配置与EAP-PEAP和本地窗口客户端的ASA IKEv2远程访问

目录

简介

本文为允许远程VPN访问使用互联网密钥交换协议的Cisco可适应安全工具(ASA)版本9.3.2和以上提供配置示例(IKEv2)以标准的可扩展的认证协议(EAP)验证。这允许一个本地Microsoft Windows 7客户端(和其他基于标准的IKEv2)连接到与IKEv2和EAP验证的ASA。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本VPN和IKEv2知识
- 基本认证、授权和核算(AAA)和RADIUS知识
- 体验与ASA VPN配置
- 与身份服务引擎(ISE)配置的体验

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco ASA软件，版本9.3.2和以上
- 思科ISE，版本1.2及以后

背景信息

AnyConnect安全移动性客户端考虑事项

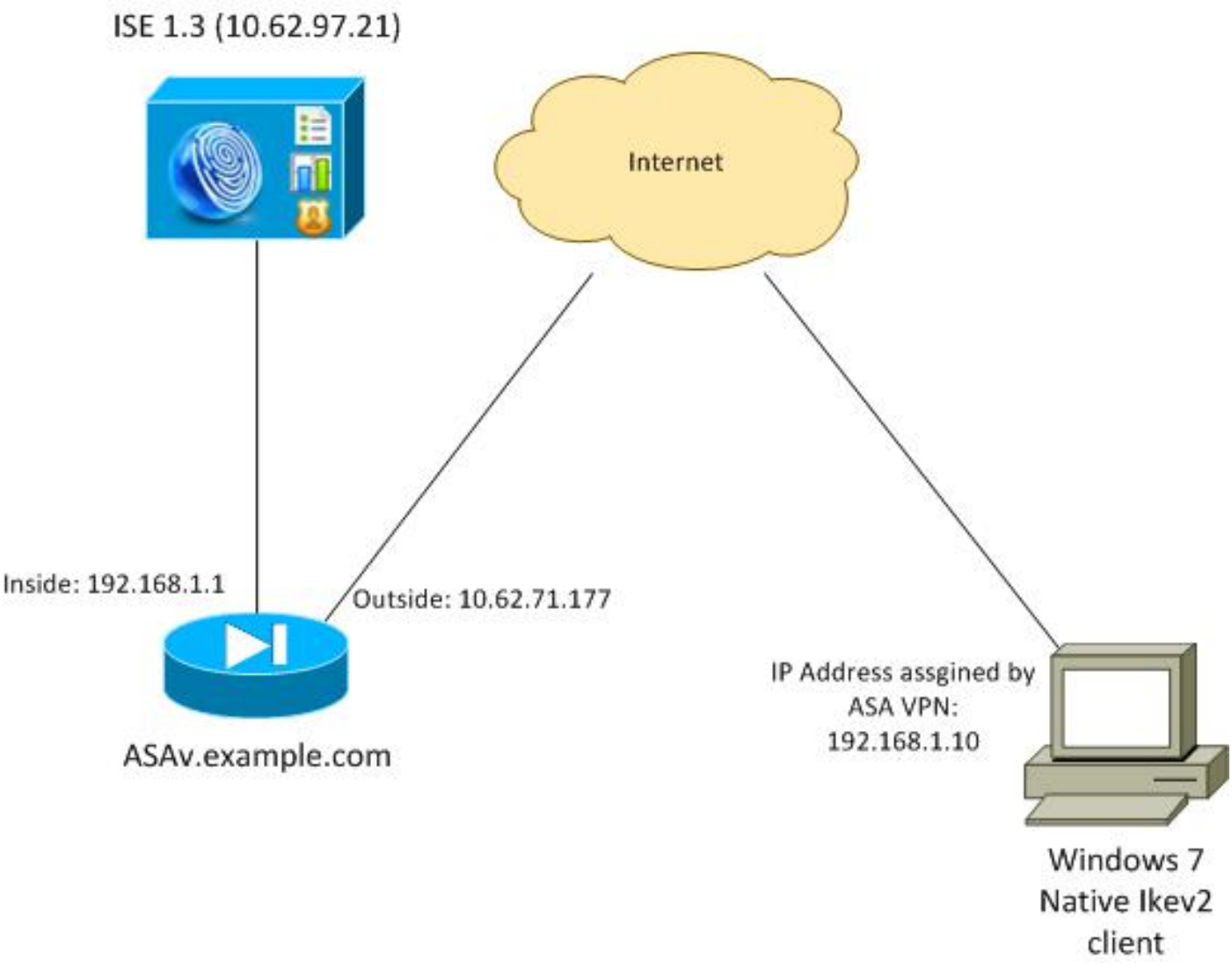
本地窗口IKEv2客户端不支持分割隧道(没有可能由Windows 7客户端接受)的CONF回复属性，因此与Microsoft客户端的唯一的可能的策略是以隧道传输所有流量(0/0流量选择器)。如果有需要对于一项特定分割隧道策略，应该使用AnyConnect。

AnyConnect不支持在AAA服务器的标准化的EAP方法(PEAP终止，传输层安全)。如果有需要终止AAA服务器的EAP会话那么可以使用Microsoft客户端。

配置

> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



ASA配置验证与证书(客户端需要委托该证书)。Windows 7客户端配置验证与EAP (EAP-PEAP)。

ASA作为终止IKEv2从客户端的VPN网关会话。ISE作为终止从客户端的AAA服务器EAP会话。EAP数据包被封装在流量的IKE_AUTH数据包客户端和ASA (IKEv2)之间然后在验证流量的RADIUS信息包ASA和ISE之间。

证书

微软认证授权(CA)用于为了生成ASA的证书。证书需求为了将由Windows 7本地客户端接受是：

- 延长的密钥用法(EKU)分机应该包括服务器验证(模板“Web服务器”用于该示例)。
- subject-name应该包括将由客户端用于为了连接的完全合格的域名(FQDN) (在本例中ASAv.example.com)。

欲了解更详细的信息在Microsoft客户端，请参阅排除故障IKEv2 VPN连接。

> **注意**：机器人4.x更加限制式并且根据RFC 6125要求正确附属的替代方案名称。欲知机器人的更多信息，请参阅从机器人strongSwan的IKEv2到与EAP和RSA验证的Cisco IOS。

为了生成在ASA的一证书签名请求，使用了此配置：

```
hostname ASAv
```

```
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

步骤1.添加ASA到在ISE的网络设备。

选择**Administration >网络设备**。设置将由ASA使用的一个预共享密码。

步骤2.在本地存储创建用户名。

选择**Administration >标识> Users**。创建用户名如所需求。

默认情况下其他设置启用为了ISE能验证与EAP-PEAP (已保护可扩展的认证协议)的终端。

ASA

远程访问的配置为IKEv1和IKEv2是类似的。

```
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
```

因为Windows 7发送在IKE_AUTH数据包的一个IKE-ID类型地址，应该用于**DefaultRAGroup**为了确保，连接在正确隧道群登陆。 ASA验证与证书(本地认证)并且盼望客户端使用EAP (远程验证)。并且， ASA需要特定发送一个EAP标识要求客户端回应EAP标识答复(查询标识)。

```
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
```

最后， IKEv2需要启用，并且正确证书使用。

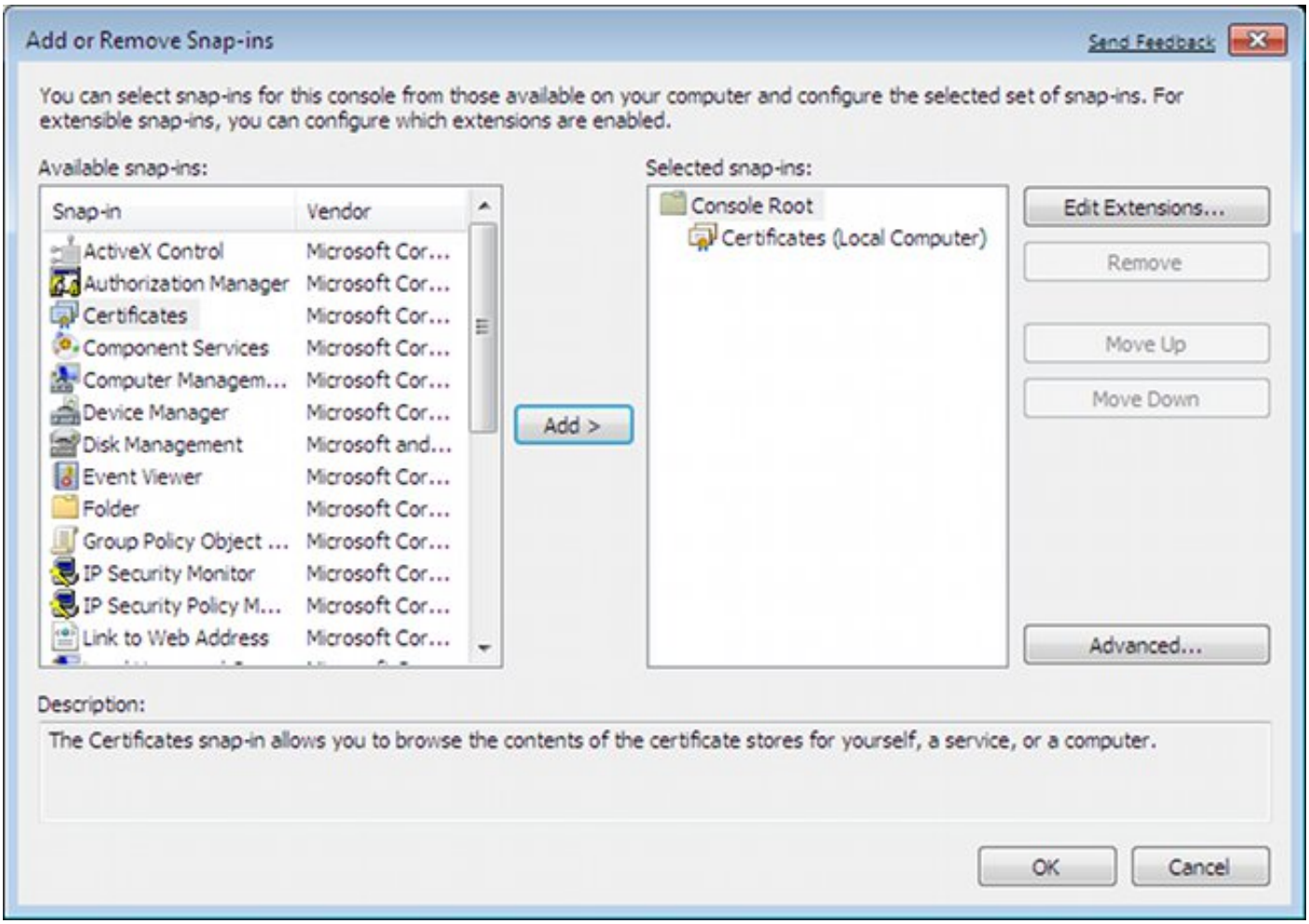
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Windows 7

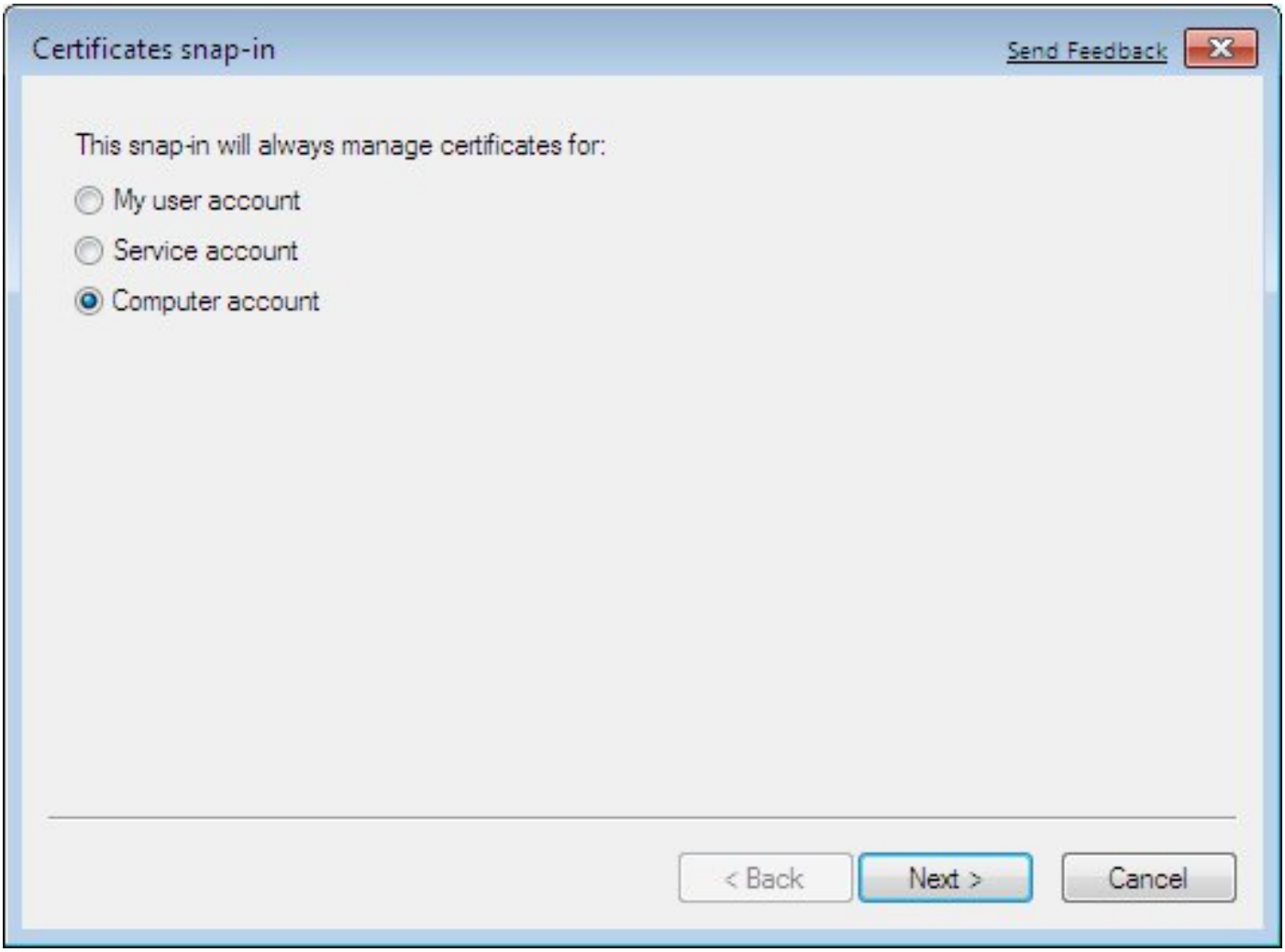
步骤1.安装CA证书。

为了委托ASA提交的证书， Windows客户端需要委托其CA。应该添加该CA证书到计算机证书存储(不是用户存储)。Windows客户端使用计算机存储设备为了验证IKEv2证书。

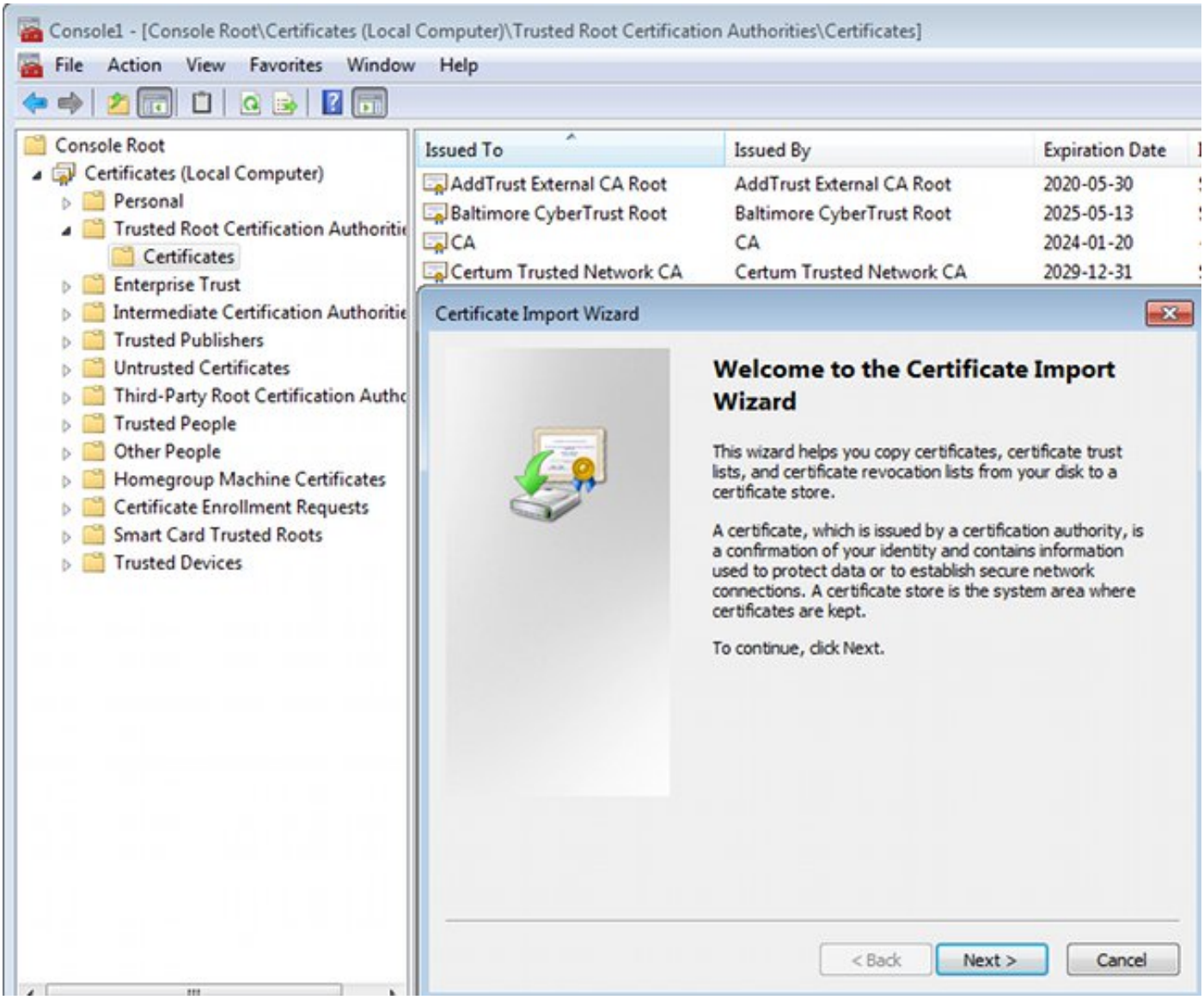
为了添加CA，请选择**MMC >Add或删除Snap-ins >证书**。



点击**计算机帐户**单选按钮。



导入CA给可信的根证书权限。

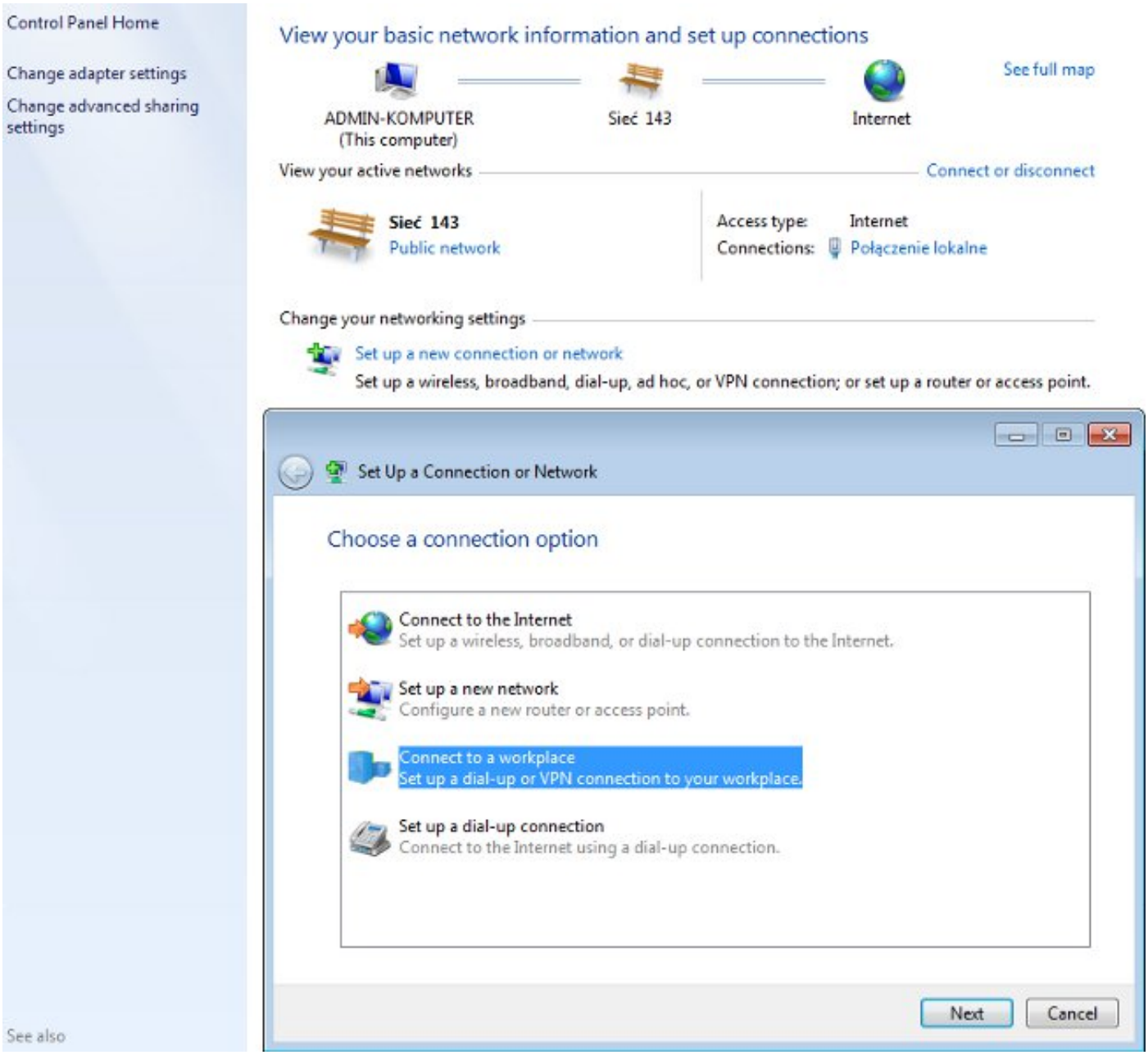


如果Windows客户端不能验证ASA提交的证书，报告：

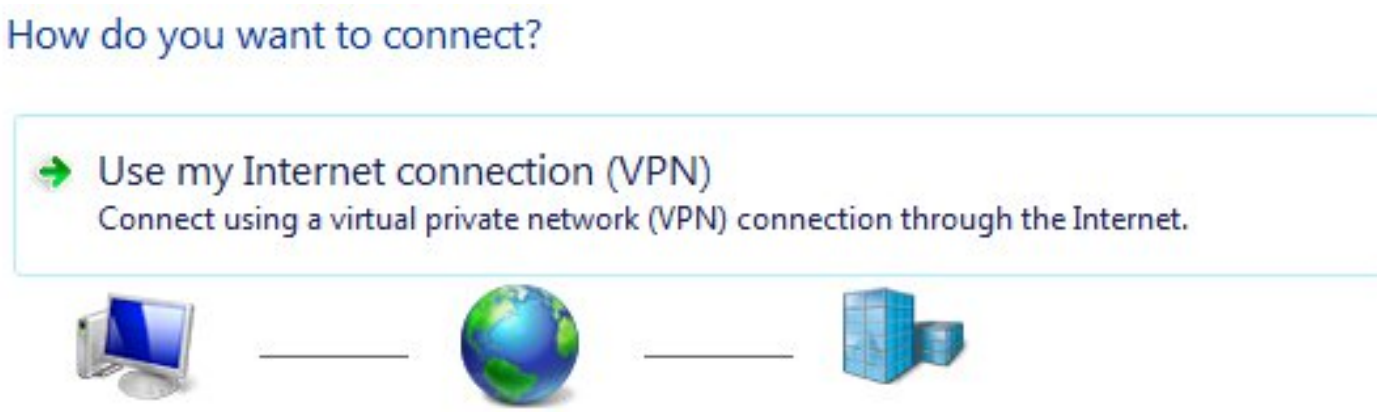
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

步骤2.配置VPN连接。

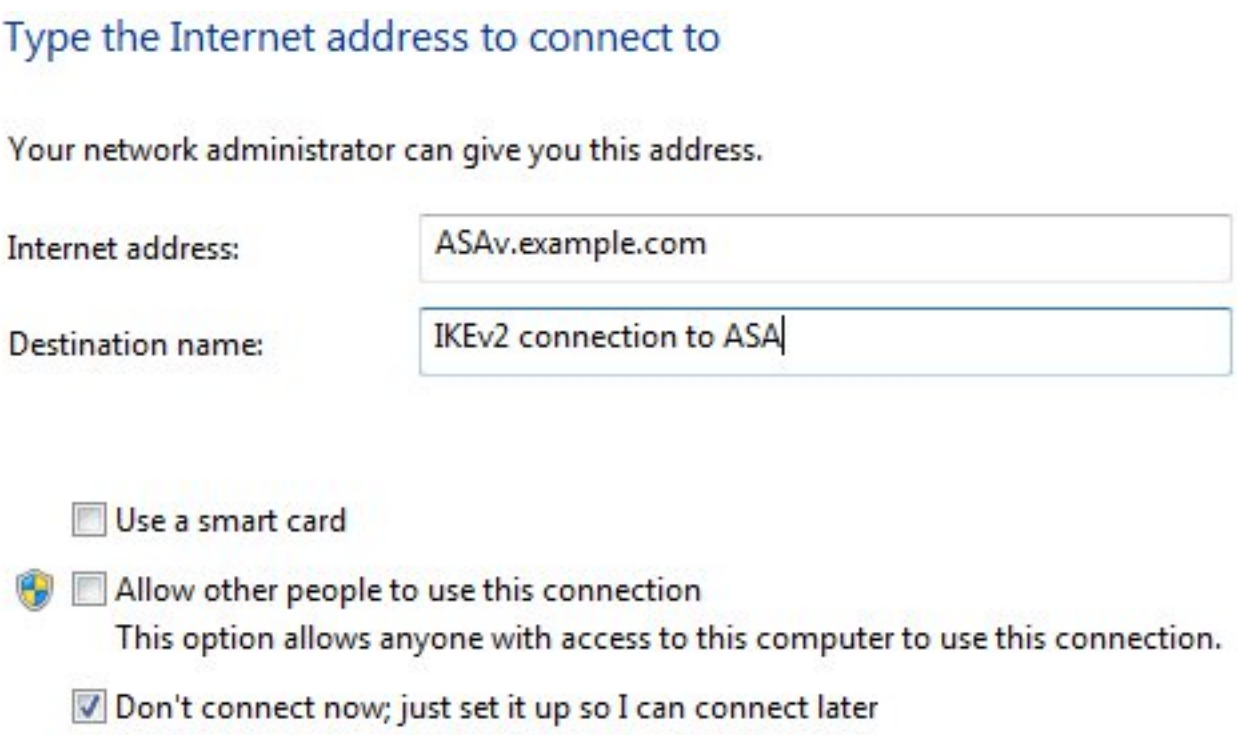
为了配置从网络和共享中心的VPN连接，请选择**连接到工作场所**为了创建VPN连接。



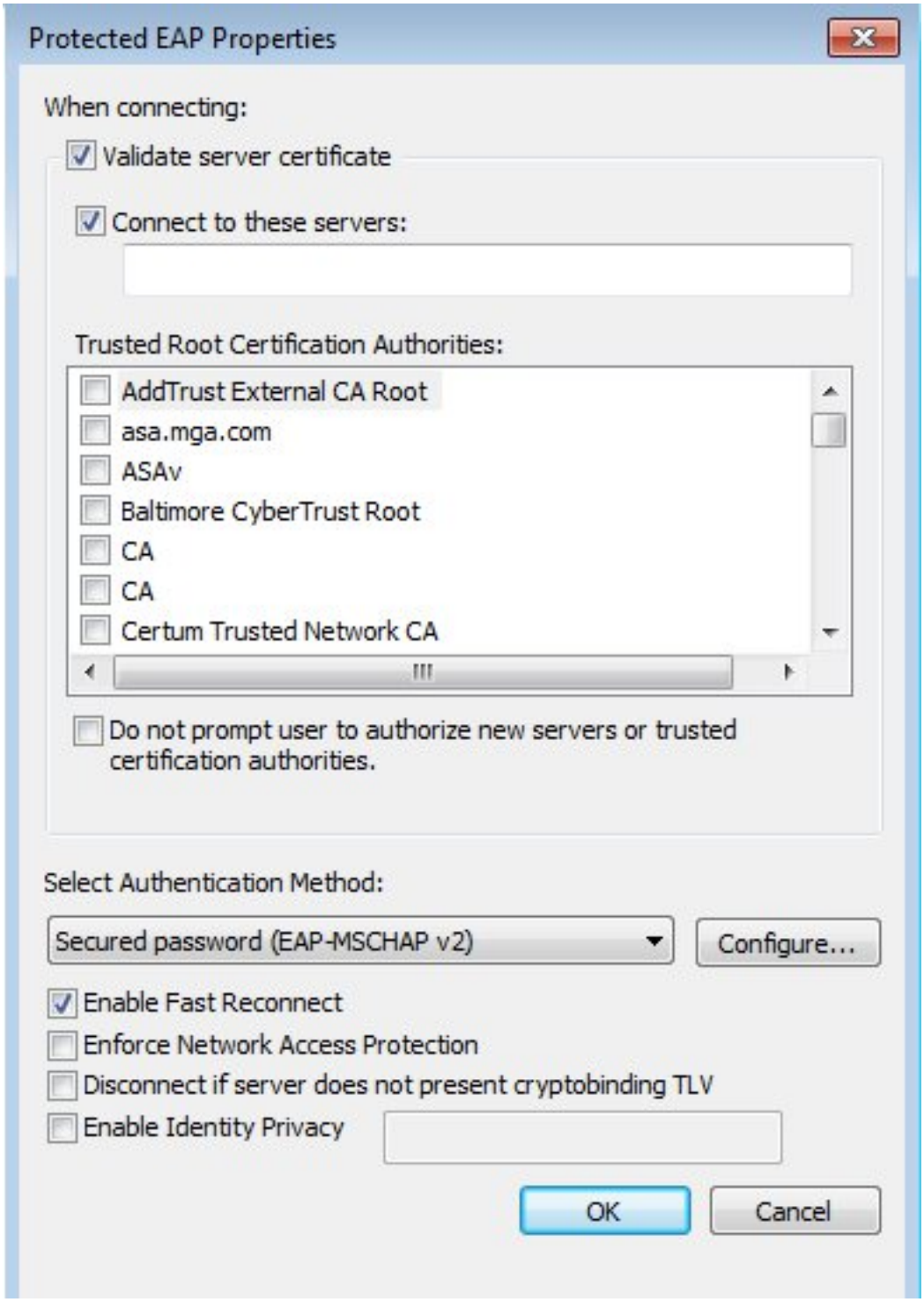
选择**使用我的互联网连接(VPN)**。



配置与ASA FQDN的地址。确保它正确地解决域名服务器(DNS)。



如果必须，请调节属性(例如证书确认)在已保护EAP属性窗口。



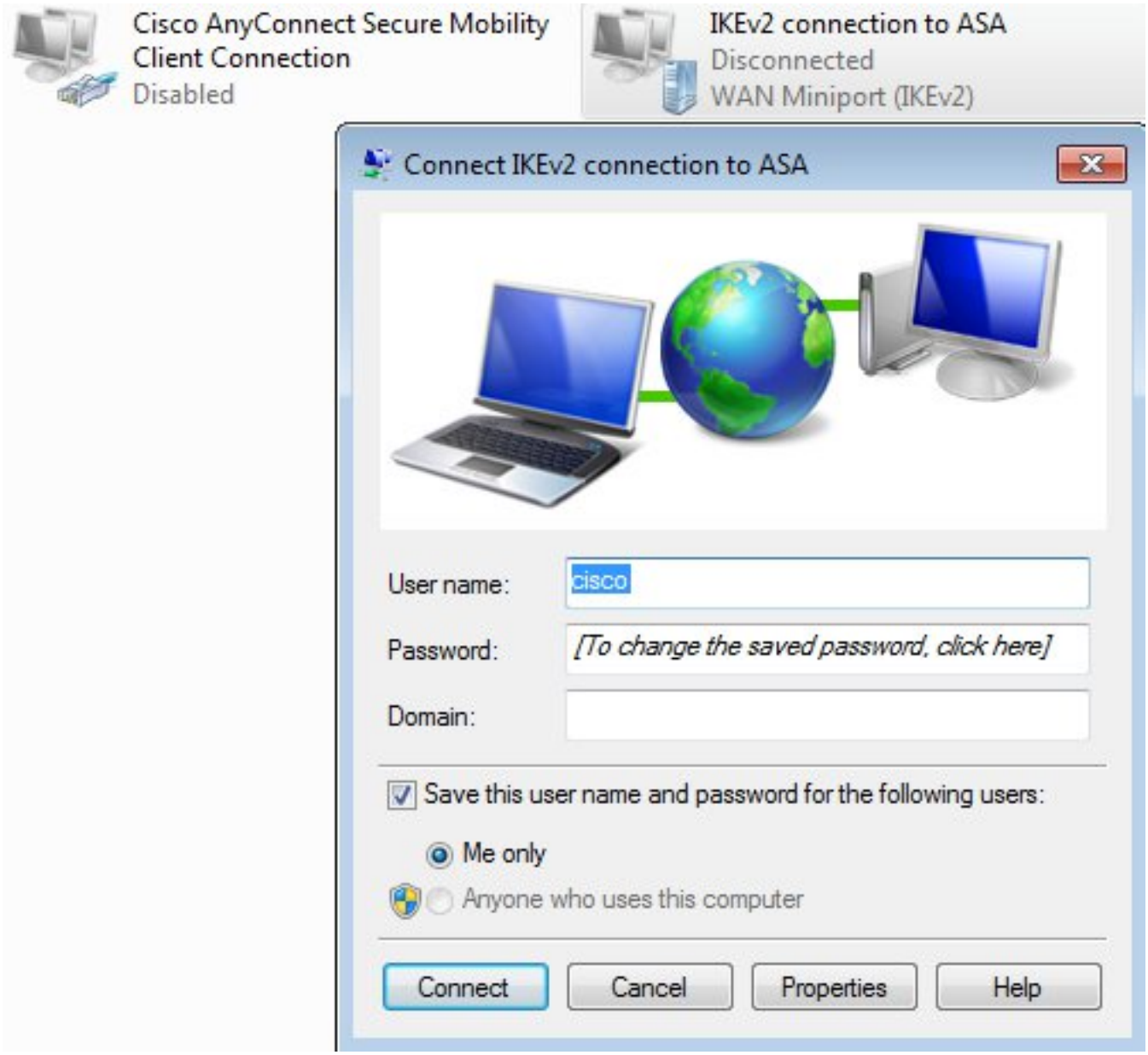
验证

使用本部分可确认配置能否正常运行。

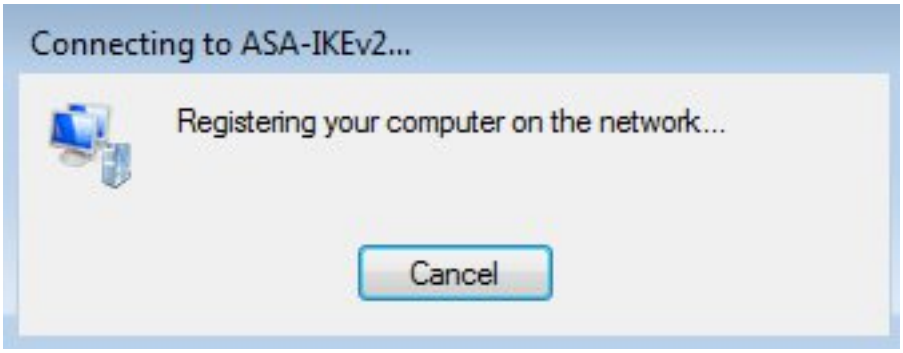
命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

Windows客户端

当您连接时，请输入您的凭证。



在成功认证以后IKEv2配置应用。



会话已启动。

路由表用有使用的默认路由更新新接口与低度量指标。

```
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
===========================================================================
```

日志

在成功认证以后ASA报告：

```
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日志指示与默认验证和授权规则的成功认证。

详细信息指示PEAP方法。

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	c0a801010001000546c424a
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

在ASA的调试

最重要的调试包括：

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

ASA接收的IKE_SA_INIT数据包(包括IKEv2提议和密钥交换对于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
.....
```

对发起者的IKE_SA_INIT答复(包括IKEv2提议、密钥交换对于DH和证书请求) ：

```
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]
```

客户端的IKE_AUTH用IKE-ID、证书请求、报价的转换集、请求的配置和流量选择器：

```
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):
```

包括EAP标识请求从ASA的IKE_AUTH答复(有EAP扩展的第一数据包)。(如果没有在那里ASA的正确证书是失败)，该数据包也包括证书：

```
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]
```

ASA接收的EAP答复(长度5，有效负载：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
```

然后多个信息包被交换作为EAP-PEAP的部分。最终EAP成功由ASA接收并且转发对请求方：

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

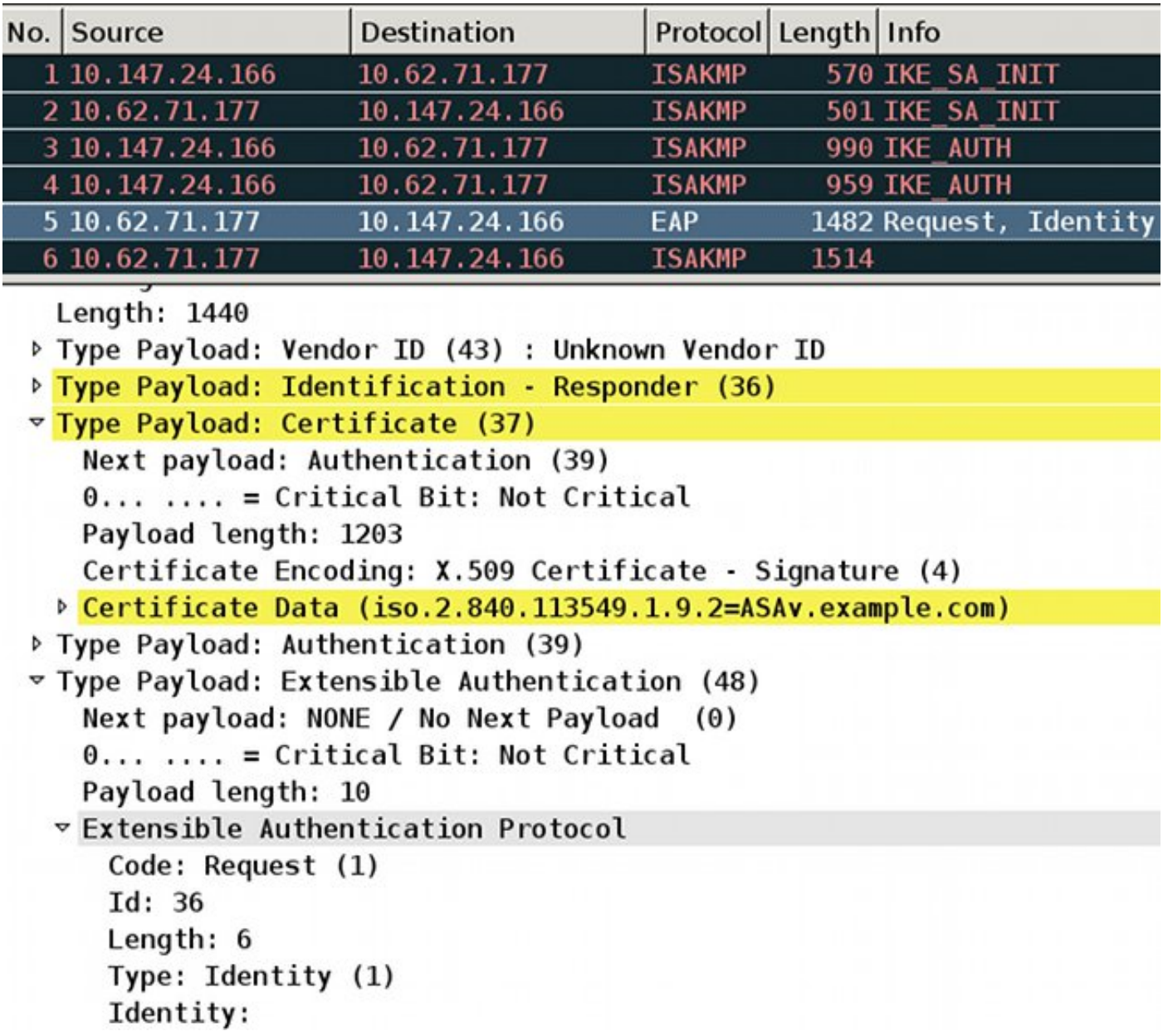
对等点身份验证是成功的：

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

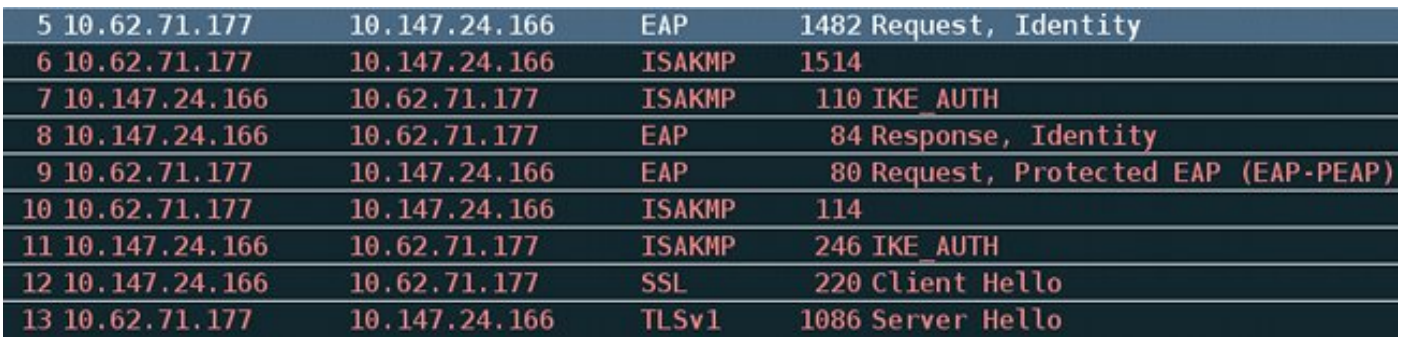
并且VPN会话正确地完成。

级的数据包

EAP标识请求在“扩展验证”被封装IKE_AUTH发送由ASA。与标识请求一起， IKE_ID和证书发送。



所有随后的EAP数据包在IKE_AUTH被封装。在请求方确认方法(EAP-PEAP)后，开始构建保护用于验证的MSCHAPv2会话的安全套接字协议层(SSL)通道。



在多个信息包被交换后ISE确认成功。

```
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
```

IKEv2会话由ASA完成，最终配置(与值的配置回复例如指定的IP地址)，转换设置，并且流量选择器推送给VPN客户端。

```
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
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科ASA系列VPN CLI配置指南， 9.3
- 思科身份服务引擎用户指南，版本1.2
- 技术支持和文档 - Cisco Systems