El marcar con etiqueta en línea de la configuración ASA 9.3.1 TrustSec

Contenido

Introducción

Este documento describe cómo utilizar la característica implementada en la versión adaptante 9.3.1 del dispositivo de seguridad (ASA) - el marcar con etiqueta en línea de TrustSec. Que la característica permite que el ASA reciba las tramas de TrustSec así como que las envíe. Esta manera ASA se puede integrar fácilmente dentro del dominio de TrustSec sin la necesidad de utilizar el Exchange Protocol de TrustSec SGT (SXP).

Este ejemplo presenta el usuario de VPN remoto que se han asignado la etiqueta de la etiqueta del grupo de seguridad (SGT) = 3 (márketing) y al usuario del 802.1x que se han asignado la etiqueta SGT = 2 (las finanzas). La aplicación del tráfico es realizada por el ASA con el uso de la lista de control de acceso del grupo de seguridad (SGACL) definido localmente y Switch del ® del Cisco IOS usando la lista de control de acceso basada papel (RBACL) descargada del Identity Services Engine (ISE).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración CLI ASA y configuración VPN del Secure Socket Layer (SSL)
- Configuración del VPN de acceso remoto en el ASA
- Servicios ISE y de TrustSec

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software de Cisco ASA, versión 9.3.1 y posterior
- Hardware 55x5 o ASAv de Cisco ASA
- Windows 7 con el Cliente de movilidad Cisco AnyConnect Secure, versión 3.1
- Cisco Catalyst 3750X Switch con el software 15.0.2 y posterior
- Cisco ISE, libera 1.2 y posterior

Configurar

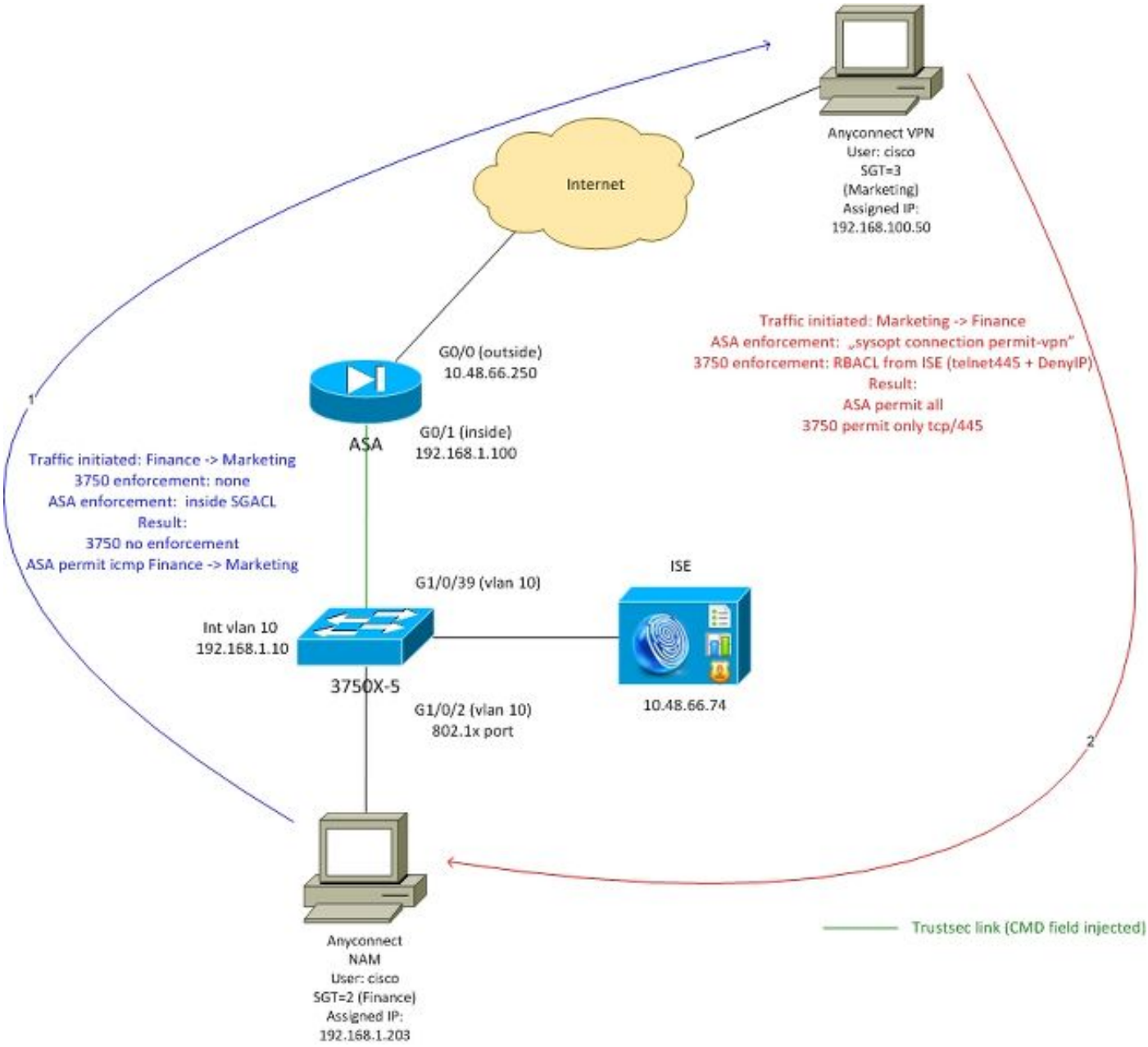
> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

