ASA y ejemplo de configuración de TrustSec del Catalyst 3750X Series Switch y guía del Troubleshooting

Contenido

Introducción

Este artículo describe cómo configurar Cisco TrustSec (CTS) en el dispositivo de seguridad adaptante seguro de Cisco (ASA) y un Cisco Catalyst 3750X Series Switch (3750X).

Para aprender la asignación entre las etiquetas del grupo de seguridad (SGTs) y los IP

Addresses, el ASA utiliza el Exchange Protocol SGT (SXP). Entonces, el Listas de control de acceso (ACL) basado en SGT se utiliza para filtrar el tráfico. El 3750X descarga las directivas basadas en Role de la lista de control de acceso (RBACL) del Cisco Identity Services Engine (ISE), y los filtros trafican basado en ellas. Este artículo detalla el nivel del paquete para describir cómo la comunicación actúa y los debugs previstos.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

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

Componentes Utilizados

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

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

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Diagrama de la red

Flujo de tráfico

Aquí está el flujo de tráfico:

- El 3750X se configura en **G1/0/1** y **G1/0/2** para la autenticación del puerto.
- El ISE se utiliza como el servidor del Authentication, Authorization, and Accounting (AAA).
- Puente de la dirección MAC (MAB) se utiliza para la autenticación para MS Windows 7.
- El IEEE 802.1X se utiliza para MS Windows XP para demostrar que no importa se utiliza qué método de autentificación.

Después de la autenticación satisfactoria, el ISE vuelve el SGT, y los lazos 3750X que marcan

con etiqueta a la sesión de la autenticación. El Switch también aprende los IP Addresses de ambas estaciones con el comando de **seguimiento del dispositivo del IP**. El Switch entonces utiliza SXP para enviar la tabla de correspondencia entre el SGT y la dirección IP al ASA. Ambo MS Windows PC tiene un ruteo predeterminado esas puntas al ASA.

Después de que el ASA reciba el tráfico de la dirección IP que se asocia al SGT, puede utilizar el ACL basado en el sargento. También, cuando usted utiliza 3750X como router (default gateway para ambas estaciones de MS Windows), puede filtrar el tráfico basado en las directivas descargadas del ISE.

Aquí están los pasos para la configuración y la verificación, que se detalla en su propia sección más adelante en el documento:

- Vire la autenticación hacia el lado de babor con el comando de **seguimiento del dispositivo del IP** en el 3750X
- Configuración ISE para la autenticación, SGT, y las directivas de la lista de control de acceso del grupo de seguridad (SGACL)
- Configuración CTS en el ASA y el 3750X
- Aprovisionamiento credencial protegido del acceso (PAC) en el 3750X (automático) y el ASA (manual)
- El entorno restaura en el ASA y el 3750X
- Verificación de autenticación y aplicación del puerto en el 3750X
- La directiva restaura en el 3750X
- Intercambio SXP (el ASA como módulo de escucha, y el 3750X como altavoz)
- Filtrado de tráfico en el ASA con SGT ACL
- Filtrado de tráfico en el 3750X con las directivas descargadas del ISE

Configuraciones

Vire la autenticación hacia el lado de babor con el comando de *seguimiento del dispositivo del IP* en el 3750X

Ésta es la configuración típica para el 802.1x o el MAB. El cambio RADIUS de la autorización (CoA) se necesita solamente cuando usted utiliza la notificación activa del 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 ISE para la autenticación, las directivas SGT, y SGACL

El ISE debe tener ambos dispositivos de red configurados bajo la **administración > dispositivos de red**:

Para MS Windows 7, que utiliza la autenticación MAB, usted debe crear la identidad del punto final (dirección MAC) conforme a la **administración > a la Administración de la identidad > a las identidades > a los puntos finales**:

Para MS Windows XP, que utiliza la autenticación del 802.1x, usted debe crear una Identificación del usuario (nombre de usuario) bajo la **administración > la Administración de la identidad > identidades > Users**:

Se utiliza el nombre de usuario cisco. Configure MS Windows XP para EAP Protocolo-protegido autenticación ampliable (EAP-PEAP) con estas credenciales.

En el ISE, se utilizan las directivas de la autenticación predeterminada (no cambie esto). El primer es la directiva para la autenticación MAB, y el segundo es 802.1x:

Para configurar las directivas de la autorización, usted debe definir los perfiles de la autorización bajo la **directiva > los resultados > la autorización > perfiles de la autorización**. El VLAN10-Profile 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 al número VLAN (20).

Para configurar los grupos SGT (etiquetas) en el ISE, navegue los **grupos del > Security (Seguridad) del acceso del grupo al > Security (Seguridad) de la directiva > de los resultados**.

> **Note**: No es posible elegir un número de Tag; es seleccionado automáticamente por el primer número libre excepto 1. Usted puede configurar el nombre SGT solamente.

Para crear el SGACL para permitir el tráfico del Internet Control Message Protocol (ICMP), navegue el **grupo ACL del > Security (Seguridad) del acceso del grupo al > Security (Seguridad)**

de la directiva > de los resultados:

Para crear las directivas, navegue al **acceso > a la política de egress del grupo del > Security (Seguridad) de la directiva**. Para el tráfico entre el VLAN10 y el VLA N o el VLAN10 o el VLAN20 desconocido, se utiliza el ICMP ACL (**ICMP del permiso**):

Para fijar las reglas de la autorización, navegue a la **directiva > a la autorización**. Para MS Windows 7 (dirección MAC específica), **VLAN10-Profile** DACL se utiliza, de la vuelta VLAN10 y, y el perfil de seguridad VLAN10 con el **VLAN10** nombrado SGT. Para MS Windows XP (nombre de usuario específico), **VLAN20-Profile** DACL se utiliza, de la vuelta VLAN20 y, y el perfil de seguridad VLAN20 con el **VLAN20** nombrado SGT.

Acabe el Switch y la configuración ASA para que validen los atributos de RADIUS SGT.

Configuración CTS en el ASA y el 3750X

Usted debe configurar las configuraciones básicas CTS. En el 3750X, usted debe indicar de qué directivas del servidor deben ser descargadas:

```
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
```

En el ASA, solamente el servidor de AAA es necesario junto con el CTS esas puntas a ese servidor:

```
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
```

> **Note**: En el 3750X, usted debe señalar explícitamente al servidor ISE con el **comando group radius**. Esto es porque el 3750X utiliza el aprovisionamiento automático PAC.

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

Cada dispositivo en la nube CTS debe autenticar al servidor de autenticación (ISE) para ser confiado en por los otros dispositivos. Utiliza la autenticación de Protocol Flexible de autenticación ampliable vía el método seguro del protocolo (EAP-FAST) (RFC 4851) para esto. Este método le requiere tener fuera de banda entregada PAC. Este proceso también se llama **phase0**, y no se define en ningún RFC. El PAC para el EAP-FAST tiene un papel similar como el certificado para la Seguridad de la capa del Protocolo-transporte de la autenticación ampliable (EAP-TLS). El PAC se utiliza para establecer un túnel seguro (phase1), que es necesario para la autenticación en phase2.

Aprovisionamiento PAC en el 3750X

El 3750X soporta el aprovisionamiento automático PAC. Una contraseña compartida se utiliza en el Switch y el ISE para descargar el PAC. Esa contraseña y ID se deben configurar en el ISE bajo la **administración > los recursos de red > dispositivos de red**. Seleccione el Switch, y amplíe la sección **avanzada de las configuraciones de TrustSec** para configurar:

Para tener PAC utilice estas credenciales, ingresan 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 PAC en el ASA

El ASA soporta solamente el aprovisionamiento manual PAC. Esto significa que usted debe generarlo manualmente en el ISE (en la red Devices/ASA):

Entonces el archivo debe ser instalado (por ejemplo, con el 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
```

El entorno restaura en el ASA y el 3750X

En esta etapa, ambos dispositivos tienen PAC instalado correctamente y comienzan automáticamente a descargar los datos del entorno ISE. Estos datos son básicamente números de Tag y sus nombres. Para accionar un entorno restaure en el ASA, ingresan este comando:

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

Para verificarlo en el ASA (desafortunadamente usted no puede ver las etiquetas específicas/los nombres SGT, 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, accione un entorno restauran 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 nombres correspondientes están descargados correctamente.

Verificación de autenticación y aplicación del puerto en el 3750X

Después de que el 3750X tenga los datos del entorno, usted debe verificar que el SGTs esté aplicado a las sesiones autenticadas.

Para verificar si MS Windows 7 se autentica 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:  C0A80001000001002B67334C
     Acct Session ID:  0x00000179
              Handle:  0x94000101

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

La salida muestra que el **VLAN10** está utilizado junto con el **SGT 0002** y DACL permitiendo para todo el tráfico.

Para verificar si MS Windows XP se autentica 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
```

La salida muestra que el **VLAN20** está utilizado junto con el **SGT 0003** y DACL permitiendo para todo el tráfico

Los IP Addresses se detectan con las funciones de **seguimiento del dispositivo del IP**. El Switch del DHCP se debe configurar para el **snooping DHCP**. Entonces, después de la respuesta DHCP del snooping, aprende el IP Address del cliente. Para un IP Address estático-configurado (como en este ejemplo), se utilizan las funciones del **snooping arp**, y un PC debe enviar cualquier paquete para que el Switch pueda detectar su IP Address.

Para el **dispositivo que seguía**, un comando oculto pudo ser necesario 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
```

La directiva restaura en el 3750X

El 3750X (a diferencia del ASA) puede descargar las directivas del ISE. Antes de que descargue y aplique una directiva, usted 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 usted no lo habilita, la directiva se descarga, pero no está instalada y no se utiliza para la aplicación.

Para accionar una directiva restaure, ingrese este comando:

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

Para verificar que la directiva esté descargada del 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
```

La salida muestra que solamente descargan a la parte de necesaria la directiva.

En la nube CTS, el paquete contiene el SGT del host de origen, y la **aplicación se hace en el dispositivo de destino**. Esto significa que el paquete está remitido de la fuente al dispositivo más reciente, que está conectado directamente con la computadora principal de destino. Ese dispositivo es la punta de la aplicación, puesto que conoce el SGTs de sus host conectados directamente, y sabe si el paquete entrante con una fuente SGT se permite o se niega para el sargento específico del destino.

Esta decisión se basa en las directivas descargadas del ISE.

En este escenario, se descargan todas las directivas. Sin embargo, si usted borra la sesión de la autenticación de MS Windows XP (SGT=VLAN20), después no hay necesidad del Switch de descargar ninguna directiva (fila) que corresponda al VLAN20, porque no hay dispositivos de eso SGT conectado con el Switch.

La sección avanzada (del troubleshooting) explica cómo el 3750X decide a qué directivas se deben descargar con un examen del nivel del paquete.

Intercambio SXP (el ASA como módulo de escucha, y el 3750X como Presidente)

El ASA no apoya al sargento. Todas las tramas con SGT son caídas por el ASA. Por eso el 3750X no puede enviar las tramas SGT-marcadas con etiqueta al ASA. En lugar, se utiliza SXP. Este protocolo permite que el ASA reciba la información del Switch sobre la asignación entre los IP Addresses y el sargento. Con esa información, el ASA puede asociar los IP Addresses a SGTs y tomar una decisión basada en SGACL.

Para configurar el 3750X como 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 módulo de escucha, 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 el ASA recibiera los mappings, 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 el ASA recibe el paquete entrante con la dirección IP de origen **192.168.1.200**, puede tratarla como si venga de **SGT=2**. Para la dirección IP de origen **192.168.200.2**, puede tratarla como si venga de **SGT=3**. Lo mismo solicita el IP Address de destino.

Note: El 3750X debe conocer la dirección IP del host asociado. Esto es hecha siguiendo del dispositivo IP. Para una dirección IP estático-configurada en el host extremo, el Switch debe recibir cualquier paquete después de la autenticación. Esto acciona el dispositivo IP que sigue para encontrar su dirección IP, que acciona una actualización SXP. Cuando solamente se sabe el SGT, no se envía vía SXP.

Filtrado de tráfico en el ASA con SGT ACL

Aquí está un control de la configuración ASA:

```
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
```

Un ACL se crea y se aplica a la interfaz interior. Permite todo el tráfico ICMP de **SGT=3 a SGT=2** (llamado **VLAN10**):

```
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
```

Note: Usted puede utilizar el nombre del número de Tag o de la etiqueta.

Si usted hace ping de 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 construye una conexión:

```
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
```

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

```
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
```

Hay más opciones de configuración en el ASA. Es posible utilizar una etiqueta de la Seguridad y una dirección IP para la fuente y el destino. Esta regla permite el tráfico del eco ICMP de la **etiqueta SGT = 3** y dirección IP 192.168.2.200 a la etiqueta SGT nombrada **VLAN10** y la dirección de host **192.168.1.200 del** destino:

```
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
```

Esto se puede también alcanzar con los grupos de objetos:

```
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
```

Filtrado de tráfico en el 3750X con las directivas descargadas del ISE (RBACL)

Es también posible definir las políticas locales en el Switch. Sin embargo, directivas de presentes de este ejemplo descargadas del ISE. Las directivas definidas en el ASA se permiten utilizar los IP Addresses y SGTs (y el nombre de usuario del Active Directory) en una regla. Las directivas definidas en el Switch (local y del ISE) permiten solamente SGTs. Si usted necesita utilizar los IP Addresses en sus reglas, después la filtración en el ASA se recomienda.

El tráfico ICMP entre MS Windows XP y MS Windows 7 se prueba. Para esto, usted debe cambiar el default gateway del ASA al 3750X en MS Windows. El 3750X tiene interfaces de la encaminamiento y puede rutear los paquetes:

```
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
```

Las directivas se descargan ya del ISE. Para verificarlas, 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
```

Tráfico del **VLAN10** (MS Windows 7) a **VLAN20** (MS WindowsXP) se sujeta a ICMP-20 ACL, que se descarga del ISE:

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

Para verificar el 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 el SGT que asocia para aseegurarse que el tráfico de ambos host está marcado con etiqueta 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
```

El ICMP de MS Windows 7 (**SGT=2**) a MS Windows XP (**SGT=3**) trabaja muy bien con ACL ICMP-20. Esto es verificada marcando los contadores para el tráfico a partir del **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 que usted intente utilizar el contador de Telnet, el aumento negado de los paquetes (no se permite 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
```

> **Note**: El carácter de la estrella (*) mostrado en la salida se relaciona con todo el tráfico que no se marque con etiqueta (esa columna y fila se llama **desconocida** en la matriz en el ISE, y el número de Tag **0 del** uso).

Cuando usted tiene una entrada ACL con la palabra clave del registro (definida en el ISE), los detalles del paquete correspondientes y medidas tomadas se registran como en cualquier ACL con la palabra clave del registro.

Verificación

Refiera a las secciones de configuración individuales para los procedimientos de verificación.

Troubleshooting

Aprovisionamiento PAC

Los problemas pudieron aparecer cuando usted utiliza el aprovisionamiento automático PAC. Recuerde utilizar la palabra clave **pac** para el servidor de RADIUS. El aprovisionamiento automático PAC en el 3750X utiliza el método del EAP-FAST con el protocolo extensible authentication con el método interno usando la autenticación del Challenge Handshake Authentication Protocol de Microsoft (EAP MSCHAPv2). Cuando usted debug, usted ve los mensajes de RADIUS múltiples que son la negociación del EAP-FAST de la parte de usada para construir el túnel seguro, que utiliza el EAP MSCHAPv2 con el ID y la contraseña para autenticación configurados.

El primer pedido de RADIUS utiliza el AAA **service-type=cts-pac-provisioning** para notificar el ISE que esto es una petición 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.
```

El rechazo RADIUS en el extremo de la salida se espera puesto que usted recibió ya el PAC, y no siguió con otro proceso de autenticación.

Recuerde que el PAC está requerido para el resto de la comunicación con el ISE. Pero, si usted no lo tiene, el Switch todavía intenta un entorno o la directiva restaura cuando se configura. Entonces, no asocia el **cts-opaqueue** (PAC) en los pedidos de RADIUS, que causa los errores.

