

ASA IKEv2 externe toegang configureren met EAP-PEAP en Native Windows-client

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[AnyConnect Secure Mobility-clientoverwegingen](#)

[Configureren](#)

[Netwerkdigram](#)

[Certificaten](#)

[ISE](#)

[Stap 1. Voeg de ASA toe aan de netwerkapparaten op ISE.](#)

[Stap 2. Maak een gebruikersnaam in de lokale winkel.](#)

[ASA](#)

[Windows 7](#)

[Stap 1. Installeer het CA-certificaat.](#)

[Stap 2. Configuratie van de VPN-verbinding.](#)

[Verifiëren](#)

[Windows-client](#)

[Logs](#)

[Debugs in de ASA](#)

[Packet Level](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een configuratievoorbeeld voor een Cisco adaptieve security applicatie (ASA) versie 9.3.2 en hoger dat externe VPN-toegang mogelijk maakt om Internet Key Exchange Protocol (IKEv2) te gebruiken met de standaard EAP-verificatie (Extensible Authentication Protocol). Hierdoor kan een native Microsoft Windows 7-client (en elke andere op standaard gebaseerde IKEv2) verbinding maken met de ASA met IKEv2 en EAP-verificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van VPN en IKEv2
- Basis verificatie, autorisatie en accounting (AAA) en RADIUS-kennis
- Ervaring met ASA VPN-configuratie
- Ervaring met configuratie van Identity Services Engine (ISE)

Gebruikte componenten

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

- Microsoft Windows 7
- Cisco ASA-software, versie 9.3.2 en hoger
- Cisco ISE, release 1.2 en hoger

Achtergrondinformatie

AnyConnect Secure Mobility-clientoverwegingen

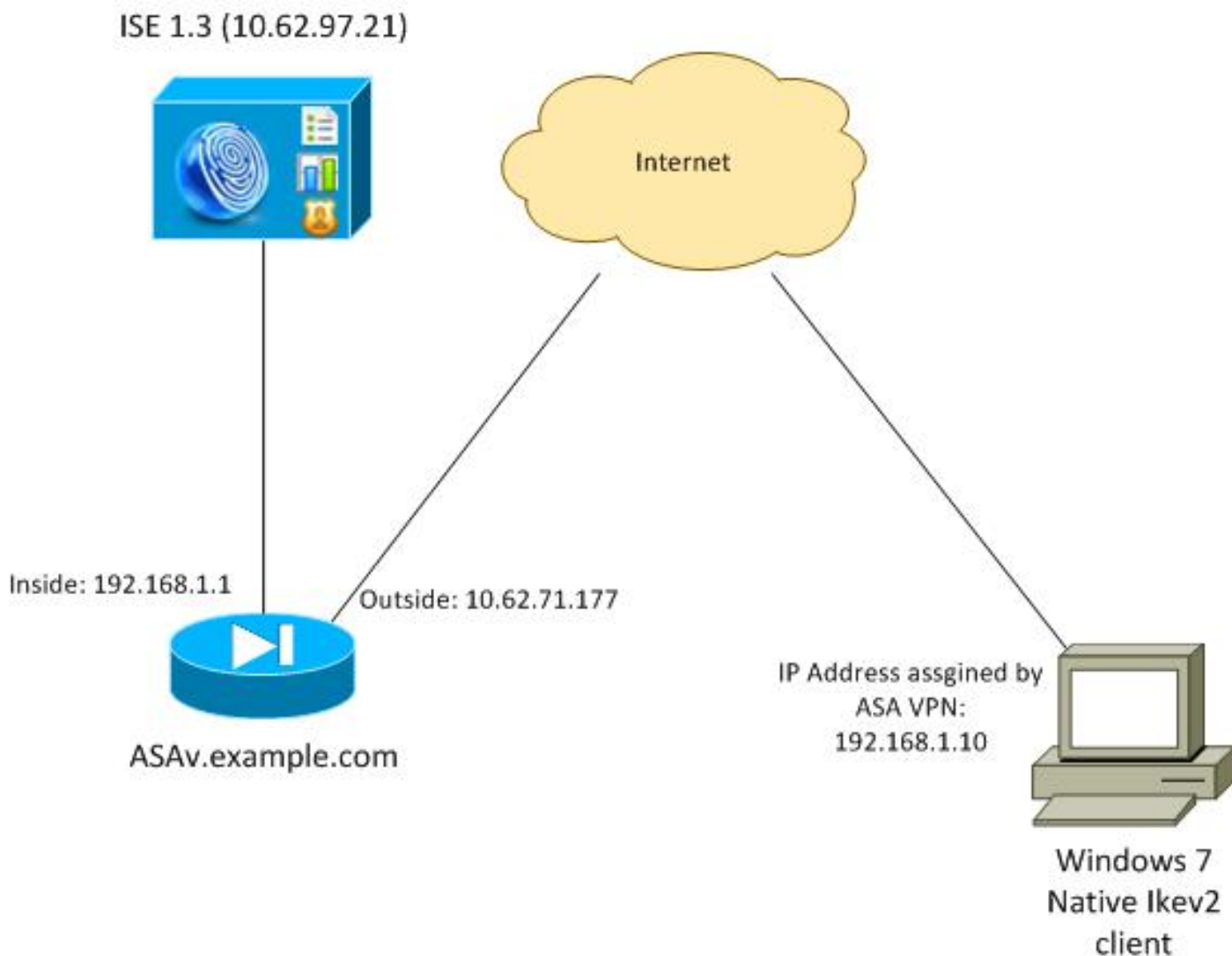
De native Windows IKEv2-client ondersteunt gesplitste tunnels niet (er zijn geen CONF REPLY-eigenschappen die door Windows 7-client kunnen worden geaccepteerd), dus het enige mogelijke beleid met de Microsoft-client is tunnelverkeer (0/0-selectors). Als er behoefte is aan een specifiek beleid voor gesplitste tunnels, moet AnyConnect worden gebruikt.

AnyConnect ondersteunt geen gestandaardiseerde MAP-methoden die op de AAA-server (PEAP, Transport Layer Security) worden afgesloten. Als er MAP-sessies op de AAA-server moeten worden afgesloten, kan de Microsoft-client worden gebruikt.

Configureren

Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreerde gebruikers\) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.](#)

Netwerkdigram



De ASA is ingesteld op authenticatie met een certificaat (de klant moet dat certificaat vertrouwen). De Windows 7-client is ingesteld op authenticatie met EAP (EAP-PEAP).

De ASA werkt als VPN gateway die IKEv2-sessie van de client beëindigen. De ISE werkt als een AAA-server die de EAP-sessie van de klant beëindigt. EAP-pakketten zijn ingekapseld in IKE_AUTH-pakketten voor verkeer tussen de client en de ASA (IKEv2) en vervolgens in RADIUS-pakketten voor verificatieverkeer tussen de ASA en de ISE.

Certificaten

Microsoft certificaatinstantie (CA) is gebruikt om het certificaat voor de ASA te genereren. De certificaateisen die moeten worden aanvaard door de oorspronkelijke klant van Windows 7 zijn:

- De Extended Key Gebruik (EKU)-uitbreiding moet serververificatie omvatten (sjabloon "webserver" is in dat voorbeeld gebruikt).
- De Onderwerp-naam dient de Fully Qualified Domain Name (FQDN) te omvatten die door de client zal worden gebruikt om verbinding te maken (in dit voorbeeld ASAv.Preview.com).

Zie [Aansluitingen](#) voor meer informatie over de Microsoft client [voor probleemoplossing IKEv2 VPN](#).

Opmerking: Android 4.x is restrictiever en vereist de juiste Onderwerp Alternatieve Naam

zoals bepaald door RFC 6125. Voor meer informatie voor Android, zie [IKEv2 van Android strongSwan tot Cisco IOS met EAP en RSA Verificatie](#).

Om een certificaatondertekeningsverzoek op de ASA te genereren, is deze configuratie gebruikt:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Stap 1. Voeg de ASA toe aan de netwerkapparaten op ISE.

Kies **Beheer > Netwerkapparaten**. Stel een vooraf gedeeld wachtwoord in dat door de ASA wordt gebruikt.

Stap 2. Maak een gebruikersnaam in de lokale winkel.

Kies **Administratie > Identiteiten > Gebruikers**. Maak de gebruikersnaam zoals vereist.

Alle andere instellingen zijn standaard ingeschakeld voor ISE om endpoints te authenticeren met EAP-PEAP (Protected Extensible Authentication Protocol).

ASA

De configuratie voor externe toegang is vergelijkbaar voor IKEv1 en 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
```

Aangezien Windows 7 een IKE-ID-type adres verstuurt in IKE_AUTH-pakket, dient **DefaultRAGGroup** gebruikt te worden om te verzekeren dat de verbinding op de juiste tunnelgroep wordt gelegd. De ASA authenticceert met een certificaat (lokale authenticatie) en verwacht dat de client EAP (externe verificatie) gebruikt. Bovendien moet de ASA specifiek een MAP-identiteitsverzoek sturen om de cliënt te laten reageren met een MAP-antwoord (query-identiteit).

```
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
```

Ten slotte moet IKEv2 worden ingeschakeld en moet het juiste certificaat worden gebruikt.

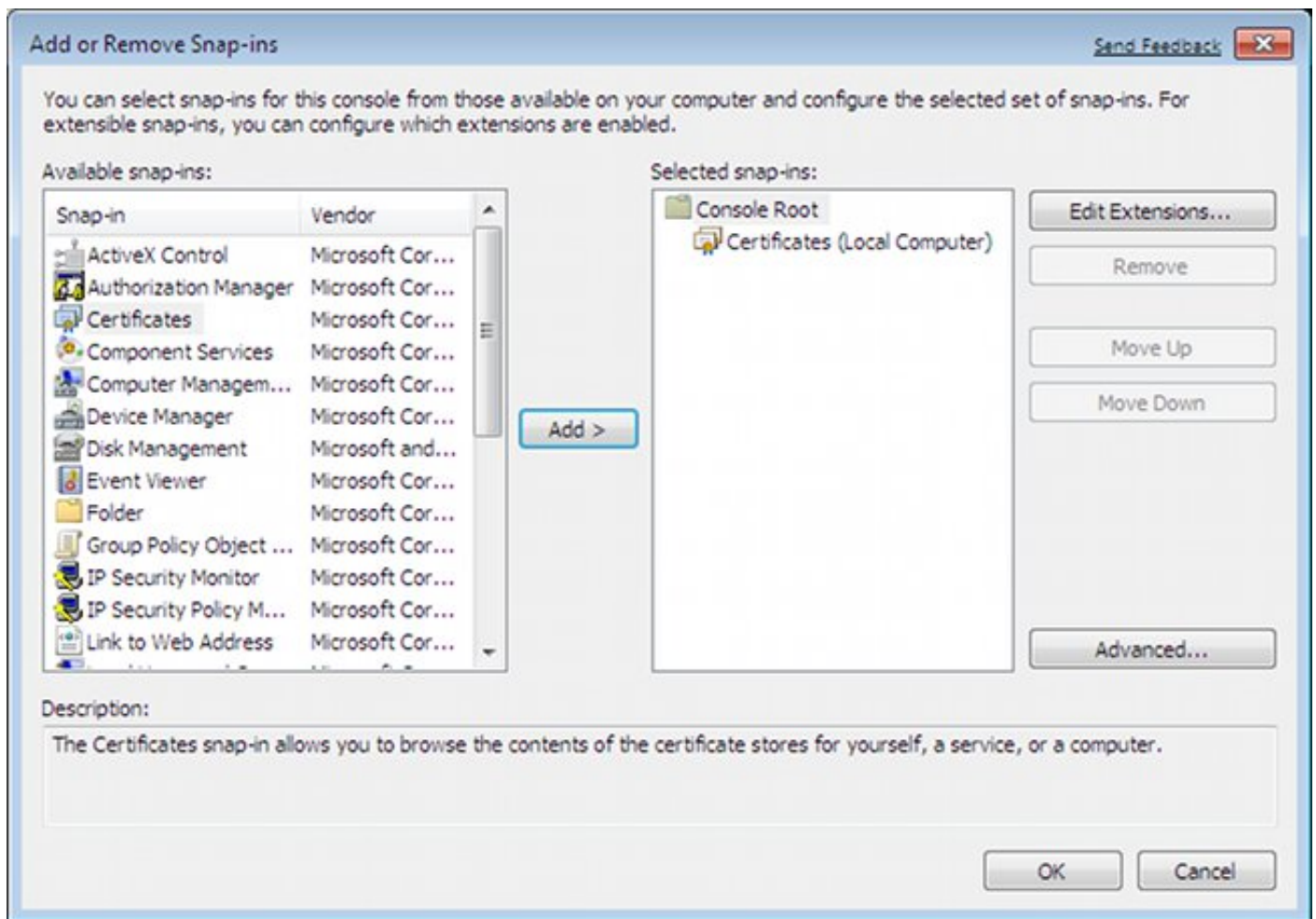
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

Windows 7

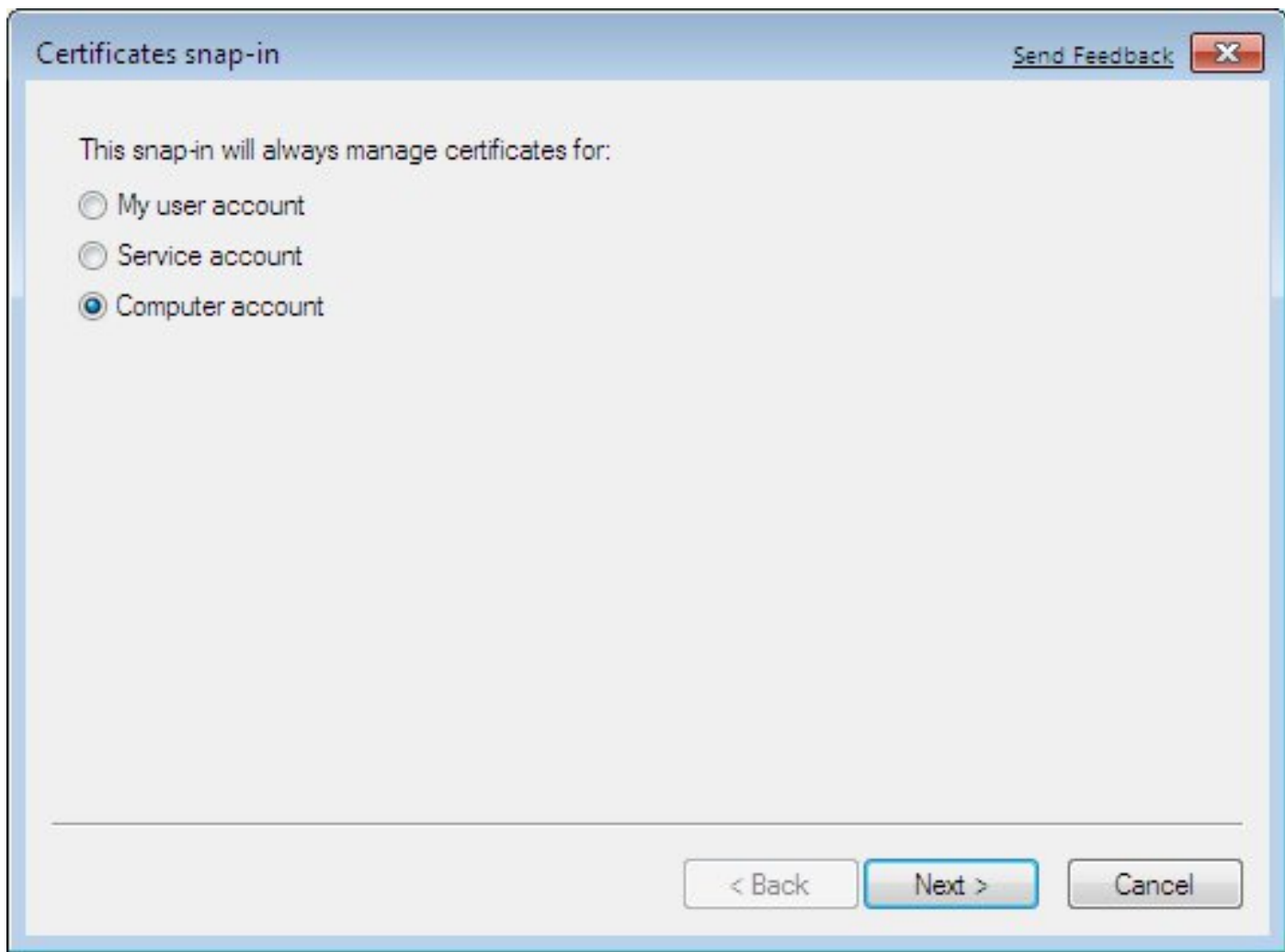
Stap 1. Installeer het CA-certificaat.

Om het certificaat te vertrouwen dat door de ASA wordt aangeboden, moet de Windows client zijn CA vertrouwen. Dat CA-certificaat moet worden toegevoegd aan de opslag van het computercertificaat (niet de gebruikerswinkel). De Windows client gebruikt de computerwinkel om het IKEv2-certificaat te valideren.

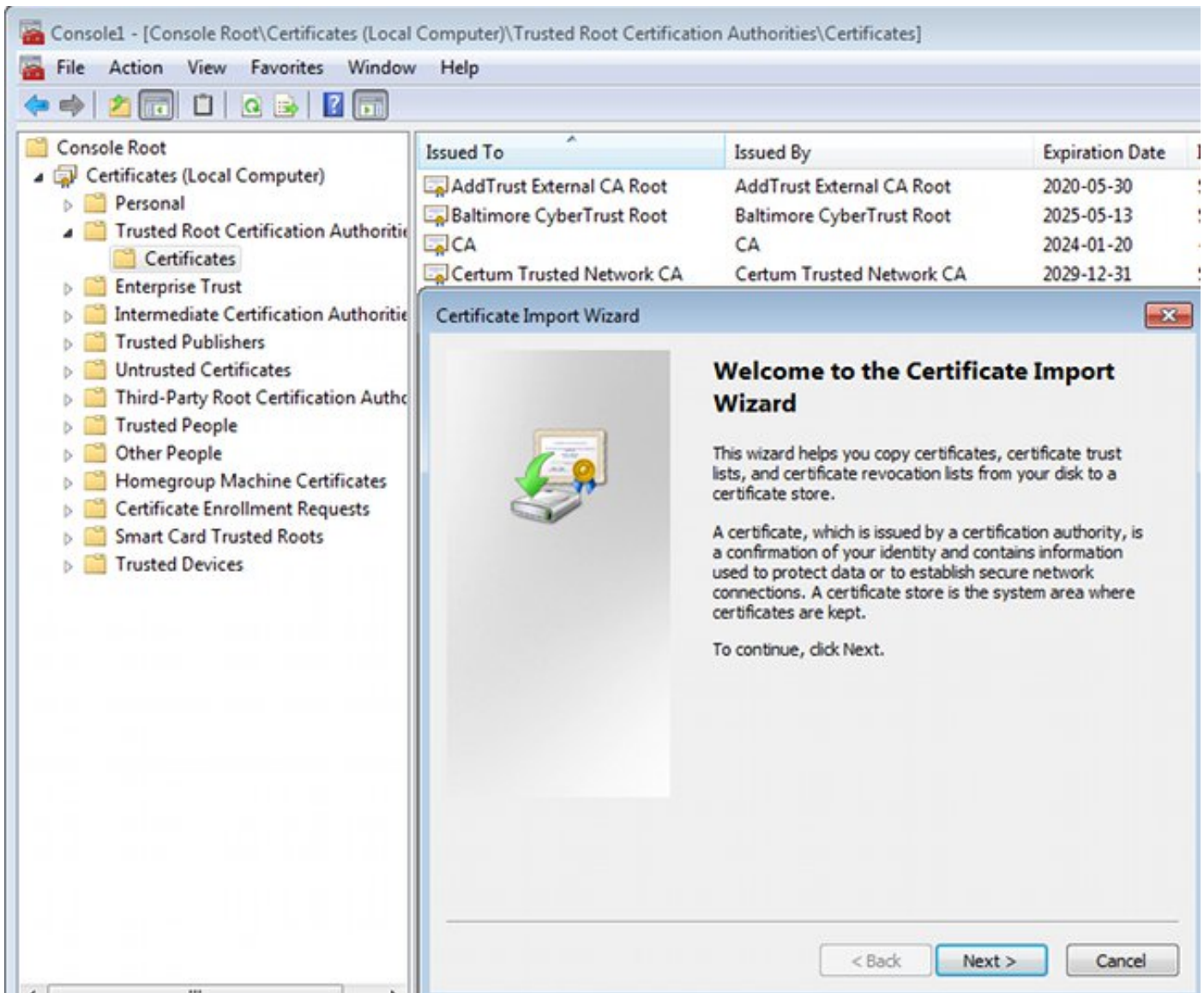
Om CA toe te voegen, kies **MMC > Magnetisch-ins toevoegen of verwijderen > Certificaten**.



Klik op het keuzerondje **Computer-account**.



Importeer de CA aan de Trusted Root certificaatautoriteiten.



Als de Windows client het door de ASA gepresenteerde certificaat niet kan valideren, meldt de klant:

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

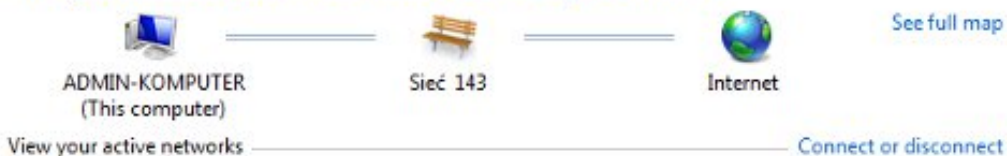
Stap 2. Configuratie van de VPN-verbinding.

Om de VPN-verbinding van het Network and Sharing Center te configureren kiest u **Connect met een werkplek** om een VPN-verbinding te maken.

Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

[See full map](#)



Sieć 143
Public network

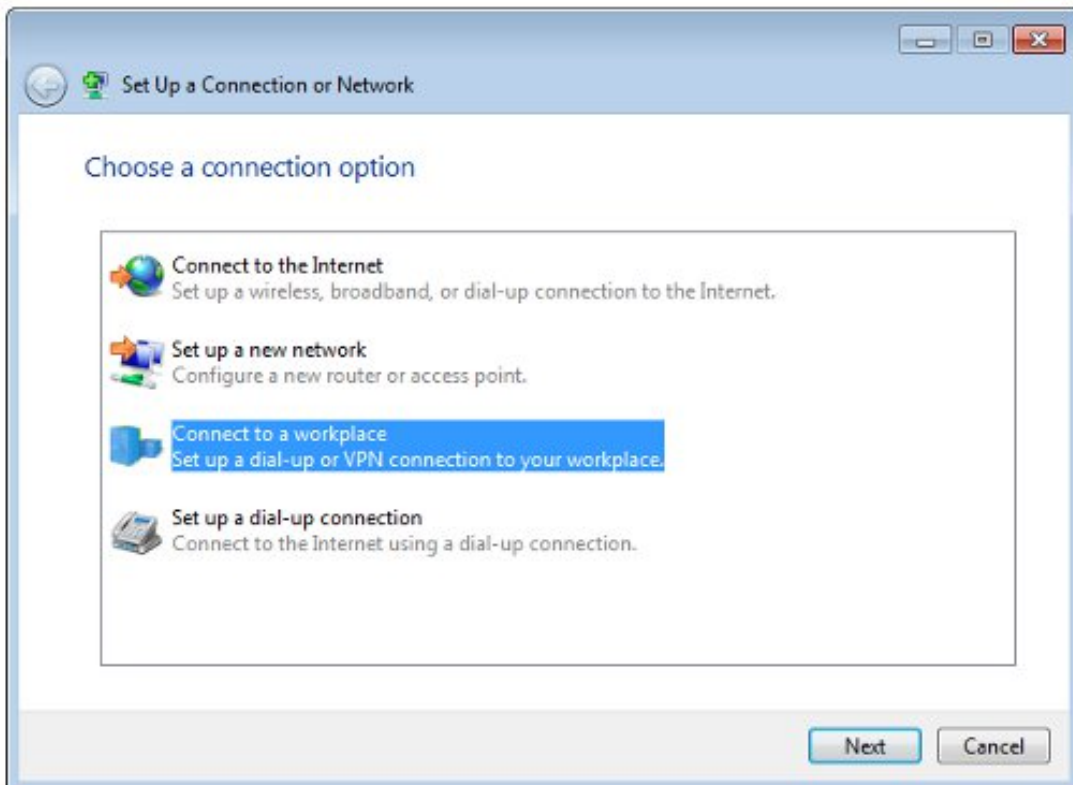
Access type: Internet
Connections: Połączenie lokalne

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.



See also

Kies **Gebruik mijn internetverbinding (VPN)**.

How do you want to connect?



Use my Internet connection (VPN)

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



Configureer het adres met een ASA FQDN. Zorg ervoor dat deze correct is opgelost door de Domain Name Server (DNS).


Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

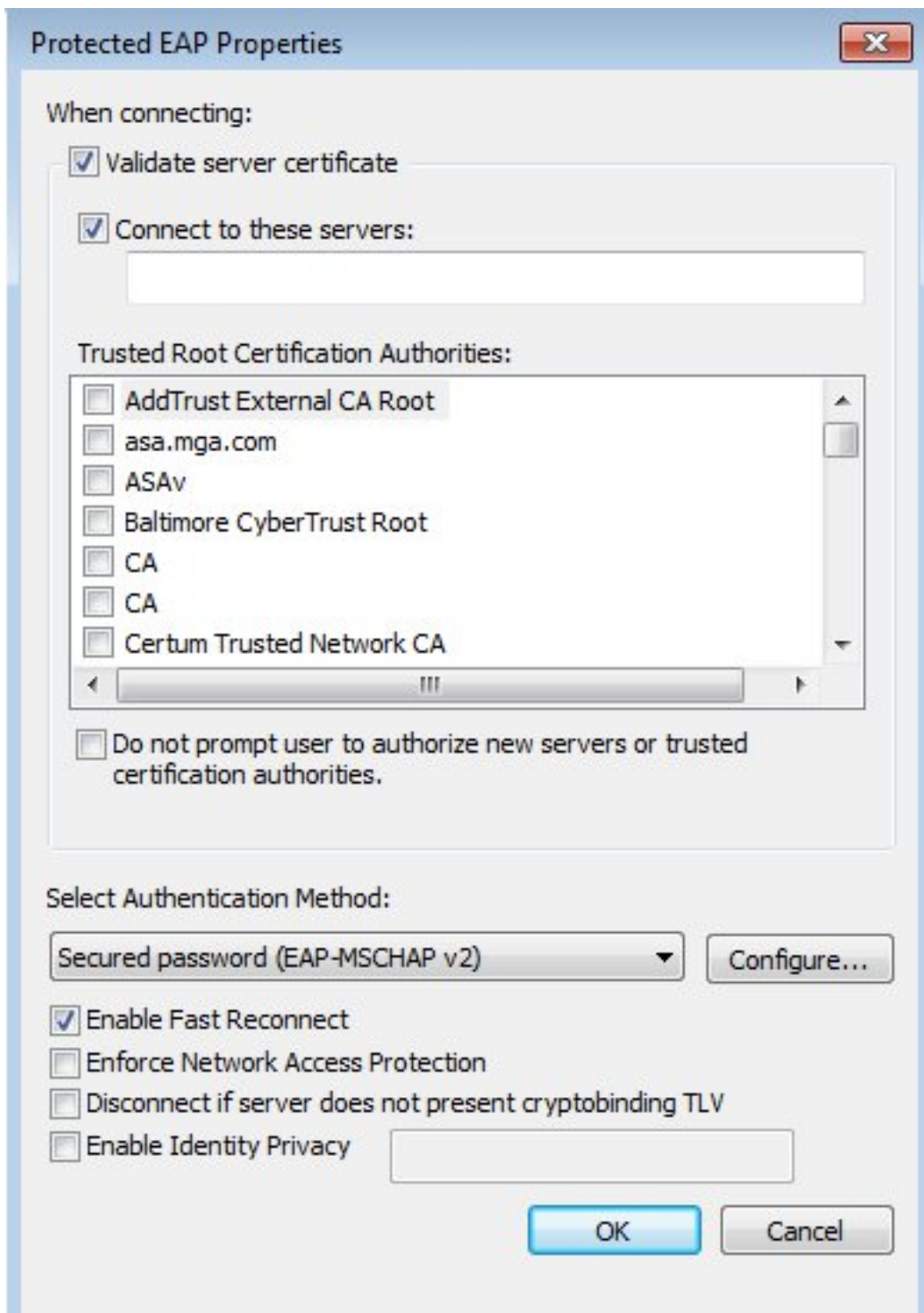
Use a smart card

 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

Indien nodig kunt u de eigenschappen (zoals certificatie) aanpassen in het venster Beveiligde MAP-eigenschappen.



Verifiëren

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

De Output Interpreter Tool (alleen voor geregistreeerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht show.

Windows-client

Voer uw referenties in wanneer u verbinding maakt.



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

Na succesvolle verificatie wordt de IKEv2-configuratie toegepast.

Connecting to ASA-IKEv2...



Registering your computer on the network...

De sessie is omhoog.

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)

De routingtabel is bijgewerkt met de standaardroute met gebruik van een nieuwe interface met de lage metriek.

```
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  
=====
```

Logs

Na succesvolle authenticatie meldt de ASA:

```
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-loggen wijzen op succesvolle authenticatie met standaard authenticatie en autorisatie regels.

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 shows: Misconfigured Suppliants: 0, Misconfigured Network Devices: 0, RADIUS Drops: 6, and Client Stopped: 0. Below this is a table of authentication sessions with columns: Time, Status, Def..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Network Device. Two sessions are listed: one at 2014-11-18 18:31:34 with status 'Success' and another at 2014-11-18 17:52:07 with status 'Success'.

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

De details geven de PEAP-methode aan.

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 in de ASA

De belangrijkste uitwerpselen zijn:

ASAv# **debug crypto ikev2 protocol 32**

<most debugs omitted for clarity....

IKE_SA_INIT pakket dat door de ASA ontvangen is (omvat IKEv2 voorstellen en de belangrijkste uitwisseling voor 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 antwoord op de initiatiefnemer (bevat IKEv2-voorstellen, belangrijke uitwisseling voor DH en certificaatverzoek):

```
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 voor client met IKE-ID, certificaataanvraag, voorgestelde transformatiesets, gevraagde configuratie en 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-respons van de ASA die een MAP-identiteitsaanvraag bevat (eerste pakket met MAP-extensies). Dat pakket bevat ook het certificaat (als er geen juist certificaat op de ASA is gevonden, is er een string):

```
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]
```

Door de ASA ontvangen EAP-respons (lengte 5, lading: 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
```


Daarna worden er meerdere pakketten uitgewisseld als onderdeel van EAP-PEAP. Tot slot wordt het succes van EAP door de ASA ontvangen en aan de aanvrager doorgestuurd:

Payload contents:

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

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

Peer-authenticatie is succesvol:

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

En de VPN sessie is correct voltooid.

Packet Level

Het EAP-identiteitsverzoek is ingesloten in "Extensible Authentication" van de IKE_AUTH die door de ASA wordt verstuurd. Gelijktijdig met het identiteitsverzoek worden IKE_ID en certificaten verzonden.

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:

Alle volgende EAP-pakketten zijn ingesloten in IKE_AUTH. Nadat de aanvrager de methode (EAP-PEAP) heeft bevestigd, begint hij een Secure Socket Layer (SSL)-tunnel te bouwen die de MSCHAPv2-sessie beschermt die voor authenticatie wordt gebruikt.

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

Nadat er meerdere pakketten zijn uitgewisseld bevestigt ISE succes.

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

De IKEv2-sessie wordt voltooid door de ASA, de laatste configuratie (configuratieantwoord met waarden zoals een toegewezen IP-adres), transformatiesets en traffic selectors worden naar de VPN-client geduwd.

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

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Cisco ASA Series 5000 Series VPN CLI-configuratiegids, 9.3](#)
- [Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)