Ejemplo de Configuración de TrustSec Cloud con 802.1x MACsec en Catalyst 3750X Series Switch

Contenido

Introducción

En este artículo se describen los pasos necesarios para configurar una nube Cisco TrustSec (CTS) con cifrado de enlaces entre dos switches Catalyst serie 3750X (3750X).

En este artículo se explica el proceso de cifrado de la seguridad de control de acceso a los medios (MACsec) de switch a switch que utiliza el protocolo de asociación de seguridad (SAP). Este proceso utiliza el modo IEEE 802.1x en lugar del modo manual.

A continuación se muestra una lista de los pasos necesarios:

- Aprovisionamiento de credenciales de acceso protegido (PAC) para dispositivos semilla y no semilla
- Autenticación mediante Network Device Admission Control (NDAC) y negociación MACsec con SAP para la gestión de claves
- Actualización de políticas y entorno

- Autenticación de puertos para clientes
- Etiquetado del tráfico con la etiqueta de grupo de seguridad (SGT)
- Aplicación de políticas con la ACL del grupo de seguridad (SGACL)

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de los componentes de CTS
- Conocimientos básicos sobre la configuración CLI de los switches Catalyst
- Experiencia con la configuración de Identity Services Engine (ISE)

Componentes Utilizados

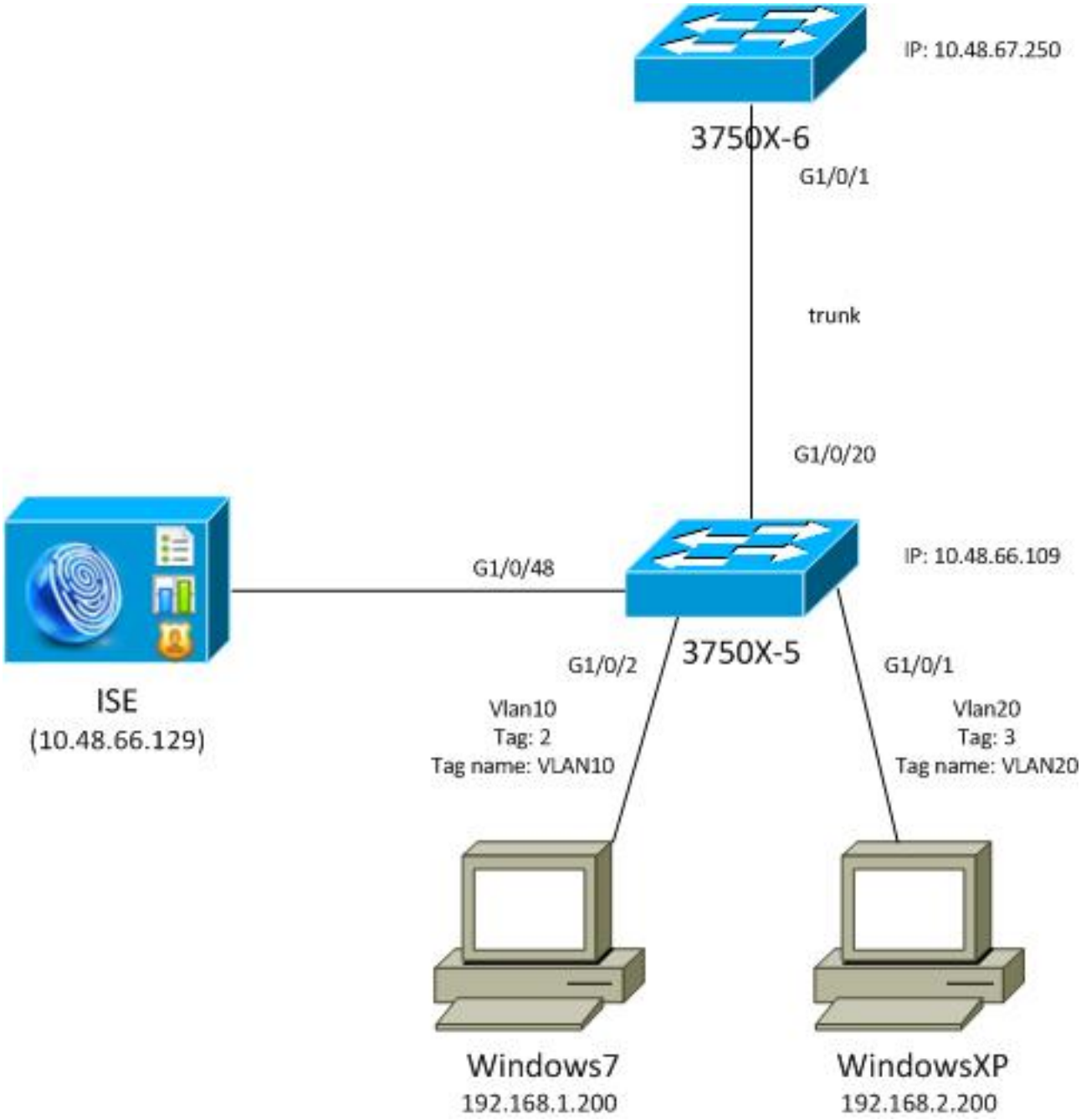
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft (MS) Windows 7 y MS Windows XP
- Software 3750X, versiones 15.0 y posteriores
- Software 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



En este diagrama de topología de red, el switch 3750X-5 es el dispositivo inicial que conoce la dirección IP de ISE y descarga automáticamente la PAC que se utiliza para la autenticación posterior en la nube de CTS. El dispositivo inicial actúa como un autenticador 802.1x para los dispositivos no iniciales. El switch Catalyst de Cisco serie 3750X-6 (3750X-6) es el dispositivo no simiente. Actúa como suplicante de 802.1x para el dispositivo inicial. Una vez que el dispositivo no simiente se autentica en ISE a través del dispositivo simiente, se le permite acceder a la nube CTS. Después de una autenticación exitosa, el estado del puerto 802.1x en el switch 3750X-5 cambia a **autenticado** y se negocia el cifrado MACsec. El tráfico entre los switches se etiqueta con SGT y se cifra.

Esta lista resume el flujo de tráfico esperado:

- El modelo simiente 3750X-5 se conecta a ISE y descarga la PAC, que se utiliza posteriormente para realizar una actualización de políticas y entorno.
- El modelo 3750X-6 no simiente realiza la autenticación 802.1x con la función de suplicante para autenticar/autorizar y descargar la PAC de ISE.
- El 3750X-6 realiza una segunda sesión de Protocolo de autenticación extensible 802.1x-

Autenticación flexible a través de protocolo seguro (EAP-FAST) para autenticarse con el túnel protegido basado en la PAC.
- El 3750X-5 descarga las políticas de SGA para sí mismo y en nombre del 3750X-6.
- Se produce una sesión SAP entre los 3750X-5 y 3750X-6, se negocian los cifrados MACsec y se intercambia la política.
- El tráfico entre los switches se etiqueta y se cifra.

Configuración de switches semilla y no semilla

El dispositivo generador (3750X-5) se configura para utilizar ISE como servidor RADIUS para CTS:

```
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

cts authorization list ise

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
```

La aplicación de la lista de control de acceso basado en roles (RBACL) y la lista de control de acceso basado en grupos de seguridad (SGACL) están habilitadas (se utilizan más adelante):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

El dispositivo no simiente (3750X-6) está configurado sólo para autenticación, autorización y administración de cuentas (AAA) sin necesidad de autorización RADIUS o CTS:

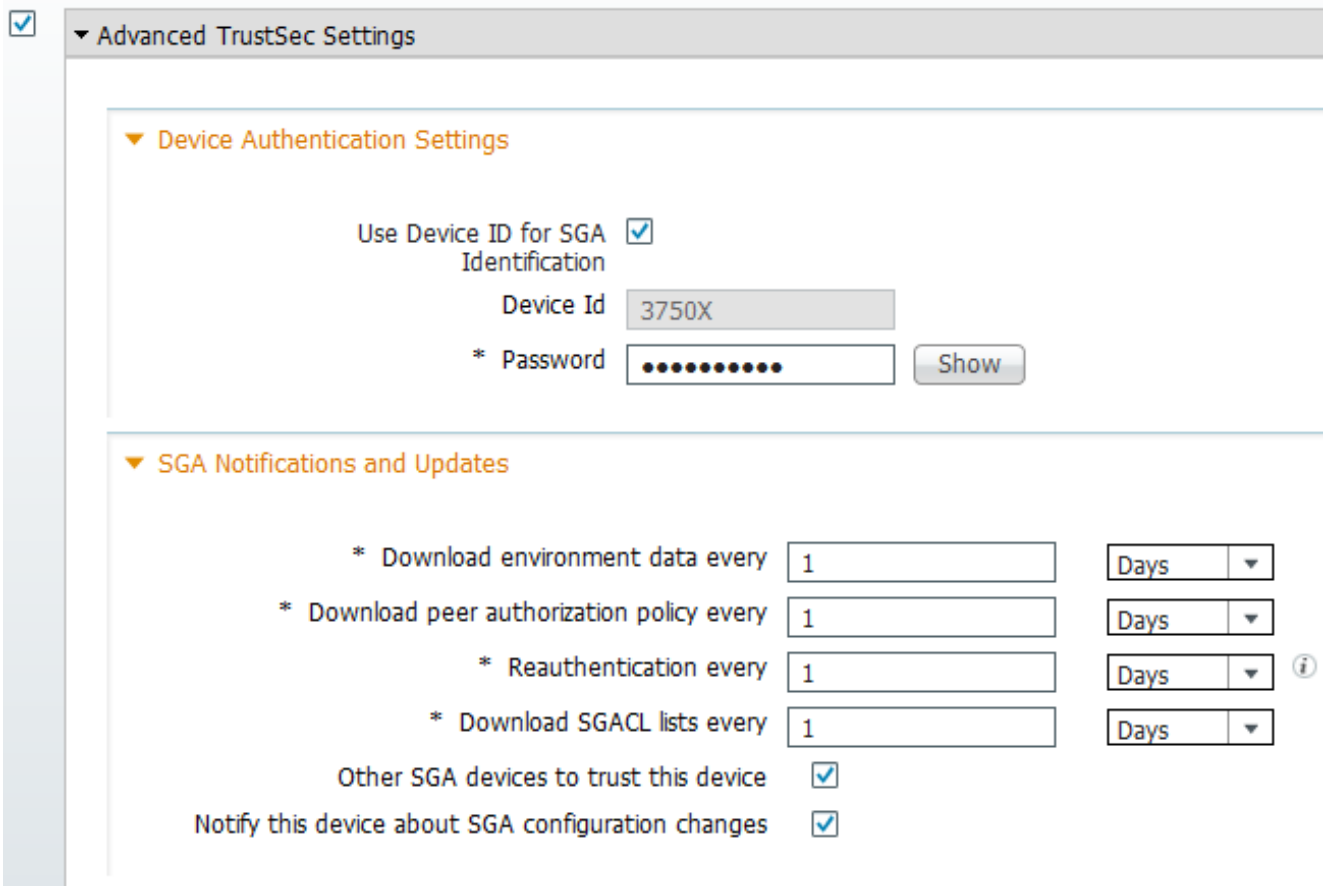
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Antes de activar 802.1x en la interfaz, es necesario configurar ISE.

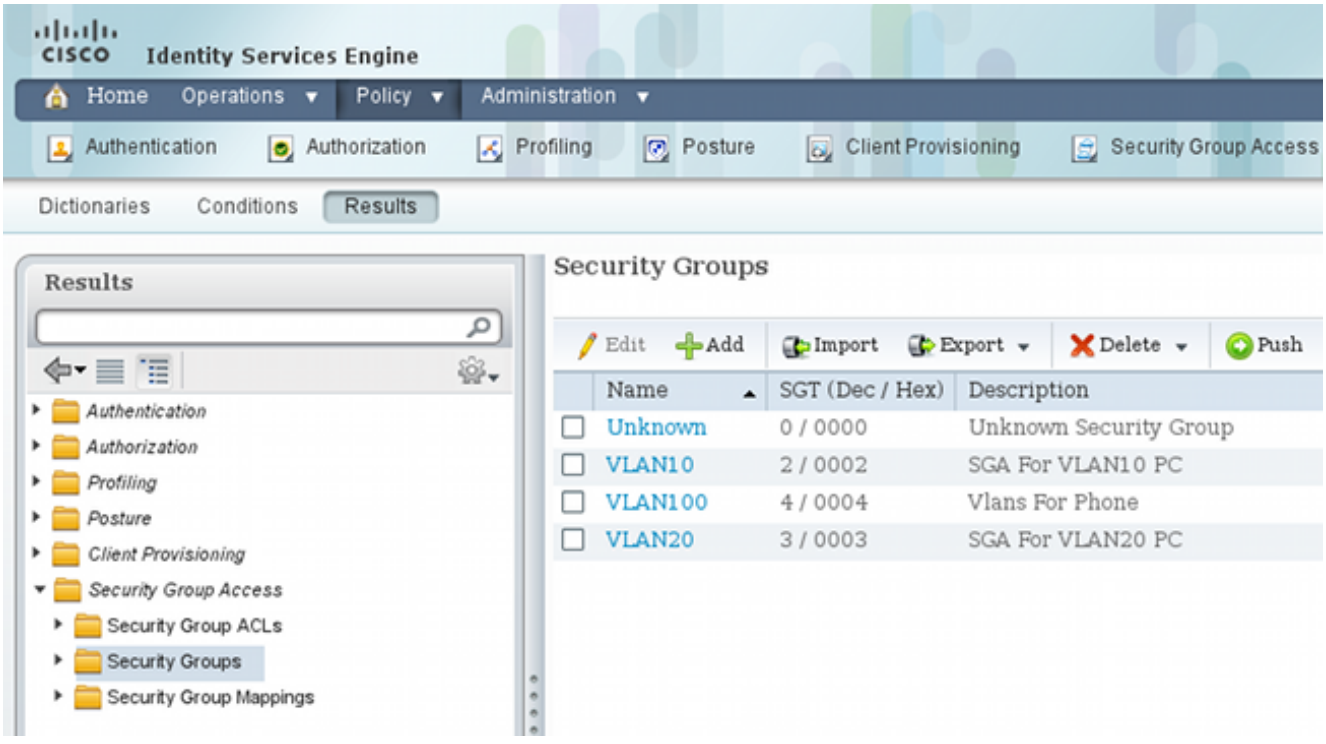
Configuración de ISE

Complete estos pasos para configurar el ISE:

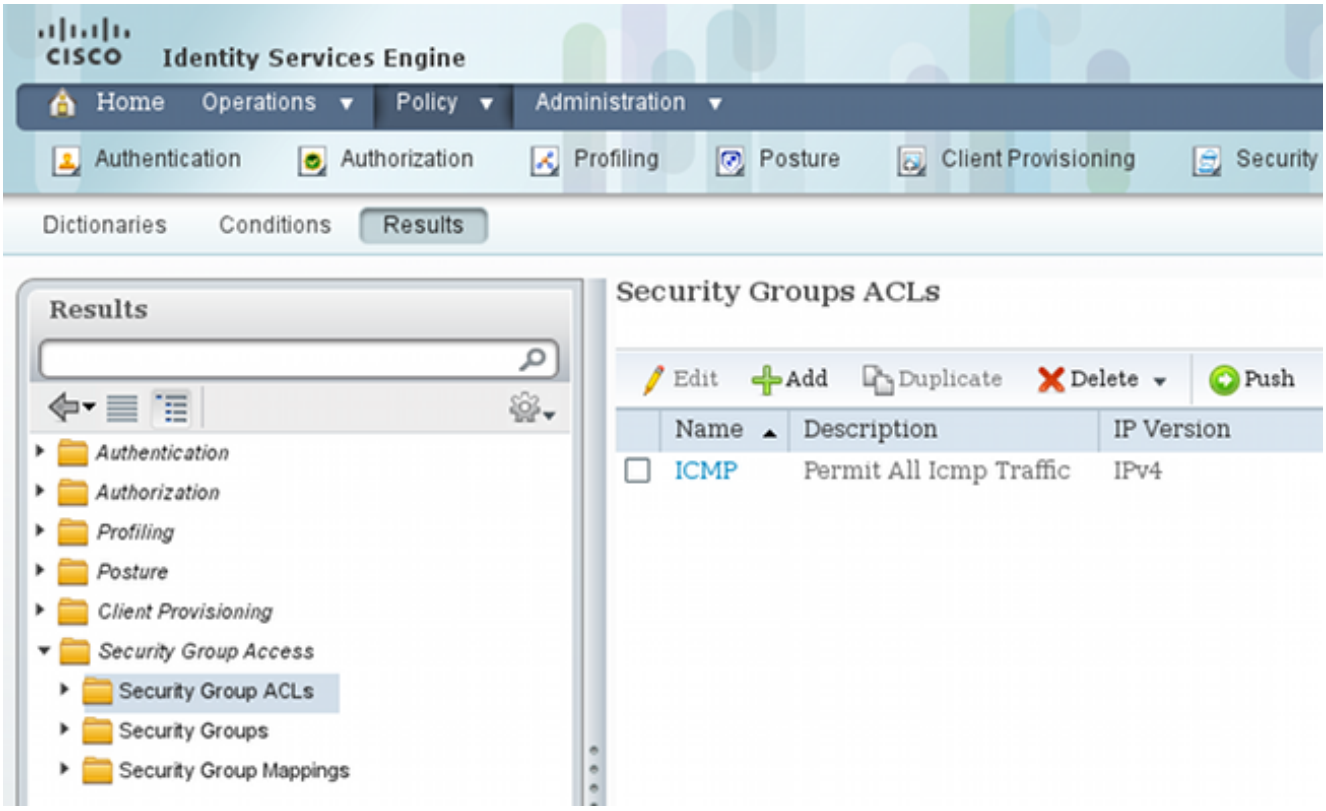
1. Vaya a **Administration > Network Resources > Network Devices**, y agregue ambos switches como Network Access Devices (NAD). En **Advanced TrustSec Settings**, configure una contraseña CTS para su uso posterior en la CLI del switch.



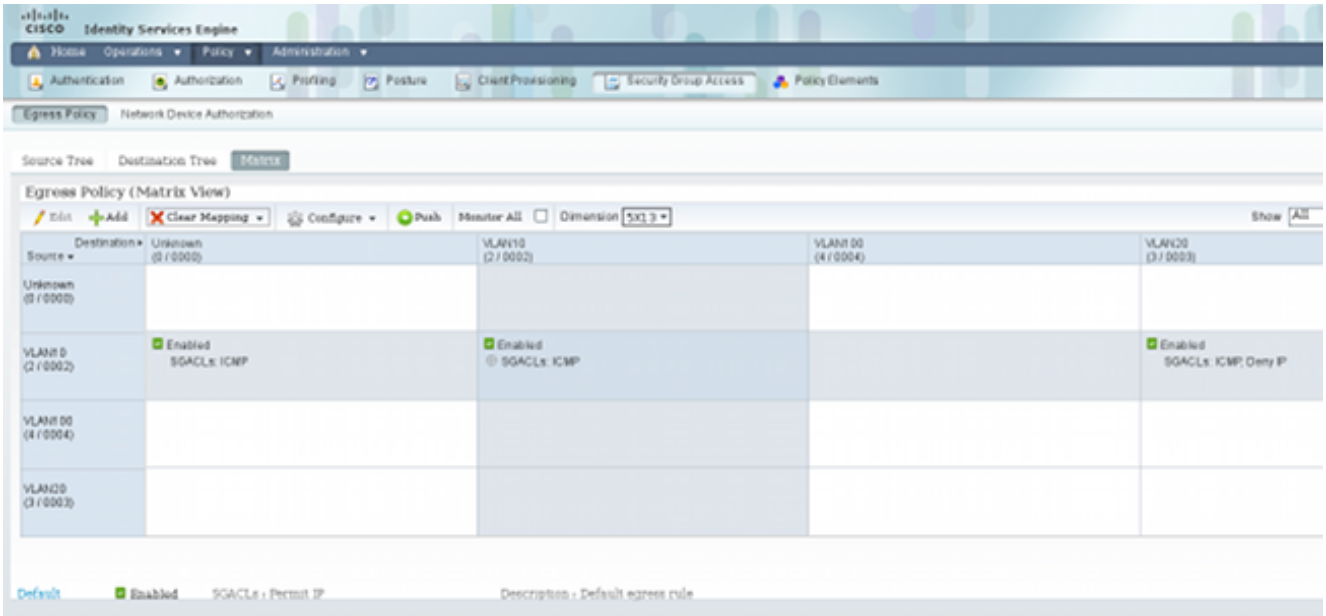
2. Navegue hasta **Política > Elementos de política > Resultados > Acceso de grupo de seguridad > Grupos de seguridad**, y agregue las SGT apropiadas. Estas etiquetas se descargan cuando los switches solicitan una actualización del entorno.



3. Vaya a **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**, y configure una SGACL.



4. Navegue hasta **Policy > Security Group Access**, y defina una política con la matriz.



Nota: Debe configurar la directiva de autorización para el solicitante de MS Windows, de modo que reciba la etiqueta correcta. Consulte el Ejemplo de Configuración de TrustSec de ASA y Catalyst 3750X Series Switch y la Guía de Troubleshooting para obtener una configuración detallada para esto.

Aprovisionamiento de PAC para el 3750X-5

La PAC es necesaria para la autenticación en el dominio CTS (como fase 1 para EAP-FAST) y también se utiliza para obtener datos de entorno y políticas de ISE. Sin la PAC correcta, no es

posible obtener esos datos de ISE.

Después de proporcionar las credenciales correctas en el 3750X-5, descarga la PAC:

```
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: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

La PAC se descarga mediante EAP-FAST con el protocolo de autenticación por desafío mutuo de Microsoft (MSCHAPv2), con las credenciales proporcionadas en CLI y las mismas credenciales configuradas en ISE.

La PAC se utiliza para la actualización del entorno y la política. Para esos switches, utilice las solicitudes RADIUS con **cisco av-pair cts-pac-opaque**, que se deriva de la clave PAC y se puede descifrar en ISE.

Aprovisionamiento de PAC para los modelos 3750X-6 y autenticación NDAC

Para que un nuevo dispositivo pueda conectarse al dominio CTS, es necesario habilitar 802.1x en los puertos correspondientes.

El protocolo SAP se utiliza para la administración de claves y la negociación de conjuntos de cifrado. El código de autenticación de mensajes Galois (GMAC) se utiliza para la autenticación y el modo Galois/Counter (GCM) para el cifrado.

En el interruptor simiente:

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

En el switch no simiente:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

Esto se soporta solamente en los puertos trunk (switch-switch MACsec). Para MACsec host de

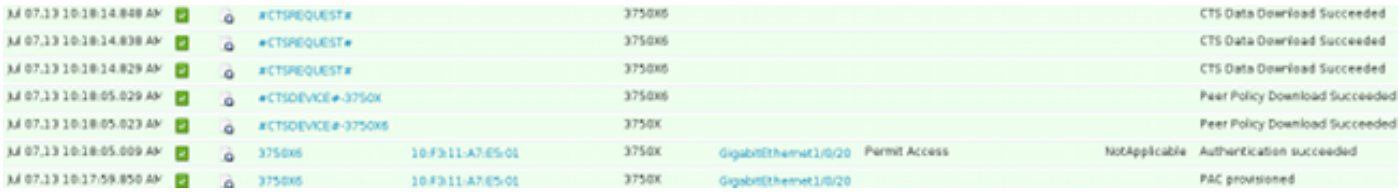
switch, que utiliza el protocolo MACsec Key Agreement (MKA) en lugar de SAP, consulte Configuración del cifrado MACsec.

Inmediatamente después de habilitar 802.1x en los puertos, el switch no simiente actúa como suplicante del switch simiente, que es el autenticador.

Este proceso se denomina NDAC y su objetivo es conectar un nuevo dispositivo al dominio CTS. La autenticación es bidireccional; el nuevo dispositivo tiene credenciales que se verifican en el servidor de autenticación ISE. Después del aprovisionamiento de PAC, el dispositivo también está seguro de que se conecta al dominio CTS.

> **Nota**: PAC se utiliza para crear un túnel de seguridad de la capa de transporte (TLS) para EAP-FAST. El 3750X-6 confía en las credenciales PAC proporcionadas por el servidor de manera similar a como un cliente confía en el certificado proporcionado por el servidor para el túnel TLS para el método EAP-TLS.

Se intercambian varios mensajes RADIUS:



La primera sesión del 3750X (switch de inicialización) se utiliza para el aprovisionamiento de PAC. EAP-FAST se utiliza sin PAC (se crea un túnel anónimo para la autenticación MSCHAPv2).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

Se utiliza el nombre de usuario y la contraseña de MSCHAPv2 configurados mediante el comando **cts credentials**. Además, un rechazo de acceso RADIUS se devuelve al final, porque después de que PAC ya se haya aprovisionado, no se necesita más autenticación.

La segunda entrada del registro hace referencia a la autenticación 802.1x. EAP-FAST se utiliza con la PAC suministrada anteriormente.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

Esta vez, el túnel no es anónimo, sino que está protegido por PAC. De nuevo, se utilizan las mismas credenciales para la sesión MSCHAPv2. A continuación, se verifica con respecto a las reglas de autenticación y autorización en ISE y se devuelve una aceptación de acceso RADIUS. Luego, el switch autenticador aplica los atributos devueltos y la sesión 802.1x para ese puerto pasa a un estado autorizado.

¿Cómo es el proceso de las dos primeras sesiones de 802.1x desde el switch inicial?

Estas son las depuraciones más importantes de la semilla. La simiente detecta que el puerto está activo e intenta determinar qué rol se debe utilizar para 802.1x: el suplicante o el autenticador:

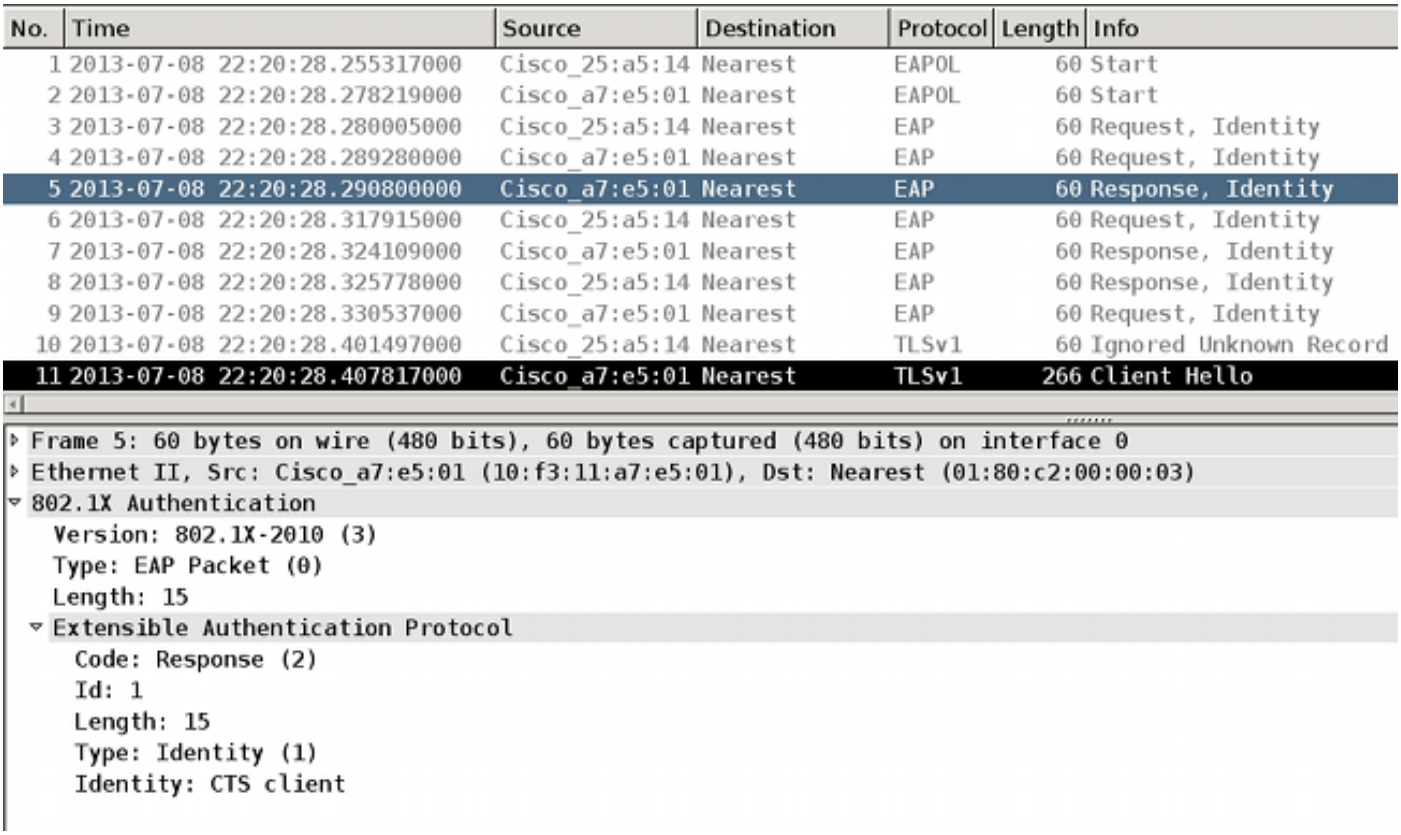
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

Por último, se utiliza la función de autenticador, ya que el switch tiene acceso a ISE. En el 3750X-6, se elige la función de suplicante.

Detalles sobre la selección de roles de 802.1x

> **Nota**: Una vez que el switch solicitante obtiene la PAC y está autenticado con 802.1x, descarga los datos del entorno (descritos más adelante) y aprende la dirección IP del servidor AAA. En este ejemplo, ambos switches tienen una conexión dedicada (de red troncal) para ISE. Posteriormente, los roles pueden ser diferentes; el primer switch que recibe una respuesta del servidor AAA se convierte en el autenticador, y el segundo se convierte en el solicitante.

Esto es posible porque ambos switches con el servidor AAA marcado como ALIVE envían una identidad de solicitud de protocolo de autenticación extensible (EAP). El primero que recibe la respuesta de identidad EAP se convierte en el autenticador y descarta las solicitudes de identidad subsiguientes.



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

Después de seleccionar el rol 802.1x (en este escenario, el 3750X-6 es el suplicante, porque aún no tiene acceso al servidor AAA), los siguientes paquetes implican el intercambio EAP-FAST para el aprovisionamiento de PAC. El nombre de usuario **CTS client** se utiliza para el nombre de usuario de solicitud RADIUS y como la identidad EAP:

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12   "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

Después de que se construya el túnel anónimo EAP-FAST, se produce una sesión MSCHAPv2 para el nombre de usuario **3750X6** (**credenciales cts**). No se puede ver en el switch, porque es un túnel TLS (cifrado), pero los registros detallados de ISE para el aprovisionamiento de PAC lo demuestran. Puede ver **CTS Client** para el nombre de usuario RADIUS y como la respuesta de identidad EAP. Sin embargo, para el método interno (MSCHAP), se utiliza el nombre de usuario **3750X6**:

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

Se produce la segunda autenticación EAP-FAST. Esta vez, utiliza la PAC que se suministró anteriormente. De nuevo, el **cliente CTS** se utiliza como nombre de usuario RADIUS e identidad externa, pero **3750X6** se utiliza para la identidad interna (MSCHAP). Autenticación correcta:

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Sin embargo, esta vez, ISE devuelve varios atributos en el paquete de aceptación de RADIUS:

Authentication Result

```
User-Name=3750X6
 State=ReauthSession:C0A800010000053A33FD79AF
 Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
 Session-Timeout=86400
 Termination-Action=RADIUS-Request
 EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
 cisco-av-pair=cts:security-group-tag=0000-01
 cisco-av-pair=cts:supplicant-cts-capabilities=sap
 MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
 MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

Aquí, el switch autenticador cambia el puerto al estado autorizado:

