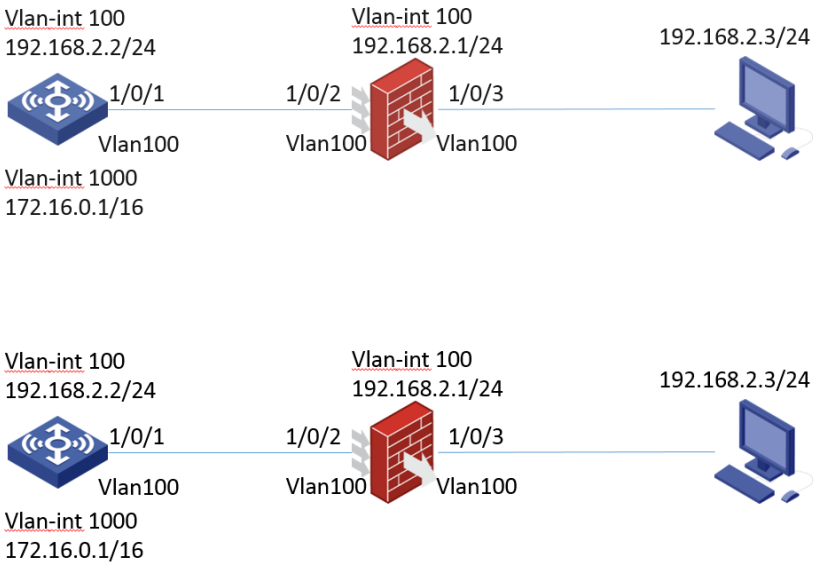
Experience case of how to deal with the issue when traffic back and forth path is inconsistent

Security 姜霁琛 2021-01-26 Published

Network Topology



The network topology is shown in the figure above. The int-vlan 1000 of wireless controller is used as the gateway of wireless clients. The 1 / 0 / 2 and 1 / 0 / 3 of firewall are all in the trust domain. The int-vlan100 is the three-layer interface of firewall, which is the gateway of terminal PC. The int-vlan100 also belongs to the trust domain. The 1 / 0 / 2 and 1 / 0 / 3 of firewall are two-layer interfaces, which permit vlan100 to go through.

Problem Description

The issue on the spot is that it is possible to Ping terminal address 192.168.2.3 directly on AC, but it i s not possible to Ping terminal address with source address 172.16.0.1 (vlan-int1000 address) on AC.
Key configuration of firewall:

```
#
interface Vlan-interface100
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
port access vlan 100
#
 interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
security-zone name Trust
 import interface Vlan-interface100
 import interface GigabitEthernet1/0/2 vlan 100 1000
 import interface GigabitEthernet1/0/3 vlan 100 1000
#
zone-pair security source Local destination Local
 packet-filter 3000
#
zone-pair security source Local destination Trust
 packet-filter 3000
#
zone-pair security source Trust destination Local
 packet-filter 3000
#
zone-pair security source Trust destination Trust
 packet-filter 3000
#
ip route-static 172.16.0.0 16 192.168.2.2
#
acl advanced 3000
 rule 0 permit ip
```

The key configuration of AC controller

```
#
interface Vlan-interface100
 ip address 192.168.2.2 255.255.255.0
#
 interface Vlan-interface1000
 ip address 172.16.0.1 255.255.0.0
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 ip route-static 0.0.0.0 0 192.168.2.1
```

Process Analysis

Session table on Firewall

dis session table ipv4 ver

Slot 1:

Initiator:

Source IP/port: 172.16.0.1/223

Destination IP/port: 192.168.2.3/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/100/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Trust

Responder:

Source IP/port: 192.168.2.3/223

Destination IP/port: 172.16.0.1/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/100/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet1/0/3

Source security zone: Trust

State: ICMP_REQUEST

Application: ICMP

Rule ID: 0

Rule name:

Start time: 2018-11-12 21:13:04 TTL: 47s

Initiator->Responder: 5 packets 510 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

It is found that the session in the initiating direction is normal, with 5 packets, but 0 packets returned.

Check with :debug ASPF packet ACL and there jumps out an error

*Nov 12 16:46:40:581 2018 FW ASPF/7/PACKET: The first packet was dropped by ASPF for invalid status. Src-ZOne=Trust, Dst-ZOne=Trust;If-In=Vlan-interface100(30), If-Out=Vlan-interface100(30); Packet Info:Src-IP=192.168.2.3, Dst-IP=172.16.0.1, VPN-Instance=none,Src-Port=29295, Dst-Port=0. Protocol=ICMP(1).

Solution

The result of "debug ASPF packet" indicates that the first packet has been discarded by ASPF because of invalid status. It means the issue may be caused by inconsistent round-trip paths.

The network between AC and PC terminal is layer-2-network, so the traffic from AC to PC terminal enters from interface 1 / 0 / 2 and exits from interface 1 / 0 / 3. However, in the opposite direction，the terminal returns packets first to its gateway, that is, the vlan-int100 on the firewall, and then back to the AC. In this case, there will be inconsistent back and forth paths. In this situation，it is recommended to configure “session state-machine mode loose”.