Ejemplo de configuración TrustSec de ASA y el Switch Catalyst Serie 3750X y guía de solución de problemas

Contenido

Introducción

En este artículo se describe cómo configurar Cisco TrustSec (CTS) en Cisco Secure Adaptive Security Appliance (ASA) y un switch Catalyst de Cisco serie 3750X (3750X).

Para aprender la correspondencia entre las etiquetas de grupos de seguridad (SGT) y las direcciones IP, ASA utiliza el SGT Exchange Protocol (SXP). A continuación, se utilizan listas de

control de acceso (ACL) basadas en SGT para filtrar el tráfico. El 3750X descarga políticas de lista de control de acceso basado en roles (RBACL) de Cisco Identity Services Engine (ISE) y filtra el tráfico en función de ellas. Este artículo detalla el nivel de paquete para describir cómo funciona la comunicación y las depuraciones esperadas.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Componentes de CTS
- Configuración CLI de ASA y Cisco IOS®

Componentes Utilizados

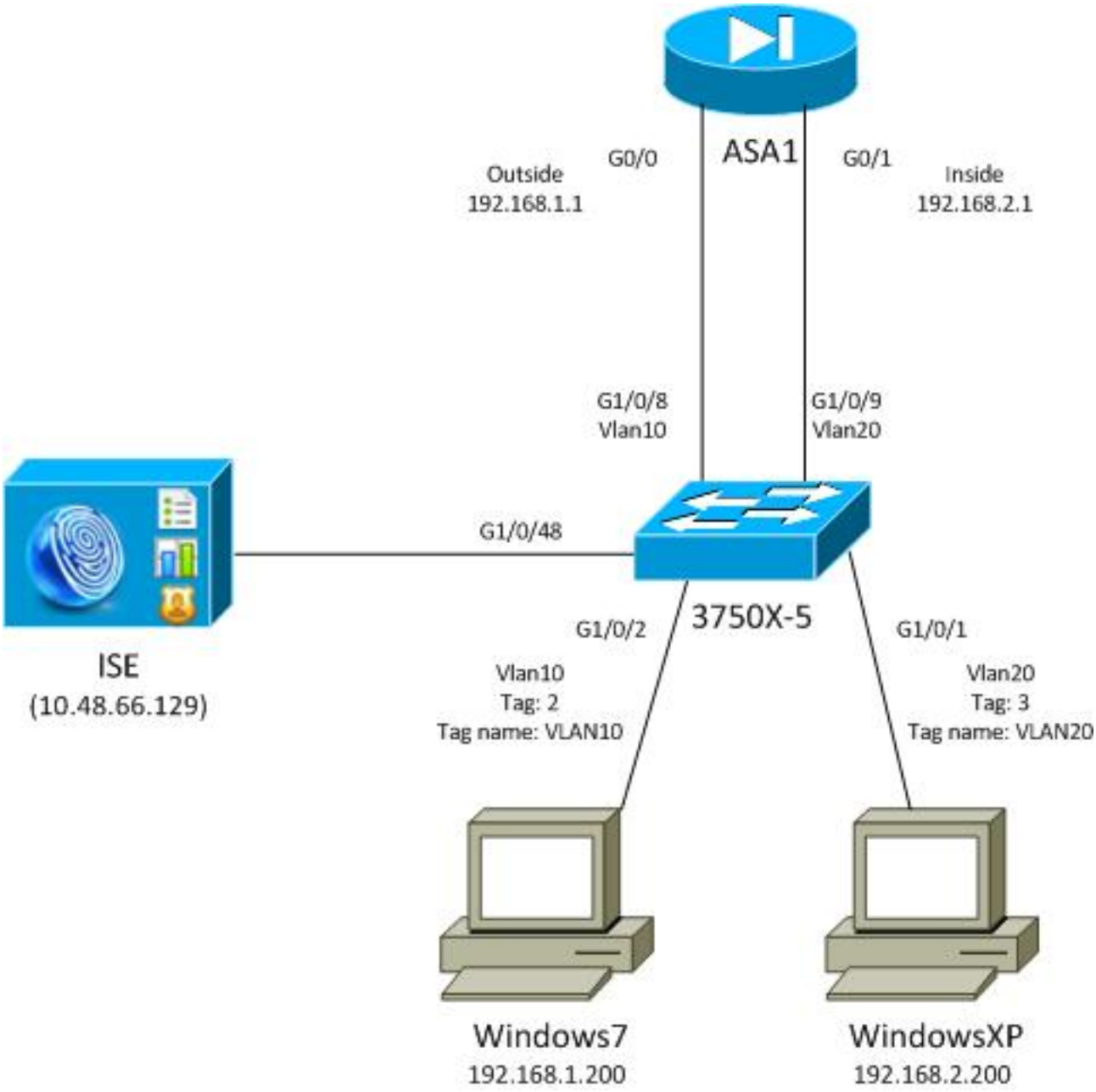
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco ASA, versiones 9.1 y posteriores
- Microsoft (MS) Windows 7 y MS Windows XP
- Software Cisco 3750X, versiones 15.0 y posteriores
- Software Cisco ISE, versiones 1.1.4 y posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de la red



Flujo de tráfico

Este es el flujo de tráfico:

- El 3750X está configurado en **G1/0/1** y **G1/0/2** para la autenticación de puertos.
- ISE se utiliza como servidor de autenticación, autorización y contabilidad (AAA).
- La omisión de direcciones MAC (MAB) se utiliza para la autenticación de MS Windows 7.
- IEEE 802.1x se utiliza para MS Windows XP para demostrar que no importa qué método de autenticación se utiliza.

Después de una autenticación correcta, ISE devuelve la SGT y el 3750X enlaza esa etiqueta a la sesión de autenticación. El switch también aprende las direcciones IP de ambas estaciones con el comando **ip device tracking**. A continuación, el switch utiliza SXP para enviar la tabla de mapeo entre la SGT y la dirección IP al ASA. Ambos PC con MS Windows tienen un ruteo predeterminado que apunta al ASA.

Una vez que ASA recibe el tráfico de la dirección IP asignada a la SGT, puede utilizar la ACL basada en la SGT. Además, cuando utiliza 3750X como router (gateway predeterminado para

ambas estaciones de MS Windows), puede filtrar el tráfico según las políticas descargadas desde ISE.

Estos son los pasos para la configuración y verificación, cada uno de los cuales se detalla en su propia sección más adelante en el documento:

- Autenticación de puerto con el comando **ip device tracking** en el 3750X
- Configuración de ISE para políticas de autenticación, SGT y lista de control de acceso de grupos de seguridad (SGACL)
- Configuración de CTS en ASA y el 3750X
- Aprovisionamiento de credenciales de acceso protegido (PAC) en el 3750X (automático) y el ASA (manual)
- Actualización del entorno en ASA y el 3750X
- Verificación y aplicación de la autenticación de puertos en el 3750X
- Actualización de políticas en el 3750X
- SXP Exchange (ASA como receptor y 3750X como altavoz)
- Filtrado de tráfico en ASA con ACL SGT
- Filtrado de tráfico en el 3750X con políticas descargadas desde ISE

Configuraciones

Autenticación de puerto con el comando *ip device tracking* en el 3750X

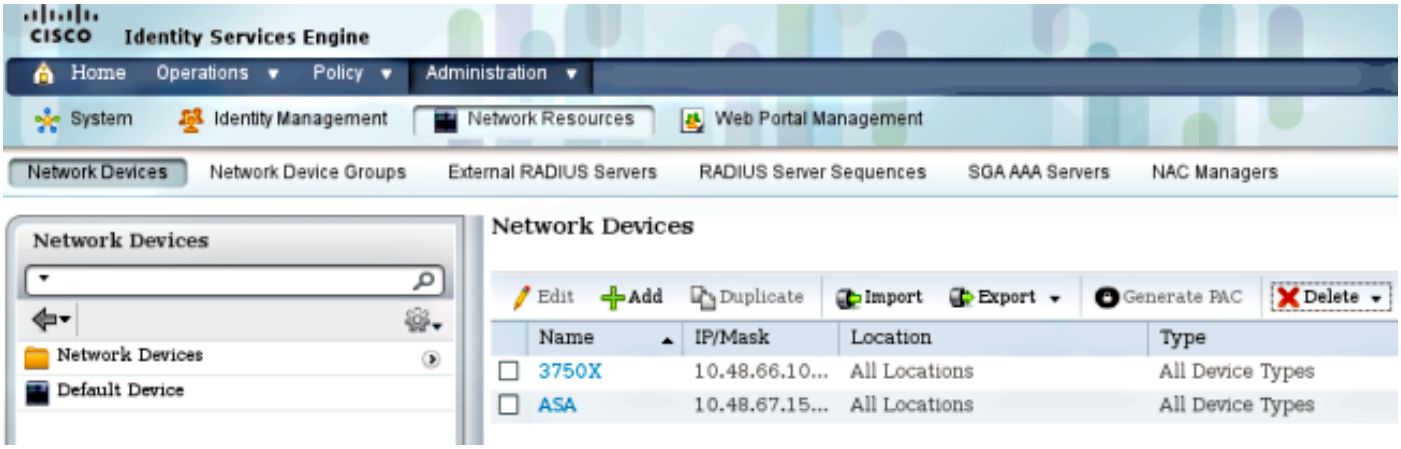
Esta es la configuración típica para 802.1x o MAB. El cambio de autorización (CoA) RADIUS solo es necesario cuando se utiliza una notificación activa de ISE.

```
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
```

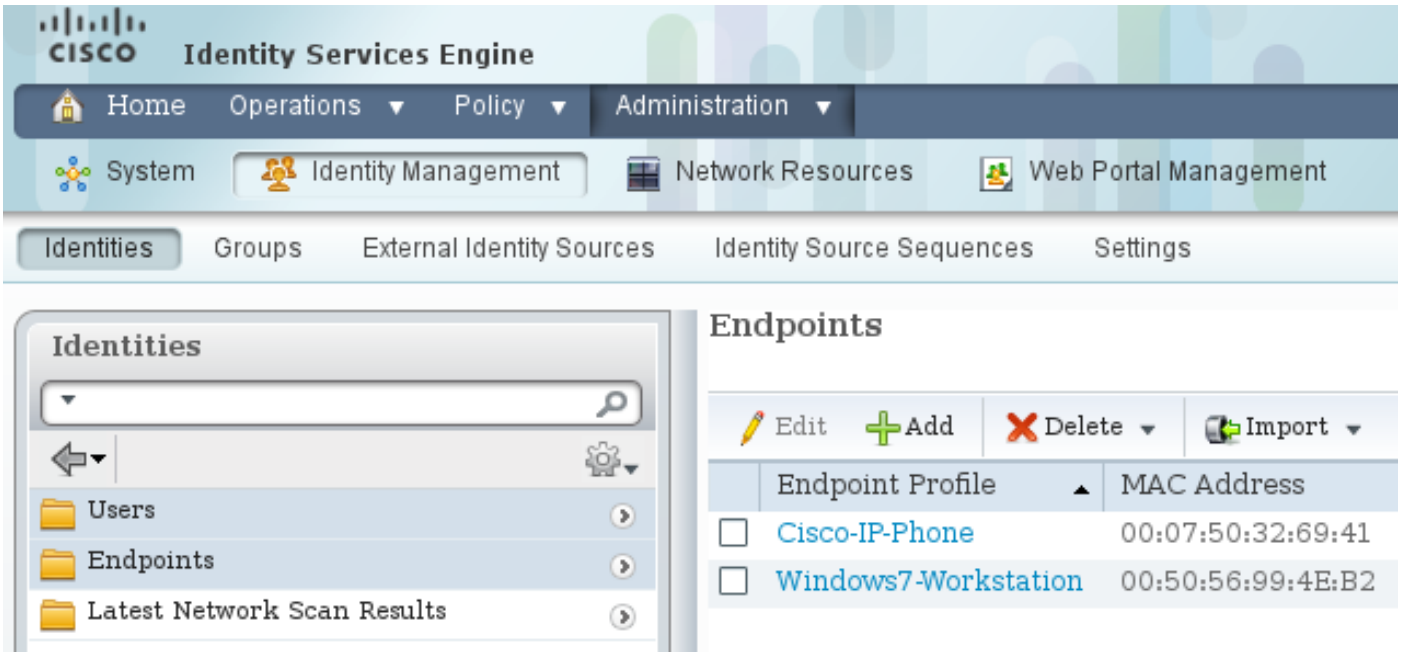
```
 mab
 dot1x pae authenticator
spanning-tree portfast

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
```

Configuración de ISE para políticas de autenticación, SGT y SGACL

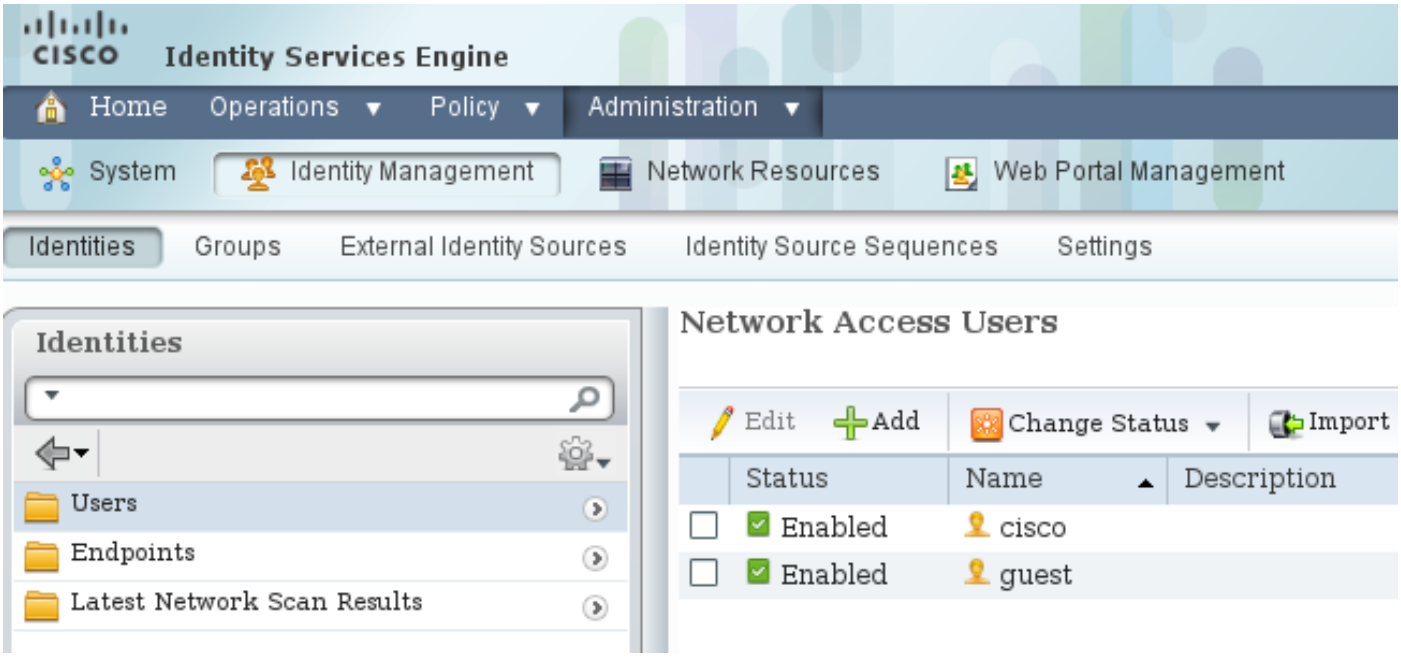
ISE debe tener ambos dispositivos de red configurados en **Administration > Network Devices**:



Para MS Windows 7, que utiliza la autenticación MAB, debe crear la identidad del terminal (dirección MAC) en **Administration > Identity Management > Identities > Endpoints**:

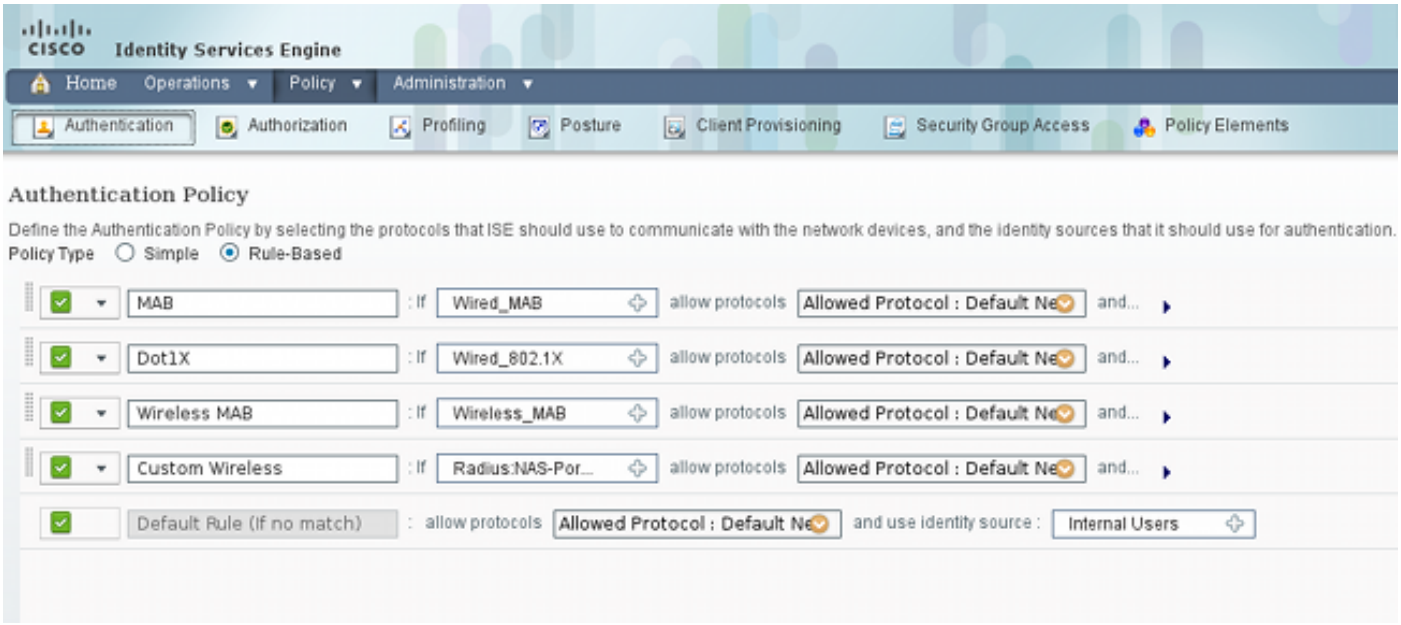


Para MS Windows XP, que utiliza autenticación 802.1x, debe crear una identidad de usuario (nombre de usuario) en **Administration > Identity Management > Identities > Users**:

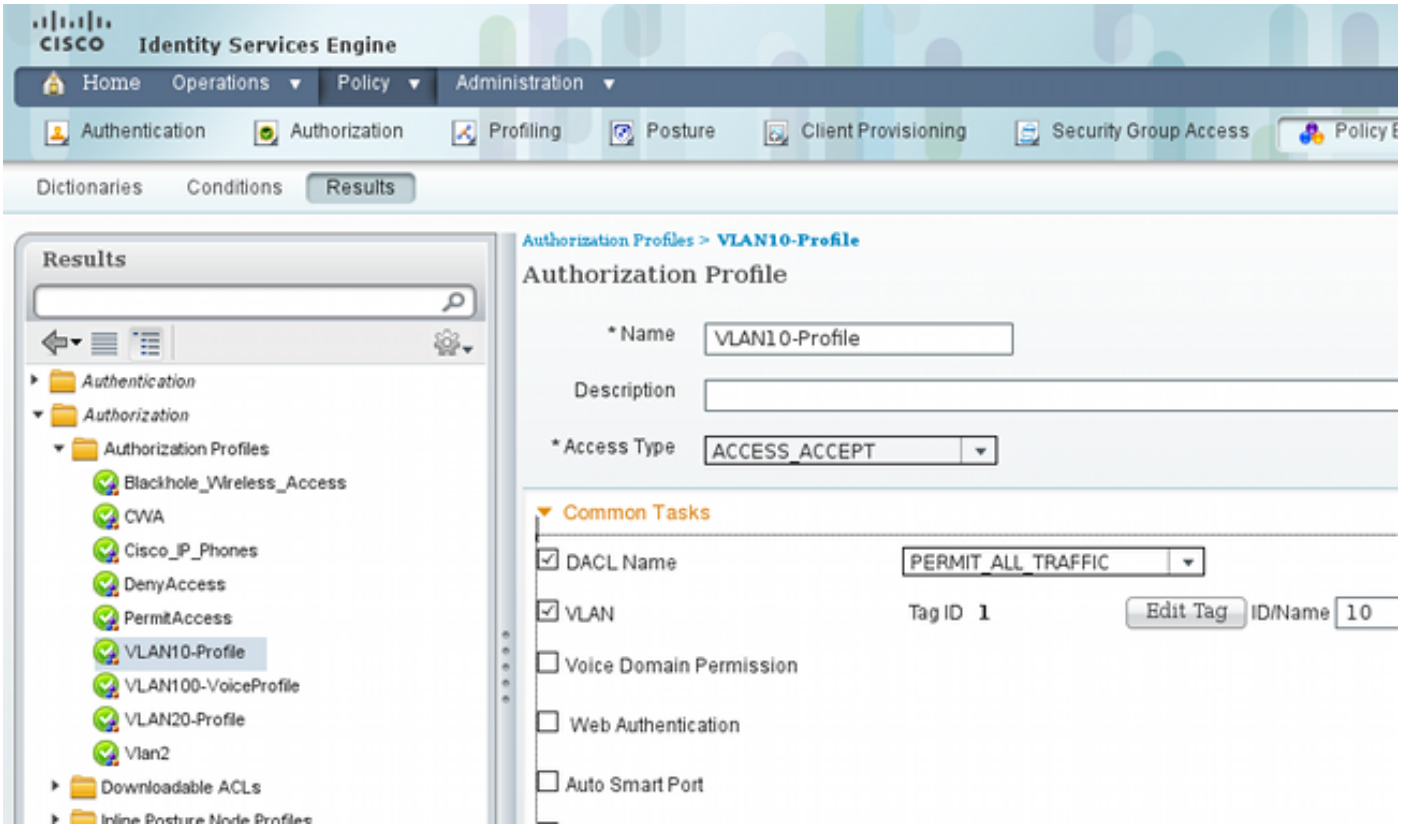


Se utiliza el nombre de usuario **cisco**. Configure MS Windows XP para EAP protegido por protocolo de autenticación extensible (EAP-PEAP) con estas credenciales.

En ISE, se utilizan las políticas de autenticación predeterminadas (no lo cambie). La primera es la política para la autenticación MAB y la segunda es 802.1x:



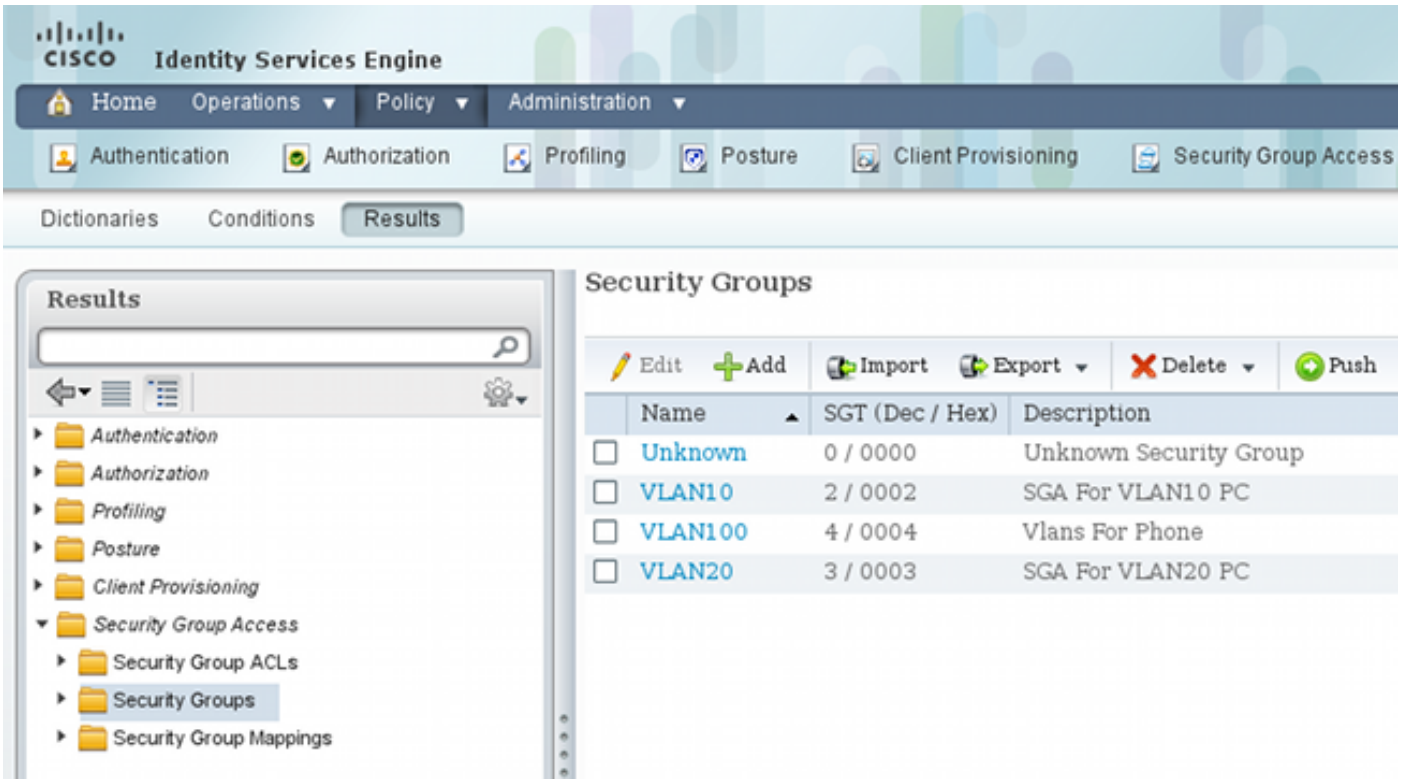
Para configurar políticas de autorización, debe definir perfiles de autorización en **Política > Resultados > Autorización > Perfiles de autorización**. El perfil de VLAN10 con ACL descargable (DACL), que permite todo el tráfico, se utiliza para el perfil de MS Windows 7:



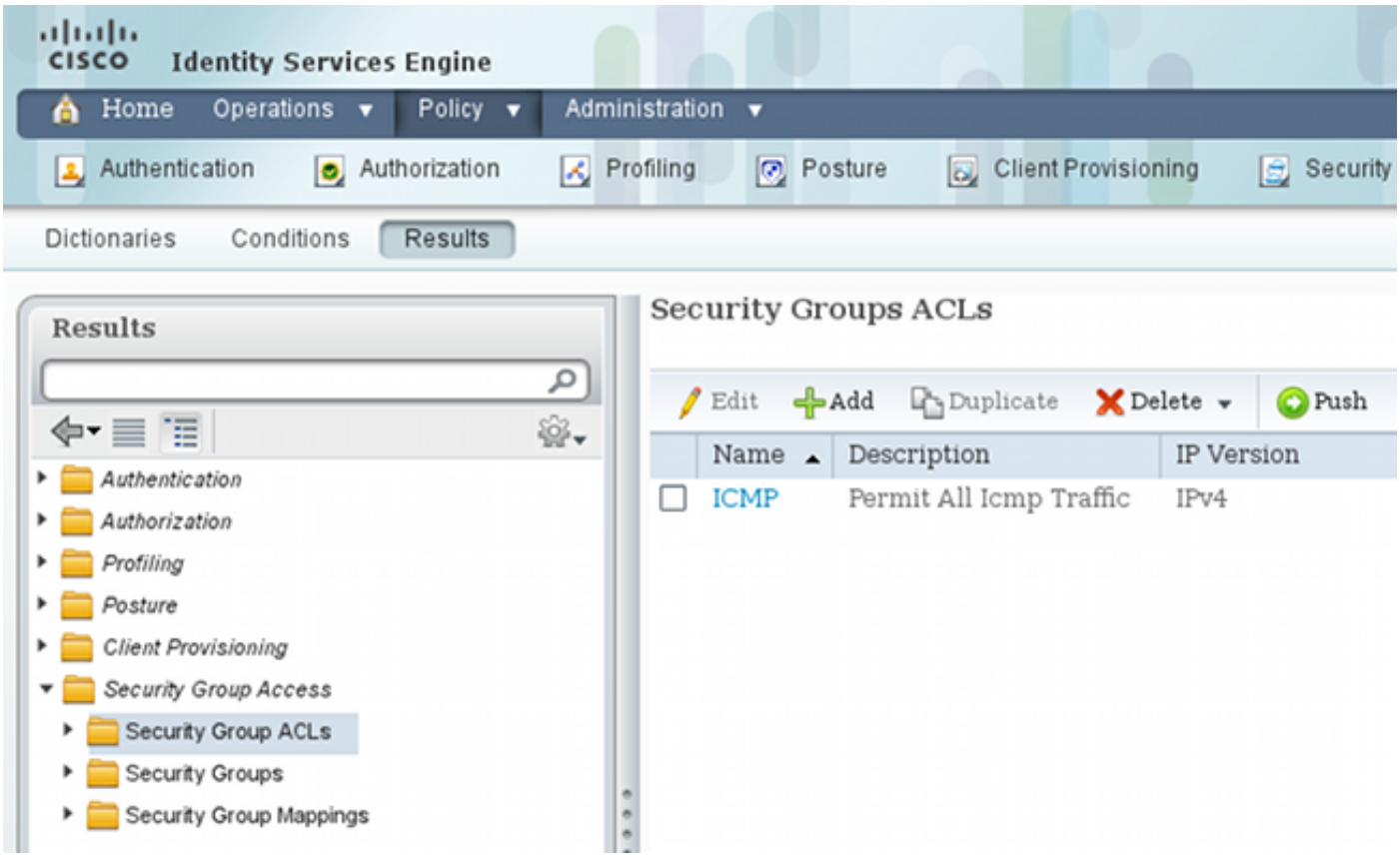
Una configuración similar, VLAN20-Profile, se utiliza para MS Windows XP con la excepción del número de VLAN (20).

Para configurar los grupos SGT (etiquetas) en ISE, navegue hasta **Política > Resultados > Acceso de grupo de seguridad > Grupos de seguridad**.

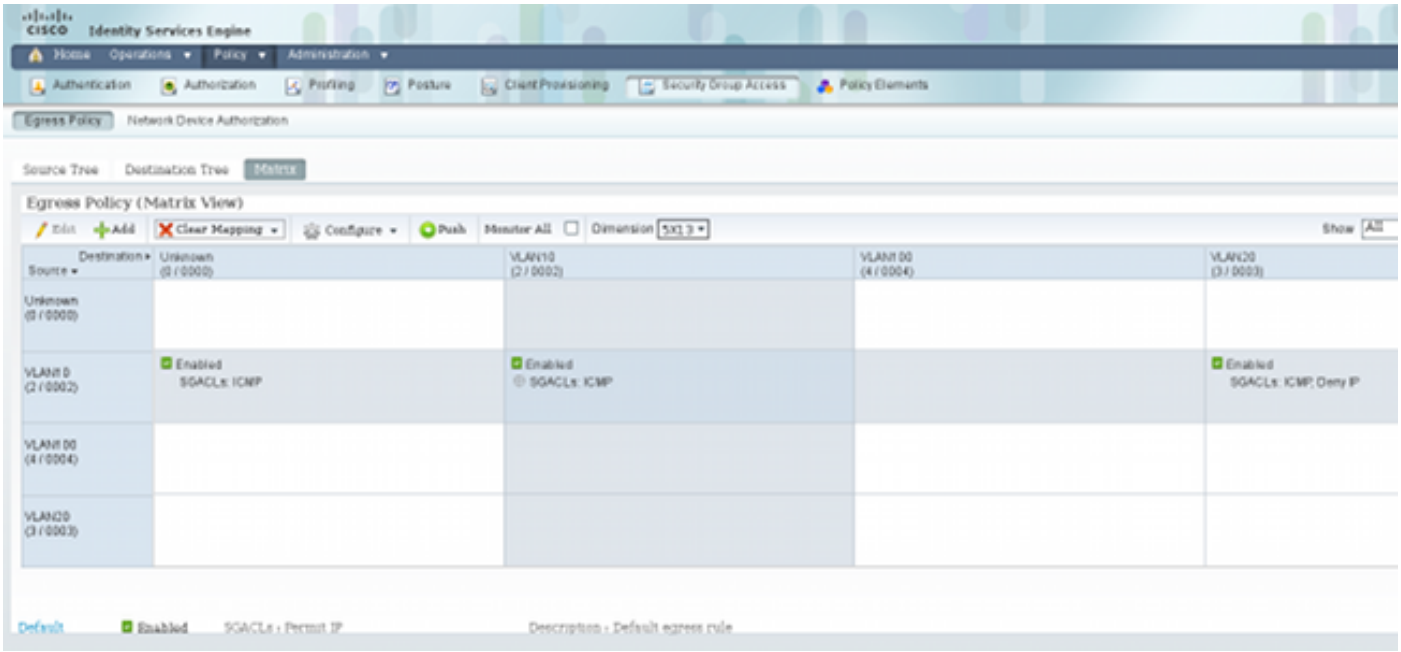
> **Nota**: No es posible elegir un número de etiqueta; se selecciona automáticamente por el primer número libre excepto 1. Sólo puede configurar el nombre de SGT.



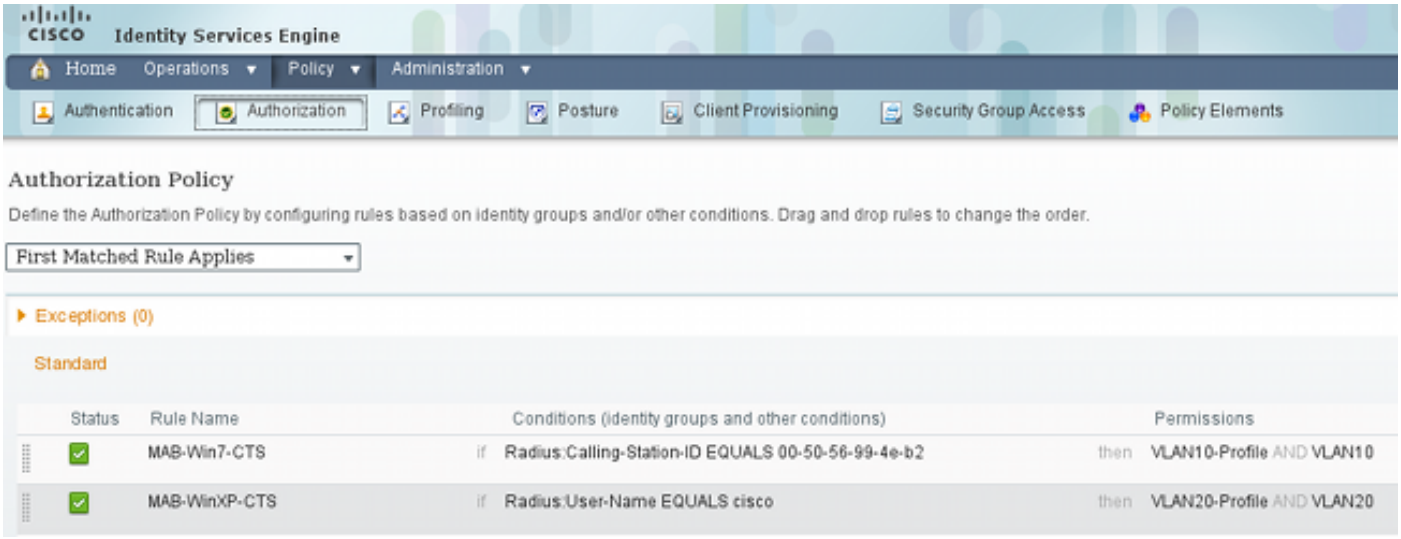
Para crear el SGACL para permitir el tráfico ICMP (Internet Control Message Protocol), navegue hasta **Policy > Results > Security Group Access > Security Group ACLs**:



Para crear políticas, navegue hasta **Política > Security Group Access > Egress Policy**. Para el tráfico entre VLAN10 y la VLAN desconocida o VLAN10 o VLAN20, se utiliza la ACL ICMP (**permit icmp**):



Para establecer reglas de autorización, navegue hasta **Policy > Authorization**. Para MS Windows 7 (dirección MAC específica), se utiliza **VLAN10-Profile**, que devuelve VLAN10 y DACL, y el perfil de seguridad VLAN10 con la SGT denominada **VLAN10**. Para MS Windows XP (nombre de usuario específico), se utiliza **VLAN20-Profile**, que devuelve VLAN 20 y DACL, y el perfil de seguridad VLAN20 con la SGT denominada **VLAN20**.



Finalice el switch y la configuración ASA para que acepten los atributos RADIUS de SGT.

Configuración de CTS en el ASA y el 3750X

Debe configurar los parámetros CTS básicos. En el 3750X, debe indicar desde qué políticas de servidor se deben descargar:

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

En ASA, solo se necesita el servidor AAA junto con CTS que apunte a ese servidor:

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

> **Nota**: En el 3750X, debe señalar explícitamente al servidor ISE con el comando **group radius**. Esto se debe a que el 3750X utiliza el aprovisionamiento automático de PAC.

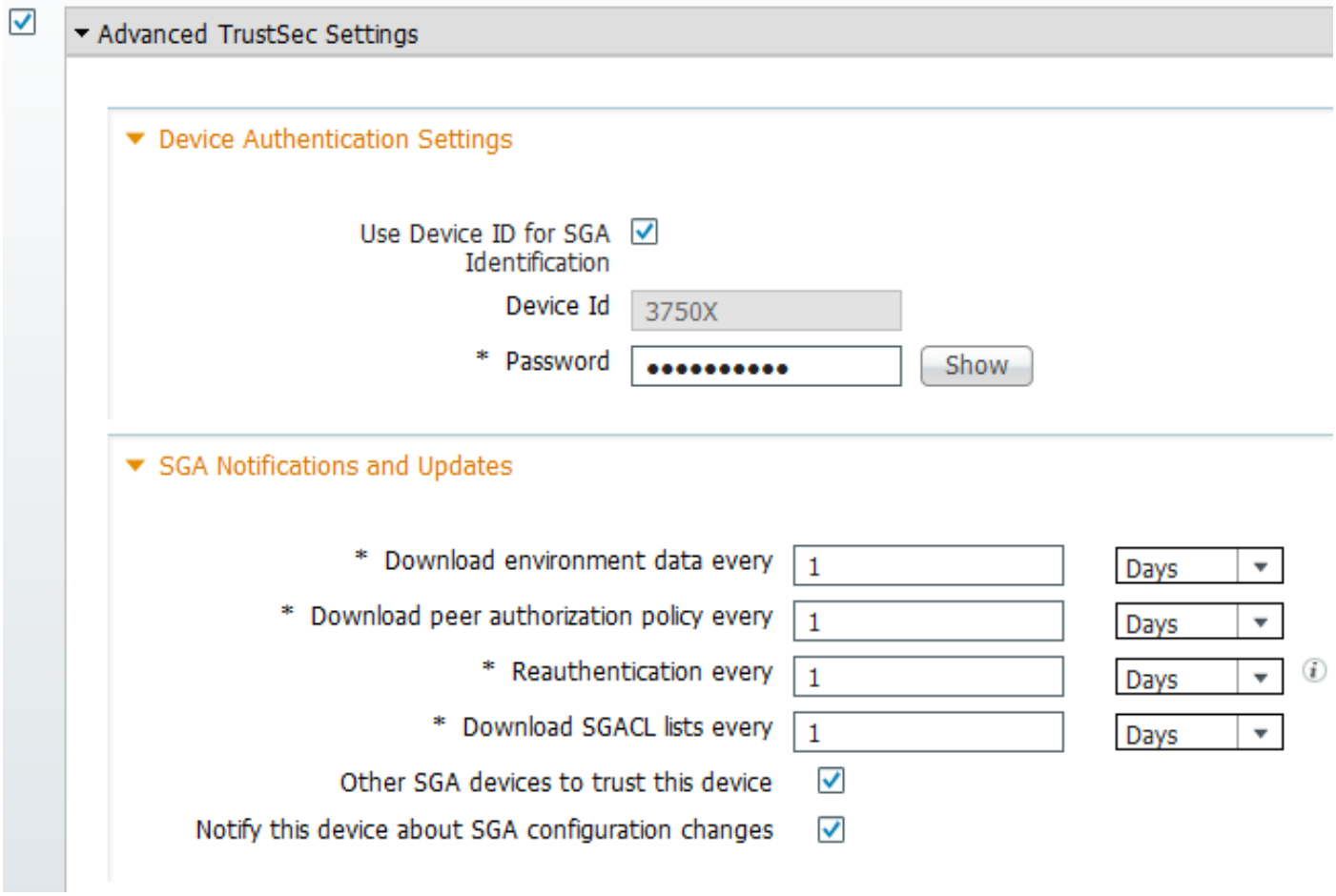
Aprovisionamiento de PAC en el 3750X (automático) y el ASA (manual)

Cada dispositivo de la nube CTS debe autenticarse en el servidor de autenticación (ISE) para que otros dispositivos confíen en él. Para ello, utiliza el método EAP-FAST (protocolo de autenticación extensible-autenticación flexible a través de protocolo seguro) (RFC 4851). Este método requiere que la PAC se entregue fuera de banda. Este proceso también se denomina **phase0** y no está definido en ningún RFC. La función PAC para EAP-FAST es similar a la del certificado de protocolo de autenticación extensible-seguridad de la capa de transporte (EAP-TLS). PAC se utiliza para establecer un túnel seguro (fase 1), que es necesario para la autenticación en la fase 2.

Aprovisionamiento de PAC en el 3750X

El 3750X admite el aprovisionamiento automático de PAC. Se utiliza una contraseña compartida en el switch y en el ISE para descargar la PAC. La contraseña y el ID deben configurarse en el

ISE en **Administration > Network Resources > Network Devices**. Seleccione el switch y expanda la sección **Configuración avanzada de TrustSec** para configurar:



Para que PAC utilice estas credenciales, ingrese estos comandos:

```
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
```

Aprovisionamiento de PAC en ASA

ASA solo admite el aprovisionamiento manual de PAC. Esto significa que debe generarlo manualmente en ISE (en Network Devices/ASA):

A continuación, se debe instalar el archivo (por ejemplo, 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
```

Actualización del entorno en ASA y el 3750X

En esta etapa, ambos dispositivos tienen PAC instalada correctamente y comienzan automáticamente a descargar los datos del entorno ISE. Estos datos son básicamente números de etiqueta y sus nombres. Para activar una actualización de entorno en el ASA, ingrese este comando:

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

Para verificarlo en el ASA (desafortunadamente no puede ver las etiquetas/nombres SGT específicos, pero se verifica más adelante), ingrese este 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)
```

Para verificarlo en 3750X, active una actualización del entorno con este comando:

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

Para verificar los resultados, ingrese este 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
```

Esto muestra que todas las etiquetas y los nombres correspondientes se descargan correctamente.

Verificación y aplicación de la autenticación de puertos en el 3750X

Después de que el 3750X tenga los datos del entorno, debe verificar que las SGT se apliquen a las sesiones autenticadas.

Para verificar si MS Windows 7 está autenticado correctamente, ingrese este 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:  C0A800010000001002B67334C
     Acct Session ID:  0x00000179
              Handle:  0x94000101

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

El resultado muestra que **VLAN10** se utiliza junto con el **SGT 0002** y DACL que permite todo el tráfico.

Para verificar si MS Windows XP está autenticado correctamente, ingrese este 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
```

El resultado muestra que **VLAN 20** se utiliza junto con **SGT 0003** y DACL que permite todo el tráfico

Las direcciones IP se detectan con la funcionalidad de **seguimiento de dispositivos IP**. El switch DHCP debe configurarse para la **indagación DHCP**. Luego, después de la respuesta DHCP de indagación, aprende la dirección IP del cliente. Para una dirección IP configurada estáticamente (como en este ejemplo), se utiliza la funcionalidad de **arp snooping**, y una PC debe enviar cualquier paquete para que el switch pueda detectar su dirección IP.

