

Exemplo de Configuração de Túnel VPN IKEv2 de Site para Site Dinâmico entre Dois ASAs

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Solução 1 - Uso do grupo L2LG padrão](#)

[Configuração do ASA estático](#)

[ASA dinâmico](#)

[Solução 2 - Criar um grupo de túnel definido pelo usuário](#)

[Configuração do ASA estático](#)

[Configuração do ASA dinâmico](#)

[Verificar](#)

[No ASA estático](#)

[No ASA dinâmico](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar um túnel VPN de Internet Key Exchange Versão 2 (IKEv2) entre dois Adaptive Security Appliances (ASAs) em que um ASA tem um endereço IP dinâmico e o outro tem um endereço IP estático.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- ASA versão 5505
- ASA versão 9.1(5)

The information in this document was created from the devices in a specific lab environment. 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

Há duas maneiras de configurar esta configuração:

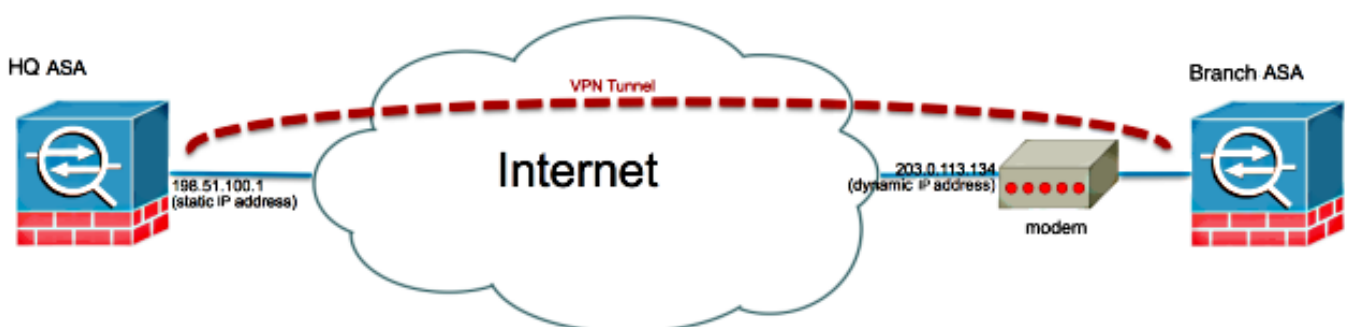
- Com o grupo de túnel DefaultL2LGroup
- Com um grupo de túnel nomeado

A maior diferença de configuração entre os dois cenários é a ID do ISAKMP (Internet Security Association and Key Management Protocol) usada pelo ASA remoto. Quando o DefaultL2LGroup é usado no ASA estático, a ID ISAKMP do peer deve ser o endereço. No entanto, se um grupo de túneis nomeado for usado, a ID ISAKMP do peer deve ser a mesma do grupo de túneis usando este comando:

```
crypto isakmp identity key-id
```

A vantagem de usar grupos de túnel nomeados no ASA estático é que quando o DefaultL2LGroup é usado, a configuração nos ASAs dinâmicos remotos, que inclui as chaves pré-compartilhadas, deve ser idêntica e não permite muita granularidade com a configuração de políticas.

Diagrama de Rede



Configurar

Esta seção descreve a configuração em cada ASA, dependendo da solução que você decidir usar.

Solução 1 - Uso do grupo L2LG padrão

Essa é a maneira mais simples de configurar um túnel de LAN para LAN (L2L) entre dois ASAs quando um ASA obtém seu endereço dinamicamente. O Grupo L2L padrão é um grupo de túnel pré-configurado no ASA e todas as conexões que não correspondem explicitamente a nenhum grupo de túnel específico caem nessa conexão. Como o ASA dinâmico não tem um endereço IP predeterminado constante, significa que o administrador não pode configurar o ASA estático para permitir a conexão em um grupo de túnel específico. Nessa situação, o Grupo L2L padrão pode ser usado para permitir as conexões dinâmicas.

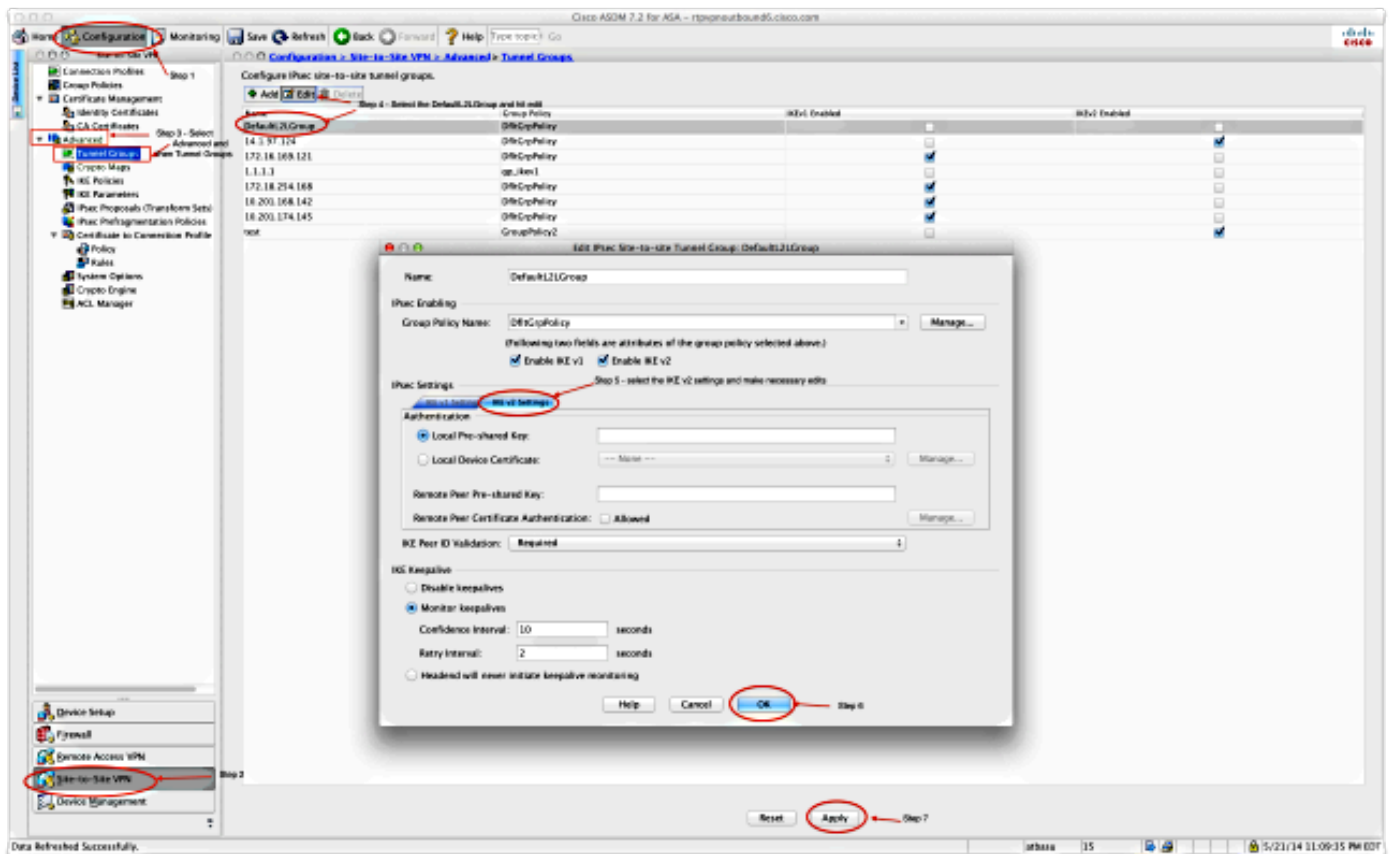
Dica: com esse método, o lado negativo é que todos os peers terão a mesma chave pré-compartilhada, pois somente uma chave pré-compartilhada pode ser definida por grupo de túnel e todos os peers se conectarão ao mesmo grupo de túneis DefaultL2LG.

Configuração do ASA estático

```
interface Ethernet0/0
 nameif inside
 security-level 100
 IP address 172.30.2.6 255.255.255.0
!
interface Ethernet0/3
 nameif Outside
 security-level 0
 IP address 207.30.43.15 255.255.255.128
!
boot system disk0:/asa915-k8.bin
crypto ipsec IKEv2 ipsec-proposal Site2Site
 protocol esp encryption aes-256
 protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 10 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-
256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map Outside_map interface Outside
```

```
crypto IKEv2 policy 2
  encryption aes-256
  integrity sha512
  group 24
  prf sha512
  lifetime seconds 86400
crypto IKEv2 policy 3
  encryption aes-256
  integrity sha group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 40
  encryption des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 enable inside client-services port 443
crypto IKEv2 enable Outside client-services port 443
group-policy Site2Site internal
group-policy Site2Site attributes
  vpn-idle-timeout none
  vpn-session-timeout none
  vpn-filter none
  vpn-tunnel-protocol IKEv2
tunnel-group DefaultL2LGroup general-attributes
  default-group-policy Site2Site
tunnel-group DefaultL2LGroup ipsec-attributes
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****
```

