Настройте удаленный доступ ASA IKEv2 с клиентом собственных окон и PEAP EAP

Содержание

Введение

Этот документ предоставляет пример конфигурации для устройства адаптивной защиты Cisco (ASA) Версия 9.3.2 и позже который предоставляет удаленный доступ VPN для использования Протокола (IKEv2) Обмена ключами между сетями со стандартной аутентификацией Протокола EAP. Это разрешает собственному Microsoft Windows 7 клиентов (и любой другой на основе стандарта IKEv2) для соединения с ASA с IKEv2 и Аутентификацией eap.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основная VPN и знание IKEv2
- Базовая проверка подлинности, Авторизация, и Бухгалтерский (AAA) и знание RADIUS
- Опыт с конфигурацией VPN ASA
- Опыт с конфигурацией платформы Identity Services Engine (ISE)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Microsoft Windows 7
- Программное обеспечение Cisco ASA, Версия 9. 3.2 и более поздние версии
- Cisco ISE, Выпуск 1.2 и позже

Общие сведения

Факторы клиента Secure Mobility Client AnyConnect

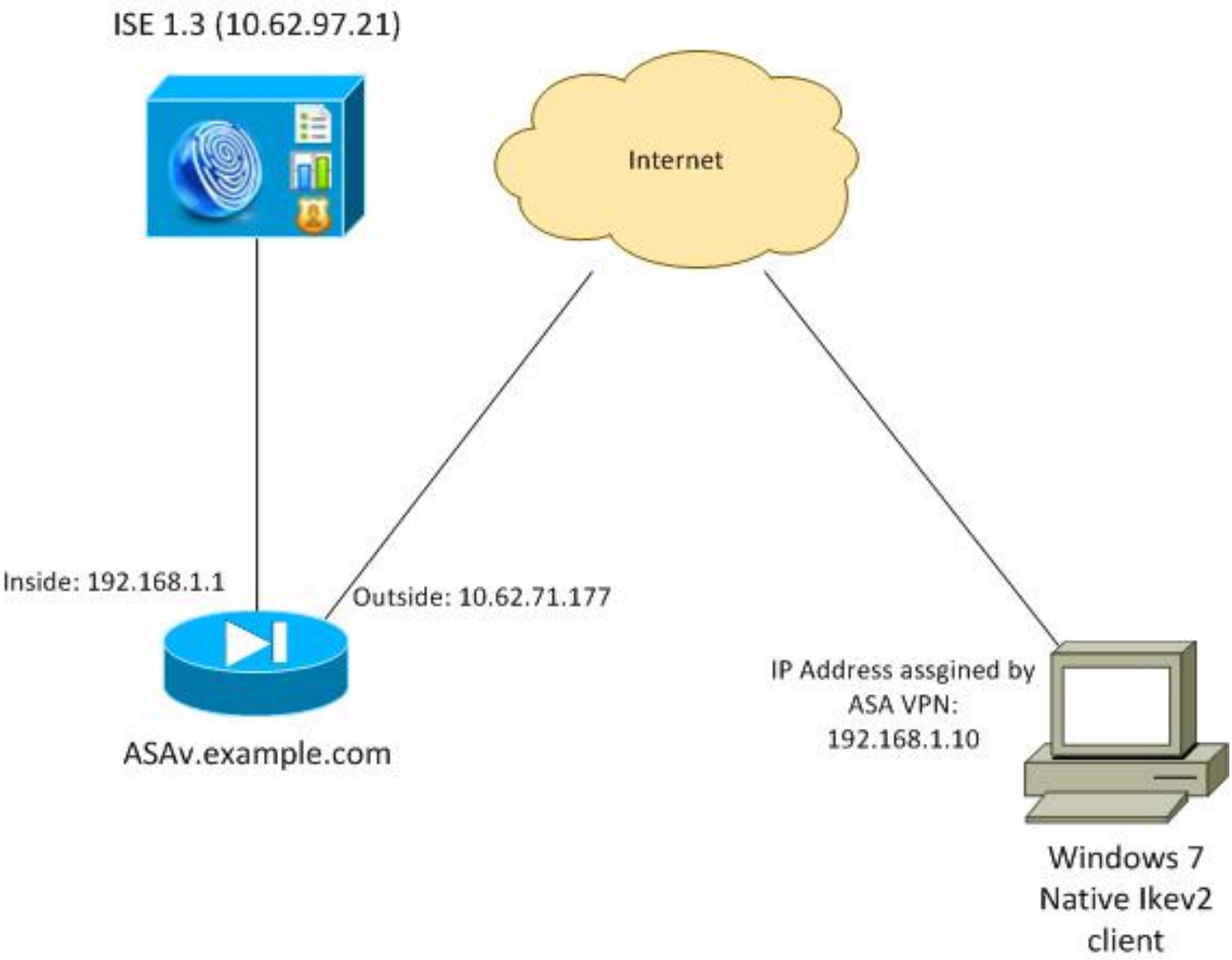
Клиент собственных окон IKEv2 не поддерживает разделение туннеля (нет никаких атрибутов OTBETA CONF, которые могли быть приняты клиентом Windows 7), таким образом, единственная возможная политика с клиентом Microsoft должна туннелировать весь трафик (0/0 селекторы трафика). Если существует потребность в определенной политике раздельных туннелей, AnyConnect должен использоваться.

AnyConnect не поддерживает стандартизированные методы EAP, которые завершены на AAA-сервере (PEAP, Transport Layer Security). Если существует потребность завершить сеансы EAP на AAA-сервере тогда, клиент Microsoft может использоваться.

Настройка

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети



ASA настроен для аутентификации с сертификатом (клиент должен доверять тому сертификату). Клиент Windows 7 настроен для аутентификации с EAP (PEAP EAP).

ASA действует как Шлюз VPN, завершающий сеанс IKEv2 от клиента. ISE действует как AAA-сервер, завершающий сеанс EAP от клиента. Пакеты EAP инкапсулируются в пакетах IKE_AUTH для трафика между клиентом и ASA (IKEv2) и затем в Пакетах RADIUS для трафика аутентификации между ASA и ISE.

Сертификаты

Microsoft Certificate Authority (CA) использовался для генерации сертификата для ASA. Требования сертификата, чтобы быть принятыми собственным клиентом Windows 7:

- Расширение расширенного использования ключа (EKU) должно включать Проверку подлинности сервера (обработайте "Web-сервер" по шаблону, использовался в том примере).
- Subject-Name должен включать Полное доменное имя (FQDN), которое будет использоваться клиентом для соединения (в данном примере ASAv. пример. com).

Для получения дополнительной информации на клиенте Microsoft, посмотрите Устранение проблем VPN-подключения IKEv2.

Примечание: Android 4.x более строг и требует корректного Альтернативного имени субъекта согласно RFC 6125. Для получения дополнительной информации для Android, см. IKEv2 от Android strongSwan до Cisco IOS с EAP и Аутентификацией RSA.

Для генерации запроса подписи сертификата на ASA эта конфигурация использовалась:

```
hostname ASAv
domain-name example.com

crypto ca trustpoint TP
enrollment terminal

crypto ca authenticate TP
crypto ca enroll TP
```

ISE

Шаг 1. Добавьте ASA к сетевым устройствам на ISE.

Выберите **Administration> Network Devices**. Установите предварительно разрешенный пароль, который будет использоваться ASA.

Шаг 2. Создайте имя пользователя в локальном хранилище.

Выберите **Administration>> Users Identities**. Создайте имя пользователя как требуется.

Все другие параметры настройки позволены по умолчанию для ISE аутентифицировать оконечные точки с PEAP EAP (Защищенный Расширяемый протокол аутентификации).

ASA

Конфигурация для удаленного доступа подобна для IKEv1 и 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
```

Так как Windows 7 передает адрес типа ID IKE в пакете IKE_AUTH, **DefaultRAGroup** должен использоваться, чтобы удостовериться, что соединение приземляется на корректную туннельную группу. ASA аутентифицируется с сертификатом (локальная проверка подлинности) и ожидает, что клиент будет использовать EAP (удаленная аутентификация). Кроме того, ASA должен в частности отправить идентификационный запрос EAP для клиента для отвечания идентификационным ответом EAP (идентичность запроса).