Si su clave PAC es incorrecta, las visualizaciones de este mensaje de error en el ISE:

```
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.
```

Usted también ve esta salida de los debugs (**cts del debug provisioning + radio del debug**) en el Switch si su 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 usted utiliza al convenio moderno del **servidor de RADIUS**, éste visualiza:

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

> **Note**: Usted debe utilizar la misma contraseña en el ISE que usted utilizó en las **configuraciones de la autenticación del dispositivo**.

Después del aprovisionamiento acertado PAC, este visualizaciones en el ISE:

El entorno restaura

El entorno restaura se utiliza para obtener los datos básicos del ISE, que incluye el número y el nombre SGT. El nivel del paquete muestra que es solamente tres pedidos de RADIUS y

respuestas con los atributos.

Para la primera petición, el Switch recibe el nombre de **CTSServerlist**. Para segundo, recibe los detalles para esa lista, y para la más reciente, recibe todo el SGTs con las etiquetas y los nombres:

Aquí usted ve el valor por defecto **SGT 0**, el **ffff**, y también dos aduana-definidos: La etiqueta 2 SGT se nombra la etiqueta 3 **VLAN10** y SGT se nombra **VLAN20**.

> **Note**: Todos los pedidos de RADIUS incluyen cts-PAC-**opaco** como resultado del aprovisionamiento PAC.

En el 3750X, usted debe ver los debugs para las tres respuestas RADIUS y las listas correspondientes, los detalles de la lista, y el específico SGT-dentro de la lista:

```
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
```

La directiva restaura

La directiva restaura se soporta solamente en el Switch. Es similar al entorno restaura. Éstos son simplemente pedidos de RADIUS y validan.

El Switch pide todos los ACL dentro de la lista predeterminada. Entonces, para cada ACL que no sea actualizado (o no existe), envía otra petición de obtener los detalles.

Aquí está una respuesta del ejemplo cuando usted pide ICMP-20 ACL:

Recuerde que usted debe hacer la **aplicación papel-basada los cts** configurar para aplicar ese ACL.

Los debugs indican si hay cambios (basados en GEN ID). Si es así usted puede desinstalar la vieja directiva si está necesitado, y instala un nuevo. Esto incluye la programación de ASIC (soporte del 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
```

Intercambio SXP

La actualización SXP es accionada por el código de dispositivo-seguimiento IP que encuentra la dirección IP del dispositivo. Entonces, el protocolo entre iguales del mensaje corto (SMPP) se utiliza para enviar las actualizaciones. Utiliza la opción TCP 19 para la autenticación, que es lo mismo que el Border Gateway Protocol (BGP). El payload SMPP no se cifra. Wireshark no tiene

un decodificador apropiado para el payload SMPP, sino que es fácil encontrar los datos dentro de él:

- Primer, **c0 a8 01 c8**, es **192.168.1.200** y tiene **etiqueta 2.**
- Segundo, **c0 a8 02 c8**, es **192.168.2.200** y tiene **etiqueta 3.**
- Tercer, **c0 a8 0a 02,** es **192.168.10.2** y tiene **etiqueta 4** (éste era para el teléfono de prueba usado **SGT=4**)

Aquí están algunos debugs en el 3750X después de que el seguimiento del dispositivo 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
```

Aquí están los debugs 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 debugs en el ASA, usted puede habilitar el nivel de la verbosidad del debugging:

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

SGACL en el ASA

Después de que el ASA instale correctamente las asignaciones SGT recibidas por SXP, los grupos de seguridad ACL deben trabajar muy bien. Cuando usted encuentra los problemas con asociar, ingrese:

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

El ACL con el grupo de seguridad trabaja exactamente lo mismo que hace para la dirección IP o la Identificación del usuario. Los registros revelan los problemas, y la entrada exacta del ACL que fue golpeado.

Aquí está un ping de MS Windows XP a MS Windows 7 que muestre los trabajos de ese trazalíneas del paquete 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
- Despliegue y mapa de ruta de Cisco TrustSec
- Soporte Técnico y Documentación - Cisco Systems