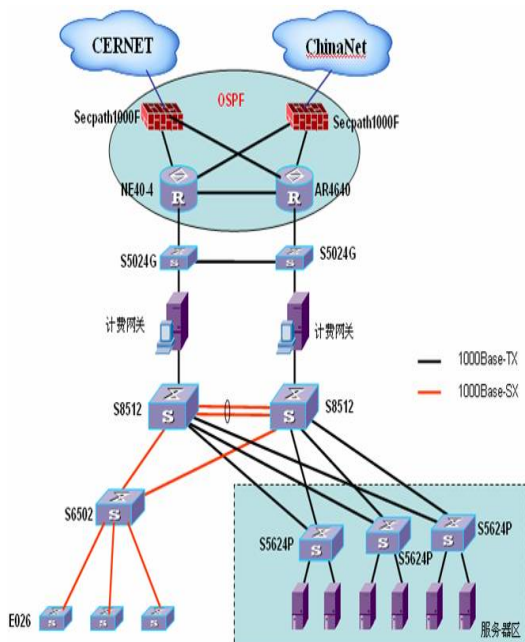


Auto-detect结合OSPF实现校园网双出口动态备份案例

【问题概述】

某大学用NE40和AR46,以及2台Secpatch1000F, 实现教育网出口和电信网出口的双向动态备份。本案例涉及到Auto-detect新功能, 这是VRP3.4刚开发的新功能, 因为Secpath是直接移植VRP3.4, 所以也具有本功能。

【拓扑结构】



【组网需求】

- 1) NE40,AR46,以及2台Secpatch1000F要做到动态备份, 即任何链路断掉, 可以自动切换到备份链路上。
- 2) 访问教育网通过左边的Secpatch1000F, 访问公网通过右边的Secpatch1000F。
- 3) 当教育网不能访问的时候, 自动切换到右边的Secpatch1000F访问教育网,
- 4) 当公网不能访问的时候, 自动切换到左边的Secpatch1000F访问公网

【实现思想】

- 1) 通过在NE40,AR46,以及2台Secpatch1000F起用OSPF(图中蓝色区域), 做到动态备份。实现任何链路断掉都能切换到备份链路上。
- 2) 在左边的防火墙配置到教育网网段的静态路由, 然后引入OSPF域内, 这样可以访问教育网网段的路由通过左边的Secpatch1000F出去。
- 3) 在右边的Secpatch1000F生成OSPF缺省路由, 这样除了教育网网段的路由都会从右边的Secpatch1000F上出去。
- 4) 怎么样能做到当教育网不可达自动切换到公网?

方案一:

可以做策略路由, 当下一跳不可达时, 自动切换到第二个下一跳。但是, 现在的组网是NE40通过光纤收发器连接到Cernet, 如果光纤收发器连接Cernet的一端down掉, 那么NE40出口仍然是up, 策略路由无法感知。显然这个方案行不通。

方案二:

(1) 通过Auto - detect功能定义侦测的教育网IP, 并且把到教育网的所有静态路由绑定到该侦测组。当侦测该IP不通的时候, 到教育网的所有路由会自动失效, 这时到教育网的网段就会通过默认路由出去, 而发布默认路由的就是右边的Secpatch1000F, 所以此时到教育网的路由已经自动切换到了右边的Secpatch1000F。

(2) 这里大家有没有考虑到这样一个问题。。。Autodetect只会让路由失效, 但是不会把路由从路由表里面删除, 所以OSPF引入的时候会删除掉这些失效的路由吗? OK, 不用担心, 容我娓娓道来。。。路由表转发数据的时候其实是匹配快转表, 如果快转表失效, 那么目的地址就不可达, 匹配该快转表项的路由表项也会失效。当Autodetect的侦测IP不可达时, 虽然路由表没有被删除, 但是该快转表项已经被删除了, 所以此时引入OSPF的路由表会自动删除。后面的试验中我会列出, 大家一看便知。

(3) 那么大家还有没有考虑到另外一个问题, 如果我到达侦测IP的快转表项都被删除, 当该IP是一个

非直连IP的时候，没有路由，如何能够继续侦测该IP（当公网也不能访问到该IP的时候）？当该IP能够ping通的时候，不能侦测，如何才能恢复到原路由？

通过以上N种情况的考虑，当教育网不可达时，链路会自动切换到公网。

5) 当公网不可达的时候如何自动切换到教育网？

我们可以在左边的Secpath1000F上发布一条默认路由，调整其cost值，让它比右边的Secpath1000F发布的默认路由cost高，所以这样的话，OSPF域内会有2条默认路由，但是右边的OSPF发布的默认路由cost小，优先级高，所以默认路由会走右边的Secpath1000F。我们此时可以对右边的Secpath1000F的默认路由做Autodetect，当侦测公网某IP不可达的时候，OSPF会自动删掉引入的该默认路由，左边的Secpath1000F的默认路由就会自动生效了。这就实现了当公网不可达的时候自动切换到教育网。

【左边的Secpath1000F配置】

```
dis cu
#
sysname Quidway
#
dvpn service enable
#
router id 1.1.1.1
#
firewall packet-filter enable
#
firewall statistic system enable
#
radius scheme system
#
domain system
#
detect-group 1
detect-list 1 ip address 6.6.6.1 nexthop 5.5.5.2  定义侦测组
#
interface Aux0
  async mode flow
#
interface GigabitEthernet0/0
  ip address 5.5.5.1 255.255.255.0      连接教育网的IP地址
#
interface GigabitEthernet0/1
  ip address 2.2.2.1 255.255.255.0      连接右边的Sepatch1000F的IP地址
#
interface NULL0
#
interface LoopBack0
  ip address 1.1.1.1 255.255.255.255    ROUTER ID
#
interface LoopBack1
  ip address 10.1.1.1 255.255.255.0
#
interface LoopBack2
  ip address 10.1.2.1 255.255.255.0
定义2个loopback IP，看右边Sepatch1000F是否能学习到
#
firewall zone local
  set priority 100
#
firewall zone trust
  add interface GigabitEthernet0/0      把端口加入到域里面
  add interface GigabitEthernet0/1
  set priority 85
#
ospf 1
  import-route direct
  import-route static
  default-route-advertise cost 15      启用OSPF,引入直连和静态路由，把教育网网段路由引入
到OSPF同时发布默认路由，但是其优先级比右边的Sepatch1000F低
```

```

area 0.0.0.0
network 2.2.2.0 0.0.0.255
network 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 5.5.5.2 preference 200      默认路由指向教育网IP，但是必须优先级比右边设备默认优先级低
ip route-static 6.6.6.0 255.255.255.0 5.5.5.2 preference 60      6.6.6.1为被探测IP.
ip route-static 7.7.1.0 255.255.255.0 5.5.5.2 preference 60 detect-group 1
ip route-static 7.7.7.0 255.255.255.0 5.5.5.2 preference 60 detect-group 1
ip route-static 202.105.0.0 255.255.255.0 5.5.5.2 preference 60 detect-group 1
ip route-static 202.105.1.0 255.255.255.0 5.5.5.2 preference 60 detect-group 1
ip route-static 202.105.2.0 255.255.255.0 5.5.5.2 preference 60 detect-group 1
.....
202.105网段的为教育网IP，共200条，不再一一列举。具体配置见附件
【右边的Secpath1000F配置】
<Quidway>dis cu
#
sysname Quidway
#
dvpn service enable
#
router id 1.1.1.2
#
firewall packet-filter enable
#
firewall statistic system enable
#
radius scheme system
#
domain system
#
detect-group 1
detect-list 1 ip address 211.198.1.3 nexthop 9.9.9.2  定义公网侦测组

#
interface Aux0
  async mode flow
#
interface Ethernet0/0
#
interface Ethernet1/0
  ip address 2.2.2.2 255.255.255.0  连接左边Sepatch1000F端口 IP
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface NULL0
#
interface LoopBack0
  ip address 1.1.1.2 255.255.255.255  作为ROUTER ID
#
interface LoopBack1
  ip address 10.2.0.1 255.255.255.0
#
interface LoopBack2
  ip address 10.2.1.1 255.255.255.0
#
interface LoopBack3
  ip address 9.9.9.1 255.255.255.0  设置3个loopback，看对方OSPF是否能学习到

#
firewall zone local

```

```

set priority 100
#
firewall zone trust
add interface Ethernet0/0
add interface Ethernet1/0
set priority 85
#
firewall zone untrust
set priority 5
#
firewall zone DMZ
set priority 50
#

#
ospf 1
default-route-advertise      OSPF通告其静态路由，让上公网IP走右边路由
area 0.0.0.0
network 2.2.2.0 0.0.0.255
network 10.2.0.0 0.0.0.255
network 10.2.1.0 0.0.0.255   发布其他几个loopback网段IP
#
ip route-static 0.0.0.0 0.0.0.0 9.9.9.2 preference 60 detect-group 1

```

配置默认路由，然后OSPF发布为默认路由，并且关联侦测组，当公网IP不可达，那么这条路由失效，OSPF会启用左边的Secpath1000F的默认路由

【教育网不可达时候的状态】

左边防火墙的路由

dis ip rou

Routing Table: public net

Destination/Mask	Protocol	Pre	Cost	NextHop	Interface
0.0.0.0/0	O_ASE	150	1	2.2.2.2	GigabitEthernet0/1
0.0.0.0/0	STATIC	200	15	2.2.2.1	GigabitEthernet0/1
1.1.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
2.2.2.0/24	DIRECT	0	0	2.2.2.1	GigabitEthernet0/1
2.2.2.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
5.5.5.0/24	DIRECT	0	0	5.5.5.1	GigabitEthernet0/0
5.5.5.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
6.6.6.0/24	STATIC	60	0	5.5.5.2	GigabitEthernet0/0
10.1.1.0/24	DIRECT	0	0	10.1.1.1	LoopBack1
10.1.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
10.1.2.0/24	DIRECT	0	0	10.1.2.1	LoopBack2
10.1.2.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
10.2.0.0/24	OSPF	10	2	2.2.2.2	GigabitEthernet0/1
10.2.1.0/24	OSPF	10	2	2.2.2.2	GigabitEthernet0/1
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0

我们可以看到，OSPF已经把到教育网路由删除，那么此时通过默认路由访问教育网

【公网不可达的状态】

右边的路由

0.0.0.0/0	STATIC	200	15	2.2.2.1	GigabitEthernet0/0
5.5.5.0/24	DIRECT	0	0	5.5.5.1	GigabitEthernet0/0
5.5.5.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
6.6.6.0/24	STATIC	60	0	5.5.5.2	GigabitEthernet0/0
7.7.1.0/24	STATIC	60	0	5.5.5.2	GigabitEthernet0/0
7.7.7.0/24	STATIC	60	0	5.5.5.2	GigabitEthernet0/0
202.105.0.0/24	O_ASE	150	1	2.2.2.1	Ethernet1/0
202.105.1.0/24	O_ASE	150	1	2.2.2.1	Ethernet1/0
202.105.2.0/24	O_ASE	150	1	2.2.2.1	Ethernet1/0

可以看到，OSPF已经把到公网的默认路由删除，默认通过左边防火墙发布的默认路由出去。