# ASA en Catalyst 3750X Series Switch TrustSec-configuratievoorbeeld en gids voor probleemoplossing

## Inhoud



## Inleiding

In dit artikel wordt beschreven hoe u Cisco TrustSec (CTS) kunt configureren op de Cisco Secure Adaptive Security Applicatie (ASA) en een Cisco Catalyst 3750X Series switch (3750X).

Om de koppeling tussen Security Group Tags (SGT's) en IP-adressen te leren, gebruikt ASA het SGT Exchange Protocol (SXP). Vervolgens worden toegangscontrolelijsten (ACL's) op basis van

SGT gebruikt om het verkeer te filteren. De 3750X downloadt op rollen gebaseerde toegangscontrolelijsten (RBACL) van de Cisco Identity Services Engine (ISE) en filtert verkeer op basis daarvan. Dit artikel beschrijft het pakketniveau om te beschrijven hoe de communicatie werkt en de verwachte debugs.

# Voorwaarden

## Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- CTS-componenten
- CLI-configuratie van ASA en Cisco IOS®

## Gebruikte componenten

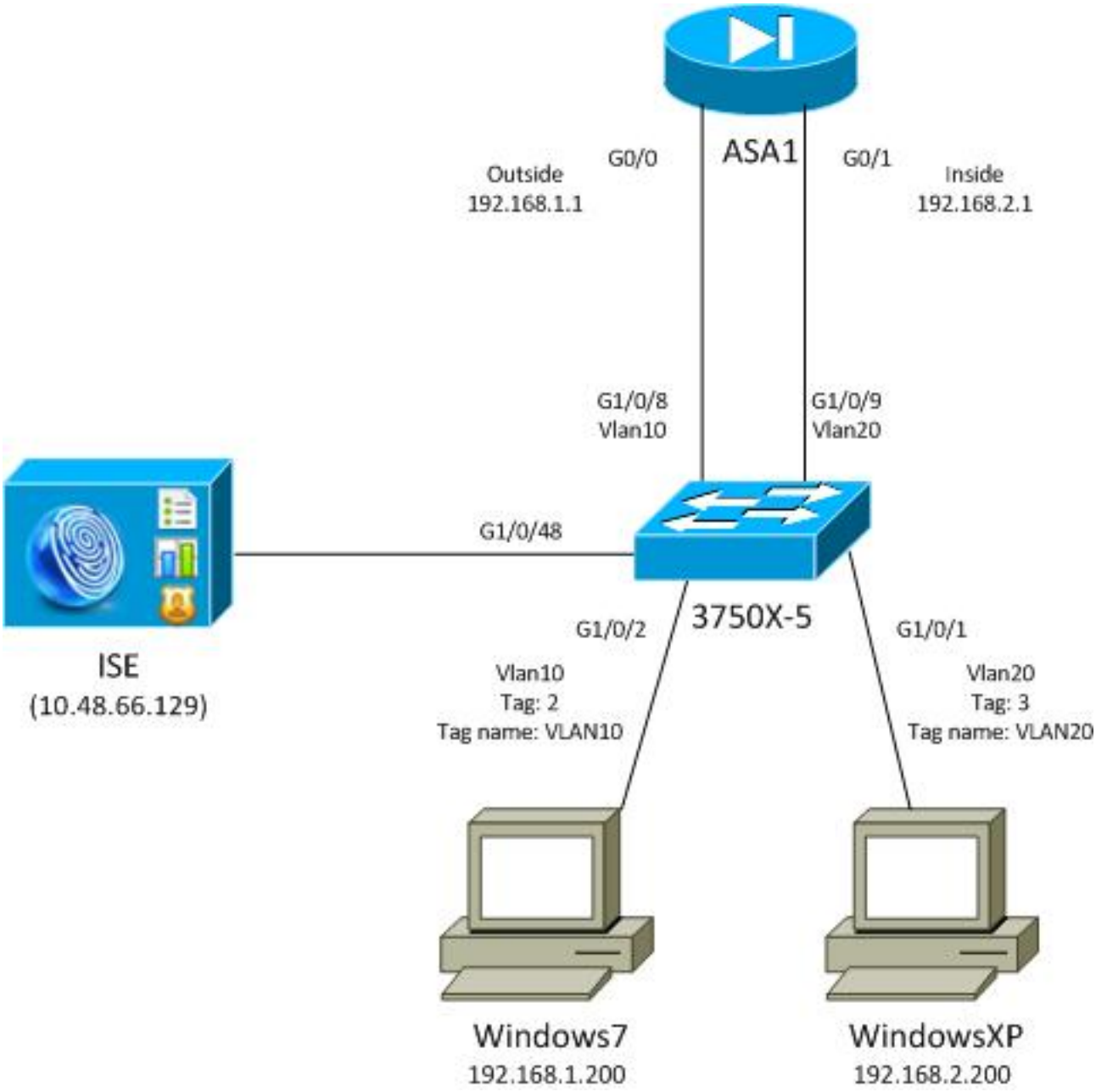
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA-software, versies 9.1 en hoger
- Microsoft (MS) Windows 7 en MS Windows XP
- Cisco 3750X-software, versies 15.0 en hoger
- Cisco ISE-software, versies 1.1.4 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Configureren

## Netwerkdiagram




## Traffic Flow

Hier is de verkeersstroom:

- De 3750X is geconfigureerd op **G1/0/1** en **G1/0/2** voor poortverificatie.
- De ISE wordt gebruikt als de verificatie-, autorisatie- en accounting (AAA) server.
- MAC Address Bypass (MAB) wordt gebruikt voor verificatie van MS Windows 7.
- IEEE 802.1x wordt gebruikt voor MS Windows XP om aan te tonen dat het niet uitmaakt welke verificatiemethode wordt gebruikt.

Na een succesvolle verificatie geeft de ISE de SGT terug en bindt de 3750X die tag aan de verificatiesessie. De switch leert ook de IP-adressen van beide stations met de opdracht **voor het bijhouden** van **IP-apparaten**. De switch gebruikt vervolgens SXP om de mapping tabel tussen de SGT en het IP-adres naar de ASA te verzenden. Beide MS Windows-pc's hebben een standaardrouting die naar de ASA wijst.

Nadat de ASA verkeer ontvangt van het IP-adres dat aan de SGT is toegewezen, kan de ASA de ACL gebruiken die op de SGT is gebaseerd. Ook, wanneer u 3750X als router (standaardgateway

voor beide MS Windows-stations) gebruikt, is het in staat om het verkeer te filteren op basis van beleid dat van de ISE is gedownload.

Hier zijn de stappen voor configuratie en verificatie, elk waarvan in zijn eigen sectie later in het document wordt gedetailleerd:

- Poortverificatie met de opdracht **IP-apparaattracering** op de 3750X
- ISE-configuratie voor verificatie, SGT en beleid op basis van Security Group Access Control List (SGACL)
- CTS-configuratie op de ASA en de 3750X
- Protected Access Credential (PAC) provisioning op de 3750X (automatisch) en de ASA (handmatig)
- Milieu vernieuwing op de ASA en de 3750X
- Verificatie en handhaving van poortverificatie op de 3750X
- Beleidsvernieuwing voor de 3750X
- SXP-uitwisseling (de ASA als luisteraar en de 3750X als luidspreker)
- Traffic filtering op de ASA met SGT ACL
- Traffic filtering op de 3750X met beleid gedownload van de ISE

## Configuraties

### Poortverificatie met *IP*-apparaattracering Opdracht op de 3750X

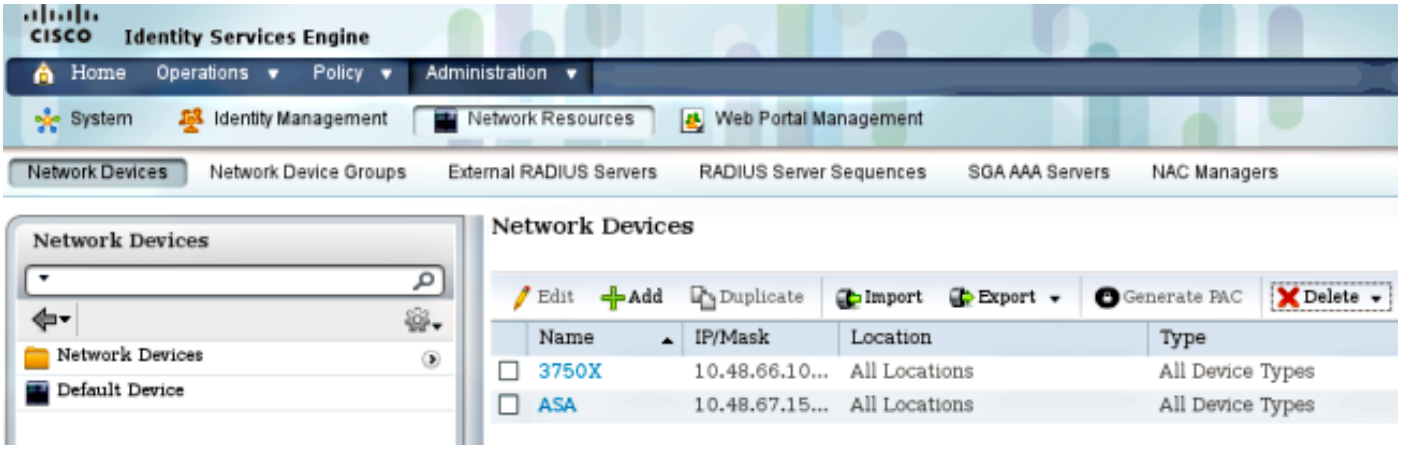
Dit is de standaardconfiguratie voor 802.1x of MAB. RADIUS-wijziging van autorisatie (CoA) is alleen nodig als u actieve meldingen van de ISE gebruikt.

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

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

ip device tracking

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

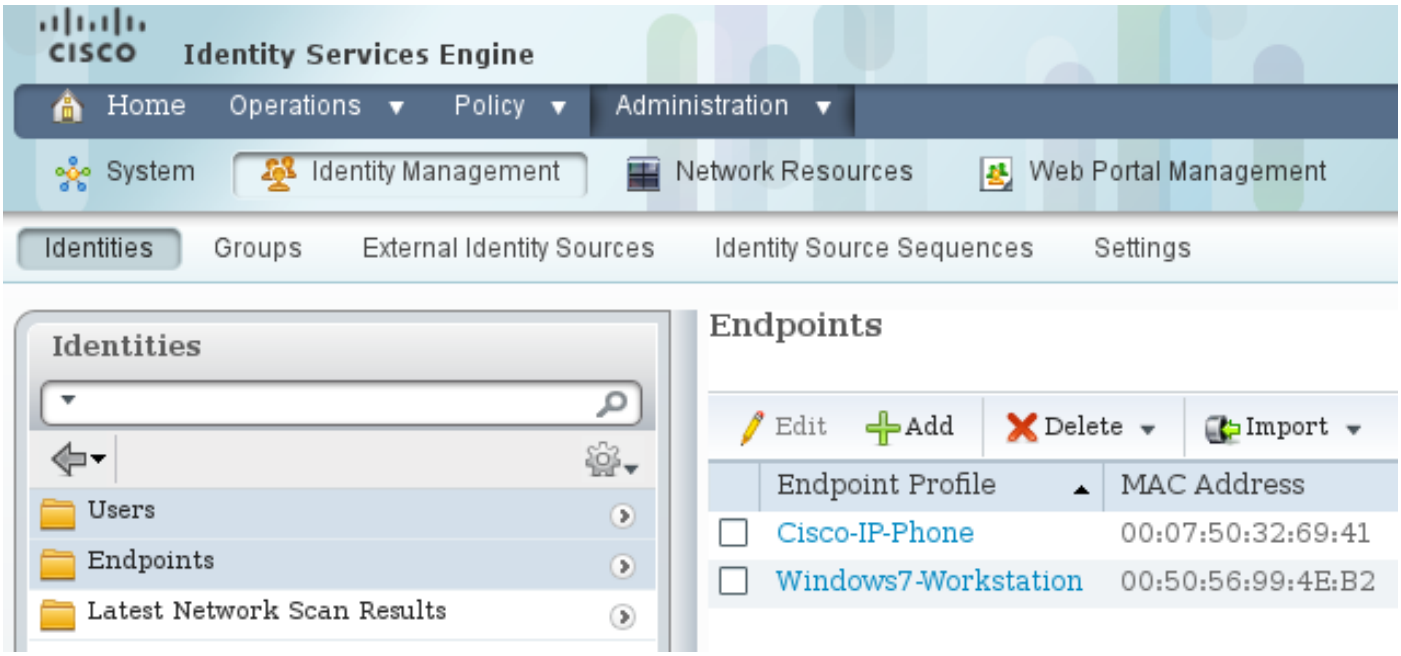
```
 mab
 dot1x pae authenticator
spanning-tree portfast

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

### ISE-configuratie voor verificatie, SGT en SGACL-beleid

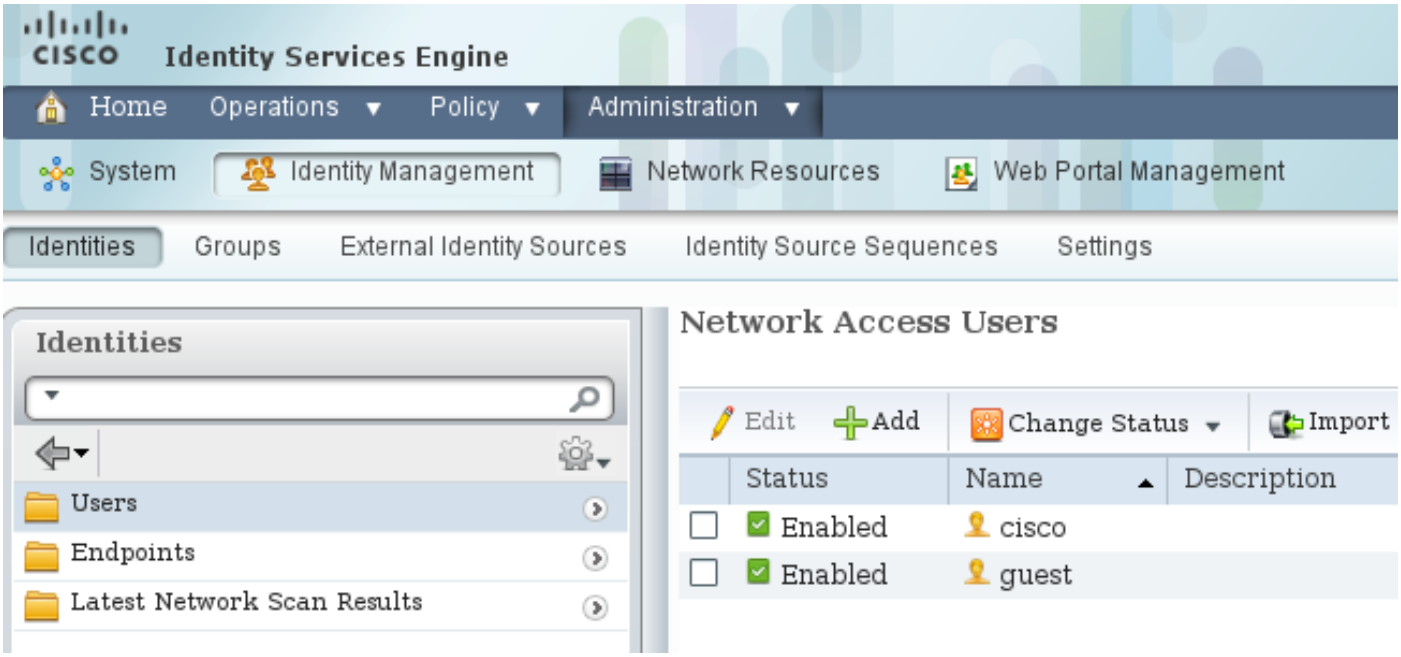
De ISE moet beide netwerkapparaten hebben geconfigureerd onder **Beheer > Netwerkapparaten**:




Voor MS Windows 7, die MAB-verificatie gebruikt, moet u Endpoint Identity (MAC-adres) maken onder **Beheer > Identity Management > Identity > Endpoints > Endpoints**:

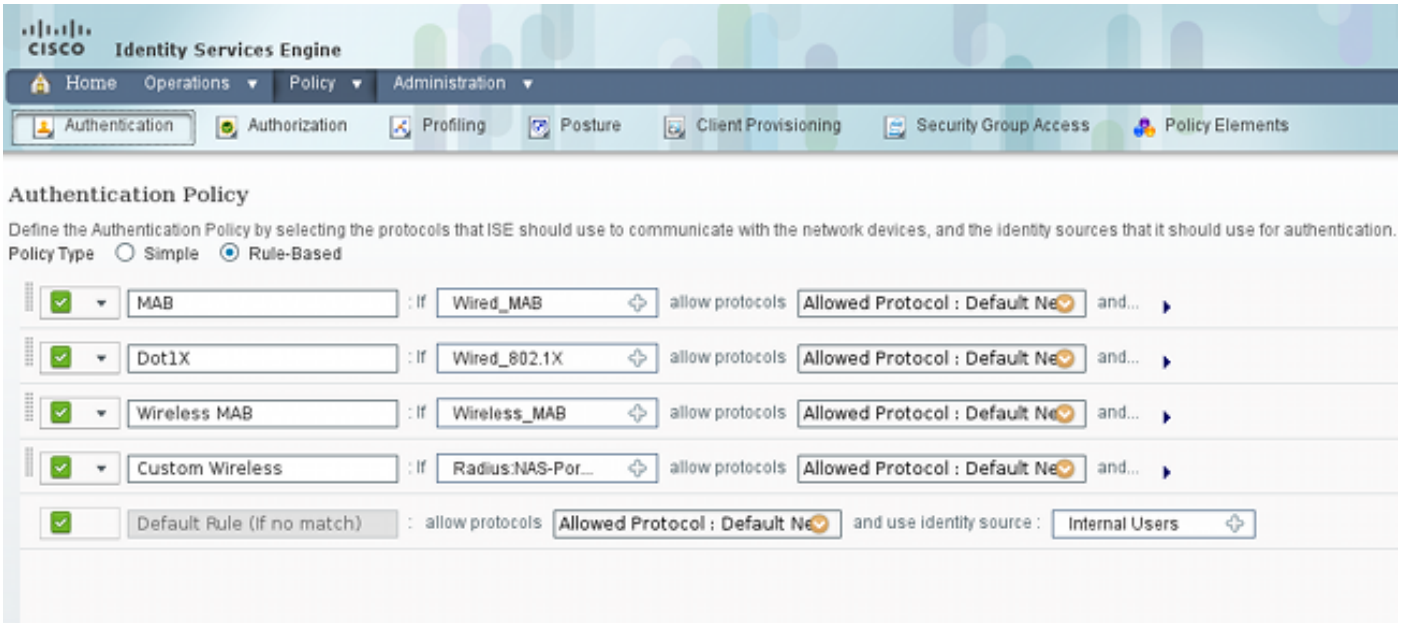



Voor MS Windows XP, die 802.1x-verificatie gebruikt, moet u een gebruikersidentificatie (gebruikersnaam) aanmaken onder **Beheer > Identity Management > Identity > Gebruikers**:

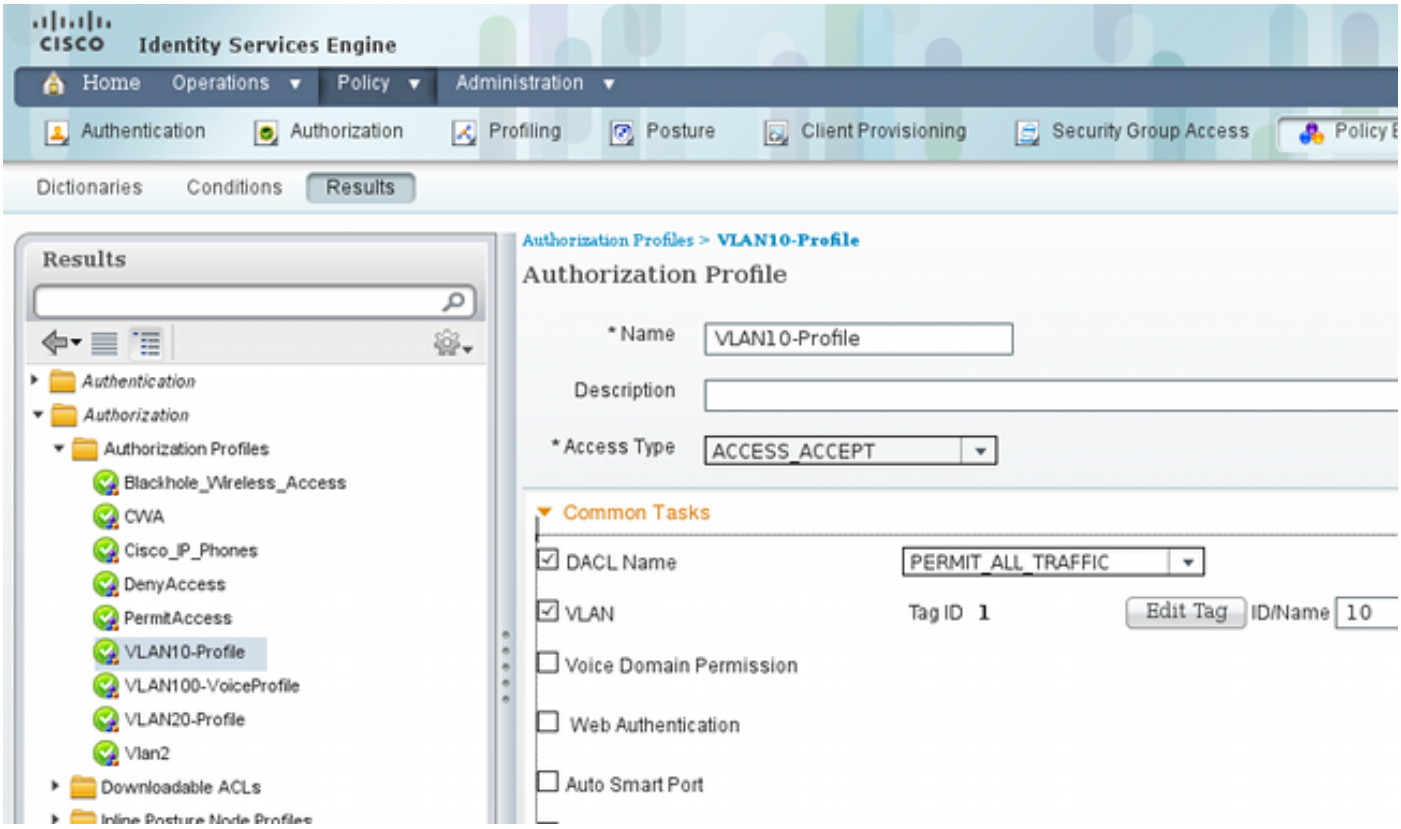



De gebruikersnaam **cisco** wordt gebruikt. Configureer MS Windows XP for Extensible Verification Protocol-Protected EAP (EAP-PEAP) met deze referenties.

Op de ISE wordt het standaard verificatiebeleid gebruikt (wijzig dit niet). Het eerste is het beleid voor MAB-authenticatie, en het tweede is 802.1x:



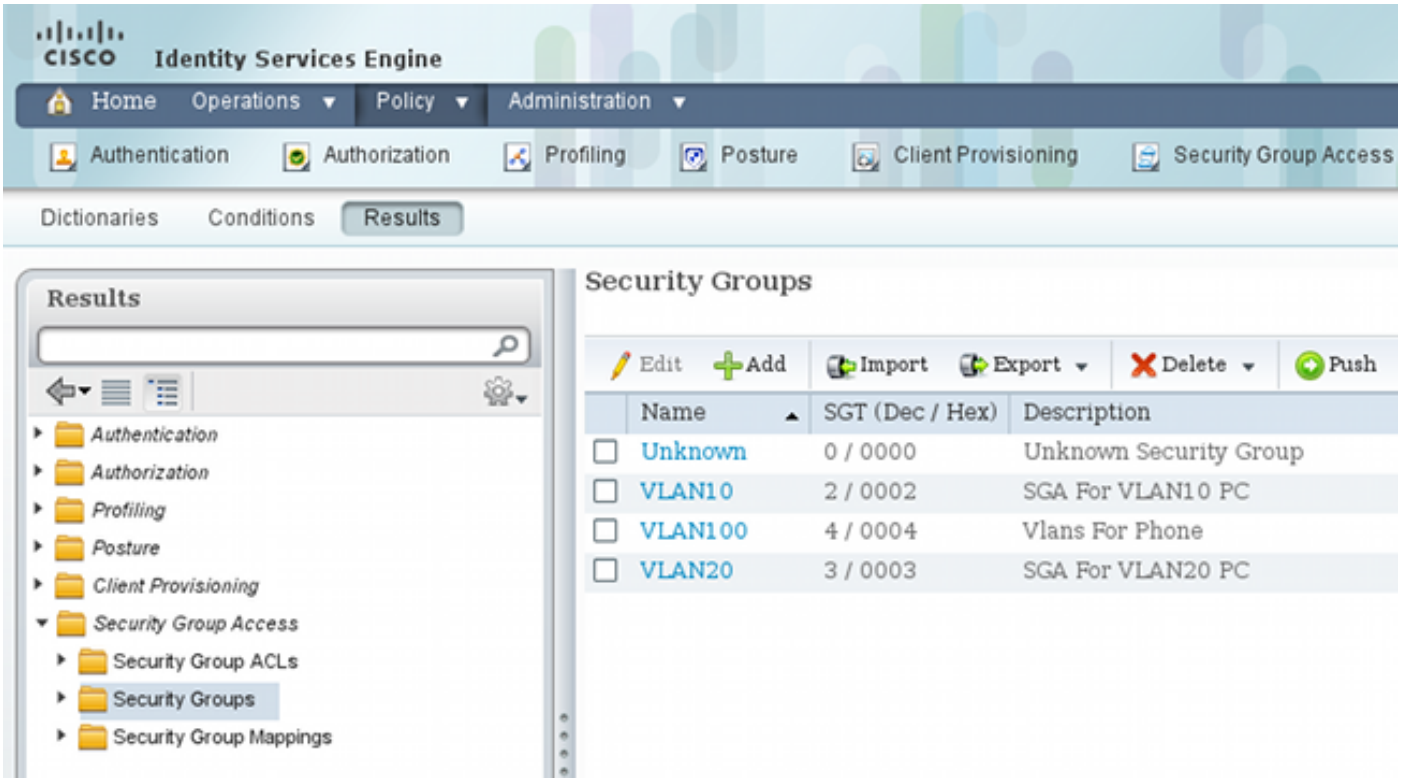

Om het autorisatiebeleid te kunnen configureren moet u autorisatieprofielen definiëren onder **Beleid > Resultaten > Autorisatie > Autorisatieprofielen**. Het VLAN10-Profile with Downloadable ACL (DACL), dat alle verkeer mogelijk maakt, wordt gebruikt voor het MS Windows 7-profiel:



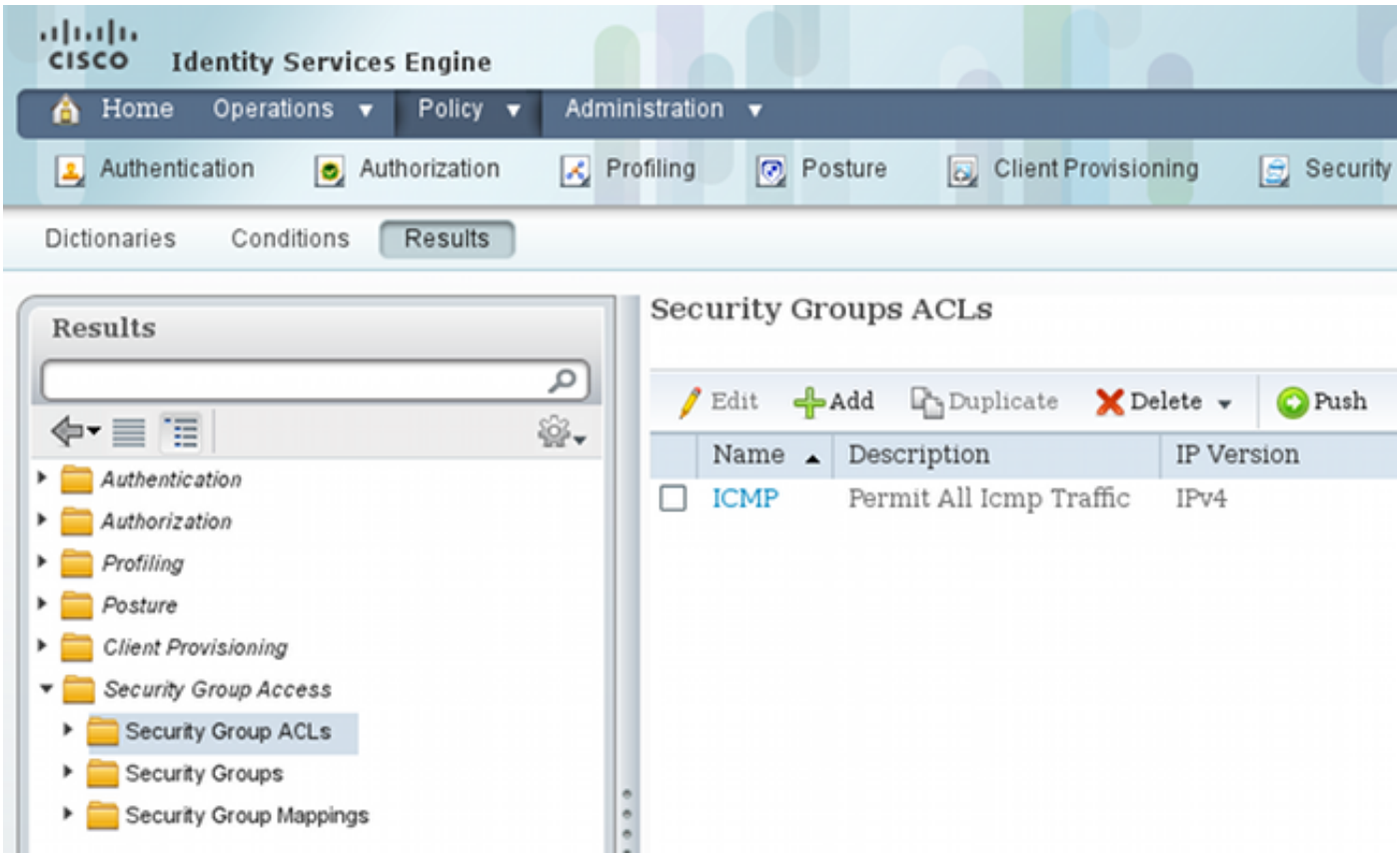

Een vergelijkbare configuratie, VLAN20-Profile, wordt gebruikt voor MS Windows XP, met uitzondering van VLAN-nummer (20).

Om de SGT-groepen (tags) op ISE te configureren, navigeer je naar **Policy > Results > Security Group Access > Security Groups**.

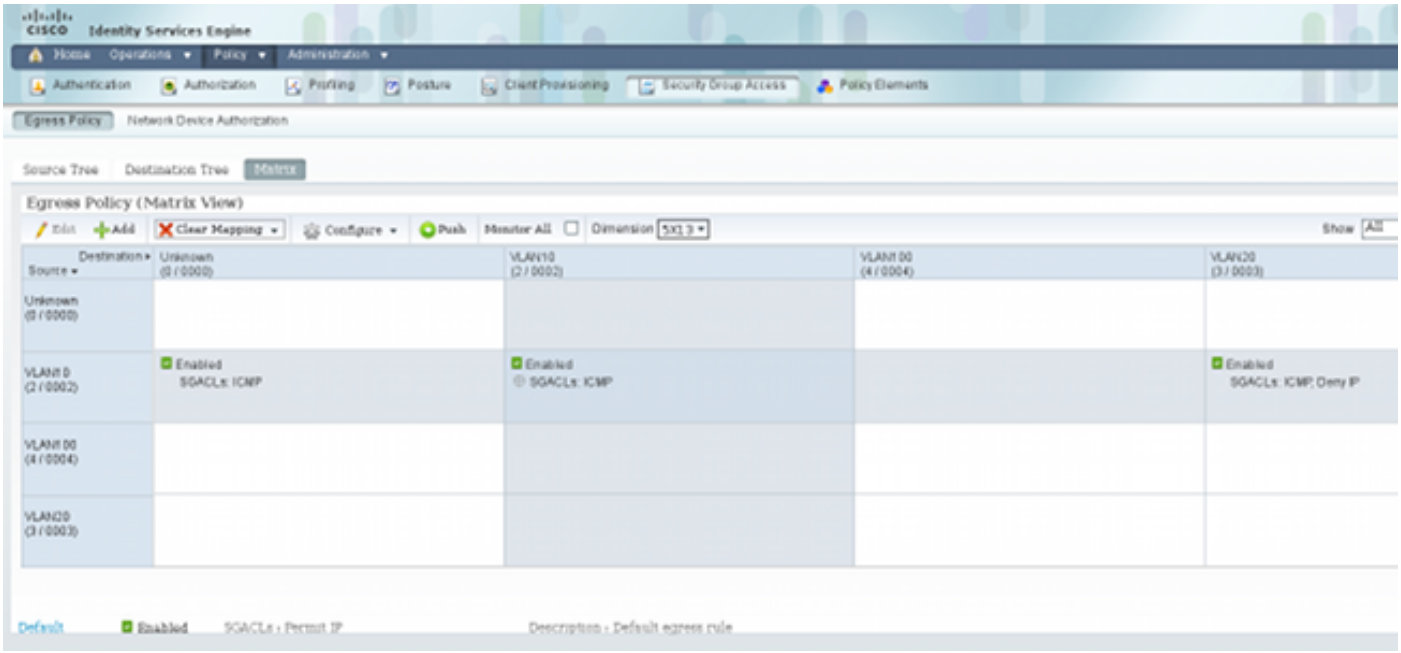
> **Opmerking**: het is niet mogelijk om een tag nummer te kiezen; het wordt automatisch geselecteerd door het eerste vrije nummer behalve 1. U kunt alleen de SGT-naam configureren.



Als u de SGACL wilt maken om ICMP-verkeer (Internet Control Message Protocol) toe te staan, navigeert u naar **Beleid > Resultaten > Toegang tot beveiligingsgroep > ACL's van beveiligingsgroep**:

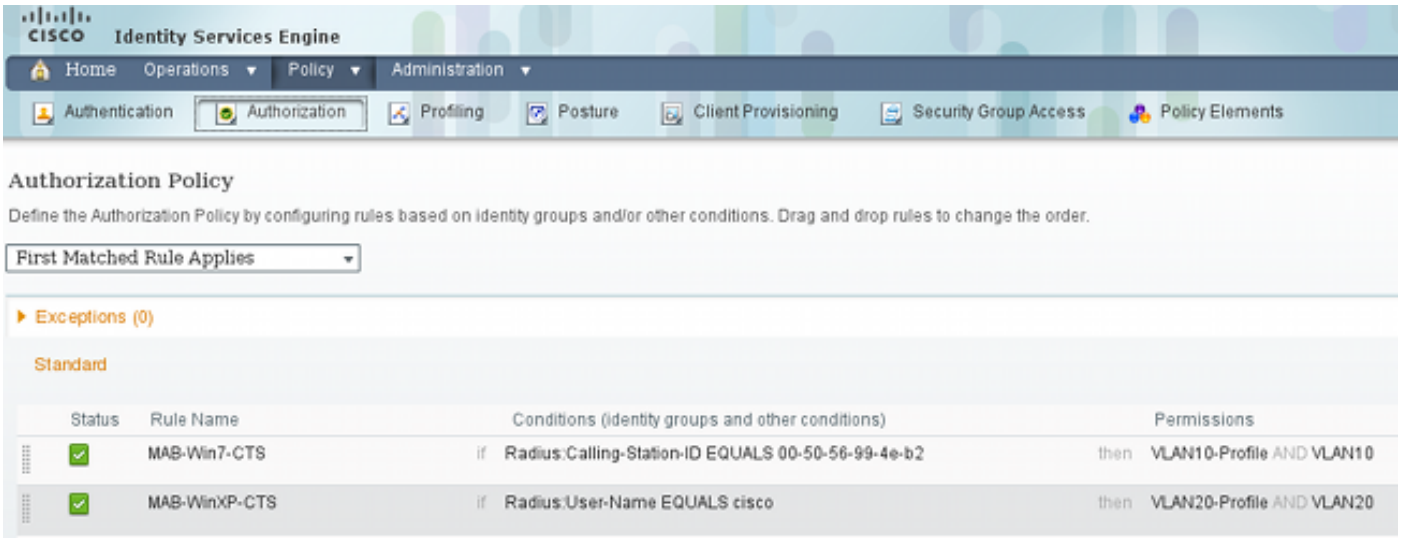



Om beleid te maken, navigeer je naar **Policy > Security Group Access > uitgaande Policy**. Voor verkeer tussen VLAN10 en het onbekende VLAN of VLAN10 of VLAN20, wordt ICMP ACL gebruikt (**vergunning icmp**):




Als u autorisatieregels wilt instellen, bladert u naar **Policy > Authorisation**. Voor MS Windows 7 (specifiek MAC-adres) wordt **VLAN10-profiel** gebruikt, VLAN10 en DACL worden geretourneerd en wordt het beveiligingsprofiel VLAN10 gebruikt met het SGT met de naam **VLAN10**. Voor MS Windows XP (specifieke gebruikersnaam) wordt **VLAN20-profiel** gebruikt, VLAN 20 en DACL

worden geretourneerd en het beveiligingsprofiel VLAN20 met SGT **VLAN20** wordt gebruikt.




Voltooi de switch- en ASA-configuratie zodat deze de SGT RADIUS-kenmerken kunnen accepteren.

### CTS-configuratie op de ASA en de 3750X

U moet basisinstellingen voor CTS configureren. Op de 3750X, moet u aangeven van welke server beleid moet worden gedownload:

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

Voor de ASA is alleen de AAA-server nodig, samen met CTS dat naar die server wijst:

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

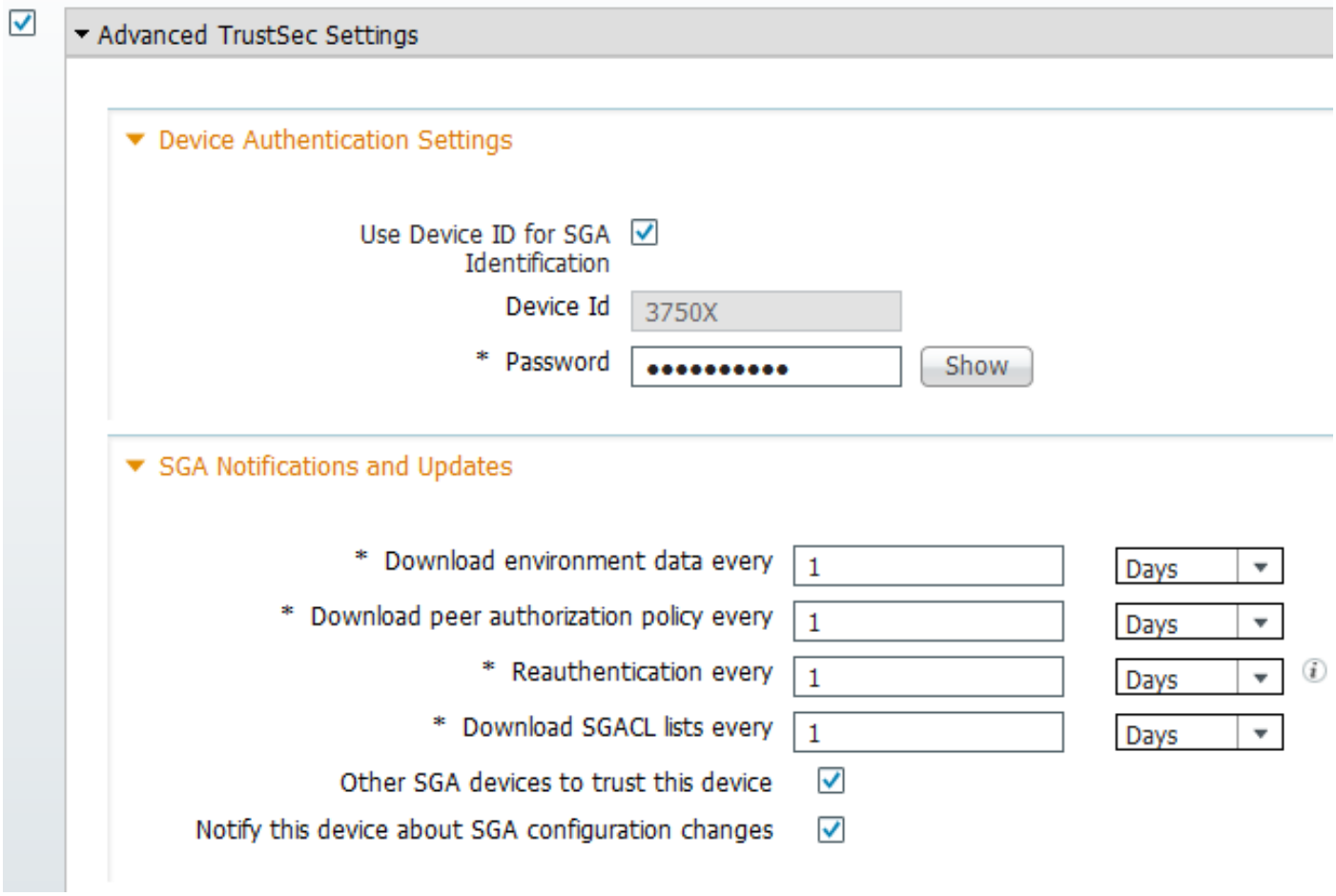
> **Opmerking**: op de 3750X moet u de ISE-server expliciet aanwijzen met de opdracht **radius** van de **groep**. Dit komt doordat de 3750X automatische PAC-levering gebruikt.

### PAC Provisioning op de 3750X (automatisch) en de ASA (handmatig)

Elk apparaat in de CTS cloud moet authenticeren aan de verificatieserver (ISE) om te worden vertrouwd door andere apparaten. Hiervoor wordt gebruik gemaakt van de Extensible Authentication Protocol-Flexible Verification via Secure Protocol (EAP-FAST) methode (RFC 4851). Deze methode vereist dat PAC out-of-band geleverd wordt. Dit proces wordt ook **fase0** genoemd, en wordt niet in een RFC gedefinieerd. PAC voor EAP-FAST heeft een soortgelijke rol als het certificaat voor Extensible Verification Protocol-Transport Layer Security (EAP-TLS). PAC wordt gebruikt om een beveiligde tunnel (fase1) tot stand te brengen, die nodig is voor authenticatie in fase2.

### PAC-provisioning op de 3750X

De 3750X ondersteunt automatische PAC-levering. Op de switch en de ISE wordt een gedeeld wachtwoord gebruikt om PAC te downloaden. Dat wachtwoord en die ID moeten op de ISE worden geconfigureerd onder **Beheer > Netwerkbronnen > Netwerkapparaten**. Selecteer de switch en vouw het gedeelte **Advanced TrustSec Settings uit** om het volgende te configureren:




Om PAC deze referenties te laten gebruiken, voert u deze opdrachten in:

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

## PAC-provisioning op de ASA

De ASA ondersteunt alleen handmatige PAC-provisioning. Dit betekent dat u deze handmatig op de ISE moet genereren (in Network Devices/ASA):


Vervolgens moet het bestand worden geïnstalleerd (bijvoorbeeld met 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
```

