

Dynamic to Dynamic IPsec Tunnel Configuration Example



Document ID: 118048

Contributed by Gustavo Medina, Wen Zhang, and Oleg Tipisov, Cisco

TAC Engineers.

Aug 11, 2014

Contents

Introduction

Prerequisites

Requirements

Components Used

Background Information

Configure

Real-Time Resolution for IPsec Tunnel Peer

Tunnel Destination Update with Embedded Event Manager (EEM)

Verify

Troubleshoot

Related Information

Introduction

This document describes how to build a LAN-to-LAN IPsec tunnel between Cisco routers when both ends have dynamic IP addresses but the Dynamic Domain Name System (DDNS) is configured.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Site-to-Site VPN with an IPsec tunnel and Generic Routing Encapsulation (GRE)
- IPsec Virtual Tunnel Interface (VTI)
- Dynamic DNS Support for Cisco IOS Software

Tip: Refer to the Configuring VPN section of the Cisco 3900 Series, 2900 Series, and 1900 Series Software Configuration Guide and the Configuring a Virtual Tunnel Interface with IP Security article for more information.

Components Used

The information in this document is based on a Cisco 2911 Integrated Services Router that runs Version 15.2(4)M6a.

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

When a LAN-to-LAN tunnel needs to be established, the IP address of both IPsec peers must be known. If one of the IP addresses is not known because it is dynamic, such as one obtained via DHCP, then an alternative is to use a dynamic crypto map. This works, but the tunnel can only be brought up by the peer that has the dynamic IP address since the other peer does not know where to find its peer.

For more information about dynamic to static, refer to [Configuring Router-to-Router Dynamic-to-Static IPsec with NAT](#).

Configure

Real-Time Resolution for IPsec Tunnel Peer

Cisco IOS® introduced a new feature in Version 12.3(4)T that allows the Fully Qualified Domain Name (FQDN) of the IPsec peer to be specified. When there is traffic that matches a crypto access list, Cisco IOS then resolves the FQDN and obtains the IP address of the peer. It then tries to bring up the tunnel.



Note: There is a limitation on this feature: DNS names resolution for remote IPsec peers will work only if they are used as an initiator. The first packet that is to be encrypted will trigger a DNS lookup; after the DNS lookup is complete, subsequent packets will trigger Internet Key Exchange (IKE). Real-time resolution will not work on the responder.

In order to address the limitation and be able to initiate the tunnel from each site, you will have a dynamic crypto map entry on both routers so you can map incoming IKE connections to the dynamic crypto. This is necessary since the static entry with the Real-time resolution feature does not work when it acts as a responder.

Router A

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
!
ip access-list extended crypto-ACL
  permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
  set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
  match address 140
  set peer example-b.cisco.com dynamic
```

```

    set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
    ip address dhcp
    crypto map secure_b

```

Router B

```

crypto isakmp policy 10
    encr aes
    authentication pre-share
    group 2
!
ip access-list extended crypto-ACL
    permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
    set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
    match address 140
    set peer example-a.cisco.com dynamic
    set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
    ip address dhcp
    crypto map secure_b

```

Note: Since you do not know which IP address the FQDN will be using, you need to use a wildcard Pre-Shared-Key: 0.0.0.0 0.0.0.0

Tunnel Destination Update with Embedded Event Manager (EEM)

You can also VTI in order to accomplish this. The basic configuration is shown here:

Router A

```

crypto isakmp policy 10
    encryption aes
    authentication pre-share
    group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
    set transform-set ESP-AES-SHA
!
interface Tunnell
    ip address 172.16.12.1 255.255.255.0
    tunnel source fastethernet0/0
    tunnel destination example-b.cisco.com
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile ipsec-profile

```

Router B

```
crypto isakmp policy 10
  encryption aes
  authentication pre-share
  group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
  set transform-set ESP-AES-SHA
!
interface Tunnell
  ip address 172.16.12.2 255.255.255.0
  tunnel source fastethernet0/0
  tunnel destination example-a.cisco.com
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-profile
```

Once the previous configuration is in place with an FQDN as the tunnel destination, the *show run* command shows the IP address instead of the name. This is because the resolution happens just once:

```
RouterA(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnell
  ip address 172.16.12.1 255.255.255.250
  tunnel source fastethernet0/0
  tunnel destination 209.165.201.1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-profile
end
```

```
RouterB(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnell
  ip address 172.16.12.2 255.255.255.250
  tunnel source fastethernet0/0
  tunnel destination 209.165.200.225
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-profile
end
```

A workaround for this is to configure an applet in order to resolve the tunnel destination every minute:

Router A

