ASA/PIX：配置并且排除反向路由注入(RRI)故障

目录

简介

本文档介绍了如何在 Cisco 安全设备 (ASA/PIX) 上配置反向路由注入 (RRI) 并进行故障排除。

注意： 有关 ASA/PIX 和 Cisco VPN 客户端上远程访问 VPN 配置的详细信息，请参阅 使用 Windows 2003 IAS RADIUS（针对 Active Directory）进行身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 8.0 的 Cisco 5500 系列自适应安全设备 (ASA)
- Cisco VPN 客户端软件 5.0 版

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。

相关产品

此配置也可用于运行软件版本 7.x 及更高版本的 Cisco 500 系列 PIX 防火墙。

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

反向路由注入(RRI)用于填充运行开放最短路径优先(OSPF)协议或路由信息协议(RIP)远程VPN客户端或LAN ² LAN会话的内部路由器的路由表。

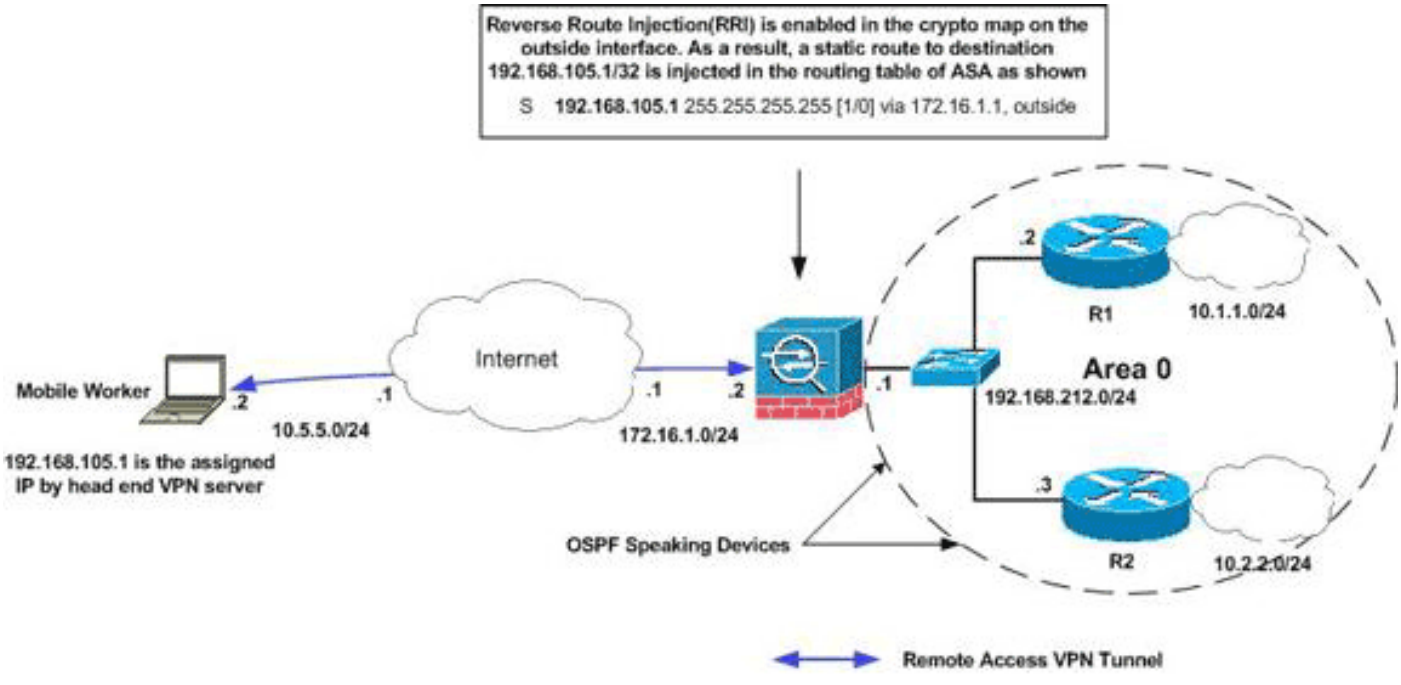
配置

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。

注意： 可以在 LAN 到 LAN VPN 隧道和 Easy VPN 方案中使用 RRI。

配置

本文档使用以下配置：

- Cisco ASA
- ASA 的 **show running-config** 输出

Cisco ASA

```
ciscoasa(config)#access-list split extended permit ip
192.168.212.0 255.255.255.0
     192.168.105.0 255.255.255.00
ciscoasa(config)#access-list redistribute standard
permit 192.168.105.0 255.255.255.0
ciscoasa(config)#ip local pool clients 192.168.105.1-
192.168.105.10 mask 255.255.255.0
ciscoasa(config)#route-map redistribute permit 1
ciscoasa(config-route-map)#match ip address redistribute
ciscoasa(config-route-map)#exit
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policy clientgroup attributes
ciscoasa(config-group-policy)#split-tunnel-policy
tunnelspecified
ciscoasa(config-group-policy)#split-tunnel-network-list
value split
ciscoasa(config-group-policy)#exit
ciscoasa(config)#isakmp nat-traversal 10
ciscoasa(config)#isakmp enable outside
ciscoasa(config)#isakmp policy 10 authentication pre-
share
ciscoasa(config)#isakmp policy 10 encryption 3des
ciscoasa(config)#isakmp policy 10 hash sha
ciscoasa(config)#isakmp policy 10 group 2
ciscoasa(config)#isakmp policy 10 lifetime 86400
ciscoasa(config)#crypto ipsec transform-set ESP-3DES-SHA
esp-3des esp-sha-hmac
ciscoasa(config)#crypto dynamic-map outside_dyn_map 20
set transform-set ESP-3DES-SHA
ciscoasa(config)#crypto dynamic-map outside_dyn_map 20
set reverse-route !--- Command to enable RRI
ciscoasa(config)#crypto map outside_map 65535 ipsec-
isakmp dynamic outside_dyn_map ciscoasa(config)#crypto
map outside_map interface outside
ciscoasa(config)#tunnel-group vpn-test type ipsec-ra
ciscoasa(config)#tunnel-group vpn-test general-
attributes ciscoasa(config-tunnel-general)#address-pool
clients ciscoasa(config-tunnel-general)#default-group-
policy clientgroup ciscoasa(config-tunnel-
general)#tunnel-group vpn-test ipsec-attributes
ciscoasa(config-tunnel-ipsec)#pre-shared-key cisco123
ciscoasa(config-tunnel-ipsec)#exit
```

Cisco ASA

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0
nameif outside security-level 0 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.212.1
255.255.255.0 ! !---Output Suppressed ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive access-list
split extended permit ip 192.168.212.0 255.255.255.0
192.168.105.0 255.255.255.0 !--- Split-tunneling ACL
access-list redistribute standard permit 192.168.105.0
255.255.255.0 !--- Match the traffic sourced from
192.168.105.0 network pager lines 24 mtu outside 1500
mtu insi 1500 ip local pool clients 192.168.105.1-
```

```
192.168.105.10 mask 255.255.255.0 no failover icmp
unreachable rate-limit 1 burst-size 1 no asdm history
enable arp timeout 14400 ! route-map redistribute permit
1 match ip address redistribute ! ! router ospf 1
network 192.168.212.0 255.255.255.0 area 0 log-adj-
changes redistribute static subnets route-map
redistribute !--- Redistribute the static routes sourced
from 192.168.105.0 !--- network into OSPF Autonomous
System (AS). ! route outside 10.5.5.0 255.255.255.0
172.16.1.1 1 !---Output Suppressed crypto ipsec
transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
dynamic-map outside_dyn_map 20 set transform-set ESP-
3DES-SHA crypto dynamic-map outside_dyn_map 20 set
reverse-route !--- Command to enable RRI crypto map
outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside crypto isakmp
enable outside crypto isakmp policy 10 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 !-
--Output Suppressed service-policy global_policy global
group-policy clientgroup internal group-policy
clientgroup attributes split-tunnel-policy
tunnelspecified split-tunnel-network-list value split
username vpnuser password gKK.Ip0zetpjju4R encrypted
tunnel-group vpn-test type remote-access tunnel-group
vpn-test general-attributes address-pool clients
default-group-policy clientgroup tunnel-group vpn-test
ipsec-attributes pre-shared-key * prompt hostname
context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

在 ASA 中启用 RRI 之前的路由表输出

注意： 假设 VPN 隧道由一个远程移动用户建立，并且 192.168.105.1 是 ASA 指定的 IP 地址。

ASA 路由表

```
ciscoasa#show route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set S 192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside C 192.168.212.0
255.255.255.0 is directly connected, insi C 172.16.1.0 255.255.255.0 is directly connected,
outside S 10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, outside O 10.2.2.1 255.255.255.255
[110/11] via 192.168.212.3, 2:09:24, insi O 10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2,
2:09:24, insi
```

提示： 即使没有配置 RRI，所连接客户端的静态路由也会注入 VPN 服务器 (ASA/PIX) 的路由表中。但是，它并不会重分配到运行动态路由协议的内部路由器（如果运行 ASA 8.0，则此类协议包括 OSPF、EIGRP 等）。

路由器 R1 路由表

```
R1#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
candidate default, U - per-user static route o - ODR, P - periodic downloaded static route
Gateway of last resort is not set C 192.168.212.0/24 is directly connected, Ethernet0 10.0.0.0/8
is variably subnetted, 2 subnets, 2 masks C 10.1.1.0/24 is directly connected, Loopback0 O
10.2.2.1/32 [110/11] via 192.168.212.3, 02:11:52, Ethernet0
```

路由器 R2 路由表

```
R2#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
candidate default, U - per-user static route o - ODR, P - periodic downloaded static route
Gateway of last resort is not set C 192.168.212.0/24 is directly connected, Ethernet0 10.0.0.0/8
is variably subnetted, 2 subnets, 2 masks C 10.2.2.0/24 is directly connected, Loopback0 O
10.1.1.1/32 [110/11] via 192.168.212.2, 02:13:03, Ethernet0
```

在 ASA 中启用 RRI 之后的路由表输出

注意： 假设 VPN 隧道由一个远程移动用户建立，并且 192.168.105.1 是 ASA 指定的 IP 地址。

ASA 路由表

```
ciscoasa#show route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set S 192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside C 192.168.212.0
255.255.255.0 is directly connected, insi C 172.16.1.0 255.255.255.0 is directly connected,
outside S 10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, outside O 10.2.2.1 255.255.255.255
[110/11] via 192.168.212.3, 2:09:24, insi O 10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2,
2:09:24, insi
```

路由器 R1 路由表

```
R1#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
candidate default, U - per-user static route o - ODR, P - periodic downloaded static route
Gateway of last resort is not set 192.168.105.0/32 is subnetted, 1 subnets O E2 192.168.105.1
[110/20] via 192.168.212.1, 00:03:06, Ethernet0 !--- Redistributed route C 192.168.212.0/24 is
directly connected, Ethernet0 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.1.1.0/24
is directly connected, Loopback0 O 10.2.2.1/32 [110/11] via 192.168.212.3, 02:11:52, Ethernet0
```

路由器 R2 路由表

```
R2#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
candidate default, U - per-user static route o - ODR, P - periodic downloaded static route
Gateway of last resort is not set 192.168.105.0/32 is subnetted, 1 subnets O E2 192.168.105.1
[110/20] via 192.168.212.1, 00:04:17, Ethernet0 !--- Redistributed route C 192.168.212.0/24 is
directly connected, Ethernet0 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.2.2.0/24
is directly connected, Loopback0 O 10.1.1.1/32 [110/11] via 192.168.212.2, 02:13:03, Ethernet0
```

相关信息

- 如何使用反向路由注入填充动态路由
- 使用 Windows 2003 IAS RADIUS（针对 Active Directory）进行身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例
- 技术支持和文档 - Cisco Systems