No Adaptive Security Device Manager (ASDM), você pode configurar o DefaultL2LGroup como mostrado aqui:



ASA dinâmico

```

interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 IP address 172.16.1.1 255.255.255.224
!
interface Vlan2
 nameif outside
 security-level 0
 IP address dhcp setroute
!
ftp mode passive
object network NETWORK_OBJ_172.16.1.0_24
 subnet 172.16.1.0 255.255.255.0

```

```
object-group network DM_INLINE_NETWORK_1
  network-object object 10.0.0.0
  network-object object 172.0.0.0
access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
object-group DM_INLINE_NETWORK_1
nat (inside,outside) source static NETWORK_OBJ_172.16.1.0_24 NETWORK_OBJ_
172.16.1.0_24 destination static DM_INLINE_NETWORK_1 DM_INLINE_NETWORK_1
nat (inside,outside) source dynamic any interface
crypto ipsec IKEv2 ipsec-proposal Site2Site
  protocol esp encryption aes-256
  protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal DES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs group5
crypto map outside_map 1 set peer 198.51.100.1
crypto map outside_map 1 set ikev1 phase1-mode aggressive group5
crypto map outside_map 1 set IKEv2 ipsec-proposal Site2Site
crypto map outside_map interface outside
crypto IKEv2 policy 2
  encryption aes-256
  integrity sha512
  group 24
  prf sha512
  lifetime seconds 86400
crypto IKEv2 policy 3
  encryption aes-256
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 40
```

```

encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 enable outside
management-access inside
group-policy GroupPolicy_198.51.100.1 internal
group-policy GroupPolicy_198.51.100.1 attributes
  vpn-tunnel-protocol IKEv2
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 general-attributes
  default-group-policy GroupPolicy_198.51.100.1
tunnel-group 198.51.100.1 ipsec-attributes
  ikev1 pre-shared-key *****
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****

```

No ASDM, você pode usar o assistente padrão para configurar o perfil de conexão apropriado ou simplesmente adicionar uma nova conexão e seguir o procedimento padrão.

Solução 2 - Criar um grupo de túnel definido pelo usuário

Esse método exige um pouco mais de configuração, mas permite mais granularidade. Cada peer pode ter sua própria política separada e chave pré-compartilhada. No entanto, aqui é importante alterar a ID ISAKMP no peer dinâmico para que ele use um nome em vez de um endereço IP. Isso permite que o ASA estático corresponda à solicitação de inicialização de ISAKMP recebida para o grupo de túnel direito e use as políticas certas.

Configuração do ASA estático

```

interface Ethernet0/0
  nameif inside
  security-level 100
  IP address 172.16.0.1 255.255.255.0
!
interface Ethernet0/3
  nameif Outside
  security-level 0
  IP address 198.51.100.1 255.255.255.128
!
boot system disk0:/asa915-k8.bin
object-group network DM_INLINE_NETWORK_1
  network-object object 10.0.0.0
  network-object object 172.0.0.0

access-list Outside_cryptomap_1 extended permit IP object-group DM_INLINE_NETWORK_
1 172.16.1.0 255.255.255.0

crypto ipsec IKEv2 ipsec-proposal Site2Site
  protocol esp encryption aes-256
  protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
  protocol esp encryption aes-192

```

```
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
protocol esp encryption 3des
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-
SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set IKEv2 ipsec-proposal
AES256 AES192 AES 3DES DES
crypto dynamic-map DynamicSite2Site1 4 match address Outside_cryptomap_1
crypto dynamic-map DynamicSite2Site1 4 set IKEv2 ipsec-proposal Site2Site
crypto map Outside_map 65534 ipsec-isakmp dynamic DynamicSite2Site1
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map Outside_map interface Outside
```

```
crypto IKEv2 policy 2
encryption aes-256
integrity sha512
group 24
prf sha512
lifetime seconds 86400
```

```
crypto IKEv2 policy 3
encryption aes-256
integrity sha
group 5 2
prf sha
lifetime seconds 86400
```

```
crypto IKEv2 policy 10
encryption aes-192
integrity sha
group 5 2
prf sha
lifetime seconds 86400
```

```
crypto IKEv2 policy 20
encryption aes
integrity sha
group 5 2
prf sha
lifetime seconds 86400
```

```
crypto IKEv2 policy 30
encryption 3des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
```

```
crypto IKEv2 policy 40
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
```

```
crypto IKEv2 enable Outside client-services port 443
management-access inside
```

