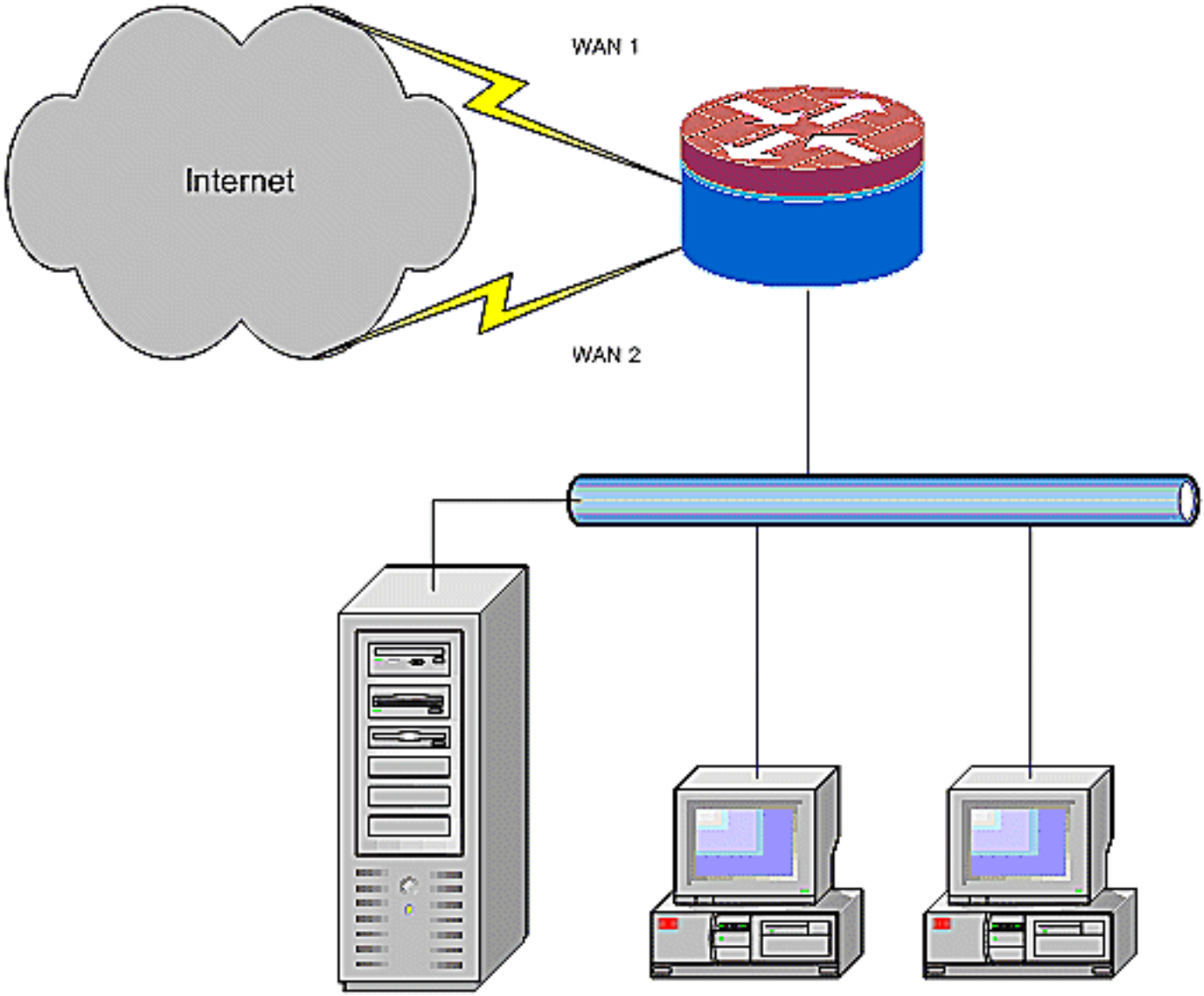
Équilibrage de charge NAT IOS avec pare-feu de stratégie basé sur la zone pour deux connexions ISP

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour qu'un routeur de Cisco IOS® connecte un réseau à l'Internet au Traduction d'adresses de réseau (NAT) par deux connexions ISP. Le logiciel de Cisco IOS NAT peut distribuer les connexions TCP et les sessions ultérieures d'UDP au-dessus de plusieurs connexions réseau si les artères de coût égal à une destination donnée sont disponibles.



Ce document décrit la configuration supplémentaire pour appliquer le Pare-feu basé sur zone de stratégie de Cisco IOS (ZFW) pour ajouter la capacité d'inspection avec état pour augmenter la protection du réseau de base fournie par NAT.

Conditions préalables

Conditions requises

Ce document vous suppose travail avec des connexions de LAN et WAN et ne fournit pas le fond de configuration ou de dépannage pour établir la connectivité initiale. Ce document ne décrit pas une manière de différencier entre les artères, tellement là n'est aucune manière de préférer une connexion plus desirable au-dessus d'une connexion moins desirable.

Composants utilisés

Les informations dans ce document sont basées sur le routeur de la gamme 1811 de Cisco avec le logiciel de Services IP avancé par 12.4(15)T3. Si une version de logiciel différente est utilisée,

quelques caractéristiques ne sont pas disponibles, ou les commandes de configuration peuvent différer de ceux affichés dans ce document. La configuration semblable est disponible sur toutes les Plateformes de routeur Cisco IOS, bien que la configuration d'interface varie vraisemblablement entre différentes Plateformes.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Configurez

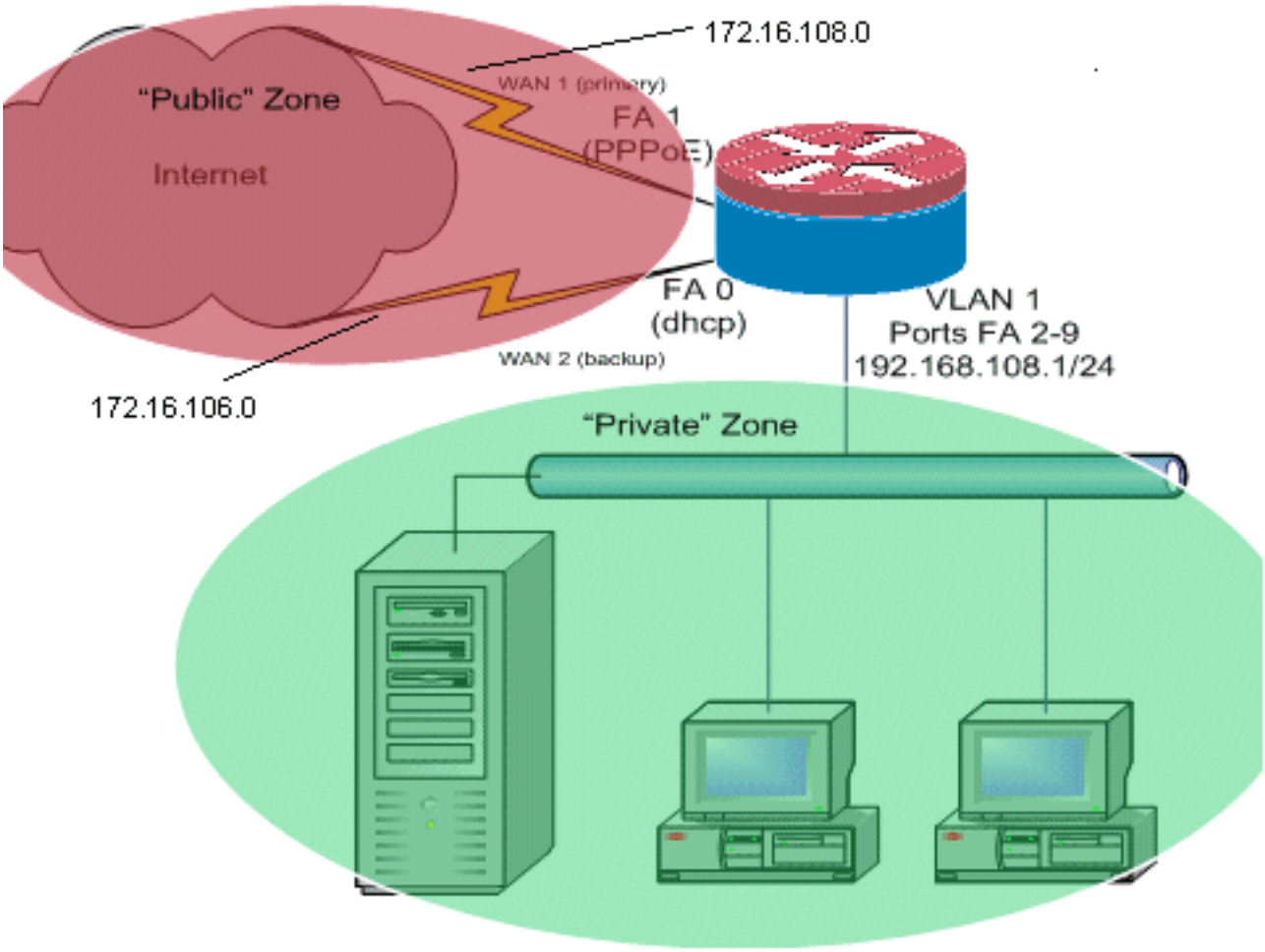
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) 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 exemples du trafic qui peuvent exiger ce comportement le trafic incluent d'IPSec de clients vpn, VoIP téléphonie, et n'importe quel autre trafic qui utilise seulement un des possibilités de connexion ISP de préférer la même adresse IP, vitesse supérieure, ou de diminuer la latence sur la connexion.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cet exemple de configuration décrit un routeur d'accès qui utilise une connexion IP DHCP-configurée à un ISP (comme affiché par FastEthernet 0), et une connexion PPPoE au-dessus de l'autre connexion ISP. Les types de connexion n'ont aucune incidence particulière sur la configuration, mais les types de quelques connexions peuvent gêner la facilité d'utilisation de cette configuration dans les scénarios de panne spécifiques. Ceci se produit en particulier dans les cas où la connectivité IP au-dessus d'un service WAN Ethernet-connecté est utilisée, par exemple, modem câble ou services DSL où un périphérique supplémentaire termine la connectivité WAN et fournit le hand-off d'Ethernets au routeur Cisco IOS. Dans les cas où l'adressage IP statique est appliqué, par opposition aux adresses ou au PPPoE DHCP-assignées, et une panne BLÊME se produit, telle que le port Ethernet met à jour toujours le lien d'Ethernets au périphérique de connectivité WAN, le routeur continue à tenter d'équilibrer la charge la Connectivité à travers les bonnes et mauvaises connexions WAN. Si votre déploiement exige que des artères inactives soient retirées de l'Équilibrage de charge, référez-vous à la configuration donnée dans l'Équilibrage de charge NAT de Cisco IOS et le Pare-feu basé sur zone de stratégie en Optimized Edge Routing pour deux connexions Internet qui décrit l'ajout d'Optimized Edge Routing pour surveiller la validité d'artère.

