ASA/PIX: Configurazione e risoluzione dei problemi di Reverse Route Injection (RRI)

Sommario

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi di Reverse Route Injection (RRI) su Cisco Security Appliance (ASA/PIX).

Nota: per ulteriori informazioni sulla configurazione della VPN di accesso remoto su ASA/PIX e sui client VPN Cisco, fare riferimento agli esempi di configurazione dell'autenticazione PIX/ASA 7.x e Cisco VPN Client 4.x con Windows 2003 RADIUS (con Active Directory).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 8.0
- Software Cisco VPN Client versione 5.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco serie 500 PIX Firewall con software versione 7.x e successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Reverse Route Injection (RRI) viene utilizzato per popolare la tabella di routing di un router interno che esegue il protocollo Open Shortest Path First (OSPF) o il protocollo Routing Information Protocol (RIP) per client VPN remoti o sessioni LAN².

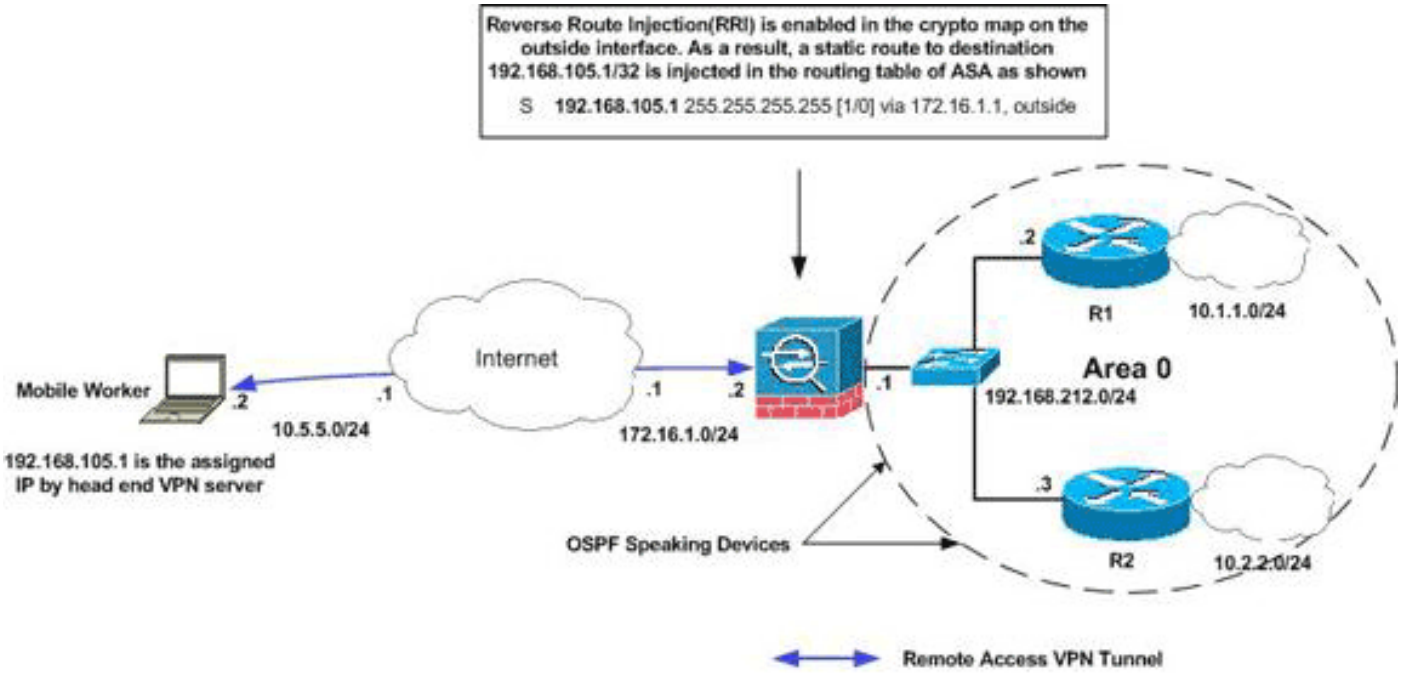
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Nota: è possibile utilizzare RRI in scenari VPN da LAN a LAN e Easy VPN.

Configurazioni

Nel documento vengono usate queste configurazioni:

- Cisco ASA
- **show running-config** output di 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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Output della tabella di routing prima dell'abilitazione di RRI nell'appliance ASA

Nota: si supponga che il tunnel VPN sia stato stabilito da un utente mobile remoto e che **192.168.105.1** sia l'indirizzo IP assegnato da ASA.

Tabella di routing 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
```

Suggerimento: anche se RRI non è configurato, la route statica del client connesso viene iniettata nella tabella di routing del server VPN (ASA/PIX). Tuttavia, non viene ridistribuito sul router interno, che esegue protocolli di routing dinamico, come OSPF, EIGRP (se si esegue ASA 8.0).

Tabella di routing del router 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
```

Tabella di routing del router 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
```

Output della tabella di routing dopo l'abilitazione di RRI nell'appliance ASA

Nota: si supponga che il tunnel VPN sia stato stabilito da un utente mobile remoto e che **192.168.105.1** sia l'indirizzo IP assegnato da ASA.

Tabella di routing 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
```

Tabella di routing del router 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
```

Tabella di routing del router 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
```

Informazioni correlate

- Come compilare le route dinamiche utilizzando Reverse Route Injection
- Esempio di configurazione dell'autenticazione PIX/ASA 7.x e Cisco VPN Client 4.x con Windows 2003 IAS RADIUS (con Active Directory)
- Documentazione e supporto tecnico – Cisco Systems