Esempio di configurazione di FlexVPN con crittografia di nuova generazione

Sommario

Introduzione

Questo documento descrive come configurare una FlexVPN tra due router che supportano il set di algoritmi Cisco Next-Generation Encryption (NGE).

Crittografia di nuova generazione

La crittografia Cisco GE protegge le informazioni che viaggiano sulle reti che utilizzano quattro algoritmi di crittografia configurabili, ben consolidati e di dominio pubblico:

- Crittografia basata sullo standard AES (Advanced Encryption Standard), che utilizza chiavi a 128 o 256 bit
- Firme digitali con l'algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm) che utilizzano curve con moduli di primi 256 bit e 384 bit
- Scambio di chiavi che utilizza il metodo ECDH (Elliptic Curve Diffie-Hellman)
- Hashing (impronte digitali) basato su Secure Hash Algorithm 2 (SHA-2)

La National Security Agency (NSA) afferma che questi quattro algoritmi in combinazione forniscono un'adeguata garanzia delle informazioni classificate. La crittografia NSA Suite B per IPsec è stata pubblicata come standard nella RFC 6379 e ha ottenuto l'approvazione del settore.

Suite-B-GCM-128

In base alla RFC 6379, questi algoritmi sono richiesti per la suite Suite-B-GCM-128.

Questa suite fornisce protezione e riservatezza dell'integrità Encapsulating Security Payload (ESP) con AES-GCM a 128 bit (vedere RFC4106). Questa suite deve essere utilizzata quando sono necessarie sia la protezione dell'integrità ESP che la crittografia.

ESP
Crittografia AES con chiavi a 128 bit e ICV (Integrity Check Value) a 16 ottetti in modalità Galois/Contatore (GCM) (RFC4106)
Integrità NULL

IKEv2
Crittografia AES con chiavi a 128 bit in modalità CBC (Cipher Block Chaining) (RFC3602)
Funzione pseudo-casuale HMAC-SHA-256 (RFC4868)
Integrità HMAC-SHA-256-128 (RFC4868)
Gruppo Diffie-Hellman con ECP casuale a 256 bit (RFC5903)

Per ulteriori informazioni su Suite B e GE, consultare il documento sulla crittografia di nuova generazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

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

- Hardware: Router per servizi integrati (ISR, Integrated Services Router) di seconda generazione (G2) che eseguono la licenza di protezione.
- Software: Software Cisco IOS® versione 15.2.3T2. È possibile usare qualsiasi versione del software Cisco IOS versione M o 15.1.2T o successive perché questa versione è stata introdotta con GCM.

Per ulteriori informazioni, fate riferimento al Navigatore funzioni.

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.

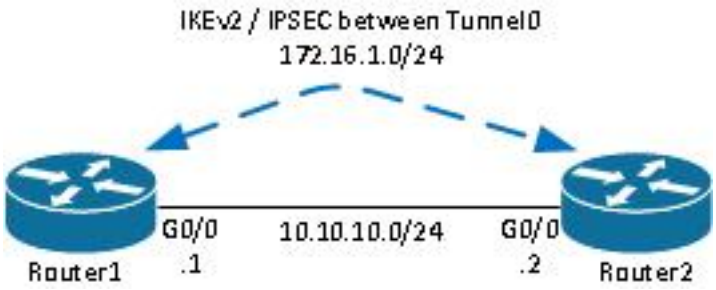
Autorità di certificazione

Al momento, il software Cisco IOS non supporta un server CA locale con ECDH, necessario per Suite B. È necessario implementare un server CA di terze parti. In questo esempio viene utilizzata una CA Microsoft basata su Suite B PKI

Configurazione

Topologia della rete

Questa guida si basa sulla topologia illustrata. Gli indirizzi IP devono essere modificati in base alle proprie esigenze.



Note:

L'installazione è costituita da due router connessi direttamente, che potrebbero essere separati da più hop. In tal caso, verificare che sia disponibile una route per raggiungere l'indirizzo IP del peer. In questa configurazione viene descritta solo la crittografia utilizzata. È necessario implementare il routing IKEv2 o un protocollo di routing sulla VPN IPSec.

Passaggi necessari per consentire al router di utilizzare l'algoritmo della firma digitale della curva ellittica

1. Creare il nome di dominio e il nome host, prerequisiti per la creazione di una coppia di chiavi EC.

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

   Nota: A meno che non si esegua una versione con l'ID bug Cisco CSCue59994, il router non consentirà di registrare un certificato con una dimensione della chiave inferiore a 768.
2. Creare un trust point locale per ottenere un certificato dalla CA.

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

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

Nota: La CA non è in linea. I controlli di revoca sono stati disabilitati. Per garantire la massima protezione in un ambiente di produzione, è necessario abilitare i controlli di revoca.

3. Autentica il trust point (ottiene una copia del certificato della CA che contiene la chiave pubblica).

```
crypto pki authenticate ecdh
```

4. Immettere il certificato codificato in base 64 della CA al prompt. Immettere **quit**, quindi **yes** per accettare.

5. Registrare il router nella PKI sulla CA.

```
crypto pki enrol ecdh
```

6. L'output visualizzato viene utilizzato per inviare una richiesta di certificato alla CA. Per la CA Microsoft, connettersi all'interfaccia Web della CA e selezionare **Invia una richiesta di certificato**.

7. Importare il certificato ricevuto dalla CA nel router. Immettere **quit** una volta importato il certificato.

```
crypto pki import ecdh certificate
```

Configurazione

La configurazione fornita qui è per Router1. Router2 richiede un mirror della configurazione in cui solo gli indirizzi IP sull'interfaccia del tunnel sono univoci.

1. Creare una mappa certificati corrispondente al certificato del dispositivo peer.

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

2. Configurare la proposta IKEv2 per Suite B.

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

Nota: IKEv2 Smart Defaults implementa una serie di algoritmi preconfigurati nella proposta IKEv2 predefinita. Poiché per la suite Suite-B-GCM-128 sono richiesti aes-cbc-128 e sha256,

è necessario rimuovere aes-cbc-256, sha384 e sha512 all'interno di questi algoritmi. La ragione di ciò è che IKEv2 sceglie l'algoritmo più avanzato quando presenta una scelta. Per garantire la massima sicurezza, usare aes-cbc-256 e sha512. Tuttavia, questo non è richiesto per Suite-B-GCM-128. Per visualizzare la proposta IKEv2 configurata, immettere il comando **show crypto ikev2 request**.

3. Configurare il profilo IKEv2 in modo che corrisponda 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 ecdh
```

4. Configurare la trasformazione IPSec per l'utilizzo di GCM.

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

5. 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
```

6. Configurare l'interfaccia del tunnel.

```
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
```

Verifica connessione

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Verificare che le chiavi ECDSA siano state generate correttamente.

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

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

3. Verificare che l'associazione di sicurezza IKEv2 sia stata creata correttamente e che utilizzi gli algoritmi 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. Verificare che l'associazione di sicurezza IKEv2 sia stata creata correttamente e che utilizzi gli algoritmi 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: In questo output, a differenza di IKEv1 (Internet Key Exchange versione 1), il valore del gruppo Diffie-Hellman (DH) PFS (Perfect Forward Secrecy) viene visualizzato come **PFS (Y/N): N, gruppo DH: nessuna** durante la prima negoziazione del tunnel, ma dopo una reimpostazione della chiave vengono visualizzati i valori corretti. Non si tratta di un bug anche se il comportamento è descritto nell'ID bug Cisco CSCug67056. La differenza tra

IKEv1 e IKEv2 è che, in quest'ultimo caso, le associazioni di sicurezza figlio (SA) vengono create come parte dello scambio AUTH. Il gruppo DH configurato nella mappa crittografica viene utilizzato solo durante la reimpostazione della chiave. Viene quindi visualizzato **PFS (S/N): N, gruppo DH: nessuna** fino alla prima reimpostazione della chiave. Con IKEv1, tuttavia, si verifica un comportamento diverso, in quanto la creazione dell'associazione di protezione figlio avviene durante la modalità rapida e il messaggio CREATE_CHILD_SA include una clausola per il trasporto del payload di scambio chiave che specifica i parametri DH per derivare un nuovo segreto condiviso.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Conclusioni

Gli algoritmi crittografici efficienti e affidabili definiti in GRE forniscono una garanzia a lungo termine che la riservatezza e l'integrità dei dati sono fornite e mantenute a un costo di elaborazione contenuto. NGE può essere implementato facilmente con FlexVPN, che fornisce la crittografia standard di Suite B.

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