在两个有叠加专用网络的IOS路由器之间的IPSec配置示例

目录

简介

本文描述如何配置在站点至站点IPSec VPN的Cisco IOS路由器与叠加专用网络网络地址在VPN网关背后。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco IOS运行软件版本12.4的3640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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

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：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

Private_LAN1和Private_LAN2有IP子网192.168.1.0/24。这模拟在IPSec隧道的每侧的后重迭的地址空间。

在本例中， Site_A路由器进行一个双向转换，以便两个专用LAN能在IPSec隧道通信。转换意味着Private_LAN1 “看到” Private_LAN2作为10.10.10.0/24通过IPSec隧道，并且Private_LAN2 “看到” Private_LAN1作为10.5.5.0/24通过IPSec隧道。

配置

本文档使用以下配置：

- Site_A路由器SDM配置
- Site_A路由器CLI配置
- Site_B路由器配置

Site_A路由器SDM配置

注意： 本文假设，路由器配置与基本设置类似接口配置使用SDM欲知更多信息，等等参考的基本路由器配置。

NAT 配置

完成这些步骤为了使用NAT配置在Site_A路由器的SDM ：

1. 选择**配置> NAT > Edit NAT配置**，并且点击**指定NAT接口**为了定义委托和不信任的接口如显示。
2. 单击 **Ok**。
3. 单击**添加**为了配置NAT转换从里向外方向如显示。
4. 单击 **Ok**。
5. 再次，请单击**添加**为了配置NAT转换从外向里方向如显示。
6. 单击 **Ok**。**注意：** 这是等同CLI配置：

VPN 配置

完成这些步骤为了使用VPN配置在Site_A路由器的SDM ：

1. 如此镜像所显示，选择**配置> VPN > VPN组件>IKE > IKE策略>Add**为了定义IKE策略。
2. 单击 **Ok**。**注意：** 这是等同CLI配置：
3. 选择**配置> VPN > VPN组件>IKE >预先共享密钥>Add**为了设置Pre-Shared Key值与对端IP地址。

4. 单击 **Ok**。**注意：** 这是等同CLI配置：
5. 如此镜像所显示，选择**配置> VPN > VPN组件> IPSec >转换集>Add**为了创建转换集合*myset*。
6. 单击 **Ok**。**注意：** 这是等同CLI配置：
7. 选择**配置> VPN > VPN组件> IPSec > IPSec规则(ACLs) >Add**为了创建crypto Access Control List(ACL) *101*。
8. 单击 **Ok**。**注意：** 这是等同CLI配置：
9. 在创建cryto地图*mymap的*奥得河选择**配置> VPN > VPN组件> IPSec > IPSec策略>Add**如此镜像所显示。
10. 单击 **Add**。点击**常规选项卡**并且保留默认设置。点击**对等体信息**选项卡为了添加对端IP地址172.16.1.2。点击**转换集**选项卡为了选择希望的转换集合*myset*。点击**IPSec规则**选项卡为了选择现有crypto ACL 101。单击 **Ok**。**注意：** 这是等同CLI配置：
11. 选择**配置> VPN >站点到站点VPN > Edit站点到站点VPN >Add**为了应用加密映射*mymap*到接口Ethernet0/0。
12. 单击 **Ok**。**注意：** 这是等同CLI配置：

