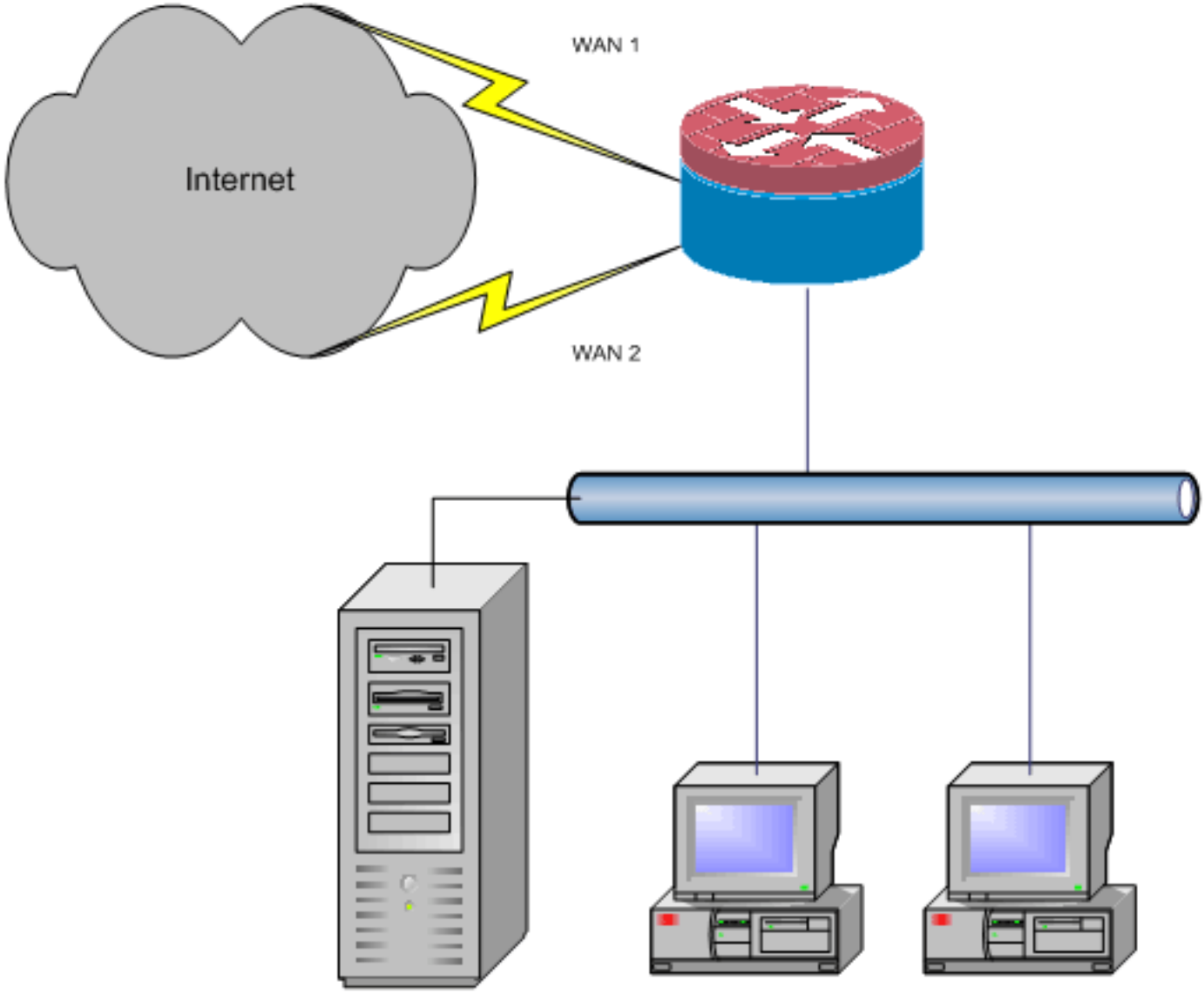
Configurazione di Cisco IOS NAT per due connessioni ISP con OER

Sommario

Introduzione

In questo documento viene descritta la configurazione di un router Cisco IOS® per connettere una rete a Internet con Network Address Translation (NAT) tramite due connessioni ISP. Cisco IOS NAT può distribuire le connessioni TCP e le sessioni UDP successive su più connessioni di rete se sono disponibili route uguali per una determinata destinazione. Nel caso in cui una delle connessioni diventi inutilizzabile, è possibile disattivare il tracciamento degli oggetti, un componente di Optimized Edge Routing (OER), fino a quando la connessione non diventa nuovamente disponibile, in modo da garantire la disponibilità della rete indipendentemente dall'instabilità o dall'inaffidabilità di una connessione Internet.



