Dynamic Site to Site IKEv2 VPN Tunnel Between Two ASAs Configuration Example

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Network Diagram
Configure
Solution 1 - Use of the DefaultL2LGroup
Static ASA Configuration
Dynamic ASA
Solution 2 - Create a User-Defined Tunnel-Group
Static ASA Configuration
Dynamic ASA Configuration
Verify
On the Static ASA
On the Dynamic ASA
Troubleshoot

Introduction

This document describes how to configure a site-to-site Internet Key Exchange Version 2 (IKEv2) VPN tunnel between two Adaptive Security Appliances (ASAs) where one ASA has a dynamic IP address and the other has a static IP address.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- ASA Version 5505
- ASA Version 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.

Background Information

There are two ways that this configuration can be set up:

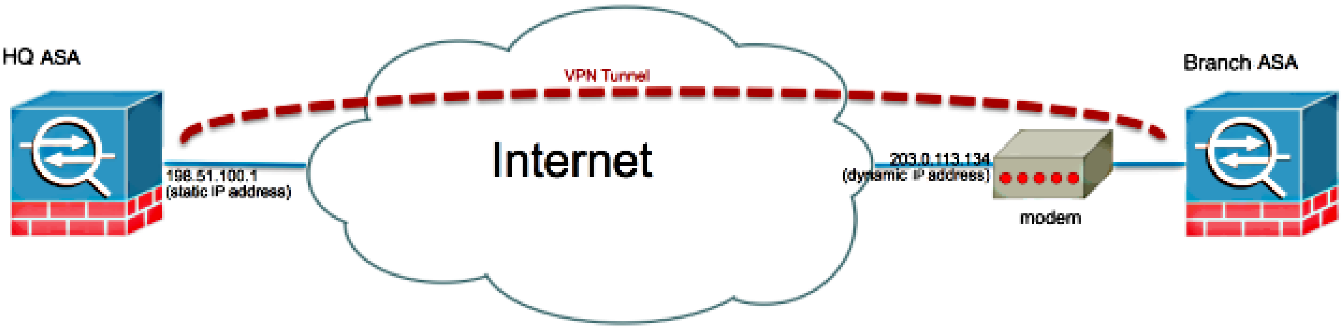
- With the DefaultL2LGroup tunnel group
- With a named tunnel group

The biggest configuration difference between the two scenarios is the Internet Security Association and Key Management Protocol (ISAKMP) ID used by the remote ASA. When the DefaultL2LGroup is used on the static ASA, the peer's ISAKMP ID has to be the address. However if a named tunnel group is used, the peer's ISAKMP ID has to be the same the tunnel group name using this command:

```
crypto isakmp identity key-id <tunnel-group_name>
```

The advantage of using named tunnel groups on the static ASA is that when the DefaultL2LGroup is used, the configuration on the remote dynamic ASAs, which includes the pre-shared keys, has to be identical and it does not allow for much granularity with the setup of policies.

Network Diagram



Configure

This section describes the configuration on each ASA depending on which solution you decide to use.

