

NAT Cisco IOS ファイアウォールを使った 2 インターフェイス ルータの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

[問題](#)

[解決方法](#)

[関連情報](#)

概要

この設定例は、インターネットに直接接続された小規模オフィスに適用されます。ドメイン サービス (DNS)、シンプル メール転送プロトコル (SMTP)、および Web サービスはインターネット サービス プロバイダー (ISP) で稼働しているリモート システムから提供されていることを想定しています。インターフェイスが 2 個しかないため、内側のネットワークではサービスはなく、最も簡単なファイアウォール設定の 1 つになります。ログイン サービスの提供に使用可能なホストが存在しないため、ログインも存在しません。

Cisco IOS® ファイアウォールを使用して、NAT を使用しない 3 インターフェイス ルータを設定するには、[NAT Cisco IOS ファイアウォール設定を使用しない 3 インターフェイス ルータを参照してください。](#)

Cisco IOS ファイアウォールを使用して、NAT を使用しない 2 インターフェイス ルータを設定するには、[NAT Cisco IOS ファイアウォール設定を使用しない 2 インターフェイス ルータを参照してください。](#)

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.2
- Cisco 3640 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

この設定では入力用のアクセス リストしか使用しないため、アンチスプーフィングとトラフィックフィルタリングは同じアクセス リスト（101）を使用して行います。この設定は、2 ポートのルータでのみ動作します。Ethernet 1 が「内部」ネットワークです。Serial 0 が外側のインターフェイスです。Serial 0 のアクセス リスト（112）は、ネットワーク アドレス変換（NAT）グローバル IP アドレス（150.150.150.x）を宛先として使用してこれを示しています。

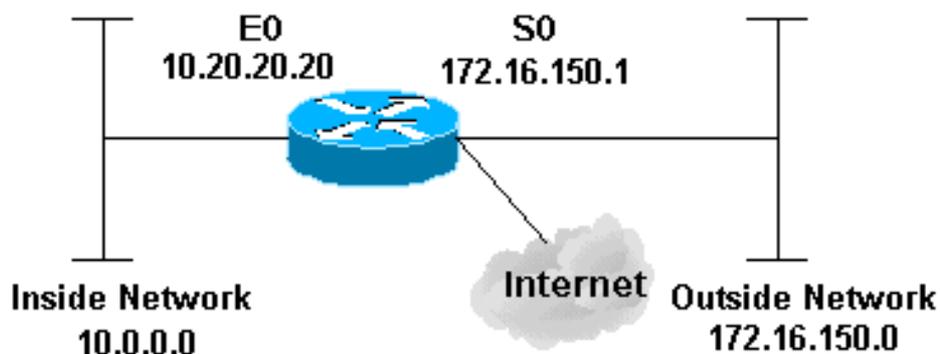
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



コンフィギュレーション

このドキュメントでは次の設定を使用します。

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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show version** : 現在ロードされているソフトウェアバージョンに関する情報を、ハードウェアおよびデバイス情報とともに表示します。
- **debug ip nat** : IP NAT 機能によって変換された IP パケットの情報を表示します。
- **show ip nat translations** : アクティブな NAT を表示します。
- **show log** : ログイン情報を表示します。
- **show ip access-list** : すべての現在の IP アクセス リストの内容を表示します。
- **show ip inspect session** : Cisco IOS Firewall によって現在追跡され、検査されている既存のセッションを表示します。
- **debug ip inspect tcp** : Cisco IOS Firewall イベントに関するメッセージを表示します。

以下に、show version コマンドのサンプル出力を示します。

```
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.

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)

まず、次の出力に示すように、`debug ip nat` と `show ip nat translations` を使用して、NAT が正しく動作することを確認します。

```
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 ステートメントを追加しないで、アクセス リストが正しく機能していることを確認します。**deny ip any any** に **log** キーワードを付けると、ブロックされているパケットがわかります。

この場合、Telnet セッションからのリターン トラフィックで、10.0.0.1 (172.16.150.4 に変換

) から 172.16.150.2 宛てです。

show log コマンドの出力例を次に示します。

```
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
```

アクセスリストと一致するパケットの数を調べるには、show ip access-lists コマンドを使用します。

```
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 ステートメントを追加すると、この Telnet セッションを許可するために次の行がアクセスリストに動的に追加されたことを確認できます。

```
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#

ファイアウォールを介して確立された現行のセッションを表示する `show ip inspect session` コマンドを使用して確認することもできます。

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

Established Sessions

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

最後に、さらに高度なレベルで、`debug ip inspect tcp` コマンドを有効にすることもできます。

```
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)
```

トラブルシューティング

IOS ファイアウォール ルータを設定した後、接続が機能しない場合は、インターフェイス上で `ip inspect (name defined) in or out` コマンドによる検査が有効にされていることを確認してください。この設定では、`ip inspect ethernetin in` はインターフェイス Ethernet0/0 に適用されます。

この設定の一般的なトラブルシューティングについては、[Cisco IOS ファイアウォール設定のトラブルシューティングと認証プロキシのトラブルシューティング](#)を参照してください。

問題

失敗するか、タイムアウトになるため、HTTP ダウンロードを実行できません。どうすれば、この問題を解決できますか。

解決方法

問題は HTTP トラフィックの `ip inspect` を除去して HTTP トラフィックが検査されないようにすることによって解決でき、予期したとおりダウンロードが行われます。

関連情報

- [IOS ファイアウォールのサポート ページ](#)

- [テクニカル サポートとドキュメント – Cisco Systems](#)