

# ASA/PIX : Configurer et dépanner l'injection de routage inversé (RRI)

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Dépannez](#)

[La sortie de Tableau de routage avant RRI est activée dans l'ASA](#)

[La sortie de Tableau de routage après RRI est activée dans l'ASA](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer et dépanner le Reverse Route Injection (RRI) du Dispositif de sécurité (ASA/PIX) dédié Cisco.

**Remarque:** Référez-vous à [PIX/ASA 7.x et Client VPN Cisco 4.x avec l'exemple de configuration d'authentification de RAYON de Windows 2003 IAS \(contre le Répertoire actif\)](#) pour plus d'informations sur la configuration du VPN d'Accès à distance sur ASA/PIX et Client VPN Cisco.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Sécurité adaptative Appliance(ASA) de gamme Cisco 5500 qui exécute la version de logiciel 8.0

- Version de logiciel 5.0 de Client VPN Cisco

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## [Produits connexes](#)

Cette configuration peut également être utilisée avec le Pare-feu de la gamme Cisco 500 PIX qui exécute la version de logiciel 7.x et plus tard.

## [Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## [Informations générales](#)

L'Injection inversée de routes (RRI) est utilisé pour remplir table de routage d'un routeur interne qui exécute le protocole ou le Protocole RIP (Routing Information Protocol) de Protocole OSPF (Open Shortest Path First) pour les clients vpn distants ou les sessions de RÉSEAU LOCAL de <sup>2</sup> de RÉSEAU LOCAL.

## [Configurez](#)

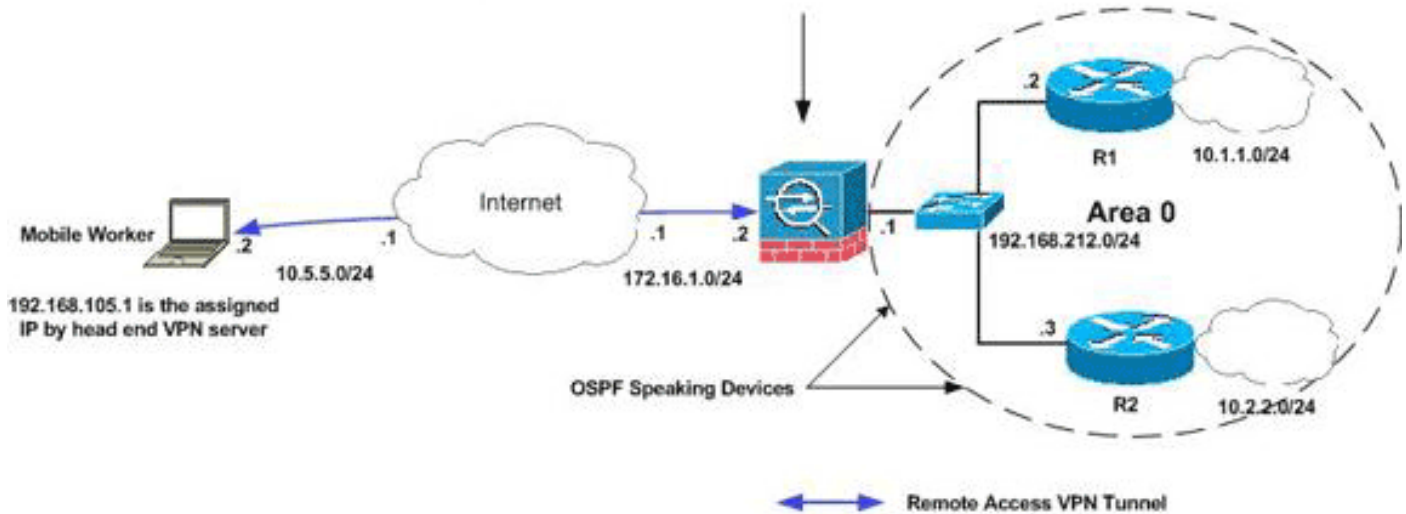
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque:** Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## [Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :

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



**Remarque:** Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

**Remarque:** Vous pouvez utiliser RRI dans des scénarios de tunnel VPN et d'Easy VPN d'entre réseaux locaux.

## Configurations

Ce document utilise les configurations suivantes :

- [Cisco ASA](#)
- [sortie de show running-config d'ASA](#)

### Cisco ASA

```
ciscoasa(config)#access-list split extended permit ip
192.168.212.0 255.255.255.0
192.168.105.0 255.255.255.0
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.Ip0zetpju4R 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
```

## [Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### [La sortie de Tableau de routage avant RRI est activée dans l'ASA](#)

**Remarque:** Supposez que le tunnel VPN est établi par un utilisateur nomade distant, et 192.168.105.1 est l'adresse IP assignée par ASA.

#### Tableau de routage ASA

```
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
```

**Conseil :** Même si RRI n'est pas configuré, l'artère statique du client connecté est injectée dans la table de routage du serveur VPN (ASA/PIX). Cependant, il n'est pas redistribué au routeur interne, qui exécute des protocoles de routage dynamique, tels que l'OSPF, EIGRP (si vous exécutez ASA 8.0).

#### Tableau de routage du routeur R1

```
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
```

#### Tableau de routage du routeur R2

```
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
```

### [La sortie de Tableau de routage après RRI est activée dans l'ASA](#)

**Remarque:** Supposez que le tunnel VPN est établi par un utilisateur nomade distant, et 192.168.105.1 est l'adresse IP assignée par ASA.

## Tableau de routage ASA

```
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
```

## Tableau de routage du routeur R1

```
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
```

## Tableau de routage du routeur R2

```
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
```

## Informations connexes

- [Comment remplir les routes dynamiques par injection de route inversée](#)
- [Exemple de configuration de l'authentification de PIX/ASA 7.x et d'un client VPN Cisco 4.x avec un serveur RADIUS IAS Windows 2003 \(par rapport à Active Directory\)](#)
- [Support et documentation techniques - Cisco Systems](#)