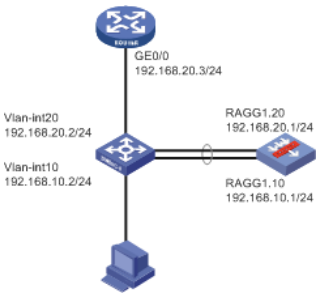
V7防火墙旁路部署结合track NQA典型配置案例

NQA Track 孙轶宁 2020-04-30 发表

组网及说明



如图，交换机的int vlan 10和防火墙的RAGG1.10处于同一网段，交换机的int vlan20、路由器的GE0/0以及防火墙的RAGG1.20处于同一网段。

现在客户需要实现如下需求：防火墙工作正常的时候，终端前往边界路由器的流量需要经过防火墙，但是当防火墙异常的时候，流量直接从交换机转发给防火墙。

在交换机和路由器上通过配置静态路由结合track NQA，使防火墙正常的时候路由指向防火墙，当防火墙出问题后，路由不再指向防火墙，直接在交换机转发。

配置步骤

防火墙配置：

```
interface Route-Aggregation1.10
 ip address 192.168.10.1 255.255.255.0
 vlan-type dot1q vid 10
#
interface Route-Aggregation1.20
 ip address 192.168.20.1 255.255.255.0
 vlan-type dot1q vid 20
#
interface GigabitEthernet1/0/0
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/1
 port link-mode route
 port link-aggregation group 1
#
security-zone name Trust
 import interface Route-Aggregation1.10
#
security-zone name Untrust
 import interface Route-Aggregation1.20
#
 ip route-static 0.0.0.0 0 192.168.20.3
 ip route-static 192.168.100.0 24 192.168.10.2
#
security-policy ip
 rule 0 name permit-all
  action pass
  source-zone untrust
  source-zone trust
  source-zone local
  destination-zone untrust
  destination-zone trust
  destination-zone local
```

交换机配置

```
track 1 nqa entry fw 1 reaction 1 //track nqa状态
#
nqa entry fw 1   //配置nqa，探测10.1是否可达，频率1秒（100厘秒），探测三次
```

```
 type icmp-echo
  destination ip 192.168.10.1
  frequency 100
  reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
#
 nqa schedule fw 1 start-time now lifetime forever  //开启nqa探测
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 10 20
#
interface Vlan-interface10
 ip address 192.168.10.2 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.20.2 255.255.255.0
#
interface Vlan-interface100
 ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
 ip route-static 0.0.0.0 0 192.168.10.1 track 1   //配置静态路由指向防火墙并调用track，当nqa探测失败的时候自动失效
 ip route-static 0.0.0.0 0 192.168.20.3 preference 70   //配置浮动路由指向路由器，当上面的静态路由失效的时候生效
```

路由器配置

```
track 1 nqa entry fw 1 reaction 1//track nqa状态
#
nqa entry fw 1   //配置nqa，探测20.1是否可达，频率1秒（100厘秒），探测三次
 type icmp-echo
  destination ip 192.168.20.1
  frequency 100
  reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
#
 nqa schedule fw 1 start-time now lifetime forever   //开启nqa探测
#
interface LoopBack0   //模拟的外网地址
 ip address 100.100.100.100 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.20.3 255.255.255.0
#
 ip route-static 192.168.100.0 24 192.168.20.1 track 1  //配置静态路由指向防火墙并调用track，当nqa探测失败的时候自动失效
 ip route-static 192.168.100.0 24 192.168.20.2 preference 70   //配置浮动路由指向交换机，当上面的静态路由失效的时候生效
```

测试结果

正常情况下的交换机路由表

```
[SW]dis ip ro
```

Destinations : 21 Routes : 21

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/0 Static 60 0 192.168.10.1 Vlan10
.....
正常情况下的路由器路由表
[RT]dis ip ro

Destinations : 14 Routes : 14

Destination/Mask Proto Pre Cost NextHop Interface
.....
192.168.100.0/24 Static 60 0 192.168.20.1 GE0/0
.....
PC(192.168.100.2)测试访问100.100.100.100
[PC]ping 100.100.100.100
Ping 100.100.100.100 (100.100.100.100): 56 data bytes, press CTRL_C to break
56 bytes from 100.100.100.100: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 100.100.100.100: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 100.100.100.100: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 100.100.100.100: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 100.100.100.100: icmp_seq=4 ttl=253 time=4.000 ms

--- Ping statistics for 100.100.100.100 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/3.000/4.000/0.632 ms
此时防火墙能够看到会话，说明流量经过防火墙
[FW]dis session table ipv4 source-ip 192.168.100.2 destination-ip 100.100.100.100 verbose
Slot 1:
Initiator:
Source IP/port: 192.168.100.2/225
Destination IP/port: 100.100.100.100/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: Route-Aggregation1.10
Source security zone: Trust
Responder:
Source IP/port: 100.100.100.100/225
Destination IP/port: 192.168.100.2/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: Route-Aggregation1.20
Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: permit-all
Start time: 2020-04-30 03:10:17 TTL: 26s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

当防火墙故障的时候，track使静态路由失效
%Apr 30 03:25:36:153 2020 SW NQA/6/NQA_ENTRY_PROBE_RESULT: Reaction entry 1 of NQA e
ntry admin-name fw operation-tag 1: probe-fail.
dis track 1
Track ID: 1
State: **Negative**
Duration: 0 days 0 hours 0 minutes 15 seconds
Tracked object type: NQA
Notification delay: Positive 0, Negative 0 (in seconds)

Tracked object:
NQA entry: fw 1
Reaction: 1
Remote IP/URL: 192.168.10.1
Local IP: --
Interface: --
%Apr 30 03:25:41:279 2020 RT NQA/6/NQA_ENTRY_PROBE_RESULT: Reaction entry 1 of NQA e
ntry admin-name fw operation-tag 1: probe-fail.
dis track 1
Track ID: 1
State: **Negative**
Duration: 0 days 0 hours 2 minutes 43 seconds
Tracked object type: NQA
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
NQA entry: fw 1
Reaction: 1
Remote IP/URL: 192.168.20.1
Local IP: --
Interface: --
此时看静态路由，发现SW、RT的路由已切换不走防火墙
dis ip ro

Destinations : 21 Routes : 21

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/0 Static 70 0 192.168.20.3 Vlan20
.....
dis ip ro

Destinations : 14 Routes : 14

.....
192.168.100.0/24 Static 70 0 192.168.20.2 GE0/0
.....
PC仍然能够ping通100.100.100.100
ping 100.100.100.100
Ping 100.100.100.100 (100.100.100.100): 56 data bytes, press CTRL_C to break
56 bytes from 100.100.100.100: icmp_seq=0 ttl=254 time=2.000 ms
56 bytes from 100.100.100.100: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 100.100.100.100: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 100.100.100.100: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 100.100.100.100: icmp_seq=4 ttl=254 time=2.000 ms

--- Ping statistics for 100.100.100.100 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.400/2.000/0.490 ms
此时由于流量不经过防火墙，防火墙上没有会话
[FW-Route-Aggregation1.10]dis session table ipv4 source-ip 192.168.100.2 destination-ip 100.100.10
0.100 verbose
Slot 1:
Total sessions found: 0

配置关键点