```
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
```

Наконец, IKEv2 должен быть включен, и корректный сертификат используется.

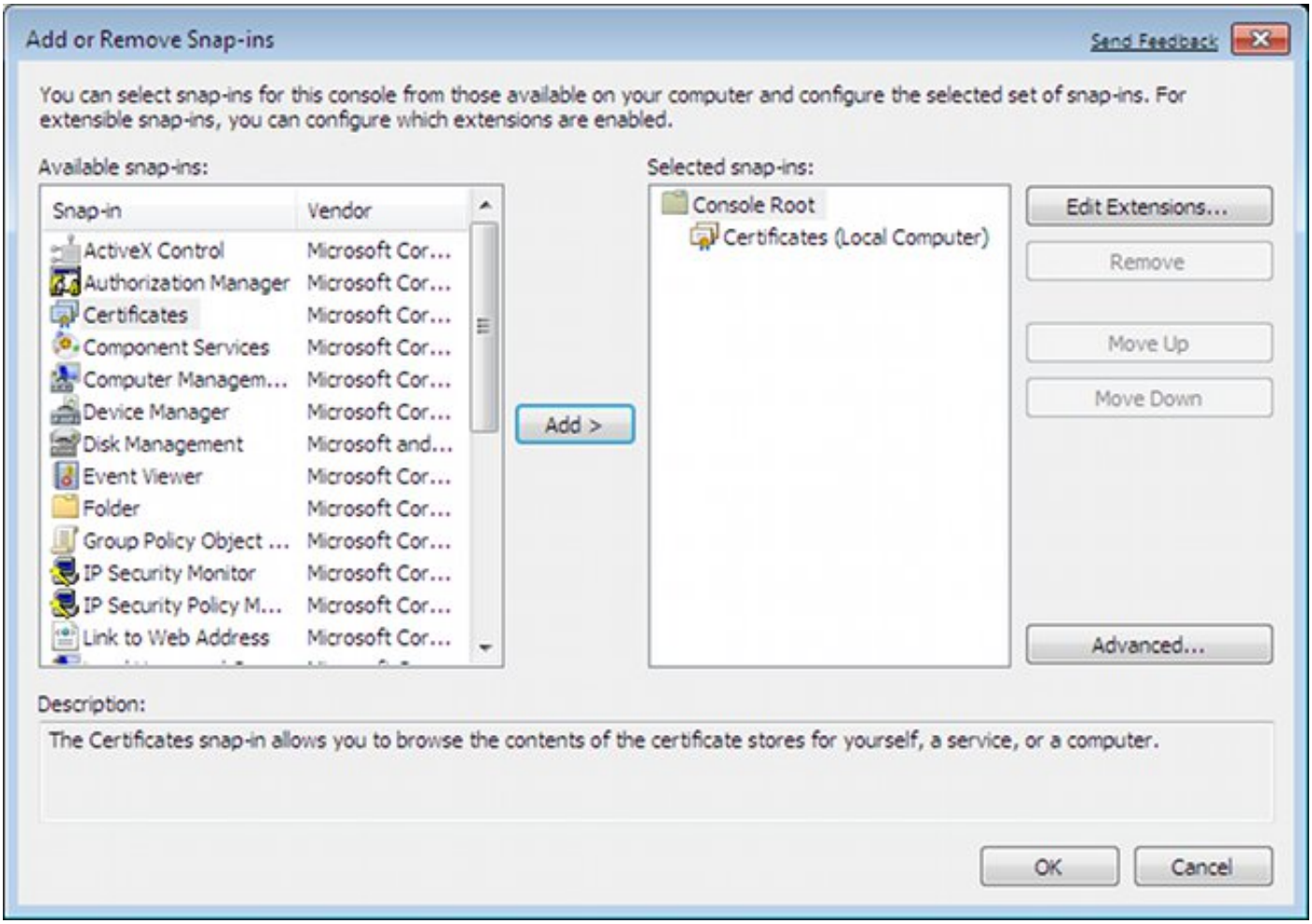
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Windows 7

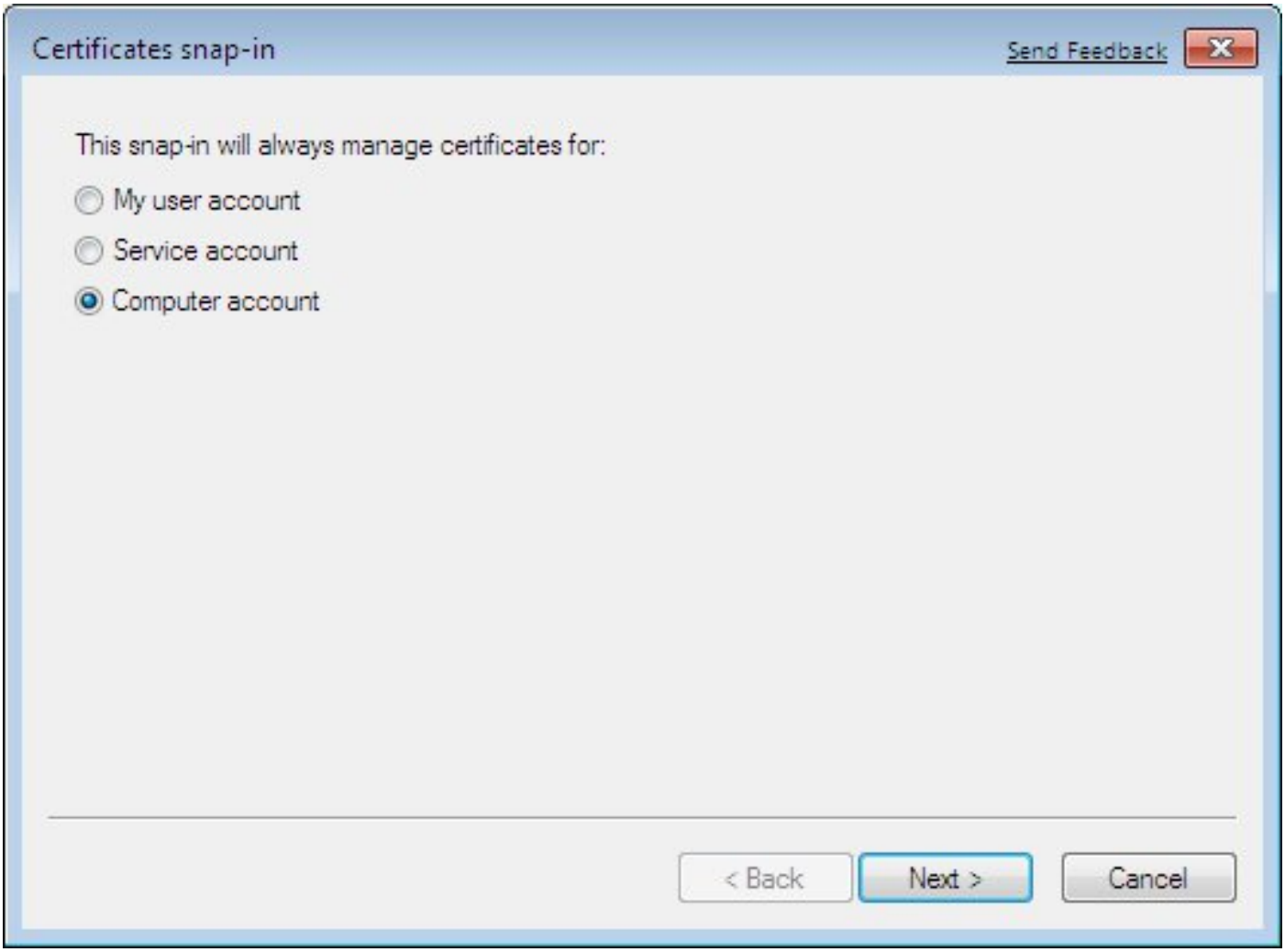
Шаг 1. Установите сертификат CA.

Для доверия сертификату, представленному ASA, Windows - клиент должен доверять его CA., Что сертификат CA должен быть добавлен к компьютерному хранилищу сертификата (не пользовательское хранилище). Windows - клиент использует компьютерный магазин для проверки сертификата IKEv2.

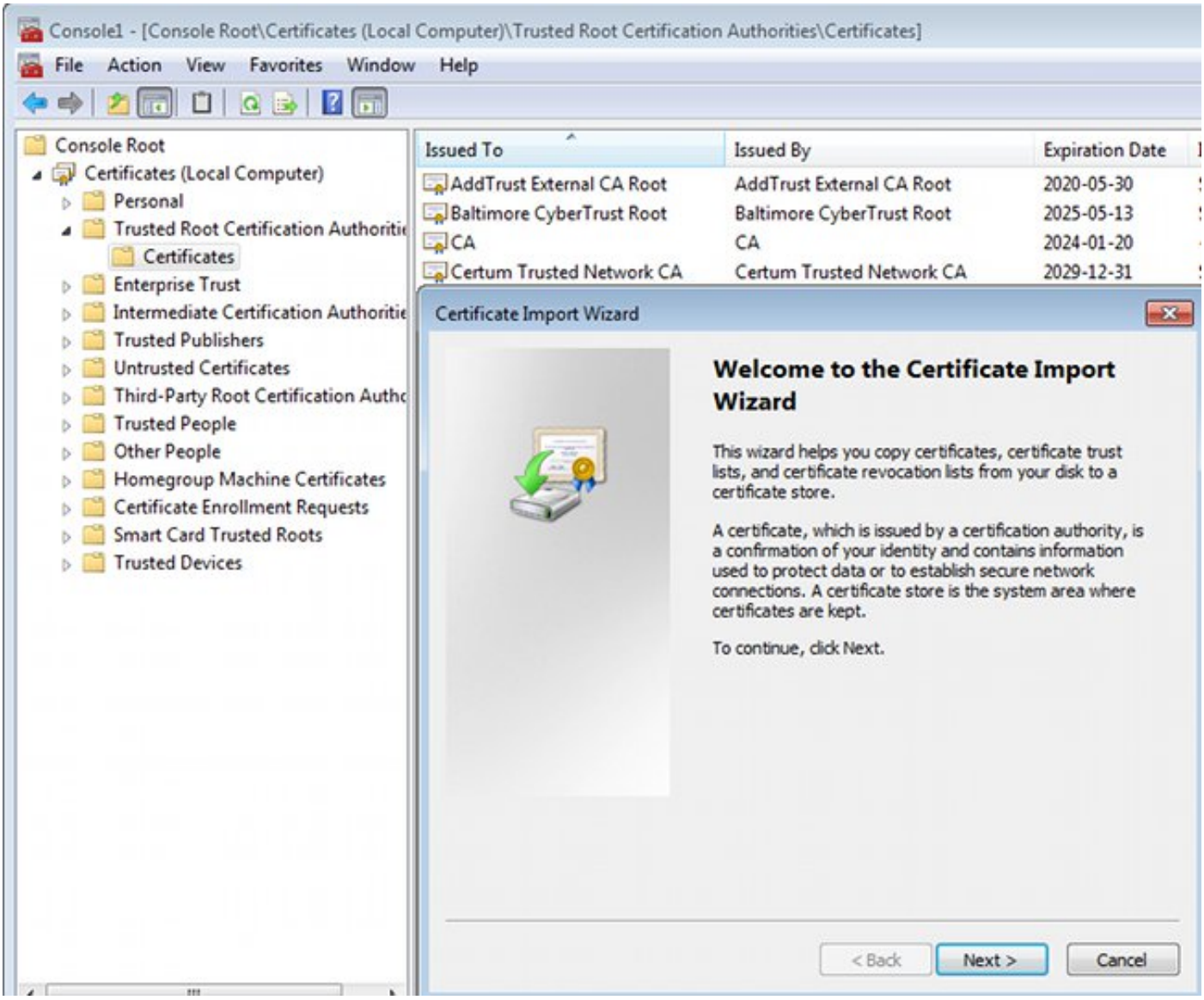
Для добавления CA выберите **MMC> Add или Remove Snap-ins> Certificates**.



Нажмите кнопку с зависимой фиксацией **Учетной записи компьютера**.



Импортируйте CA к полномочиям сертификата доверенного корня.

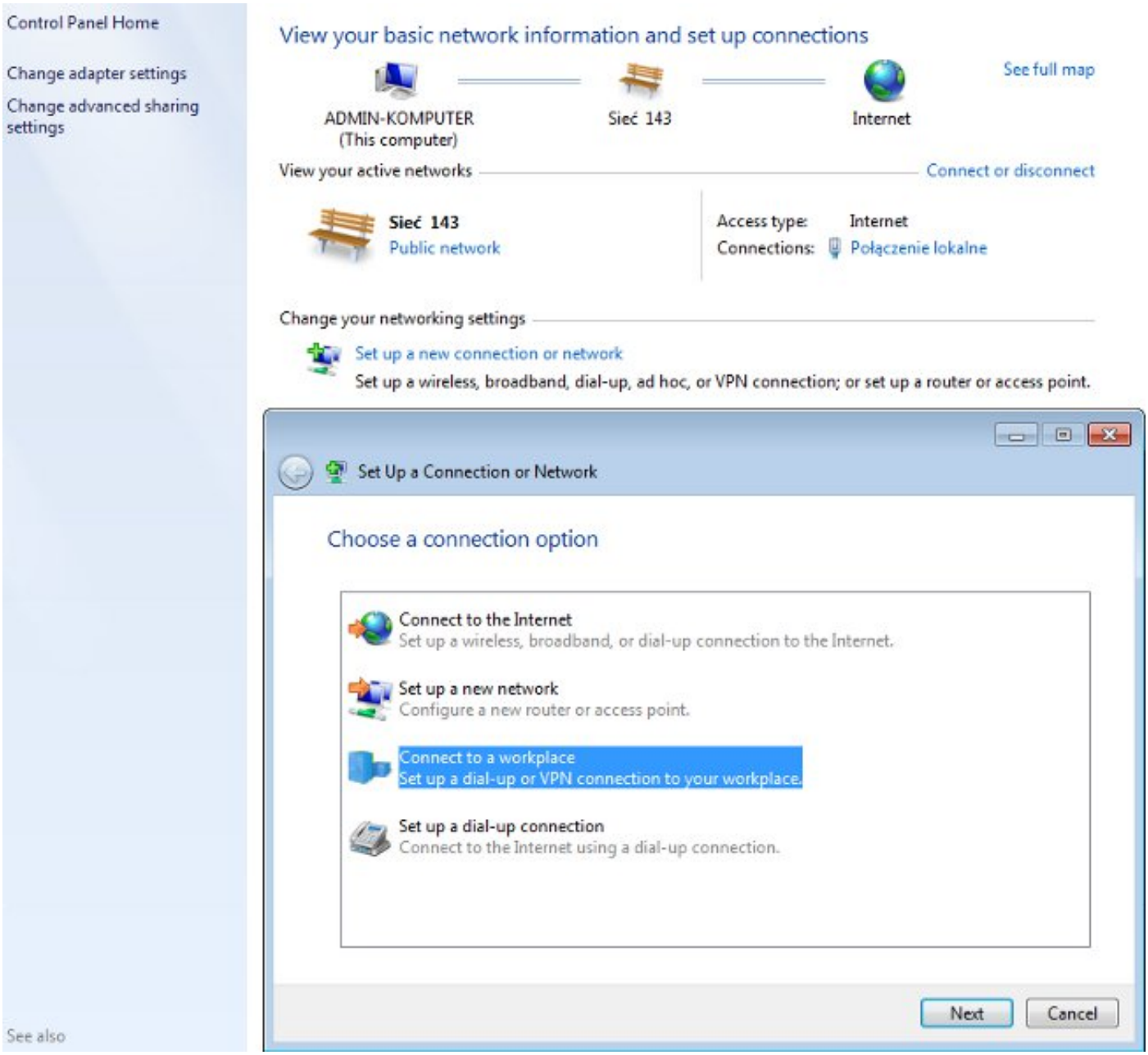


Если Windows - клиент не в состоянии проверить сертификат, представленный ASA, он сообщает:

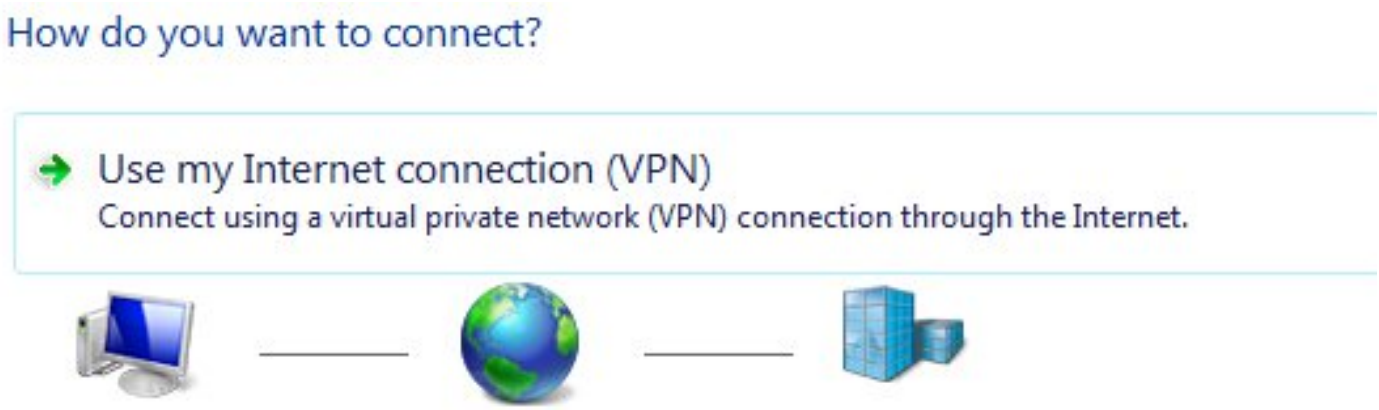
```
tunnel-group DefaultRAGroup general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy AllProtocols
tunnel-group DefaultRAGroup ipsec-attributes
 ikev2 remote-authentication eap query-identity
 ikev2 local-authentication certificate TP
```

Шаг 2. Настройте VPN-подключение.

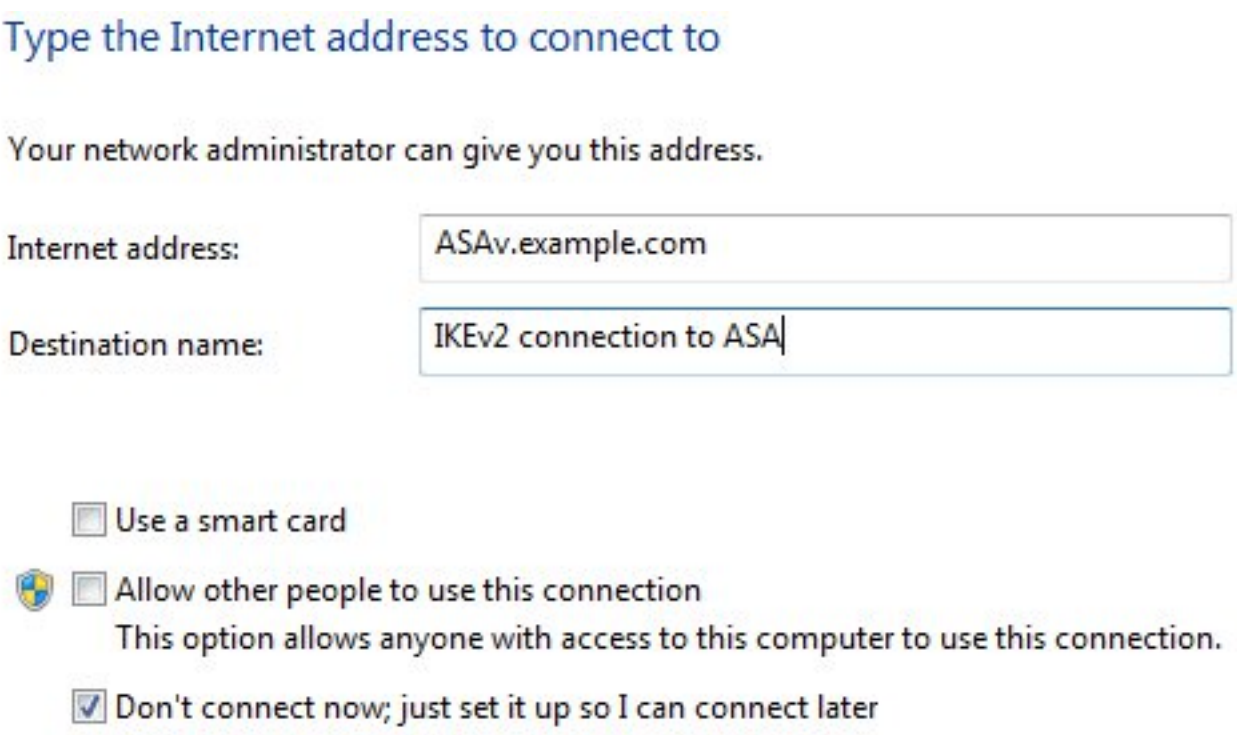
Для настройки VPN-подключения от Сети и Совместного использования Центра, выберите **Connect к рабочему месту** для создания VPN-подключения.



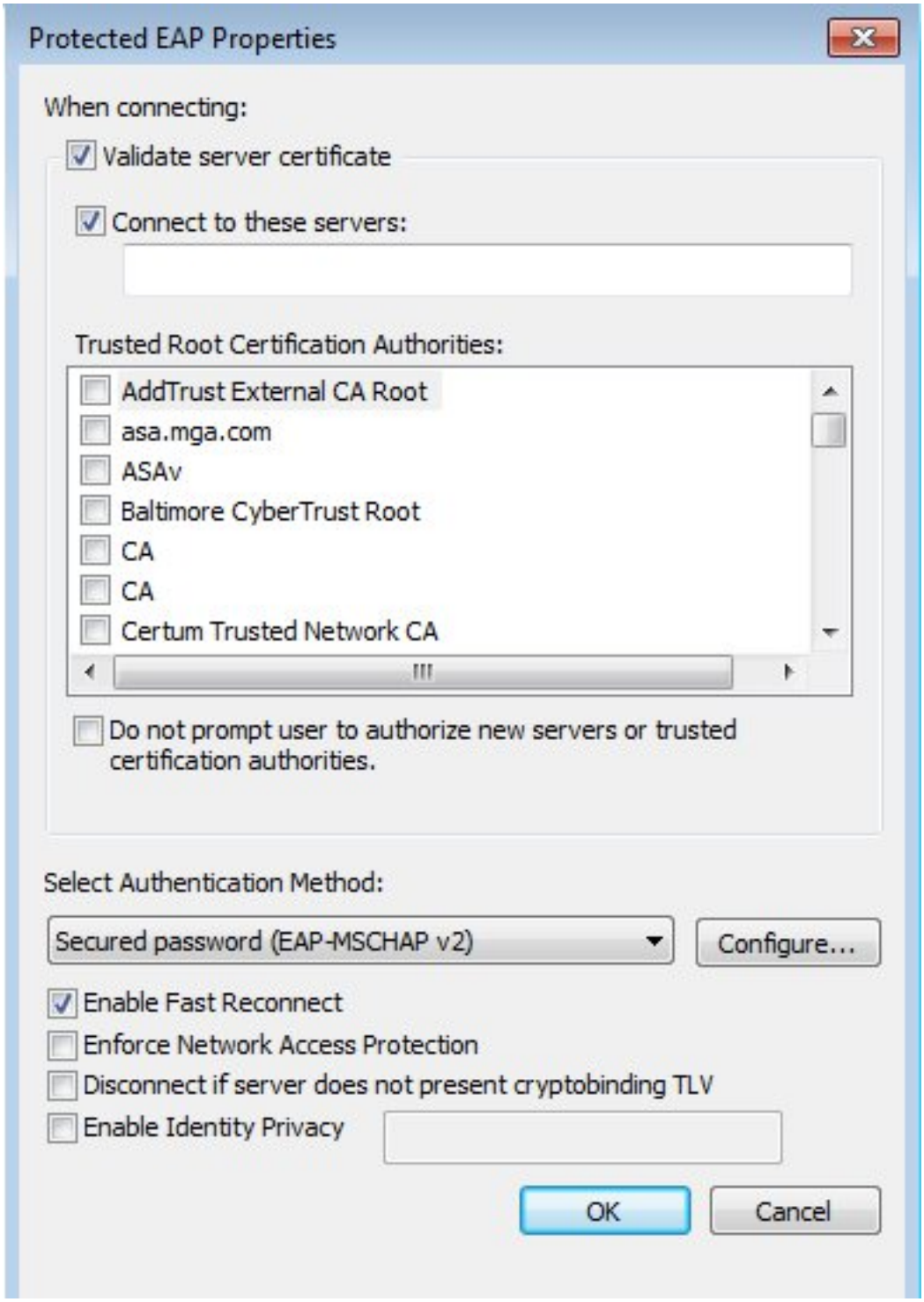
Выберите **Use мое Интернет-соединение (VPN)**.



Настройте адрес с ASA FQDN. Удостоверьтесь, что это правильно решено Сервером доменных имен (DNS).



При необходимости отрегулируйте свойства (такие как проверка достоверности сертификата) на Защищенном Окне свойств EAP.



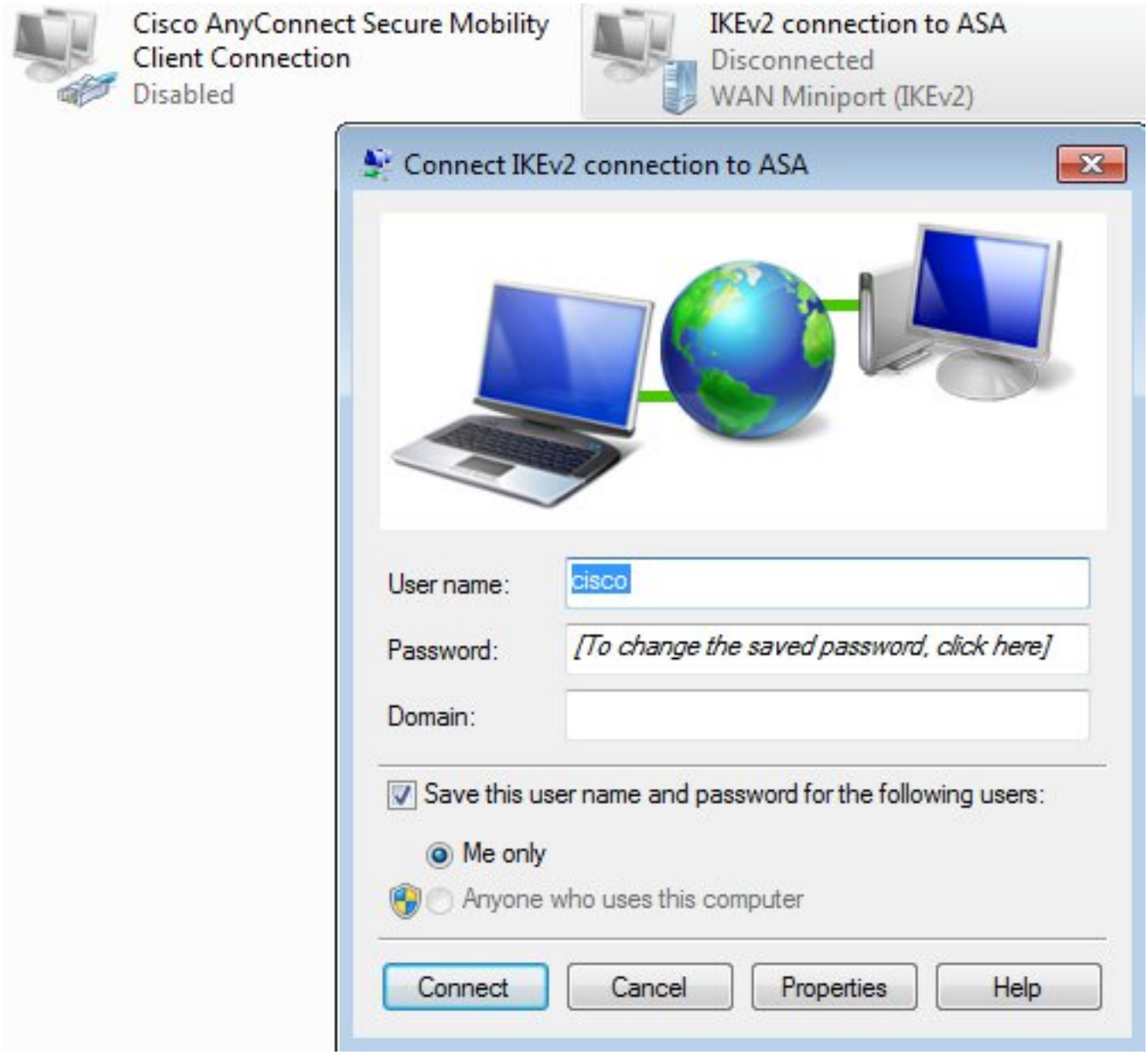
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

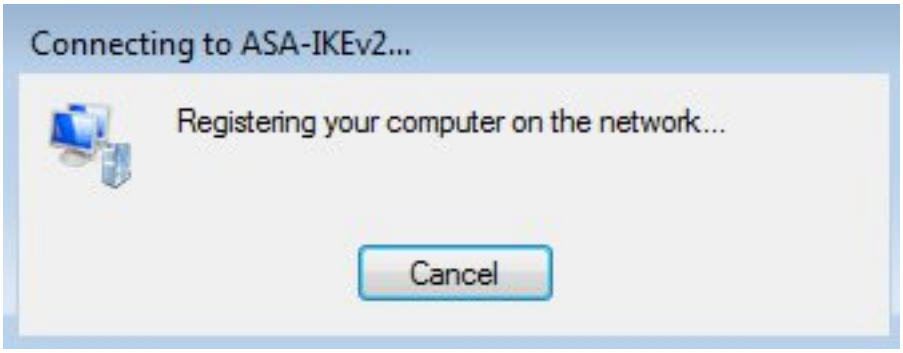
Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show . Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Windows - клиент

Когда вы соединитесь, введите свои учетные данные.



После успешной аутентификации применена конфигурация IKEv2.



Сеанс находится в рабочем состоянии.

Таблица маршрутизации была обновлена с маршрутом по умолчанию с использованием нового интерфейса с низким значением метрики.

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

Журналы

После успешной аутентификации отчёты о 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
```

Журналы ISE указывают на успешную аутентификацию с проверкой подлинности по умолчанию и правилами авторизации.

Подробные данные указывают на метод 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

Отладки на ASA

Самые важные отладки включают:

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

Пакет IKE_SA_INIT, полученный ASA (включает предложения IKEv2 и обмен ключами для 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
.....
```

Ответ IKE_SA_INIT инициатору (включает предложения IKEv2, обмен ключами для DH и запрос сертификата):

```
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 для клиента с ID IKE, запросом сертификата, предложил наборы преобразований, запрошенную конфигурацию и селекторы трафика:

```
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):
```

Ответ IKE_AUTH от ASA, который включает идентификационный запрос EAP (первый пакет с расширениями EAP). Тот пакет также включает сертификат (если нет никакого корректного сертификата на ASA существует сбой):

```
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]
```

Ответ EAP, полученный ASA (длина 5, информационное наполнение: 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
```

Затем несколькими пакетов обмениваются как часть PEAP EAP. Наконец успех EAP получен ASA и передан соискателю:

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

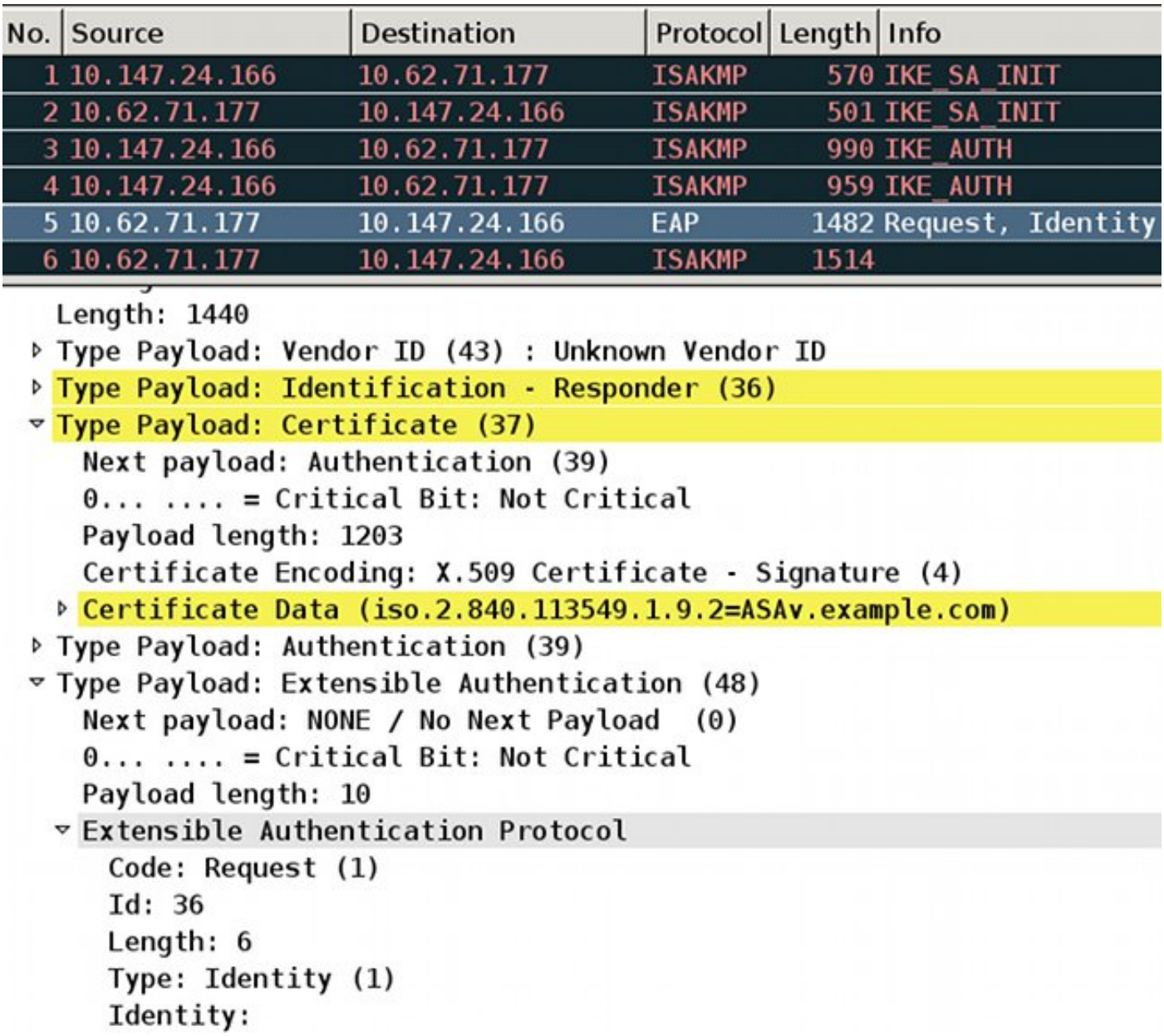
Аутентификация однорангового узла успешна:

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

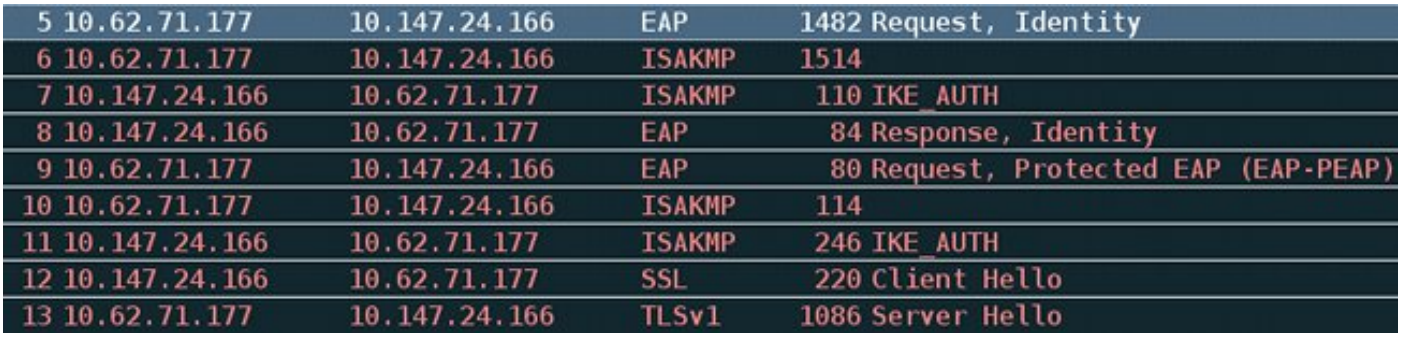
И сеанс VPN закончен правильно.

Пакетный уровень

Идентификационный запрос EAP инкапсулируется в "Расширенной проверке подлинности" IKE_AUTH, передают ASA. Наряду с идентификационным запросом, передаются IKE_ID и сертификаты.

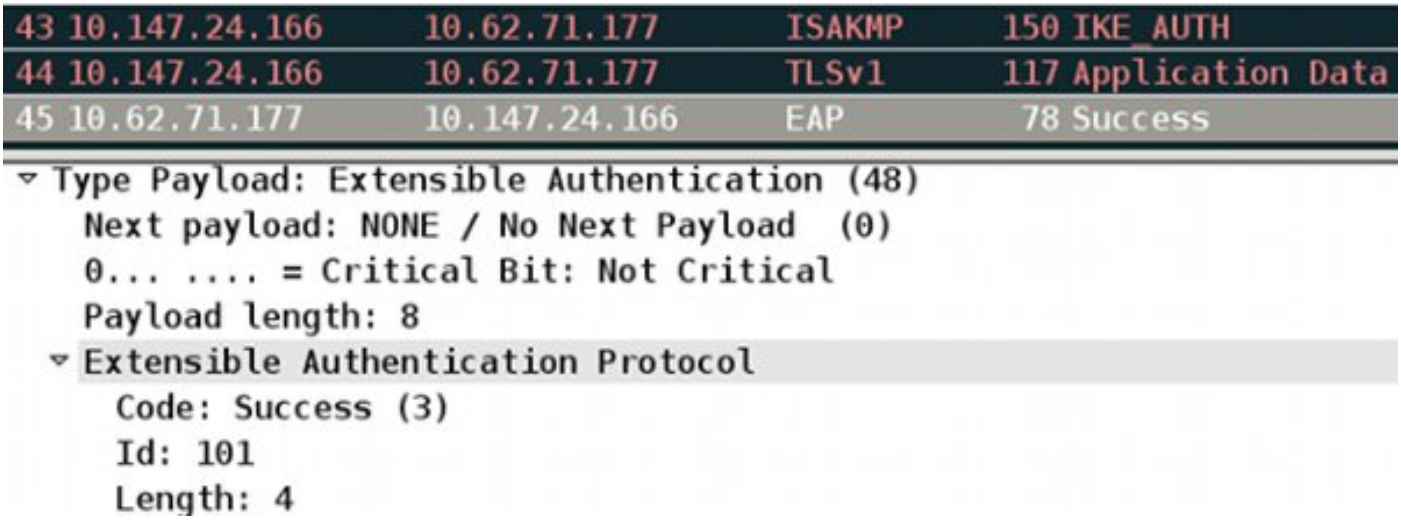


Все последующие пакеты EAP инкапсулируются в IKE_AUTH. После того, как соискатель подтверждает метод (PEAP EAP), он начинает создавать туннель Уровня защищенных сокетов (SSL), который защищает сеанс MSCHAPv2, используемый для аутентификации.



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

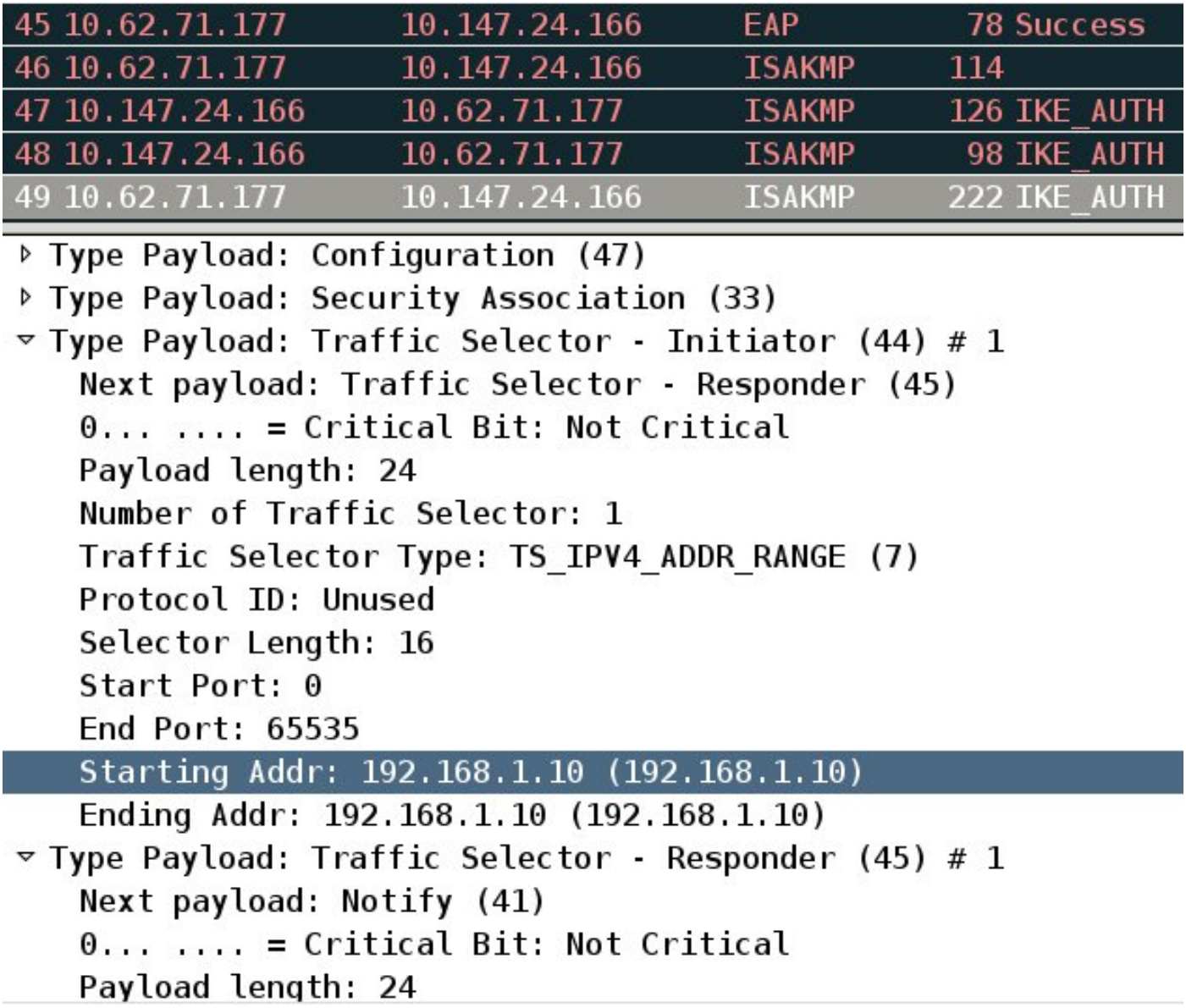
После того, как несколькими пакетов обмениваются, ISE подтверждает успех.



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
```

Сеанс IKEv2 завершен ASA, окончательная конфигурация (ответ конфигурации со значениями, такими как назначенный IP - адрес), наборы преобразований, и селекторы трафика выдвинуты клиенту VPN.



Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Руководство конфигурации интерфейса командой строки VPN серии Cisco ASA, 9.3
- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.2
- Cisco Systems – техническая поддержка и документация