Ejemplo de Configuración de FlexVPN con Cifrado de Última Generación

Contenido

Introducción

Este documento describe cómo configurar FlexVPN entre dos routers que admiten el conjunto de algoritmos Cisco Next-Generation Encryption (NGE).

Cifrado de última generación

La criptografía de Cisco NGE protege la información que viaja por redes que utilizan cuatro algoritmos criptográficos configurables, bien establecidos y de dominio público:

- Cifrado basado en el estándar de cifrado avanzado (AES), que utiliza claves de 128 o 256 bits
- Firmas digitales con el algoritmo de firma digital de curva elíptica (ECDSA) que utilizan curvas con módulos primos de 256 bits y 384 bits
- Intercambio de claves que utiliza el método Diffie-Hellman de curva elíptica (ECDH)
- Hashing (huellas digitales) basado en el algoritmo hash seguro 2 (SHA-2)

La Agencia Nacional de Seguridad (NSA) afirma que estos cuatro algoritmos combinados proporcionan una garantía de información adecuada para la información clasificada. La criptografía de NSA Suite B para IPsec se ha publicado como estándar en RFC 6379 y ha ganado aceptación en el sector.

Suite Suite-B-GCM-128

Según RFC 6379, estos algoritmos son necesarios para el conjunto Suite-B-GCM-128.

Este conjunto proporciona protección de integridad y confidencialidad de la carga de seguridad de encapsulación (ESP) con AES-GCM de 128 bits (consulte RFC4106). Este conjunto de aplicaciones se debe utilizar cuando se necesitan protección de integridad ESP y cifrado.

ESP
AES de cifrado con claves de 128 bits y valor de comprobación de integridad (ICV) de 16 octetos en modo Galois/Counter (GCM) (RFC4106)
Integridad NULA

IKEv2
AES de cifrado con claves de 128 bits en modo de encadenamiento de bloques cifrados (CBC) (RFC3602)
Función pseudoaleatoria HMAC-SHA-256 (RFC4868)
Integridad HMAC-SHA-256-128 (RFC4868)
Grupo ECP aleatorio Diffie-Hellman de 256 bits (RFC5903)

Puede encontrar más información sobre Suite B y NGE en Encriptación de última generación.

Prerequisites

Requirements

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 Routers de servicios integrados (ISR) de segunda generación (G2) que ejecutan la licencia de seguridad.
- Software: Versión 15.2.3T2 del software Cisco IOS®. Cualquier versión de Cisco IOS Software Release M o 15.1.2T o posterior se puede utilizar ya que es cuando se introdujo GCM.

Para obtener más información, consulte el Navegador de funciones.

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.

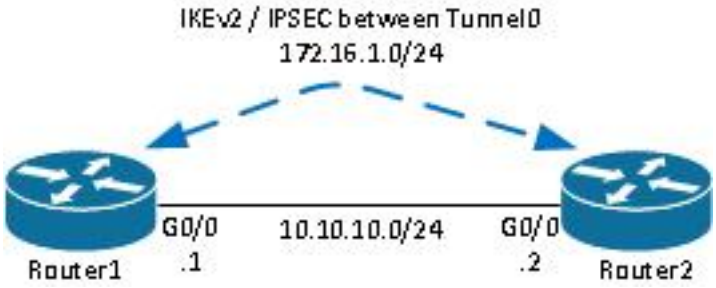
Autoridad de certificados

Actualmente, el software Cisco IOS no admite un servidor local de Autoridad de Certificación (CA) que ejecute ECDH, que es necesario para la Suite B. Se debe implementar un servidor CA de terceros. Este ejemplo utiliza una CA de Microsoft basada en PKI Suite B

Configurar

Topología de red

Esta guía se basa en esta topología ilustrada. Las direcciones IP se deben modificar para adaptarlas a sus requisitos.



Notas:

La configuración consta de dos routers conectados directamente, que podrían estar separados por muchos saltos. Si es así, asegúrese de que haya una ruta para llegar a la dirección IP del par. Esta configuración sólo detalla el cifrado utilizado. El ruteo IKEv2 o un protocolo de ruteo deben implementarse sobre la VPN IPSec.

