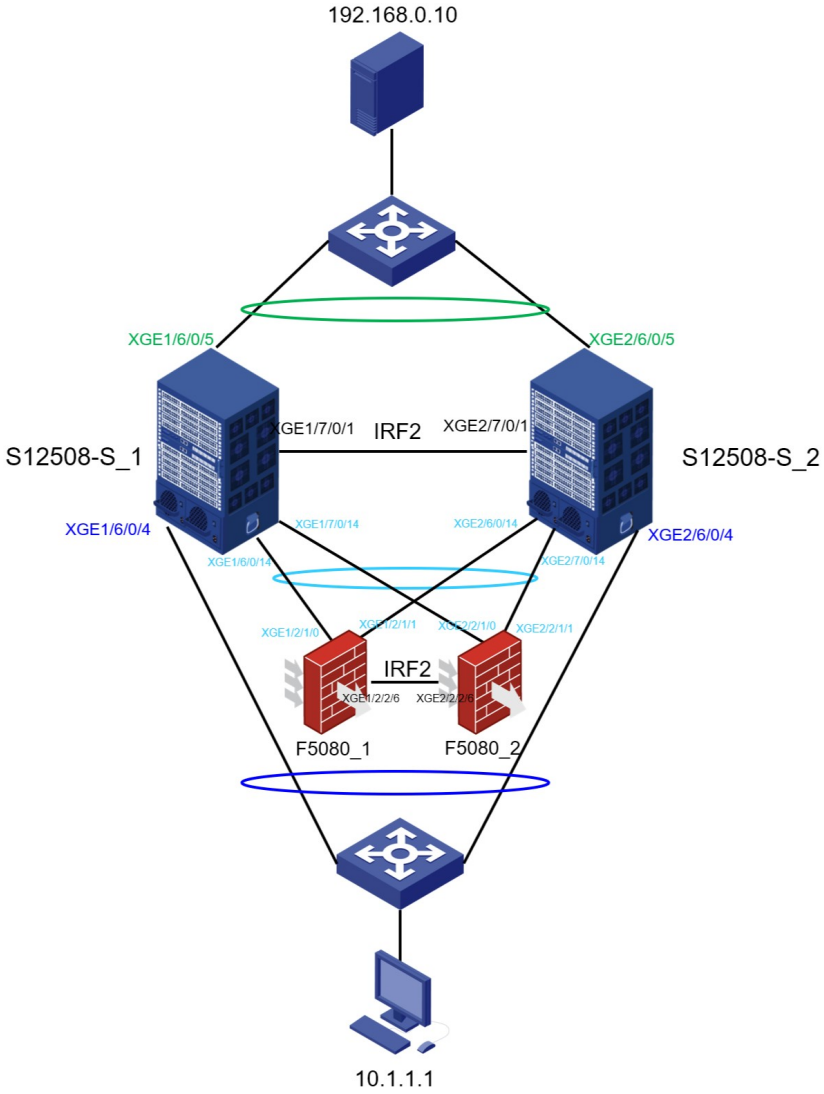
H3C F5080-D 防火墙主备二层跨VLAN转发（旁路部署）经验案例

IRF　二层转发　旁路部署　丁犁　2019-01-16 发表

组网及说明

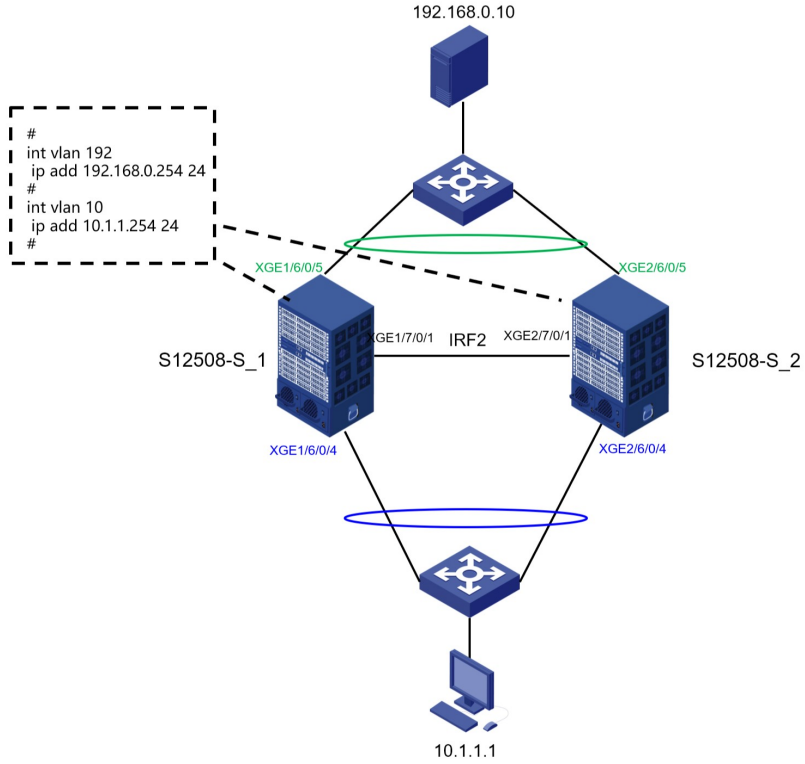
组网拓扑如下：



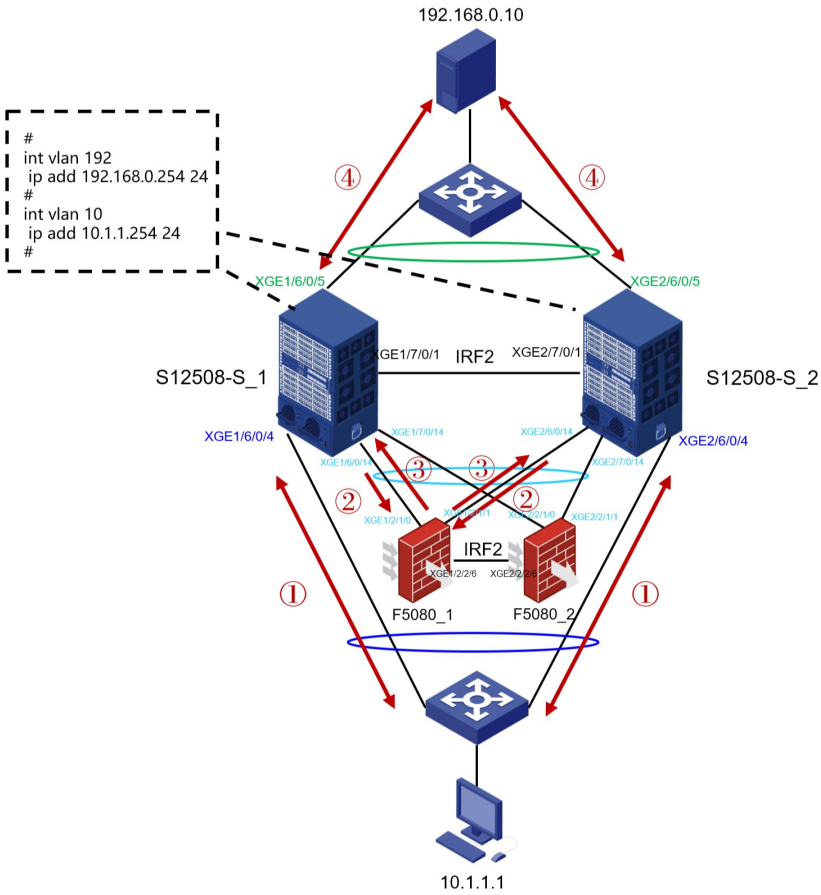
F5080-D防火墙采用Release 9608P13版本

问题描述

初始，F5080-D 防火墙没有部署在网络中，终端（10.1.1.1）和服务器（192.168.0.10）网关均在S12508-S交换机上（S12508-S交换机部署IRF2），如下图所示，终端与服务器经过S12508-S交换机三层转发均可互通：



后续，客户采购两台F5080-D防火墙部署IRF2，计划旁挂在S12508-S交换机上，实现终端（10.1.1.1）与服务器（192.168.0.10）互联流量经过F5080-D防火墙，具体设备互联及流量走向如下图所示：



终端（10.1.1.1）去往服务器（192.168.0.10）流量走向为：①-->②-->③-->④

服务器（192.168.0.10）去往终端（10.1.1.1）流量走向为：④ -->②-->③-->①

增加防火墙旁挂部署后，客户要求：

1、终端（10.1.1.1）和服务器（192.168.0.10）网关仍然保持在S12508-S交换机上；

2、F5080-D需要部署IRF2，且承担业务二层转发；

3、终端（10.1.1.1）和服务器（192.168.0.10）互访流量均需要经过F5080-D防火墙。

请问怎样合理部署，实现F5080-D防火墙部署要求?

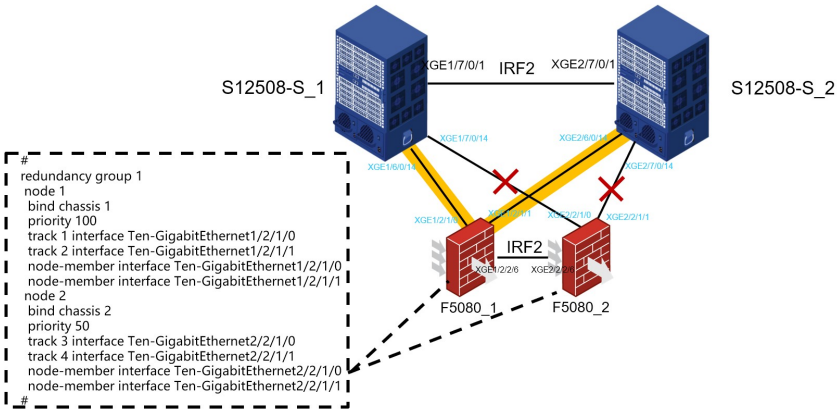
过程分析

为实现客户部署要求，需要注意如下事宜：

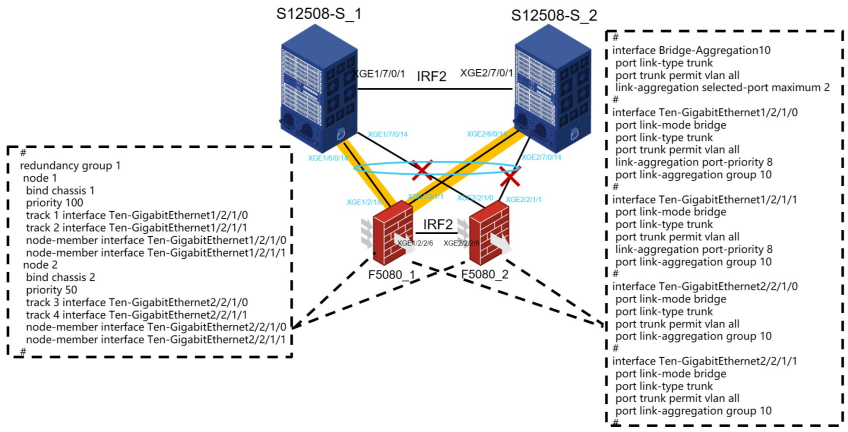
1、V5/V7平台交换机部署IRF2后，IRF-Port可承担业务流量转发；

2、F5080-D（目前新版本Release 9608P13）部署IRF2，旁路二层转发时，IRF-Port不能承担业务流量转发。

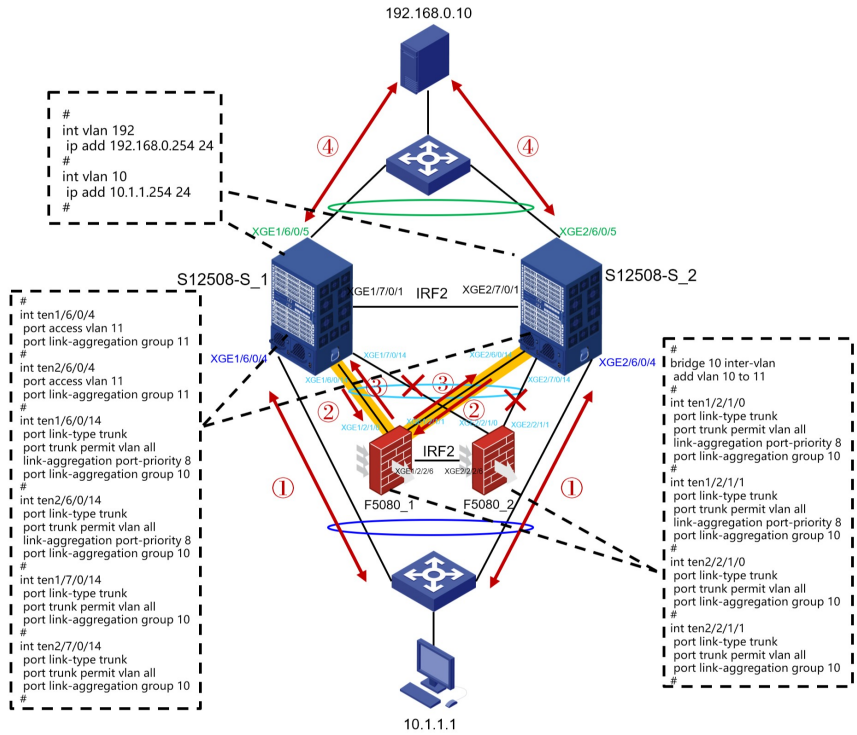
受FW IRF2限制，F5080-D IRF2 旁路二层部署时，需要在FW上创建冗余组。正常情况下，业务在 F5080_1 黄色链路中转发，F5080_2 链路不转发业务流量，如下图所示：



同时，未避免S12508-S交换机与F5080-D之间产生二层环路，需要将S12508-S交换机与F5080-D之间的 4 条链路进行聚合，且最大聚合成员接口数量为 2 （因为 F5080-D IRF2 正常情况下，仅两台链路承担业务转发），及如下图所示：



另外，为避免S12508-S 交换机与 F5080-D防火墙之间二层报文来回转发，造成S12508-S交换机 MAC地址表出现漂移的情况，需要在F5080-D设备二层转发



按照的转发路径：①-->②-->③-->④

- 链路 ① 时，数据报文不携带VLAN-ID；
- 进入报文进入S12508-S后，由于XGE1/6/0/4和XGE2/6/0/4的PVID=11，因此报文在交换机内部携带VLAN-ID=11的标记；
- 之后报文从交换机 XGE1/6/0/14 或 XGE2/6/0/14 二层透传发给防火墙，在链路 ② 时，数据报文携带VLAN-ID=11；
- 防火墙收到携带VLAN-ID=11 的报文后，根据防火墙部署的bridge 10 inter-vlan策略，将VLAN-ID从11替换为10，经过安全策略判断后，转发回交换机；
- 数据报文，在链路 ③ 时，携带转化后的VLAN-ID= 10，送达S12508-S交换机 interface vlan 10虚接口，三层转发处理，送达链路 ④ 。

解决方法

F5080-D防火墙关键配置如下：

```
#
failover group 1
 bind chassis 1 slot 2 primary
 bind chassis 2 slot 2 secondary
#
track 1 interface Ten-GigabitEthernet1/2/1/0 physical
#
track 2 interface Ten-GigabitEthernet1/2/1/1 physical
#
track 3 interface Ten-GigabitEthernet2/2/1/0 physical
#
track 4 interface Ten-GigabitEthernet2/2/1/1 physical
#
vlan 10 to 11
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/2/2/6
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/2/2/6
#
bridge 10 inter-vlan
 add vlan 10 to 11
#
interface Bridge-Aggregation10
 port link-type trunk
 port trunk permit vlan all
```

```
 link-aggregation selected-port maximum 2
#
interface Route-Aggregation 3
 mad bfd enable
 mad ip address 192.1.1.1 24 member 1
 mad ip address 192.1.1.2 24 member 2
#
interface GigabitEthernet1/2/4/0
 port link-mode route
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/2/1/0
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 link-aggregation port-priority 8
 port link-aggregation group 10
#
interface Ten-GigabitEthernet1/2/1/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 link-aggregation port-priority 8
 port link-aggregation group 10
#
interface Ten-GigabitEthernet2/2/1/0
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 10
#
interface Ten-GigabitEthernet2/2/1/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 10
#
security-zone name Trust
 import vlan 10 11
#
redundancy group 1
 node 1
  bind chassis 1
  priority 100
  track 1 interface Ten-GigabitEthernet1/2/1/0
  track 2 interface Ten-GigabitEthernet1/2/1/1
  node-member interface Ten-GigabitEthernet1/2/1/0
  node-member interface Ten-GigabitEthernet1/2/1/1
 node 2
  bind chassis 2
  priority 50
  track 3 interface Ten-GigabitEthernet2/2/1/0
  track 4 interface Ten-GigabitEthernet2/2/1/1
  node-member interface Ten-GigabitEthernet2/2/1/0
  node-member interface Ten-GigabitEthernet2/2/1/1
#
 session statistics enable
 session synchronization enable
 session synchronization dns http
#
security-policy ip
 rule 1 name Trust
  action pass
  counting enable
```

```
 source-zone Trust
 destination-zone Trust
rule 2 name Local
 action pass
 counting enable
 source-zone Local
 destination-zone Local
rule 3 name 3
 action pass
 counting enable
 source-zone Trust
 destination-zone Local
rule 4 name 4
 action pass
 counting enable
 source-zone Local
 destination-zone Trust
rule 17 name permit_any
 action pass
 counting enable
#
```

S12508-S交换机关键配置如下：

```
#
vlan 3
#
vlan 10
#
vlan 11
#
vlan 192
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/7/0/1 mode enhanced
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/7/0/1 mode enhanced
#
 stp global enable
#
interface Bridge-Aggregation10
 port link-type trunk
 port trunk permit vlan all
 stp disable
 link-aggregation selected-port maximum 2
#
interface Bridge-Aggregation11
 port access vlan 11
#
interface Bridge-Aggregation192
 port access vlan 192
#
interface Vlan-interface3
 mad bfd enable
 mad ip address 192.168.2.1 24 member 1
 mad ip address 192.168.2.2 24 member 2
#
interface Vlan-interface10
 ip address 10.1.1.254 255.255.255.0
#
interface Vlan-interface192
 ip address 192.168.0.254 255.255.255.0
#
interface Ten-GigabitEthernet1/6/0/2
```

```
 port link-mode bridge
 port access vlan 3
 stp disable
#
interface Ten-GigabitEthernet1/6/0/4
 port link-mode bridge
 port access vlan 11
 port link-aggregation group 11
#
interface Ten-GigabitEthernet1/6/0/5
 port link-mode bridge
 port access vlan 192
 port link-aggregation group 192
#
interface Ten-GigabitEthernet1/6/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 stp disable
 link-aggregation port-priority 8
 port link-aggregation group 10
#
interface Ten-GigabitEthernet1/7/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 stp disable
 port link-aggregation group 10
#
interface Ten-GigabitEthernet2/6/0/2
 port link-mode bridge
 port access vlan 3
 stp disable
#
interface Ten-GigabitEthernet2/6/0/4
 port link-mode bridge
 port access vlan 11
 port link-aggregation group 11
#
interface Ten-GigabitEthernet2/6/0/5
 port link-mode bridge
 port access vlan 192
 port link-aggregation group 192
#
interface Ten-GigabitEthernet2/6/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 stp disable
 link-aggregation port-priority 8
 port link-aggregation group 10
#
interface Ten-GigabitEthernet2/7/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 stp disable
 port link-aggregation group 10
#
```

具体详细配置信息请参考附件文档。

正常情况下，FW上冗余组和聚合接口状态如下：

```
[FW]display redundancy group
```

```
Redundancy group 1 (ID 1):
  Node ID      Chassis       Priority   Status        Track weight
  1            Chassis1      100        Primary       255
  2            Chassis2      50         Secondary     255

Preempt delay time remained     : 0    min
Preempt delay timer setting     : 1    min
Remaining hold-down time        : 0    sec
Hold-down timer setting         : 1    sec
Manual switchover request       : No

Member interfaces:

Node 1:
  Node member     Physical status
    XGE1/2/1/0    UP
    XGE1/2/1/1    UP
  Track info:
    Track    Status          Reduced weight     Interface
    1        Positive        255                XGE1/2/1/0
    2        Positive        255                XGE1/2/1/1
Node 2:
  Node member     Physical status
    XGE2/2/1/0    UP
    XGE2/2/1/1    UP
  Track info:
    Track    Status          Reduced weight     Interface
    3        Positive        255                XGE2/2/1/0
    4        Positive        255                XGE2/2/1/1

[FW]display link-agg verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Aggregation Mode: Static
Loadsharing Type: Shar
  Port            Status  Priority Oper-Key
--------------------------------------------------------------------------------
  XGE1/2/1/0      S       8        2
  XGE1/2/1/1      S       8        2
  XGE2/2/1/0      U       32768    2
  XGE2/2/1/1      U       32768    2
```

当链路② ③ 相关接口down掉后，流量将切换到备F5080-D_2上进行转发，其冗余组和聚合接口状态如下（当FW XGE1/2/1/0接口down后）：

```
[FW]dis redundancy group
Redundancy group 1 (ID 1):
  Node ID      Chassis       Priority   Status        Track weight
  1            Chassis1      100        Secondary     -255
  2            Chassis2      50         Primary       255

Preempt delay time remained     : 0    min
Preempt delay timer setting     : 1    min
Remaining hold-down time        : 0    sec
Hold-down timer setting         : 1    sec
Manual switchover request       : No

Member interfaces:

Node 1:
```

```
  Node member     Physical status
    XGE1/2/1/0    DOWN
    XGE1/2/1/1    DOWN(redundancy down)
  Track info:
    Track    Status           Reduced weight     Interface
    1        Negative(Faulty) 255                XGE1/2/1/0
    2        Negative         255                XGE1/2/1/1
Node 2:
  Node member     Physical status
    XGE2/2/1/0    UP
    XGE2/2/1/1    UP
  Track info:
    Track    Status           Reduced weight     Interface
    3        Positive         255                XGE2/2/1/0
    4        Positive         255                XGE2/2/1/1

[FW]display link-agg verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  XGE1/2/1/0       U       8        2
  XGE1/2/1/1       U       64       2
  XGE2/2/1/0       S       32768    2
  XGE2/2/1/1       S       32768    2
```

注意：请避免F5080-D与S12508-S交换机之间正常转发时的链路接口，频繁down/up.造成防火墙冗余组状态频繁切换，导致丢包。

附件下载： 配置信息.rar