Configurar o Acesso remoto ASA IKEv2 com EAP-PEAP e cliente das janelas nativas

Índice

Introdução

Este documento fornece um exemplo de configuração para uma versão 9.3.2 e mais recente adaptável da ferramenta de segurança de Cisco (ASA) que permita que o acesso remoto VPN use o protocolo do intercâmbio de chave de Internet (IKEv2) com autenticação padrão do Extensible Authentication Protocol (EAP). Isto permite que um cliente nativo de Microsoft Windows 7 (e algum outro IKEv2 com base em padrões) conectem ao ASA com o IKEv2 e a autenticação de EAP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento VPN e IKEv2 básico
- Conhecimento da autenticação básica, da autorização, e da contabilidade (AAA) e do RAIO
- Experiência com configuração de VPN ASA
- Experiência com configuração do Identity Services Engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Software de Cisco ASA, versão 9.3.2 e mais recente
- Cisco ISE, libera 1.2 e mais atrasado

Informações de Apoio

Considerações seguras do cliente da mobilidade de AnyConnect

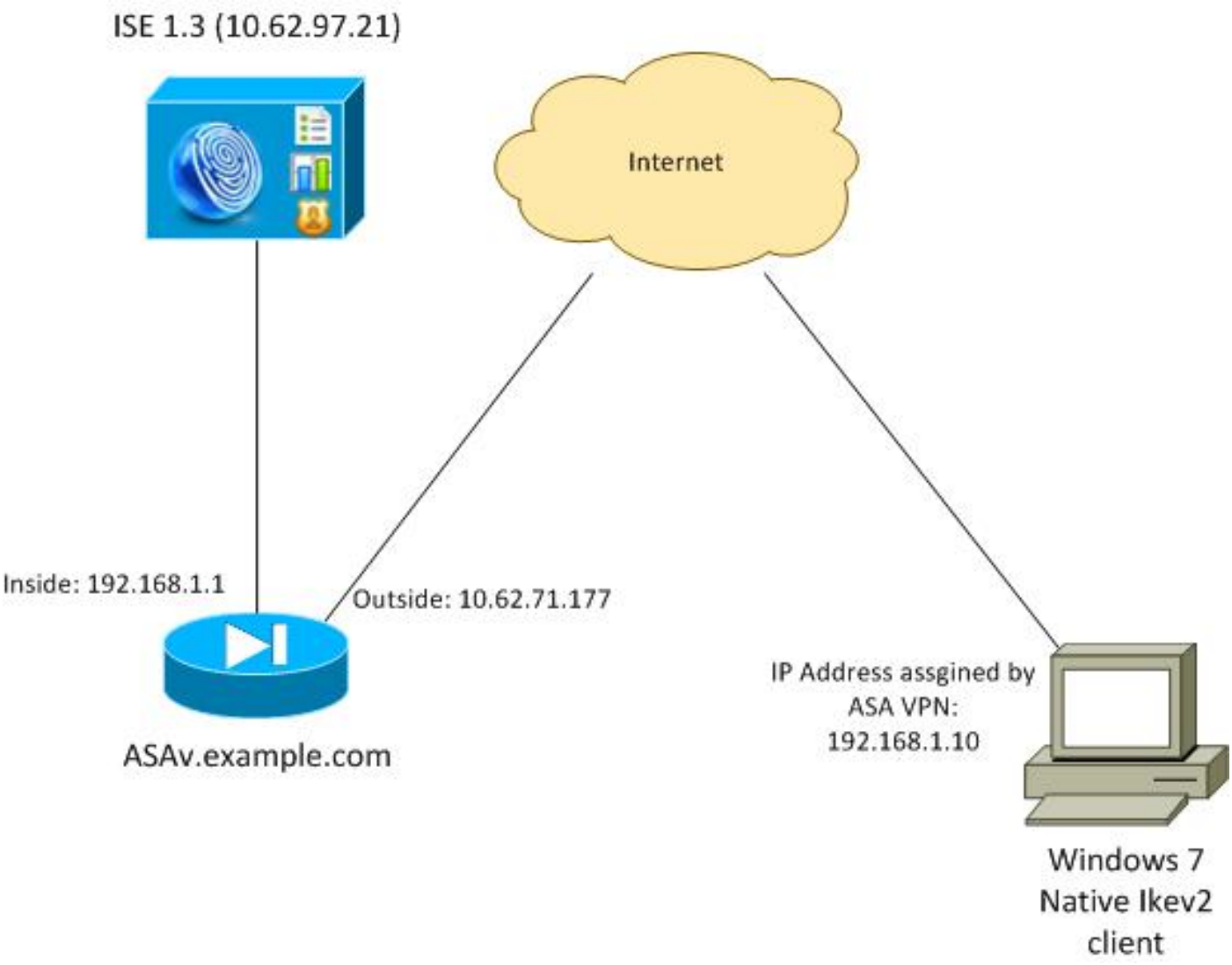
O cliente das janelas nativas IKEv2 não apoia o túnel em divisão (não há nenhum atributo da RESPOSTA de CONF que poderiam ser aceitados pelo cliente de Windows 7), assim que a única política possível com o cliente Microsoft é escavar um túnel todo o tráfego (seletores de 0/0 de tráfego). Se há uma necessidade para uma política específica do túnel em divisão, AnyConnect deve ser usado.

AnyConnect não apoia os métodos de EAP estandardizados que são terminados no servidor AAA (PEAP, Transport Layer Security). Se há uma necessidade de terminar sessões EAP no servidor AAA então o cliente Microsoft pode ser usado.

Configurar

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



O ASA é configurado para autenticar com um certificado (o cliente precisa de confiar esse certificado). O cliente de Windows 7 é configurado para autenticar com EAP (EAP-PEAP).

O ASA atua como o gateway de VPN que termina a sessão IKEv2 do cliente. O ISE atua como um servidor AAA que termina a sessão EAP do cliente. Os pacotes EAP são encapsulados em uns pacotes IKE_AUTH para o tráfego entre o cliente e o ASA (IKEv2) e então em uns pacotes de informação de RADIUS para o tráfego da autenticação entre o ASA e o ISE.

Certificados

Microsoft Certificate Authority (CA) foi usado a fim gerar o certificado para o ASA. As exigências do certificado a fim para ser aceitado pelo cliente nativo de Windows 7 são:

- A extensão chave prolongada do uso (EKU) deve incluir a autenticação de servidor (o molde “servidor de Web” foi usado nesse exemplo).
- O Assunto-nome deve incluir o nome de domínio totalmente qualificado (FQDN) que serão usados pelo cliente a fim conectar (neste exemplo ASAv.example.com).

