MACsec Switch-host encryptie met Cisco AnyConnect en ISE Configuration Voorbeeld

Inhoud

Inleiding

Dit document biedt een configuratievoorbeeld voor Media Access Control Security (MACsec) encryptie tussen een 802.1x-smeekbede (Cisco AnyConnect Mobile Security) en een authenticator (switch). Cisco Identity Services Engine (ISE) wordt gebruikt als verificatie- en beleidsserver.

MACsec is gestandaardiseerd in 802.1AE en wordt ondersteund op Cisco 3750X, 3560X en 4500 SUP7E switches. 802.1AE definieert linkencryptie via bekabelde netwerken die gebruik maken van out-of-band toetsen. Deze encryptiesleutels worden onderhandeld met het protocol van MACsec Key Agreement (MKA), dat wordt gebruikt na succesvolle 802.1x-verificatie. MKA is gestandaardiseerd in IEEE 802.1X-2010.

Een pakket is alleen versleuteld op de koppeling tussen de pc en de switch (point-to-point encryptie). Het pakket dat door de switch wordt ontvangen wordt ontsleuteld en onversleuteld via uplinks. Om de overdracht tussen de switches te versleutelen, wordt een switch-switch-encryptie aanbevolen. Voor die encryptie wordt Security Association Protocol (SAP) gebruikt om sleutels te onderhandelen en te regenereren. SAP is een protocol dat is gebaseerd op een standaardsleutelovereenkomst dat door Cisco is ontwikkeld.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de configuratie van 802.1x
- Basiskennis van de CLI-configuratie van Catalyst-switches
- Ervaring met ISE-configuratie

Gebruikte componenten

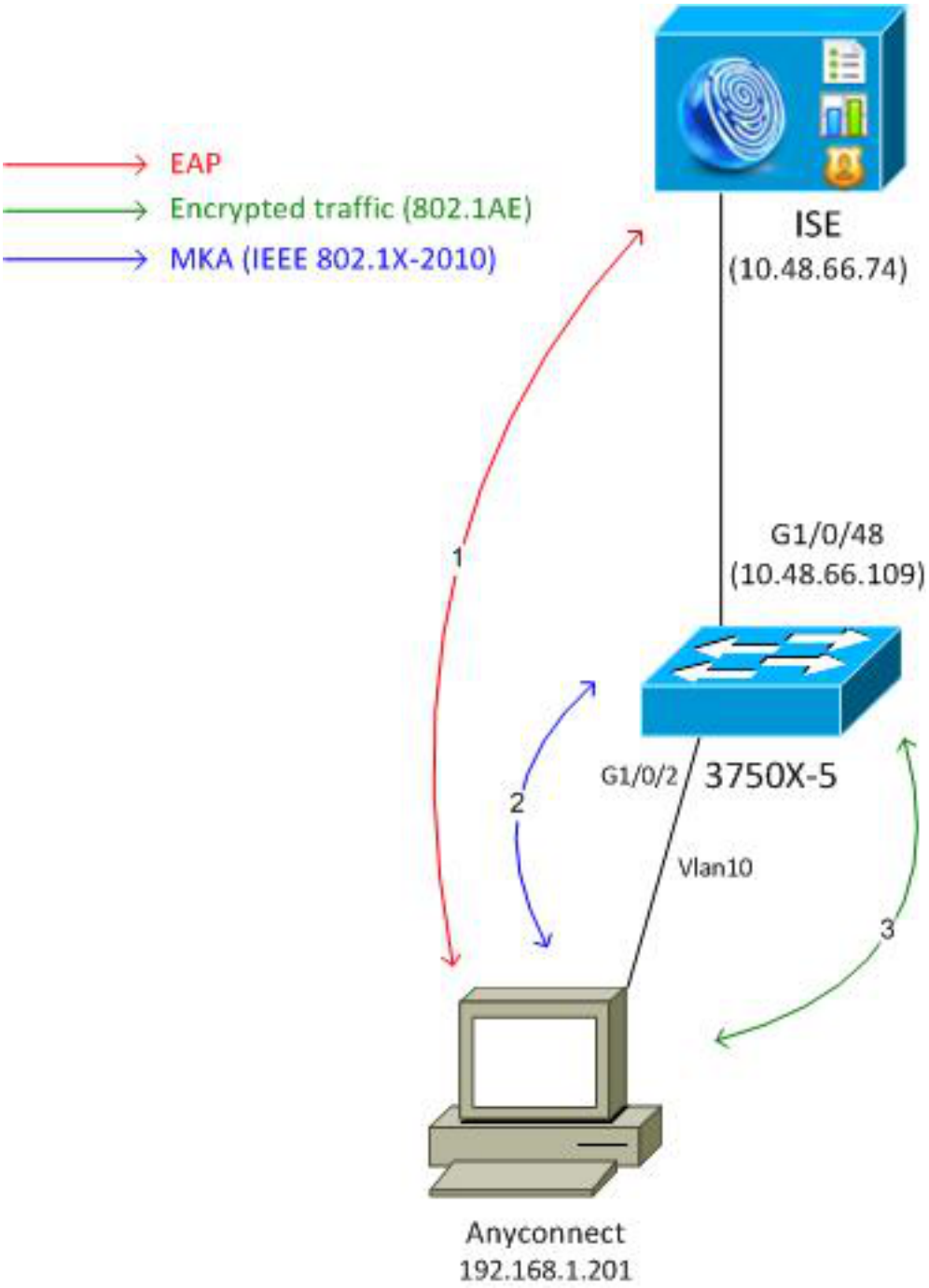
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7- en Microsoft Windows XP-besturingssystemen
- Cisco Catalyst 3750X software, versie 15.0 en hoger
- Cisco ISE-software, versie 1.1.4 en hoger
- Cisco AnyConnect mobiele beveiliging met Network Access Manager (NAM), versie 3.1 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkdiagram en verkeersstroom



Stap 1. De aanvrager (AnyConnect NAM) start de 802.1x-sessie. De switch is de authenticator en ISE is de authenticatieserver. Extensible Authentication Protocol over LAN (EAPOL) wordt gebruikt als transport voor EAP tussen de aanvrager en de switch. RADIUS wordt gebruikt als transportprotocol voor EAP tussen de switch en de ISE. MAC-verificatieBypass (MAB) kan niet worden gebruikt, omdat de EAPOL-toetsen van ISE moeten worden teruggestuurd en gebruikt voor de MACsec Key Agreement (MKA)-sessie.

