Exemplo de configuração de um túnel VPN IKEv2 de site para site dinâmico entre um ASA e um roteador IOS

Contents

Introduction

Este documento explica como configurar um túnel VPN de site para site com protocolo Internet Key Exchange versão 2 (IKEv2) entre um Adaptive Security Appliance (ASA) e um roteador Cisco, considerando que o roteador tenha um endereço IP dinâmico e o ASA tenha um endereço IP estático nas interfaces voltadas ao público.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS® versão 15.1(1)T ou posterior
- Cisco ASA versão 8.4(1) ou posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico.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.

Informações de Apoio

Este documento aborda os seguintes cenários:

- Cenário 1:O ASA está configurado com um endereço IP estático que usa um grupo nomeado de túneis, e o roteador está configurado com um endereço IP dinâmico.
- Cenário 2:O ASA está configurado com um endereço IP dinâmico, e o roteador está configurado com um endereço IP dinâmico.
- Cenário 3:Este cenário não será abordado neste documento.Neste cenário, o ASA está configurado com um endereço IP estático, mas usa o grupo de túneis DefaultL2LGroup.A configuração para este cenário é semelhante à descrita no artigo Exemplo de configuração de um túnel VPN dinâmico de site para site com protocolo IKEv2 entre dois ASAs.

A diferença de configuração mais significativa entre os cenários 1 e 3 é a ID do Protocolo de gerenciamento de chaves e associações de segurança da Internet (Internet Security Association and Key Management Protocol ou ISAKMP) usada pelo roteador remoto.Quando o DefaultL2LGroup é usado no ASA estático, a ID de ISAKMP do par no roteador precisa ser o endereço do ASA.Contudo, se um grupo nomeado de túneis é usado, a ID de ISAKMP do par no roteador precisa ser igual ao nome do grupo de túneis configurado no ASA.Para isso, segue o comando no roteador:

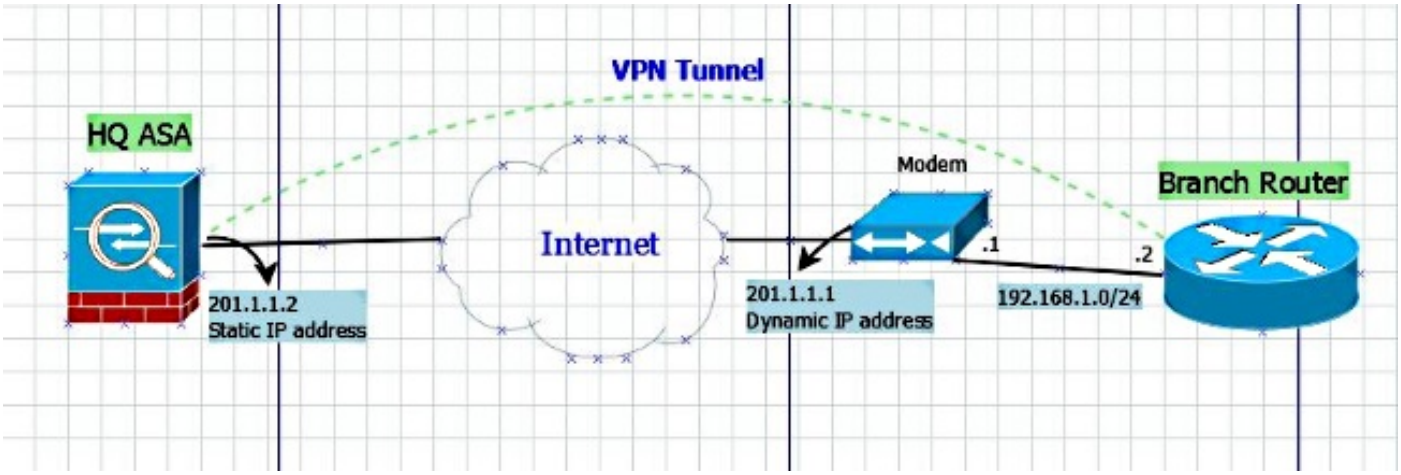
```
identity local key-id
```

A vantagem de usar grupos nomeados de túneis, como o DefaultL2LGroup, no ASA estático é que a configuração nos ASAs/roteadores dinâmicos remotos (inclusive as chaves pré-compartilhadas) deve ser idêntica, o que não permite muita granularidade quanto à definição de políticas.

Configurar

Cenário 1

Diagrama de Rede



Configuração

Esta seção descreve a configuração do ASA e do roteador com base na definição de um grupo nomeado de túneis.

Configuração do ASA estático

```
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
```

Configuração do roteador dinâmico

O Roteador Dinâmico é configurado quase da mesma forma que você configura normalmente nos casos em que o roteador é um local dinâmico para o túnel L2L IKEv2 com a adição de um comando, como mostrado aqui:

```
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
```

Assim, a ID da chave é diferente em cada par dinâmico, e um grupo de túneis correspondente deve ser criado no ASA estático com o nome correto, o que também aumenta a granularidade das políticas implementadas no ASA.

Cenário 2

> **Observação**: essa configuração só é possível quando pelo menos um lado é um roteador.Se ambos os pontos forem ASAs, essa configuração não funciona no momento.Na versão 8.4, o ASA não consegue usar o Nome de domínio totalmente qualificado (Fully Qualified Domain Name ou FQDN) com o comando set peer, mas o aperfeiçoamento do CSCus37350 já foi solicitado para as versões futuras.

Se o endereço IP do ASA remoto for dinâmico e tiver, contudo, um Nome de domínio totalmente qualificado atribuído à interface VPN, então, em vez de definir o endereço IP do ASA remoto, é

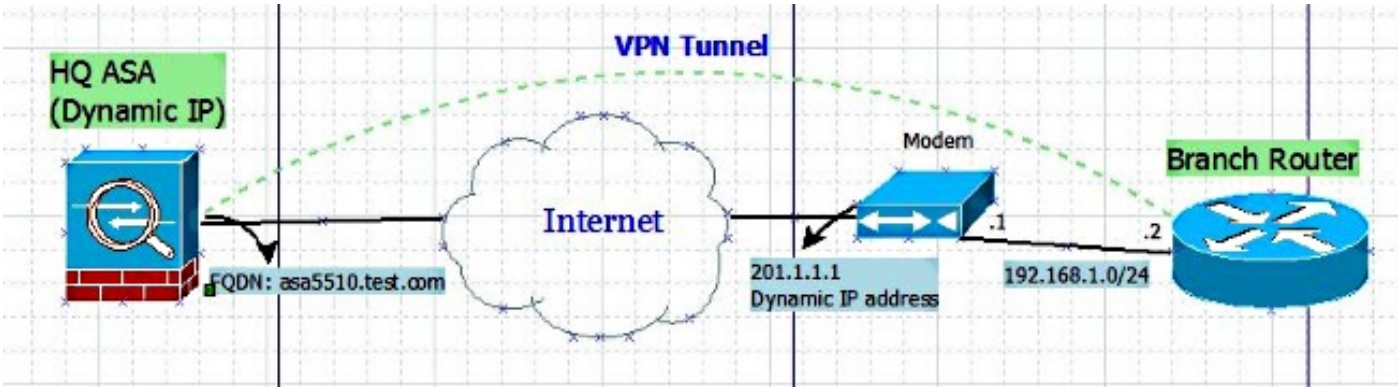
preciso definir o FQDN do ASA remoto com o seguinte comando no roteador:

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

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

> Dica:A palavra-chave dinâmica é opcional.Ao especificar o nome do host de um par IPsec remoto pelo comando set peer, também é possível emitir uma palavra-chave dinâmica que adiará a definição do Sistema de nomes de domínio (Domain Name Server ou DNS) até pouco antes do estabelecimento do túnel IPsec.
>
> O adiamento da resolução permite que o software do Cisco IOS detecte a possível alteração do endereço IP do par IPsec remoto.Assim, o software pode entrar em contato com o par no novo endereço IP.Se a palavra-chave dinâmica não for emitida, o nome do host é resolvido imediatamente após ser especificado.Assim, o software do Cisco IOS não consegue detectar a alteração do endereço IP e tenta se conectar ao endereço IP resolvido anteriormente.

Diagrama de Rede



Configuração

Configuração do ASA dinâmico

A configuração do ASA é a mesma que a Configuração do ASA estático , com apenas uma exceção: o endereço IP da interface física não está definido de modo estático.

Configuração do roteador

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

ASA estático

- Abaixo, segue o resultado do 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
```

- Abaixo, segue o resultado do 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
```

Roteador dinâmico

- Abaixo, segue o resultado do 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
```

- Abaixo, segue o resultado do 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:
```

Roteador dinâmico (com ASA dinâmico remoto)

- Abaixo, segue o resultado do 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:Para verificar se foi direcionado ao grupo de túneis correto, as IDs local e remota desse resultado devem ser o grupo nomeado de túneis que você definiu no ASA.Isso também pode ser verificado se você realizar o debug do IKEv2 nas duas extremidades.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição..Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

> Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

No roteador do Cisco IOS, use:

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

No ASA, use:

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