La conexión entre el ASA y 3750X se configura para los cts manuales. Eso significa que ambos dispositivos pueden enviar y recibir las tramas Ethernet modificadas con los meta datos de Cisco coloque (CMD). Ese campo incluye la etiqueta del grupo de seguridad (SGT) que describe la fuente del paquete.

El usuario de VPN remoto termina a la sesión SSL en el ASA y se asigna la etiqueta 3 (márketing) SGT.

Usuario corporativo local del 802.1x después de que la autenticación satisfactoria se haya asignado la etiqueta 2 (finanzas) SGT.



El ASA tiene SGACL configurado en la interfaz interior que permite el tráfico ICMP iniciado de las finanzas a la comercialización.

El ASA permite todo el tráfico iniciado de quita al usuario de VPN (debido a “la configuración de permiso-VPN de la conexión del sysopt”).

SGACL en el ASA es stateful que significa que el flujo está creado una vez, paquete de devolución se valida automáticamente (basado en el examen).

El 3750 Switch utiliza RBACL para controlar el tráfico recibido del márketing para financiar.

RBACL es apátrida que significa que cada paquete está marcado pero la aplicación de TrustSec en la plataforma 3750X está realizada en el destino. Este Switch de la manera es responsable de la aplicación del tráfico del márketing financiar.

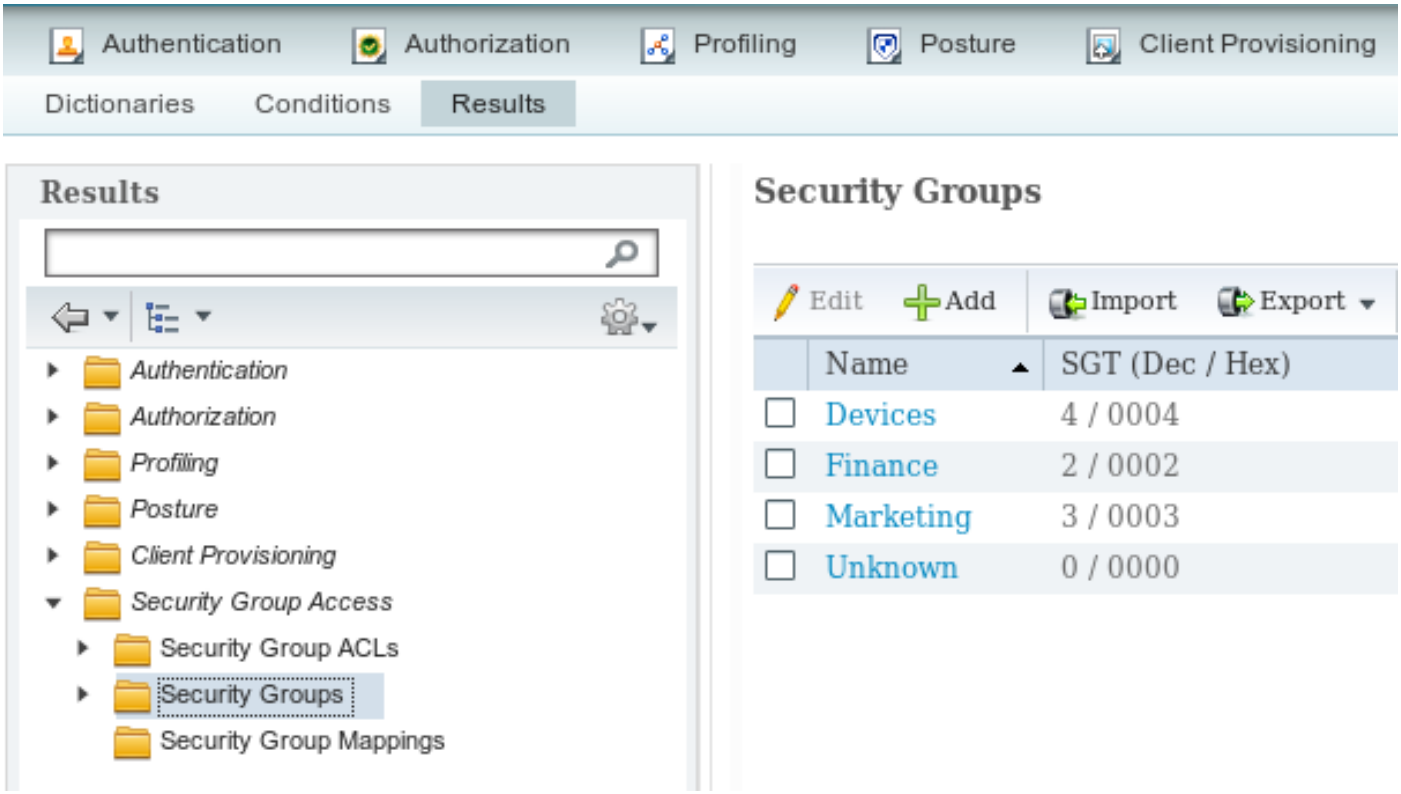
> **Note**: Para el escudo de protección con estado enterado de Trustsec en el Firewall basado zona del ® del Cisco IOS puede ser utilizado, por ejemplo, refiérase:

Note: El ASA podría tener tráfico que controlaba SGACL que viene del usuario de VPN remoto. Para simplificar el escenario, no se ha presentado en este artículo. Por ejemplo refiérase: Clasificación de ASA versión 9.2 VPN SGT y ejemplo de configuración de aplicación

ISE - Pasos de configuración

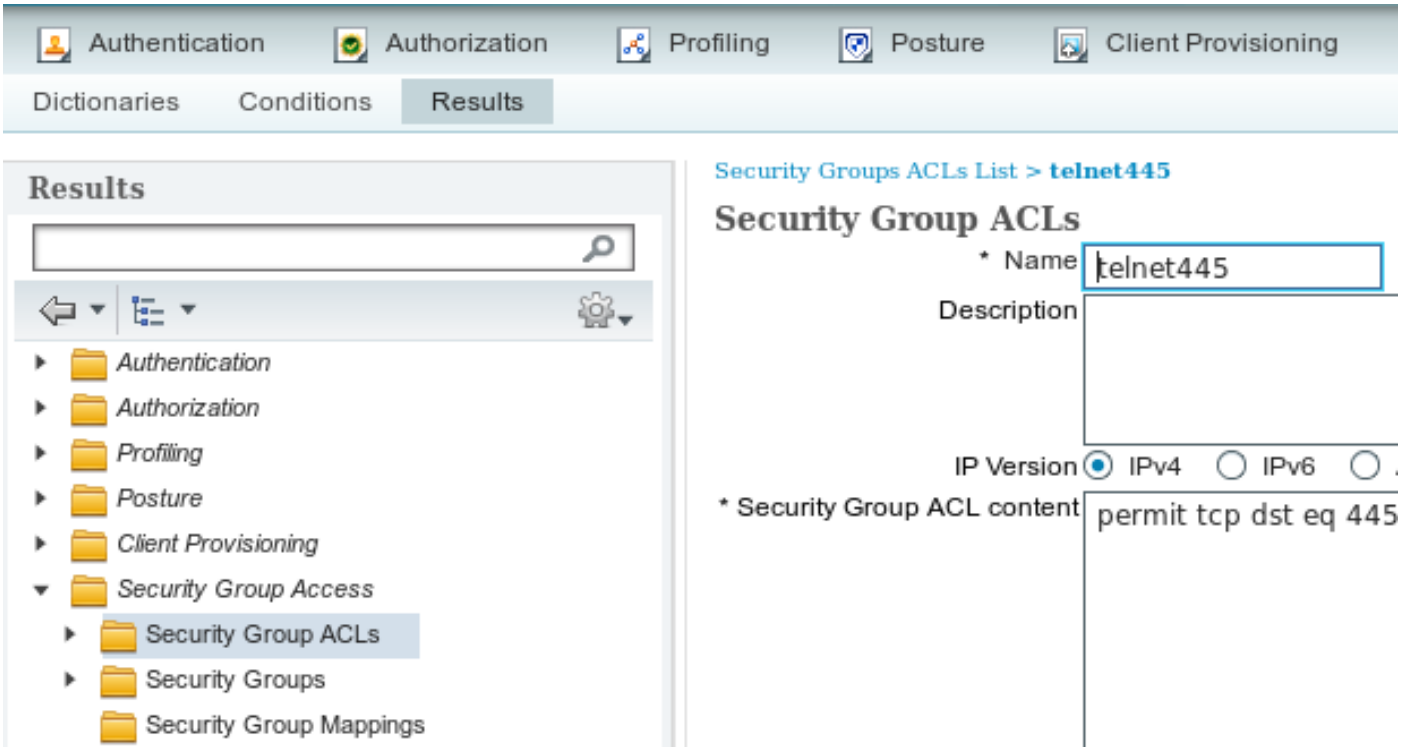
1. SGT para las finanzas y el márketing

Navegue los **grupos del > Security (Seguridad) del acceso del grupo al > Security (Seguridad) de la directiva > de los resultados** y cree SGT para las finanzas y el márketing tal y como se muestra en de esta imagen.



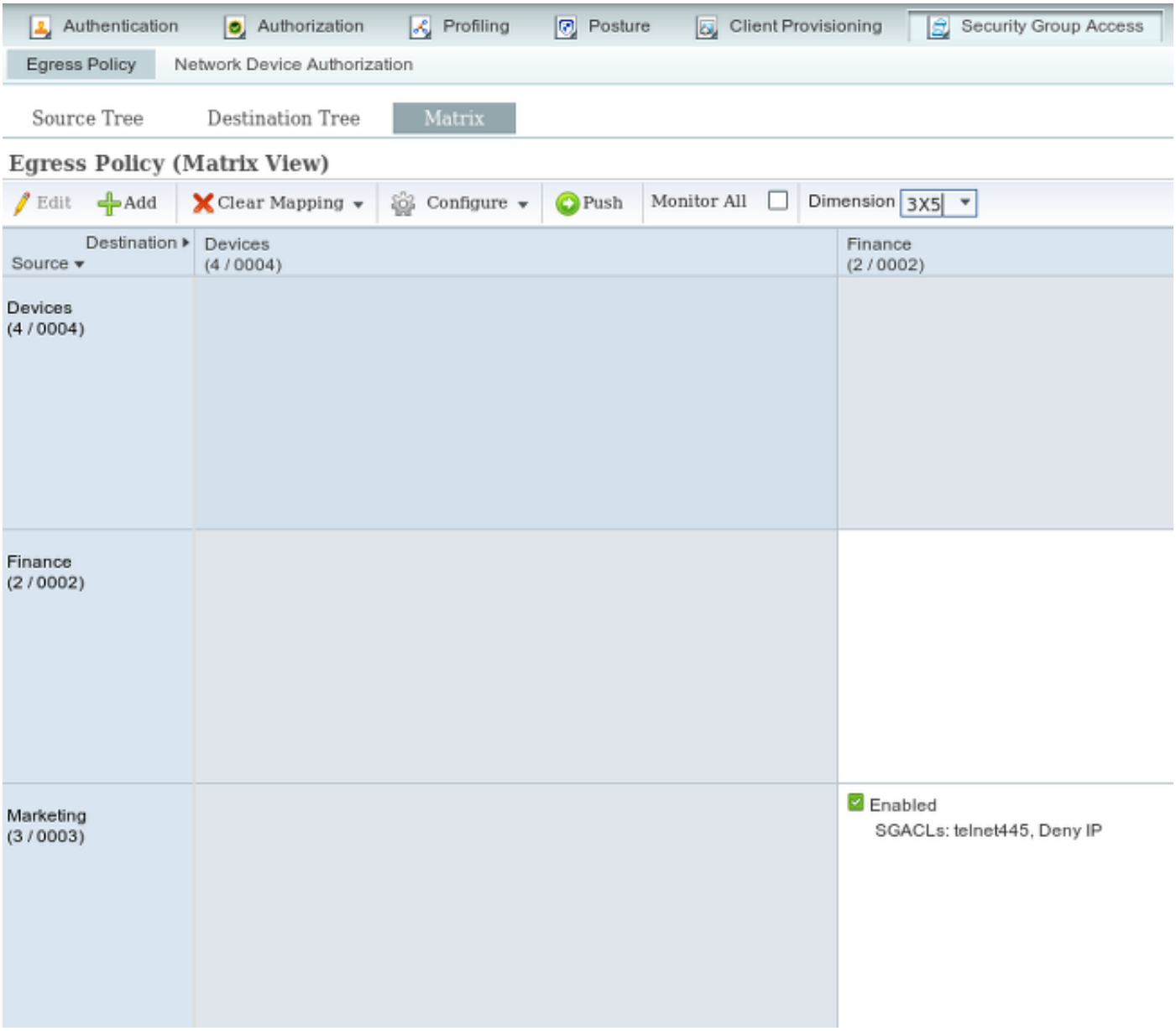
2. Grupo de seguridad ACL para el márketing > las finanzas del tráfico

Navegue el **grupo ACL del > Security (Seguridad) del acceso del grupo al > Security (Seguridad) de la directiva > de los resultados** y cree el ACL que se utiliza al tráfico de control del márketing para financiar. Solamente tcp/445 se permite tal y como se muestra en de esta imagen.



