Esempio di tunnel VPN da sito a sito dinamico IKEv2 tra un'ASA e un router IOS

Sommario

Introduzione

In questo documento viene descritto come configurare un tunnel VPN IKEv2 (Internet Key Exchange versione 2) da sito a sito tra un'appliance ASA (Adaptive Security Appliance) e un router Cisco, in cui il router ha un indirizzo IP dinamico e l'ASA ha un indirizzo IP statico sulle interfacce pubbliche.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

hardware:

- Cisco IOS® versione 15.1(1)T o successiva
- Cisco ASA versione 8.4(1) o successive

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.

Premesse

In questo documento vengono illustrati i seguenti scenari:

- Scenario 1: Un'ASA è configurata con un indirizzo IP statico che usa un gruppo di tunnel denominato e il router è configurato con un indirizzo IP dinamico.
- Scenario 2: Un'ASA è configurata con un indirizzo IP dinamico e il router è configurato con un indirizzo IP dinamico.
- Scenario 3: Questo scenario non viene discusso in questa sede. In questo scenario, l'ASA è configurata con un indirizzo IP statico ma utilizza il gruppo di tunnel DefaultL2LGroup. La configurazione di questo comando è simile a quella descritta nell'articolo di esempio della configurazione del tunnel VPN da sito dinamico a sito IKEv2 tra due appliance ASA.

La maggiore differenza di configurazione tra gli scenari 1 e 3 è rappresentata dall'ID Internet Security Association and Key Management Protocol (ISAKMP) utilizzato dal router remoto. Quando si usa il gruppo L2L predefinito sull'appliance ASA statica, l'ID ISAKMP del peer sul router deve essere l'indirizzo dell'appliance ASA. Tuttavia, se si usa un gruppo di tunnel denominato, l'ID ISAKMP del peer sul router deve essere uguale al nome del gruppo di tunnel configurato sull'appliance ASA. A tal fine, usare questo comando sul router:

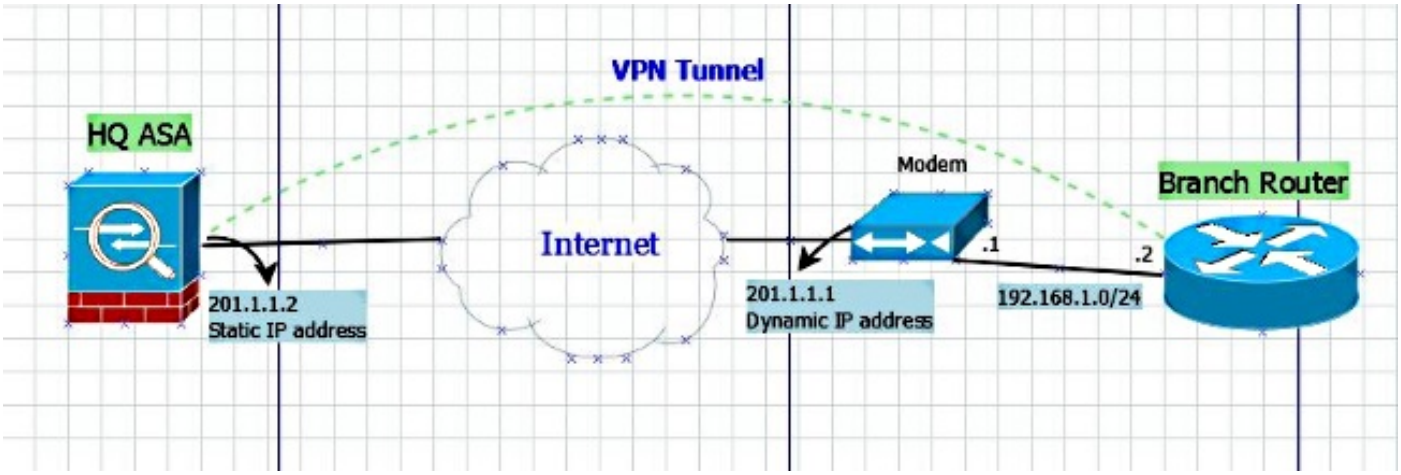
```
identity local key-id
```

Il vantaggio dell'utilizzo di gruppi di tunnel denominati sull'appliance ASA statica è che quando si utilizza il gruppo L2L predefinito, la configurazione sui router/appliance ASA dinamici remoti, che include le chiavi già condivise, deve essere identica e non consente una grande granularità con l'impostazione dei criteri.

