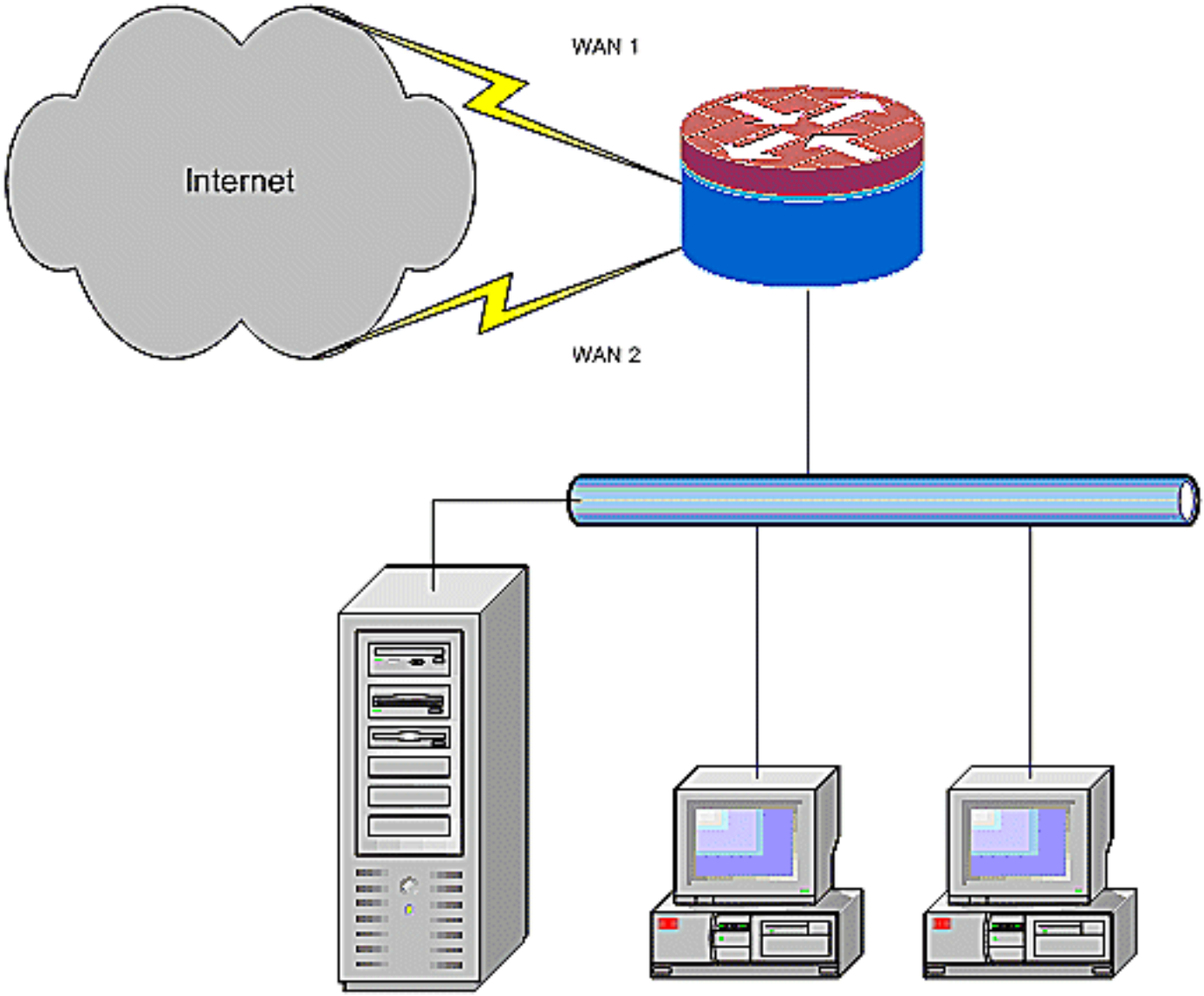
Load balancing IOS NAT con firewall dei criteri basato su zone per due connessioni ISP

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per un router Cisco IOS® che consente di connettere una rete a Internet con Network Address Translation (NAT) tramite due connessioni ISP. Il software Cisco IOS NAT può distribuire le successive connessioni TCP e sessioni UDP su più connessioni di rete se sono disponibili route uguali per una determinata destinazione.



Questo documento descrive la configurazione aggiuntiva per applicare Cisco IOS Zone-Based Policy Firewall (ZFW) per aggiungere funzionalità di ispezione con stato e aumentare la protezione di rete base fornita da NAT.

Prerequisiti

Requisiti

in questo documento si presume che l'utente lavori con le connessioni LAN e WAN e non fornisce informazioni di configurazione o risoluzione dei problemi per stabilire la connettività iniziale. Questo documento non descrive un modo per distinguere tra i percorsi, quindi non c'è modo di preferire un collegamento più desiderabile rispetto a uno meno desiderabile.

Componenti usati

Per la stesura del documento, sono stati usati router Cisco serie 1811 con software 12.4(15)T3 Advanced IP Services. Se si utilizza una versione software diversa, alcune funzionalità non sono

disponibili o i comandi di configurazione possono essere diversi da quelli mostrati in questo documento. Una configurazione simile è disponibile su tutte le piattaforme di router Cisco IOS, anche se la configurazione dell'interfaccia probabilmente varia 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

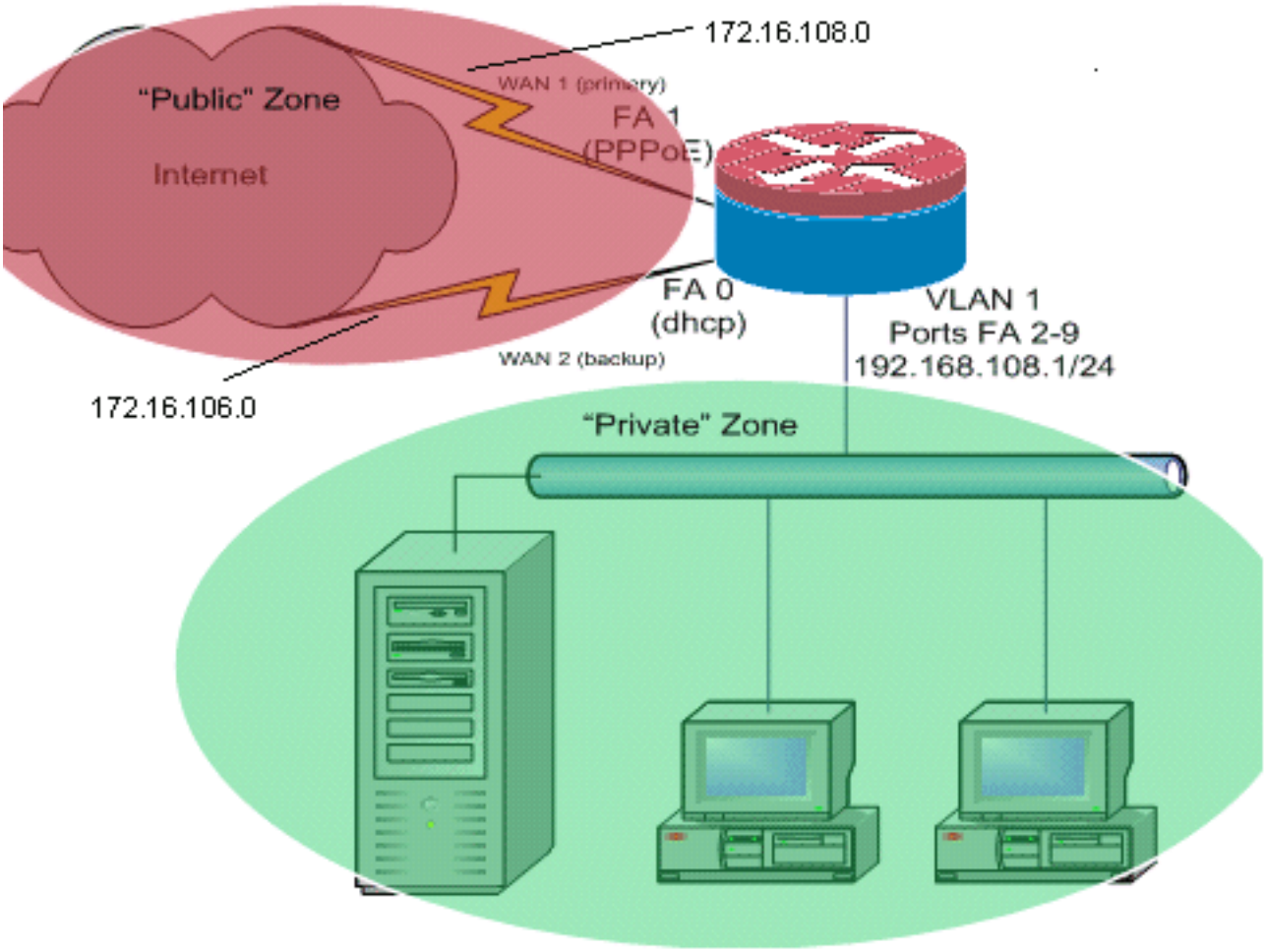
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

Ènecessario aggiungere il routing basato su criteri per il traffico specifico per essere certi che utilizzi sempre una connessione ISP. Esempi di traffico che può richiedere questo comportamento includono i client VPN IPSec, il traffico di telefonia VoIP e qualsiasi altro traffico che utilizza solo una delle opzioni di connessione ISP per preferire lo stesso indirizzo IP, una velocità maggiore o una latenza inferiore sulla connessione.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nell'esempio di configurazione che segue viene descritto un router di accesso che utilizza una connessione IP configurata tramite 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, ma alcuni tipi di connessione possono ostacolare l'utilizzabilità della configurazione in scenari di errore specifici. Questo si verifica in particolare nei casi in cui viene utilizzata la connettività IP su un servizio WAN connesso via Ethernet, ad esempio un modem via cavo o i servizi DSL, in cui un dispositivo aggiuntivo termina la connettività WAN e fornisce il collegamento Ethernet al router Cisco IOS. Nei casi in cui viene applicato un indirizzo IP statico, in contrapposizione agli indirizzi assegnati dal DHCP o al PPPoE, e si verifica un errore della WAN, in modo che la porta Ethernet conservi ancora il collegamento Ethernet al dispositivo di connettività WAN, il router continua a tentare di bilanciare il carico di connettività su entrambe le connessioni WAN, buona e cattiva. Se la distribuzione richiede la rimozione delle route inattive dal bilanciamento del carico, fare riferimento alla configurazione fornita in Cisco IOS NAT Load-Balancing e Zone-Based Policy Firewall con Optimized Edge Routing per due connessioni Internet che descrive l'aggiunta di Optimized Edge Routing per monitorare la validità della route.

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 equivalente per i trasferimenti FTP attivi e passivi. Tutto il traffico di applicazioni complesse, ad esempio la segnalazione VoIP e i supporti, che non viene gestito da questa policy di base, probabilmente funziona con funzionalità ridotte o può fallire completamente. Questo criterio firewall blocca tutte le connessioni dall'area di sicurezza "pubblica" alla zona "privata", incluse tutte le connessioni supportate dall'inoltro della porta NAT. Se necessario, è necessario modificare i criteri di ispezione del firewall in modo che riflettano il

profilo dell'applicazione e i criteri di protezione.

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

Configurazioni

Nel documento vengono usate queste configurazioni:

Configurazione

```
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
```

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 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**: 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 degli host interni venga ispezionato quando gli host comunicano con i servizi nell'area di sicurezza "esterna".

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Dopo aver configurato il router Cisco IOS con NAT, se le connessioni non funzionano, verificare quanto segue:

- 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.
- I criteri del firewall riflettono accuratamente la natura del traffico che si desidera consentire attraverso il router.

Informazioni correlate

- Supporto alla tecnologia vocale
- Supporto ai prodotti voce e Unified Communications
- Risoluzione dei problemi di Cisco IP Telephony
- Guida alla progettazione e all'applicazione di firewall per i criteri basati su zone
- Documentazione e supporto tecnico – Cisco Systems