```
event manager applet change-tunnel-dest
  event timer cron name TAC cron-entry "* * * * *"
  action 1.0 cli command "enable"
  action 1.1 cli command "configure terminal"
  action 1.2 cli command "interface tunnell"
  action 1.3 cli command "tunnel destination example-b.cisco.com"
```

Router B

```

event manager applet change-tunnel-dest
  event timer cron name TAC cron-entry "* * * * *"
  action 1.0 cli command "enable"
  action 1.1 cli command "configure terminal"
  action 1.2 cli command "interface tunnell"
  action 1.3 cli command "tunnel destination example-a.cisco.com"

```

Verify

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

```
RouterA(config)#do show ip int brie
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	209.165.200.225	YES	NVRAM	up	up
FastEthernet0/1	192.168.10.1	YES	NVRAM	up	up
Tunnell	172.16.12.1	YES	manual	up	up

```
RouterB(config)#do show ip int brie
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	209.165.201.1	YES	TFTP	up	up
FastEthernet0/1	192.168.20.1	YES	manual	up	up
Tunnell	172.16.12.2	YES	manual	up	up

```
RouterA(config)#do show cry isa sa
```

dst	src	state	conn-id	slot	status
209.165.200.225	209.165.201.1	QM_IDLE	2	0	ACTIVE

```
RouterB(config)#do show cry isa sa
```

dst	src	state	conn-id	slot	status
209.165.200.225	209.165.201.1	QM_IDLE	1002	0	ACTIVE

```
RouterA(config)#do show cry ipsec sa
```

```
interface: Tunnell
```

```
  Crypto map tag: Tunnell-head-0, local addr 209.165.200.225
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer 209.165.201.1 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
```

```
  #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
```

```
  #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.: 209.165.200.225, remote crypto endpt.: 209.165.201.1
```

```
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
```

```
current outbound spi: 0x8F1592D2(2400555730)
```

```
inbound esp sas:
```

```
  spi: 0xF7B373C0(4155732928)
```

```
  transform: esp-3des esp-sha-hmac ,
```

```
  in use settings = {Tunnel, }
```

```
  conn id: 2002, flow_id: AIM-VPN/BPII-PLUS:2, crypto map: Tunnell-head-0
```

```
  sa timing: remaining key lifetime (k/sec): (4501866/3033)
```

```
  IV size: 8 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE
```

```
inbound ah sas:
```

inbound pcp sas:

outbound esp sas:

```
spi: 0x8F1592D2(2400555730)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2001, flow_id: AIM-VPN/BPII-PLUS:1, crypto map: Tunnel1-head-0
  sa timing: remaining key lifetime (k/sec): (4501866/3032)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

RouterB(config)#do show cry ipsec sa

interface: Tunnel1

Crypto map tag: Tunnel1-head-0, local addr 209.165.201.1

protected vrf: (none)

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 209.165.200.225 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#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.: 209.165.201.1, remote crypto endpt.: 209.165.200.225

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xF7B373C0(4155732928)

PFS (Y/N): N, DH group: none

inbound esp sas:

```
spi: 0x8F1592D2(2400555730)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: Tunnel1-head-0
  sa timing: remaining key lifetime (k/sec): (4424128/3016)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xF7B373C0(4155732928)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: Tunnel1-head-0
  sa timing: remaining key lifetime (k/sec): (4424128/3016)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

After you change the DNS record for b.cisco.com on the DNS server from 209.165.201.1 to 209.165.202.129, the EEM will make cause Router A to realize and the tunnel will reestablish with the correct new IP address.

```
RouterB(config)#do show ip int brief
Interface          IP-Address      OK?  Method  Status  Protocol
FastEthernet0/0    209.165.202.129 YES   TFTP    up      up
FastEthernet0/1    192.168.20.1    YES   manual  up      up
Tunnell            172.16.12.2     YES   manual  up      up
```

```
RouterA(config-if)#do show run int tunn1
Building configuration...
```

```
Current configuration : 192 bytes
!
interface Tunnell
 ip address 172.16.12.1 255.255.255.252
 tunnel source fastethernet0/0
 tunnel destination 209.165.202.129
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile
end
```

```
Router1841A#show cry isa sa
dst          src          state          conn-id slot status
209.165.200.225 209.165.202.129 QM_IDLE          3      0 ACTIVE
```

Troubleshoot

You can refer to IOS IPsec and IKE debugs – IKEv1 Main Mode Troubleshooting for common IKE/IPsec troubleshooting.

Related Information

- *Real-Time Resolution for IPsec Tunnel Peer*
- *Technical Support & Documentation – Cisco Systems*