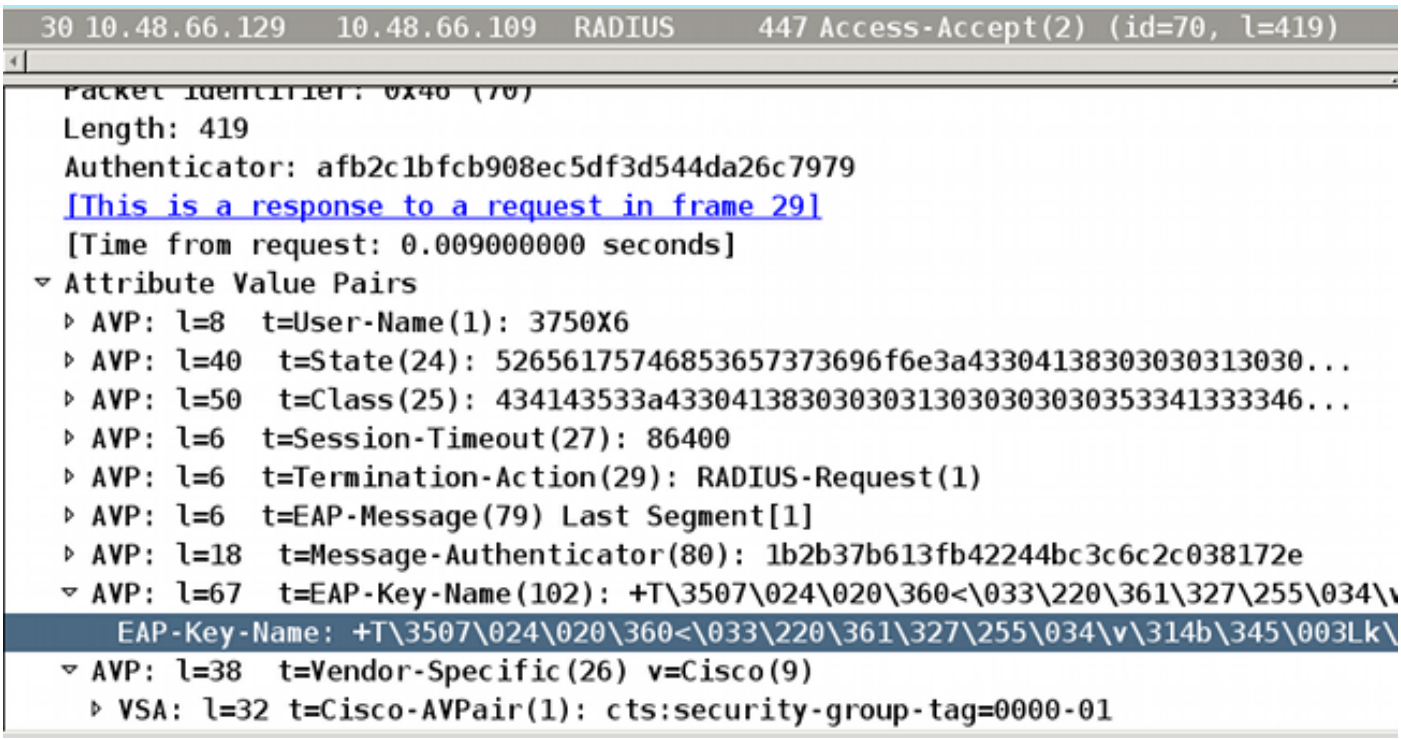
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
                Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

¿Cómo aprende el switch autenticador que el nombre de usuario es **3750X6**? Para el nombre de usuario RADIUS y la identidad EAP externa, se utiliza el **cliente CTS** y la identidad interna se cifra

y no es visible para el autenticador. ISE aprende el nombre de usuario. El último paquete RADIUS (Access-Accept) contiene **username=3750X6**, mientras que todos los demás contenían **username = cliente Cts**. Esta es la razón por la que el switch solicitante reconoce el nombre de usuario real. Este comportamiento es compatible con RFC. Desde la sección 3.0 de RFC3579:

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

En el último paquete de la sesión de autenticación 802.1x, el ISE devuelve un mensaje de aceptación RADIUS **cisco-av-pair** con el **EAP-Key-Name**:

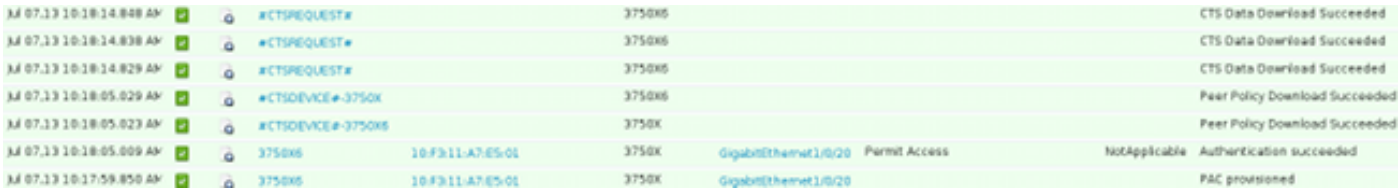


Se utiliza como material de claves para la negociación SAP.

Además, se pasa el SGT. Esto significa que el switch autenticador etiqueta el tráfico del solicitante con un **valor predeterminado = 0**. Puede configurar un valor específico en ISE para que devuelva cualquier otro valor. Esto solo se aplica al tráfico sin etiqueta; el tráfico etiquetado no se reescribe porque, de forma predeterminada, el switch autenticador confía en el tráfico del solicitante autenticado (pero esto también se puede cambiar en ISE).

Descarga de políticas de SGA

Existen intercambios RADIUS adicionales (sin EAP) distintos de las dos primeras sesiones EAP-FAST 802.1x (la primera para el aprovisionamiento de PAC y la segunda para la autenticación). Estos son los registros de ISE de nuevo:



El tercer registro (**Peer Policy Download**) indica un intercambio RADIUS simple: Solicitud RADIUS

