

Cisco: Konfiguracja Zone-Based Firewall (ZBF)

Wprowadzenie

Zone-Based Firewall (ZBF) to nowoczesne podejście do filtrowania ruchu w routerach Cisco, zastępujące klasyczne ACL i CBAC. Bazuje na przydzieleniu interfejsów do stref (zones), a następnie definiowaniu polityk między strefami.

Kroki konfiguracji

Tworzenie stref

Zdefiniuj strefy, do których przypiszesz interfejsy:

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

Przypisanie interfejsów do stref

```
interface GigabitEthernet0/0  
zone-member security ZONA-WEW  
  
interface GigabitEthernet0/1  
zone-member security ZONA-INTERNET
```

Tworzenie klasy ruchu

Określ, jaki typ ruchu będzie rozpoznawany:

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

Tworzenie polityki ruchu

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

```
drop
```

Powiązanie polityki z ruchem między strefami

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

Weryfikacja

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

Uwagi

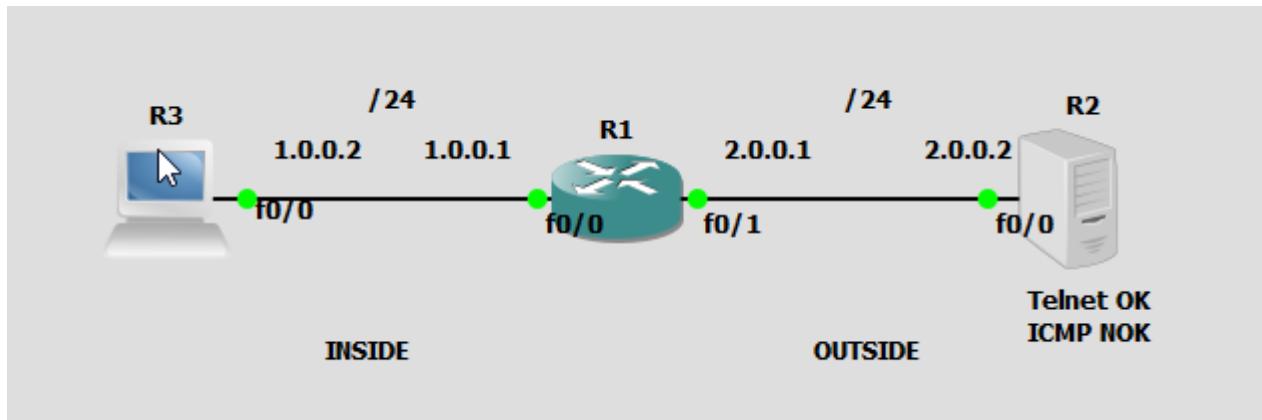
- Jeśli interfejs nie należy do żadnej strefy, to nie może wymieniać ruchu z żadnym innym interfejsem.
- Komenda `inspect` oznacza zezwolenie i śledzenie sesji.
- Komenda `drop` blokuje nieokreślony ruch domyślnie.

Przykład rozszerzenia

Dodanie reguły dla 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
```

Przykład konfiguracji



konfiguracja routera:

```
*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>
```

From:
<http://wiki.ostrowski.net.pl/> - Kacper's Wiki

Permanent link:
http://wiki.ostrowski.net.pl/doku.php?id=notatki:cisco_zbf

Last update: **2025/05/16 17:24**