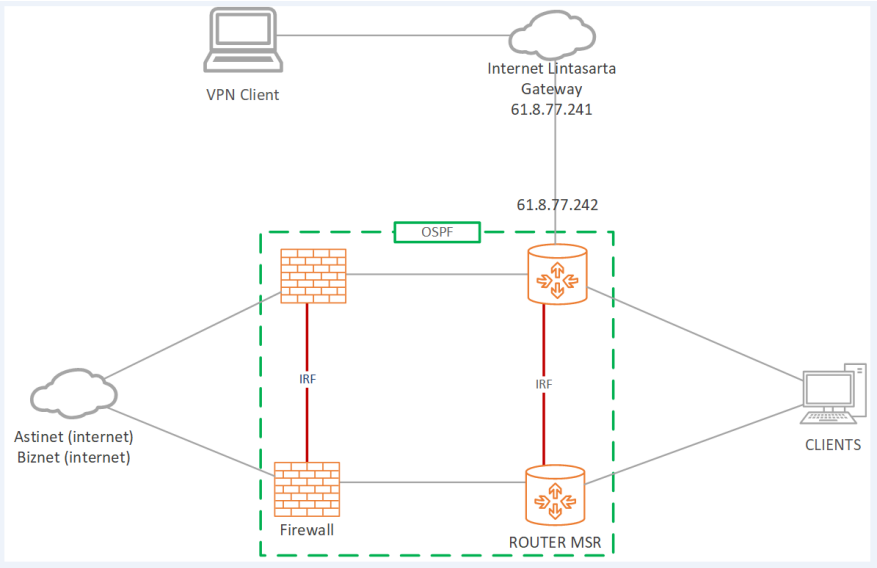
L2TP Over Ipsec Failure Caused By Unidirectional Routing

Routers 龚训杰 2021-03-31 Published

Network Topology

AS



Problem Description

The customer uses the computer to dial L2TP OVER IPSEC directly. On the F1000 series firewall, the computer with the same configuration can be successfully connected, but it cannot be successfully connected on the MSR5600.

Keep reminding:

%Mar 28 01:36:42:809 2021 BNC-JKT-MSR IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 in Main mode IKE_P1_STATE_INIT state.

Reason: Unsupported DH group: 20.. Attribute GROUP_DESCRIPTION..

%Mar 28 01:36:42:810 2021 BNC-JKT-MSR IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 in Main mode IKE_P1_STATE_INIT state.

Reason: Unsupported DH group: 19.. Attribute GROUP_DESCRIPTION..

Process Analysis

1.Check device configuration: The original routing information is as follows:

```
interface Route-Aggregation10
 description LAGG-FW
 ip address 10.1.1.2 255.255.255.252
 link-aggregation mode dynamic
 ip route-static 0.0.0.0 0 10.1.1.1 preference 50//
```
The default traffic is restored to the firewall

2.The router receives the IKE packet from the PC and sends it directly to the firewall when it replies to the packet, causing the IKE negotiation to fail.

Solution

The modification is as follows: add PBR traffic, match the traffic whose source address is the router's public network port address, and the next hop is to 61.8.77.241.

Acl advanced 3005

Rule permit ip source **61.8.77.242 0**

[Device] policy-based-route 1 permit node 0

[Device-pbr-pbr1-0] if-match acl 3005

[Device-pbr-pbr1-0] apply next-hop 61.8.77.241 //Specify the next hop

[Device-pbr-pbr1-0] quit

Apply the policy to the public network port of the Device interface.

[Device] interface gigabitethernet 3/0/1

[Device-GigabitEthernet3/0/1] **ip policy-based-route 1** //Apply the policy on the interface