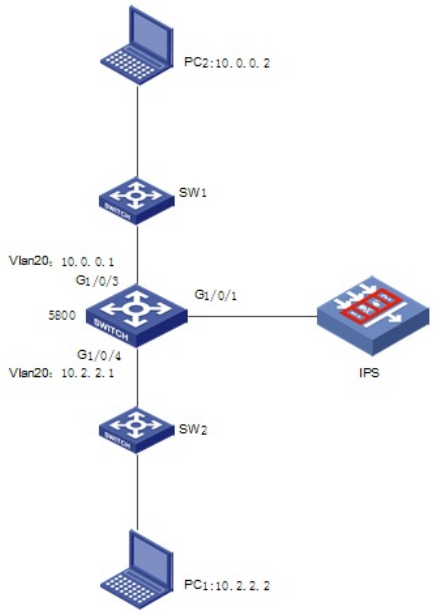
V5平台（iware）IPS旁路模式单区域典型配置

IPS防攻击 特征库 **郑标** 2019-12-30 发表

组网及说明

组网如下，IPS设备单个端口旁挂核心交换机：



配置步骤

一、核心交换机配置（图中S5800设备）：

1、端口镜像模式

//单区域模式只需要配置一个端口镜像组

```
 mirroring-group 1 local
#
vlan 1
#
vlan 10 to 20
#
interface NULL0
#
interface Vlan-interface10
 ip address 10.2.2.1 255.255.255.0
#
interface Vlan-interface20
 ip address 10.0.0.1 255.255.255.0
#
//将G1/0/3和G1/0/4的入方向数据镜像到G1/0/1
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-address mac-learning disable
mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/2
 port link-mode bridge
#
interface GigabitEthernet1/0/3
 port access vlan 20
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/4
 port access vlan 10
 mirroring-group 1 mirroring-port inbound
```

2、MQC镜像模式

acl number 3888

```
 rule 0 permit ip source 10.0.0.0 0.0.0.255 destination 10.2.2.0 0.0.0.255
acl number 3999
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.0.0.0 0.0.0.255
#
vlan 1
#
vlan 10 to 20
#
traffic classifier down operator and
 if-match acl 3888
traffic classifier up operator and
 if-match acl 3999
#
traffic behavior down
 mirror-to interface GigabitEthernet1/0/1
traffic behavior up
 mirror-to interface GigabitEthernet1/0/1
#
qos policy down
 classifier down behavior down
qos policy up
 classifier up behavior up
#
interface Vlan-interface10
 ip address 10.2.2.1 255.255.255.0
#
interface Vlan-interface20
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-address mac-learning disable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
#
interface GigabitEthernet1/0/3
 port access vlan 20
 qos apply policy down inbound
#
interface GigabitEthernet1/0/4
 port access vlan 10
 qos apply policy up inbound
```

二、单区域下IPS WEB 配置指导:

IPS配置可参照双区域IPS配置指导，参考知了案例 https://zhiliao.h3c.com/theme/details/9497

需要注意的是，尽管只用了一个物理链路，但是依然需要设置外部区域和内部区域，并划分一对业务端口。在段的方向选取时，若实际使用的是内部区域端口，方向为由里到外；若实际使用外部区域端口，方向为由外向里。

段的创建也要引用物理上的端口对，如图所示，你可能只使用eth0/2，但是另一个区域不能设空物理端口，否则策越引用此段是无效的，所以即使是单区域，也需要两个区域都关联物理端口对，不可有某一区域端口列表为空。

配置关键点

需要注意的是，尽管只用了一个物理链路，但是依然需要设置外部区域和内部区域，并划分一对业务端口。在段的方向选取时，若实际使用的是内部区域端口，方向为由里到外；若实际使用外部区域端口，方向为由外向里。

示例中使用了两种镜像方式：端口镜像方式和MQC流镜像方式，这两种方式选取一种单独使用即可。