Ejemplo de Configuración de MACsec Switch-Host Encryption with Cisco AnyConnect and ISE

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para el cifrado de Seguridad de control de acceso a medios (MACsec) entre un suplicante 802.1x (Cisco AnyConnect Mobile Security) y un autenticador (switch). Cisco Identity Services Engines (ISE) se utiliza como servidor de políticas y autenticación.

MACsec está estandarizado en 802.1AE y es compatible con los switches SUP7E 3750X, 3560X y 4500 de Cisco. 802.1AE define el cifrado de enlaces en redes por cable que utilizan claves fuera de banda. Estas claves de cifrado se negocian con el protocolo MACsec Key Agreement (MKA), que se utiliza después de una autenticación 802.1x correcta. MKA está estandarizado en IEEE 802.1X-2010.

Un paquete se cifra solamente en el enlace entre el PC y el switch (cifrado punto a punto). El paquete recibido por el switch se descifra y se envía a través de enlaces ascendentes sin cifrar. Para cifrar la transmisión entre los switches, se recomienda el cifrado del switch. Para ese cifrado, se utiliza el protocolo de asociación de seguridad (SAP) para negociar y regenerar claves. SAP es un protocolo de acuerdo clave previo al estándar desarrollado por Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración 802.1x
- Conocimiento básico de la configuración CLI de switches Catalyst
- Experiencia con la configuración de ISE

Componentes Utilizados

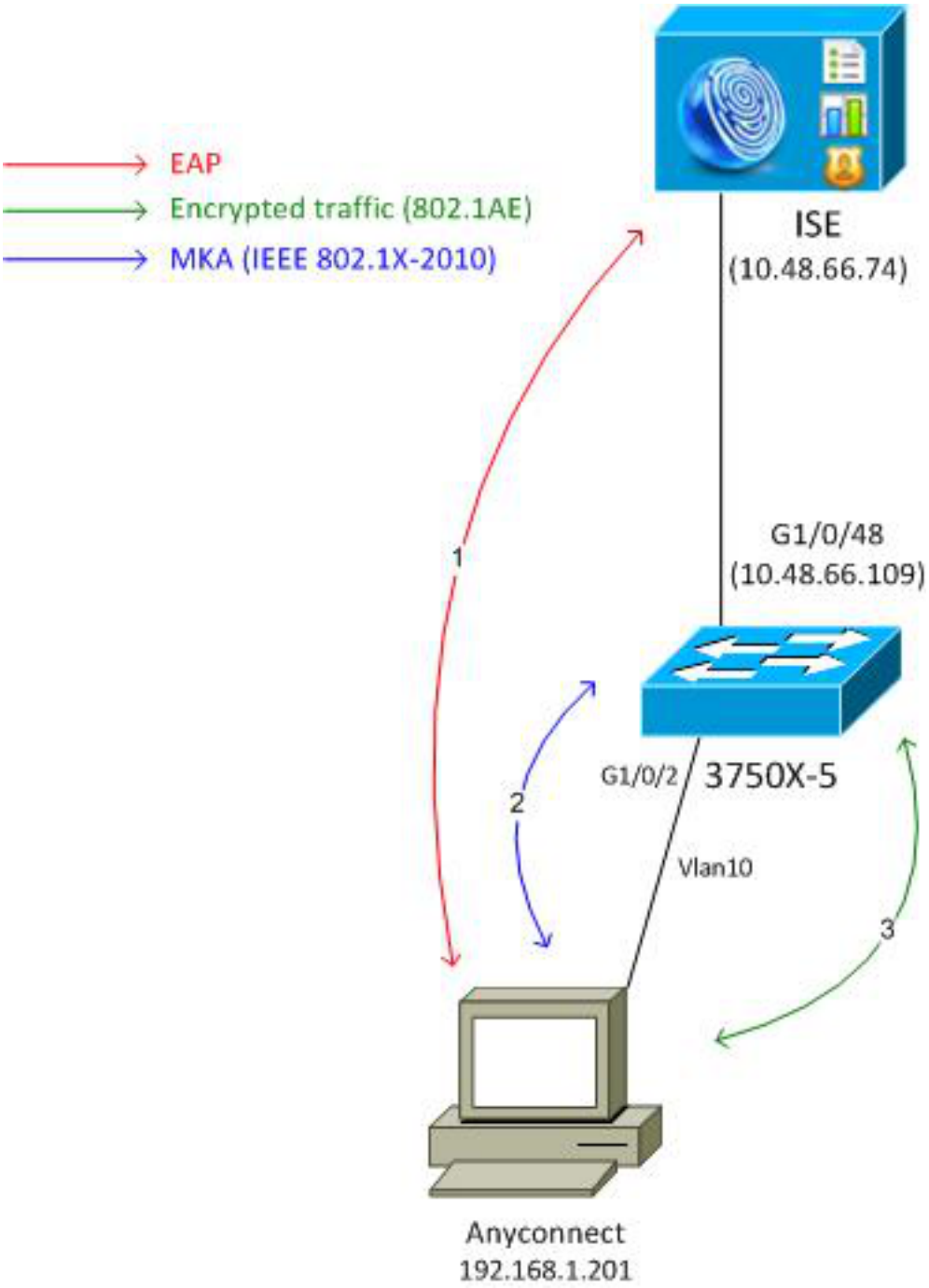
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Sistemas operativos Microsoft Windows 7 y Microsoft Windows XP
- Software Cisco 3750X, versión 15.0 y posteriores
- Software Cisco ISE, versión 1.1.4 y posteriores
- Cisco AnyConnect Mobile Security con Network Access Manager (NAM), versión 3.1 y posteriores

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de red y flujo de tráfico



Paso 1. El solicitante (AnyConnect NAM) inicia la sesión 802.1x. El switch es el autenticador y el ISE es el servidor de autenticación. El protocolo Extensible Authentication Protocol over LAN (EAPOL) se utiliza como transporte para EAP entre el suplicante y el switch. RADIUS se utiliza como protocolo de transporte para EAP entre el switch y el ISE. No se puede utilizar la derivación de autenticación MAC (MAB), porque las claves EAPOL deben devolverse de ISE y utilizarse para la sesión de MACsec Key Agreement (MKA).

Paso 2. Después de que se complete la sesión 802.1x, el switch inicia una sesión MKA con EAPOL como protocolo de transporte. Si el suplicante está configurado correctamente, las claves para el cifrado AES-GCM (modo Galois/Contador) simétrico de 128 bits coinciden.

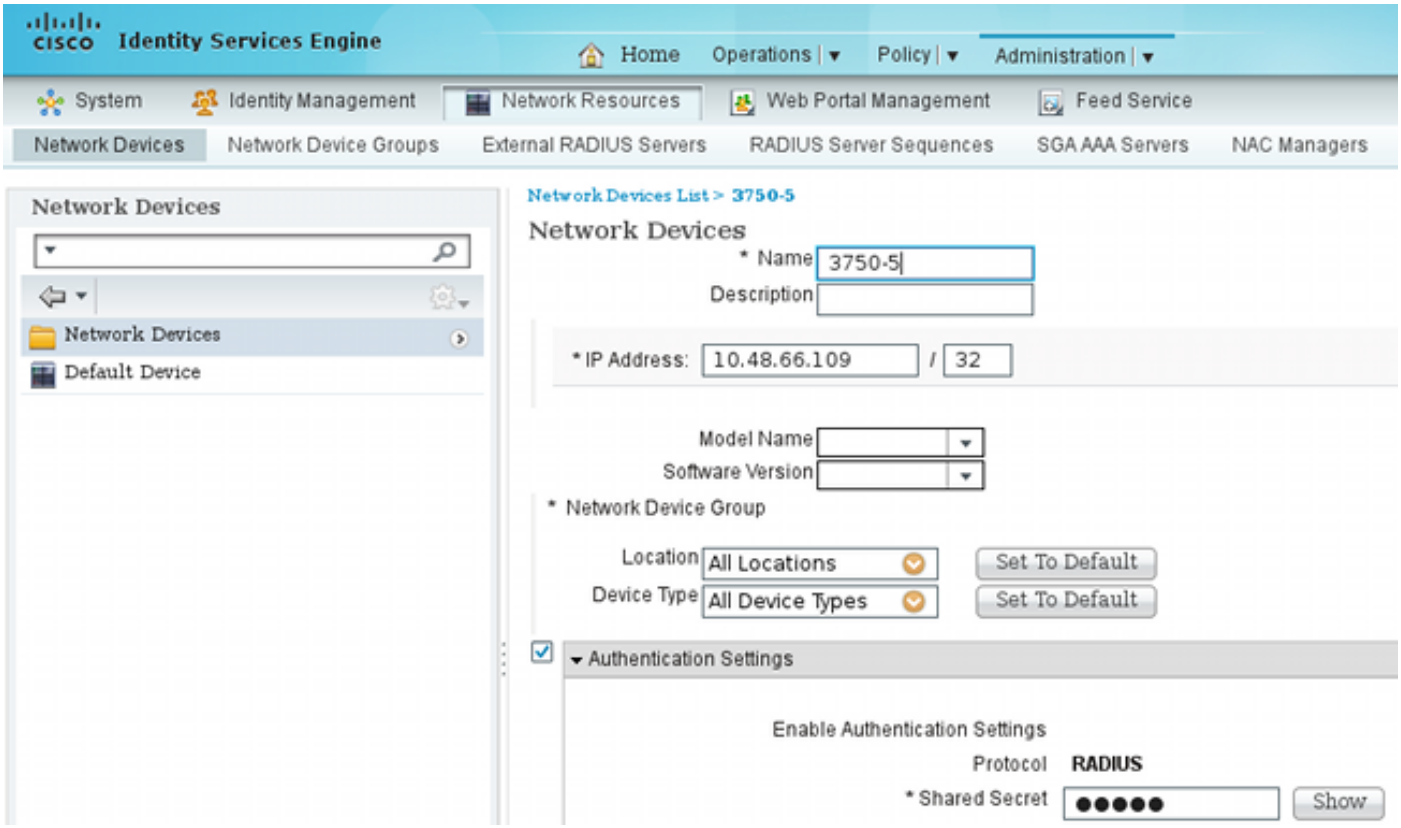
Paso 3. Todos los paquetes subsiguientes entre el solicitante y el switch están cifrados (encapsulación 802.1AE).

Configuraciones

ISE

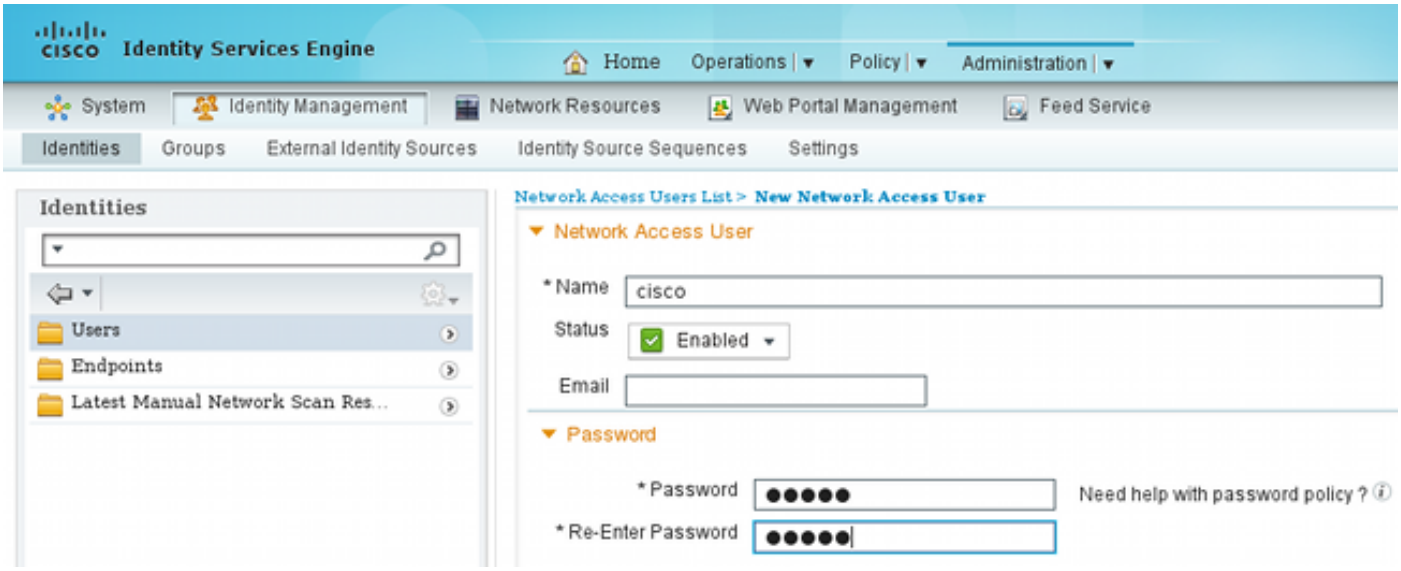
La configuración de ISE implica un escenario 802.1x típico con una excepción al perfil de autorización que podría incluir políticas de cifrado.

Elija **Administration > Network Resources > Network Devices** para agregar el switch como un dispositivo de red. Introduzca una clave precompartida RADIUS (clave secreta compartida).



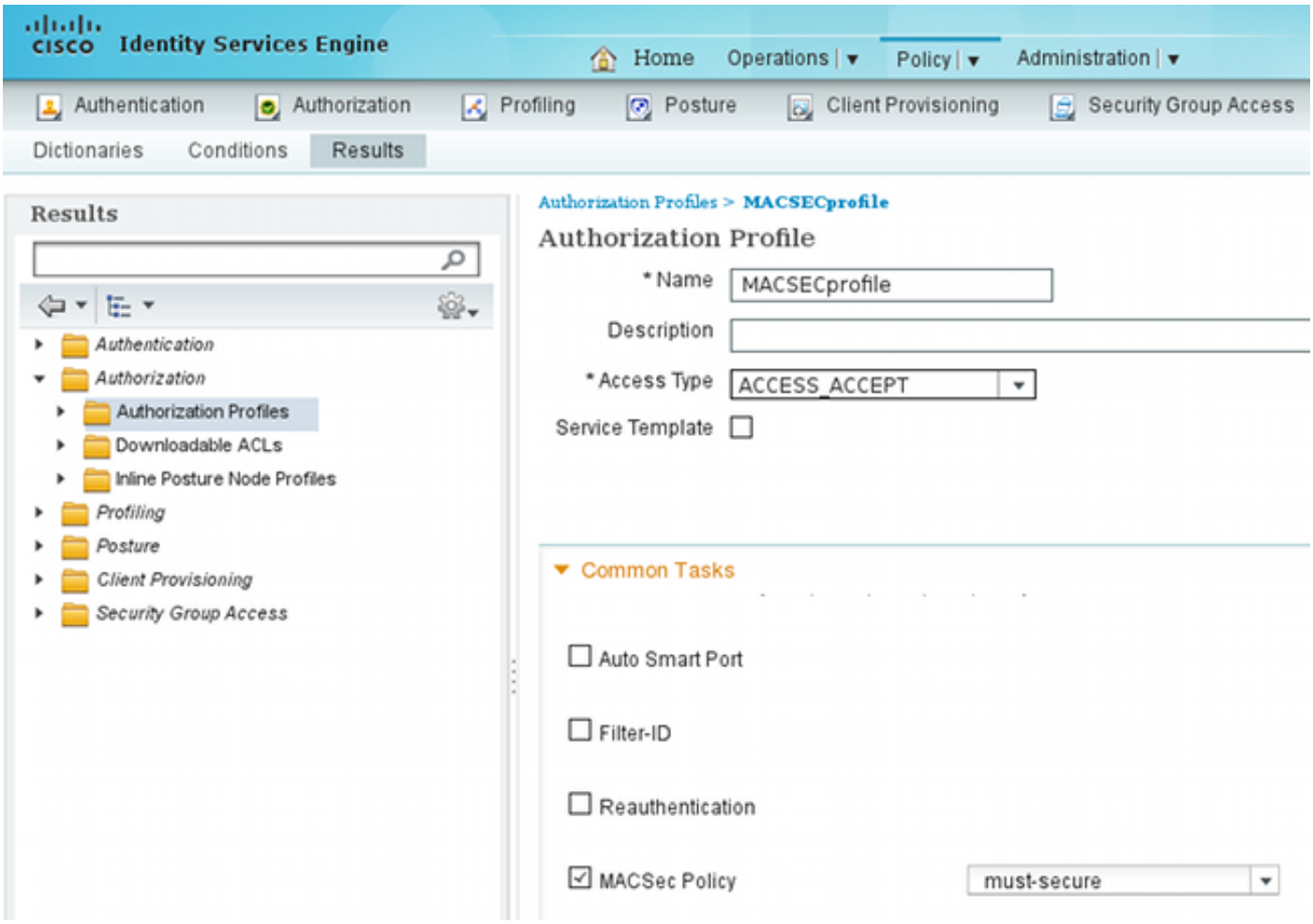
Se puede utilizar la regla de autenticación predeterminada (para los usuarios definidos localmente en ISE).

Elija **Administration > Identity Management > Users** para definir el usuario "cisco" localmente.

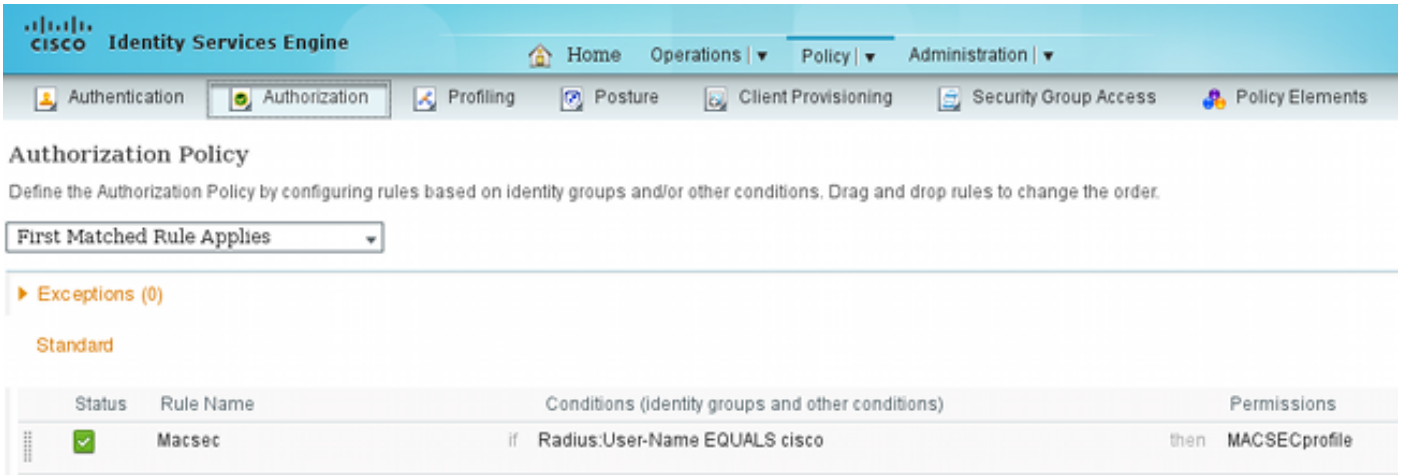


El perfil de autorización puede incluir políticas de cifrado. Como se muestra en este ejemplo, elija **Policy > Results > Authorization Profiles** para ver la información que ISE devuelve al switch que el

cifrado de link es obligatorio. Además, se ha configurado el número de VLAN (10).



Elija **Policy > Authorization** para utilizar el perfil de autorización en la regla de autorización. Este ejemplo devuelve el perfil configurado para el usuario "cisco". Si 802.1x se realiza correctamente, ISE devuelve Radius-Accept al switch con Cisco AVPair linksec-policy=must-secure. Ese atributo obliga al switch a iniciar una sesión MKA. Si esa sesión falla, la autorización 802.1x en el switch también falla.



Switch

La configuración típica del puerto 802.1x incluye (la parte superior se muestra):

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

aaa group server radius ISE
 server name ISE

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order dot1x
 authentication port-control auto
 dot1x pae authenticator

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 timeout 5
 retransmit 2
key cisco
```

La política MKA local se crea y se aplica a la interfaz. Además, MACsec está habilitado en la interfaz.

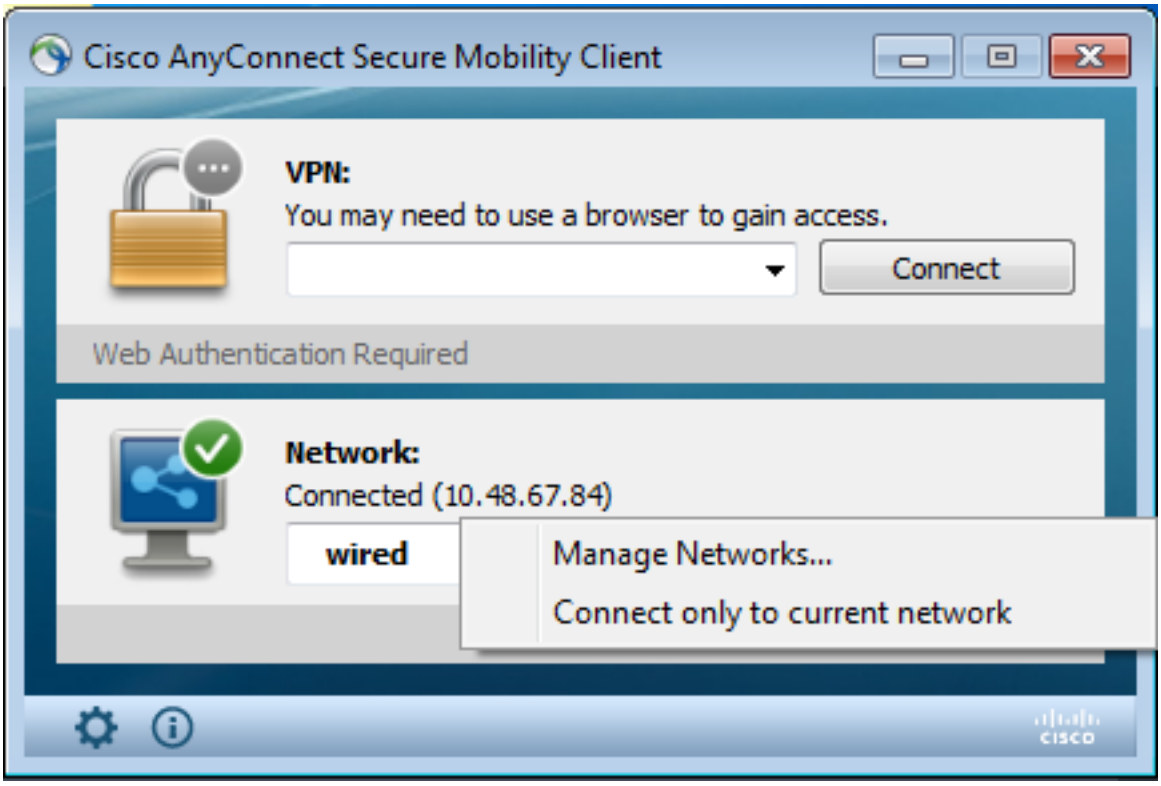
```
mka policy mka-policy
 replay-protection window-size 5000

