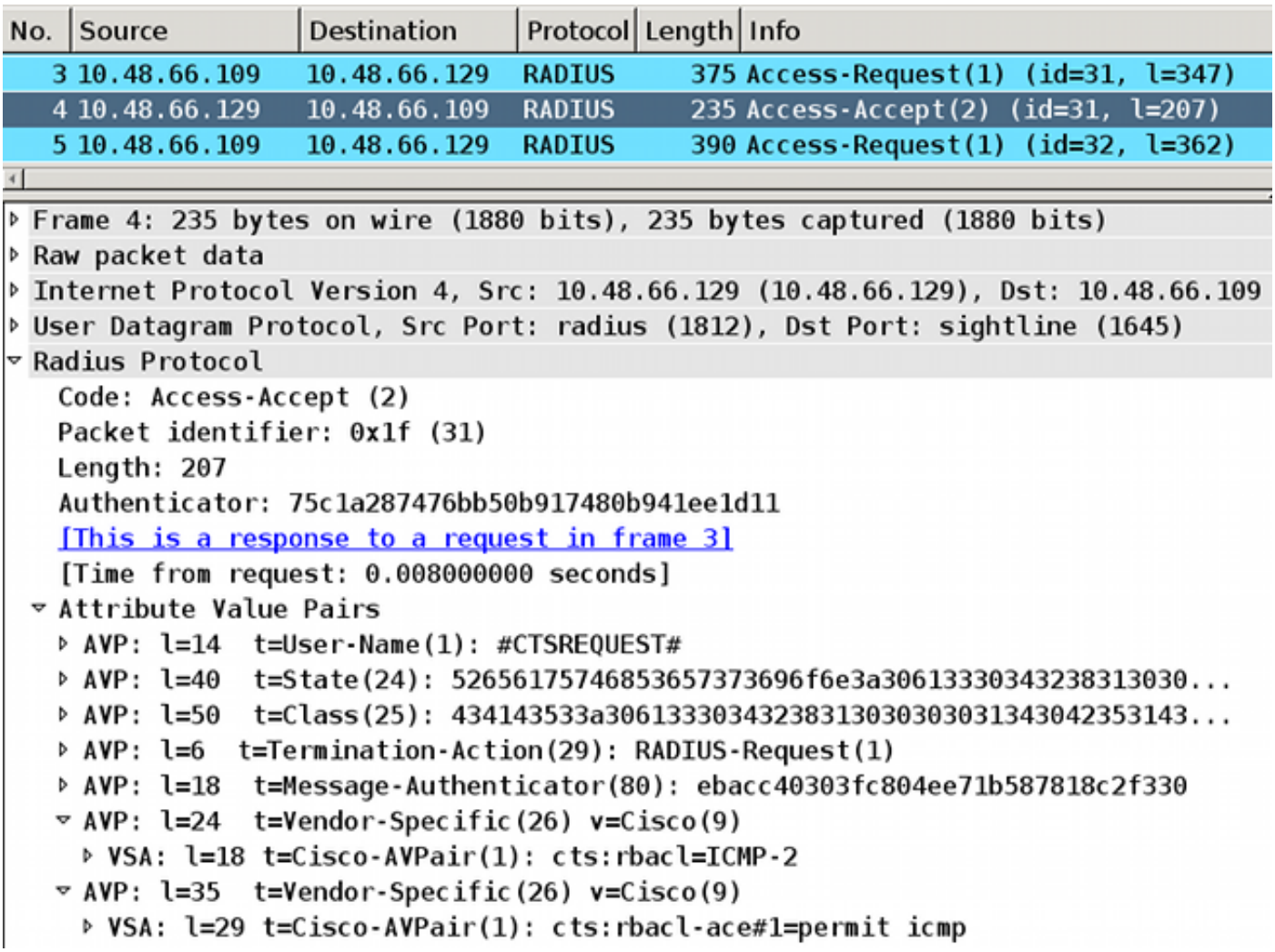
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: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

Aggiornamento criteri

L'aggiornamento dei criteri è supportato solo sullo switch. È simile all'aggiornamento dell'ambiente. Si tratta semplicemente di richieste e accettazioni RADIUS.

Lo switch chiede tutti gli ACL compresi nell'elenco predefinito. Quindi, per ciascun ACL non aggiornato (o non esistente), invia un'altra richiesta per ottenere i dettagli.

Di seguito è riportata una risposta di esempio quando si chiede un ACL ICMP-20:



Tenere presente che per applicare l'ACL occorre configurare l'**imposizione basata sui ruoli** cts.

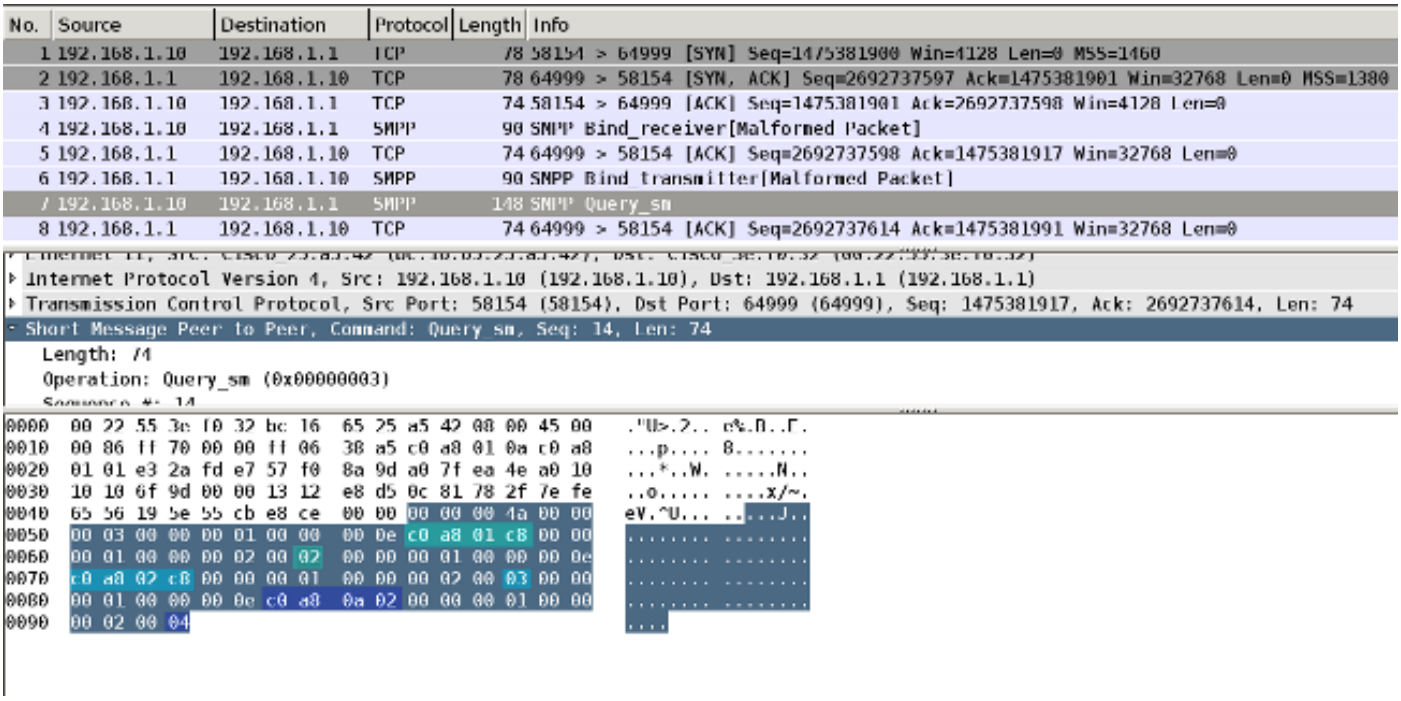
I debug indicano se sono presenti modifiche (in base all'ID gen). In tal caso, è possibile disinstallare il criterio precedente, se necessario, e installarne uno nuovo. Ciò include la programmazione ASIC (supporto hardware).

```
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

L'aggiornamento SXP viene attivato dal codice di rilevamento della periferica IP che individua l'indirizzo IP della periferica. Quindi, per inviare gli aggiornamenti, viene utilizzato il protocollo SMPP (Short Message Peer-to-Peer). Per l'autenticazione viene usata l'**opzione TCP 19**, simile al Border Gateway Protocol (BGP). Payload SMPP non crittografato. Wireshark non dispone di un decodificatore adeguato per il payload SMPP, ma è facile trovare i dati al suo interno:



- Il primo, **c0 a8 01 c8**, è **192.168.1.200** e ha il **tag 2**.
- Il secondo, **c0 a8 02 c8**, è **192.168.2.200** e ha il **tag 3**.
- Il terzo, **c0 a8 0a 02,** è **192.168.10.2** e ha il **tag 4** (questo è stato usato per testare il telefono **SGT=4**)

Di seguito sono riportati alcuni debug del router 3750X dopo che il rilevamento dispositivi IP ha rilevato l'indirizzo IP di MS Windows 7:

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

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

Di seguito sono riportati i corrispondenti debug sull'appliance ASA:

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

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

Per visualizzare altri debug sull'appliance ASA, è possibile abilitare il livello di dettaglio del debug:

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

SGACL sull'appliance ASA

Dopo aver installato correttamente i mapping SGT ricevuti da SXP, l'ACL dei gruppi di sicurezza deve funzionare correttamente. In caso di problemi con il mapping, immettere:

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

Il funzionamento dell'ACL con il gruppo di sicurezza è identico a quello dell'indirizzo IP o dell'identità dell'utente. I log rivelano i problemi, e la voce esatta dell'ACL che è stato colpito.

Di seguito viene riportato un ping tra MS Windows XP e MS Windows 7 che indica che Packet Tracer funziona correttamente:

```
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>
```

Informazioni correlate

- Guida alla configurazione di Cisco TrustSec per 3750
- Guida alla configurazione di Cisco TrustSec per ASA 9.1
- Implementazione di Cisco TrustSec e roadmap
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).