IOS VPN路由器：添加或删除在L2L VPN隧道配置示例的网络

目录

简介

本文如何提供一配置示例为添加或删除在一个现有LAN对LAN (L2L) VPN通道的网络。

先决条件

要求

保证您正确地配置您的当前L2L IPSec VPN通道，在您尝试此配置前。

使用的组件

本文档中的信息根据两个Cisco IOS路由器该运行软件版本12.4(15)T1。

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

当前有在总部(HQ)办公室和分支机构(BO)之间的一个L2L VPN通道。总部添加了销售团队将使用的新的网络。此团队需要对位于BO办公室的资源的访问。手头的任务是添加每新的网络到已经现有L2L VPN通道。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文在此部分使用描述的配置。这些配置包括L2L运行在总部172.16.10.0网络和BO办公室的10.10.10.0网络之间的VPN。在粗体文本显示的输出显示必需的配置集成总部的新的网络192.168.10.0到有10.10.10.0的同一个VPN通道象目的地网络。

HQ路由器

```
HQ-Router#show running-config Building configuration...
Current configuration : 1439 bytes ! version 12.4
service timestamps debug uptime service timestamps log
uptime no service password-encryption ! hostname HQ-
Router ! !--- Output suppressed. ! crypto isakmp policy
1 hash md5 authentication pre-share crypto isakmp key
cisco123 address 209.165.200.225 ! ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac ! crypto map
rtp 1 ipsec-isakmp set peer 209.165.200.225 set
transform-set rtpset match address 115 ! interface
Ethernet0 ip address 172.16.10.1 255.255.255.0 ip nat
inside ! interface Ethernet1 ip address 209.165.201.2
255.255.255.224 ip nat outside crypto map rtp !
interface Ethernet2 ip address 192.168.10.1
255.255.255.0 ip nat inside ! interface Serial0 no ip
address shutdown no fair-queue ! interface Serial1 no ip
address shutdown ! ip nat inside source route-map nonat
interface Ethernet1 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.201.1 ! !--- Output suppressed.
access-list 110 deny ip 172.16.10.0 0.0.0.255 10.10.10.0
0.0.0.255 access-list 110 permit ip 172.16.10.0
0.0.0.255 any ! !--- Add this ACL entry to include
192.168.10.0 !--- network with the nat-exemption rule.
access-list 110 deny ip 192.168.10.0 0.0.0.255
10.10.10.0 0.0.0.255 access-list 110 permit ip
192.168.10.0 0.0.0.255 any access-list 115 permit ip
172.16.10.0 0.0.0.255 10.10.10.0 0.0.0.255 ! !--- Add
this ACL entry to include 192.168.10.0 !--- network into
the crypto map. access-list 115 permit ip 192.168.10.0
0.0.0.255 10.10.10.0 0.0.0.255 route-map nonat permit 10
match ip address 110 ! !--- Output suppressed. end
```

BO路由器

```
BO-Router#show running-config Building configuration...
Current configuration : 2836 bytes ! version 12.4
service timestamps debug datetime msec service
```

```
timestamps log datetime msec no service password-
encryption ! hostname BO-Router ! !--- Output
suppressed. ! crypto isakmp policy 1 hash md5
authentication pre-share crypto isakmp key cisco123
address 209.165.201.2 ! ! crypto ipsec transform-set
rtpset esp-des esp-md5-hmac ! crypto map rtp 1 ipsec-
isakmp set peer 209.165.201.2 set transform-set rtpset
match address 115 ! !--- Output suppressed. interface
FastEthernet0/0 ip address 209.165.200.225
255.255.255.224 ip nat outside ip virtual-reassembly
duplex auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.10.10.1 255.255.255.0 ip
nat inside ip virtual-reassembly duplex auto speed auto
! ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 ! !--- Output
suppressed. ! ip http server no ip http secure-server ip
nat inside source route-map nonat interface
FastEthernet0/0 overload ! !--- Add this ACL entry to
include 192.168.10.0 !--- network with the nat-exemption
rule. access-list 110 deny ip 10.10.10.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 access-list
110 permit ip 10.10.10.0 0.0.0.255 any access-list 115
permit ip 10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 !
!--- Add this ACL entry to include 192.168.10.0 !---
network into the crypto map. access-list 115 permit ip
10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255 ! route-map
nonat permit 10 match ip address 110 ! !--- Output
suppressed. ! end
```

从IPSec隧道删除网络

完成在此部分描述的步骤为了从IPSec隧道配置删除网络。注意网络192.168.10.0/24从HQ路由器配置删除。

1. 请使用此命令为了切断IPSec连接：`HQ-Router#clear crypto sa`
2. 请使用此命令为了清除ISAKMPSecurity关联(SAS) ：`HQ-Router#clear crypto isakmp`
3. 请使用此命令为了删除IPSec隧道的触发流量的ACL ：`HQ-Router(config)#no access-list 115 permit ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255`
4. 请使用此命令为了删除192.168.10.0网络的nat豁免ACL语句：`HQ-Router(config)#no access-list 110 deny ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255`
5. 请使用此命令为了清除NAT转换：`HQ-Router#clear ip nat translation *`
6. 请使用这些命令为了删除和重新应用在接口的加密映射保证当前加密配置生效：`HQ-Router(config)#int ethernet 1 HQ-Router(config-if)#no crypto map rtp *May 25 10:35:12.153: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF HQ-Router(config-if)#crypto map rtp *May 25 10:36:09.305: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON` **注意：** 删除加密映射从接口撕毁所有现有VPN连接关联与该加密映射。在执行此前，请确保您需要了需要的停工期并且相应地遵从您的组织更改控制控制政策。
7. 请使用**write memory命令**为了保存活动配置到闪存。
8. 完成在VPN通道(BO路由器)的另一端的这些步骤为了删除配置。
9. 发起IPSec隧道并且验证连接。

验证

使用本部分可确认配置能否正常运行。

请使用此ping顺序为了保证新的网络能通过VPN通道传递数据：

```
HQ-Router#clear crypto sa HQ-Router# HQ-Router#ping 10.10.10.1 source 172.16.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 172.16.10.1 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms HQ-Router#ping 10.10.10.1 source 192.168.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.10.1 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms HQ-Router#ping 10.10.10.1 source 192.168.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.10.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

show crypto ipsec sa

```
HQ-Router#show crypto ipsec sa interface: Ethernet1
Crypto map tag: rtp, local addr. 209.165.201.2 local
ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 9, #pkts encrypt:
9, #pkts digest 9 #pkts decaps: 9, #pkts decrypt: 9,
#pkts verify 9 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: FB52B5AB
inbound esp sas: spi: 0x612332E(101856046) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2002, flow_id: 3, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607998/3209) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xFB52B5AB(4216501675) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2003,
flow_id: 4, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607998/3200) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
local ident (addr/mask/prot/port):
(172.16.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt:
4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4,
#pkts verify 4 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: C9E9F490
inbound esp sas: spi: 0x1291F1D3(311554515) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2000, flow_id: 1, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607999/3182) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xC9E9F490(3387552912) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2001,
flow_id: 2, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607999/3182) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
```

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输

出的分析。

故障排除

使用本部分可排除配置的故障。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。
- **debug crypto engine** — 显示加密会话。

相关信息

- IP 安全 (IPsec) 加密简介
- IPsec 协商/IKE 协议支持页
- 配置 IPsec 路由器动态局域网到局域网对等体和 VPN 客户端
- 技术支持和文档 - Cisco Systems