ASA/PIX:配置反向路由注入(RRI)並對其進行故障排除

目錄

簡介

本文檔介紹如何在思科安全裝置(ASA/PIX)上配置反向路由注入(RRI)並對其進行故障排除。

註：有關ASA/PIX和Cisco VPN客戶端上的遠端訪問VPN配置的詳細資訊，請參閱PIX/ASA 7.x和Cisco VPN Client 4.x with Windows 2003 IAS RADIUS(Against Active Directory)身份驗證配置示例。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本8.0的Cisco 5500系列調適型安全裝置(ASA)
- Cisco VPN使用者端軟體版本5.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置也可以用於運行軟體版本7.x及更高版本的Cisco 500系列PIX防火牆。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

反向路由注入(RRI)用於為遠端VPN客戶端或LAN/LAN會話填充運行開放最短路徑優先(OSPF)協定或路由資訊協定(RIP)的內部路由器²路由表。

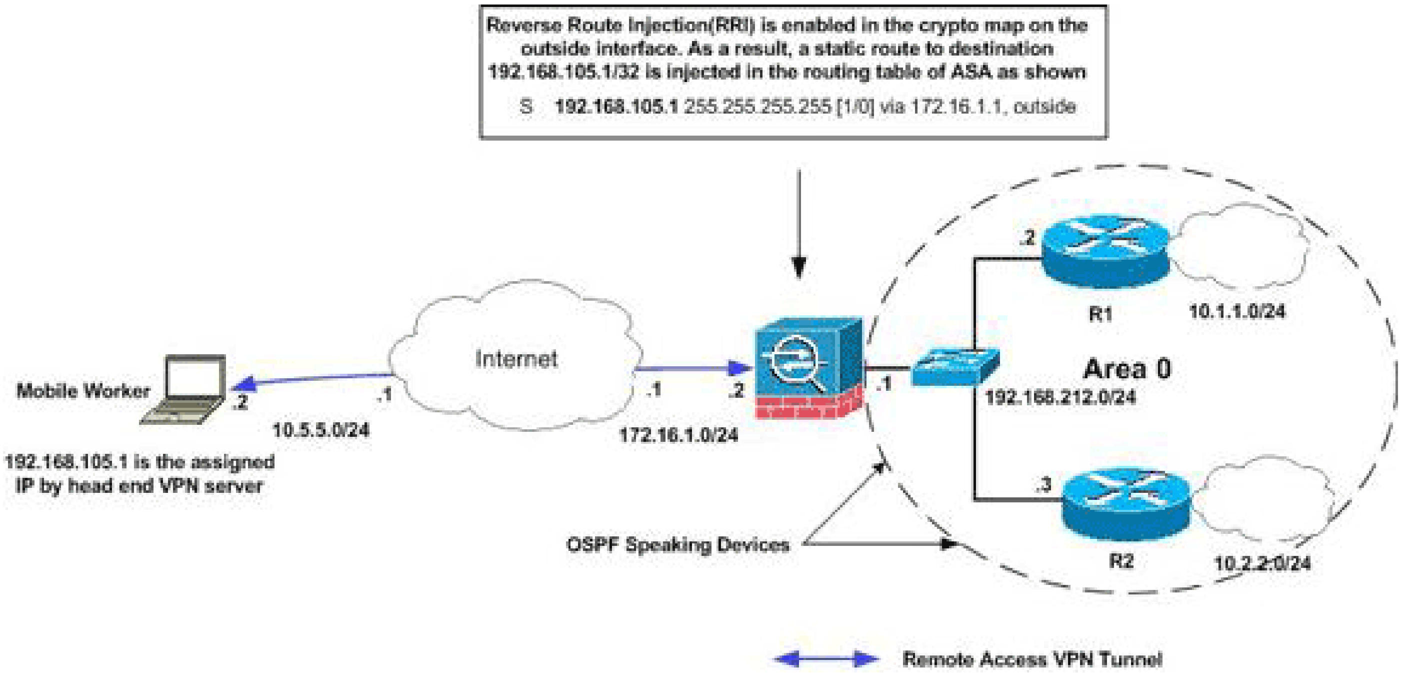
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



Reverse Route Injection(RRI) is enabled in the crypto map on the outside interface. As a result, a static route to destination 192.168.105.1/32 is injected in the routing table of ASA as shown

```
S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside
```

192.168.105.1 is the assigned IP by head end VPN server

注意：此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

注意：您可以在LAN到LAN VPN隧道和Easy VPN場景中使用RRI。

組態

本檔案會使用以下設定：

- Cisco ASA
- **show running-config** output of ASA

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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在ASA中啟用RRI之前的路由表輸出

注意：假設VPN隧道由遠端移動使用者建立，**192.168.105.1是ASA分配的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：即使未配置RRI，連線的客戶端的靜態路由也會被注入到VPN伺服器(ASA/PIX)的路由表中。但是，它不會重新分發到運行動態路由協定（如OSPF、EIGRP）的內部路由器（如果您運行ASA 8.0）。

路由器R1的路由表

```
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中啟用RRI後的路由表輸出

注意：假設VPN隧道由遠端移動使用者建立，**192.168.105.1是ASA分配的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的路由表

```
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
```

相關資訊

- 如何使用反向路由注入填充動態路由
- 採用Windows 2003 IAS RADIUS（針對Active Directory）的PIX/ASA 7.x和Cisco VPN客戶端4.x驗證配置示例
- 技術支援與文件 - Cisco Systems