Esempio di crittografia host dello switch MACsec con Cisco AnyConnect e configurazione ISE

Sommario

Introduzione

In questo documento viene fornito un esempio di configurazione della crittografia MACsec (Media Access Control Security) tra un supplicant 802.1x (Cisco AnyConnect Mobile Security) e un autenticatore (switch). Cisco Identity Services Engine (ISE) viene utilizzato come server per l'autenticazione e le policy.

MACsec è standardizzato in 802.1AE e supportato sugli switch Cisco 3750X, 3560X e 4500 SUP7E. 802.1AE definisce la crittografia dei collegamenti su reti cablate che utilizzano chiavi fuori banda. Tali chiavi di crittografia vengono negoziate con il protocollo MACsec Key Agreement (MKA), utilizzato dopo la riuscita dell'autenticazione 802.1x. MKA è standardizzato in IEEE 802.1X-2010.

Un pacchetto viene crittografato solo sul collegamento tra il PC e lo switch (crittografia point-to-point). Il pacchetto ricevuto dallo switch viene decrittografato e inviato tramite uplink non crittografati. Per crittografare la trasmissione tra gli switch, è consigliata la crittografia dello switch. Per tale crittografia viene utilizzato il protocollo SAP (Security Association Protocol) per negoziare e rigenerare le chiavi. SAP è un protocollo standard sviluppato da Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione 802.1x
- Conoscenze base della configurazione CLI degli switch Catalyst
- Esperienza nella configurazione ISE

Componenti usati

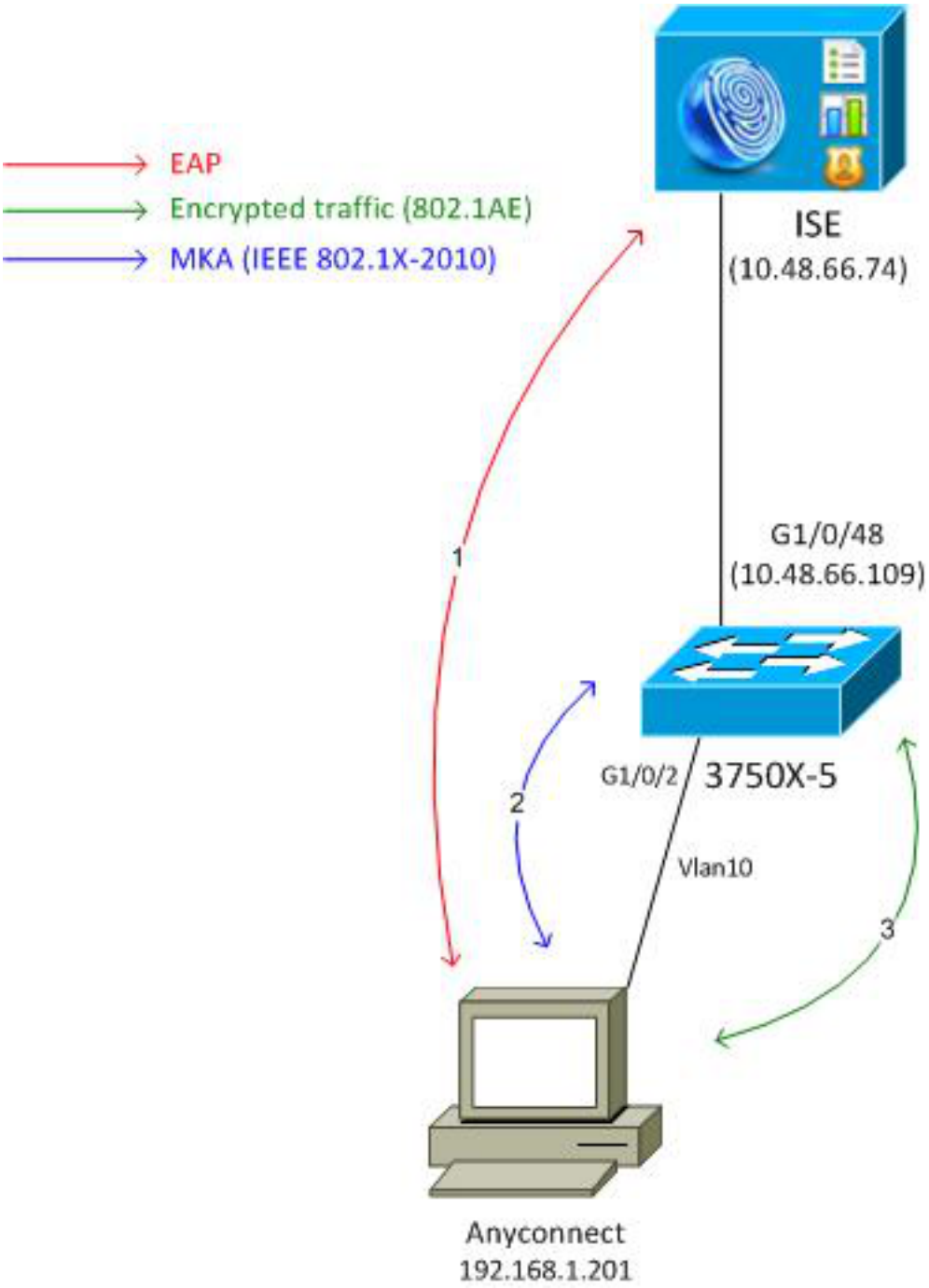
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Sistemi operativi Microsoft Windows 7 e Microsoft Windows XP
- Software Cisco 3750X versione 15.0 e successive
- Software Cisco ISE, versione 1.1.4 e successive
- Cisco AnyConnect Mobile Security con Network Access Manager (NAM), versione 3.1 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete e flusso del traffico



Passaggio 1. Il richiedente (AnyConnect NAM) avvia la sessione 802.1x. Lo switch è l'autenticatore e l'ISE è il server di autenticazione. Il protocollo EAPOL (Extensible Authentication Protocol over LAN) viene utilizzato come trasporto per EAP tra il richiedente e lo switch. RADIUS è utilizzato come protocollo di trasporto per EAP tra lo switch e l'ISE. Non è possibile usare MAB (MAC Authentication Bypass) perché le chiavi EAPOL devono essere restituite da ISE e usate per la sessione MKA (MACsec Key Agreement).

Passaggio 2. Al termine della sessione 802.1x, lo switch avvia una sessione MKA con EAPOL come protocollo di trasporto. Se il supplicant è configurato correttamente, le chiavi per la crittografia AES-GCM (modalità Galois/Contatore) simmetrica a 128 bit corrispondono.

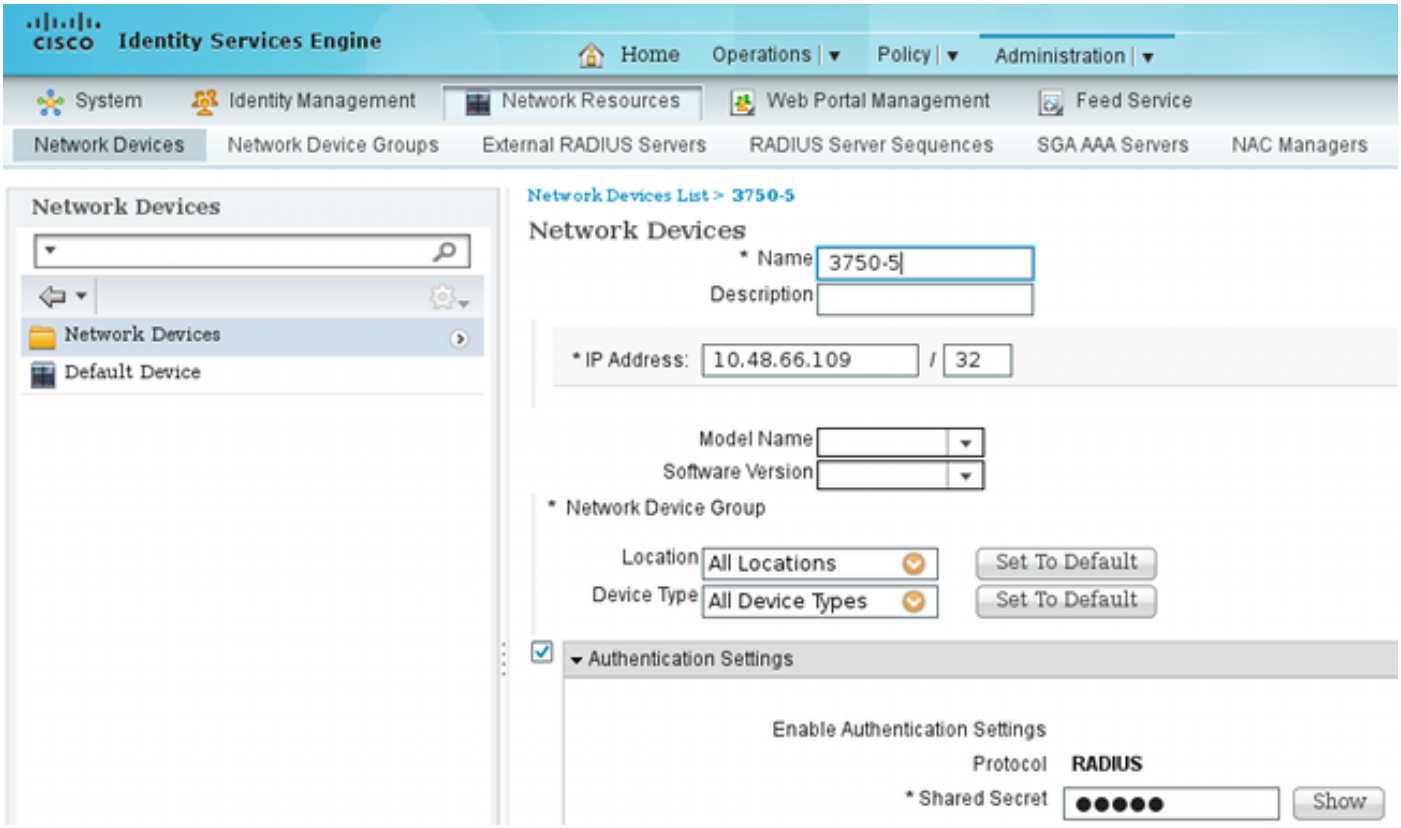
Passaggio 3. Tutti i pacchetti successivi tra il richiedente e lo switch sono crittografati (incapsulamento 802.1AE).

Configurazioni

ISE

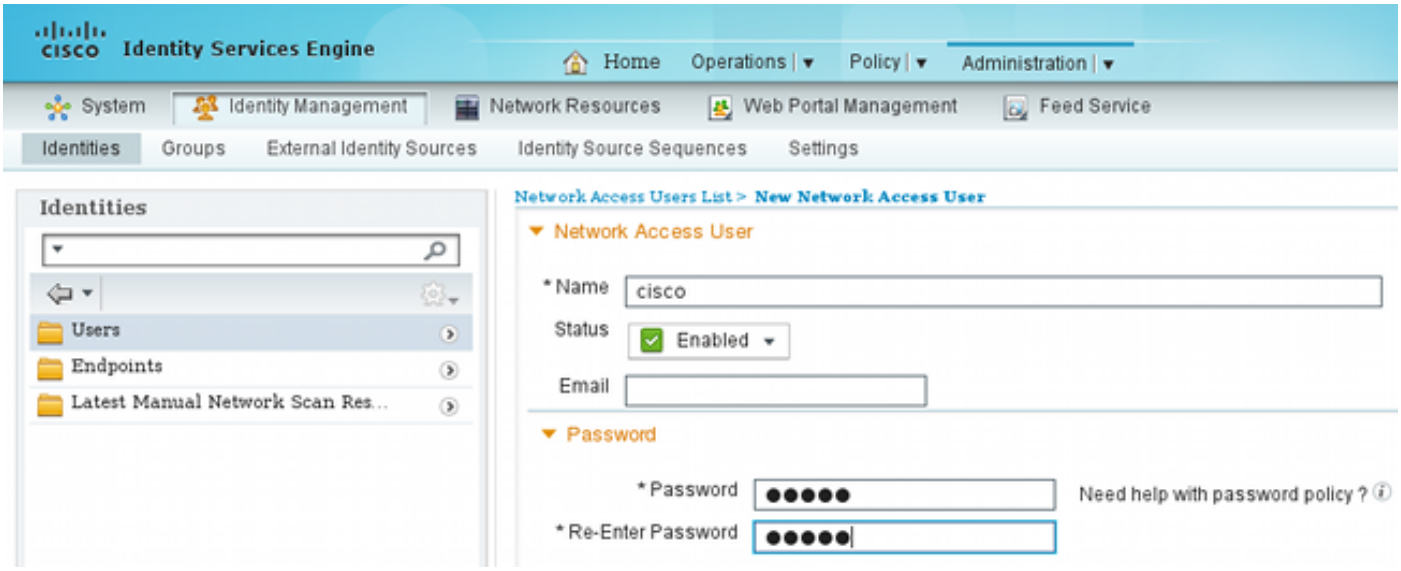
La configurazione ISE prevede uno scenario 802.1x tipico con un'eccezione al profilo di autorizzazione che potrebbe includere criteri di crittografia.

Per aggiungere lo switch come dispositivo di rete, scegliere **Amministrazione > Risorse di rete > Dispositivi di rete**. Immettere una chiave già condivisa RADIUS (segreto condiviso).



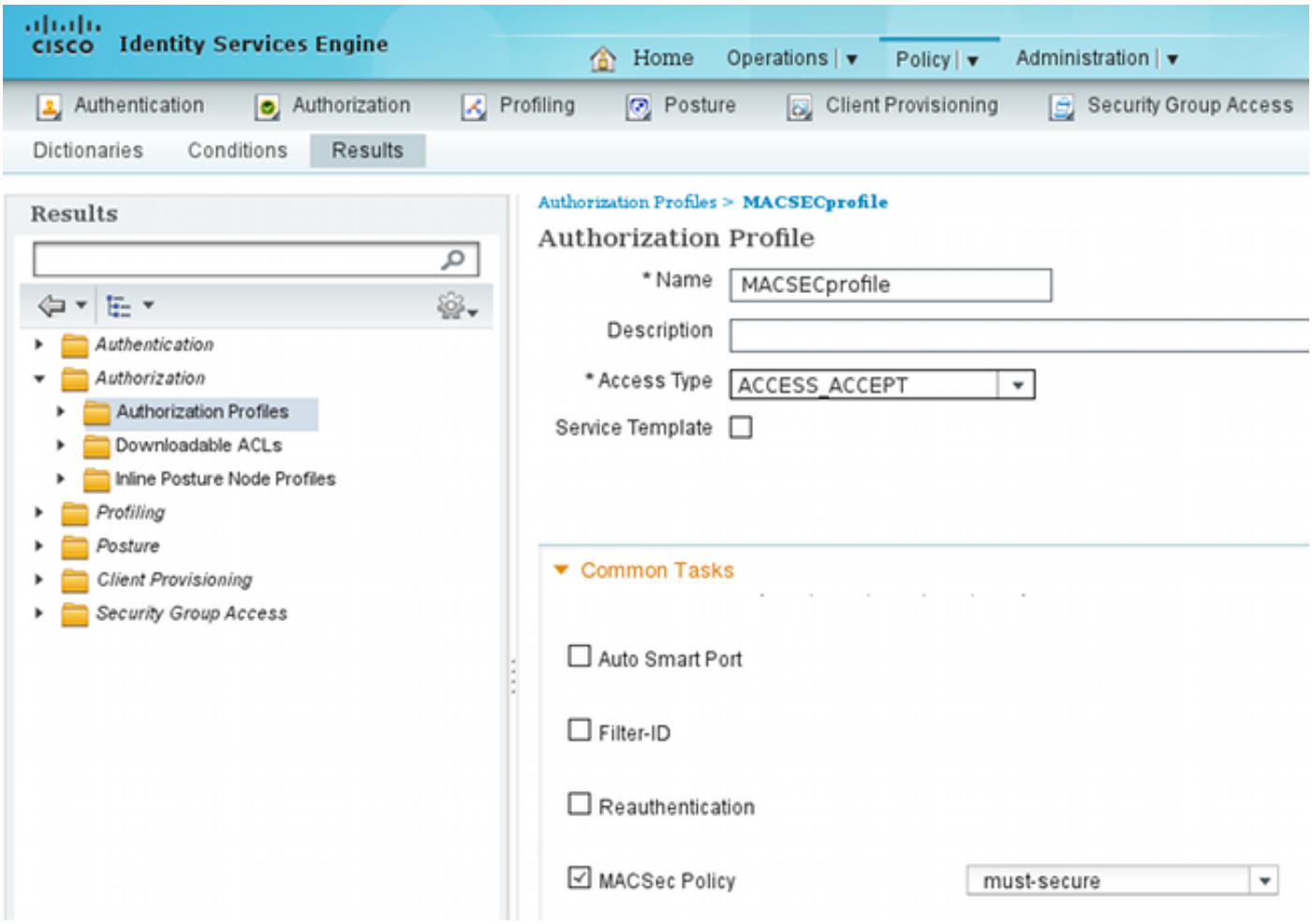
Si può usare la regola di autenticazione predefinita (per gli utenti definiti localmente su ISE).

Per definire l'utente "cisco" localmente, scegliere **Amministrazione > Gestione delle identità > Utenti**.

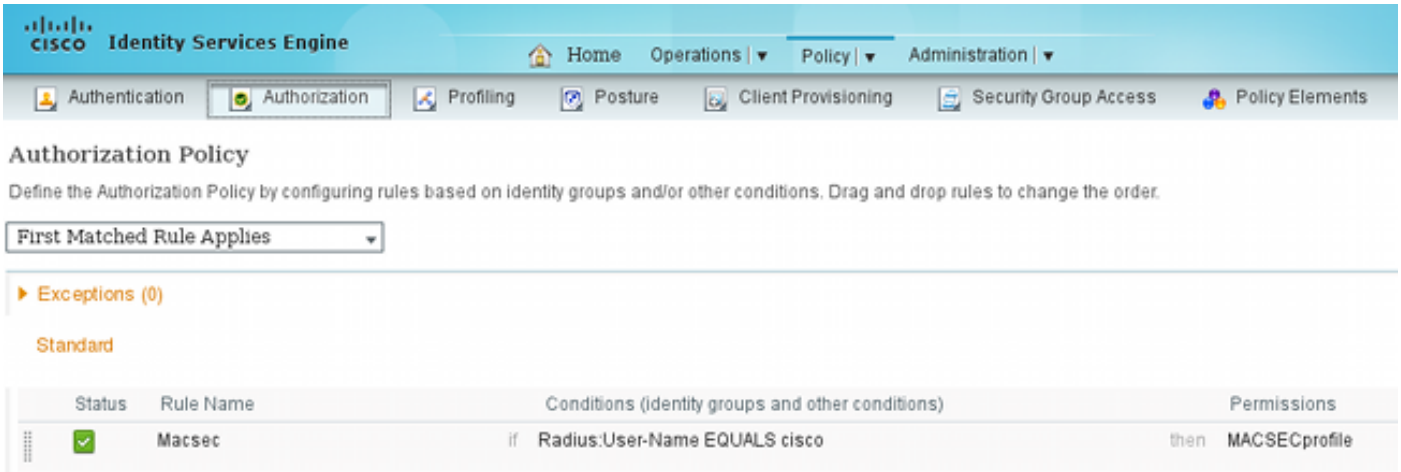


Il profilo di autorizzazione può includere criteri di crittografia. Come mostrato nell'esempio, selezionare **Policy > Results > Authorization Profiles** (Policy > Risultati > Profili di autorizzazione)

per visualizzare le informazioni restituite da ISE allo switch in cui la crittografia del collegamento è obbligatoria. Inoltre, è stato configurato il numero VLAN (10).



Per utilizzare il profilo di autorizzazione nella regola di autorizzazione, scegliere **Criterio > Autorizzazione**. In questo esempio viene restituito il profilo configurato per l'utente "cisco". Se 802.1x ha esito positivo, ISE restituisce Radius-Accept allo switch con Cisco AVPair link-policy=must-secure. Questo attributo forza lo switch ad avviare una sessione MKA. Se la sessione ha esito negativo, anche l'autorizzazione 802.1x sullo switch ha esito negativo.



Switch

Le impostazioni tipiche della porta 802.1x includono (parte superiore mostrata):

```
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
```

Il criterio MKA locale viene creato e applicato all'interfaccia. Inoltre, MACsec è abilitato sull'interfaccia.

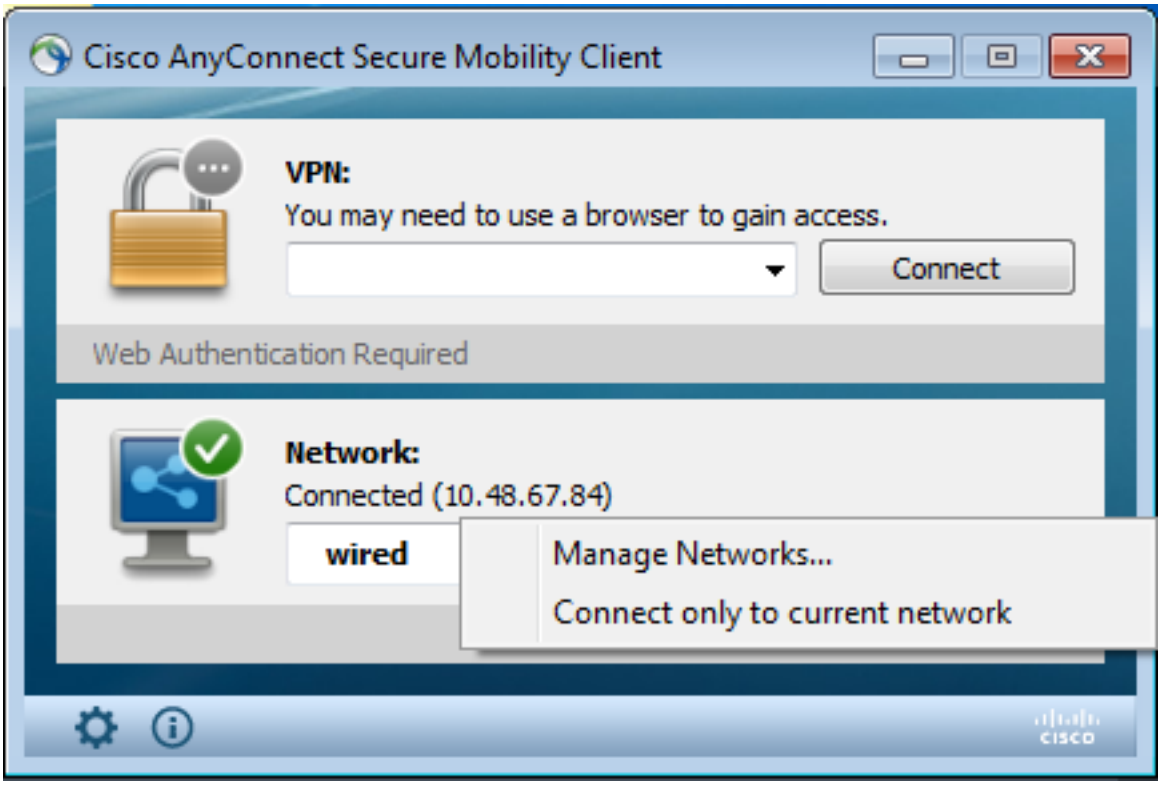
```
mka policy mka-policy
 replay-protection window-size 5000

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

Il criterio MKA locale consente di configurare impostazioni dettagliate che non possono essere estratte dall'ISE. Il criterio MKA locale è facoltativo.

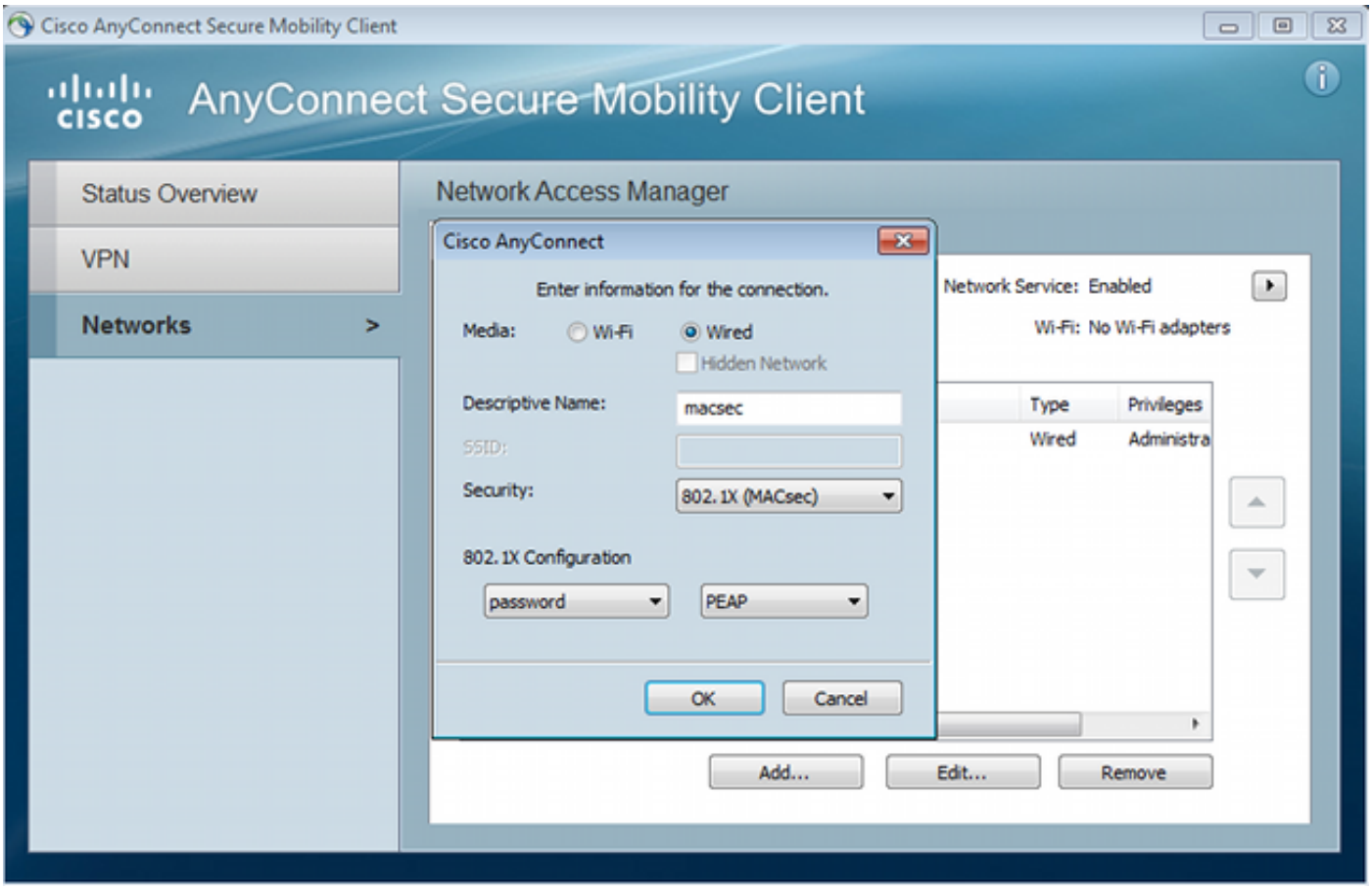
AnyConnect NAM

Il profilo del supplicant 802.1x può essere configurato manualmente o push tramite Cisco ASA. Nei passaggi successivi viene illustrata una configurazione manuale.

Per gestire i profili NAM:



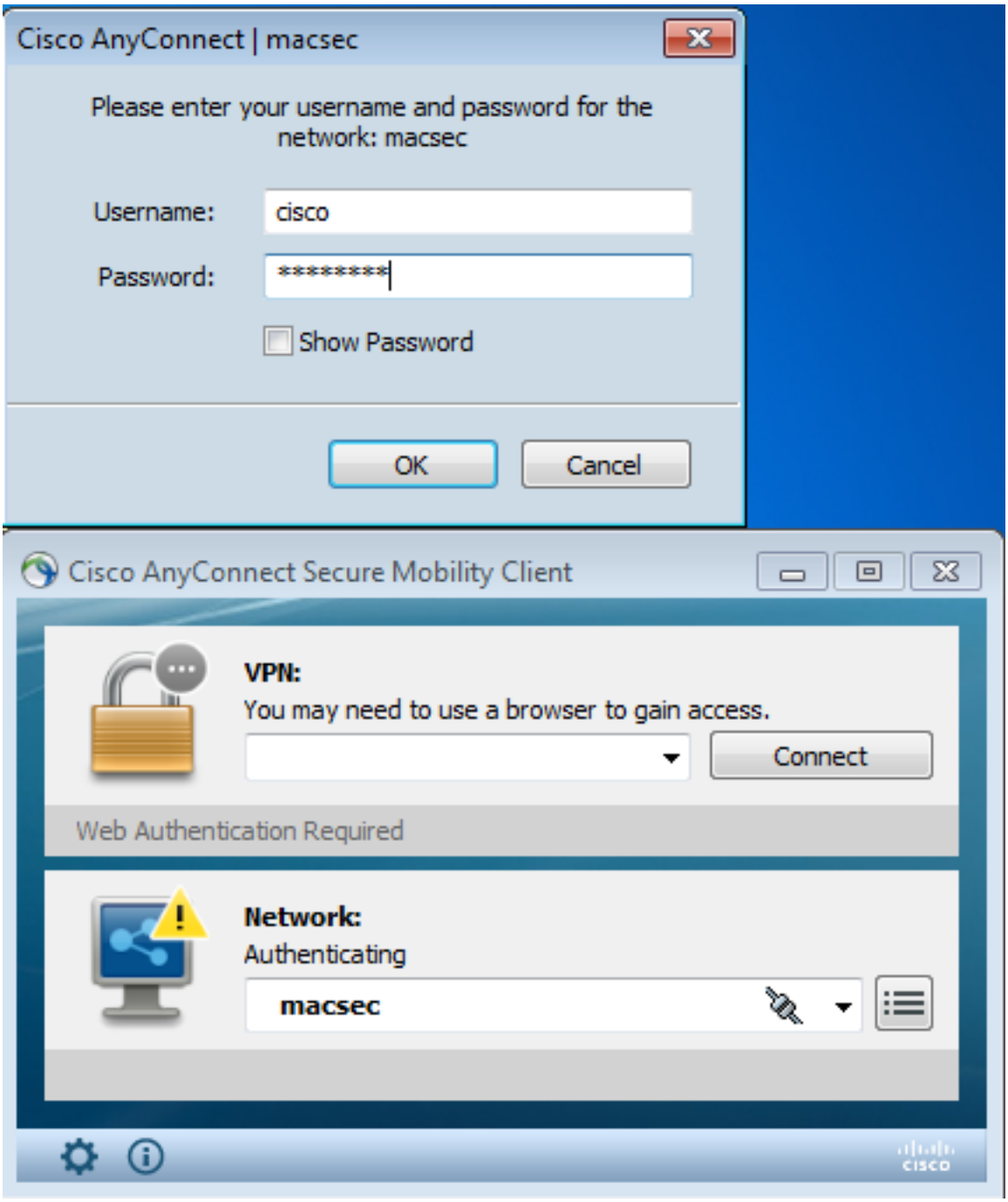
Aggiungere un nuovo profilo 802.1x con MACsec. Per lo standard 802.1x, viene utilizzato il protocollo PEAP (Protected Extensible Authentication Protocol) (configurato dall'utente "cisco" su ISE):



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

AnyConnect NAM configurato per EAP-PEAP richiede le credenziali corrette.



La sessione sullo switch deve essere autenticata e autorizzata. Lo stato di protezione deve essere "Protetto":

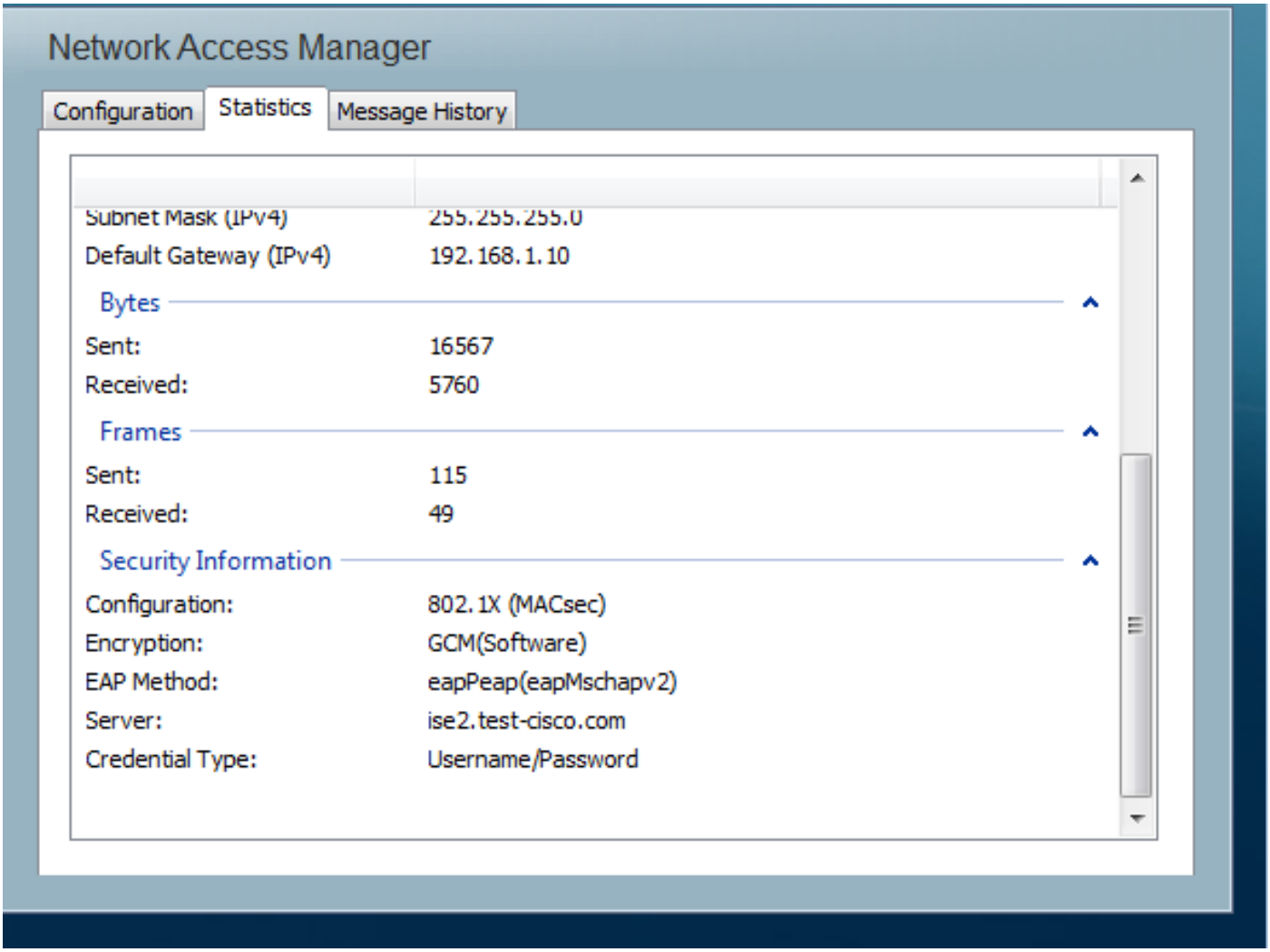
```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must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

Le statistiche MACsec sullo switch forniscono i dettagli relativi all'impostazione della policy locale, gli identificatori di canale sicuri (SCI) per il traffico ricevuto/inviato, nonché le statistiche delle porte e gli errori.

```
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
```

Su AnyConnect, le statistiche indicano l'utilizzo della crittografia e le statistiche dei pacchetti.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

debug per uno scenario di lavoro

Abilitare i debug sullo switch (alcuni output sono stati omessi per chiarezza).

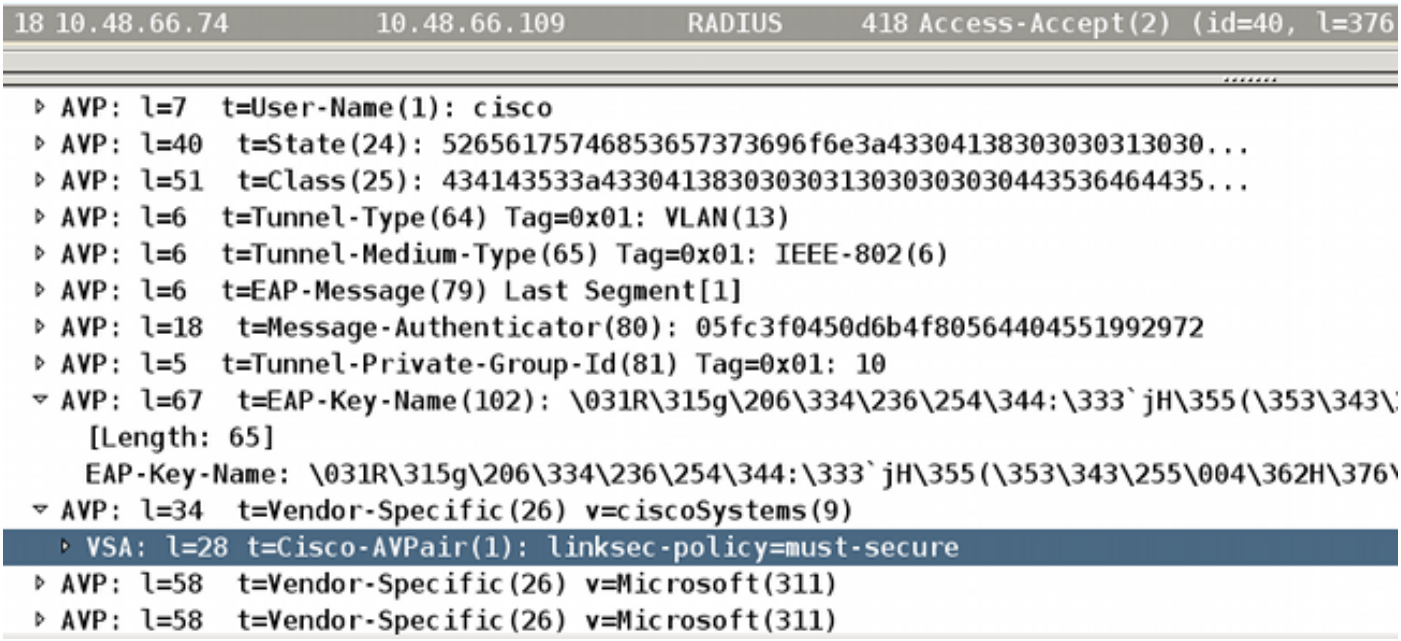
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

Una volta stabilita una sessione 802.1x, vengono scambiati più pacchetti EAP tramite EAPOL. L'ultima risposta di successo da ISE (EAP success) trasmessa all'interno di Radius-Accept include anche diversi attributi 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 viene utilizzato per la sessione MKA. Il criterio di sec di collegamento impone allo switch di utilizzare MACsec. Se l'autorizzazione non è completa, non verrà eseguita. Questi attributi possono essere verificati anche nelle acquisizioni dei pacchetti.



Autenticazione completata.

```
%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
```

Lo switch applica gli attributi (inclusi un numero VLAN opzionale che è stato anch'esso inviato).

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

Lo switch avvia quindi la sessione MKA quando invia e riceve pacchetti 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
```

Dopo la creazione di 4 identificatori di protezione per lo scambio di pacchetti insieme all'associazione di protezione di ricezione (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
```

La sessione è terminata e viene aggiunta l'associazione di protezione Trasmissione (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/
```

Il criterio "must-secure" corrisponde e l'autorizzazione ha esito positivo.

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

Ogni 2 secondi i pacchetti MKA Hello vengono scambiati per garantire che tutti i partecipanti siano vivi.

```
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
```

Debug di uno scenario con esito negativo

Quando il richiedente non è configurato per MKA e ISE richiede la crittografia dopo un'autenticazione 802.1x riuscita:

```
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
```

Lo switch cerca di avviare una sessione MKA quando invia 5 pacchetti 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 alla fine esce e manca l'autorizzazione.

```
 %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 sessione 802.1x riporta l'autenticazione riuscita, ma l'autorizzazione non è riuscita.

```
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
```

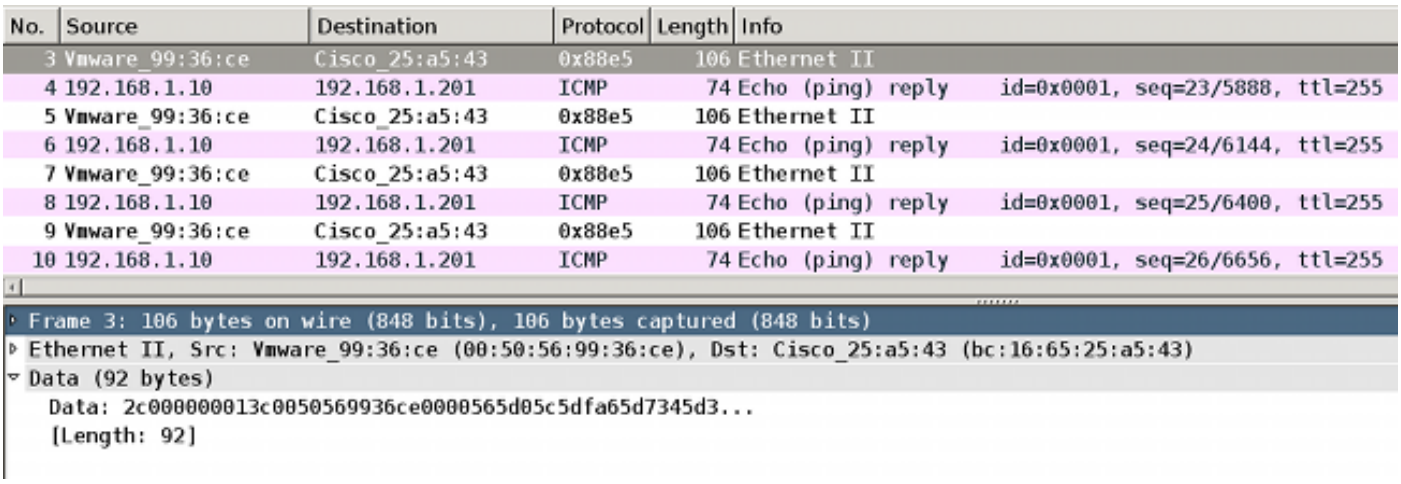
Il traffico di dati verrà bloccato.

Acquisizioni pacchetti

Quando il traffico viene acquisito sul sito supplicant 4, vengono inviate e ricevute richieste/risposte echo Internet Control Message Protocol (ICMP), si verificherà quanto segue:

- 4 richieste echo ICMP crittografate inviate allo switch (88e5 è riservato per 802.1AE)
- 4 risposte echo ICMP decrittografate ricevute

Ciò è dovuto al modo in cui AnyConnect si collega all'API Windows (prima di libpcap quando i pacchetti vengono inviati e prima di libpcap quando i pacchetti vengono ricevuti):



> **Nota:** non è supportata la possibilità di verificare il traffico MKA o 802.1AE sullo switch con funzionalità quali SPAN (Switched Port Analyzer) o EPC (Embedded Packet Capture).

Modalità MACsec e 802.1x

Non tutte le modalità 802.1x sono supportate per MACsec.

La *Guida alle procedure di Cisco TrustSec 3.0: Introduzione agli* stati *MACsec e NDAC* che:

- **Modalità host singolo**: **MACsec è supportato** in modalità host singolo. In questa modalità, solo un indirizzo MAC o IP singolo può essere autenticato e protetto con MACsec. Se viene rilevato un indirizzo MAC diverso sulla porta dopo l'autenticazione di un endpoint, sulla porta verrà attivata una violazione della sicurezza.
- **Modalità Multi-Domain Authentication (MDA)**: In questa modalità, un endpoint può trovarsi nel dominio dati e un altro nel dominio voce. **MACsec è completamente supportato in modalità MDA**. Se entrambi gli endpoint sono compatibili con MACsec, ciascuno di essi verrà protetto tramite una sessione MACsec indipendente. Se solo un endpoint supporta MACsec, è possibile proteggere tale endpoint mentre l'altro invia il traffico in modalità non crittografata.
- **Modalità multi-autenticazione**: In questa modalità, è possibile autenticare un numero illimitato di endpoint su una singola porta dello switch. **MACsec non supportato in questa modalità.**
- **Modalità multi-host**: L'utilizzo di MACsec in questa modalità è tecnicamente possibile, **ma non è consigliato**. In modalità multi-host, il primo endpoint sulla porta viene autenticato e quindi tutti gli endpoint aggiuntivi verranno autorizzati all'accesso alla rete tramite la prima autorizzazione. MACsec funzionerebbe con il primo host connesso, ma in realtà non passerebbe alcun traffico di altri endpoint, in quanto non sarebbe traffico crittografato.

Informazioni correlate

- Guida alla configurazione di Cisco TrustSec per 3750
- Guida alla configurazione di Cisco TrustSec per ASA 9.1
- Servizi Identity-Based Networking: Sicurezza MAC
- Esempio di configurazione di TrustSec Cloud con 802.1x MACsec sugli switch Catalyst serie 3750X
- Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi
- Implementazione di Cisco TrustSec e roadmap
- Documentazione e supporto tecnico – Cisco Systems