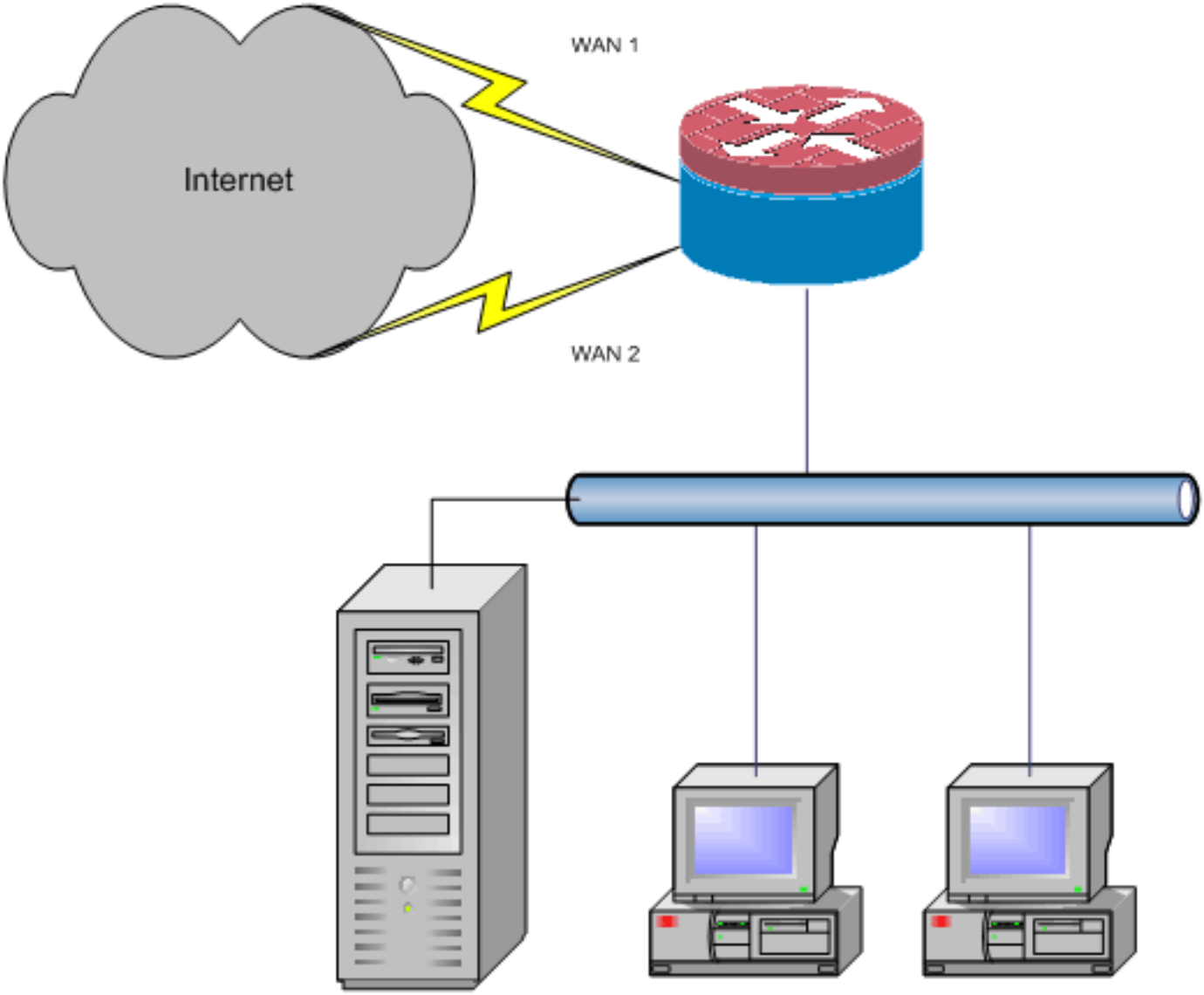
# Configuration de Cisco IOS NAT pour deux connexions ISP avec OER

## Contenu



## Introduction

Ce document décrit la configuration d'un routeur Cisco IOS® pour connecter un réseau à Internet avec la traduction d'adresses de réseau (NAT) via deux connexions ISP. La fonction NAT de 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. Si l'une des connexions devient inutilisable, le suivi d'objets, un composant du routage de périphérie optimisé (OER), peut être utilisé pour désactiver la route jusqu'à ce que la connexion soit à nouveau disponible, ce qui garantit la disponibilité du réseau malgré l'instabilité ou le manque de fiabilité d'une connexion Internet.




Ce document décrit des configurations supplémentaires pour appliquer le pare-feu de stratégie basé sur les zones Cisco IOS afin d'ajouter une fonctionnalité d'inspection dynamique pour augmenter la protection de base du réseau fournie par NAT.

# Conditions préalables

## Conditions requises

Ce document suppose que vous avez déjà des connexions LAN et WAN qui fonctionnent 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. Par conséquent, il n'y a aucun moyen de préférer une connexion plus souhaitable à une connexion moins souhaitable.

Ce document décrit comment configurer OER afin d'activer ou de désactiver l'une ou l'autre route Internet en fonction de l'accessibilité des serveurs DNS du FAI. Vous devez identifier des hôtes spécifiques qui sont accessibles via une seule des connexions ISP et qui pourraient ne pas être disponibles si cette connexion ISP n'est pas disponible.

## Components Used

Cette configuration a été développée avec un routeur Cisco 1811 qui exécute le logiciel Advanced IP Services 12.4(15)T2. Si une autre version du logiciel est utilisée, certaines fonctionnalités peuvent ne pas être disponibles ou les commandes de configuration peuvent différer de celles présentées dans ce document. Des configurations similaires doivent être disponibles 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

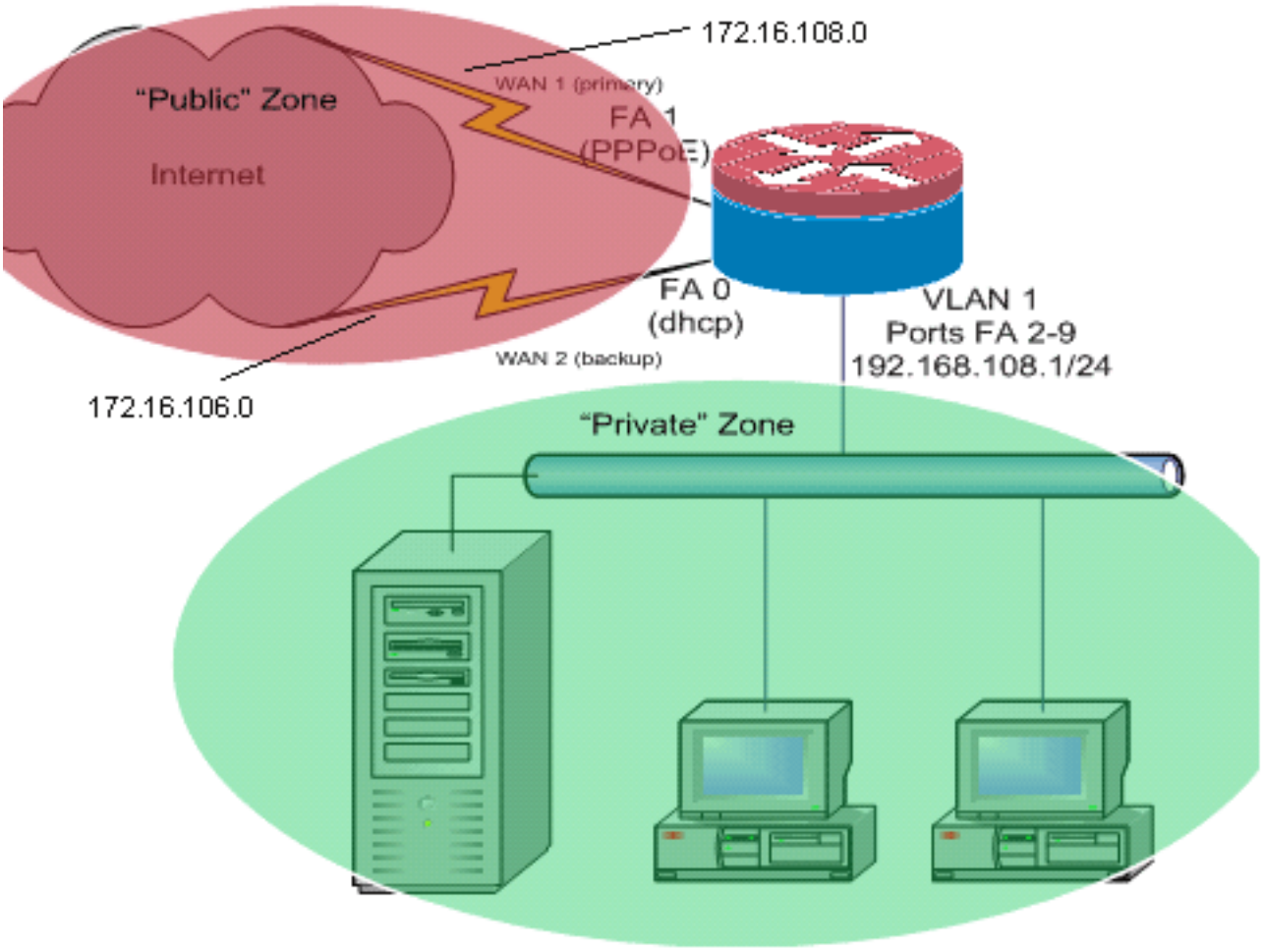
Vous devrez peut-être ajouter un routage basé sur des stratégies pour un trafic spécifique afin de vous assurer qu'il utilise toujours une connexion ISP. Les clients VPN IPsec, les combinés VoIP et tout autre trafic qui doit toujours utiliser une seule des options de connexion ISP pour préférer la même adresse IP, une vitesse supérieure ou une latence inférieure à la connexion sont des exemples de trafic qui peuvent nécessiter ce comportement.

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.

### Diagramme du réseau

Ce document utilise la configuration réseau suivante :