Configurazione

Scenario 1

Esempio di rete



Configurazione

In questa sezione viene descritta la configurazione sull'ASA e sul router basata sulla configurazione del gruppo di tunnel con nome.

Configurazione ASA statica

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

Configurazione dinamica del router

La configurazione del router dinamico è quasi identica a quella usata normalmente nei casi in cui il router è un sito dinamico per il tunnel IKEv2 L2L con l'aggiunta di un comando, come mostrato di seguito:

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

Pertanto, su ogni peer dinamico, l'ID della chiave è diverso e occorre creare un gruppo di tunnel corrispondente sull'appliance ASA statica con il nome corretto, il che aumenta anche la granularità dei criteri implementati sull'appliance ASA.

Scenario 2

> **Nota**: questa configurazione è possibile solo quando almeno un lato è un router. Se le appliance ASA sono di entrambi i lati, la configurazione non funziona. Nella versione 8.4, l'ASA non è in grado di usare il nome di dominio completo (FQDN) con il comando **set peer**, ma per le versioni future è stato richiesto il miglioramento di CSCus37350.

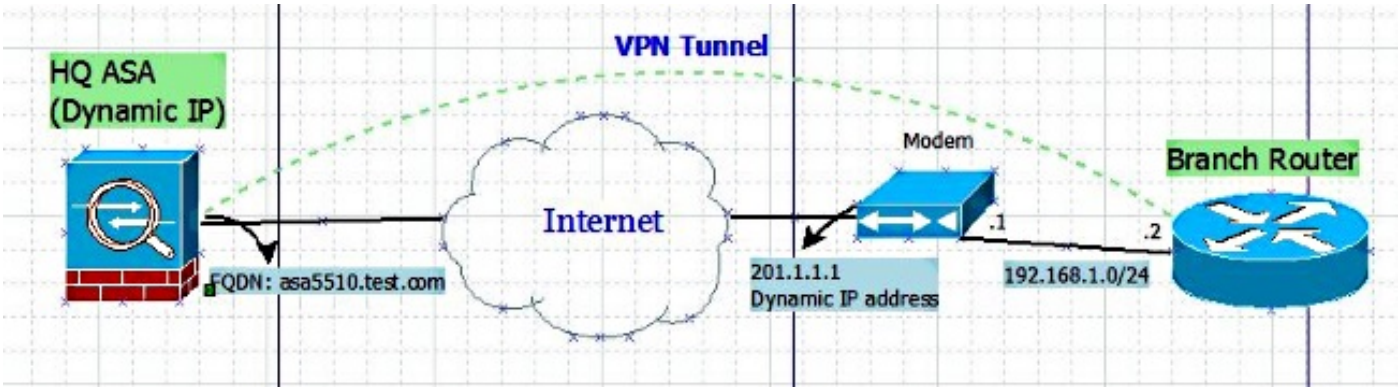
Se l'indirizzo IP dell'ASA remota è dinamico ma all'interfaccia VPN è assegnato un nome di dominio completo (FQDN), anziché definire l'indirizzo IP dell'ASA remota, è possibile definire l'FQDN dell'ASA remota con questo comando sul router:

```
C1941(config)#do show run | sec crypto map

crypto map vpn 10 ipsec-isakmp
 set peer <FQDN> dynamic
```

> **Suggerimento**: La parola chiave **dynamic** è facoltativa. Quando si specifica il nome host di un peer IPsec remoto tramite il comando **set peer**, è inoltre possibile utilizzare la parola chiave dynamic, che rinvia la risoluzione DNS (Domain Name Server) del nome host fino a quando non viene stabilito il tunnel IPsec.
>
> Il rinvio della risoluzione consente al software Cisco IOS di rilevare se l'indirizzo IP del peer IPsec remoto è stato modificato. Pertanto, il software può contattare il peer al nuovo indirizzo IP. Se la parola chiave dynamic non viene emessa, il nome host viene risolto immediatamente dopo che è stato specificato. Pertanto, il software Cisco IOS non è in grado di rilevare una modifica all'indirizzo IP e, pertanto, tenta di connettersi all'indirizzo IP precedentemente risolto.

