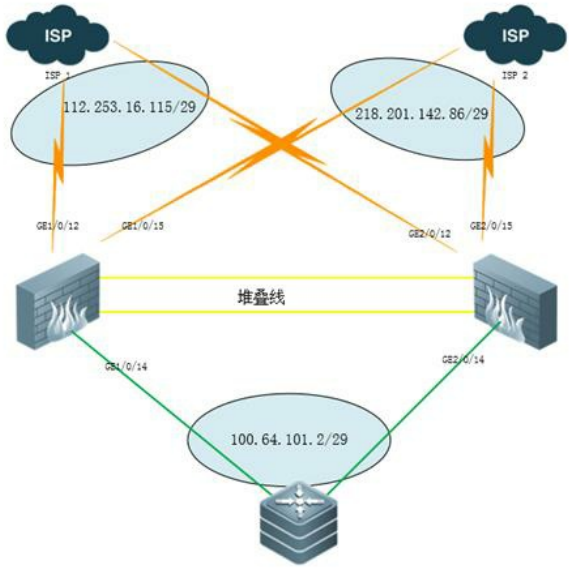
F1020防火墙堆叠ipsec冗余备份

李旭东 2017-12-30 发表



对应物理拓扑，配置双出口ipsec冗余备份，主设备宕机之后ipsec业务切换异常。

```
[IPSEC]display current-configuration
#
 version 7.1.064, Release 9313P15
#
 sysname IPSEC
#
context Admin id 1
#
 telnet server enable
 telnet server acl 2001
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 32
 irf member 2 priority 1
#
 ip ttl-expires enable
#
 password-recovery enable
#
vlan 1
#
irf-port 1/1
 port group interface GigabitEthernet1/0/3
 port group interface GigabitEthernet1/0/5
#
irf-port 2/2
 port group interface GigabitEthernet2/0/3
 port group interface GigabitEthernet2/0/5
#
nqa entry admin1 test1
 type icmp-echo
  destination ip 218.201.142.81
  frequency 100
  next-hop ip 218.201.142.81
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
```

```
  source ip 218.201.142.86
#
nqa entry admin2 test2
 type icmp-echo
  destination ip 112.253.16.113
  frequency 100
  next-hop ip 112.253.16.113
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
  source ip 112.253.16.115
#
 nqa schedule admin2 test2 start-time now lifetime forever
#
interface Reth1
 ip address 112.253.16.115 255.255.255.248
 member interface GigabitEthernet1/0/12 priority 255
 member interface GigabitEthernet2/0/12 priority 50
 ipsec apply policy policy2
#
interface Reth2
 ip address 218.201.142.86 255.255.255.248
 member interface GigabitEthernet1/0/15 priority 255
 member interface GigabitEthernet2/0/15 priority 50
 ipsec apply policy policy1
#
interface Reth3
 ip address 100.64.101.2 255.255.255.248
 member interface GigabitEthernet1/0/14 priority 255
 member interface GigabitEthernet2/0/14 priority 50
#
interface NULL0
#
interface GigabitEthernet1/0/0
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
#
interface GigabitEthernet1/0/2
 port link-mode route
#
interface GigabitEthernet1/0/4
 port link-mode route
#
interface GigabitEthernet1/0/6
 port link-mode route
#
interface GigabitEthernet1/0/7
 port link-mode route
#
interface GigabitEthernet1/0/8
 port link-mode route
#
interface GigabitEthernet1/0/9
 port link-mode route
#
interface GigabitEthernet1/0/10
 port link-mode route
#
interface GigabitEthernet1/0/11
 port link-mode route
#
interface GigabitEthernet1/0/12
 port link-mode route
```

```
#
interface GigabitEthernet1/0/13
 port link-mode route
#
interface GigabitEthernet1/0/14
 port link-mode route
#
interface GigabitEthernet1/0/15
 port link-mode route
#
interface GigabitEthernet1/0/16
 port link-mode route
#
interface GigabitEthernet1/0/17
 port link-mode route
#
interface GigabitEthernet1/0/18
 port link-mode route
#
interface GigabitEthernet1/0/19
 port link-mode route
#
interface GigabitEthernet1/0/20
 port link-mode route
#
interface GigabitEthernet1/0/21
 port link-mode route
#
interface GigabitEthernet1/0/22
 port link-mode route
 shutdown
#
interface GigabitEthernet1/0/23
 port link-mode route
 shutdown
#
interface GigabitEthernet2/0/0
 port link-mode route
#
interface GigabitEthernet2/0/1
 port link-mode route
#
interface GigabitEthernet2/0/2
 port link-mode route
#
interface GigabitEthernet2/0/4
 port link-mode route
#
interface GigabitEthernet2/0/6
 port link-mode route
#
interface GigabitEthernet2/0/7
 port link-mode route
#
interface GigabitEthernet2/0/8
 port link-mode route
#
interface GigabitEthernet2/0/9
 port link-mode route
#
interface GigabitEthernet2/0/10
 port link-mode route
#
interface GigabitEthernet2/0/11
```

```
 port link-mode route
#
interface GigabitEthernet2/0/12
 port link-mode route
#
interface GigabitEthernet2/0/13
 port link-mode route
#
interface GigabitEthernet2/0/14
 port link-mode route
#
interface GigabitEthernet2/0/15
 port link-mode route
#
interface GigabitEthernet2/0/16
 port link-mode route
#
interface GigabitEthernet2/0/17
 port link-mode route
