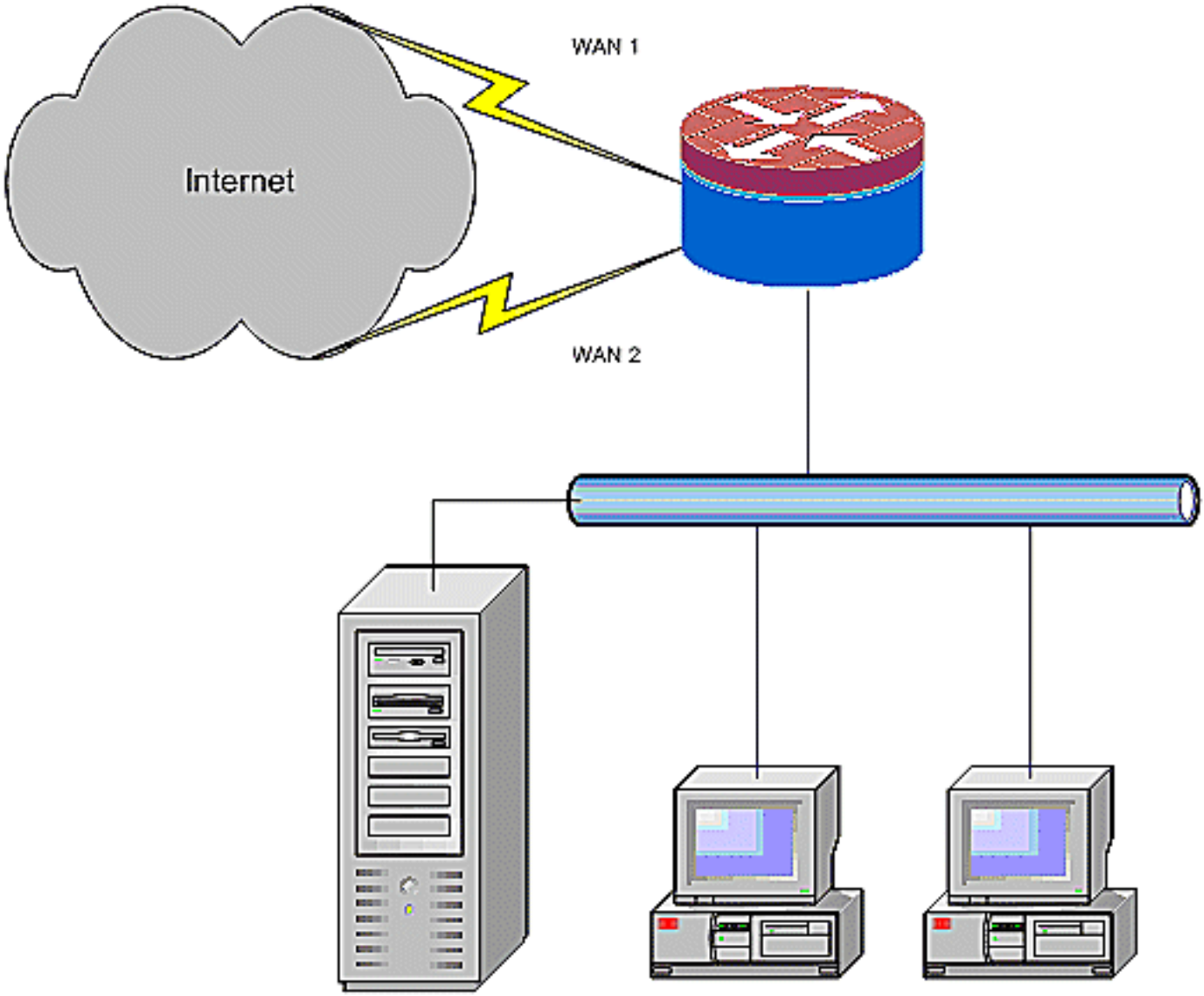
Équilibrage de charge NAT IOS avec pare-feu de stratégie basé sur la zone pour deux connexions ISP

Contenu

Introduction

Ce document fournit un exemple de configuration pour un routeur Cisco IOS® pour connecter un réseau à Internet avec la traduction d'adresses de réseau (NAT) via deux connexions ISP. La NAT du logiciel Cisco IOS peut distribuer les connexions TCP et les sessions UDP suivantes sur plusieurs connexions réseau si des routes à coût égal vers une destination donnée sont disponibles.



Ce document décrit une configuration supplémentaire pour appliquer le pare-feu ZFW (Zone-Based Policy Firewall) de Cisco IOS afin d'ajouter une fonctionnalité d'inspection dynamique afin d'augmenter la protection de base du réseau fournie par NAT.

Conditions préalables

Conditions requises

Ce document suppose que vous travaillez avec des connexions LAN et WAN et ne fournit pas d'arrière-plan de configuration ou de dépannage pour établir la connectivité initiale. Ce document ne décrit pas un moyen de différencier les routes, il n'y a donc aucun moyen de préférer une connexion plus souhaitable à une connexion moins souhaitable.

Components Used

Les informations de ce document sont basées sur le routeur Cisco 1811 avec le logiciel Advanced IP Services 12.4(15)T3. Si une autre version du logiciel est utilisée, certaines fonctionnalités ne

sont pas disponibles ou les commandes de configuration peuvent différer de celles présentées dans ce document. Une configuration similaire est disponible sur toutes les plates-formes de routeur Cisco IOS, bien que la configuration de l'interface varie probablement d'une plate-forme à l'autre.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

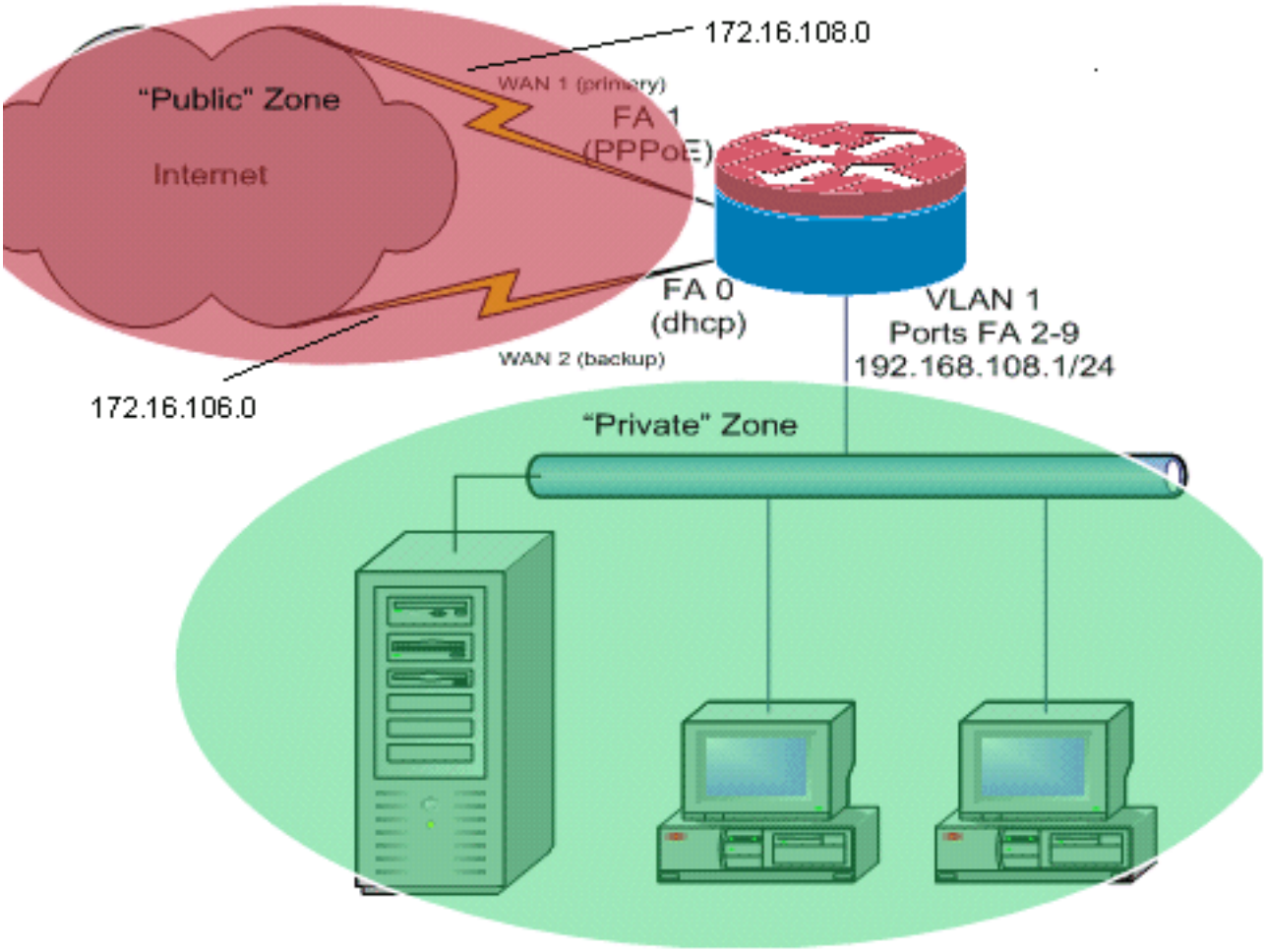
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Vous devez ajouter le routage basé sur une réglementation pour le trafic spécifique afin de s'assurer qu'il utilise toujours une connexion ISP. Les clients VPN IPSec, le trafic de téléphonie VoIP et tout autre trafic qui n'utilise qu'une seule des options de connexion du FAI pour préférer la même adresse IP, une vitesse supérieure ou une latence inférieure à la connexion sont des exemples de trafic pouvant nécessiter ce comportement.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cet exemple de configuration décrit un routeur d'accès qui utilise une connexion IP configurée par DHCP à un FAI (comme illustré par FastEthernet 0) et une connexion PPPoE sur l'autre connexion FAI. Les types de connexion n'ont pas d'impact particulier sur la configuration, mais certains types de connexions peuvent entraver l'utilisation de cette configuration dans des scénarios d'échec spécifiques. Cela se produit en particulier dans les cas où la connectivité IP sur un service WAN Ethernet est utilisée, par exemple, les services par modem câble ou DSL lorsqu'un périphérique supplémentaire termine la connectivité WAN et fournit un transfert Ethernet au routeur Cisco IOS. Dans les cas où l'adressage IP statique est appliqué, par opposition aux adresses attribuées par DHCP ou PPPoE, et où une défaillance WAN se produit, de sorte que le port Ethernet conserve une liaison Ethernet au périphérique de connectivité WAN, le routeur continue à tenter d'équilibrer la charge de la connectivité entre les connexions WAN bonnes et mauvaises. Si votre déploiement nécessite que les routes inactives soient supprimées de l'équilibrage de charge, reportez-vous à la configuration fournie dans Cisco IOS NAT Load-Balancing et Zone-Based Policy Firewall avec routage de périphérie optimisé pour deux connexions Internet qui décrit l'ajout du routage de périphérie optimisé pour surveiller la validité de la route.

Discussion sur la politique de pare-feu

Cet exemple de configuration décrit une stratégie de pare-feu qui autorise des connexions TCP, UDP et ICMP simples de la zone de sécurité “ interne ” à la zone de sécurité “ externe ” et prend en charge les connexions FTP sortantes et le trafic de données équivalent pour les transferts FTP actifs et passifs. Tout trafic d'application complexe, par exemple la signalisation VoIP et les supports, qui n'est pas géré par cette stratégie de base fonctionne probablement avec une capacité réduite ou peut échouer entièrement. Cette stratégie de pare-feu bloque toutes les connexions de la zone de sécurité ” publique “ à la zone ” privée “, qui inclut toutes les connexions

qui sont prises en charge par le transfert de port NAT. Si nécessaire, vous devez ajuster la stratégie d'inspection de pare-feu pour refléter votre profil d'application et votre stratégie de sécurité.

Si vous avez des questions sur la conception et la configuration de la stratégie de pare-feu de stratégie basée sur les zones, reportez-vous au Guide de conception et d'application de la stratégie basée sur les zones.

Configurations

Ce document utilise les configurations suivantes :

Configuration

```
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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **show ip nat translation - Affiche l'activité NAT entre les hôtes internes NAT et les hôtes NAT**

extérieurs. Cette commande permet de vérifier que les hôtes internes sont traduits en adresses externes NAT.

```
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 - Vérifie que plusieurs itinéraires vers Internet sont disponibles.**

```
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
     172.16.0.0/24 is subnetted, 2 subnets
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
               [1/0] via 172.16.106.1
```

- **show policy-map type inspect zone-pair sessions** - Affiche l'activité d'inspection de pare-feu entre “ hôtes de zone ” privée et “ hôtes de zone ” publique. Cette commande permet de vérifier que le trafic des hôtes internes est inspecté lorsque les hôtes communiquent avec les services de la zone de sécurité “ externe ”.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Après avoir configuré le routeur Cisco IOS avec la fonction NAT, si les connexions ne fonctionnent pas, assurez-vous des éléments suivants :

- NAT est appliqué convenablement sur les interfaces externes et internes.
- La configuration NAT est complète et la liste reflète le trafic qui doit être soumis à NAT.
- Plusieurs itinéraires vers Internet/WAN sont disponibles.
- La politique de pare-feu reflète fidèlement la nature du trafic que vous souhaitez autoriser via le routeur.

Informations connexes

- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Dépannage des problèmes de téléphonie IP Cisco
- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Support et documentation techniques - Cisco Systems