Router a due interfacce con configurazione NAT Cisco IOS Firewall

Sommario

Introduzione

Questa configurazione di esempio funziona per un ufficio di dimensioni molto ridotte connesso direttamente a Internet. Si presuppone che i servizi DNS (Domain Name Service), SMTP (Simple Mail Transfer Protocol) e Web siano forniti da un sistema remoto eseguito dal provider di servizi Internet (ISP). Non ci sono servizi nella rete interna, il che rende questa una delle configurazioni del firewall più semplici, dato che ci sono solo due interfacce. Non è disponibile alcuna registrazione perché non è disponibile alcun host per la fornitura dei servizi di registrazione.

Per configurare un router a tre interfacce senza NAT con Cisco IOS Firewall, consultare il documento sulla configurazione del firewall a tre interfacce senza NAT con Cisco IOS® Firewall.

Per configurare un router a due interfacce senza NAT con Cisco IOS Firewall, consultare il documento sulla configurazione del firewall a due interfacce senza NAT con Cisco IOS Firewall.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 12.2
- Cisco 3640 router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Poiché questa configurazione utilizza solo elenchi degli accessi di input, esegue sia l'anti-spoofing che il filtro del traffico con lo stesso elenco degli accessi (101). Questa configurazione funziona solo con un router a due porte. Ethernet 1 è la rete "interna". Il numero di serie 0 è l'interfaccia esterna. L'elenco degli accessi (112) sul numero di serie 0 mostra questo usando gli indirizzi IP globali NAT (Network Address Translation) (150.150.150.x) come destinazioni.

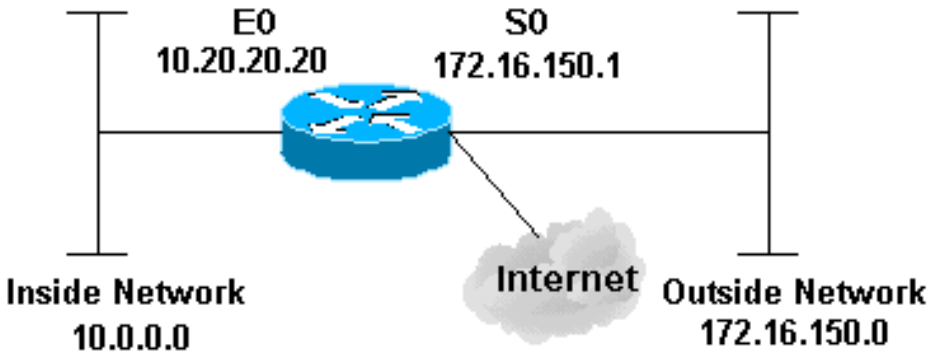
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete.



Configurazione

Nel documento viene usata questa configurazione.

3640 Router

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show version**: visualizza le informazioni sulla versione software attualmente caricata, insieme alle informazioni sull'hardware e sul dispositivo.
- **debug ip nat**: visualizza le informazioni sui pacchetti IP convertiti dalla funzionalità IP NAT.
- **show ip nat translation**: visualizza i NAT attivi.
- **show log**: visualizza le informazioni di log.
- **show ip access-list**: visualizza il contenuto di tutti gli elenchi degli accessi IP correnti.
- **show ip inspect session**: visualizza le sessioni esistenti attualmente tracciate e ispezionate da Cisco IOS Firewall.
- **debug ip inspect tcp**: visualizza i messaggi relativi agli eventi di Cisco IOS Firewall.

In questo esempio, i risultati restituiti dal comando **show version**.

```
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)
```

Innanzitutto, verificare che NAT funzioni correttamente usando **debug ip nat** e **visualizzare le traduzioni ip nat**, come mostrato in questo output.

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

Senza aggiungere l'istruzione **ip inspect**, verificare che gli elenchi degli accessi funzionino correttamente. La parola chiave **deny ip any any** con la parola chiave **log** indica i pacchetti bloccati.

In questo caso, il traffico di ritorno da una sessione Telnet a 172.16.150.2 da 10.0.0.1 (convertito

in 172.16.150.4).

Di seguito viene riportato un output di esempio del comando **show log**.

```
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
```

Per verificare quanti pacchetti corrispondono all'elenco, usare il comando **show ip access-lists**.

```
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#
```

Dopo aver aggiunto l'istruzione **ip inspect**, è possibile verificare che questa riga è stata aggiunta dinamicamente nell'elenco degli accessi per consentire la sessione Telnet:

```
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#
```

Èinoltre possibile eseguire il controllo utilizzando il comando **show ip inspect session** per visualizzare le sessioni correnti stabilite attraverso il firewall.

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

Infine, a un livello più avanzato, è possibile abilitare il comando **debug ip inspect tcp**.

```
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)
```

Risoluzione dei problemi

Dopo aver configurato il router del firewall IOS, se le connessioni non funzionano, verificare di aver abilitato l'ispezione con il comando **ip inspect (nome definito)** sull'interfaccia **in o out**. In questa configurazione, l'**interfaccia Ethernet0/0** è configurata con l'**interfaccia ip inspect ethernet in**.

Per informazioni generali sulla risoluzione dei problemi relativi a questa configurazione, vedere Risoluzione dei problemi di configurazione di Cisco IOS Firewall e Risoluzione dei problemi del proxy di autenticazione.

Problema

Non è possibile eseguire download HTTP perché si è verificato un errore o un timeout. Come si risolve tutto questo?

Soluzione

Il problema può essere risolto rimuovendo **ip inspect** per il traffico http in modo che il traffico http non venga ispezionato e il download avvenga come previsto.

Informazioni correlate

- Pagina di supporto di IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems