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

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Conventions](#)
[Configuration](#)
[Diagramme du réseau](#)
[Configurations](#)
[Vérification](#)
[Dépannage](#)
[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration type pour une petite entreprise connectée à Internet et exécutant ses propres serveurs. La connexion à Internet se fait par une ligne série. Ethernet 0 est connecté au réseau interne (un réseau local unique). Ethernet 1 est connecté à un réseau DMZ, dont un noeud unique est utilisé pour fournir des services au monde extérieur. Le FAI a attribué à la société le netblock 192.168.27.0/24. Ceci est également partagé entre la DMZ et le réseau local interne avec le masque de sous-réseau 255.255.255.128. La politique de base est la suivante :

- Autoriser les utilisateurs du réseau interne à se connecter à n'importe quel service sur l'Internet public.
- Autoriser toute personne sur Internet à se connecter aux services WWW, FTP et SMTP (Simple Mail Transfer Protocol) sur le serveur DMZ, et à lui envoyer des requêtes DNS (Domain Name System). Cela permet aux personnes extérieures de consulter les pages Web de la société, de récupérer les fichiers que la société a publiés pour consommation externe et d'envoyer des courriels à la société.
- Autoriser les utilisateurs internes à se connecter au service POP sur le serveur DMZ (pour récupérer leur courrier) et à établir une connexion Telnet avec lui (pour l'administrer).
- Ne permet à aucune connexion de la zone démilitarisée d'établir une connexion, que ce soit au réseau privé ou à Internet.
- Audit de toutes les connexions qui traversent le pare-feu vers un serveur SYSLOG sur le réseau privé. Les machines du réseau interne utilisent le serveur DNS sur la DMZ. Les listes d’accès d’entrée sont utilisées sur toutes les interfaces afin d’empêcher l’usurpation. Les listes d’accès en sortie permettent de contrôler le trafic pouvant être envoyé à n’importe quelle

interface donnée.

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

Référez-vous à Configuration de pare-feu Cisco IOS pour deux interfaces avec NAT afin de configurer un routeur à deux interfaces avec NAT à l'aide d'un pare-feu Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Logiciel Cisco IOS Version 12.2(15)T13 avec jeu de fonctions de pare-feu
- Routeur Cisco 7204 VXR

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

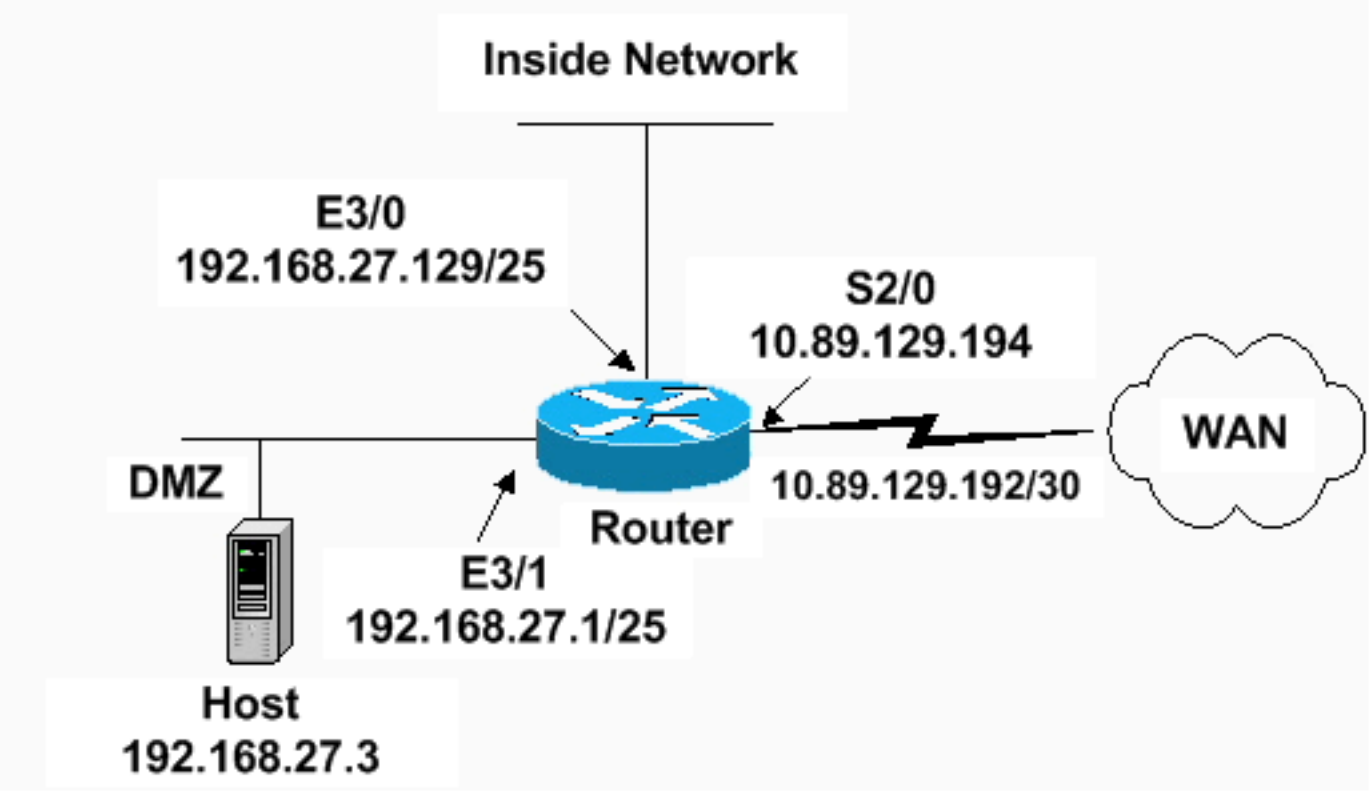
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) 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 la configuration suivante .

Routeur VXR 7204

```
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
```

Vérification

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** .

- **show access-list** - Vérifie la configuration correcte des listes d'accès configurées dans la configuration en cours.

```
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#
```

- **show ip audit all** : vérifie la configuration des commandes logging.

```
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#
```

- **show ip inspect all** - Vérifie la configuration des règles d'inspection du 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#
```

Dépannage

Après avoir configuré le routeur de pare-feu IOS, si les connexions ne fonctionnent pas, assurez-vous que vous avez activé l'inspection avec la commande **ip inspect (nom défini) dans ou out** sur

l'interface. Dans cette configuration, la **norme ip inspect in** est appliquée à l'interface ethernet 3/0 et la **norme ip inspect out** est appliquée à l'interface ethernet 3/1.

Référez-vous à Dépannage des configurations de pare-feu Cisco IOS pour plus d'informations sur le dépannage.

Informations connexes

- Page d'assistance Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems