Criptografia de host de switch MACsec com o exemplo de configuração do Cisco AnyConnect e ISE

Contents

Introduction

Este documento fornece um exemplo de configuração para a criptografia MACsec (Media Access Control Security) entre um suplicante 802.1x (Cisco AnyConnect Mobile Security) e um autenticador (switch). O Cisco Identity Services Engine (ISE) é usado como servidor de autenticação e política.

O MACsec é padronizado em 802.1AE e é suportado nos switches Cisco 3750X, 3560X e 4500 SUP7E. O 802.1AE define a criptografia de link em redes com fio que usam chaves fora da banda. Essas chaves de criptografia são negociadas com o protocolo MACsec Key Agreement (MKA) que é utilizado após a autenticação 802.1x bem-sucedida. O MKA é padronizado no IEEE 802.1X-2010.

Um pacote é criptografado somente no link entre o PC e o switch (criptografia ponto a ponto). O pacote recebido pelo switch é descriptografado e enviado por uplinks não criptografados. Para criptografar a transmissão entre os switches, recomenda-se a criptografia do switch-switch. Para essa criptografia, o Security Association Protocol (SAP) é usado para negociar e regenerar chaves. O SAP é um protocolo de acordo chave pré-padrão desenvolvido pela Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração 802.1x
- Conhecimento básico da configuração de CLI dos switches Catalyst
- Experiência com a configuração do ISE

Componentes Utilizados

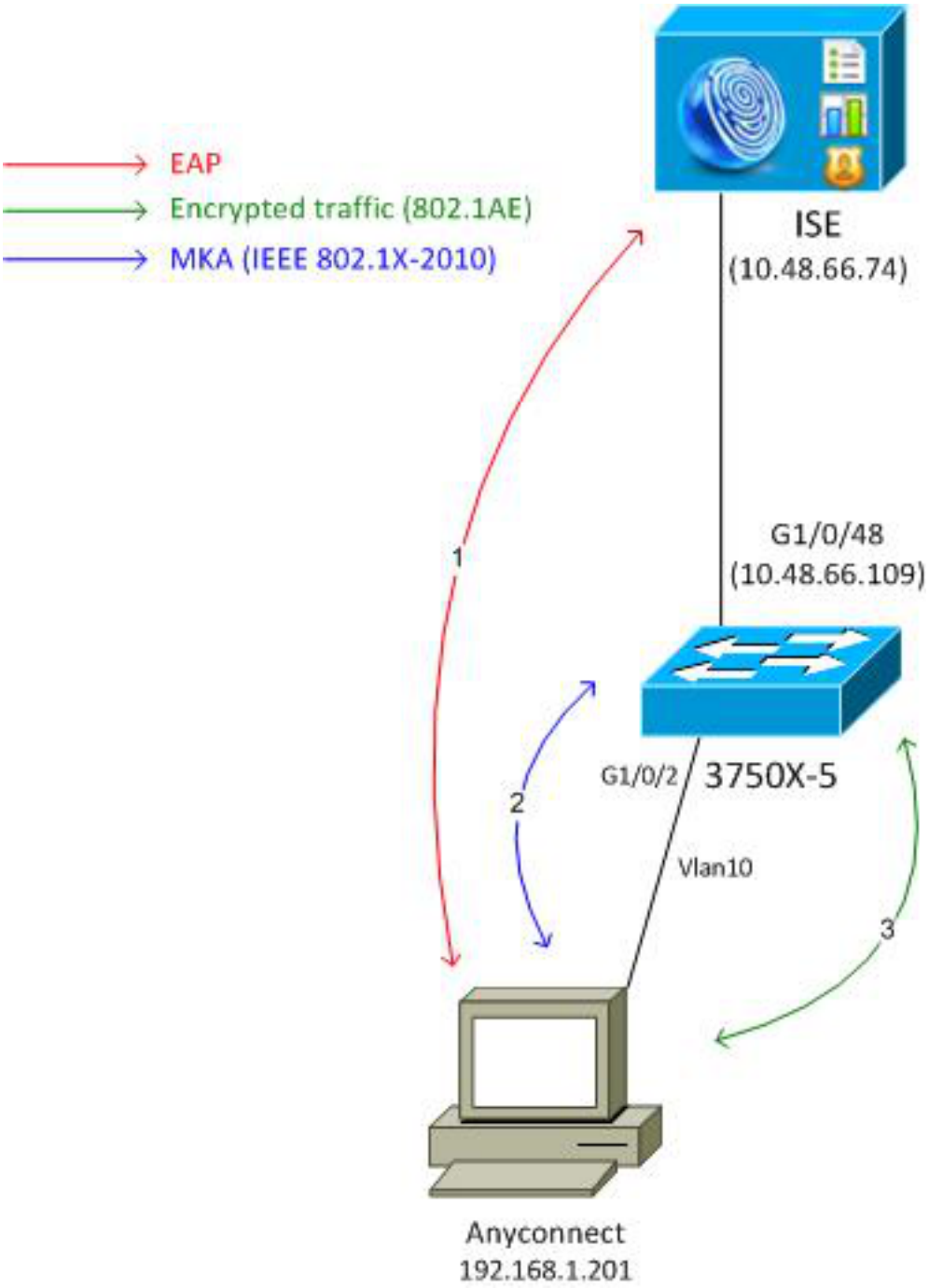
As informações neste documento são baseadas nestas versões de software e hardware:

- Sistemas operacionais Microsoft Windows 7 e Microsoft Windows XP
- Software Cisco 3750X, versão 15.0 e posterior
- Software Cisco ISE, versão 1.1.4 e posterior
- Cisco AnyConnect Mobile Security com Network Access Manager (NAM), versão 3.1 e posterior

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 rede e fluxo de tráfego



Etapa 1. O requerente (AnyConnect NAM) inicia a sessão 802.1x. O switch é o autenticador e o ISE é o servidor de autenticação. O protocolo EAPOL (Extensible Authentication Protocol over LAN) é usado como transporte para EAP entre o requerente e o switch. O RADIUS é usado como um protocolo de transporte para EAP entre o switch e o ISE. Não é possível usar o MAC Authentication Bypass (MAB), pois as chaves EAPOL precisam ser retornadas do ISE e usadas para a sessão MACsec Key Agreement (MKA).

Etapa 2. Após a conclusão da sessão 802.1x, o switch inicia uma sessão MKA com EAPOL como protocolo de transporte. Se o requerente estiver configurado corretamente, as chaves para a criptografia AES-GCM simétrica de 128 bits (modo Galois/Counter) coincidem.

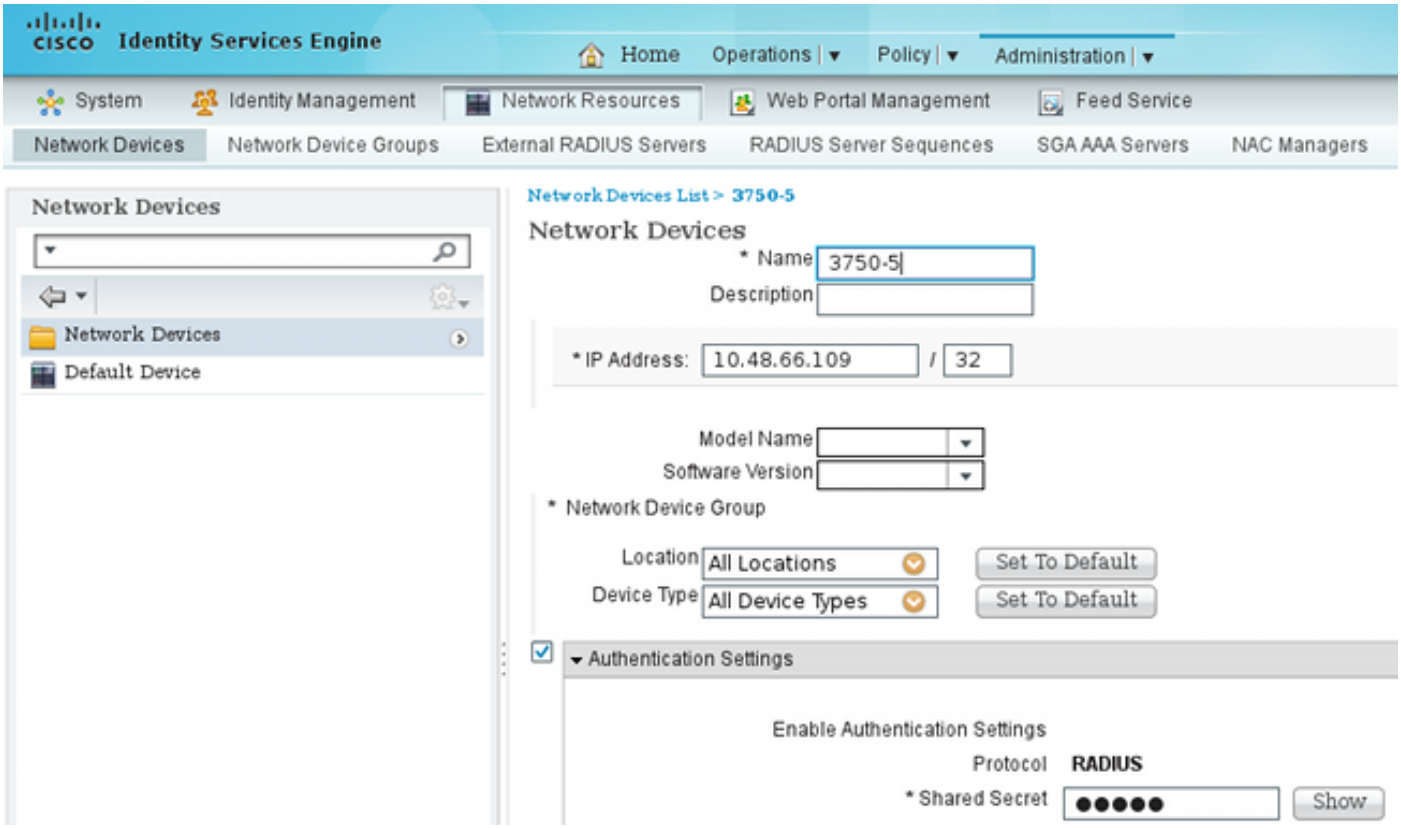
Etapa 3. Todos os pacotes subsequentes entre o requerente e o switch são criptografados (encapsulamento 802.1AE).

Configurações

ISE

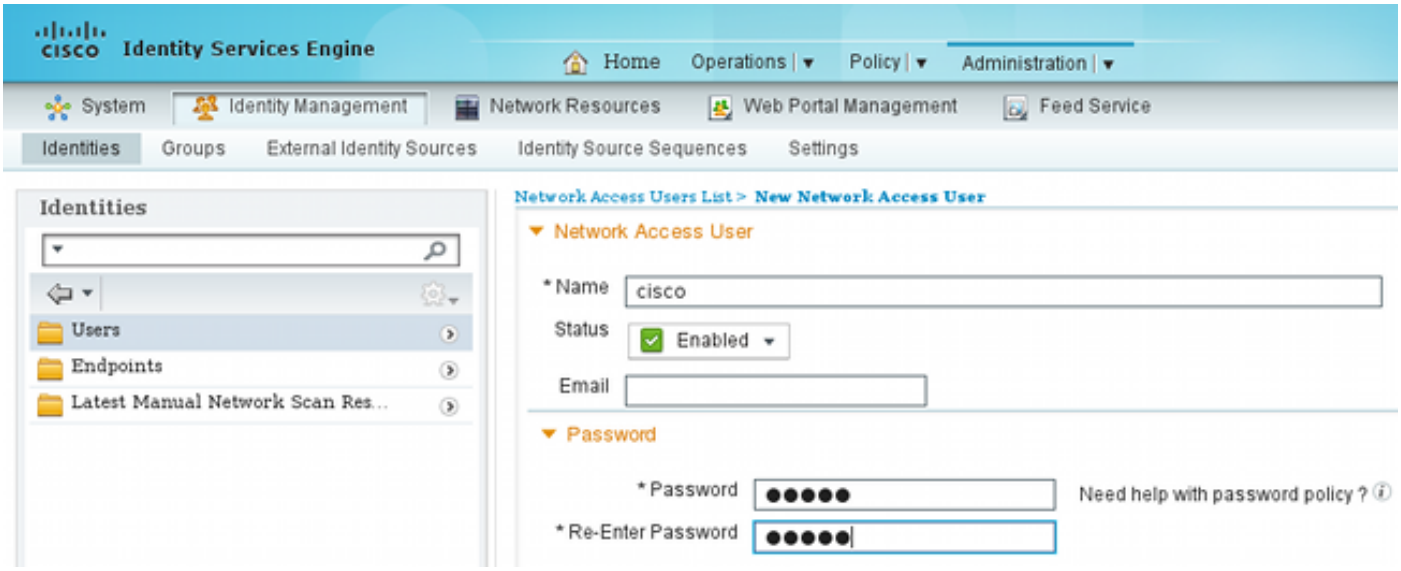
A configuração do ISE envolve um típico cenário 802.1x com uma exceção ao perfil de autorização que pode incluir políticas de criptografia.

Escolha **Administration > Network Resources > Network Devices** para adicionar o switch como um dispositivo de rede. Insira uma chave pré-compartilhada RADIUS (Shared Secret).



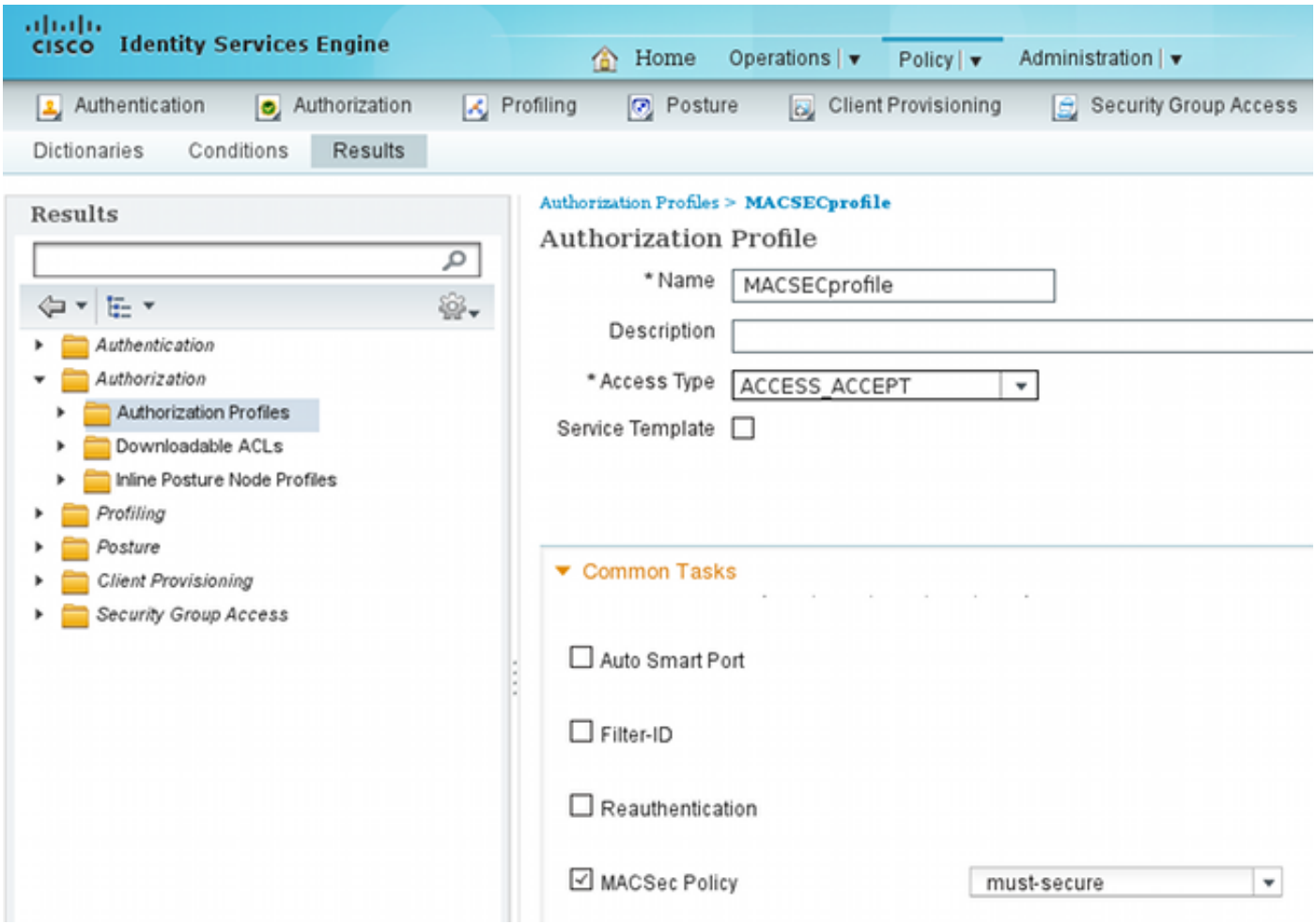
A regra de autenticação padrão pode ser usada (para usuários definidos localmente no ISE).

Escolha **Administration > Identity Management > Users** para definir o usuário "cisco" localmente.

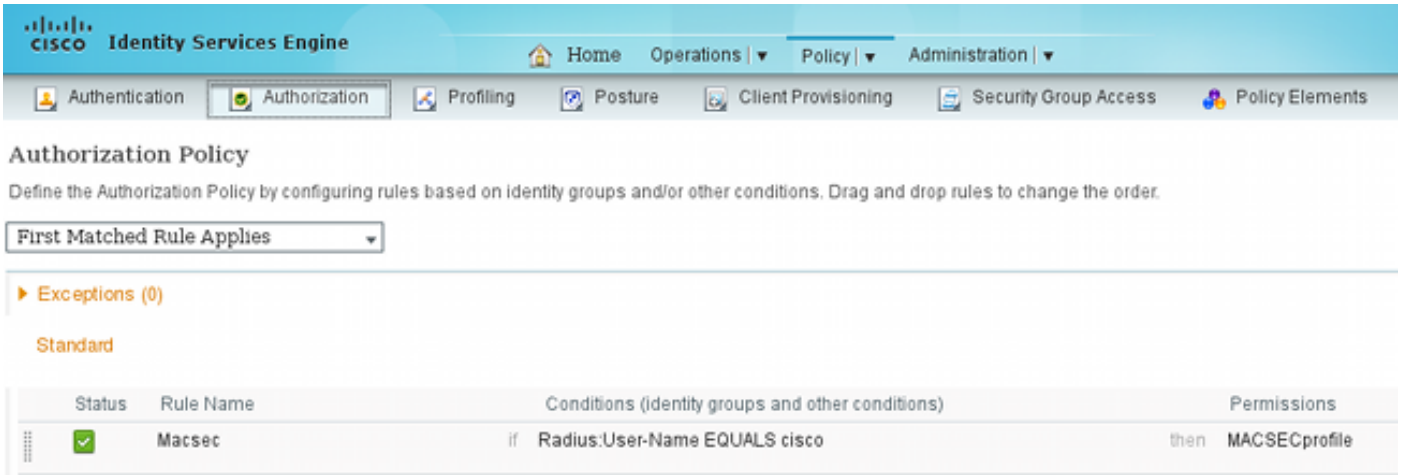


O perfil de autorização pode incluir políticas de criptografia. Como mostrado neste exemplo, escolha **Policy > Results > Authorization Profiles** para exibir as informações que o ISE retorna ao switch de que a criptografia de link é obrigatória. Além disso, o número da VLAN (10) foi

configurado.



Escolha **Política > Autorização** para usar o perfil de autorização na regra de autorização. Este exemplo retorna o perfil configurado para o usuário "cisco". Se o 802.1x for bem-sucedido, o ISE retorna Radius-Accept para o switch com o Cisco AVPair linksec-policy=must-secure. Esse atributo força o switch a iniciar uma sessão MKA. Se essa sessão falhar, a autorização 802.1x no switch também falhará.



Switch

As configurações típicas da porta 802.1x incluem (parte 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
```

A política MKA local é criada e aplicada à interface. Além disso, o MACsec está ativado na interface.

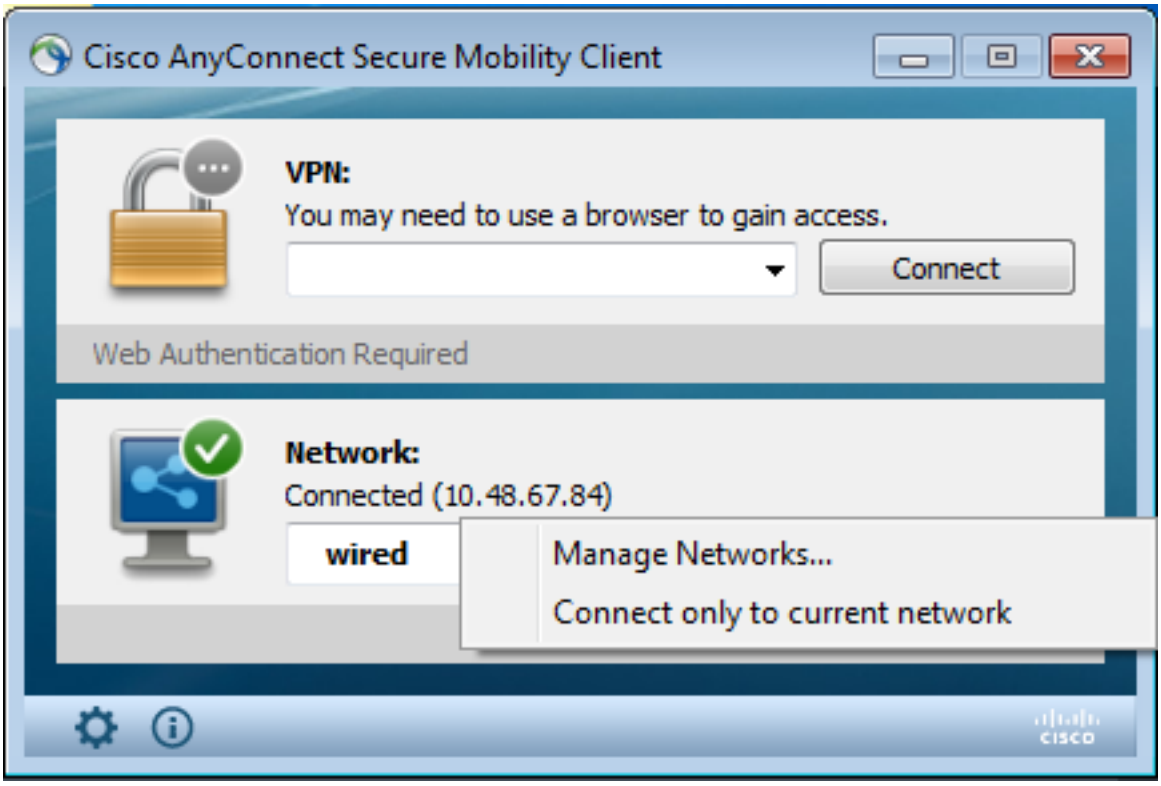
```
mka policy mka-policy
 replay-protection window-size 5000

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

A política MKA local permite que você defina configurações detalhadas que não podem ser enviadas do ISE. A política MKA local é opcional.

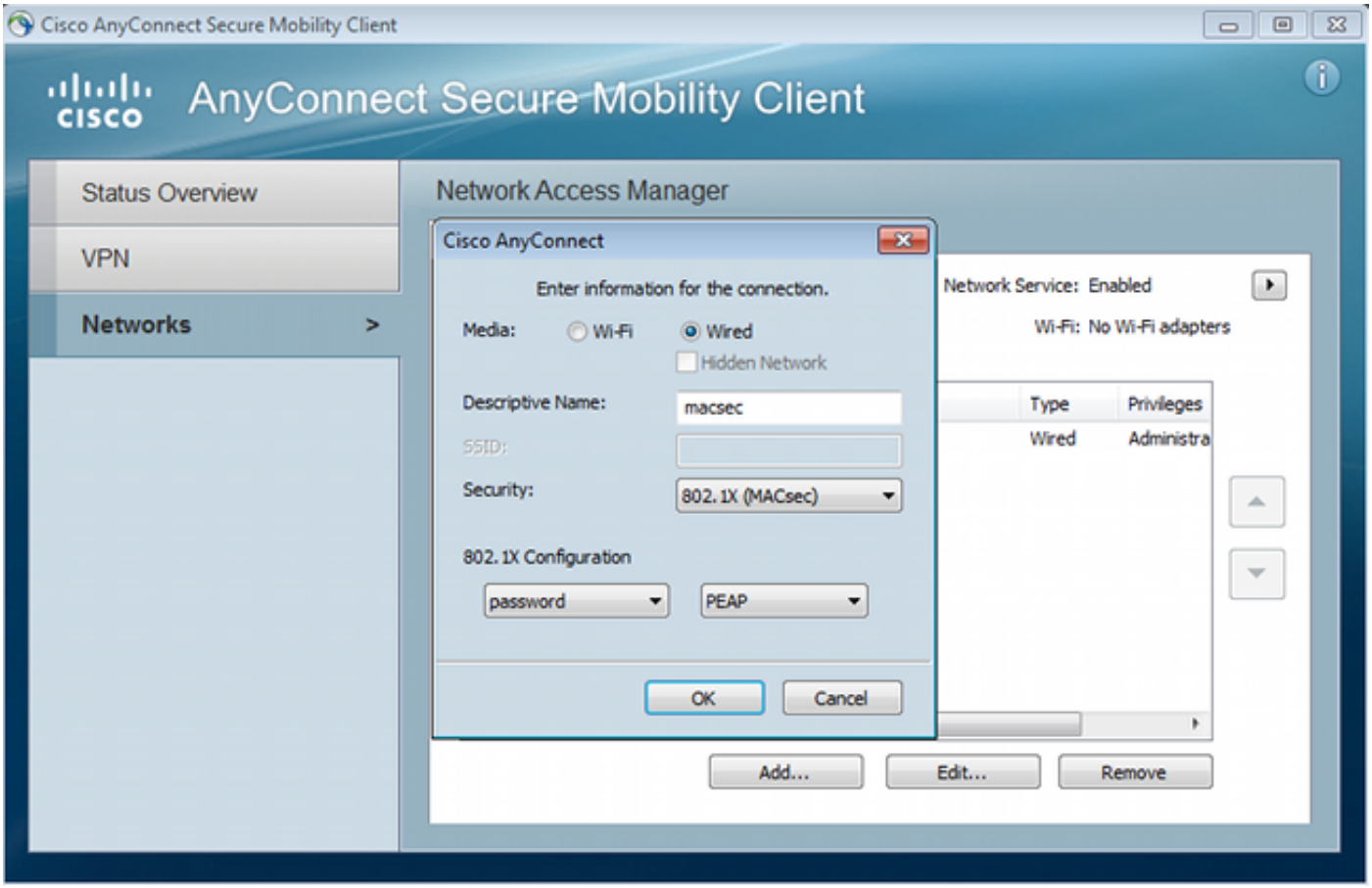
NAM do AnyConnect

O perfil do suplicante 802.1x pode ser configurado manualmente ou enviado por meio do Cisco ASA. As próximas etapas apresentam uma configuração manual.

Para gerenciar perfis NAM:



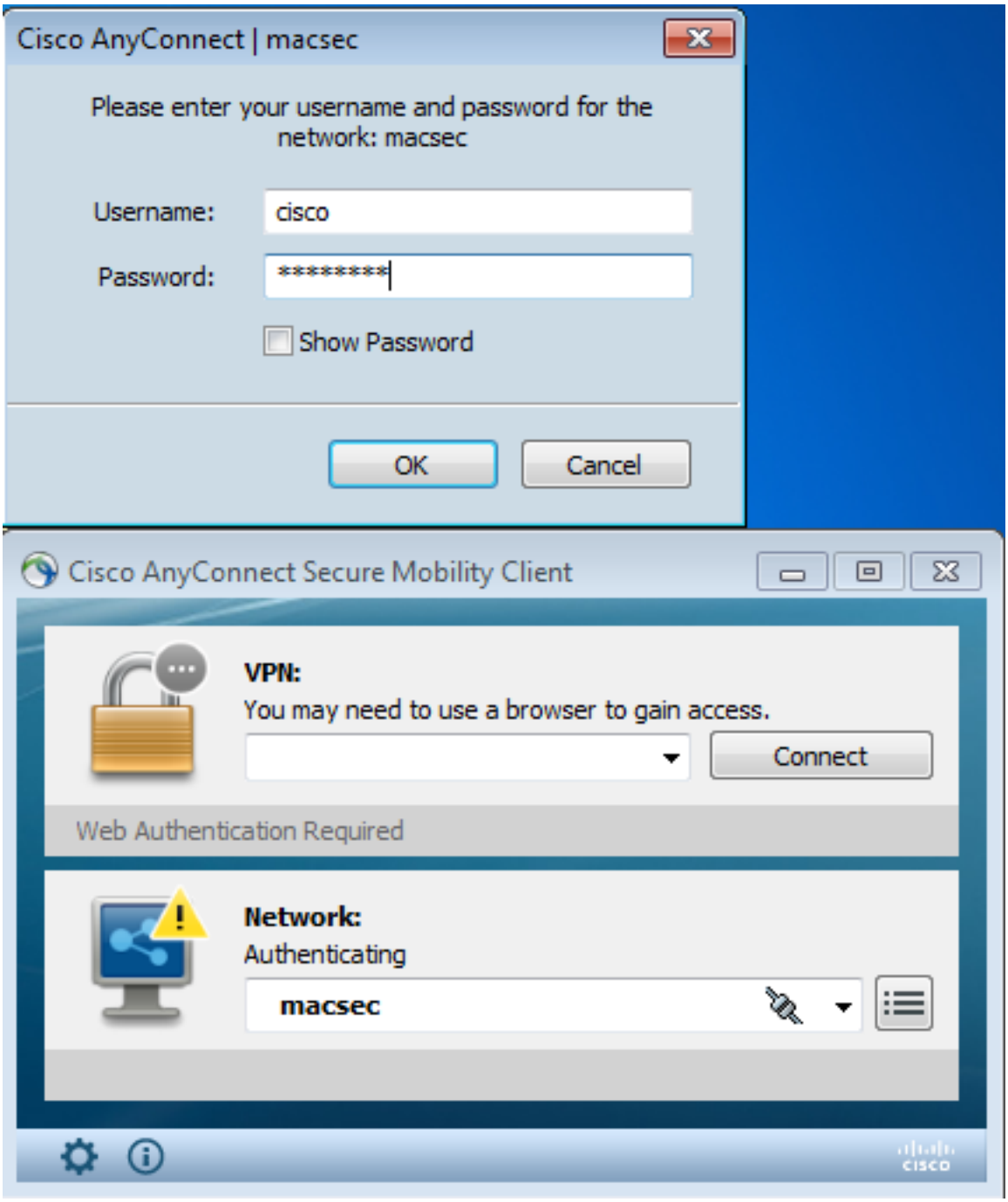
Adicione um novo perfil 802.1x com MACsec. Para o 802.1x, o PEAP (Protected Extensible Authentication Protocol) é usado (o usuário configurado "cisco" no ISE):



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O AnyConnect NAM configurado para EAP-PEAP requer credenciais corretas.



A sessão no switch deve ser autenticada e autorizada. O status de segurança deve ser "Protegido":

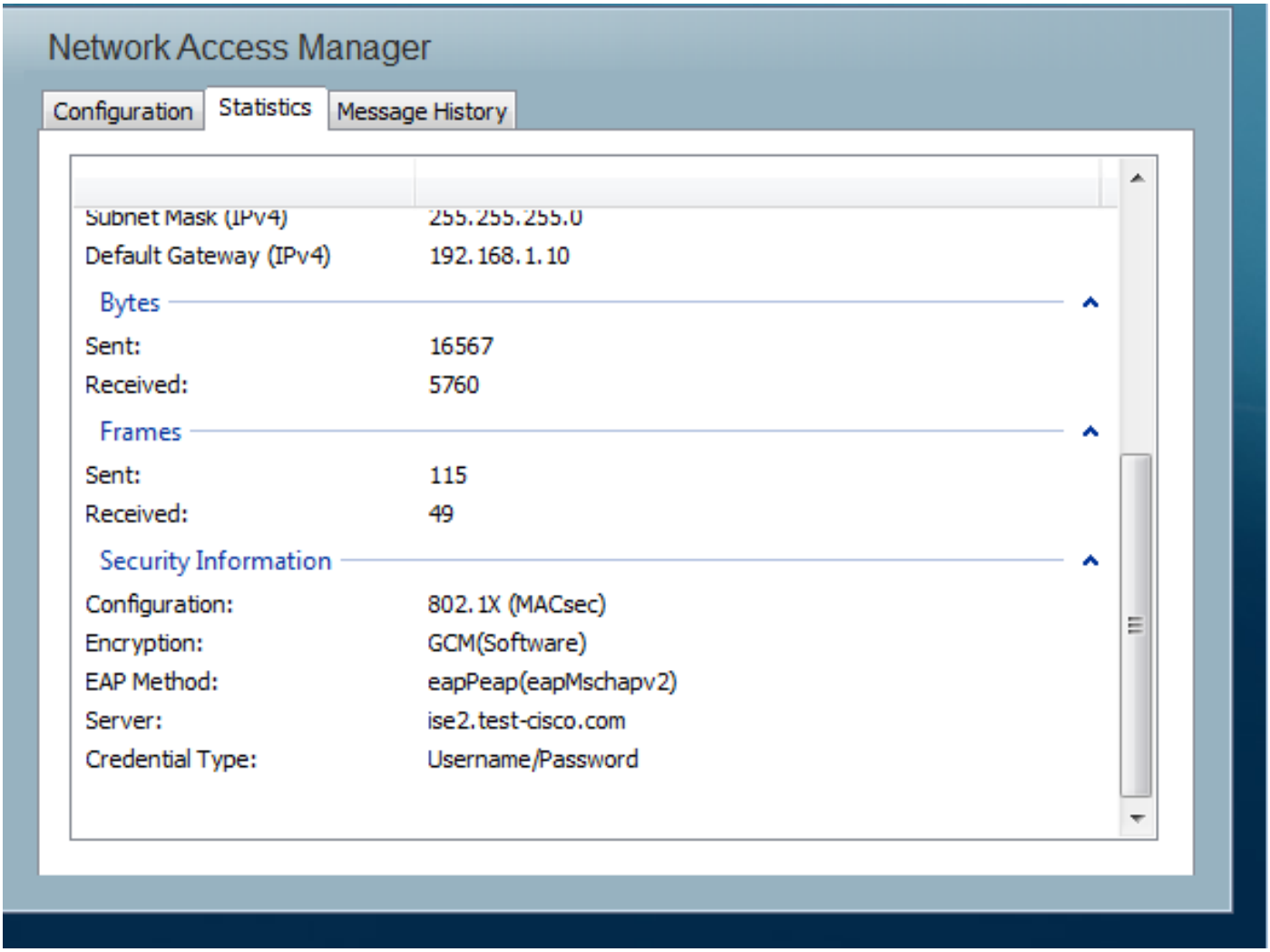
```
bsns-3750-5#show authentication sessions interface g1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5699.36ce
           IP Address:  192.168.1.201
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  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
```

As estatísticas de MACsec no switch fornecem os detalhes em relação à configuração de política local, identificadores de canal seguro (SCIs) para tráfego recebido/enviado e também estatísticas e erros de porta.

```
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
```

No AnyConnect, as estatísticas indicam o uso de criptografia e as estatísticas de pacotes.



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Depurações para um cenário funcional

Ative as depurações no switch (algumas saídas foram omitidas para maior clareza).

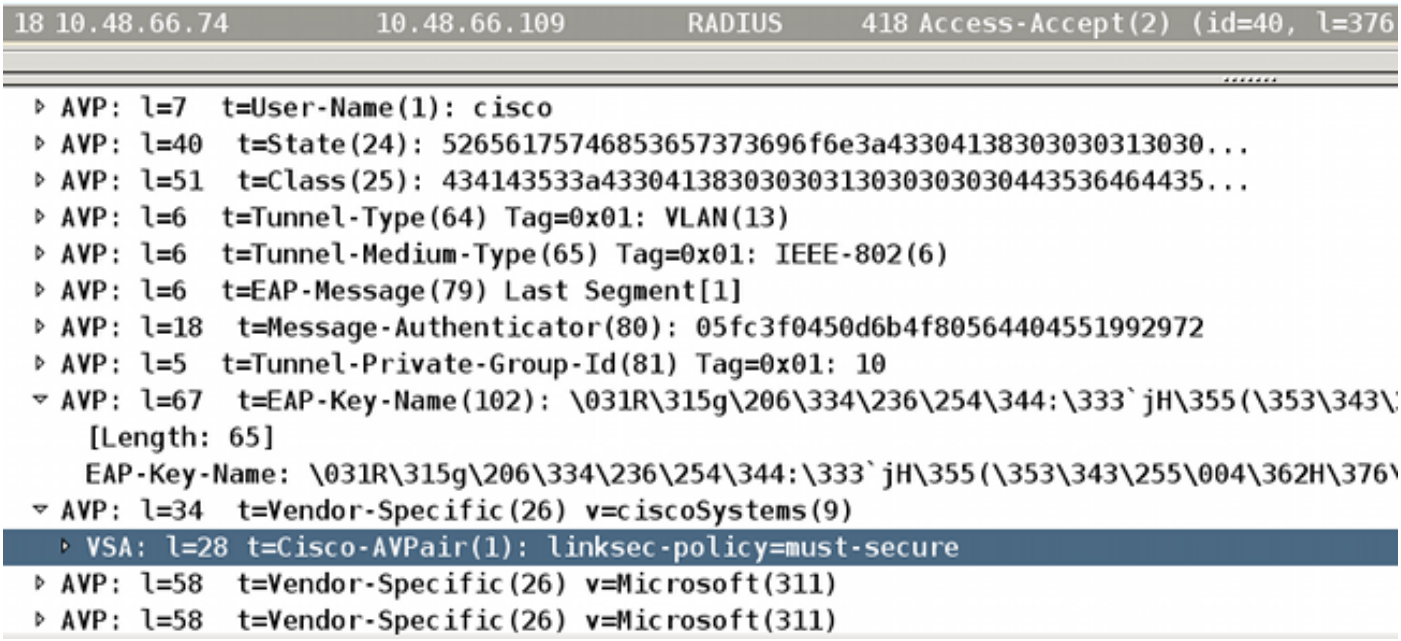
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

Depois que uma sessão 802.1x é estabelecida, vários pacotes EAP são trocados pelo EAPOL. A última resposta bem-sucedida do ISE (sucesso EAP) transportada dentro do Radius-Acccept também inclui vários atributos do 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 é usado para a sessão MKA. A política de linksec força o switch a usar o MACsec (falha na autorização se isso não estiver concluído). Esses atributos também podem ser verificados nas capturas de pacotes.



Autenticação bem-sucedida.

```
%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
```

O switch aplica os atributos (eles incluem um número de VLAN opcional que também foi enviado).

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

Em seguida, o switch inicia a sessão MKA quando envia e recebe pacotes 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
```

Depois que 4 identificadores seguros de troca de pacotes são criados junto com a associação de segurança Receber (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
```

A sessão foi concluída e a associação de segurança Transmit (TX) foi adicionada.

```
%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/
```

A política "must-secure" é correspondida e a autorização é bem-sucedida.

