Configuration d'un routeur à trois interfaces sans un pare-feu NAT Cisco IOS Firewall

Contenu

Introduction

Ce document fournit un exemple d'une configuration typique pour une petite entreprise qui est connectée à l'Internet et exécute ses propres serveurs. La connexion à Internet est au-dessus d'une ligne série. L'Ethernet 0 est connecté au réseau interne (un LAN unique). L'Ethernet 1 est connecté à un réseau DMZ, qui a un noeud simple utilisé pour fournir des services au monde extérieur. L'ISP a assigné à la société le netblock 192.168.27.0/24. Ceci est également séparé entre le DMZ et le RÉSEAU LOCAL interne avec le masque de sous-réseau 255.255.255.128. La stratégie de base est à :

- Permettez aux utilisateurs sur le réseau intérieur pour se connecter à n'importe quel service sur l'Internet public.
- Permettez à n'importe qui sur l'Internet pour se connecter au WWW, au FTP, et aux services de Protocole SMTP (Simple Mail Transfer Protocol) sur le serveur DMZ, et pour leur faire des requêtes de Système de noms de domaine (DNS). Ceci permet aux personnes extérieures pour visualiser des pages Web de société, reprendre classe la société a signalé pour la consommation extérieure, et envoyer la messagerie dans la société.
- Permettez aux utilisateurs intérieurs pour se connecter au service POP sur le serveur DMZ (pour prendre leur messagerie) et au telnet à lui (pour le gérer).
- Ne permettre rien à sur le DMZ initier toutes connexions, au réseau privé ou à l'Internet.
- Apurez toutes les connexions qui croisent le Pare-feu à un serveur de SYSLOG sur le net privé. Les ordinateurs sur le réseau intérieur utilisent le serveur DNS sur le DMZ. Des listes d'accès en entrée sont utilisées sur toutes les interfaces afin d'empêcher charrier. Des listes d'accès de sortie sont utilisées pour contrôler quel trafic peut être envoyé à n'importe quelle interface donnée.

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

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 Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document sont basées sur les versions de logiciel et matériel suivantes :

- Version du logiciel Cisco IOS 12.2(15)T13 avec le Firewall Feature Set
- Routeur Cisco 7204VXR

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.

