FlexVPN部署：与EAP-MD5的AnyConnect IKEv2远程访问

目录

简介

使用FlexVPN工具套件，本文提供配置示例如何设置在IOS的远程访问。

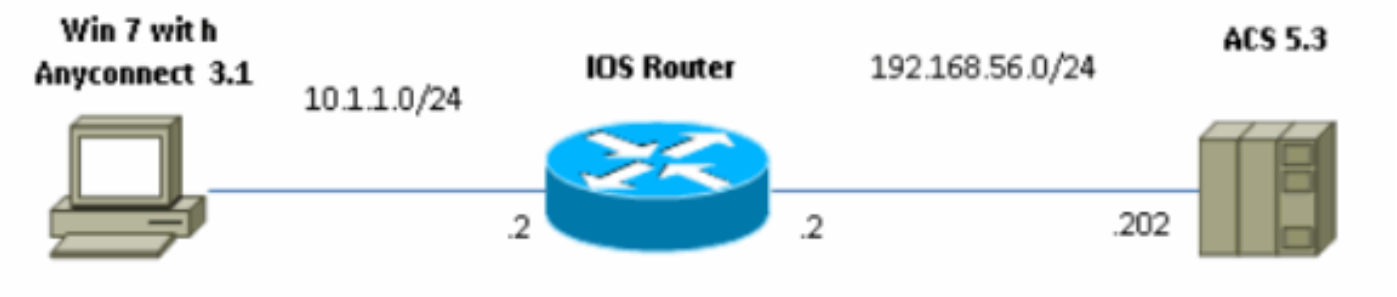
远程访问VPN允许使用多种操作系统的END客户端安全地连接到他们的公司或家庭网络通过不安全的介质例如互联网。使用IKEv2协议，在提交方案中， VPN通道在Cisco IOS路由器终止。

本文显示如何验证和认证使用访问控制服务器(ACS)的用户通过EAP-MD5方法。

先决条件

网络图

Cisco IOS路由器有两个接口-一个往ACS 5.3 ：



要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 与补丁程序6的ACS 5.3
- 有15.2(4)M软件的IOS路由器
- 有AnyConnect的3.1.01065 Windows 7 PC

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景

在IKEv1中XAUTH用于相位1.5，使用RADIUS/TACACS+，您能执行用户的验证本地在IOS路由器和远程。IKEv2不再支持XAUTH和相位1.5。它包含内置的EAP支持，在相位IKE_AUTH完成。此的最大的优点在IKEv2设计，并且EAP是一个著名的标准。

EAP支持两个模式：

- 建立隧道— EAP-TLS、EAP/PSK， EAP-PEAP等。
- 非隧道— EAP-MSCHAPv2、EAP-GTC， EAP-MD5等。

在本例中，在非隧道模式的EAP-MD5，因为是当前支持它ACS EAP外面认证方法5.3，使用。

EAP可以只用于验证发起者(客户端)对响应方(IOS在这种情况下)。

IOS初始配置

IOS - CA

首先您需要创建Certificate Authority (CA)和创建IOS路由器的一身份证书。客户端将验证根据该证书的路由器的标识。

CA的配置在IOS的看似类似：

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

您需要记住关于延长的密钥用法(为EAP需要的服务器验证， RSA-SIG您的也需要客户端验证)。

使用**no shutdown命令**在crypto pki server CA，启用CA。

IOS -身份证书

其次，证书的enable (event)简单认证登记协议(SCEP)和配置信任点。

```
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
```

然后，请验证并且登记证书：

```
(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
```

如果在AnyConnect不要安排提示消息记住cn需要是相等的与在AnyConnect配置文件/IP地址配置的主机名。

在本例中， cn=10.1.1.2。所以，在AnyConnect 10.1.1.2被输入作为服务器的IP地址在AnyConnect xml配置文件的。

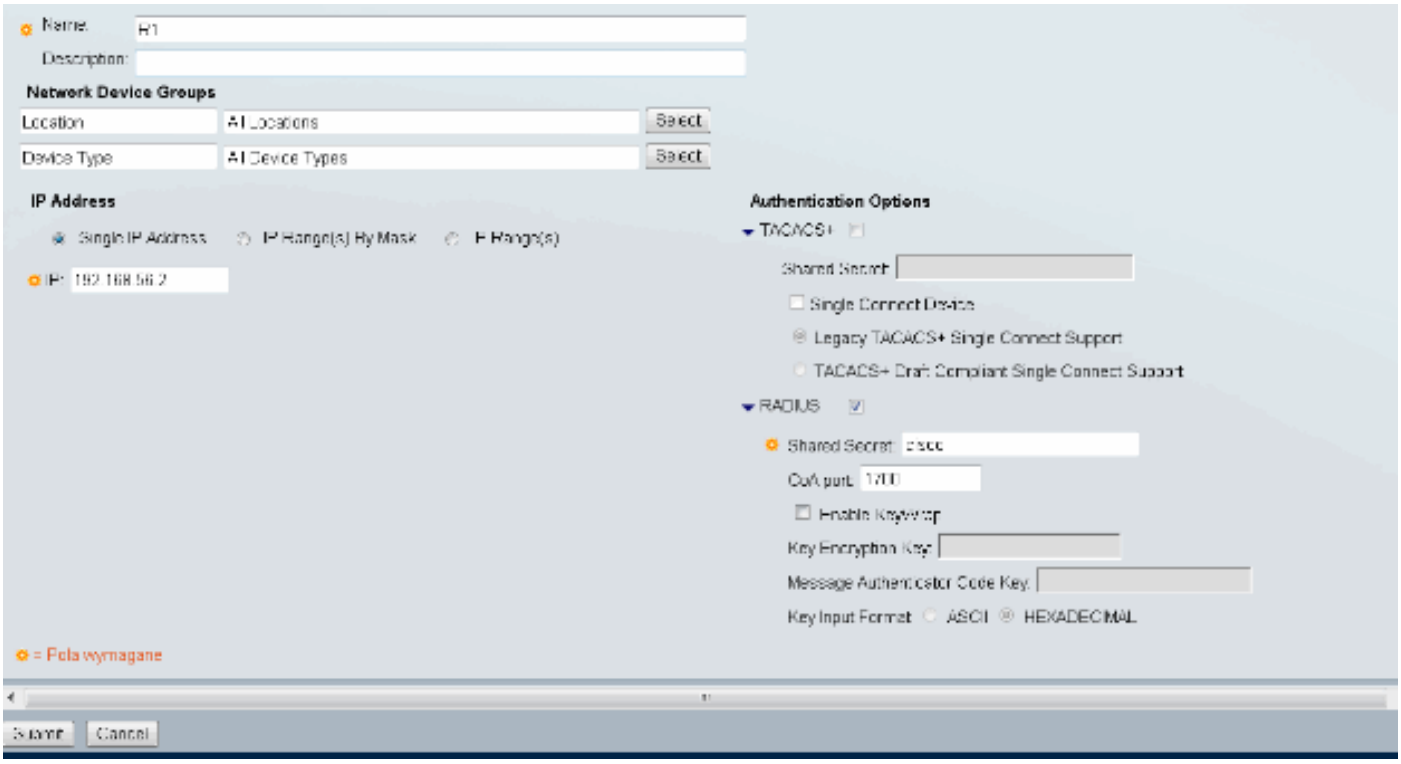
IOS - AAA和RADIUS配置

您需要配置Radius和AAA认证和授权：

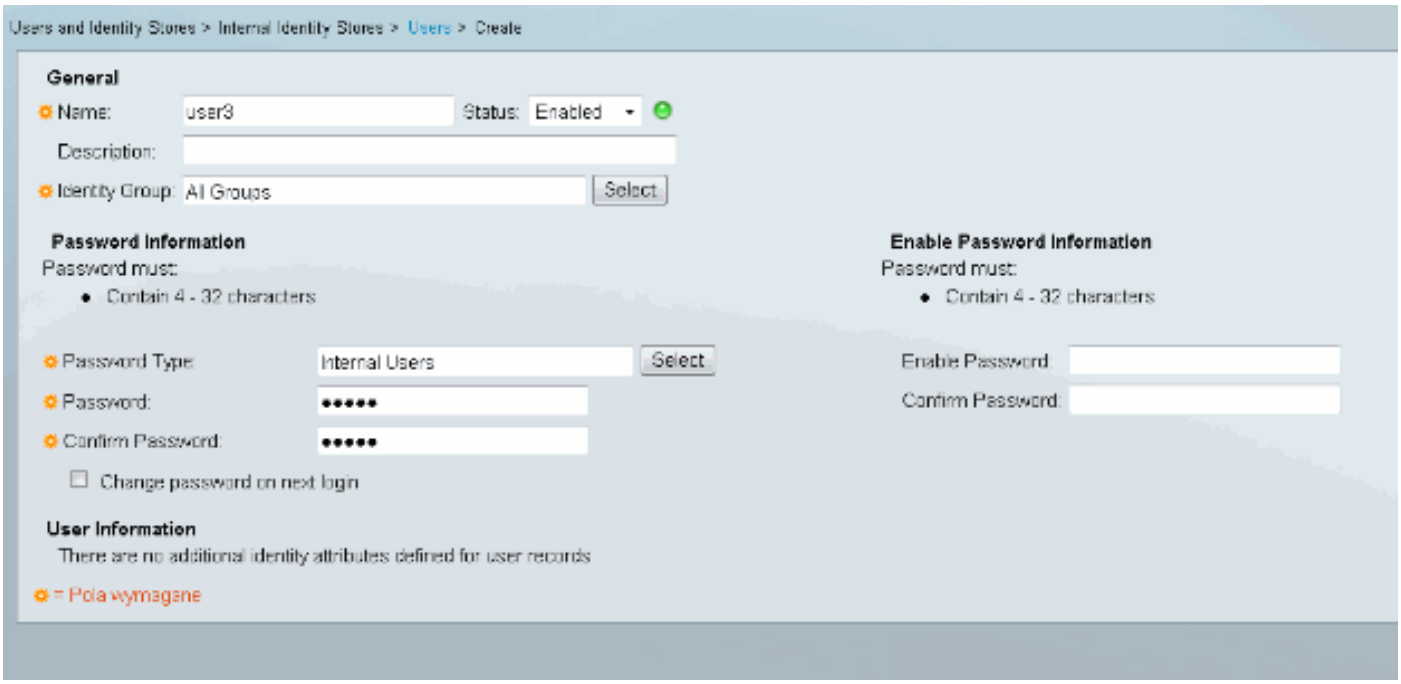
```
(config)#crypto pki authenticate CA-self
Certificate has the following attributes:
       Fingerprint MD5: 741C671C 3202B3AE 6E05161C 694CA53E
      Fingerprint SHA1: 8C99513C 2198470F 7CB58FA2 32D8AA8D FC31D1ED
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

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
```

ACS初始配置

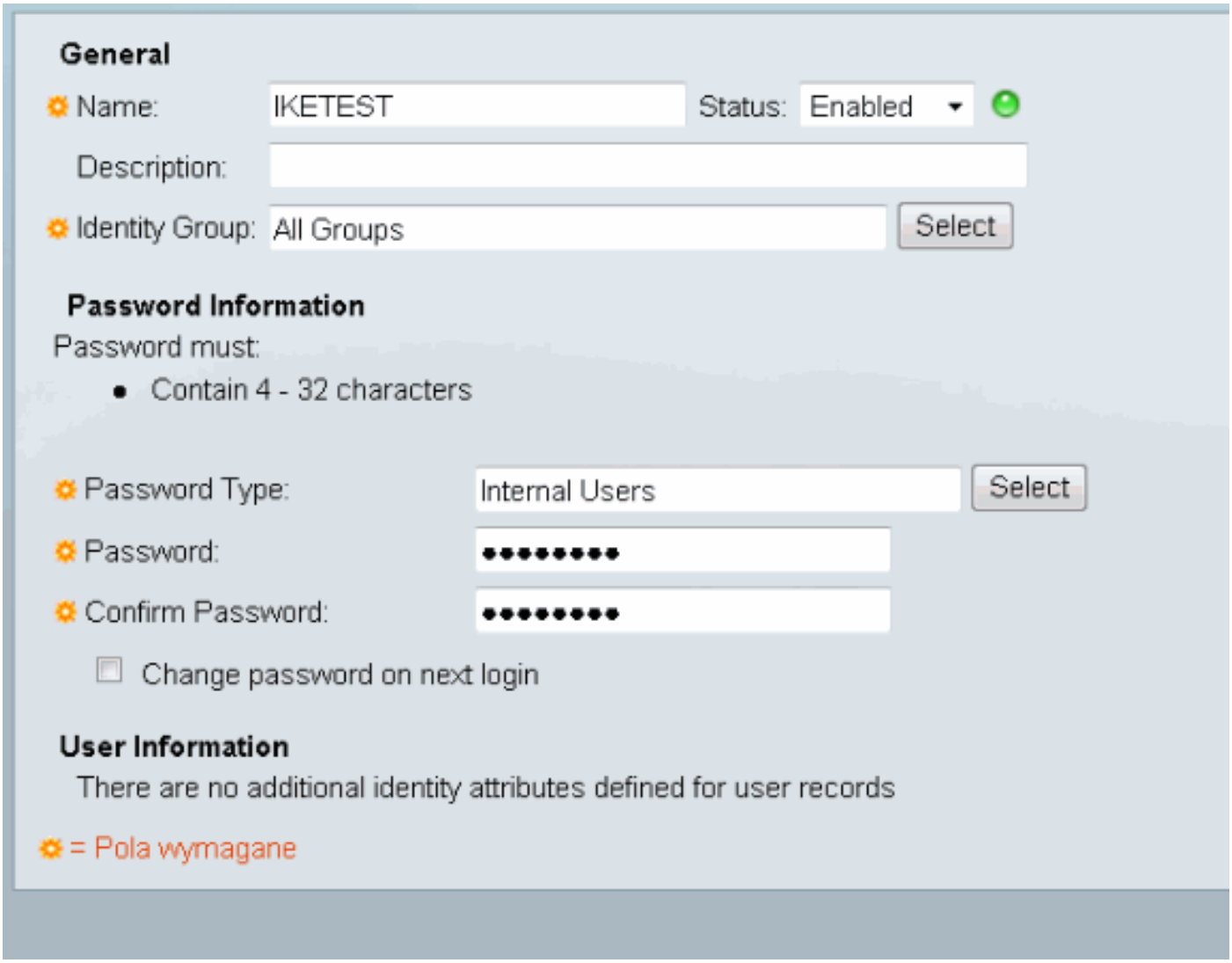
首先，请添加在ACS的新的网络设备(网络资源>网络设备和AAA客户端>创建) ：



添加一个用户(用户和标识存储>内部标识存储> Users >创建) ：

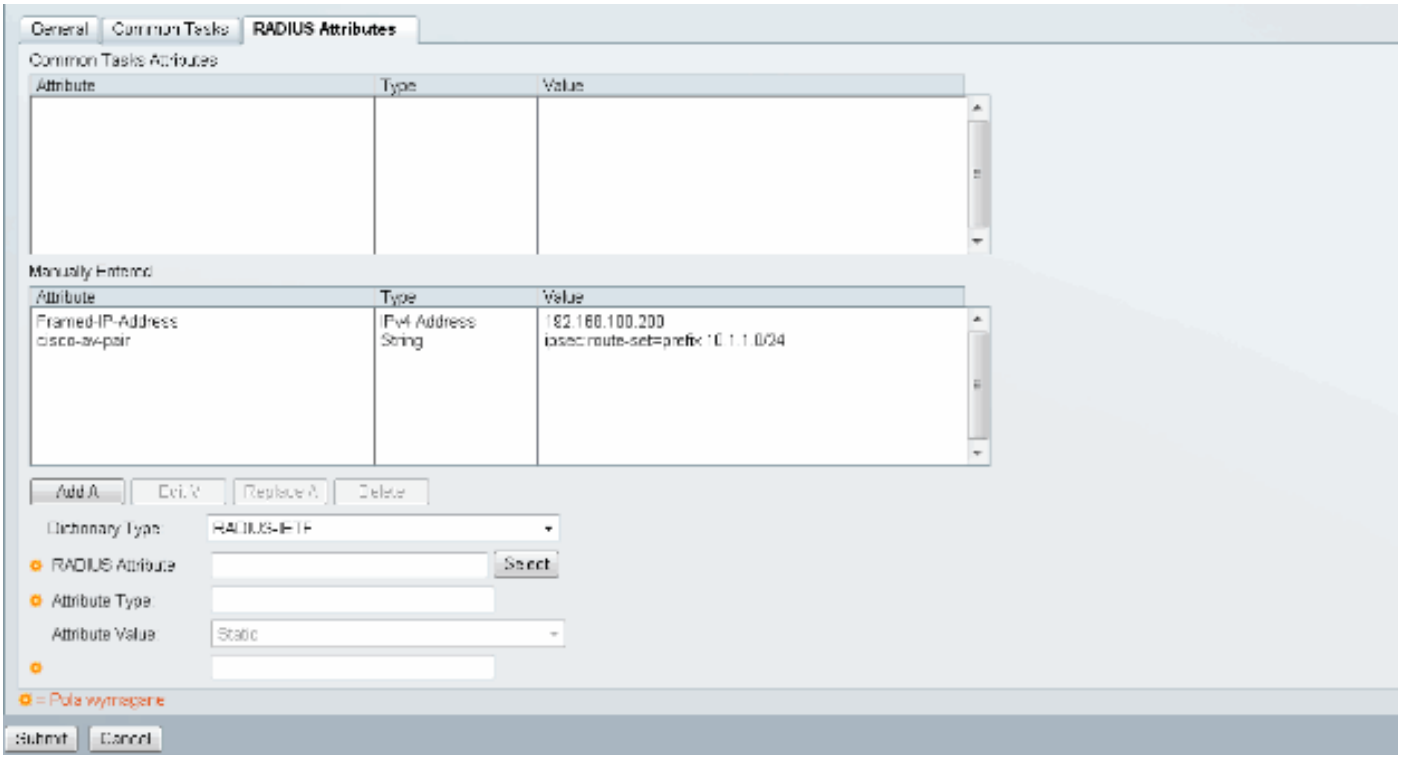


添加授权的一个用户。在本例中，它是IKETEST。因为它是IOS，发送的默认密码需要是“cisco”。

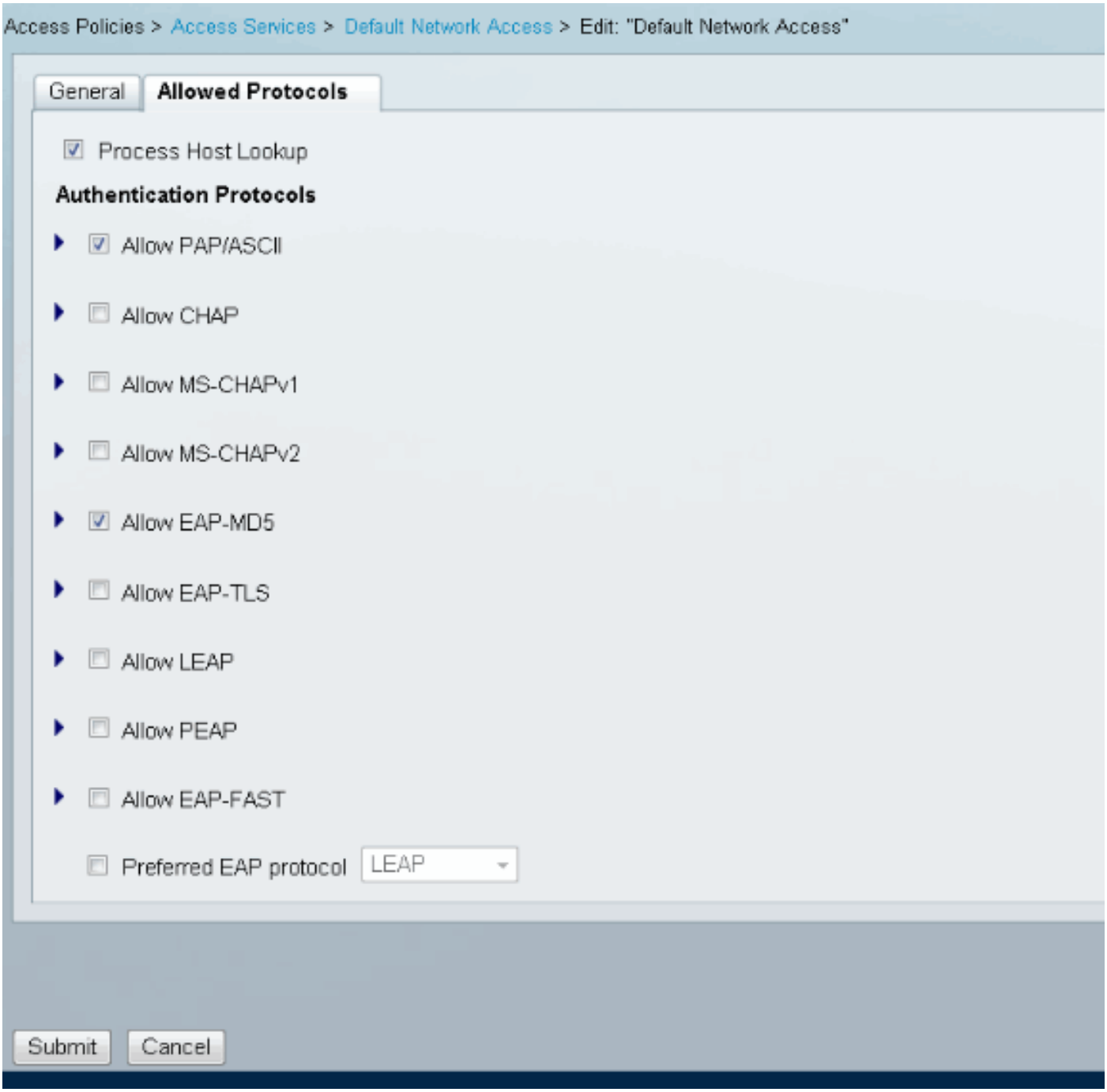


其次，请创建用户的一授权配置文件(策略元素>授权和权限>网络访问>授权Profiles>创建)。

在本例中，它呼叫池。在本例中，独立的隧道AV对(作为前缀)被输入和framed-ip-address作为分配到连接的客户端的IP地址。可以找到所有支持的AV对列表此处：http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



然后，您需要打开EAP-MD5 (验证)和PAP/ASCII支持(授权)在访问策略。默认用于此示例(访问策略>默认网络网络访问) ：



创造在访问策略的条件并且分配创建的授权配置文件。在这种情况下NDG的一个条件：位置在所有位置创建，因而对于所有RADIUS授权请求将提供池授权配置文件(访问策略>Access Services>默认网络网络访问)：

如果用户能正确，验证您在IOS路由器应该能测试：

```
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"
```

IOS FlexVPN配置

您需要创建IKEv2建议和策略(您不可能必须，参考CSCtn59317)。策略为其中一个IP地址仅创建(10.1.1.2)在本例中。

```
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"
```

然后，请创建将绑定到虚拟模板的IKEV2配置文件和IPSec简档。

确保您关闭HTTP URL cert，如建议在配置指南。

```
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"
```

在本例中，授权设置根据用户IKETEST，在ACS配置里创建。

Windows正在配置

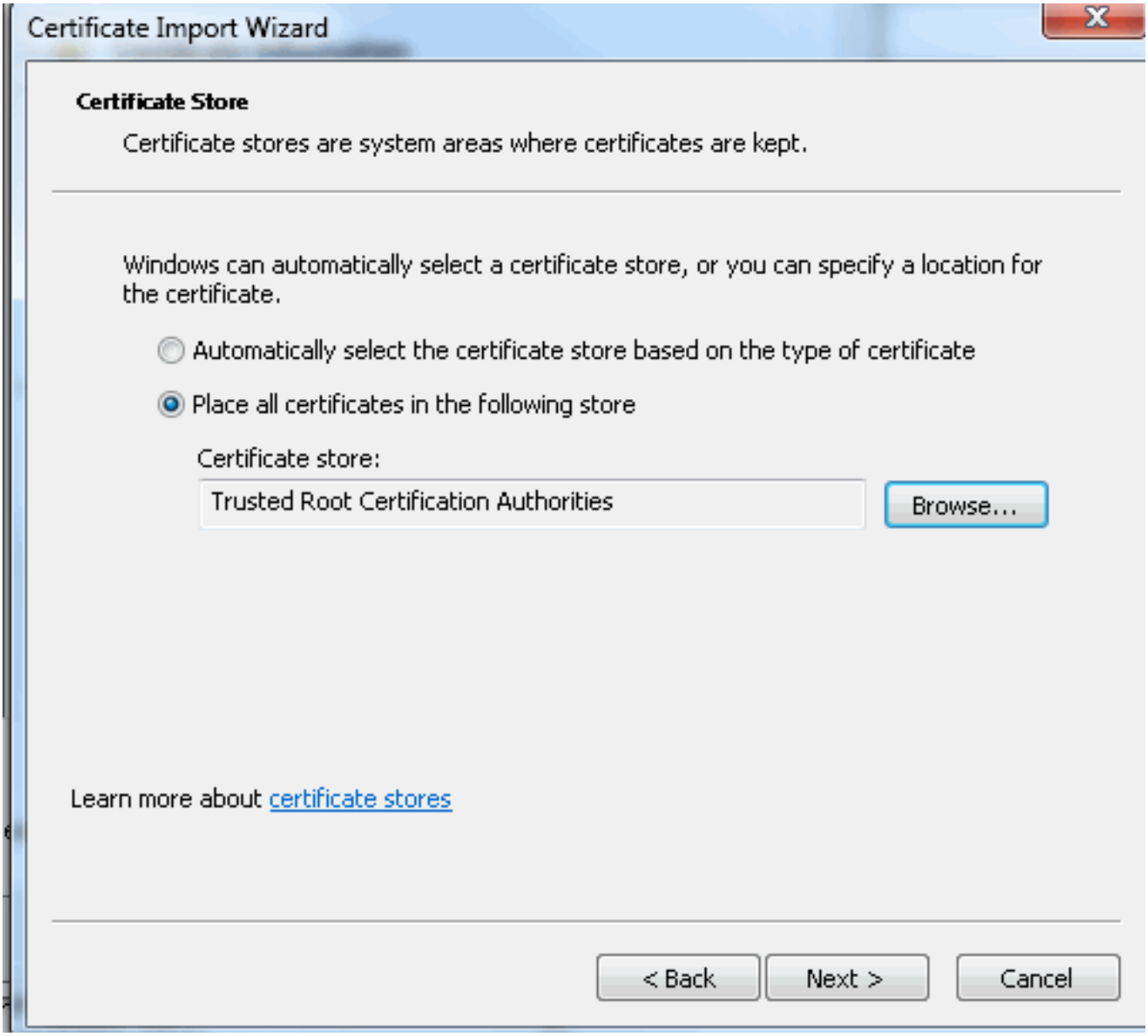
导入对Windows信任的CA

导出在IOS的CA证书(请确保导出身份证书和采取仅第一部分)：

```
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-----
```

复制之间零件开始证书和END证书并且粘贴它对在Windows的Notepad并且保存作为文件CA.crt。

您在可信的根权限(在file>安装证书>地方的双击需要安装它正如在以下存储>可靠的根证书颁发机构的所有证书)：



配置AnyConnect XML配置文件

在C:\ProgramData\Cisco\Cisco AnyConnect安全移动性客户端\配置文件请创建文件“whatever.xml”并且粘贴此：

```
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-----
```

确保10.1.1.2条目正确地是相同的象为身份证书被输入的CN=10.1.1.2。

测验

在此方案SSL中没有使用VPN，因此请确保HTTP服务器禁用在IOS (no ip http server)。否则，您在陈述的AnyConnect收到一错误消息，“使用浏览器获得访问”。

当连接在AnyConnect时，应该提示对于密码。在本例中，创建的它是用户3

在那以后，用户连接。

验证

IOS 路由器

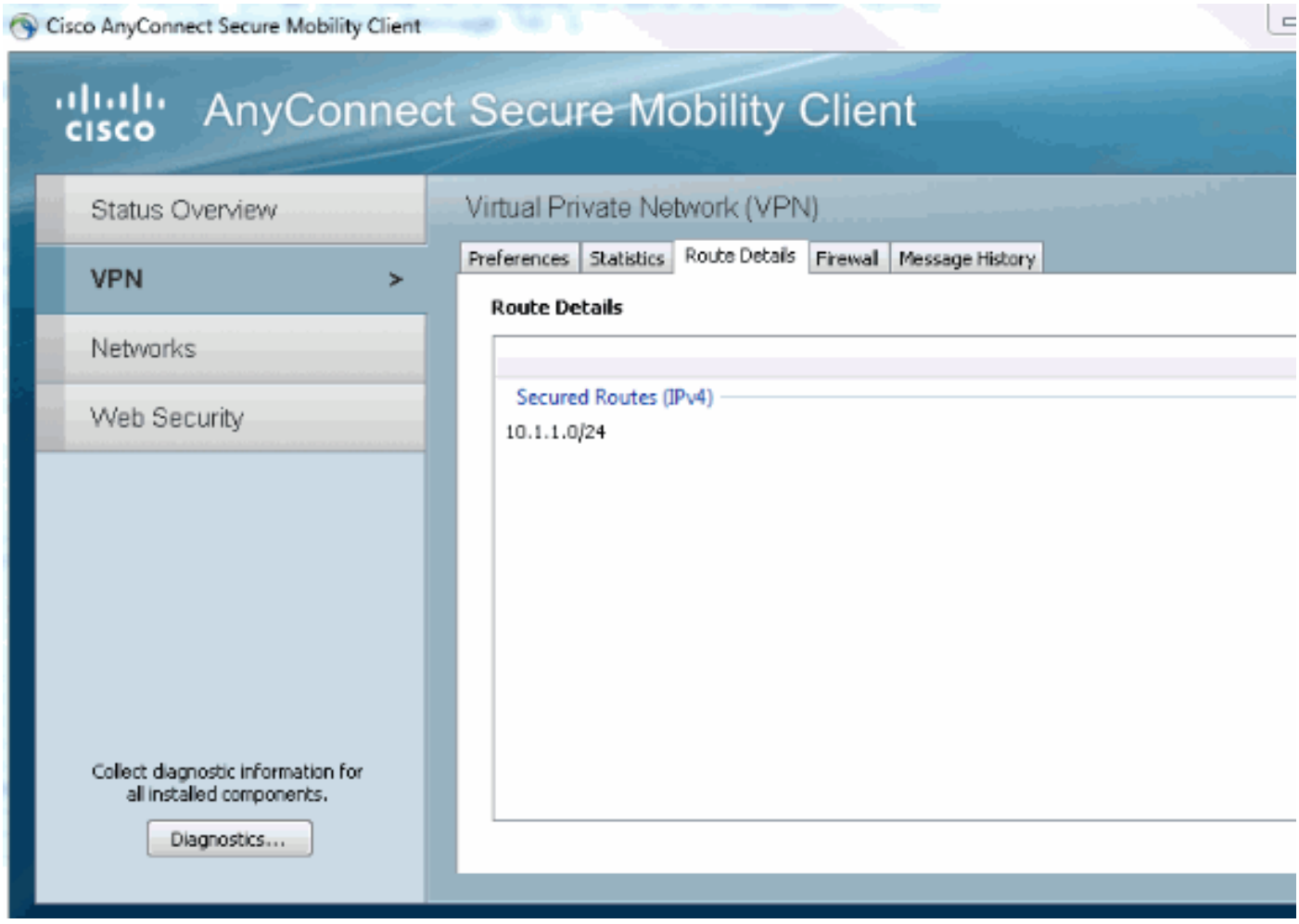
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Template1  10.1.1.2  YES unset  up down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly 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
```

您可执行调试(debug crypto ikev2)。

Windows

在AnyConnect的高级选项在VPN的您能检查路由详细信息发现分割隧道网络：



已知问题说明和问题

- 请切记，当有SHA1在签名哈希和在IKEv2 (参考的Cisco Bug ID CSCtn59317 (仅限注册用户)的)完整性策略。
- 在IOS身份证书的CN必须是在ACS XML配置文件的相等的主机名。
- 如果要使用在验证时通过的Radius AV对和根本不使用组的授权，您在IKEv2配置文件能使用此：

```
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
```

- 授权总是使用密码“cisco”组/用户授权。这也许是混乱的，当曾经时

```
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
```

因为它将设法授权使用在AnyConnect通过的用户作为用户和密码“cisco”，很可能不是用户的密码。

- 在所有问题的情况下这些是您能分析和提供给Cisco TAC的输出：debug crypto ikev2内部的debug crypto ikev2箭输出
- 如果不使用SSL VPN请切记禁用ip http server (no ip http server)。否则， AnyConnect将设法连接到HTTP服务器，并且收到结果，“使用一个浏览器获得访问”。

下一代加密算法

上述配置提供供参考显示一个minimalistic工作配置。

思科推荐尽可能使用下一代加密算法(NGC)。

可以找到迁移的当前建议此处
：http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

当选择NGC配置时，请确保客户端软件和头端硬件支持它。ISR生成2和ASR 1000路由器推荐作为头端由于他们的NGC的硬件支持。

在AnyConnect侧，根据AnyConnect 3.1版本， NSA的套件B支持algorythm套件。

相关信息

- 思科ASA IKEv2 PKI站点对站点VPN
- 在IOS的IKEv2 Site2-Site调试
- FlexVPN/IKEv2 ：Windows 7 Builtin客户端：IOS头端：第I部分-证书验证
- FlexVPN和互联网密钥交换版本2配置指南， Cisco IOS版本15.2M&T
- 技术支持和文档 - Cisco Systems