

# Local dinâmico para situar o túnel IKEv2 VPN entre um ASA e um exemplo de configuração do IOS Router

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Cenário 1](#)

[Diagrama de Rede](#)

[Configuração](#)

[Cenário 2](#)

[Diagrama de Rede](#)

[Configuração](#)

[Verificar](#)

[ASA estático](#)

[Roteador dinâmico](#)

[Roteador dinâmico \(com o ASA dinâmico remoto\)](#)

[Troubleshooting](#)

## Introdução

Este documento descreve como configurar um túnel de site para site da versão 2 do intercâmbio de chave de Internet (IKEv2) VPN entre uma ferramenta de segurança adaptável (ASA) e um roteador Cisco onde o roteador tenha um endereço IP dinâmico e o ASA tenha um endereço IP estático nas relações do público-revestimento.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

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

- Versão do <sup>®</sup> do Cisco IOS 15.1(1)T ou mais tarde
- Versão ASA de Cisco 8.4(1) ou mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Informações de Apoio

Este documento discute estas encenações:

- Cenário 1: Um ASA é configurado com um endereço IP estático que use um grupo de túneis Nomeado e o roteador seja configurado com um endereço IP dinâmico.
- Cenário 2: Um ASA é configurado com um endereço IP dinâmico e o roteador é configurado com um endereço IP dinâmico.
- Cenário 3: Esta encenação não é discutida aqui. Nesta encenação, o ASA é configurado com um endereço IP estático mas usa o grupo de túneis DefaultL2LGroup. A configuração para esta é similar ao que é descrito no [local dinâmico para situar um túnel IKEv2 VPN entre o artigo do exemplo de configuração dois ASA](#).

A diferença de configuração a mais grande entre as encenações 1 e 3 é o Internet Security Association and Key Management Protocol (ISAKMP) ID usado pelo roteador remoto. Quando o DefaultL2LGroup é usado no ASA estático, o ISAKMP ID do par no roteador deve ser o endereço do ASA. Contudo, se um grupo de túneis Nomeado é usado, o ISAKMP ID do par no roteador deve ser o mesmo que o nome de grupo de túneis configurado no ASA. Isto é realizado com este comando no roteador:

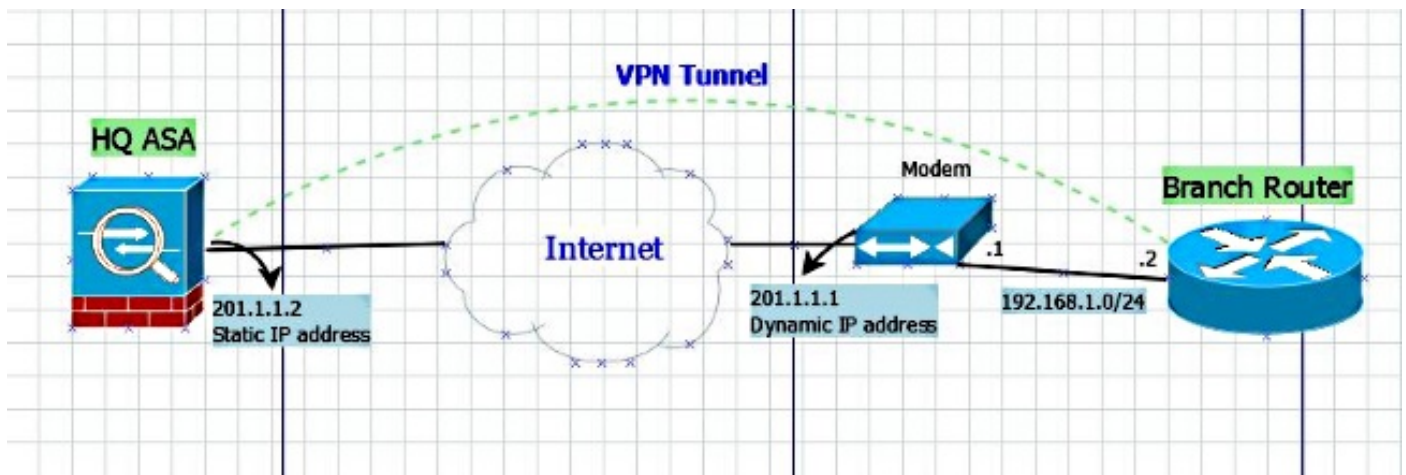
```
identity local key-id <name of the tunnel-group on the static ASA>
```

A vantagem de usar grupos de túneis Nomeados no ASA estático é que quando o DefaultL2LGroup é usado, a configuração nos ASA/Roteadores dinâmicos remotos, que inclui as chaves pré-compartilhada, deve ser idêntica e não permite muita granularidade com a instalação das políticas.

## Configurar

### Cenário 1

#### Diagrama de Rede



## Configuração

Esta seção descreve a configuração no ASA e no roteador baseados na configuração Nomeado do grupo de túneis.

### Configuração estática ASA

```
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 de roteador dinâmica

O roteador dinâmico é configurado quase a mesma maneira que você configura normalmente nos casos onde o roteador é um local dinâmico para o túnel IKEv2 L2L 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 em cada par dinâmico, a chave-identificação é diferente e um grupo de túneis correspondente deve ser criado no ASA estático com o nome direito, que igualmente aumenta a granularidade dos policias que são executados em um ASA.

## Cenário 2

Nota: Esta configuração é somente possível quando pelo menos um lado é um roteador. Se os ambos os lados são ASA, esta instalação não trabalha neste tempo. Na versão 8.4, o ASA não pode usar o nome de domínio totalmente qualificado (FQDN) com o **comando set peer**, mas o realce [CSCus37350](#) foi pedido para as liberações futuras.

Se o endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA remoto é dinâmico também contudo tem um nome de domínio totalmente qualificado atribuído para sua relação VPN, a seguir um pouco do que define o endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA remoto, você definem agora o FQDN do ASA remoto com este comando no roteador:

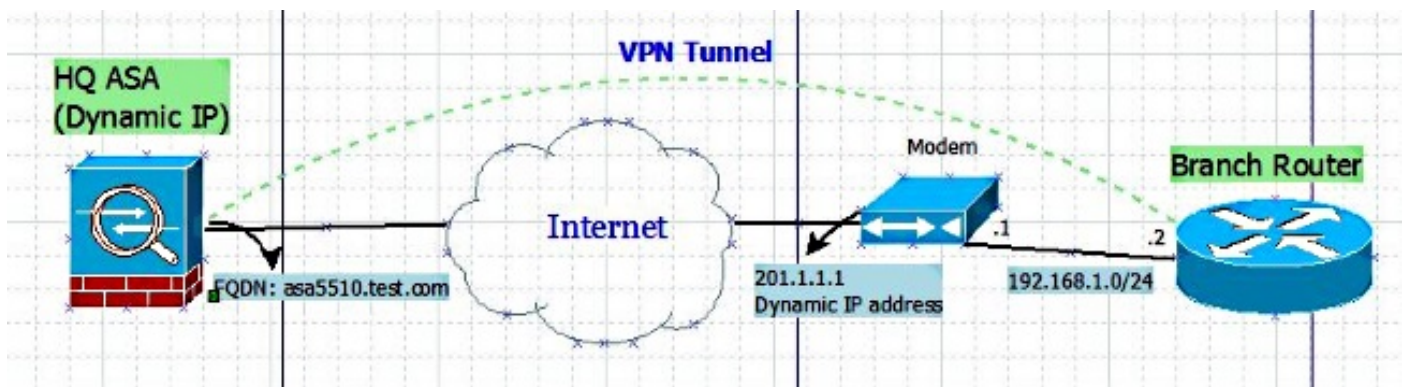
```
C1941(config)#do show run | sec crypto map
```

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

Dica: **A palavra-chave dinâmica** é opcional. Quando você especifica o hostname de um ipsec peer remoto através do **comando set peer**, você pode igualmente emitir a palavra-chave dinâmica, que adie a definição do Domain Name Server (DNS) do hostname até que mesmo antes do túnel de IPsec foi estabelecida.

A definição de adiamento permite o Cisco IOS Software de detectar se o endereço IP de Um ou Mais Servidores Cisco ICM NT do ipsec peer remoto mudou. Assim, o software pode contactar o par no endereço IP de Um ou Mais Servidores Cisco ICM NT novo. Se a palavra-chave dinâmica não é emitida, o hostname é resolved imediatamente depois que se especifica. Assim, o Cisco IOS Software não pode detectar uma mudança do endereço IP de Um ou Mais Servidores Cisco ICM NT e, conseqüentemente, tentativas de conectar ao endereço IP de Um ou Mais Servidores Cisco ICM NT esse resolveu previamente.

## Diagrama de Rede



## Configuração

### Configuração dinâmica ASA

A configuração no ASA é a mesma que a [configuração estática ASA](#) com somente uma exceção, que é que o endereço IP de Um ou Mais Servidores Cisco ICM NT na interface física não está definido estaticamente.

### 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

- Está aqui o resultado do comando **cripto do det IKEv2 sa da mostra:**

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
```

- Está aqui o resultado do comando **show crypto ipsec sa:**

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

```

## Roteador dinâmico

- Está aqui o resultado do comando **detail crypto IKEv2 sa** da mostra:

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

- Está aqui o resultado do comando **show crypto ipsec sa**:

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

## Roteador dinâmico (com o ASA dinâmico remoto)

- Está aqui o resultado do comando `detail cripto IKEv2 sa` da mostra:

```

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: O ID remoto e local nesta saída é o **grupo de túneis que Nomeado** você definiu no ASA para verificar se você cai no grupo de túneis adequado. Isto pode igualmente ser verificado se você debuga IKEv2 em uma ou outra extremidade.

## Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

[A ferramenta Output Interpreter \(clientes registrados somente\)](#) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

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
```