Solution 1 - Use of the DefaultL2LGroup

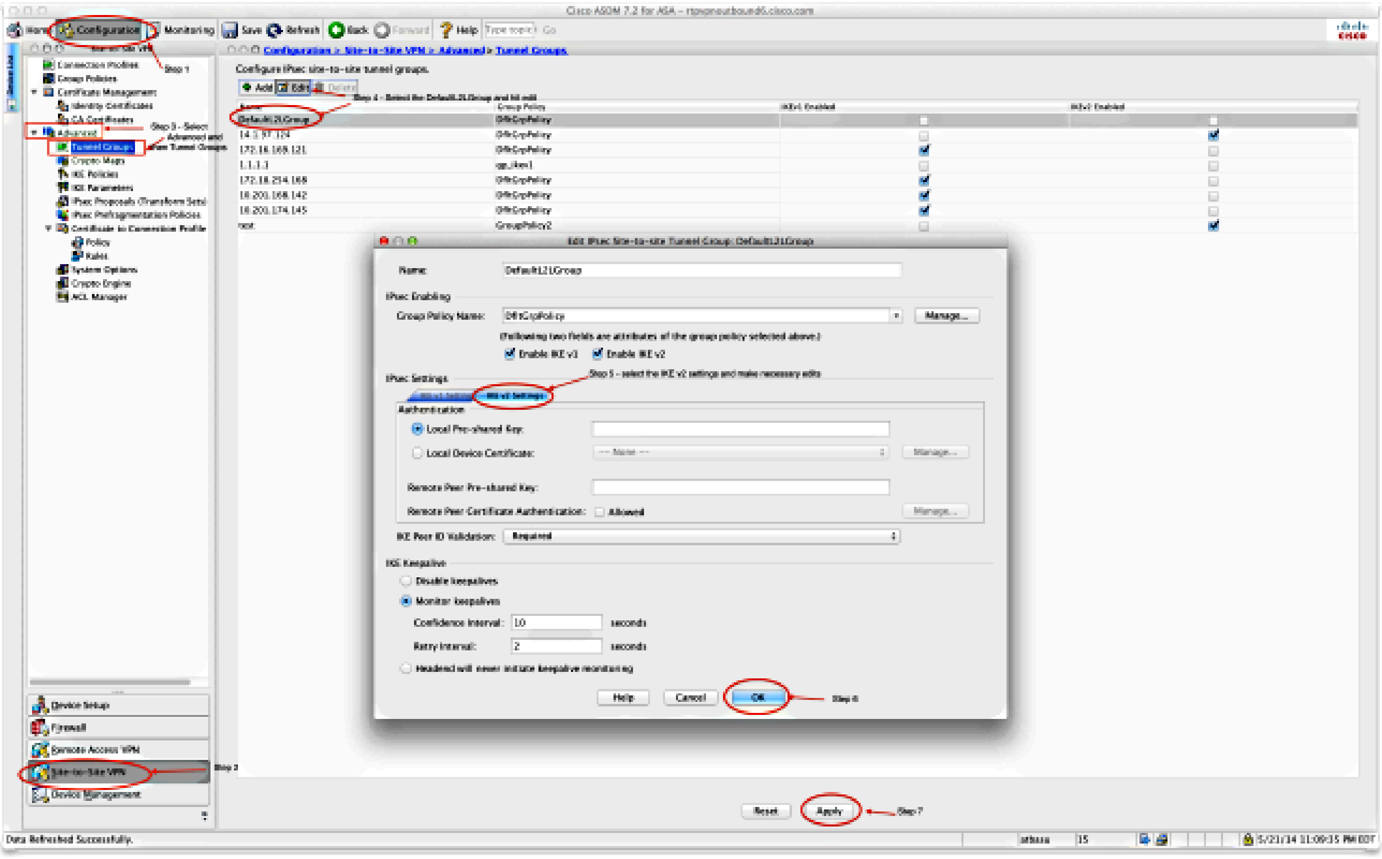
This is the simplest way to configure a LAN-to-LAN (L2L) tunnel betwen two ASAs when one ASA gets its address dynamically. The DefaultL2L Group is a preconfigured tunnel group on the ASA and all connections that do not explicitly match any particular tunnel group fall on this connection. Since the Dynamic ASA does not have a constant predetermined IP address, it means the admin cannot configure the Statis ASA in order to allow the connection on a specific tunnel group. In this situation, the DefaultL2L Group can be used in order to allow the dynamic connections.

> **Tip**: With this method, the downside is that all peers will have the same pre-shared key since only one pre-shared key can be defined per tunnel-group and all of the peers will connect to the same DefaultL2LGroup tunnel-group.

Static ASA Configuration

```
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_CRYPTO_MAP 10 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 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_CRYPTO_MAP 65535 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
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 *****
```

On the Adaptive Security Device Manager (ASDM), you can configure the DefaultL2LGroup as shown here:



Cisco ASDM 7.2 for ASA - rtpvpnoutbound6.cisco.com

Configuration > Site-to-Site VPN > Advanced > Tunnel Groups

Step 1

Step 2

Step 3 - Select Advanced and then Tunnel Groups

Step 4 - Select the DefaultL2LGroup and hit edit

Configure IPsec site-to-site tunnel groups.