Stap 2. Nadat de 802.1x-sessie is voltooid, start de switch een MKA-sessie met EAPOL als transportprotocol. Als de aanvrager correct is geconfigureerd, worden de toetsen voor symmetrische 128-bits AES-GCM (Galois/Teller Mode)-encryptie matchen.

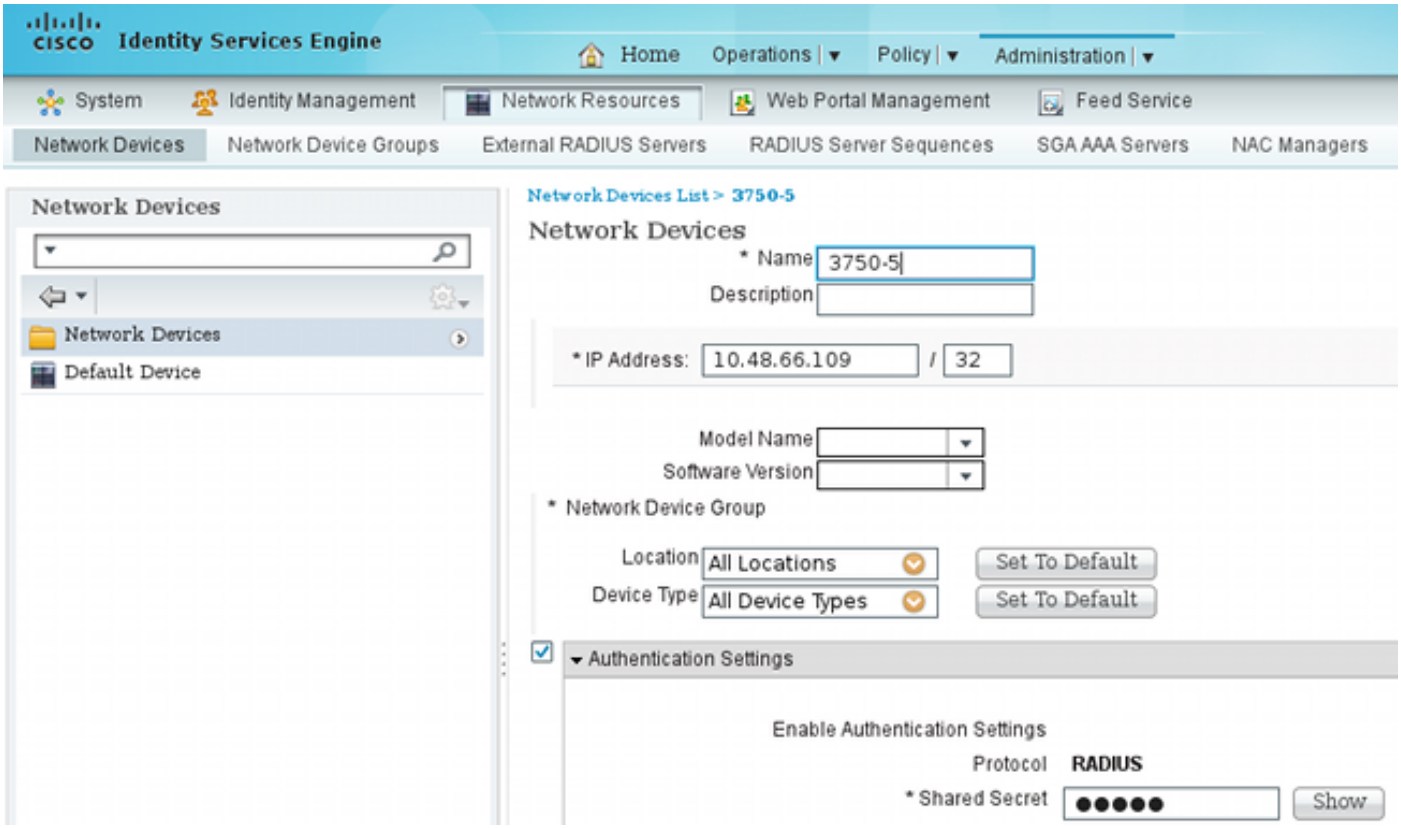
Stap 3. Alle volgende pakketten tussen de aanvrager en de switch worden versleuteld (802.1AE-insluiting).

Configuraties

ISE

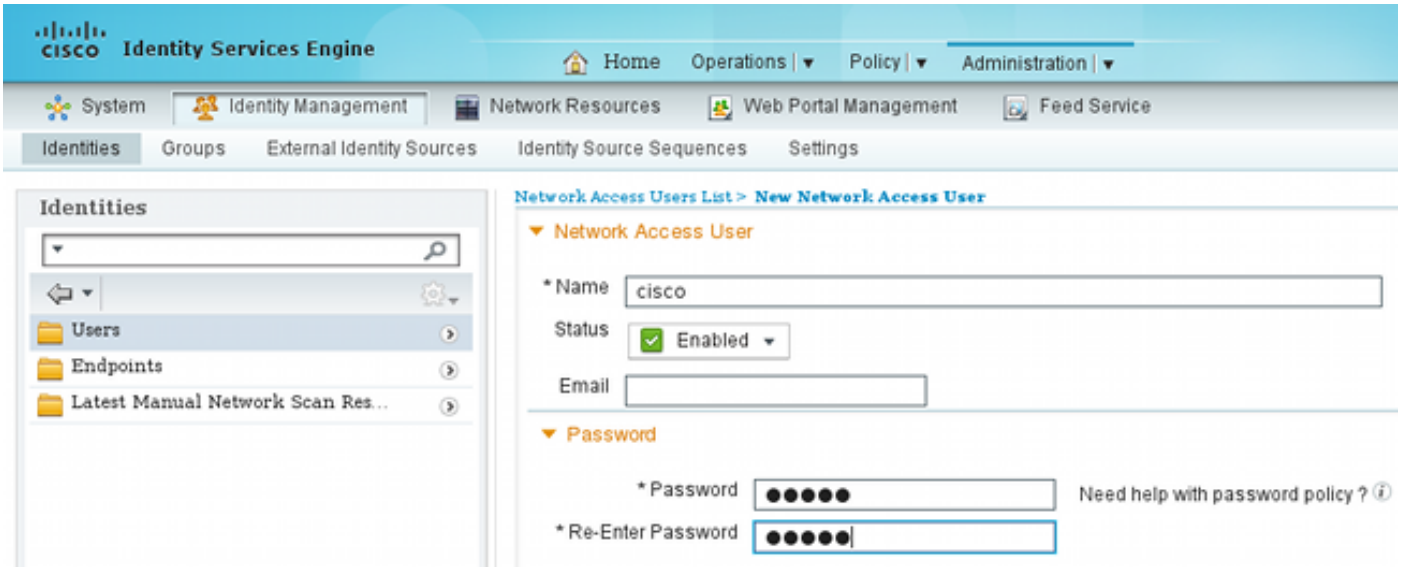
De ISE-configuratie omvat een typisch 802.1x-scenario met uitzondering van het machtigingsprofiel, dat ook een coderingsbeleid kan omvatten.

Kies **Beheer > Netwerkbronnen > Netwerkapparaten** om de switch als netwerkapparaat toe te voegen. Voer een vooraf gedeelde RADIUS-toets (gedeeld geheim) in.



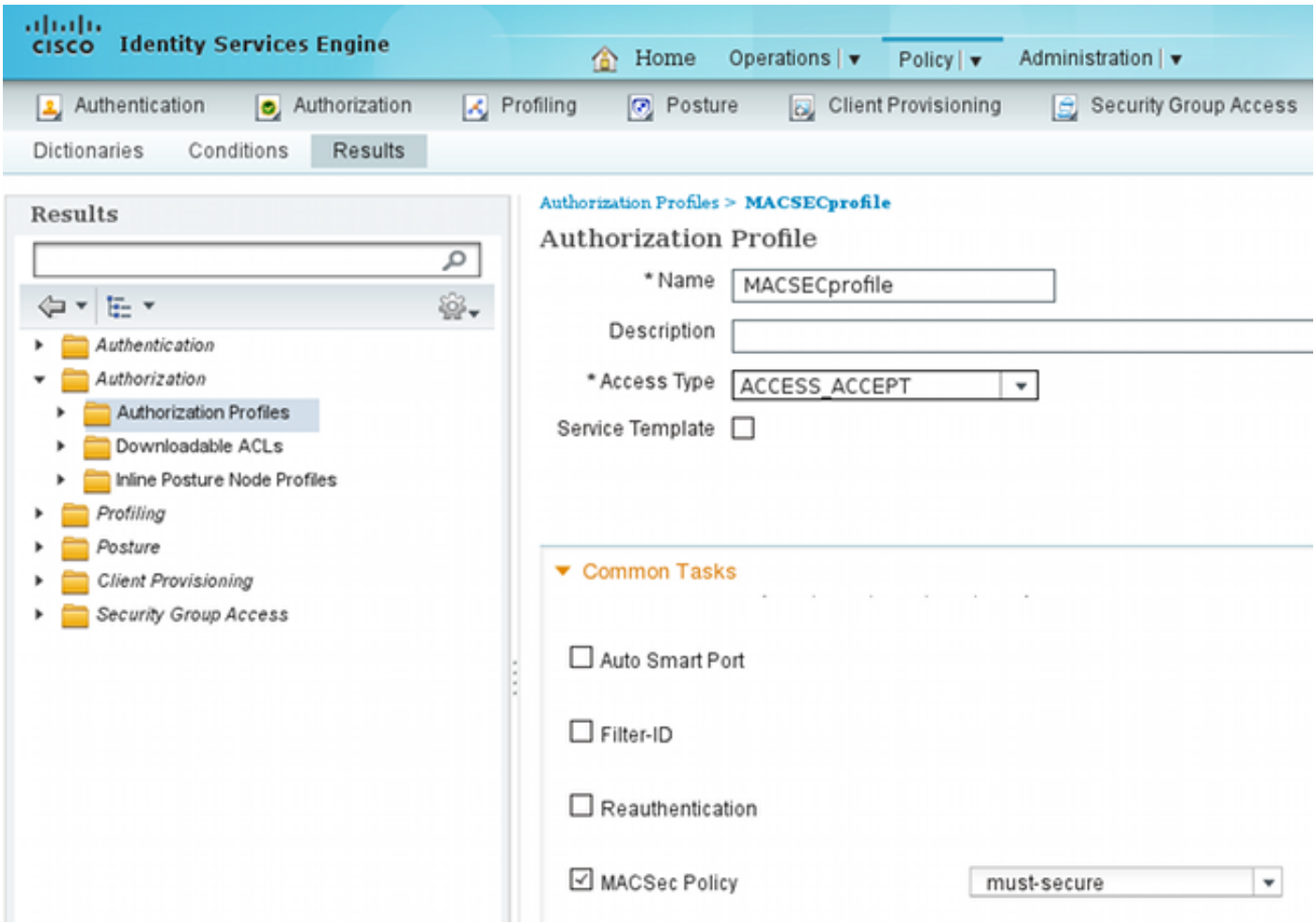
De standaard verificatieregel kan worden gebruikt (voor gebruikers die lokaal op ISE zijn gedefinieerd).

Kies **Beheer > Identity Management > Gebruikers** om de gebruiker "cisco" lokaal te definiëren.

