Router a due interfacce senza NAT con configurazione Cisco IOS Firewall

Sommario

Introduzione

Questa configurazione di esempio funziona per un ufficio molto piccolo che si connette direttamente a Internet, presupponendo che i servizi DNS (Domain Name Service), SMTP (Simple Mail Transfer Protocol) e Web siano forniti da un sistema remoto eseguito dal provider di servizi Internet (ISP). La rete interna non contiene servizi e sono presenti solo due interfacce. Inoltre, non è disponibile alcuna registrazione perché non è disponibile alcun host per fornire i servizi di registrazione.

Poiché questa configurazione utilizza solo elenchi degli accessi di input, esegue sia l'anti-spoofing che il filtro del traffico con lo stesso elenco degli accessi. Questa configurazione funziona solo con un router a due porte. Ethernet 0 è la rete "interna". Il numero seriale 0 è un collegamento Frame Relay all'ISP.

Per configurare un router a due interfacce con NAT usando un firewall Cisco IOS, consultare il documento sulla configurazione del firewall NAT di Cisco IOS®.

Per configurare un router a tre interfacce senza NAT con un firewall Cisco IOS, consultare il documento sulla configurazione del firewall a tre interfacce senza NAT.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si applicano alle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.2(15)T13, supportato dal software Cisco IOS versione 11.3.3.T
- Cisco 2611 router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

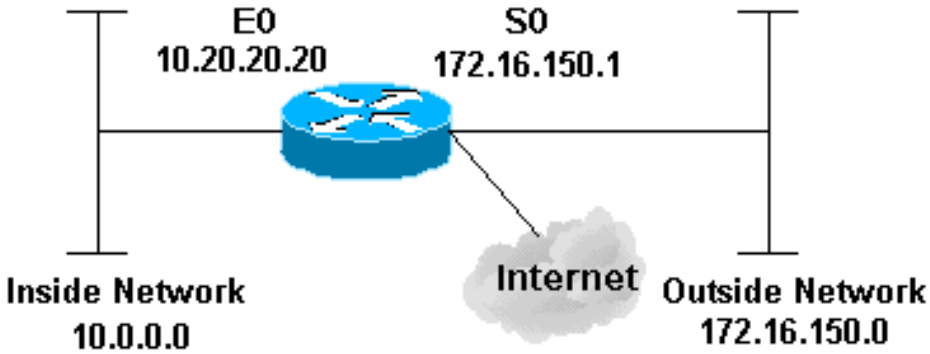
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione

Nel documento viene usata questa configurazione:

2514 Router

```
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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Dopo aver configurato il router del firewall IOS, se le connessioni non funzionano, verificare di aver abilitato l'ispezione con il comando **ip inspect (nome definito)** sull'interfaccia **in o out**. In

questa configurazione, l'opzione **ip inspect myfw in** viene applicata all'interfaccia Ethernet0/0.

Per questi comandi e altre informazioni sulla risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi del proxy di autenticazione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Informazioni correlate

- Pagina di supporto di IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems