MACsec-Switch-Host-Verschlüsselung mit Cisco AnyConnect und ISE - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel für die MACsec-Verschlüsselung (Media Access Control Security) zwischen einer 802.1x-Komponente (Cisco AnyConnect Mobile Security) und einem Authentifizierer (Switch). Cisco Identity Services Engines (ISE) werden als Authentifizierungs- und Richtlinienserver verwendet.

MACsec ist in 802.1AE standardisiert und wird von Cisco Switches der Serien 3750X, 3560X und 4500 SUP7E unterstützt. 802.1AE definiert die Link-Verschlüsselung über kabelgebundene Netzwerke, die Out-of-Band-Schlüssel verwenden. Diese Verschlüsselungsschlüssel werden mit dem MACsec Key Agreement (MKA)-Protokoll ausgehandelt, das nach erfolgreicher 802.1x-Authentifizierung verwendet wird. MKA ist in IEEE 802.1X-2010 standardisiert.

Ein Paket wird nur über die Verbindung zwischen PC und Switch verschlüsselt (Point-to-Point-Verschlüsselung). Das vom Switch empfangene Paket wird entschlüsselt und unverschlüsselt über Uplinks gesendet. Um die Übertragung zwischen den Switches zu verschlüsseln, wird eine Switch-Switch-Verschlüsselung empfohlen. Für diese Verschlüsselung wird das Security Association Protocol (SAP) verwendet, um Schlüssel auszuhandeln und neu zu generieren. SAP ist ein von Cisco entwickeltes Prestandard Key Agreement-Protokoll.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der 802.1x-Konfiguration
- Grundkenntnisse der CLI-Konfiguration von Catalyst Switches
- Erfahrung mit ISE-Konfiguration

Verwendete Komponenten

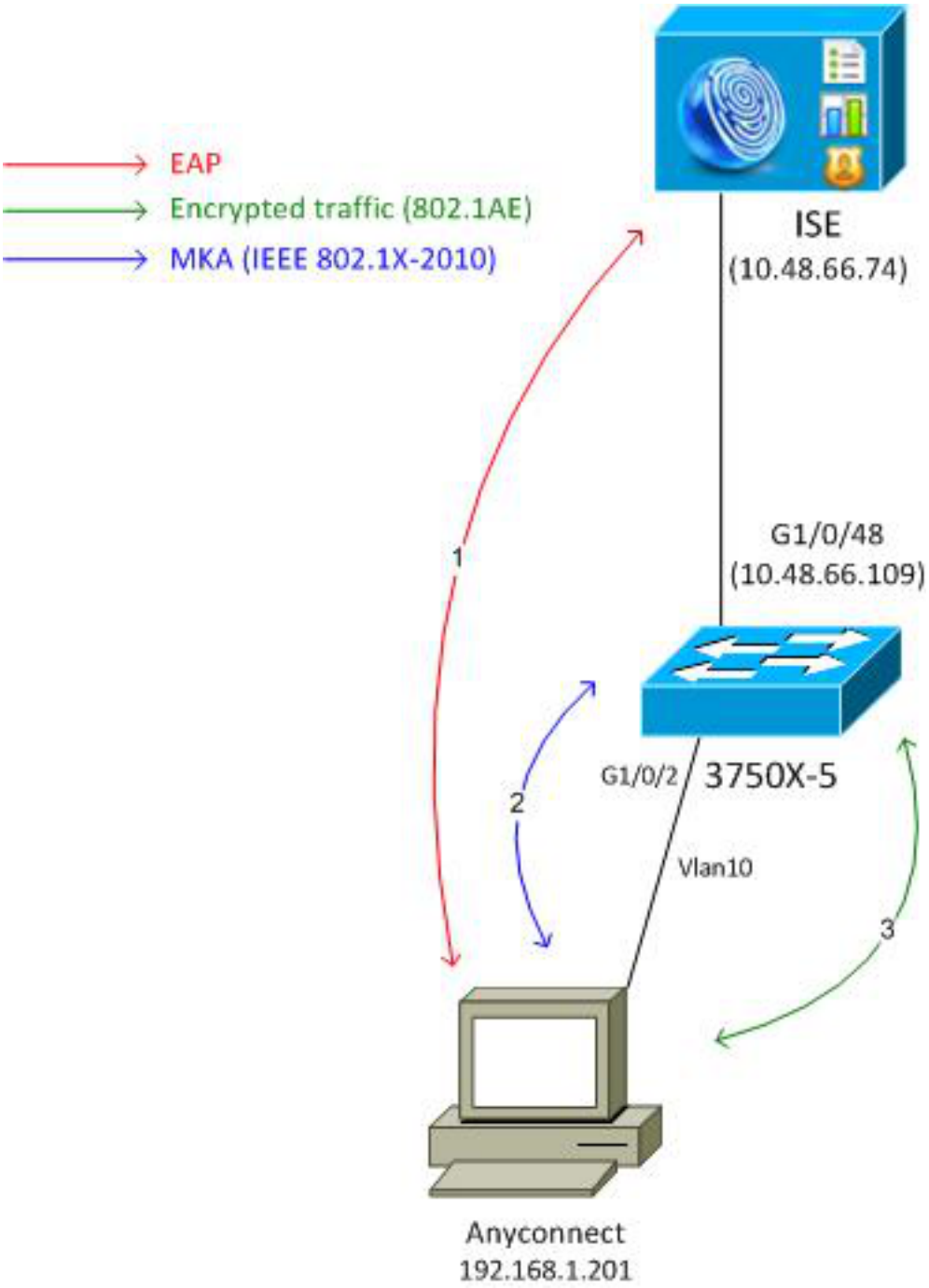
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7 und Microsoft Windows XP-Betriebssysteme
- Cisco 3750X Software, Version 15.0 und höher
- Cisco ISE Software, Version 1.1.4 und höher
- Cisco AnyConnect Mobile Security mit Network Access Manager (NAM), Version 3.1 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm und Datenverkehrsfluss



Schritt 1: Die Komponente (AnyConnect NAM) startet die 802.1x-Sitzung. Der Switch ist der Authentifizierer und die ISE der Authentifizierungsserver. Das Extensible Authentication Protocol over LAN (EAPOL)-Protokoll wird als Transport für EAP zwischen der Komponente und dem Switch verwendet. RADIUS wird als Transportprotokoll für EAP zwischen Switch und ISE verwendet. MAB (MAC Authentication Bypass) kann nicht verwendet werden, da EAPOL-Schlüssel von der ISE zurückgegeben und für die MACsec Key Agreement (MKA)-Sitzung verwendet werden müssen.

Schritt 2: Nach Abschluss der 802.1x-Sitzung startet der Switch eine MKA-Sitzung mit EAPOL als Transportprotokoll. Wenn die Komponente korrekt konfiguriert ist, stimmen die Schlüssel für die symmetrische 128-Bit-AES-GCM-Verschlüsselung (Galois/Counter Mode) überein.

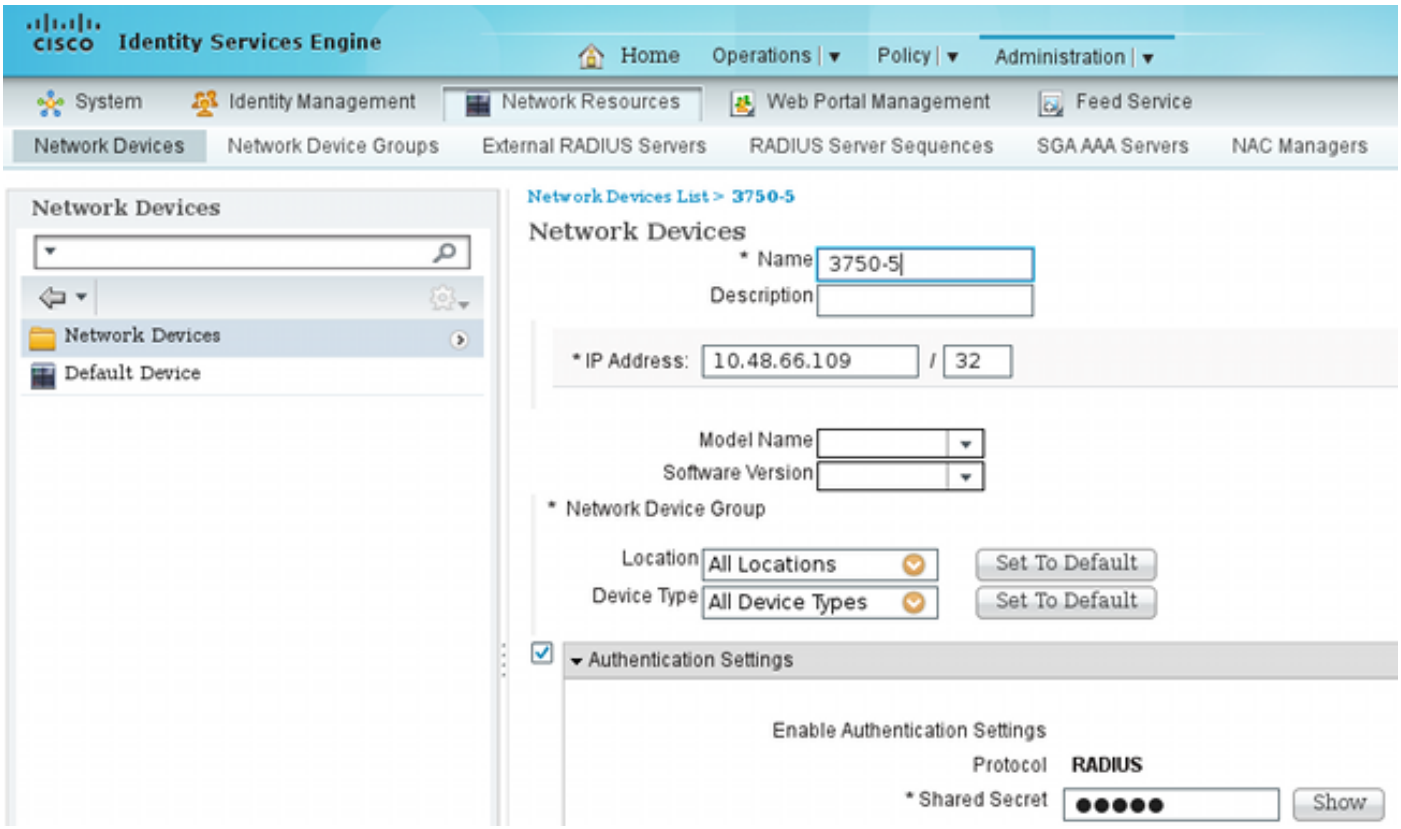
Schritt 3: Alle nachfolgenden Pakete zwischen der Komponente und dem Switch werden verschlüsselt (802.1AE-Kapselung).

Konfigurationen

ISE

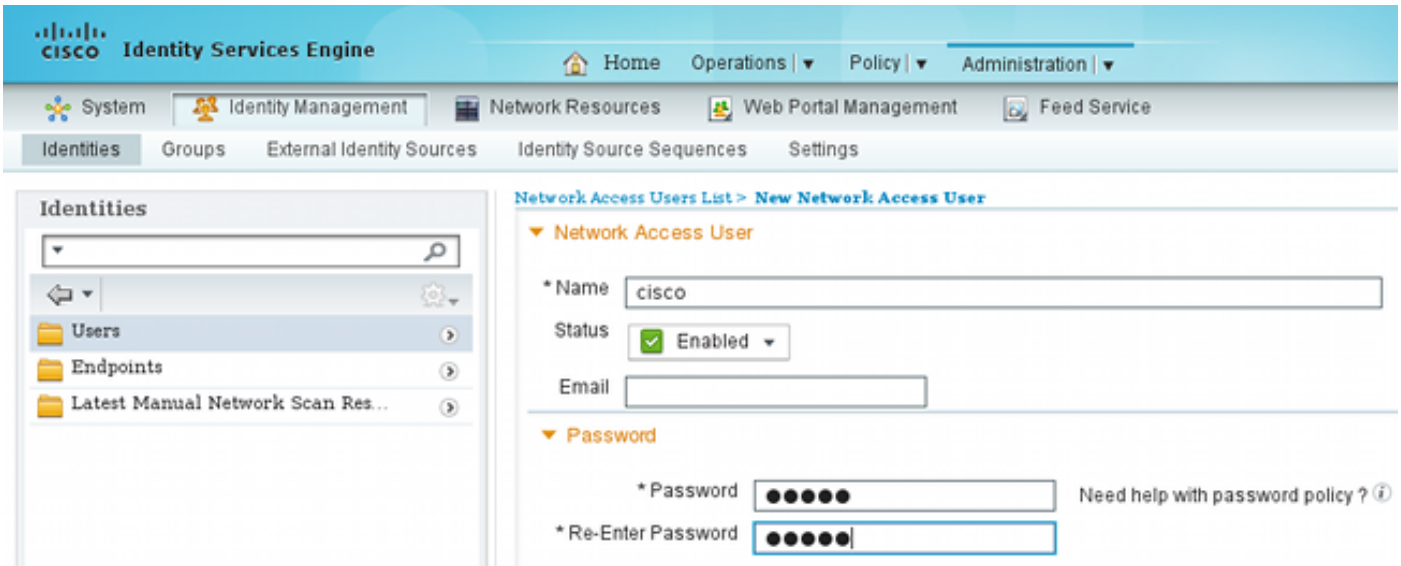
Die ISE-Konfiguration umfasst ein typisches 802.1x-Szenario mit Ausnahme des Authorization Profile, das möglicherweise Verschlüsselungsrichtlinien enthält.

Wählen Sie **Administration > Network Resources > Network Devices**, um den Switch als Netzwerkgerät hinzuzufügen. Geben Sie einen vorinstallierten RADIUS-Schlüssel (Shared Secret) ein.

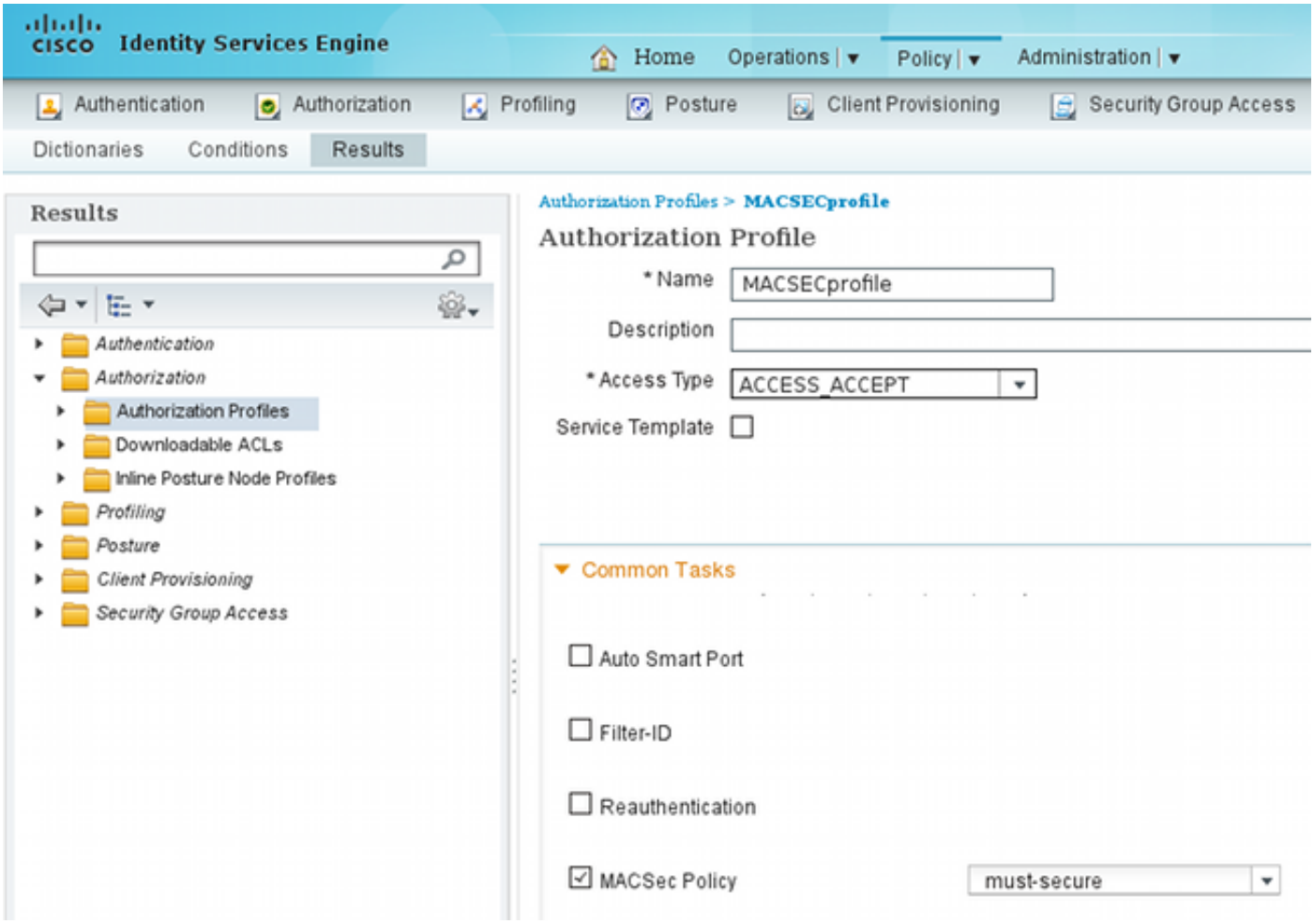


Die Standardauthentifizierungsregel kann verwendet werden (für Benutzer, die lokal auf der ISE definiert sind).

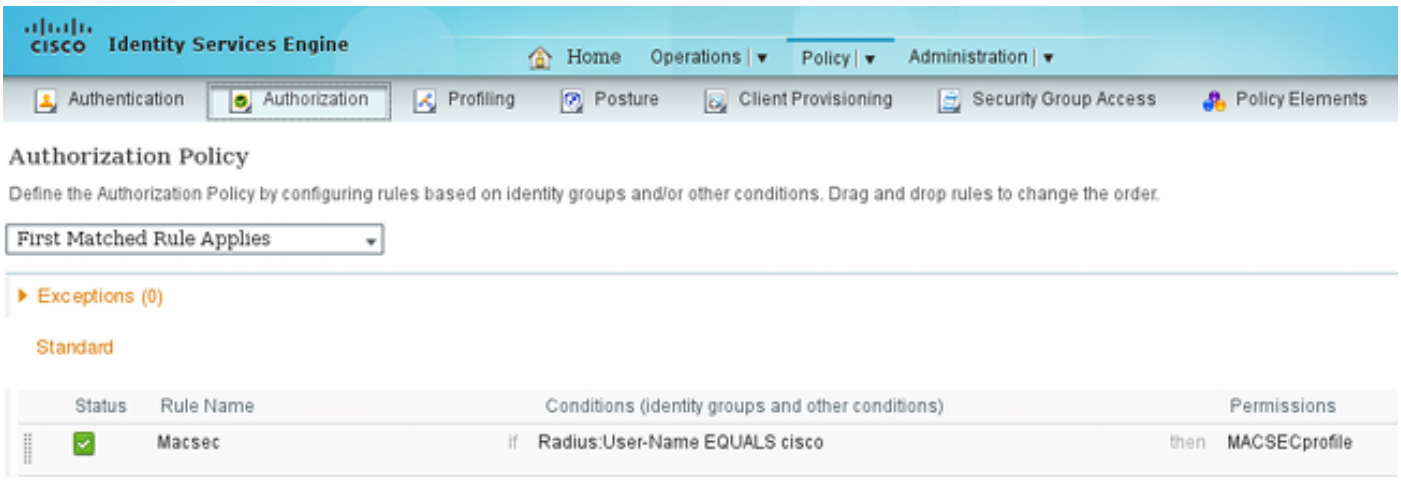
Wählen Sie **Administration > Identity Management > Users aus**, um den Benutzer "cisco" lokal zu definieren.



Das Authorization-Profil kann Verschlüsselungsrichtlinien enthalten. Wählen Sie, wie in diesem Beispiel gezeigt, **Policy > Results > Authorization Profiles (Richtlinien > Ergebnisse > Autorisierungsprofile**, um die Informationen anzuzeigen, die ISE an den Switch zurückgibt, wenn die Link-Verschlüsselung obligatorisch ist. Außerdem wurde die VLAN-Nummer (10) konfiguriert.



Wählen Sie **Policy > Authorization (Richtlinie > Autorisierung)**, um das Autorisierungsprofil in der Autorisierungsregel zu verwenden. In diesem Beispiel wird das konfigurierte Profil für den Benutzer "cisco" zurückgegeben. Wenn 802.1x erfolgreich ist, gibt die ISE RADIUS-Accept für den Switch mit Cisco AVPair linksec-policy=must-secure zurück. Dieses Attribut zwingt den Switch, eine MKA-Sitzung zu starten. Wenn diese Sitzung fehlschlägt, schlägt auch die 802.1x-Autorisierung auf dem Switch fehl.



Switch

Typische 802.1x-Porteinstellungen sind (oben abgebildet):

```
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
```

Die lokale MKA-Richtlinie wird erstellt und auf die Schnittstelle angewendet. Außerdem ist MACsec auf der Schnittstelle aktiviert.

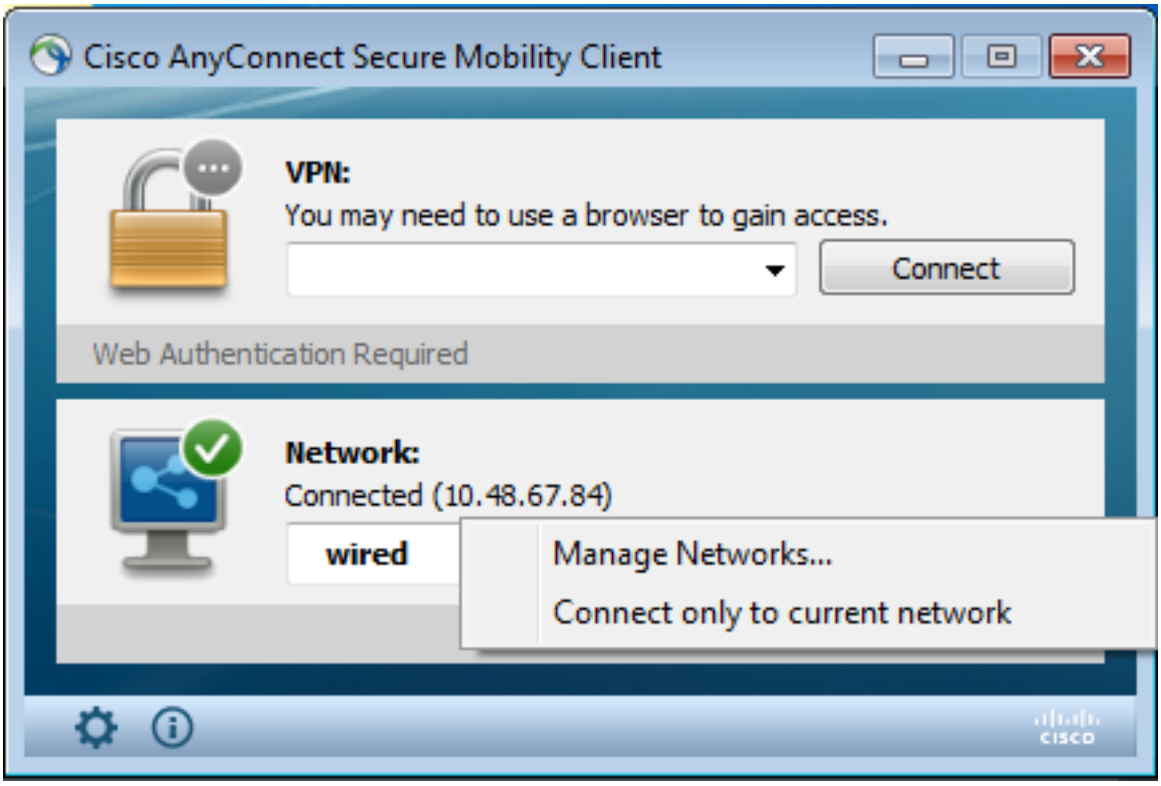
```
mka policy mka-policy
 replay-protection window-size 5000

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

Mit der lokalen MKA-Richtlinie können Sie detaillierte Einstellungen konfigurieren, die nicht von der ISE übertragen werden können. Die lokale MKA-Richtlinie ist optional.

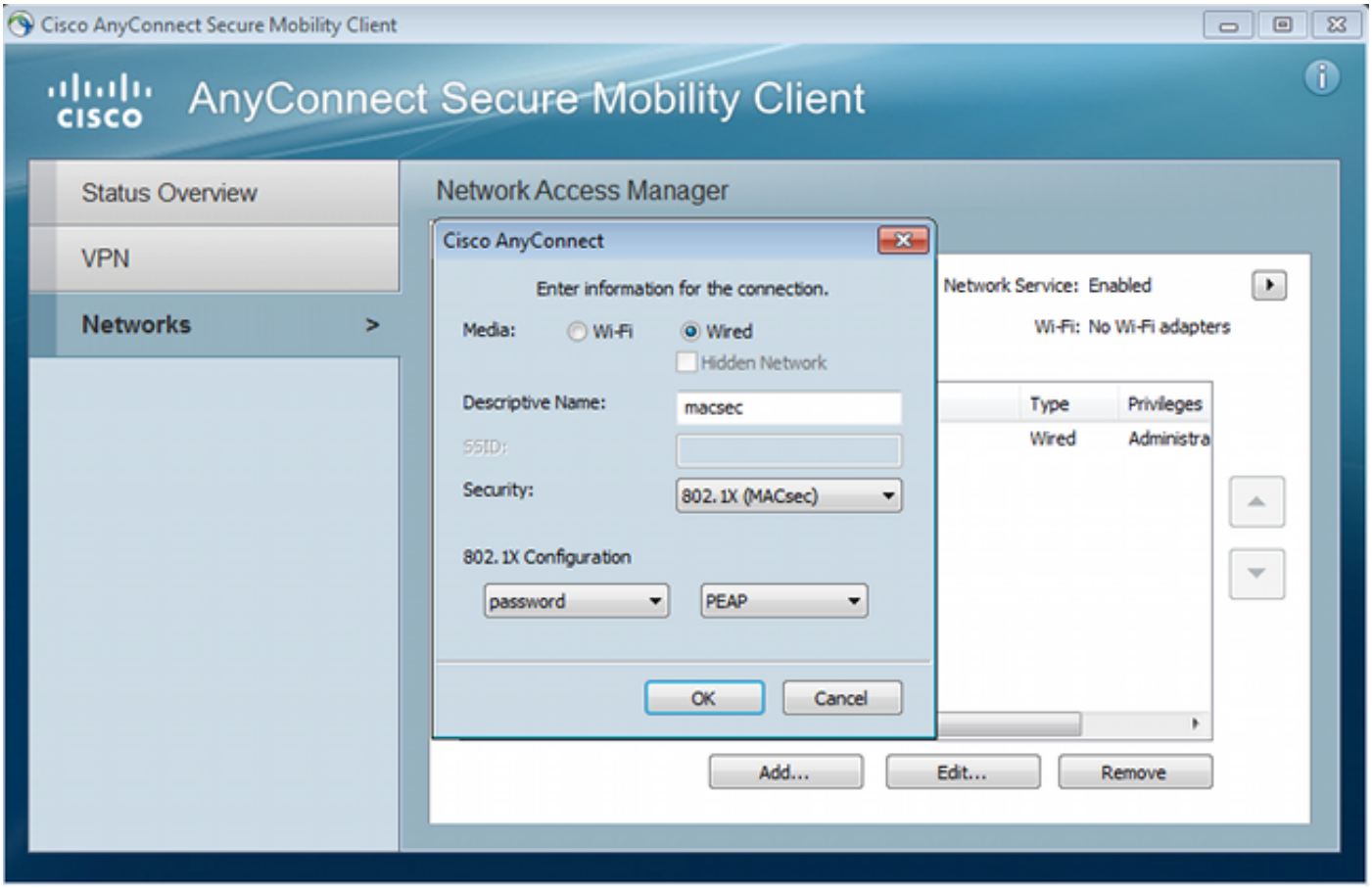
AnyConnect NAM

Das Profil für die 802.1x-Komponente kann manuell konfiguriert oder über die Cisco ASA weitergeleitet werden. Die nächsten Schritte stellen eine manuelle Konfiguration dar.

So verwalten Sie NAM-Profile:



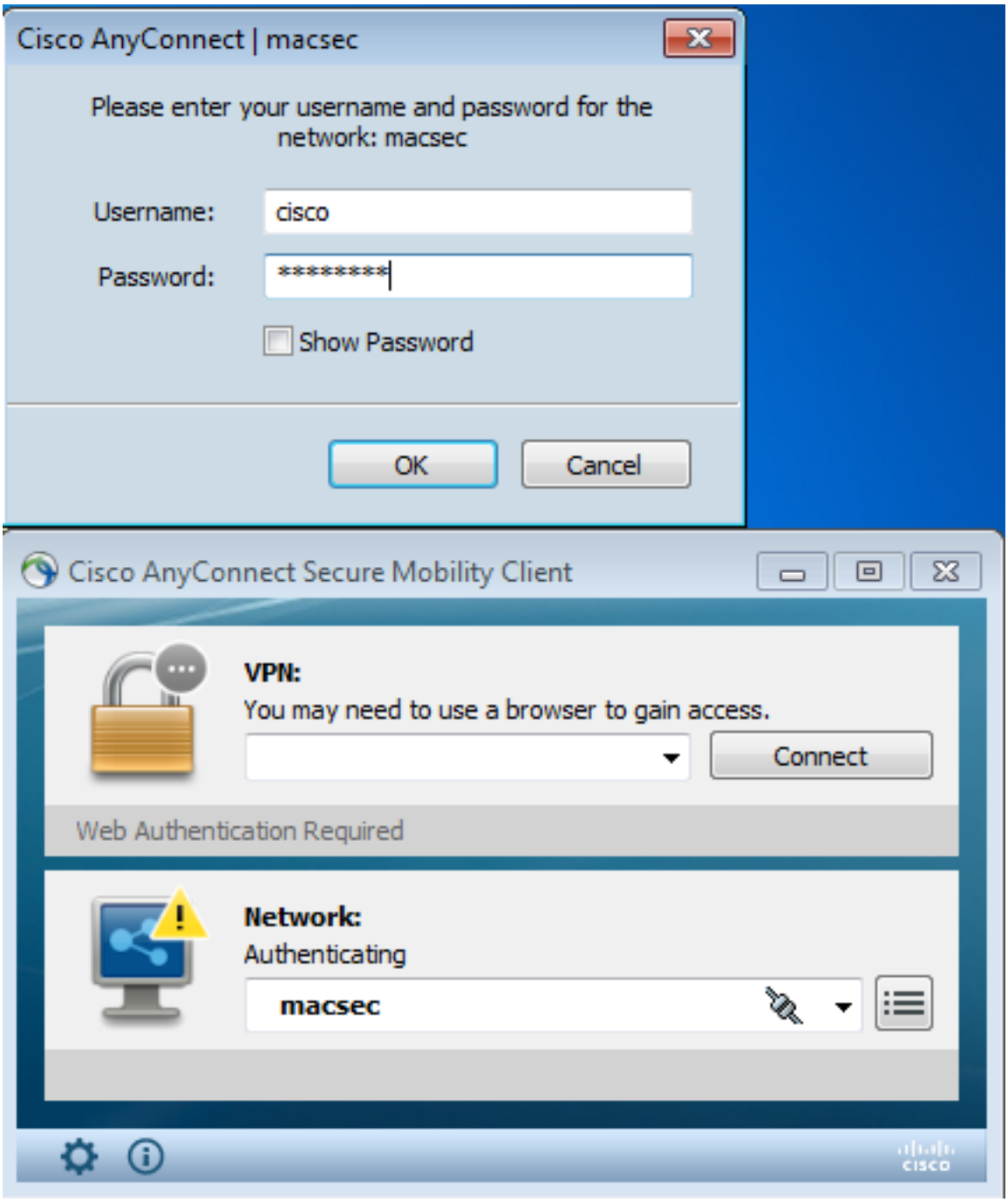
Fügen Sie ein neues 802.1x-Profil mit MACsec hinzu. Für 802.1x wird Protected Extensible Authentication Protocol (PEAP) verwendet (konfigurierter Benutzer "cisco" auf ISE):



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das für EAP-PEAP konfigurierte AnyConnect NAM erfordert korrekte Anmeldeinformationen.



Die Sitzung am Switch muss authentifiziert und autorisiert werden. Der Sicherheitsstatus sollte "Gesichert" lauten:

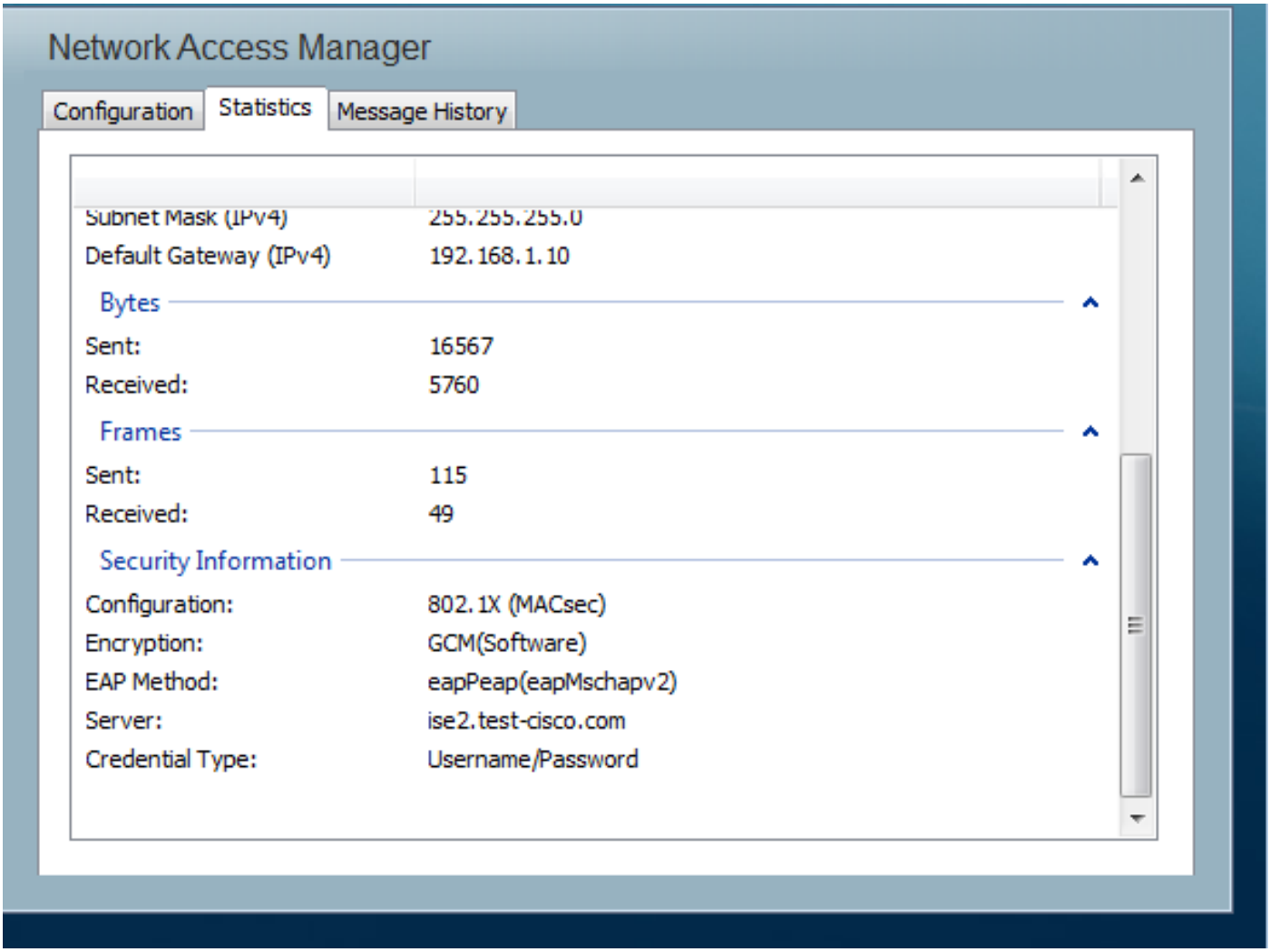
```
bsns-3750-5#show authentication sessions interface g1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5699.36ce
           IP Address:  192.168.1.201
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy: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