interface GigabitEthernet1/0/2
 macsec
 mka policy mka-policy
```

La política MKA local le permite configurar los ajustes detallados que no se pueden enviar desde el ISE. La política MKA local es opcional.

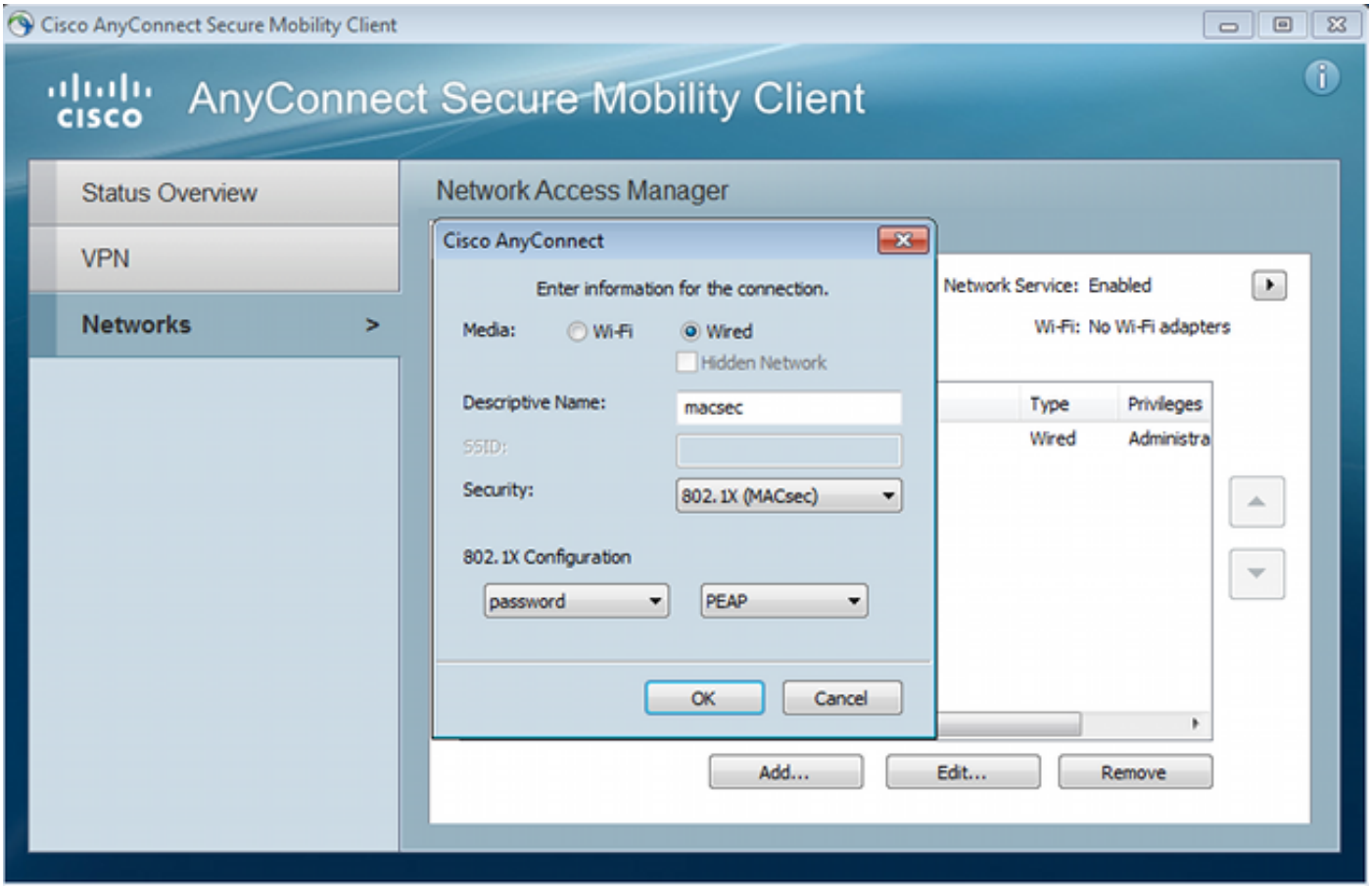
NAM de AnyConnect

El perfil del suplicante 802.1x se puede configurar manualmente o enviar a través de Cisco ASA. Los siguientes pasos presentan una configuración manual.

Para administrar los perfiles NAM:



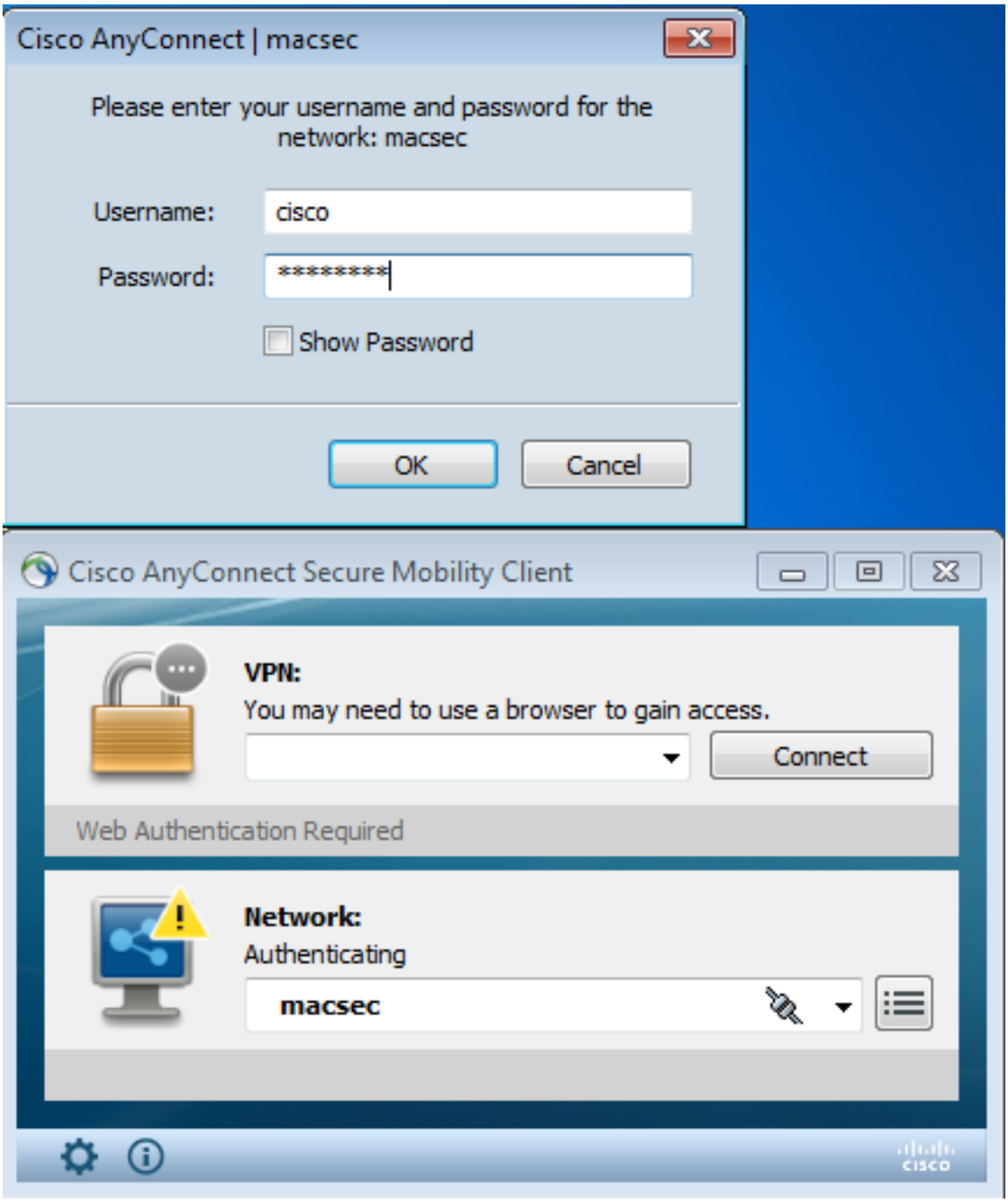
