Cisco IOS ファイアウォールを使用した NAT を使用しない 3 インターフェイス ルータの設定

目次

概要

この文書では、インターネットに接続して独自のサーバを実行する中小企業向けの典型的な設定の例を示します。 インターネットへの接続はシリアル回線を経由します。 イーサネット 0 は内部ネットワーク (単一の LAN) に接続します。 イーサネット 1 は「DMZ」ネットワークに接続します。このネットワークには、外部へのサービス提供に使用する単一のノードがあります。 ISP からはネットブロック 192.168.27.0/24 が会社に割り当てられています。 このネットブロックはサブネット マスク 255.255.255.128 を使用して DMZ と内部 LAN とに均等に分割されています。 基本ポリシーを次に示します。

- 内部ネットワークのユーザがパブリック インターネット上のあらゆるサービスに接続できる。
- インターネット上のだれもが DMZ サーバ上の WWW、FTP、SMTP の各サービスに接続でき、DMZ サーバに DNS 問い合せを実行できる。 これにより、外部ユーザは会社の Web ページを閲覧したり、外部で利用してもらうために会社が掲載したファイルを選択したり、メールを会社に送信したりできます。
- 内部ユーザが DMZ サーバ上の POP サービスに接続し (自分のメールを選択するため)、DMZ サーバに Telnet できる (DMZ サーバを管理するため)。
- DMZ 上からプライベート ネットワークまたはインターネットへの接続をいっさい開始できない。
- ファイアウォールを経由するすべての接続をプライベート ネットワーク上の SYSLOG サーバで監査する。 内部ネットワーク上のコンピュータは DMZ 上の DNS サーバを使用します。 すべてのインターフェイス上で入力アクセス リストを使用し、スプーフィングを防ぎます。 出力アクセス リストを使用し、どのトラフィックが特定のインターフェイスに送信されるのかを制御します。

Cisco IOS® ファイアウォールを使用して、NAT を使用しない 2 インターフェイス ルータを設定するには、『Cisco IOS ファイアウォールを使用した、NAT を使用しない 2 インターフェイス ルータの設定』を参照してください。

Cisco IOS ファイアウォールを使用して、NAT を使用する 2 インターフェイス ルータを設定するには、『NAT CBAC 設定での 2 インターフェイス ルータ』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.2(15)T13（ファイアウォール機能セット付き）
- Cisco 7204 VXR ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

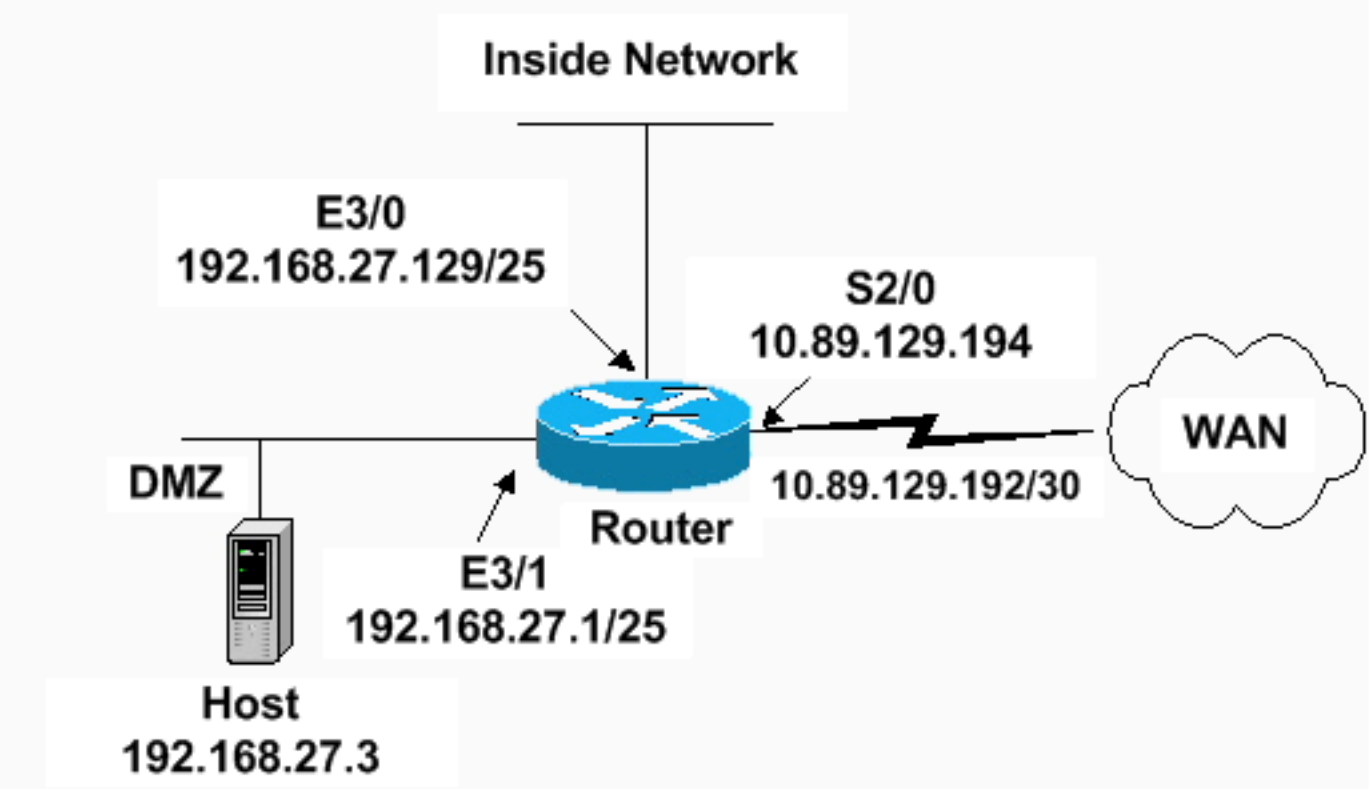
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは次の設定を使用します。

7204VXR ルータ

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show access-list**：上の例で設定されたアクセス リストが正しく設定されていることを確認します。`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#`
- **全 IP が監査** logging コマンドの設定を確認することを示して下さい。`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#`
- **全 ip inspect が**インターフェイスごとの Cisco IOS ファイアウォール インスペクション ルールの設定を確認することを示して下さい。`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#
```

トラブルシューティング

IOS ファイアウォール ルータを設定した後、接続が機能しない場合は、インターフェイス上で **ip inspect (name defined) in or out** コマンドによる検査を有効にしてあることを確認してください。この設定では、**ip inspect standard in** がインターフェイス イーサネット 3/0 に適用され、**ip inspect standard out** がインターフェイス イーサネット 3/1 に適用されています。

トラブルシューティングの詳細については、『CBAC 設定のトラブルシューティング』を参照してください。

関連情報

- Cisco IOS Firewall に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems