

# Настройка межсетевого экрана Cisco IOS Firewall для маршрутизатора с двумя интерфейсами с поддержкой NAT

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[!--- конфигурацию](#)

[Проверка](#)

[Устранение неполадок](#)

[Проблема](#)

[Решение](#)

[Дополнительные сведения](#)

## [Введение](#)

Данный образец конфигурации работает для небольшого офиса, подключенного напрямую к Интернету. При этом предполагается, что система доменных имен (DNS), простой протокол передачи почты (SMTP) и веб-службы предоставлены удаленной системой, запущенной на сервере поставщика услуг Интернета (ISP). Внутри сети имеется только два интерфейса и отсутствуют службы. Это делает сеть простой по конфигурации межсетевого экрана. Нет ведения журнала, потому что нет доступного узла, предоставляющего службы ведения журнала.

[Для получения информации о настройке маршрутизатора с тремя интерфейсами без поддержки NAT с использованием межсетевого экрана Cisco IOS® Firewall см. Настройка межсетевого экрана Cisco IOS Firewall для маршрутизатора с тремя интерфейсами без поддержки NAT.](#)

[Для получения информации о настройке маршрутизатора с двумя интерфейсами без поддержки NAT с использованием межсетевого экрана Cisco IOS Firewall см. Настройка межсетевого экрана Cisco IOS Firewall для маршрутизатора с двумя интерфейсами без поддержки NAT.](#)

## [Предварительные условия](#)

## Требования

Для этого документа отсутствуют особые требования.

## Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco IOS Software Release 12.2
- Маршрутизатор Cisco 3640

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

## Общие сведения

Поскольку данная конфигурация использует только входные списки доступа, она поддерживает антиспуфинг и фильтрацию трафика в одном и том же списке доступа (101). Данная конфигурация работает только для двухпортового маршрутизатора. Ethernet 1 является "внутренней" сетью. Serial 0 является внешним интерфейсом. Список доступа (112) в Serial 0 показывает использование трансляции сетевых адресов (NAT) глобальных IP-адресов (150.150.150.x), как мест назначения.

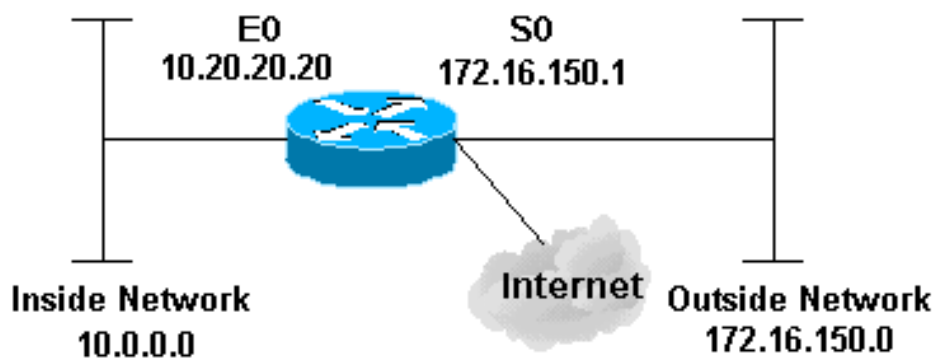
## Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

**Примечание:** [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\)](#) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

## Схема сети

В настоящем документе используется следующая схема сети.



## !--- конфигурацию

В данном документе используется следующая конфигурация.

### Маршрутизатор 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

```

## Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Посредством OIT можно анализировать выходные данные команд show.

- **show version** — отображение информации о текущей загруженной версии программного обеспечения с информацией об оборудовании и устройстве.
- **debug ip nat** — отображение данных о пакетах IP, преобразованных с помощью функции IP NAT.
- **show ip nat translations** — отображение активных трансляций NAT.
- **show log** — отображение информации системного журнала.
- **show ip access-list** — отображение содержимого всех текущих списков доступа IP.
- **show ip inspect session** — отображение существующих сессий, отслеживаемых и проверяемых межсетевым экраном Cisco IOS Firewall.
- **debug ip inspect tcp** — отображение сообщений о событиях межсетевого экрана Cisco IOS Firewall.

В данном примере показаны выходные данные команды **show version**.

```

pig#show version Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3640-
JK903S-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](mailto: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)

**Прежде всего, проверьте корректную работу NAT с помощью команд `debug ip nat` и `show ip nat translations` как показано в выходных данных.**

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

**Без добавления оператора `ip inspect` убедитесь, что все списки доступа работают должным образом. Команда `deny ip any any` с ключевым словом `log` помогут выяснить, какие пакеты заблокированы.**

В этом случае, это ответный трафик Telnet-сессии из 172.16.150.2 от 10.0.0.1 (преобразован в 172.16.150.4).

**В данном примере показаны выходные данные команды `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
```

**Чтобы просмотреть, сколько пакетов соответствуют списку доступа, используйте команду `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#
```

**После добавления оператора ip inspect эта строка будет добавлена в список доступа для разрешения данной Telnet-сессии:**

```
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#
```

**Чтобы просмотреть соединения текущих сессий, установленные через межсетевой экран, можно использовать команду show ip inspect session.**

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

**Со временем (на более "продвинутом" уровне) можно также включить команду 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)
```

## Устранение неполадок

Если соединение не работает после настройки меж сетевого экрана IOS для маршрутизатора, убедитесь, что для интерфейса включена команда проверки ip inspect (name defined) in or out. В данной конфигурации ip inspect ethernetin in применена к интерфейсу Ethernet0/0.

[Для устранения неисправностей для данной конфигурации см. Устранение неисправностей конфигурации Cisco IOS Firewall и Устранение неполадок прокси-сервера аутентификации.](#)

### Проблема

Вы не можете выполнить загрузки http, потому что это отказывает или вызвано таймаут. Как устранить эту проблему?

### Решение

Вопрос может быть решен путем удаления ip inspect для трафика HTTP так, чтобы трафик HTTP не был осмотрен, и загрузка происходит как ожидалось.

## Дополнительные сведения

- [Страница поддержки межсетевого экрана IOS](#)
- [Cisco Systems – техническая поддержка и документация](#)