Cifrado del Switch-host de MACsec con Cisco AnyConnect y el ejemplo de configuración ISE

ID del Documento: 117277

Actualizado: De enero el 31 de 2014

Contribuido por Michal Garcarz y Machulik romano, ingenieros de Cisco TAC.

Productos Relacionados

- Security
- 802.1x
- Cisco Identity Services Engine

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para el cifrado de la Seguridad del control de acceso a los medios (MACsec) entre un supplicant del 802.1x (Mobile Security de Cisco AnyConnect) y un authenticator (Switch). Los Ciscos Identity Services Engine (ISE) se utilizan como la autenticación y servidor de políticas.

MACsec se estandardiza en 802.1AE y se soporta en Cisco 3750X, 3560X, y 4500 Switches SUP7E. 802.1AE define el cifrado de link sobre las redes alámbricas que utilizan las claves fuera de banda. Esas claves de encripción se negocian con el protocolo del acuerdo de la clave de MACsec (MKA) que se utiliza después de la autenticación acertada del 802.1x. MKA se estandardiza en IEEE 802.1X-2010.

Un paquete se cifra solamente en el link entre el PC y el Switch (Point-to-Point Encryption). El paquete recibido por el Switch se desencripta y se envía vía el uplinks unencrypted. Para cifrar la transmisión entre el Switches, se recomienda el cifrado del switch switch. Para ese cifrado, el protocolo de la asociación de seguridad (SAP) se utiliza para negociar y para regenerar las claves. El SAP es un protocolo del acuerdo de la clave del prestandard desarrollado por Cisco.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

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

- Sistemas operativos de Microsoft Windows 7 y del Microsoft Windows XP
- Software de Cisco 3750X, versión 15.0 y posterior
- Software de Cisco ISE, versión 1.1.4 y posterior
- Mobile Security de Cisco AnyConnect con el administrador del acceso a la red (NAM), versión 3.1 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 y flujo de tráfico

Paso 1. El supplicant (AnyConnect NAM) comienza la sesión del 802.1x. El Switch es el authenticator y el ISE es el servidor de autenticación. El protocolo extensible authentication sobre el protocolo LAN (EAPOL) se utiliza como un transporte para el EAP entre el supplicant y el Switch. El RADIUS se utiliza como Transport Protocol para el EAP entre el Switch y el ISE. Puente de la autenticación de MAC (MAB) no puede ser utilizado, porque las claves EAPOL necesitan ser vueltas del ISE y ser utilizadas para la sesión del acuerdo de la clave de MACsec (MKA).

Paso 2. Después de que la sesión del 802.1x sea completa, el Switch inicia una sesión MKA con el EAPOL como Transport Protocol. Si el supplicant se configura correctamente, las claves para el cifrado simétrico del 128-bit AES-GCM (Galois/modo contrario) hacen juego.

Paso 3. Todos los paquetes subsiguientes entre el supplicant y el Switch se cifran (la encapsulación 802.1AE).

Configuraciones

ISE

La configuración ISE implica un escenario típico del 802.1x con una excepción al perfil de la autorización que pudo incluir las políticas de encripción.

Elija la **administración > los recursos de red > los dispositivos de red** para agregar el Switch como dispositivo de red. Ingrese una clave del preshared del RADIO (secreto compartido).

La regla de la autenticación predeterminada puede ser utilizada (para los usuarios definidos localmente en el ISE).

Elija la **administración > la Administración de la identidad > Users** para definir al usuario “Cisco” localmente.

El perfil de la autorización pudo incluir las políticas de encripción. Tal y como se muestra en de este ejemplo, elija la **directiva > los resultados > los perfiles de la autorización** para ver las devoluciones de la información ISE al Switch que el cifrado de link es obligatorio. También, el número VLAN (se ha configurado 10).

Elija la **directiva > la autorización** para utilizar el perfil de la autorización en la regla de la autorización. Este ejemplo vuelve el perfil configurado para el usuario “Cisco”. Si el 802.1x es acertado, las devoluciones ISE Radio-validan al Switch con el linksec-policy=must-secure de Cisco AVPair. Ese atributo fuerza el Switch para iniciar una sesión MKA. Si esa sesión falla, la autorización del 802.1x en el Switch también falla.

Switch

Las configuraciones de puerto típicas del 802.1x incluyen (porción superior mostrada):

```
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 directiva local MKA se crea y se aplica a la interfaz. También, MACsec se habilita en la interfaz.

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

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

La directiva local MKA permite que usted configure las configuraciones detalladas que no se pueden avanzar del ISE. La directiva local MKA es opcional.

AnyConnect NAM

El perfil para el supplicant del 802.1x se puede configurar manualmente o avanzar vía Cisco ASA. Los siguientes pasos presentan una configuración manual.

Para manejar los perfiles NAM:

Agregue un nuevo perfil del 802.1x con MACsec. Para el 802.1x, se utiliza el protocolo extensible authentication protegido (PEAP) (el usuario configurado “Cisco” en el ISE):

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

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

La sesión sobre el Switch debe ser autenticada y ser autorizada. El estado de seguridad debe “ser asegurado”:

```
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 de MACsec sobre el Switch proporcionan los detalles con respecto a la configuración de la política local, a los identificadores del canal seguro (SCIs) para el tráfico recibido/enviado, y también a las estadísticas de puerto y a los errores.

```
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 y las estadísticas de paquete del cifrado.

Troubleshooting

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

Debugs para un escenario de trabajo

Debugs del permiso en el Switch (una cierta salida se ha omitido para mayor clareza).

