

# ASA/PIX: Configure and Troubleshoot the Reverse Route Injection (RRI)

Document ID: 107596

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

### Background Information

#### Configure

- Network Diagram
- Configurations

#### Troubleshoot

- Routing Table Output Before RRI is Enabled in the ASA
- Routing Table Output After RRI is Enabled in the ASA

### Related Information

---

## Introduction

This document describes how to configure and troubleshoot the Reverse Route Injection (RRI) on the Cisco Security Appliance (ASA/PIX).

**Note:** Refer to PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example for more information on remote access VPN configuration on ASA/PIX and Cisco VPN client.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance(ASA) that runs software version 8.0
- Cisco VPN Client software version 5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Related Products

This configuration can also be used with Cisco 500 Series PIX Firewall that runs software version 7.x and later.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

Reverse Route Injection (RRI) is used to populate the routing table of an internal router that runs Open Shortest Path First (OSPF) protocol or Routing Information Protocol (RIP) for remote VPN Clients or LAN-to-LAN sessions.

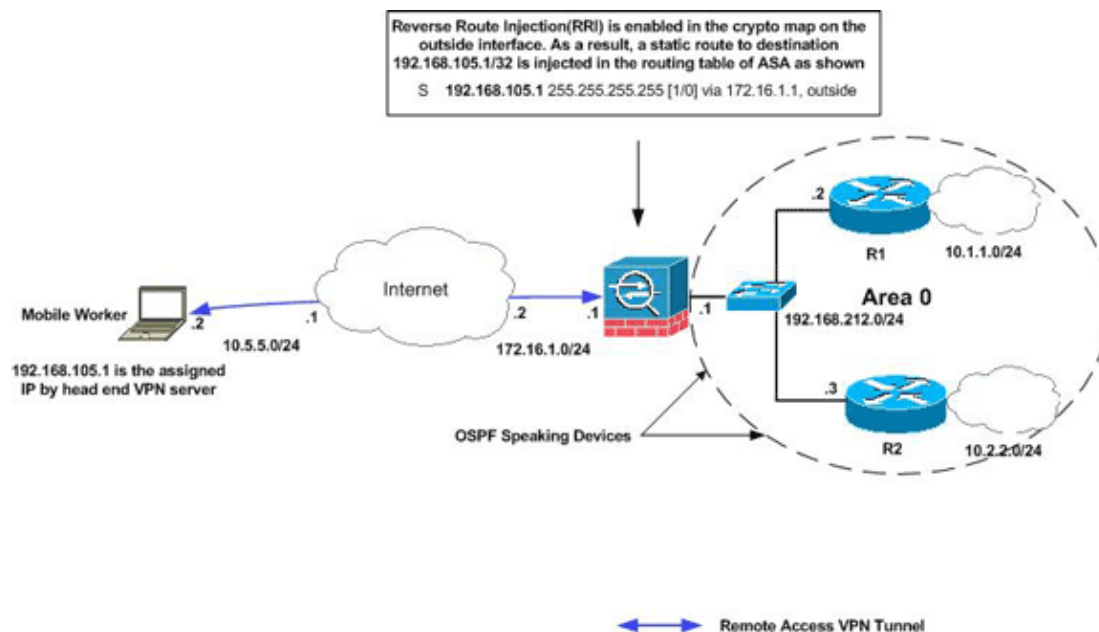
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



**Note:** The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

**Note:** You can use RRI in LAN-to-LAN VPN tunnel and Easy VPN scenarios.

## Configurations

This document uses these configurations:

- 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
```

## Troubleshoot

This section provides information you can use to troubleshoot your configuration.

### Routing Table Output Before RRI is Enabled in the ASA

**Note:** Assume the VPN tunnel is established by a remote mobile user, and **192.168.105.1** is the assigned IP address by ASA.

#### ASA Routing Table

```
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
```

**Tip:** Even if RRI is not configured, the static route of the connected client is injected into the routing table of the VPN server (ASA/PIX). However, it is not redistributed to the internal router, which runs dynamic routing protocols, such as OSPF, EIGRP (if you run ASA 8.0).

#### Router R1 Routing Table

```
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
```

## Router R2 Routing Table

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
```

## Routing Table Output After RRI is Enabled in the ASA

**Note:** Assume the VPN tunnel is established by a remote mobile user, and **192.168.105.1** is the assigned IP address by ASA.

## ASA Routing Table

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
```

## Router R1 Routing Table

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

## Router R2 Routing Table

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

---

## Related Information

- [How to Populate Dynamic Routes Using Reverse Route Injection](#)
- [PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS \(Against Active Directory\) Authentication Configuration Example](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jul 24, 2008

Document ID: 107596

---