Ejemplo de Configuración de FlexVPN entre un Router y un ASA con Cifrado de Última Generación

Contenido

Introducción

Este documento describe cómo configurar una VPN entre un router con FlexVPN y un dispositivo de seguridad adaptable (ASA) que admita los algoritmos de cifrado de última generación (NGE) de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

- Criptografía de última generación

Componentes Utilizados

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

- **Hardware** Router IOS Generation 2 (G2) que ejecuta la licencia de seguridad.
- **Software:** Versión 15.2-3.T2 del software del IOS® de Cisco. Se puede utilizar cualquier versión de M o T para versiones posteriores a la versión 15.1.2T del software del IOS® de Cisco, ya que se incluye con la introducción del modo de contador Galois (GCM).
- **Hardware** ASA compatible con NGE.**Nota:** Sólo las plataformas de varios núcleos admiten GCM estándar de cifrado avanzado (AES).
- **Software:** Versión 9.0 o posterior del software ASA compatible con NGE.
- OpenSSL.

Para obtener más información, consulte 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Creación dinámica de asociaciones de seguridad IPSec

La interfaz IPSec recomendada en IOS es una interfaz de túnel virtual (VTI), que crea una interfaz de encapsulación de routing genérico (GRE) protegida por IPsec. Para un VTI, el selector de tráfico (qué tráfico deben estar protegidos por las asociaciones de seguridad (SA) IPSec) consta del tráfico GRE desde el origen del túnel hasta el destino del túnel. Debido a que ASA no implementa interfaces GRE, sino que crea SA IPSec basadas en el tráfico definido en una lista de control de acceso (ACL), debemos habilitar un método que permita al router responder al inicio de IKEv2 con una réplica de los selectores de tráfico propuestos. El uso de la interfaz de túnel virtual dinámico (DVTI) en el router FlexVPN permite que este dispositivo responda al selector de tráfico presentado con una réplica del selector de tráfico que se presentó.

Este ejemplo cifra el tráfico entre ambas redes internas. Cuando el ASA presenta los selectores de tráfico de la red interna ASA a la red interna del IOS, `192.168.1.0/24` a `172.16.10.0/24`, la interfaz DVTI responde con una réplica de los selectores de tráfico, que es `172.16.10.0/24` a `192.168.1.0/24`.

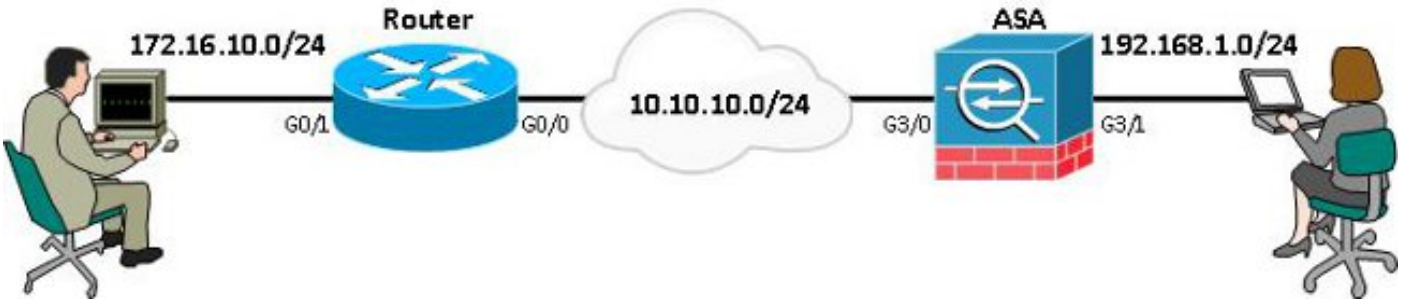
Autoridad de certificados

Actualmente, IOS y ASA no admiten un servidor de autoridad de certificados (CA) local con certificados de algoritmo de firma digital de curva elíptica (ECDSA), que es necesario para Suite-B. Por lo tanto, se debe implementar un servidor de CA de terceros. Por ejemplo, utilice OpenSSL para actuar como una CA.

Configuración

Topología de red

Esta guía se basa en la topología que se muestra en este diagrama. Debe modificar las direcciones IP para adaptarlas.



Nota: La configuración incluye una conexión directa del router y el ASA. Estos podrían estar separados por muchos saltos. Si es así, asegúrese de que haya una ruta para llegar a la dirección IP del par. La siguiente configuración sólo detalla el cifrado utilizado.

