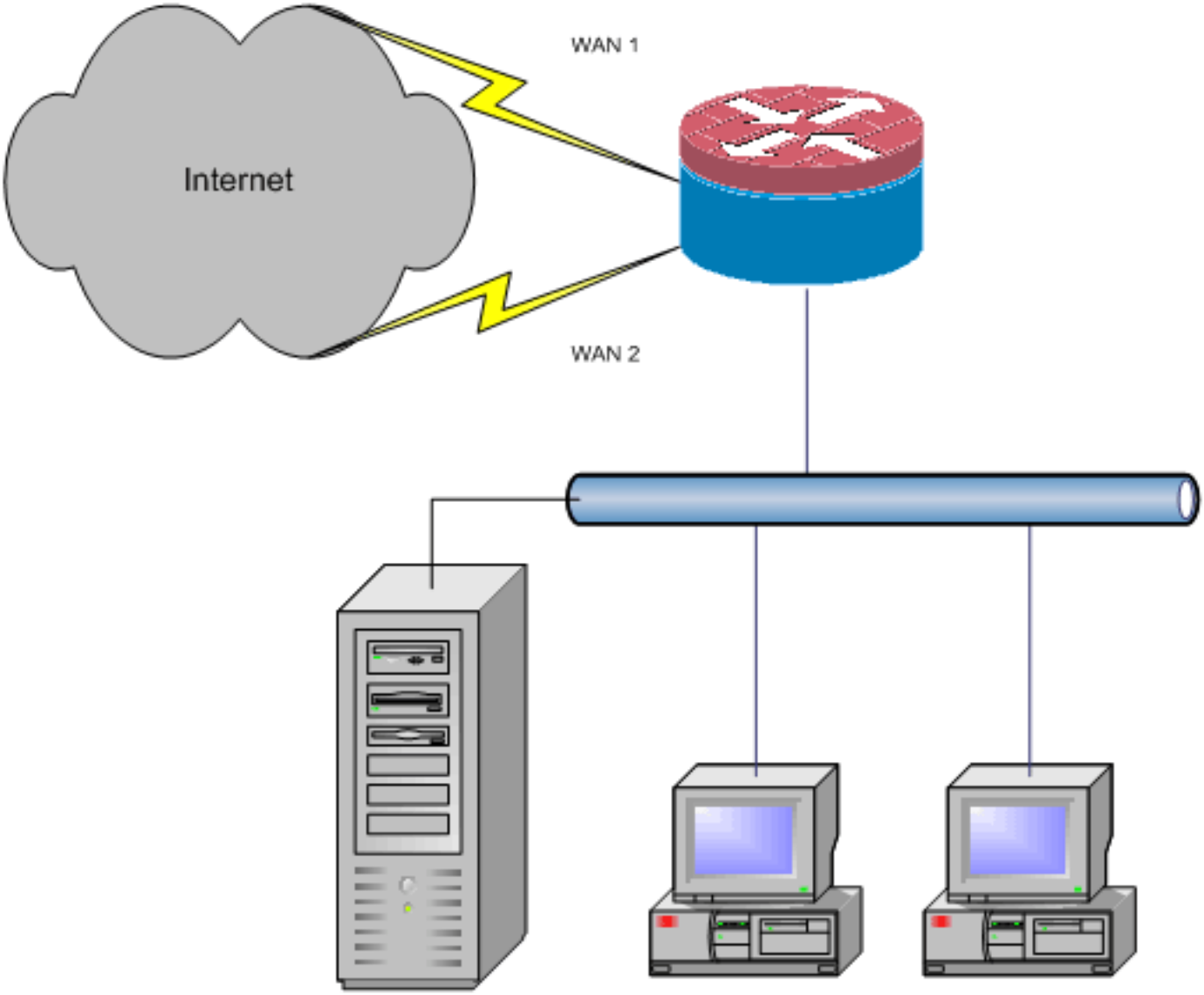
تكوين IOS NAT من Cisco لاتصالي ISP باستخدام OER

المحتويات

المقدمة

يصف هذا المستند تكوين موجه Cisco IOS® لتوصيل شبكة بالإنترنت باستخدام ترجمة عنوان الشبكة (NAT) عبر إتصالين ISP. يمكن أن يقوم Cisco IOS NAT بتوزيع إتصالات TCP وجلسات عمل UDP التالية عبر إتصالات شبكة متعددة إذا كانت مسارات متساوية التكلفة إلى وجهة معينة متوفرة. في حالة عدم إستخدام أحد الاتصالات، يمكن إستخدام تعقب الكائنات وهو أحد مكونات توجيه الحافة المحسن (OER) لإلغاء تنشيط المسار حتى يصبح الاتصال متاحا مرة أخرى، مما يضمن توفر الشبكة على الرغم من عدم إستقرار اتصال الإنترنت أو عدم موثوقيته.



يصف هذا المستند التكوينات الإضافية لتطبيق جدار حماية السياسة المستند إلى منطقة Cisco IOS لإضافة إمكانية فحص حالة لزيادة حماية الشبكة الأساسية التي توفرها NAT.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن لديك بالفعل إتصالات LAN و WAN التي تعمل ولا يوفر تكوين أو أستكشاف الأخطاء وإصلاحها في الخلفية لإنشاء اتصال أولي.

لا يصف هذا وثيقة طريقة أن يميز بين المسارات. لذلك لا توجد طريقة لتفضيل الاتصال المرغوب فيه أكثر من الاتصال الاقل جاذبية.

يوضح هذا المستند كيفية تكوين OER لتمكين أو تعطيل أي من المسارات المستندة إلى إمكانية الوصول الخاصة بخوادم DNS ل ISP. ستحتاج إلى تحديد مضيفين محددين يمكن الوصول إليهم عبر اتصال واحد فقط من إتصالات ISP وقد لا يكون متوفرا إذا لم يكن اتصال ISP هذا متوفرا.

المكونات المستخدمة

تم تطوير هذا التكوين باستخدام موجه Cisco 1811 الذي يشغل برنامج خدمات IP المتقدمة 12.4(15)T2. إذا تم

إستخدام إصدار برنامج مختلف، فقد لا تتوفر بعض الميزات، أو قد تختلف أوامر التكوين عن تلك الموضحة في هذا المستند. يجب توفر تكوينات مماثلة على جميع الأنظمة الأساسية لموجه Cisco IOS، رغم أنه من المحتمل أن يختلف تكوين الواجهة بين الأنظمة الأساسية المختلفة.

