# Zwei-Schnittstellen-Router mit NAT-Konfiguration der Cisco IOS-Firewall

## Inhalt



## Einführung

Diese Beispielkonfiguration funktioniert für ein sehr kleines Büro, das direkt mit dem Internet verbunden ist. Es wird davon ausgegangen, dass Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP) und Web-Services von einem Remote-System bereitgestellt werden, das vom Internet Service Provider (ISP) ausgeführt wird. Im internen Netzwerk gibt es keine Services. Dies ist eine der einfachsten Firewall-Konfigurationen, da es nur zwei Schnittstellen gibt. Es wird keine Protokollierung durchgeführt, da kein Host für Protokollierungsdienste verfügbar ist.

Informationen zur Konfiguration eines Routers mit drei Schnittstellen ohne NAT unter Verwendung der Cisco IOS® Firewall finden Sie unter Router mit drei Schnittstellen ohne NAT.

Informationen zur Konfiguration eines Zwei-Schnittstellen-Routers ohne NAT mithilfe der Cisco IOS-Firewall-Konfiguration finden Sie unter Zwei-Schnittstellen-Router ohne NAT unter Verwendung der Cisco IOS-Firewall.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Softwareversion 12.2
- Cisco Router 3640

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

## Hintergrundinformationen

Da bei dieser Konfiguration nur Zugriffslisten für die Eingabe verwendet werden, werden Spoofing- und Datenverkehrsfilter mit derselben Zugriffsliste ausgeführt (101). Diese Konfiguration funktioniert nur bei Routern mit zwei Ports. Ethernet 1 ist das "interne" Netzwerk. Serial 0 ist die externe Schnittstelle. Die Zugriffsliste (112) von Serial 0 zeigt dies anhand der globalen IP-Adressen (150.150.150.x) für Network Address Translation (NAT) als Ziele.

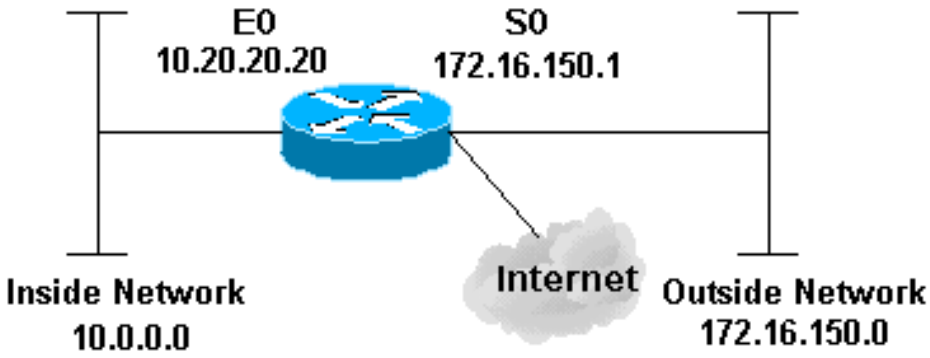
## Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

### Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.




## Konfiguration

In diesem Dokument wird diese Konfiguration verwendet.

**Router 3640**

```
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
```

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show version**: Zeigt Informationen über die aktuell geladene Softwareversion sowie Hardware- und Geräteinformationen an.
- **debug ip nat**: Zeigt Informationen über IP-Pakete an, die durch die IP NAT-Funktion übersetzt wurden.
- **show ip nat translations**: Zeigt aktive NATs an.
- **show log**: Zeigt Protokollierungsinformationen an.
- **show ip access-list**: Zeigt den Inhalt aller aktuellen IP-Zugriffslisten an.
- **show ip inspect session**: Zeigt vorhandene Sitzungen an, die derzeit von der Cisco IOS Firewall überwacht und inspiziert werden.
- **debug ip inspect tcp**: Zeigt Meldungen über Cisco IOS Firewall-Ereignisse an.

Dies ist die Beispielbefehlsausgabe aus dem Befehl **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)
```

Überprüfen Sie zunächst, ob NAT mit **debug ip nat** ordnungsgemäß funktioniert und **zeigen Sie ip nat-Übersetzungen** an, wie in dieser Ausgabe gezeigt.

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

Stellen Sie sicher, dass die Zugriffslisten korrekt funktionieren, ohne die **ip inspect**-Anweisung hinzuzufügen. Die **deny ip any any any any** mit dem **log-**Schlüsselwort sagt Ihnen, welche Pakete blockiert werden.

In diesem Fall ist dies der Rückverkehr von einer Telnet-Sitzung zu 172.16.150.2 von 10.0.0.1

(übersetzt in 172.16.150.4).

Dies ist die Beispielausgabe des Befehls **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
```

Verwenden Sie den Befehl **show ip access-lists**, um zu sehen, wie viele Pakete mit der Zugriffsliste übereinstimmen.

```
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#
```

Nachdem Sie die **ip inspect**-Anweisung hinzugefügt haben, können Sie sehen, dass diese Leitung dynamisch in die Zugriffsliste hinzugefügt wurde, um diese Telnet-Sitzung zuzulassen:

```
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#
```

Sie können die Prüfung auch mit dem Befehl **show ip inspect session** durchführen, der die aktuell über die Firewall eingerichteten Sitzungen anzeigt.

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

Schließlich können Sie auf einer erweiterten Ebene auch den Befehl **debug ip inspect tcp** aktivieren.

```
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)
```

# Fehlerbehebung

Wenn Sie den IOS-Firewall-Router konfiguriert haben und die Verbindungen nicht funktionieren, stellen Sie sicher, dass die Überprüfung mit dem Befehl **ip inspect (name defined) in oder out** auf der Schnittstelle aktiviert ist. In dieser Konfiguration wird **ip inspect Ethernet in** für die Schnittstelle **Ethernet0/0** angewendet.

Eine allgemeine Fehlerbehebung für diese Konfiguration finden Sie unter Fehlerbehebung bei Cisco IOS Firewall-Konfigurationen und Fehlerbehebung beim Authentifizierungsproxy.

## Problem

HTTP-Downloads können nicht ausgeführt werden, da sie fehlschlagen oder das Zeitlimit überschreiten. Wie wird das gelöst?

## Lösung

Das Problem kann behoben werden, indem der **ip inspect** für HTTP-Datenverkehr entfernt wird, sodass der HTTP-Datenverkehr nicht überprüft wird und der Download wie erwartet erfolgt.

# Zugehörige Informationen

- Support-Seite für IOS-Firewall
- Technischer Support und Dokumentation - Cisco Systems