

Three–interface Router without NAT Cisco IOS Firewall Configuration

Document ID: 13893

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

Related Information

Introduction

This document provides an example of a typical configuration for a small business that is connected to the Internet and runs its own servers. The connection to the Internet is over a serial line. Ethernet 0 is connected to the internal network (a single LAN). Ethernet 1 is connected to a DMZ network, which has a single node used to provide services to the outside world. The ISP has assigned the company the netblock 192.168.27.0/24. This is equally split between the DMZ and the internal LAN with subnet mask 255.255.255.128. The basic policy is to:

- Allow users on the inside network to connect to any service on the public Internet.
- Allow anyone on the Internet to connect to the WWW, FTP, and Simple Mail Transfer Protocol (SMTP) services on the DMZ server, and to make Domain Name System (DNS) queries to it. This allows outside people to view company web pages, pick up files the company has posted for outside consumption, and send mail into the company.
- Allow inside users to connect to the POP service on the DMZ server (to pick up their mail) and to Telnet to it (to administer it).
- Not allow anything on the DMZ to initiate any connections, either to the private network or to the Internet.
- Audit all connections that cross the firewall to a SYSLOG server on the private net. Machines on the inside network use the DNS server on the DMZ. Input access lists are used on all interfaces in order to prevent spoofing. Output access lists are used to control what traffic can be sent to any given interface.

Refer to [Two–Interface Router without NAT Using Cisco IOS Firewall Configuration](#) in order to configure a two interface router without NAT using the Cisco IOS® Firewall.

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.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the software and hardware versions:

- Cisco IOS Software Release 12.2(15)T13 with firewall feature set
- Cisco 7204 VXR 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.

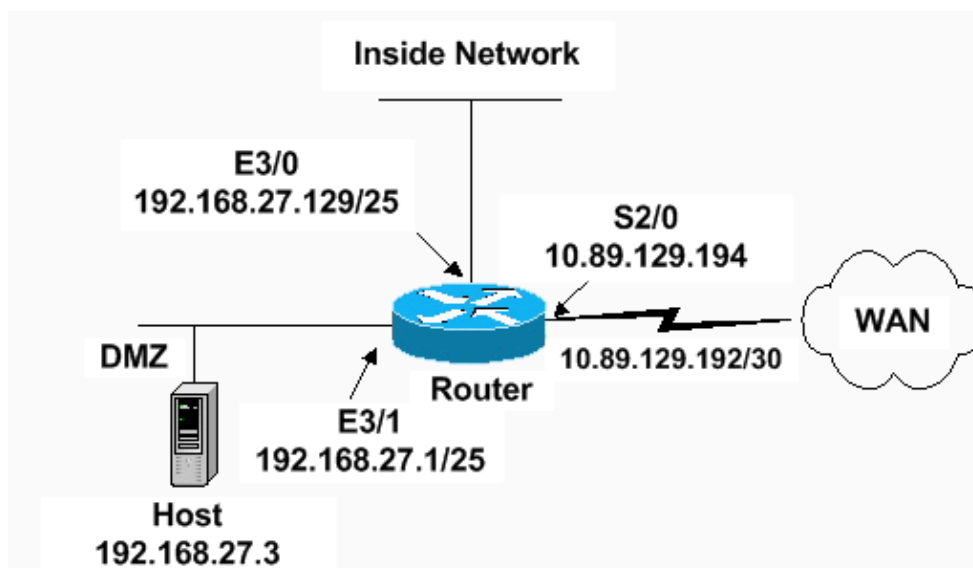
Configure

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:



Configurations

This document uses this configuration.

7204 VXR Router

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
logging queue-limit 100
enable secret 5 <something>
!
ip subnet-zero
ip cef
no ip domain lookup
!
ip inspect audit-trail
!

!--- Sets the length of time a TCP session
!--- is still managed after no activity.

!
ip inspect tcp idle-time 14400
!

!--- Sets the length of time a UDP session
!--- is still managed after no activity.

!
ip inspect udp idle-time 1800
!

!--- Sets the length of time a DNS name lookup session
!--- is still managed after no activity.

!
ip inspect dns-timeout 7
!

!--- Sets up inspection list "standard"
!--- to be used for inspection of inbound Ethernet 0
!--- and inbound serial (applied to both interfaces).

!
ip inspect name standard cuseeme
ip inspect name standard ftp
ip inspect name standard h323
ip inspect name standard http
ip inspect name standard rcmd
ip inspect name standard realaudio
ip inspect name standard smtp
ip inspect name standard sqlnet
ip inspect name standard streamworks
ip inspect name standard tcp
ip inspect name standard tftp
ip inspect name standard udp
ip inspect name standard vdolive
ip audit notify log
ip audit po max-events 100
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
```

```
interface ethernet 3/0
ip address 192.168.27.129 255.255.255.128
!
!---- Apply the access list to allow all legitimate
!---- traffic from the inside network and prevent spoofing.
!
ip access-group 101 in
!
!---- Apply inspection list "standard" for inspection
!---- of inbound Ethernet traffic. This inspection opens
!---- temporary entries on access lists 111 and 121.
!
ip inspect standard in
duplex full

interface ethernet 3/1
ip address 192.168.27.1 255.255.255.128
!
!---- Apply the access list to permit DMZ traffic (except spoofing)
!---- on the DMZ interface inbound. The DMZ is not permitted to initiate
!---- any outbound traffic except Internet Control Message Protocol (ICMP).
!
ip access-group 111 in
!
!---- Apply inspection list "standard" for inspection of outbound
!---- traffic from e1. This adds temporary entries on access list 111
!---- to allow return traffic, and protects servers in DMZ from
!---- distributed denial of service (DDoS) attacks.

ip inspect standard out
duplex full
!
interface serial 2/0
ip address 10.89.129.194 255.255.255.252

!---- Apply the access list to allow legitimate traffic.
!
ip access-group 121 in
serial restart_delay 0
!
ip classless
no ip http-server

!---- A syslog server is located at this address.

logging 192.168.27.131

!---- This command enables the logging of session
!---- information (addresses and bytes).

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

!
access-list 20 permit 192.168.27.5
```

```

!
!---- Use an access list to allow all legitimate traffic from
!---- the inside network and prevent spoofing. The inside
!---- network can only connect to the Telnet and POP3
!---- service of 192.168.27.3 on DMZ, and can ping (ICMP) to the DMZ.
!---- Additional entries can be added to permit SMTP, WWW, and
!---- so forth, if necessary. In addition, the inside network can
!---- connect to any service on the Internet.

!
access-list 101 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3
access-list 101 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq telnet
access-list 101 permit icmp 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127
access-list 101 deny ip 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127
access-list 101 permit ip 192.168.27.128 0.0.0.127 any
access-list 101 deny ip any any
!
!

!---- The access list permits ping (ICMP) from the DMZ and denies all
!---- traffic initiated from the DMZ. Inspection opens
!---- temporary entries to this list.

!
access-list 111 permit icmp 192.168.27.0 0.0.0.127 any
access-list 111 deny ip any any
!
!
!

!---- Access list 121 allows anyone on the Internet to connect to
!---- WWW, FTP, DNS, and SMTP services on the DMZ host. It also
!---- allows some ICMP traffic.

access-list 121 permit udp any host 192.168.27.3 eq domain
access-list 121 permit tcp any host 192.168.27.3 eq domain
access-list 121 permit tcp any host 192.168.27.3 eq www
access-list 121 permit tcp any host 192.168.27.3 eq ftp
access-list 121 permit tcp any host 192.168.27.3 eq smtp
access-list 121 permit icmp any 192.168.27.0 0.0.0.255 administratively-prohibited
access-list 121 permit icmp any 192.168.27.0 0.0.0.255 echo
access-list 121 permit icmp any 192.168.27.0 0.0.0.255 echo-reply
access-list 121 permit icmp any 192.168.27.0 0.0.0.255 packet-too-big
access-list 121 permit icmp any 192.169.27.0 0.0.0.255 time-exceeded
access-list 121 permit icmp any 192.168.27.0 0.0.0.255 traceroute
access-list 121 permit icmp any 192.168.27.0 0.0.0.255 unreachable
access-list 121 deny ip any any

!

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

!
snmp-server community secret RO 20
snmp-server enable traps tty
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper shutdown
!

```

```
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

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 access-list** Verifies the correct configuration of the access lists configured in the running-configuration.

```
Router#show access-list
Standard IP access list 20
  10 permit 192.168.27.5
Extended IP access list 101
  10 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3
  20 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq telnet
  30 permit icmp 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127
  40 deny ip 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127
  50 permit ip 192.168.27.128 0.0.0.127 any
  60 deny ip any any
Extended IP access list 111
  10 permit icmp 192.168.27.0 0.0.0.127 any
  20 deny ip any any (9 matches)
Extended IP access list 121
  10 permit udp any host 192.168.27.3 eq domain
  20 permit tcp any host 192.168.27.3 eq domain
  30 permit tcp any host 192.168.27.3 eq www
  40 permit tcp any host 192.168.27.3 eq ftp
  50 permit tcp any host 192.168.27.3 eq smtp
  60 permit icmp any 192.168.27.0 0.0.0.255 administratively-prohibited
  70 permit icmp any 192.168.27.0 0.0.0.255 echo
  80 permit icmp any 192.168.27.0 0.0.0.255 echo-reply
  90 permit icmp any 192.168.27.0 0.0.0.255 packet-too-big
  100 permit icmp any 192.169.27.0 0.0.0.255 time-exceeded
  110 permit icmp any 192.168.27.0 0.0.0.255 traceroute
  120 permit icmp any 192.168.27.0 0.0.0.255 unreachable
  130 deny ip any any (4866 matches)
Router#
```

- **show ip audit all** Verifies the configuration of the logging commands.

```
Router#show ip audit all
Event notification through syslog is enabled
Event notification through Net Director is disabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 250
PostOffice:HostID:0 OrgID:0 Msg dropped:0
      :Curr Event Buf Size:0 Configured:100
Post Office is not enabled - No connections are active
```

Router#

- **show ip inspect all** Verifies the configuration of the Cisco IOS Firewall inspection rules per interface.

Router#**show ip inspect all**

```
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 14400 sec -- udp idle-time is 1800 sec
dns-timeout is 7 sec
Inspection Rule Configuration
Inspection name standard
  cuseeme alert is on audit-trail is on timeout 14400
  ftp alert is on audit-trail is on timeout 14400
  h323 alert is on audit-trail is on timeout 14400
  http alert is on audit-trail is on timeout 14400
  rcmd alert is on audit-trail is on timeout 14400
  realaudio alert is on audit-trail is on timeout 14400
  smtp alert is on audit-trail is on timeout 14400
  sqlnet alert is on audit-trail is on timeout 14400
  streamworks alert is on audit-trail is on timeout 1800
  tcp alert is on audit-trail is on timeout 14400
  tftp alert is on audit-trail is on timeout 1800
  udp alert is on audit-trail is on timeout 1800
  vdolive alert is on audit-trail is on timeout 14400
```

Interface Configuration

Interface Ethernet3/0

```
Inbound inspection rule is standard
  cuseeme alert is on audit-trail is on timeout 14400
  ftp alert is on audit-trail is on timeout 14400
  h323 alert is on audit-trail is on timeout 14400
  http alert is on audit-trail is on timeout 14400
  rcmd alert is on audit-trail is on timeout 14400
  realaudio alert is on audit-trail is on timeout 14400
  smtp alert is on audit-trail is on timeout 14400
  sqlnet alert is on audit-trail is on timeout 14400
  streamworks alert is on audit-trail is on timeout 1800
  tcp alert is on audit-trail is on timeout 14400
  tftp alert is on audit-trail is on timeout 1800
  udp alert is on audit-trail is on timeout 1800
  vdolive alert is on audit-trail is on timeout 14400
```

Outgoing inspection rule is not set

Inbound access list is 101

Outgoing access list is not set

Interface Ethernet3/1

Inbound inspection rule is not set

Outgoing inspection rule is standard

```
  cuseeme alert is on audit-trail is on timeout 14400
  ftp alert is on audit-trail is on timeout 14400
  h323 alert is on audit-trail is on timeout 14400
  http alert is on audit-trail is on timeout 14400
  rcmd alert is on audit-trail is on timeout 14400
  realaudio alert is on audit-trail is on timeout 14400
  smtp alert is on audit-trail is on timeout 14400
  sqlnet alert is on audit-trail is on timeout 14400
  streamworks alert is on audit-trail is on timeout 1800
  tcp alert is on audit-trail is on timeout 14400
  tftp alert is on audit-trail is on timeout 1800
  udp alert is on audit-trail is on timeout 1800
  vdolive alert is on audit-trail is on timeout 14400
```

Inbound access list is 111

Outgoing access list is not set

Router#

Troubleshoot

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 standard in** is applied for the interface ethernet 3/0 and **ip inspect standard out** is applied for the interface ethernet 3/1.

Refer to Troubleshooting Cisco IOS Firewall Configurations for further information on troubleshooting.

Related Information

- [Cisco IOS Firewall Support Page](#)
 - [Cisco IOS Firewall in IOS Documentation](#)
 - [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: Feb 20, 2007

Document ID: 13893
