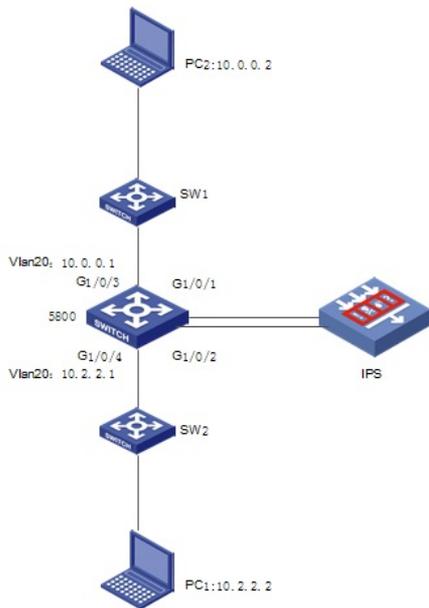


组网及说明

组网如下，IPS设备旁挂核心交换机：



配置步骤

一、核心交换机配置 (图中S5800设备) :

1.端口镜像模式

//双区域模式，这里要设定两个镜像组。

```

mirroring-group 1 local
mirroring-group 2 local
#
vlan 1
#
vlan 10 to 20
#
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
mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/2
port link-mode bridge
mac-address mac-learning disable
// 在S75E上，关闭设备全局、以太网接口或端口组的MAC地址学习功能用mac-address max-mac-count 0,S95E为mac-address mac-learning disable。具体视设备而定。这条命令防止镜像口mac学习造成环路。还可以保护设备的安全，可以有效地防止攻击者用大量不同MAC地址的帧攻击设备。
mirroring-group 2 monitor-port
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 20
mirroring-group 1 mirroring-port inbound //将G1/0/3入方向的数据镜像到G1/0/1
#
    
```

```
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 10
mirroring-group 2 mirroring-port inbound //将G1/0/4入方向的数据镜像到G1/0/2
#
```

2.MQC流镜像模式

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
```

```
#
```

```
//用访问控制列表匹配两个感兴趣流。
```

```
traffic classifier down operator and
```

```
if-match acl 3888
```

```
traffic classifier up operator and
```

```
if-match acl 3999
```

```
#
```

```
//设定对感兴趣流匹配数据的动作
```

```
traffic behavior down
```

```
mirror-to interface GigabitEthernet1/0/1
```

```
traffic behavior up
```

```
mirror-to interface GigabitEthernet1/0/2
```

```
#
```

```
//对感兴趣流实施动作
```

```
qos policy down
```

```
classifier down behavior down
```

```
qos policy up
```

```
classifier up behavior up
```

```
#
```

```
user-group system
```

```
#
```

```
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
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-mode bridge
```

```
mac-address mac-learning disable
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
port link-mode bridge
```

