

# 使用EAP-PEAP和本地Windows客户端配置ASA IKEv2远程访问

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[AnyConnect安全移动客户端注意事项](#)

[配置](#)

[网络图](#)

[证书](#)

[ISE](#)

[步骤1.将ASA添加到ISE上的网络设备。](#)

[步骤2.在本地存储中创建用户名。](#)

[ASA](#)

[Windows 7](#)

[步骤1.安装CA证书。](#)

[步骤2.配置VPN连接。](#)

[验证](#)

[Windows客户端](#)

[日志](#)

[ASA上的调试](#)

[数据包级别](#)

[故障排除](#)

[相关信息](#)

## 简介

本文档提供思科自适应安全设备(ASA)版本9.3.2及更高版本的配置示例，允许远程VPN访问使用具有标准可扩展身份验证协议(EAP)身份验证的互联网密钥交换协议(IKEv2)。这允许本地Microsoft Windows 7客户端（和任何其他基于标准的IKEv2）通过IKEv2和EAP身份验证连接到ASA。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 基本VPN和IKEv2知识
- 基本身份验证、授权和记帐(AAA)和RADIUS知识
- ASA VPN配置体验
- 体验身份服务引擎(ISE)配置

## 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9.3.2版及更高版本
- 思科ISE版本1.2及更高版本

## 背景信息

### AnyConnect安全移动客户端注意事项

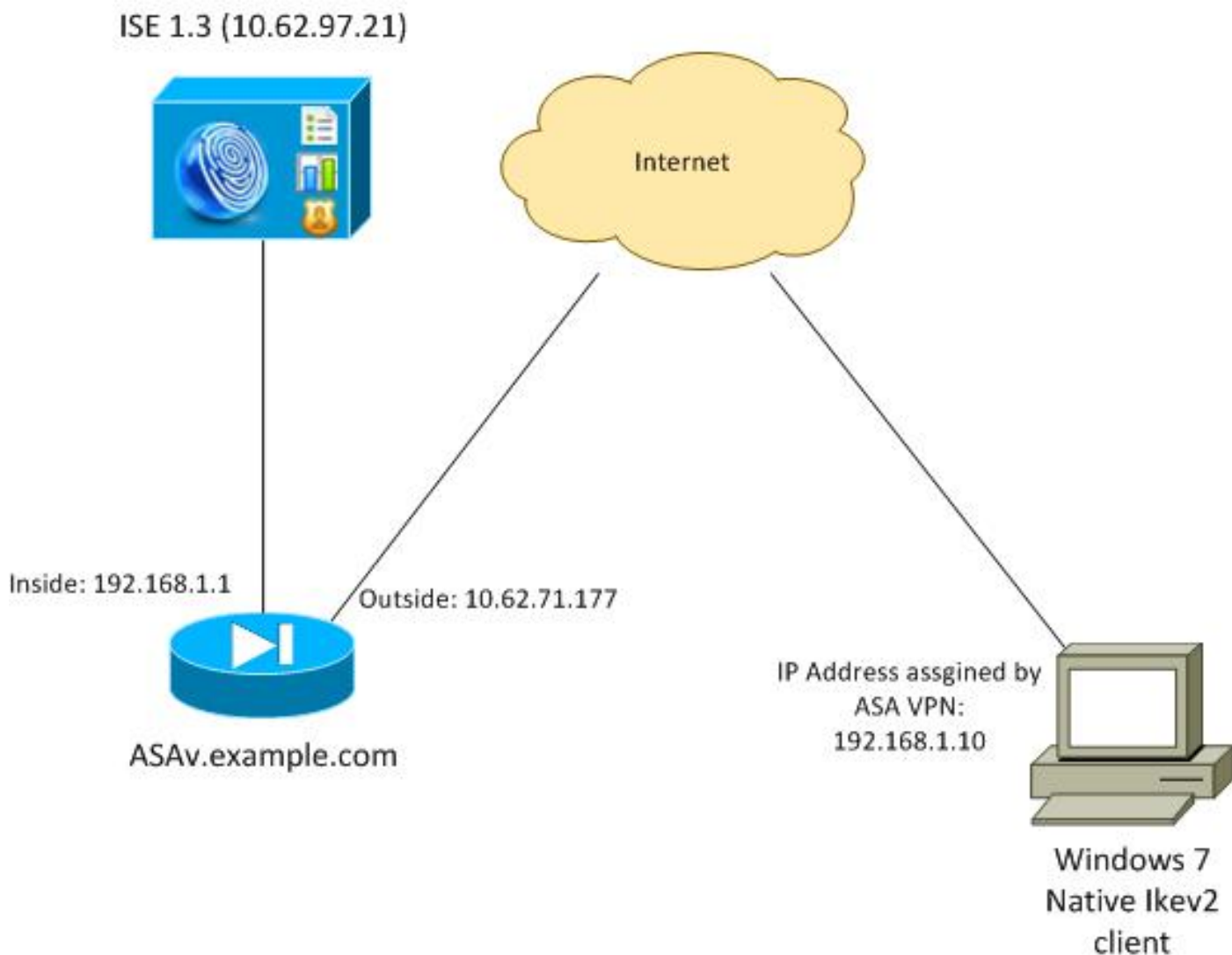
本地Windows IKEv2客户端不支持拆分隧道（没有Windows 7客户端可以接受的CONF REPLY属性），因此Microsoft客户端的唯一可能策略是隧道所有流量（0/0流量选择器）。如果需要特定拆分隧道策略，应使用AnyConnect。

AnyConnect不支持在AAA服务器（PEAP、传输层安全）上终止的标准化EAP方法。如果需要终止AAA服务器上的EAP会话，则可以使用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配置为使用证书进行身份验证（客户端需要信任该证书）。Windows 7客户端配置为使用EAP(EAP-PEAP)进行身份验证。

ASA充当从客户端终止IKEv2会话的VPN网关。ISE充当从客户端终止EAP会话的AAA服务器。EAP数据包封装在IKE\_AUTH数据包中，用于客户端与ASA(IKEv2)之间的流量，然后封装在RADIUS数据包中，用于ASA和ISE之间的身份验证流量。

## 证书

已使用Microsoft证书颁发机构(CA)为ASA生成证书。Windows 7本地客户端要接受的证书要求为：

- 扩展密钥使用(EKU)扩展应包括服务器身份验证（该示例中已使用模板“Web服务器”）。
- Subject-Name应包括客户端将用于连接的完全限定域名(FQDN)（在本例中为ASAv.example.com）。

有关Microsoft客户端的详细信息，请参阅[IKEv2 VPN连接故障排除](#)。

**注意：**Android 4.x限制性更强，并且根据RFC 6125要求使用正确的主题备用名称。有关Android的详细信息，请参阅[从Android strongSwan到Cisco IOS的IKEv2和EAP和RSA身份验证](#)。

为了在ASA上生成证书签名请求，已使用此配置：

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

```
crypto ca trustpoint TP
enrollment terminal
```

```
crypto ca authenticate TP
crypto ca enroll TP
```

## ISE

### 步骤1.将ASA添加到ISE上的网络设备。

选择Administration > Network Devices。设置ASA将使用的预共享密码。

### 步骤2.在本地存储中创建用户名。

选择管理>身份>用户。根据需要创建用户名。

默认情况下，ISE启用所有其他设置，以使用EAP-PEAP（受保护可扩展身份验证协议）对终端进行身份验证。

## ASA

远程访问的配置与IKEv1和IKEv2类似。

```
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
```

由于Windows 7在IKE\_AUTH数据包中发送IKE-ID类型地址，因此应使用DefaultRAGroup来确保连接在正确的隧道组上。ASA使用证书（本地身份验证）进行身份验证，并期望客户端使用EAP（远

程身份验证)。此外，ASA需要专门发送EAP身份请求，以便客户端使用EAP身份响应(query-identity)进行响应。

```
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，需要启用IKEv2并使用正确的证书。

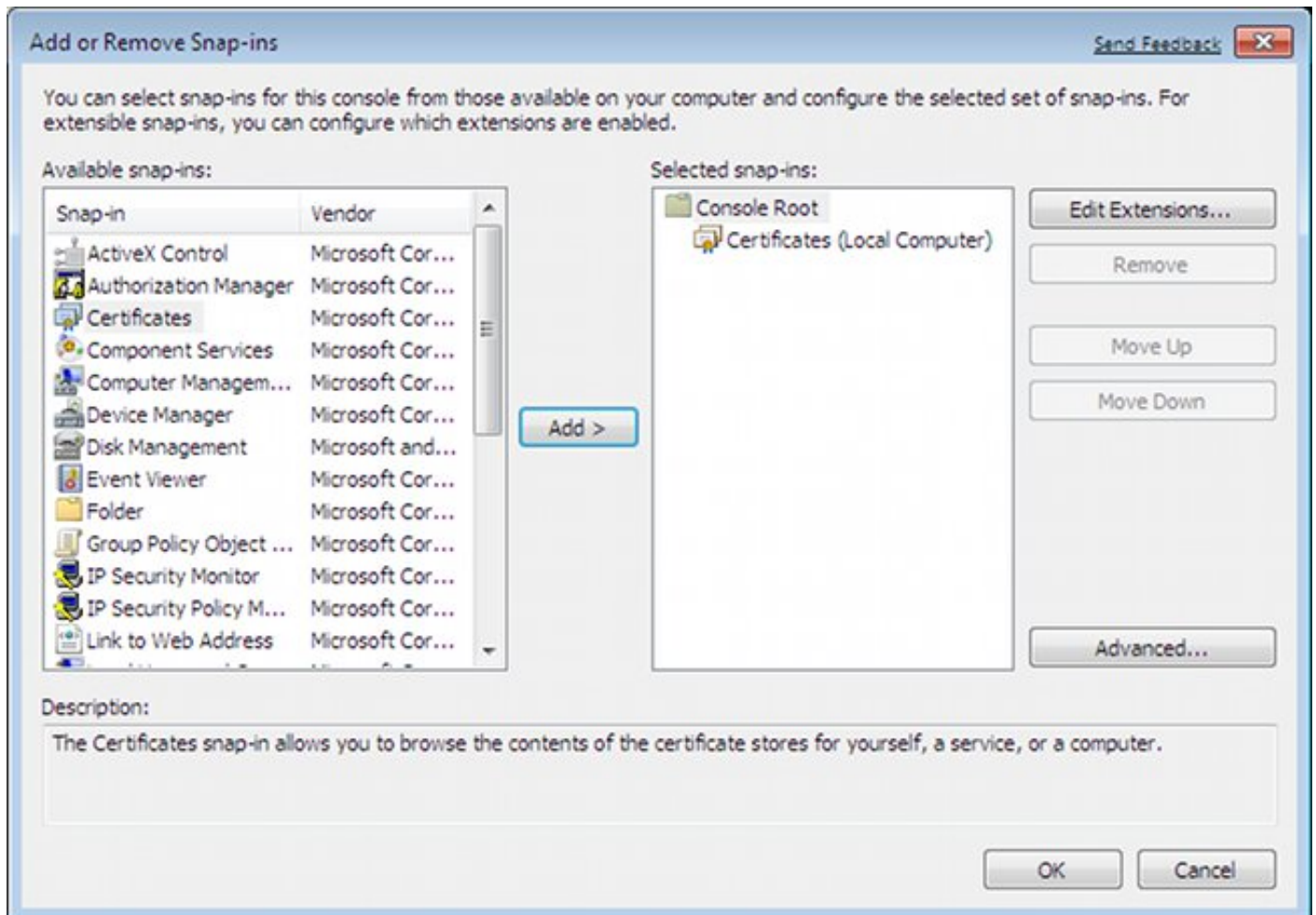
```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint TP
```

## Windows 7

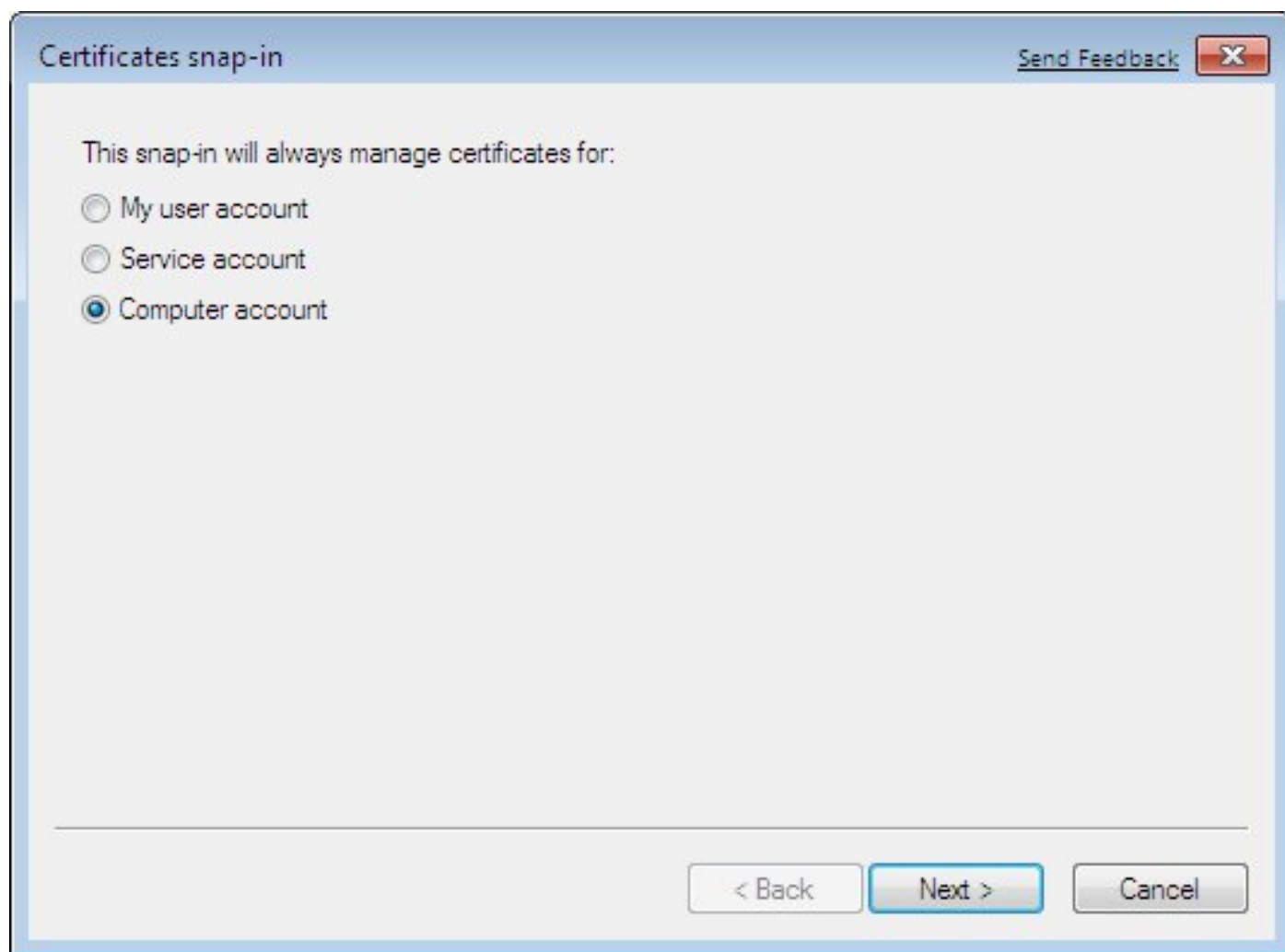
### 步骤1.安装CA证书。

要信任ASA提供的证书，Windows客户端需要信任其CA。该CA证书应添加到计算机证书存储区（而不是用户存储区）。Windows客户端使用计算机存储区来验证IKEv2证书。

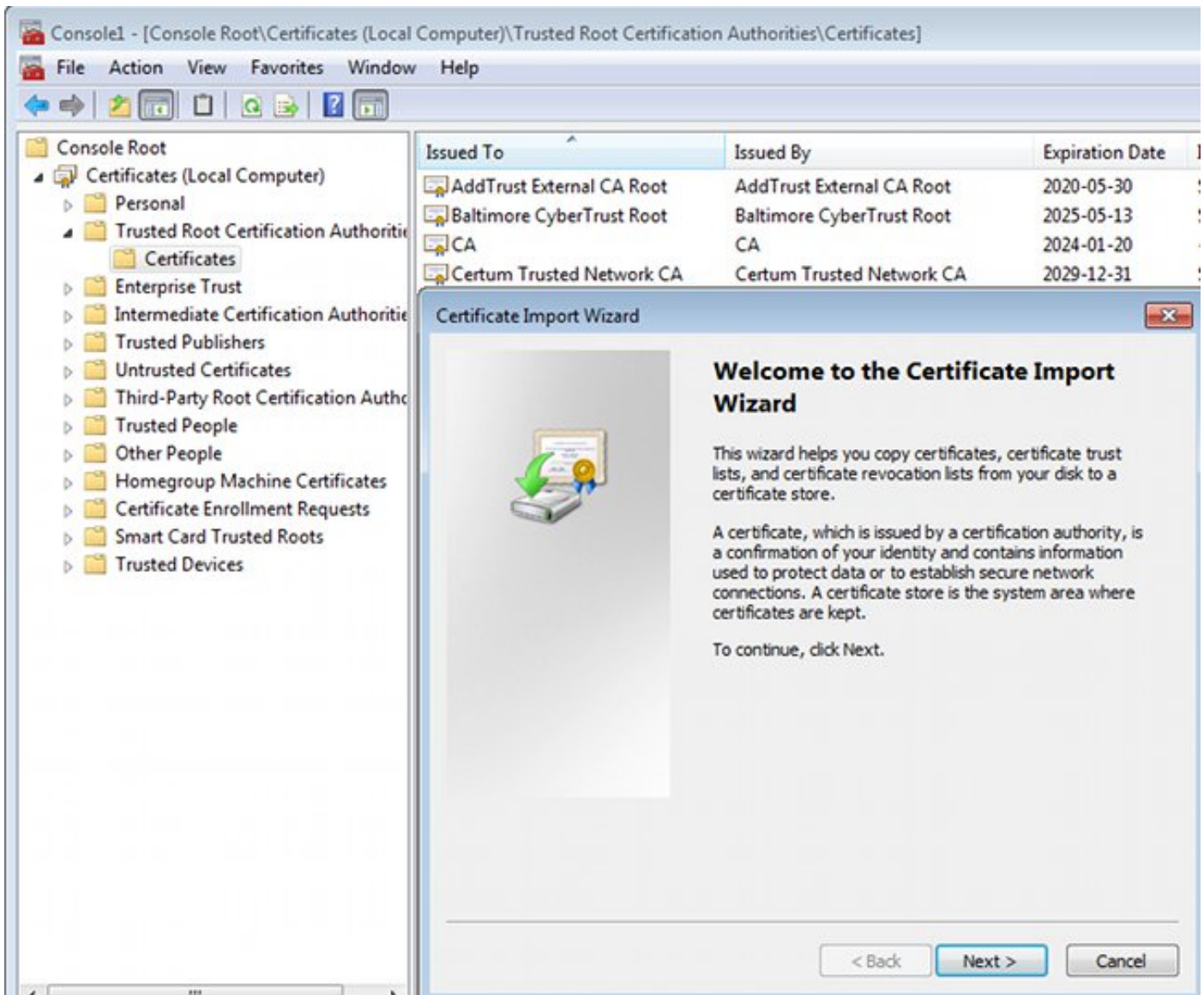
要添加CA，请选择MMC >添加或删除管理单元>证书。



单击“Computer account(计算机帐户)”单选按钮。



将CA导入受信任根证书颁发机构。



如果Windows客户端无法验证ASA提供的证书，它会报告：

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

## 步骤2.配置VPN连接。

要从网络和共享中心配置VPN连接，请选择**Connect to a workplace** 以创建VPN连接。

Control Panel Home  
Change adapter settings  
Change advanced sharing settings  
  
See also

### View your basic network information and set up connections



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.

Next Cancel

选择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.



使用ASA FQDN配置地址。确保域名服务器(DNS)正确解析了它。



## Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

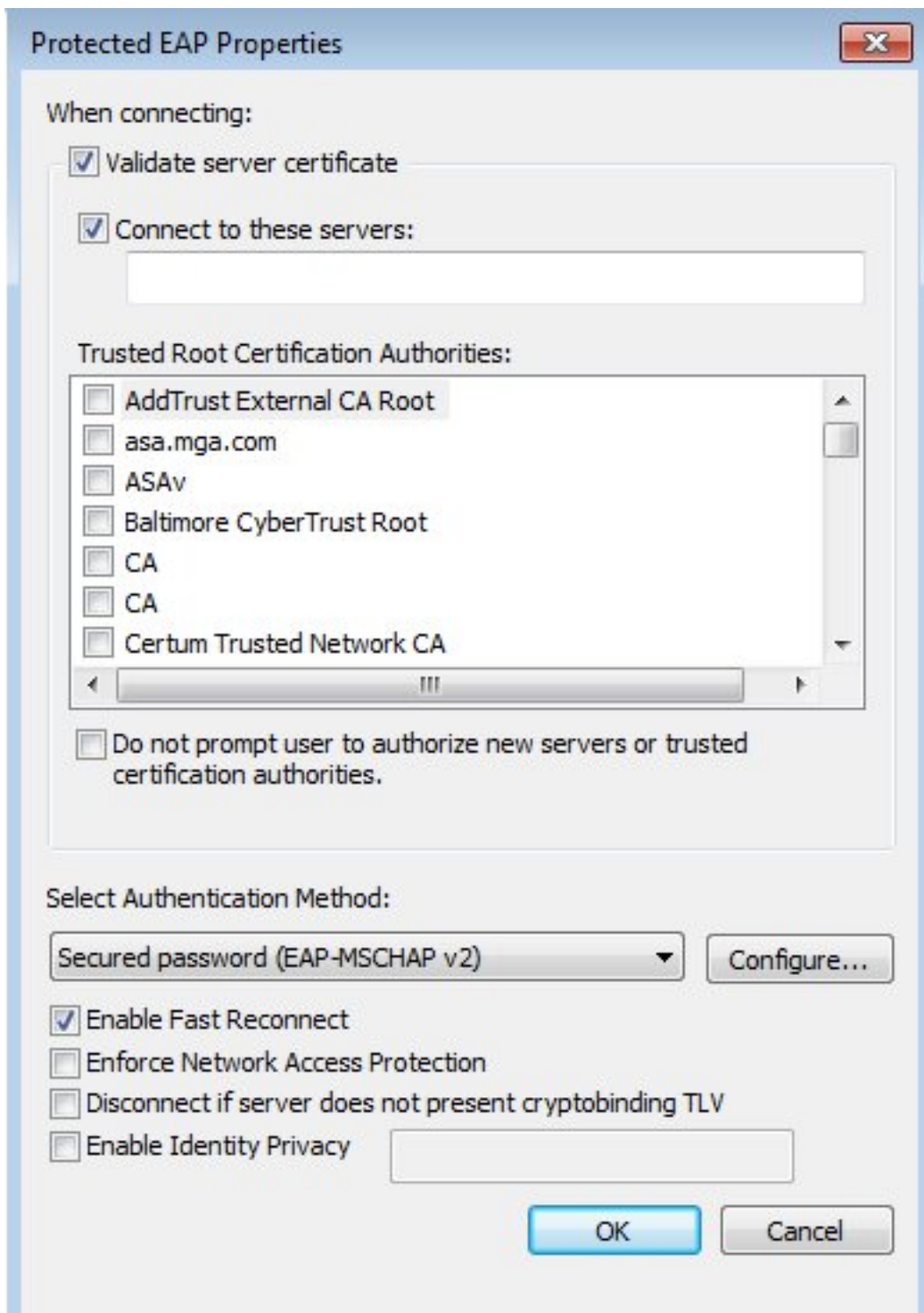


Allow other people to use this connection

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

如果需要，在“受保护的EAP属性”窗口中调整属性（如证书验证）。



## 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。使用输出解释器工具来查看 show 命令输出的分析。

## Windows客户端

连接时，输入您的凭证。



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

身份验证成功后，将应用IKEv2配置。

Connecting to ASA-IKEv2...



Registering your computer on the network...

会话已启动。

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)

路由表已使用默认路由更新，使用度量较低的新接口。

```
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

身份验证成功后，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日志指示使用默认身份验证和授权规则成功进行身份验证。



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	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

### ASA上的调试

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Diffie-Hellman(DH)的密钥交换):

```
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
.....
```

对启动器的IKE\_SA\_INIT响应 ( 包括IKEv2提议、DH的密钥交换和证书请求 ) :

```
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]
```

IKE\_AUTH用于具有IKE-ID、证书请求、建议的转换集、请求的配置和流量选择器的客户端 :

```
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):
```

来自ASA的IKE\_AUTH响应, 包括EAP身份请求 ( 第一个具有EAP扩展的数据包 )。该数据包还包含证书 ( 如果ASA上没有正确的证书, 则出现故障 ) :

```
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收到的EAP响应(长度5, 负载: 思科):

```
(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
```

然后, 多个数据包作为EAP-PEAP的一部分进行交换。最后, ASA收到EAP成功并转发给请求方 :

Payload contents:

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

对等身份验证成功：

IKEv2-PROTO-2: (30): Verification of peer's authentication data PASSED  
VPN会话已正确完成。

## 数据包级别

EAP身份请求封装在ASA发送的IKE\_AUTH的“可扩展身份验证”中。连同身份请求，IKE\_ID和证书也会发送。

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:

所有后续EAP数据包都封装在IKE\_AUTH中。请求方确认方法(EAP-PEAP)后，开始构建安全套接字层(SSL)隧道，该隧道保护用于身份验证的MSCHAPv2会话。



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

交换多个数据包后，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（配置回复，包含值，如分配的IP地址）、转换集和流量选择器被推送到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, 版本 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](#)