

Esempio di configurazione di un tunnel VPN da sito a sito IKEv2 tra due appliance ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Soluzione 1 - Utilizzo del gruppo L2L predefinito](#)

[Configurazione ASA statica](#)

[ASA dinamica](#)

[Soluzione 2 - Creazione di un gruppo di tunnel definito dall'utente](#)

[Configurazione ASA statica](#)

[Configurazione ASA dinamica](#)

[Verifica](#)

[Sull'appliance ASA statica](#)

[Sull'appliance ASA dinamica](#)

[Risoluzione dei problemi](#)

Introduzione

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

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:

- ASA versione 5505
- ASA versione 9.1(5)

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

È possibile impostare questa configurazione in due modi:

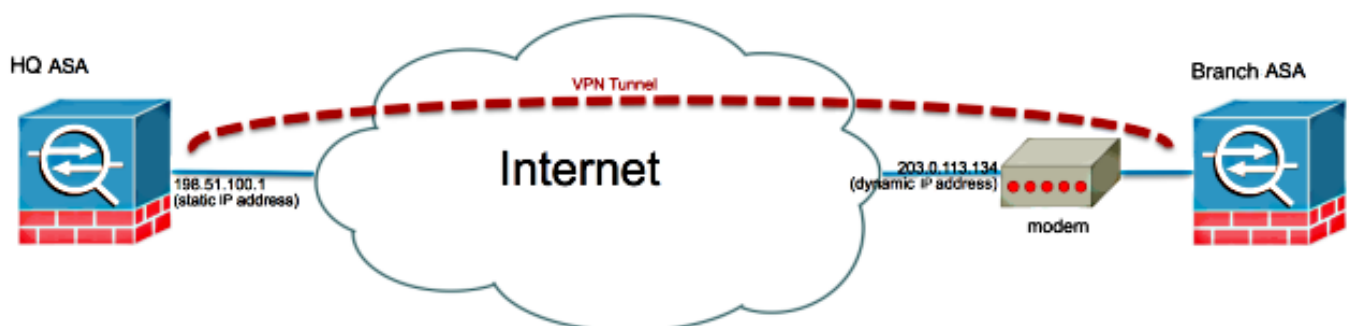
- Con il gruppo di tunnel DefaultL2LGroup
- Con un gruppo di tunnel denominato

La differenza di configurazione più grande tra i due scenari è che l'ID ISAKMP (Internet Security Association) e l'ID del protocollo ISAKMP (Key Management Protocol) vengono utilizzati dall'appliance ASA remota. Quando si usa DefaultL2LGroup sull'appliance ASA statica, l'ID ISAKMP del peer deve essere l'indirizzo. Tuttavia, se si usa un gruppo di tunnel denominato, l'ID ISAKMP del peer deve essere lo stesso nome del gruppo di tunnel usando questo comando:

```
crypto isakmp identity 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 sulle appliance ASA dinamiche remote, che include le chiavi già condivise, deve essere identica e non consente una grande granularità con l'impostazione dei criteri.

Esempio di rete



Configurazione

In questa sezione viene descritta la configurazione di ciascuna ASA a seconda della soluzione

che si decide di usare.

Soluzione 1 - Utilizzo del gruppo L2L predefinito

Questo è il modo più semplice per configurare un tunnel LAN-LAN (L2L) tra due appliance ASA quando un'appliance ASA ottiene il proprio indirizzo in modo dinamico. Il gruppo DefaultL2L è un gruppo di tunnel preconfigurato sull'appliance ASA e tutte le connessioni che non corrispondono esplicitamente a un particolare gruppo di tunnel appartengono a questa connessione. Poiché l'appliance ASA dinamica non ha un indirizzo IP predeterminato costante, significa che l'amministratore non può configurare l'appliance ASA statica per consentire la connessione su un gruppo di tunnel specifico. In questo caso, è possibile utilizzare il gruppo DefaultL2L per consentire le connessioni dinamiche.

Suggerimento: con questo metodo, l'aspetto negativo è che tutti i peer avranno la stessa chiave precondivisa, in quanto è possibile definire una sola chiave precondivisa per gruppo di tunnel e tutti i peer si conetteranno allo stesso gruppo di tunnel DefaultL2LGroup.

Configurazione ASA statica

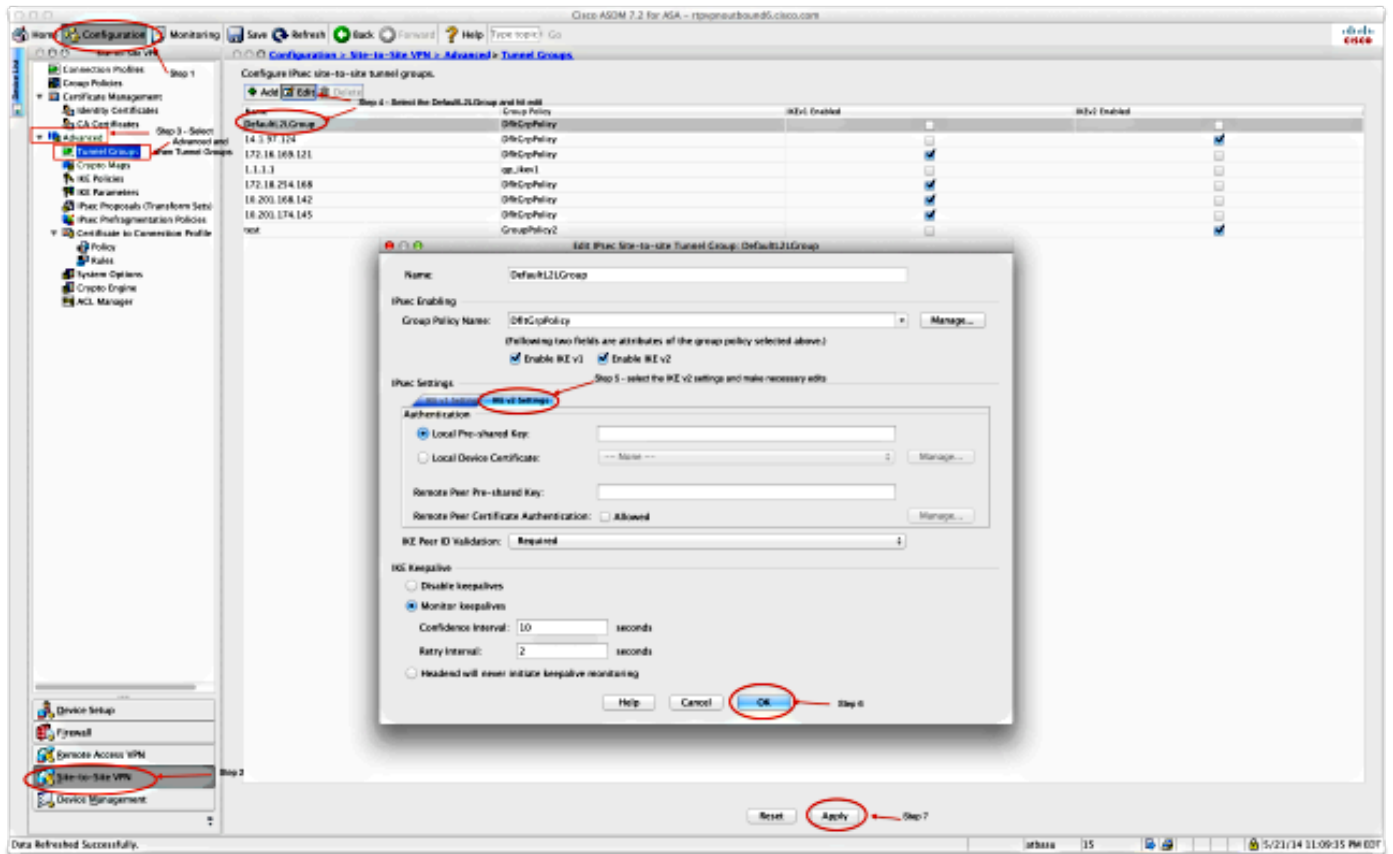
```
interface Ethernet0/0
 nameif inside
 security-level 100
 IP address 172.30.2.6 255.255.255.0
!
interface Ethernet0/3
 nameif Outside
 security-level 0
 IP address 207.30.43.15 255.255.255.128
!
boot system disk0:/asa915-k8.bin
crypto ipsec IKEv2 ipsec-proposal Site2Site
 protocol esp encryption 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 *****

```

In Adaptive Security Device Manager (ASDM) è possibile configurare il gruppo L2L predefinito come mostrato di seguito:



ASA dinamica

```

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 *****

```

Su ASDM, è possibile utilizzare la procedura guidata standard per impostare il profilo di connessione appropriato oppure è sufficiente aggiungere una nuova connessione e seguire la procedura standard.

Soluzione 2 - Creazione di un gruppo di tunnel definito dall'utente

Questo metodo richiede una configurazione leggermente maggiore, ma consente una maggiore granularità. Ogni peer può disporre di criteri separati e di una chiave già condivisa. In questo caso, tuttavia, è importante modificare l'ID ISAKMP nel peer dinamico in modo che utilizzi un nome anziché un indirizzo IP. In questo modo, l'appliance ASA statica può far corrispondere la richiesta di inizializzazione ISAKMP in arrivo al gruppo di tunnel corretto e usare i criteri corretti.

Configurazione ASA statica

```

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

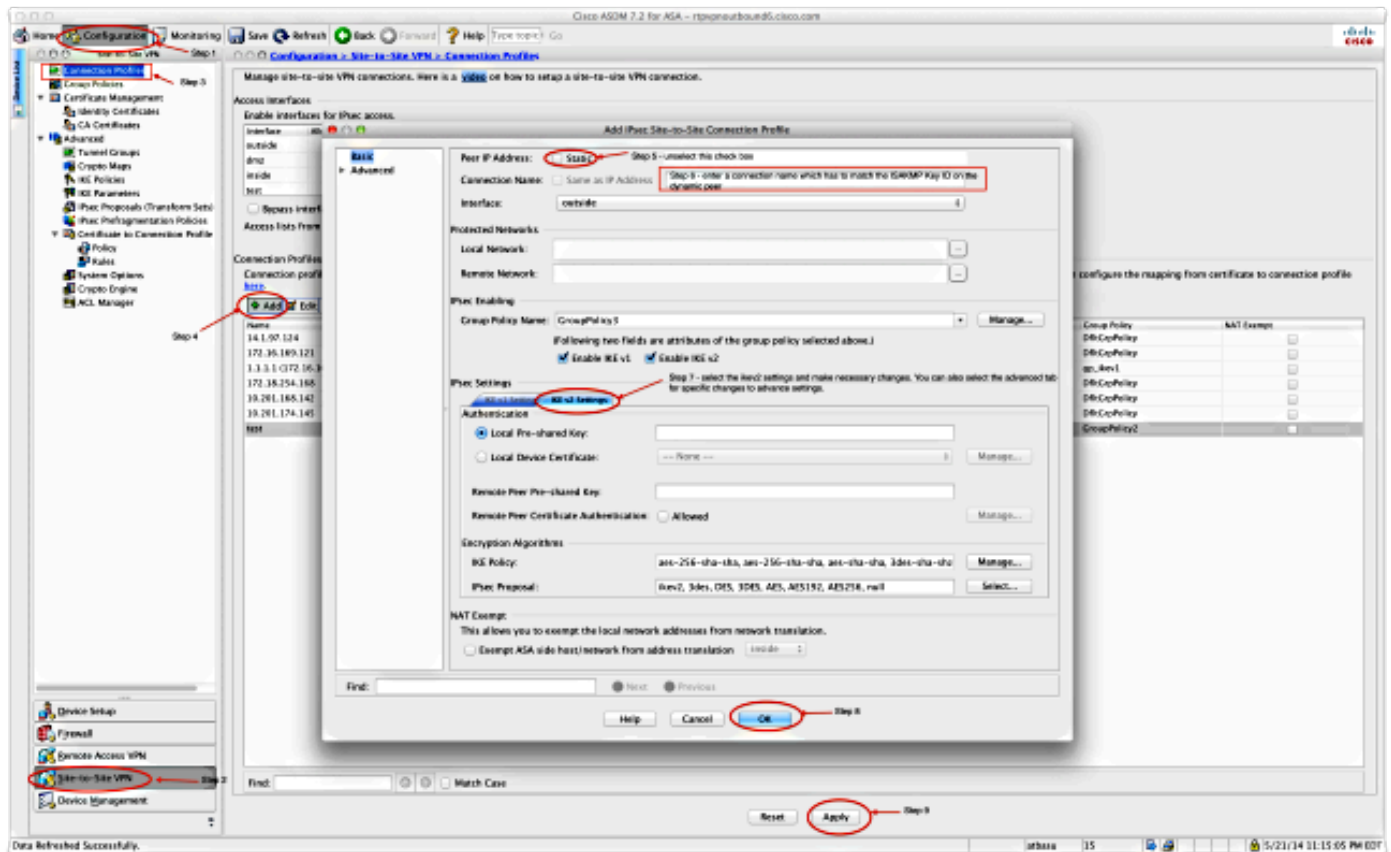
group-policy GroupPolicy4 internal
```



```
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 *****
```

In ASDM, il nome del profilo di connessione è un indirizzo IP per impostazione predefinita. Quindi, quando lo create, dovete cambiarlo per dargli un nome, come mostrato nello screenshot qui:



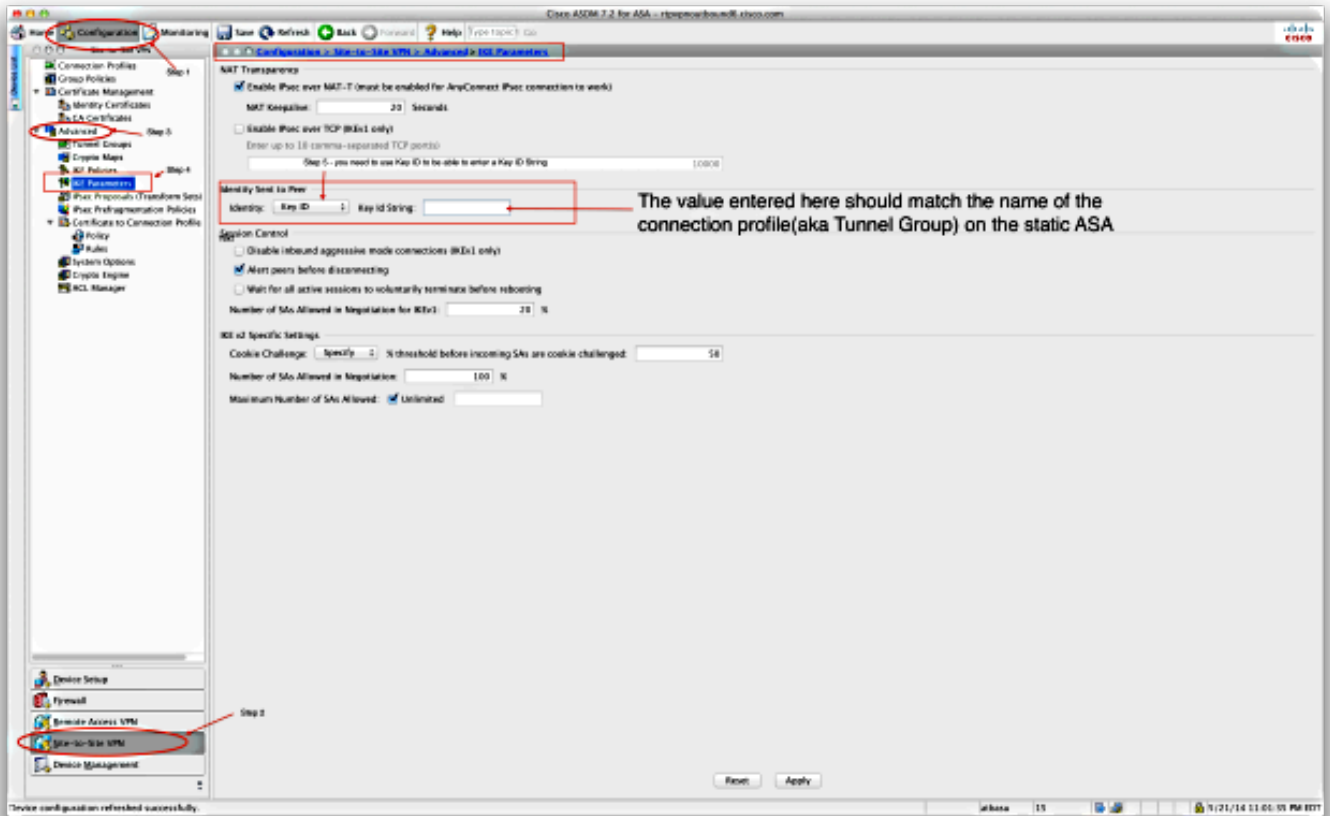
Configurazione ASA dinamica

La configurazione dell'ASA dinamica è quasi identica in entrambe le soluzioni con l'aggiunta di un comando, come mostrato di seguito:

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

Come descritto sopra, per impostazione predefinita l'ASA usa l'indirizzo IP dell'interfaccia a cui è mappato il tunnel VPN come ID della chiave ISAKMP. Tuttavia, in questo caso, l'ID della chiave sull'appliance ASA dinamica è uguale al nome del gruppo di tunnel sull'appliance ASA statica. Pertanto, su ogni peer dinamico, l'ID della chiave sarà diverso e sarà necessario creare un gruppo di tunnel corrispondente sull'appliance ASA statica con il nome corretto.

Sull'appliance ASDM, è possibile configurare la porta come mostrato in questa schermata:



Verifica

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

Sull'appliance ASA statica

Di seguito viene riportato il risultato del 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: 4FDFF215BDEC73EC          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
```

Di seguito viene riportato il risultato del 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
```

Sull'appliance ASA dinamica

Di seguito viene riportato il risultato del 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
```

Di seguito viene riportato il risultato del 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
```

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.

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.

- **Deb crypto IKEv2 packet**
- **deb crypto IKEv2 internal**