使用Cisco IOS防火牆配置的無NAT的雙介面路由器

目錄

簡介

此示例配置適用於直接連線到Internet的小型辦公室，其假設前提是域名服務(DNS)、簡單郵件傳輸協定(SMTP)和Web服務由由Internet服務提供商(ISP)運行的遠端系統提供。 內部網路中沒有服務，只有兩個介面。也沒有日誌記錄，因為沒有主機可以提供日誌記錄服務。

由於此組態僅使用輸入存取清單，因此它會使用相同的存取清單進行反詐騙和流量過濾。此配置僅適用於雙埠路由器。乙太網0是「內部」網路。Serial 0是通向ISP的幀中繼鏈路。

請參閱使用NAT Cisco IOS防火牆配置的雙介面路由器，以使用Cisco IOS®防火牆配置使用NAT的雙介面路由器。

請參閱不帶NAT的三介面路由器Cisco IOS防火牆配置，以使用Cisco IOS防火牆配置不帶NAT的三介面路由器。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊適用於以下軟體和硬體版本：

- Cisco IOS®軟體版本12.2(15)T13，受Cisco IOS軟體版本11.3.3.T支援
- 思科2611路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

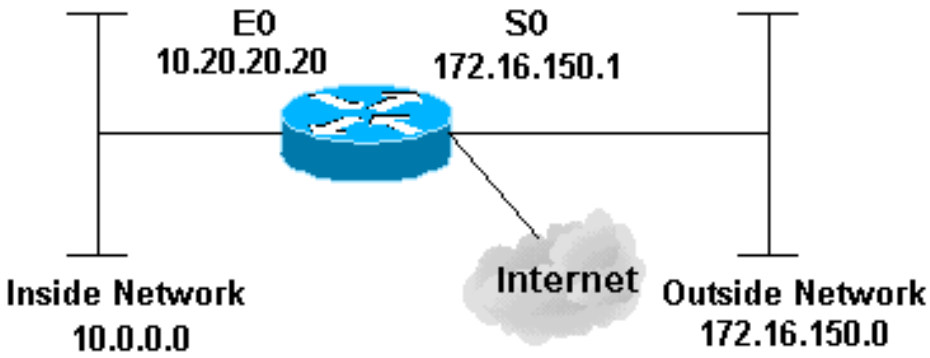
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

設定IOS防火牆路由器後，如果連線無法運作，請確認已在介面上使用**ip inspect（定義名稱）in或out指令啟用檢**測。在此配置中，**ip inspect myfw in**應用於介面Ethernet0/0。

如需這些命令以及其他疑難排解資訊，請參閱驗證代理疑難排解。

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

相關資訊

- IOS防火牆支援頁面
- 技術支援與文件 - Cisco Systems