AnyConnect по IKEv2 к ASA с AAA и проверкой подлинности сертификата

Содержание

Введение

Этот документ описывает, как подключить ПК с устройством адаптивной защиты Cisco (ASA) с использованием IPsec AnyConnect (IKEv2), а также аутентификация Аутентификации, авторизации и учета (AAA) и сертификат.

> **Примечание:** Пример, который предоставлен в этом документе , описывает только соответствующие части, которые используются для получения соединения IKEv2 между ASA и AnyConnect. Пример полной конфигурации не предоставлен. Конфигурация Технологии NAT или access-list не описывается или требуется в этом документе.

Подготовьте к соединению

В этом разделе описываются perparations, которые требуются, прежде чем можно будет подключить ПК с ASA.

Сертификаты с надлежащим EKU

Следует отметить, что даже при том, что это не требуется для ASA и комбинации AnyConnect, RFC требует, чтобы сертификаты имели расширенное использование ключа (EKU):

- Сертификат для ASA должен содержать **подлинный сервером** EKU.
- Сертификат для ПК должен содержать **клиентско-подлинный** EKU.

  Примечание: Маршрутизатор IOS с пересмотром новейшего ПО может разместить EKU на сертификаты.

Конфигурация на ASA

В этом разделе описываются конфигурации ASA, которые требуются, прежде чем соединение происходит.

> **Примечание:** Cisco Adaptive Security Device Manager (ASDM) позволяет вам создавать базовую конфигурацию только несколькими щелчками. Cisco рекомендует использовать ее во избежание ошибок.

Конфигурация криптокарты

Вот пример конфигурации криптокарты:

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

Предложения по ipsec

Вот пример конфигурации предложения по Ipsec:

```
crypto ipsec ikev2 ipsec-proposal secure
 protocol esp encryption aes 3des
 protocol esp integrity sha-1
crypto ipsec ikev2 ipsec-proposal AES256-SHA
 protocol esp encryption aes-256
 protocol esp integrity sha-1
```

Политика IKEv2

Вот пример конфигурации политики IKEv2:

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
prf sha
```

```
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
```

Сервисы клиента и сертификат

Необходимо включить сервисы клиента и сертификаты на корректном интерфейсе, который является внешним интерфейсом в этом случае. Вот пример конфигурации:

```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint OUTSIDE
ssl trust-point OUTSIDE outside
```

> **Примечание:** Та же точка доверия также назначена для Уровня защищенных сокетов (SSL), который предназначается и требуется.

Включите профиль AnyConnect

Необходимо включить профиль AnyConnect на ASA. Вот пример конфигурации:

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.5080-k9.pkg 1 regex "Windows NT"
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect enable
tunnel-group-list enable
```

Имя пользователя, групповая политика и туннельная группа

Вот пример конфигурации для основного имени пользователя, групповой политики и туннельной группы на ASA:

```
group-policy GroupPolicy_AC internal
group-policy GroupPolicy_AC attributes
 dns-server value 4.2.2.2
```

```
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value cisco.com
webvpn
anyconnect profiles value Anyconnect type user
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
tunnel-group AC type remote-access
tunnel-group AC general-attributes
address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 authentication aaa certificate
 group-alias AC enable
 group-url https://bsns-asa5520-1.cisco.com/AC enable
 without-csd
```

Профиль AnyConnect

Вот профиль в качестве примера с соответствующими частями, показанными полужирным:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
 "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false
 </AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="true">Automatic
 </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>bsns-asa5520-1</HostName>
<HostAddress>bsns-asa5520-1.cisco.com</HostAddress>
```

```
<UserGroup>AC</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Вот некоторые важные замечания об этом примере конфигурации:

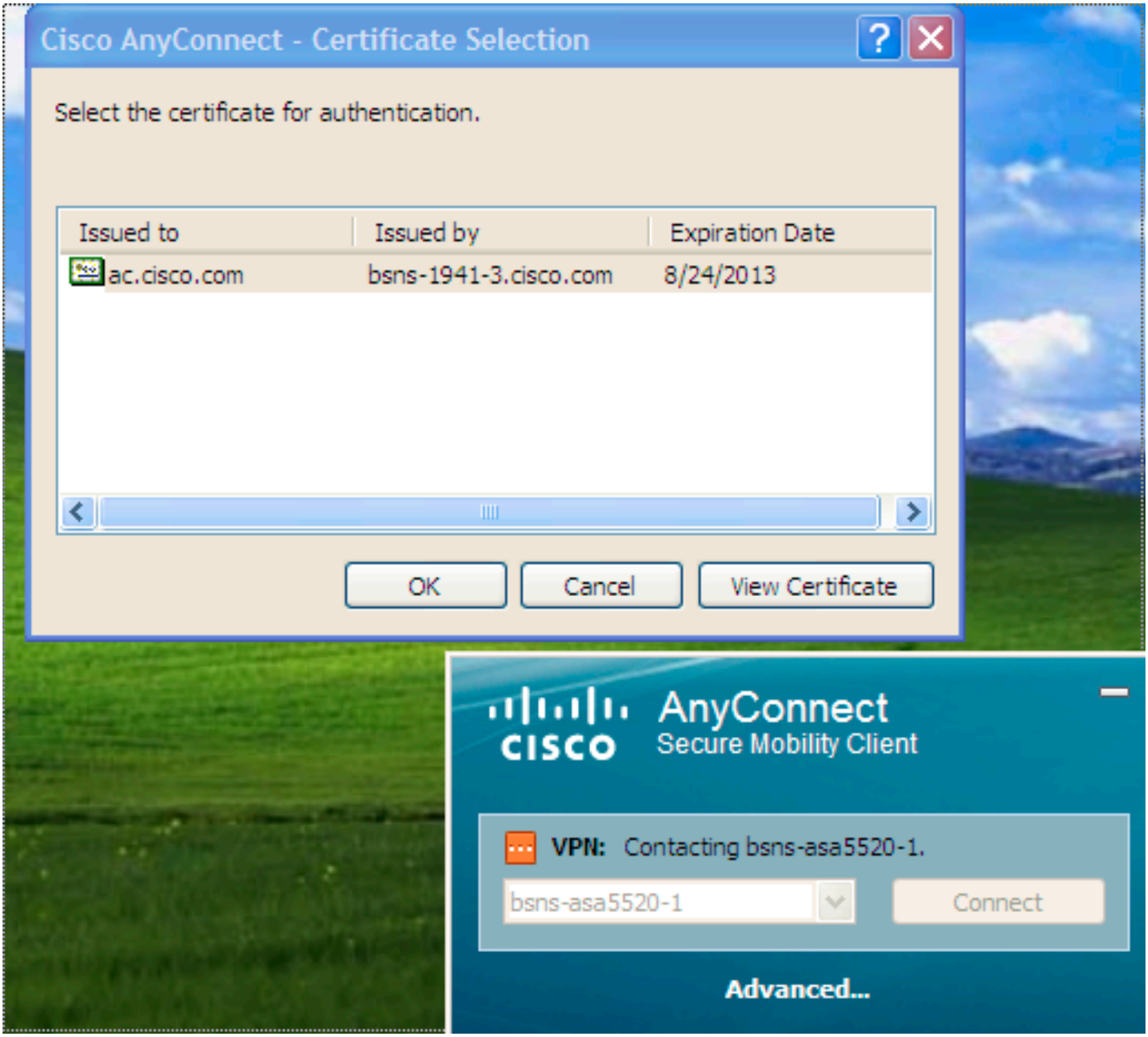
- При создании профиля HostAddress должен совпасть с Названием сертификата (CN) на сертификате, который используется для IKEv2. Введите **крипто-ikev2** команду **точки доверия удаленного доступа** для определения этого.
- UserGroup должен совпасть с названием tunnelgroup, на который падает соединение IKEv2. Если они не совпадают, связь часто прерывается, и отладки указывают на несоответствие группы Diffie-Hellman (DH) или подобного ложного отрицательного.

Сделайте соединение

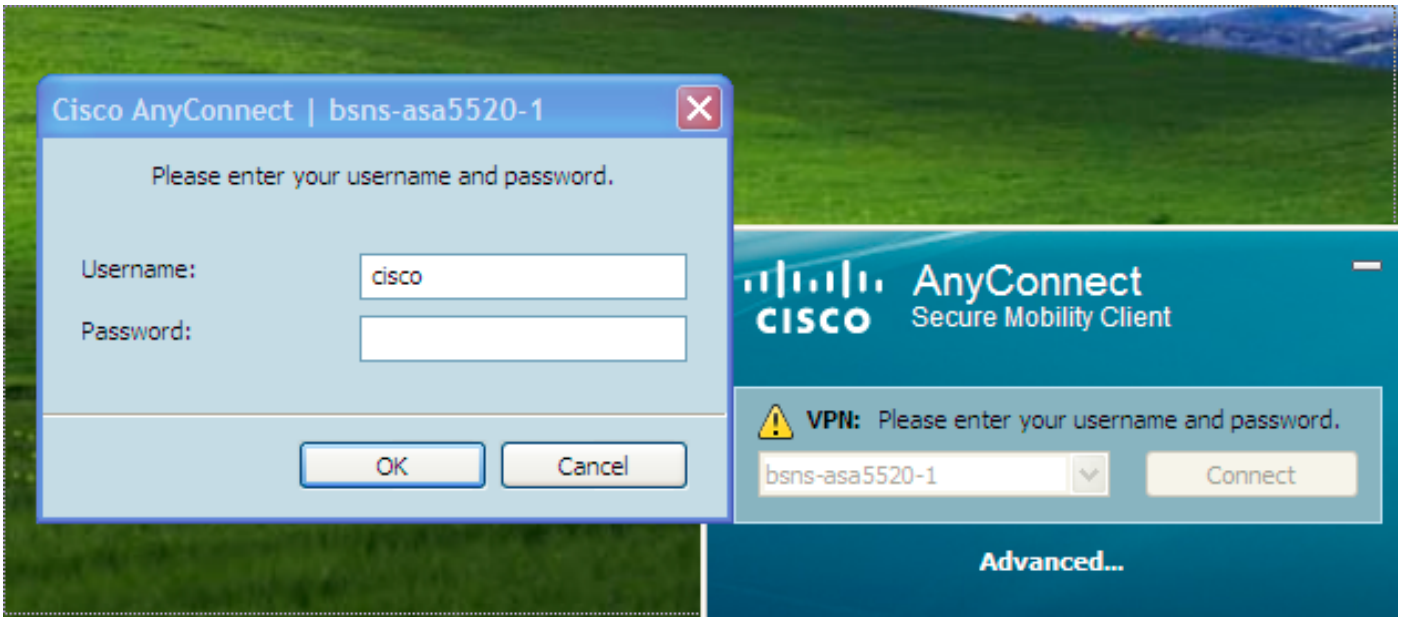
Когда профиль уже присутствует, этот раздел описывает соединение ПК К ASA.

> **Примечание:** Информацией, которую вы вводите в GUI для соединения является значение <hostname>, которое настроено в профиле AnyConnect. В этом случае **bsns-asa5520-1** введен, не завершенное Полное доменное имя (FQDN).

Когда вы сначала пытаетесь соединиться через AnyConnect, шлюз побуждает вас выбирать сертификат (если автоматический выбор сертификата отключен):

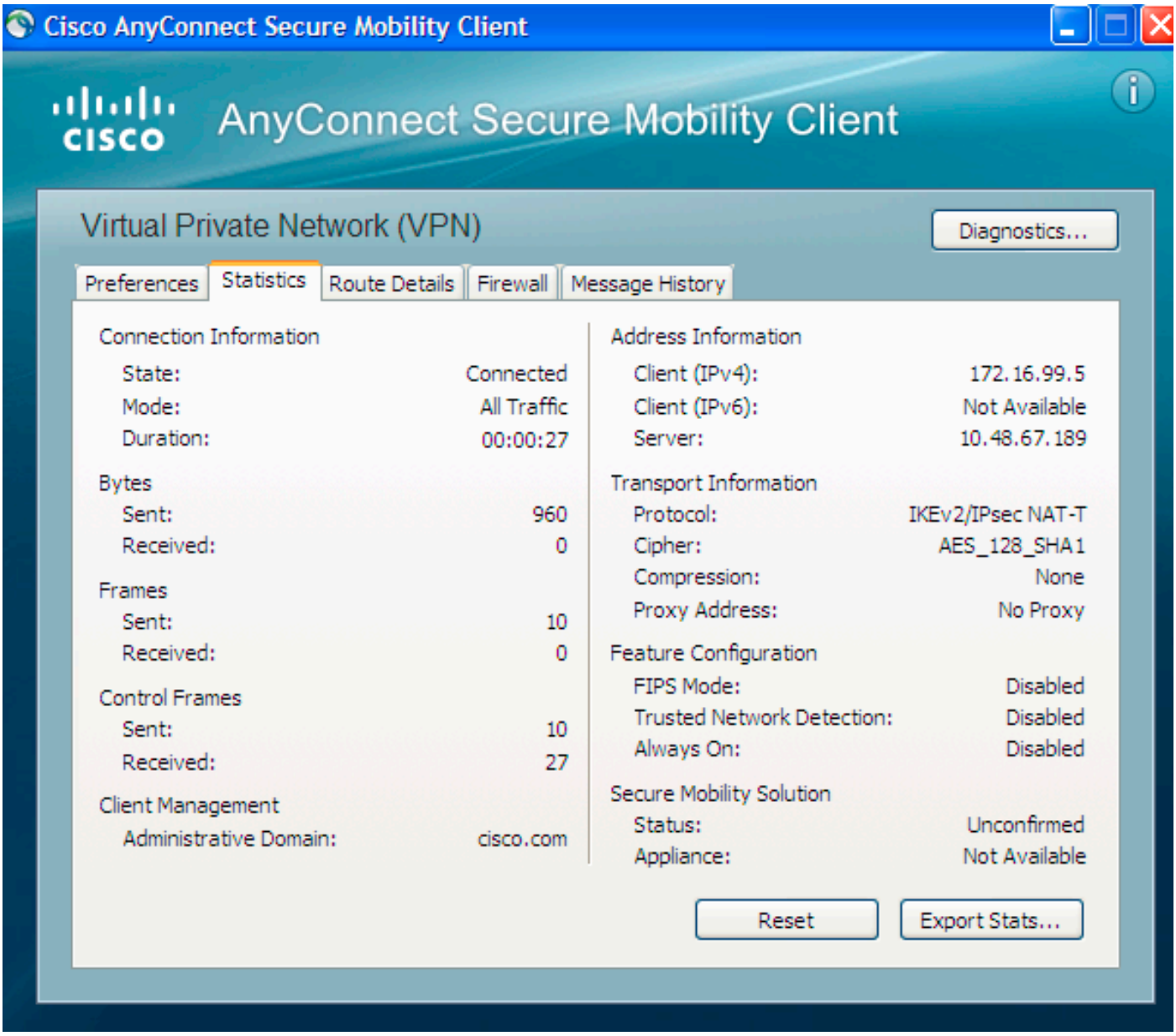


Необходимо тогда ввести Имя пользователя и пароль:



Однажды Имя пользователя и пароль приняты, соединение успешно, и статистика

AnyConnect может быть проверена:



Проверка на ASA

Введите эту команду в ASA, чтобы проверить, что соединение использует IKEv2, а также AAA и проверку подлинности сертификата:

```
bsns-asa5520-1# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed
Username : cisco Index : 6
Assigned IP : 172.16.99.5 Public IP : 1.2.3.4
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : AES256 AES128 Hashing : none SHA1 SHA1
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_AC Tunnel Group : AC
Login Time : 15:45:41 UTC Tue Aug 28 2012
Duration : 0h:02m:41s
```

```
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 6.1
Public IP : 1.2.3.4
Encryption : none Auth Mode : Certificate and userPassword
 Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client Type : AnyConnect
Client Ver : 3.0.08057
IKEv2:
Tunnel ID : 6.2
UDP Src Port : 60468 UDP Dst Port : 4500
Rem Auth Mode: Certificate and userPassword
 Loc Auth Mode: rsaCertificate
 Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86238 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
Client OS : Windows
IPsecOverNatT:
Tunnel ID : 6.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.99.5/255.255.255.255/0/0
Encryption : AES128 Hashing : SHA1\
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28638 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
```

Известные предупреждения

Это известные предупреждения и проблемы, которые отнесены к информации, которая описана в этом документе:

- IKEv2 и точки доверия SSL должны быть тем же.
- Cisco рекомендует использовать FQDN в качестве CN для сертификатов стороны ASA. Гарантируйте ссылку на тот же FQDN для <HostAddress> в профиле AnyConnect.
- Не забудьте вставлять значение <hostname> от профиля AnyConnect, когда вы соединитесь.
- Даже в конфигурации IKEv2, когда AnyConnect соединяется с ASA, он загружает профиль и двоичные обновления по SSL, но не IPsec.
- Соединение AnyConnect по IKEv2 к ASA использует AnyConnect EAP, собственный механизм, который позволяет более простую реализацию.