Name	Group Policy	IKEv1 Enabled	IKEv2 Enabled
DefaultL2LGroup	DfltGrpPolicy	☐	☐
14.1.97.124	DfltGrpPolicy	☐	☑
172.16.169.121	DfltGrpPolicy	☑	☐
1.1.1.1	gp_ikev1	☐	☐
172.18.214.169	DfltGrpPolicy	☑	☐
10.201.168.142	DfltGrpPolicy	☑	☐
10.201.174.145	DfltGrpPolicy	☑	☐
test	GroupPolicy2	☐	☑

Edit IPsec Site-to-site Tunnel Group: DefaultL2LGroup

Name: DefaultL2LGroup

IPsec Enabling

Group Policy Name: DfltGrpPolicy

(Following two fields are attributes of the group policy selected above.)

☑ Enable IKE v1 ☑ Enable IKE v2

IPsec Settings

Step 5 - select the IKE v2 settings and make necessary edits

IKE v1 Settings | IKE v2 Settings

Authentication

● Local Pre-shared Key:

○ Local Device Certificate: -- None --

Remote Peer Pre-shared Key:

Remote Peer Certificate Authentication: ☐ Allowed

IKE Peer ID Validation: Required

IKE Keepalive

○ Disable keepalives

● Monitor keepalives

Confidence Interval: 10 seconds

Retry Interval: 2 seconds

○ Headend will never initiate keepalive monitoring

Step 6

Step 7

Data Refreshed Successfully. 15 5/21/14 11:09:15 PM EDT

Dynamic ASA

```
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 *****
```

On the ASDM, you can use the standard wizard in order to set up the appropriate connection profile or you can simply add a new connection and follow the standard procedure.

Solution 2 - Create a User-Defined Tunnel-Group

This method requires slighly more configuration, but it allows for more granularity. Each peer can have its own separate policy and pre-shared key. However here it is important to change the ISAKMP ID on the dynamic peer so that it uses a name instead of an IP address. This allows the static ASA to match the incoming ISAKMP initialisation request to the right tunnel group and to use the right policies.

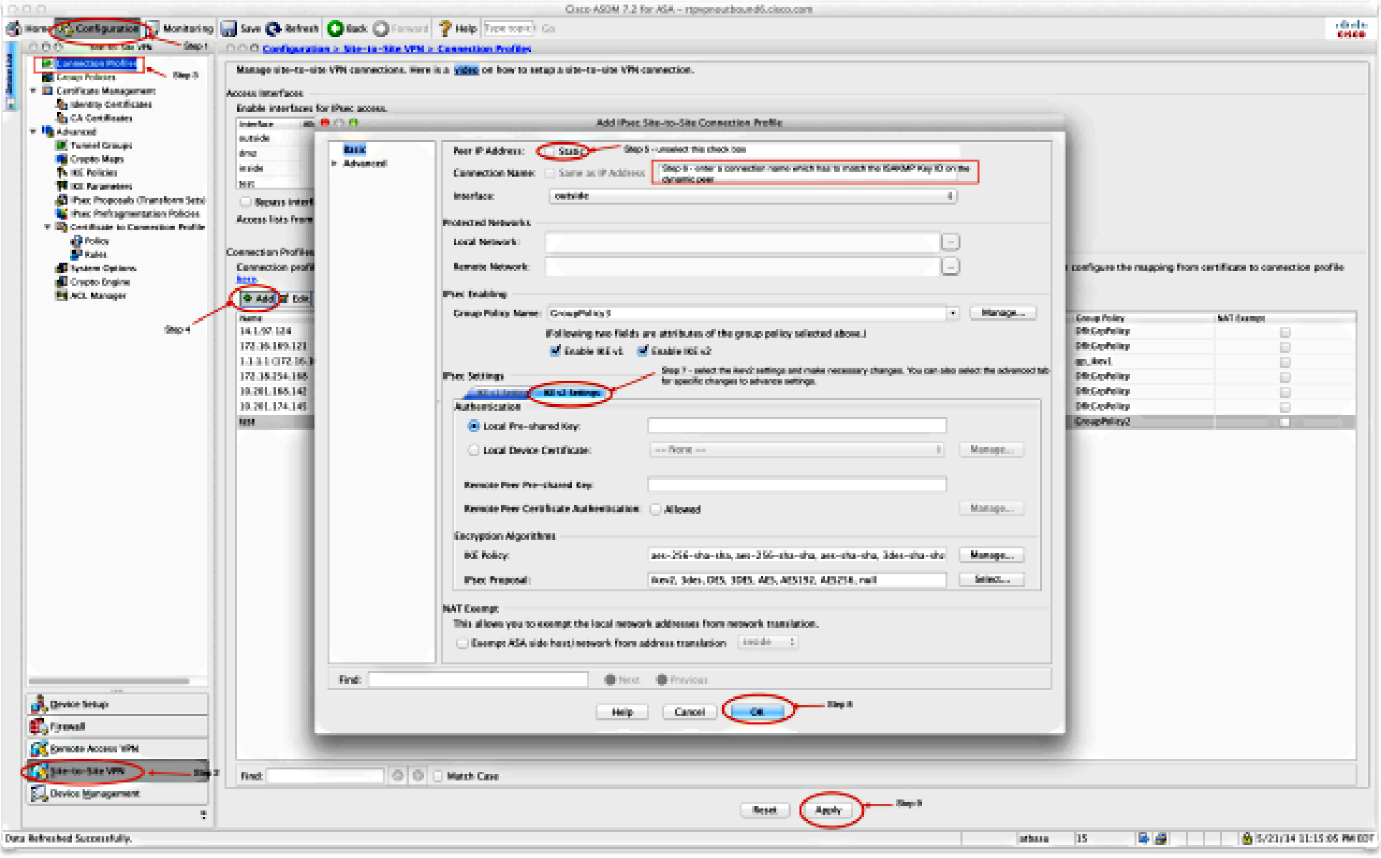
Static ASA Configuration

```
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_CRYPTO_MAP 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_CRYPTO_MAP 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_CRYPTO_MAP
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 *****
```

On the ASDM, the connection profile name is an IP address by default. So when you create it, you must change it in order to give it a name as shown in the screenshot here:



Cisco ASDM 7.2 for ASA

Configuration > Site-to-Site VPN > Connection Profiles

Manage site-to-site VPN connections. Here is a video on how to setup a site-to-site VPN connection.

Step 1 - Configuration

Step 2 - Site-to-Site VPN

Step 3 - Connection Profiles

Step 4 - Add

Add IPsec Site-to-Site Connection Profile

Peer IP Address: □ Static

Step 5 - unselect this check box

Connection Name: □ Same as IP Address

Step 6 - enter a connection name which has to match the ISAKMP Key ID on the dynamic peer

Interface: outside

Group Policy Name: GroupPolicy3

☑ Enable IKE v1 ☑ Enable IKE v2

Step 7 - select the ikev2 settings and make necessary changes. You can also select the advanced tab for specific changes to advance settings.

● Local Pre-shared Key:

○ Local Device Certificate: -- None --

Remote Peer Certificate Authentication: □ Allowed

IKE Policy: aes-256-sha-sha, aes-256-sha-sha, aes-sha-sha, 3des-sha-sha

IPsec Proposal: ikev2, 3des, DES, 3DES, AES, AES192, AES256, null

Step 8 - OK

Step 9 - Apply

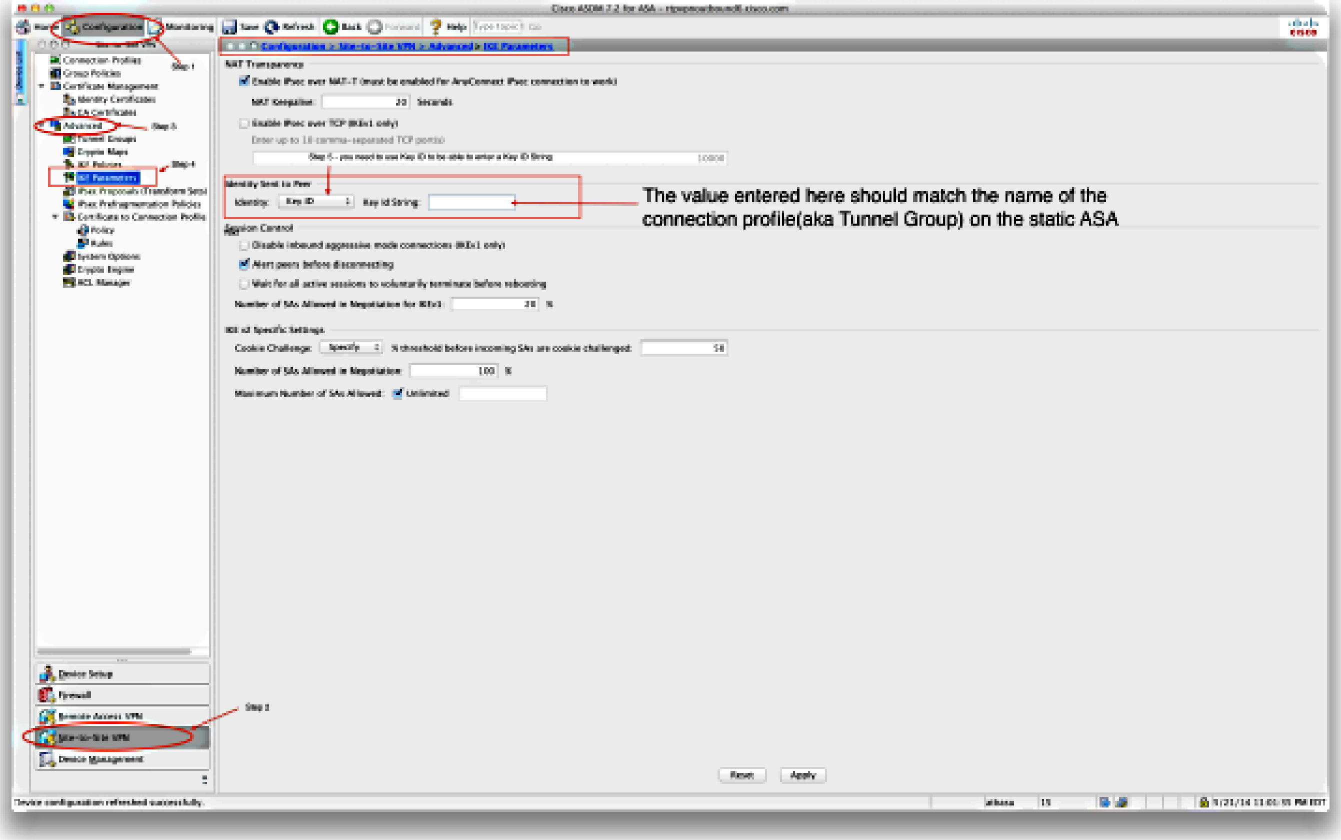
Dynamic ASA Configuration

The Dynamic ASA is configured almost the same way in both solutions with the addition of one command as shown here:

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

As described previously, by default the ASA uses the IP address of the interface that the VPN tunnel is mapped to as the ISAKMP key-ID. However in this case, the key-ID on the dynamic ASA is the same as the name of the tunnel-group on the Static ASA. So on every dynamic peer, the key-id will be different and a corresponding tunnel-group must be created on the Static ASA with the right name.

