IOS VPN (路由器) ：向现有 L2L VPN 添加新 L2L 隧道或远程访问

目录

简介

本文档提供向 IOS 路由器中已经存在的 L2L VPN 配置中添加新的 L2L VPN 隧道或远程访问 VPN 所需的步骤。

先决条件

要求

保证您正确地配置当前是可操作的L2L IPSec VPN通道，在您尝试此配置前。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 12.4 和 12.2 的两个 IOS 路由器
- 运行软件版本 8.0 的一台 Cisco 自适应安全设备 (ASA)

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。

网络图

本文档使用以下网络设置：

以下输出是 HQ（中心）路由器和分支机构 1 (BO1) ASA 的当前运行配置。在此配置中，在 HQ 和 BO1 ASA 之间配有一条 IPSec L2L 隧道。

当前 HQ（中心）路由器配置

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
!
!
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
```

```
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

BO1 ASA 配置

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list 100 extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list nonat extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
```

```
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
```

```
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

背景信息

当前，在 HQ 办公室和 BO1 办公室之间设有一条现有的 L2L 隧道。您的公司最近新开了一个办公室 (BO2)。这个新办公室需要连接到位于 HQ 办公室的本地资源。此外，还要求允许员工在家工作并且在远程安全地访问位于内部网络的资源。在本示例中，配置一条新的 VPN 隧道以及位于 HQ 办公室的远程访问 VPN 服务器。

向配置中添加另外一条 L2L 隧道

以下是此配置的网络图：

逐步指导

本部分提供必须在中心 HQ 路由器上执行的过程。

完成这些步骤：

1. 创建以下用于加密映射的新访问列表以定义相关数据流：`HQ_HUB(config)#ip access-list extended VPN_BO2`
   `HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255`
   `HQ_HUB(config-ext-nacl)#exit`
   警告： 要实现通信，隧道的另一端必须有与此特定网络的访问控制列表 (ACL) 条目相反的条目。
2. 将以下条目添加到 no nat 语句以免除在这些网络之间的 NAT：`HQ_HUB(config)#ip access-list extended NAT_Exempt`
   `HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255`
   `HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any`
   将以下 ACL 添加到现有路由映射 nonat 中：`HQ_HUB(config)#route-map nonat permit 10`
   `HQ_HUB(config-route-map)#match ip address NAT_Exempt`
   `HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload`
   警告： 要实现通信，隧道的另一端必须有与此特定网络的 ACL 条目相反的条目。
3. 如下所示在阶段 1 配置中指定对等体地址：`HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2`
   注意： 隧道两端的预共享密钥必须完全一致。
4. 为新的 VPN 隧道创建加密映射配置。请使用在第一种 VPN 配置中使用的同一转换集，因为所有第 2 阶段的设置都是相同的。`HQ_HUB(config)#crypto map map1 10 ipsec-isakmp`
   `HQ_HUB(config-crypto-map)#set peer 192.168.12.2`
   `HQ_HUB(config-crypto-map)#set transform-set newset`
   `HQ_HUB(config-crypto-map)#match address VPN_BO2`
5. 既然您配置了新隧道，您必须通过隧道发送相关数据流才能启用该隧道。要执行此操作，请发出扩展 ping 命令对远程隧道内部网络上的一台主机执行 ping 操作。在本示例中，对隧道另一端地址为 10.20.20.16 的工作站执行 ping 操作。这将启用 HQ 与 BO2 之间的隧道。此时，有两条隧道连接到总部。如果您无法访问隧道后方的系统，请参阅最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案以查找关于使用 management-access 的备用解决方案。