Pasos necesarios para permitir que el router utilice el algoritmo de firma digital de curva elíptica

1. Cree el nombre de dominio y el nombre de host, que son requisitos previos para crear un par de claves EC.

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

   Nota: A menos que ejecute una versión con la corrección del Id. de error de Cisco CSCue59994, el router no le permitirá inscribir un certificado con un tamaño de clave inferior a 768.
2. Cree un punto de confianza local para obtener un certificado de la CA.

```
crypto pki trustpoint ecdh
 enrollment terminal
```

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

Nota: Dado que la CA estaba desconectada, las comprobaciones de revocación se desactivaron. Las comprobaciones de revocación deben habilitarse para obtener la máxima seguridad en un entorno de producción.

3. Autentique el punto de confianza (esto obtiene una copia del certificado de la CA que contiene la clave pública).

```
crypto pki authenticate ecdh
```

4. Ingrese el certificado codificado base 64 de la CA en el mensaje. Ingrese **quit** y luego ingrese **yes** para aceptar.

5. Inscriba el router en la PKI en la CA.

```
crypto pki enrol ecdh
```

6. El resultado mostrado se utiliza para enviar una solicitud de certificado a la CA. Para la CA de Microsoft, conéctese a la interfaz web de la CA y seleccione **Enviar una solicitud de certificado**.

7. Importe el certificado recibido de la CA en el router. Ingrese **quit** una vez que se importa el certificado.

```
crypto pki import ecdh certificate
```

Configuración

La configuración proporcionada aquí es para el Router1. El Router 2 requiere una réplica de la configuración donde solamente las direcciones IP en la interfaz de túnel son únicas.

1. Cree un mapa de certificado para que coincida con el certificado del dispositivo de par.

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

2. Configure la propuesta IKEv2 para la Suite B.

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

Nota: IKEv2 Smart Defaults implementa una serie de algoritmos preconfigurados dentro de

la propuesta IKEv2 predeterminada. Debido a que se requieren aes-cbc-128 y sha256 para la suite Suite Suite-B-GCM-128, debe eliminar aes-cbc-256, sha384 y sha512 dentro de estos algoritmos. La razón de esto es que IKEv2 elige el algoritmo más fuerte cuando se le presenta una opción. Para obtener la máxima seguridad, utilice aes-cbc-256 y sha512. Sin embargo, esto no es necesario para Suite-B-GCM-128. Para ver la propuesta IKEv2 configurada, ingrese el comando **show crypto ikev2 project**.

3. Configure el perfil IKEv2 para que coincida con el mapa del certificado y utilice ECDSA con el punto de confianza 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 la transformación IPSec para utilizar GCM.

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

5. Configure el perfil IPSec con los parámetros configurados anteriormente.

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

6. Configure la interfaz 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
```

Verificar conexión

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Verifique que las claves ECDSA se hayan generado correctamente.

```
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 se importó correctamente y que se utiliza ECDH.

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

3. Verifique que IKEv2 SA se haya creado correctamente y utilice los 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 que IKEv2 SA se haya creado correctamente y utilice los 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)
```

Nota: En este resultado, a diferencia de la versión 1 de Intercambio de claves de Internet (IKEv1), el valor de grupo Diffie-Hellman (DH) de confidencialidad directa perfecta (PFS) se muestra como **PFS (Y/N): N, grupo DH: ninguno** durante la primera negociación de túnel, pero después de que se produce una nueva clave, se muestran los valores correctos. Esto no es un error aunque el comportamiento se describe en el Id. de bug Cisco CSCug67056. La diferencia entre IKEv1 e IKEv2 es que, en estos últimos, las asociaciones de seguridad infantil (SA) se crean como parte del intercambio AUTH en sí. El grupo DH

configurado bajo el mapa criptográfico se utiliza solamente durante la nueva clave. Por lo tanto, puede ver **PFS (S/N): N, grupo DH: ninguno** hasta la primera llave. Pero con IKEv1, se observa un comportamiento diferente porque la creación de SA secundaria se produce durante el modo rápido y el mensaje CREATE_CHILD_SA tiene una provisión para llevar la carga útil Key Exchange que especifica los parámetros DH para derivar un nuevo secreto compartido.

Troubleshoot

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

Conclusión

Los algoritmos criptográficos eficientes y sólidos definidos en NGE ofrecen garantías a largo plazo de que los datos se proporcionan y se mantienen de forma confidencial y con un bajo coste de procesamiento. NGE se puede implementar fácilmente con FlexVPN, que proporciona criptografía estándar Suite B.

Puede encontrar más información sobre la implementación de Cisco de la Suite B en Encriptación de última generación.