```
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
```

Después de que se establezca una sesión del 802.1x, los paquetes EAP múltiples se intercambian sobre el EAPOL. La respuesta acertada más reciente del radio-Acccept interior llevado ISE (éxito EAP) también incluye varios atributos de 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  *
```

El EAP-Clave-nombre se utiliza para la sesión MKA. La linksec-directiva fuerza el Switch para utilizar MACsec (la autorización falla si ésa no es completa). Esos atributos se pueden también verificar en las capturas de paquetes.

La autenticación es acertada.

```
%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 (éstos incluyen un número VLAN opcional que también se ha enviado).

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

El Switch entonces comienza la sesión MKA cuando envía y recibe los paquetes EAPOL.

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

Después de que 4 identificadores seguros del intercambio de paquetes se creen junto con la asociación de seguridad de la recepción (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
```

Se acaba la sesión y agregan a la asociación de seguridad del transmitir (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 directiva “deber-segura” se corresponde con y la autorización es acertada.

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

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

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

Debugs para un escenario que falla

Cuando el supplicant no se configura para MKA y el ISE pide el cifrado después de una autenticación acertada del 802.1x:

```
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.

```
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
```

Y finalmente mide el tiempo hacia fuera y falla 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 del 802.1x señala la autenticación satisfactoria, pero la 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 será bloqueado.

Capturas de paquetes

Cuando el tráfico se captura en los pedidos de eco/las contestaciones del Internet Control Message Protocol (ICMP) del sitio 4 del supplicant se envían y recibido, habrá:

- 4 cifraron los pedidos de eco ICMP enviados al Switch (88e5 es reservado para 802.1AE)
- 4 desencriptaron las respuestas de eco ICMP recibidas

Eso está debido a cómo los ganchos de AnyConnect en Windows API (antes del libpcap cuando se envían los paquetes y antes del libpcap cuando se reciben los paquetes):

> **Note**: La capacidad de oler el tráfico MKA o 802.1AE en el Switch con las características tales como Switched Port Analyzer (SPAN) o captura de paquetes integrada (EPC) no se soporta.

Modos de MACsec y del 802.1x

No todos los modos del 802.1x se soportan para MACsec.

La guía de Cómo del 3.0 de Cisco TrustSec: Introducción a MACsec y a los estados *NDAC* eso:

- **Modo del solo host**: **MACsec se soporta completamente** en el modo del solo host. En este modo, solamente un solo MAC o dirección IP se puede autenticar y asegurar con MACsec. Si una diversa dirección MAC se detecta en el puerto después de que un punto final haya autenticado, una violación de seguridad será accionada en el puerto.
- **Modo de la autenticación del Multi-dominio (MDA)**: En este modo, un punto final puede estar en el dominio de los datos y otro punto final puede estar en el dominio de la Voz. **MACsec se soporta completamente en el modo MDA**. Si ambos puntos finales son MACsec-capaces, cada uno será asegurada por su propia sesión independiente de MACsec. Si solamente un punto final es MACsec-capaz, ese punto final puede ser asegurado mientras que el otro punto final envía el tráfico en el claro.
- **Modo de la Multi-autenticación**: En este modo, un número sin límite de puntos finales se puede autenticar virtualmente a un puerto del un solo switch. **MACsec no se soporta en este modo.**
- **Modo del Multi-host**: Mientras que el uso de MACsec en este modo es técnico posible, **no se recomienda**. En el modo del Multi-host, el primer punto final en el puerto autentica, y entonces cualquier punto final adicional será permitido sobre la red vía la primera autorización. ¿MACsec trabajaría con el primer host conectado, pero ningún otro punto final? el tráfico s pasaría realmente, puesto que no sería tráfico encriptado.

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 la identidad: Seguridad MAC
- Nube de TrustSec con el 802.1x MACsec en el ejemplo de configuración del Catalyst 3750X Series Switch
- ASA y ejemplo de configuración de TrustSec del Catalyst 3750X Series Switch y guía del Troubleshooting
- Despliegue y mapa de ruta de Cisco TrustSec
- Soporte Técnico y Documentación - Cisco Systems

Gracias por su feedback.

Abra un caso de soporte (requiere un contrato de servicios con Cisco.)

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De enero el 31 de 2014
ID del Documento: 117277