Configuration d'un routeur à deux interfaces sans NAT à l'aide du pare-feu Cisco IOS Firewall

Contenu

Introduction

Cette configuration d'échantillon fonctionne pour une très petite entreprise qui se connecte directement à l'Internet, à la supposition que le domain name service (DN), 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 services sur le réseau intérieur et seulement deux interfaces. Il n'y a également aucun se connecter parce qu'il n'y a aucun hôte disponible pour fournir se connecter des services.

Puisque cette configuration utilise seulement des listes d'accès en entrée, elle fait l'anti-mystification et le filtrage de trafic avec la même liste d'accès. Cette configuration fonctionne seulement pour un routeur à deux orifices. L'Ethernet 0 est le réseau de « intérieur ». L'interface série 0 est un lien de Relais de trames à l'ISP.

Référez-vous au routeur à deux interfaces avec la configuration NAT de Pare-feu Cisco IOS afin de configurer un routeur de deux interfaces avec NAT utilisant un Pare-feu de Cisco IOS®.

Référez-vous au routeur à trois interfaces sans configuration NAT de Pare-feu Cisco IOS afin de configurer un routeur de trois interfaces sans NAT utilisant un Pare-feu Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document appliquent aux ces le logiciel et les versions de matériel :

- Version de logiciel 12.2(15)T13 de Cisco IOS®, prise en charge de la version du logiciel Cisco IOS 11.3.3.T
- Routeur de Cisco 2611

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

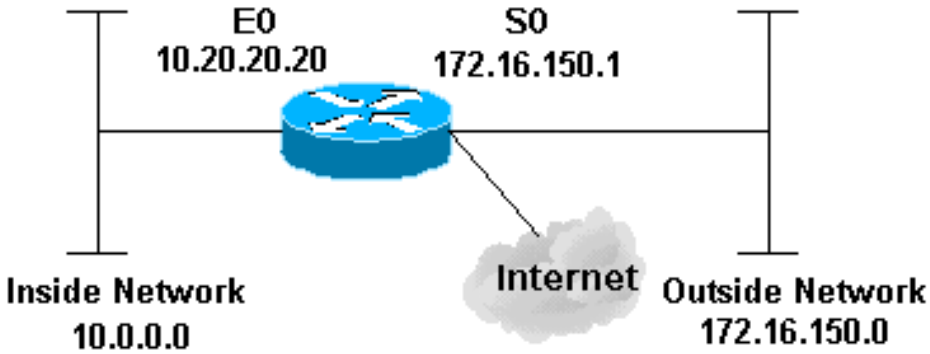
Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

Ce document utilise la configuration suivante :

Routeur 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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Après que vous configuriez le routeur du pare-feu d'IOS, si les connexions ne fonctionnent pas, assurez-vous que vous avez activé l'inspection avec l'**ip inspect (nom défini) dans ou** commandez sur l'interface. Dans cette configuration, le **myfw d'ip inspect** est **dedans** appliqué pour l'interface Ethernet0/0.

Pour ces commandes, avec l'autre information de dépannage, référez-vous au Seveur mandataire d'authentification de dépannage.

Remarque: Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **debug**.

Informations connexes

- Page de support pour le pare-feu d'IOS
- Support et documentation techniques - Cisco Systems