配置NAT Cisco IOS防火牆的雙介面路由器

目錄

簡介

此示例配置適用於直接連線到Internet的小型辦公室。假設域名服務(DNS)、簡單郵件傳輸協定(SMTP)和Web服務由網際網路服務提供商(ISP)運行的遠端系統提供。 內部網路中沒有服務，因此這是最簡單的防火牆配置之一，因為只有兩個介面。沒有日誌記錄，因為沒有主機可以提供日誌記錄服務。

請參閱無NAT的三介面路由器Cisco IOS防火牆配置，以使用Cisco IOS®防火牆配置無NAT的三介面路由器。

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

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本12.2

- 思科3640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。

背景資訊

由於此配置僅使用輸入訪問清單，因此它使用相同的訪問清單(101)同時執行反欺騙和流量過濾。此配置僅適用於雙埠路由器。乙太網1是「內部」網路。Serial 0是外部介面。Serial 0上的訪問清單(112)將網路地址轉換(NAT)全域性IP地址(150.150.150.x)作為目標來說明這一點。

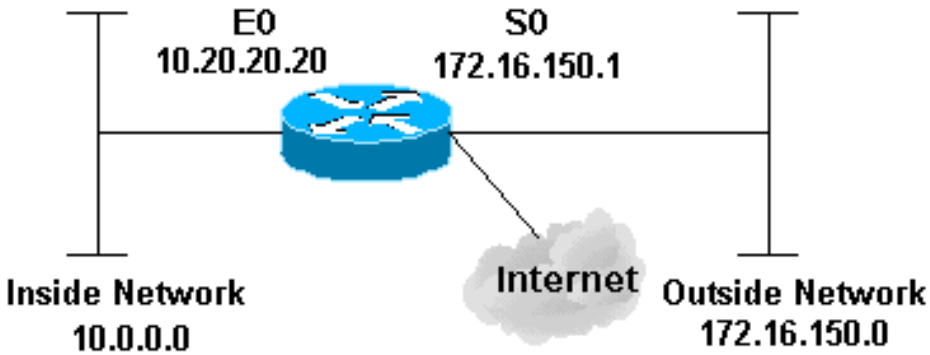
設定

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

本檔案會使用此網路設定。



組態

本檔案會使用此組態。

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show version** — 顯示當前載入的軟體版本資訊以及硬體和裝置資訊。
- **debug ip nat** — 顯示由IP NAT功能轉換的IP資料包的相關資訊。
- **show ip nat translations** — 顯示活動NAT。
- **show log** — 顯示日誌記錄資訊。
- **show ip access-list** — 顯示所有當前IP訪問清單的內容。
- **show ip inspect session** — 顯示Cisco IOS防火牆當前跟蹤和檢查的現有會話。
- **debug ip inspect tcp** — 顯示有關Cisco IOS防火牆事件的消息。

以下是**show version**命令的輸出示例。

```
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**驗證NAT是否正常工作，如以下輸出所示。

```
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           ---                ---
```

如果不新增**ip inspect**語句，請確認訪問清單是否正常工作。使用**log**關鍵字的**deny ip any any**會告訴您哪些封包遭封鎖。

在本例中，這是從10.0.0.1（轉換為172.16.150.4）到172.16.150.2的Telnet會話返回流量。

以下是**show log**命令的輸出示例。

```
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
```

使用**show ip access-lists**命令檢視有多少封包與存取清單相符。

```
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#
```

一旦新增了ip inspect語句，就可以看到此行已動態新增到訪問清單中，以允許此Telnet會話：

```
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#
```

您還可以使用show ip inspect session命令進行檢查，該命令會顯示已通過防火牆建立的目前作業階段。

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

最後，在更高級的級別上，您還可以啟用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)
```

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 ethernet in應用於介面Ethernet0/0。

如需此組態的一般疑難排解，請參閱疑難排解Cisco IOS防火牆組態和驗證代理疑難排解。

問題

無法執行http下載，因為它失敗或超時。這個問題如何解決？

解決方案

可以通過刪除**ip inspect** for http traffic來解決問題，這樣就不會檢查http通訊量，並會按預期進行下載。

相關資訊

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