F1000-X-G2/F100-X-G2系列防火墙GRE VPN配置案例（WEB）

GRE VPN　叶佳豪　2019-09-19 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

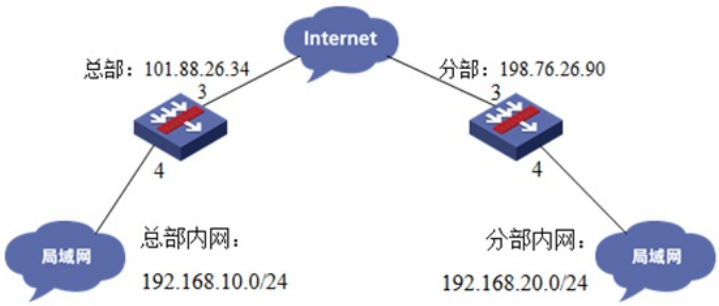
本案例适用于如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

1.2 配置需求及实现的效果

总部和分部各有一台防火墙部署在互联网出口，因业务需要两端内网业务需要通过GRE VPN相互访问。IP地址及接口规划如下表所示：

公司名称	外网接口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部	1/0/3	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部	1/0/3	198.76.26.90/30	198.76.26.89	1/0/4	192.168.20.0/24

2 组网图



配置步骤

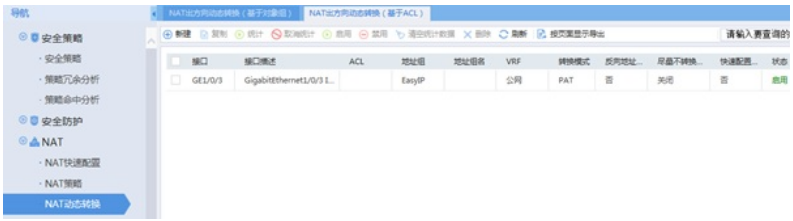
3 配置步骤

3.1 总部侧防火墙基本网络配置

3.1.1 设置总部侧外网接口地址

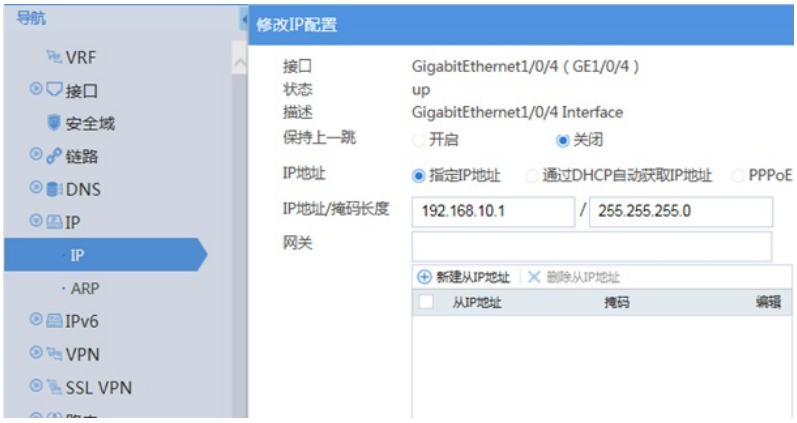
#在“网络”>“IP”中找到1/0/3接口配置101.88.26.34/30的地址。

#在“策略”>“NAT”>“NAT动态转换”中选择NAT出方向动态转换（基于ACL选项）。



3.1.2 设置总部侧内网接口地址

#在“网络”>“IP”中找到1/0/4接口配置IP地址：192.168.10.1/24。



3.1.3 设置总部侧到公网路由

#选择“网路”>“路由”>“静态路由新建到公网网关的默认路由。

3.2 总部侧GRE VPN配置

3.2.1 新建Tunnel 0隧道接口

#在“网络”>“VPN”>“GRE”中新建Tunnel 0隧道接口，并配置IP地址为1.1.1.1/24，指定Tunnel 0接口源地址与目的地址分别对应总部分支侧的公网地址。

3.2.2 新建到tunnel接口的明细路由

#选择“网路”>“路由”>“静态路由建一条目的地址为192.168.20.0/24，下一跳（网关）地址为tunnel0接口的路由，用于匹配去往192.168.20.0/24网段的路由客户通过隧道转发。

3.3 总部侧安全策略配置

3.3.1 将外网、内网、tunnel接口加入对应安全

#在“网络”>“安全域”中将外网接口加untrust区域，内网接口及tunnel接口加入trust区域。

3.3.2 放通安全策略使数据通信正常

1. 放通trust到untrust、local的安全策略，使内网用户访问网络的同时能管理防火墙设备。
#在“策略”>“安全策略”中选择新建，源安全域选择trust，目的安全域选择untrust和local。

2. 放通untrust到trust目的地址为192.168.20.0/24网段到192.168.10.0/24网段的数据，以及trust到trust的安全策略。
#在“对象”>“对象组”>“IPV4地址对象组”中新建分部网段与总部网段。

#在“策略”>“安全策略”中选择新建，源安全域选择untrust，目的安全域选择trust点击确定。

#在“策略”>“安全策略”中选择新建，源安全域选择trust，目的安全域选择trust点击确定，用来放通同安全域之间的访问。

3.4 分部侧防火墙GRE配置

分部防火墙与总部侧防火墙配置方法一致。

3.5 结果测试

#使用总部侧PC机PING测试分部侧PC机测试：

可以看到在总部侧访问分部数据可达，并且通过“display interface Tunnel 0”可以看到收发包数量。

display interface Tunnel 0

Tunnel0

Current state: UP

Line protocol state: UP

Description: Tunnel0 Interface

Bandwidth: 64 kbps

Maximum transmission unit: 1476

Internet address: 1.1.1.1/24 (primary)

Tunnel source 101.88.26.34, destination 198.76.26.90

Tunnel keepalive disabled

Tunnel TTL 255

Tunnel protocol/transport GRE/IP

GRE key disabled

Checksumming of GRE packets disabled

Last clearing of counters: Never

Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec

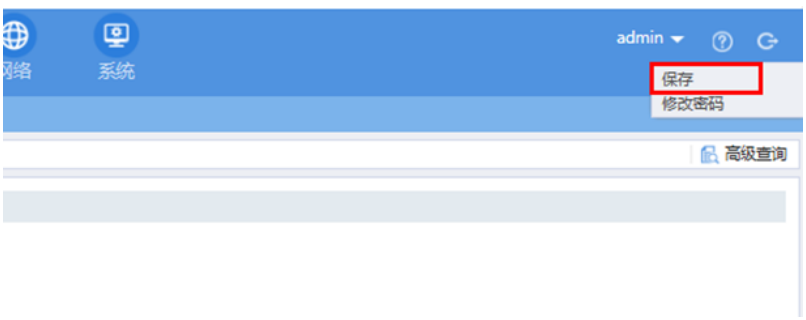
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec

Input: 5 packets, 420 bytes, 0 drops

Output: 5 packets, 420 bytes, 0 drops

3.6 保存配置

在页面右上角点击保存按钮保存配置。



配置关键点