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

الاصطلاحات

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

التكوين

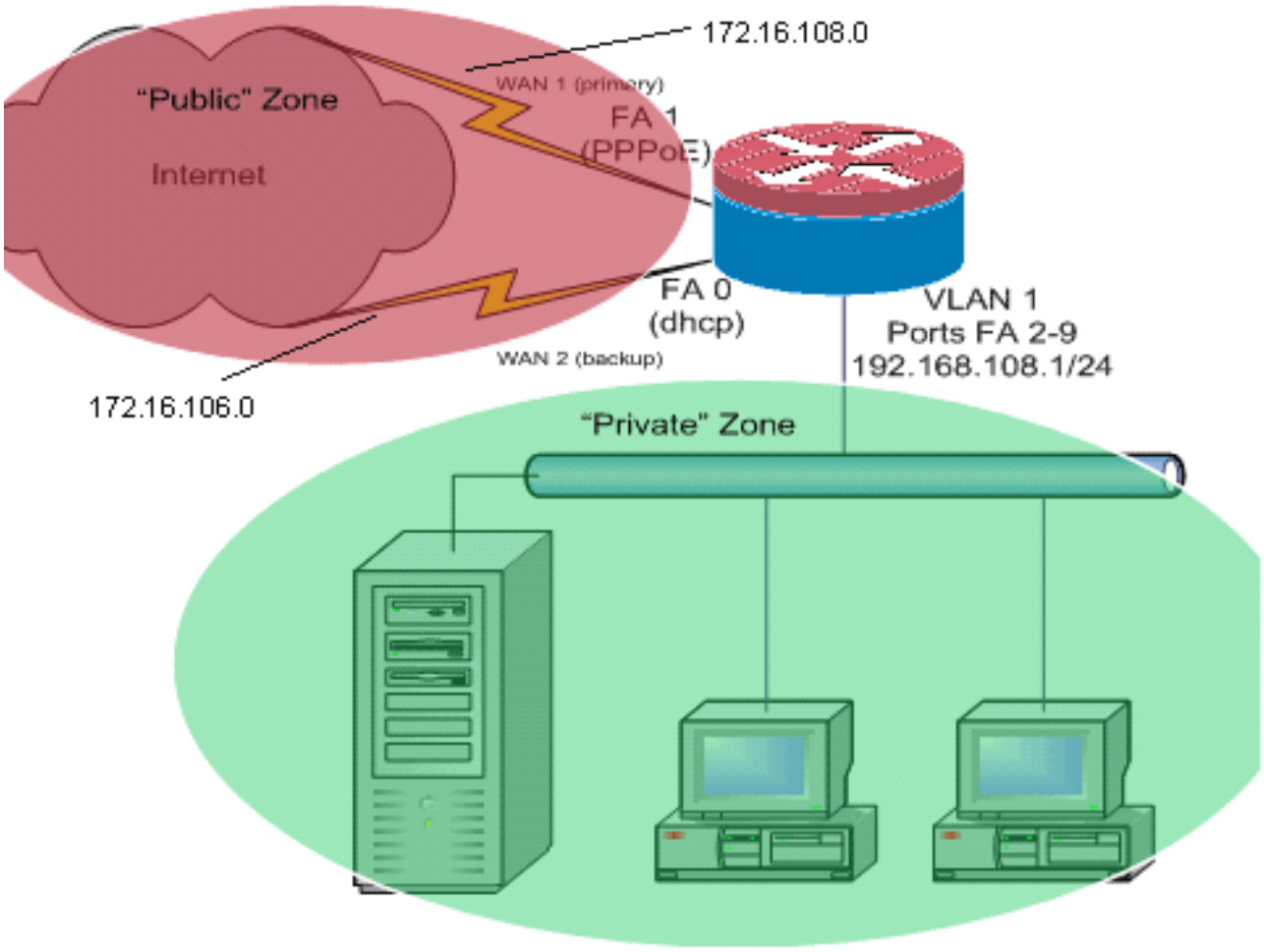
قد تحتاج إلى إضافة توجيه مستند إلى السياسة لحركة مرور معينة للتأكد من أنها تستخدم اتصال ISP واحد دائما. وتتضمن أمثلة حركة المرور التي قد تتطلب هذا السلوك عملاء IPsec VPN وسماعات الهاتف VoIP وأي حركة مرور أخرى يجب أن تستخدم دائما أحد خيارات اتصال ISP فقط لتفضيل عنوان IP نفسه أو السرعة الأعلى أو زمن الوصول الأقل على الاتصال.

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:



يصف مثال التكوين هذا، كما هو موضح في الرسم التخطيطي للشبكة، موجه وصول يستخدم اتصال IP تم تكوينه من DHCP ببروتوكول ISP واحد (كما هو موضح بواسطة FastEthernet 0) واتصال PPPoE عبر اتصال ISP الآخر. لا تؤثر أنواع الاتصال بشكل خاص على التكوين، ما لم يتم إستخدام تعقب الكائنات والتوجيه المحسن للحافة (OER) و/أو التوجيه المستند إلى السياسة مع اتصال إنترنت معين من DHCP. في هذه الحالات، قد يكون من الصعب للغاية تحديد موجه من الخطوة التالية لتوجيه السياسة أو OER.