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

A cada 2 segundos, os pacotes de saudação do MKA são trocados para garantir que todos os participantes estejam 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
```

Depurações para um cenário com falha

Quando o requerente não está configurado para MKA e o ISE solicita criptografia após uma autenticação 802.1x bem-sucedida:

```
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
```

O switch tenta iniciar uma sessão MKA quando envia 5 pacotes 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
```

E finalmente o tempo limite e falha na autorização.

```
 %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
```

A sessão 802.1x relata autenticação bem-sucedida, mas falha na autorização.

```
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
```

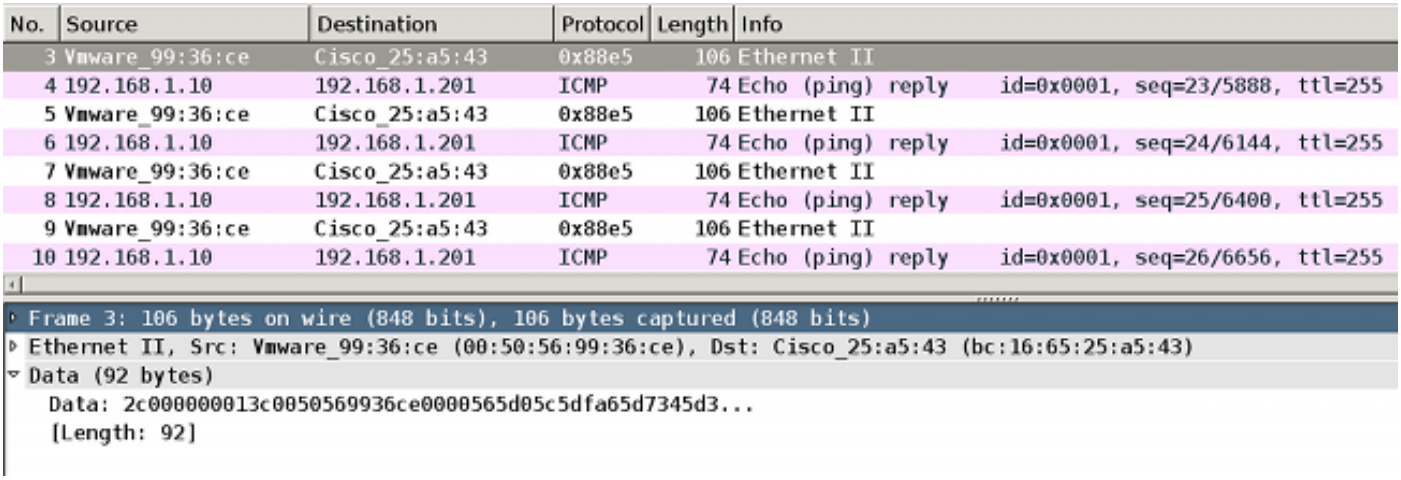
O tráfego de dados será bloqueado.

Capturas de pacotes

Quando o tráfego é capturado no site suplicante 4 as solicitações/respostas de eco ICMP (Internet Control Message Protocol) são enviadas e recebidas, haverá:

- 4 solicitações de eco ICMP criptografadas enviadas ao switch (88e5 é reservado para 802.1AE)
- 4 respostas de eco ICMP descriptografadas recebidas

Isso é devido ao modo como o AnyConnect se conecta à API do Windows (antes da libpcap quando os pacotes são enviados e antes da libpcap quando os pacotes são recebidos):



> **Note**: Não há suporte para a capacidade de detectar tráfego MKA ou 802.1AE no switch com recursos como o Switched Port Analyzer (SPAN) ou o Embedded Packet Capture (EPC).

Modos MACsec e 802.1x

Nem todos os modos 802.1x são suportados para MACsec.

O *guia de instruções do Cisco TrustSec 3.0: A Introdução ao MACsec e ao NDAC* afirma que:

- **Modo de host único**: **O MACsec é totalmente suportado** no modo de host único. Nesse modo, somente um único endereço MAC ou IP pode ser autenticado e protegido com MACsec. Se um endereço MAC diferente for detectado na porta após a autenticação de um ponto final, uma violação de segurança será acionada na porta.
- **Modo de autenticação multidomínio (MDA - Multi-Domain Authentication)**: Nesse modo, um endpoint pode estar no domínio de dados e outro endpoint pode estar no domínio de voz. **O MACsec é totalmente suportado no modo MDA**. Se ambos os endpoints tiverem capacidade de MACsec, cada um será protegido por sua própria sessão MACsec independente. Se apenas um endpoint for compatível com MACsec, esse endpoint poderá ser protegido enquanto o outro endpoint envia tráfego em branco.
- **Modo multiautenticação**: Nesse modo, um número praticamente ilimitado de endpoints pode ser autenticado em uma única porta do switch. **Não há suporte para MACsec neste modo.**
- **Modo multihost**: Embora o uso de MACsec neste modo seja tecnicamente possível, **não é recomendado**. No modo multihost, o primeiro endpoint na porta é autenticado e, em seguida, todos os endpoints adicionais serão permitidos na rede por meio da primeira autorização. O MACsec funcionaria com o primeiro host conectado, mas nenhum tráfego de outro endpoint passaria, pois não seria tráfego criptografado.

Informações Relacionadas

- Guia de configuração do Cisco TrustSec para 3750
- Guia de configuração do Cisco TrustSec para ASA 9.1
- Serviços de rede baseados em identidade: Segurança MAC
- Cloud TrustSec com 802.1x MACsec no exemplo de configuração do switch Catalyst 3750X Series
- Exemplo de configuração do TrustSec com ASA e o switch Catalyst 3750-X Series e Guia de solução de problemas
- Implantação e roteiro do Cisco TrustSec
- Suporte Técnico e Documentação - Cisco Systems