FlexVPN con el ejemplo de la configuración de encripción de la última generación

Contenido

Introducción

Este documento describe cómo configurar un FlexVPN entre dos Routers que soporte la última generación de Cisco que el cifrado (NGE) fijó de los algoritmos.

Cifrado de la última generación

La criptografía de Cisco NGE asegura la información que viaja sobre las redes que utilizan cuatro configurables, establecido, y los algoritmos criptográficos del public domain:

- Cifrado basado en el Advanced Encryption Standard (AES), que utiliza el 128-bit o las claves del 256-bit
- Firmas digitales con el Digital Signature Algorithm elíptico de la curva (ECDSA) que ese uso curva con el 256-bit y los módulos primeros del 384-bit
- Intercambio de claves que utiliza el método elíptico de Diffie Hellman de la curva (ECDH)
- El desmenuzar (huellas dactilares digitales) basado en el algoritmo de troceo seguro 2 (SHA-2)

Los estados del National Security Agency (NSA) que estos cuatro algoritmos en la combinación ofrecen la garantía de la información adecuada para la información clasificada. La criptografía de la habitación B NSA para el IPSec se ha publicado como estándar en el RFC 6379 y ha ganado la

aceptación en la industria.

Habitación Suite-B-GCM-128

Según el RFC 6379, estos algoritmos se requieren para la habitación Suite-B-GCM-128.

Esta habitación proporciona la protección y la confidencialidad de la integridad del Encapsulating Security Payload (ESP) con el 128-bit AES-GCM (véase el RFC4106). Esta habitación debe ser utilizada cuando se necesitan la protección y el cifrado ambas de la integridad ESP.

ESP
Cifrado AES con las claves y el valor de la verificación de la integridad 16-octet (ICV) del 128-bit en Galois/el modo contrario (GCM) (RFC4106)
FALTA DE INFORMACIÓN de la integridad

IKEv2
Cifrado AES con las claves del 128-bit en el modo del Cipher Block Chaining (CBC) (RFC3602)
Función pseudoaleatoria HMAC-SHA-256 (RFC4868)
Integridad HMAC-SHA-256-128 (RFC4868)
Grupo al azar del 256-bit ECP del grupo Diffie-Hellman (RFC5903)

Más información sobre la habitación B y NGE se puede encontrar en el cifrado de la última generación.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexVPN
- Intercambio de claves de Internet versión 2 (IKEv2)
- IPSec

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Hardware Ese de la generación 2 (G2) del Routers de los Servicios integrados (ISR) ejecutado la licencia de la Seguridad.
- Software: Versión 15.2.3T2 del Cisco IOS ® Software. Cualquier versión de la versión de Cisco IOS Software puede ser utilizada M o 15.1.2T o más adelante puesto que es ésta cuando GCM fue introducido.

Para los detalles, refiera al navegador de la característica.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

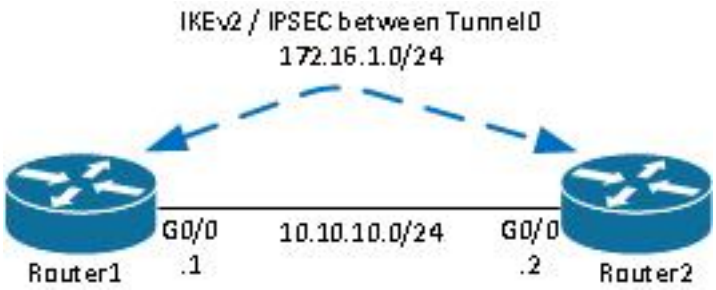
Certificate Authority

Actualmente, el Cisco IOS Software no soporta un servidor local del Certificate Authority (CA) que ejecute ECDH, que se requiere para el paquete B. Un servidor del otro vendedor CA debe ser implementado. Este ejemplo utiliza Microsoft CA basado en el paquete B PKI

Configurar

Topología de red

Esta guía se basa en esta topología ilustrada. Los IP Addresses se deben enmendar para adaptarse a sus requisitos.



Notas:

La configuración consiste en dos Routers conectado directamente, que pudieron ser separados por muchos saltos. Si es así asegúrese de que haya una ruta a conseguir al IP Address de Peer. Esta configuración detalla solamente el cifrado usado. La encaminamiento IKEv2 o un Routing Protocol se debe implementar sobre el IPSec VPN.

Pasos requeridos para permitir al router para utilizar el Digital Signature Algorithm elíptico de la curva

1. Cree el Domain Name y el nombre de host, que son requisitos previos para crear un keypair EC.
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label Router1.cisco.com
   ```
   Nota: A menos que usted funcione con una versión con el arreglo para el Id. de bug Cisco CSCue59994, el router no permitirá que usted aliste un certificado con un keysize menos de 768.
2. Cree un trustpoint local para ganar un certificado de CA.

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

Nota: Puesto que CA era offline, los controles de la revocación fueron inhabilitados. Los controles de la revocación se deben habilitar para la seguridad máxima en un entorno de producción.

3. Autentique el trustpoint (esto obtiene una copia del certificado de CA que contiene la clave pública).
```
crypto pki authenticate ecdh
```

4. Ingrese el certificado codificado base64 del CA en el prompt. Ingrese **salido** y después ingrese **sí** para validar.

5. Aliste al router en el PKI en CA.
```
crypto pki enrol ecdh
```

6. La salida visualizada se utiliza para presentar un pedido de certificado a CA. Para Microsoft CA, conecte con la interfaz Web de CA y selecto **presente un pedido de certificado**.

7. Importe el certificado recibido de CA en el router. Ingrese **salido** una vez que se importa el certificado.
```
crypto pki import ecdh certificate
```

Configuración

La configuración proporcionada aquí está para el router1. El router2 requiere un espejo de la configuración donde solamente están únicos los IP Addresses en la interfaz del túnel.

1. Cree una correspondencia del certificado para hacer juego el certificado del dispositivo de peer.
```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

2. Configure la oferta IKEv2 para la habitación B.
```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

Nota: Los valores por defecto elegantes IKEv2 implementan varios algoritmos preconfigurados dentro de la oferta del valor por defecto IKEv2. Puesto que aes-cbc-128 y sha256 se requieren para la habitación Suite-B-GCM-128, usted debe quitar aes-cbc-256, sha384, y sha512 dentro de estos algoritmos. La razón de esto es que IKEv2 elige el algoritmo más fuerte cuando está presentado con una opción. Para la seguridad máxima, el uso aes-cbc-256 y sha512. Sin embargo, esto no se requiere para Suite-B-GCM-128. Para ver la oferta configurada IKEv2, ingrese el comando **crypto de la oferta ikev2 de la demostración**.

3. Configure el perfil IKEv2 para hacer juego la correspondencia del certificado y para utilizar ECDSA con el trustpoint definido anterior.

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

4. Configure el IPSec transforman para utilizar GCM.

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

5. Configure el perfil de ipsec con los parámetros configurados anterior.

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

6. Configure la interfaz del 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 la conexión

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Verifique que las claves ECDSA fueran generadas con éxito.

```
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 el certificado fuera importado con éxito y que ECDH está utilizado.

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

3. Verifique que IKEv2 SA fuera creado con éxito y utiliza los algoritmos de la habitación 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 fuera creado con éxito y utiliza los algoritmos de la habitación 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)
```

Nota: En esta salida, a diferencia en de la versión 1 (IKEv1) del intercambio de claves de Internet, el valor de grupo del Diffie-Hellman (DH) del Confidencialidad directa perfecta (PFS) muestra como **PFS (Y/N): N, grupo DH: ningunos** durante la primera negociación de túnel, pero después de que ocurra una reintroducción, los valores correctos muestran. Esto no es un bug aunque el comportamiento se describe en el Id. de bug Cisco CSCug67056. La diferencia entre IKEv1 e IKEv2 es que, en estos últimos, crean a las asociaciones de seguridad del niño (SA) como parte del intercambio sí mismo AUTH. Utilizan al grupo DH configurado bajo correspondencia de criptografía solamente durante la reintroducción. Por lo tanto, usted ve el **PFS (Y/N): N, grupo DH: ningunos** hasta los primeros reintroducen. Pero con IKEv1, usted ve un diverso comportamiento porque la creación niño SA sucede durante el Quick Mode y el mensaje CREATE_CHILD_SA tiene una disposición para llevar el payload del intercambio de claves que especifica los parámetros DH para derivar un nuevo secreto compartido.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Conclusión

Los algoritmos criptográficos eficientes y fuertes definidos en NGE ofrecen la garantía a largo plazo que los datos confidencial y la integridad está proporcionados y mantenidos en un costo bajo para procesar. NGE se puede implementar fácilmente con FlexVPN, que proporciona la criptografía del estándar de la habitación B.

La Más información en la implementación de Cisco de la habitación B se puede encontrar en el cifrado de la última generación.