FlexVPN com exemplo da configuração de criptografia da próxima geração

Índice

Introdução

Este documento descreve como configurar um FlexVPN entre dois Roteadores que apoia a criptografia da próxima geração de Cisco (NGE) se ajusta dos algoritmos.

Criptografia da próxima geração

A criptografia de Cisco NGE fixa a informação que viaja sobre as redes que usam quatro configuráveis, bem conhecido, e os algoritmos criptográficos do public domain:

- Criptografia baseada no Advanced Encryption Standard (AES), que usa o 128-bit ou as chaves do 256-bit
- Assinaturas digital com o Digital Signature Algorithm elíptico da curva (ECDSA) que esse uso se curva com 256-bit e os módulos principais do 384-bit
- Trocas de chave que usam o método elíptico de Diffie-Hellman da curva (ECDH)
- Picar (impressões digitais digitais) baseado no algoritmo de mistura segura 2 (SHA-2)

O National Security Agency (NSA) indica que estes quatro algoritmos na combinação oferecem a garantia da informação adequada para a informação secreta. A criptografia da série B NSA para o IPsec foi publicada como um padrão no RFC 6379 e ganhou a aceitação na indústria.

Série Suite-B-GCM-128

Conforme o RFC 6379, estes algoritmos são exigidos para a série Suite-B-GCM-128.

Esta série fornece a proteção e a confidencialidade da integridade do Encapsulating Security Payload (ESP) o 128-bit AES-GCM (veja o RFC4106). Esta série deve ser usada quando a proteção da integridade ESP e a criptografia ambos são precisadas.

ESP
Criptografia AES com chaves do 128-bit e valor da verificação de integridade 16-octet (ICV) em Galois/modo contrário (GCM) (RFC4106)
ZERO da integridade

IKEv2
Criptografia AES com chaves do 128-bit no modo do Cipher Block Chaining (CBC) (RFC3602)
função Pseudo--aleatória HMAC-SHA-256 (RFC4868)
Integridade HMAC-SHA-256-128 (RFC4868)
Grupo aleatório do 256-bit ECP do grupo Diffie-Hellman (RFC5903)

Mais informação na série B e NGE pode ser encontrada na criptografia da próxima geração.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- Versão 2 do intercâmbio de chave de Internet (IKEv2)
- IPsec

Componentes Utilizados

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

- Hardware: Esse da geração 2 do Roteadores dos Serviços integrados (ISR) (G2) executado a licença da Segurança.
- Software: Liberação 15.2.3T2 do Cisco IOS ® Software. Toda a liberação do Cisco IOS Software Release M ou 15.1.2T ou mais tarde pode ser usada desde que esta é quando GCM foi introduzido.

Para detalhes, refira o navegador da característica.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Certificate Authority

Atualmente, o Cisco IOS Software não apoia um server local do Certificate Authority (CA) que execute ECDH, que é exigido para a série B. Um server de CA da terceira parte deve ser executado. Este exemplo usa Microsoft CA baseado na série B PKI

Configurar

Topologia de rede

Este guia é baseado nesta topologia ilustrada. Os endereços IP de Um ou Mais Servidores Cisco ICM NT devem ser alterados para serir suas exigências.

Notas:

A instalação consiste em dois Roteadores conectados diretamente, que puderam ser separados por muitos saltos. Em caso afirmativo, assegure-se de que haja uma rota a obter ao endereço IP do peer. Esta configuração detalha somente a criptografia usada. O roteamento IKEv2 ou um protocolo de roteamento devem ser executados sobre o IPSec VPN.

Etapas exigidas para permitir o roteador de usar o Digital Signature Algorithm elíptico da curva

1. Crie o Domain Name e o hostname, que são condições prévias para criar um keypair EC.

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

   Note: A menos que você executar uma versão com o reparo para a identificação de bug Cisco CSCue59994, o roteador não permitirá que você registre um certificado com um keysize menos de 768.
2. Crie um ponto confiável local a fim ganhar um certificado de CA.

```
crypto pki trustpoint ecdh
 enrollment terminal
 revocation-check none
 eckeypair Router1.cisco.com
```

   Note: Desde que CA era autônomo, as verificações da revogação foram desabilitadas. As verificações da revogação devem ser permitidas para a segurança máxima em um ambiente de produção.

3. Autentique o ponto confiável (isto obtém uma cópia do certificado de CA que contém a

chave pública).

```
crypto pki authenticate ecdh
```

4. Entre no certificado codificado da base 64 de CA na alerta. Entre **parado** e entre então **sim** para aceitar.

5. Registre o roteador no PKI em CA.

```
crypto pki enrol ecdh
```

6. A saída indicada é usada a fim submeter um pedido do certificado a CA. Para Microsoft CA, conecte à interface da WEB de CA e seleto **submeta um pedido do certificado**.

7. Importe o certificado recebido de CA no roteador. Entre **parado** uma vez que o certificado é importado.

```
crypto pki import ecdh certificate
```

Configuração

A configuração fornecida aqui é para o roteador1. O roteador2 exige um espelho da configuração onde somente os endereços IP de Um ou Mais Servidores Cisco ICM NT na interface de túnel são originais.

1. Crie um mapa do certificado para combinar o certificado do dispositivo de peer.

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

2. Configurar a proposta IKEv2 para a série B.

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

Note: Os padrões IKEv2 espertos executam um número de algoritmos preconfigured dentro da proposta do padrão IKEv2. Desde que aes-cbc-128 e sha256 são exigidos para a série Suite-B-GCM-128, você deve remover aes-cbc-256, sha384, e sha512 dentro destes algoritmos. A razão para esta é que IKEv2 escolhe o algoritmo o mais forte quando apresentado com uma escolha. Para a segurança máxima, use aes-cbc-256 e sha512. Contudo, isto não é exigido para Suite-B-GCM-128. A fim ver a proposta IKEv2 configurada, incorpore o comando **cripto da proposta ikev2 da mostra**.

3. Configurar o perfil IKEv2 para combinar o mapa do certificado e para usar ECDSA com o

ponto confiável definido mais cedo.

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

4. Configurar o IPsec transformam para usar GCM.

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

5. Configurar o perfil IPSec com os parâmetros configurados mais cedo.

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

6. Configurar a interface de 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
```

Verifique a conexão

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

1. Verifique que as chaves ECDSA estiveram geradas com sucesso.

```
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 que o certificado esteve importado com sucesso e que ECDH está usado.

```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
```

```
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. Verifique que IKEv2 SA esteve criado com sucesso e use os algoritmos da série 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 que IKEv2 SA esteve criado com sucesso e use os algoritmos da série 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 na versão 1 do intercâmbio de chave de Internet (IKEv1), o valor de grupo do Diffie-Hellman (DH) do discrição perfeita adiante (PFS) mostra como o **PFS (Y/N): N, grupo DH: nenhuns** durante a primeira negociação do túnel, mas depois que um rekey ocorre, os valores direitos mostram. Este não é um erro mesmo que o comportamento seja descrito na identificação de bug Cisco CSCug67056. A diferença entre IKEv1 e IKEv2 é que, nos últimos, as associações de segurança da criança (SA) estão criadas como parte da troca própria do AUTH. O grupo DH configurado sob o crypto map é usado somente durante o rekey. Daqui, você vê o **PFS (Y/N): N, grupo DH: nenhuns** até os primeiros rekey. Mas com IKEv1, você vê um comportamento diferente porque a criação criança SA acontece durante o Quick Mode e a mensagem CREATE_CHILD_SA tem uma disposição para levar o payload das trocas de chave que especifica os parâmetros DH para derivar um segredo compartilhado novo.

Troubleshooting

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

Conclusão

Os algoritmos criptográficos eficientes e fortes definidos em NGE oferecem a garantia a longo prazo que os dados confidencialmente e a integridade estão fornecidos e mantidos a baixos custos para processar. NGE pode facilmente ser executado com FlexVPN, que fornece a criptografia do padrão da série B.

A informação adicional na aplicação de Cisco da série B pode ser encontrada na criptografia da próxima geração.