动态对动态IPSec隧道配置示例

目录

简介

本文描述如何构建在Cisco路由器之间的一个LAN到LAN IPSec隧道，当两端有动态IP地址时，但是动态域名系统(DDNS)配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 与IPSec隧道和通用路由封装(GRE)的站点到站点VPN
- IPsec虚拟隧道接口(VTI)
- Cisco IOS软件的动态DNS支持

提示：参考Cisco 3900系列， 2900系列和1900系列软件配置指南和配置与IP安全条款的一个虚拟隧道接口的配置的VPN部分欲知更多信息。

使用的组件

运行版本15.2(4)M6a的本文档中的信息根据Cisco 2911集成业务路由器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

当LAN-to-LAN隧道需要设立时，必须知道两IPSec对等体的IP地址。如果其中一个IP地址不知道，因为是动态，例如通过DHCP，则替代方案获取的一个是使用动态加密映射。这工作，但是通道可能由有动态IP地址的对等体只启动，因为另一对等体在哪里不知道找到其对等体。

关于动态的更多信息对静态，参考配置路由器到路由器动态到静态使用NAT的IPSec。

配置

IPSec隧道对等体的实时解决方法

Cisco IOS在允许IPSec对等体完全合格的域名(FQDN)将指定的版本12.3(4)T介绍新特性。当有然后匹配一crypto访问列表的流量时， Cicso IOS解决FQDN并且获取对等体的IP地址。 它然后设法启动通道。

> **Note**:有在此功能的一个限制： 只有当他们使用作为发起者，远程IPSec对等体的DNS名解决方法将工作。将加密的第一数据包将触发DNS查找;在DNS查找完成后，后续信息包将触发Internet Key Exchange (IKE)。 实时解决方法在响应方不会工作。

为了寻址限制和能发起从每个站点的通道，您将有在两路由器的一个动态加密映射条目，因此您能映射对动态crypto的流入IKE连接。这是必要的，因为与实时解决方法功能的静态条目不工作，当作为响应方。

路由器 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
```

路由器 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: 因为您不知道哪个IP地址FQDN使用，您需要使用通配符预共享密钥：0.0.0.0 0.0.0.0

与嵌入式活动管理器(EEM)的隧道目的地更新

您能VTI为了也完成此。基本配置显示此处：

路由器 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
```

路由器 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
```

一旦先前配置是到位与FQDN作为隧道目的地， **show run命令**显示IP地址而不是名称。这是因为解决方法一次发生：

```
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
```

此的一应急方案是配置applet为了每分钟解决隧道目的地：

路由器 A

```
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
```

路由器 B

```
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
```

验证

使用本部分可确认配置能否正常运行。

```
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:
```

在您更改b.cisco.com的DNS记录在从209.165.201.1的DNS服务器到209.165.202.129后， EEM将使原因路由器A认识到，并且通道将重建用正确新建的IP地址。

```
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
```

故障排除

能参考IOS IPSec和IKE调试- IKEv1主模式排除故障为普通的IKE/IPsec故障排除的您。

相关信息

- IPSec隧道对等体的实时解决方法
- 技术支持和文档 - Cisco Systems