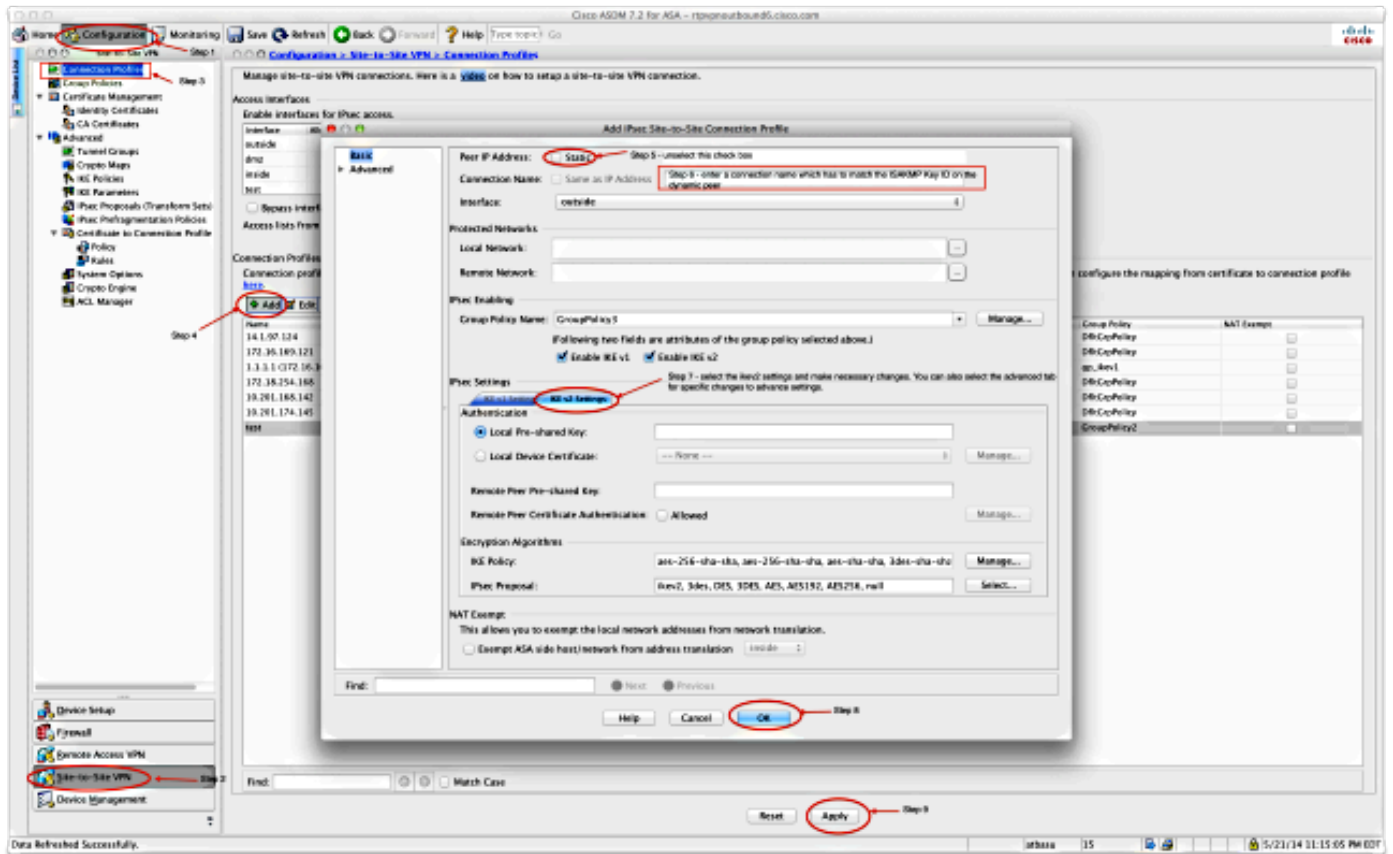
```
group-policy GroupPolicy4 internal
group-policy GroupPolicy4 attributes
```



```
vpn-tunnel-protocol IKEv2
```

```
tunnel-group DynamicSite2Site1 type ipsec-l2l  
tunnel-group DynamicSite2Site1 general-attributes  
  default-group-policy GroupPolicy4  
tunnel-group DynamicSite2Site1 ipsec-attributes  
  IKEv2 remote-authentication pre-shared-key *****  
  IKEv2 local-authentication pre-shared-key *****
```

No ASDM, o nome do perfil de conexão é um endereço IP por padrão. Então, ao criá-la, você deve alterá-la para dar um nome como mostrado na imagem aqui:



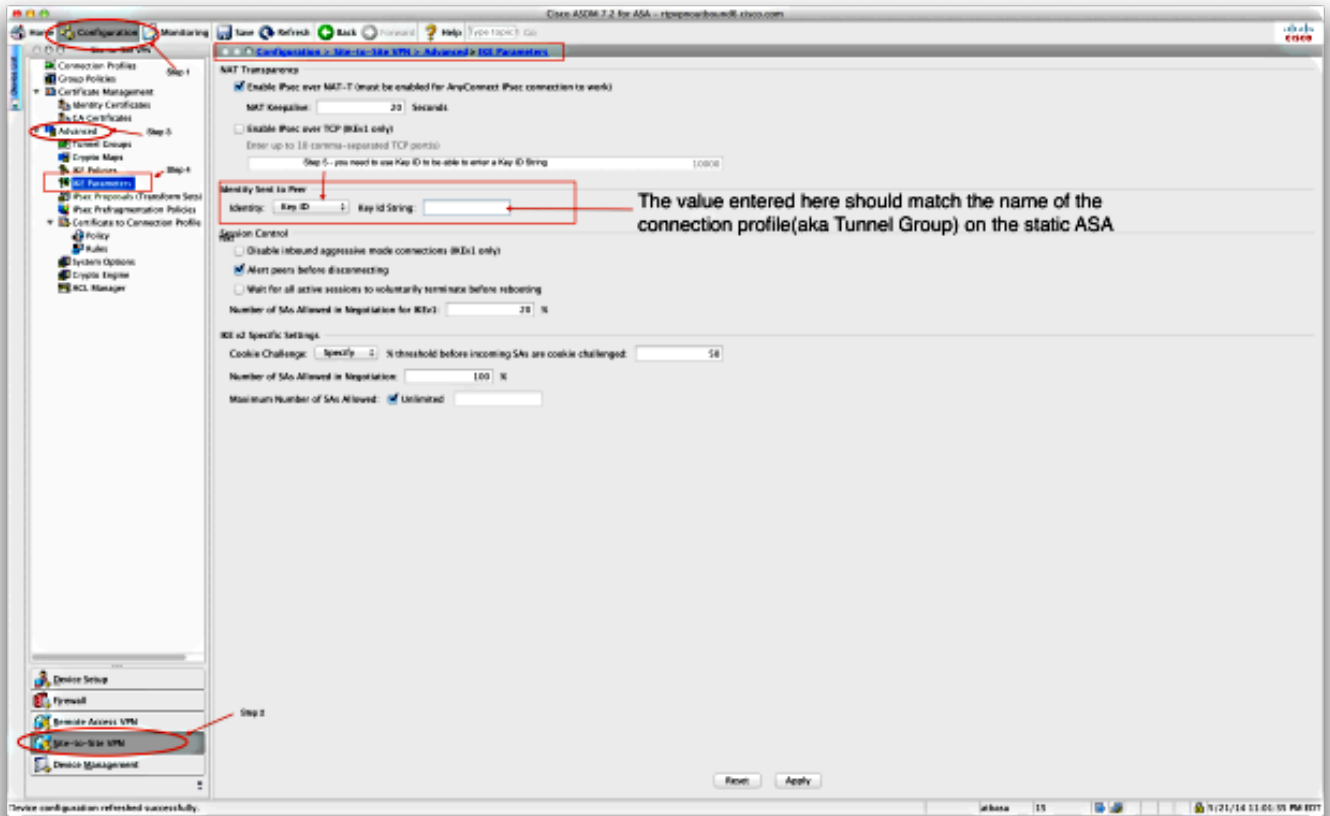
Configuração do ASA dinâmico

O ASA dinâmico é configurado quase da mesma maneira em ambas as soluções com a adição de um comando, como mostrado aqui:

```
crypto isakmp identity key-id DynamicSite2Site1
```

Como descrito anteriormente, por padrão, o ASA usa o endereço IP da interface para a qual o túnel VPN está mapeado como ID-chave ISAKMP. Entretanto, nesse caso, a ID da chave no ASA dinâmico é igual ao nome do grupo de túneis no ASA estático. Assim, em cada peer dinâmico, o key-id será diferente e um grupo de túneis correspondente deve ser criado no ASA estático com o nome correto.

No ASDM, isso pode ser configurado conforme mostrado nesta captura de tela:



Verificar

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

No ASA estático

Abaixo, segue o resultado do comando **show crypto IKEv2 sa det:**

IKEv2 SAs:

Session-id:132, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id           Local              Remote            Status            Role
1574208993          198.51.100.1/4500 203.0.113.134/4500  READY            RESPONDER
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK,
```

Auth verify: PSK

Life/Active Time: 86400/352 sec

Session-id: 132

Status Description: Negotiation done

Local spi: 4FDF215BDEC73EC Remote spi: 2414BEA1E10E3F70

Local id: 198.51.100.1

Remote id: DynamicSite2Site1

Local req mess id: 13

Remote req mess id: 17

Local next mess id: 13

Remote next mess id: 17

Local req queued: 13

Remote req queued: 17

Local window: 1

Remote window: 1

DPD configured for 10 seconds, retry 2

NAT-T is detected outside

```
Child sa: local selector 172.0.0.0/0 - 172.255.255.255/65535
remote selector 172.16.1.0/0 - 172.16.1.255/65535
ESP spi in/out: 0x9fd5c736/0x6c5b3cc9
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, 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: DynamicSite2Site1, seq num: 4, local addr: 198.51.100.1

access-list Outside_cryptomap_1 extended permit IP 172.0.0.0 255.0.0.0
172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 203.0.113.134

#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 12, #pkts decrypt: 12, #pkts verify: 12
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1, #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.: 198.51.100.1/4500, remote crypto endpt.:
203.0.113.134/4500
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: 6C5B3CC9
current inbound spi : 9FD5C736

inbound esp sas:
spi: 0x9FD5C736 (2681587510)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
sa timing: remaining key lifetime (kB/sec): (4193279/28441)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00001FFF

outbound esp sas:
spi: 0x6C5B3CC9 (1817918665)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
sa timing: remaining key lifetime (kB/sec): (3962879/28441)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

No ASA dinâmico

Abaixo, segue o resultado do comando **show crypto IKEv2 sa detail:**

IKEv2 SAs:

Session-id:11, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id          Local              Remote            Status            Role
1132933595        192.168.50.155/4500  198.51.100.1/4500  READY            INITIATOR
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK,
Auth verify: PSK
  Life/Active Time: 86400/267 sec
  Session-id: 11
  Status Description: Negotiation done
  Local spi: 2414BEA1E10E3F70      Remote spi: 4FDFF215BDEC73EC
  Local id: DynamicSite2Site1
  Remote id: 198.51.100.1
  Local req mess id: 13             Remote req mess id: 9
  Local next mess id: 13           Remote next mess id: 9
  Local req queued: 13             Remote req queued: 9
  Local window: 1                  Remote window: 1
  DPD configured for 10 seconds, retry 2
  NAT-T is detected inside
Child sa: local selector 172.16.1.0/0 - 172.16.1.255/65535
  remote selector 172.0.0.0/0 - 172.255.255.255/65535
  ESP spi in/out: 0x6c5b3cc9/0x9fd5c736
  AH spi in/out: 0x0/0x0
  CPI in/out: 0x0/0x0
  Encr: AES-CBC, keysize: 256, 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: outside_map, seq num: 1, local addr: 192.168.50.155

  access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
172.0.0.0 255.0.0.0
  local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
  current_peer: 198.51.100.1

  #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
  #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 12, #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.: 192.168.50.155/4500, remote crypto endpt.:
198.51.100.1/4500
  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: 9FD5C736
  current inbound spi : 6C5B3CC9

inbound esp sas:
  spi: 0x6C5B3CC9 (1817918665)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 5, IKEv2, }
  slot: 0, conn_id: 77824, crypto-map: outside_map
```

```
sa timing: remaining key lifetime (kB/sec): (4008959/28527)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000003
outbound esp sas:
spi: 0x9FD5C736 (2681587510)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 5, IKEv2, }
slot: 0, conn_id: 77824, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4147199/28527)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000001
```

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..

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..

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

- pacote de criptografia deb IKEv2
- deb crypto IKEv2 internal