Desenvolvimento de FlexVPN: Acesso remoto de AnyConnect IKEv2 com EAP-MD5

Índice

Introdução

Este documento fornece uma configuração de exemplo de como estabelecer o Acesso remoto em IO usando o conjunto de ferramentas de FlexVPN.

O acesso remoto VPN permite os fim-clientes que usam vários sistemas operacionais para conectar firmemente a suas redes corporativas ou home com o media NON-seguro tal como o Internet. Na encenação apresentada, o túnel VPN está sendo terminado em um roteador do Cisco IOS que usa o protocolo IKEv2.

Este documento mostra como autenticar e autorizar os usuários que usam o Access Control Server (ACS) com o método do EAP-MD5.

Pré-requisitos

Diagrama de Rede

O roteador do Cisco IOS tem duas relações - uma para ACS 5.3:

Requisitos

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 correção de programa 6
- IOS Router com software de 15.2(4)M
- Windows 7 PC com AnyConnect 3.1.01065

Convenções

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

Background

Em IKEv1 o XAUTH é usado na fase 1.5, você pode fazer a autenticação dos usuários localmente em um IOS Router e RADIUS/TACACS+ remotamente da utilização. IKEv2 não apoia o XAUTH e a fase 1.5 any more. Contém o apoio do acessório EAP, que é feito na fase IKE_AUTH. A vantagem a mais grande desta está no projeto IKEv2 e o EAP é um padrão conhecido.

O EAP apoia dois modos:

- Escavação de um túnel — EAP-TLS, EAP/PSK, EAP-PEAP etc.
- NON-Tunelamento — EAP-MSCHAPv2, EAP-GTC, EAP-MD5 etc.

Neste exemplo, o EAP-MD5 no modo do NON-Tunelamento é usado porque é método de autenticação exterior EAP apoiado atualmente em ACS 5.3.

O EAP pode somente ser usado ao iniciador da autenticação (cliente) ao que responde (IO neste caso).

Configuração inicial IO

IO - CA

Antes de mais nada você precisa de criar o Certificate Authority (CA) e criar um certificado de identidade para o IOS Router. O cliente verificará a identidade do roteador baseada nesse certificado.

A configuração de CA em IO olha como:

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

Você precisa de recordar sobre uso chave prolongado (Server-AUTH necessário para o EAP, porque RSA-SIG você igualmente precisa o Cliente-AUTH).

Permita CA usando o **comando no shutdown no** server cripto CA do pki.

IO - Certificado de identidade

Em seguida, permita o protocolo simple certificate enrollment (SCEP) para o certificado e configurar o ponto confiável.

```
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
```

Então, autentique e registre 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 quer mandar mensagens imediata em AnyConnect recordar que a NC precisa de ser igual ao hostname/endereços IP de Um ou Mais Servidores Cisco ICM NT configurados no perfil de AnyConnect.

Neste exemplo, cn=10.1.1.2. Consequentemente, em AnyConnect 10.1.1.2 é entrado como o endereço IP de Um ou Mais Servidores Cisco ICM NT do server no perfil do xml de AnyConnect.

IO - AAA e configuração RADIUS

Você precisa de configurar o raio e a autenticação de AAA e a autorização:

```
(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
```

Configuração inicial ACS

Primeiramente, adicionar o dispositivo de rede novo no ACS (os recursos de rede > os dispositivos de rede e os clientes de AAA > criam):

Adicionar um usuário (os usuários e a identidade armazenam > identidade interna armazenam > usuários > criam):

Adicionar um usuário para a autorização. Neste exemplo, é IKETEST. A senha precisa de ser “Cisco” porque é o padrão enviado por IO.

Em seguida, crie um perfil da autorização para os usuários (os elementos da política > a autorização e as permissões > os perfis do acesso de rede > da autorização > criam).

Neste exemplo, é chamado POOL. Neste exemplo, o par AV do túnel em divisão (como um prefixo) é inscrito e Framed-IP-endereço como o endereço IP de Um ou Mais Servidores Cisco ICM NT que está indo ser atribuído ao cliente conectado. A lista de todos os pares AV apoiados 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

Então, você precisa de girar sobre o apoio do EAP-MD5 (para a autenticação) e do PAP/ASCII (para a autorização) na política de acesso. O padrão é usado neste exemplo (políticas de acesso > acesso de rede padrão):

Crie uma condição para na política de acesso e atribua o perfil da autorização que foi criado. Neste caso uma condição para NDG: O lugar em todos os lugar é criado, assim para todo o pedido das autorizações RADIUS fornecerá o perfil da autorização do POOL (as políticas de acesso > o acesso prestam serviços de manutenção > acesso de rede padrão):

Você deve poder testar em um IOS Router se o usuário pode 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 IO FlexVPN

Você precisa de criar a proposta IKEv2 e a política (você não pôde tem que, para referir CSCtn59317). A política é criada somente para um dos endereços IP de Um ou Mais Servidores Cisco ICM NT (10.1.1.2) neste exemplo.

```
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"
```

Então, crie um perfil IKEV2 e um perfil IPSec que liguem ao Virtual-molde.

Certifique-se que você está desligando o CERT do URL do HTTP, como recomendado no manual de configuração.

```
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"
```

Neste exemplo, a autorização estabelece-se baseou no usuário IKETEST, que foi criado na configuração ACS.

Configuração de Windows

Importando CA às confianças de Windows

Exporte o certificado de CA em IO (se certifique exportar o certificado de identidade e tomar somente 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 no meio COMEÇAM O CERTIFICADO e TERMINAM O CERTIFICADO e colam-no ao bloco de notas em Windows e salvar como um arquivo CA.crt.

Você precisa de instalá-lo como em autoridades do root confiável (fazer duplo clique no arquivo > instalam o certificado > o lugar todos os Certificados na seguintes loja > Autoridades de certificação de raiz confiável):

Configurando o perfil de AnyConnect XML

No cliente seguro \ perfil da mobilidade de C:\ProgramData\Cisco\Cisco AnyConnect crie um arquivo “whatever.xml” e cole isto:


```
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-----
```


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

Testes

Nesta encenação SSL O VPN não é usado, assim que certifique-se que o Server do HTTP está desabilitado em IO (nenhum server do HTTP de IP). Se não, você recebe um Mensagem de Erro em AnyConnect que indica, “usa um navegador para aceder”.

Ao conectar em AnyConnect, você deve ser alertado para uma senha. Neste exemplo, é User3 que foi criado

Após o esse, o usuário é 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 debugar (debug crypto ikev2).

Windows

Nas opções avançadas de AnyConnect no VPN você pode verificar detalhes da rota para ver as redes do Split Tunneling:

Advertências conhecidas e edições

- Recorde ao ter o SHA1 na mistura da assinatura e na política da integridade em IKEv2 (refira a identificação de bug Cisco CSCtn59317 (clientes registrados somente)).
- O CN no certificado de identidade IO tem que ser hostname igual no perfil ACS XML.
- Se você quer usar os pares AV do raio passados durante a autenticação e não a autorização do uso do grupo de todo, você pode usar este no perfil IKEv2:

```
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
```

- A autorização está usando sempre a senha “Cisco” para a autorização do grupo/usuários. Isto pôde ser desconcertante ao usar-se

```
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
```

porque tentará autorizar usando o usuário passado em AnyConnect como o usuário e a senha “Cisco”, que não é provavelmente a senha para o usuário.

- Em caso de todas as edições estas são as saídas que você pode analisar e fornecer ao tac Cisco:debug crypto ikev2debug crypto ikev2 internoSaídas do DARDO
- Se não usando SSL VPN recorde desabilitar o server do HTTP de IP (nenhum server do HTTP de IP). Se não, AnyConnect tentará conectar ao Server do HTTP e receber o resultado, “usa um navegador para aceder”.

Criptografia da próxima geração

A configuração acima é fornecida para que a referência mostre uma configuração em funcionamento minimalistic.

Cisco recomenda usar a criptografia da próxima geração (NGC) sempre que seja possível.

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

Ao escolher a configuração NGC, certifique-se de que software do cliente e suporte a hardware do final do cabeçalho ele. A geração 2 ISR e os 1000 Router ASR são recomendados como finais do cabeçalho devido a seu suporte a hardware para NGC.

No lado de AnyConnect, até à data da versão de AnyConnect 3.1, a série do algorythm da série B do NSA é apoiada.

Informações Relacionadas

- Local-local VPN de Cisco ASA IKEv2 PKI
- IKEv2 Site2-Site debuga em IO
- FlexVPN/IKEv2: Acessório de Windows 7 - Cliente: Final do cabeçalho IO: Parte mim - Certificado de autenticação
- FlexVPN e manual de configuração da versão 2 do intercâmbio de chave de Internet, Cisco IOS Release 15.2M&T
- Suporte Técnico e Documentação - Cisco Systems