Basic-Zone-Policy3

yydcnjjw

2018 年 11 月 30 日

目录

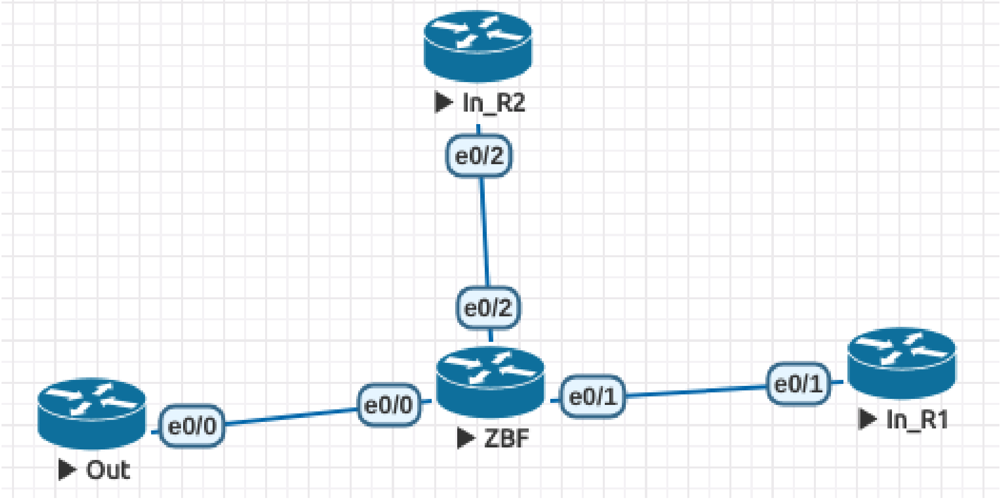


图 1: Topology

Configure:

- Out:

```
interface Ethernet0/0
 ip address 202.100.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 202.100.1.10
```

- ZBF:

```
!
class-map type inspect match-all Self-to-Outside.class
 match access-group name Self-to-Outside
class-map type inspect match-all Self-to-Inside.class
```

```
 match access-group name Self-to-Inside
class-map type inspect match-all Inside-to-Self.class
 match access-group name Inside-to-Self
!
policy-map type inspect Self-to-Inside.policy
 class type inspect Self-to-Inside.class
  inspect
 class class-default
  drop log
policy-map type inspect Outside-to-Self.policy
 class class-default
  drop log
policy-map type inspect Self-to-Outside.policy
 class type inspect Self-to-Outside.class
  inspect
 class class-default
  drop log
policy-map type inspect Inside-to-Self.policy
 class type inspect Inside-to-Self.class
  inspect
 class class-default
  drop log
!
zone security Outside
zone security Inside
zone-pair security Self-Outside source self destination Outside
 service-policy type inspect Self-to-Outside.policy
zone-pair security Self-Inside source self destination Inside
 service-policy type inspect Self-to-Inside.policy
zone-pair security Inside-Self source Inside destination self
 service-policy type inspect Inside-to-Self.policy
zone-pair security Outside-Self source Outside destination self
 service-policy type inspect Outside-to-Self.policy
!
interface Ethernet0/0
 ip address 202.100.1.10 255.255.255.0
 zone-member security Outside
```

```
!
interface Ethernet0/1
 ip address 10.1.1.10 255.255.255.0
 zone-member security Inside
!
interface Ethernet0/2
 ip address 172.16.1.10 255.255.255.0
!
ip access-list extended Inside-to-Self
 permit tcp host 10.1.1.1 host 10.1.1.10 eq 22
ip access-list extended Self-to-Inside
 permit tcp host 10.1.1.10 host 10.1.1.1 eq telnet
ip access-list extended Self-to-Outside
 permit icmp host 202.100.1.10 host 202.100.1.1 echo
!
```

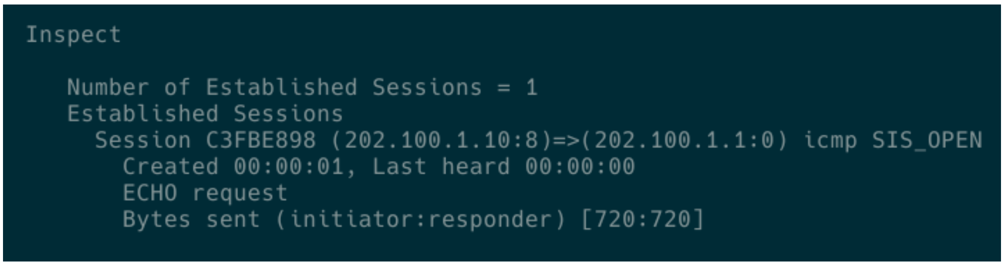
- In_R2:

```
interface Ethernet0/2
 ip address 172.16.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.1.10
```

- In_R1:

```
interface Ethernet0/1
  ip address 10.1.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.1.1.10
```

Test: ping:



```
Inspect

   Number of Established Sessions = 1
   Established Sessions
     Session C3FBE898 (202.100.1.10:8)=>(202.100.1.1:0) icmp SIS_OPEN
       Created 00:00:01, Last heard 00:00:00
       ECHO request
       Bytes sent (initiator:responder) [720:720]
```