IPSECVPN安全策略放行

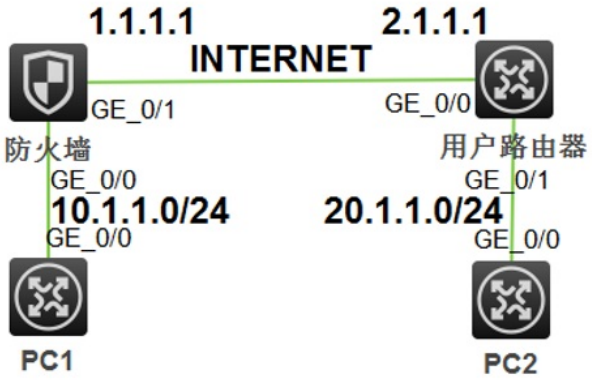
IPSec VPN 吴君 2022-11-07 发表

组网及说明

一、 组网图和描述

防火墙内网接口1/0/0接内网，外网接口1/0/1作为外网上网，现外网用户路由器通过访问防火墙外网口的1.1.1.1地址建立Ipsec，让对端20.1.1.0/24网段地址和防火墙内网10.1.1.0/24网段互访。

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。



组网配置：

外网用户端通过防火墙1.1.1.1地址建立vpn实现内网互访。

配置步骤

二、安全策略配置

IPSECVPN建立

```
security-policy ip
rule 1 name ipsec
  action pass
  source-zone Untrust
  destination-zone Local
source-ip-host 2.1.1.1
destination-ip-host 1.1.1.1
service-port udp destination eq 500
service-port udp destination eq 4500

security-policy ip
rule 2 name ipsec2
  action pass
  source-zone Local
  destination-zone Untrust
source-ip-host 1.1.1.1
destination-ip-host 2.1.1.1
service-port udp destination eq 500
service-port udp destination eq 4500
```

IPSECVPN用户互访

```
rule 3 name ipsec3
  action pass
  source-zone Untrust
  destination-zone Trust
source-ip-subnet 20.1.1.0 255.255.255.0
destination-ip-subnet 10.1.1.0 255.255.255.0

rule 4 name ipsec4
  action pass
  source-zone Trust
  destination-zone Untrust
source-ip-subnet 10.1.1.0 255.255.255.0
destination-ip-subnet 20.1.1.0 255.255.255.0
```

配置关键点

策略解释：

创建rule1、rule2：

Rule1:对端路由器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ipsec的udp500和4500端口，目的ip是防火墙公网地址1.1.1.1，源地址是对端路由器的公网地址2.1.1.1（如对端路由器没有公网地址可不填写源ip）。

Rule2规则为rule1规则安全域、地址互反，可以主动找对端建立链接，（同样如对端没有公网地址可不填写对端ip）。

创建rule3、rule4：

Rule3:IPSEC建立成功后对端网络需要访问本端网络，防火墙从1/0/1口接收ipsec流量后，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，1/0/1接口属于Untrust安全域，所以流量的走向是：源安全域Untrust到目的安全域trust。源地址为对端内网网段20.1.1.0/24目的网段为本地内网10.1.1.0/24。

Rule4规则为rule3规则安全域、地址互反，用于主动访问对端内网时候放通。