Site_A路由器CLI配置

Site_A路由器

```
Site_A#show running-config
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from
console by console
Building configuration...

Current configuration : 1545 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!--- Defines ISAKMP policy. crypto isakmp key 6 L2L12345
address 172.16.1.2 255.255.255.0

!--- Defines pre-shared secret used for IKE
authentication ! ! crypto ipsec transform-set myset esp-
des esp-md5-hmac
!--- Defines IPSec encryption and authentication
algorithms. ! crypto map mymap 10 ipsec-isakmp
```

```
 set peer 172.16.1.2
 set transform-set myset
 match address 101
!--- Defines crypto map. ! ! ! ! interface Loopback0 ip
address 192.168.1.1 255.255.255.0 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 half-duplex
 crypto map mymap
!--- Apply crypto map on the outside interface. ! ! !---
Output Suppressed ! ip http server no ip http secure-
server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0
/24

!--- Static translation defined to translate
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
source static network 192.168.1.0 10.10.10.0 /24

!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
! access-list 101 permit ip 10.5.5.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- Defines IPSec interesting traffic. !--- Note that
the host behind Site_A router communicates !--- to
Private_LAN2 using 10.10.10.0/24. !--- When the packets
arrive at the Site_A router, they are first !---
translated to 192.168.1.0/24 and then encrypted by
IPSec. ! ! control-plane ! ! line con 0 line aux 0 line
vty 0 4 ! ! end Site_A#
```

Site_B路由器CLI配置

Site_B路由器

```
Site_B#show running_config
Building configuration...

Current configuration : 939 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
!
!
crypto isakmp policy 10
```

```
 hash md5
 authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set myset
 match address 101
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 ip address 172.16.1.2 255.255.255.0
 crypto map mymap
!
!--- Output Suppressed ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end

Site_B#
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

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。

- **show crypto isakmp sa** -显示所有当前在对等端的互联网密钥交换(IKE)安全关联(SAs)。
  ```
  Site_A#show crypto isakmp sa
  dst             src             state          conn-id slot status
  172.16.1.2      10.1.1.2        QM_IDLE              1    0 ACTIVE
  ```
- **show crypto isakmp sa详细信息**—显示所有当前IKE SAS详细信息在对等体。`Site_A#show cryto isakmp sa detail`
  ```
  Codes: C - IKE configuration mode, D - Dead Peer Detection
         K - Keepalives, N - NAT-traversal
         X - IKE Extended Authentication
         psk - Preshared key, rsig - RSA signature
         renc - RSA encryption

  C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime
   Cap.
  1     10.1.1.2        172.16.1.2              ACTIVE des  md5  psk  1  23:59:42
  ```

```
       Connection-id:Engine-id =  1:1(software)
```

- **show crypto ipsec sa** - 显示当前 SA 使用的设置。`Site_A#`**`show crypto ipsec sa`**

```
interface: Ethernet0/0
    Crypto map tag: mymap, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 172.16.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 3, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x1A9CDC0A(446487562)

     inbound esp sas:
      spi: 0x99C7BA58(2580003416)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4478520/3336)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A9CDC0A(446487562)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4478520/3335)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
Site_A#
```

- **show ip nat translations** —显示转换插槽信息。`Site_A#`**`show ip nat translations`**

```
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.10.10.1         192.168.1.1
--- ---                ---                10.10.10.0         192.168.1.0
--- 10.5.5.1           192.168.1.1        ---                ---
--- 10.5.5.0           192.168.1.0        ---                ---
```

- **show ip nat statistics** —显示关于转换的静态信息。`Site_A#`**`show ip nat statistics`**

```
Total active translations: 4 (2 static, 2 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Loopback0
```

```
    Hits: 42  Misses: 2
    CEF Translated packets: 13, CEF Punted packets: 0
    Expired translations: 7
    Dynamic mappings:
    Queued Packets: 0
    Site_A#
```

- 完成这些步骤为了验证连接：在SDM，请选择**Tools> Ping**为了设立有来源IP作为192.168.1.1和目的地IP的IPSec VPN通道作为10.10.10.1。如此镜像所显示，点击**测验通道**为了检查IPSec VPN通道设立。单击开始。

故障排除

本部分提供的信息可用于对配置进行故障排除。

```
Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
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 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
Site_A#
*Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
```

```
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
```

相关信息

- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- 在ASA/PIX和Cisco VPN 3000集中器之间的IPSec有叠加专用网络配置示例的
- 技术支持和文档 - Cisco Systems