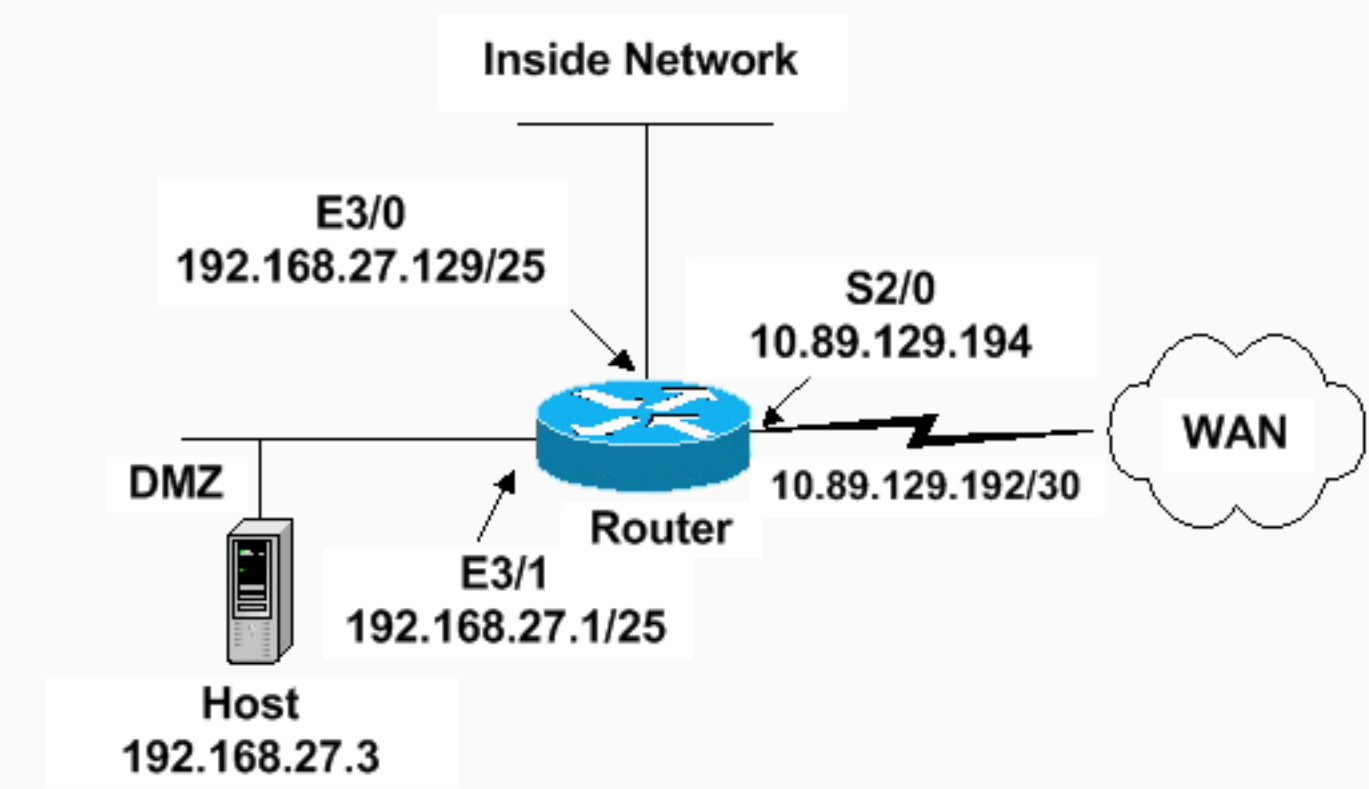
Configurez

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 :



Configurations

Ce document utilise cette configuration.

Routeur 7204 VXR

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
logging queue-limit 100
enable secret 5 <something>
!
ip subnet-zero
ip cef
no ip domain lookup
!
ip inspect audit-trail
!
 !--- Sets the length of time a TCP session !--- is
still managed after no activity. ! ip inspect tcp idle-
time 14400 ! !--- Sets the length of time a UDP session
!--- is still managed after no activity. ! ip inspect
udp idle-time 1800 ! !--- Sets the length of time a DNS
name lookup session !--- is still managed after no
activity. ! ip inspect dns-timeout 7 ! !--- Sets up
inspection list "standard" !--- to be used for
inspection of inbound Ethernet 0 !--- and inbound serial
(applied to both interfaces). ! ip inspect name standard
cuseeme ip inspect name standard ftp ip inspect name
standard h323 ip inspect name standard http ip inspect
name standard rcmd ip inspect name standard realaudio ip
inspect name standard smtp ip inspect name standard
sqlnet ip inspect name standard streamworks ip inspect
```

```
name standard tcp ip inspect name standard tftp ip
inspect name standard udp ip inspect name standard
vdolive ip audit notify log ip audit po max-events 100 !
no voice hpi capture buffer no voice hpi capture
destination ! mta receive maximum-recipients 0 !
interface ethernet 3/0 ip address 192.168.27.129
255.255.255.128 ! !--- Apply the access list to allow
all legitimate !--- traffic from the inside network and
prevent spoofing. ! ip access-group 101 in ! !--- Apply
inspection list "standard" for inspection !--- of
inbound Ethernet traffic. This inspection opens !---
temporary entries on access lists 111 and 121. ! ip
inspect standard in duplex full interface ethernet 3/1
ip address 192.168.27.1 255.255.255.128 ! !--- Apply the
access list to permit DMZ traffic (except spoofing) !---
on the DMZ interface inbound. The DMZ is not permitted
to initiate !--- any outbound traffic except Internet
Control Message Protocol (ICMP). ! ip access-group 111
in ! !--- Apply inspection list "standard" for
inspection of outbound !--- traffic from e1. This adds
temporary entries on access list 111 !--- to allow
return traffic, and protects servers in DMZ from !---
distributed denial of service (DDoS) attacks. ip inspect
standard out duplex full ! interface serial 2/0 ip
address 10.89.129.194 255.255.255.252 !--- Apply the
access list to allow legitimate traffic. ! ip access-
group 121 in serial restart_delay 0 ! ip classless no ip
http-server !--- A syslog server is located at this
address. logging 192.168.27.131 !--- This command
enables the logging of session !--- information
(addresses and bytes). !--- Access list 20 is used to
control which !--- network management stations can
access via SNMP. ! access-list 20 permit 192.168.27.5 !
!--- Use an access list to allow all legitimate traffic
from !--- the inside network and prevent spoofing. The
inside !--- network can only connect to the Telnet and
POP3 !--- service of 192.168.27.3 on DMZ, and can ping
(ICMP) to the DMZ. !--- Additional entries can be added
to permit SMTP, WWW, and !--- so forth, if necessary. In
addition, the inside network can !--- connect to any
service on the Internet. ! access-list 101 permit tcp
192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3
access-list 101 permit tcp 192.168.27.128 0.0.0.127 host
192.168.27.3 eq telnet access-list 101 permit icmp
192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 access-
list 101 deny ip 192.168.27.128 0.0.0.127 192.168.27.0
0.0.0.127 access-list 101 permit ip 192.168.27.128
0.0.0.127 any access-list 101 deny ip any any ! ! !---
The access list permits ping (ICMP) from the DMZ and
denies all !--- traffic initiated from the DMZ.
Inspection opens !--- temporary entries to this list. !
access-list 111 permit icmp 192.168.27.0 0.0.0.127 any
access-list 111 deny ip any any ! ! ! !--- Access list
121 allows anyone on the Internet to connect to !---
WWW, FTP, DNS, and SMTP services on the DMZ host. It
also !--- allows some ICMP traffic. access-list 121
permit udp any host 192.168.27.3 eq domain access-list
121 permit tcp any host 192.168.27.3 eq domain access-
list 121 permit tcp any host 192.168.27.3 eq www access-
list 121 permit tcp any host 192.168.27.3 eq ftp access-
list 121 permit tcp any host 192.168.27.3 eq smtp
access-list 121 permit icmp any 192.168.27.0 0.0.0.255
administratively-prohibited access-list 121 permit icmp
any 192.168.27.0 0.0.0.255 echo access-list 121 permit
```

```
icmp any 192.168.27.0 0.0.0.255 echo-reply access-list
121 permit icmp any 192.168.27.0 0.0.0.255 packet-too-
big access-list 121 permit icmp any 192.169.27.0
0.0.0.255 time-exceeded access-list 121 permit icmp any
192.168.27.0 0.0.0.255 traceroute access-list 121 permit
icmp any 192.168.27.0 0.0.0.255 unreachable access-list
121 deny ip any any ! !--- Apply access list 20 for SNMP
process. ! snmp-server community secret RO 20 snmp-
server enable traps tty ! call rsvp-sync ! mgcp profile
default ! dial-peer cor custom ! gatekeeper shutdown !
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

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **liste d'accès d'exposition** — Vérifie la configuration correcte des Listes d'accès configurées en configuration courante.`Router#show access-list Standard IP access list 20 10 permit 192.168.27.5 Extended IP access list 101 10 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq pop3 20 permit tcp 192.168.27.128 0.0.0.127 host 192.168.27.3 eq telnet 30 permit icmp 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 40 deny ip 192.168.27.128 0.0.0.127 192.168.27.0 0.0.0.127 50 permit ip 192.168.27.128 0.0.0.127 any 60 deny ip any any Extended IP access list 111 10 permit icmp 192.168.27.0 0.0.0.127 any 20 deny ip any any (9 matches) Extended IP access list 121 10 permit udp any host 192.168.27.3 eq domain 20 permit tcp any host 192.168.27.3 eq domain 30 permit tcp any host 192.168.27.3 eq www 40 permit tcp any host 192.168.27.3 eq ftp 50 permit tcp any host 192.168.27.3 eq smtp 60 permit icmp any 192.168.27.0 0.0.0.255 administratively-prohibited 70 permit icmp any 192.168.27.0 0.0.0.255 echo 80 permit icmp any 192.168.27.0 0.0.0.255 echo-reply 90 permit icmp any 192.168.27.0 0.0.0.255 packet-too-big 100 permit icmp any 192.169.27.0 0.0.0.255 time-exceeded 110 permit icmp any 192.168.27.0 0.0.0.255 traceroute 120 permit icmp any 192.168.27.0 0.0.0.255 unreachable 130 deny ip any any (4866 matches) Router#`
- **l'audit de show ip** vérifie **entièrement la** configuration des commandes se connectantes.`Router#show ip audit all Event notification through syslog is enabled Event notification through Net Director is disabled Default action(s) for info signatures is alarm Default action(s) for attack signatures is alarm Default threshold of recipients for spam signature is 250 PostOffice:HostID:0 OrgID:0 Msg dropped:0 :Curr Event Buf Size:0 Configured:100 Post Office is not enabled - No connections are active Router#`
- **le show ip inspect** vérifie **entièrement la** configuration des règles d'inspection de Pare-feu Cisco IOS par interface.`Router#show ip inspect all Session audit trail is enabled Session alert is enabled one-minute (sampling period) thresholds are [400:500] connections max-incomplete sessions thresholds are [400:500] max-incomplete tcp connections per host is 50. Block-time 0 minute. tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec tcp idle-time is 14400 sec -- udp idle-time is 1800 sec dns-timeout is 7 sec Inspection Rule Configuration Inspection name standard cuseeme alert is on audit-trail is on timeout 14400 ftp alert is on audit-trail is on timeout 14400 h323 alert is on audit-trail is on timeout 14400 http alert is on audit-trail is on timeout 14400 rcmd alert is on audit-trail is on timeout 14400 realaudio alert is on audit-trail is on timeout 14400 smtp alert is on audit-trail is on timeout 14400 sqlnet alert is on audit-trail is on timeout 14400 streamworks alert is on audit-trail is on timeout 1800 tcp alert is on audit-trail is on timeout 14400 tftp alert is on audit-trail is on timeout 1800 udp alert is on audit-trail is on timeout 1800 vdolive alert is on audit-trail is on timeout 14400 Interface Configuration Interface Ethernet3/0 Inbound inspection rule is standard cuseeme alert is on audit-trail is on timeout 14400 ftp alert is on audit-trail is on timeout 14400 h323 alert is on audit-trail is on timeout 14400`

```
http alert is on audit-trail is on timeout 14400 rcmd alert is on audit-trail is on timeout
14400 realaudio alert is on audit-trail is on timeout 14400 smtp alert is on audit-trail is
on timeout 14400 sqlnet alert is on audit-trail is on timeout 14400 streamworks alert is on
audit-trail is on timeout 1800 tcp alert is on audit-trail is on timeout 14400 tftp alert is
on audit-trail is on timeout 1800 udp alert is on audit-trail is on timeout 1800 vdolive
alert is on audit-trail is on timeout 14400 Outgoing inspection rule is not set Inbound
access list is 101 Outgoing access list is not set Interface Ethernet3/1 Inbound inspection
rule is not set Outgoing inspection rule is standard cuseeme alert is on audit-trail is on
timeout 14400 ftp alert is on audit-trail is on timeout 14400 h323 alert is on audit-trail
is on timeout 14400 http alert is on audit-trail is on timeout 14400 rcmd alert is on audit-
trail is on timeout 14400 realaudio alert is on audit-trail is on timeout 14400 smtp alert
is on audit-trail is on timeout 14400 sqlnet alert is on audit-trail is on timeout 14400
streamworks alert is on audit-trail is on timeout 1800 tcp alert is on audit-trail is on
timeout 14400 tftp alert is on audit-trail is on timeout 1800 udp alert is on audit-trail is
on timeout 1800 vdolive alert is on audit-trail is on timeout 14400 Inbound access list is
111 Outgoing access list is not set Router#
```

Dépannez

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, la **norme d'ip inspect** est **dedans** appliquée pour les Ethernets 3/0 d'interface et la **norme d'ip inspect** est appliquée pour les Ethernets 3/1 d'interface.

Référez-vous aux configurations de Pare-feu Cisco IOS de dépannage pour plus d'informations sur le dépannage.

Informations connexes

- Page de support de Pare-feu Cisco IOS
- Support et documentation techniques - Cisco Systems