Развертывания FlexVPN: удаленный доступ AnyConnect IKEv2 с EAP-MD5

Содержание

Введение

Этот документ предоставляет пример конфигурации того, как установить Удаленный доступ на IOS с помощью инструментария FlexVPN.

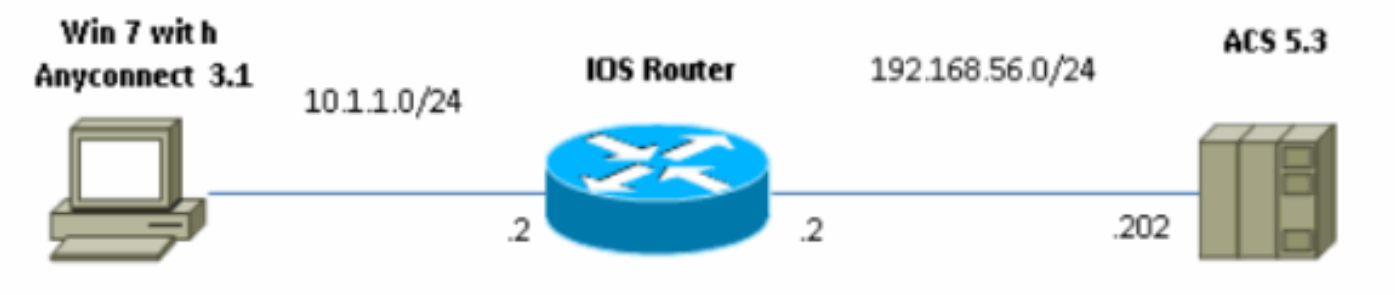
VPN для удаленного доступа позволяет конечным клиентам, использующим различные Операционные системы надежно соединяться с их Корпоративными или Домашними сетями через незащищенную среду, такими как Интернет. В представленном сценарии VPN-туннель завершается на маршрутизаторе Cisco IOS с помощью протокола IKEv2.

Этот документ показывает, как аутентифицировать и авторизовать пользователей, использующих Access Control Server (ACS) через метод EAP-MD5.

Предварительные условия

Схема сети

Маршрутизатор Cisco IOS имеет два интерфейса - один к ACS 5.3:



Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- ACS 5.3 с исправлением 6
- Маршрутизатор IOS с 15.2 (4) программное обеспечение M
- Windows 7 PC с AnyConnect 3.1.01065

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В IKEv1 XAUTH используется в фазе 1.5, можно сделать аутентификацию пользователей локально на маршрутизаторе IOS и удаленно использовании RADIUS/TACACS +. IKEv2 больше не поддерживает XAUTH и фазу 1.5. Это содержит встроенную поддержку EAP, которая сделана синфазный IKE_AUTH. Самое большое преимущество этого находится в дизайне IKEv2, и EAP является известным стандартом.

EAP поддерживает два режима:

- Туннелируя — EAP-TLS, EAP/PSK, PEAP EAP и т.д.
- Нетуннелируя — EAP-MSCHAPv2, EAP-GTC, EAP-MD5 и т.д.

В данном примере используется EAP-MD5 в нетуннелирующем режиме, потому что это - EAP внешний метод аутентификации, поддерживаемый в настоящее время в ACS 5.3.

EAP может только использоваться к опознавательному инициатору (клиент) респонденту

(IOS в этом случае).

Начальная конфигурация IOS

IOS - CA

В первую очередь, необходимо создать Центр сертификации (CA) и создать сертификат идентификации для Маршрутизатора IOS. Клиент проверит идентичность маршрутизатора на основе того Сертификата.

Конфигурация CA на IOS похожа:

```
crypto pki server CA
grant auto
hash sha1
eku server-auth client-auth
```

Необходимо помнить о Расширенном Ключевом Использовании (Для Аутентификации сервера было нужно для EAP для RSA-СИГНАЛА, вам также нужна Клиентская Аутентификация).

Включите CA с помощью **команды no shutdown** в CA. crypto pki server

IOS - Сертификат идентификации

Затем, включите Протокол SCEP (SCEP) для сертификата и настройте точку доверия.

```
ip http server
crypto pki trustpoint CA-self
enrollment url http://10.1.1.2:80
fqdn 10.1.1.2
ip-address 10.1.1.2
subject-name cn=10.1.1.2,ou=TAC
revocation-check none
eku request server-auth client-auth
```

