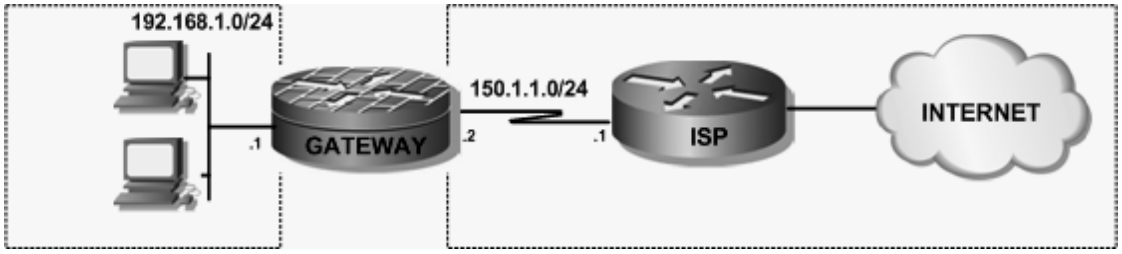
LAB – Cấu hình Zone-Based cơ bản



Mô tả

Cisco IOS Firewall hay CBAC truyền thống được triển khai theo cổng dựa vào khả năng giám sát (inspect) trạng thái của giao thức. Tất cả luồng dữ liệu vào và ra trên cổng sẽ nhận cùng chính sách giám sát. Mô hình này có những hạn chế:

- Không thể phân loại cho việc giám sát lưu lượng dữ liệu theo địa chỉ hay theo mạng.
- Sử dụng kết hợp với ACL nên rất phức tạp trong việc xác định luồng dữ liệu cho phép hay bị từ chối truy cập.
- Sự mở rộng không cao khi môi trường hiện nay cần thực hiện bảo mật theo vùng như: vùng tin cậy, vùng không tin cậy...

Với Zone-Based cho phép bạn có thể khắc phục những nhược điểm đó, với việc sử dụng khái niệm Zone (vùng), bạn có thể định nghĩa vùng với những chính sách khác nhau phụ thuộc vào việc trao đổi dữ liệu giữa các vùng một cách linh động. Trong vùng có thể có một hoặc nhiều cổng, mặc định giữa các vùng không cho phép truy cập lẫn nhau (ngoại trừ cùng vùng), do đó bạn giảm áp lực trong việc sử dụng ACL. Ngoài ra tính linh động còn thể hiện ở việc sử dụng MQC (Module QoS Command), bạn có thể phân loại theo địa chỉ, mạng, giao thức, ứng dụng dựa theo class-map và áp đặt hành động inspect, drop, pass cho những class-map tùy thuộc vào chính sách xác định.

Thực hiện Zone-Based với yêu cầu:

- Tạo 2 vùng PRIVATE thuộc mạng 192.168.1.0/24 và vùng PUBLIC.
- Cho phép vùng PRIVATE có thể sử dụng một số dịch vụ với TCP, UDP và ICMP.
- Hạn chế việc truy cập vào vùng PRIVATE từ vùng PUBLIC.

Cấu hình

Tạo 2 vùng PUBLIC và PRIVATE:

```
GATEWAY(config)#zone security PUBLIC
GATEWAY(config-sec-zone)#exit
GATEWAY(config)#zone security PRIVATE
GATEWAY(config-sec-zone)#exit
```

Gán cổng vào vùng:

```
GATEWAY(config)#interface fa0/0
GATEWAY(config-if)#zone-member security PRIVATE
GATEWAY(config)#interface s0/2/0
GATEWAY(config-if)#zone-member security PUBLIC
```

Định nghĩa class-map:

```
GATEWAY(config)#class-map type inspect match-any POLICY
GATEWAY(config-cmap)#match protocol tcp
GATEWAY(config-cmap)#match protocol udp
GATEWAY(config-cmap)#match protocol icmp
```

Định nghĩa policy-map:

```
GATEWAY(config)#policy-map type inspect POLICY
GATEWAY(config-pmap)#class type inspect POLICY
GATEWAY(config-pmap-c)#inspect
```

Gán chính sách lên 2 vùng (gói tin sẽ được "inspect" từ vùng PRIVATE khi đi ra vùng PUBLIC):

```
GATEWAY(config)#zone-pair security ZONE source PRIVATE destination PUBLIC
GATEWAY(config-sec-zone-pair)#service-policy type inspect POLICY
```

Cấu hình đầy đủ

ISP

```
Building configuration...
Current configuration : 1120 bytes
!
hostname ISP
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
```

```
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 150.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no fair-queue
!
ip classless
ip route 192.168.1.0 255.255.255.0 150.1.1.2
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 150.1.1.0 0.0.0.255
!
```

GATEWAY

```
Building configuration...
Current configuration : 1262 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GATEWAY
!
```

```
class-map type inspect match-any POLICY
 match protocol tcp
 match protocol udp
 match protocol icmp
!
policy-map type inspect POLICY
 class type inspect POLICY
  inspect
 class class-default
!
zone security PUBLIC
zone security PRIVATE
zone-pair security ZONE source PRIVATE destination PUBLIC
 service-policy type inspect POLICY
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 zone-member security PRIVATE
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 clock rate 64000
!
interface Serial0/2/0
 ip address 150.1.1.2 255.255.255.0
 zone-member security PUBLIC
```

```
 clock rate 64000
!
ip route 0.0.0.0 0.0.0.0 150.1.1.1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
```

Kiểm tra

```
GATEWAY#sh zone security
zone self
  Description: System defined zone
zone PUBLIC
  Member Interfaces:
    Serial0/2/0
zone PRIVATE
  Member Interfaces:
    FastEthernet0/0
GATEWAY#sh zone-pair security
Zone-pair name ZONE
    Source-Zone PRIVATE  Destination-Zone PUBLIC
    service-policy POLICY
```

Truy cập thành công những dịch vụ ngoài Internet như DNS, HTTP, SMTP, POP3, ICMP…

```
GATEWAY#sh policy-map type inspect zone-pair sessions
 Zone-pair: ZONE
  Service-policy inspect : POLICY
    Class-map: POLICY (match-any)
      Match: protocol tcp
```

```
      51 packets, 1428 bytes
      30 second rate 0 bps
    Match: protocol udp
      8 packets, 361 bytes
      30 second rate 0 bps
    Match: protocol icmp
      1 packets, 40 bytes
      30 second rate 0 bps
    Inspect
      Established Sessions
       Session 47A8EDA0 (192.168.1.2:1754)=>(222.255.27.96:80) tcp SIS_OPEN
        Created 00:00:04, Last heard 00:00:00
        Bytes sent (initiator:responder) [613:0]
       Session 47A8E2A0 (192.168.1.2:1640)=>(125.252.224.80:80) tcp SIS_OPEN
        Created 00:04:05, Last heard 00:00:00
        Bytes sent (initiator:responder) [792:1168913]
       Session 47A90920 (192.168.1.2:1633)=>(125.56.162.70:80) tcp SIS_OPEN
        Created 00:04:12, Last heard 00:01:53
        Bytes sent (initiator:responder) [790:434]
  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      2 packets, 80 bytes
```

Lưu ý: *Từ vùng PUBLIC vẫn có thể truy cập vào tất cả các cổng của GATEWAY.*

```
ISP#ping 150.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/40/60 ms
ISP#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/40/60 ms
ISP#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```