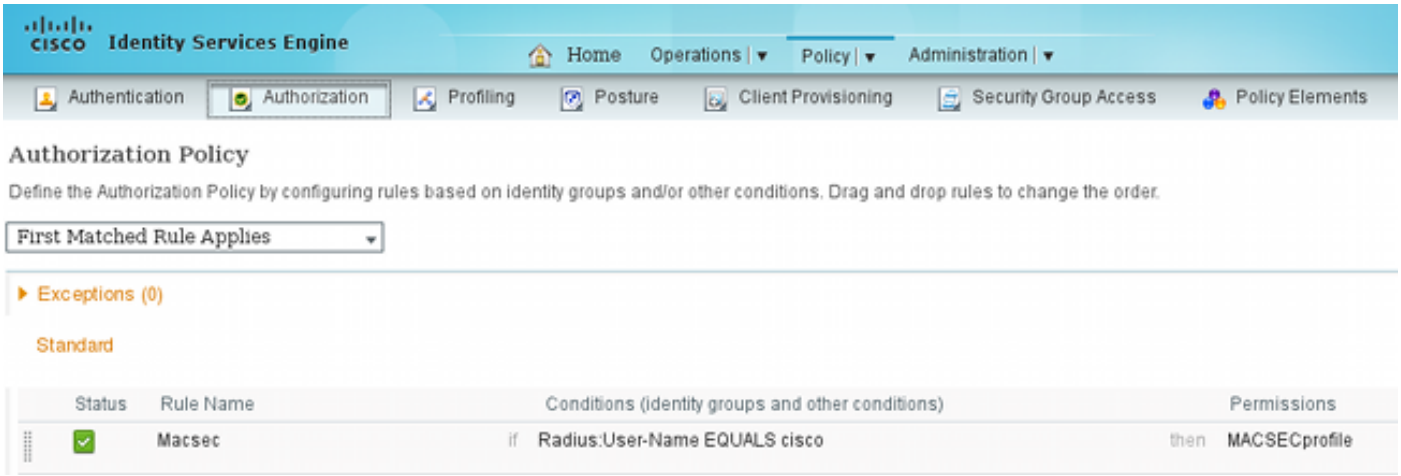


Het autorisatieprofiel kan een coderingsbeleid omvatten. Zoals in dit voorbeeld wordt getoond, kies **Beleid > Resultaten > Vergunningsprofielen** om de informatie terug te zien ISE naar de switch

die de verbindingsencryptie verplicht is. Ook is het VLAN-nummer (10) geconfigureerd.



Kies **beleid > Toestemming** om het vergunningprofiel in de vergunningsregel te gebruiken. Dit voorbeeld retourneert het geconfigureerde profiel voor gebruiker "cisco". Als 802.1x succesvol is, keert ISE Radius-Accept terug aan de switch met Cisco AVPair linksec-beleid=must-secure. Deze eigenschap dwingt de switch om een MKA-sessie te initiëren. Als die sessie mislukt, wordt de 802.1x-autorisatie op de switch ook mislukt.



Switch

De populaire 802.1x poortinstellingen omvatten (weergegeven bovenste gedeelte):

```
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
```

Het lokale MKA-beleid wordt gecreëerd en toegepast op de interface. MACsec is ook ingeschakeld op de interface.

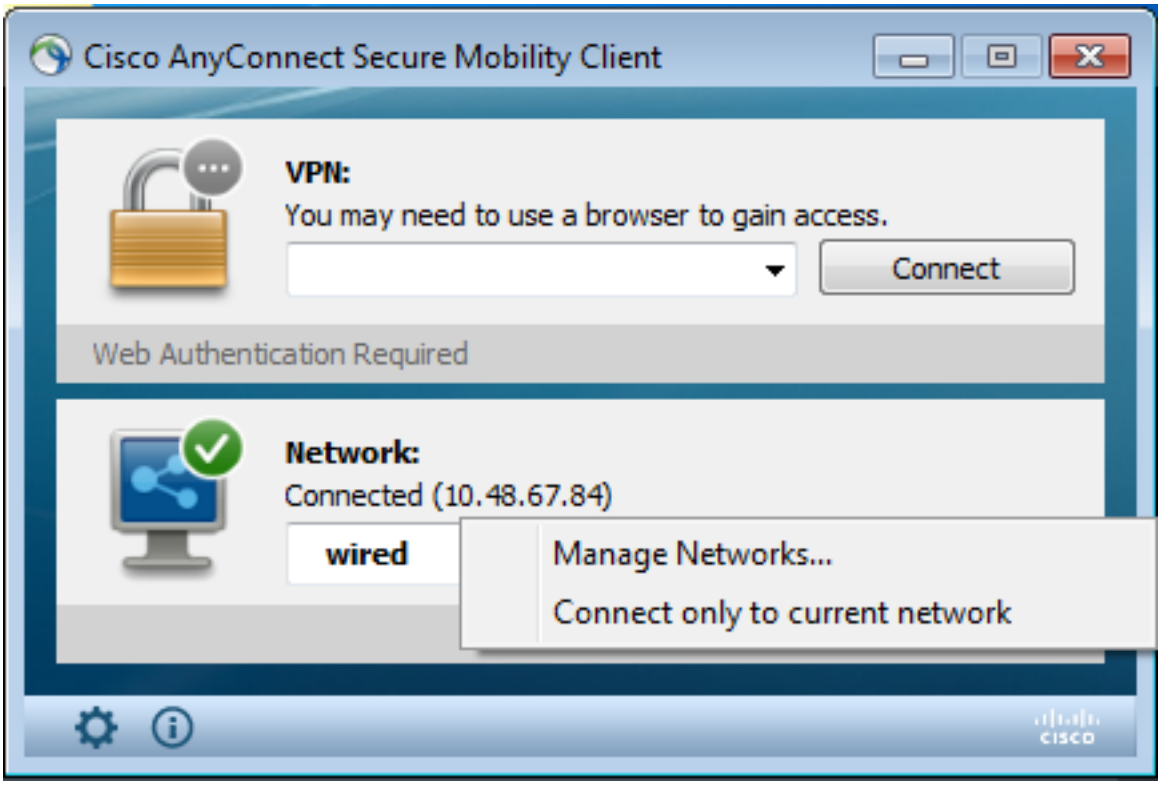
```
mka policy mka-policy
 replay-protection window-size 5000

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

Met het lokale MKA-beleid kunt u gedetailleerde instellingen configureren die niet vanaf de ISE kunnen worden geduwd. Het lokale MKA-beleid is optioneel.

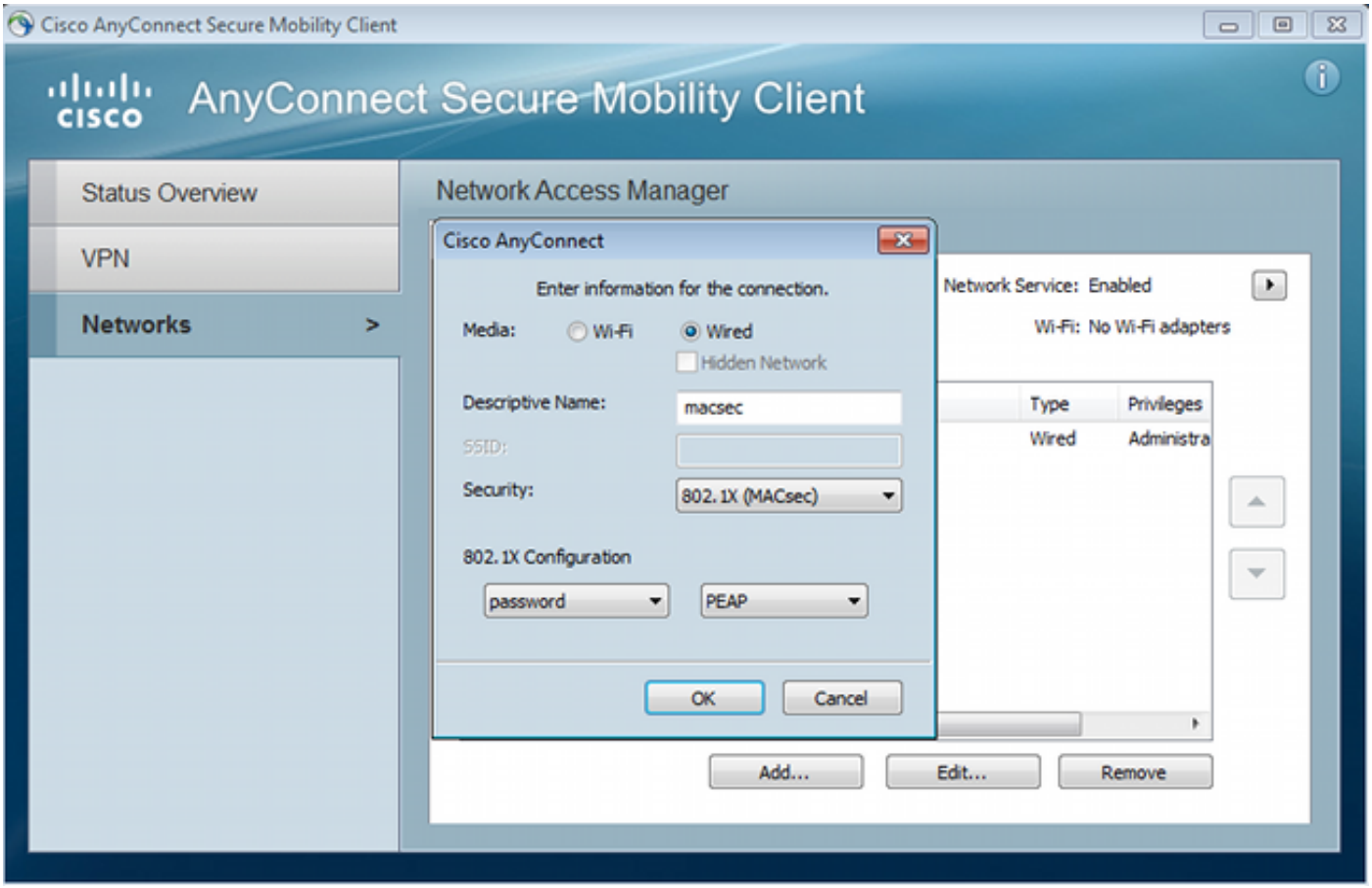
AnyConnect-NAM

Het profiel voor de 802.1x-applicatie kan handmatig worden ingesteld of via Cisco ASA worden geduwd. De volgende stappen bieden een handmatige configuratie aan.

Zo beheert u NAM-profielen:



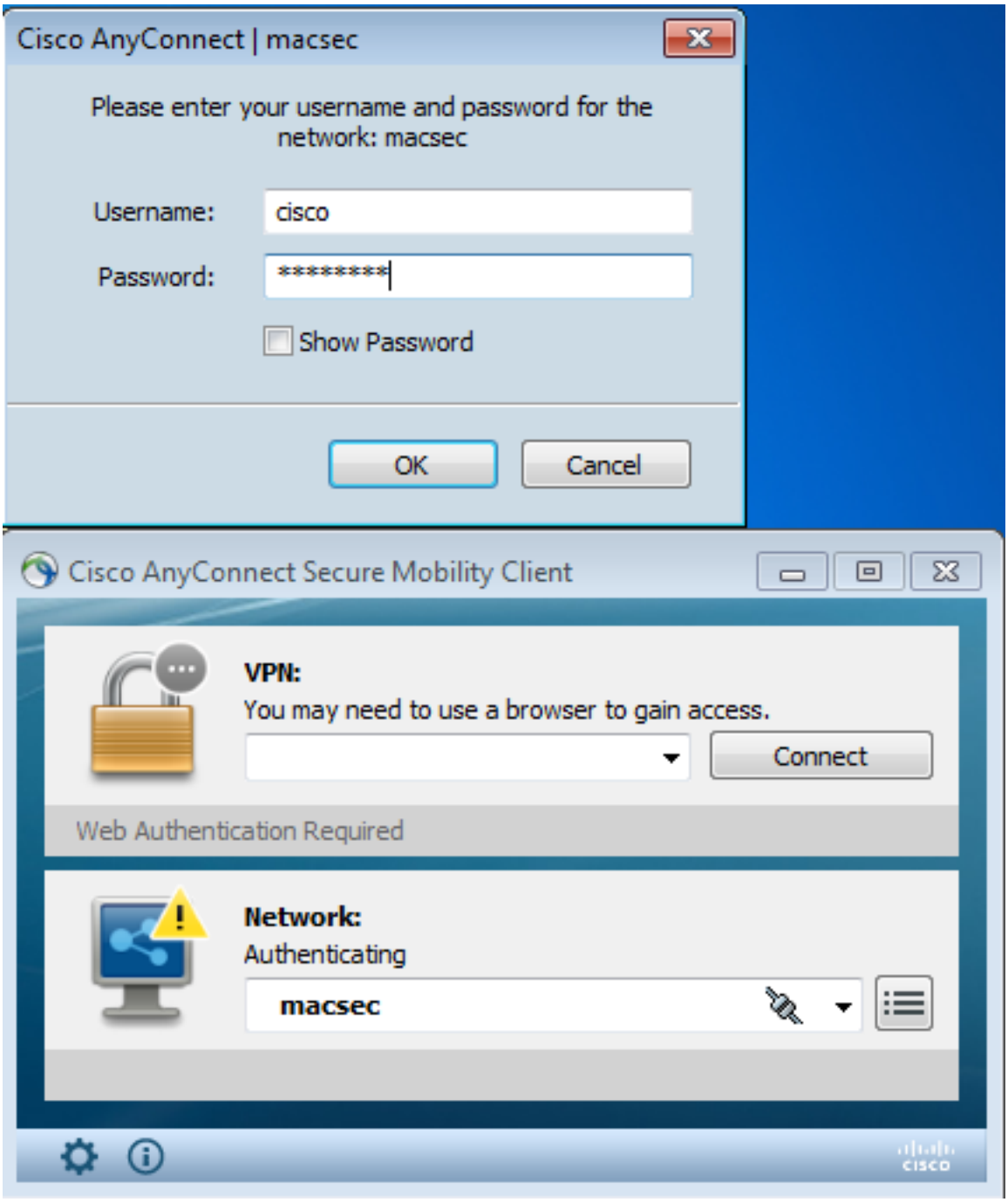
Voeg een nieuw 802.1x-profiel toe met MACsec. Voor 802.1x wordt het Protected Extensible Authentication Protocol (PEAP) gebruikt (geconfigureerde gebruiker "cisco" op ISE):



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Voor de AnyConnect NAM die voor EAP-PEAP is ingesteld, zijn correcte aanmeldingsgegevens nodig.



De sessie over de switch moet gewaarmerkt en geautoriseerd worden. De veiligheidsstatus dient "beveiligd" te zijn:

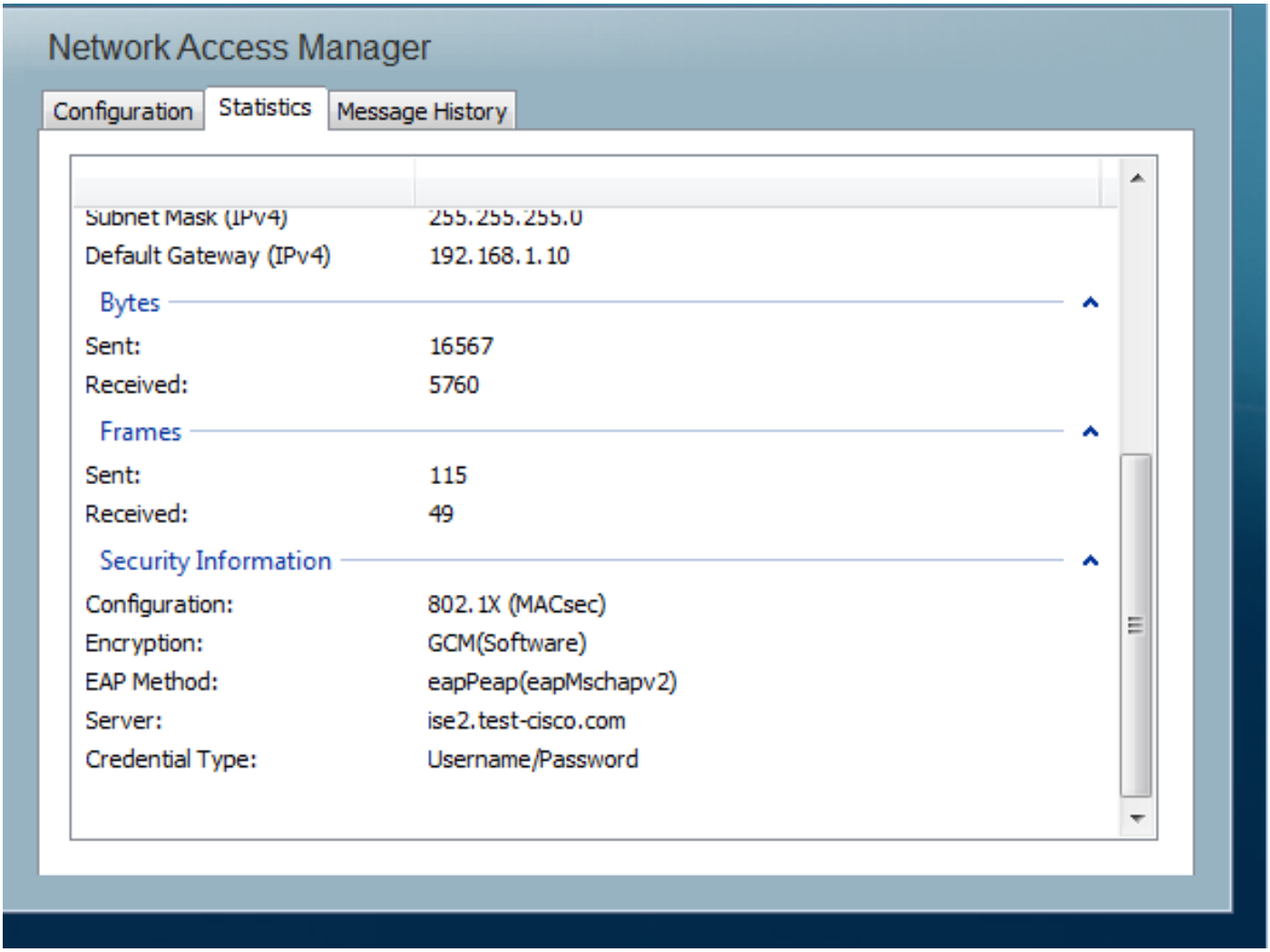
```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must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