3. ACL obligatorio en la matriz

Navegue a la **directiva > a la política de egress > a la matriz** ACL configurado lazo para la fuente: **Márketing** y destino: **Finanzas**. También la fijación **niega el IP** como el último ACL para caer el resto del tráfico tal y como se muestra en de la imagen. (sin esa política predeterminada será asociado, valor por defecto es permiso)



4. Regla de la autorización para el acceso VPN que asigna SGT = 3 (márketing)

Navegue a la **directiva > a la autorización** y cree una regla para el acceso del telecontrol VPN. Todas las conexiones VPN establecidas vía el cliente de AnyConnect 4.x conseguirán el acceso total (PermitAccess) y serán asignadas la etiqueta 3 (márketing) SGT. La condición es utilizar la identidad Extentions (ACIDEX) de AnyConnect:

```
Rule name: VPN
Condition: Cisco:cisco-av-pair CONTAINS mdm-tlv=ac-user-agent=AnyConnect Windows 4
Permissions: PermitAccess AND Marketing
```

5. Regla de la autorización para el acceso del 802.1x que asigna SGT = 2 (finanzas)

Navegue a la **directiva > a la autorización** y cree una regla para el acceso del 802.1x. El supplicant que termina la sesión del 802.1x sobre el 3750 Switch con el nombre de usuario cisco conseguirá el acceso total (PermitAccess) y será asignado la etiqueta 2 (finanzas) SGT.

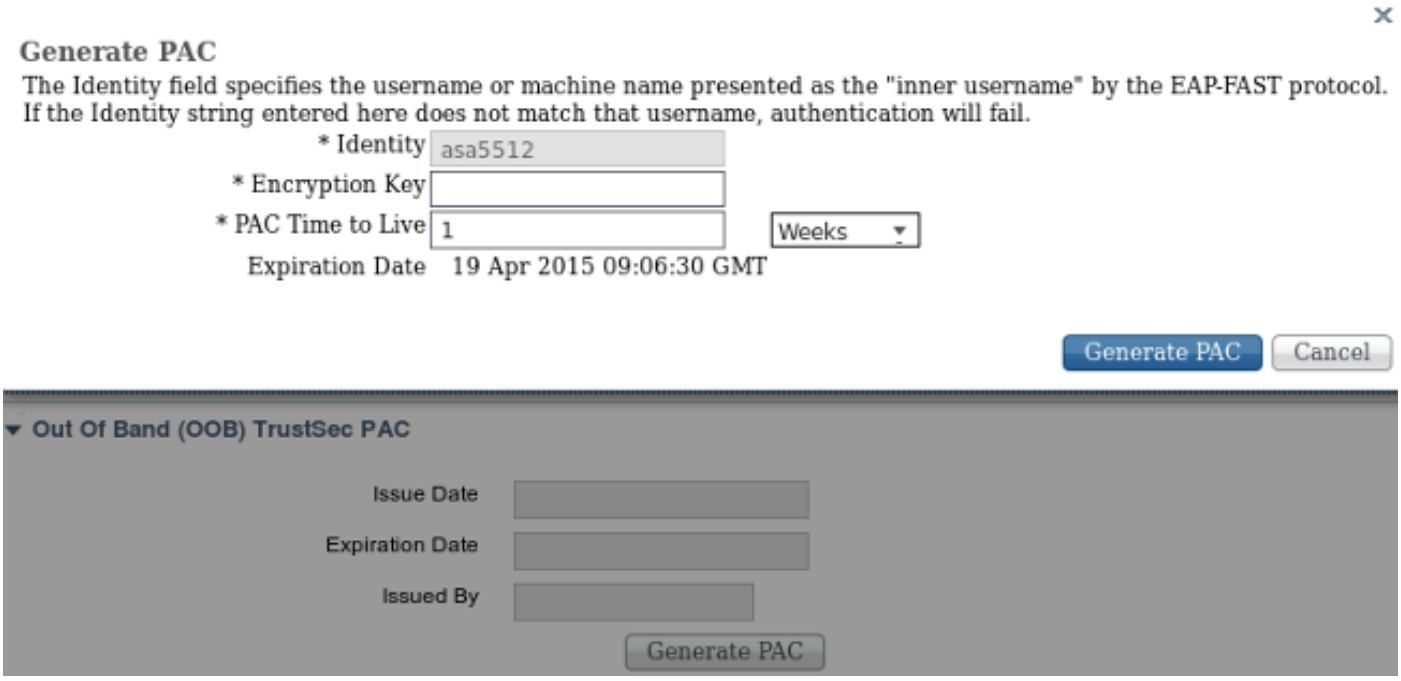
```
Rule name: 802.1x
```

```
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance
```

6. Agregando el dispositivo de red, generando el PAC para el ASA

Para agregar el ASA al dominio de TrustSec, es necesario generar el archivo PAC manualmente. Ese archivo se importa en el ASA.

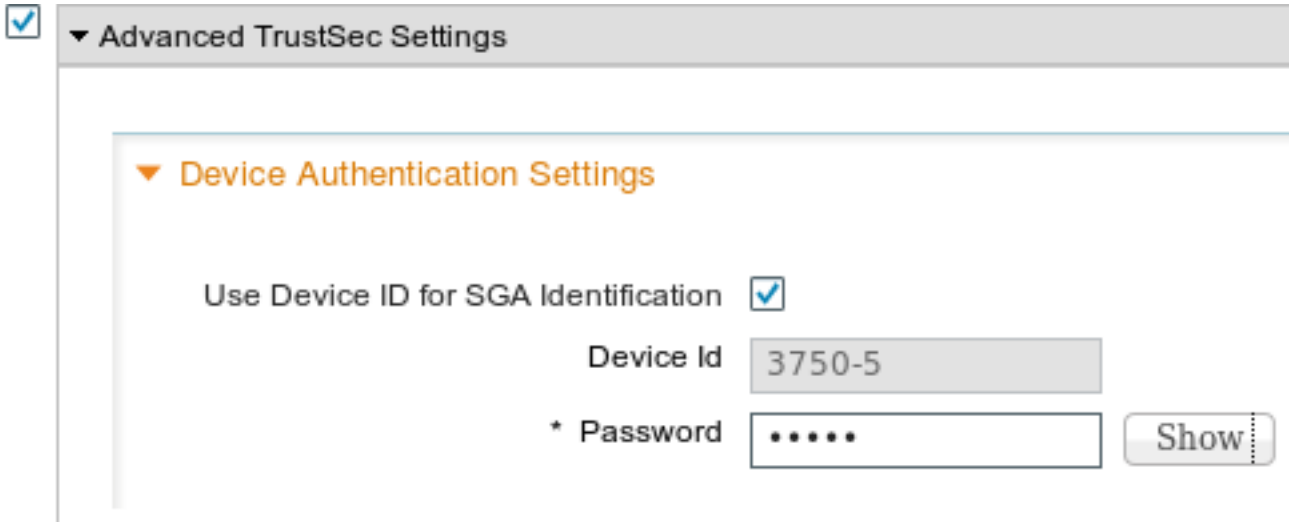
Se puede configurar desde **Administration (Administración) > Network Devices (Dispositivos de red)**. Después de que se agregue el ASA, navegue hacia abajo a las **configuraciones de TrustSec** y **genere el PAC** tal y como se muestra en de esta imagen.



El Switches (3750X) soporta el aprovisionamiento automático PAC, de modo que los pasos necesiten ser ejecutados solamente para el ASA que soporta solamente el aprovisionamiento manual PAC.

7. Agregue el dispositivo de red, secreto de la configuración para el aprovisionamiento automático del Switch PAC

Para el Switch que utiliza el aprovisionamiento automático PAC, un secreto correcto se debe fijar, tal y como se muestra en de esta imagen.



Note: El PAC se utiliza para autenticar el ISE y para descargar los datos del entorno (eg. SGT) junto con la directiva (ACL). El ASA soporta solamente los datos del entorno, las directivas necesita ser configurado manualmente en el ASA. El ® del Cisco IOS soporta ambos, así que las directivas se pueden descargar del ISE.

ASA - Pasos de configuración

1. Acceso básico VPN

Configure el acceso básico SSL VPN para AnyConnect usando el ISE para la autenticación.

```
Rule name: 802.1x
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance
```

2. Importe el PAC y habilite los cts

Importe el PAC generado para el ASA (del paso 6 de la configuración ISE). Utilice la misma clave de encripción:

```
BSNS-ASA5512-4# cts import-pac http://10.229.20.86/asa5512.pac password ciscocisco
PAC Imported Successfully
```

Para verificar:

```
BSNS-ASA5512-4# show cts pac

 PAC-Info:
   Valid until: Apr 11 2016 10:16:41
   AID:         c2dcb10f6e5474529815aed11ed981bc
   I-ID:        asa5512
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b000030001000400010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
```

```
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

Cts del permiso:

```
BSNS-ASA5512-4# show cts pac

 PAC-Info:
   Valid until: Apr 11 2016 10:16:41
   AID:         c2dcb10f6e5474529815aed11ed981bc
   I-ID:        asa5512
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

Después de que usted habilite los cts, el ASA debe descargar los datos del entorno del ISE:

```
BSNS-ASA5512-4# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          10:21:41 UTC Apr 11 2015
Env-data expires in:       0:00:37:31 (dd:hr:mm:sec)
Env-data refreshes in:     0:00:27:31 (dd:hr:mm:sec)
```

