Router mit zwei Schnittstellen ohne NAT mithilfe der Cisco IOS Firewall-Konfiguration

Inhalt

Einführung

Diese Beispielkonfiguration funktioniert in einem sehr kleinen Büro, das direkt mit dem Internet verbunden ist. Dabei wird davon ausgegangen, dass der Domain Name Service (DNS), das Simple Mail Transfer Protocol (SMTP) und die Webdienste von einem Remote-System bereitgestellt werden, das vom Internet Service Provider (ISP) ausgeführt wird. Innerhalb des Netzwerks gibt es keine Services und nur zwei Schnittstellen. Es wird auch keine Protokollierung durchgeführt, da kein Host für Protokollierungsdienste verfügbar ist.

Da bei dieser Konfiguration nur Zugriffslisten für die Eingabe verwendet werden, werden Spoofing- und Datenverkehrsfilter mit derselben Zugriffsliste ausgeführt. Diese Konfiguration funktioniert nur bei Routern mit zwei Ports. Ethernet 0 ist das "interne" Netzwerk. Serial 0 ist ein Frame Relay-Link zum ISP.

Unter Konfiguration der NAT-Cisco IOS-Firewall mit Zweischnittstelle-Router können Sie einen Zwei-Schnittstellen-Router mit NAT mithilfe einer Cisco IOS®-Firewall konfigurieren.

Informationen zur Konfiguration eines Routers mit drei Schnittstellen ohne NAT unter Verwendung einer Cisco IOS Firewall finden Sie unter Drei-Schnittstellen-Router ohne NAT.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument gelten für die folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.2(15)T13, unterstützt von der Cisco IOS Softwareversion 11.3.3.T
- Cisco 2611-Router

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

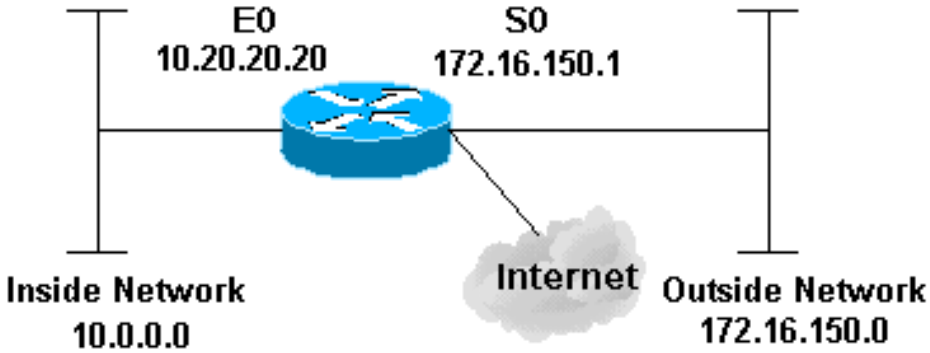
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

Router 2514

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Wenn Sie den IOS-Firewall-Router konfiguriert haben und die Verbindungen nicht funktionieren, stellen Sie sicher, dass die Überprüfung mit dem Befehl **ip inspect (name defined) in oder out** auf der Schnittstelle aktiviert ist. In dieser Konfiguration wird **ip inspect myfw in** für die Schnittstelle

Ethernet0/0 angewendet.

Weitere Informationen zu diesen Befehlen sowie weitere Informationen zur Fehlerbehebung finden Sie unter Troubleshooting Authentication Proxy.

Hinweis: Lesen Sie vor dem Ausgabe von **Debug**-Befehlen unter Wichtige Informationen zu Debug-Befehlen nach.

Zugehörige Informationen

- Support-Seite für IOS-Firewall
- Technischer Support und Dokumentation - Cisco Systems