Two−interface Router without NAT Using Cisco IOS Firewall Configuration

Document ID: 13892

Contents

Introduction

This sample configuration works for a very small office that connects directly to the Internet, with the assumption that Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP) and Web services are provided by a remote system run by the Internet Service Provider (ISP). There are no services on the inside network and only two interfaces. There is also no logging because there is no host available to provide logging services.

Since this configuration uses only input access lists, it does both anti−spoofing and traffic filtering with the same access list. This configuration only works for a two−port router. Ethernet 0 is the "inside" network. Serial 0 is a Frame Relay link to the ISP.

Refer to Two−Interface Router with NAT Cisco IOS Firewall Configuration in order to configure a two interface router with NAT using a Cisco IOS® Firewall.

Refer to Three−Interface Router without NAT Cisco IOS Firewall Configuration in order to configure a three interface router without NAT using a Cisco IOS Firewall.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document applies to these software and hardware versions:

- Cisco IOS® Software Release 12.2(15)T13, supported from Cisco IOS Software Release 11.3.3.T
- Cisco 2611 router

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.

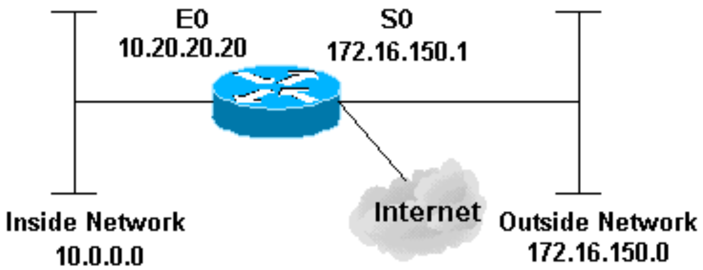
Configure

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.

Network Diagram

This document uses this network setup:



Configuration

This document uses this configuration:

2514 Router

```
version 12.2
!
service password-encryption
no service udp-small-servers
no service tcp-small-servers
no cdp run
!
hostname cbac-cisco
!
no ip source-route
!
enable secret 5 $1$FrMn$wBu0Xgv/Igy5Y.DarCmrm/
!
username cisco privilege 15 password 7 0822455D0A16
no ip source-route
ip domain-name cisco.com
ip name-server 172.16.150.5
!

!--- Set up inspection list "myfw".
!--- Inspect for the protocols that actually get used.

!
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!
interface Ethernet0/0
description Cisco Ethernet RTP
 ip address 10.20.20.20 255.255.255.0
 no ip directed-broadcast
 !

!--- Apply the access list in order to allow all legitimate traffic
 !--- from the inside network but prevent spoofing.

 !
 ip access-group 101 in
 !
 no ip proxy-arp
 !

!--- Apply inspection list "myfw" to Ethernet 0 inbound.
 !--- When conversations are initiated from the internal network
 !--- to the outside, this inspection list causes temporary additions
 !--- to the traffic allowed in by serial interface 0 acl 111 when
 !--- traffic returns in response to the initiation.

 !
 ip inspect myfw in
 no ip route-cache
 !
 no cdp enable
 !
 interface Serial0/0
 description Cisco FR
 ip address 172.16.150.1 255.255.255.0
 encapsulation frame-relay IETF
 no ip route-cache
 no arp frame-relay
 bandwidth 56
 service-module 56 clock source line
 service-module 56k network-type dds
 frame-relay lmi-type ansi
 !

!--- Access list 111 allows some ICMP traffic and administrative Telnet,
 !--- and does anti-spoofing. There is no inspection on Serial 0.
 !--- However, the inspection on the Ethernet interface adds temporary entries
 !--- to this list when hosts on the internal network make connections
 !--- out through the Frame Relay.

 !
 ip access-group 111 in
 no ip directed-broadcast
 no ip route-cache
 bandwidth 56
 no cdp enable
 frame-relay interface-dlci 16
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 Serial0
!

!--- Access list 20 is used to control which network management stations
!--- can access through SNMP.

!
 access-list 20 permit 172.16.150.8
!

!--- The access list allows all legitimate traffic from the inside network
 !--- but prevents spoofing.

!
 access-list 101 permit tcp 172.16.150.0 0.0.0.255 any
 access-list 101 permit udp 172.16.150.0 0.0.0.255 any
 access-list 101 permit icmp 172.16.150.0 0.0.0.255 any

!--- This deny is the default.

 access-list 101 deny ip any any
 !

!--- Access list 111 controls what can come from the outside world
 !--- and it is anti-spoofing.

 !
 access-list 111 deny ip 127.0.0.0 0.255.255.255 any
 access-list 111 deny ip 172.16.150.0 0.0.0.255 any
!

!--- Perform an ICMP stuff first. There is some danger in these lists.
 !--- They are control packets, and allowing *any* packet opens
 !--- you up to some possible attacks. For example, teardrop-style
 !--- fragmentation attacks can come through this list.

!
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 administratively-prohibited
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 echo
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 echo-reply
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 packet-too-big
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 traceroute
 access-list 111 permit icmp any 172.16.150.0 0.0.0.255 unreachable
!

!--- Allow Telnet access from 10.11.11.0 corporate network administration people.

!
 access-list 111 permit tcp 10.11.11.0 0.0.0.255 host 172.16.150.1 eq telnet
!

!--- This deny is the default.

!
 access-list 111 deny ip any any
 !

!--- Apply access list 20 for SNMP process.

 !
```

```
snmp−server community secret RO 20
!
line con 0
exec−timeout 5 0
password 7 14191D1815023F2036
login local
line vty 0 4
exec−timeout 5 0
password 7 14191D1815023F2036
login local
length 35
end
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

After you configure the IOS Firewall router, if the connections do not work, ensure that you have enabled inspection with the **ip inspect (name defined) in or out** command on the interface. In this configuration, **ip inspect myfw in** is applied for the interface Ethernet0/0.

For these commands, along with other troubleshooting information, refer to Troubleshooting Authentication Proxy.

Note: Refer to Important Information on Debug Commands before you issue **debug** commands.

Related Information

- **IOS Firewall Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 20, 2007 Document ID: 13892