Die MACsec-Statistiken auf dem Switch liefern Details zu lokalen Richtlinieneinstellungen, SCIs (Secure Channel Identifiers) für empfangenen/gesendeten Datenverkehr sowie Portstatistiken und -fehlern.

```
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
```

Die Statistiken für AnyConnect geben die Verschlüsselungsnutzung und Paketstatistiken an.



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Debugger für ein Arbeitsszenario

Aktivieren Sie Debug auf dem Switch (einige Ausgaben wurden aus Gründen der Klarheit weggelassen).

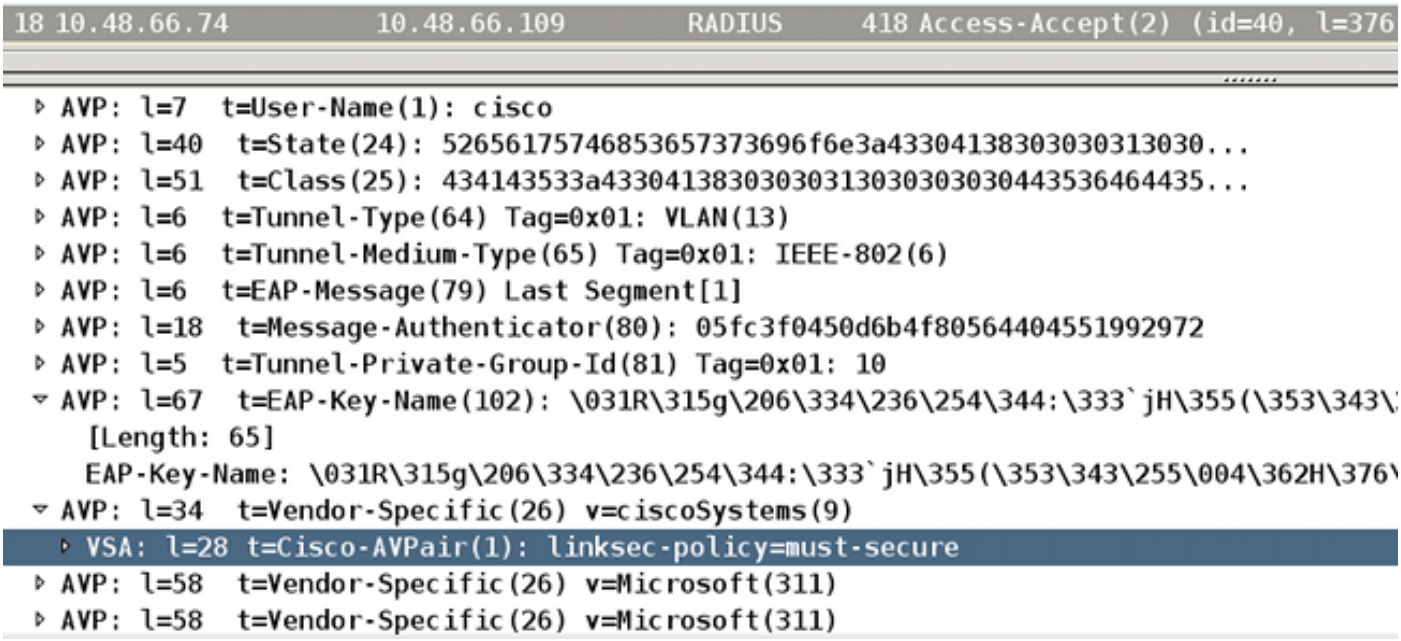
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

Nach Einrichtung einer 802.1x-Sitzung werden mehrere EAP-Pakete über EAPOL ausgetauscht. Die letzte erfolgreiche Antwort der ISE (EAP Success), die innerhalb von Radius-Acccept durchgeführt wurde, umfasst auch mehrere Radius-Attribute.

```
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 wird für die MKA-Sitzung verwendet. Die linksec-Policy zwingt den Switch zur Verwendung von MACsec (die Autorisierung schlägt fehl, wenn dies nicht abgeschlossen ist). Diese Attribute können auch in der Paketerfassung überprüft werden.



Die Authentifizierung ist erfolgreich.

```
%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
```

Der Switch wendet die Attribute an (dazu gehört auch eine optionale VLAN-Nummer, die ebenfalls gesendet wurde).

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

Der Switch startet dann die MKA-Sitzung, wenn er EAPOL-Pakete sendet und empfängt.

```
%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
```

Nach dem Austausch von vier Paketen werden sichere IDs zusammen mit der Receive (RX)-Sicherheitszuordnung erstellt.

```
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
```

Die Sitzung ist beendet, und die Transmit (TX)-Sicherheitszuordnung wird hinzugefügt.

```
%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/
```

Die Richtlinie "must-secure" ist zugeordnet, und die Autorisierung ist erfolgreich.

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

Alle 2 Sekunden werden MKA Hello-Pakete ausgetauscht, um sicherzustellen, dass alle Teilnehmer am Leben sind.

```
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
```

Debugger für ein Fehlerszenario

Wenn die Komponente nicht für MKA konfiguriert ist und die ISE nach erfolgreicher 802.1x-Authentifizierung eine Verschlüsselung anfordert:

```
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
```

Der Switch versucht, eine MKA-Sitzung zu starten, wenn er 5 EAPOL-Pakete sendet.

```
%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
```

Und schließlich wird die Autorisierung abgebrochen und versagt.

```
 %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
```

Die 802.1x-Sitzung meldet eine erfolgreiche Authentifizierung, aber eine fehlgeschlagene

Autorisierung.

```
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
```

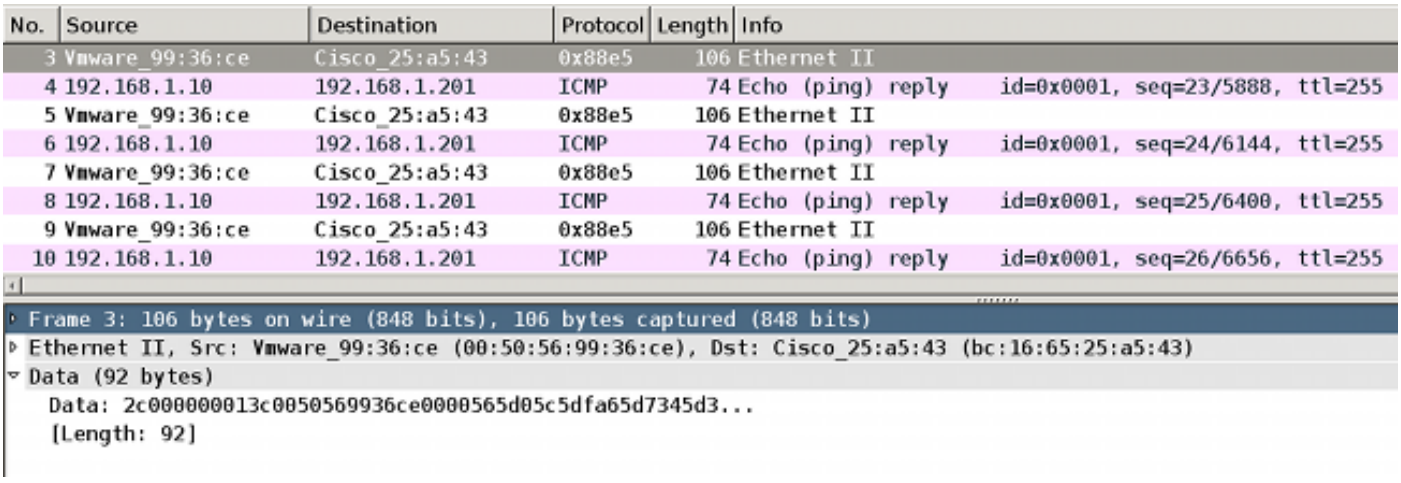
Datenverkehr wird blockiert.

Paketerfassung

Wenn Datenverkehr auf dem Supplicant Site 4 Internet Control Message Protocol (ICMP)-Echoanfragen/-antworten erfasst wird, werden folgende Meldungen gesendet und empfangen:

- 4 verschlüsselte ICMP-Echoanfragen, die an den Switch gesendet werden (88e5 ist für 802.1AE reserviert)
- 4 entschlüsselte ICMP-Echo-Antworten erhalten

Dies liegt daran, wie AnyConnect über die Windows-API (vor libpcap beim Senden von Paketen und vor libpcap beim Empfang von Paketen) angeheftet wird:



Hinweis: Die Möglichkeit, MKA- oder 802.1AE-Datenverkehr auf dem Switch mit Funktionen wie Switched Port Analyzer (SPAN) oder Embedded Packet Capture (EPC) zu schnappen, wird nicht unterstützt.

MACsec- und 802.1x-Modi

Nicht alle 802.1x-Modi werden für MACsec unterstützt.

Anleitung *zu Cisco TrustSec 3.0: In der Einführung in MACsec und NDAC* heißt es:

- **Single-Host-Modus**: **MACsec wird** im Single-Host-Modus **vollständig unterstützt**. In diesem Modus kann nur eine einzige MAC- oder IP-Adresse mit MACsec authentifiziert und gesichert werden. Wenn eine andere MAC-Adresse auf dem Port erkannt wird, nachdem ein Endpunkt authentifiziert wurde, wird eine Sicherheitsverletzung auf dem Port ausgelöst.
- **MDA-Modus (Multi-Domain Authentication)**: In diesem Modus kann sich ein Endpunkt in der Datendomäne und ein anderer Endpunkt in der Sprachdomäne befinden. **MACsec wird im MDA-Modus vollständig unterstützt**. Wenn beide Endpunkte MACsec-fähig sind, wird jeder Endpunkt durch eine eigene unabhängige MACsec-Sitzung gesichert. Wenn nur ein Endpunkt MACsec-fähig ist, kann dieser Endpunkt gesichert werden, während der andere Endpunkt Datenverkehr in Clear sendet.
- **Multi-Authentication-Modus**: In diesem Modus kann eine praktisch unbegrenzte Anzahl von Endpunkten an einem einzelnen Switch-Port authentifiziert werden. **MACsec wird in diesem Modus nicht unterstützt.**
- **Multi-Host-Modus**: Während eine MACsec-Nutzung in diesem Modus technisch möglich ist, **wird sie nicht empfohlen**. Im Multi-Host-Modus authentifiziert sich der erste Endpunkt am Port, und weitere Endpunkte werden über die erste Autorisierung in das Netzwerk aufgenommen. MACsec würde mit dem ersten angeschlossenen Host funktionieren, aber kein Datenverkehr eines anderen Endpunkts würde tatsächlich weitergeleitet, da es sich nicht um verschlüsselten Datenverkehr handelt.

Zugehörige Informationen

- Cisco TrustSec-Konfigurationsleitfaden für 3750
- Cisco TrustSec-Konfigurationsleitfaden für ASA 9.1
- Identitätsbasierte Netzwerkservices: MAC-Sicherheit
- TrustSec Cloud mit 802.1x MACsec auf Catalyst Switches der Serie 3750X - Konfigurationsbeispiel
- ASA und Catalyst Switch der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung
- Cisco TrustSec-Bereitstellung und Roadmap
- Technischer Support und Dokumentation - Cisco Systems