OSPF over IPSec 及路由冗余

版本	1.0
时间	2011 年 12 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiOS v4.x
状态	草稿

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

目录

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

1.目的

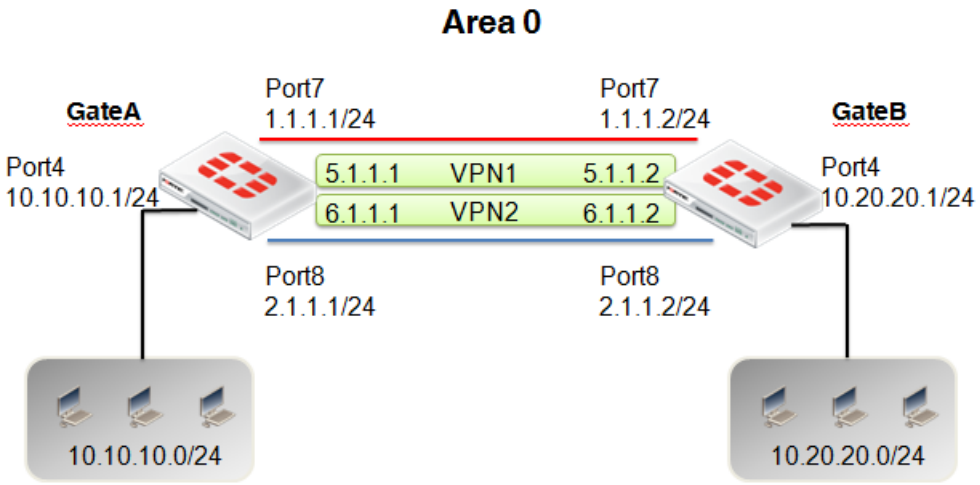
OSPF 使用组播协议路由,由于 IPSec VPN 不能支持组播和广播,因此不能运行动态路由协议,此时需要使用 GRE 协议封装 OSPF 后经过 IPSec 进行数据交互。所以常用的多为 OSPF over GRE。

Route-based 方式的 IPSec VPN 极大的方便了 OSPF over IPSec 的配置,无需再将数据先用 GRE 封装然后在运行在 IPSec 链路上。

本文档针对 FortiGate 的 OSPF over IPSec 的冗余路由进行说明。

2.环境介绍

本文使用 2 台 FortiGate 进行说明, GateA 与 GateB 建立 2 条 IPSec VPN,在 IPSec VPN 链路上运行 OSPF 协议并同处于 Area 0 区域,以期达到任意主 VPN 隧道中断后,备份 VPN 隧道仍然继续工作,实现 OSPF over IPSec 及路由冗余的目的,本文使用的系统版本为 FortiOS v4.0MR2 Patch8。



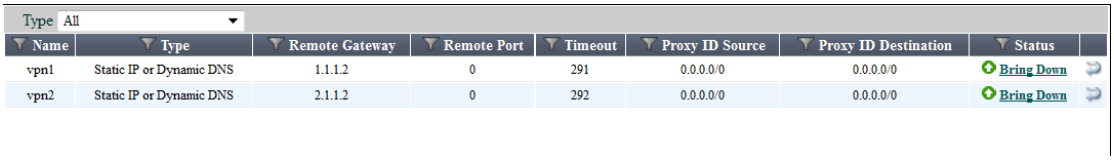
北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

Router	Port7 IP	Port8 IP	VPN1 IP	VPN2 IP	Loopback IP
GateA	1.1.1.1	2.1.1.1	5.1.1.1	6.1.1.1	10.1.1.1
GateB	1.1.1.2	2.1.1.2	5.1.1.2	6.1.1.2	10.2.2.1

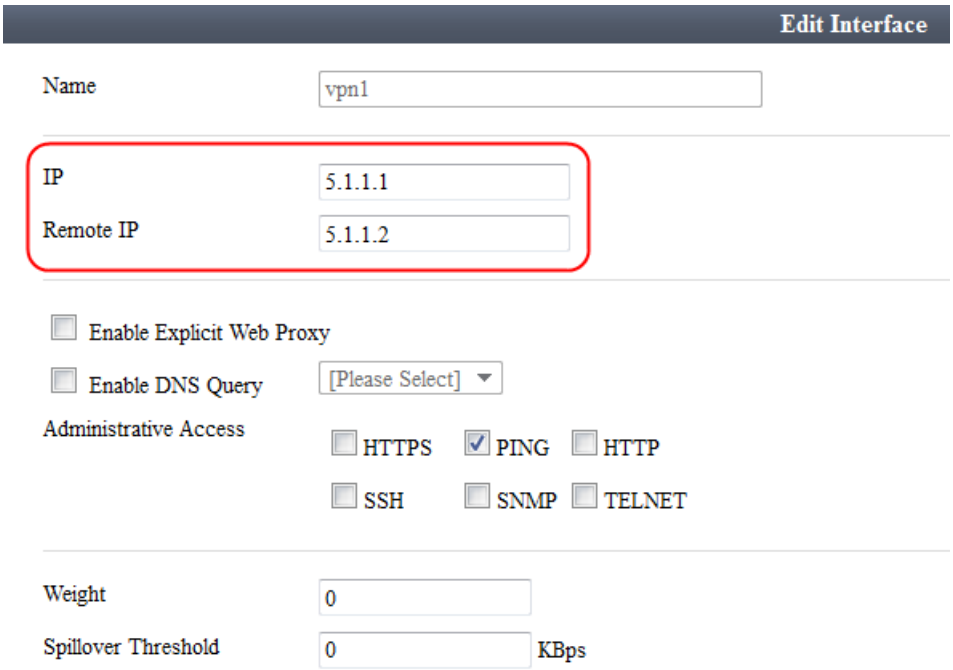
3.IPSec VPN 配置

配置 route-based 模式(即接口模式) IPSec VPN 的具体方法请参考站到站 IPSec VPN 设置 4.2

配置完成后在 VPN-IPSec-监视器可以查看 VPN 状态。



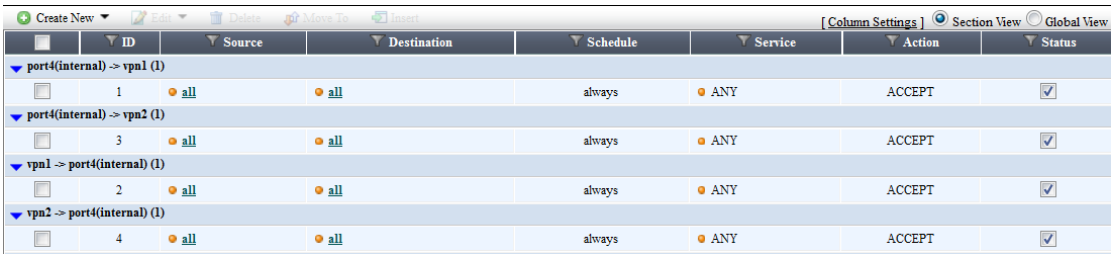
在 GateA,GateB 的 VPN1,VPN2 虚拟接口中配置本地地址及远端地址。



