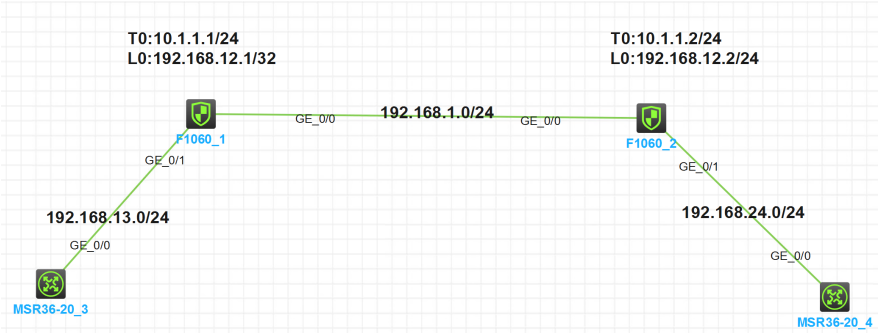
如何利用NAT技术隐藏GRE报文中的源地址信息

ACL GRE VPN NAT 孔凡安 2023-04-23 发表

组网及说明



注：如无特别说明，描述中的 FW1 或 MSR1 对应拓扑中设备名称末尾数字为 1 的设备，FW2 或 MSR2 对应拓扑中设备名称末尾数字为 2 的设备，以此类推；另外，同一网段中，IP 地址的主机位为其设备编号，如 FW1 的 g0/0 接口若在 192.168.1.0/24 网段，则其 IP 地址为 192.168.1.1/24，以此类推。

****

****

实验需求：

由于GRE报文为明文封装，在网络中传输容易被监听导致信息泄漏。基于此，本案例提供一种方案，使用NAT技术隐藏客户端源地址。

配置步骤

FW1	FW2
# nat static inbound 192.168.13.3 1.1.1.1 acl 3000 reversible # interface LoopBack0 ip address 192.168.12.1 255.255.255.255 # interface GigabitEthernet1/0/0 port link-mode route combo enable copper ip address 192.168.1.1 255.255.255.0 nat outbound # interface GigabitEthernet1/0/1 port link-mode route combo enable copper ip address 192.168.13.1 255.255.255.0 nat static enable # interface Tunnel0 mode gre ip address 10.1.1.1 255.255.255.0 source 192.168.12.1 destination 192.168.12.2 # security-zone name Local # security-zone name Trust import interface GigabitEthernet1/0/1 # security-zone name DMZ # security-zone name Untrust import interface GigabitEthernet1/0/0 import interface Tunnel0 # security-zone name Management # ip route-static 1.1.1.1 32 192.168.13.3 ip route-static 1.1.1.2 32 Tunnel0 ip route-static 192.168.12.2 32 192.168.1.2 ip route-static 192.168.24.4 32 Tunnel0 # acl advanced 3000 rule 5 permit ip source 192.168.13.3 0 destination 1.1.1.2 0 # session statistics enable # ip http enable ip https enable # security-policy ip rule 0 name any action pass	# nat static inbound 192.168.24.4 1.1.1.2 acl 3000 reversible # interface LoopBack0 ip address 192.168.12.2 255.255.255.255 # interface GigabitEthernet1/0/0 port link-mode route combo enable copper ip address 192.168.1.2 255.255.255.0 nat outbound # interface GigabitEthernet1/0/1 port link-mode route combo enable copper ip address 192.168.24.2 255.255.255.0 nat static enable # interface Tunnel0 mode gre ip address 10.1.1.2 255.255.255.0 source 192.168.12.2 destination 192.168.12.1 # security-zone name Local # security-zone name Trust import interface GigabitEthernet1/0/1 # security-zone name DMZ # security-zone name Untrust import interface GigabitEthernet1/0/0 import interface Tunnel0 # security-zone name Management # ip route-static 1.1.1.1 32 Tunnel0 ip route-static 1.1.1.2 32 192.168.24.4 ip route-static 192.168.12.1 32 192.168.1.1 ip route-static 192.168.13.3 32 Tunnel0 # acl advanced 3000 rule 5 permit ip source 192.168.24.4 0 destination 1.1.1.1 0 # session statistics enable # ip http enable ip https enable # security-policy ip rule 0 name any action pass

配置关键点

注意事项：需要注意添加对应的静态路由

以R3访问R4为例，访问过程如下：

FW1上的业务点	FW2上的业务点
NAT转换： 192.168.13.3:10965 - 1.1.1.2: 2048(VPN: 0) ------> 1.1.1.1:10965 - 1.1.1.2: 2048(VPN: 0) GRE封装： 192.168.12.1 - 192.168.12.2	GRE解封装： 192.168.12.1 - 192.168.12.2 NAT转换： 1.1.1.1:10965 - 1.1.1.2: 2048(VPN: 0) ----->1.1.1.1:10965 - 192.168.24.4: 2048(VPN: 0)