De MACsec-statistieken over de switch geven de details met betrekking tot de plaatselijke beleidsinstelling, veilige kanaalidentificatoren (SCI's) voor ontvangen/verzonden verkeer, en ook havenstatistieken en -fouten.

```
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
```

Op AnyConnect duiden de statistieken op coderingsgebruik en pakketstatistieken.



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Debugs voor een werkscenario

Schakel debugs in op de switch (sommige uitvoer is voor de duidelijkheid weggelaten).

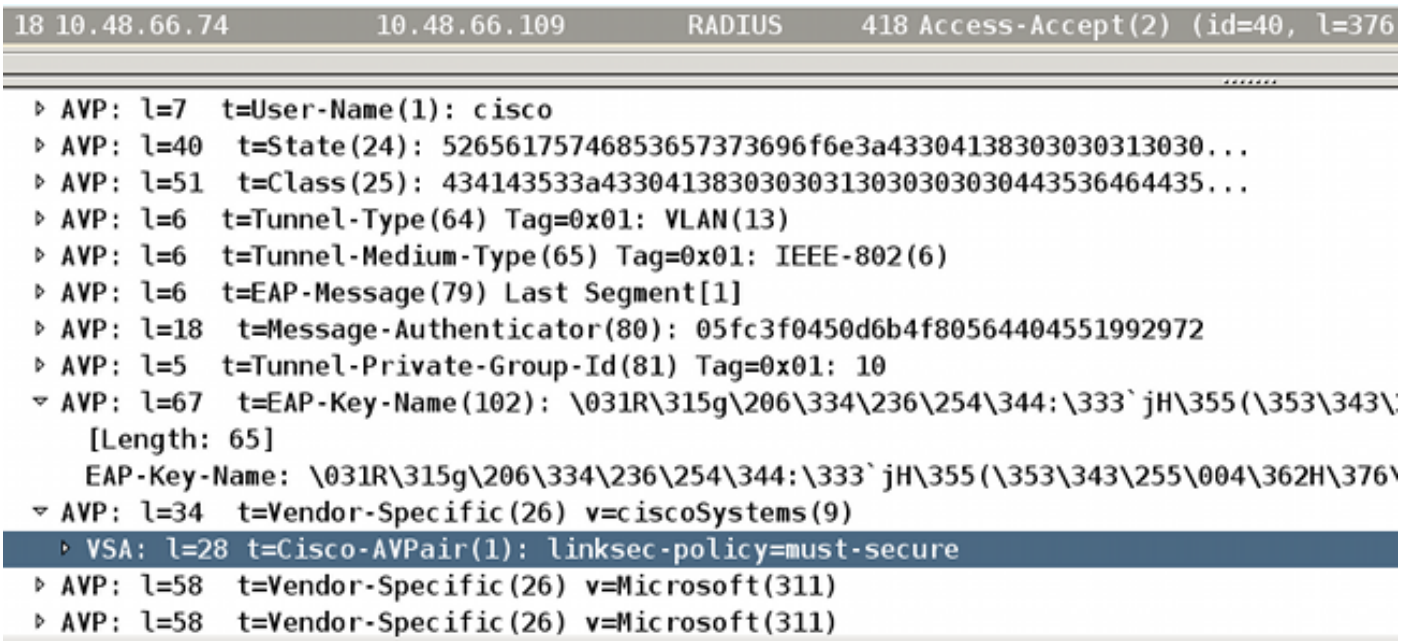
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

Na het opzetten van een 802.1x-sessie worden er meerdere MAP-pakketten uitgewisseld via EAPOL. Het laatste succesvolle antwoord van de ISE (EAP-succes) dat werd uitgevoerd binnen Radius-Acccept bevat ook diverse Radius-eigenschappen.

```
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 wordt gebruikt voor de MKA-sessie. Het linksec-beleid dwingt de switch om MACsec (de autorisatie mislukt als dat niet volledig is) te gebruiken. Deze eigenschappen kunnen ook worden geverifieerd in de pakketvastlegging.



Verificatie is geslaagd.

```
%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
```

De switch past de eigenschappen toe (deze omvatten een optioneel VLAN aantal dat ook verzonden is).

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

De switch start vervolgens de MKA-sessie wanneer deze wordt verzonden en EAPOL-pakketten ontvangt.

```
%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
```

Na 4 pakketuitwisselingen worden de veilige identificatoren gecreëerd samen met de ontvangstbeveiliging (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
```

De sessie is beëindigd en de TX-beveiligingsvereniging (Transmit) is toegevoegd.

```
%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/
```

Het beleid "moet veilig" is gelijk aan dat van de autorisatie en de autorisatie is succesvol.

