

# Configuration d'un routeur à deux interfaces avec un pare-feu NAT Cisco IOS Firewall

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Problème](#)

[Solution](#)

[Informations connexes](#)

## [Introduction](#)

Cet exemple de configuration fonctionne pour un tout petit bureau connecté directement à Internet. L'hypothèse est que le service de nom de domaine (DNS), le protocole SMTP (Simple Mail Transfer Protocol) et les services Web sont fournis par un système distant exploité par le fournisseur de services Internet (ISP). Il n'y a aucun service sur le réseau intérieur, ce qui fait de cette configuration de pare-feu l'une des plus simples, car il y a seulement deux interfaces. Il n'est pas nécessaire de se connecter, car il n'y a aucun hôte disponible pour fournir des services de connexion.

Référez-vous à [Routeur à trois interfaces sans configuration de pare-feu Cisco IOS NAT](#) afin de configurer un routeur à trois interfaces sans NAT à l'aide du pare-feu Cisco IOS®.

Référez-vous à [Routeur à deux interfaces sans NAT utilisant la configuration du pare-feu Cisco IOS](#) afin de configurer un routeur à deux interfaces sans NAT utilisant le pare-feu Cisco IOS.

## [Conditions préalables](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

## Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS version 12.2
- Routeur Cisco 3640

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Informations générales

Puisque cette configuration utilise uniquement des listes d'accès d'entrée, elle effectue à la fois un filtrage de trafic et un anti-usurpation avec la même liste d'accès (101). Cette configuration ne fonctionne que pour un routeur à deux ports. Ethernet 1 est le réseau interne. Serial 0 est l'interface externe. La liste d'accès (112) sur l'interface Serial 0 illustre cette situation en utilisant les adresses IP globales de traduction d'adresses de réseau (NAT) (150.150.150.x) comme destinations.

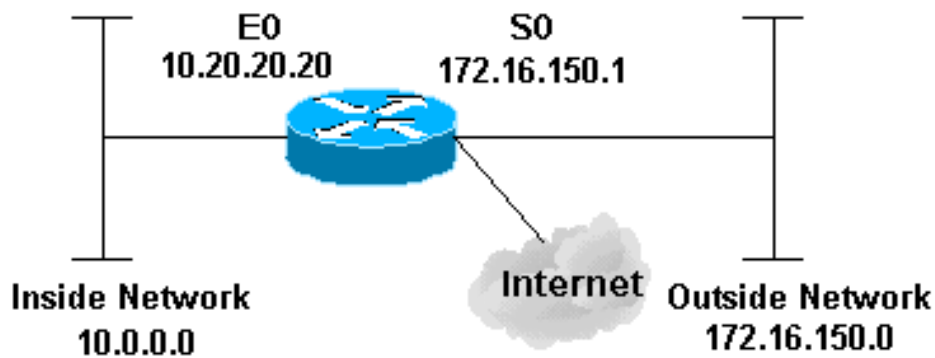
## Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque** : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

Ce document utilise cette configuration du réseau.



## [Configuration](#)

Ce document utilise la configuration suivante .

### Routeur 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
```

## Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines commandes `show`. Utilisez l'OIT pour afficher une analyse de la sortie de la commande `show`.

- **show version** : affiche des informations sur la version logicielle actuellement chargée, ainsi que des informations sur le matériel et les périphériques.
- **debug ip nat** : affiche des informations sur les paquets IP traduits par la fonction NAT IP.
- **show ip nat translations** : affiche les NAT actifs.
- **show log** : affiche les informations de journalisation.
- **show ip access-list** : affiche le contenu de toutes les listes d'accès IP actuelles.
- **show ip inspect session** - Affiche les sessions existantes actuellement suivies et inspectées par le pare-feu Cisco IOS.
- **debug ip inspect tcp** - Affiche les messages relatifs aux événements du pare-feu Cisco IOS.

Voici un exemple de sortie de commande de la commande **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/wvl/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)

**Tout d'abord, vérifiez que NAT fonctionne correctement à l'aide de `debug ip nat` et `show ip nat translations` comme indiqué dans ce résultat.**

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

**Sans ajouter l'instruction `ip inspect`, vérifiez que les listes d'accès fonctionnent correctement. Le `deny ip any any` avec le mot clé `log` vous indique quels paquets sont bloqués.**

Dans ce cas, il s'agit du trafic de retour d'une session Telnet vers 172.16.150.2 à partir de 10.0.0.1 (traduit en 172.16.150.4).

Voici un exemple de sortie de la commande **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
```

Utilisez la commande **show ip access-lists** afin de voir combien de paquets correspondent à la liste d'accès.

```
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#
```

Une fois que vous avez ajouté l'instruction **ip inspect**, vous pouvez voir que cette ligne a été ajoutée dynamiquement dans la liste d'accès afin d'autoriser cette session 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#

Vous pouvez également vérifier à l'aide de la commande **show ip inspect session** qui affiche les sessions en cours qui ont été établies via le pare-feu.

```
pig#show ip inspect session
```

Established Sessions

```
Session 624C31A4 (10.0.0.1:11006)=>(172.16.150.2:23) tcp SIS_OPEN
```

Finalement, à un niveau plus avancé, vous pouvez également activer la commande **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)
```

## Dépannage

Après avoir configuré le routeur de pare-feu IOS, si les connexions ne fonctionnent pas, assurez-vous que vous avez activé l'inspection avec la commande **ip inspect (nom défini) dans ou out** sur l'interface. Dans cette configuration, **ip inspect ethernet in** est appliquée à l'interface **Ethernet0/0**.

Pour un dépannage général sur cette configuration, référez-vous à [Dépannage des configurations de pare-feu Cisco IOS](#) et [Dépannage du proxy d'authentification](#).

## Problème

Vous ne pouvez pas effectuer de téléchargements http, car il échoue ou expire. Comment résoudre ce problème ?

## Solution

Le problème peut être résolu en supprimant **ip inspect** pour le trafic http afin que le trafic http ne soit pas inspecté et que le téléchargement se produise comme prévu.

## Informations connexes

- [Page de support pour le pare-feu d'IOS](#)
- [Support et documentation techniques - Cisco Systems](#)