Exemplo de configuração de FlexVPN entre um roteador e um ASA com criptografia de próxima geração

Contents

Introduction

Este documento descreve como configurar uma VPN entre um roteador com FlexVPN e um Adaptive Security Appliance (ASA) que suporta os algoritmos de criptografia de próxima geração (NGE) da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- Internet Key Exchange versão 2 (IKEv2)
- IPSec
- ASA

- Criptografia de próxima geração

Componentes Utilizados

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

- **Hardware:** Roteador IOS geração 2 (G2) que executa a licença de segurança.
- **Software:** Software Cisco IOS® versão 15.2-3.T2. Qualquer versão de M ou T para versões posteriores à versão 15.1.2T do software Cisco IOS® pode ser usada porque isso está incluído na introdução do Modo de contador Galois (GCM).
- **Hardware:** ASA que suporta NGE.**Observação:** somente as plataformas de multi-núcleo suportam o Advanced Encryption Standard (AES) GCM.
- **Software:** Software ASA versão 9.0 ou posterior compatível com NGE.
- OpenSSL.

Para obter detalhes, consulte o Cisco Feature Navigator.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Criar dinamicamente associações de segurança IPSec

A interface IPSec recomendada no IOS é uma Virtual Tunnel Interface (VTI), que cria uma interface GRE (Generic Routing Encapsulation) protegida por IPsec. Para um VTI, o Seletor de Tráfego (que tráfego deve ser protegido pelas associações de segurança (SA) do IPSec) consiste no tráfego GRE da origem do túnel até o destino do túnel. Como o ASA não implementa interfaces GRE, mas cria SAs IPSec com base no tráfego definido em uma lista de controle de acesso (ACL), devemos habilitar um método que permita ao roteador responder à iniciação do IKEv2 com um espelho dos seletores de tráfego propostos. O uso de Dynamic Virtual Tunnel Interface (DVTI) no roteador FlexVPN permite que esse dispositivo responda ao Seletor de Tráfego apresentado com um espelho do Seletor de Tráfego apresentado.

Este exemplo criptografa o tráfego entre as duas redes internas. Quando o ASA apresenta os seletores de tráfego da rede interna do ASA para a rede interna do IOS, `192.168.1.0/24` para `172.16.10.0/24`, a interface DVTI responde com um espelho dos seletores de tráfego, que é `172.16.10.0/24` para `192.168.1.0/24`.

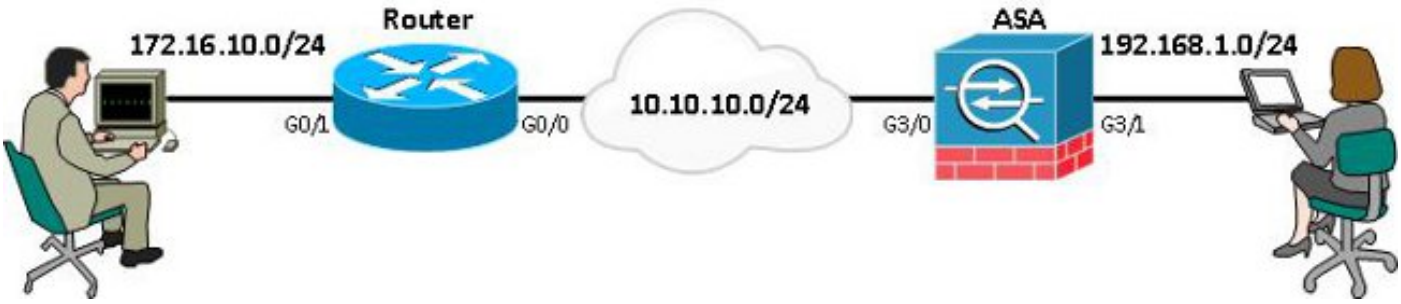
Autoridade de certificação

Atualmente, o IOS e o ASA não suportam um servidor de Autoridade de Certificação (CA) local com certificados Elliptic Curve Digital Signature Algorithm (ECDSA), necessários para o Suite-B. Portanto, um servidor de CA de terceiros deve ser implementado. Por exemplo, use o OpenSSL para atuar como uma CA.

Configuração

Topologia de rede

Este guia é baseado na topologia mostrada neste diagrama. Você deve alterar os endereços IP para se adequar.



Observação: a configuração inclui uma conexão direta do roteador e do ASA. Eles podem ser separados por muitos saltos. Se sim, certifique-se de que haja uma rota para chegar ao endereço IP do peer. A configuração a seguir detalha somente a criptografia usada.

Etapas necessárias para permitir que o roteador use o ECDSA

Autoridade de certificação

1. Criar um **par de chaves de curva elíptica.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. Criar um **certificado autoassinado com curva elíptica**.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. Crie **nome de domínio** e **nome de host**, que são pré-requisitos para criar um par de chaves de curva elíptica (EC).
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. Crie um **ponto de confiança** local para obter um certificado da AC.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   Nota: Como a AC está offline, a verificação de revogação está desativada; a verificação de revogação deve ser habilitada para a segurança máxima em um ambiente de produção.
3. Autentique o **ponto de confiança**. Isso obtém uma cópia do certificado da CA, que contém a chave pública.
   ```
   crypto pki authenticate ec_ca
   ```
4. Em seguida, é solicitado que você insira o certificado codificado base 64 da CA. Este é o arquivo ca.pem, criado com o OpenSSL. Para visualizar esse arquivo, abra-o em um editor ou com o comando OpenSSL **openssl x509 -in ca.pem**. Digite **quit** quando colar isto. Em

seguida, digite **yes** para aceitar.

5. Inscreva o roteador na Public Key Infrastructure (PKI) na CA.
   ```
   crypto pki enrol ec_ca
   ```
6. A saída que você recebe precisa ser usada para enviar uma solicitação de certificado para a CA. Isso pode ser salvo como um arquivo de texto (flex.csr) e assinado com o comando OpenSSL.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
   ```
7. Importe o certificado, que está contido no arquivo flex.pem, gerado da CA, para o roteador depois de inserir esse comando. Em seguida, insira **sair** quando terminar.
   ```
   crypto pki import ec_ca certificate
   ```

ASA

1. Crie **nome de domínio** e **nome de host**, que são pré-requisitos para criar um par de chaves EC.
   ```
   domain-name cisco.com
   hostname ASA1
   crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
   ```
2. Crie um **ponto de confiança** local para obter um certificado da AC.
   ```
   crypto ca trustpoint ec_ca
    enrollment terminal
    subject-name cn=asa1.cisco.com
    revocation-check none
    keypair asa1.cisco.com
   ```
   Nota: Como a AC está offline, a verificação de revogação está desativada; a verificação de revogação deve ser habilitada para a segurança máxima em um ambiente de produção.
3. Autentique o **ponto de confiança**. Isso obtém uma cópia do certificado da CA, que contém a chave pública.
   ```
   crypto ca authenticate ec_ca
   ```
4. Em seguida, é solicitado que você insira o certificado codificado base 64 da CA. Este é o arquivo ca.pem, criado com o OpenSSL. Para visualizar esse arquivo, abra-o em um editor ou com o comando OpenSSL **openssl x509 -in ca.pem**. Digite **quit** quando colar este arquivo e digite **yes** para aceitar.
5. Inscreva o ASA no PKI na CA.
   ```
   crypto ca enrol ec_ca
   ```
6. A saída que você recebe deve ser usada para enviar uma solicitação de certificado para a CA. Isso pode ser salvo como um arquivo de texto (asa.csr) e, em seguida, assinado com o comando OpenSSL.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
   ```
7. Importe o certificado, que está contido no arquivo como a.pem, gerado da CA para o roteador depois que esse comando for inserido. Em seguida, **digite** quit quando concluído.
   ```
   crypto ca import ec_ca certificate
   ```

Configuração

FlexVPN

Crie um mapa de certificado para corresponder ao certificado do dispositivo de peer.

```
crypto pki certificate map certmap 10
```

```
 subject-name co cisco.com
```

Insira estes comandos para a configuração do Suite-B na Proposta de IKEv2:

Observação: para segurança máxima, configure com o comando **aes-cbc-256 com sha512 hash**.

```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

Faça a correspondência do perfil IKEv2 com o mapa de certificados e use ECDSA com o **ponto de confiança** previamente definido.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ec_ca
 virtual-template 1
```

Configure a transformação de IPSec para usar o Modo de Contador Galois (GCM).

```
crypto ipsec transform-set ESP_GCM esp-gcm
 mode transport
```

Configure o perfil de IPSec com os parâmetros configurados anteriormente.

```
crypto ipsec profile default
 set transform-set ESP_GCM
 set pfs group19
 set ikev2-profile default
```

Configure a interface do túnel:

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Aqui está a configuração da interface:

```
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 172.16.10.1 255.255.255.0
```

ASA

Use esta configuração de interface:

```
interface GigabitEthernet3/0
 nameif outside
 security-level 0
```

```
 ip address 10.10.10.2 255.255.255.0
interface GigabitEthernet3/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

Insira este comando da lista de acesso para definir o tráfego a ser criptografado:

```
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0 255.255.255.0
```

Insira este comando de proposta de IPSec com o NGE:

```
crypto ipsec ikev2 ipsec-proposal prop1
 protocol esp encryption aes-gcm
 protocol esp integrity null
```

Comandos do mapa de criptografia:

```
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 10.10.10.1
crypto map mymap 10 set ikev2 ipsec-proposal prop1
crypto map mymap 10 set trustpoint ec_ca
crypto map mymap interface outside
```

Este comando configura a política de IKEv2 com o NGE:

```
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
```

Grupo de túnel configurado para comandos peer:

```
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 peer-id-validate cert
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate ec_ca
```

Verificação de conexão

Verifique se as chaves ECDSA foram geradas com êxito.

```
Router1#show crypto key mypubkey ec router1.cisco.com
% Key pair was generated at: 21:28:26 UTC Feb 19 2013
Key name: router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
<...omitted...>

ASA-1(config)#show crypto key mypubkey ecdsa
Key pair was generated at: 21:11:24 UTC Feb 19 2013
```

```
Key name: asa1.cisco.com
 Usage: General Purpose Key
 EC Size (bits): 256
 Key Data&colon;
<...omitted...>
```

Verifique se o certificado foi importado com êxito e se ECDSA foi usado.

```
Router1#show crypto pki certificates verbose
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0137
  Certificate Usage: General Purpose
  Issuer:
<...omitted...>
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    EC Public Key:  (256 bit)
  Signature Algorithm: SHA256 with ECDSA


ASA-1(config)#show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 00a293f1fe4bd49189
  Certificate Usage: General Purpose
  Public Key Type: ECDSA (256 bits)
  Signature Algorithm: SHA256 with ECDSA Encryption
 <...omitted...>
```

Verifique se o SA IKEv2 foi criado com êxito e usa os algoritmos NGE configurados.

```
Router1#show crypto ikev2 sa  detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        10.10.10.2/500        none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      Life/Active Time: 86400/94 sec


ASA-1#show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status         Role
268364957        10.10.10.2/500        10.10.10.1/500      READY    INITIATOR
      Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      <...omitted...>
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xe847d8/0x12bce4d
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Verifique se a SA IPSec foi criada com êxito e usa os algoritmos NGE configurados.

Observação: o FlexVPN pode encerrar conexões IPSec de clientes não IOS que suportam os protocolos IKEv2 e IPSec.

```
Router1#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.10.10.2 port 500
     PERMIT, flags={origin_is_acl,}
<...omitted...>

     inbound esp sas:
      spi: 0x12BCE4D(19648077)
        transform: esp-gcm ,
        in use settings ={Tunnel, }

ASA-1#show crypto ipsec sa detail
interface: outside
    Crypto map tag: mymap, seq num: 10, local addr: 10.10.10.2

      access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0
        255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
      current_peer: 10.10.10.1
<...omitted...>


    inbound esp sas:
      spi: 0x00E847D8 (15222744)
         transform: esp-aes-gcm esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
```

Para obter mais informações sobre a implementação do Suite-B pela Cisco, consulte o white paper Criptografia de próxima geração.

Consulte a página da solução de criptografia de próxima geração para saber mais sobre a implementação da criptografia de próxima geração da Cisco.

Informações Relacionadas

- White paper sobre criptografia de próxima geração
- Página da solução de criptografia de próxima geração
- Secure Shell (SSH)
- Negociação IPsec/Protocolos IKE
- Depurações do ASA IKEv2 para VPN site a site com PSKs TechNote
- ASA IPSec e IKE debugs (modo principal IKEv1) - Nota técnica de solução de problemas
- IOS IPSec e depurações IKE - IKEv1 Main Mode Troubleshooting TechNote
- IPSec ASA e depurações de IKE - modo agressivo IKEv1 TechNote
- Suporte Técnico e Documentação - Cisco Systems