Cet exemple de configuration, illustré dans le schéma de réseau, 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 aucun impact particulier sur la configuration, à moins que le suivi d'objet et le routage de périphérie optimisé (OER) et/ou le routage basé sur des stratégies ne soient utilisés avec une connexion Internet attribuée par DHCP. Dans ces cas, il peut être très difficile de définir un routeur de tronçon suivant pour le routage de stratégie ou OER.

## 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 correspondant pour les transferts FTP actifs et passifs. Tout trafic d'application complexe (par exemple, signalisation VoIP et support) qui n'est pas géré par cette stratégie de base fonctionnera 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. Vous devez construire des configurations de stratégie de pare-feu supplémentaires pour prendre en charge un trafic supplémentaire qui n'est pas géré par cette configuration de base.

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.

### Configuration CLI

## Configuration de l'interface 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
```

**Utilisez le suivi de route attribué par dhcp :**

**Configuration de l'interface 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
```

# 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 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
```

- **show policy-map type inspect zone-pair sessions** - Affiche l'activité d'inspection de pare-feu entre les hôtes de zone privée et 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

Vérifiez ces éléments si les connexions ne fonctionnent pas après avoir configuré 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 le suivi de route, vérifiez l'état du suivi de route afin de vous assurer que les connexions Internet sont disponibles.
- La politique de pare-feu reflète fidèlement la nature du trafic que vous souhaitez autoriser via le routeur.

# Informations connexes

- Cisco IOS Firewall
- Référence des commandes des services d'adressage IP Cisco IOS - Commandes NAT
- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Guide de configuration du routage de périphérie optimisé Cisco IOS, version 12.4T
- Support et documentation techniques - Cisco Systems