

Configurazione dell'accesso remoto ASA IKEv2 con EAP-PEAP e client Windows nativo

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Considerazioni sul client AnyConnect Secure Mobility](#)

[Configurazione](#)

[Esempio di rete](#)

[Certificati](#)

[ISE](#)

[Passaggio 1. Aggiungere l'ASA ai dispositivi di rete sull'ISE.](#)

[Passaggio 2. Creare un nome utente nell'archivio locale.](#)

[ASA](#)

[Windows 7](#)

[Passaggio 1. Installare il certificato CA.](#)

[Passaggio 2. Configurare la connessione VPN.](#)

[Verifica](#)

[Client Windows](#)

[Log](#)

[Debug dell'appliance ASA](#)

[Livello pacchetto](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene illustrato un esempio di configurazione di Cisco Adaptive Security Appliance (ASA) versione 9.3.2 e successive che consente all'accesso VPN remoto di utilizzare il protocollo IKEv2 (Internet Key Exchange Protocol) con autenticazione EAP (Extensible Authentication Protocol) standard. Ciò consente a un client Microsoft Windows 7 nativo (e a qualsiasi altro client IKEv2 basato su standard) di connettersi all'appliance ASA con autenticazione IKEv2 e EAP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN e IKEv2
- Autenticazione di base, autorizzazione e accounting (AAA) e conoscenza RADIUS
- Esperienza nella configurazione di ASA VPN
- Esperienza nella configurazione di Identity Services Engine (ISE)

Componenti usati

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

- Microsoft Windows 7
- Software Cisco ASA, versione 9.3.2 e successive
- Cisco ISE versione 1.2 e successive

Premesse

Considerazioni sul client AnyConnect Secure Mobility

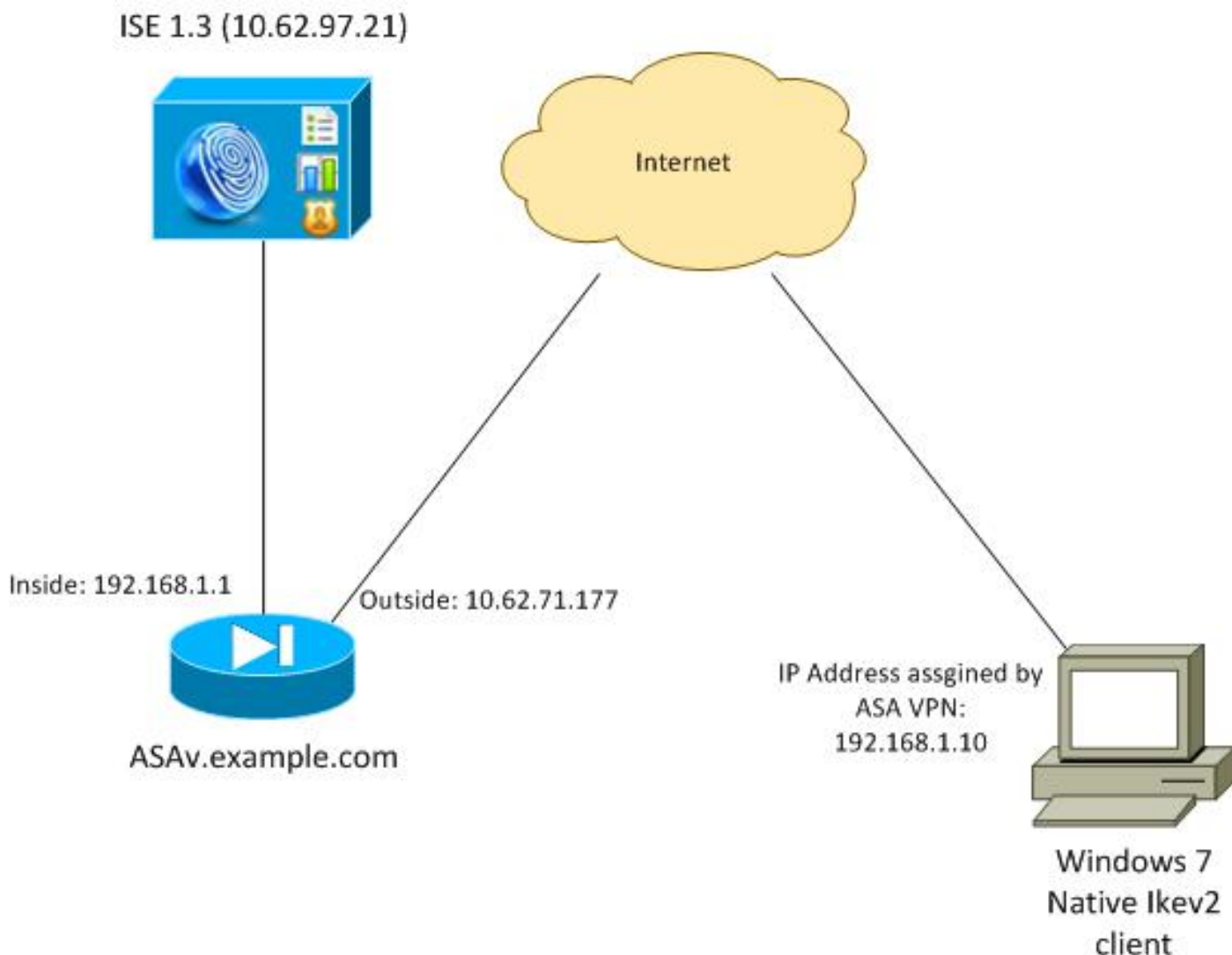
Il client Windows IKEv2 nativo non supporta lo split tunnel (non sono presenti attributi CONF REPLY che potrebbero essere accettati dal client Windows 7), quindi l'unico criterio possibile con il client Microsoft è quello di eseguire il tunnel di tutto il traffico (0/0 selettori traffico). Se è necessario specificare un criterio per il tunnel suddiviso, usare AnyConnect.

AnyConnect non supporta metodi EAP standardizzati che vengono terminati sul server AAA (PEAP, Transport Layer Security). Se è necessario terminare le sessioni EAP sul server AAA, è possibile utilizzare il client Microsoft.

Configurazione

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi \(solo utenti registrati\)](#).

Esempio di rete



L'appliance ASA è configurata per l'autenticazione con un certificato (il client deve considerare attendibile il certificato). Il client Windows 7 è configurato per l'autenticazione con EAP (EAP-PEAP).

L'ASA agisce come gateway VPN per terminare la sessione IKEv2 dal client. L'ISE agisce come server AAA terminando la sessione EAP dal client. I pacchetti EAP vengono incapsulati nei pacchetti IKE_AUTH per il traffico tra il client e l'ASA (IKEv2) e quindi nei pacchetti RADIUS per il traffico di autenticazione tra l'ASA e l'ISE.

Certificati

Per generare il certificato per l'appliance ASA, è stata usata l'autorità di certificazione (CA) Microsoft. I requisiti del certificato che devono essere accettati dal client nativo di Windows 7 sono:

- L'estensione per l'utilizzo chiavi esteso deve includere l'autenticazione del server (nell'esempio riportato è stato utilizzato il modello "server Web").
- Il nome soggetto deve includere il nome di dominio completo (FQDN) che verrà utilizzato dal client per la connessione (in questo esempio ASAv.example.com).

Per ulteriori informazioni sul client Microsoft, vedere [Risoluzione dei problemi di connessioni VPN IKEv2](#).

Nota: Android 4.x è più restrittivo e richiede il nome alternativo soggetto corretto come indicato nella RFC 6125. Per ulteriori informazioni su Android, vedere [IKEv2 da Android strongSwan a Cisco IOS con autenticazione EAP e RSA](#).

Per generare una richiesta di firma del certificato sull'appliance ASA, è stata utilizzata questa configurazione:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Passaggio 1. Aggiungere l'ASA ai dispositivi di rete sull'ISE.

Scegliere **Amministrazione > Dispositivi di rete**. Impostare una password già condivisa che verrà utilizzata dall'appliance ASA.

Passaggio 2. Creare un nome utente nell'archivio locale.

Scegliere **Amministrazione > Identità > Utenti**. Creare il nome utente come richiesto.

Per impostazione predefinita, tutte le altre impostazioni sono abilitate per ISE per l'autenticazione degli endpoint con EAP-PEAP (Protected Extensible Authentication Protocol).

ASA

La configurazione per l'accesso remoto è simile per IKEv1 e IKEv2.

```
aaa-server ISE2 protocol radius
aaa-server ISE2 (inside) host 10.62.97.21
key cisco

group-policy AllProtocols internal
group-policy AllProtocols attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

crypto ipsec ikev2 ipsec-proposal ipsec-proposal
protocol esp encryption aes-256 aes-192 aes
protocol esp integrity sha-256 sha-1 md5

crypto dynamic-map DYNMAP 10 set ikev2 ipsec-proposal ipsec-proposal
crypto map MAP 10 ipsec-isakmp dynamic DYNMAP
```

```
crypto map MAP interface outside
```

```
crypto ikev2 policy 10  
  encryption 3des  
  integrity sha  
  group 2  
  prf sha  
  lifetime seconds 86400
```

Poiché Windows 7 invia un indirizzo di tipo IKE-ID nel pacchetto IKE_AUTH, è consigliabile utilizzare **DefaultRAGroup** per assicurarsi che la connessione termini sul gruppo di tunnel corretto. L'ASA esegue l'autenticazione con un certificato (autenticazione locale) e prevede che il client utilizzi l'autenticazione EAP (autenticazione remota). Inoltre, l'ASA deve inviare specificamente una richiesta di identità EAP affinché il client risponda con una risposta di identità EAP (query-identity).

```
tunnel-group DefaultRAGroup general-attributes  
  address-pool POOL  
  authentication-server-group ISE  
  default-group-policy AllProtocols  
tunnel-group DefaultRAGroup ipsec-attributes  
  ikev2 remote-authentication eap query-identity  
  ikev2 local-authentication certificate TP
```

Infine, è necessario abilitare IKEv2 e utilizzare il certificato corretto.

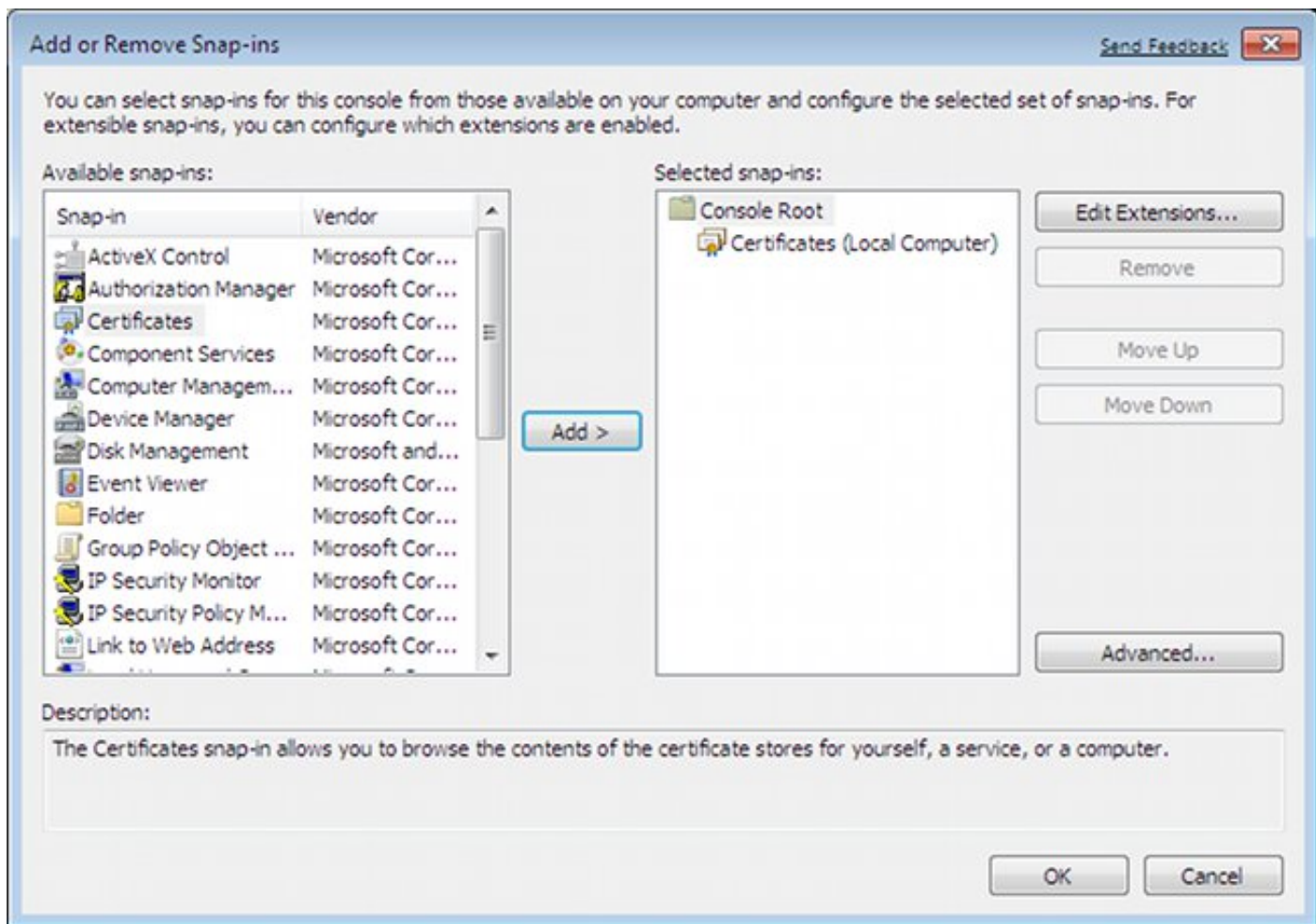
```
crypto ikev2 enable outside client-services port 443  
crypto ikev2 remote-access trustpoint TP
```

Windows 7

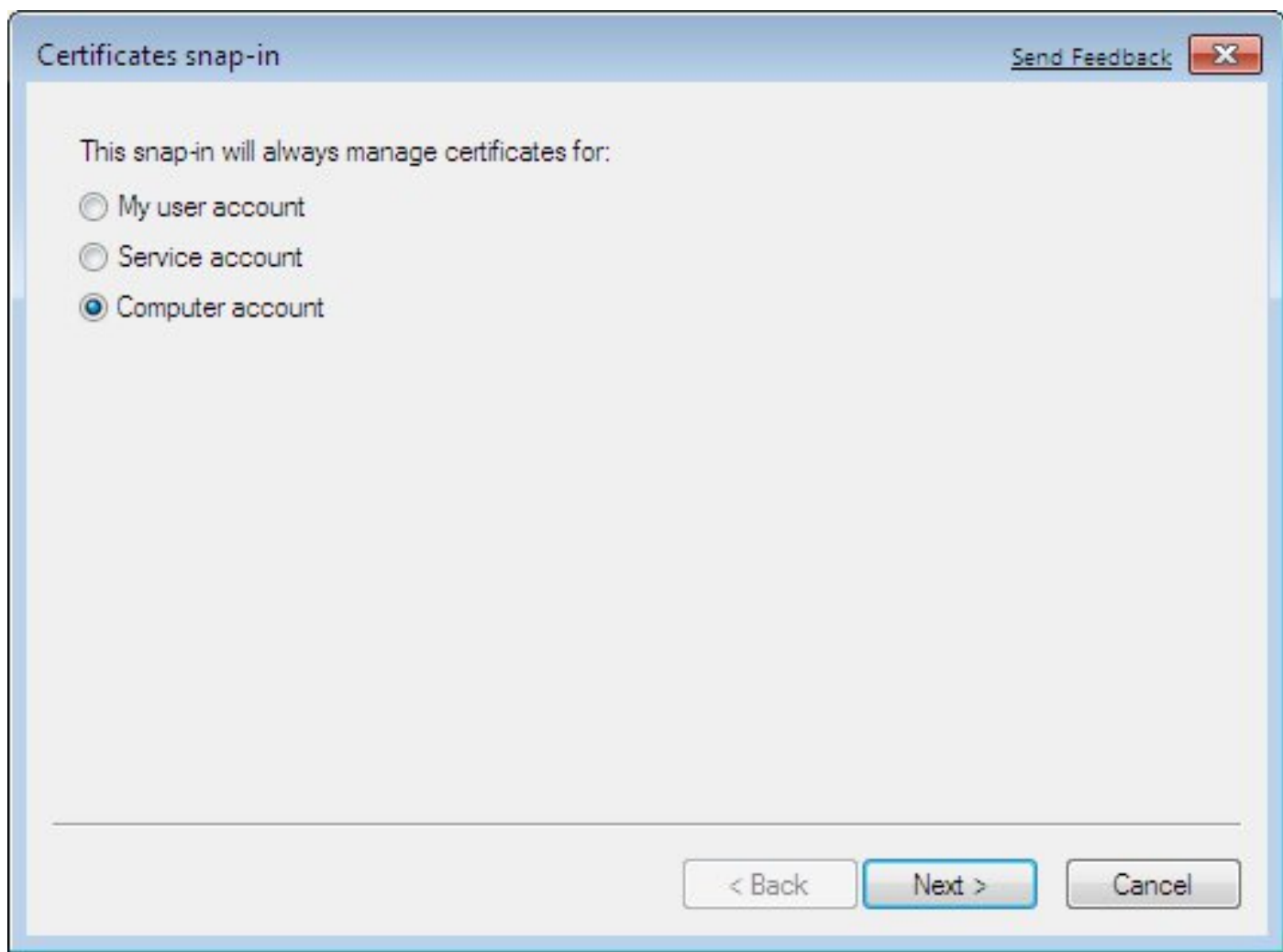
Passaggio 1. Installare il certificato CA.

Per considerare attendibile il certificato presentato dall'ASA, il client Windows deve considerare attendibile la relativa CA. È necessario aggiungere il certificato CA all'archivio certificati del computer (non all'archivio utenti). Il client Windows utilizza l'archivio del computer per convalidare il certificato IKEv2.

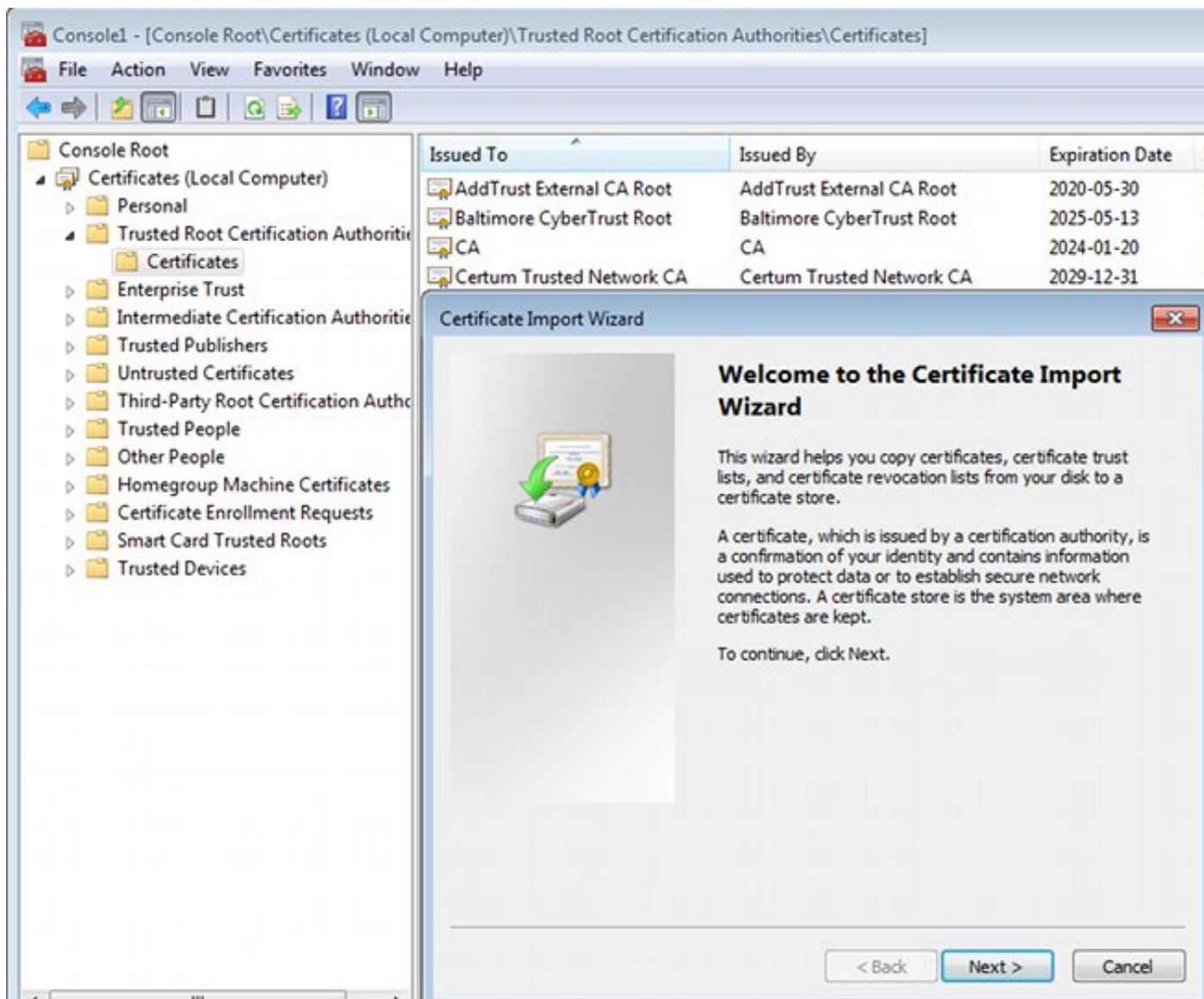
Per aggiungere la CA, scegliere **MMC > Aggiungi o rimuovi snap-in > Certificati**.



Fare clic sul pulsante di opzione **Account computer**.



Importare la CA nelle Autorità di certificazione radice attendibili.



Se il client Windows non è in grado di convalidare il certificato presentato dall'ASA, restituisce:

```
13801: IKE authentication credentials are unacceptable
```

Passaggio 2. Configurare la connessione VPN.

Per configurare la connessione VPN da Centro connessioni di rete e condivisione, scegliere **Connetti a una rete aziendale** per creare una connessione VPN.

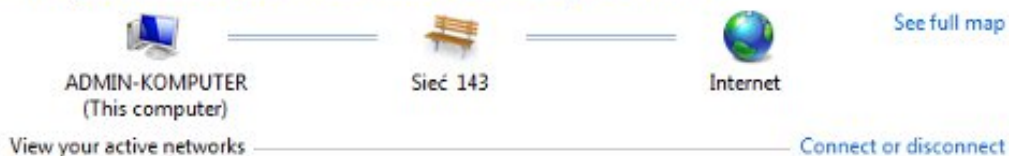
Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

[See full map](#)

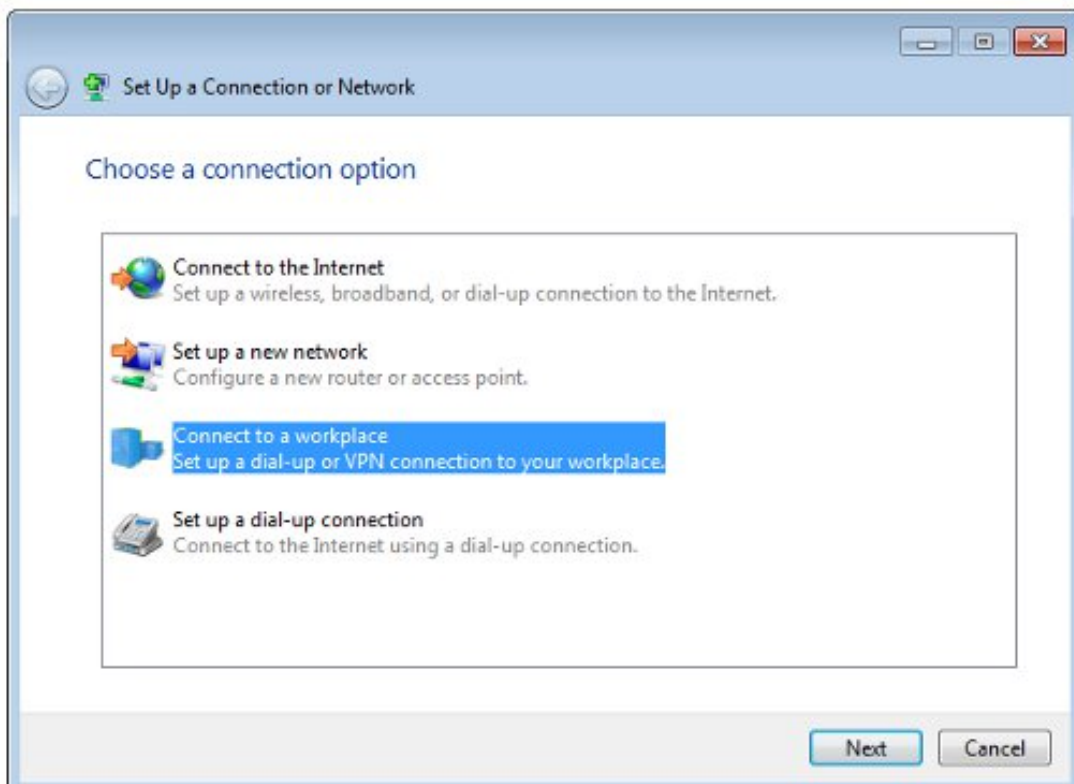


View your active networks [Connect or disconnect](#)



Change your networking settings

- [Set up a new connection or network](#)
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.



See also

Scegliere **Usa connessione Internet (VPN)**.

How do you want to connect?

- Use my Internet connection (VPN)**
Connect using a virtual private network (VPN) connection through the Internet.



Configurare l'indirizzo con un FQDN ASA. Verificare che sia risolto correttamente dal DNS (Domain Name Server).


Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

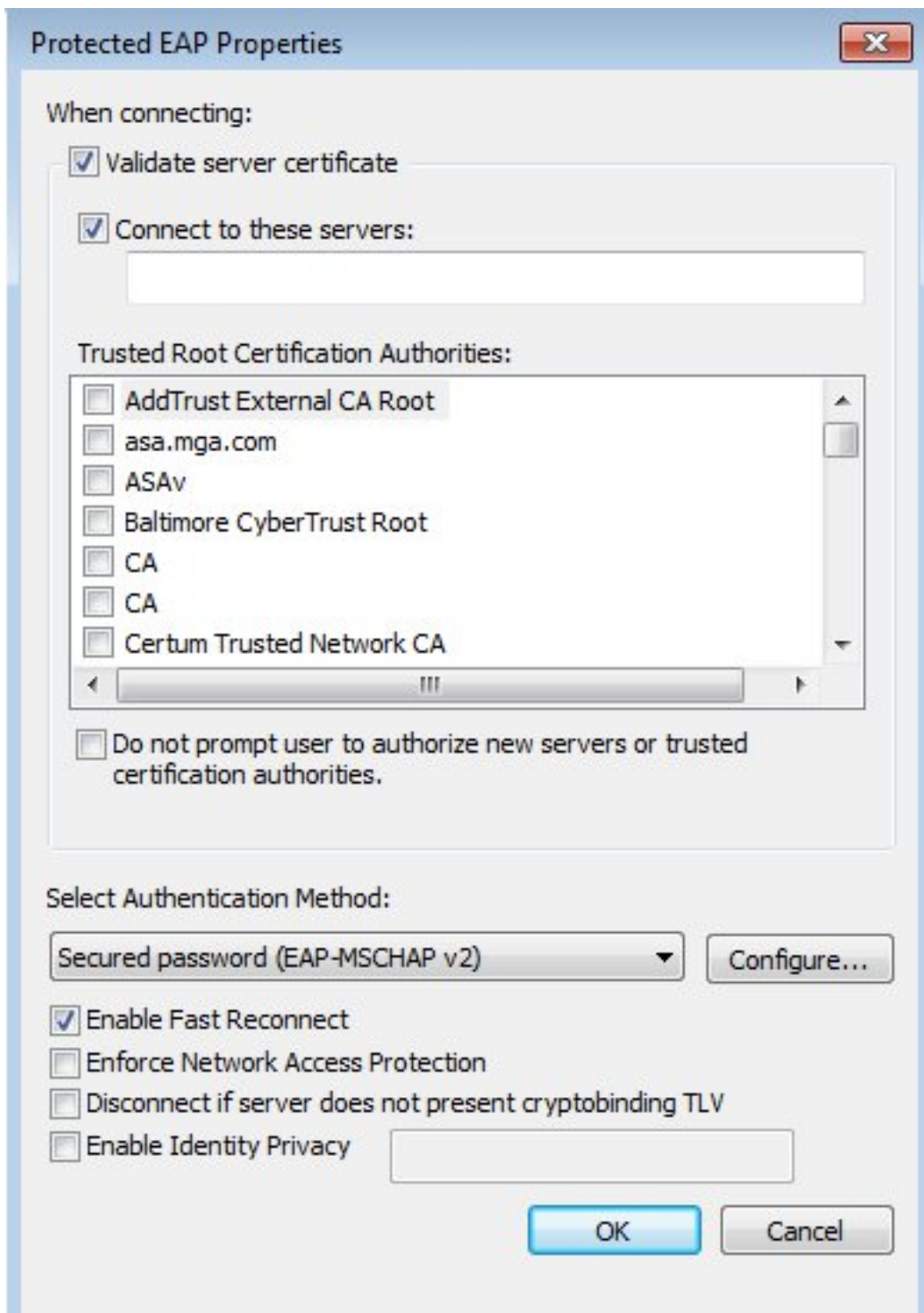
Use a smart card

 Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

Se necessario, modificare le proprietà, ad esempio la convalida del certificato, nella finestra Proprietà PEAP.



Verifica

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

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando show.

Client Windows

Quando ci si connette, immettere le credenziali.



Cisco AnyConnect Secure Mobility
Client Connection
Disabled



Ikev2 connection to ASA
Disconnected
WAN Miniport (Ikev2)

Connect IKEv2 connection to ASA



User name:

Password:

Domain:


Save this user name and password for the following users:

Me only

Anyone who uses this computer

Dopo l'autenticazione, viene applicata la configurazione IKEv2.

Connecting to ASA-IKEv2...



Registering your computer on the network...

La sessione è attiva.

Internet ▶ Network Connections ▶

Rename this connection

View status of this connection

Delete this connection



Cisco AnyConnect Secure Mobility
Client Connection
Disabled



Ikev2 connection to ASA
Ikev2 connection to ASA
WAN Miniport (Ikev2)

La tabella di routing è stata aggiornata con la route predefinita utilizzando una nuova interfaccia con metrica di livello inferiore.

```
C:\Users\admin>route print
```

```
=====  
Interface List  
41.....Ikev2 connection to ASA  
11...08 00 27 d2 cb 54 .....Karta Intel(R) PRO/1000 MT Desktop Adapter  
1.....Software Loopback Interface 1  
15...00 00 00 00 00 00 e0 Karta Microsoft ISATAP  
12...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface  
22...00 00 00 00 00 00 e0 Karta Microsoft ISATAP #4  
=====
```

```
IPv4 Route Table
```

```
=====  
Active Routes:  
Network Destination        Netmask          Gateway           Interface        Metric  
0.0.0.0                    0.0.0.0          192.168.10.1     192.168.10.68    4491  
    0.0.0.0                0.0.0.0          On-link         192.168.1.10    11  
10.62.71.177              255.255.255.255  192.168.10.1     192.168.10.68    4236  
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        4531  
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        4531  
127.255.255.255           255.255.255.255  On-link          127.0.0.1        4531  
192.168.1.10              255.255.255.255  On-link          192.168.1.10     266  
192.168.10.0              255.255.255.0    On-link          192.168.10.68    4491  
192.168.10.68            255.255.255.255  On-link          192.168.10.68    4491  
192.168.10.255           255.255.255.255  On-link          192.168.10.68    4491  
224.0.0.0                 240.0.0.0        On-link          127.0.0.1        4531  
224.0.0.0                 240.0.0.0        On-link          192.168.10.68    4493  
224.0.0.0                 240.0.0.0        On-link          192.168.1.10     11  
255.255.255.255           255.255.255.255  On-link          127.0.0.1        4531  
255.255.255.255           255.255.255.255  On-link          192.168.10.68    4491  
255.255.255.255           255.255.255.255  On-link          192.168.1.10     266  
=====
```

Log

Dopo aver completato l'autenticazione, l'appliance ASA segnala:

```
ASAv(config)# show vpn-sessiondb detail ra-ikev2-ipsec
```

```
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
```



```

Username      : cisco                               Index       : 13
Assigned IP   : 192.168.1.10                         Public IP    : 10.147.24.166
Protocol      : IKEv2 IPsecOverNatT
License       : AnyConnect Premium
Encryption    : IKEv2: (1)3DES IPsecOverNatT: (1)AES256
Hashing       : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1
Bytes Tx      : 0                                     Bytes Rx    : 7775
Pkts Tx       : 0                                     Pkts Rx     : 94
Pkts Tx Drop  : 0                                     Pkts Rx Drop : 0
Group Policy : AllProtocols                       Tunnel Group : DefaultRAGroup
Login Time    : 17:31:34 UTC Tue Nov 18 2014
Duration      : 0h:00m:50s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                                  VLAN         : none
Audt Sess ID  : c0a801010000d000546b8276
Security Grp  : none

```

```

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1

```

```

IKEv2:
Tunnel ID     : 13.1
UDP Src Port  : 4500                                UDP Dst Port : 4500
Rem Auth Mode: EAP
Loc Auth Mode: rsaCertificate
Encryption    : 3DES                                 Hashing       : SHA1
Rekey Int (T) : 86400 Seconds                        Rekey Left(T) : 86351 Seconds
PRF           : SHA1                                 D/H Group    : 2
Filter Name   :

```

```

IPsecOverNatT:
Tunnel ID     : 13.2
Local Addr   : 0.0.0.0/0.0.0.0/0/0
Remote Addr  : 192.168.1.10/255.255.255.255/0/0
Encryption    : AES256                               Hashing       : SHA1
Encapsulation : Tunnel
Rekey Int (T) : 28800 Seconds                        Rekey Left(T) : 28750 Seconds
Idle Time Out : 30 Minutes                            Idle TO Left  : 29 Minutes
Bytes Tx      : 0                                     Bytes Rx     : 7834
Pkts Tx       : 0                                     Pkts Rx     : 95

```

I registri ISE indicano che l'autenticazione è riuscita con le regole di autenticazione e autorizzazione predefinite.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs: Authentications, Reports, Endpoint Protection Service, and Troubleshoot. A summary bar displays four metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (6), and Client Stopped (0). The main area shows a table of authentication sessions with columns for Time, Status, Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Network Device. Two sessions are visible: one at 2014-11-18 18:31:34 with status 'All' and another at 2014-11-18 17:52:07 with status 'Success'.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device
2014-11-18 18:31:34...	All			cisco	10.147.24.166			
2014-11-18 17:52:07...	Success			cisco	10.147.24.166	Default >> Basic_Authenticated_Access	PermitAccess	ASAv

I dettagli indicano il metodo PEAP.

Authentication Details

Source Timestamp	2014-11-19 08:10:02.819
Received Timestamp	2014-11-19 08:10:02.821
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	cisco
User Type	User
Endpoint Id	10.147.24.166
Endpoint Profile	
IP Address	
Authentication Identity Store	Internal Users
Identity Group	
Audit Session Id	c0a8010100010000546c424a
Authentication Method	MSCHAPV2
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Login
Network Device	ASAv
Device Type	All Device Types
Location	All Locations
NAS IP Address	10.62.71.177
NAS Port Id	
NAS Port Type	Virtual
Authorization Profile	PermitAccess

Debug dell'appliance ASA

I debug più importanti includono:

ASAv# **debug crypto ikev2 protocol 32**

<most debugs omitted for clarity....

Pacchetto IKE_SA_INIT ricevuto dall'ASA (include le proposte IKEv2 e lo scambio di chiavi per Diffie-Hellman (DH)):

```
IKEv2-PROTO-2: Received Packet [From 10.147.24.166:500/To 10.62.71.177:500/VRF i0:f0]
Initiator SPI : 7E5B69A028355701 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUESTIKEv2-PROTO-3: Next payload: SA,
version: 2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 528
Payload contents:
  SA Next payload: KE, reserved: 0x0, length: 256
  last proposal: 0x2, reserved: 0x0, length: 40
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 4    last transform: 0x3,
reserved: 0x0: length: 8
.....
```

Risposta IKE_SA_INIT all'iniziatore (include le proposte IKEv2, lo scambio di chiavi per DH e la richiesta di certificato):

```
IKEv2-PROTO-2: (30): Generating IKE_SA_INIT message
IKEv2-PROTO-2: (30): IKE Proposal: 1, SPI size: 0 (initial negotiation),
Num. transforms: 4
(30):    3DES(30):    SHA1(30):    SHA96(30):    DH_GROUP_1024_MODP/Group
2IKEv2-PROTO-5:
Construct Vendor Specific Payload: DELETE-REASONIKEv2-PROTO-5: Construct Vendor
Specific Payload: (CUSTOM)IKEv2-PROTO-5: Construct Notify Payload:
NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: Construct Notify Payload:
NAT_DETECTION_DESTINATION_IPIKEv2-PROTO-5: Construct Vendor Specific Payload:
FRAGMENTATION(30):
IKEv2-PROTO-2: (30): Sending Packet [To 10.147.24.166:500/From
10.62.71.177:500/VRF i0:f0]
```

IKE_AUTH per il client con IKE-ID, richiesta di certificato, set di trasformazioni proposti, configurazione richiesta e selettori traffico:

```
IKEv2-PROTO-2: (30): Received Packet [From 10.147.24.166:4500/To 10.62.71.177:500/VRF
i0:f0]
(30): Initiator SPI : 7E5B69A028355701 - Responder SPI : 1B1A94C7A7739855 Message id: 1
(30): IKEv2 IKE_AUTH Exchange REQUESTIKEv2-PROTO-3: (30): Next payload: ENCR,
version: 2.0 (30): Exchange type: IKE_AUTH, flags: INITIATOR (30): Message id: 1,
length: 948(30):
```

Risposta IKE_AUTH dall'appliance ASA che include una richiesta di identità EAP (primo pacchetto con estensioni EAP). Il pacchetto include anche il certificato (se non è presente un certificato corretto sull'appliance ASA, è presente un errore):

```
IKEv2-PROTO-2: (30): Generating EAP request
IKEv2-PROTO-2: (30): Sending Packet [To 10.147.24.166:4500/From 10.62.71.177:4500/VRF
i0:f0]
```

Risposta EAP ricevuta dall'ASA (lunghezza 5, payload: cisco)

```
(30): REAL Decrypted packet:(30): Data: 14 bytes
(30): EAP(30): Next payload: NONE, reserved: 0x0, length: 14
(30): Code: response: id: 36, length: 10
(30): Type: identity
(30): EAP data: 5 bytes
```


Successivamente, vengono scambiati più pacchetti come parte di EAP-PEAP. Infine, il successo EAP viene ricevuto dall'ASA e inoltrato al richiedente:

Payload contents:

(30): EAP(30): Next payload: NONE, reserved: 0x0, length: 8

(30): Code: success: id: 76, length: 4

Autenticazione peer riuscita:

IKEv2-PROTO-2: (30): Verification of peer's authentication data PASSED

E la sessione VPN è terminata correttamente.

Livello pacchetto

La richiesta di identità EAP è incapsulata nella "Extensible Authentication" di IKE_AUTH inviato dall'appliance ASA. Insieme alla richiesta di identità, vengono inviati IKE_ID e certificati.

No.	Source	Destination	Protocol	Length	Info
1	10.147.24.166	10.62.71.177	ISAKMP	570	IKE_SA_INIT
2	10.62.71.177	10.147.24.166	ISAKMP	501	IKE_SA_INIT
3	10.147.24.166	10.62.71.177	ISAKMP	990	IKE_AUTH
4	10.147.24.166	10.62.71.177	ISAKMP	959	IKE_AUTH
5	10.62.71.177	10.147.24.166	EAP	1482	Request, Identity
6	10.62.71.177	10.147.24.166	ISAKMP	1514	

Length: 1440

▸ Type Payload: Vendor ID (43) : Unknown Vendor ID

▸ Type Payload: Identification - Responder (36)

▾ Type Payload: Certificate (37)

Next payload: Authentication (39)

0... = Critical Bit: Not Critical

Payload length: 1203

Certificate Encoding: X.509 Certificate - Signature (4)

▸ Certificate Data (iso.2.840.113549.1.9.2=ASAv.example.com)

▸ Type Payload: Authentication (39)

▾ Type Payload: Extensible Authentication (48)

Next payload: NONE / No Next Payload (0)

0... = Critical Bit: Not Critical

Payload length: 10

▾ Extensible Authentication Protocol

Code: Request (1)

Id: 36

Length: 6

Type: Identity (1)

Identity:

Tutti i pacchetti EAP successivi sono incapsulati in IKE_AUTH. Dopo la conferma del metodo

(EAP-PEAP), il supplicant avvia la generazione di un tunnel SSL (Secure Sockets Layer) che protegge la sessione MSCHAPv2 utilizzata per l'autenticazione.

5	10.62.71.177	10.147.24.166	EAP	1482 Request, Identity
6	10.62.71.177	10.147.24.166	ISAKMP	1514
7	10.147.24.166	10.62.71.177	ISAKMP	110 IKE_AUTH
8	10.147.24.166	10.62.71.177	EAP	84 Response, Identity
9	10.62.71.177	10.147.24.166	EAP	80 Request, Protected EAP (EAP-PEAP)
10	10.62.71.177	10.147.24.166	ISAKMP	114
11	10.147.24.166	10.62.71.177	ISAKMP	246 IKE_AUTH
12	10.147.24.166	10.62.71.177	SSL	220 Client Hello
13	10.62.71.177	10.147.24.166	TLSv1	1086 Server Hello

Dopo lo scambio di più pacchetti, ISE conferma il successo.

43	10.147.24.166	10.62.71.177	ISAKMP	150 IKE_AUTH
44	10.147.24.166	10.62.71.177	TLSv1	117 Application Data
45	10.62.71.177	10.147.24.166	EAP	78 Success

```
▼ Type Payload: Extensible Authentication (48)
  Next payload: NONE / No Next Payload (0)
  0... .... = Critical Bit: Not Critical
  Payload length: 8
  ▼ Extensible Authentication Protocol
    Code: Success (3)
    Id: 101
    Length: 4
```

La sessione IKEv2 viene completata dall'ASA, la configurazione finale (risposta della configurazione con valori quali un indirizzo IP assegnato), i set di trasformazioni e i selettori del traffico vengono inviati al client VPN.

45	10.62.71.177	10.147.24.166	EAP	78 Success
46	10.62.71.177	10.147.24.166	ISAKMP	114
47	10.147.24.166	10.62.71.177	ISAKMP	126 IKE_AUTH
48	10.147.24.166	10.62.71.177	ISAKMP	98 IKE_AUTH
49	10.62.71.177	10.147.24.166	ISAKMP	222 IKE_AUTH

- Type Payload: Configuration (47)
- Type Payload: Security Association (33)
- ▾ Type Payload: Traffic Selector - Initiator (44) # 1
 - Next payload: Traffic Selector - Responder (45)
 - 0... .. = Critical Bit: Not Critical
 - Payload length: 24
 - Number of Traffic Selector: 1
 - Traffic Selector Type: TS_IPV4_ADDR_RANGE (7)
 - Protocol ID: Unused
 - Selector Length: 16
 - Start Port: 0
 - End Port: 65535

Starting Addr: 192.168.1.10 (192.168.1.10)

Ending Addr: 192.168.1.10 (192.168.1.10)

- ▾ Type Payload: Traffic Selector - Responder (45) # 1
 - Next payload: Notify (41)
 - 0... .. = Critical Bit: Not Critical
 - Payload length: 24

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [Guida alla configurazione di Cisco ASA VPN CLI, 9.3](#)
- [Guida dell'utente di Cisco Identity Services Engine, versione 1.2](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)