#
interface GigabitEthernet2/0/18
 port link-mode route
#
interface GigabitEthernet2/0/19
 port link-mode route
#
interface GigabitEthernet2/0/20
 port link-mode route
#
interface GigabitEthernet2/0/21
 port link-mode route
#
interface GigabitEthernet2/0/22
 port link-mode route
#
interface GigabitEthernet2/0/23
 port link-mode route
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/5
#
interface GigabitEthernet2/0/3
#
interface GigabitEthernet2/0/5
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet1/0/14
 import interface GigabitEthernet2/0/14
 import interface Reth3
#
security-zone name DMZ
#
security-zone name Untrust
 import interface GigabitEthernet1/0/12
 import interface GigabitEthernet1/0/15
 import interface GigabitEthernet2/0/12
 import interface GigabitEthernet2/0/15
 import interface Reth1
 import interface Reth2
#
security-zone name Management
```

```
 import interface GigabitEthernet1/0/0
#
zone-pair security source Local destination Trust
 packet-filter 3000
#
zone-pair security source Local destination Untrust
 packet-filter 3000
#
zone-pair security source Trust destination Local
 packet-filter 3000
#
zone-pair security source Trust destination Untrust
 packet-filter 3000
#
zone-pair security source Untrust destination Local
 packet-filter 3000
#
zone-pair security source Untrust destination Trust
 packet-filter 3000
#
 scheduler logfile size 16
#
line class aux
 user-role network-operator
#
line class console
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line aux 1
 user-role network-operator
#
line con 0 1
 authentication-mode scheme
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 ip route-static 0.0.0.0 0 218.201.142.81 track 10
 ip route-static 0.0.0.0 0 112.253.16.113 track 20 preference 61
 ip route-static 10.19.184.0 24 100.64.101.1
 ip route-static 10.19.209.0 26 100.64.101.1
 ip route-static 192.169.250.0 24 100.64.101.1 description guanli
#
 ssh server enable
 ssh server acl 2001
#
redundancy group aaa
 member interface Reth1
 member interface Reth2
 member interface Reth3
 node 1
  bind slot 1
  priority 100
  track 1 interface GigabitEthernet1/0/12
  track 2 interface GigabitEthernet1/0/14
  track 3 interface GigabitEthernet1/0/15
```

```
 node 2
  bind slot 2
  priority 50
  track 4 interface GigabitEthernet2/0/12
  track 5 interface GigabitEthernet2/0/14
  track 6 interface GigabitEthernet2/0/15
#
acl basic 2001
 description user login
 rule 10 permit source 192.169.250.0 0.0.0.255
 rule 70 permit source 218.201.142.80 0.0.0.7
 rule 75 permit source 218.59.137.216 0.0.0.7
 rule 80 permit source 58.58.75.176 0.0.0.7
#
acl advanced 3000
 rule 0 permit ip
#
acl advanced 3001
 rule 0 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.190.0 0.0.0.255
 rule 1 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.188.0 0.0.0.255
 rule 2 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.194.0 0.0.0.255
 rule 3 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.80.0 0.0.0.255
 rule 4 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.90.0 0.0.0.255
 rule 5 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.98.0 0.0.0.255
 rule 6 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.89.0 0.0.0.255
 rule 7 permit ip source 10.19.184.0 0.0.0.255 destination 10.213.53.0 0.0.0.255
 rule 8 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.191.0 0.0.0.255
 rule 9 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.181.0 0.0.0.255
 rule 10 permit ip source 10.19.184.0 0.0.0.255 destination 218.206.83.167 0
 rule 11 permit ip source 10.19.184.0 0.0.0.255 destination 10.213.51.0 0.0.0.255
 rule 12 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.222.0 0.0.0.255
 rule 13 permit ip source 10.19.184.0 0.0.0.255 destination 218.206.83.0 0.0.0.255
 rule 14 permit ip source 10.19.184.0 0.0.0.255 destination 58.58.116.38 0
 rule 15 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.251.11 0
 rule 16 permit ip source 10.19.184.0 0.0.0.255 destination 10.19.244.0 0.0.0.255
 rule 17 permit ip source 10.19.209.0 0.0.0.255 destination 10.19.244.0 0.0.0.255
 rule 18 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.190.0 0.0.0.255
 rule 19 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.188.0 0.0.0.255
 rule 20 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.194.0 0.0.0.255
 rule 21 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.80.0 0.0.0.255
 rule 22 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.90.0 0.0.0.255
 rule 23 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.98.0 0.0.0.255
 rule 24 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.89.0 0.0.0.255
 rule 25 permit ip source 10.19.209.0 0.0.0.63 destination 10.213.53.0 0.0.0.255
 rule 26 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.191.0 0.0.0.255
 rule 27 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.181.0 0.0.0.255
 rule 28 permit ip source 10.19.209.0 0.0.0.63 destination 218.206.83.167 0
 rule 29 permit ip source 10.19.209.0 0.0.0.63 destination 10.213.51.0 0.0.0.255
 rule 30 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.222.0 0.0.0.255
 rule 31 permit ip source 10.19.209.0 0.0.0.63 destination 218.206.83.0 0.0.0.255
 rule 32 permit ip source 10.19.209.0 0.0.0.63 destination 58.58.116.38 0
 rule 33 permit ip source 10.19.209.0 0.0.0.63 destination 10.19.251.11 0
#
domain system
#
 aaa session-limit ftp 16
 aaa session-limit telnet 16
 aaa session-limit ssh 16
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
```

```
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$THKMatT1IyqeCupX$PZU1fGdQkPethCIXJ/qK1jvBldBUPk6Or8DD2wBFGLh+cfAJTD9Pe4kB
WqCvEJKbU9iJCbeKjxzCzIGrDx1o4g==
 service-type ssh telnet terminal https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
ipsec transform-set tran1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy policy1 10 isakmp
 transform-set tran1
 security acl 3001
 local-address 218.201.142.86
 remote-address 211.137.182.6
 ike-profile 10
#
ipsec policy policy2 10 isakmp
```

```
 transform-set tran1
 security acl 3001
 local-address 112.253.16.115
 remote-address 211.137.182.6
 ike-profile 20
#
 ike dpd interval 10 periodic
#
ike profile 10
 keychain keychain1
 dpd interval 10 periodic
 match remote identity address 211.137.182.6 255.255.255.255
 proposal 10
#
ike profile 20
 keychain keychain2
 dpd interval 10 periodic
 match remote identity address 211.137.182.6 255.255.255.255
 proposal 10
#
ike proposal 10
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain keychain1
 pre-shared-key address 211.137.182.6 255.255.255.255 key cipher $c$3$lOJ84oScQ8HRESAdxXV
ooLpz/dYqQxdnp7sf3r91GA==
#
ike keychain keychain2
 pre-shared-key address 211.137.182.6 255.255.255.255 key cipher $c$3$O11+/3JqxnjYV9z2o67WL
Y16asAHtrMz/4tCzGuX5Q==
#
 ip https acl 2001
 ip https enable
#
inspect block-source parameter-profile ips_block_default_parameter
#
ips policy default
#
anti-virus policy default
#
 track 1 interface GigabitEthernet1/0/12 physical
 track 2 interface GigabitEthernet1/0/14 physical
 track 3 interface GigabitEthernet1/0/15 physical
 track 4 interface GigabitEthernet2/0/12 physical
 track 5 interface GigabitEthernet2/0/14 physical
 track 6 interface GigabitEthernet2/0/15 physical
 track 10 nqa entry admin1 test1 reaction 1
 track 20 nqa entry admin2 test2 reaction 1
#
return
```

[IPSEC]

配置防火墙会话松散模式和会话同步依然没有解决，

ipsec流量切换不能是简单的通过路由和会话备份来切换。

开启IPsec冗余备份功能。

```
<Sysname> system-view
[Sysname] ipsec redundancy enable
```

开启冗余备份功能后，系统会根据命令redundancy replay-interval指定的备份间隔对系统中的所有IPsec SA进行抗重放窗口值和序列号的备份，当发生主备切换时，可以保证主备IPsec流量不中断和抗重放保护不间断。