ASA/PIX: تكوين حقن المسار العكسي (RRI) واستكشاف أخطاء هذه العملية وإصلاحها

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
استكشاف الأخطاء وإصلاحها
إخراج جدول التوجيه قبل تمكين RRI في ASA
إخراج جدول التوجيه بعد تمكين RRI في ASA
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين حقن المسار العكسي (RRI) واستكشاف أخطاء هذه العملية وإصلاحها على جهاز أمان Cisco (ASA/PIX).

ملاحظة: ارجع إلى PIX/ASA 7.x و Cisco VPN Client 4.x مع Windows 2003 IAS RADIUS (مقابل Active Directory) مثال تكوين المصادقة للحصول على مزيد من المعلومات حول تكوين VPN للوصول عن بعد على ASA/PIX وعميل Cisco VPN.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار 8.0 من البرنامج
- برنامج عميل شبكة VPN من Cisco، الإصدار 5.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جدار حماية Cisco 500 Series PIX الذي يشغل الإصدار x.7 من البرنامج والإصدارات الأحدث.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يتم إستخدام إدخال المسار العكسي (RRI) لملء جدول التوجيه لموجه داخلي يشغل بروتوكول فتح أقصر مسار أولا (OSPF) أو بروتوكول معلومات التوجيه (RIP) لعملاء شبكة VPN البعيدة أو جلسات LAN ².

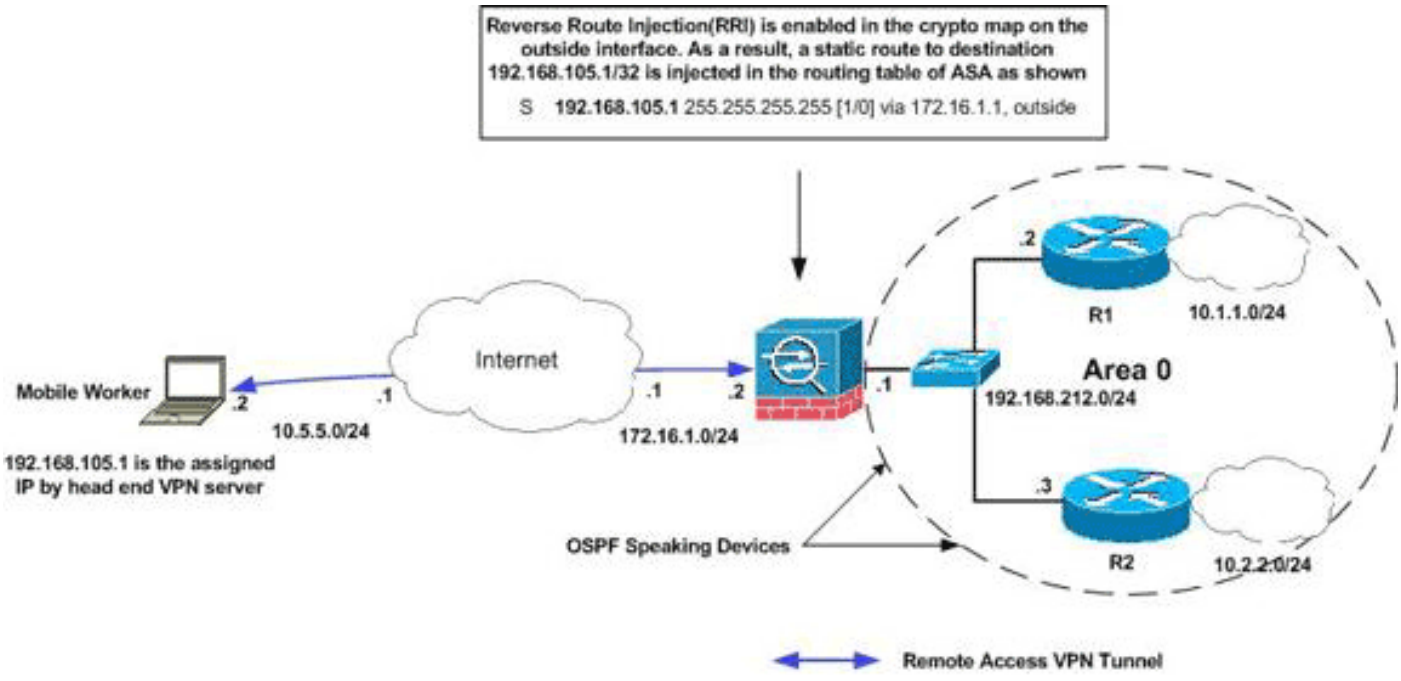
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

ملاحظة: يمكنك إستخدام RRI في نفق شبكة VPN من شبكة LAN إلى شبكة LAN وسيناريوهات شبكات VPN سهلة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- ASA من Cisco
- show running-config output من ASA

ASA من Cisco

```
ciscoasa(config)#access-list split extended permit ip
                                192.168.212.0 255.255.255.0
                            255.255.255.00 192.168.105.0
      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
```

ASA من Cisco

```
                                    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
255.255.255.0 192.168.105.0

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 :
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إخراج جدول التوجيه قبل تمكين RRI في ASA

ملاحظة: افترض أن نفق VPN تم إنشاؤه بواسطة مستخدم هاتف محمول عن بعد، **و 192.168.105.1** هو عنوان IP المعين من قبل ASA.

جدول توجيه 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
```

تلميح: حتى في حالة عدم تكوين RRI، يتم حقن المسار الثابت للعميل المتصل في جدول توجيه خادم VPN ASA/PIX)). ومع ذلك، لا تتم إعادة توزيعه على الموجه الداخلي، الذي يشغل بروتوكولات التوجيه الديناميكية، مثل OSPF، EIGRP (إذا قمت بتشغيل ASA 8.0).

جدول توجيه 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
                    is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
                          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
```

جدول توجيه الموجه 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
                    is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
                          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
```

إخراج جدول التوجيه بعد تمكين RRI في ASA

ملاحظة: افترض أن نفق VPN تم إنشاؤه بواسطة مستخدم هاتف محمول عن بعد، **و 192.168.105.1** هو عنوان IP المعين من قبل ASA.

جدول توجيه 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
```

جدول توجيه 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

                                                                  is subnetted, 1 subnets 192.168.105.0/32
                                  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
```

جدول توجيه الموجه 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

                                                                  is subnetted, 1 subnets 192.168.105.0/32
                                  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
```

معلومات ذات صلة

- كيفية ملء المسارات الديناميكية باستخدام حقن المسار العكسي
- مثال تكوين المصادقة PIX/ASA 7.x و Cisco VPN Client 4.x مع Windows 2003 IAS RADIUS (مقابل Active Directory)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).