Configure ASA IKEv2 Remote Access with EAP−PEAP and Native Windows Client

Document ID: 119208

Contributed by Michal Garcarz, Eugene Korneychuk, and Wojciech
Cecot, Cisco TAC Engineers.

Jul 17, 2015

Contents

Introduction

This document provides a configuration example for a Cisco Adaptive Security Appliance (ASA) Version 9.3.2 and later that allows remote VPN access to use Internet Key Exchange Protocol (IKEv2) with standard Extensible Authentication Protocol (EAP) authentication. This allows a native Microsoft Windows 7 client (and any other standard−based IKEv2) to connect to the ASA with IKEv2 and EAP authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic VPN and IKEv2 knowledge
- Basic Authentication, Authorization, and Accounting (AAA) and RADIUS knowledge
- Experience with ASA VPN configuration

- Experience with Identity Services Engine (ISE) configuration

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco ASA software, Version 9.3.2 and later
- Cisco ISE, Release 1.2 and later

Background Information

AnyConnect Secure Mobility Client Considerations

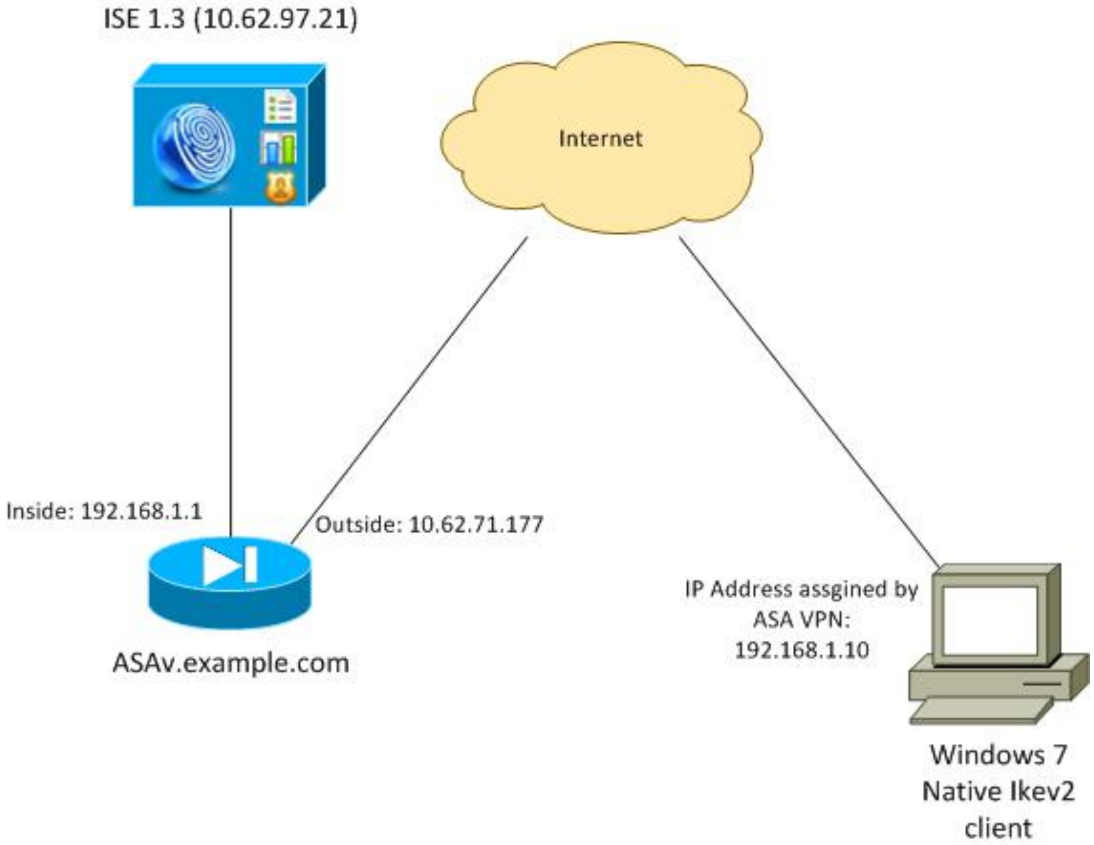
The native Windows IKEv2 client does not support split tunnel (there are no CONF REPLY attributes which could be accepted by the Windows 7 client), so the only possible policy with the Microsoft client is to tunnel all traffic (0/0 traffic selectors). If there is a need for a specific split tunnel policy, AnyConnect should be used.

AnyConnect does not support standardized EAP methods which are terminated on the AAA server (PEAP, Transport Layer Security). If there is a need to terminate EAP sessions on the AAA server then the Microsoft client can be used.

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram



The ASA is configured to authenticate with a certificate (the client needs to trust that certificate). The Windows 7 client is configured to authenticate with EAP (EAP−PEAP).

The ASA acts as VPN gateway terminating IKEv2 session from the client. The ISE acts as an AAA server terminating EAP session from the client. EAP packets are encapsulated in IKE_AUTH packets for traffic between the client and the ASA (IKEv2) and then in RADIUS packets for authentication traffic between the ASA and the ISE.

Certificates

Microsoft Certificate Authority (CA) has been used in order to generate the certificate for the ASA. The certificate requirements in order to be accepted by the Windows 7 native client are:

- The Extended Key Usage (EKU) extension should include Server Authentication (template "Web server" has been used in that example).
- The Subject−Name should include the Fully Qualified Domain Name (FQDN) which will be used by the client in order to connect (in this example ASAv.example.com).

For more details on the Microsoft client, see Troubleshooting IKEv2 VPN Connections.

Note: Android 4.x is more restrictive and requires the correct Subject Alternative Name as per RFC 6125. For more information for Android, see IKEv2 from Android strongSwan to Cisco IOS with EAP and RSA Authentication.