Pasos necesarios para permitir que el router utilice el ECDSA

Autoridad de certificados

1. Cree un **par de teclas de curva elíptica.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. Crear un **certificado autofirmado de curva elíptica**.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. Cree **nombre de dominio** y **nombre de host**, que son requisitos previos para crear un par de claves de curva elíptica (EC).
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. Cree un **punto de confianza** local para obtener un certificado de la CA.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   Nota: Debido a que la CA está desconectada, la verificación de revocación está inhabilitada; la verificación de revocación debe 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 ec_ca
   ```
4. A continuación, se le solicitará que introduzca el certificado codificado base 64 de la CA. Este es el archivo ca.pem, que se creó con OpenSSL. Para ver este archivo, ábralo en un

editor o con el comando OpenSSL **openssl x509 -en ca.pem**. Introduzca **quit** cuando pegue esto. A continuación, escriba **yes** para aceptar.

5. Inscriba el router en la infraestructura de clave pública (PKI) de la CA.
```
crypto pki enrol ec_ca
```
6. El resultado que recibe debe utilizarse para enviar una solicitud de certificado a la CA. Esto se puede guardar como un archivo de texto (flex.csr) y firmar con el comando OpenSSL.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```
7. Importe el certificado, que se encuentra dentro del archivo flex.pem, generado desde la CA, en el router después de ingresar este comando. A continuación, introduzca **quit** cuando haya finalizado.
```
crypto pki import ec_ca certificate
```

ASA

1. Cree **nombre de dominio** y **nombre de host**, que son requisitos previos para crear un par de claves EC.
```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```
2. Cree un **punto de confianza** local para obtener un certificado de la CA.
```
crypto ca trustpoint ec_ca
 enrollment terminal
 subject-name cn=asa1.cisco.com
 revocation-check none
 keypair asa1.cisco.com
```
Nota: Debido a que la CA está desconectada, la verificación de revocación está inhabilitada; la verificación de revocación debe 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 ca authenticate ec_ca
```
4. A continuación, se le solicitará que introduzca el certificado codificado base 64 de la CA. Este es el archivo ca.pem, que se creó con OpenSSL. Para ver este archivo, ábralo en un editor o con el comando OpenSSL **openssl x509 -en ca.pem**. Ingrese **quit** cuando pegue este archivo y luego escriba **yes** para aceptar.
5. Inscriba el ASA en la PKI en la CA.
```
crypto ca enrol ec_ca
```
6. El resultado que recibe debe utilizarse para enviar una solicitud de certificado a la CA. Esto se puede guardar como un archivo de texto (asa.csr) y luego firmar con el comando OpenSSL.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
```
7. Importe el certificado, que se encuentra dentro del archivo como a.pem, generado desde la CA en el router después de ingresar este comando. A continuación, **introduzca** quit cuando haya finalizado.
```
crypto ca import ec_ca certificate
```

Configuración

FlexVPN

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
```

Ingrese estos comandos para la propuesta IKEv2 para la configuración Suite-B:

Nota: Para obtener la máxima seguridad, configure con el **comando** hash **aes-cbc-256 con sha512**.

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

Haga coincidir el perfil IKEv2 con el mapa del certificado y utilice ECDSA con el **punto de confianza** definido previamente.

```
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 el conjunto de transformación IPSec para utilizar el modo de contador Galois (GCM).

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

Configure el perfil IPSec con los parámetros previamente configurados.

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

Configure la interfaz de túnel:

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

Esta es la configuración de la interfaz:

```
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

Utilice esta configuración de interfaz:

```
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
```

Ingrese este comando de lista de acceso para definir el tráfico que se cifrará:

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

Ingrese este comando de propuesta IPSec con NGE:

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

Comandos de mapa criptográfico:

```
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 la política IKEv2 con 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 de 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
```

Verificación de la conexión

Verifique que las claves ECDSA se hayan generado correctamente.

```
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 que el certificado se ha importado correctamente y que se utiliza ECDSA.

```
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 que la SA IKEv2 se haya creado correctamente y utilice los 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 que la SA IPSec se haya creado correctamente y utilice los algoritmos NGE configurados.

Nota: FlexVPN puede finalizar conexiones IPSec de clientes que no sean IOS y que admitan tanto los protocolos IKEv2 como 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 obtener más información sobre la implementación de Suite-B por parte de Cisco, refiérase al Informe Técnico de Cifrado de Última Generación.

Consulte la página Solución de Cifrado de Última Generación para obtener más información sobre la implementación de Cisco del Cifrado de Última Generación.

Información Relacionada

- Informe técnico sobre cifrado de última generación
- Página de la solución de cifrado de última generación
- Secure Shell (SSH)
- Negociación IPSec/Protocolos IKE
- Depuraciones ASA IKEv2 para VPN de sitio a sitio con PSK TechNote

- Depuraciones ASA IPSec e IKE (modo principal IKEv1) Solución de problemas de TechNote
- Depuraciones de IOS IPSec e IKE - Nota técnica de resolución de problemas del modo principal IKEv1
- Depuraciones de ASA IPSec e IKE - IKEv1 Modo agresivo TechNote
- Soporte Técnico y Documentación - Cisco Systems