동적 대 동적 IPsec 터널 컨피그레이션 예

목차

소개

이 문서에서는 양쪽 끝에 동적 IP 주소가 있지만 DDNS(Dynamic Domain Name System)가 구성된 경우 Cisco 라우터 간에 LAN-to-LAN IPsec 터널을 구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IPSec 터널 및 GRE(Generic Routing Encapsulation)를 사용하는 Site-to-Site VPN
- IPsec VTI(Virtual Tunnel Interface)
- Cisco IOS 소프트웨어에 대한 동적 DNS 지원

팁: 자세한 내용은 Cisco 3900 Series, 2900 Series 및 1900 Series 소프트웨어 구성 가이드 및 IP 보안으로 가상 터널 인터페이스 구성 문서의 VPN 구성 섹션을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 버전 15.2(4)M6a를 실행하는 Cisco 2911 Integrated Services Router를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

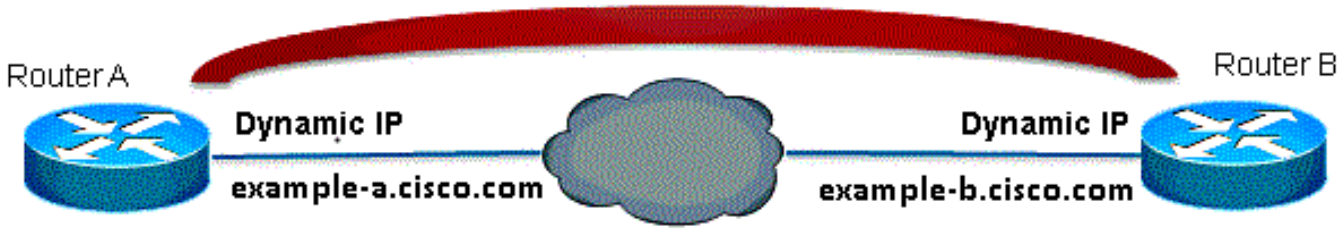
LAN-to-LAN 터널을 설정해야 하는 경우 두 IPSec 피어의 IP 주소를 모두 알고 있어야 합니다. DHCP를 통해 얻은 것과 같이 IP 주소 중 하나가 동적 주소이기 때문에 알 수 없는 경우 동적 암호화 맵을 사용하는 것이 대체 방법입니다. 이는 작동하지만 다른 피어가 피어를 찾을 위치를 모르기 때문에 동적 IP 주소가 있는 피어가 터널을 생성할 수만 있습니다.

동적에서 정적으로 이동하는 방법에 대한 자세한 내용은 NAT를 사용하여 라우터 간 동적-고정 IPSec 구성을 참조하십시오.

구성

IPsec 터널 피어에 대한 실시간 확인

Cisco IOS®는 IPSec 피어의 FQDN(Fully Qualified Domain Name)을 지정할 수 있는 버전 12.3(4)T에 새로운 기능을 도입했습니다. 암호화 액세스 목록과 일치하는 트래픽이 있는 경우 Cisco IOS는 FQDN을 확인하고 피어의 IP 주소를 얻습니다. 그런 다음 터널을 실행하려고 시도합니다.



참고: 이 기능에는 제한이 있습니다. 원격 IPsec 피어에 대한 DNS 이름 확인은 개시자로 사용되는 경우에만 작동합니다. 암호화할 첫 번째 패킷은 DNS 조회를 트리거합니다. DNS 조회가 완료되면 후속 패킷은 IKE(Internet Key Exchange)를 트리거합니다. 응답자에서 실시간 확인이 작동하지 않습니다.

제한 사항을 해결하고 각 사이트에서 터널을 시작할 수 있도록 두 라우터에 동적 암호화 맵 항목이 있으므로 수신 IKE 연결을 동적 암호화에 매핑할 수 있습니다. 실시간 해결 기능이 있는 정적 엔트리는 responder 역할을 할 때 작동하지 않으므로 이 작업이 필요합니다.

라우터 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
```

라우터 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
```

참고: FQDN에서 사용할 IP 주소를 모르므로 와일드카드 사전 공유 키를 사용해야 합니다. 0.0.0.0 0.0.0.0

EEM(Embedded Event Manager)을 통한 터널 대상 업데이트

이를 위해 VTI도 사용할 수 있습니다. 기본 컨피그레이션은 다음과 같습니다.

라우터 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 Tunnel1
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
```

라우터 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 Tunnel1
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
```

이전 컨피그레이션이 터널 대상으로 FQDN이 있는 경우 **show run** 명령은 이름 대신 IP 주소를 표시

합니다. 이는 해결 방법이 한 번만 이루어지기 때문입니다.

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

Current configuration : 130 bytes
!
interface Tunnel1
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 Tunnel1
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
```

이에 대한 해결 방법은 분당 터널 대상을 확인하기 위해 애플릿을 구성하는 것입니다.

라우터 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 tunnel1"
action 1.3 cli command "tunnel destination example-b.cisco.com"
```

라우터 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 tunnel1"
action 1.3 cli command "tunnel destination example-a.cisco.com"
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

```
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
Tunnel1 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
Tunnel1 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: Tunnel1
Crypto map tag: Tunnel1-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: Tunnel1-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:
```

DNS 서버에서 b.cisco.com의 DNS 레코드를 209.165.201.1에서 209.165.202.129으로 변경하면 EEM에서 라우터 A를 인식하게 되고 올바른 새 IP 주소로 터널이 다시 설정됩니다.

```
RouterB(config)#do show ip int brie
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
Tunnel1 172.16.12.2 YES manual up up
```

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

Current configuration : 192 bytes
!
interface Tunnel1
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
```

문제 해결

일반적인 IKE/IPsec 트러블슈팅에 대해서는 IOS IPSec 및 IKE 디버깅 - IKEv1 기본 모드 트러블슈팅을 참조할 수 있습니다.

관련 정보

- IPsec 터널 피어에 대한 실시간 확인
- 기술 지원 및 문서 – Cisco Systems