```
mac-address mac-learning disable
```

```
#
```

```
//在相应接口下发策略
```

```
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
```

```
#
```

```
//两种镜像方式对于上下行交换机的配置都是相同的。
```

二、双区域下IPS WEB配置指导:

1.在配置之前首先要将“工作模式”中的“连接模式”设置为旁路模式，在这种模式下，IPS收到数据包检测之后会丢弃，不会将收到的数据发送出去，直连模式则是将数据收到检测后再发出去，如果物理上是

旁路逻辑上是直连会造成环路。在设置的时候，旁路和“只上报日志”这种应用模式配合使用，直连和“完整功能集”配合使用。



2.划分区域。

在“网络管理”-“安全区域”里建立两个区域，并划分端口，分为内部区域和外部区域。图中分别命名为“in”和“out”。



如下图所示，在端口划分区域界面可设定vlan，可以只允许添加的vlan数据进入端口并接受，如果勾选方框可以设定vlan的范围。不设定vlan，默认是所有数据。



3.段设置。

在“网络管理”-“段配置”里设置段。在IPS里，应用策略对数据生效需要引用到段上。图中内部区域为“in”，外部区域为“out”，段为0。



4.新建策略。

“IPS”-“策略管理”-“新建策略应用”，策略名称自定，在下方选择需要检测的段和方向。不要忘记激活“段”。





策略规则可以自己修改，在规则管理里选择自定义的策略名，点查询即出现所有规则。

因为是旁路模式，可以设定“阻隔+记录日志”动作，选中所有在下方选择动作点击“修改动作”即可。若要使能规则，选中需要的规则点击“使能规则”。

可以选择“修改查询出的所有规则”和“修改本页选中规则”两种不同的修改范围，最后，切记要激活规则。

<input type="checkbox"/>	优先级	名称	分类	级别	默认	防护对象	规则类型	动作	状态	操作
<input type="checkbox"/>	15099200	phpBB search.php SQL注入漏洞	Vulnerability	警告	已激活	Web应用程序-PHP	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	15099891	Wu-Ftpd二进制格式化字符串堆栈溢出漏洞	Vulnerability	一般	已激活	FTP服务器-WU-FTPD	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	15099707	MS05-047 Microsoft Windows 远程调用漏洞 (PHP) LAMP/MPGR DLL esp/offset 缓冲区溢出	Vulnerability	一般	已激活	操作系统-Windows	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150997267	MS05-039 Microsoft Windows 远程调用漏洞 (PHP) 缓冲区溢出漏洞	Vulnerability	严重	已激活	操作系统-Windows	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150997291	MS05-044 Microsoft Management Console 区域标识漏洞	Vulnerability	一般	已激活	操作系统-Windows	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150997929	MS07-031 Windows Schannel 安全进程控制中解密过程执行异常漏洞	Vulnerability	一般	已激活	操作系统-Windows	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150997984	MS07-059 微软 IE 浏览器处理未初始化对象时发生崩溃漏洞	Vulnerability	一般	已激活	浏览器-Internet Explorer	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150997993	MS08-010 微软 IE HTML 呈现内存溢出漏洞	Vulnerability	一般	已激活	浏览器-Internet Explorer	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150997994	MS08-010 微软 IE 浏览器图像处理内存溢出漏洞	Vulnerability	一般	已激活	浏览器-Internet Explorer	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	150998012	MS08-055 Windows 新闻阅读器处理任意二进制数据缓冲区溢出漏洞	Vulnerability	一般	已激活	浏览器-Internet Explorer	预定义	阻隔+记录日志	使能	
<input type="checkbox"/>	42000000	Windows Libraries ER Design File LMI	Vulnerability	致命	已激活	操作系统-Windows	预定义	阻隔+记录日志	使能	

4.模拟对目标主机进行网页攻击，通过交换机将数据镜像到IPS进行探测，IPS检测到攻击，可以在“日志管理”-“攻击日志”里查看。

序号	攻击IP	时间	标题	攻击名称	段	方向	源IP	目的IP	源端口	目的端口	应用协议	级别	Packet Trace
1	151001888	2012-11-05 15:22:21	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	192.168.0.1	64237	161	snmp(UDP)	提示	
2	151001888	2012-11-05 15:22:14	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	10.165.20.104	59548	161	snmp(UDP)	提示	
3	151001888	2012-11-05 15:22:14	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	10.165.20.140	59548	161	snmp(UDP)	提示	
4	151001888	2012-11-05 15:21:55	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	10.165.138.79	64233	161	snmp(UDP)	提示	
5	151001888	2012-11-05 15:21:55	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	192.168.0.1	64234	161	snmp(UDP)	提示	
6	151001888	2012-11-05 15:21:55	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	10.165.138.79	64235	161	snmp(UDP)	提示	
7	151001888	2012-11-05 15:21:55	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	192.168.0.1	64236	161	snmp(UDP)	提示	
8	151001888	2012-11-05 15:21:51	SNMP 缺省口全探测	snmp(0.0.0.0:161)	0	从外到里	10.2.2.2	192.168.0.1	64232	161	snmp(UDP)	提示	

配置关键点

双区域模式是比较常见的一种旁路模式情况。IPS定义内部区域和外部区域，组成段，并将段引用到策略上。能够很好的区分来自不同方向流量的攻击。

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。