

Konfigurieren des ASA IKEv2-Remote-Zugriffs mit EAP-PEAP und dem nativen Windows-Client

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Überlegungen zum AnyConnect Secure Mobility Client](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Zertifikate](#)

[ISE](#)

[Schritt 1: Fügen Sie die ASA den Netzwerkgeräten auf der ISE hinzu.](#)

[Schritt 2: Erstellen Sie einen Benutzernamen im lokalen Speicher.](#)

[ASA](#)

[Windows 7](#)

[Schritt 1: Installieren Sie das Zertifizierungsstellenzertifikat.](#)

[Schritt 2: Konfigurieren Sie die VPN-Verbindung.](#)

[Überprüfen](#)

[Windows-Client](#)

[Protokolle](#)

[Debugger auf der ASA](#)

[Paketebene](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel für eine Cisco Adaptive Security Appliance (ASA) Version 9.3.2 oder höher, die den Remote-VPN-Zugriff auf das Internet Key Exchange Protocol (IKEv2) mit der Standard-EAP-Authentifizierung (Extensible Authentication Protocol) ermöglicht. Auf diese Weise kann ein nativer Microsoft Windows 7-Client (und jeder andere standardbasierte IKEv2-Client) mit der ASA mit IKEv2- und EAP-Authentifizierung verbunden werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegendes VPN- und IKEv2-Wissen
- Grundlegende AAA-Kenntnisse (Authentication, Authorization, and Accounting) und RADIUS-Kenntnisse
- Erfahrung mit ASA VPN-Konfiguration
- Erfahrung mit der ISE-Konfiguration (Identity Services Engine)

Verwendete Komponenten

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

- Microsoft Windows 7
- Cisco ASA Software, Version 9.3.2 und höher
- Cisco ISE, Version 1.2 und höher

Hintergrundinformationen

Überlegungen zum AnyConnect Secure Mobility Client

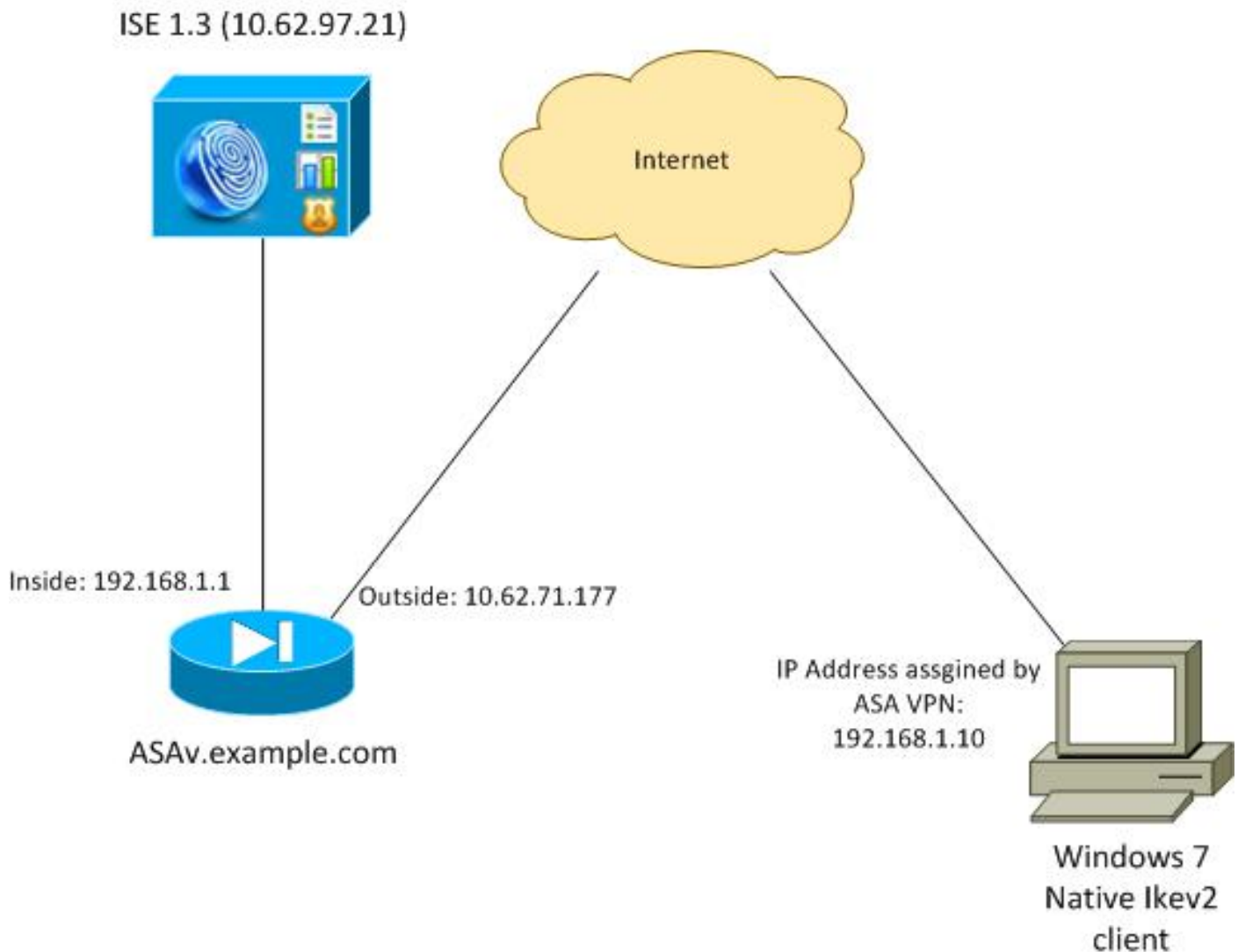
Der native Windows IKEv2-Client unterstützt keinen Split-Tunnel (es gibt keine CONF REPLY-Attribute, die vom Windows 7-Client akzeptiert werden könnten). Die einzige mögliche Richtlinie mit dem Microsoft-Client besteht in der Tunnelung des gesamten Datenverkehrs (0/0-Datenverkehrsauswahl). Wenn eine spezielle Split-Tunnel-Richtlinie erforderlich ist, sollte AnyConnect verwendet werden.

AnyConnect unterstützt keine standardisierten EAP-Methoden, die auf dem AAA-Server terminiert werden (PEAP, Transport Layer Security). Wenn EAP-Sitzungen auf dem AAA-Server beendet werden müssen, kann der Microsoft-Client verwendet werden.

Konfigurieren

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Die ASA ist für die Authentifizierung mit einem Zertifikat konfiguriert (der Client muss diesem Zertifikat vertrauen). Der Windows 7-Client ist für die Authentifizierung mit EAP (EAP-PEAP) konfiguriert.

Die ASA fungiert als VPN-Gateway, das die IKEv2-Sitzung vom Client beendet. Die ISE fungiert als AAA-Server, der die EAP-Sitzung vom Client beendet. EAP-Pakete werden für den Datenverkehr zwischen dem Client und der ASA (IKEv2) in IKE_AUTH-Pakete gekapselt und dann in RADIUS-Paketen für den Authentifizierungsdatenverkehr zwischen der ASA und der ISE.

Zertifikate

Microsoft Certificate Authority (CA) wurde zur Generierung des Zertifikats für die ASA verwendet. Die Zertifikatanforderungen, die vom systemeigenen Windows 7-Client akzeptiert werden müssen, sind:

- Die EKU-Erweiterung (Extended Key Usage) sollte die Serverauthentifizierung beinhalten (in diesem Beispiel wurde die Vorlage "Webserver" verwendet).
- Der Betreffname sollte den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) enthalten, der vom Client für die Verbindung verwendet wird (in diesem Beispiel ASAv.example.com).

Weitere Informationen zum Microsoft-Client finden Sie unter [Problembehandlung bei IKEv2-VPN-Verbindungen](#).

Hinweis: Android 4.x ist restriktiver und erfordert den richtigen Subject Alternative Name gemäß RFC 6125. Weitere Informationen zu Android finden Sie unter [IKEv2 von Android strongSwan zu Cisco IOS mit EAP und RSA-Authentifizierung](#).

Zur Generierung einer Zertifikatssignierungsanfrage auf der ASA wurde diese Konfiguration verwendet:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Schritt 1: Fügen Sie die ASA den Netzwerkgeräten auf der ISE hinzu.

Wählen Sie **Administration > Network Devices (Verwaltung > Netzwerkgeräte)**. Legen Sie ein vorinstalliertes Kennwort fest, das von der ASA verwendet wird.

Schritt 2: Erstellen Sie einen Benutzernamen im lokalen Speicher.

Wählen Sie **Administration > Identities > Users aus**. Erstellen Sie nach Bedarf den Benutzernamen.

Alle anderen Einstellungen sind standardmäßig für die ISE aktiviert, um Endpunkte mit EAP-PEAP (Protected Extensible Authentication Protocol) zu authentifizieren.

ASA

Die Konfiguration für den Remote-Zugriff ist für IKEv1 und IKEv2 ähnlich.

```
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
```

Da Windows 7 eine IKE-ID-Typadresse im IKE_AUTH-Paket sendet, sollte die **DefaultRAGroup** verwendet werden, um sicherzustellen, dass die Verbindung in der richtigen Tunnelgruppe landet. Die ASA authentifiziert sich mit einem Zertifikat (lokale Authentifizierung) und erwartet, dass der Client EAP (Remote-Authentifizierung) verwendet. Darüber hinaus muss die ASA eine spezielle EAP-Identitätsanfrage senden, damit der Client mit EAP-Identitätsantwort (Abfrage-Identität) antworten kann.

```
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
```

Schließlich muss IKEv2 aktiviert und das richtige Zertifikat verwendet werden.

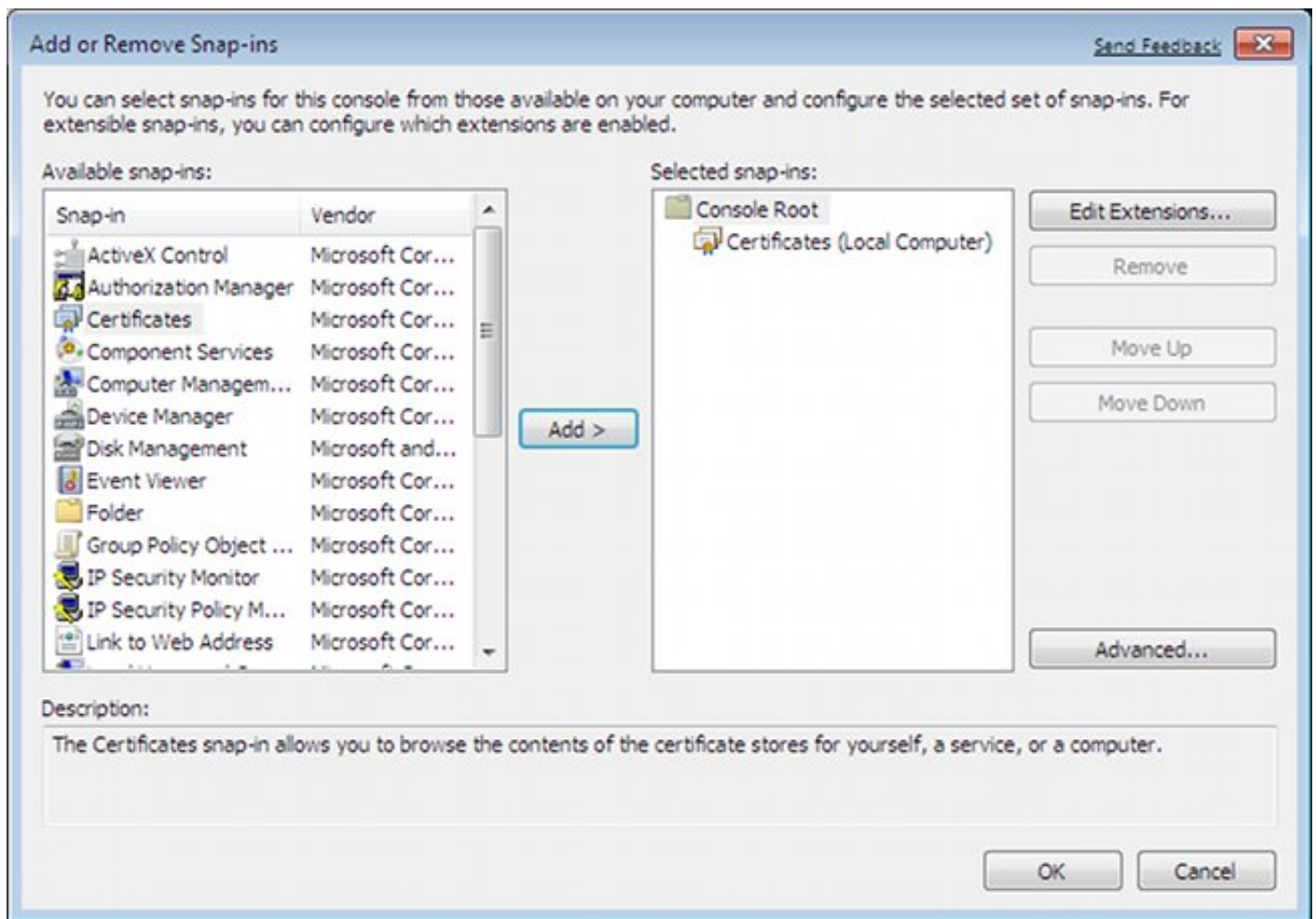
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

Windows 7

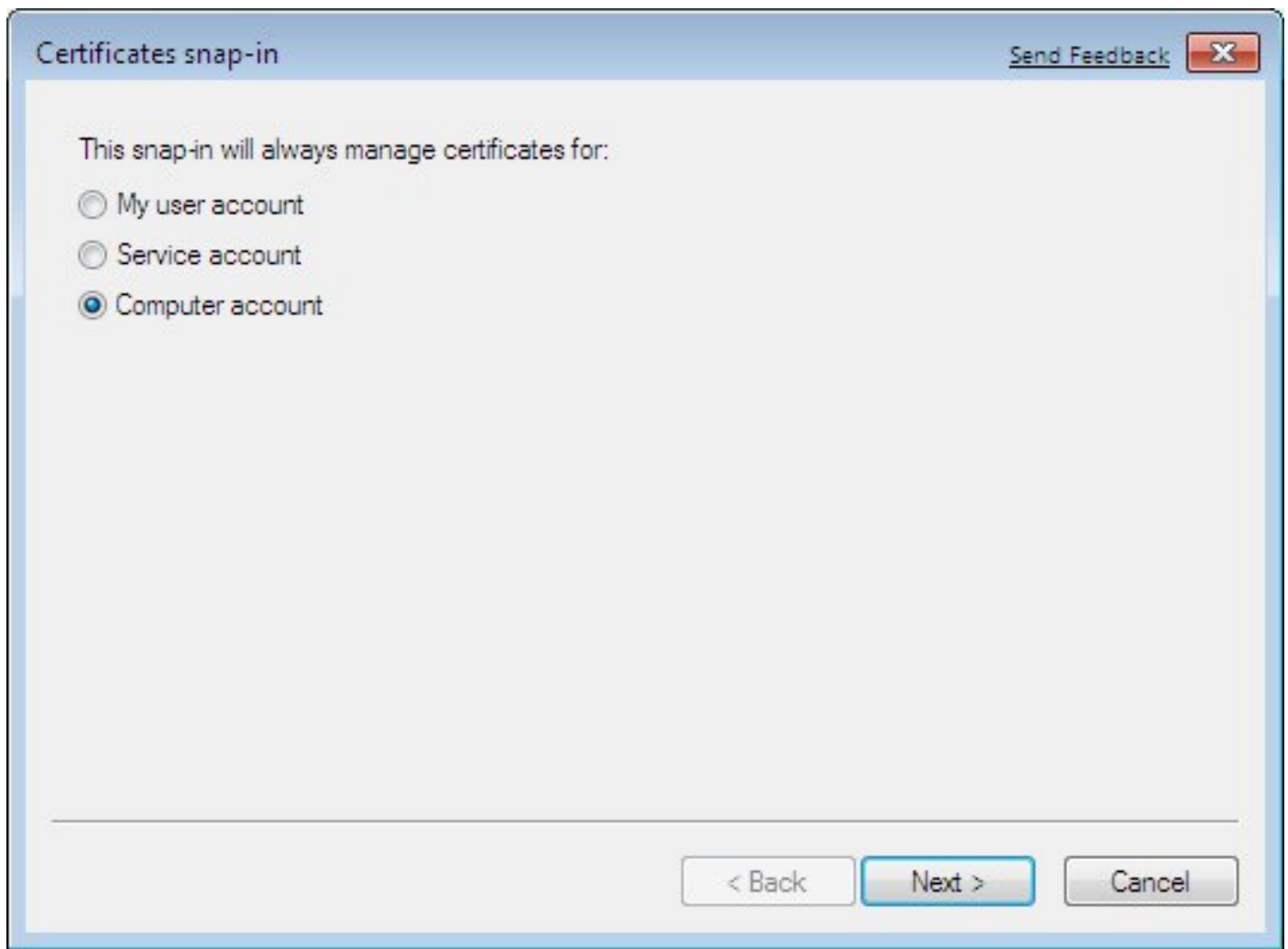
Schritt 1: Installieren Sie das Zertifizierungsstellenzertifikat.

Damit das von der ASA präsentierte Zertifikat vertrauenswürdig ist, muss der Windows-Client seiner CA vertrauen. Dieses Zertifizierungsstellenzertifikat sollte dem Computerzertifikatspeicher (nicht dem Benutzerspeicher) hinzugefügt werden. Der Windows-Client verwendet den Computerspeicher, um das IKEv2-Zertifikat zu validieren.

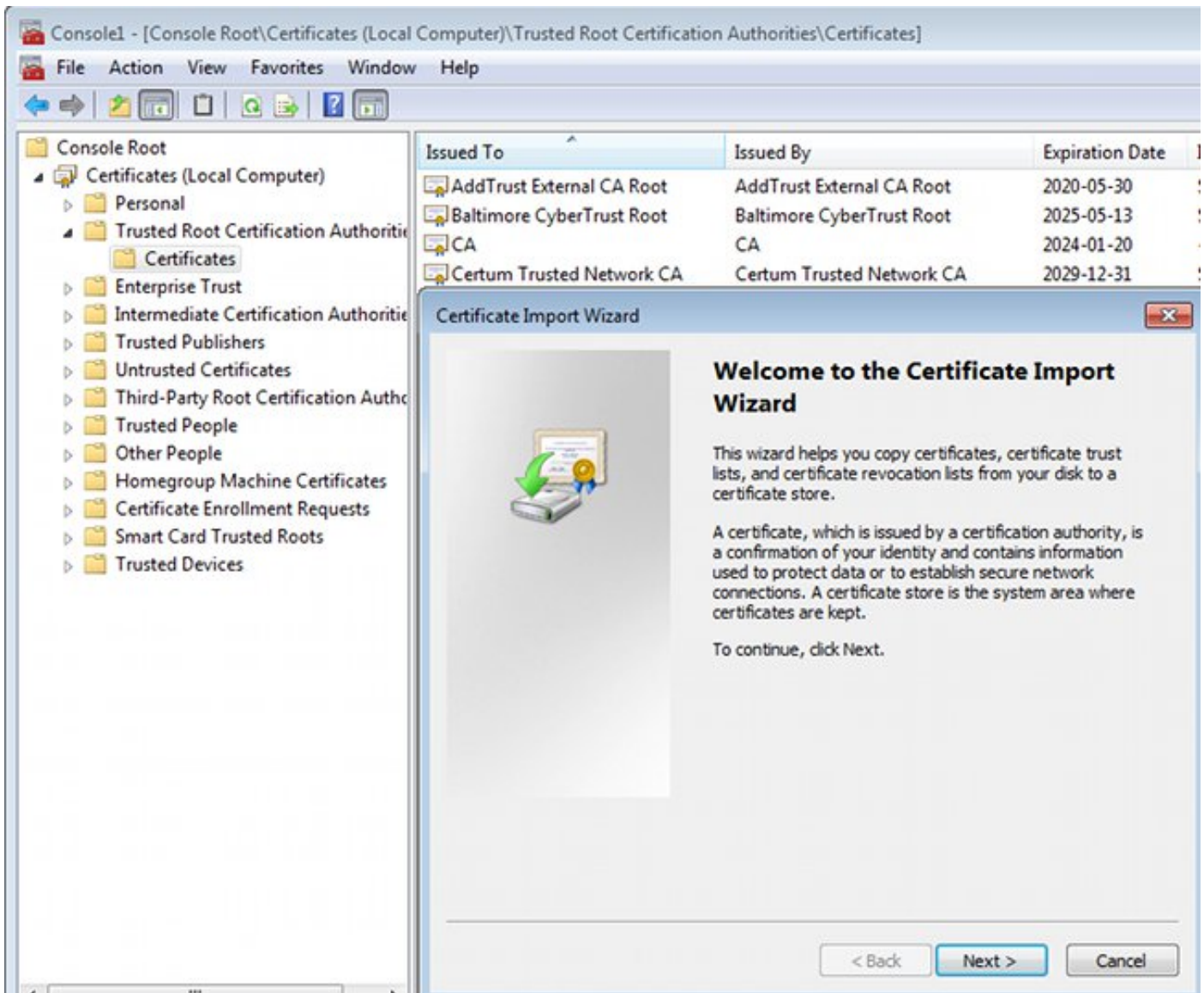
Um die CA hinzuzufügen, wählen Sie **MMC > Snap-Ins hinzufügen oder entfernen > Zertifikate aus**.



Klicken Sie auf das Optionsfeld **Computerkonto**.



Importieren Sie die CA in die vertrauenswürdigen Stammzertifizierungsstellen.



Wenn der Windows-Client das von der ASA präsentierte Zertifikat nicht validieren kann, meldet er Folgendes:

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

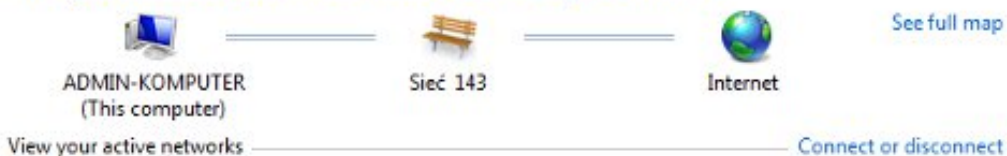
Schritt 2: Konfigurieren Sie die VPN-Verbindung.

Um die VPN-Verbindung vom Netzwerk- und Freigabecenter aus zu konfigurieren, wählen Sie **Verbindung mit einem Arbeitsplatz** konfigurieren, um eine VPN-Verbindung zu erstellen.

Control Panel Home
Change adapter settings
Change advanced sharing settings

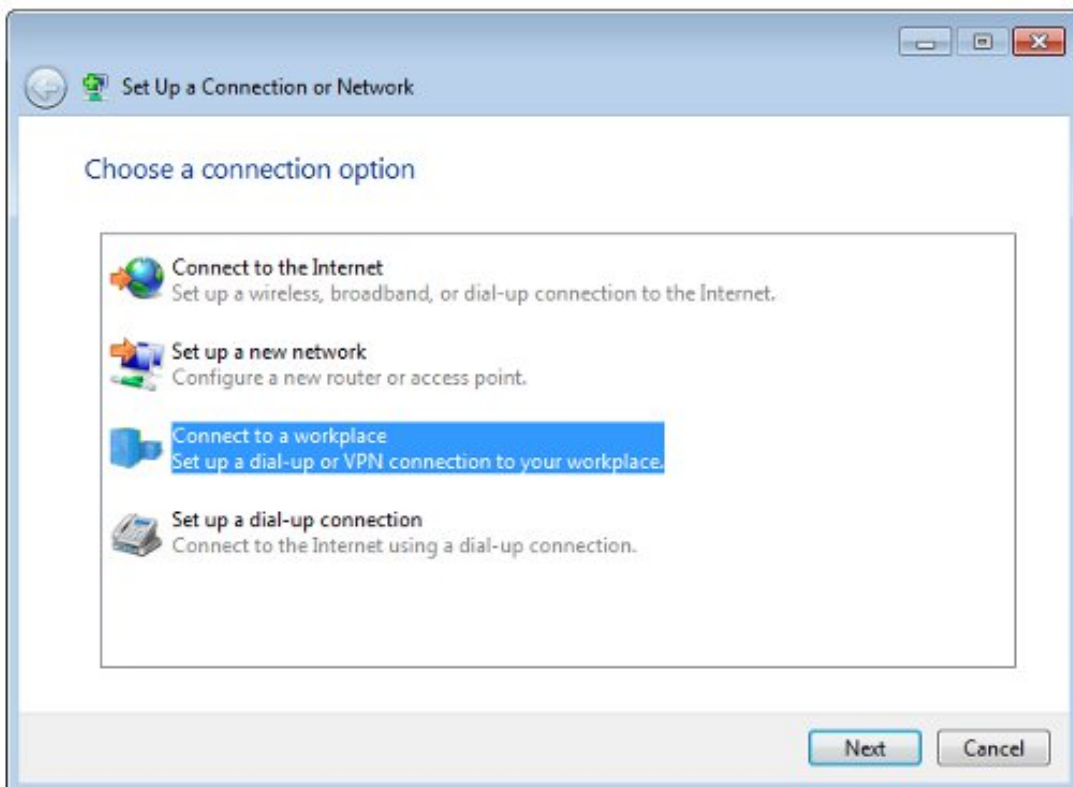
View your basic network information and set up connections

[See full map](#)



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

Wählen Sie **Meine Internetverbindung (VPN) verwenden** aus.

How do you want to connect?

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



Konfigurieren Sie die Adresse mit einem ASA FQDN. Stellen Sie sicher, dass der Domänenname Server (DNS) eine korrekte Auflösung aufweist.


Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

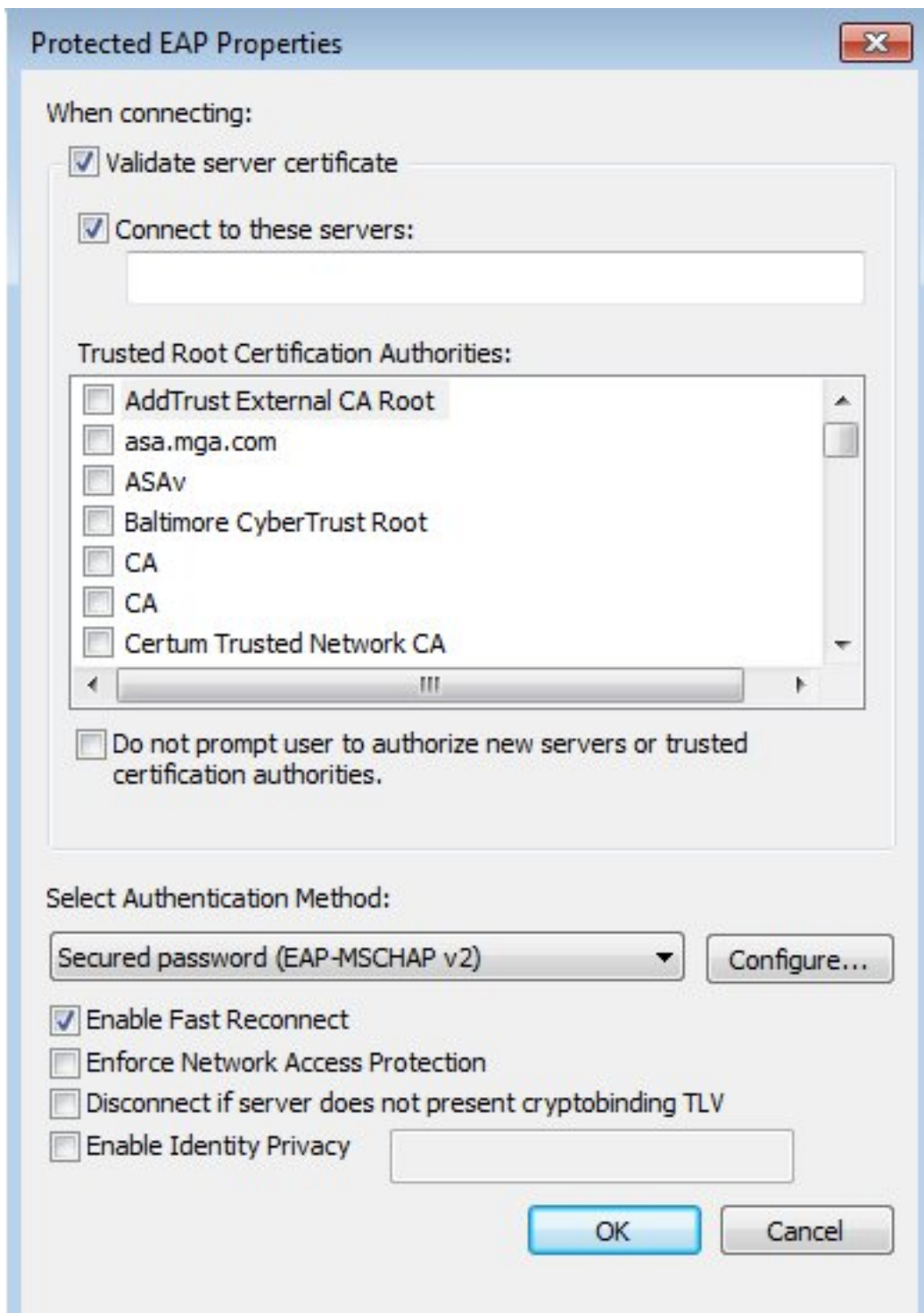
Use a smart card

 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

Passen Sie ggf. Eigenschaften (z. B. Zertifikatsvalidierung) im Fenster Protected EAP Properties (Protected EAP-Eigenschaften) an.



Überprüfen

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

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

Windows-Client

Wenn Sie eine Verbindung herstellen, geben Sie Ihre Anmeldeinformationen ein.



Cisco AnyConnect Secure Mobility
Client Connection
Disabled



IKEv2 connection to ASA
Disconnected
WAN Miniport (IKEv2)

Connect IKEv2 connection to ASA



User name:

Password:

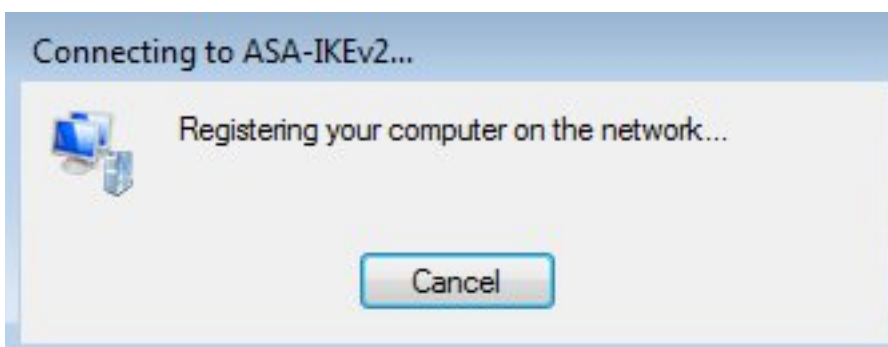
Domain:

Save this user name and password for the following users:

Me only

Anyone who uses this computer

Nach erfolgreicher Authentifizierung wird die IKEv2-Konfiguration angewendet.



Die Sitzung ist beendet.

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)

Die Routing-Tabelle wurde mithilfe einer neuen Schnittstelle mit der niedrigen Metrik mit der Standardroute aktualisiert.

```
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
=====
```

Protokolle

Nach erfolgreicher Authentifizierung meldet die ASA Folgendes:

```
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-Protokolle zeigen eine erfolgreiche Authentifizierung mit Standardauthentifizierungs- und Autorisierungsregeln an.

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 the navigation, there are several status indicators: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (6), and Client Stopped (0). The main area displays a table of live sessions. The table has columns for Time, Status, Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Network Device. The first row shows a session at 2014-11-18 18:31:34 with status 'All' and identity 'cisco'. The second row shows a session at 2014-11-18 17:52:07 with status 'All' and identity 'cisco', with authorization policy 'Default >> Basic_Authenticated_Access' and network device 'ASAv'.

Time	Status	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...	All	cisco	10.147.24.166	Default >> Basic_Authenticated_Access	PermitAccess	ASAv

Die Details geben die PEAP-Methode an.

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

Debugger auf der ASA

Zu den wichtigsten DebuggingInnen gehören:

ASAv# **debug crypto ikev2 protocol 32**

<most debugs omitted for clarity....

Von der ASA empfangenes IKE_SA_INIT-Paket (beinhaltet IKEv2-Vorschläge und Schlüsselaustausch für 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-Antwort auf den Initiator (umfasst IKEv2-Vorschläge, Schlüsselaustausch für DH und Zertifikatsanforderung):

```
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 für Client mit IKE-ID, Zertifikatsanforderung, vorgeschlagenen Transformationssätzen, angeforderter Konfiguration und Datenverkehrsauswahlen:

```
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-Antwort der ASA, die eine EAP-Identitätsanforderung enthält (erstes Paket mit EAP-Erweiterungen). Dieses Paket enthält auch das Zertifikat (wenn auf der ASA kein richtiges Zertifikat vorhanden ist, tritt ein Fehler auf):

```
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]
```

Von der ASA erhaltene EAP-Antwort (Länge 5, Nutzlast: 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
```


Anschließend werden mehrere Pakete als Teil von EAP-PEAP ausgetauscht. Schließlich wird der EAP-Erfolg von der ASA empfangen und an die Komponente weitergeleitet:

Payload contents:

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

Peer-Authentifizierung erfolgreich:

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

Die VPN-Sitzung ist korrekt beendet.

Paketebene

Die EAP-Identitätsanforderung wird in "Extensible Authentication" der von der ASA gesendeten IKE_AUTH-Nachricht eingekapselt. Neben der Identitätsanforderung werden IKE_ID und Zertifikate gesendet.

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 nachfolgenden EAP-Pakete werden in IKE_AUTH eingekapselt. Nachdem der Supplicant die Methode (EAP-PEAP) bestätigt hat, beginnt er mit dem Aufbau eines SSL-Tunnels (Secure Sockets Layer), der die für die Authentifizierung verwendete MSCHAPv2-Sitzung schützt.

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

Nach dem Austausch mehrerer Pakete bestätigt die ISE den Erfolg.

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
  
```

Die IKEv2-Sitzung wird von der ASA abgeschlossen, die endgültige Konfiguration (Konfigurationsantwort mit Werten wie einer zugewiesenen IP-Adresse), Transformationssätze und Datenverkehrsauswahlen werden an den VPN-Client übertragen.

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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Konfigurationsleitfaden für die CLI der Cisco ASA-Serie 9.3](#)
- [Cisco Identity Services Engine-Benutzerhandbuch, Version 1.2](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)