

## 多链路负载均衡及冗余

版本	1.0
时间	2011 年 10 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiOS v3.x,v4.x
状态	草稿

## 目录

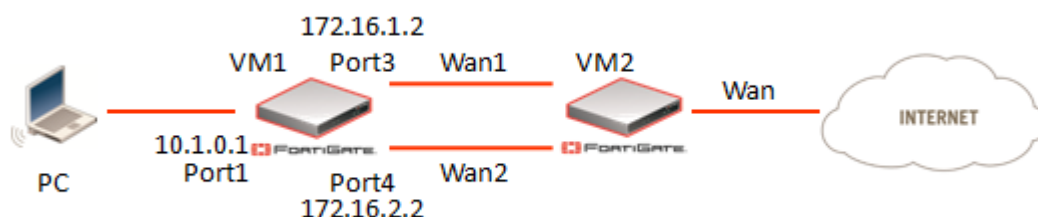
1.目的.....	3
2.环境拓扑.....	3
3.链路负载均衡.....	3
3.1 基于源 IP 的负载均衡.....	4
3.2 基于权重的负载均衡.....	6
3.3 基于出口流量阈值的负载均衡.....	7
3.4 其他负载均衡.....	7
3.5 策略路由.....	8
4.链路冗余.....	8
4.1 检测服务器.....	8
4.2 管理距离与优先级.....	9
5.负载均衡与冗余.....	10
6.参考.....	10

## 1.目的

本文档针对 FortiGate 在具有两条或两条以上出口时的负载均衡及链路冗余配置进行说明。Fortigate 在多链路可以支持不同方式的负载均衡,在链路负载均衡的同时,也可以实现链路的冗余。

## 2.环境拓扑

本文使用 FortiGate-VM 做演示。本文支持的系统版本为 FortiOS v4.0MR3 Patch2 及更高。



该配置中使用 FortiGate-VM1 模拟两条 WAN 线路,通过 FortiGate-VM2 连接至外网,实际环境可以据此参考。

## 3.链路负载均衡

链路负载均衡功能需要为 2 个不同的出网接口分别配置一条默认路由,如果实现负载均衡,需要 2 条或多条静态路由的管理距离以及优先级保持一致。同时也需要保证配置内网去往 2 条出口的策略。

如果使用静态路由的话可以把出网路由的管理距离配置成相等的,也就是等

价格路由。如果是 ADSL、DHCP 等动态获取的网关的话可以把“从服务器中重新得到网关”选中同时将动态获取的路由的管理距离配置即可。在默认路由已经配置完成的情况下，如果仍然有某些特定的数据流需要从指定的出口出网的话，可以使用策略路由功能来完成这样的需求。策略路由的优先级高于动态和静态路由，按照从上到下的次序来匹配的。

负载均衡包括三种模式：

1. 基于源 IP 的负载均衡；
2. 基于权重的负载均衡；
3. 基于出口流量阈值的负载均衡。

类型	子类型	网络地址	路径长度	路径成本	网关	接口	持续时间 (d h:m:s)
静态		0.0.0.0/0	10	0	172.16.1.1	port3	
静态		0.0.0.0/0	10	0	172.16.2.1	port4	
直连		10.1.0.0/24	0	0	0.0.0.0	port1	
直连		172.16.1.0/24	0	0	0.0.0.0	port3	
直连		172.16.2.0/24	0	0	0.0.0.0	port4	
直连		192.168.147.0/24	0	0	0.0.0.0	port2	

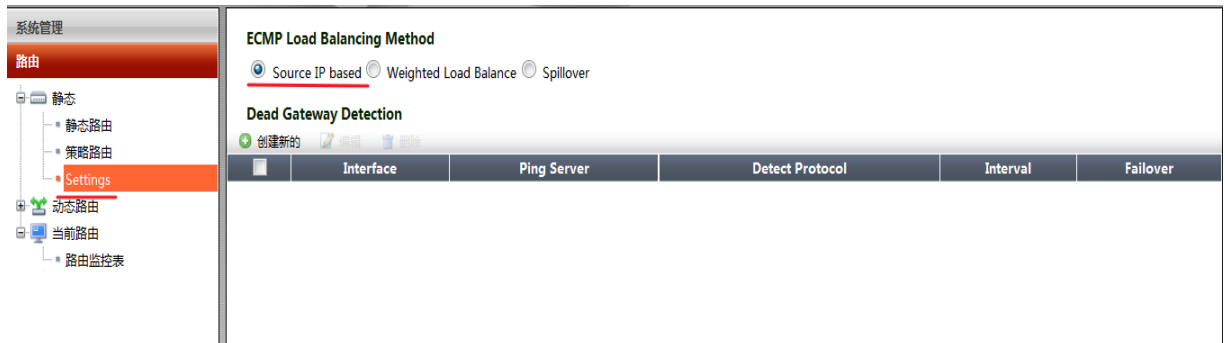
序列号	源地址	目的地址	认证	时间表	服务	动作	记录日志
<b>port1(Internal) -&gt; port3(ToWan1) (5)</b>							
1	all	SSLVPN_TUNNEL_ADDR1	>	>	>	SSL-VPN	>
2	pptp	all	always		ANY	ACCEPT	☑
3	Android_Range	all	always		ANY	ACCEPT	☒
4	all	ftp	always		ANY	ACCEPT	☒
5	all	all	always		ANY	ACCEPT	☒
<b>port1(Internal) -&gt; port4(ToWan2) (1)</b>							
6	all	all	always		ANY	ACCEPT	☒
<b>port3(ToWan1) -&gt; port1(Internal) (8)</b>							
<b>port3(ToWan1) -&gt; port3(ToWan1) (1)</b>							

### 3.1 基于源 IP 的负载均衡

基于源 IP 的负载均衡，当路由表中有多个出网路由时，FortiGate 设备会按内置的算法实现负载均衡，这个算法不能被修改。这个算法是：假设路由表中有 n 条出网路由，则防火墙会将内网源 IP 地址的最后一组数值除 n 取余，余 1 走

第一条出网路由，余 n-1 走第 n-1 条出网路由，余 0 走第 n 条出网路由。

本例的出网规则是：,如果想让某些 IP 走特定的接口需要策略路由来实现。



偶数 IP 走 port3,如下图

```
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 10.1.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.0.1

Ethernet adapter 本地连接 2:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\Administrator>tracert -d www.fortinet.com

Tracing route to www.fortinet.com [66.171.121.34]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    10.1.0.1
  1  1 ms     <1 ms    <1 ms    172.16.1.1
  2  11 ms    3 ms     3 ms     192.168.8.1
  3  15 ms    *        22 ms    113.47.240.1
```

奇数 IP 走 port4

```

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 10.1.0.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.0.1

Ethernet adapter 本地连接 2:

    Media State . . . . . : Media disconnected

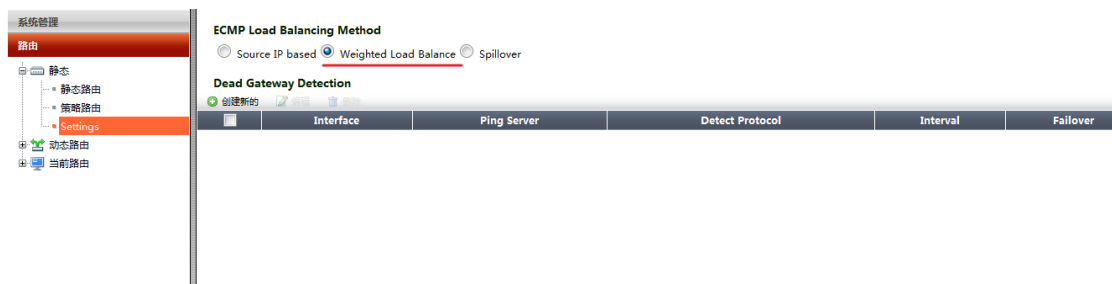
C:\Documents and Settings\Administrator>tracert -d www.fortinet.com

Tracing route to www.fortinet.com [66.171.121.34]
over a maximum of 30 hops:

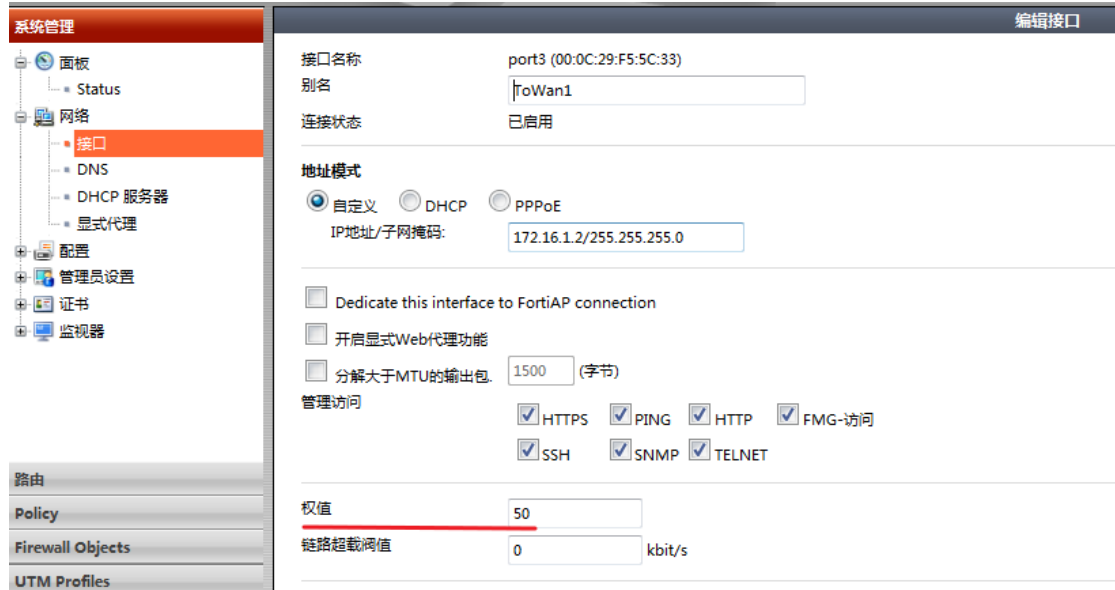
  0  <1 ms    <1 ms    <1 ms    10.1.0.1
  1  <1 ms    <1 ms    <1 ms    172.16.2.1
  2   3 ms     2 ms     2 ms    192.168.8.1
  3  17 ms     9 ms     *        113.47.240.1
    
```

### 3.2 基于权重的负载均衡

基于权重的负载均衡, FortiGate 将根据接口的权值来分配所有的会话。那么同一源的多个会话有可能被均匀的分配在多条链路上时,此时理论上可以起到带宽叠加的效果。

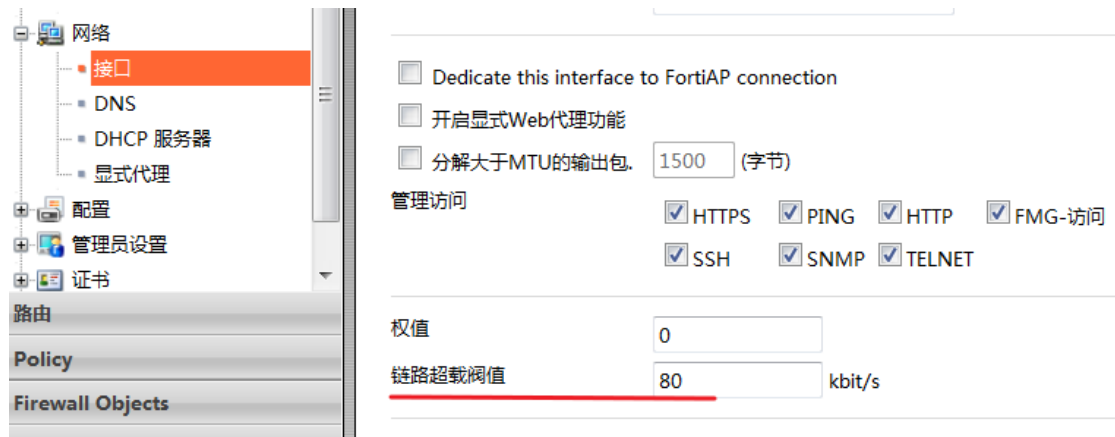


此例中, port3 与 port4 权值均为 50, 意味 FortiGate 将平均分配会话在 2 个接口上。如果希望更多的流量走 Port3, 可以增加该接口的权值。



### 3.3 基于出口流量阈值的负载均衡

针对接口定义流量阈值,当出口流量,即上行流量达到指定阈值后,系统将切换链路至另外一条链路。目前 FortiGate 仅能基于出口流量进行切换。



### 3.4 其他负载均衡

另外一种情况,很多用户希望通过根据相应目的地来决定链路的选择,例如对指定电信的资源流经电信出口访问等。可以通过设置多条静态路由来实现。

以下为电信及联通(原网通)路由,(仅供参考使用,如用于生产网络使用,请自

行核实后替换接口及网关地址使用！)

[电信路由](#)

[网通路由](#)

## 3.5 策略路由

在执行负载均衡的同时,部分源 IP 希望从指定接口流出,这时需要用到策略路由,通过定义策略路由,可以设定源及目标地址,当匹配该设定的流量从指定接口流出。

The screenshot shows the FortiGate configuration interface for editing a Policy Route. The left sidebar shows the navigation menu with '策略路由' (Policy Route) selected. The main configuration area is titled '编辑策略路由' (Edit Policy Route) and contains the following fields:

- 如果进入流量匹配: (If incoming traffic matches:)
- 协议端口: (Protocol port) 1
- 进入接口: (Incoming interface) port1(Internal)
- 源地址/掩码: (Source address/mask) 10.1.0.3/255.255.255.255
- 目的地址/掩码: (Destination address/mask) 0.0.0.0/0.0.0.0
- 目的端口: (Destination port) 从: 1 至: 65535
- 服务类型: (Service type) bit模板: 00 (十六进制) bit掩码: 00 (十六进制)
- 强制流量到: (Force traffic to:)
- 流出接口: (Outgoing interface) port3(ToWan1)
- 网关地址: (Gateway address) 0.0.0.0

Buttons for '确认' (Confirm) and '取消' (Cancel) are located at the bottom right of the configuration area.

## 4.链路冗余

### 4.1 检测服务器

路由-settings 可以设置网关检测功能(Dead Gateway Dectection),分别在 2 个出网接口上配置 PING Server,告诉 FortiGate 可以通过 ping(也可以选择 TCP 或 UDP 的 echo)是否被响应来确定线路是否仍然连通。Ping server 的配置原则是:尽量配置成防火墙的网关(请先确认此网关允许被 ping ,在拨号环境中



同时确认网关地址不会由于客户端地址改变而发生改变)。

当系统检测到 5 个连续 ICMP 包无回应(可以修改默认值),则认为该链路已失效,将该链路的默认路由从当前路由表中删除,那么流量将重新负载在剩余的链路上。

The screenshot shows the 'ECMP Load Balancing Method' configuration page. Under 'Dead Gateway Detection', there are two entries:

Interface	Ping Server	Detect Protocol	Interval	Failover
port3	61.135.169.105	ICMP Ping	10	5
port4	61.135.169.105	ICMP Ping	10	5

The screenshot shows the 'Current Routing Table' (当前路由表) with the following entries:

类型	子类型	网络地址	路径长度	路径成本	网关	接口
静态		0.0.0.0/0	10	0	172.16.1.1	port3
静态		0.0.0.0/0	10	0	172.16.2.1	port4
直连		10.1.0.0/24	0	0	0.0.0.0	port1
直连		172.16.1.0/24	0	0	0.0.0.0	port3
直连		172.16.2.0/24	0	0	0.0.0.0	port4
直连		192.168.147.0/24	0	0	0.0.0.0	port2

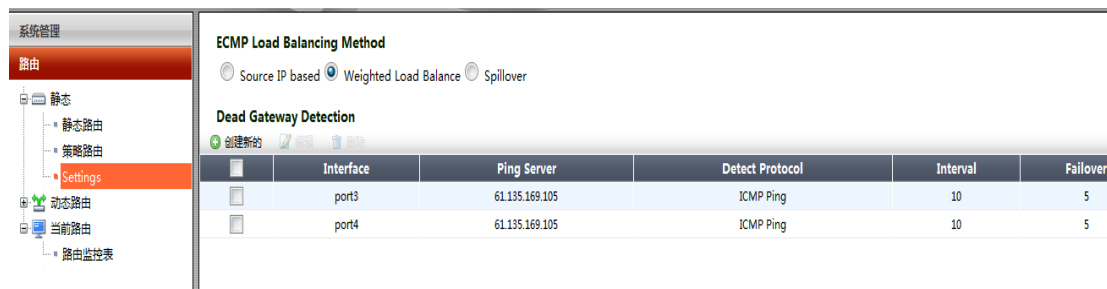
## 4.2 管理距离与优先级

通过调整设备接口的管理距离,同样可以用于链路冗余使用,当设置 2 条不同管理距离的路由时,仅管理距离较低的那条路由会出现在当前路由表中,即只有低管理距离路由才会生效,当该路由失效后,高管理距离才会出现在当前路由表中,此时无法实现流量负载均衡。

关于管理距离与路由优先的详细设置,请参考[静态路由的管理距离和优先级](#)。

## 5.负载均衡与冗余

负载均衡与冗余可以同时生效,即在配置好负载均衡的链路上启用检测服务器即可,这样既可以做到负载均衡,同时当链路失效时仍可以使用另外一条链路访问 Internet。



The screenshot shows the 'Settings' page for ECMP Load Balancing Method. Under 'ECMP Load Balancing Method', 'Weighted Load Balance' is selected. Under 'Dead Gateway Detection', a table lists the configured detection parameters:

	Interface	Ping Server	Detect Protocol	Interval	Failover
<input type="checkbox"/>	port3	61.135.169.105	ICMP Ping	10	5
<input type="checkbox"/>	port4	61.135.169.105	ICMP Ping	10	5

## 6.参考

[Configuring link redundancy-Traffic load-balancing/load-sharing - ECMP \(Equal Cost Multiple Path\)-Dual Internet or WAN scenario](#)

[Detecting a link failure using Dead Gateway Detection\(ping server\)to ensure a link fail-over](#)

[Configuring Dual Internet Links \(Design Considerations\)](#)