Cisco: Configuring the Zone-Based Firewall (ZBF)

Introduction

Zone-Based Firewall (ZBF) is a modern approach to traffic filtering in Cisco routers, replacing classic ACLs and CBACs. It is based on assigning interfaces to zones and then defining policies between zones.

Configuration steps

Create zones

Define the zones to which you will assign the interfaces:

```
zone security ZONA-WEW
zone security ZONA-INTERNET
```

Assigning interfaces to zones

```
interface GigabitEthernet0/0
zone-member security ZONA-WEW

interface GigabitEthernet0/1
zone-member security ZONA-INTERNET
```

Creating a traffic class

Specify what type of movement will be recognised:

```
class-map type inspect match-any CMAP-WWW
match protocol http
match protocol https
```

Creating a traffic policy

```
policy-map type inspect PMAP-WEW-INTERNET
class type inspect CMAP-WWW
inspect
class class-default
```

```
drop
```

Linking policy to traffic between zones

```
zone-pair security ZP-WEW-DO-INTERNET source ZONA-WEW destination ZONA-
INTERNET
service-policy type inspect PMAP-WEW-INTERNET
```

Verification

```
show zone security
show zone-pair security
show policy-map type inspect zone-pair
```

Comments

- If an interface does not belong to any zone, it cannot exchange traffic with any other interface.
- The `inspect` command means to allow and track sessions.
- The `drop` command blocks unspecified traffic by default.

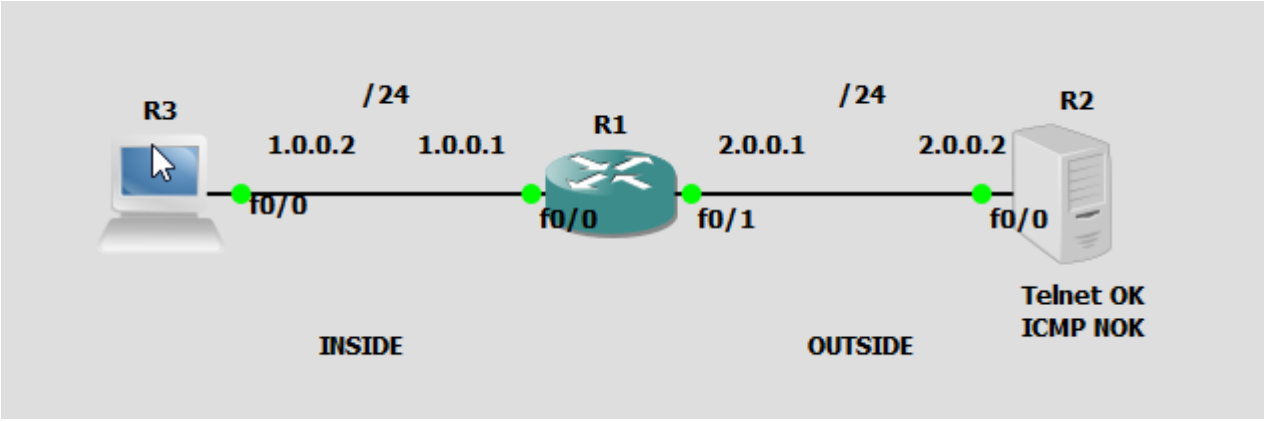
Example of extension

Adding a rule for ICMP:

```
class-map type inspect match-any CMAP-PING
match protocol icmp

policy-map type inspect PMAP-WEW-INTERNET
class type inspect CMAP-WWW
inspect
class type inspect CMAP-PING
inspect
class class-default
drop
```

Configuration example



router configuration:

```
*Mar  1 00:20:35.819: %SYS-5-CONFIG_I: Configured from console by console
R1#show running-config
Building configuration...

Current configuration : 1701 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
class-map type inspect match-any TELNET-CLASS
 match protocol telnet
!
!
policy-map type inspect POLICY-INSIDE-TO-OUTSIDE
 class type inspect TELNET-CLASS
  inspect
 class class-default
  drop
!
zone security INSIDE
zone security OUTSIDE
zone-pair security ZP-INSIDE-OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect POLICY-INSIDE-TO-OUTSIDE
!
!
!
!
interface FastEthernet0/0
 ip address 1.0.0.1 255.255.255.0
 zone-member security INSIDE
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
```

```
 ip address 2.0.0.1 255.255.255.0
 zone-member security OUTSIDE
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Test:

```
R3# ping 2.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R3#telnet 2.0.0.2
Trying 2.0.0.2 ... Open


User Access Verification

Username: admin
Password:
R2>
```