ダイナミックからダイナミックへの IPSec トンネルの設定例

目次

概要

このドキュメントでは、シスコ ルータ間の LAN 間 IPsec トンネルを構築する場合に、両端にダイナミック IP アドレスがあるが、ダイナミック ドメイン ネーム システム（DDNS）が設定されているときの構築方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IPSec トンネルおよび Generic Routing Encapsulation（GRE）を使用したサイト間 VPN
- IPSec Virtual Tunnel Interface（VTI）
- Cisco IOS ソフトウェアのためのダイナミッ ク DNS サポート

ヒント： 詳細については、『Cisco 3900 シリーズ、2900 シリーズ、および 1900 シリーズのソフトウェア コンフィギュレーション ガイド』の「VPN の設定」の項、および「IP セキュリティを使用した仮想トンネル インターフェイスの設定」という記事を参照してください。

使用するコンポーネント

このドキュメントの情報は、バージョン 15.2(4)M6a が稼働する Cisco 2911 サービス統合型ルータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

LAN 間 トンネルを確立する必要がある場合、両方の IPSec ピアの IP アドレスを認識している必要があります。 IP アドレスの 1 つがダイナミック IP アドレス（DHCP によって取得される IP アドレスなど）のために不明な場合、代替手段としてダイナミック暗号マップを使用します。 このマップは機能しますが、トンネルはダイナミック IP アドレスを持つピアによってのみ確立できます。これは、そのピアのアドレスをもう一方のピアが認識していないためです。

「ダイナミックからスタティック」に関する詳細は、「NAT を使用したルータ間のダイナミックからスタティックへの IPSec の設定」を参照してください。

設定

IPsec トンネル ピアの Real-Time Resolution

Cisco IOS® バージョン 12.3(4)T で、IPSec ピアの完全修飾ドメイン名（FQDN）を指定できる機能が新しく導入されました。 Cisco IOS では、暗号アクセス リストと一致するトラフィックがある場合、その FQDN を解決してピアの IP アドレスを取得します。 その後、トンネルの確立を試みます。

注: この機能には次の制限があります。 DNS によるリモート IPsec ピアの名前解決が機能

するのは、ピアを発信側として使用する場合だけです。 暗号化されることになっている最初のパケットによって、DNS ルックアップがトリガーされます。 DNS ルックアップが完了すると、後続のパケットによってインターネット キー エクスチェンジ（IKE）がトリガーされます。 リアルタイム解決は、応答側では機能しません。

この制限に対処して各サイトからトンネルを開始できるようにするため、両方のルータにダイナミック暗号マップ エントリを保持させます。これにより、着信 IKE 接続をダイナミック暗号にマッピングできるようになります。 これが必要なのは、リアルタイム解決機能が備わったスタティック エントリは、応答側として動作するときには機能しないためです。

ルータ 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
```

ルータ 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
```

> **注:** FQDN で使用される IP アドレスが不明なため、ワイルドカード事前共有キーの 0.0.0.0 0.0.0.0 を使用する必要があります。

Embedded Event Manager (EEM; 組み込みイベント マネージャ) を使用したトンネルの宛先の更新

この実行には VTI を使用することもできます。 この基本設定を次に示します。

ルータ 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
```

ルータ 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
```

前の設定がトンネルの宛先としてある 1 つの FQDN を使用して配置されると、下に示すように **show run** コマンドではその名前ではなく、IP アドレスが表示されます。 これは、解決が 1 度だけ実行されるためです。

```
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
```

これを回避するには、次に示すようにトンネルの宛先を 1 分ごとに解決するためのアプレットを設定します。

ルータ 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"
```

ルータ 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"
```

確認

このセクションでは、設定が正常に機能していることを確認します。

```
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 サーバ上にある b.cisco.com に対する DNS レコードを 209.165.201.1 から 209.165.202.129 に変更すると、EEM が Router A に認知させ、トンネルが新しい正しい IP アドレスで再確立されます。

```
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
```

トラブルシューティング

一般的な IKE/IPsec のトラブルシューティングについては、「IOS IPSec および IKE のデバッグ：IKEv1 メイン モードのトラブルシューティング」を参照してください。

関連情報

- IPsec トンネル ピアの Real-Time Resolution
- テクニカルサポートとドキュメント - Cisco Systems