Agregue un nuevo perfil 802.1x con MACsec. Para 802.1x, se utiliza el protocolo de autenticación extensible protegido (PEAP) (usuario "cisco" configurado en ISE):



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

El NAM de AnyConnect configurado para EAP-PEAP requiere las credenciales correctas.



La sesión en el switch debe autenticarse y autorizarse. El estado de seguridad debe ser "Protegido":

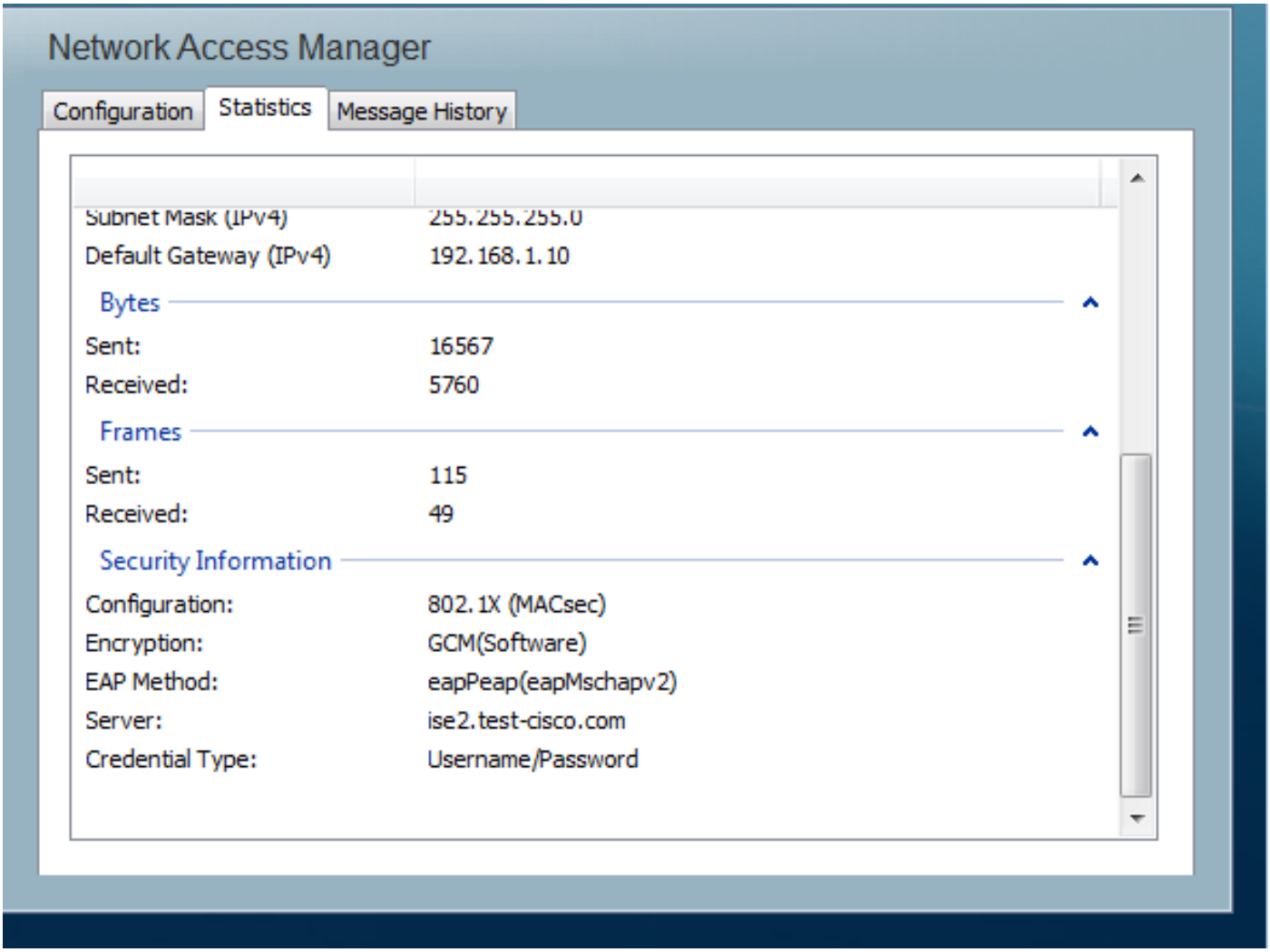
```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Secured
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
```

```
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D56FD55B3BF
     Acct Session ID:  0x00011CB4
              Handle:  0x97000D57

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

Las estadísticas MACsec del switch proporcionan los detalles sobre la configuración de políticas locales, los identificadores de canal seguros (SCI) para el tráfico recibido/enviado, así como las estadísticas y los errores de puerto.

```
bsns-3750-5#show macsec interface g1/0/2
MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
 Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
 SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

En AnyConnect, las estadísticas indican el uso de cifrado y las estadísticas de paquetes.



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Depuraciones para un escenario de trabajo

Habilitar depuraciones en el switch (se ha omitido alguna salida para mayor claridad).

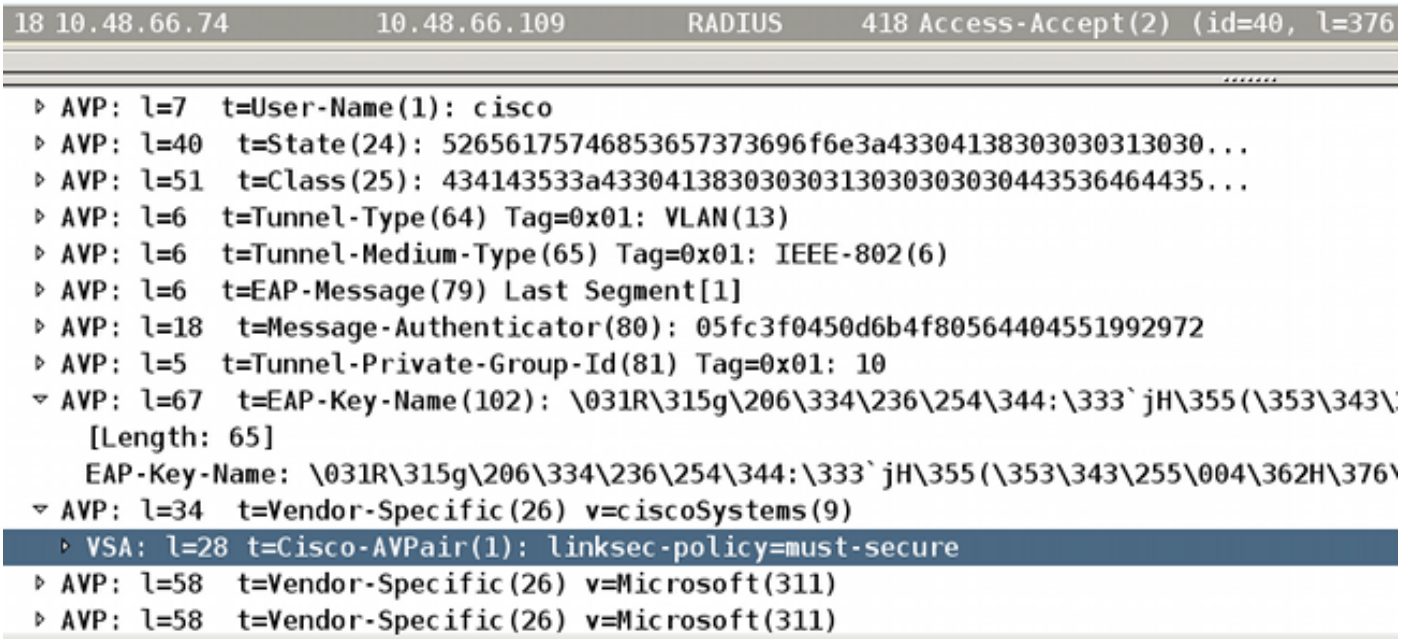
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

Después de establecer una sesión 802.1x, se intercambian varios paquetes EAP a través de EAPOL. La última respuesta exitosa de ISE (EAP exitoso) llevada dentro de Radius-Acccept también incluye varios atributos Radius.

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS:  EAP-Key-Name        [102] 67  *
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "linksec-policy=must-secure"
```

```
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Send-Key   [16]  52  *
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Recv-Key   [17]  52  *
```

EAP-Key-Name se utiliza para la sesión MKA. La política de linksec obliga al switch a utilizar MACsec (la autorización falla si no se completa). Estos atributos también se pueden verificar en las capturas de paquetes.



La autenticación es correcta.

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

El switch aplica los atributos (estos incluyen un número de VLAN opcional que también se ha enviado).

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

Luego, el switch inicia la sesión MKA cuando envía y recibe paquetes EAPOL.

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D56FD55B3BF, AuthMgr-Handle 97000D57
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
EAPOL pak dump rx
dot1x-packet(Gi1/0/2): Received an EAPOL frame
dot1x-packet(Gi1/0/2): Received an MKA packet
```

Después de crear 4 identificadores de seguridad de intercambio de paquetes junto con la asociación de seguridad Receive (RX).

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```

La sesión ha finalizado y se ha agregado la asociación de seguridad Transmit (TX).

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
HULC-MACsec: Process install TxSA request66B4EEC for interface GigabitEthernet1/0/
```

La política "imprescindible" coincide y la autorización se realiza correctamente.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Cada 2 segundos se intercambian paquetes MKA Hello para asegurarse de que todos los participantes estén vivos.

```
dot1x-ev(Gi1/0/2): Received TX PDU (5) for the client 0x6E0001EC (0050.5699.36ce)
dot1x-packet(Gi1/0/2): MKA length: 0x0084 data&colon; ^A
dot1x-ev(Gi1/0/2): Sending EAPOL packet to group PAE address
EAPOL pak dump Tx
```

Depuraciones para una situación de fallo

Cuando el solicitante no está configurado para MKA y el ISE solicita cifrado después de una autenticación 802.1x exitosa:

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

El switch intenta iniciar una sesión MKA cuando envía 5 paquetes EAPOL.

