ASA/PIX： Reverse Route Injection（RRI）の設定とトラブルシューティング

目次

概要

このドキュメントは、Cisco セキュリティ アプライアンス（ASA/PIX）での Reverse Route Injection（RRI; 逆ルート注入）の設定とトラブルシューティングの方法について説明しています。

注: ASA/PIX および Cisco VPN Client でのリモート アクセス VPN の設定の詳細は、『PIX/ASA 7.x および Cisco VPN Client 4.x で Active Directory に対する Windows 2003 IAS RADIUS 認証を使用するための設定例』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.0 が稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）

- Cisco VPN Client ソフトウェア バージョン 5.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、ソフトウェア バージョン 7.x 以降が稼働する Cisco 500 シリーズ PIX ファイアウォールにも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Reverse Route Injection （RRI）がリモート VPN クライアントまたは LAN ² LAN セッションのための Open Shortest Path First （OSPF） プロトコルかルーティング情報プロトコル （RIP）を実行する内部ルータのルーティング テーブルを読み込むのに使用されています。

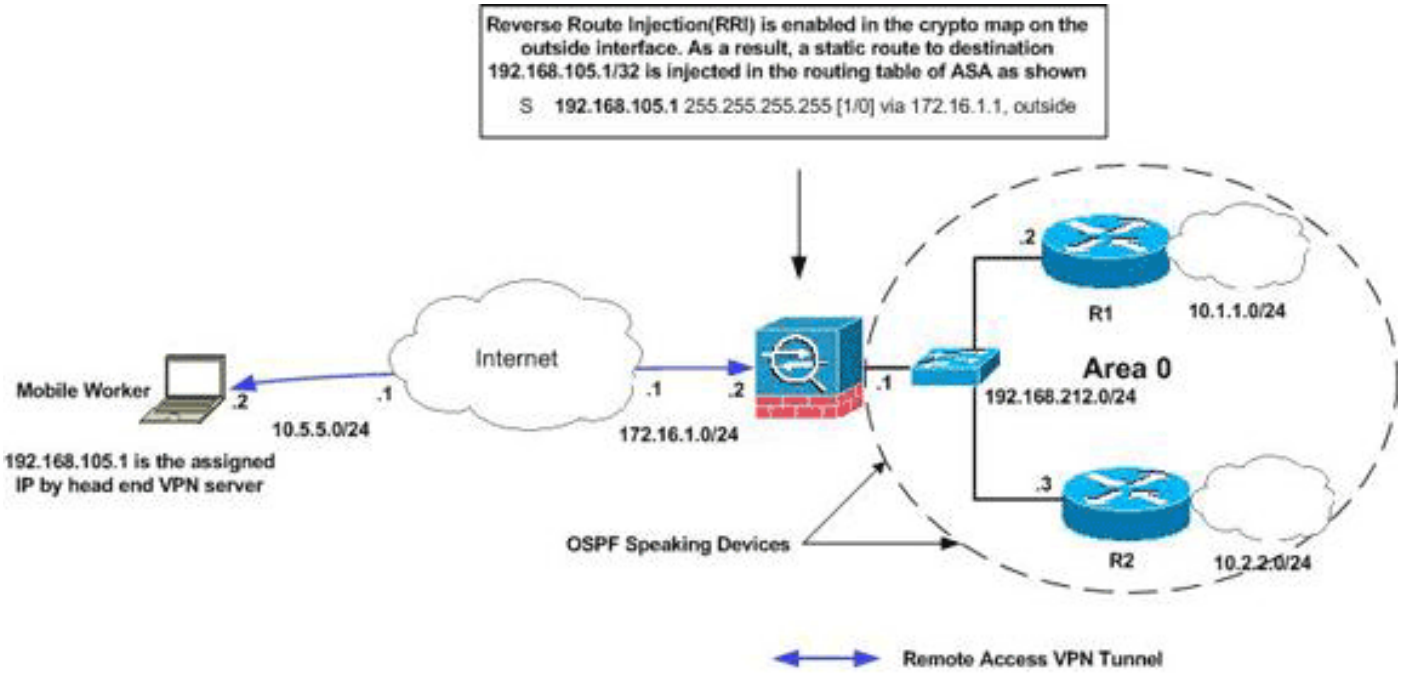
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

注: RRI は、LAN-to-LAN VPN トンネルと Easy VPN のシナリオで使用できます。

設定

このドキュメントでは、次の設定を使用します。

- Cisco ASA
- ASA の show running-config 出力

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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

ASA で RRI が有効にされる前のルーティング テーブルの出力

注: VPN トンネルはリモート モバイル ユーザによって確立されており、**192.168.105.1** が ASA によって割り当てられた IP アドレスであると仮定します。

ASA ルーティング テーブル

```
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
```

ヒント： 接続されたクライアントのスタティック ルートは、RRI が設定されていない場合でも、VPN サーバ（ASA/PIX）のルーティング テーブルに注入されます。 ただし、OSPF、EIGRP（ASA 8.0 が稼働している場合）などのダイナミック ルーティング プロトコルを実行する内部ルータへの再配布は行われません。

ルータ R1 のルーティング テーブル

```
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
```

ルータ R2 のルーティング テーブル

```
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
```

ASA で RRI が有効にされた後のルーティング テーブルの出力

注: VPN トンネルはリモート モバイル ユーザによって確立されており、**192.168.105.1** が ASA によって割り当てられた IP アドレスであると仮定します。

ASA ルーティング テーブル

```
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
```

ルータ R1 のルーティング テーブル

```
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
```

ルータ R2 のルーティング テーブル

```
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
```

関連情報

- Reverse Route Injection 機能を使用してダイナミック ルートを読み込む方法
- PIX/ASA 7.x および Cisco VPN Client 4.x で Active Directory に対する Windows 2003 IAS RADIUS 認証を使用するための設定例
- テクニカルサポートとドキュメント - Cisco Systems