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

Om de 2 seconden worden MKA Hallo-pakketten uitgewisseld om er zeker van te zijn dat alle deelnemers nog leven.

```
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
```

Debugs voor een falend scenario

Wanneer de aanvrager niet voor MKA is geconfigureerd en ISE om encryptie vraagt na een succesvolle 802.1x-verificatie:

```
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
```

De switch probeert een MKA-sessie te starten wanneer er 5 EAPOL-pakketten worden verzonden.

```
%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
```

En eindelijk af en toe de vergunning niet.

```
 %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
```

De 802.1x-sessie meldt succesvolle authenticatie, maar heeft geen toestemming gegeven.

```
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
```

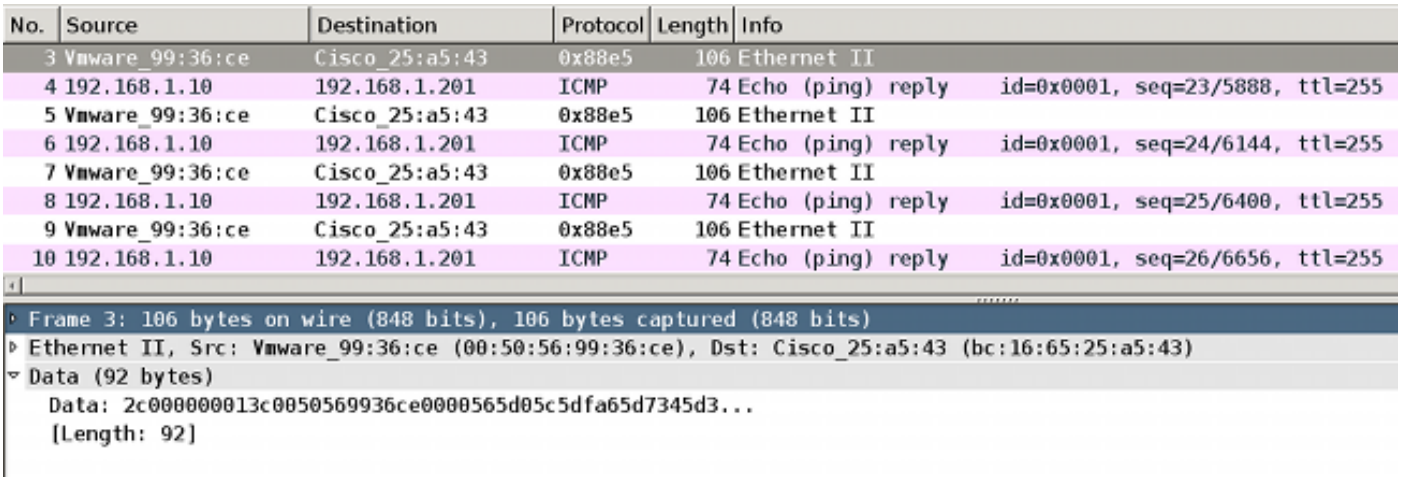
Het gegevensverkeer wordt geblokkeerd.

Packet Capture

Wanneer het verkeer wordt opgenomen op de aanvragende site 4 Internet Control Message Protocol (ICMP), worden de verzoeken/antwoorden verzonden en ontvangen,

- 4 versleutelde ICMP-echo-verzoeken die naar de switch zijn gestuurd (88e5 is gereserveerd voor 802.1AE)
- 4 ontvangen antwoorden van ICMP-echo's met decryptie

Dit is vanwege de manier waarop AnyConnect op Windows API kan worden aangesloten (vóór libpcap wanneer pakketten worden verzonden en vóór libpcap wanneer pakketten worden ontvangen):



Opmerking: De mogelijkheid om MKA- of 802.1AE-verkeer op de switch te doorsluizen met functies zoals Switched Port Analyzer (SPAN) of Embedded Packet Capture (EPC) wordt niet ondersteund.

MACsec en 802.1x-modellen

Niet alle 802.1x-modi worden ondersteund voor MACsec.

De *Cisco TrustSEC 3.0 Hoe-te gids: In de introductie van MACsec en NDAC* staat:

- **Single-Host Mode**: **MACsec wordt volledig ondersteund** in single-host modus. In deze modus kan slechts één MAC- of IP-adres als zodanig worden geauthentiseerd en beveiligd met MACsec. Als een ander MAC-adres op de poort wordt gedetecteerd nadat een eindpunt voor verificatie is geweest, zal er een security schending op de poort worden geactiveerd.
- **MDA-modus (Multi-Domain Authentication)**: In deze modus kan één eindpunt op het data domein zijn en kan een ander eindpunt op het voice-domein zijn. **MACsec wordt volledig ondersteund in MDA-modus**. Als beide eindpunten MACsec-mogelijk zijn, zullen beide worden beveiligd door de eigen onafhankelijke MACsec-sessie. Als slechts één eindpunt MACsec-geschikt is, kan dat eindpunt worden beveiligd terwijl het andere eindpunt verkeer in de helder stuurt.
- **Multi-verificatiemodus**: In deze modus kan een vrijwel onbeperkt aantal eindpunten worden geauthentiseerd naar één switch poort. **MACsec wordt in deze modus niet ondersteund.**
- **Multi-hostmodus**: Terwijl het gebruik van MACsec in deze modus technisch mogelijk is, **wordt het niet aanbevolen**. In Multi-Host Mode wordt het eerste eindpunt op de haven authentiek, en dan zullen om het even welke extra eindpunten op het netwerk via de eerste vergunning worden toegestaan. MACsec zou met de eerste aangesloten host werken, maar geen ander eindpunt zou in feite het verkeer passeren omdat het niet versleuteld verkeer zou zijn.

Gerelateerde informatie

- Cisco TrustSec-configuratiegids voor 3750
- Cisco TrustSec-configuratiegids voor ASA 9.1
- Op identiteit gebaseerde netwerkservices: MAC-beveiliging
- TrustSec-cloud met 802.1x MACsec op Catalyst 3750X Series Switch-configuratievoorbeeld
- ASA en Catalyst 3750X Series Switch TrustSec Configuration-voorbeeld en probleemoplossing
- Cisco TrustSec-implementatie en RoadMap
- Technische ondersteuning en documentatie – Cisco Systems