3. SGACL para las finanzas > el márketing del tráfico

Configuración SGACL en la interfaz interior. El ACL permite iniciar solamente el tráfico ICMP de las finanzas a la comercialización.

```
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
access-group inside in interface inside
```

El ASA debe ampliar el nombre de la etiqueta para numerar:

```
BSNS-ASA5512-4(config)# show access-list inside
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=47) 0x5633b153
```

4. Cts del permiso en la interfaz interior

Después de que usted habilite los cts en la interfaz interior del ASA:

```
interface GigabitEthernet0/1
 nameif inside
cts manual
  policy static sgt 100 trusted
 security-level 100
 ip address 192.168.1.100 255.255.255.0
```

El ASA puede enviar y recibir las tramas de TrustSec (tramas Ethernet con el campo del CMD). El ASA asume que todas las tramas del ingreso sin una etiqueta se deben tratar como con la etiqueta 100. Todas las tramas del ingreso que incluyen ya la etiqueta serán confiadas en.

Pasos de la configuración del switch

1. 802.1x básico

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

Con esa configuración, después de que sea acertado la autorización del 802.1x el usuario (autorizado vía el ISE) se debe asignar la etiqueta 2 (finanzas).

2. Configuración y aprovisionamiento CTS

Semejantemente, en cuanto al ASA, se configuran los cts y punta al ISE:

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

También, la aplicación se habilita para Layer3 y Layer2 (todo el vlans):

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius
```

```
dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

Para provision el PAC automáticamente:

```
bsns-3750-5#cts credentials id 3750-5 password ciscocisco
```

Una vez más la contraseña debe hacer juego con la configuración correspondiente en ISE (**dispositivo de red > Switch> TrustSec**). Ahora, el ® del Cisco IOS inicia la sesión del EAP-FAST con el ISE para conseguir el PAC. Más detalle en ese proceso se puede encontrar aquí:

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

Para verificar si el PAC está instalado:

```
bsns-3750-5#show cts pacs
 AID: EA48096688D96EF7B94C679A17BDAD6F
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: EA48096688D96EF7B94C679A17BDAD6F
   I-ID: 3750-5
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 14:41:24 CEST Jul 10 2015
 PAC-Opaque:
000200B000030001000400010EA48096688D96EF7B94C679A17BDAD6F000600940003010036 5AB3133998C86C1BA1B418
968C6069000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
 Refresh timer is set for 4y14w
```

3. Cts del permiso en la interfaz al ASA

```
interface GigabitEthernet1/0/39
 switchport access vlan 10
 switchport mode access
 cts manual
  policy static sgt 101 trusted
```

De ahora en adelante, el Switch debe estar listo para procesar y para enviar las tramas de TrustSec y para aplicar las directivas descargadas del ISE.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La verificación se cubre en las secciones individuales de este documento.

Troubleshooting

Asignación SGT

Después de que establezcan a la sesión de VPN al ASA, la asignación correcta SGT debe ser confirmada:

```
BSNS-ASA5512-4# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 13
Assigned IP  : 192.168.100.50         Public IP    : 10.229.20.86
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10308                  Bytes Rx     : 10772
Group Policy : TAC                    Tunnel Group : TAC
Login Time   : 15:00:13 UTC Mon Apr 13 2015
Duration     : 0h:00m:25s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801640000d000552bd9fd
Security Grp : 3:Marketing
```

Según la autorización gobierna en el ISE, todos los usuarios AnyConnect4 se ha asignado a la etiqueta del márketing.

Lo mismo con la sesión del 802.1x sobre el Switch. Después de que los finales del módulo Network Analysis Modules de AnyConnect (NAM), Switch de la autenticación apliquen la etiqueta correcta vuelta del ISE:

```
bsns-3750-5#show authentication sessions interface g1/0/2 details
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
        IPv6 Address:  Unknown
        IPv4 Address:  192.168.1.203
           User-Name:  cisco
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A30426D000000130001B278
     Acct Session ID:  Unknown
              Handle:  0x53000002
      Current Policy:  POLICY_Gi1/0/2

Local Policies:
       Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:
```

```
          SGT Value:  2

Method status list:
      Method           State
      dot1x            Authc Success
      mab              Stopped
```

Según la autorización gobierna en el ISE, todos los usuarios conectados con ese Switch debe ser asignado a SGT = 2 (las finanzas).

