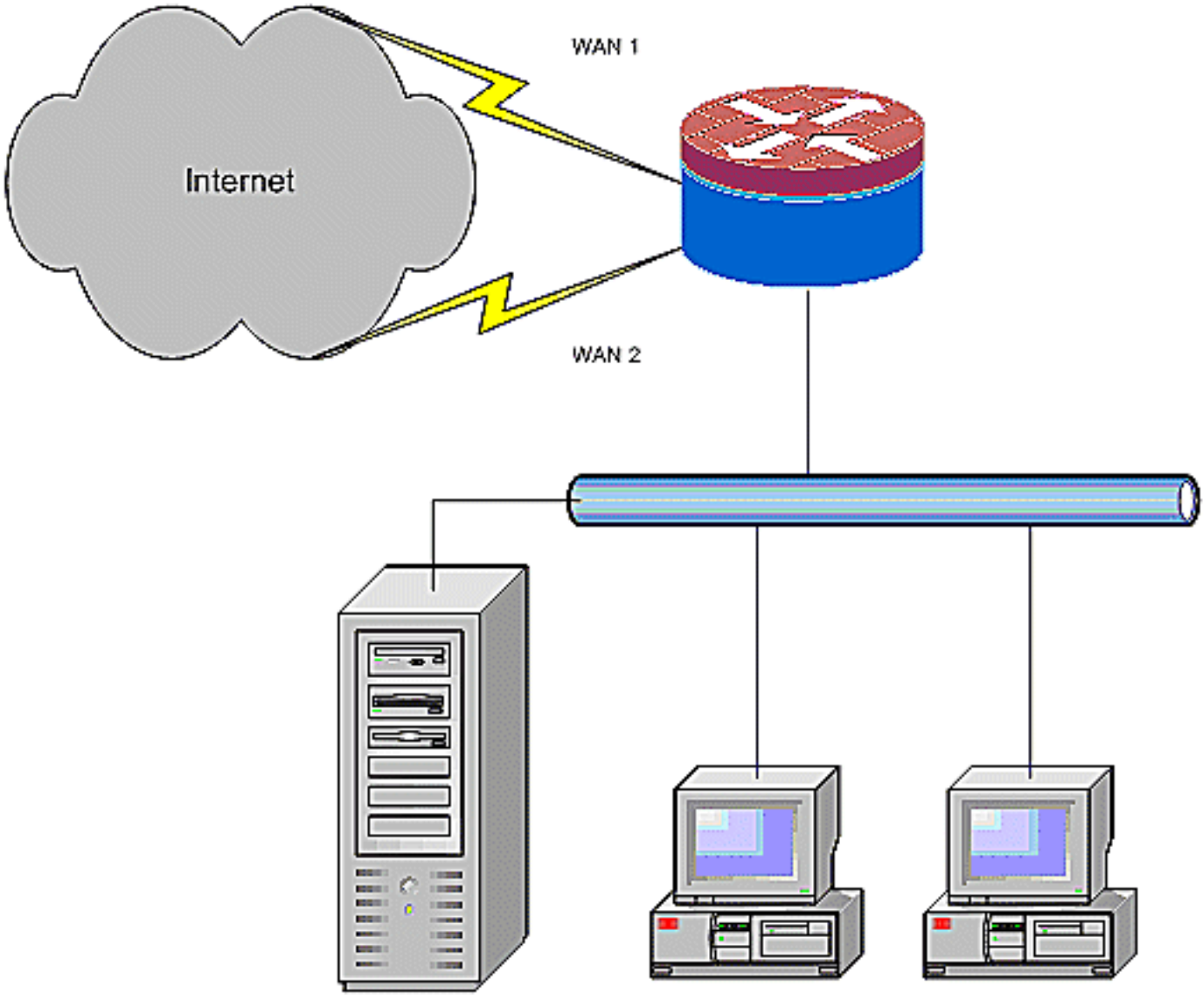
موازنة حمل IOS NAT مع جدار حماية السياسات القائم على المنطقة لاتصالاتي ISP

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
مناقشة سياسة جدار الحماية
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يزود هذا وثيقة عينة تشكيل ل cisco ios ® مسحاج تخديد أن يربط شبكة إلى الإنترنت مع شبكة عنوان ترجمة (NAT) من خلال إثنان isp توصيل. يمكن ل Cisco IOS Software NAT توزيع إتصالات TCP وجلسات عمل UDP اللاحقة عبر إتصالات الشبكة المتعددة إذا كانت مسارات التكلفة المتساوية إلى وجهة معينة متوفرة.