y aceptación RADIUS para el usuario **3760X6**. Esto es necesario para descargar las políticas para el tráfico del solicitante. Los dos atributos más importantes son:

```
▾ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

Debido a esto, el switch autenticador confía en el tráfico etiquetado SGT por el solicitante (**cts:trusted-device=true**), y también etiqueta el tráfico sin etiqueta con **tag=0**.

El cuarto registro indica el mismo intercambio RADIUS. Sin embargo, esta vez es para el usuario **3750X5** (autenticador). Esto se debe a que ambos pares deben tener una política para cada uno. Es interesante notar que el solicitante todavía no conoce la dirección IP del servidor AAA. Esta es la razón por la que el switch autenticador descarga la política en nombre del solicitante. Esta información se pasa posteriormente al solicitante (junto con la dirección IP de ISE) en la negociación SAP.

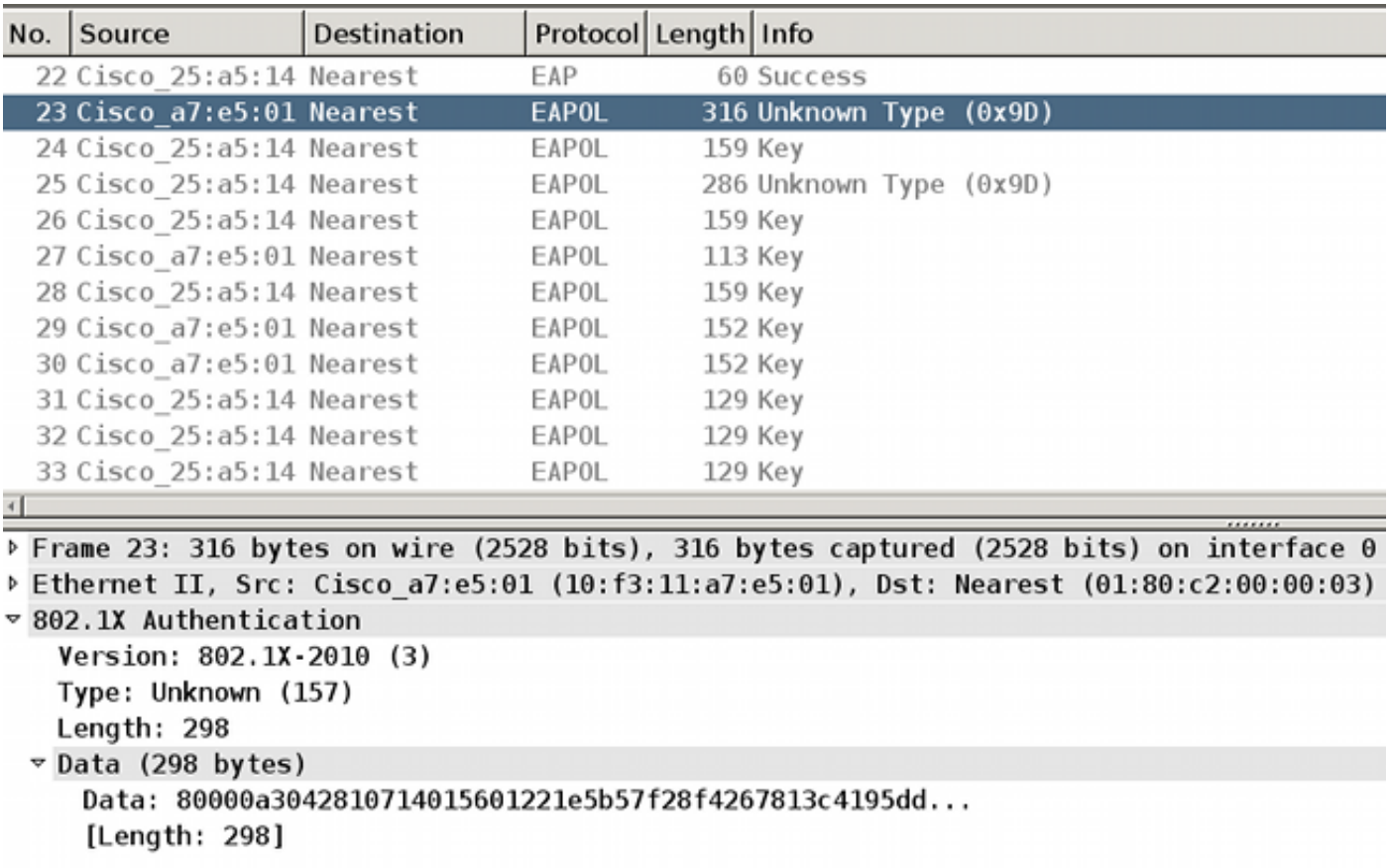
Negociación SAP

Inmediatamente después de que finalice la sesión de autenticación 802.1x, se produce la negociación SAP. Esta negociación es necesaria para:

- Negocie los niveles de cifrado (con el comando **sap mode-list gcm-encrypt**) y los conjuntos de cifrado
- Derivar claves de sesión para el tráfico de datos
- Someterse al proceso de cambio de clave
- Realice comprobaciones de seguridad adicionales y asegúrese de que los pasos anteriores están protegidos

SAP es un protocolo diseñado por Cisco Systems basado en una versión de borrador de 802.11i/D6.0. Para obtener más información, solicite acceso a la página Cisco TrustSec Security Association Protocol: protocolo compatible con Cisco Trusted Security para Cisco Nexus 7000.

SAP Exchange cumple con 802.1AE. Se produce un intercambio de claves de protocolo de autenticación extensible sobre LAN (EAPOL) entre el solicitante y el autenticador para negociar un conjunto de cifrado, intercambiar parámetros de seguridad y administrar claves. Desafortunadamente, Wireshark no tiene un decodificador para todos los tipos de EAP requeridos:



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

La finalización con éxito de estas tareas se traduce en el establecimiento de una asociación de seguridad (SA).

En el switch solicitante:

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
```

```
        authc success:              12
        authc reject:               1556
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                12
        sap fail:                   0
        authz success:              12
        authz fail:                 0
        port auth fail:             0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

En el autenticador:

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
```

```
        Peer ID               : unknown
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Aquí, los puertos utilizan el modo **gcm-encrypt**, lo que significa que el tráfico se autentica y se cifra, así como se etiqueta correctamente con SGT. Ninguno de los dos dispositivos utiliza ninguna política de autorización de dispositivos de red específica en el ISE, lo que significa que todo el tráfico iniciado desde el dispositivo utiliza la etiqueta predeterminada de **0**. Además, ambos switches confían en las SGT recibidas del par (debido a los atributos RADIUS de la fase de descarga de la política del par).

Actualización de entorno y política

Una vez conectados ambos dispositivos a la nube de CTS, se inicia una actualización de entorno y política. La actualización del entorno es necesaria para obtener las SGT y los nombres, y una actualización de la política para descargar la SGACL definida en ISE.

En esta etapa, el solicitante ya conoce la dirección IP del servidor AAA, por lo que puede hacerlo por sí mismo.

Consulte el Ejemplo de Configuración de TrustSec del Switch Catalyst serie 3750X y ASA y la Guía de Resolución de Problemas para obtener detalles sobre el entorno y la actualización de políticas.

El switch suplicante recuerda la dirección IP del servidor RADIUS, incluso cuando no hay ningún servidor RADIUS configurado y cuando el link CTS deja de funcionar (hacia el switch autenticador). Sin embargo, es posible forzar al switch a olvidarlo:

```
bsns-3750-6#show run | i radius
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-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

Para verificar el entorno y la política en el switch solicitante, ingrese estos comandos:

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

```
bsns-3750-6#show cts role-based permissions
```

¿Por qué no se muestra ninguna política? No se muestra ninguna política, porque debe habilitar **cts enforce** para aplicarlas:

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#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
```

¿Por qué el solicitante tiene solamente una política para **agrupar Desconocido** mientras que el autenticador tiene más?

```
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 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Autenticación de puertos para clientes

El cliente MS Windows está conectado y autenticado al puerto **g1/0/1** del switch 3750-5:

```
bsns-3750-5#show authentication sessions int 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:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


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

Aquí, el switch 3750-5 sabe que el tráfico de ese host debe etiquetarse con **SGT=3** cuando se envía a la nube CTS.

Etiquetado de tráfico con SGT

¿Cómo se olfatea y verifica el tráfico?

Esto es difícil porque:

- La captura de paquetes integrada sólo es compatible con el tráfico IP (y se trata de una trama Ethernet modificada con SGT y carga MACsec).
- Puerto del analizador de puerto conmutado (SPAN) con la palabra clave **replication** - esto podría funcionar, pero el problema es que cualquier PC con Wireshark conectado al puerto de destino de una sesión de monitoreo descarta las tramas debido a la falta de soporte de 802.1ae, lo que puede suceder en el nivel de hardware.
- El puerto SPAN sin la palabra clave **replication** quita el encabezado **cts** antes de colocarlo en un puerto de destino.

Aplicación de políticas con SGACL

La aplicación de políticas en la nube CTS siempre se realiza en el puerto de destino. Esto se debe a que solo el último dispositivo conoce la SGT de destino del dispositivo terminal que está conectado directamente a ese switch. El paquete sólo transporta la SGT de origen. Tanto la SGT de origen como la de destino son necesarias para tomar una decisión.

Este es el motivo por el que los dispositivos no necesitan descargar todas las políticas de ISE. En su lugar, solo necesitan la parte de la política relacionada con la SGT para la que el dispositivo tiene dispositivos conectados directamente.

Aquí está el 3750-6, que es el switch suplicante:

```
bsns-3750-6#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
```

Hay dos políticas aquí. El primero es el valor predeterminado para el tráfico sin etiqueta (hacia/desde). La segunda es de **SGT=2** a la SGT sin etiqueta, que es **0**. Esta política existe porque el dispositivo en sí utiliza la política SGA de ISE y pertenece a **SGT=0**. Además, **SGT=0** es una etiqueta predeterminada. Por lo tanto, debe descargar todas las políticas que tienen las reglas para el tráfico **hacia/desde SGT=0**. Si observa la matriz, sólo verá una de estas políticas: **de 2 a 0**.

Aquí está el 3750-5, que es el switch autenticador:

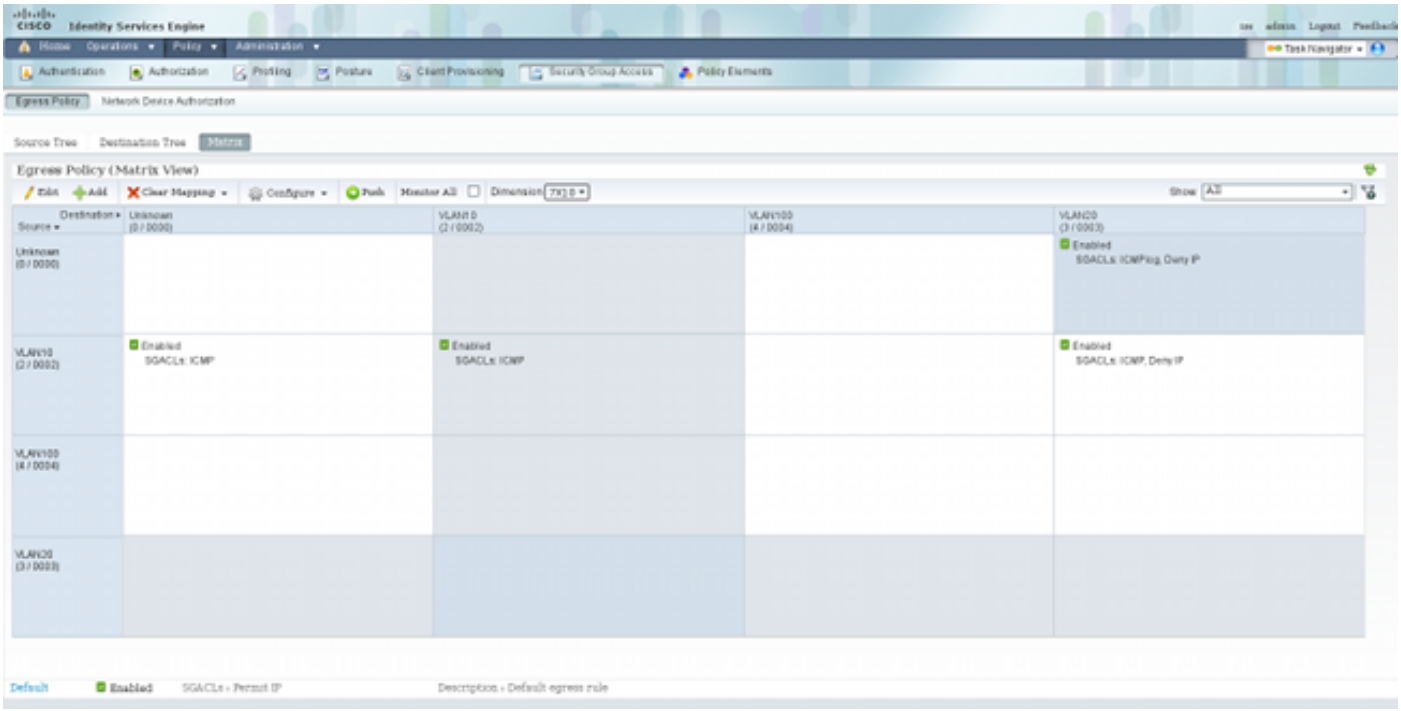
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Hay una política más aquí: **de 2 a 3**. Esto se debe a que el cliente 802.1x (MS Windows) está

conectado a **g1/0/1** y etiquetado con **SGT=3**. Es por esto que debe descargar todas las políticas **a SGT=3**.

Intente hacer ping desde 3750X-6 (**SGT=0**) a MS Windows XP (**SGT=3**). El 3750X-5 es el dispositivo de aplicación.

Antes de esto, debe configurar una política en el ISE para el tráfico de **SGT=0 a SGT=3**. Este ejemplo creó un registro de Protocolo de mensajes de control de Internet (ICMP) SGACL con solo la línea, **permit icmp log**, y lo utilizó en la matriz para el tráfico de **SGT=0 a SGT=3**:



A continuación se muestra una actualización de la política en el switch de aplicación y una verificación de la nueva política:

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

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 Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Para verificar que la Lista de control de acceso (ACL) se descarga desde ISE, ingrese este comando:

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

Para verificar que la ACL esté aplicada (soporte de hardware), ingrese este comando:

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name    = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
 flag    = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale   = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

Estos son los contadores antes de ICMP:

```
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               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

Aquí hay un ping de **SGT=0** (switch 3750-6) a MS Windows XP (**SGT=3**) y los contadores:

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

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               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

Estos son los contadores de ACL:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
```

```
    10 permit icmp log (5 matches)
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

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).