Para mais detalhes no cliente Microsoft, veja pesquisando defeitos as conexões de VPN IKEv2.

> Nota: Android 4.x é mais restritivo e exige o nome alternativo sujeito correto conforme o RFC 6125. Para mais informação para Android, veja IKEv2 de Android strongSwan ao Cisco

IOS com EAP e autenticação de RSA.

A fim gerar uma solicitação de assinatura de certificado no ASA, esta configuração foi usada:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Etapa 1. Adicionar o ASA aos dispositivos de rede no ISE.

Escolha a **administração > dispositivos de rede**. Ajuste uma senha preshared que seja usada pelo ASA.

Etapa 2. Crie um username na loja local.

Escolha a **administração > identidades > usuários**. Crie o username como necessário.

Todos ajustes restantes são permitidos à revelia para que o ISE autentique valores-limite com EAP-PEAP (protocolo extensible authentication protegido).

ASA

A configuração para o Acesso remoto é similar para IKEv1 e 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
```

Desde que Windows 7 envia um tipo endereço IKE-ID no pacote IKE_AUTH, o **DefaultRAGroup** deve ser usado a fim certificar-se de que a conexão aterra no grupo de túneis correto. O ASA autentica com um certificado (autenticação local) e espera o cliente usar EAP (autenticação remota). Também, o ASA precisa de enviar especificamente um pedido da identidade EAP para que o cliente responda com resposta da identidade EAP (pergunta-identidade).

```
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
```

Finalmente, IKEv2 precisa de ser permitido e o certificado correto de ser usado.

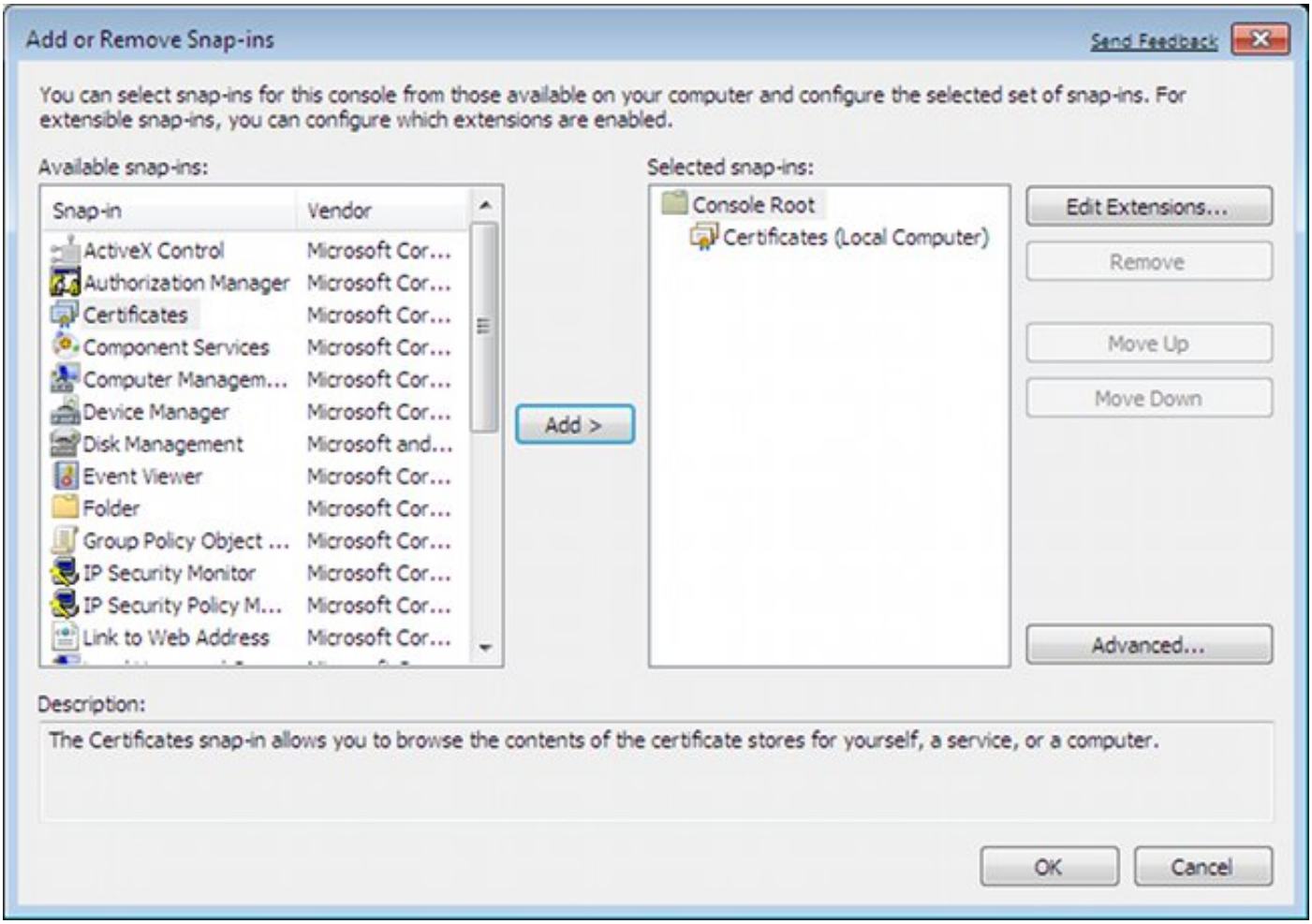
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Windows 7

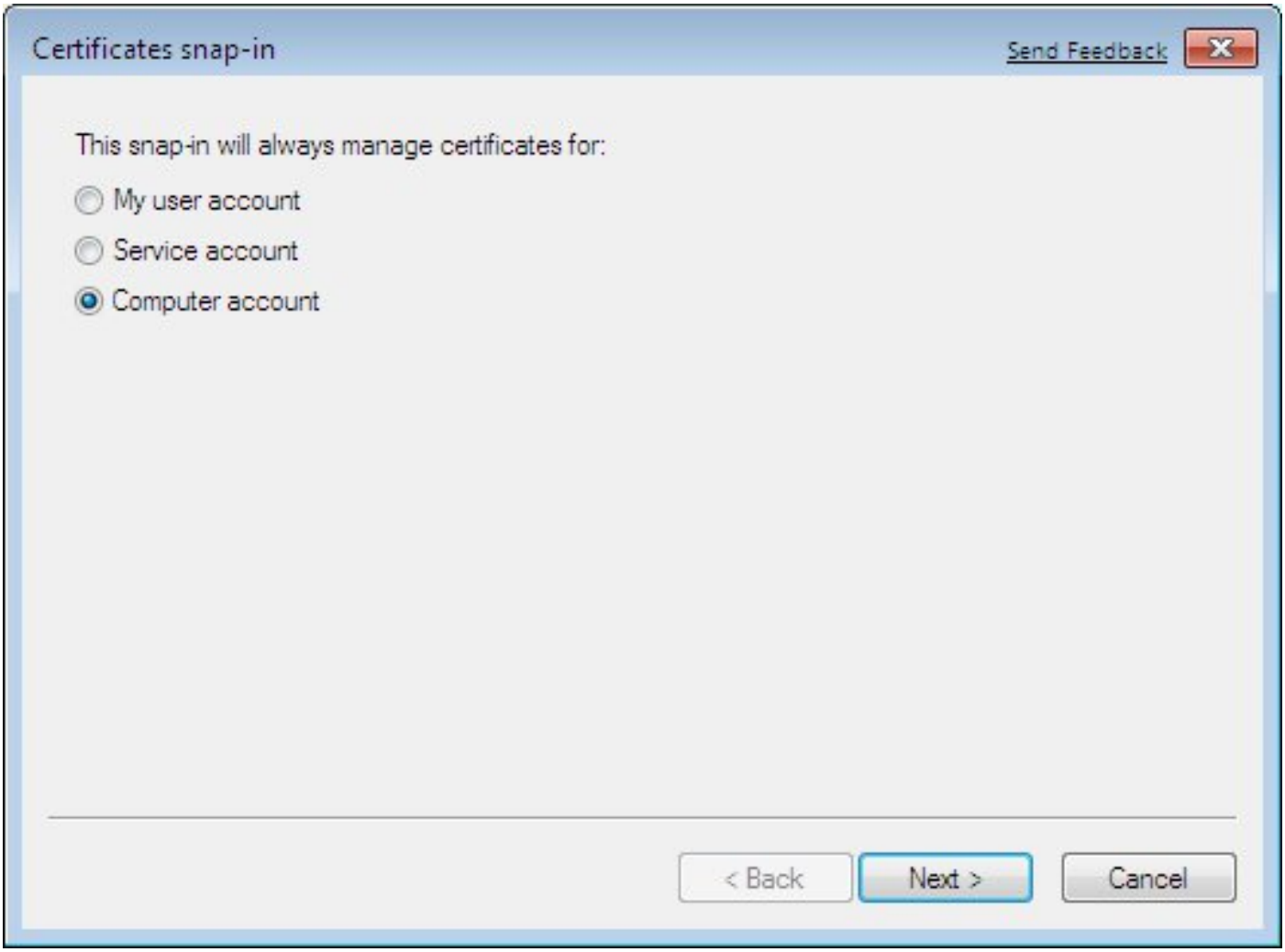
Etapa 1. Instale o certificado de CA.

A fim confiar o certificado apresentado pelo ASA, o cliente do Windows precisa de confiar seu CA. Esse certificado de CA deve ser adicionado à loja do certificado do computador (não a loja do usuário). O cliente do Windows usa a loja de computadores a fim validar o certificado IKEv2.

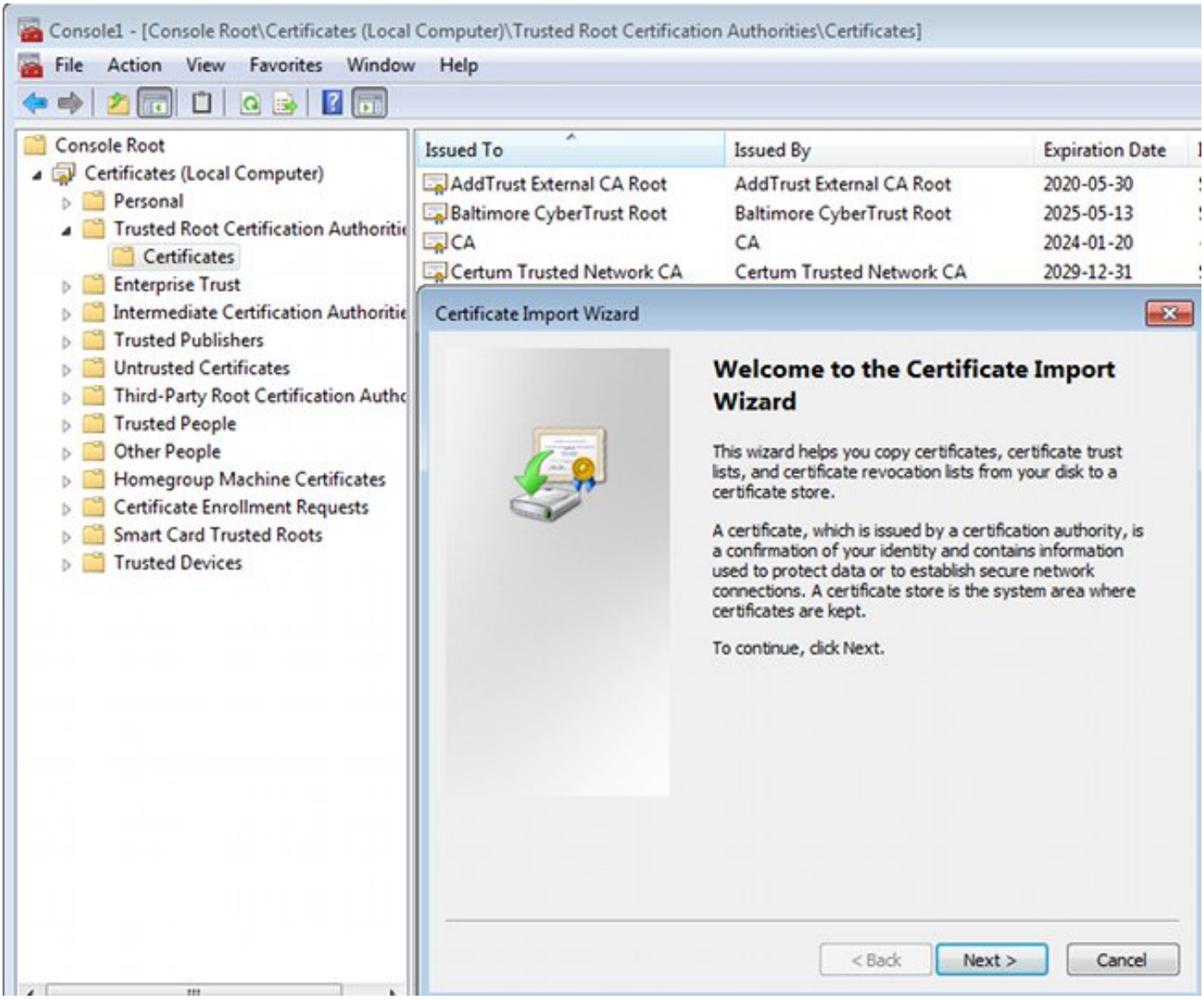
A fim adicionar o CA, escolha o **> Add MMC ou remova-o Pressão-INS > Certificados**.



Clique o botão de rádio da **conta do computador**.



Importe CA às autoridades de certificação do root confiável.

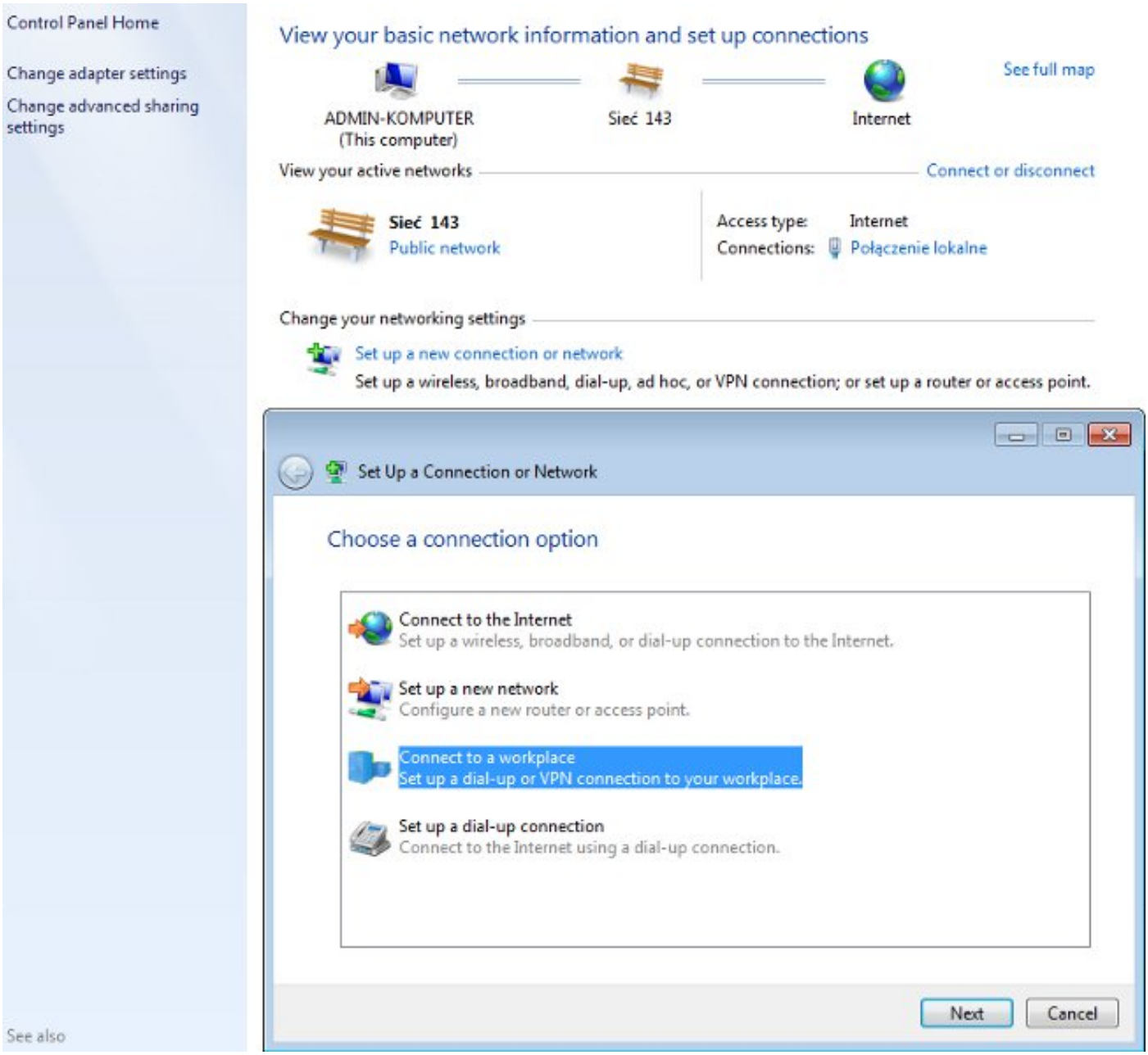


Se o cliente do Windows não pode validar o certificado apresentado pelo ASA, relata:

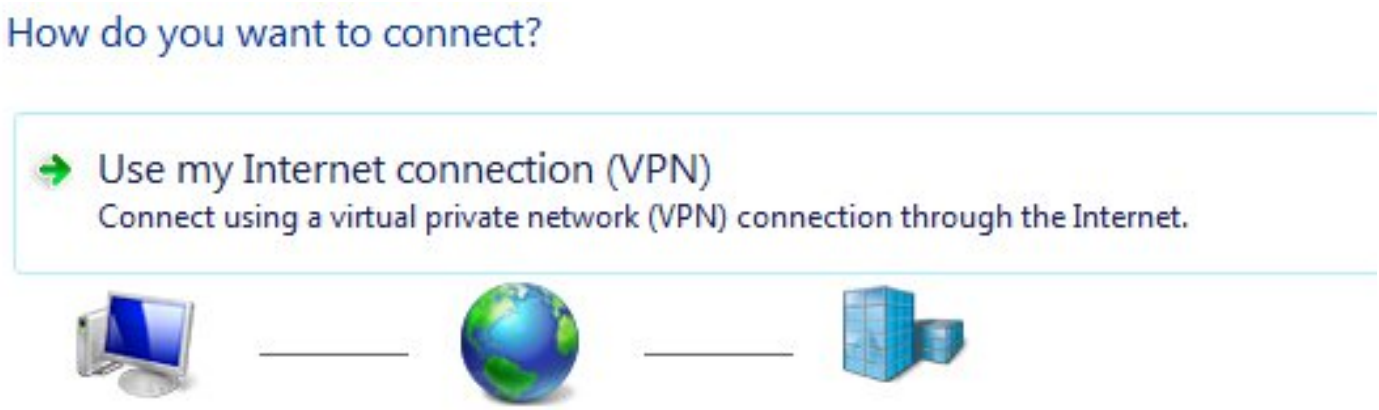
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Etapa 2. Configurar a conexão de VPN.

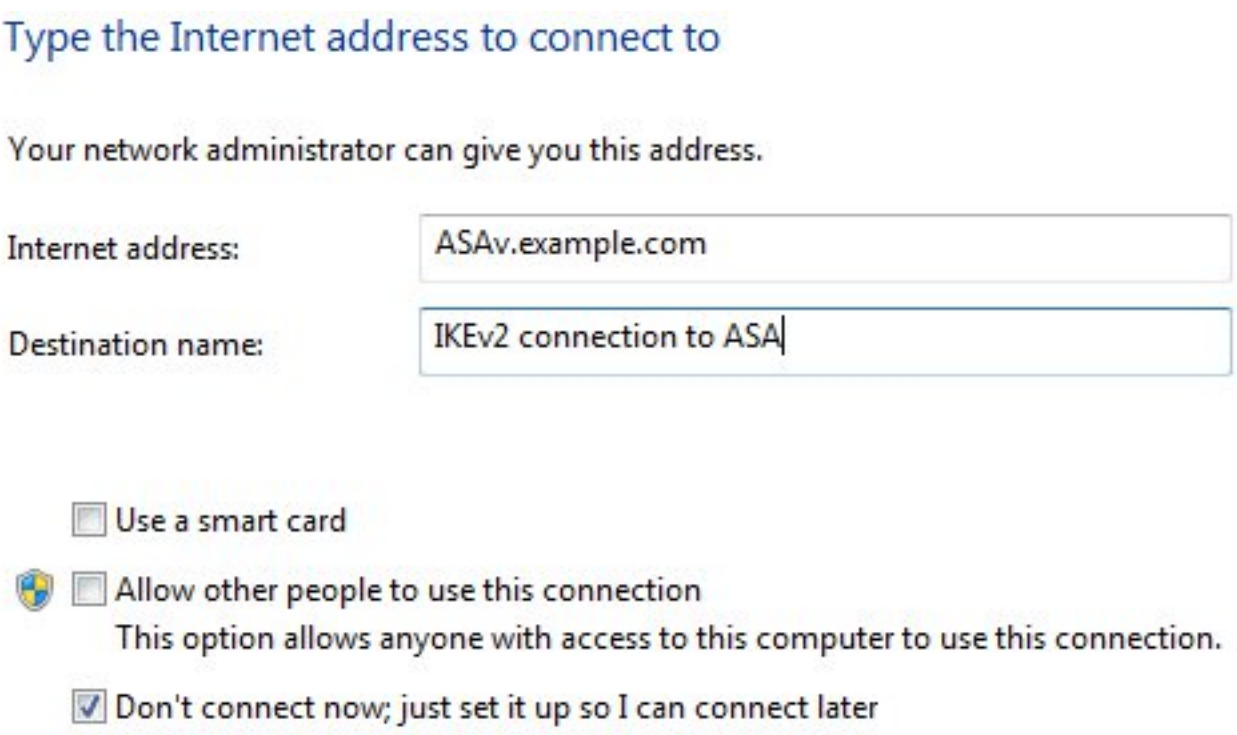
A fim configurar a conexão de VPN da rede e do centro da partilha, escolha **conectam a um local de trabalho** a fim criar uma conexão de VPN.



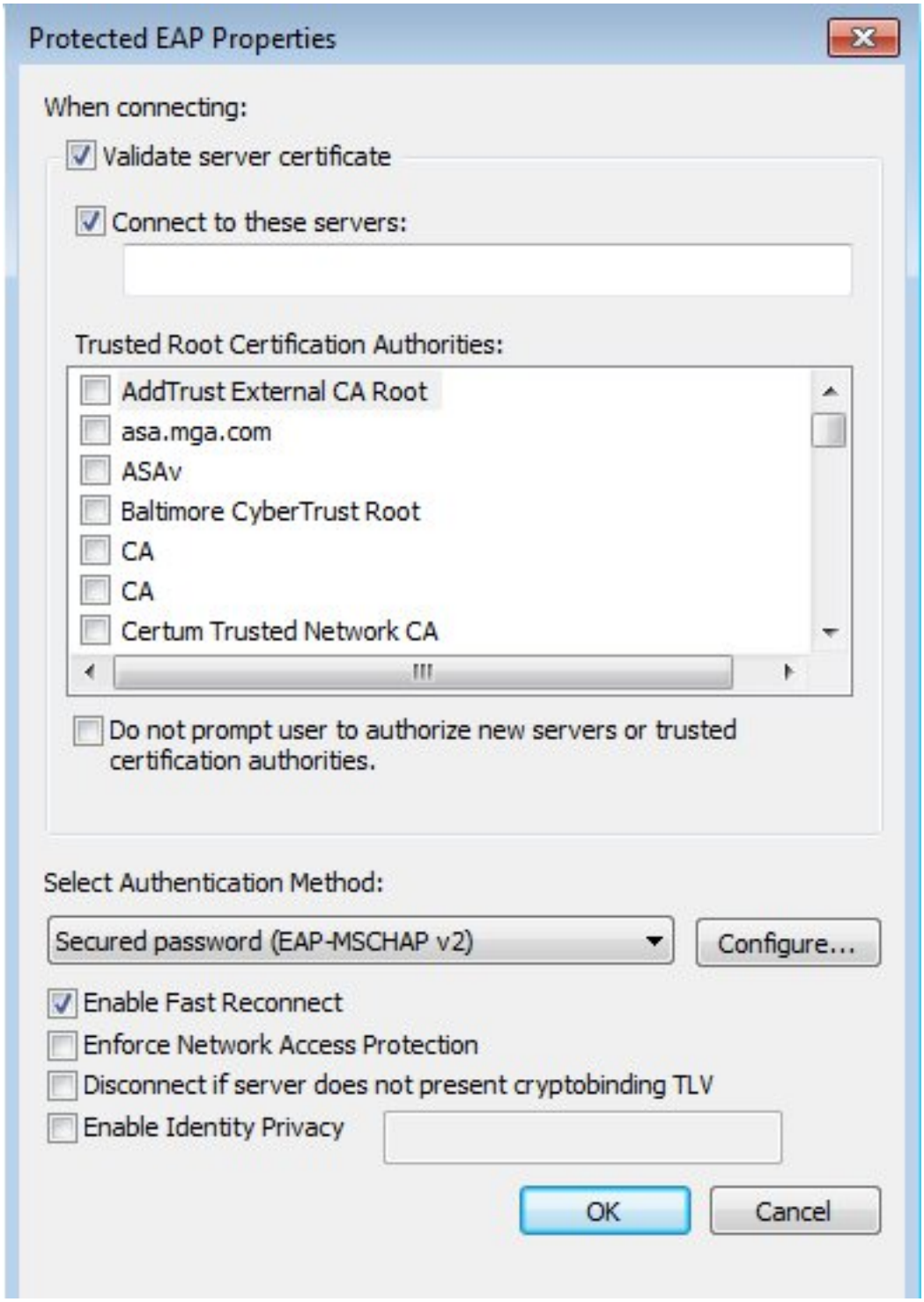
Escolha o **uso minha conexão com o Internet (VPN)**.



Configurar o endereço com um FQDN ASA. Certifique-se que está resolvido corretamente pelo Domain Name Server (DNS).



Se for necessário, ajuste propriedades (tais como a validação certificada) na janela de propriedades protegida EAP.



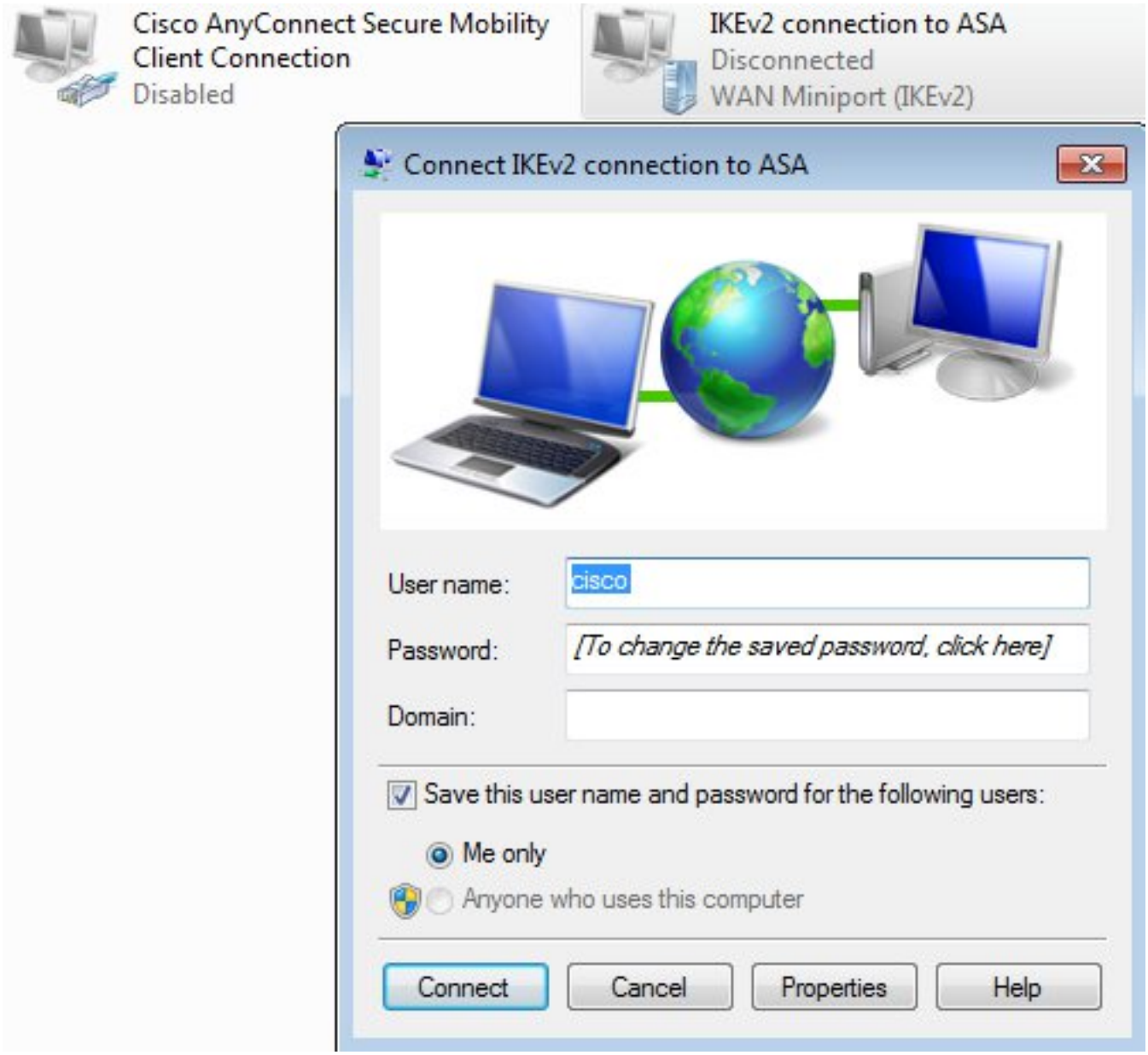
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

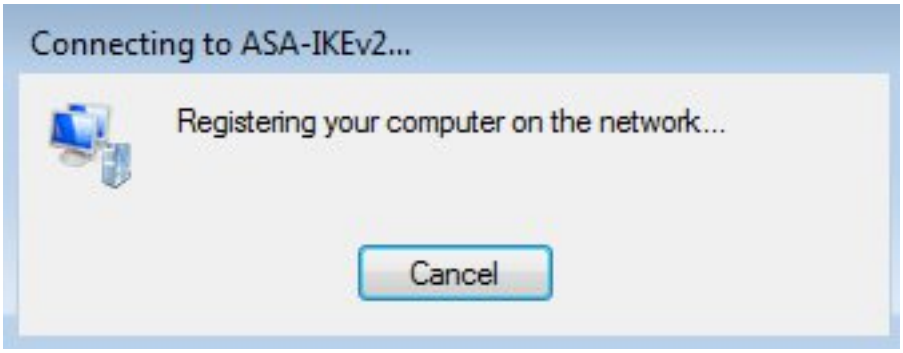
A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Cliente do Windows

Quando você conecta, incorpore suas credenciais.



Após a autenticação bem sucedida a configuração IKEv2 é aplicada.



A sessão está ativa.

A tabela de roteamento foi atualizada com a rota padrão com uso de uma relação nova com a métrica baixa.

```
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

Após a autenticação bem sucedida os relatórios 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
```

Os logs ISE indicam a autenticação bem sucedida com as regras da autenticação padrão e da autorização.

Os detalhes indicam o método PEAP.

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

Debuga no ASA

O mais importante debuga inclui:

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

Pacote IKE_SA_INIT recebido pelo ASA (inclui as propostas IKEv2 e as trocas de chave para o 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
.....
```

Resposta IKE_SA_INIT ao iniciador (inclui as propostas IKEv2, as trocas de chave para o DH, e o pedido do certificado):

```
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_AUTHENTIC para o cliente com IKE-ID, pedido do certificado, proposto transformam grupos, configuração pedida, e seletores do tráfego:

```
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):
```

Resposta IKE_AUTHENTIC do ASA que inclui um pedido da identidade EAP (primeiro pacote com Ramais EAP). Esse pacote igualmente inclui o certificado (se não há nenhum certificado correto no ASA lá está uma falha):

```
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]
```

Resposta EAP recebida pelo ASA (comprimento 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
```

Os pacotes múltiplos são trocados então como parte de um EAP-PEAP. Finalmente o sucesso EAP é recebido pelo ASA e enviado ao suplicante:

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

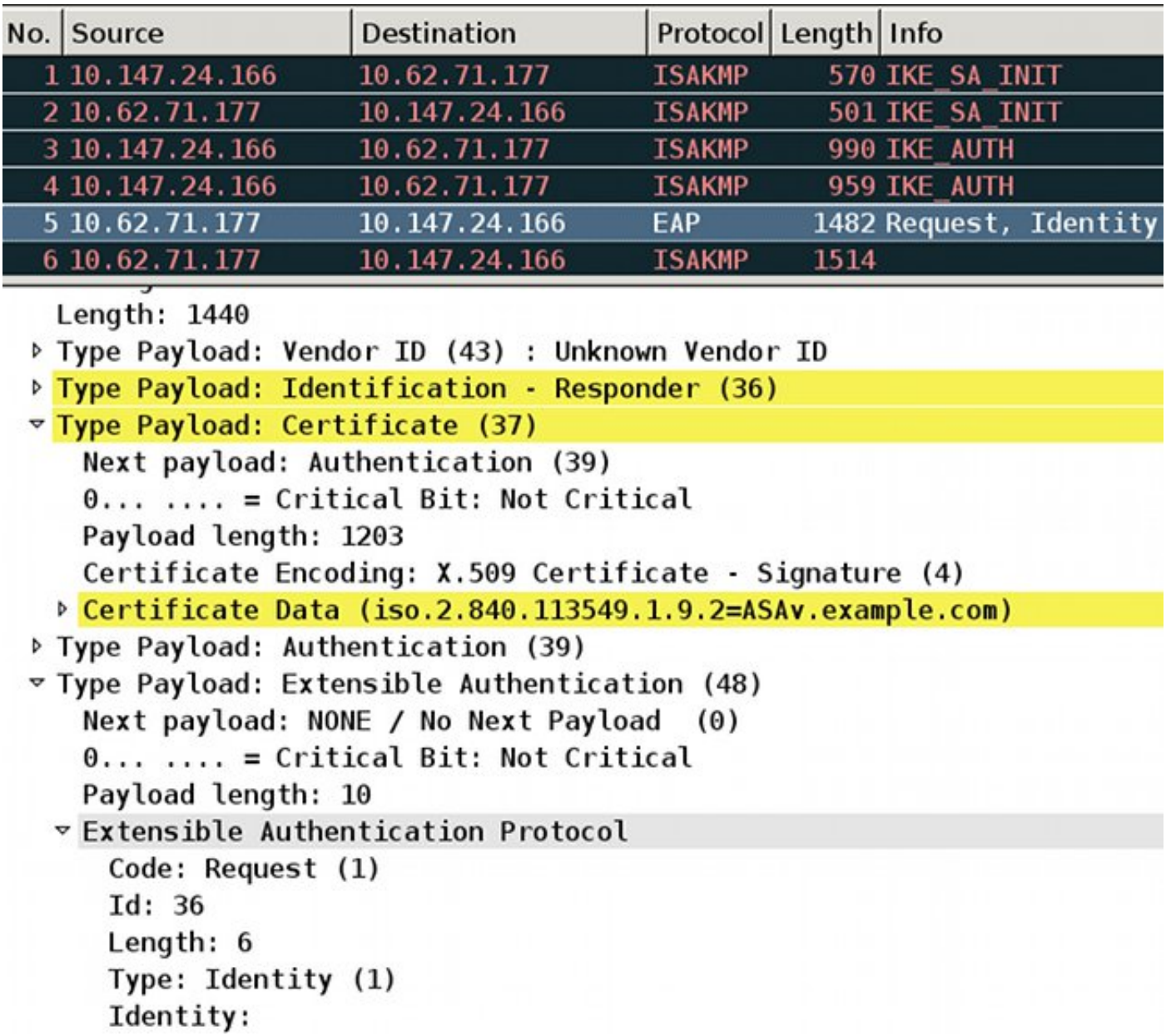
A autenticação de peer é bem sucedida:

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

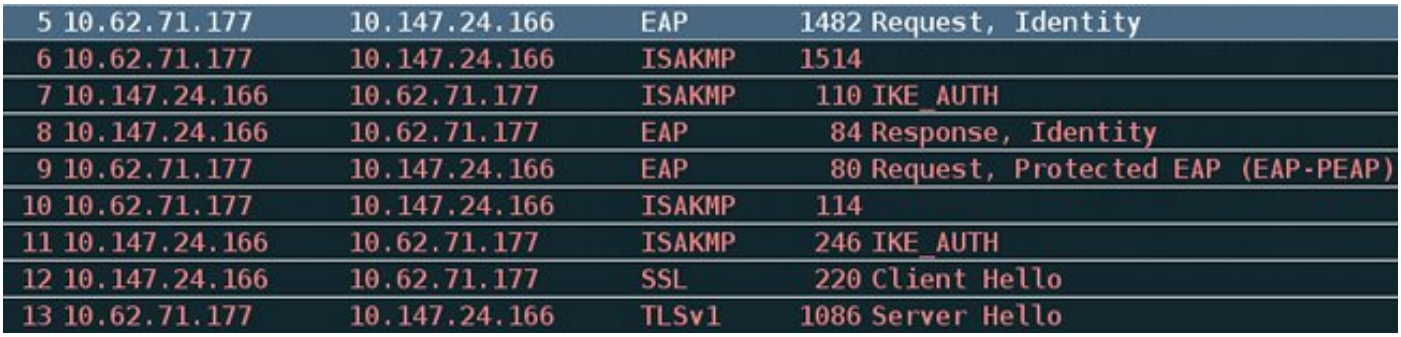
E a sessão de VPN é terminada corretamente.

Pacote em nível

O pedido da identidade EAP é encapsulado na “autenticação extensível” do IKE_AUTH envia pelo ASA. Junto com o pedido da identidade, IKE_ID e os Certificados são enviados.

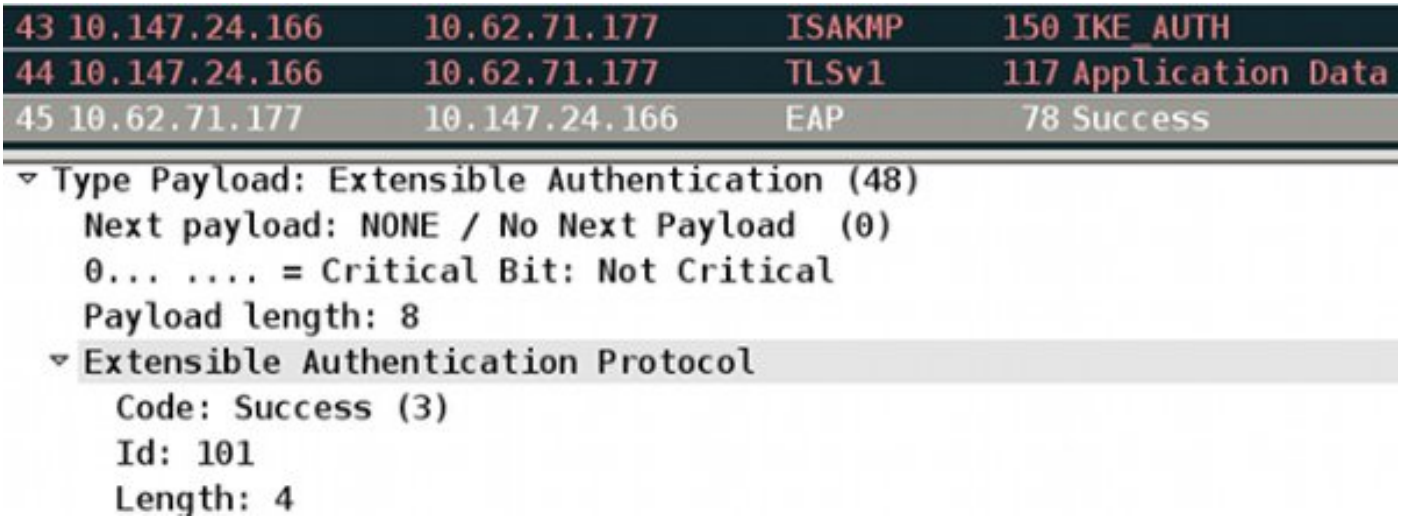


Todos os pacotes EAP subsequentes são encapsulados em IKE_AUTH. Depois que o suplicante confirma o método (EAP-PEAP), começa construir um túnel do secure sockets layer (SSL) que proteja a sessão MSCHAPv2 usada para a autenticação.



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

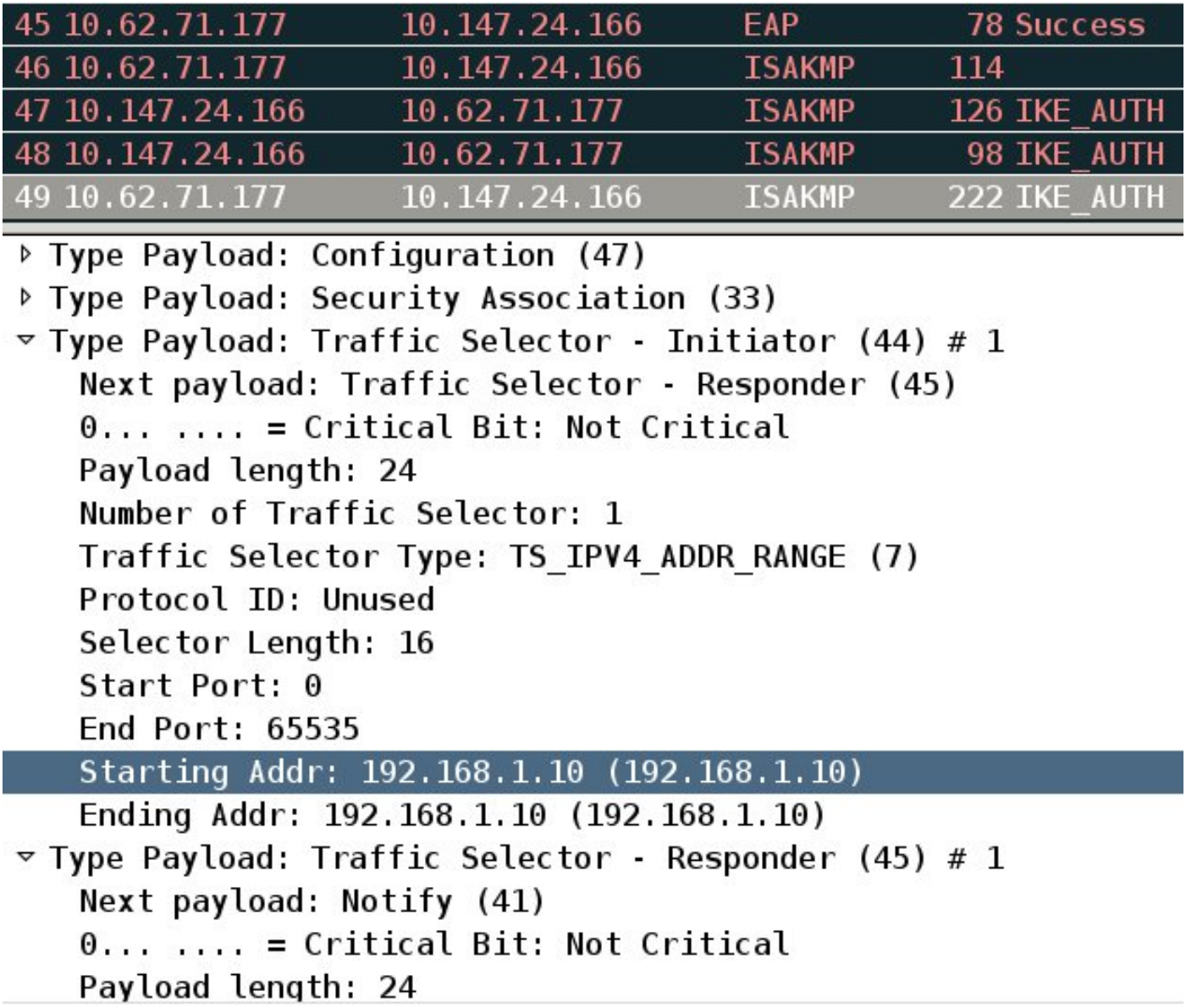
Depois que os pacotes múltiplos são trocados o ISE confirma o sucesso.



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
```

A sessão IKEv2 é terminada pelo ASA, a configuração final (resposta da configuração com valores tais como um endereço IP atribuído), transforma grupos, e os seletores do tráfego são empurrados para o cliente VPN.



Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração de CLI da série VPN de Cisco ASA, 9.3
- Guia do Usuário do Cisco Identity Services Engine, liberação 1.2
- Suporte Técnico e Documentação - Cisco Systems