Discussion de stratégie de Pare-feu

Cet exemple de configuration décrit une stratégie de Pare-feu qui permet les connexions simples de TCP, d'UDP, et d'ICMP de la zone de Sécurité de « intérieur » à la zone de Sécurité de « extérieur », et facilite les connexions FTP sortantes et le trafic de données équivalent pour les deux transferts de FTP actif et passif. N'importe quel trafic de l'application complexe, par exemple, signalisation VoIP et support, qui n'est pas manipulé par cette stratégie de base vraisemblablement fonctionne avec la capacité diminuée 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 facilitées par la transmission du port NAT. S'il y a lieu, vous devez ajuster la stratégie d'inspection de Pare-feu pour refléter votre profil et stratégie de sécurité d'application.

Si vous avez des questions sur la conception et la configuration de stratégie basées sur zone de Pare-feu de stratégie, référez-vous au guide basé sur zone de conception et d'application de Pare-feu de stratégie.

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
```

Vérifiez

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 fournit la vérification que des hôtes internes sont traduits aux

deux adresses NAT d'extérieur.`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`
- **sessions de show policy-map type inspect zone-pair** — Activité d'inspection de Pare-feu d'affichages entre - hôtes et « public » de zone - les hôtes « privés » de zone. Cette commande fournit la vérification que le trafic des hôtes internes est examiné comme les hôtes communiquent avec des services dans la zone de Sécurité de « extérieur ».

Dépannez

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

Après que vous configuriez le routeur Cisco IOS avec NAT, si les connexions ne fonctionnent pas, soyez sûr de ces derniers :

- 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 stratégie de Pare-feu reflète exactement la nature du trafic que vous souhaitez permettre par 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