# Criptografia do Interruptor-host de MACsec com Cisco AnyConnect e exemplo de configuração ISE

ID do Documento: 117277

Atualizado em: janeiro 31, 2014

Contribuído por Michal Garcarz e por Machulik romano, engenheiros de TAC da Cisco.



## Produtos Relacionados

- Security
- 802.1x
- Cisco Identity Services Engine

## Índice

# Introdução

Este documento fornece um exemplo de configuração para a criptografia da Segurança do Media Access Control (MACsec) entre um suplicante do 802.1x (Mobile Security de Cisco AnyConnect) e um autenticador (interruptor). Os Cisco Identity Services Engine (ISE) são usados como a autenticação e o servidor da política.

MACsec é estandardizado em 802.1AE e apoiado em Cisco 3750X, 3560X, e 4500 Switches SUP7E. 802.1AE define a criptografia de link sobre as redes ligadas com fio que usam chaves fora da banda. Aquelas chaves de criptografia são negociadas com o protocolo do acordo da chave de MACsec (MKA) que é utilizado após a autenticação bem sucedida do 802.1x. MKA é estandardizado na IEEE 802.1X-2010.

Um pacote é cifrado somente no link entre o PC e o interruptor (criptografia Point-to-Point). O pacote recebido pelo interruptor é decifrado e enviado através de uplinks unencrypted. A fim cifrar a transmissão entre o Switches, a criptografia do switch-switch é recomendada. Para essa criptografia, o protocolo da associação de segurança (SAP) é usado para negociar e regenerar chaves. SAP é um protocolo do acordo da chave do prestandard desenvolvido por Cisco.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

## Componentes Utilizados

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

- Sistemas operacionais de Microsoft Windows 7 e do Microsoft Windows XP
- Software de Cisco 3750X, versão 15.0 e mais recente
- Software de Cisco ISE, versão 1.1.4 e mais recente
- Mobile Security de Cisco AnyConnect com gerente do acesso de rede (NAM), versão 3.1 e mais recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

# Configurar

## Diagrama da rede e fluxo de tráfego

**Etapa 1.** O suplicante (AnyConnect NAM) começa a sessão do 802.1x. O interruptor é o autenticador e o ISE é o Authentication Server. O protocolo extensible authentication sobre o protocolo LAN (EAPOL) é usado como um transporte para o EAP entre o suplicante e o interruptor. O RAIO é usado como um protocolo de transporte para o EAP entre o interruptor e o ISE. O desvio da autenticação de MAC (MAB) não pode ser usado, porque as chaves EAPOL precisam de ser retornadas do ISE e de ser usadas para a sessão do acordo da chave de MACsec (MKA).

**Etapa 2.** Depois que a sessão do 802.1x está completa, o interruptor inicia uma sessão MKA com EAPOL como um protocolo de transporte. Se o suplicante é configurado corretamente, as chaves para a criptografia simétrica do 128-bit AES-GCM (Galois/modo contrário) combinam.

**Etapa 3.** Todos os pacotes subsequente entre o suplicante e o interruptor são cifrados (encapsulamento 802.1AE).

## Configurações

### ISE

A configuração ISE envolve uma encenação típica do 802.1x com uma exceção ao perfil da autorização que pôde incluir políticas de criptografia.

Escolha a **administração > recursos de rede > dispositivos de rede** a fim adicionar o interruptor como um dispositivo de rede. Incorpore uma chave preshared do RAIO (segredo compartilhado).

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

Escolha a **administração > o Gerenciamento de identidades > os usuários** a fim definir localmente o usuário “Cisco”.

O perfil da autorização pôde incluir políticas de criptografia. Segundo as indicações deste exemplo, escolha a **política > os resultados > a autorização perfila** a fim ver os retornos da informação ISE ao interruptor que a criptografia de link é imperativa. Também, o número de VLAN (10) foi configurado.

Escolha a **política > a autorização** a fim usar o perfil da autorização na regra da autorização. Este exemplo retorna o perfil configurado para o usuário “Cisco”. Se o 802.1x é bem sucedido, os retornos ISE Raio-aceitam ao interruptor com o linksec-policy=must-secure de Cisco AVPair. Esse atributo força o interruptor para iniciar uma sessão MKA. Se essa sessão falha, a autorização do 802.1x no interruptor igualmente falha.

### Switch

As configurações de porta típicas do 802.1x incluem (parcela 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 local MKA é criada e aplicada à relação. Também, MACsec é permitido na relação.

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

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

A política local MKA permite que você configure os ajustes detalhados que não podem ser empurrados do ISE. A política local MKA é opcional.

### AnyConnect NAM

O perfil para o suplicante do 802.1x pode ser configurado manualmente ou empurrado através de Cisco ASA. As próximas etapas apresentam uma configuração manual.

A fim controlar perfis NAM:

Adicionar um perfil novo do 802.1x com MACsec. Para o 802.1x, o protocolo extensible authentication protegido (PEAP) é usado (usuário configurado “Cisco” no ISE):

## Verificar

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

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

A sessão no interruptor deve ser autenticada e autorizado. O status de segurança deve “ser fixado”:

```
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 interruptor fornecem os detalhes com respeito ao ajuste da política local, aos identificadores do canal seguro (SCIs) para tráfego recebido/enviado, e igualmente às estatísticas de porta e aos erros.

```
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
```

Em AnyConnect, as estatísticas indicam o uso e as estatísticas de pacote da criptografia.

# Troubleshooting

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

## Debuga para uma encenação de trabalho

Permita debuga no interruptor (alguma saída foi omitida para maior 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
```

Depois que uma sessão do 802.1x é estabelecida, os pacotes EAP múltiplos estão trocados sobre o EAPOL. A última resposta bem sucedida do raio-Acccept interno levado ISE (sucesso EAP) igualmente inclui diversos 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  *
```

O EAP-Chave-nome é usado para a sessão MKA. A linksec-política força o interruptor para usar

MACsec (a autorização falha se aquela não está completa). Aqueles atributos podem igualmente ser verificados nas capturas de pacote de informação.

A autenticação é 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 interruptor aplica os atributos (estes incluem um número de VLAN opcional que seja enviado igualmente).

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

O interruptor começa então a sessão MKA quando envia e recebe pacotes EAPOL.

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

Depois que 4 identificadores seguros do intercâmbio de pacotes estão criados junto com a associação de segurança da recepção (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 é terminada e a associação de segurança transmitir (TX) é 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 “dever-segura” é combinada e a autorização é bem sucedida.

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

Cada pacotes Hello de 2 segundos MKA são trocados a fim assegurar-se de que todos os participantes estejam vivos.

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

## Debuga para uma encenação de falha

Quando o suplicante não é configurado para MKA e o ISE pede a criptografia após uma autenticação bem sucedida do 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
```

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

E cronometra finalmente para fora e falha a 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 do 802.1x relata a autenticação bem sucedida, mas a autorização falha.

```
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 obstruído.

## Capturas de pacote de informação

Quando o tráfego é capturado nas requisições de eco/respostas do Internet Control Message Protocol (ICMP) do local 4 do suplicante estão enviados e recebido, haverá:

- 4 cifraram as requisições de eco ICMP enviadas ao interruptor (88e5 é reservado para 802.1AE)
- 4 decifraram as respostas de eco ICMP recebidas

Isso é devido a como os ganchos de AnyConnect em Windows API (antes do libpcap quando os pacotes são enviados e antes do libpcap quando os pacotes são recebidos):

**Note**: A capacidade para aspirar o tráfego MKA ou 802.1AE no interruptor com características tais como o Switched Port Analyzer (SPAN) ou a captura de pacote de informação encaixada (EPC) não é apoiada.

### Modos de MACsec e de 802.1x

Não todos os modos do 802.1x são apoiados para MACsec.

*De Cisco TrustSec do 3.0 o guia Como: A introdução a MACsec e a NDAC* indica aquela:

- **Modo do host único**: **MACsec é apoiado inteiramente no** modo do host único. Neste modo, somente um único MAC ou endereço IP de Um ou Mais Servidores Cisco ICM NT podem ser autenticados e fixado com MACsec. Se um MAC address diferente está detectado na porta depois que um valor-limite autenticou, uma violação de segurança estará provocada na porta.
- **Modo da autenticação do Multi-domínio (MDA)**: Neste modo, um valor-limite pode estar no domínio dos dados e um outro valor-limite pode estar no domínio da Voz. **MACsec é apoiado inteiramente no modo MDA**. Se ambos os valores-limite são MACsec-capazes, cada um estará fixado por sua própria sessão independente de MACsec. Se somente um valor-limite é MACsec-capaz, esse valor-limite pode ser fixado quando o outro valor-limite enviar o tráfego na claro.
- **Modo da Multi-autenticação**: Neste modo, virtualmente um número ilimitado de valores-limite pode ser autenticado a uma porta do switch único. **MACsec não é apoiado neste modo.**
- **Modo do Multi-host**: Quando o uso de MACsec neste modo for tecnicamente possível, **não se recomenda**. No modo do Multi-host, o primeiro valor-limite na porta autentica, e todos os valores-limite adicionais serão permitidos então na rede através da primeira autorização. MACsec trabalharia com o primeiro host conectado, mas nenhum outro valor-limite? o tráfego s passaria realmente, desde que não seria tráfego criptografado.

## Informações Relacionadas

- Manual de configuração de Cisco TrustSec para 3750
- Manual de configuração de Cisco TrustSec para ASA 9.1
- Serviços de rede Identidade-baseados: Segurança MAC
- Nuvem de TrustSec com 802.1x MACsec no exemplo de configuração do Catalyst 3750X Series Switch
- O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e pesquisam defeitos o guia
- Desenvolvimento e mapa rodoviário de Cisco TrustSec
- Suporte Técnico e Documentação - Cisco Systems

# Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: janeiro 31, 2014
ID do Documento: 117277