Esempio di configurazione di FlexVPN tra un router e un'ASA con crittografia di nuova generazione

Sommario

Introduzione

In questo documento viene descritto come configurare una VPN tra un router con FlexVPN e un'appliance ASA (Adaptive Security Appliance) che supporta gli algoritmi Cisco Next Generation Encryption (NGE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FlexVPN
- IKEv2 (Internet Key Exchange versione 2)
- IPSec
- ASA

- Crittografia di nuova generazione

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- **Hardware:** Router IOS generazione 2 (G2) con licenza di protezione.
- **Software:** Software Cisco IOS® versione 15.2-3.T2. È possibile usare qualsiasi versione di M o T per versioni successive alla versione 15.1.2T del software Cisco IOS®, in quanto inclusa nell'introduzione della modalità GCM (Galois Counter Mode).
- **Hardware:** ASA che supporta GRE.**Nota:** solo le piattaforme multi-core supportano GCM Advanced Encryption Standard (AES).
- **Software:** Software ASA versione 9.0 o successive che supporta NGE.
- OpenSSL.

Per ulteriori informazioni, consultare Cisco Feature Navigator.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Creazione dinamica delle associazioni di protezione IPSec

L'interfaccia IPSec consigliata su IOS è una VTI (Virtual Tunnel Interface) che crea un'interfaccia GRE (Generic Routing Encapsulation) protetta da IPsec. Per una VTI, il selettore del traffico (il traffico che deve essere protetto dalle associazioni di sicurezza IPSec (SA)) è costituito dal traffico GRE tra l'origine del tunnel e la destinazione del tunnel. Poiché l'ASA non implementa le interfacce GRE, ma crea le associazioni di protezione IPSec in base al traffico definito in un elenco di controllo di accesso (ACL), è necessario abilitare un metodo che consenta al router di rispondere all'avvio di IKEv2 con un mirror dei selettori di traffico proposti. L'uso di DVTI (Dynamic Virtual Tunnel Interface) sul router FlexVPN consente al dispositivo di rispondere al selettore del traffico presentato con un mirror del selettore del traffico presentato.

In questo esempio viene crittografato il traffico tra entrambe le reti interne. Quando l'ASA presenta i selettori di traffico della rete interna dell'ASA alla rete interna di IOS, da `192.168.1.0/24` a `172.16.10.0/24`, l'interfaccia DVTI risponde con un mirror dei selettori di traffico, ossia da `172.16.10.0/24` a `192.168.1.0/24`.

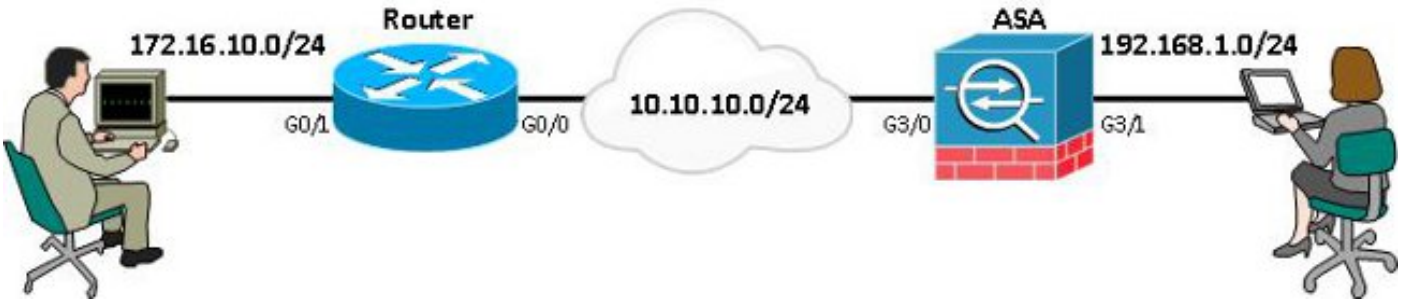
Autorità di certificazione

Al momento, IOS e ASA non supportano un server CA (Certification Authority) locale con certificati ECDSA (Elliptic Curve Digital Signature Algorithm), richiesto per Suite-B. È quindi necessario implementare un server CA di terze parti. Utilizzare ad esempio OpenSSL per operare come CA.

Configurazione

Topologia della rete

Questa guida si basa sulla topologia mostrata nel diagramma. Modificare gli indirizzi IP in base alle proprie esigenze.



Nota: la configurazione include una connessione diretta del router e dell'ASA. Questi possono essere separati da molti hop. In tal caso, assicurarsi che sia disponibile una route per raggiungere l'indirizzo IP del peer. Nella configurazione seguente viene descritta solo la crittografia utilizzata.

Passaggi necessari per consentire al router di utilizzare l'ECDSA

Autorità di certificazione

1. Create una **coppia di chiavi ellittica.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. Crea un **certificato autofirmato di curva ellittica**.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. Creare **domain-name** e **hostname**, prerequisiti per la creazione di una coppia di chiavi a curva ellittica (EC).
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. Creare un **trust point** locale per ottenere un certificato dalla CA.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   Nota: poiché la CA è offline, il controllo delle revoche è disabilitato. è necessario abilitare la verifica delle revoche per la massima protezione in un ambiente di produzione.
3. Autentica il **trust point**. In questo modo si ottiene una copia del certificato della CA, che contiene la chiave pubblica.
   ```
   crypto pki authenticate ec_ca
   ```
4. Viene quindi richiesto di immettere il certificato con codifica Base 64 della CA. Si tratta del file ca.pem, creato con OpenSSL. Per visualizzare questo file, aprirlo in un editor o con il comando OpenSSL **openssl x509 -in ca.pem**. Immettere **quit** quando si incolla. Quindi

digitare **sì** per accettare.

5. Registrare il router nell'infrastruttura a chiave pubblica (PKI) sulla CA.
   ```
   crypto pki enrol ec_ca
   ```
6. L'output ricevuto deve essere utilizzato per inviare una richiesta di certificato alla CA. Può essere salvato come file di testo (flex.csr) e firmato con il comando OpenSSL.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
   ```
7. Dopo aver immesso questo comando, importare nel router il certificato contenuto nel file flex.pem generato dalla CA. Al termine, immettere **quit**.
   ```
   crypto pki import ec_ca certificate
   ```

ASA

1. Creare **domain-name** e **hostname**, prerequisiti per la creazione di una coppia di chiavi EC.
   ```
   domain-name cisco.com
   hostname ASA1
   crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
   ```
2. Creare un **trust point** locale per ottenere un certificato dalla CA.
   ```
   crypto ca trustpoint ec_ca
    enrollment terminal
    subject-name cn=asa1.cisco.com
    revocation-check none
    keypair asa1.cisco.com
   ```
   Nota: poiché la CA è offline, il controllo delle revoche è disabilitato. è necessario abilitare la verifica delle revoche per la massima protezione in un ambiente di produzione.
3. Autentica il **trust point**. In questo modo si ottiene una copia del certificato della CA, che contiene la chiave pubblica.
   ```
   crypto ca authenticate ec_ca
   ```
4. Viene quindi richiesto di immettere il certificato con codifica Base 64 della CA. Si tratta del file ca.pem, creato con OpenSSL. Per visualizzare questo file, aprirlo in un editor o con il comando OpenSSL **openssl x509 -in ca.pem**. Immettere **quit** quando si incolla il file e quindi digitare **yes** per accettare.
5. Registrare l'ASA nella PKI sulla CA.
   ```
   crypto ca enrol ec_ca
   ```
6. L'output ricevuto deve essere utilizzato per inviare una richiesta di certificato alla CA. È possibile salvare il file come file di testo (asa.csr) e quindi firmarlo con il comando OpenSSL.
   ```
   openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
   ```
7. Importare il certificato, contenuto nel file come a.pem, generato dalla CA nel router dopo l'immissione di questo comando. Al termine **immettere** quit.
   ```
   crypto ca import ec_ca certificate
   ```

Configurazione

FlexVPN

Creare una mappa certificati corrispondente al certificato del dispositivo peer.

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

Immettere questi comandi per la proposta IKEv2 per la configurazione Suite-B:

Nota: per la massima sicurezza, configurare con il comando **aes-cbc-256 con hash sha512**.

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

Associare il profilo IKEv2 alla mappa dei certificati e utilizzare ECDSA con il **trust point** definito in precedenza.

```
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
```

Configurare il set di trasformazioni IPSec per l'utilizzo della modalità Contatore di Galois (GCM).

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

Configurare il profilo IPSec con i parametri configurati in precedenza.

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

Configurare l'interfaccia del tunnel:

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

Di seguito è riportata la configurazione dell'interfaccia:

```
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

Utilizzare la seguente configurazione di interfaccia:

```
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
```

Immettere questo comando dell'elenco degli accessi per definire il traffico da crittografare:

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

Immettere questo comando di proposta IPSec con NGE:

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

Comandi mappa crittografia:

```
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
```

Con questo comando viene configurato il criterio IKEv2 con NGE:

```
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
```

Gruppo di tunnel configurato per i comandi 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
```

Verifica connessione

Verificare che le chiavi ECDSA siano state generate correttamente.

```
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...>
```

Verificare che il certificato sia stato importato correttamente e che sia utilizzato 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...>
```

Verificare che l'associazione di sicurezza IKEv2 sia stata creata correttamente e che utilizzi gli algoritmi GE configurati.

```
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
```

Verificare che l'associazione di protezione IPSec sia stata creata correttamente e che utilizzi gli algoritmi GE configurati.

Nota: FlexVPN può terminare le connessioni IPSec da client non IOS che supportano entrambi i

protocolli IKEv2 e 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, }
```

Per ulteriori informazioni sull'implementazione di Suite-B da parte di Cisco, consultare il white paper sulla crittografia di nuova generazione.

Per ulteriori informazioni sull'implementazione della crittografia di nuova generazione da parte di Cisco, consultare la pagina Next-Generation Encryption Solution.

Informazioni correlate

- White paper sulla crittografia di nuova generazione
- Pagina Soluzione di crittografia di nuova generazione
- SSH (Secure Shell)
- Negoziazione IPSec/protocolli IKE
- Nota tecnica sui debug ASA IKEv2 per la VPN da sito a sito con PSK
- Nota tecnica sulla risoluzione dei problemi relativi ai debug ASA IPSec e IKE (modalità principale IKEv1)
- Note tecniche sulla risoluzione dei problemi relativi alla modalità principale IOS IPSec e IKE
- Debug ASA IPSec e IKE - Nota tecnica sulla modalità aggressiva IKEv1
- Documentazione e supporto tecnico – Cisco Systems