IOS NAT Load–Balancing with Zone–Based Policy Firewall for Two ISP Connections

Document ID: 100657

Contents

Introduction

This document provides a sample configuration for a Cisco IOS® router to connect a network to the Internet with Network Address Translation (NAT) through two ISP connections. The Cisco IOS software NAT can distribute subsequent TCP connections and UDP sessions over multiple network connections if equal–cost routes to a given destination are available.
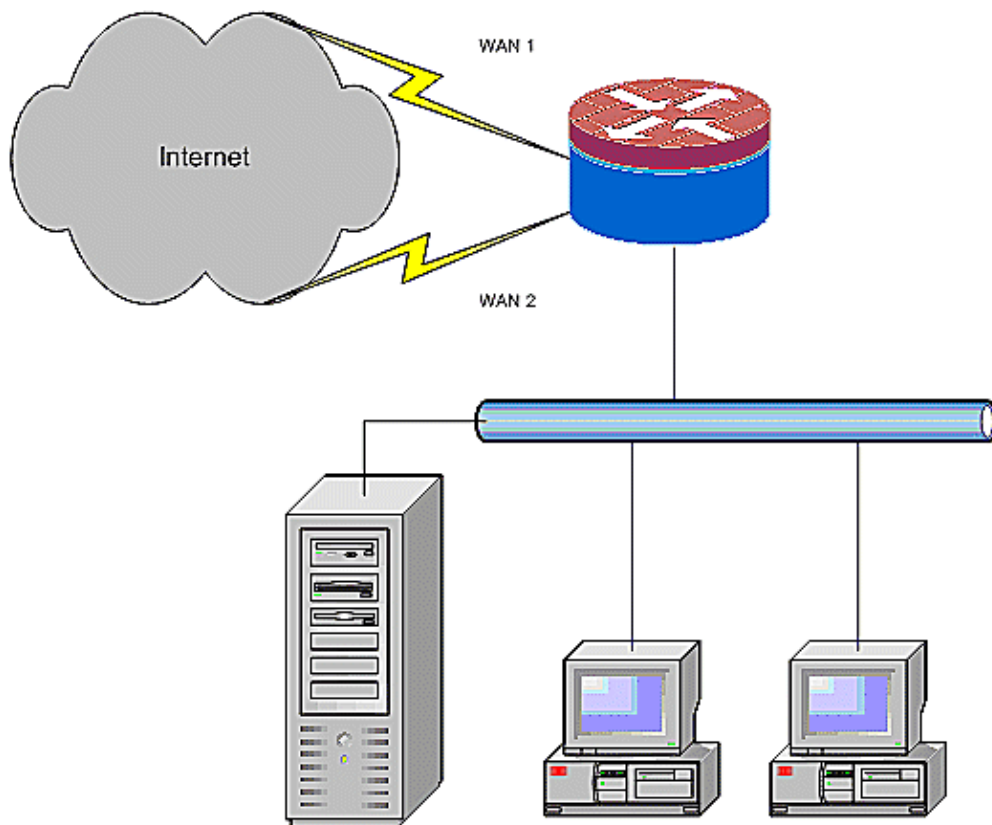
This document describes additional configuration to apply the Cisco IOS Zone−Based Policy Firewall (ZFW) to add stateful inspection capability to augment the basic network protection provided by NAT.

Prerequisites

Requirements

This document assumes you work with LAN and WAN connections and does not provide configuration or troubleshooting background to establish initial connectivity. This document does not describe a way to differentiate between the routes, so there is no way to prefer a more desirable connection over a less desirable connection.

Components Used

The information in this document is based on the Cisco Series 1811 Router with 12.4(15)T3 Advanced IP Services software. If a different software version is used, some features are not available, or the configuration commands can differ from those shown in this document. Similar configuration is available on all Cisco IOS router platforms, although the interface configuration likely varies 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.
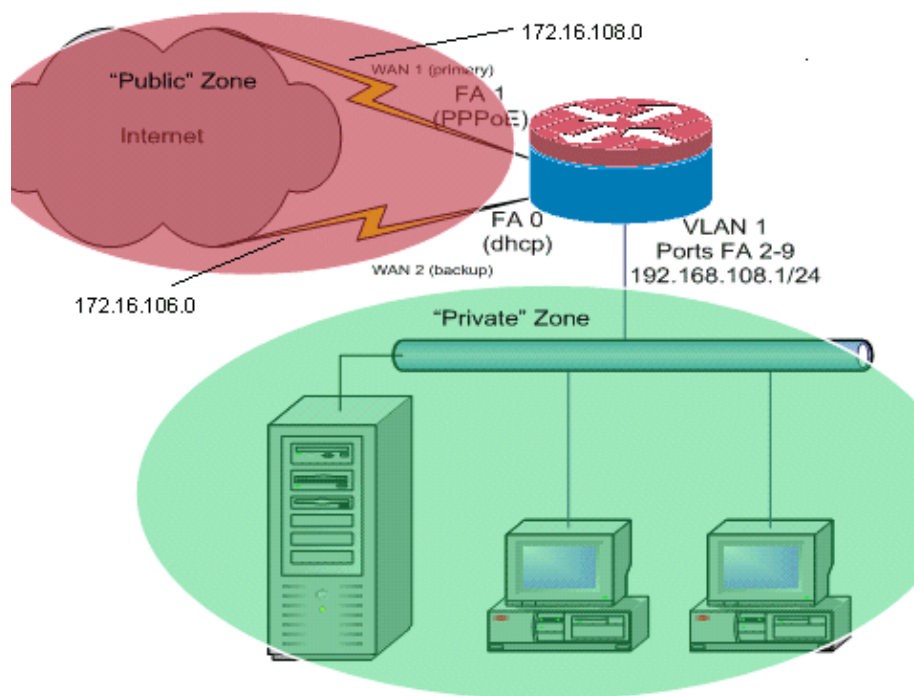
Configure

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.

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

Network Diagram

This document uses this network setup:

This configuration example 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, but some connections types can hinder the usability of this configuration in specific failure scenarios. This occurs particularly in cases where IP connectivity over an Ethernet−connected WAN service is used, for example, cable modem or DSL services where an additional device terminates the WAN connectivity and provides Ethernet hand−off to the Cisco IOS router. In cases where static IP addressing is applied, as opposed to DHCP−assigned addresses or PPPoE, and a WAN failure occurs, such that the Ethernet port still maintains Ethernet link to the WAN connectivity device, the router continues to attempt to load−balance connectivity across both the good and bad WAN connections. If your deployment requires that inactive routes be removed from load−balancing, refer to the configuration provided in Cisco IOS NAT Load−Balancing and Zone−Based Policy Firewall with Optimized Edge Routing For Two Internet Connections that describes the addition of Optimized Edge Routing to monitor route validity.

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 equivalent 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 likely operates with diminished capability or can 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. If necessary, you need to adjust the firewall inspection policy to reflect your application profile and security policy.

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

Configurations

This document uses these configurations:

Configuration

<pre>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
 	
</pre>

```
!--- 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
```

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 translated to both NAT outside addresses.

```
        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** 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 of inside hosts is inspected as hosts communicate with services in the outside security zone.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

After you configure the Cisco IOS router with NAT, if the connections do not work, be sure of these:

- 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.

- The firewall policy accurately reflects the nature of the traffic that you wish to allow through the router.

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Zone–Based Policy Firewall Design and Application Guide**
- **Technical Support & Documentation – Cisco Systems**

Updated: Aug 15, 2008   Document ID: 100657