مناقشة سياسة جدار الحماية

يصف مثال التكوين هذا سياسة جدار حماية تسمح باتصالات TCP و UDP و ICMP البسيطة من منطقة الأمان "الداخلية" إلى منطقة الأمان "الخارجية" وتحتوي على إتصالات FTP الصادرة وحركة مرور البيانات المقابلة لعمليات نقل FTP النشطة والسلبية على حد سواء. أي حركة مرور تطبيقات معقدة (على سبيل المثال، إرسال إشارات VoIP والوسائط) لا تتم معالجتها بواسطة هذه السياسة الأساسية من المرجح أن تعمل بقدرات متناقصة أو قد تفشل بالكامل. يمنع نهج جدار الحماية هذا جميع الاتصالات من منطقة الأمان "العامة" إلى المنطقة "الخاصة"، والتي تتضمن جميع الاتصالات التي يتم إستيعابها بواسطة إعادة توجيه منفذ NAT. يجب إنشاء تكوينات إضافية لنهج جدار الحماية لاستيعاب حركة المرور الإضافية التي لا تتم معالجتها بواسطة هذا التكوين الأساسي.

إذا كانت لديك أسئلة حول تصميم سياسة جدار الحماية القائم على المنطقة وتكوينها، ارجع إلى دليل تصميم جدار الحماية وتطبيقه المستند إلى المنطقة.

تكوين واجهة سطر الأوامر (CLI)

تكوين Cisco IOS CLI
track timer interface 5 ! ! track 123 rtr 1 reachability

```
                                        delay down 15 up 10
                                                          !
                                    track 345 rtr 2 reachability
                                        delay down 15 up 10
                                                          !
 Configure timers on route tracking class-map type---!
 inspect match-any priv-pub-traffic match protocol ftp
  match protocol tcp match protocol udp match protocol
  icmp ! policy-map type inspect priv-pub-policy class
    type inspect priv-pub-traffic inspect class class-
  default ! zone security public zone security private
zone-pair security priv-pub source private destination
public service-policy type inspect priv-pub-policy ! !
interface FastEthernet0 ip address dhcp ip dhcp client
                                              route track 345
                                                ip nat outside
                                      ip virtual-reassembly
                                       zone security public
                                                          !
 Use "ip dhcp client route track [number]" !--- to---!
 monitor route on DHCP interfaces !--- Define ISP-facing
interfaces with "ip nat outside" interface FastEthernet1
  no ip address pppoe enable no cdp enable ! interface
FastEthernet2 no cdp enable ! interface FastEthernet3 no
  cdp enable ! interface FastEthernet4 no cdp enable !
    interface FastEthernet5 no cdp enable ! interface
FastEthernet6 no cdp enable ! interface FastEthernet7 no
  cdp enable ! interface FastEthernet8 no cdp enable !
   interface FastEthernet9 no cdp enable ! ! interface
Vlan1 description LAN Interface ip address 192.168.108.1
255.255.255.0 ip nat inside ip virtual-reassembly ip tcp
 adjust-mss 1452 zone security private !--- Define LAN-
  facing interfaces with "ip nat inside" ! ! Interface
 Dialer 0 description PPPoX dialer ip address negotiated
 ip nat outside ip virtual-reassembly ip tcp adjust-mss
  zone security public !---Define ISP-facing interfaces
 with "ip nat outside" ! ip route 0.0.0.0 0.0.0.0 dialer
0 track 123 ! ! ip nat inside source route-map fixed-nat
 interface Dialer0 overload ip nat inside source route-
    map dhcp-nat interface FastEthernet0 overload !---
  Configure NAT overload (PAT) to use route-maps ! ! ip
  sla 1 icmp-echo 172.16.108.1 source-interface Dialer0
 timeout 1000 threshold 40 frequency 3 !---Configure an
       OER tracking entry to monitor the !---first ISP
connection ! ! ! ip sla 2 icmp-echo 172.16.106.1 source-
      interface FastEthernet0 timeout 1000 threshold 40
 frequency 3 !--- Configure a second OER tracking entry
  to monitor !---the second ISP connection ! ! ! ip sla
schedule 1 life forever start-time now ip sla schedule 2
life forever start-time now !---Set the SLA schedule and
 duration ! ! ! access-list 110 permit ip 192.168.108.0
 0.0.0.255 any !--- Define ACLs for traffic that will be
!--- NATed to the ISP connections ! ! ! route-map fixed-
     nat permit 10 match ip address 110 match interface
 Dialer0 ! route-map dhcp-nat permit 10 match ip address
      110 match interface FastEthernet0 !--- Route-maps
   associate NAT ACLs with NAT !--- outside on the ISP-
                                              facing interfaces
```