## Environment Refresh op de ASA en de 3750X

In deze fase hebben beide apparaten PAC correct geïnstalleerd en starten ze automatisch met het downloaden van de ISE-omgevingsgegevens. Deze gegevens zijn in principe tagnummers en hun namen. Voer deze opdracht in om een omgevingsvernieuwing te starten op de ASA:

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

Om het op ASA te verifiëren (helaas kunt u de specifieke SGT-tags/namen niet zien, maar het wordt later geverifieerd), voert u deze opdracht in:

```
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)
```

Om dit op 3750X te controleren, start u een omgevingsvernieuwing met deze opdracht:

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

Voer deze opdracht in om de resultaten te controleren:

```
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
```

Dit toont aan dat alle tags en bijbehorende namen correct zijn gedownload.

## Poortverificatie - Verificatie en handhaving op de 3750X

Nadat de 3750X de omgevingsgegevens heeft, moet u verifiëren dat de SGT's worden toegepast op geverifieerde sessies.

Voer deze opdracht in om te controleren of MS Windows 7 correct is geverifieerd:

```
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
```

De output toont aan dat **VLAN10** samen met **SGT 0002** en DACL wordt gebruikt die voor al verkeer toestaan.

Voer deze opdracht in om te controleren of MS Windows XP correct is geverifieerd:

```
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
```

De output toont aan dat **VLAN 20** samen met **SGT 0003** en DACL wordt gebruikt die voor al verkeer toestaan

IP-adressen worden gedetecteerd met de functionaliteit voor het **traceren** van **IP-apparaten**. De DHCP-switch moet worden geconfigureerd voor **DHCP-snooping**. Na het snuffelen van DHCP-respons leert het vervolgens het IP-adres van de client. Voor een statisch geconfigureerd IP-adres (zoals in dit voorbeeld) wordt de **arp-spionagefunctionaliteit** gebruikt en moet een pc elk pakket verzenden zodat de switch zijn IP-adres kan detecteren.

Voor **apparaattracering** is mogelijk een verborgen opdracht nodig om deze op poorten te activeren:

```
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
```

## Beleidsvernieuwing voor de 3750X

De 3750X (in tegenstelling tot de ASA) kan beleid downloaden van de ISE. Alvorens het downloadt en een beleid afdwingt, moet u het met deze bevelen toelaten:

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

Als u het niet toelaat, wordt het beleid gedownload, maar niet geïnstalleerd en niet gebruikt voor handhaving.

Voer deze opdracht in om een beleidsvernieuwing te starten:

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

Om te verifiëren dat het beleid van ISE wordt gedownload, ga dit bevel in:

```
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
```

De output toont aan dat slechts het noodzakelijke deel van het beleid wordt gedownload.

In de CTS cloud bevat het pakket het SGT van de bronhost en **wordt de afdwinging uitgevoerd op het doelapparaat**. Dit betekent dat het pakket van de bron naar het laatste apparaat wordt doorgestuurd, dat rechtstreeks met de doelhost is verbonden. Dat apparaat is het punt van handhaving, omdat het de SGTs van zijn direct-aangesloten hosts kent, en weet of het inkomende pakket met een bron SGT moet worden toegestaan of geweigerd voor de specifieke bestemming SGT.

Dit besluit is gebaseerd op beleid dat van de ISE is gedownload.

In dit scenario, worden alle beleid gedownload. Als u echter de MS Windows XP-verificatiesessie (SGT=VLAN20) leeg maakt, hoeft de switch geen beleid (rij) te downloaden dat overeenkomt met VLAN20, omdat er geen apparaten meer zijn van dat SGT die zijn aangesloten op de switch.

In het gedeelte Advanced (Problemen oplossen) wordt uitgelegd hoe de 3750X bepaalt welk beleid moet worden gedownload na een onderzoek van het pakketniveau.

## SXP Exchange (de ASA als Luidspreker en de 3750X als Luidspreker)

ASA ondersteunt SGT niet. Alle frames met SGT worden door de ASA verwijderd. Dat is de reden dat de 3750X geen SGT-gelabelde frames naar de ASA kan sturen. In plaats daarvan wordt SXP gebruikt. Dankzij dit protocol kan de ASA informatie van de switch ontvangen over het in kaart brengen van de IP-adressen en SGT. Met die informatie kan de ASA IP-adressen aan SGT's toewijzen en een beslissing nemen op basis van SGACL.

Typ de volgende opdrachten om de 3750X als luidspreker te kunnen configureren:

```
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
```

Voer deze opdrachten in om de ASA als luisteraar te configureren:

```
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
```

Om te verifiëren dat ASA de toewijzingen heeft ontvangen, voert u deze opdracht in:

```
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
```

Nu, wanneer ASA het inkomende pakket met het bronIP adres **192.168.1.200** ontvangt, kan het het behandelen alsof het uit **SGT=2** komt. Voor het IP-bronadres **192.168.200.2** kan het worden behandeld alsof het afkomstig is van **SGT=3**. Hetzelfde geldt voor het IP-adres van de bestemming.

> **Opmerking**: de 3750X moet het IP-adres van de gekoppelde host kennen. Dit gebeurt door het volgen van IP-apparaten. Voor een statisch geconfigureerd IP-adres op de eindhost moet de switch elk pakket na verificatie ontvangen. Hierdoor wordt het IP-apparaat gevolgd om het IP-adres te vinden, wat een SXP-update teweegbrengt. Wanneer alleen de SGT bekend is, wordt deze niet verzonden via SXP.

## Traffic filtering op ASA met SGT ACL

Hier is een controle van de ASA configuratie:

```
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
```

Er wordt een ACL gemaakt die op de interne interface wordt toegepast. Het staat voor al ICMP verkeer van **SGT=3** aan **SGT=2** (genoemd **VLAN10**) toe:

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

> **Opmerking**: u kunt het tagnummer of de tagnaam gebruiken.

Als u vanuit MS Windows XP pingt met een IP-bronadres van **192.168.2.200** (**SGT=3**) naar MS Windows 7 met een IP-adres van **192.168.1.200** (**SGT=2**), bouwt de ASA een verbinding:

```
%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)
```

Wanneer u hetzelfde probeert met Telnet, wordt het verkeer geblokkeerd:

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

Er zijn meer configuratieopties op de ASA. Het is mogelijk om zowel een beveiligingstag als een IP-adres te gebruiken voor zowel de bron als de bestemming. Deze regel staat ICMP-echoverkeer toe van **SGT-tag = 3** en IP-adres **192.168.2.200** naar de SGT-tag **VLAN10** en het adres van de bestemmingshost **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
```

Dit kan ook worden bereikt met doelgroepen:

```
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 op de 3750X met beleid gedownload van de ISE (RBACL)

Het is ook mogelijk om lokaal beleid op de switch te bepalen. In dit voorbeeld worden echter de beleidsmaatregelen gepresenteerd die van de ISE zijn gedownload. In de ASA gedefinieerde beleidsregels mogen in één regel zowel IP-adressen als SGT's (en de gebruikersnaam uit Active Directory) gebruiken. Het beleid dat op de switch wordt bepaald (zowel lokaal als van de ISE) staat alleen SGT's toe. Als u IP-adressen in uw regels moet gebruiken, wordt filtering op de ASA aanbevolen.

ICMP-verkeer tussen MS Windows XP en MS Windows 7 wordt getest. Hiervoor moet u de standaardgateway van de ASA wijzigen in de 3750X op MS Windows. De 3750X heeft routeringsinterfaces en kan de pakketten routeren:

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

Het beleid is al gedownload van de ISE. Voer deze opdracht in om deze te controleren:

```
 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
```

Het verkeer van VLAN10 (MS Windows 7) naar VLAN20 (MS WindowsXP) wordt onderworpen aan ICMP-20 ACL, die van ISE wordt gedownload:

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

Om ACL te verifiëren, ga dit bevel in:

```
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
```

Om de SGT-toewijzing te verifiëren om ervoor te zorgen dat het verkeer vanaf beide hosts correct is gelabeld, voert u deze opdracht in:

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

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

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

ICMP van MS Windows 7 (**SGT=2**) naar MS Windows XP (**SGT=3**) werkt prima met ACL ICMP-20. Dit wordt gecontroleerd door tellers te controleren op verkeer van **2** tot **3** (15 toegestane pakketten):

```
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
```

Nadat u hebt geprobeerd de teller Telnet te gebruiken, worden de geweigerde pakketten verhoogd (dit is niet toegestaan op ICMP-20 ACL):

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

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

*       *       0               0               133281          132969

2       3       0               2               0               15
```

**Opmerking**: het sterteken (*) dat in het uitvoerdocument wordt getoond, heeft betrekking op al het verkeer dat niet is gelabeld (die kolom en rij worden in Matrix op de ISE **onbekend** genoemd en gebruiken tag nummer **0**).

Wanneer u een ACL-ingang met het logboeksleutelwoord (gedefinieerd op de ISE) hebt, worden de bijbehorende pakketdetails en de ondernomen acties zoals in elke ACL met het logboeksleutelwoord vastgelegd.

# Verifiëren

Raadpleeg de afzonderlijke configuratiesecties voor de verificatieprocedures.

# Problemen oplossen

## PAC-provisioning

Er kunnen problemen optreden bij het gebruik van automatische PAC-provisioning. Vergeet niet het **pakketsleutelwoord** te gebruiken voor de RADIUS-server. Automatische PAC-levering op de 3750X gebruikt de EAP-FAST-methode met het Extensible Verification Protocol met interne methode met behulp van Microsoft's Challenge Handshake Verification Protocol (EAP-MSCHAPv2)-verificatie. Wanneer u debug, ziet u meerdere RADIUS-berichten die het deel zijn van EAP-FAST-onderhandeling die wordt gebruikt om de beveiligde tunnel te bouwen, die EAP-MSCHAPv2 gebruikt met de geconfigureerde ID en het wachtwoord voor verificatie.

Het eerste RADIUS-verzoek maakt gebruik van AAA**-service-type=cts-pac-provisioning** om de ISE ervan op de hoogte te stellen dat dit een PAC-verzoek is.

```
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.
```

De **RADIUS-afwijzing** aan het einde van de uitvoer wordt verwacht omdat u al PAC hebt ontvangen en niet hebt gevolgd met een verder verificatieproces.

Vergeet niet dat PAC vereist is voor alle andere communicatie met de ISE. Maar als u het niet hebt, probeert de switch nog steeds een omgeving of beleid verversen wanneer het is geconfigureerd. Vervolgens wordt er geen **cts-opaqueue** (PAC) bevestigd in de RADIUS-aanvragen, waardoor de fouten worden veroorzaakt.

Als uw PAC-toets onjuist is, wordt deze foutmelding op de ISE weergegeven:

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

U ziet deze uitvoer ook van debugs (**debug cts provisioning + debug radius**) op de switch als uw PAC-toets verkeerd is:

```
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
```

Als u de moderne conventie voor **radiusservers** gebruikt, wordt het volgende weergegeven:

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

> **Opmerking**: u moet hetzelfde wachtwoord gebruiken op de ISE dat u hebt gebruikt in de **instellingen voor apparaatverificatie**.

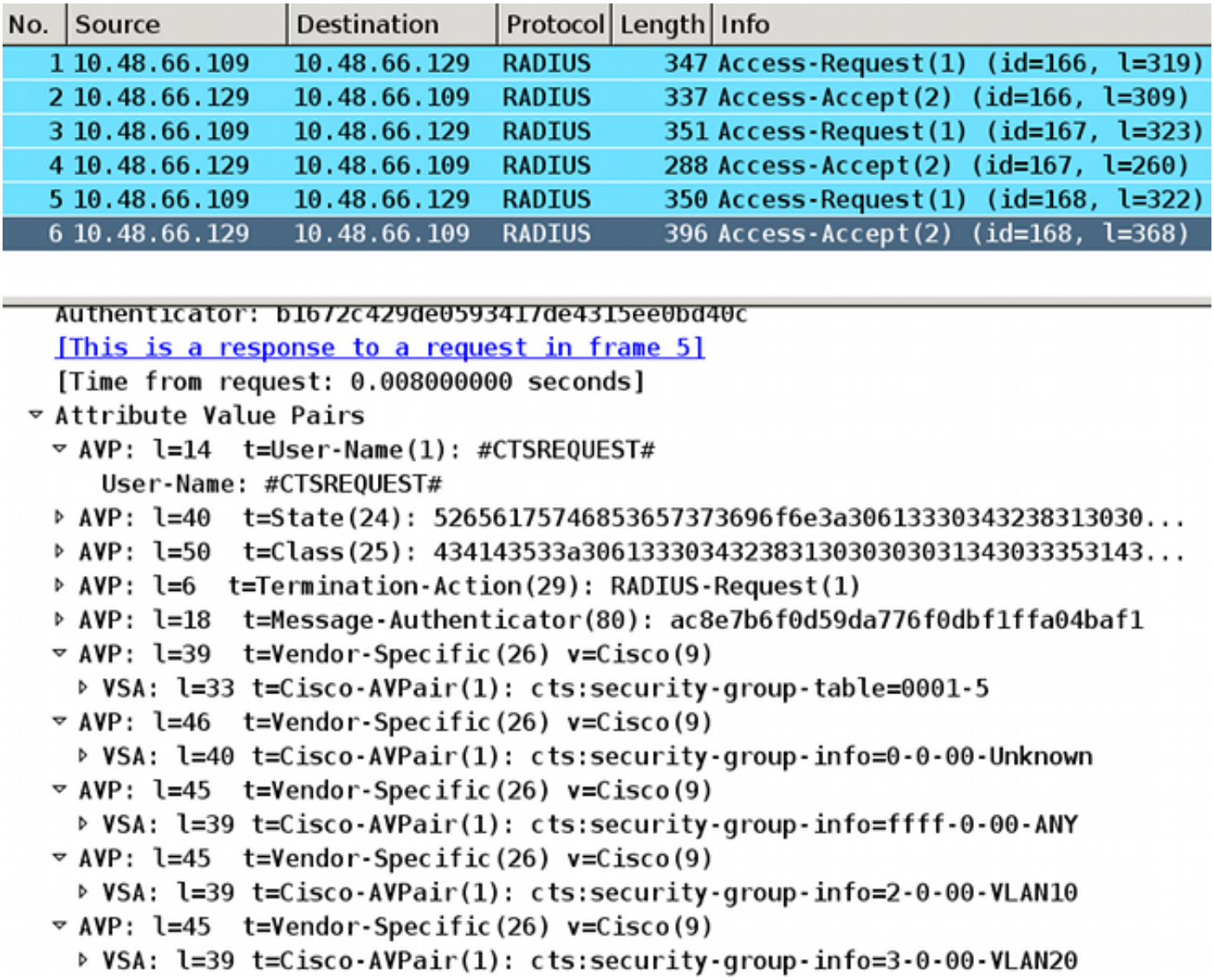
Na succesvolle PAC-levering wordt dit weergegeven op de ISE:

| 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) |

## Milieu verversen

De omgeving verfrissen wordt gebruikt om basisgegevens te verkrijgen van de ISE, die het SGT-nummer en de naam bevat. Het pakketniveau toont aan dat het slechts drie RADIUS-verzoeken en antwoorden met kenmerken is.

Voor het eerste verzoek krijgt de switch de naam **CTSServerlist**. Voor de tweede krijgt hij de gegevens van die lijst en voor de laatste krijgt hij alle SGT's met tags en namen:

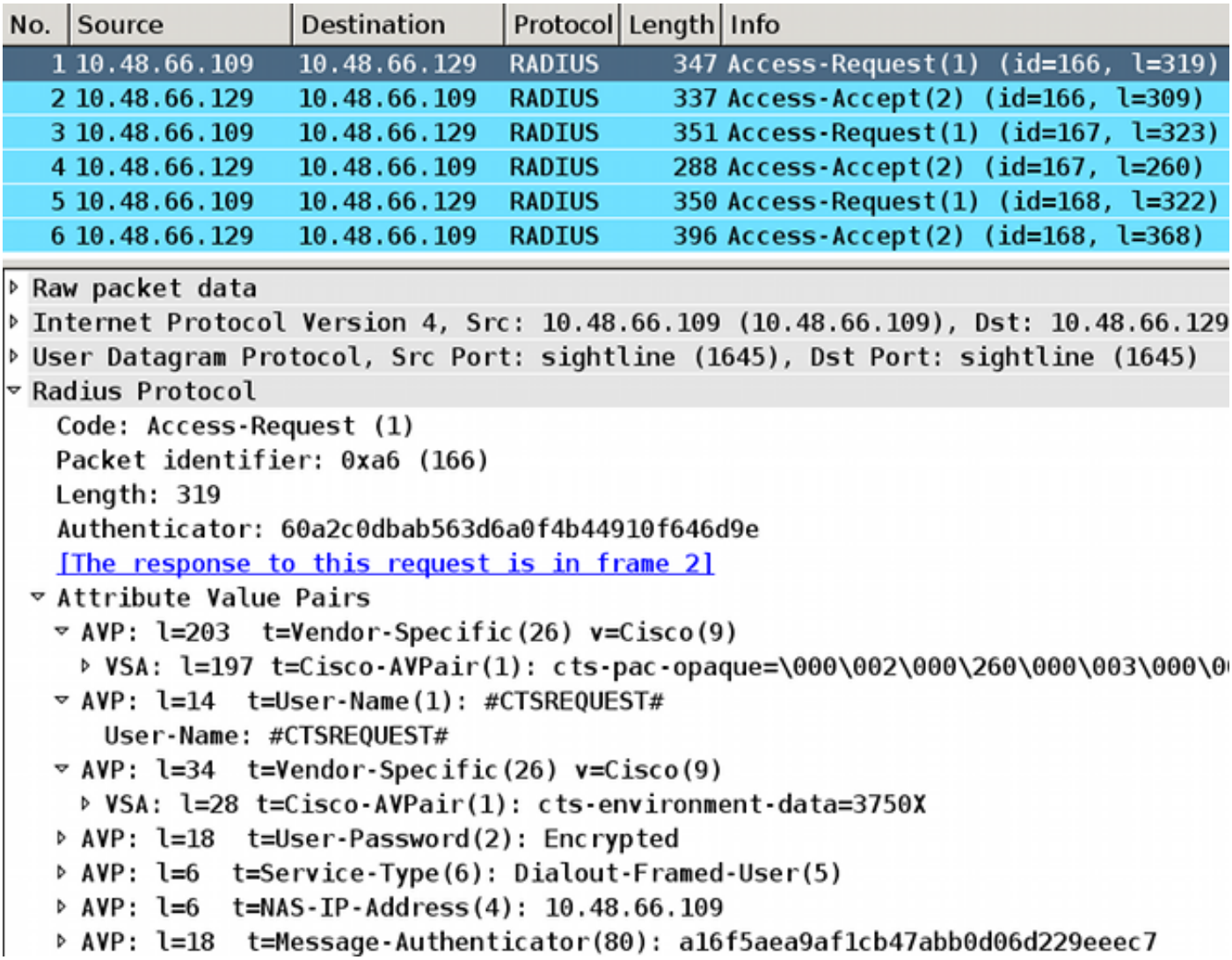


| No. | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|
| 1 | 10.48.66.109 | 10.48.66.129 | RADIUS | 347 | Access-Request(1) (id=166, l=319) |
| 2 | 10.48.66.129 | 10.48.66.109 | RADIUS | 337 | Access-Accept(2) (id=166, l=309) |
| 3 | 10.48.66.109 | 10.48.66.129 | RADIUS | 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) |



Hier ziet u de standaard **SGT 0**, **ffff**, en ook twee op maat gedefinieerde: SGT-tag 2 heet **VLAN10** en SGT-tag 3 heet **VLAN20**.

> **Opmerking**: alle RADIUS-verzoeken bevatten **cts-pac-opaque** als resultaat van PAC-levering.



| 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) |



Op de 3750X moet u debugs zien voor alle drie RADIUS-reacties en de bijbehorende lijsten, lijstdetails en de specifieke SGT-inside-lijst:

```
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)
```

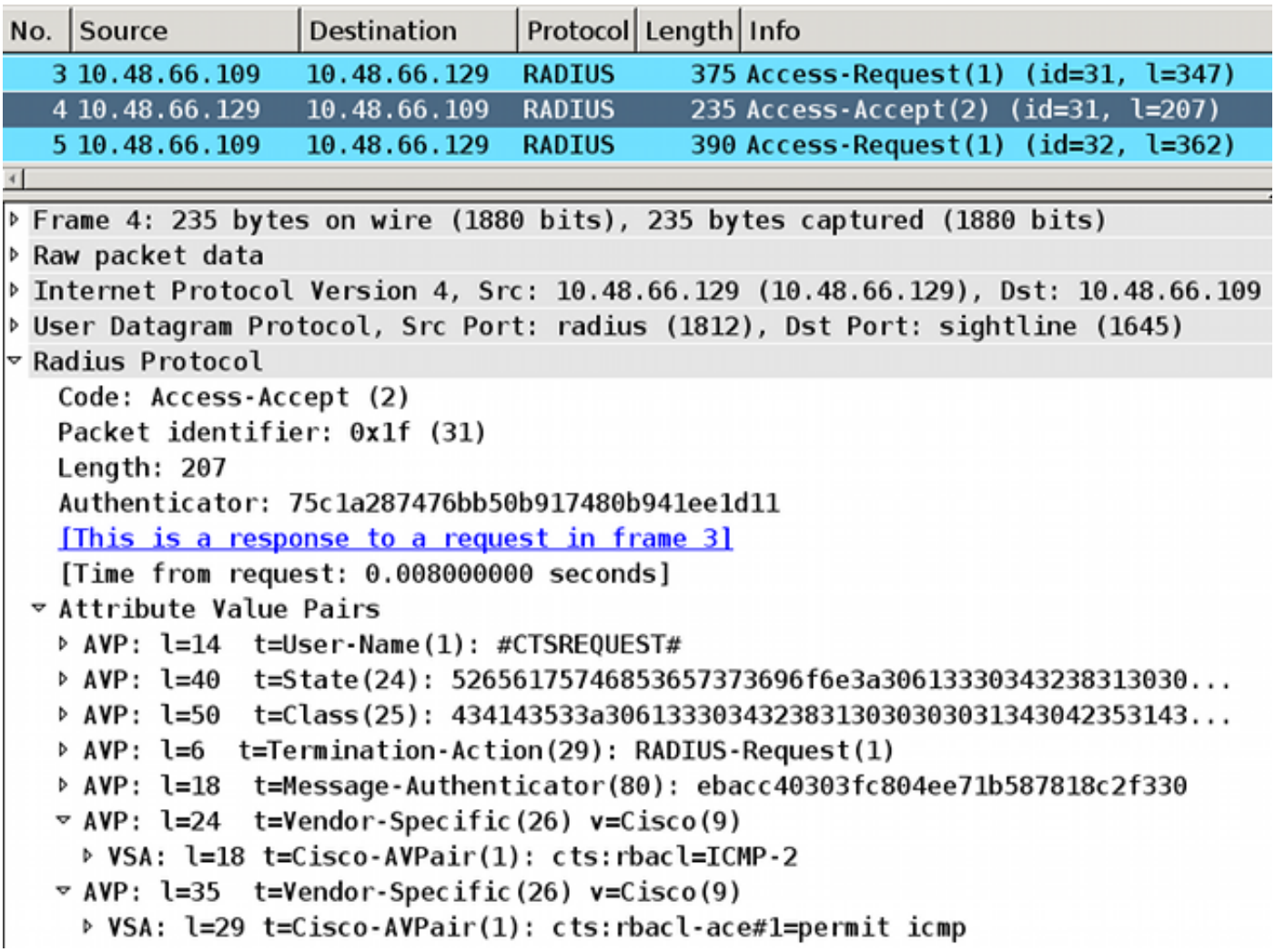
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: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

## Beleidsvernieuwing

Het vernieuwen van het beleid wordt alleen op de switch ondersteund. Het is vergelijkbaar met de omgeving verfrissen. Dit zijn gewoon RADIUS-aanvragen en -acceptaties.

De switch vraagt om alle ACL's in de standaardlijst. Vervolgens wordt voor elke ACL die niet up-to-date is (of niet bestaat) een ander verzoek verzonden om de gegevens te verkrijgen.

Hier is een voorbeeldreactie wanneer u om ICMP-20 ACL vraagt:




Herinner dat u **cts op rol-gebaseerde handhaving** moet hebben gevormd om dat ACL af te dwingen.

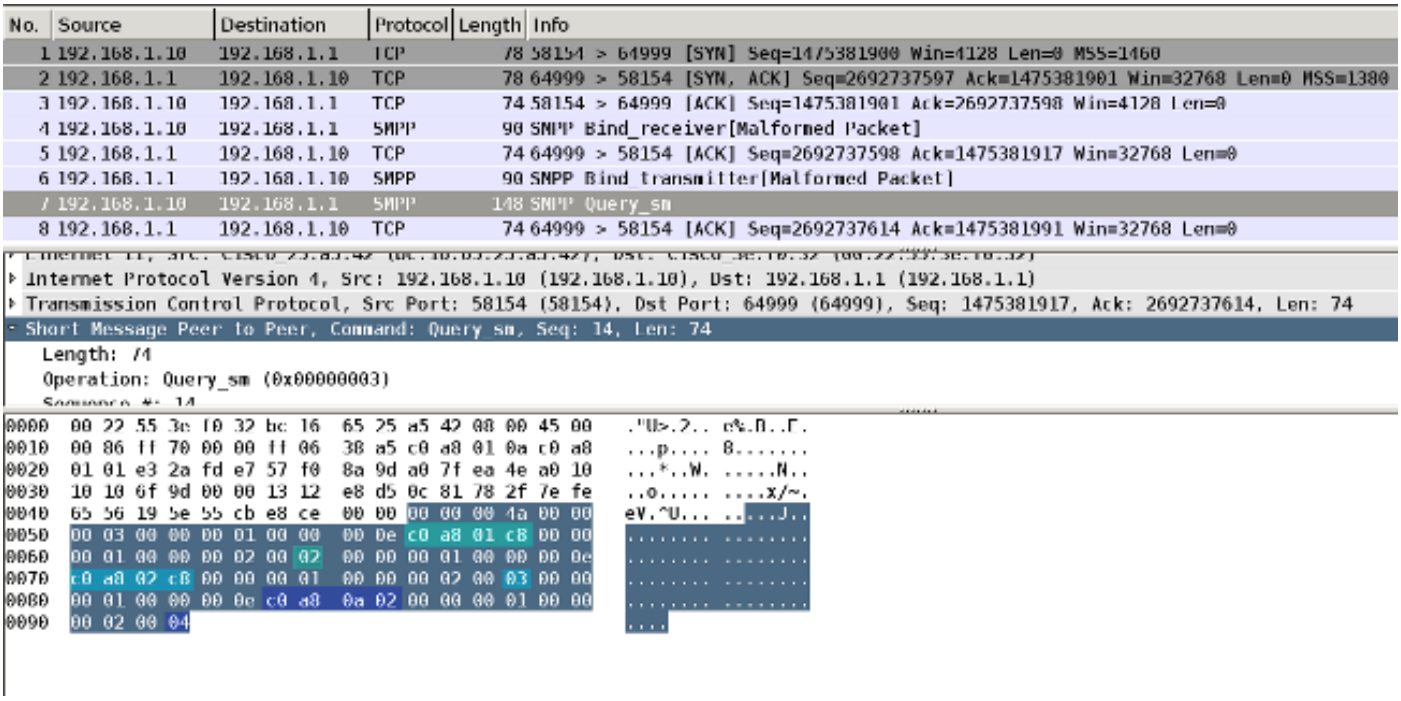
Debugs geven aan of er wijzigingen zijn (gebaseerd op gen ID). Als dit het geval is, kunt u het oude beleid desgewenst verwijderen en een nieuw beleid installeren. Dit omvat ASIC-programmering (hardwareondersteuning).

```
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

De SXP-update wordt geactiveerd door de IP-apparaattraceringscode die het IP-adres van het apparaat vindt. Vervolgens wordt het SMPP-protocol (Short Message Peer-to-Peer) gebruikt om de updates te verzenden. Het maakt gebruik van **TCP-optie 19** voor verificatie, wat hetzelfde is als BGP (border gateway protocol). De SMPP-payload is niet versleuteld. Wireshark heeft geen goede decoder voor de SMPP payload, maar het is gemakkelijk om gegevens in het te vinden:




- De eerste, **c0 a8 01 c8**, is **192.168.1.200** en heeft **tag 2**.
- De tweede, **c0 a8 02 c8**, is **192.168.2.200** en heeft **tag 3**.
- De derde, **c0 a8 0a 02,** is **192.168.10.2** en heeft **tag 4** (deze werd gebruikt om te testen telefoon **SGT=4**)

Hier zijn enkele debugs op de 3750X nadat het IP-apparaat volgen het IP-adres van MS Windows 7 vindt:

```
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
```

Hier zijn de overeenkomstige debugs op de 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.
```

Om meer debugs op ASA te zien, kunt u het debugging breedbandniveau inschakelen:

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

## SGACL op de ASA

Nadat de ASA de SGT-toewijzingen correct heeft geïnstalleerd die door SXP zijn ontvangen, moeten de beveiligingsgroepen ACL goed werken. Wanneer u problemen ondervindt met de toewijzing, voert u het volgende in:

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

De ACL met de beveiligingsgroep werkt precies hetzelfde als bij het IP-adres of de gebruikersidentiteit. De logboeken onthullen problemen, en de nauwkeurige ingang van ACL die werd geraakt.

Hier is een ping van MS Windows XP naar MS Windows 7 die aantoont dat de pakkettracer correct werkt:

```
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>
```

# Gerelateerde informatie

- Cisco TrustSec-configuratiehandleiding voor 3750
- Cisco TrustSec-configuratiehandleiding voor ASA 9.1
- Cisco TrustSec-implementatie en routekaart
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.