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D55FD4D7529, AuthMgr-Handle A4000D56
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
```

Y, finalmente, se agota el tiempo de espera y se produce un error en la autorización.

```
 %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) MKA Session was stopped by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

La sesión 802.1x informa de una autenticación exitosa, pero de una autorización fallida.

```
bsns-3750-5#show authentication sessions int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Failed
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D55FD4D7529
     Acct Session ID:  0x00011CA0
              Handle:  0xA4000D56

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

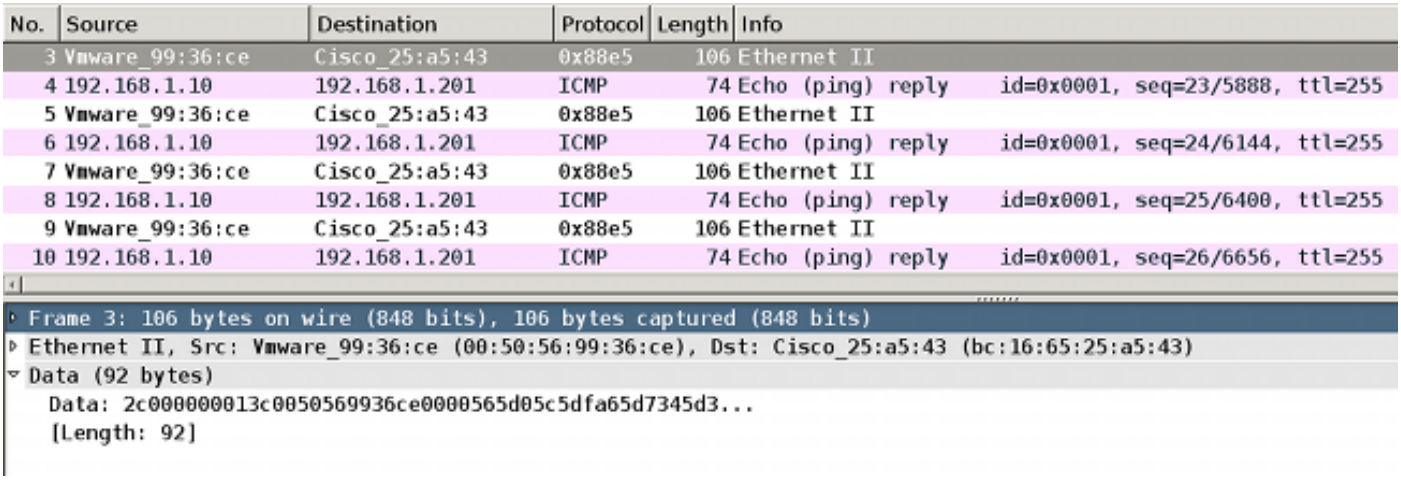
El tráfico de datos se bloqueará.

Capturas de paquetes

Cuando el tráfico se captura en el sitio del solicitante 4, se envían y reciben solicitudes de eco/respuestas del Protocolo de mensajes de control de Internet (ICMP), habrá:

- 4 solicitudes de eco ICMP cifradas enviadas al switch (88e5 está reservado para 802.1AE)
- 4 respuestas de eco ICMP descifradas recibidas

Esto se debe a cómo AnyConnect se conecta en la API de Windows (antes de libpcap cuando se envían los paquetes y antes de libpcap cuando se reciben los paquetes):



> **Nota:** No se admite la capacidad de detectar tráfico MKA o 802.1AE en el switch con funciones como el analizador de puertos conmutados (SPAN) o la captura de paquetes integrados (EPC).

Modos MACsec y 802.1x

No todos los modos 802.1x son compatibles con MACsec.

Guía de uso de Cisco TrustSec 3.0: La introducción a MACsec y NDAC establece que:

- **Modo de host único**: **MACsec se soporta completamente** en el modo de host único. En este modo, sólo se puede autenticar y proteger una única dirección MAC o IP con MACsec. Si se detecta una dirección MAC diferente en el puerto después de que se haya autenticado un punto final, se activará una violación de seguridad en el puerto.
- **Modo de autenticación multidominio (MDA)**: En este modo, un extremo puede estar en el dominio de datos y otro extremo puede estar en el dominio de voz. **MACsec se soporta completamente en el modo MDA**. Si ambos extremos son compatibles con MACsec, cada uno estará protegido por su propia sesión MACsec independiente. Si sólo un punto final es compatible con MACsec, ese punto final se puede proteger mientras que el otro punto final envía tráfico en el punto claro.
- **Modo Multi-Authentication**: En este modo, un número prácticamente ilimitado de terminales puede autenticarse en un único puerto del switch. **MACsec no se soporta en este modo.**
- **Modo de host múltiple**: Aunque el uso de MACsec en este modo es técnicamente posible, **no se recomienda**. En el modo de host múltiple, el primer punto final del puerto se autentica y, a continuación, cualquier punto final adicional se permitirá en la red a través de la primera autorización. MACsec funcionaría con el primer host conectado, pero en realidad no pasaría tráfico de otro terminal, ya que no sería tráfico cifrado.

Información Relacionada

- Guía de configuración de Cisco TrustSec para 3750
- Guía de configuración de Cisco TrustSec para ASA 9.1
- Servicios de red basados en identidad: Seguridad MAC
- Ejemplo de Configuración de la Nube TrustSec con MACsec 802.1x en Catalyst 3750X Series Switch
- Ejemplo de configuración TrustSec de ASA y el Switch Catalyst Serie 3750X y guía de solución de problemas
- Implementación y hoja de ruta de Cisco TrustSec
- Soporte Técnico y Documentación - Cisco Systems