Esempio di rete



Configurazione

Configurazione ASA dinamica

La configurazione sull'appliance ASA è la stessa della configurazione ASA statica, con una sola eccezione: l'indirizzo IP sull'interfaccia fisica non è definito in modo statico.

Configurazione router

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
 hostname asa5510.test.com
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
 !
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
 identity local key-id S2S-IKEv2
```

```
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel

crypto map vpn 10 ipsec-isakmp
 set peer asa5510.test.com dynamic
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
```

Verifica

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

ASA statica

- Di seguito viene riportato il risultato del comando **show crypto IKEv2 sa det**:

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
120434199        201.1.1.2/4500        201.1.1.1/4500      READY    RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C       Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
      Remote id: S2S-IKEv2
     Local req mess id: 43             Remote req mess id: 2
     Local next mess id: 43            Remote next mess id: 2
     Local req queued: 43              Remote req queued: 2
     Local window: 1                   Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected  outside
Child sa: local selector  201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

- Di seguito viene riportato il risultato del comando **show crypto ipsec sa**:

```
interface: outside
   Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2

     local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
```

```
    remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
    current_peer: 201.1.1.1


    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
    path mtu 1500, ipsec overhead 82(52), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 41AA84F4
    current inbound spi : 00853C02

  inbound esp sas:
    spi: 0x00853C02 (8731650)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
       slot: 0, conn_id: 94208, crypto-map: dmap
       sa timing: remaining key lifetime (kB/sec): (4101119/27843)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x0000001F
  outbound esp sas:
    spi: 0x41AA84F4 (1101694196)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
       slot: 0, conn_id: 94208, crypto-map: dmap
       sa timing: remaining key lifetime (kB/sec): (4055039/27843)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

Router dinamico

- Di seguito viene riportato il risultato del comando **show crypto IKEv2 sa detail**:

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
     Local spi: 67E01CB8E8619AF1       Remote spi: 97272A4B4DED4A5C
      Local id: S2S-IKEv2
     Remote id: 201.1.1.2
     Local req msg id:  2              Remote req msg id:  48
     Local next msg id: 2              Remote next msg id: 48
     Local req queued:  2              Remote req queued:  48
     Local window:      5              Remote window:      1
```

```
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

- Di seguito viene riportato il risultato del comando **show crypto ipsec sa**:

```
interface: GigabitEthernet0/0
   Crypto map tag: vpn, local addr 192.168.1.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
  current_peer 201.1.1.2 port 4500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
    plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0x853C02(8731650)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x41AA84F4(1101694196)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x853C02(8731650)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

Router dinamico (con appliance ASA dinamica remota)

- Di seguito viene riportato il risultato del comando **show crypto IKEv2 sa detail**:

```
C1941#show cry ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1516 sec
     CE id: 1034, Session-id: 24
     Status Description: Negotiation done
     Local spi: 98322AED6163EE83       Remote spi: 092A1E5620F6AA9C
      Local id: S2S-IKEv2
      Remote id: asa5510.test.com
     Local req msg id:  2              Remote req msg id:  73
     Local next msg id: 2              Remote next msg id: 73
     Local req queued:  2              Remote req queued:  73
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

> **Nota:** L'ID locale e remoto nell'output è il **gruppo di tunnel denominato** definito sull'appliance ASA per verificare se ci si trova sul gruppo di tunnel corretto. È possibile verificare questa condizione anche se si esegue il debug di IKEv2 su entrambe le estremità.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando show.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

Sul router Cisco IOS, utilizzare:

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Sull'appliance ASA, usare:

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```