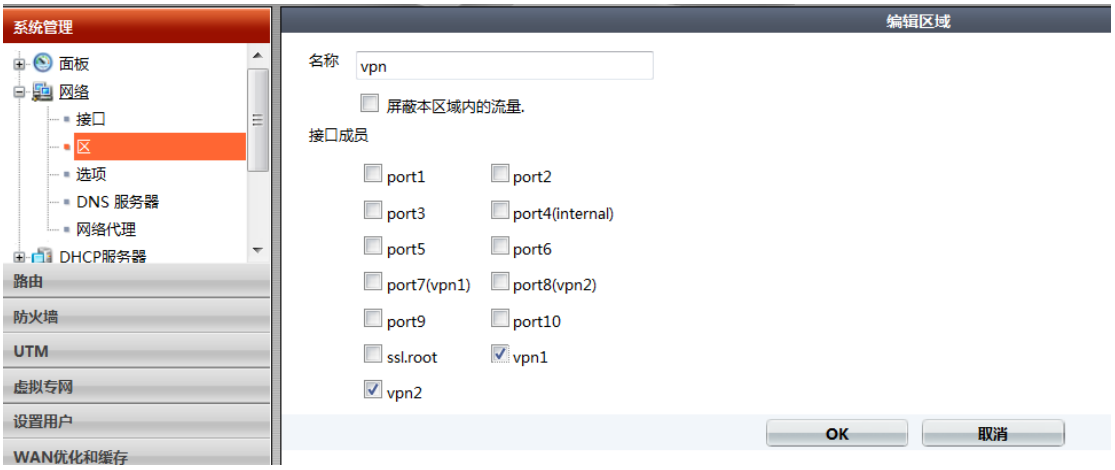
北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

	port7 (vpn1)	1.1.1.1 / 255.255.255.0	HTTP,PING,TELNET
	vpn1	5.1.1.1 / 255.255.255.255	PING
	port8 (vpn2)	2.1.1.1 / 255.255.255.0	HTTP,HTTPS,PING
	vpn2	6.1.1.1 / 255.255.255.255	PING

配置 4 条策略用于 Port4 与 2 条 VPN 之间的通讯



也可以创建区 Zone,将 vpn1,vpn2 划为一个区,此时可以用 2 条策略代替之前的 4 条策略,方便策略的管理。



此时仅需 Port 至 VPN 区接口的 2 条策略即可

4.OSPF 配置

OSPF 的详细设置方法请参考 FortiGate OSPF 设置。

4.1 GateA 配置

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

将 VPN 虚拟接口网络及其他需要发布的网络至 OSPF 中,创建 OSPF 接口,将 VPN 接口加入 OSPF 接口

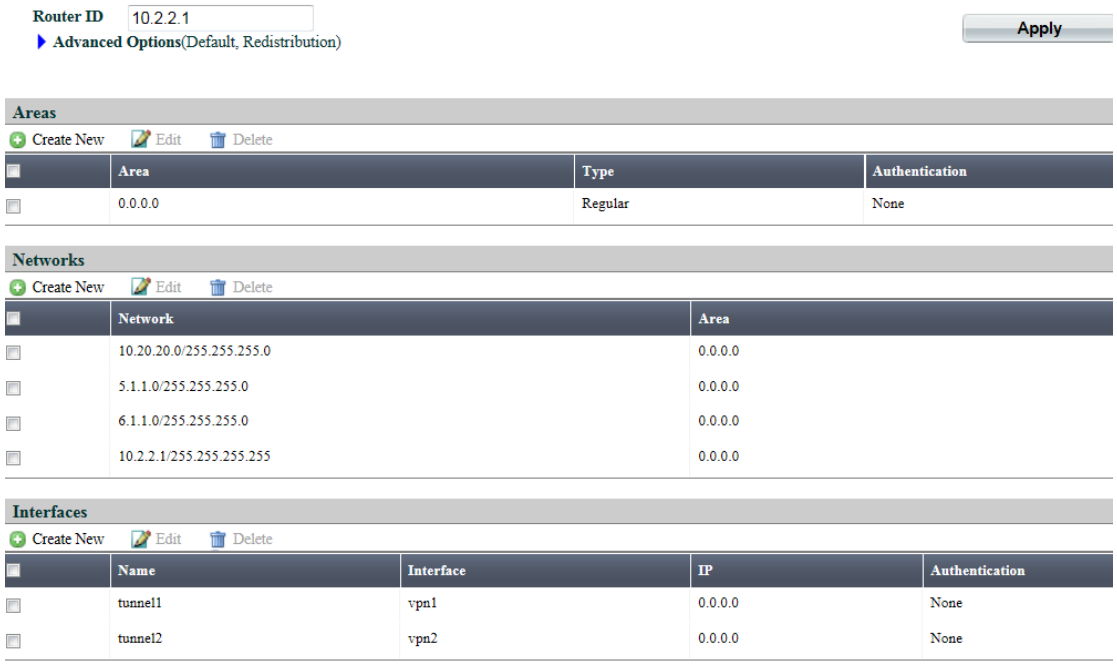
OSPF 配置完成后,进入命令行,为冗余链路配置 VPN 接口的 cost 值及网络类型。此处将 VPN1 接口 cost 设置为 100,VPN2 接口 cost 为 200,那么 OSPF 将优选 VPN1 的路由。另需将网络类型设置为 point-to-point。

```
config router ospf
        config ospf-interface
            edit "tunnel1"
                set cost 100
                set interface "vpn1"
                set network-type point-to-point
            next
            edit "tunnel2"
                set cost 200
                set interface "vpn2"
                set network-type point-to-point
            next
        end
end
```

4.2 GateB 配置

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

GateB 配置与 GateA 基本相似



同样需要在命令行中设置接口 cost 及网络类型

```
config router ospf
        config ospf-interface
            edit "tunnel1"
                set cost 100
                set interface "vpn1"
                set network-type point-to-point
            next
            edit "tunnel2"
                set cost 200
                set interface "vpn2"
                set network-type point-to-point
            next
        end
end
```

4.3 配置完成后各 FortiGate 路由表

GateA OSPF 路由表

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

Type: OSPF Network: Gateway: Apply Filter

Type	Subtype	Network	Distance	Metric	Gateway	Interface	Up Time (d h:m:s)
OSPF		10.2.2.1/32	110	200	5.1.1.2	vpn1	0 02:35:19
OSPF		10.20.20.0/24	110	110	5.1.1.2	vpn1	0 02:35:19

GateB OSPF 路由表

Type: OSPF Network: Gateway: Apply Filter

Type	Subtype	Network	Distance	Metric	Gateway	Interface	Up Time (d h:m:s)
OSPF		10.1.1.1/32	110	200	5.1.1.1	vpn1	0 02:36:07
OSPF		10.10.10.0/24	110	110	5.1.1.1	vpn1	0 02:36:07

4.4 通过命令查看 OSPF 状态

查看 OSPF 邻居状态

GateA # get router info ospf neighbor

OSPF process 0:

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.2.2.1	1	Full/ -	00:00:38	5.1.1.2	vpn1
10.2.2.1	1	Full/ -	00:00:34	6.1.1.2	vpn2

查看 OSPF 路由表

GateA # get router info routing-table ospf
O 10.2.2.1/32 [110/200] via 5.1.1.2, vpn1, 02:38:37
O 10.20.20.0/24 [110/110] via 5.1.1.2, vpn1, 02:38:37

5.冗余路由的验证

GateB 上开启 Debug 查看 OSPF 路由的计算信息，关闭 GateA 上的 VPN1 接口查看 debug 输出信息。

GateB # diagnose debug reset
GateB # diagnose debug enable
GateB # diagnose ip router ospf route enable
GateB # diagnose ip router ospf level info

GateB # diagnose ip router ospf show
OSPF debugging status:

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

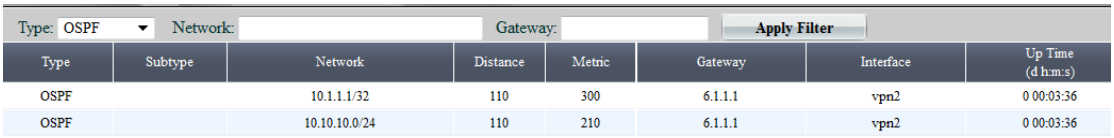
OSPF all route calculation debugging is on
OSPF debugging level is INFO

将 VPN1 的物理接口 Port7 的管理状态关闭后 ,OSPF 将重新计算最优路径。

****

GateB # id=36870 msg="OSPF: RT[Delete:0.0.0.0]: 5.1.1.2/32, connected network"
id=36870 msg="OSPF: SPF[0.0.0.0]: Calculation timer scheduled (delay 5.000000 secs)"
id=36870 msg="OSPF: SPF[0.0.0.0]: SPF calculation (1st STAGE)"
id=36870 msg="OSPF: SPF[0.0.0.0]: Vertex[10.2.2.1] Router(root)"
id=36870 msg="OSPF: SPF[0.0.0.0]: Link #0 (10.20.20.0): Stub Network"
id=36870 msg="OSPF: SPF[0.0.0.0]: Link #1 (10.1.1.1): Point-to-Point"
id=36870 msg="OSPF: SPF[0.0.0.0]: Calculate nexthop for (10.1.1.1)"
id=36870 msg="OSPF: SPF[0.0.0.0]: Link #2 (6.1.1.2): Stub Network"
id=36870 msg="OSPF: SPF[0.0.0.0]: Link #3 (6.1.1.1): Stub Network"
id=36870 msg="OSPF: SPF[0.0.0.0]: Link #4 (10.2.2.1): Stub Network"
id=36870 msg="OSPF: SPF[0.0.0.0]: Vertex[10.1.1.1] Router"
id=36870 msg="OSPF: SPF[]: Link #0 (10.2.2.1): Point-to-Point"
id=36870 msg="OSPF: SPF[0.0.0.0]: LSA[Type1:0.0.0.0:Type1:10.2.2.1:(self)] is already in SPF tree"
id=36870 msg="OSPF: SPF[]: Link #1 (6.1.1.1): Stub Network"
id=36870 msg="OSPF: SPF[]: Link #2 (6.1.1.2): Stub Network"
id=36870 msg="OSPF: SPF[]: Link #3 (10.1.1.1): Stub Network"
id=36870 msg="OSPF: SPF[]: Link #4 (10.10.10.0): Stub Network"
id=36870 msg="OSPF: SPF[0.0.0.0]: SPF calculation (2nd STAGE)"
id=36870 msg="OSPF: SPF[0.0.0.0]: Calculating stub network for (10.1.1.1)"
id=36870 msg="OSPF: RT[Install:0.0.0.0]: 6.1.1.1/32, cost(200) stub network"
id=36870 msg="OSPF: RT[Install:0.0.0.0]: 6.1.1.2/32, cost(400) stub network"
id=36870 msg="OSPF: RT[Install:0.0.0.0]: 10.1.1.1/32, cost(300) stub network"
id=36870 msg="OSPF: RT[Install:0.0.0.0]: 10.10.10.0/24, cost(210) stub network"
id=36870 msg="OSPF: Route[IA:0.0.0.0]: Cleanup IA route"
id=36870 msg="OSPF: SPF[0.0.0.0]: Calculation finished (0.000000 sec)"
id=36870 msg="OSPF: Route[ASE]: ASE calculation starts"
id=36870 msg="OSPF: Route[ASE]: ASE calculation completed"

经过 SPF 重新计算后的路由表


Type: OSPF Network: Gateway: Apply Filter

Type	Subtype	Network	Distance	Metric	Gateway	Interface	Up Time (d h:m:s)
OSPF		10.1.1.1/32	110	300	6.1.1.1	vpn2	0 00:03:36
OSPF		10.10.10.0/24	110	210	6.1.1.1	vpn2	0 00:03:36

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

GateB # get router info routing-table ospf
O 10.1.1.1/32 [110/300] via 6.1.1.1, vpn2, 00:04:07
O 10.10.10.0/24 [110/210] via 6.1.1.1, vpn2, 00:04:07

6.参考

Technical Note:OSPF route redundancy over 2 VPN IPSec tunnels

FortiGate OSPF 设置

站到站 IPSec VPN 设置 4.2

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255