Затем аутентифицируйте и зарегистрируйте сертификат:

```
(config)#crypto pki authenticate CA-self Certificate has the following attributes: Fingerprint
MD5: 741C671C 3202B3AE 6E05161C 694CA53E Fingerprint SHA1: 8C99513C 2198470F 7CB58FA2 32D8AA8D
FC31D1ED % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted.
R1(config)#crypto pki enroll CA-self % % Start certificate enrollment .. % Create a challenge
password. You will need to verbally provide this password to the CA Administrator in order to
revoke your certificate. For security reasons your password will not be saved in the
configuration. Please make a note of it. Password: Re-enter password: % The subject name in the
certificate will include: cn=10.1.1.2,ou=TAC % The subject name in the certificate will include:
10.1.1.2 % Include the router serial number in the subject name? [yes/no]: no % The IP address
in the certificate is 10.1.1.2 Request certificate from CA? [yes/no]: yes % Certificate request
sent to Certificate Authority % The 'show crypto pki certificate verbose CA-self' command will
show the fingerprint. R1(config)# *Dec 2 10:57:44.141: CRYPTO_PKI: Certificate Request
Fingerprint MD5: BF8EF4B6 87FA8162 9079F917 698A5F36 *Dec 2 10:57:44.141: CRYPTO_PKI:
Certificate Request Fingerprint SHA1: AC13FEA3 295F7AE6 7014EF60 784E33AF FD94C41D R1(config)#
*Dec 2 10:57:44.198: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

Если вы не хотите иметь подсказки в AnyConnect, помнят, что cn должен быть равен ИМЕНИ ХОСТА/IP-АДРЕСАМ, настроенному в профиле AnyConnect.

В данном примере, cn=10.1.1.2. Поэтому в AnyConnect 10.1.1.2 введен как IP-адрес сервера

в профиле xml AnyConnect.

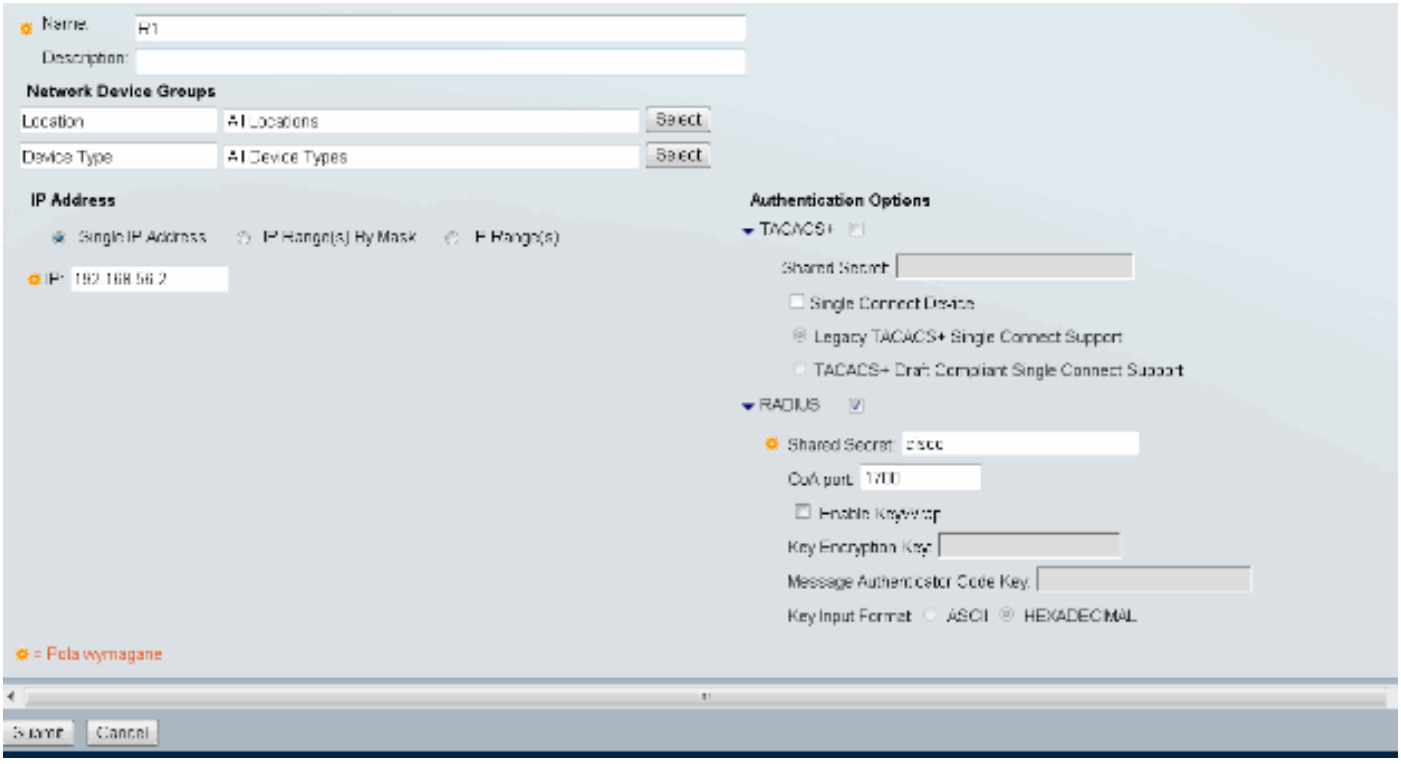
IOS - AAA и Конфигурация RADIUS

Необходимо настроить Радиус и аутентификацию AAA (проверка подлинности, авторизация и учет) и авторизацию:

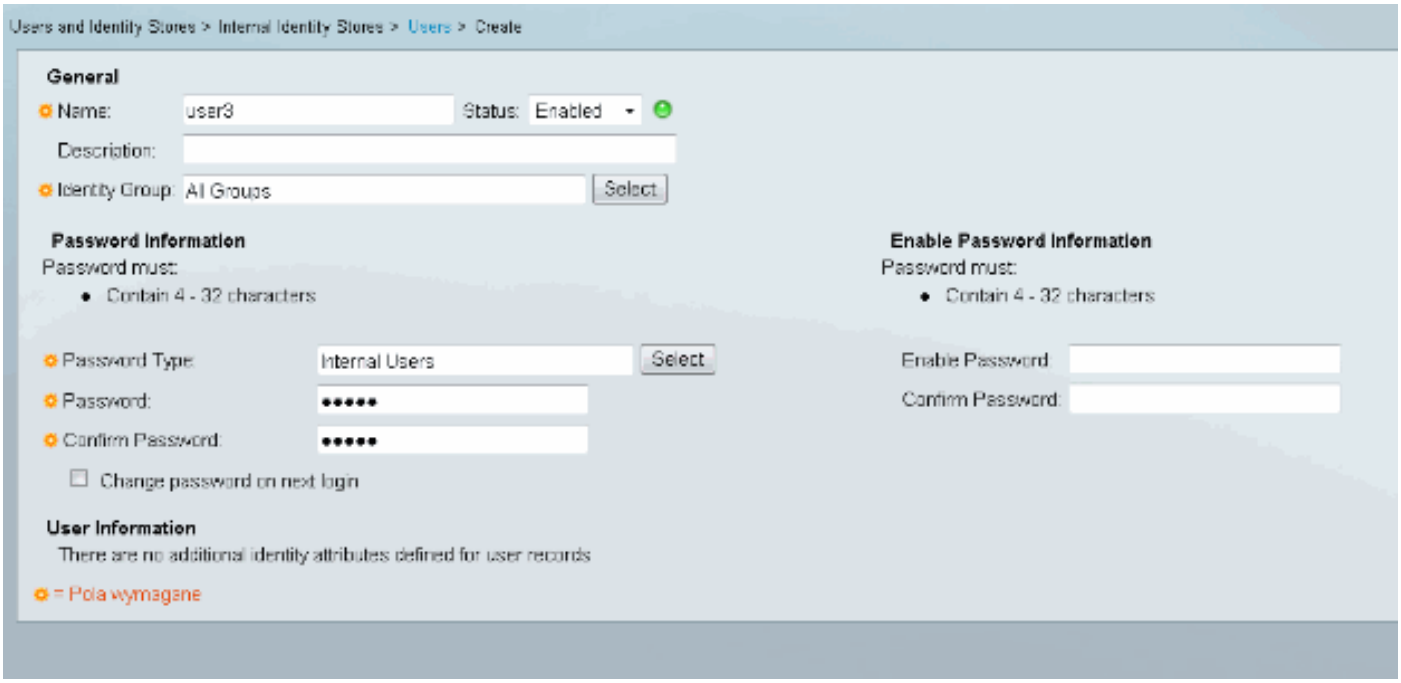
```
aaa new-model
radius-server host 192.168.56.202 key cisco
aaa group server radius SERV
server 192.168.56.202
aaa authentication login eap-list group SERV
aaa authorization network eap-list group SERV
```

Начальная конфигурация ACS

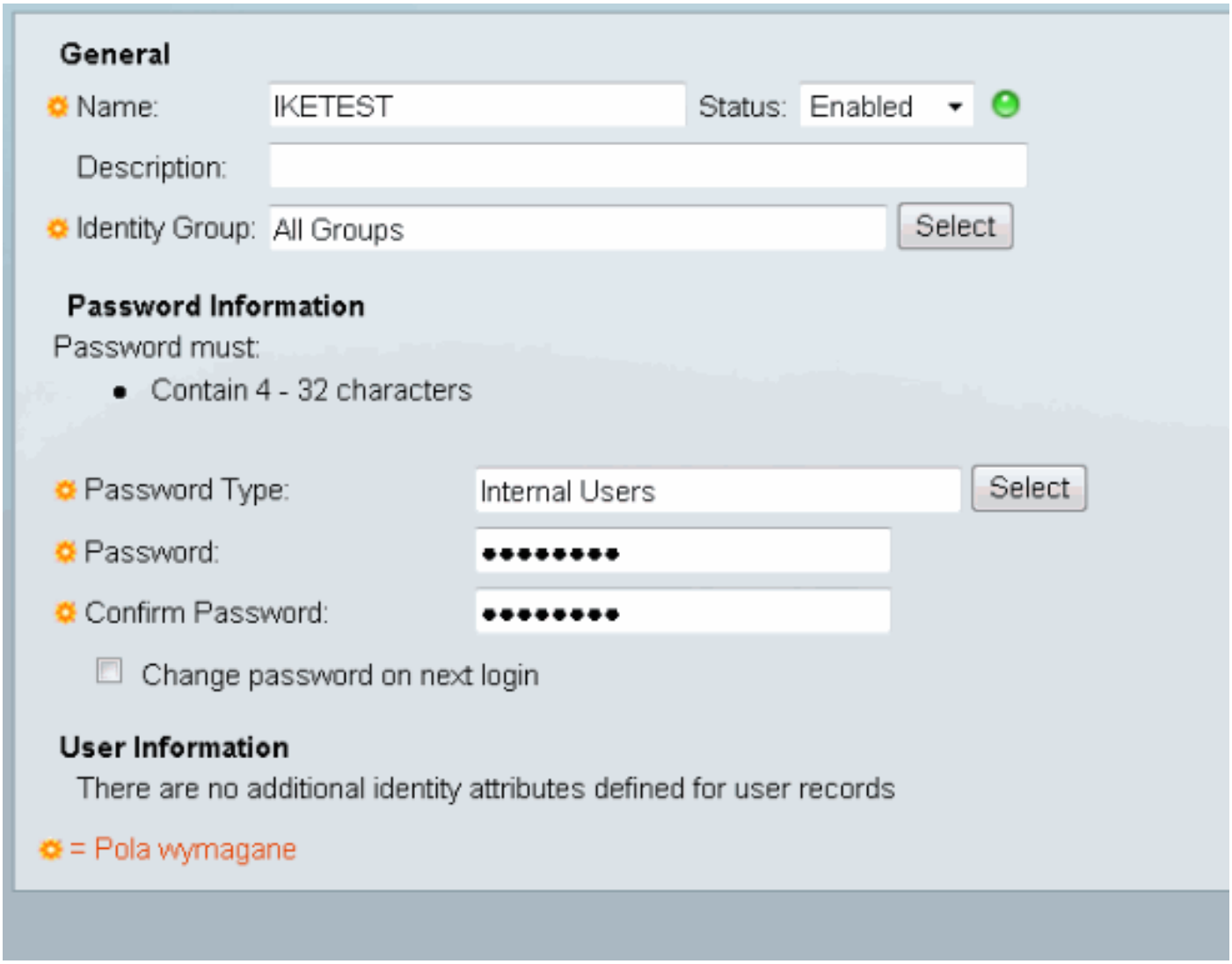
Во-первых, добавьте новое Сетевое устройство в ACS (Сетевые ресурсы>, Сетевые устройства и Клиенты AAA> Создают):



Добавьте пользователя (Пользователи и Идентификационные Хранилища>, Внутренний Идентификационный> Users Хранилищ> Создает):

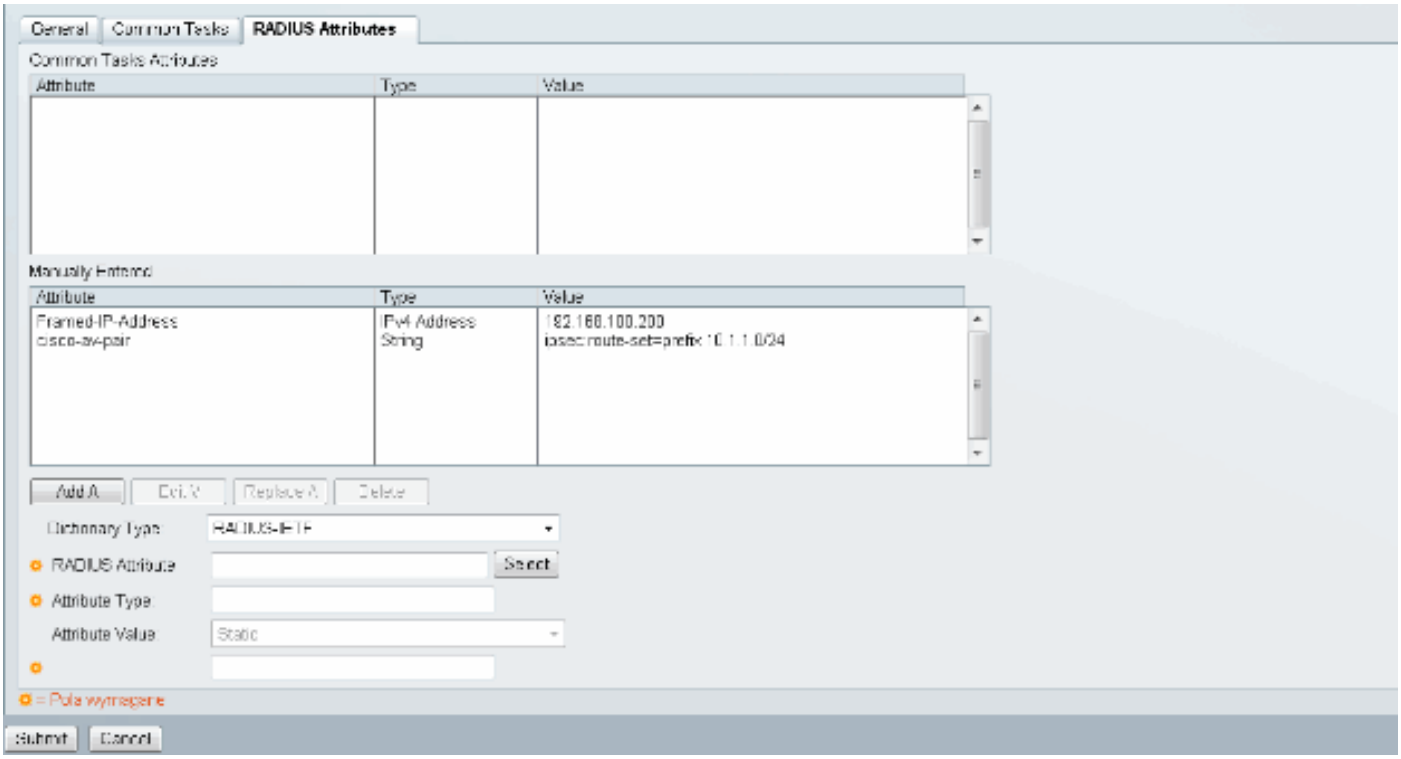


Добавьте пользователя для авторизации. В данном примере это - IKETEST. Пароль должен быть "Cisco", потому что это - по умолчанию, передаваемый IOS.

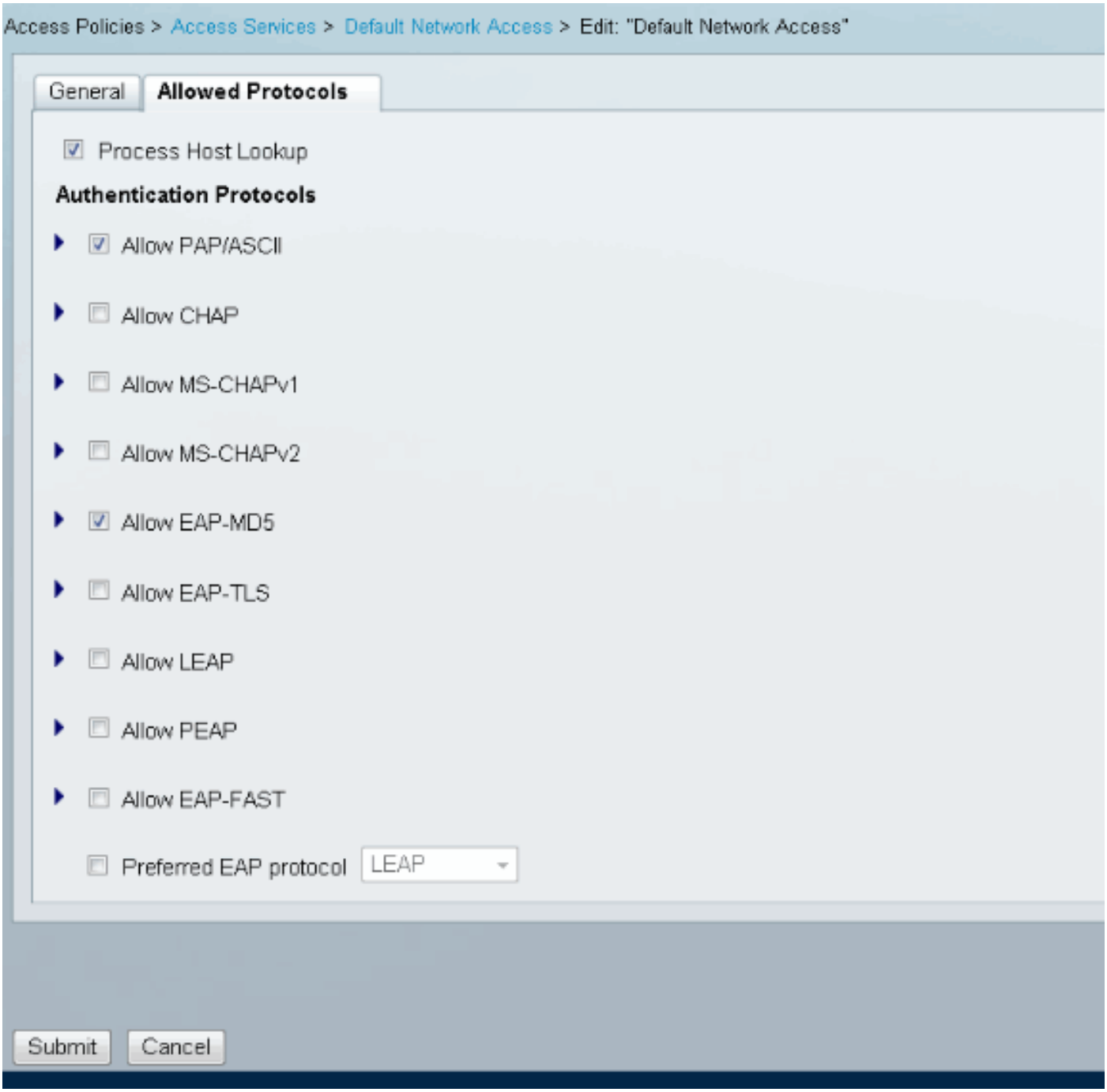


Затем, создайте профиль Авторизации для пользователей (Элементы политики> Авторизация и Разрешения> Доступ к сети>, Профили Авторизации> Создают).

В данном примере это называют ПУЛОМ. В данном примере пара значение-атрибут Разделения туннеля (как префикс) введена и Обрамленный IP-адрес как IP-адрес, который будет назначенным на подключенного клиента. Список всех поддерживаемых пар значение-атрибут может быть найден здесь: http://www. cisco . com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



Затем необходимо включить поддержку EAP-MD5 (для аутентификации) и PAP/ASCII (для авторизации) в Политике доступа. По умолчанию используется в данном примере (Политика доступа> Доступ к сети по умолчанию):



Создайте условие для в Политике доступа и назначьте профиль авторизации, который был создан. В этом случае условие для NDG:Location во Всех Местоположениях создано, таким образом для всех Проверок подлинности RADIUS, запрос предоставит Профиль Авторизации ПУЛА (Политика доступа> Службы доступа> Доступ к сети по умолчанию):

Должна существовать возможность для тестирования на маршрутизаторе IOS, если пользователь может аутентифицироваться должным образом:

```
R1#test aaa group SERV user3 Cisco123 new-code User successfully authenticated USER ATTRIBUTES
username 0 "user3" addr 0 192.168.100.200 route-set 0 "prefix 10.1.1.0/24"
```

Конфигурация IOS FlexVPN

Необходимо создать предложение IKEv2 и политику (вы не могли бы иметь к, обратиться к CSCtn59317). Политика создана только для одного из IP-адресов (10.1.1.2) в данном примере.

```
crypto ikev2 proposal PROP
encryption 3des
integrity sha1
group 2

crypto ikev2 policy 5
match address local 10.1.1.2
proposal PROP
```

Затем создайте профиль IKEV2 и Профиль IPSEC, который свяжет с Virtual-Template.

Удостоверьтесь, что вы выключаете свидетельство http url, как рекомендуется в руководстве по конфигурации.

```
crypto ikev2 profile PROF
match identity remote address 0.0.0.0
match identity remote key-id IKETEST
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint CA-self
```

```
aaa authentication eap eap-list
aaa authorization user eap list eap-list IKETEST
virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set transform1 esp-3des esp-sha-hmac
crypto ipsec profile PROF
set transform-set transform1
set ikev2-profile PROF
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

В данном примере авторизация установлена на основе пользователя IKETEST, который был создан в конфигурации AcS.

Конфигурация Windows

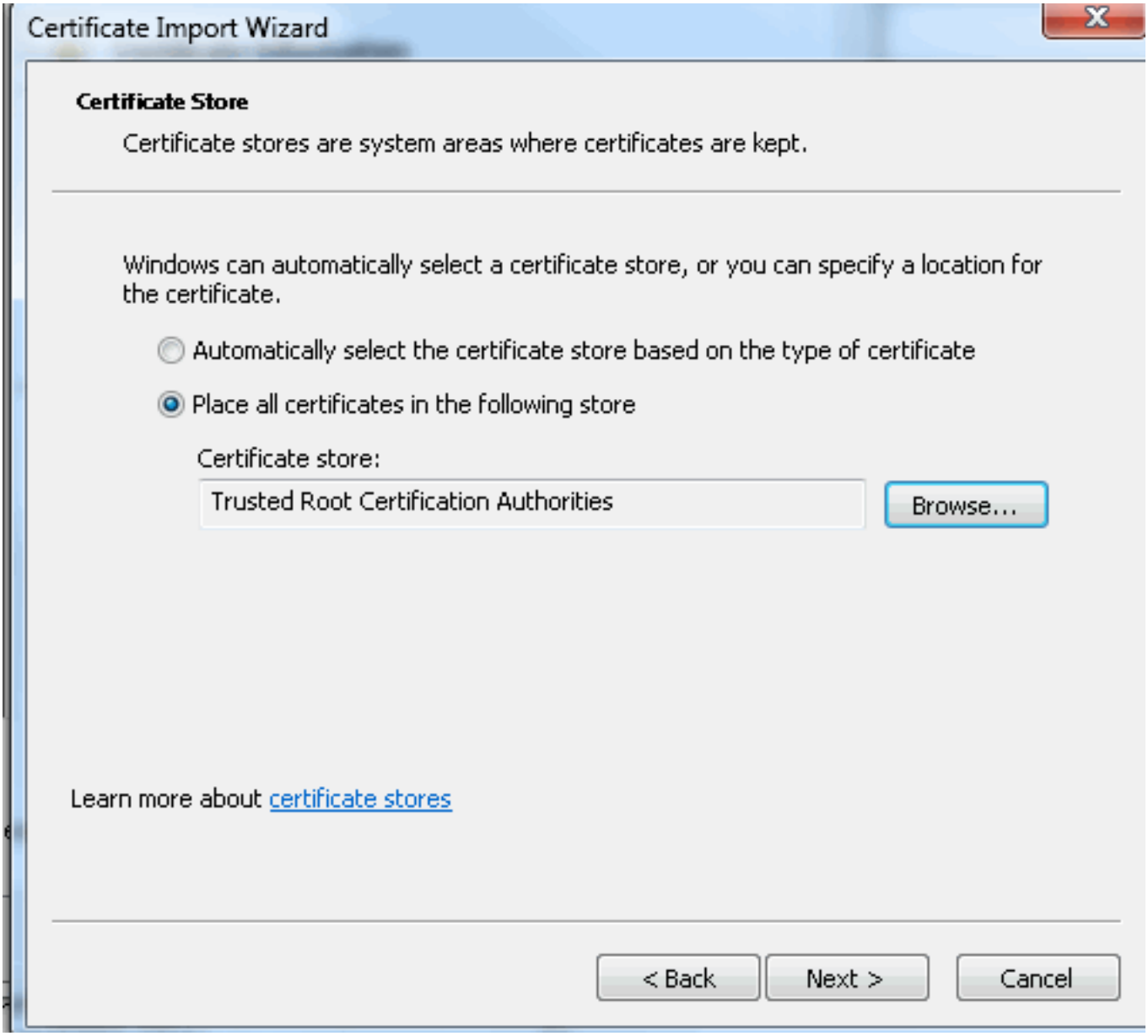
Импорт CA к Windows Trusts

Экспортируйте сертификат CA на IOS (удостоверьтесь, что экспортировали сертификат идентификации и приняли только первое участие):

```
R1(config)#crypto pki export CA-self pem terminal % CA certificate: -----BEGIN CERTIFICATE-----
MIIB8zCCAVygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAe
Fw0xMjExMjYxNzMzMzlaFw0xNTExMjYxNzMzMzlaMA0xCzAJBgNVBAMTAkNBMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvDR4lHOcrj42QfHpRuNu4EyFrLR8H
TbPanXYV+GdCBmu53pDILE00ASEHByD6DYBx01EZuDsiolJ7t2MPTguB+YZe6V4O
JbtayyxtZGmF7+eDqRegQHHC394adQQWl2ojgQiuTHeRDTqDJR8i5gN2Ee+KOsr3
+OjnHjUmXb/I6QIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAfBgNVHSMEGDAWgBTH5Sdh69q4HAJulLQYLbYH0Nk9zzAdBgNVHQ4EFgQU
x+UnYevauBwCbpS0GC22B9DZPc8wDQYJKoZIhvcNAQEFBQADgYEADtBLiNXnl+LC
PIgJ0nl/jH5p2IwVlzwbPbZcOsZ9mn54QaqrhmhbHnmqKQJl/20+JPE6p+4noICq
VBrxoiX2KYQ1OwmEScPpQ2XJ9vhGqtQ4Xcx3g20HhxxFDfp2XuW7hwU0W8dTCmZw
4vodj47qEXKI6pGuzauw9MN1xhkNarc= -----END CERTIFICATE-----
```

Скопируйте часть между СЕРТИФИКАТОМ BEGIN и КОНЕЧНЫМ СЕРТИФИКАТОМ и вставьте его к Блокноту в Windows и сохраните как файл CA.crt.

Необходимо установить его как в полномочиях Trusted Root (двойной щелчок на файле> Сертификат Установки> Место все сертификаты в следующем хранилище> Доверенные корневые центры сертификации):



Профиль XML AnyConnect Настройки

В C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile создают файл "whatever.xml" и вставляют это:

```
<?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>
```

```
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        <AutoReconnect UserControllable="false">true
            <AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
            </AutoReconnectBehavior>
        </AutoReconnect>
        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">
         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>IOSEAP-MD5</HostName>
            <HostAddress>10.1.1.2</HostAddress>
            <PrimaryProtocol>IPsec
                <StandardAuthenticationOnly>true
                    <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
                    <IKEIdentity>IKETEST</IKEIdentity>
                </StandardAuthenticationOnly>
            </PrimaryProtocol>
        </HostEntry>
     </ServerList>
</AnyConnectProfile>
```

Удостоверьтесь, что 10.1.1.2 записи являются точно тем же как CN=10.1.1.2, который был введен для сертификата идентификации.

Тесты

В этом сценарии не используется VPN SSL, поэтому удостоверьтесь, что сервер HTTP отключен на IOS (no ip http server). В противном случае вы получаете сообщение об ошибках в AnyConnect, который сообщает, "Используйте браузер для получения доступа".

При соединении в AnyConnect вам нужно предложить для пароля. В данном примере это - User3, который был создан

После этого пользователь связан.

Проверка

Маршрутизатор IOS

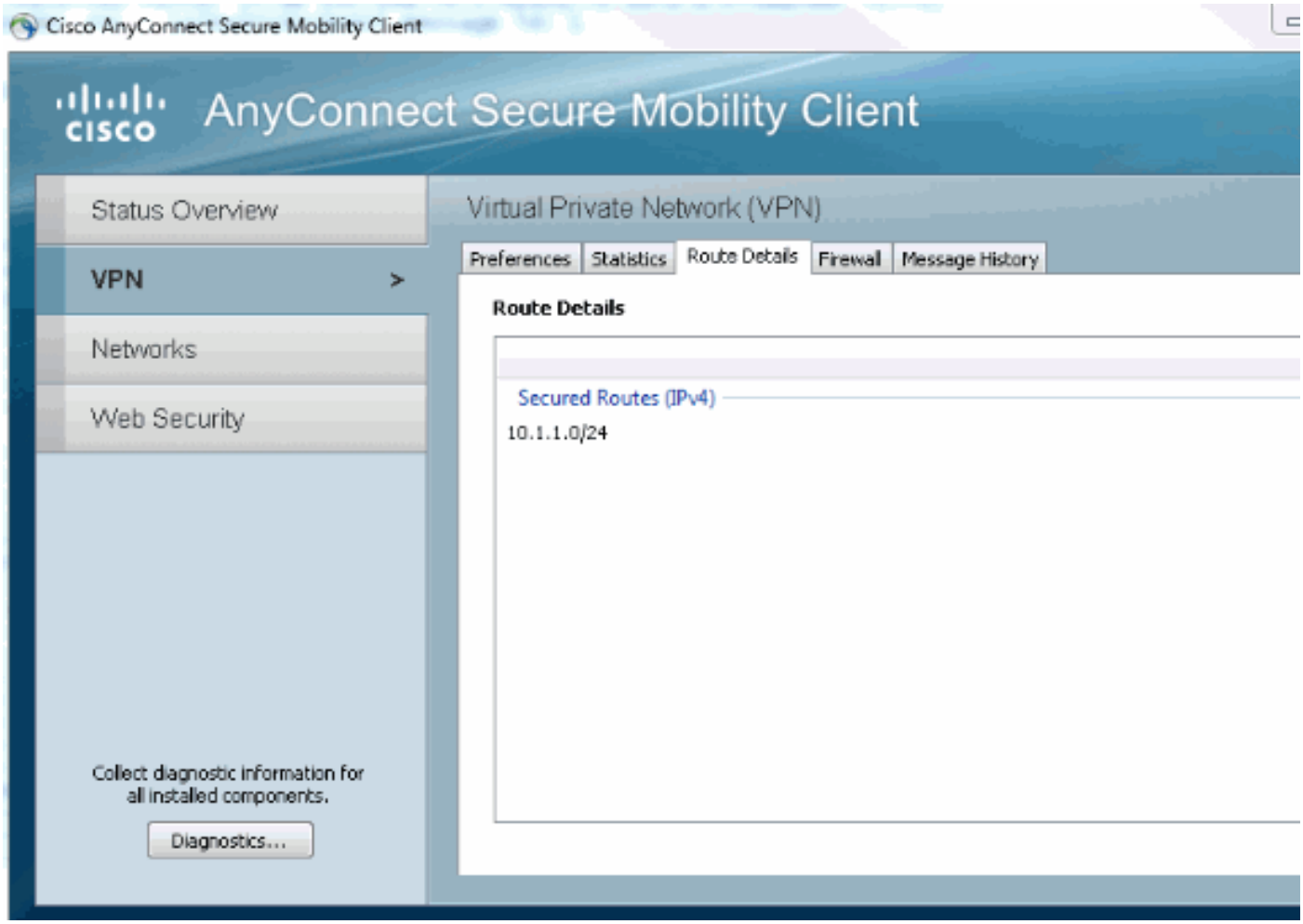
```
R1#show ip inter brief | i Virtual Virtual-Access1 10.1.1.2 YES unset up up Virtual-Template1
10.1.1.2 YES unset up down R1# show ip route 192.168.100.200 Routing entry for
192.168.100.200/32 Known via "static", distance 1, metric 0 (connected) Routing Descriptor
Blocks: * directly connected, via Virtual-Access1 Route metric is 0, traffic share count is 1
R1#show crypto ikev2 sa IPv4 Crypto IKEv2 SA Tunnel-id Local Remote fvrf/ivrf Status 1
10.1.1.2/4500 110.1.1.100/61021 none/none READY Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign:
RSA, Auth verify: EAP Life/Active Time: 86400/94 sec IPv6 Crypto IKEv2 SA R1#show crypto session
detail Crypto session current status Code: C - IKE Configuration mode, D - Dead Peer Detection K
- Keepalives, N - NAT-traversal, T - cTCP encapsulation X - IKE Extended Authentication, F - IKE
Fragmentation Interface: Virtual-Access1 Uptime: 00:04:06 Session status: UP-ACTIVE Peer:
192.168.56.1 port 61021 fvrf: (none) ivrf: (none) Phase1_id: IKETEST Desc: (none) IKEv2 SA:
local 10.1.1.2/4500 remote 10.1.1.100/61021 Active Capabilities:(none) connid:1
lifetime:23:55:54 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.100.200 Active SAs: 2,
origin: crypto map Inbound: #pkts dec'ed 1 drop 0 life (KB/Sec) 4160122/3353 Outbound: #pkts
enc'ed 0 drop 0 life (KB/Sec) 4160123/3353
```

Можно выполнить отладку (debug crypto ikev2).

Windows

В Расширенных настройках AnyConnect в VPN можно проверить Подробные данные

Маршрута для наблюдения сетей Split Tunneling:



Известные предупреждения и проблемы

- Помните при наличии SHA1 в хэше подписи, и в политике целостности в IKEv2 (обратитесь к идентификатору ошибки Cisco CSCtn59317 (только зарегистрированные клиенты)).
- CN в сертификате идентификации IOS должен быть равным именем хоста в профиле XML ACS.
- Если вы хотите использовать пары значение-атрибут Радиуса, которые передают во время аутентификации и не использовать авторизацию группы вообще, можно использовать это в профиле IKEv2:`aaa authorization user eap cached`
- Авторизация всегда использует пароль "Cisco" для авторизации группы/пользователей. Это могло бы сбить с толку при использовании`aaa authorization user eap list SERV (without any paramaters)`потому что это попытается авторизовать использовать пользователя, которого передают в AnyConnect как пользователь и пароль "Cisco", который является, вероятно, не паролем для пользователя.
- В случае любых проблем это выходные данные, которые можно проанализировать и предоставить Центру технической поддержки Cisco:debug crypto ikev2debug crypto ikev2 внутреннийВыходные данные DART
- Если не использование VPN SSL не забывает отключать ip http server (no ip http server). В противном случае AnyConnect попытается соединиться с сервером HTTP и получить результат, "Используйте браузер для получения доступа".

Криптография следующего поколения

Вышеупомянутая конфигурация предоставлена для ссылки для показа минималистической действующей конфигурации.

Cisco рекомендует использовать Криптографию следующего поколения (NGC), если это возможно.

Текущие рекомендации для миграции могут быть найдены здесь: http://www. cisco . com/web/about/security/intelligence/nextgen_crypto.html

При выборе конфигурации NGC удостоверьтесь что и клиентское программное обеспечение и аппаратная поддержка головного узла это. Поколение 2 ISR и ASR 1000 маршрутизаторов рекомендуются как головные узлы из-за их аппаратной поддержки для NGC.

На стороне AnyConnect, с версии AnyConnect 3.1, поддерживается Комплект NSA B комплект алгоритма.

Дополнительные сведения

- VPN узла узла PKI Cisco ASA IKEv2
- Site2-узел IKEv2 отлаживает на IOS
- FlexVPN / IKEv2: Windows 7 Builtin-Client: Головной узел IOS: Первая часть - Проверка подлинности сертификата
- FlexVPN и руководство по конфигурации версии 2 обмена ключами между сетями, Cisco IOS Release 15.2M&T
- Cisco Systems – техническая поддержка и документация