

IOS NAT Load–Balancing and Zone–Based Policy Firewall with Optimized Edge Routing For Two Internet Connections

Document ID: 100568

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Network Diagram

- Firewall Policy Discussion

Verify

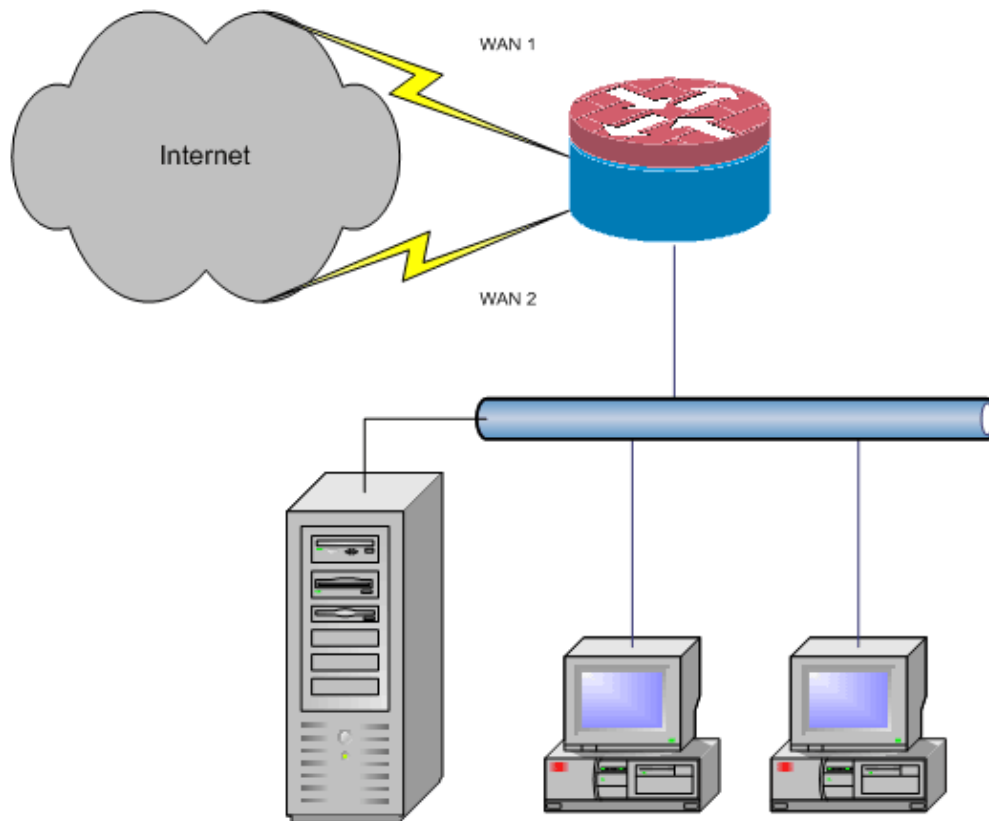
Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes a configuration for a Cisco IOS[®] router to connect a network to the Internet with Network Address Translation (NAT) via two ISP connections. Cisco IOS NAT can distribute subsequent TCP connections and UDP sessions over multiple network connections if equal–cost routes to a given destination are available. In the event that one of the connections becomes unusable, object–tracking, a component of Optimized Edge Routing (OER), can be used to deactivate the route until the connection becomes available again, which ensures network availability inspite of instability or unreliability of an Internet connection.



This document describes additional configurations to apply Cisco IOS Zone-Based Policy Firewall to add stateful inspection capability to augment the basic network protection provided by NAT.

Prerequisites

Requirements

This document assumes you already have LAN and WAN connections that work and does not provide configuration or troubleshooting background to establish initial connectivity.

This document does not describe a way to differentiate between the routes. Therefore, there is no way to prefer a more desirable connection over a less-desirable connection.

This document describes how to configure OER in order to enable or disable either Internet route-based on reachability of the ISP's DNS servers. You need to identify specific hosts that are reachable via only one of the ISP connections and might not be available if that ISP connection is not available.

Components Used

This configuration was developed with a Cisco 1811 router that runs 12.4(15)T2 Advanced IP Services software. If a different software version is used, some features may not be available, or the configuration commands might differ from those shown in this document. Similar configurations should be available on all Cisco IOS router platforms, although the interface configuration will likely vary between different platforms.

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

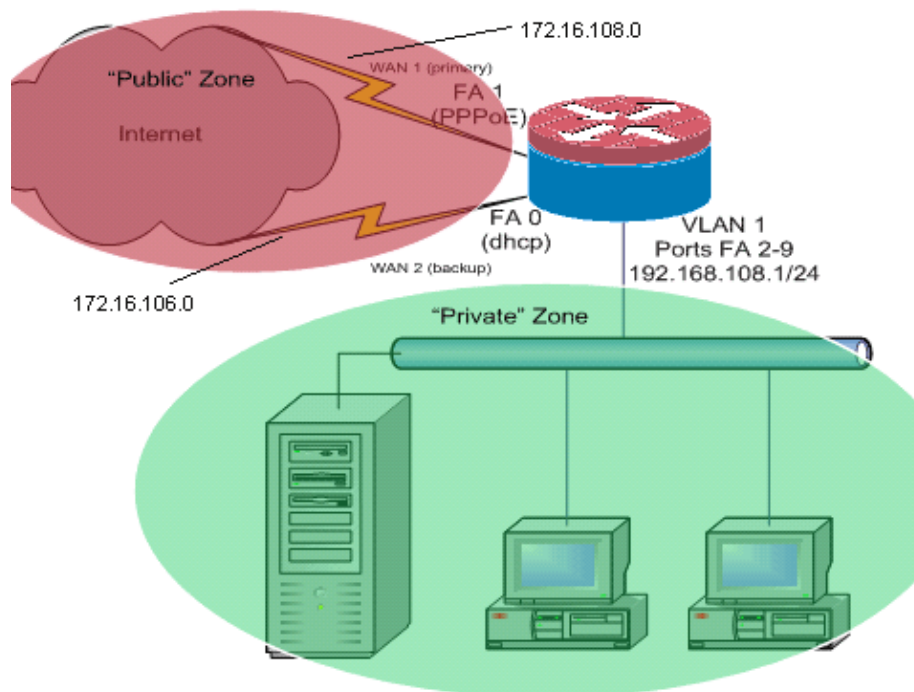
You might need to add policy-based routing for specific traffic to be sure that it always uses one ISP connection. Examples of traffic that might require this behavior include IPsec VPN clients, VoIP handsets, and any other traffic that should always use only one of the ISP connection options to prefer the same IP address, higher speed, or lower latency on the connection.

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



This configuration example, as illustrated in the network diagram, describes an access router that uses a DHCP-configured IP connection to one ISP (as shown by FastEthernet 0) and a PPPoE connection over the other ISP connection. The connection types have no particular impact on the configuration, unless object-tracking and Optimized Edge Routing (OER) and/or policy-based routing is to be used with a DHCP-assigned Internet connection. In these cases, it may be very difficult to define a next-hop router for policy routing or OER.

Firewall Policy Discussion

This configuration example describes a firewall policy that allows simple TCP, UDP, and ICMP connections from the inside security zone to the outside security zone and accommodates outbound FTP connections and the corresponding data traffic for both active and passive FTP transfers. Any complex application traffic

(for example, VoIP signaling and media) that is not handled by this basic policy will likely operate with diminished capability, or may fail entirely. This firewall policy blocks all connections from the public security zone to the private zone, which includes all connections that are accommodated by NAT port forwarding. You must construct additional firewall policy configurations to accommodate additional traffic that is not handled by this basic configuration.

If you have questions on Zone-Based Policy Firewall policy design and configuration, refer to Zone-Based Policy Firewall Design and Application Guide.

CLI Configuration

```

Cisco IOS CLI Configuration

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

```

Use dhcp-assigned route tracking:

Cisco IOS CLI Configuration
<pre> 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 </pre>

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ip nat translation** Displays NAT activity between NAT inside hosts and NAT outside hosts. This command provides verification that inside hosts are being translated to both NAT outside addresses.

```
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** Verifies that multiple routes to the Internet are available.

```
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** Displays firewall inspection activity between private-zone hosts and public-zone hosts. This command provides verification that the traffic on the inside hosts are inspected as hosts communicate with services in the outside security zone.

Troubleshoot

Verify these items if the connections do not work after you configure the Cisco IOS router with NAT:

- NAT is applied appropriately on outside and inside interfaces.
- NAT configuration is complete, and ACLs reflect the traffic that must be NATed.
- Multiple routes to the Internet/WAN are available.
- If you use route tracking, check the state of the route tracking in order to ensure the Internet connections are available.
- The firewall policy accurately reflects the nature of the traffic that you wish to allow through the router.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security

Security: Intrusion Detection [Systems]

Security: AAA

Security: General

Security: Firewalling

Related Information

- [Cisco IOS Firewall](#)
- [Cisco IOS 12.4 NAT configuration Reference](#)
- [Zone–Based Policy Firewall Design and Application Guide](#)
- [Cisco IOS Optimized Edge Routing Configuration Guide, Release 12.4T](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 15, 2008

Document ID: 100568
