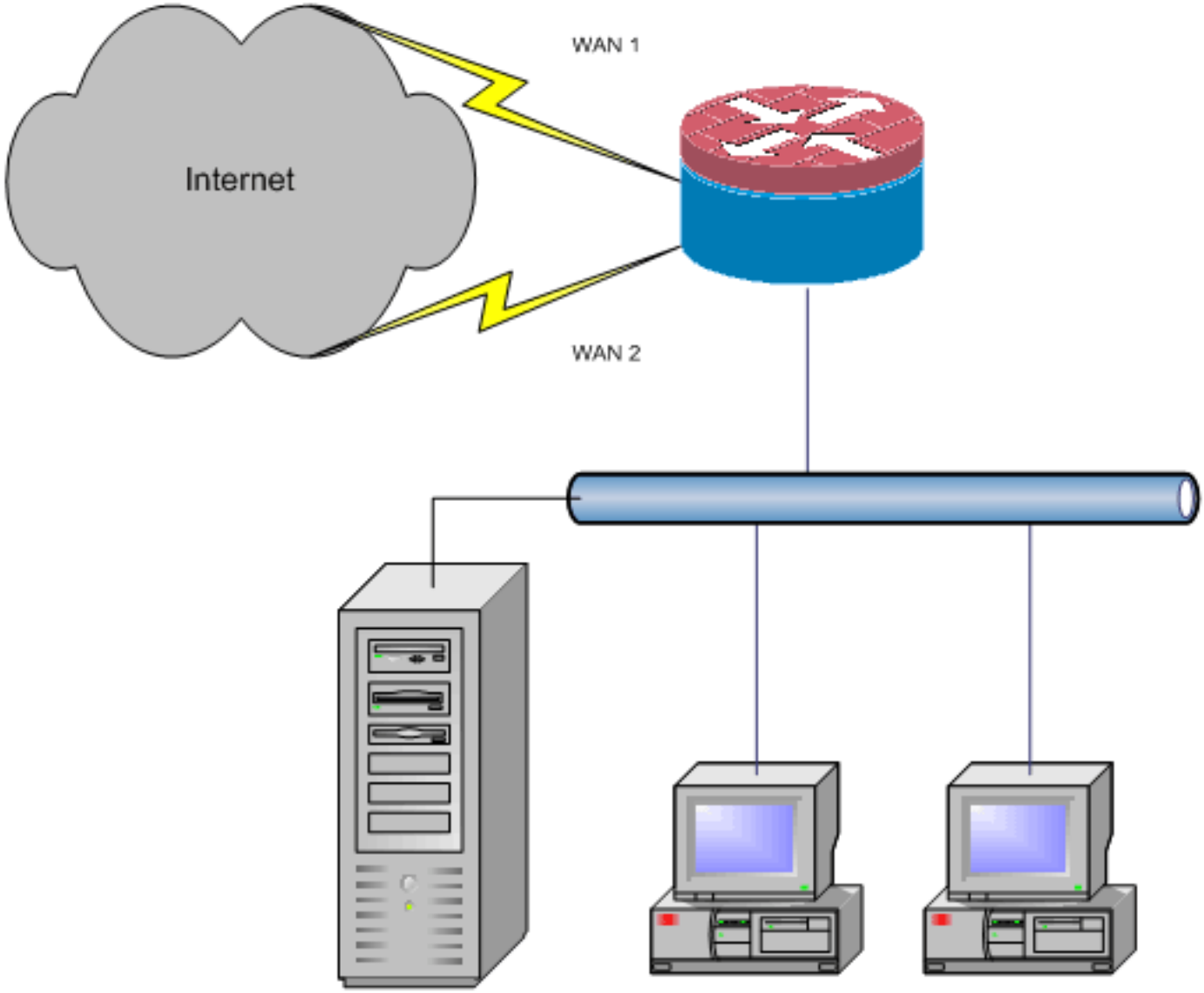
Équilibrage de charge NAT IOS et pare-feu de stratégie basé sur la zone avec routage de périphérie optimisé pour deux connexions Internet

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Diagramme du réseau
Discussion de stratégie de Pare-feu
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document décrit une configuration pour qu'un routeur de Cisco IOS® connecte un réseau à l'Internet au Traduction d'adresses de réseau (NAT) par l'intermédiaire de deux connexions ISP. Le 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. Au cas où une des connexions deviendrait inutilisable, le Suivi d'objets, un composant d'Optimized Edge Routing (OER), peut être utilisé pour désactiver l'artère jusqu'à ce que la connexion devienne disponible de nouveau, qui assure la Disponibilité de réseau malgré l'instabilité ou le manque de fiabilité d'une connexion Internet.



Ce document décrit des configurations supplémentaires pour appliquer le Pare-feu basé sur zone de stratégie de Cisco IOS 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 suppose que vous déjà entretenez des relations de LAN et WAN qui fonctionnent et ne fournissez 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. Par conséquent, il n'y a aucune manière de préférer une connexion plus desirable au-dessus d'une connexion moins-desirable.

Ce document décrit comment configurer l'OER afin d'activer ou désactiver l'un ou l'autre de routage en fonction d'Internet sur l'accessibilité des serveurs DNS de l'ISP. Vous devez identifier les hôtes spécifiques qui sont accessibles par l'intermédiaire seulement d'un des connexions ISP et ne pourraient pas être disponibles si cette connexion ISP n'est pas disponible.

Composants utilisés

Cette configuration a été développée avec un routeur de Cisco 1811 qui exécute le logiciel de Services IP avancé par 12.4(15)T2. Si une version de logiciel différente est utilisée, quelques caractéristiques peuvent ne pas être disponibles, ou les commandes de configuration pourraient différer de ceux affichés dans ce document. Les configurations semblables devraient être disponibles 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

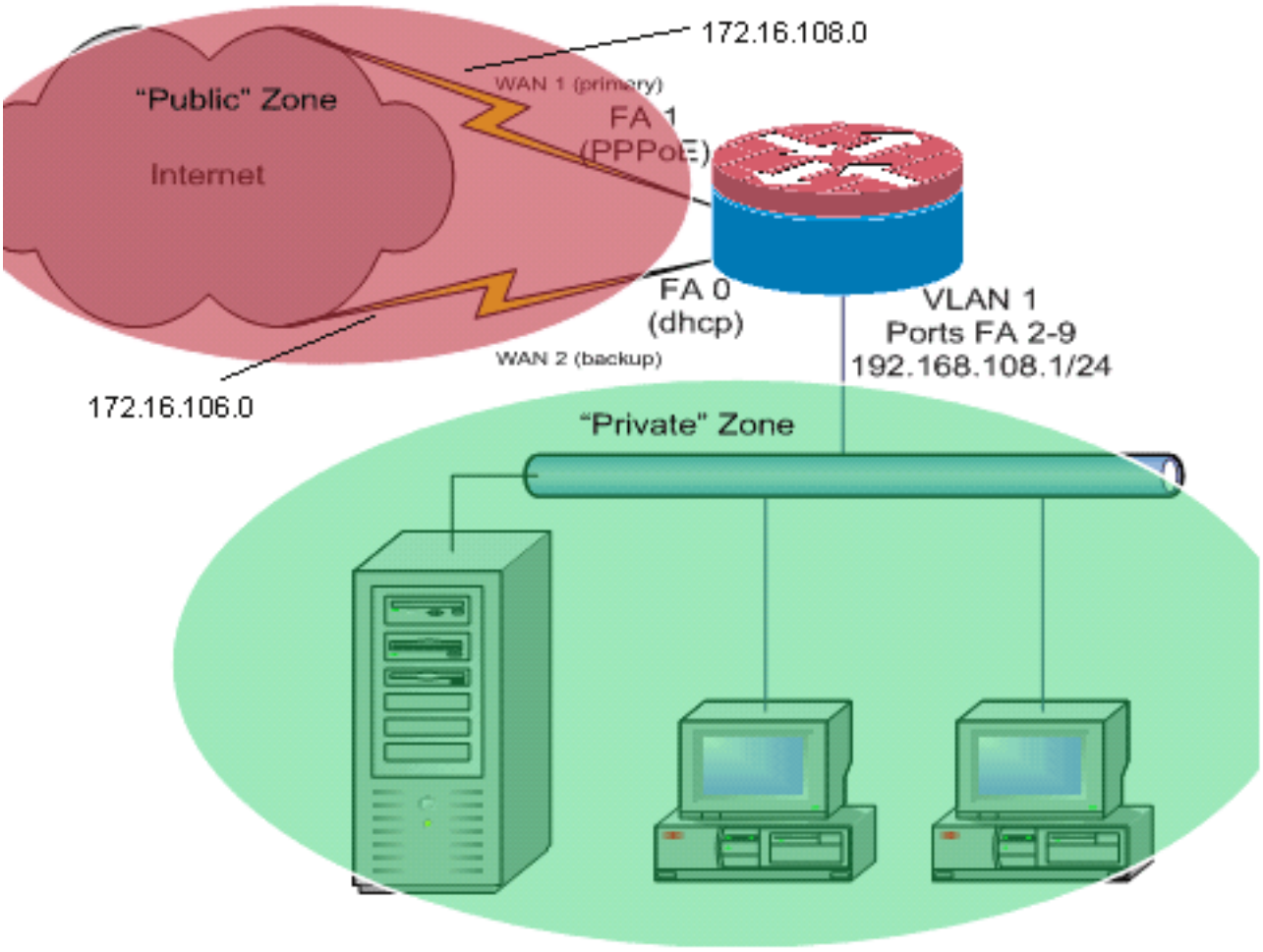
Vous pourriez devoir ajouter le routage basé sur la politique pour que le trafic spécifique soit sûr qu'il utilise toujours une connexion ISP. Les exemples du trafic qui pourraient exiger ce comportement incluent les combinés téléphoniques de clients vpn, VoIP d'IPsec, et n'importe quel autre trafic qui devrait toujours utiliser seulement un des possibilités de connexion ISP de préférer la même adresse IP, vitesse supérieure, ou de diminuer la latence sur la connexion.

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cet exemple de configuration, comme illustré dans le schéma de réseau, 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, à moins que le Suivi d'objets et l'Optimized Edge Routing (OER) et/ou le routage basé sur la politique doive être utilisé avec une connexion Internet DHCP-assignée. Dans des ces cas, il peut être très difficile de définir un routeur du prochain saut pour le routage ou l'OER de stratégie.

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 correspondantes pour les deux transferts de FTP actif et passif. N'importe quel trafic de l'application complexe (par exemple, signalisation VoIP et medias) qui n'est pas manipulé par cette stratégie de base fonctionnera vraisemblablement 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. Vous devez construire des configurations de politique supplémentaires de Pare-feu pour faciliter le trafic supplémentaire qui n'est pas traité par cette configuration de base.

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

Configuration CLI

Configuration CLI de Cisco IOS

```
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
```

Cheminement d'artère DHCP-assigné par utilisation :

Configuration CLI de Cisco IOS
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

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 externes.`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** - 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 les hôtes de privé-zone et les hôtes de public-zone. Cette commande fournit la vérification que le trafic sur les hôtes internes sont examinés comme les hôtes communiquent avec des services dans la zone de titre externe.

Dépannez

Vérifiez ces éléments si les connexions ne fonctionnent pas après que vous configuriez le routeur Cisco IOS avec NAT :

- 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.
- Si vous utilisez l'artère dépistant, vérifiez l'état de l'artère dépistant afin de s'assurer que les connexions Internet sont disponibles.
- La stratégie de Pare-feu reflète exactement la nature du trafic que vous souhaitez permettre par le routeur.

Informations connexes

- Cisco IOS Firewall
- Référence de commandes de Services d'adressage IP de Cisco IOS - Commandes NAT
- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Guide de configuration d'Optimized Edge Routing de Cisco IOS, version 12.4T
- Support et documentation techniques - Cisco Systems