Aplicación en el ASA

Cuando usted intenta enviar un tráfico de las finanzas (192.168.1.203) a la comercialización (192.168.100.50), golpea la interfaz interior del ASA. Para el pedido de eco ICMP, crea la sesión:

```
Built outbound ICMP connection for faddr 192.168.100.50/0(LOCAL\cisco, 3:Marketing) gaddr
192.168.1.203/1 laddr 192.168.1.203/1(2)
```

y aumenta los contadores ACL:

```
BSNS-ASA5512-4(config)# sh access-list

access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=138)
```

Eso se puede también confirmar mirando a las capturas de paquetes. Observe que las etiquetas correctas están visualizadas:

```
BSNS-ASA5512-4(config)# capture CAP interface inside
BSNS-ASA5512-4(config)# show capture CAP

  1: 15:13:05.736793       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  2: 15:13:05.772237       INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
  3: 15:13:10.737236       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  4: 15:13:10.772726       INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
```

Hay pedido de eco ICMP entrante marcado con etiqueta con SGT = 2 (las finanzas) y entonces una respuesta del usuario de VPN con quien es marcado con etiqueta por el ASA SGT = 3 (márketing). Otra herramienta de Troubleshooting, paquete-trazalíneas es también TrustSec listo.

Desafortunadamente, el 802.1x PC no ve esa respuesta porque ha bloqueado por RBACL apátrida en el Switch (explicación en la siguiente sección).

Otra herramienta de Troubleshooting, paquete-trazalíneas es también TrustSec listo. Confirmemos si los paquetes icmp entrantes de las finanzas son validados:

```
BSNS-ASA5512-4# packet-tracer input inside icmp inline-tag 2 192.168.1.203 8 0 192.168.100.50
Mapping security-group 3:Marketing to IP address 192.168.100.50

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.48.66.1 using egress ifc  outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
Additional Information:

<some output omitted for clarity>

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4830, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: allow
```

También intentemos iniciar cualquier conexión TCP de las finanzas a la comercialización, eso debe ser bloqueado por el ASA:

```
Deny tcp src inside:192.168.1.203/49236 dst outside:192.168.100.50/445(LOCAL\cisco, 3:Marketing)
by access-group "inside" [0x0, 0x0]
```

Conmute la aplicación

Verifiquemos si el Switch ha descargado las directivas del ISE correctamente:

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:Finance to group Unknown:
       test_deny-30
```

```
IPv4 Role-based permissions from group 8 to group Unknown:
       permit_icmp-10
IPv4 Role-based permissions from group Unknown to group 2:Finance:
       test_deny-30
       Permit IP-00
IPv4 Role-based permissions from group 3:Marketing to group 2:Finance:
        telnet445-60
        Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

La directiva que controla el tráfico del márketing para financiar está instalada correctamente. Solamente tcp/445 se permite según RBACL:

```
bsns-3750-5#show cts rbacl telnet445
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
 name   = telnet445-60
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   permit tcp dst eq 445
```

Ésa es la razón por la que se ha caído la respuesta del eco ICMP que viene del márketing financiar. Eso puede ser confirmada marcando los contadores para el tráfico de SGT 3 a SGT 2:

```
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

*       *       0               0               223613          3645233

0       2       0               0               0               122

3       2       0               65              0               0

2       0       0               0               179             0

8       0       0               0               0               0
```

Los paquetes han sido caídos por el hardware (el contador actual es 65 y aumento de cada 1 segundo).

¿Qué si la conexión tcp/445 se inicia del márketing?

El ASA admite que (valida todo el tráfico VPN debido a la “conexión permiso-VPN del sysopt”):

```
Built inbound TCP connection 4773 for outside:192.168.100.50/49181
(192.168.100.50/49181)(LOCAL\cisco, 3:Marketing) to inside:192.168.1.203/445 (192.168.1.203/445)
(cisco)
```

Se crea la sesión correcta:

```
BSNS-ASA5512-4(config)#  show conn all | i 192.168.100.50
TCP outside  192.168.100.50:49181 inside  192.168.1.203:445, idle 0:00:51, bytes 0, flags UB
```

Y, el ® del Cisco IOS la valida puesto que hace juego telnet445 RBACL. Los aumentos correctos de los contadores:

```
bsns-3750-5#show cts role-based counters from 3 to 2
3       2       0               65              0               3
```

(la columna más reciente es tráfico permitido por el hardware). Se permite la sesión.

Este ejemplo se presenta a propósito para mostrar la diferencia en las directivas configuración y aplicación de TrustSec en el ASA y el ® del Cisco IOS. Sea consciente de las diferencias de las directivas del ® del Cisco IOS descargadas de ISE (RBACL apátrida) y del Firewall basado zona stateful enterada de TrustSec.

Información Relacionada

- Ejemplo de Configuración de la Postura VPN de ASA Versión 9.2.1 con ISE
- Ejemplo de configuración TrustSec de ASA y el Switch Catalyst Serie 3750X y guía de solución de problemas
- Guía de configuraicón del Switch Cisco TrustSec Comprensión Cisco TrustSec
- Configuración de un servidor externo para la autorización de usuario de dispositivo de seguridad
- Guía de configuración CLI VPN Cisco Serie ASA, 9.1
- Guía de usuario de Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems