Exemplo de configuração de FlexVPN com criptografia de próxima geração

Contents

Introduction

Este documento descreve como configurar um FlexVPN entre dois roteadores que suportam o conjunto de algoritmos Cisco Next-Generation Encryption (NGE).

Criptografia de última geração

A criptografia Cisco NGE protege informações que trafegam por redes que usam quatro algoritmos criptográficos configuráveis, bem estabelecidos e de domínio público:

- Criptografia baseada no Advanced Encryption Standard (AES), que usa chaves de 128 ou 256 bits
- Assinaturas digitais com o Elliptic Curve Digital Signature Algorithm (ECDSA) que utilizam curvas com módulo prime de 256 e 384 bits
- Troca de chave que usa o método Elliptic Curve Diffie-Hellman (ECDH)
- Hashing (impressões digitais) com base no Secure Hash Algorithm 2 (SHA-2)

A Agência Nacional de Segurança (NSA) afirma que estes quatro algoritmos combinados fornecem garantia de informações adequadas para informações classificadas. A criptografia do NSA Suite B para IPsec foi publicada como padrão no RFC 6379 e ganhou aceitação no setor.

Suite-B-GCM-128

De acordo com o RFC 6379, esses algoritmos são necessários para o conjunto Suite-B-GCM-128.

Este pacote oferece proteção de integridade e confidencialidade de carga útil de segurança de encapsulamento (ESP - Encapsulating Security Payload) com AES-GCM de 128 bits (consulte RFC4106). Esse conjunto deve ser usado quando a proteção de integridade e a criptografia do ESP forem necessárias.

ESP
Criptografia AES com chaves de 128 bits e valor de verificação de integridade (ICV) de 16 octetos no modo Galois/Counter (GCM) (RFC4106)
Integridade NULO

IKEv2
Criptografia AES com chaves de 128 bits no modo CBC (Cipher Block Chaining) (RFC3602)
Função pseudoaleatória HMAC-SHA-256 (RFC4868)
Integridade HMAC-SHA-256-128 (RFC4868)
Grupo Diffie-Hellman 256-bit aleatório ECP group (RFC5903)

Mais informações sobre o Suite B e o NGE podem ser encontradas na Criptografia de última geração.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- Internet Key Exchange versão 2 (IKEv2)
- IPsec

Componentes Utilizados

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

- Hardware: Integrated Services Routers (ISR) Generation 2 (G2) que executam a licença de segurança.
- Software: Software Cisco IOS® versão 15.2.3T2. Qualquer versão do Cisco IOS Software Release M ou 15.1.2T ou posterior pode ser usada, pois é quando o GCM foi introduzido.

Para obter detalhes, consulte o Navegador de Recursos.

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.

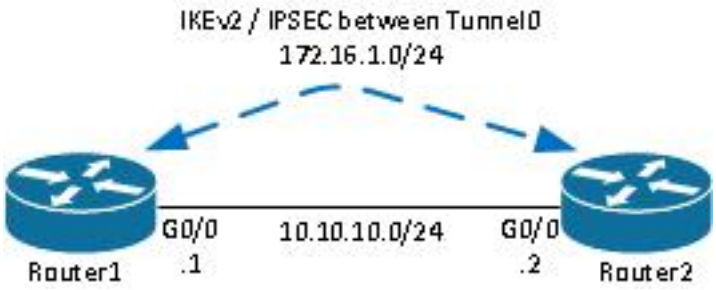
Autoridade de certificação

Atualmente, o software Cisco IOS não oferece suporte a um servidor de Autoridade de Certificação (CA - Certificate Authority) local que executa o ECDH, necessário para o Suite B. Um servidor de CA de terceiros deve ser implementado. Este exemplo usa um Microsoft CA baseado em Suite B PKI

Configurar

Topologia de rede

Este guia é baseado nessa topologia ilustrada. Os endereços IP devem ser alterados de acordo com seus requisitos.



Notas:

A configuração consiste em dois roteadores conectados diretamente, que podem ser separados por muitos saltos. Em caso afirmativo, certifique-se de que haja uma rota para chegar ao endereço IP do peer. Essa configuração detalha apenas a criptografia usada. O roteamento IKEv2 ou um protocolo de roteamento deve ser implementado através do IPSec VPN.

Etapas necessárias para permitir que o roteador use o algoritmo de assinatura digital de curva elíptica

1. Crie o nome de domínio e o nome de host, que são pré-requisitos para criar um par de chaves EC.

   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label Router1.cisco.com
   ```

   Note: A menos que você execute uma versão com a correção para o bug da Cisco ID CSCue59994, o roteador não permitirá que você inscreva um certificado com um tamanho de chave inferior a 768.
2. Crie um ponto confiável local para obter um certificado da CA.

   ```
   crypto pki trustpoint ecdh
   ```

```
 enrollment terminal
 revocation-check none
 eckeypair Router1.cisco.com
```

Note: Como a AC estava offline, as verificações de revogação foram desativadas. As verificações de revogação devem ser habilitadas para garantir a segurança máxima em um ambiente de produção.

3. Autentique o ponto de confiança (obtém uma cópia do certificado da AC que contém a chave pública).

```
crypto pki authenticate ecdh
```

4. Insira o certificado codificado base 64 da CA no prompt. Digite **quit** e digite **yes** para aceitar.

5. Inscreva o roteador no PKI na CA.

```
crypto pki enrol ecdh
```

6. A saída exibida é usada para enviar uma solicitação de certificado à CA. Para a AC da Microsoft, conecte-se à interface da Web da AC e selecione **Submit a certificate request**.

7. Importar o certificado recebido da CA para o roteador. Insira **quit** depois que o certificado for importado.

```
crypto pki import ecdh certificate
```

Configuração

A configuração fornecida aqui é para Router1. O Roteador 2 exige um espelho da configuração em que somente os endereços IP na interface do túnel são exclusivos.

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

```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

2. Configure a proposta de IKEv2 para o Suite B.

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

Note: Os padrões inteligentes IKEv2 implementam vários algoritmos pré-configurados na proposta padrão de IKEv2. Como aes-cbc-128 e sha256 são necessários para o conjunto

Suite-B-GCM-128, você deve remover aes-cbc-256, sha384 e sha512 nesses algoritmos. A razão para isso é que o IKEv2 escolhe o algoritmo mais forte quando apresentado com uma escolha. Para máxima segurança, use aes-cbc-256 e sha512. No entanto, isso não é necessário para o Suite-B-GCM-128. Para visualizar a proposta configurada de IKEv2, insira o comando **show crypto ikev2 Proposal**.

3. Configure o perfil IKEv2 para corresponder ao mapa de certificados e use ECDSA com o ponto de confiança definido anteriormente.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ecdh
```

4. Configure a transformação de IPSec para usar o GCM.

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

5. 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
```

6. Configure a interface do túnel.

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Gigabit0/0 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

Verificar a conexão

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Verifique se as chaves ECDSA foram geradas com êxito.

```
Router1#show crypto key mypubkey ec
% Key pair was generated at: 04:05:07 JST Jul 6 2012
Key name: Router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
 30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 4200048F 2B0B5B5E
(...omitted...)
```

2. Verifique se o certificado foi importado com êxito e se ECDH é usado.

```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. Verifique se o SA IKEv2 foi criado com êxito e usa os algoritmos Suite B.

```
Router1#show crypto ikev2 sa
 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: SHA256, DH Grp:19, Auth sign: ECDSA, Auth verify:
ECDSA
     Life/Active Time: 86400/20 sec
```

4. Verifique se o SA IKEv2 foi criado com êxito e usa os algoritmos Suite B.

```
Router1#show crypto ipsec sa

interface: Tunnel0
   Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

(...omitted...)

    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
    plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xAC5845E1(2891466209)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xAEF7FD9C(2935487900)
       transform: esp-gcm ,
       in use settings ={Transport, }
       conn id: 6, flow_id: SW:6, sibling_flags 80000000, crypto map: Tunnel0-head-0
       sa timing: remaining key lifetime (k/sec): (4341883/3471)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
```

Note: Nesta saída, ao contrário do Internet Key Exchange versão 1 (IKEv1), o valor do grupo Diffie-Hellman (DH) do PFS (Forwarding Signal Signal Segredo) é mostrado como **PFS (Y/N): N, grupo DH: nenhum** durante a primeira negociação de túnel, mas depois que uma chave de rechaveamento ocorre, os valores corretos são exibidos. Este não é um bug embora o comportamento seja descrito na ID de bug da Cisco CSCug67056. A diferença entre IKEv1 e IKEv2 é que, neste último caso, as associações de segurança infantil (SAs) são criadas como parte da própria troca de AUTH. O Grupo DH configurado no mapa de

criptografia é usado somente durante a chave de rechaveamento. Assim, você vê **PFS (S/N): N, grupo DH: nenhuma** até a primeira chave. Mas com IKEv1, você vê um comportamento diferente porque a criação de SA filho acontece durante o Modo rápido e a mensagem CREATE_CHILD_SA tem uma provisão para transportar a carga útil do Key Exchange que especifica os parâmetros DH para derivar um novo segredo compartilhado.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Conclusão

Os algoritmos criptográficos eficientes e fortes definidos na NGE fornecem garantia a longo prazo de que a confidencialidade e a integridade dos dados são fornecidas e mantidas a um baixo custo de processamento. O NGE pode ser facilmente implementado com o FlexVPN, que fornece criptografia padrão da Suite B.

Mais informações sobre a implementação da Suite B da Cisco podem ser encontradas na Criptografia de última geração.