On the ASDM, this can be configured as shown in this screenshot:



Step 1

Step 2

Step 3

Step 4

Step 5 - you need to use Key ID to be able to enter a Key ID String

NAT Transparency

☑ Enable IPsec over NAT-T (must be enabled for AnyConnect IPsec connection to work)

NAT Keepalive: 20 Seconds

☐ Enable IPsec over TCP (IKEv1 only)

Identity Sent to Peer

Identity: Key ID Key Id String:

The value entered here should match the name of the connection profile(aka Tunnel Group) on the static ASA

Session Control

☐ Disable inbound aggressive mode connections (IKEv1 only)

☑ Alert peers before disconnecting

☐ Wait for all active sessions to voluntarily terminate before rebooting

Number of SAs Allowed in Negotiation for IKEv1: 20 %

IKE v2 Specific Settings

Cookie Challenge: Specify % threshold before incoming SAs are cookie challenged: 50

Number of SAs Allowed in Negotiation: 100 %

Maximum Number of SAs Allowed: ☑ Unlimited

Device configuration refreshed successfully.

Verify

Use this section in order to confirm that your configuration works properly.

On the Static ASA

Here is the result of the **show crypto IKEv2 sa det** command:

```
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
```

Here is the result of the **show crypto ipsec sa** command:

```
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
```

On the Dynamic ASA

Here is the result of the **show crypto IKEv2 sa detail** command:

```
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
```

Here is the result of the **show crypto ipsec sa** command:

```
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
```

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

> **Note**: Refer to Important Information on Debug Commands before you use **debug** commands.

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