NAT Cisco IOS 방화벽 컨피그레이션이 포함된 2인터페이스 라우터

목차

소개

이 샘플 컨피그레이션은 인터넷에 직접 연결된 소규모 사무실에서 작동합니다. DNS(Domain Name Service), SMTP(Simple Mail Transfer Protocol) 및 웹 서비스는 ISP(Internet Service Provider)가 실행하는 원격 시스템에서 제공된다고 가정합니다. 내부 네트워크에는 서비스가 없으며, 이는 인터페이스가 두 개뿐이므로 가장 간단한 방화벽 컨피그레이션 중 하나입니다. 로깅 서비스를 제공할 수 있는 호스트가 없기 때문에 로깅이 없습니다.

Cisco IOS® Firewall을 사용하여 NAT 없이 3개의 인터페이스 라우터를 구성하려면 NAT Cisco IOS Firewall Configuration이 없는 3개의 인터페이스 라우터를 참조하십시오.

Cisco IOS Firewall을 사용하여 NAT 없이 2개의 인터페이스 라우터를 구성하려면 Two-interface Router Using Cisco IOS Firewall Configuration을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2
- Cisco 3640 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

이 컨피그레이션에서는 입력 액세스 목록만 사용하므로 동일한 액세스 목록(101)을 사용하여 스푸핑 방지 및 트래픽 필터링을 모두 수행합니다. 이 컨피그레이션은 2포트 라우터에서만 작동합니다. 이더넷 1은 "내부" 네트워크입니다. 직렬 0은 외부 인터페이스입니다. 직렬 0의 액세스 목록(112)은 NAT(Network Address Translation) 전역 IP 주소(150.150.150.x)를 대상으로 사용하여 이를 보여줍니다.

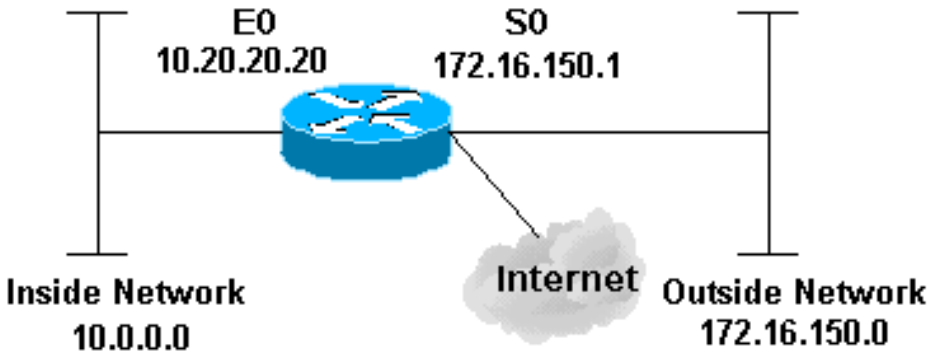
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



구성

이 문서에서는 이 구성을 사용합니다.

3640 라우터

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show version** - 현재 로드된 소프트웨어 버전에 대한 정보와 하드웨어 및 디바이스 정보를 표시합니다.
- **debug ip nat** - IP NAT 기능으로 변환된 IP 패킷에 대한 정보를 표시합니다.
- **show ip nat translations** - 활성 NAT를 표시합니다.
- **show log** - 로깅 정보를 표시합니다.
- **show ip access-list** - 현재 모든 IP 액세스 목록의 내용을 표시합니다.
- **show ip inspect session**—Cisco IOS 방화벽에서 현재 추적 및 검사하는 기존 세션을 표시합니다.
- **debug ip inspect tcp** - Cisco IOS 방화벽 이벤트에 대한 메시지를 표시합니다.

show version 명령의 샘플 명령 출력입니다.

```
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)
```

먼저 NAT가 **디버그 ip nat**를 사용하여 올바르게 작동하는지 확인하고 이 출력에 표시된 대로 **show ip nat translation**을 표시합니다.

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

ip inspect 문을 추가하지 않고 액세스 목록이 올바르게 작동하는지 확인합니다. deny **ip any any** with **log** 키워드는 차단된 패킷을 알려줍니다.

이 경우 텔넷 세션에서 10.0.0.1에서 172.16.150.2(172.16.150.4으로 변환)으로 반환 트래픽입니다.

show log 명령의 샘플 출력입니다.

```
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
```

액세스 목록과 일치하는 패킷 수를 확인하려면 **show ip access-lists** 명령을 사용합니다.

```
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#
```

ip inspect 문을 추가한 후에는 이 텔넷 세션을 허용하기 위해 액세스 목록에 이 행이 동적으로 추가되었음을 확인할 수 있습니다.

```
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#
```

방화벽을 통해 설정된 현재 세션을 보여주는 **show ip inspect session** 명령을 사용하여 확인할 수도 있습니다.

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

더 고급 레벨에서 debug ip inspect tcp 명령을 활성화할 수도 있습니다.

```
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)
```

문제 해결

IOS Firewall 라우터를 구성한 후 연결이 작동하지 않을 경우 인터페이스에서 **ip inspect(name defined) 또는 out** 명령**으로** 검사를 활성화했는지 확인합니다. 이 컨피그레이션에서는 **ip inspect ethernin**이 인터페이스 **Ethernet0/0**에 **적용됩니다**.

이 컨피그레이션에 대한 일반적인 트러블슈팅은 Troubleshooting Cisco IOS Firewall Configurations and Troubleshooting Authentication Proxy를 참조하십시오.

문제

http 다운로드가 실패하거나 시간 초과되어 수행할 수 없습니다. 이 문제는 어떻게 해결됩니까?

솔루션

http 트래픽이 검사되지 않고 다운로드가 예상대로 이루어지도록 http 트래픽에 대한 **ip 검사**를 제거하여 문제를 해결할 수 있습니다.

관련 정보

- IOS 방화벽 지원 페이지
- 기술 지원 및 문서 – Cisco Systems