إستخدام تعقب المسار المعين من DHCP:

تكوين Cisco IOS CLI

```
interface FastEthernet0
 description Internet Intf
 ip dhcp client route track 123
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 speed 100
 full-duplex
 no cdp enable
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **عرض ip nat ترجمة**—يعرض نشاط nat بين nat داخل مضيف و nat خارج مضيف. يزود هذا أمر تحقق أن داخل مضيف يكون ترجمت إلى كلا nat عنوان خارجي.

```
Router#show ip nat tra
  Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.108.44:54486 192.168.108.3:54486 172.16.104.10:22 172.16.104.10:22
tcp 172.16.106.42:49620 192.168.108.3:49620 172.16.102.11:80 172.16.102.11:80
tcp 172.16.108.44:1623 192.168.108.4:1623 172.16.102.11:445  172.16.102.11:445
#Router
```

- **show ip route**—يتحقق من توفر مسارات متعددة إلى الإنترنت.

```
Router#show ip route
Codes: C - connected, S - static, 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
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 172.16.108.1 to network 0.0.0.0

C    192.168.108.0/24 is directly connected, Vlan1
     is subnetted, 2 subnets 172.16.0.0/24
C       172.16.108.0 is directly connected, FastEthernet4
C       172.16.106.0 is directly connected, Vlan106
S*   0.0.0.0/0 [1/0] via 172.16.108.1
via 172.16.106.1 [1/0]
```

- **show policy-map type فحص جلسات زوج المنطقة**—يعرض نشاط فحص جدار الحماية بين مضيفي المنطقة الخاصة ومضيفي المنطقة العامة. يوفر هذا الأمر التحقق من فحص حركة مرور البيانات على الأجهزة المضيفة الداخلية أثناء اتصال الأجهزة المضيفة بالخدمات في المنطقة الأمنية الخارجية.

استكشاف الأخطاء وإصلاحها

دققت هذا مادة إن لا يعمل توصيل بعد أن يشكل أنت ال cisco ios مسحاج تخديد مع nat:

- يتم تطبيق NAT بشكل مناسب على الواجهات الخارجية والداخلية.
- اكتمل تكوين NAT، وتعكس قوائم التحكم في الوصول حركة المرور التي يجب أن تكون NATed.
- تتوفر مسارات متعددة إلى شبكة الإنترنت/شبكة الاتصال واسعة النطاق (WAN).

- إذا كنت تستخدم تعقب المسار، فتحقق من حالة تعقب المسار لضمان توفر إتصالات الإنترنت.
- يعكس نهج جدار الحماية طبيعة حركة المرور التي ترغب في السماح بها من خلال الموجه بدقة.

معلومات ذات صلة

- جدار حماية Cisco IOS
- cisco ios ip عنونة خدمة أمر مرجع - nat أمر
- دليل تصميم وتطبيق جدار الحماية القائم على المناطق
- دليل تكوين توجيه الحافة المحسنة IOS، الإصدار 12.4T من Cisco
- 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).