يصف هذا المستند التكوين الإضافي لتطبيق جدار حماية السياسة (ZFW) المستندة إلى منطقة CISCO IOS لإضافة قدرة فحص حالة لزيادة حماية الشبكة الأساسية التي توفرها NAT.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أنك تعمل مع إتصالات LAN و WAN ولا يوفر التكوين أو أستكشاف الأخطاء وإصلاحها في الخلفية لإنشاء الاتصال الأولي. لا يصف هذا المستند طريقة للتمييز بين المسارات، لذلك لا توجد طريقة لتفضيل اتصال مرغوب فيه أكثر من اتصال أقل رغبة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى موجه Cisco Series 1811 مع برنامج خدمات IP المتقدمة T3(15)12.4. إذا تم إستخدام إصدار برنامج مختلف، فلن تتوفر بعض الميزات، أو قد تختلف أوامر التكوين عن تلك الموضحة في هذا المستند. يتوفر تكوين مماثل على جميع الأنظمة الأساسية لموجه Cisco IOS، رغم احتمال أختلاف 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

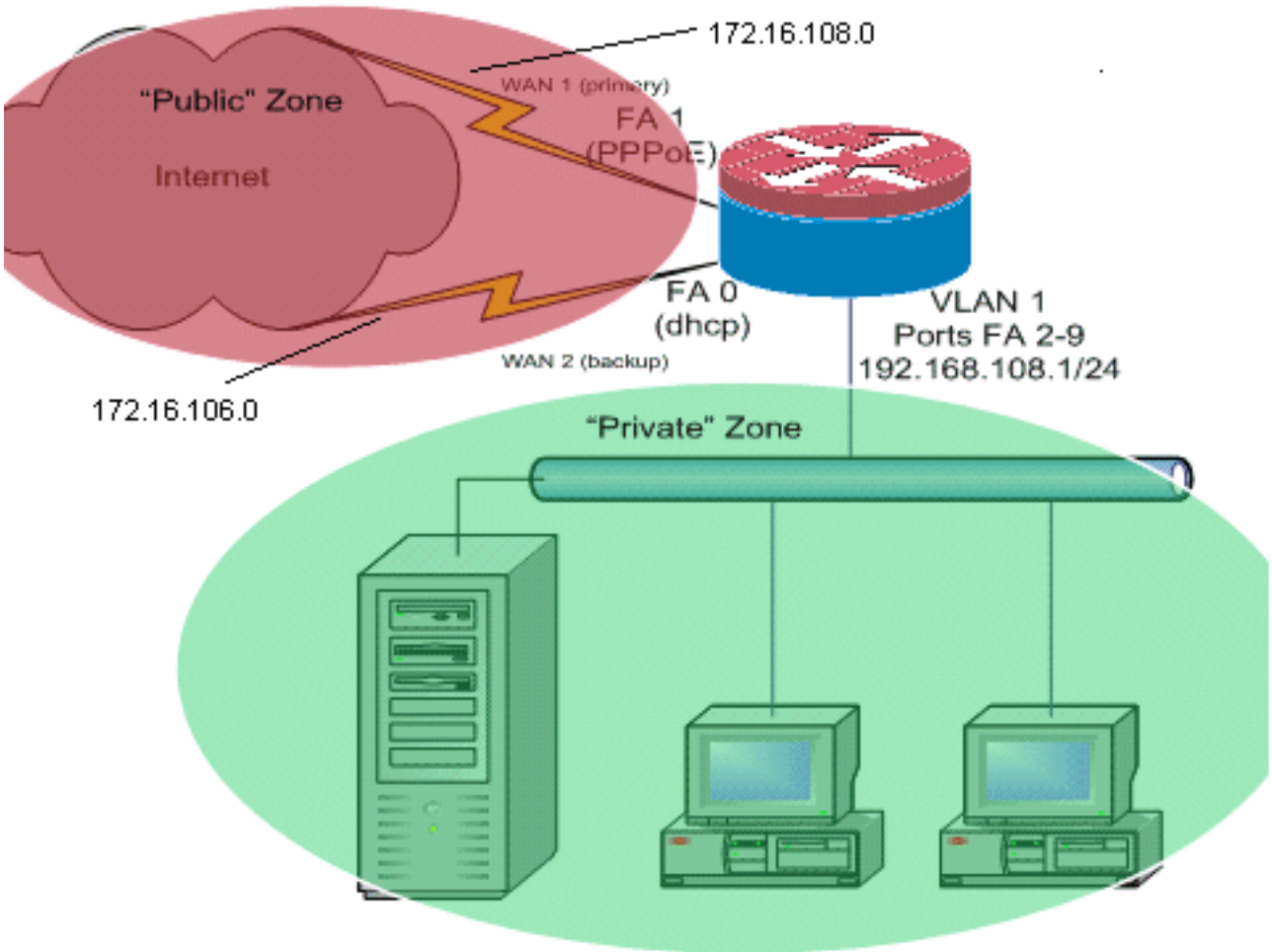
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



يصف مثال التكوين هذا موجه وصول يستخدم اتصال IP تم تكوينه من DHCP بواحد من ISP (كما هو موضح

بواسطة FastEthernet 0)، واتصال PPPoE عبر اتصال ISP الآخر. لا تؤثر أنواع الاتصال بشكل خاص على التكوين، ولكن بعض أنواع الاتصالات يمكن أن تعيق إستخدام هذا التكوين في سيناريوهات فشل محددة. وهذا يحدث بشكل خاص في الحالات التي يتم فيها إستخدام اتصال IP عبر خدمة WAN المتصلة بالإيثرنت، على سبيل المثال، مودم الكبل أو خدمات DSL حيث يقوم جهاز إضافي بإنهاء اتصال WAN ويوفر ميزة التسليم عبر الإيثرنت إلى موجه Cisco IOS. في الحالات التي يتم فيها تطبيق عنونة IP الثابتة، مقارنة بالعناوين التي تم تعيينها إلى DHCP أو PPPoE، ويحدث فشل WAN، بحيث يظل منفذ الإيثرنت يحتفظ بارتباط إيثرنت بجهاز اتصال WAN، يستمر الموجه في محاولة موازنة الأحمال بالاتصال عبر إتصالات WAN الجيدة والسيئة. إذا كان النشر لديك يتطلب إزالة المسارات غير النشطة من موازنة الأحمال، فارجع إلى التكوين المتوفر في موازنة أحمال بطاقة واجهة الشبكة (NAT) من Cisco IOS وجدار حماية السياسات المستند إلى المنطقة مع توجيه الحافة المحسن لاثنين من إتصالات الإنترنت يصف إضافة توجيه الحافة المحسن لمراقبة صحة المسار.

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 ومن المحتمل أن تعمل بقدرات منخفضة أو يمكن أن تفشل بالكامل. تمنع سياسة جدار الحماية هذه جميع الاتصالات من منطقة الأمان "العامة" إلى المنطقة "الخاصة"، والتي تتضمن جميع الاتصالات التي يتم تمكينها بواسطة إعادة توجيه منفذ NAT. إذا تطلب الأمر، تحتاج إلى ضبط سياسة فحص جدار الحماية لتعكس ملف تعريف التطبيق وسياسة الأمان.

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

التكوينات

يستخدم هذا المستند التكوينات التالية:

التكوين

```
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 nat outside ip virtual-
           reassembly zone security public ! interface
FastEthernet1 no ip address pppoe enable no cdp enable !
      interface FastEthernet2 no cdp enable !--- Output
Suppressed 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 ! 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 ! 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
```

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 translation
  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 أنه يتم فحص حركة مرور الأجهزة المضيفة الداخلية أثناء اتصال الأجهزة المضيفة بالخدمات في منطقة الأمان "الخارجية".

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

بعد تكوين موجه Cisco IOS باستخدام NAT، إذا لم تعمل الاتصالات، فتأكد من التالي:

- 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).
- يعكس نهج جدار الحماية طبيعة حركة المرور التي ترغب في السماح بها من خلال الموجه بدقة.

معلومات ذات صلة

- دعم تقنية الصوت
- دعم منتجات الاتصالات الصوتية والاتصالات الموحّدة
- استكشاف أخطاء خدمة IP الهاتفية من Cisco وإصلاحها
- دليل تصميم وتطبيق جدار الحماية القائم على المناطق
- 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).