Questo documento descrive altre configurazioni per applicare Cisco IOS Zone-Based Policy Firewall per aggiungere funzionalità di ispezione con stato per aumentare la protezione di rete base fornita da NAT.

Prerequisiti

Requisiti

in questo documento si presume che le connessioni LAN e WAN funzionino già e che non vengano fornite informazioni di configurazione o risoluzione dei problemi per stabilire la connettività iniziale.

Questo documento non descrive un modo per distinguere tra i percorsi. Pertanto, non è possibile preferire una connessione più desiderabile a una meno desiderabile.

In questo documento viene descritto come configurare OER in modo da abilitare o disabilitare la route Internet in base alla raggiungibilità dei server DNS dell'ISP. È necessario identificare gli host specifici raggiungibili tramite una sola connessione ISP e che potrebbero non essere disponibili se tale connessione non è disponibile.

Componenti usati

Questa configurazione è stata sviluppata con un router Cisco 1811 con software 12.4(15)T2 Advanced IP Services. Se si utilizza una versione software diversa, alcune funzionalità potrebbero non essere disponibili o i comandi di configurazione potrebbero essere diversi da quelli mostrati in questo documento. Configurazioni simili dovrebbero essere disponibili su tutte le piattaforme di router Cisco IOS, anche se la configurazione dell'interfaccia potrebbe variare tra le diverse piattaforme.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

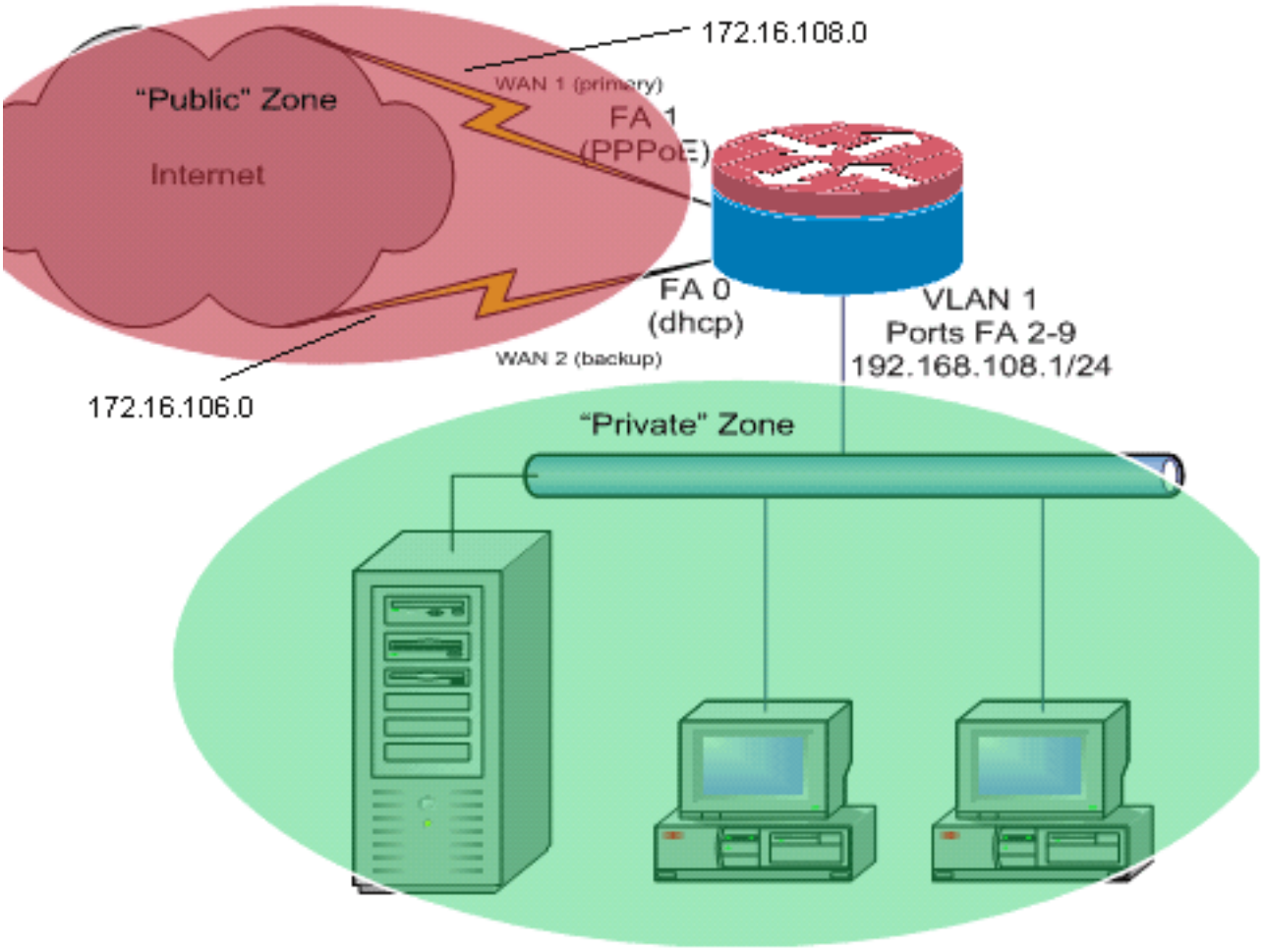
Potrebbe essere necessario aggiungere il routing basato su criteri per il traffico specifico per assicurarsi che utilizzi sempre una connessione ISP. Esempi di traffico che potrebbe richiedere questo comportamento includono i client VPN IPSec, i telefoni VoIP e qualsiasi altro traffico che deve sempre utilizzare solo una delle opzioni di connessione ISP per preferire lo stesso indirizzo IP, una velocità maggiore o una latenza inferiore sulla connessione.

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



L'esempio di configurazione riportato di seguito, come mostrato nel diagramma di rete, descrive un router di accesso che utilizza una connessione IP configurata con DHCP a un ISP (come mostrato da Fast Ethernet 0) e una connessione PPPoE sull'altra connessione ISP. I tipi di connessione non hanno un impatto particolare sulla configurazione, a meno che non si desideri utilizzare il tracciamento degli oggetti, il routing ottimizzato sul perimetro (OER) e/o il routing basato su criteri con una connessione Internet assegnata a DHCP. In questi casi, potrebbe essere molto difficile definire un router dell'hop successivo per il routing delle policy o il sistema OER.

Discussione sui criteri firewall

In questo esempio di configurazione viene descritto un criterio firewall che consente semplici connessioni TCP, UDP e ICMP dall'area di sicurezza "interna" all'area di sicurezza "esterna" e supporta le connessioni FTP in uscita e il traffico di dati corrispondente per i trasferimenti FTP attivi e passivi. Qualsiasi traffico di applicazioni complesso (ad esempio, segnalazione VoIP e supporti) che non viene gestito da questa policy di base probabilmente funzionerà con funzionalità ridotte o potrebbe fallire completamente. Questo criterio firewall blocca tutte le connessioni dall'area di sicurezza "pubblica" alla zona "privata", incluse tutte le connessioni ospitate dall'inoltro della porta NAT. È necessario creare ulteriori configurazioni dei criteri firewall per gestire il traffico aggiuntivo non gestito da questa configurazione di base.

Per domande sulla progettazione e la configurazione dei criteri di Firewall criteri basati sulle zone, fare riferimento alla Guida alla progettazione e alla configurazione di Firewall criteri basati sulle zone.

Configurazione CLI

Configurazione CLI di 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

Utilizza tracciabilità route assegnata da dhcp:

Configurazione CLI di 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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show ip nat translation**: visualizza l'attività NAT tra gli host interni NAT e gli host esterni NAT. Questo comando verifica che gli host interni vengano convertiti in entrambi gli indirizzi esterni NAT.

```
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**: verifica che siano disponibili più route a Internet.

```
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**: visualizza l'attività di ispezione del firewall tra gli host delle zone private e gli host delle zone pubbliche. Questo comando verifica che il traffico sugli host interni venga ispezionato mentre gli host comunicano con i servizi nell'area di sicurezza esterna.

Risoluzione dei problemi

Verificare questi elementi se le connessioni non funzionano dopo aver configurato il router Cisco IOS con NAT:

- Il protocollo NAT viene applicato correttamente sulle interfacce esterna e interna.
- La configurazione NAT è completa e gli ACL riflettono il traffico che deve essere NAT.
- Sono disponibili più percorsi verso Internet/WAN.
- Se si utilizza la traccia del percorso, controllare lo stato della traccia per verificare che le connessioni Internet siano disponibili.
- I criteri del firewall riflettono accuratamente la natura del traffico che si desidera consentire attraverso il router.

Informazioni correlate

- Cisco IOS Firewall
- Guida di riferimento ai comandi di Cisco IOS IP Addressing Services - Comandi NAT
- Guida alla progettazione e all'applicazione di firewall per i criteri basati su zone
- Guida alla configurazione di Cisco IOS Optimized Edge Routing, versione 12.4T
- Documentazione e supporto tecnico – Cisco Systems