带NAT的双接口路由器的 Cisco IOS防火墙配置

目录

简介
先决条件
要求
使用的组件
规则
背景信息
配置
网络图
配置
验证
故障排除
问题
解决方案
相关信息

简介

此示例配置适用于直接连接到 Internet 的小型办公室。假定域名服务 (DNS)、Simple Mail Transfer Protocol (SMTP) 和 Web 服务由 Internet 服务提供商 (ISP) 运行的远程系统提供。在内部网络中没有服务，这使它成为最简单的防火墙配置之一，因为只有两个接口。因为没有可用于提供日志记录服务的主机，所以没有日志记录功能。

要使用 Cisco IOS® 防火墙配置不带 NAT 的三接口路由器，请参阅不带 NAT 的三接口路由器 Cisco IOS 防火墙配置。

要使用 Cisco IOS 防火墙配置不带 NAT 的两接口路由器，请参阅使用 Cisco IOS 防火墙配置的不带 NAT 的两接口路由器。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 软件版本 12.2

- Cisco 3640路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

因为此配置仅使用输入访问列表，所以可使用同一个访问列表(101)进行反欺骗和流量过滤。此配置只为双端口路由器工作。以太网 1 是“内部”网络。Serial 0 是外部接口。Serial 0 上的访问列表 (112) 使用网络地址转换 (NAT) 全局 IP 地址 (150.150.150.x) 作为目标来说明这种情况。

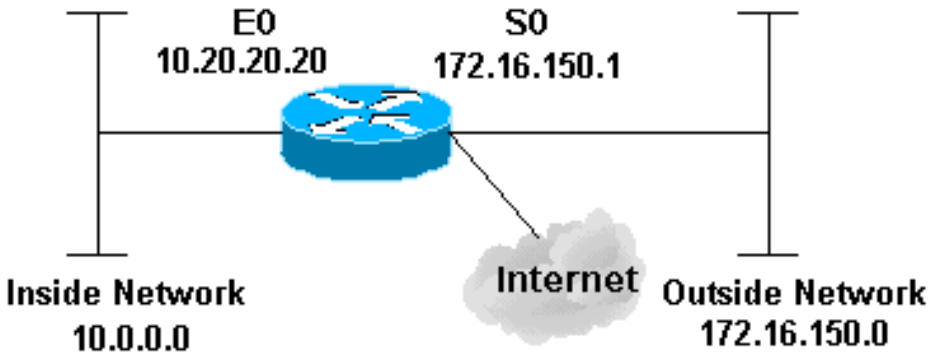
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

3640路由器
version 12.2 service timestamps debug datetime msec localtime show-

```
timezone
service timestamps log datetime msec localtime show-
timezone
no service password-encryption
!
hostname pig
!
boot system flash flash:c3640-jk9o3s-mz.122-21a.bin
logging buffered 4096 debugging
enable secret 5 $1$chHU$wiC58FP/IDloZuorCkzEz1
enable password ww
!
clock timezone CET 1
clock summer-time CET recurring
ip subnet-zero
!
!
no ip domain-lookup
!
!--- This is the Cisco IOS Firewall !--- configuration
and what to inspect. ip inspect name ethernetin cuseeme
timeout 3600 ip inspect name ethernetin ftp timeout 3600
ip inspect name ethernetin h323 timeout 3600 ip inspect
name ethernetin http timeout 3600 ip inspect name
ethernetin rcmd timeout 3600 ip inspect name ethernetin
realaudio timeout 3600 ip inspect name ethernetin smtp
timeout 3600 ip inspect name ethernetin sqlnet timeout
3600 ip inspect name ethernetin streamworks timeout 3600
ip inspect name ethernetin tcp timeout 3600 ip inspect
name ethernetin tftp timeout 30 ip inspect name
ethernetin udp timeout 15 ip inspect name ethernetin
vdolive timeout 3600 ip audit notify log ip audit po
max-events 100 ! call rsvp-sync ! ! ! ! ! ! ! !--- This
is the inside of the network. interface Ethernet0/0 ip
address 10.20.20.20 255.255.255.0 ip access-group 101 in
ip nat inside ip inspect ethernetin in half-duplex !
interface Ethernet0/1 no ip address shutdown half-duplex
! interface Serial1/0 no ip address shutdown ! interface
Serial1/1 no ip address shutdown ! interface Serial1/2
no ip address shutdown ! !--- This is the outside of the
interface. interface Serial1/3 ip address 172.16.150.1
255.255.255.0 ip access-group 112 in ip nat outside ! !-
-- Define the NAT pool. ip nat pool mypool 172.16.150.3
172.16.150.255 netmask 255.255.255.0 ip nat inside
source list 1 pool mypool ip classless ip route 0.0.0.0
0.0.0.0 172.16.150.2 ip http server ! access-list 1
permit 10.0.0.0 0.255.255.255 !--- Access list applied
on the inside for anti-spoofing reasons. access-list 101
permit tcp 10.0.0.0 0.255.255.255 any access-list 101
permit udp 10.0.0.0 0.255.255.255 any access-list 101
permit icmp 10.0.0.0 0.255.255.255 any access-list 101
deny ip any any log !--- Access list applied on the
outside for security reasons. access-list 112 permit
icmp any 172.16.150.0 0.0.0.255 unreachable access-list
112 permit icmp any 150.150.150.0 0.0.0.255 echo-reply
access-list 112 permit icmp any 172.16.150.0 0.0.0.255
packet-too-big access-list 112 permit icmp any
172.16.150.0 0.0.0.255 time-exceeded access-list 112
permit icmp any 172.16.150.0 0.0.0.255 traceroute
access-list 112 permit icmp any 172.16.150.0 0.0.0.255
administratively-prohibited access-list 112 permit icmp
any 172.16.150.0 0.0.0.255 echo access-list 112 deny ip
any any log ! ! dial-peer cor custom ! ! ! ! ! line con
0 exec-timeout 0 0 line 97 102 line aux 0 line vty 0 4
```

```
exec-timeout 0 0 password ww login ! end
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show version** — 显示当前加载的软件版本的相关信息、硬件信息以及设备信息。
- **debug ip nat** - 显示由 IP NAT 功能转换的 IP 数据包的相关信息。
- **show ip nat translations** — 显示处于活动状态的 NAT。
- **show log** — 显示日志记录信息。
- **show ip access-list** - 显示所有当前 IP 访问列表的内容。
- **show ip inspect session** — 显示 Cisco IOS 防火墙当前跟踪和检查的现有会话。
- **debug ip inspect tcp** — 显示有关 Cisco IOS 防火墙事件的消息。

以下是 **show version 命令**的示例命令输出。

```
pig#show version Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3640-
JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2) Copyright (c) 1986-2004 by cisco Systems,
Inc. Compiled Fri 09-Jan-04 16:23 by kellmill Image text-base: 0x60008930, data-base: 0x615DE000
ROM: System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1) pig uptime is
59 minutes System returned to ROM by reload at 16:05:44 CET Wed Jan 14 2004 System image file is
"flash:c3640-jk9o3s-mz.122-21a.bin" This product contains cryptographic features and is subject
to United States and local country laws governing import, export, transfer and use. Delivery of
Cisco cryptographic products does not imply third-party authority to import, export, distribute
or use encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws, return this product
immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html If you require further assistance please
contact us by sending email to export@cisco.com. cisco 3640 (R4700) processor (revision 0x00)
with 126976K/4096K bytes of memory. Processor board ID 10577176 R4700 CPU at 100Mhz,
Implementation 33, Rev 1.0 MICA-6DM Firmware: CP ver 2730 - 5/23/2001, SP ver 2730 - 5/23/2001.
Bridging software. X.25 software, Version 3.0.0. SuperLAT software (copyright 1990 by Meridian
Technology Corp). TN3270 Emulation software. 2 Ethernet/IEEE 802.3 interface(s) 4 Low-speed
serial(sync/async) network interface(s) 6 terminal line(s) 1 Virtual Private Network (VPN)
Module(s) DRAM configuration is 64 bits wide with parity disabled. 125K bytes of non-volatile
configuration memory. 32768K bytes of processor board System flash (Read/Write)
```

首先，使用 **debug ip nat** 和 **show ip nat translations** 验证 NAT 是否可以正常工作，如以下输出所示。

```
pig#debug ip nat IP NAT debugging is on pig# *Mar 1 01:40:47.692 CET: NAT: s=10.0.0.1-
>172.16.150.4, d=172.16.150.2 [80] *Mar 1 01:40:47.720 CET: NAT*: s=172.16.150.2,
d=172.16.150.4->10.0.0.1 [80] *Mar 1 01:40:47.720 CET: NAT*: s=10.0.0.1->172.16.150.4,
d=172.16.150.2 [81] *Mar 1 01:40:47.748 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [81]
*Mar 1 01:40:47.748 CET: NAT*: s=10.0.0.1->172.16.150.4, d=172.16.150.2 [82] *Mar 1 01:40:47.784
CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [82] *Mar 1 01:40:47.784 CET: NAT*:
s=10.0.0.1->172.16.150.4, d=172.16.150.2 [83] *Mar 1 01:40:47.836 CET: NAT*: s=172.16.150.2,
d=172.16.150.4->10.0.0.1 [83] *Mar 1 01:40:47.836 CET: NAT*: s=10.0.0.1->172.16.150.4,
d=172.16.150.2 [84] *Mar 1 01:40:47.884 CET: NAT*: s=172.16.150.2, d=172.16.150.4->10.0.0.1 [84]
pig#show ip nat translations Pro Inside global Inside local Outside local Outside global ---
172.16.150.4 10.0.0.1 --- ---
```

在不添加 **ip inspect** 语句的情况下，验证访问列表是否可以正常工作。具有 **log 关键字**的 **deny ip any any** 告知您阻止的数据包。

在本示例中，这是 10.0.0.1（转换为 172.16.150.4）与 172.16.150.2 之间的 Telnet 会话的回程数据流。

以下是 **show log 命令**的示例输出。

```
pig#show log Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns) Console logging: level debugging, 92 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 60 messages logged Logging Exception size (4096 bytes) Trap logging: level informational, 49 message lines logged Log Buffer (4096 bytes): *Mar 1 01:24:08.518 CET: %SYS-5-CONFIG_I: Configured from console by console *Mar 1 01:26:47.783 CET: %SYS-5-CONFIG_I: Configured from console by console *Mar 1 01:27:09.876 CET: %SEC-6-IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23) -> 172.16.150.4(11004), 1 packet *Mar 1 01:33:03.371 CET: %SEC-6-IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23) -> 172.16.150.4(11004), 3 packets
```

要查看有多少数据包与访问列表匹配，请使用 **show ip access-lists 命令**。

```
pig#show ip access-lists Standard IP access list 1 permit 10.0.0.0, wildcard bits 0.255.255.255 (28 matches) Extended IP access list 101 permit tcp 10.0.0.0 0.255.255.255 any (32 matches) permit udp 10.0.0.0 0.255.255.255 any permit icmp 10.0.0.0 0.255.255.255 any (22 matches) deny ip any any log Extended IP access list 112 permit icmp any 172.16.150.0 0.0.0.255 unreachable permit icmp any 172.16.150.0 0.0.0.255 echo-reply (10 matches) permit icmp any 172.16.150.0 0.0.0.255 packet-too-big permit icmp any 172.16.150.0 0.0.0.255 time-exceeded permit icmp any 172.16.150.0 0.0.0.255 traceroute permit icmp any 172.16.150.0 0.0.0.255 administratively-prohibited permit icmp any 172.16.150.0 0.0.0.255 echo deny ip any any log (12 matches) pig#
```

添加 **ip inspect** 语句后，您可以看到以下行已动态添加到访问列表中，以允许此 Telnet 会话：

```
permit tcp host 172.16.150.2 eq telnet host 172.16.150.4 eq 11004 (16 matches)pig#show ip access-lists Standard IP access list 1 permit 10.0.0.0, wildcard bits 0.255.255.255 (44 matches) Extended IP access list 101 permit tcp 10.0.0.0 0.255.255.255 any (50 matches) permit udp 10.0.0.0 0.255.255.255 any permit icmp 10.0.0.0 0.255.255.255 any (22 matches) deny ip any any log Extended IP access list 112 permit tcp host 172.16.150.2 eq telnet host 172.16.150.4 eq 11004 (16 matches) permit icmp any 172.16.150.0 0.0.0.255 unreachable permit icmp any 172.16.150.0 0.0.0.255 echo-reply (10 matches) permit icmp any 172.16.150.0 0.0.0.255 packet-too-big permit icmp any 172.16.150.0 0.0.0.255 time-exceeded permit icmp any 172.16.150.0 0.0.0.255 traceroute permit icmp any 172.16.150.0 0.0.0.255 administratively-prohibited permit icmp any 172.16.150.0 0.0.0.255 echo deny ip any any log (12 matches) pig#
```

还可以使用 **show ip inspect session 命令**检查，该命令显示已通过防火墙建立的当前会话。

```
pig#show ip inspect session Established Sessions Session 624C31A4 (10.0.0.1:11006)=>(172.16.150.2:23) tcp SIS_OPEN
```

最终，在更高级的级别，您也可以启用debug ip inspect tcp命令。

```
pig#debug ip inspect tcp INSPECT TCP Inspection debugging is on pig# *Mar 1 01:49:51.756 CET: CBAC sis 624C31A4 pak 624D0FA8 TCP S seq 2890060460(0) (172.16.150.4:11006) => (172.16.150.2:23) *Mar 1 01:49:51.776 CET: CBAC sis 624C31A4 pak 624D0CC4 TCP S ack 2890060461 seq 1393191461(0) (10.0.0.1:11006) <= (172.16.150.2:23) *Mar 1 01:49:51.776 CET: CBAC* sis 624C31A4 pak 62576284 TCP ack 1393191462 seq 2890060461(0) (172.16.150.4:11006) => (172.16.150.2:23) *Mar 1 01:49:51.776 CET: CBAC* sis 624C31A4 pak 62576284 TCP P ack 1393191462 seq 2890060461(12) (172.16.150.4:11006) => (172.16.150.2:23) *Mar 1 01:49:51.780 CET: CBAC* sis 624C31A4 pak 62576284 TCP ack 1393191462 seq 2890060473(0) (172.16.150.4:11006) => (172.16.150.2:23)
```

故障排除

配置 IOS 防火墙路由器后，如果连接不起作用，请确保已使用 **ip inspect (定义的名称) in/out 命令**对接口启用检查。在此配置中，**ip inspect ethernetin in** 应用于接口 **Ethernet0/0**。

有关此配置的常规故障排除，请参阅对 Cisco IOS 防火墙配置进行故障排除以及对认证代理进行故障排除。

问题

不能执行 http 下载，因为它会失败或者超时。如何解决这一问题？

解决方案

可以通过以下方式解决该问题：删除 http 数据流的 **ip inspect**，以便不检查 http 数据流并且下载按照预期执行。

相关信息

- IOS防火墙支持页面
- 技术支持和文档 - Cisco Systems