使用Cisco IOS防火墙配置的没有NAT的两接口路由器

目录

简介

此配置示例为直接连接到互联网的小型办公室工作，假设域名服务器(DNS)，简单邮件转发协议(SMTP)和互联网服务由互联网服务提供商(ISP)运行的远程系统提供。网络内部和两个端口没有服务。因为没有提供日志服务的主机联机，所以也没有日志。

因为此配置只使用输入访问列表，所以可使用相同的访问列表，进行反欺骗和流量过滤。此配置只为双端口路由器工作。Ethernet0是“里面”网络。Serial0是帧中继链路对ISP。

要使用思科 IOS 防火墙配置带 NAT 的双接口路由器，请参阅使用思科 IOS 防火墙配置带 NAT 的双接口路由器。

使用Cisco IOS防火墙，没有NAT Cisco IOS防火墙配置的参考的三接口路由器为了配置三个接口路由器，不用NAT。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息适用于以下软件和硬件版本：

- 从Cisco IOS软件版本11.3.3.T的Cisco IOS软件版本12.2(15)T13，支持
- Cisco 2611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。

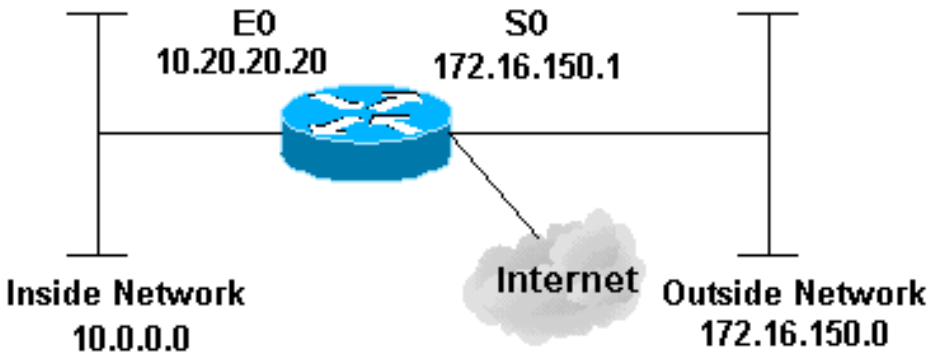
配置

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

本文档使用以下网络设置：



配置

本文档使用以下配置：

2514路由器

```
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
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

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 myfw**为接口Ethernet0/0应用。

对于这些指令和其他故障排除信息，请参见排错认证代理。

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

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