L2TPVPN安全策略放行

L2TP VPN 吴君 2022-11-07 发表

组网及说明

一、 组网图和描述

防火墙内网接口1/0/0接server，外网接口1/0/1作为外网上网，现外网用户通过访问防火墙外网口的1.1.1.1地址拨入l2tpvpn，获取20.1.1.0网段地址后，来访问内网10.1.1.2服务器80端口。

防火墙内网口1/0/0为trust安全域、外网口1/0/1为untrust安全域，virtual-template1网关接口为l2tp安全域。

组网配置:

L2tpvpn拨入后的地址池20.1.1.1/24

网关接口为virtual-template1

服务默认udp 1701端口

配置步骤

二、安全策略配置

L2TPVPN拨入

```
security-policy ip
rule 1 name l2tpvpn
  action pass
  source-zone Untrust
  destination-zone Local
destination-ip-host 1.1.1.1
service-port udp destination eq 1701
```

L2TPVPN用户访问服务器

```
rule 2 name l2tpvpn2
  action pass
  source-zone l2tpvpn
  destination-zone Trust
destination-ip-host 10.1.1.2
service-port tcp destination eq 80
```

配置关键点

策略解释：

创建rule1：

Sslvpn拨入到防火墙需要外网流量从g1/0/1进入防火墙，且目的为防火墙本身，属于本地报文，因此目的安全域为Local，而g1/0/1属于Untrust安全域，所以流量的走向是：源安全域Untrust到目的安全域Local，目的端口为本身的l2tpvpn的udp1701端口。

创建rule2：

拨入成功后用户网段属virtual-template1接口网段，防火墙根据目的地址再将流量从g1/0/0转发出去。而g1/0/0属于trust安全域，virtual-template1接口属于l2tpvpn安全域，所以流量的走向是：源安全域l2tpvpn到目的安全域trust。目的地址和端口为服务器的10.1.1.2的80端口。