Para el **seguimiento de dispositivos**, puede ser necesario un comando oculto para activarlo en los puertos:

```
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
```

Actualización de políticas en el 3750X

El 3750X (a diferencia del ASA) puede descargar políticas desde ISE. Antes de que descargue y aplique una política, debe habilitarla con estos comandos:

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

Si no lo habilita, la directiva se descarga, pero no se instala y no se utiliza para la aplicación.

Para activar una actualización de política, ingrese este comando:

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

Para verificar que la política se descarga desde ISE, ingrese este 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
```

El resultado muestra que sólo se descarga la parte necesaria de la política.

En la nube CTS, el paquete contiene la SGT del host de origen y la **aplicación se realiza en el dispositivo de destino**. Esto significa que el paquete se reenvía desde el origen al último dispositivo, que está conectado directamente al host de destino. Ese dispositivo es el punto de aplicación, ya que conoce las SGT de sus hosts conectados directamente, y sabe si el paquete entrante con una SGT de origen debe permitirse o denegarse para la SGT de destino específica.

Esta decisión se basa en las políticas descargadas de ISE.

En este escenario, se descargan todas las políticas. Sin embargo, si borra la sesión de autenticación de MS Windows XP (SGT=VLAN20), no es necesario que el switch descargue ninguna política (fila) que corresponda a VLAN20, ya que no hay más dispositivos de esa SGT conectados al switch.

La sección Advanced (Troubleshooting) explica cómo el 3750X decide qué políticas se deben descargar con un examen del nivel de paquete.

SXP Exchange (ASA como receptor y 3750X como altavoz)

ASA no admite SGT. ASA descarta todas las tramas con SGT. Es por eso que el 3750X no puede enviar tramas con etiquetas SGT al ASA. En su lugar, se utiliza SXP. Este protocolo permite que ASA reciba información del switch sobre la asignación entre las direcciones IP y SGT. Con esta información, ASA puede asignar direcciones IP a SGT y tomar una decisión basada en SGACL.

Para configurar el 3750X como un altavoz, ingrese estos comandos:

```
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
```

Para configurar el ASA como receptor, ingrese estos comandos:

```
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
```

Para verificar que ASA recibió los mapeos, ingrese este 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
```

Ahora, cuando ASA recibe el paquete entrante con la dirección IP de origen **192.168.1.200**, puede tratarlo como si viniera de **SGT=2**. Para la dirección IP de origen **192.168.200.2**, puede tratarla como si viniera de **SGT=3**. Lo mismo se aplica a la dirección IP de destino.

> **Nota**: El 3750X debe conocer la dirección IP del host asociado. Esto se realiza mediante el seguimiento de dispositivos IP. Para una dirección IP configurada estáticamente en el host final, el switch debe recibir cualquier paquete después de la autenticación. Esto activa el seguimiento del dispositivo IP para encontrar su dirección IP, que activa una actualización SXP. Cuando solo se conoce el SGT, no se envía a través de SXP.

Filtrado de tráfico en ASA con ACL SGT

A continuación se presenta una comprobación de la configuración de 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
```

Se crea una ACL y se aplica a la interfaz interna. Permite todo el tráfico ICMP de **SGT=3** a **SGT=2** (denominado **VLAN10**):

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

Nota: Puede utilizar el número de etiqueta o el nombre de etiqueta.

Si hace ping desde MS Windows XP con una dirección IP de origen de **192.168.2.200** (**SGT=3**) a MS Windows 7 con una dirección IP de **192.168.1.200** (**SGT=2**), el ASA crea una conexión:

```
%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)
```

Cuando intenta hacer lo mismo con Telnet, el tráfico se bloquea:

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

Hay más opciones de configuración en el ASA. Es posible utilizar una etiqueta de seguridad y una dirección IP tanto para el origen como para el destino. Esta regla permite el tráfico de eco ICMP desde la **etiqueta SGT = 3** y la dirección IP **192.168.2.200** hasta la etiqueta SGT denominada **VLAN10** y la dirección de host de destino **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
```

Esto también se puede lograr con grupos de objetos:

```
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
```

Filtrado de tráfico en el 3750X con políticas descargadas desde ISE (RBACL)

También es posible definir políticas locales en el switch. Sin embargo, este ejemplo presenta las políticas descargadas desde ISE. Las políticas definidas en ASA pueden utilizar direcciones IP y SGT (y el nombre de usuario de Active Directory) en una sola regla. Las políticas definidas en el switch (tanto locales como de ISE) solo permiten SGT. Si necesita utilizar direcciones IP en sus reglas, se recomienda filtrar en ASA.

Se prueba el tráfico ICMP entre MS Windows XP y MS Windows 7. Para esto, debe cambiar la gateway predeterminada de ASA a 3750X en MS Windows. El 3750X tiene interfaces de ruteo y puede rutear los paquetes:

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

Las políticas ya se han descargado de ISE. Para verificarlos, ingrese este 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
```

El tráfico de VLAN10 (MS Windows 7) a VLAN20 (MS Windows XP) está sujeto a ICMP-20 ACL, que se descarga desde ISE:

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

Para verificar la ACL, ingrese este 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
```

Para verificar la asignación de SGT y asegurarse de que el tráfico de ambos hosts esté etiquetado correctamente, ingrese este 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
```

ICMP de MS Windows 7 (**SGT=2**) a MS Windows XP (**SGT=3**) funciona bien con ACL ICMP-20. Esto se verifica mediante la verificación de los contadores para el tráfico de **2**a **3** (15 paquetes permitidos):

```
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
```

Después de intentar utilizar el contador Telnet, los paquetes denegados aumentan (no está permitido en 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
```

> **Nota**: el carácter asterisco (*) que se muestra en la salida está relacionado con todo el tráfico que no está etiquetado (esa columna y esa fila se denominan **desconocidas** en Matrix en ISE y utilizan el número de etiqueta **0**).

Cuando tiene una entrada de ACL con la palabra clave log (definida en ISE), los detalles del paquete correspondientes y las acciones realizadas se registran como en cualquier ACL con la palabra clave log.

Verificación

Consulte las secciones de configuración individuales para ver los procedimientos de verificación.

Troubleshoot

Aprovisionamiento de PAC

Pueden aparecer problemas al utilizar el aprovisionamiento automático de PAC. Recuerde utilizar la palabra clave **pac** para el servidor RADIUS. El aprovisionamiento automático de PAC en el 3750X utiliza el método EAP-FAST con el protocolo de autenticación extensible con el método interno mediante la autenticación del protocolo de autenticación por desafío mutuo de Microsoft (EAP-MSCHAPv2). Al depurar, verá varios mensajes RADIUS que forman parte de la negociación EAP-FAST utilizada para crear el túnel seguro, que utiliza EAP-MSCHAPv2 con el ID y la contraseña configurados para la autenticación.

La primera solicitud RADIUS utiliza AAA **service-type=cts-pac-provisioning** para notificar al ISE que se trata de una solicitud 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.
```

Se espera el **rechazo RADIUS** al final de la salida porque ya recibió PAC y no siguió con un proceso de autenticación adicional.

Recuerde que la PAC es obligatoria para todas las demás comunicaciones con ISE. Pero, si no lo tiene, el switch aún intenta realizar una actualización de entorno o política cuando está configurado. Luego, no adjunta **cts-opaqueue** (PAC) en las solicitudes RADIUS, lo que causa las fallas.

Si la clave PAC es incorrecta, se muestra este mensaje de error en ISE:

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

También puede ver este resultado de los debugs (**debug cts provisioning + debug radius**) en el switch si la clave PAC es incorrecta:

```
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
```

Si utiliza la convención de **servidor radius** moderna, se muestra:

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

> **Nota**: debe utilizar la misma contraseña en el ISE que utilizó en la **Configuración de autenticación de dispositivo**.

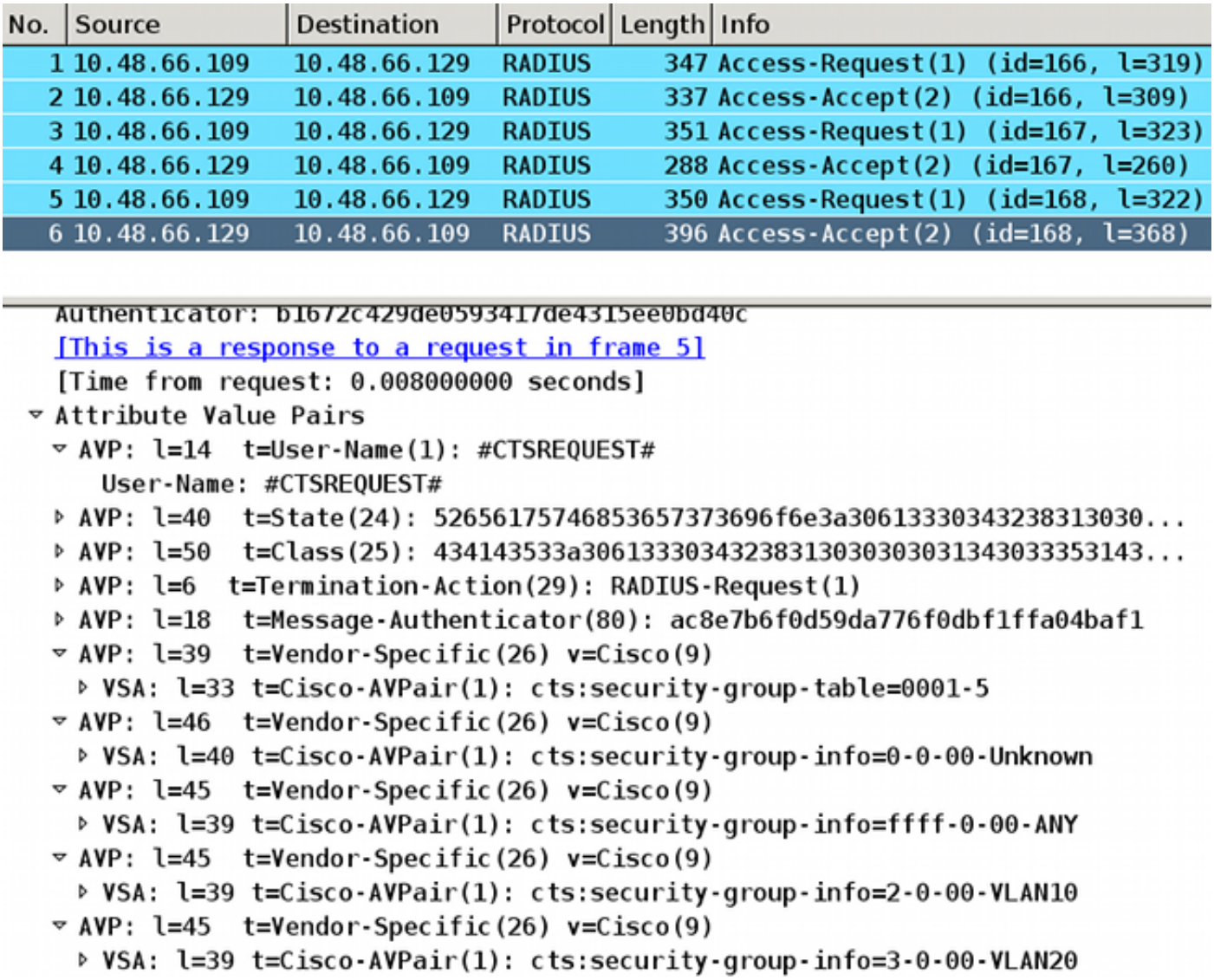
Después de aprovisionar PAC correctamente, se muestra en el ISE:

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)

Actualización del entorno

La actualización del entorno se utiliza para obtener datos básicos de ISE, que incluyen el número y el nombre de SGT. El nivel de paquete muestra que son solo tres solicitudes RADIUS y respuestas con atributos.

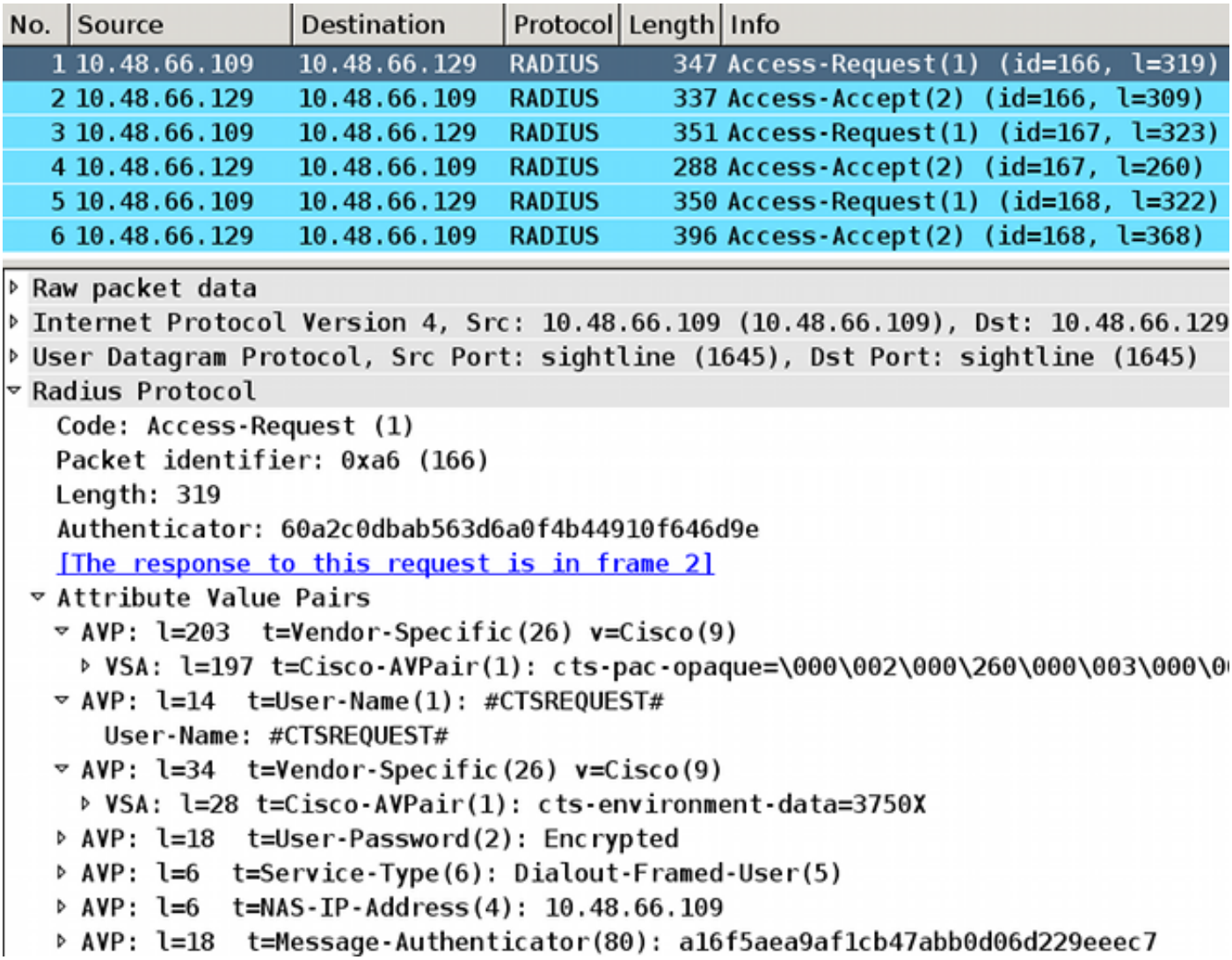
Para la primera solicitud, el switch recibe el nombre **CTSServerlist**. Para la segunda, recibe los detalles de esa lista, y para la última, recibe todas las SGT con etiquetas y nombres:



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)

Aquí puede ver el valor predeterminado **SGT 0**, **ffff**, y también dos valores definidos de forma personalizada: la etiqueta SGT 2 se denomina **VLAN10** y la etiqueta SGT 3 se denomina **VLAN20**.

> **Nota**: Todas las solicitudes RADIUS incluyen **cts-pac-opaque como resultado del aprovisionamiento de 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)

En el 3750X, debería ver depuraciones para las tres respuestas RADIUS y las listas correspondientes, los detalles de la lista y la lista SGT-inside específica:

```
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)
```

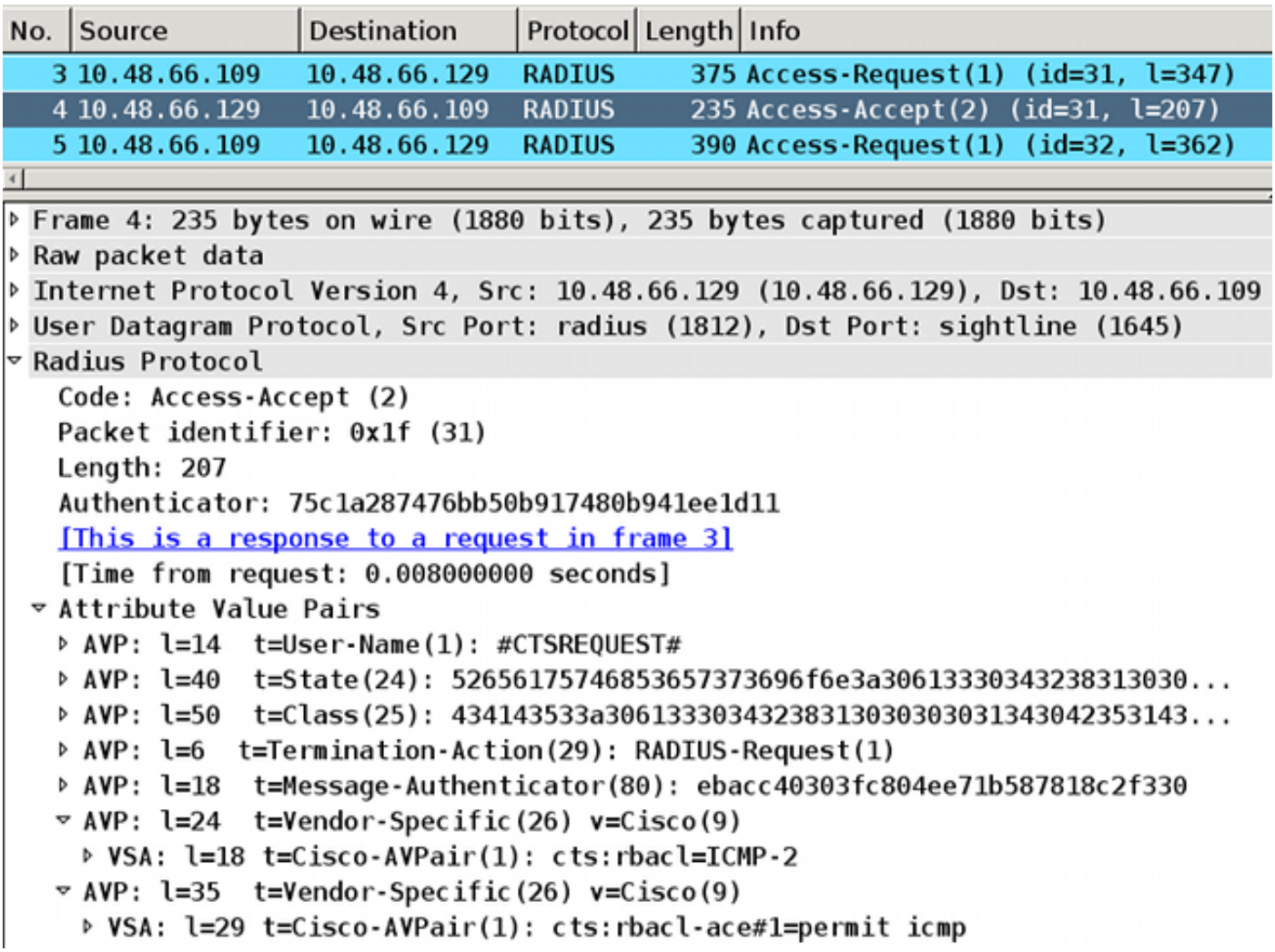
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: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

Actualización de políticas

La actualización de políticas sólo se admite en el switch. Es similar a la actualización del entorno. Se trata simplemente de solicitudes y aceptaciones RADIUS.

El switch solicita todas las ACL dentro de la lista predeterminada. Luego, para cada ACL que no está actualizada (o no existe), envía otra solicitud para obtener los detalles.

Aquí hay un ejemplo de respuesta cuando solicita ICMP-20 ACL:



Recuerde que debe tener **la aplicación basada en roles de cts** configurada para hacer cumplir esa ACL.

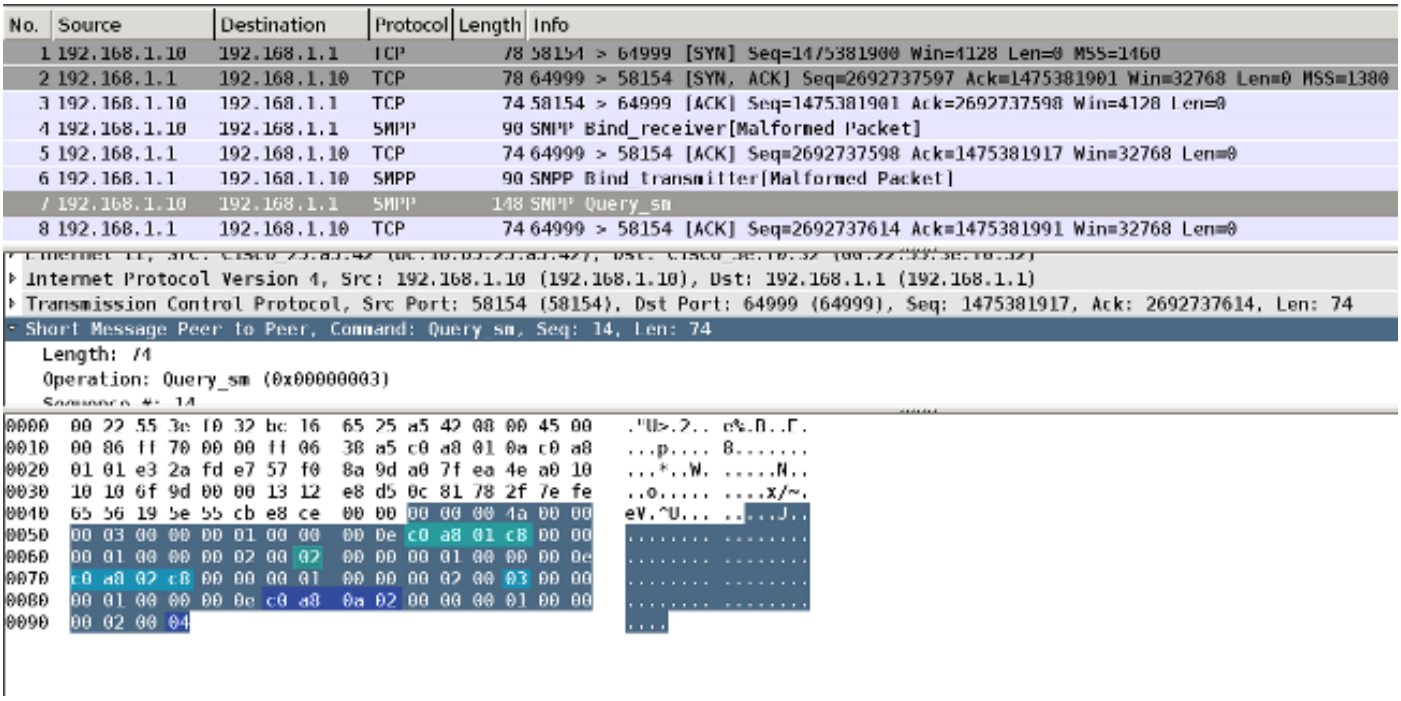
Las depuraciones indican si hay cambios (basados en el ID de generación). Si es así, puede desinstalar la directiva antigua si es necesario e instalar una nueva. Esto incluye la programación ASIC (compatibilidad de hardware).

```
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

La actualización de SXP es activada por el código de seguimiento de dispositivos IP que encuentra la dirección IP del dispositivo. A continuación, se utiliza el protocolo de mensaje corto de igual a igual (SMPP) para enviar las actualizaciones. Utiliza la **opción 19 de TCP** para la autenticación, que es la misma que el protocolo de gateway fronterizo (BGP). La carga de SMPP no está cifrada. Wireshark no tiene un decodificador adecuado para la carga útil de SMPP, pero es fácil encontrar datos en su interior:



- El primero, **c0 a8 01 c8**, es **192.168.1.200** y tiene la **etiqueta 2**.
- El segundo, **c0 a8 02 c8**, es **192.168.2.200** y tiene la **etiqueta 3**.
- El tercero, **c0 a8 0a 02,** es **192.168.10.2** y tiene la **etiqueta 4** (esta se utilizó para probar el teléfono **SGT=4**)

A continuación se muestran algunas depuraciones en el 3750X después de que el seguimiento de dispositivos IP encuentre la dirección IP de 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
```

Estas son las depuraciones correspondientes en el 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.
```

Para ver más depuraciones en el ASA, puede habilitar el nivel de detalle de la depuración:

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

SGACL en ASA

Después de que ASA instale correctamente las asignaciones SGT recibidas por SXP, la ACL de grupos de seguridad debería funcionar correctamente. Cuando tenga problemas con la asignación, introduzca:

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

La ACL con el grupo de seguridad funciona exactamente igual que para la dirección IP o la identidad del usuario. Los registros revelan problemas, y la entrada exacta de la ACL que fue alcanzada.

Aquí hay un ping de MS Windows XP a MS Windows 7 que muestra que el rastreador de paquetes funciona correctamente:

```
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>
```

Información Relacionada

- Guía de configuración de Cisco TrustSec para 3750
- Guía de configuración de Cisco TrustSec para ASA 9.1
- Implementación y hoja de ruta de Cisco TrustSec
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).