Implantação de FlexVPN: Acesso remoto do AnyConnect IKEv2 com EAP-MD5

Contents

[Introduction](#)
[Prerequisites](#)
[Diagrama de Rede](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Background](#)
[Configuração inicial do IOS](#)
[IOS - CA](#)
[IOS - Certificado de identidade](#)
[IOS - configuração de AAA e Radius](#)
[configuração inicial do ACS](#)
[Configuração do IOS FlexVPN](#)
[configuração do Windows](#)
[Importando CA para Confianças do Windows](#)
[Configurando o perfil XML do AnyConnect](#)
[Testes](#)
[Verificação](#)
[Roteador IOS](#)
[Windows](#)
[Problemas conhecidos](#)
[Criptografia de próxima geração](#)
[Informações Relacionadas](#)

Introduction

Este documento fornece uma configuração de exemplo de como configurar o acesso remoto no IOS usando o kit de ferramentas FlexVPN.

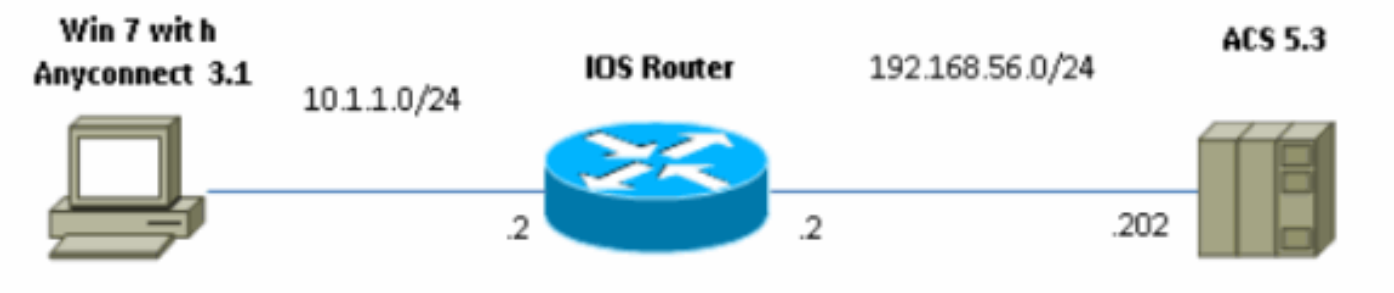
A VPN de acesso remoto permite que os clientes finais que usam vários sistemas operacionais se conectem com segurança a suas redes corporativas ou domésticas por meio de meios não seguros, como a Internet. No cenário apresentado, o túnel VPN está sendo encerrado em um Cisco IOS Router usando o protocolo IKEv2.

Este documento mostra como autenticar e autorizar usuários usando o Access Control Server (ACS) através do método EAP-MD5.

Prerequisites

Diagrama de Rede

O Cisco IOS Router tem duas interfaces - uma em direção ao ACS 5.3:



Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- ACS 5.3 com patch 6
- Roteador IOS com software 15.2(4)M
- Windows 7 PC com AnyConnect 3.1.01065

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Background

No IKEv1 XAUTH é usado na fase 1.5, você pode fazer autenticação de usuários localmente em um roteador IOS e remotamente usando RADIUS/TACACS+. IKEv2 não suporta mais XAUTH e fase 1.5. Ele contém suporte EAP integrado, que é feito na fase IKE_AUTH. A maior vantagem disso é o projeto IKEv2 e o EAP é um padrão conhecido.

O EAP suporta dois modos:

- Encapsulamento—EAP-TLS,EAP/PSK, EAP-PEAP, etc.
- Não tunelamento—EAP-MSCHAPv2, EAP-GTC, EAP-MD5 etc.

Neste exemplo, o EAP-MD5 no modo não de tunelamento é usado porque é o método de autenticação do roteador EAP suportado atualmente no ACS 5.3.

O EAP só pode ser usado para iniciador de autenticação (cliente) para respondente (IOS neste caso).

Configuração inicial do IOS

IOS - CA

Primeiro, você precisa criar uma autoridade de certificação (CA) e um certificado de identidade para o roteador IOS. O cliente verificará a identidade do roteador com base nesse certificado.

A configuração da CA no IOS é semelhante a:

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

Lembre-se do uso de chave estendida (Server-Auth necessário para EAP, para RSA-SIG você também precisa de Client-Auth).

Ative a AC usando o comando **no shutdown** na CA do servidor crypto pki.

IOS - Certificado de identidade

Em seguida, habilite o Simple Certificate Enrollment Protocol (SCEP) para obter o certificado e configure o ponto de confiança.

```
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
```

Em seguida, autentique e inscreva o certificado:

```
(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
```

Se você não quiser ter mensagens de prompt no AnyConnect, lembre-se de que ele precisa ser igual ao nome do host/endereços IP configurados no perfil do AnyConnect.

Neste exemplo, cn=10.1.1.2. Portanto, no AnyConnect 10.1.1.2 é inserido como endereço IP do servidor no perfil xml do AnyConnect.

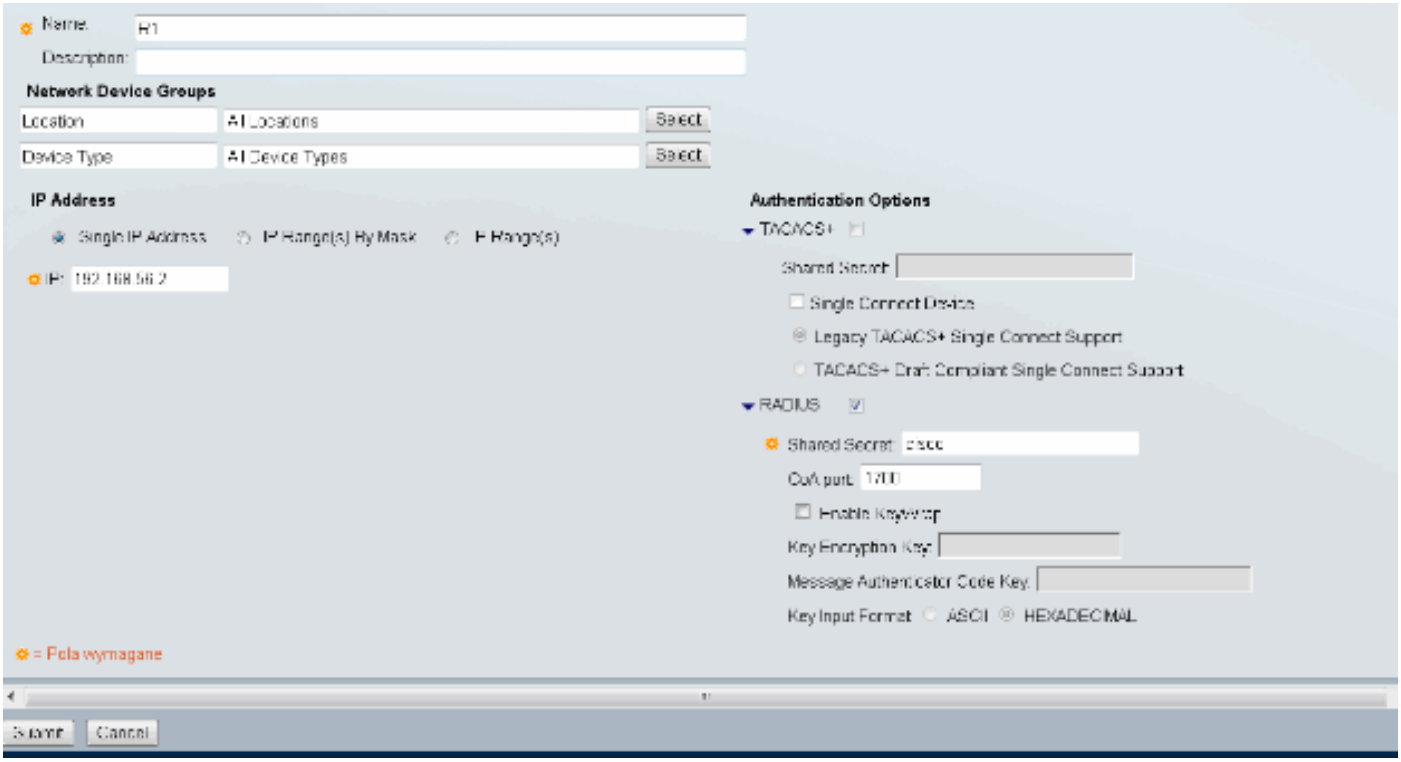
IOS - configuração de AAA e Radius

Você precisa configurar a autenticação e a autorização de RADIUS e AAA:

```
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
```

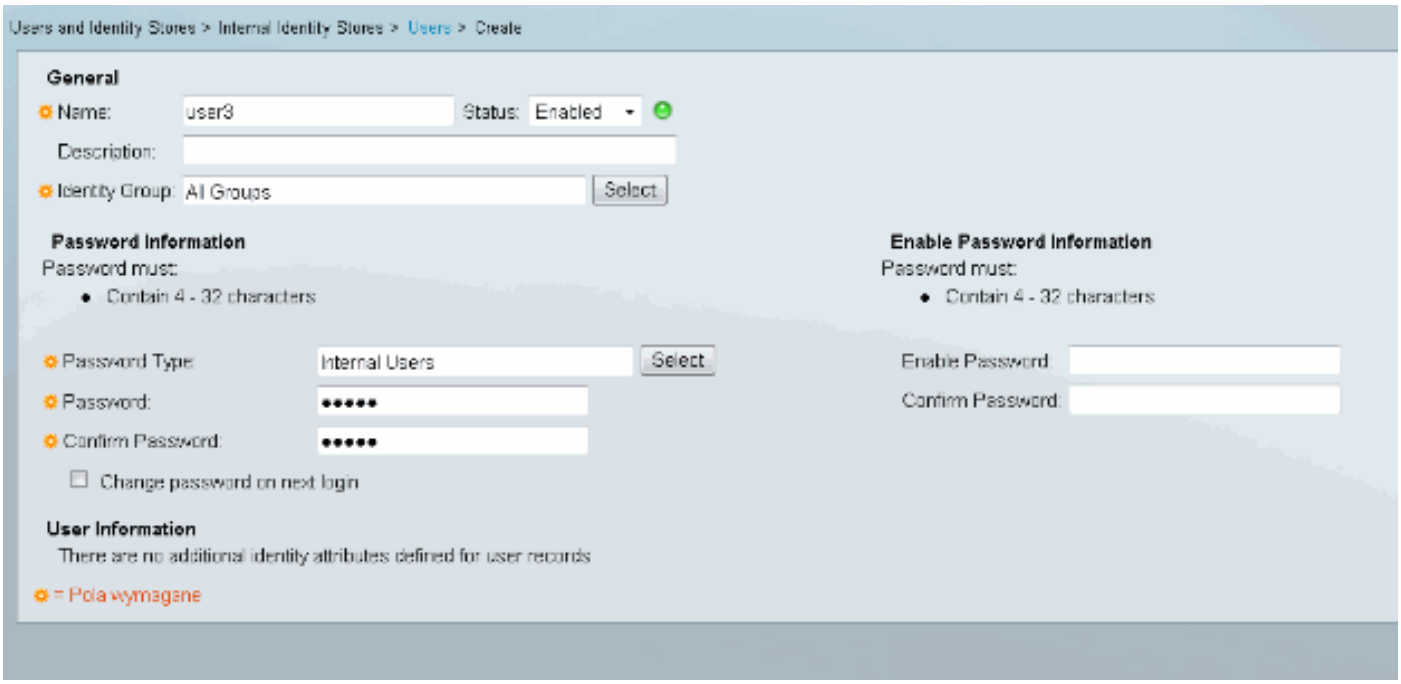
configuração inicial do ACS

Primeiro, adicione o novo dispositivo de rede no ACS (Network Resources > Network Devices and AAA Clients > Create):

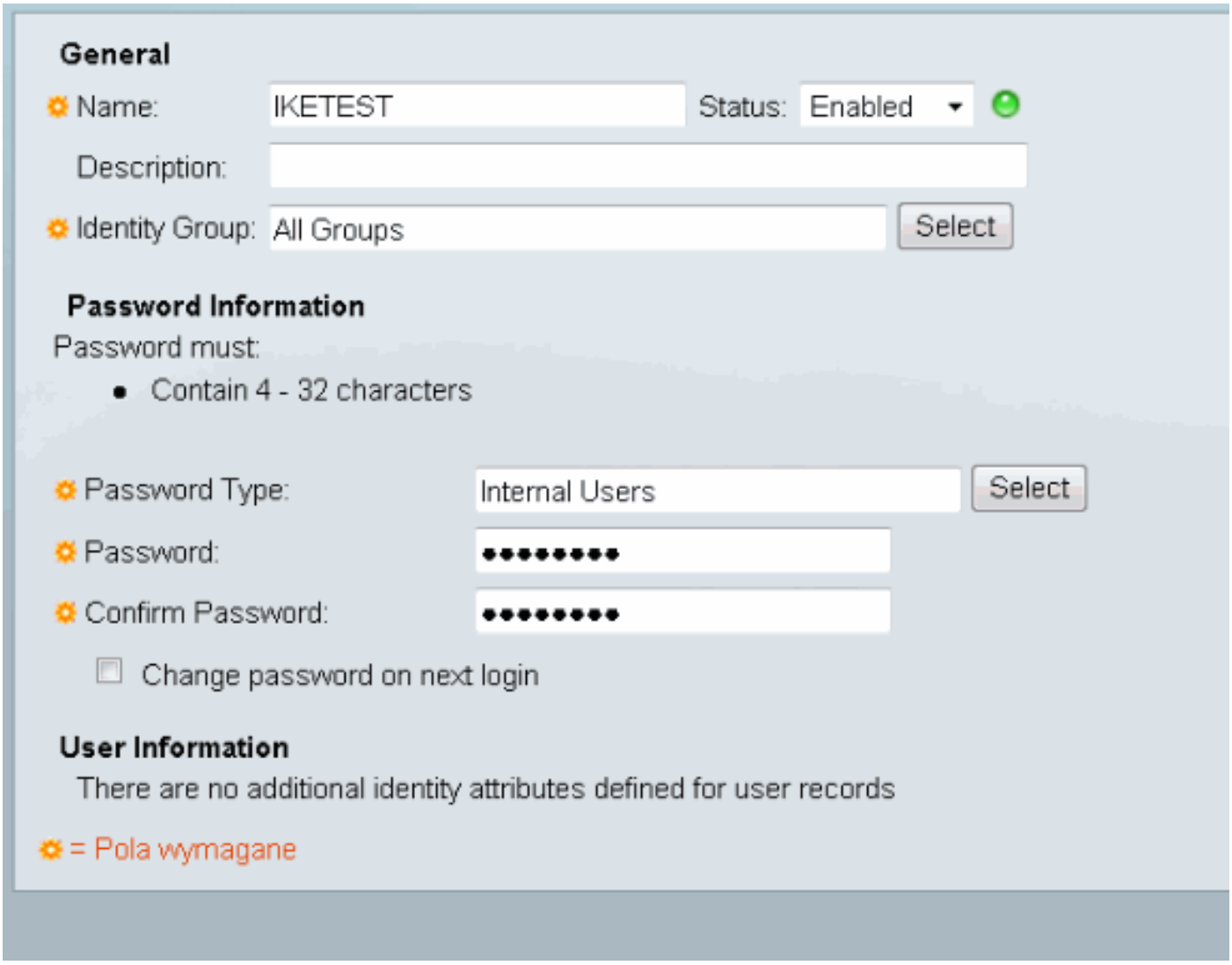


Adicione um usuário (Usuários e lojas de identidade > Lojas de identidade internas > Usuários >

Criar):

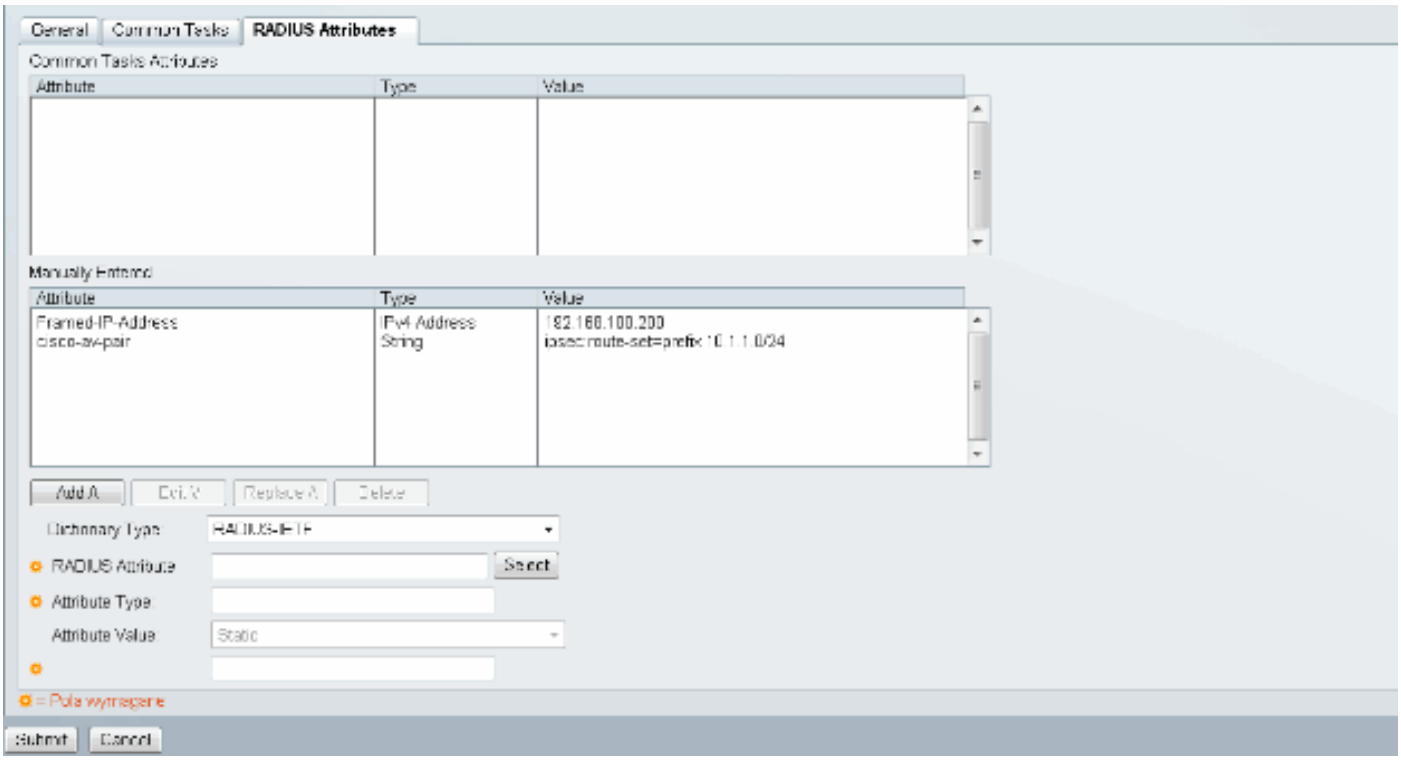


Adicionar um usuário para autorização. Neste exemplo, é IKETEST. A senha precisa ser "cisco" porque é o padrão enviado pelo IOS.

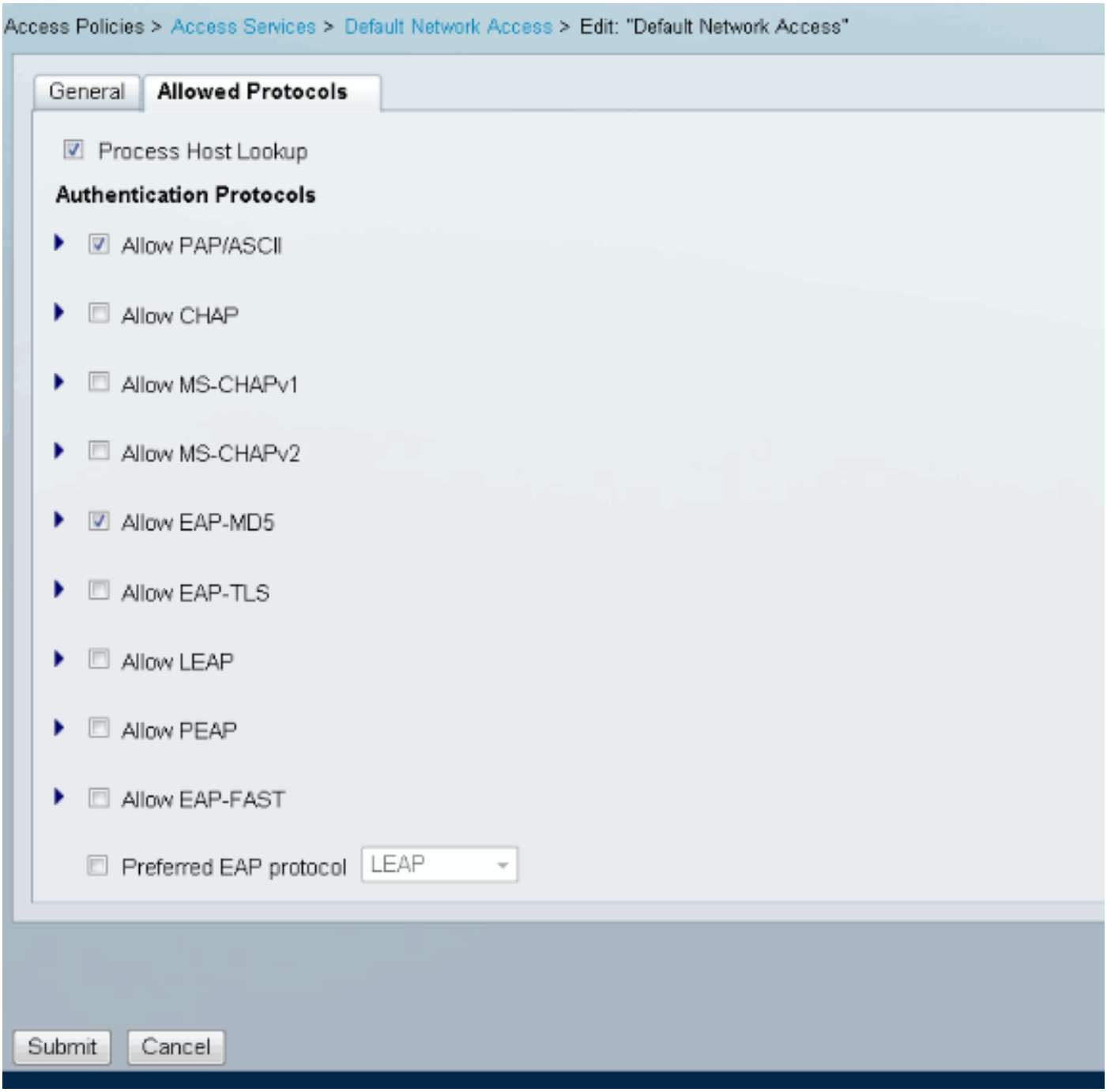


Em seguida, crie um perfil de autorização para os usuários (Elementos de política > Autorização e permissões > Acesso à rede > Perfis de autorização > Criar).

Neste exemplo, ele é chamado POOL. Neste exemplo, o par AV de túnel dividido (como um prefixo) é inserido e o endereço IP enquadrado como endereço IP que será atribuído ao cliente conectado. A lista de todos os pares de antivírus suportados pode ser encontrada aqui: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-apx-flex-rad.html



Em seguida, você precisa ativar o suporte de EAP-MD5 (para autenticação) e PAP/ASCII (para autorização) na Política de acesso. O padrão é usado neste exemplo (Políticas de acesso > Acesso de rede padrão):



Crie uma condição para na Diretiva de acesso e atribua o perfil de autorização que foi criado. Nesse caso, uma condição para NDG:Location in All Locations (Local em Todos os Locais) é criada, portanto, para todas as solicitações de autorização de RADIUS, será fornecido o perfil de autorização de POOL (Políticas de acesso > Serviços de acesso > Acesso à rede padrão):

Você deve ser capaz de testar em um roteador IOS se o usuário puder autenticar corretamente:

```
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"
```

Configuração do IOS FlexVPN

Você precisa criar proposta e política de IKEv2 (talvez não seja necessário, consulte CSCtn59317). A política é criada somente para um dos endereços IP (10.1.1.2) neste exemplo.

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

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

Em seguida, crie um perfil IKEV2 e um perfil IPsec que se vincularão ao Modelo Virtual.

Certifique-se de desligar o certificado http-url, conforme indicado no guia de configuração.

```
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
```

Neste exemplo, a autorização é configurada com base no usuário IKETEST, que foi criado na configuração do ACS.

configuração do Windows

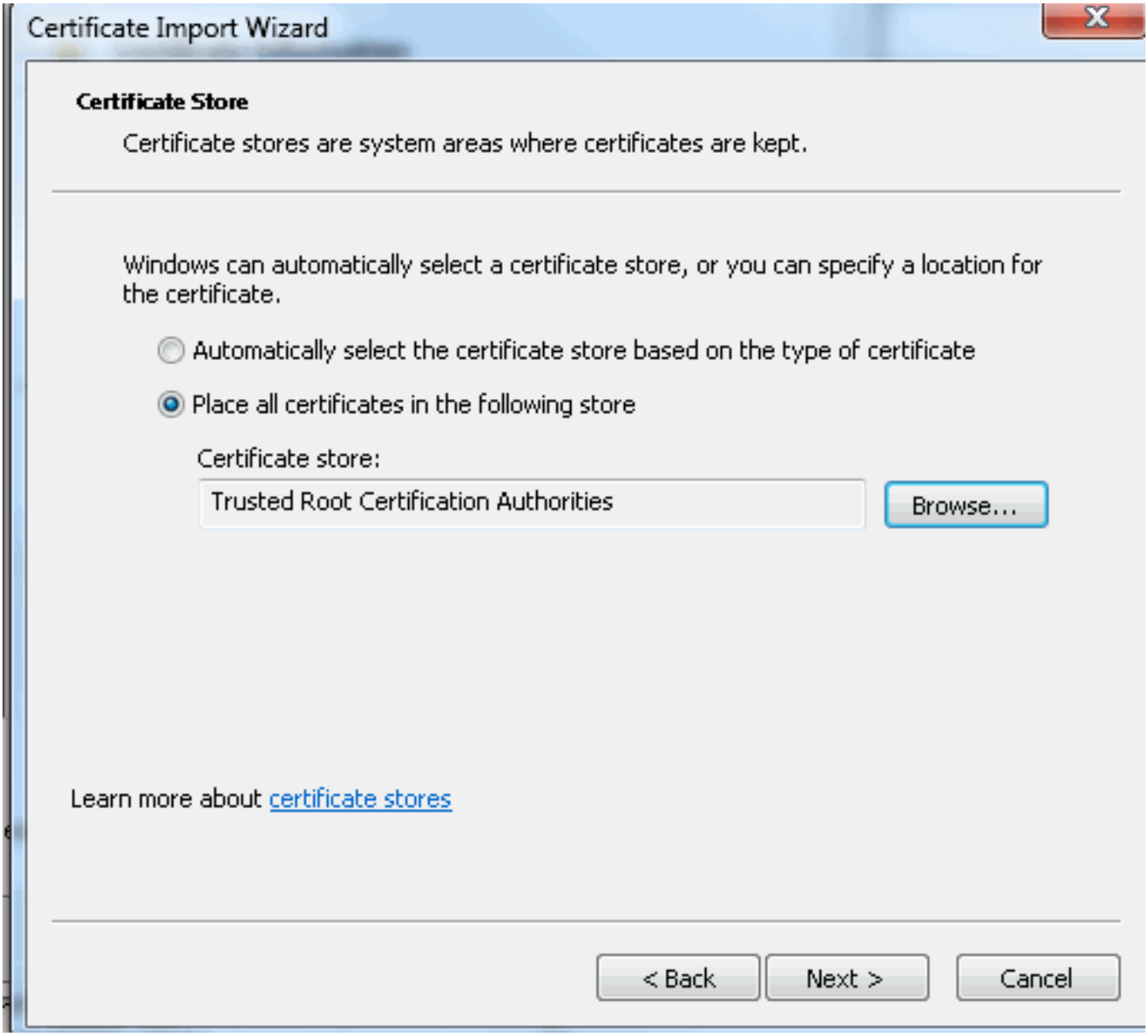
Importando CA para Confianças do Windows

Exportar o certificado CA no IOS (certifique-se de exportar o certificado de identidade e tomar apenas a primeira parte):

```
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-----
```

Copie a peça entre o CERTIFICADO BEGIN e o CERTIFICADO FINAL e cole-o no Bloco de Notas no Windows e salve como arquivo CA.crt.

Você precisa instalá-lo como em Autoridades de Raiz Confiáveis (clique duas vezes em arquivo > Instalar certificado > Colocar todos os certificados no seguinte repositório > Autoridades de Certificação de Raiz Confiáveis):



Configurando o perfil XML do AnyConnect

Em C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile create a file "what.xml" e cole isto:

```
<?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>
```

Certifique-se de que a entrada 10.1.1.2 é exatamente a mesma que CN=10.1.1.2 que foi inserida para o certificado de identidade.

Testes

Neste cenário, a VPN SSL não é usada, portanto, verifique se o servidor HTTP está desabilitado no IOS (sem servidor ip http). Caso contrário, você receberá uma mensagem de erro no AnyConnect que indica: "Use um navegador para obter acesso".

Ao se conectar no AnyConnect, você deve ser solicitado a fornecer uma senha. Neste exemplo, foi criado o Usuário3

Depois disso, o usuário está conectado.

Verificação

Roteador IOS

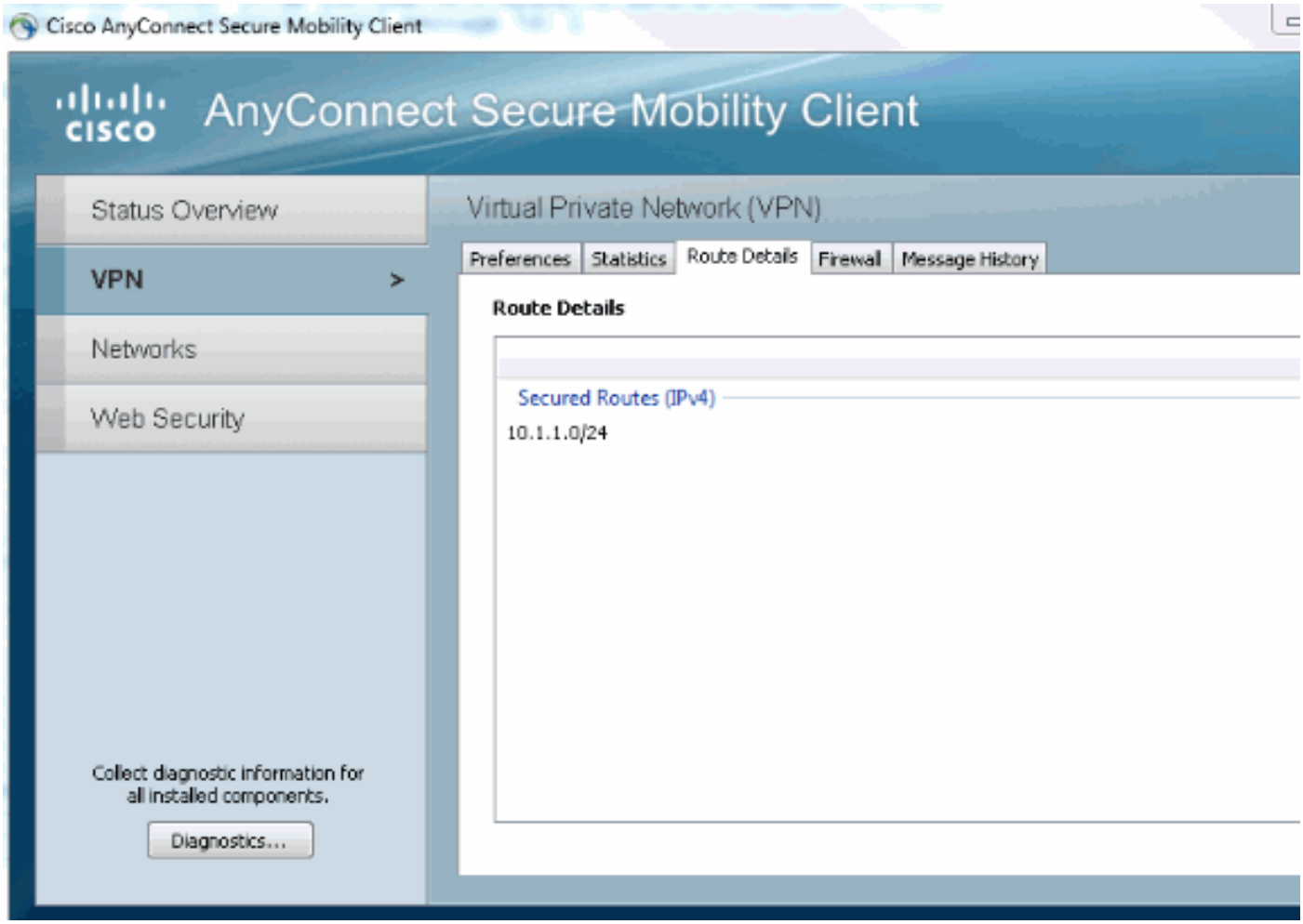
```
R1#show ip inter brief | i Virtual
Virtual-Access1    10.1.1.2  YES unset  up  up
Virtual-Template1  10.1.1.2  YES unset  up down
R1# show ip route 192.168.100.200
Routing entry for 192.168.100.200/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly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

Você pode executar uma depuração (debug crypto ikev2).

Windows

Nas opções avançadas do AnyConnect em VPN, você pode verificar os detalhes da rota para ver as redes de tunelamento dividido:



Problemas conhecidos

- Lembre-se de ter SHA1 em hash de assinatura e na política de integridade em IKEv2 (consulte o bug da Cisco ID CSCtn59317 (somente clientes registrados)).
- CN no certificado de identidade do IOS deve ser igual ao nome do host no perfil XML do ACS.

- Se quiser usar pares de AV de RADIUS aprovados durante a autenticação e não usar a autorização do grupo, você pode usar isso no perfil IKEv2:
  `aaa authorization user eap cached`
- A autorização está sempre usando a senha "cisco" para autorização de grupo/usuários. Isso pode ser confuso ao usar
  `aaa authorization user eap list SERV (without any paramaters)`
  porque ele tentará autorizar o uso do usuário transmitido no AnyConnect como usuário e senha "cisco", que provavelmente não é a senha do usuário.
- Em caso de problemas, essas são saídas que você pode analisar e fornecer ao Cisco TAC:debug crypto ikev2debug crypto ikev2 internalSaídas de DART
- Se não estiver usando SSL VPN, lembre-se de desabilitar o ip http server (no ip http server). Caso contrário, o AnyConnect tentará se conectar ao servidor HTTP e receberá o resultado, "Use um navegador para obter acesso".

Criptografia de próxima geração

A configuração acima é fornecida como referência para mostrar uma configuração de trabalho minimalista.

A Cisco recomenda o uso da Next Generation Cryptography (NGC) onde possível.

As recomendações atuais para migração podem ser encontradas aqui:
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Ao escolher a configuração da NGC, certifique-se de que o software cliente e o hardware de headend o suportem. Os roteadores ISR geração 2 e ASR 1000 são recomendados como headends devido ao suporte de hardware para NGC.

No lado do AnyConnect, a partir da versão 3.1 do AnyConnect, o conjunto de algoritmos Suite B da NSA é suportado.

Informações Relacionadas

- VPN de local de PKI do Cisco ASA IKEv2
- IKEv2 Site2-Site debugs no IOS
- FlexVPN / IKEv2: Cliente incorporado do Windows 7: Headend do IOS: Parte I - Autenticação do certificado
- Guia de Configuração do FlexVPN e Internet Key Exchange Versão 2, Cisco IOS Versão 15.2M&T
- Suporte Técnico e Documentação - Cisco Systems