FortiGate-v4.0-通用路由封装

版本	1.0
时间	2015 年 1 月
支持的版本	FortiOS v4.0.x
作者	黄豪赫
状态	已审核
反馈	support_cn@fortinet.com

目　录

简介

隧道技术（Tunneling）是一种常见在互联网络的网络设备之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将其它协议的数据帧或包重新封装然后通过隧道发送。新的帧头提供路由信息，以便通过互联网传递被封装的负载数据。

本文主要简述 FortiGate 上通过 GRE(通用路由封装)隧道和异厂商实现互联互通的实例。

通用路由封装介绍

通用路由封装（GRE：Generic Routing Encapsulation）在 RFC1701/RFC1702 中定义，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法。GRE 的隧道由两端的源 IP 地址和目的 IP 地址来定义，它允许用户使用 IP 封装 IP、IPX、AppleTalk，并支持全部的路由协议，如 RIP、OSPF、IGRP、EIGRP。通过 GRE，用户可以利用公用 IP 网络连接 IPX 网络和 AppleTalk 网络，还可以使用保留地址进行网络互联，或对公网隐藏企业网的 IP 地址。

相关组件

FortiGate 防火墙。

参考文档

《FortiOS™ CLI Reference》

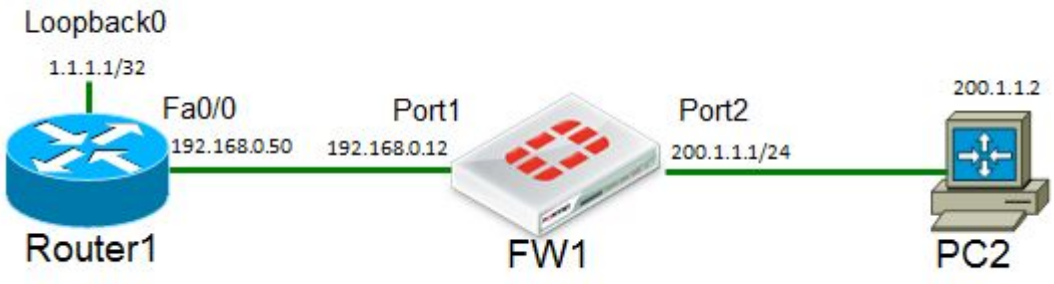
FortiGate 相关命令介绍

配置命令：

```
config system gre-tunnel
  edit <tunnel_name>                  //定义tunnel接口的名称//
    set interface <interface_name>   //指定tunnel所属接口//
    set local-gw <localgw_IP>       //指定tunnel的源地址//
```

```
        set remote-gw <remotegw_IP>    //指定tunnel的目的地址//
    end
```

测试拓扑图



测试内容

FW1 和 Router1 建立 GRE tunnel，PC2 和 Router 1 之间能直接互访。

1.在 FW1 和 Router1 上建立 GRE tunnel，配置如下：

FW1 配置:

```
config system gre-tunnel                    //进入 GRE tunnel 配置层次//
    edit "Tun0"                             //定义名为 Tun0 的 tunnel 接口//
        set interface "port1"               //指定归属端口//
        set local-gw 192.168.0.12           //指定 tunnel 的源 IP 地址//
        set remote-gw 192.168.0.50          //指定 tunnel 的目的地址//
    next
end
注：配置 gre tunnel 后，在接口上能系统自动产生 Tun0 的虚端口
config system interface                     //进入 system interface 配置 Tun0 接口
//
 edit "Tun0"
        set ip 12.1.1.1 255.255.255.255     //配置 Tun0 的 IP 地址//
        set allowaccess ping https http telnet
        set remote-ip 12.1.1.2              //配置对端 tunnel 的 IP 地址//
    next
  end
```

Router1 配置:

```
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
```

```
interface Tunnel0
 ip address 12.1.1.2 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 192.168.0.12
!
interface FastEthernet0/0
 ip address 192.168.0.50 255.255.255.0
 duplex half
```

2.GRE tunnel 建后，需要完成路由配置和 FW1 策略的配置，

FW1 配置:

```
config router static //配置静态路由//
    edit 1
        set device "Tun0"
        set dst 1.1.1.0 255.255.255.0    //将去往 1.1.1.0/24 的路由送往 Tun0//
```

注：不需要指明 gateway，配置完成后，可以通过 get router info route-table all 去检测路由是否生效

```
config firewall policy    //配置防火墙策略//
    edit 1
        set srcintf "port2"
        set dstintf "Tun0"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set srcintf "Tun0"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
```

Router1 配置:

```
ip route 200.1.1.0 255.255.255.0 12.1.1.1
```

3.从 Router 1 ping 测 PC2，在防火墙上 debug flow 结果如下：

```
id=0 trace_id=621 msg="vd-root received a packet(proto=1, 1.1.1.1:8->200.1.1.2:8) from Tun0. code=8, type=0, id=8, seq=4."
```

```
        id=0 trace_id=621 msg="Find an existing session, id-00000e00, original direction"
        id=0 trace_id=621 msg="enter fast path"
        id=0 trace_id=622 msg="vd-root received a packet(proto=1, 200.1.1.2:8->1.1.1.1:0) from port2. code=0, type=0, id=8, seq=4."
        id=0 trace_id=622 msg="Find an existing session, id-00000e00, reply direction"
        id=0 trace_id=622 msg="enter fast path"
```