配置示例

HUB_HQ -添加了一个新的L2L VPN隧道配置

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
```

```
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255



!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

BO2 L2L VPN 隧道配置

```
BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
```

```
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match address 100
!
!
!
!
interface Ethernet0
 ip address 10.20.20.10 255.255.255.0
 ip nat inside
!

!
interface Ethernet1
 ip address 192.168.12.2 255.255.255.0
 ip nat outside
 crypto map map1
!
interface Serial0
 no ip address
 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 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0
0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

向配置中添加一个远程访问 VPN

以下是此配置的网络图：

在本示例中，使用了名为**分割隧道**的功能。此功能允许远程访问 IPSec 客户端有条件地以加密形式通过 IPsec 隧道定向数据包，或者以明文形式将数据包定向到网络接口。启用分割隧道时，在 IPSec 隧道另一端通往目标的数据包不必加密、通过隧道发送、解密，然后路由到最终目标。这一

概念将分割隧道策略应用到指定的网络。默认值是以隧道传输所有数据流。要设置分割隧道策略，请指定可在其中说明要访问 Internet 的数据流的 ACL。

逐步指导

本部分提供添加远程访问功能并允许远程用户访问所有站点所需的过程。

完成这些步骤：

1. 创建一个 IP 地址池以用于通过 VPN 隧道连接的客户端。此外，创建一个基本用户，以便在配置完成后访问 VPN。`HQ_HUB(config)#ip local pool ippool 10.10.120.10 10.10.120.50`
   `HQ_HUB(config)#username vpnuser password 0 vpnuser123`
2. 使特定的数据流免于进行 NAT 处理。`HQ_HUB(config)#ip access-list extended NAT_Exempt`
   ```
   HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
   HQ_HUB(config-ext-nacl)#exit
   ```
   将以下 ACL 添加到现有路由映射 nonat 中：`HQ_HUB(config)#route-map nonat permit 10`
   ```
   HQ_HUB(config-route-map)#match ip address NAT_Exempt
   HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
   ```
   请注意，在本示例中免除了 VPN 隧道之间的 NAT 通信。
3. 允许现有 L2L 隧道与远程访问 VPN 用户之间的通信。`HQ_HUB(config)#ip access-list extended VPN_BO1`
   ```
   HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#exit
   HQ_HUB(config)#ip access-list extended VPN_BO2
   HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#exit
   ```
   此操作使远程访问用户能够与指定的隧道之后的网络进行通信。**警告：** 要实现通信，隧道的另一端必须有与此特定网络的 ACL 条目相反的条目。
4. **配置分割隧道**要对 VPN 连接启用分割隧道，请确保在路由器上配置 ACL。在本示例中，**access-list split_tunnel** 命令与用于分割隧道的组关联，并且该隧道通向 10.10.10.0 /24、10.20.20.0/24 和 172.16.1.0/24 网络。数据流在未加密的情况下流向 ACL 分割隧道以外的设备（例如 Internet）。`HQ_HUB(config)#ip access-list extended split_tunnel`
   ```
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#exit
   ```
5. 为 VPN 客户端配置本地身份验证、授权和客户端配置信息，例如 wins、dns、相关数据流 acl 和 ip 池。`HQ_HUB(config)#aaa new-model`
   ```
   HQ_HUB(config)#aaa authentication login userauthen local
   HQ_HUB(config)#aaa authorization network groupauthor local
   HQ_HUB(config)#crypto isakmp client configuration group vpngroup
   HQ_HUB(config-isakmp-group)#key cisco123
   HQ_HUB(config-isakmp-group)#dns 10.10.10.10
   HQ_HUB(config-isakmp-group)#wins 10.10.10.20
   HQ_HUB(config-isakmp-group)#domain cisco.com
   HQ_HUB(config-isakmp-group)#pool ippool
   HQ_HUB(config-isakmp-group)#acl split_tunnel
   HQ_HUB(config-isakmp-group)#exit
   ```
6. 配置创建 VPN 隧道所需的动态映射和加密映射信息。`HQ_HUB(config)#crypto isakmp profile vpnclient`
   ```
   HQ_HUB(config-isakmp-group)#match identity group vpngroup
   HQ_HUB(config-isakmp-group)#client authentication list userauthen
   HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthor
   ```

```
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

配置示例

配置示例 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl split_tunnel
crypto isakmp profile vpnclient
   match identity group vpngroup
   client authentication list userauthen
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
hmac
```

```
!
crypto dynamic-map dynmap 10
 set transform-set remote-set
 set isakmp-profile vpnclient
 reverse-route
!
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
```

```
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

验证

使用本部分可确认配置能否正常运行。

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。

- **ping** — 此命令可启动 L2L VPN 隧道，如下所示。

故障排除

有关排除配置故障时可用的信息，请参阅以下文档：

- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- IP安全故障排除-了解和使用debug命令

提示： 当清除安全关联且这无法解决 IPsec VPN 问题时，请删除并重新应用相关加密映射，以解决各种问题。

警告： 如果从接口删除加密映射，则会关闭与该加密映射关联的所有 IPSec 隧道。请小心按照以下步骤操作，在继续之前，请考虑您组织的更改控制策略。

示例

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

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