In order to generate a certificate signing request on the ASA, this configuration has been used:

```
hostname ASAv
domain−name example.com
```

```
crypto ca trustpoint TP
 enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Step 1. Add the ASA to the network devices on the ISE.

Choose ***Administration*** > ***Network Devices***. Set a preshared password which will be used by the ASA.

Step 2. Create a username in the local store.

Choose ***Administration*** > ***Identities*** > ***Users***. Create the username as required.

All other settings are enabled by default for the ISE to authenticate endpoints with EAP−PEAP (Protected Extensible Authentication Protocol).

ASA

The configuration for remote access is similar for IKEv1 and 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
```

Since Windows 7 sends an IKE−ID type address in IKE_AUTH packet, the ***DefaultRAGroup*** should be used in order to make sure that the connection lands on the correct tunnel−group. The ASA authenticates with a certificate (local−authentication) and expects the client to use EAP (remote−authentication). Also, the ASA needs to specifically send an EAP identity request for the client to respond with EAP identity response (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
```

Finally, IKEv2 needs to be enabled and the correct certificate used.

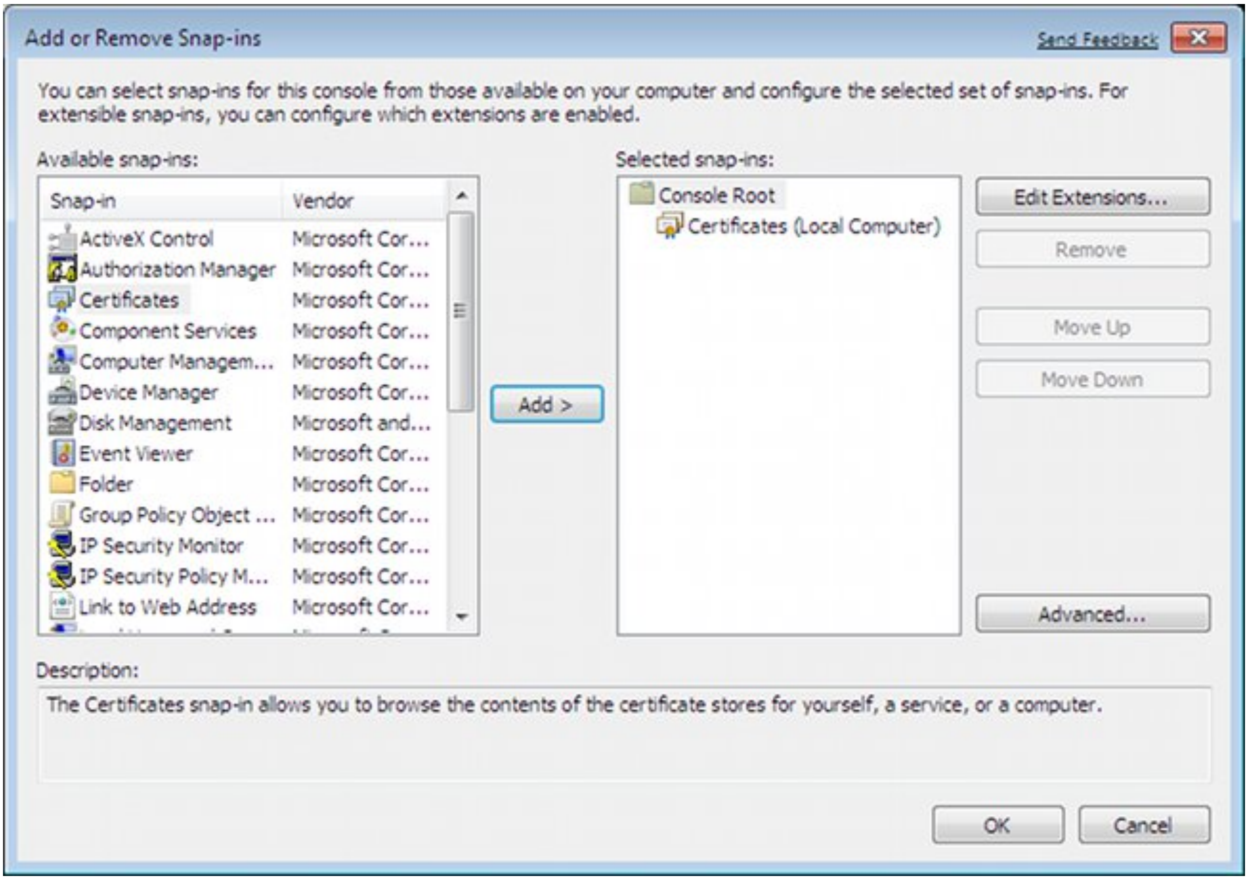
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

Windows 7

Step 1. Install the CA certificate.

In order to trust the certificate presented by the ASA, the Windows client needs to trust its CA. That CA certificate should be added to the computer certificate store (not the user store). The Windows client uses the computer store in order to validate the IKEv2 certificate.

In order to add the CA, choose ***MMC* > *Add or Remove Snap−ins* > *Certificates***.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

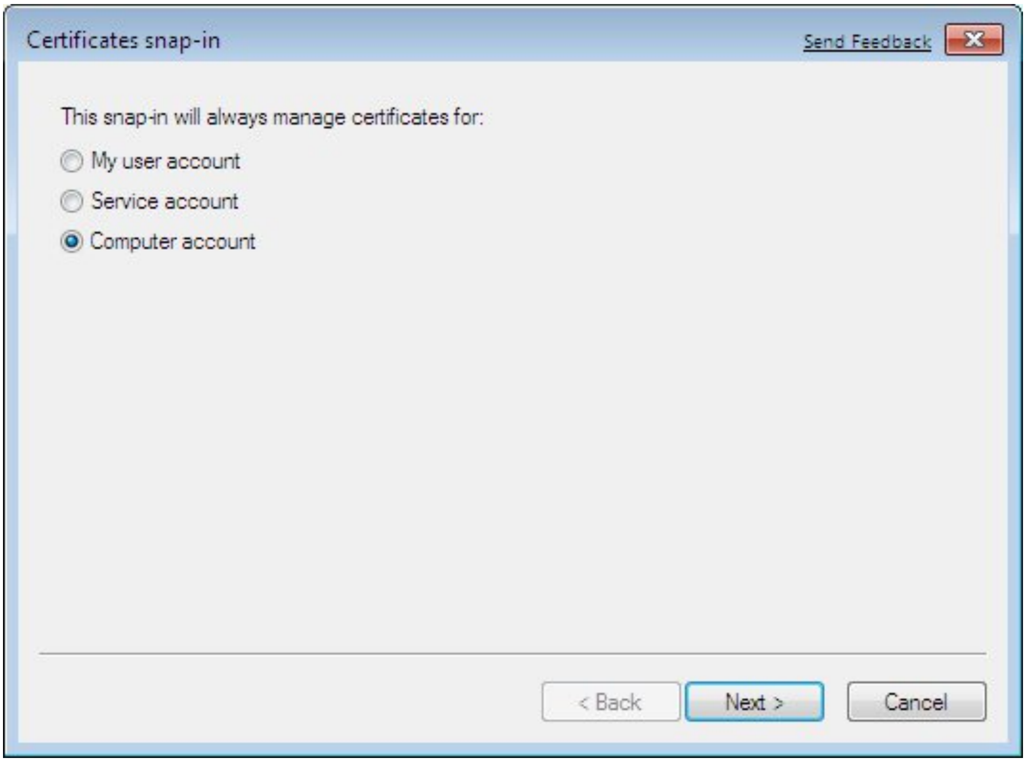
Selected snap-ins:

Console Root
  Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Click the ***Computer account*** radio button.



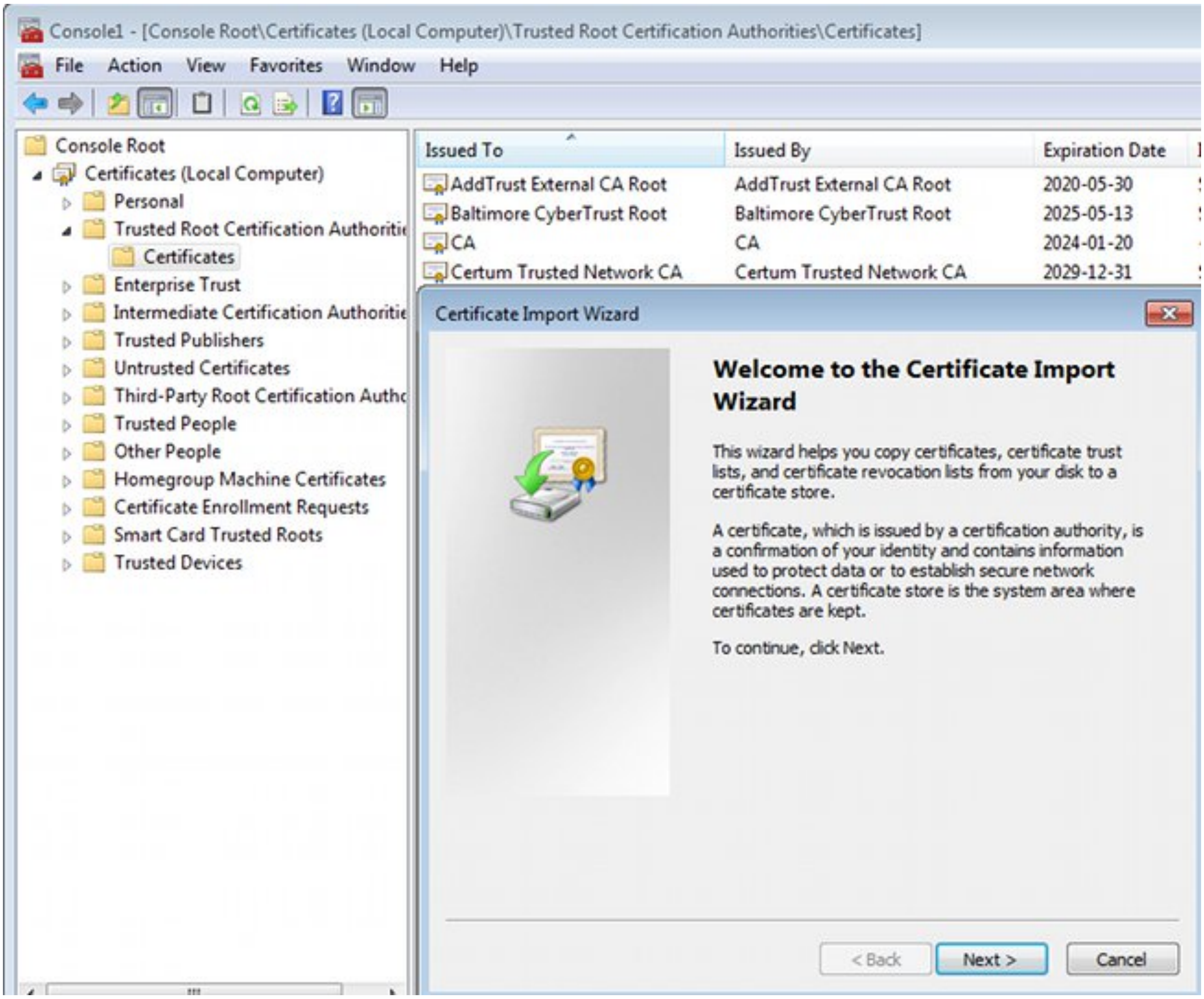
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

Import the CA to the Trusted Root Certificate Authorities.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authoritie
Certificates
Enterprise Trust
Intermediate Certification Authoritie
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authc
Trusted People
Other People
Homegroup Machine Certificates
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Certificate Import Wizard
< Back
Next >
Cancel

Issued To	Issued By	Expiration Date
AddTrust External CA Root	AddTrust External CA Root	2020-05-30
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025-05-13
CA	CA	2024-01-20
Certum Trusted Network CA	Certum Trusted Network CA	2029-12-31

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

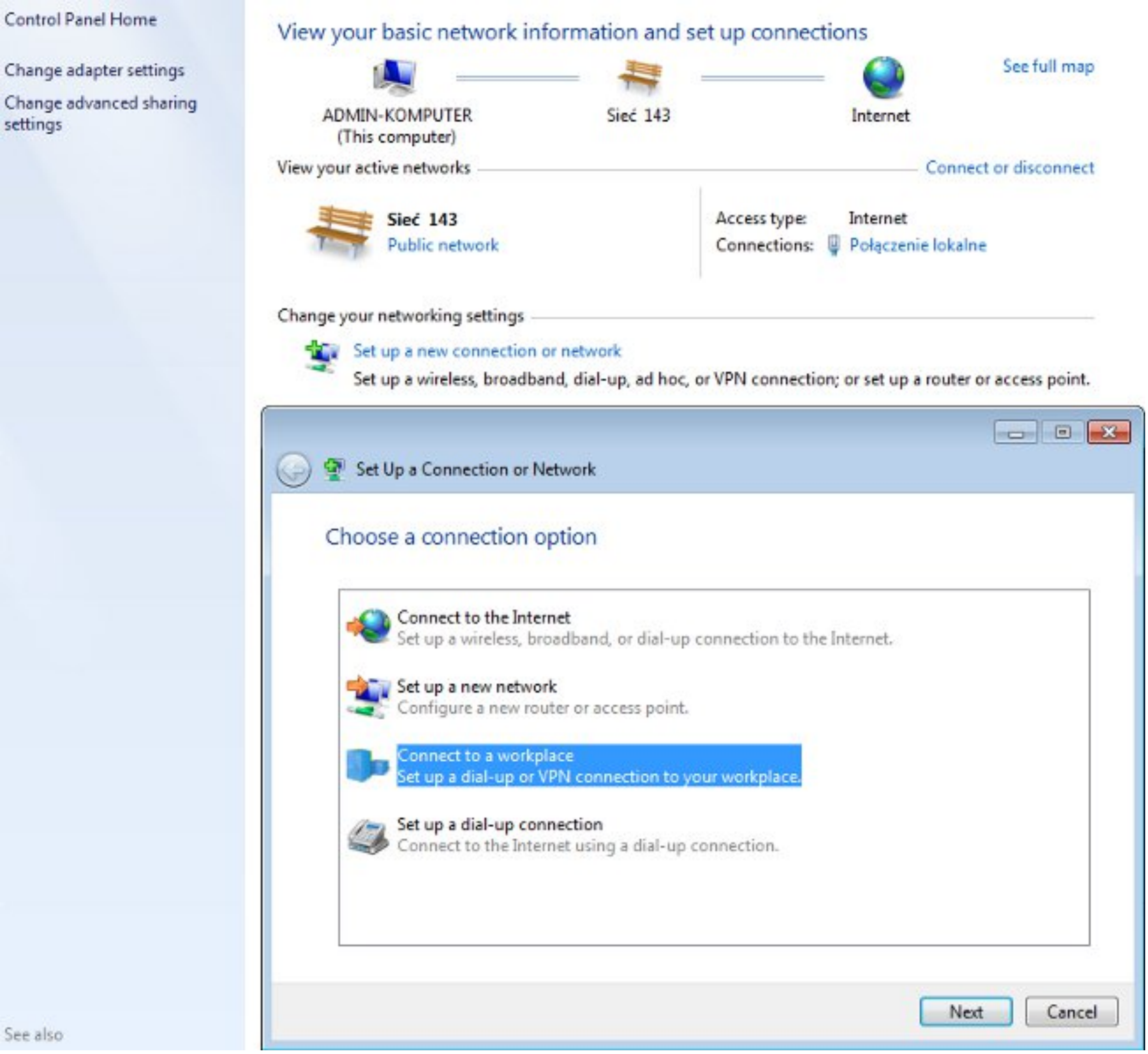
To continue, click Next.

If the Windows client is not able to validate the certificate presented by the ASA, it reports:

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

Step 2. Configure the VPN connection.

In order to configure the VPN connection from the Network and Sharing Center, choose ***Connect to a workplace*** in order to create a VPN connection.



Control Panel Home

Change adapter settings

Change advanced sharing settings

See also

View your basic network information and set up connections

ADMIN-KOMPUTER (This computer) — Sieć 143 — Internet

See full map

View your active networks — Connect or disconnect

Sieć 143
Public network

Access type: Internet
Connections: Połączenie lokalne

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.

Set Up a Connection or Network

Choose a connection option

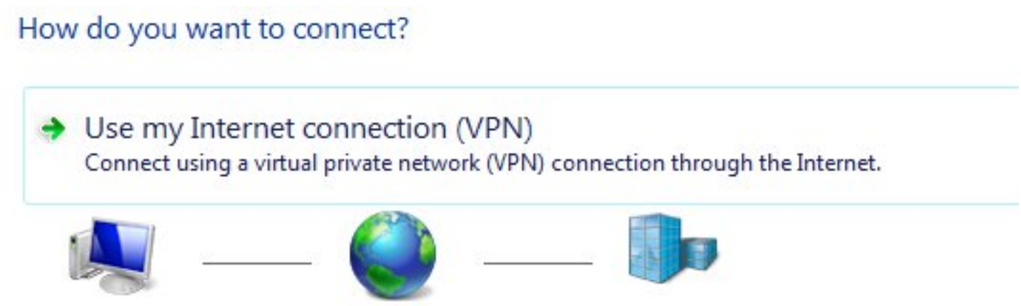
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

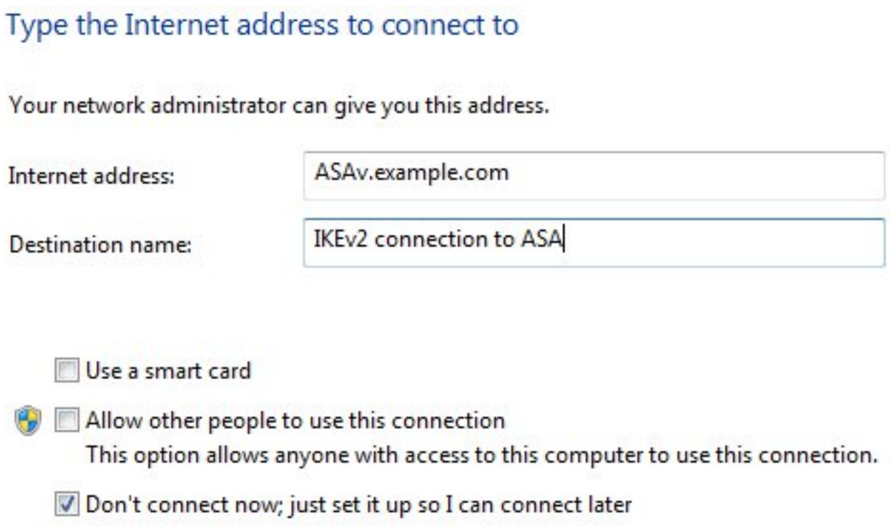
Choose ***Use my Internet connection (VPN)***.



How do you want to connect?

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

Configure the address with an ASA FQDN. Make sure it is correctly resolved by the Domain Name Server (DNS).



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: ASAv.example.com

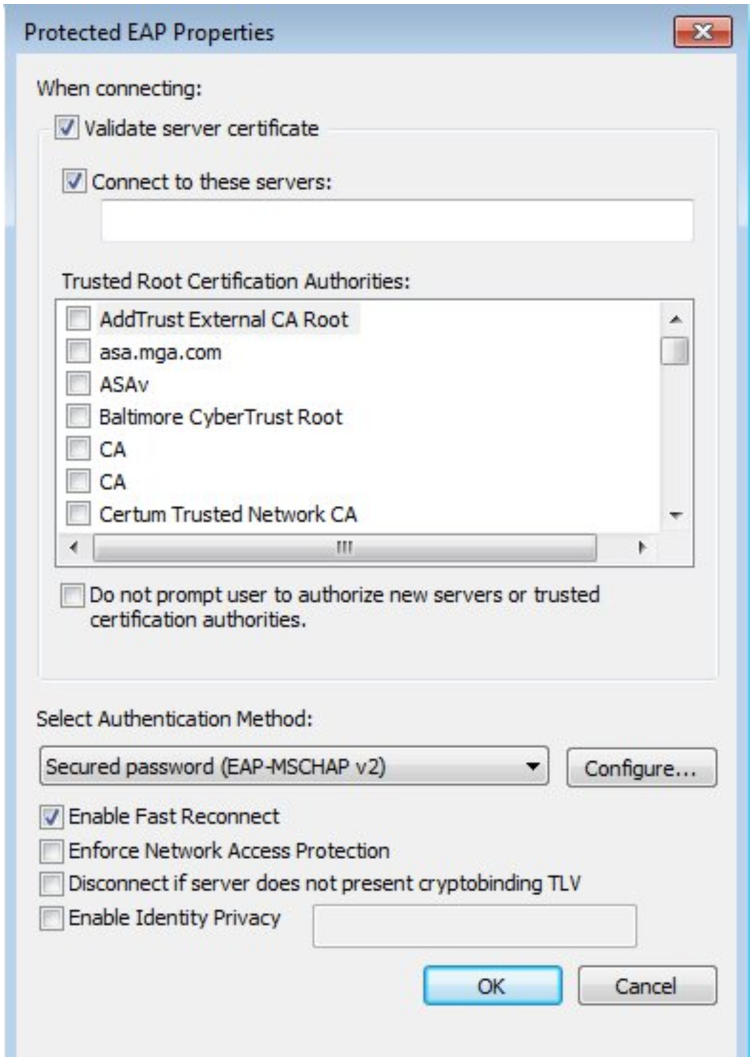
Destination name: IKEv2 connection to ASA

□ 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

If required, adjust properties (such as certificate validation) on the Protected EAP Properties window.



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ asa.mga.com
□ ASAv
□ Baltimore CyberTrust Root
□ CA
□ CA
□ Certum Trusted Network CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

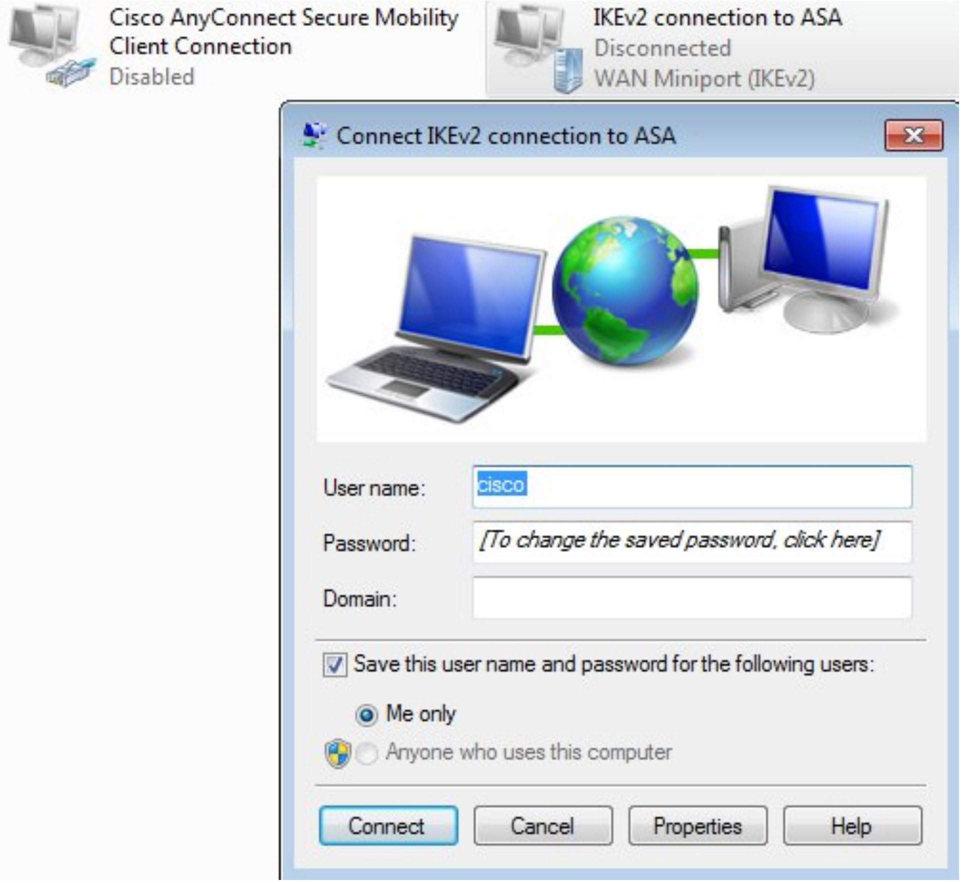
Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Windows Client

When you connect, enter your credentials.



Cisco AnyConnect Secure Mobility Client Connection
Disabled

IKEv2 connection to ASA
Disconnected
WAN Miniport (IKEv2)

Connect IKEv2 connection to ASA

User name: cisco

Password: [To change the saved password, click here]

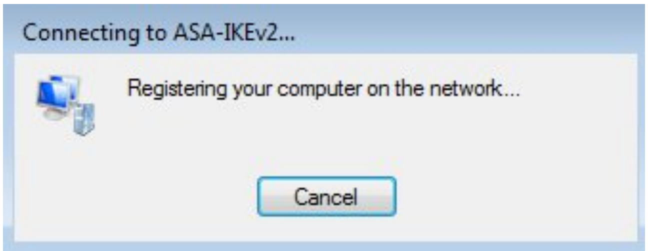
Domain:

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

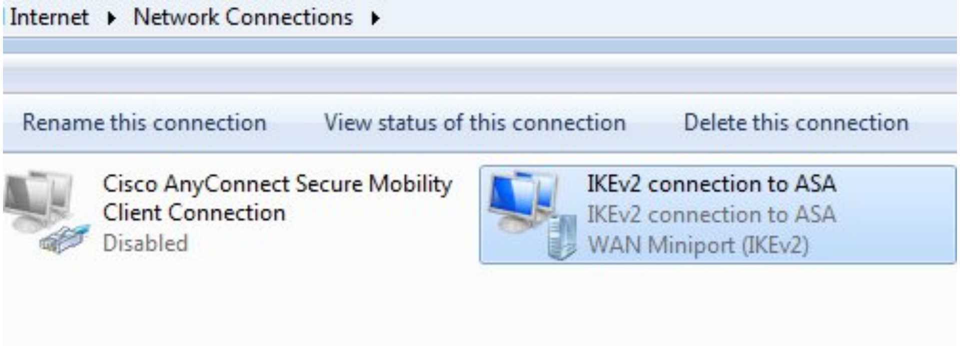
After successful authentication the IKEv2 configuration is applied.



Connecting to ASA-IKEv2...

Registering your computer on the network...

The session is UP.



The routing table has been updated with the default route with use of a new interface with the low metric.

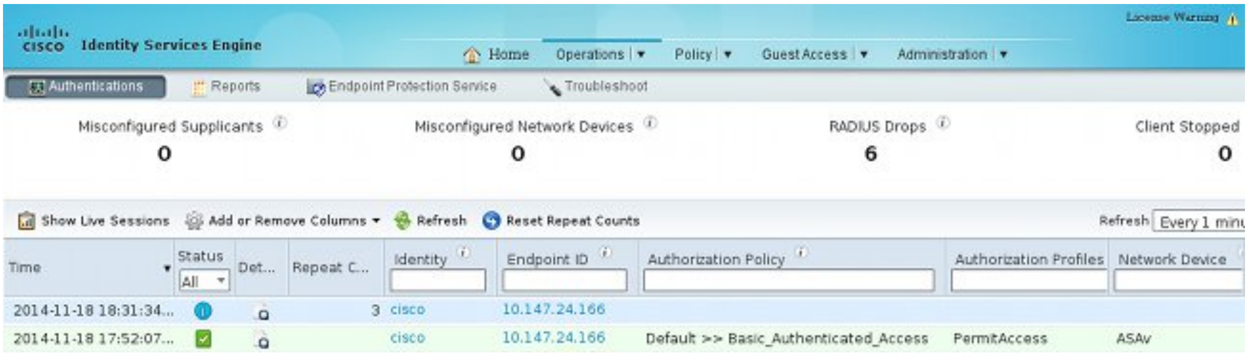
```
C:\Users\admin>route print
===========================================================================
Interface List
 41...........................IKEv2 connection to ASA
 11...08 00 27 d2 cb 54 ......Karta Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
 15...00 00 00 00 00 00 00 e0 Karta Microsoft ISATAP
 12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 22...00 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
===========================================================================
```

Logs

After successful authentication the ASA reports:

```
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
```

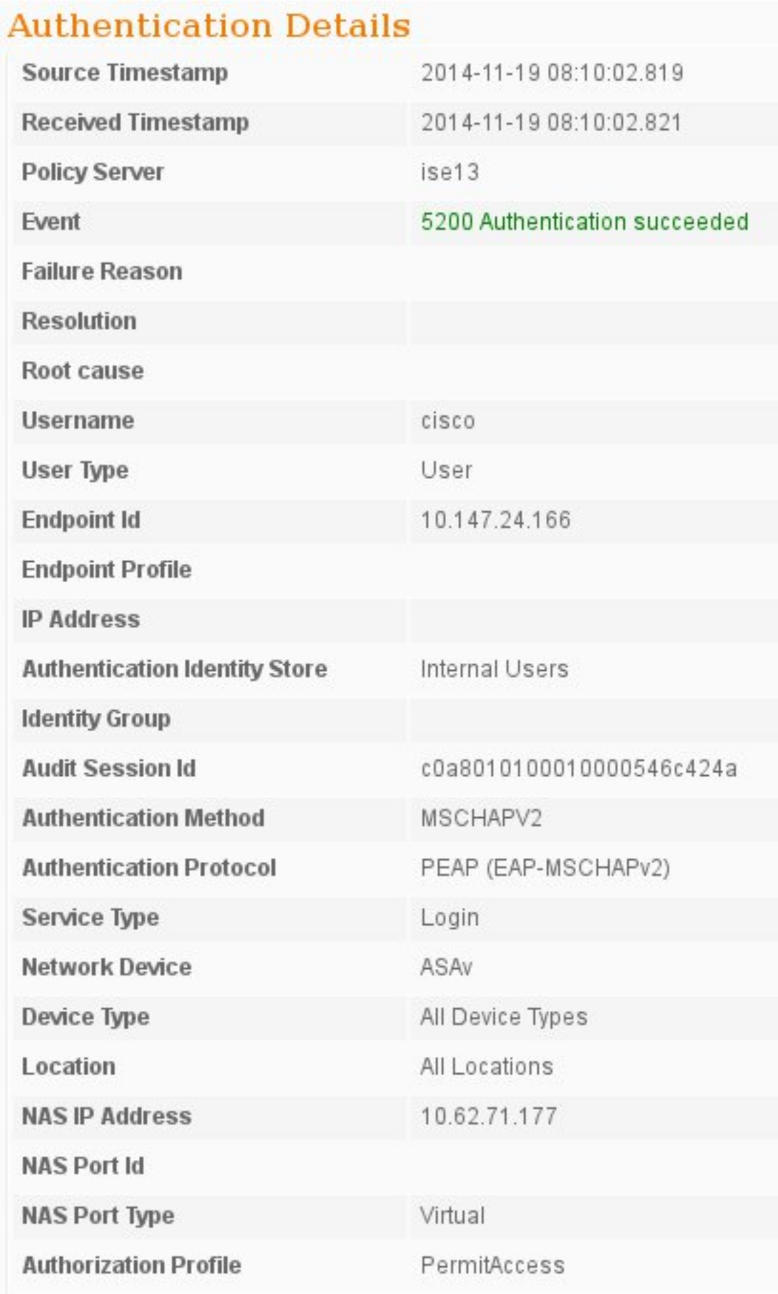
ISE logs indicate successful authentication with default authentication and authorization rules.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped
0	0	6	0

Time	Status All	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device
2014-11-18 18:31:34...	●		3	cisco	10.147.24.166			
2014-11-18 17:52:07...	✓			cisco	10.147.24.166	Default >> Basic_Authenticated_Access	PermitAccess	ASAv

The details indicate the PEAP method.



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

Debugs on the ASA

The most important debugs include:

```
ASAv# debug crypto ikev2 protocol 32
<most debugs omitted for clarity....
```

IKE_SA_INIT packet received by the ASA (includes IKEv2 proposals and key exchange for 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
.....
```

IKE_SA_INIT response to the initiator (includes IKEv2 proposals, key exchange for DH, and certificate request):

```
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 for client with IKE−ID, certificate request, proposed transform sets, requested configuration, and traffic selectors:

```
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):
```

IKE_AUTH response from the ASA that includes an EAP identity request (first packet with EAP extensions). That packet also includes the certificate (if there is no correct certificate on the ASA there is a failure):

```
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]
```

EAP response received by the ASA (length 5, payload: cisco):

```
(30): REAL Decrypted packet:(30): Data&colon; 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&colon; 5 bytes
```

Then multiple packets are exchanged as a part of EAP−PEAP. Finally EAP success is received by the ASA and forwarded to the supplicant:

```
Payload contents:
(30):  EAP(30):   Next payload: NONE, reserved: 0x0, length: 8
(30):     Code: success: id: 76, length: 4
```

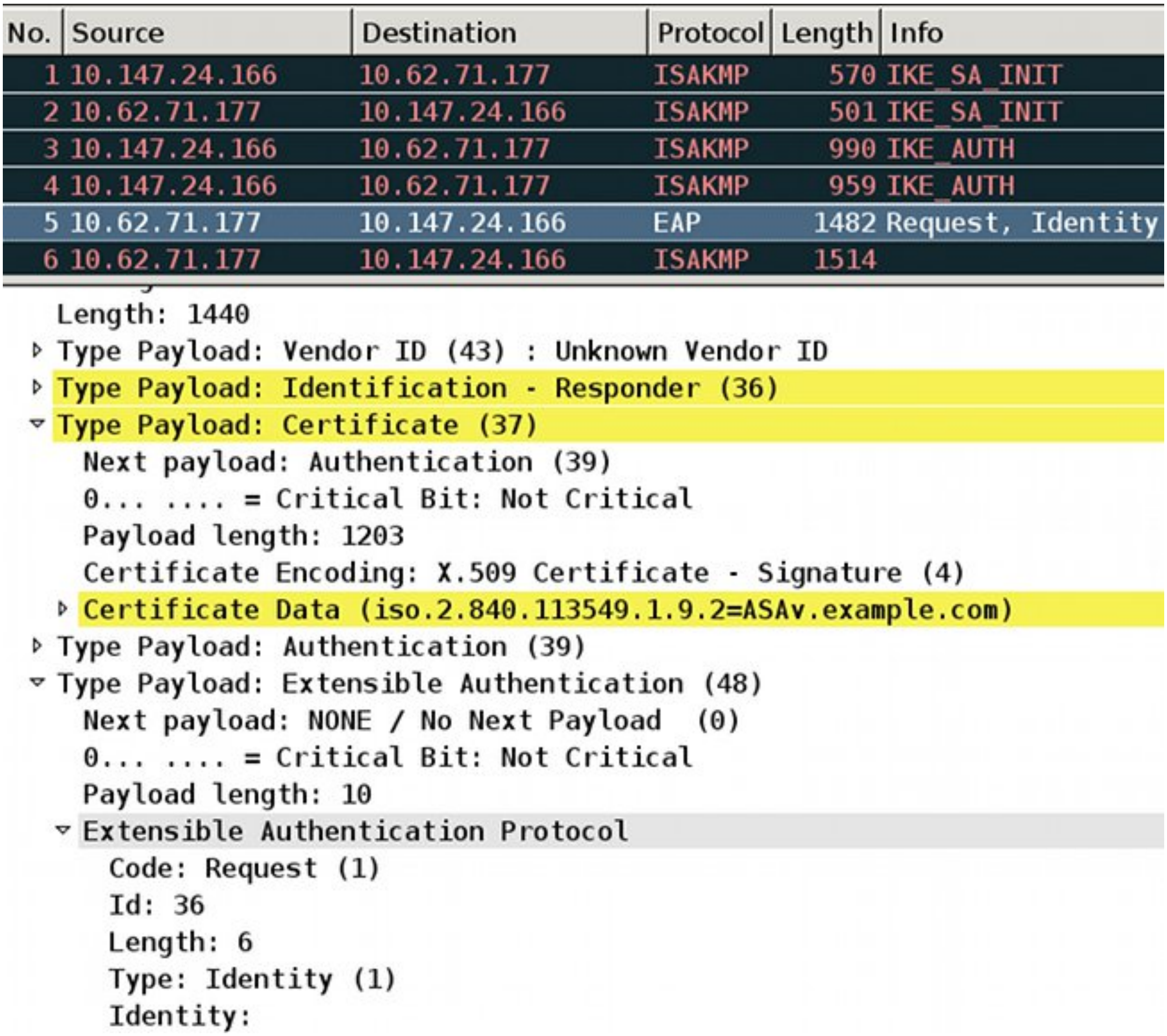
Peer authentication is successful:

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

And the VPN session is finished correctly.

Packet Level

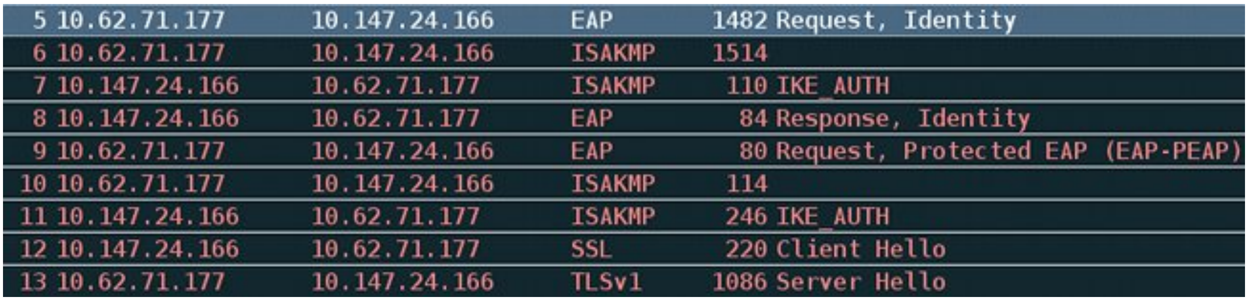
The EAP identity request is encapsulated in "Extensible Authentication" of the IKE_AUTH send by the ASA. Along with the identity request, IKE_ID and certificates are sent.



```
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
```

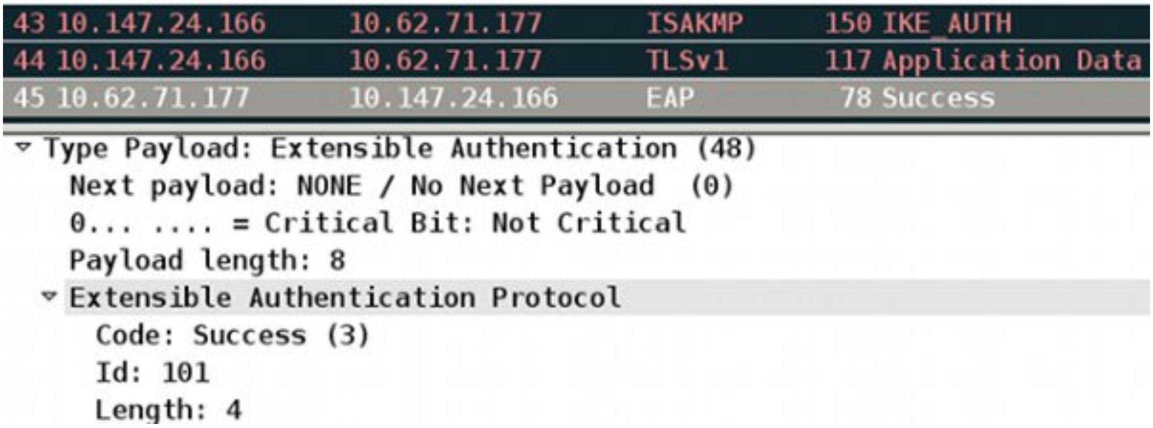
```
  Length: 1440
▷ Type Payload: Vendor ID (43) : Unknown Vendor ID
▷ Type Payload: Identification - Responder (36)
▽ Type Payload: Certificate (37)
    Next payload: Authentication (39)
    0... .... = Critical Bit: Not Critical
    Payload length: 1203
    Certificate Encoding: X.509 Certificate - 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:
```

All subsequent EAP packets are encapsulated in IKE_AUTH. After the supplicant confirms the method (EAP−PEAP), it starts to build an Secure Sockets Layer (SSL) tunnel which protects the MSCHAPv2 session used for authentication.



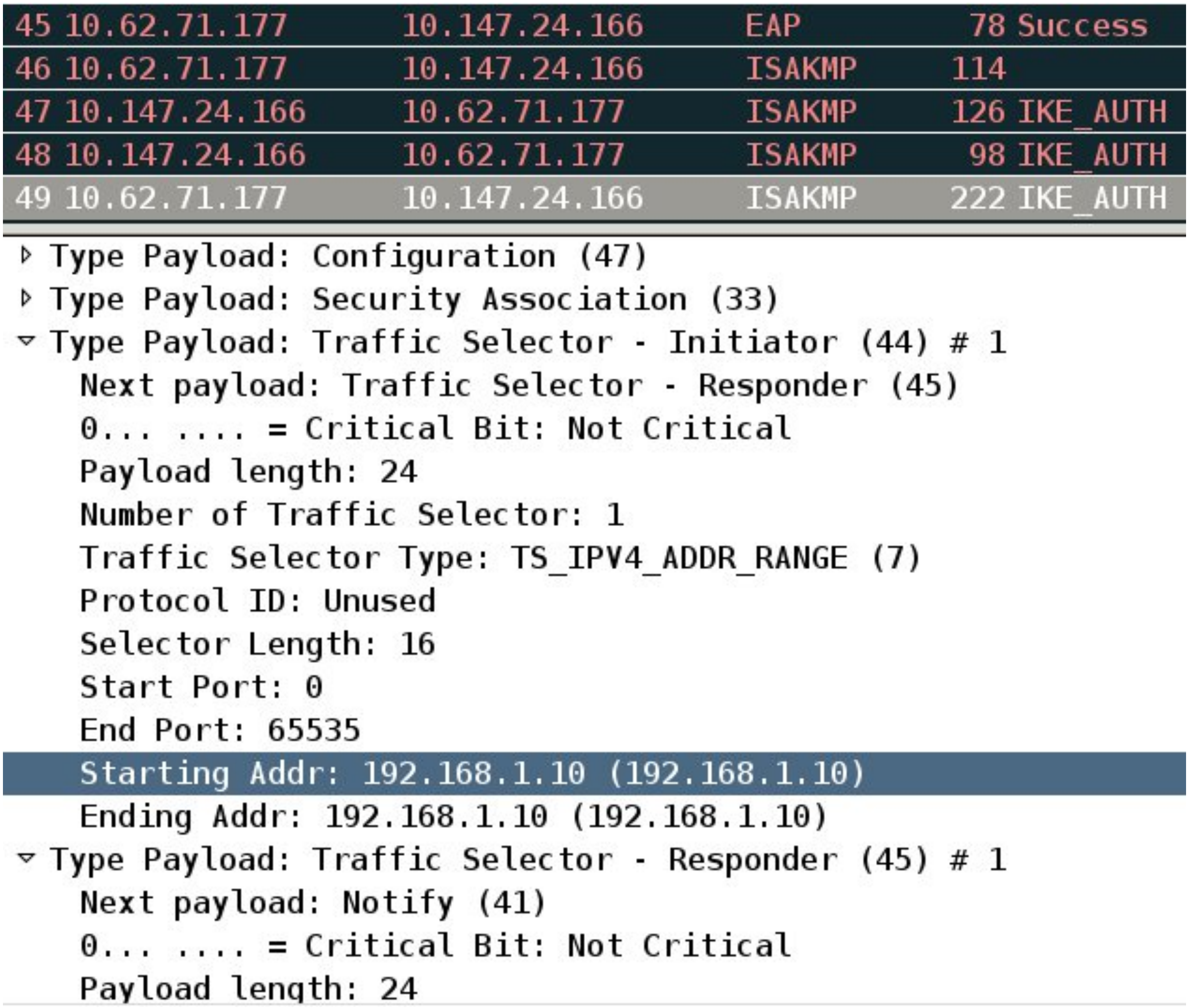
```
 5 10.62.71.177    10.147.24.166   EAP     1482 Request, Identity
 6 10.62.71.177    10.147.24.166   ISAKMP  1514
 7 10.147.24.166   10.62.71.177    ISAKMP   110 IKE_AUTH
 8 10.147.24.166   10.62.71.177    EAP       84 Response, Identity
 9 10.62.71.177    10.147.24.166   EAP       80 Request, Protected 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
```

After multiple packets are exchanged the ISE confirms success.



```
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
```

The IKEv2 session is completed by the ASA, final configuration (configuration reply with values such as an assigned IP address), transform sets, and traffic selectors are pushed to the VPN client.



```
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
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***Cisco ASA Series VPN CLI Configuration Guide, 9.3***
- ***Cisco Identity Services Engine User Guide, Release 1.2***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Jul 17, 2015 Document ID: 119208