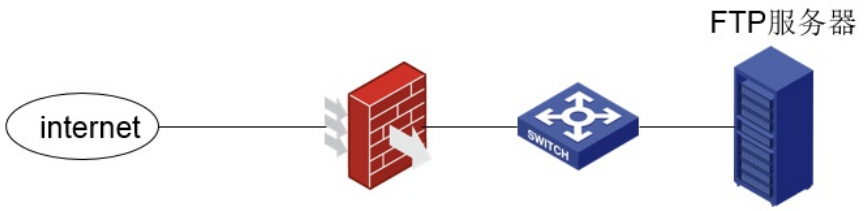
SecPath F1000-C8150(V7)The external network access to the internal network ftp server fails to connect for the first time

Security 郭尧 2020-03-24 18:41:11 Published

Network Topology

Public network-F1000-Core SW-ftp server



The firewall makes ports to perform source-to-address address translation to enable external networks to access internal servers

Problem Description

When the external network accesses the internal FTP server, the FTP software connection is rejected for the first time, and you need to refresh and reconnect to connect successfully

Process Analysis

Collect firewall diagnostic information, check the configuration of the external network interface, and map the nat server port to the internal FTP server. The configuration is as follows:

```
interface GigabitEthernet1/0/2
 port link-mode route
 description Telecom fixed extranet
 mtu 1460
 ip address 220.160.54.204 255.255.255.192
 ip address 220.160.54.220 255.255.255.192 sub
 tcp mss 1280
 nat outbound
 nat server protocol tcp global 220.160.54.204 9091 inside 192.168.0.226 21 rule jf双向 counting
 gateway 220.160.54.254
```

The interface configuration shows that the port of the FTP server has been changed to 9091 and the default port number of FTP is 2021.

View the firewall session information during the first access. The session can be established normally, but one packet is lost.

```
Initiator:
  Source      IP/port: 125.77.89.113/36755
  Destination IP/port: 220.160.54.204/9091
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: 192.168.0.226/21
  Destination IP/port: 125.77.89.113/36755
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: GENERAL_TCP
Rule ID: 0
Rule name: 0
Start time: 2020-03-24 10:19:20  TTL: 3598s
Initiator->Responder:           17 packets         822 bytes
Responder->Initiator:           16 packets        1289 bytes
```

NAT server address translation actually works, let's analyze the principle of FTP: First of all, FTP has the difference between active mode and passive mode. The first active mode analysis: The active mode works by the FTP client sending a PORT command to the server to tell the server the temporary port number that the client uses to transmit data. When data needs to

be transmitted, the server establishes a data transmission channel through the TCP20 port and the client's temporary port to complete the data transmission. This temporary port is calculated by P1 * 256 + P2. The PORT command mainly sends this parameter, the format is (x, x, x, x, p1, p2) x, x, x, x is the server IP, and p1, p2 are the parameters randomly generated by the server.
At this time, we found that if the port number of the client's data connection is changed, and the server is blocked by the NAT device, the server knows the port number, but the NAT device does not know. If the FTP port number is not changed, the NAT device The received packet is a packet whose source port is a newly calculated port number, and the first source port number of the data connection is 20. At this time, the packet cannot be sent to the client through the router. Because there is no NAT Session, this This is the case of the active mode.

Analysis of the second PASV mode:
The previous control connection is basically the same, except that the last message of the control connection is that the FTP server sends the PORT parameter to the client, and then the client uses the temporary port number calculated by this parameter to initiate a data connection to the internal network. If the same NAT device does not know the modified FTP service port, then the temporary port used by the client cannot be calculated by ALG to generate a NAT session.
The working principle of NAT ALG is that in the active mode of FTP, when the last control connection message is sent, the PORT command of the message is checked, and the new port number generated by the PORT parameter is taken out to generate a NAT session. A prerequisite for this is that NAT ALG must recognize that this packet is a FTP control connection, and the basis for distinguishing this packet is the port number. Therefore, in the packet whose destination port number is 21, we consider it to be an FTP service. For NAT ALG to work properly. If we change the FTP port number, there will be problems when establishing a data connection.

Solution

Through the above analysis, we already know the reason why the data connection cannot be established, because we cannot recognize the packets that have been modified to control the port number of FTP. NAT ALG cannot work normally. If we can make the router recognize FTP Control the connection packet, then the problem will be solved, the firewall can achieve this requirement by configuring a common port, as follows:
port-mapping
The port-mapping command configures general port mapping.

Use the undo port-mapping command to delete the specified general port mapping.

【command】
port-mapping application application-name port port-number [protocol protocol-name]
undo port-mapping application application-name port port-number [protocol protocol-name]
[Default situation]
Each application layer protocol is mapped to its corresponding well-known port number.
【view】
System view
[Default user role]
network-admin
context-admin
【parameter】
application application-name: Specifies the application layer protocol for port mapping. application-name indicates the application protocol name. The value is a string of 1 to 63 characters, which is not case sensitive. Invalid and other are not allowed to be reserved for the system. The application layer protocol name must be standard and recognized by the device.
port port-number: Specifies the port to be mapped to the application layer protocol. port-number specifies the port number, which ranges from 0 to 65535.
protocol protocol-name: specifies the transport layer protocol name used by the application layer protocol. Its value and meaning are as follows:

· Dccp: Datagram Congestion Control Protocol (DCCP).

· Sctp: Stream Control Transmission Protocol (SCTP).

· Tcp: TCP protocol.

· Udp: UDP protocol.

· Udp-lite: UDP-Lite protocol.

【User guides】
If the protocol parameter is not specified, all specified packets of the transport layer protoc ol can be identified as packets of the specified application layer protocol.
If the destination port number of a message matches a general port mapping, the message will be identified as a corresponding application layer protocol message.
For two configurations with the same port number and transport layer protocol parameters but different application layer protocol names, the new configuration will overwrite the origi nal configuration.
Mappings that specify a transport layer protocol name take precedence over mappings that do not specify a transport layer protocol name.
[Example]
Establish a common port mapping from port 9091 to the FTP protocol.
<Sysname> system-view
[Sysname] port-mapping application ftp port 9091