

Cisco IOS Firewall を使用する NAT なし 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](#)

[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](#)

[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ている非常に小規模のオフィスで動作するもので、ドメイン ネーム 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と仮定しています。内側のネットワークではサービスは何もなく、インターフェイスが 2 つあるだけです。ロギング サービスを提供するために使用できるホストがないので、ロギングもありません。

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 0 が「内側」のネットワークです。Serial 0 は ISP へのフレーム リレー リンクです。

Cisco IOS® ファイアウォールを使用して、NAT を使用する 2 インターフェイス ルータを設定するには、[Cisco IOS ファイアウォールを使用した NAT を使用する 2 インターフェイス ルータの設定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 3 インターフェイス ルータを設定するには、[Cisco IOS ファイアウォールを使用した NAT を使用しない 3 インターフェイス ルータの設定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適用されます。

- Cisco IOS® ソフトウェア リリース 12.2(15)T13 (Cisco IOS ソフトウェア リリース 11.3.3.T からサポート)
- Cisco 2611 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。

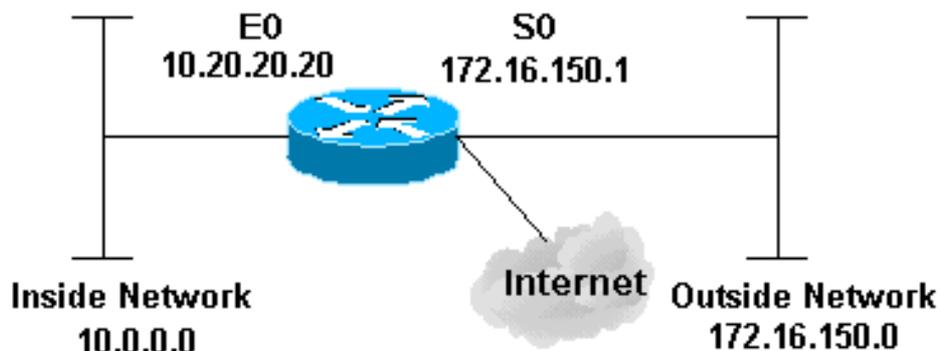
設定

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 セットアップを使用します。



コンフィギュレーション

このドキュメントでは、次の設定を使用しています。

2514 ルータ

```
version 12.2
!
service password-encryption
no service udp-small-servers
no service tcp-small-servers
no cdp run
!
hostname cbac-cisco
!
no ip source-route
!
enable secret 5 $1$FrMn$wBu0Xgv/Igy5Y.DarCmrm/
!
username cisco privilege 15 password 7 0822455D0A16
no ip source-route
ip domain-name cisco.com
ip name-server 172.16.150.5
!
!--- Set up inspection list "myfw". !--- Inspect for the
protocols that actually get used. ! ip inspect name myfw
cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!
interface Ethernet0/0
description Cisco Ethernet RTP
ip address 10.20.20.20 255.255.255.0
no ip directed-broadcast
!
!--- Apply the access list in order to allow all
legitimate traffic !--- from the inside network but
prevent spoofing. ! ip access-group 101 in ! no ip
proxy-arp ! !--- Apply inspection list "myfw" to
Ethernet 0 inbound. !--- When conversations are
initiated from the internal network !--- to the outside,
this inspection list causes temporary additions !--- to
the traffic allowed in by serial interface 0 acl 111
when !--- traffic returns in response to the initiation.
! ip inspect myfw in
no ip route-cache
!
no cdp enable
!
interface Serial0/0
description Cisco FR
ip address 172.16.150.1 255.255.255.0
encapsulation frame-relay IETF
no ip route-cache
no arp frame-relay
bandwidth 56
```

```
service-module 56 clock source line
service-module 56k network-type dds
frame-relay lmi-type ansi
!
!--- Access list 111 allows some ICMP traffic and
administrative Telnet, !--- and does anti-spoofing.
There is no inspection on Serial 0. !--- However, the
inspection on the Ethernet interface adds temporary
entries !--- to this list when hosts on the internal
network make connections !--- out through the Frame
Relay. ! ip access-group 111 in no ip directed-broadcast
no ip route-cache bandwidth 56 no cdp enable frame-relay
interface-dlci 16 ! ip classless ip route 0.0.0.0
0.0.0.0 Serial0 ! !--- Access list 20 is used to control
which network management stations !--- can access
through SNMP. ! access-list 20 permit 172.16.150.8 ! !--
- The access list allows all legitimate traffic from the
inside network !--- but prevents spoofing. ! access-list
101 permit tcp 172.16.150.0 0.0.0.255 any access-list
101 permit udp 172.16.150.0 0.0.0.255 any access-list
101 permit icmp 172.16.150.0 0.0.0.255 any !--- This
deny is the default. access-list 101 deny ip any any !
!--- Access list 111 controls what can come from the
outside world !--- and it is anti-spoofing. ! access-
list 111 deny ip 127.0.0.0 0.255.255.255 any access-list
111 deny ip 172.16.150.0 0.0.0.255 any ! !--- Perform an
ICMP stuff first. There is some danger in these lists.
!--- They are control packets, and allowing *any* packet
opens !--- you up to some possible attacks. For example,
teardrop-style !--- fragmentation attacks can come
through this list. ! access-list 111 permit icmp any
172.16.150.0 0.0.0.255 administratively-prohibited
access-list 111 permit icmp any 172.16.150.0 0.0.0.255
echo access-list 111 permit icmp any 172.16.150.0
0.0.0.255 echo-reply access-list 111 permit icmp any
172.16.150.0 0.0.0.255 packet-too-big access-list 111
permit icmp any 172.16.150.0 0.0.0.255 time-exceeded
access-list 111 permit icmp any 172.16.150.0 0.0.0.255
traceroute access-list 111 permit icmp any 172.16.150.0
0.0.0.255 unreachable ! !--- Allow Telnet access from
10.11.11.0 corporate network administration people. !
access-list 111 permit tcp 10.11.11.0 0.0.0.255 host
172.16.150.1 eq telnet ! !--- This deny is the default.
! access-list 111 deny ip any any ! !--- Apply access
list 20 for SNMP process. ! snmp-server community secret
RO 20 ! line con 0 exec-timeout 5 0 password 7
14191D1815023F2036 login local line vty 0 4 exec-timeout
5 0 password 7 14191D1815023F2036 login local length 35
end
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

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 myfw in はインターフェイス Ethernet0/0 に適用されます。

[これらのコマンド、およびその他のトラブルシューティング情報については、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。](#)

注：debugコマンドを発行する前に、『[debugコマンドの重要な情報](#)』を参照してください。

[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](#)