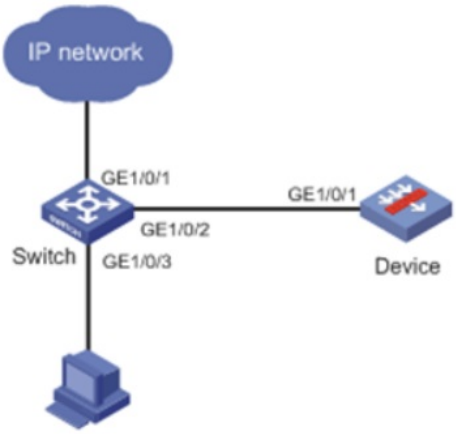
F1000-AK1242(V7)旁路部署场景下配置镜像后安全策略没有命中次数

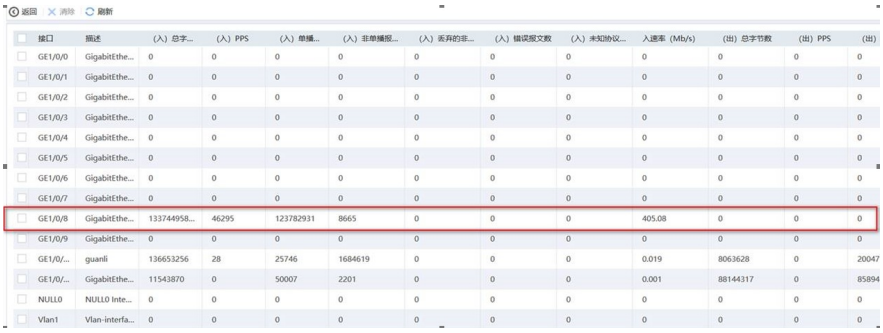
旁路部署 **邵亮** 2023-01-28 发表

组网及说明



问题描述

防火墙旁挂，将SW流量镜像至防火墙，防火墙监控从SW上来的流量，镜像目的接口能看到有流量记数，但是安全策略却无命中次数



接口	描述	（入）总字...	（入）PPS	（入）单播...	（入）非单播报...	（入）丢弃的非...	（入）错误报文数	（入）未知协议...	入速率（Mb/s）	（出）总字节数	（出）PPS	（出）
GE1/0/0	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/1	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/2	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/3	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/4	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/5	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/6	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/7	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/8	GigabitEthe...	133744958...	46295	123782931	8665	0	0	0	405.08	0	0	0
GE1/0/9	GigabitEthe...	0	0	0	0	0	0	0	0	0	0	0
GE1/0/...	guanli	136653256	28	25746	1684619	0	0	0	0.019	8063628	0	20047
GE1/0/...	GigabitEthe...	11543870	0	50007	2201	0	0	0	0.001	88144317	0	85894
NULL0	NULL0 Inte...	0	0	0	0	0	0	0	0	0	0	0
Vlan1	Vlan-interfa...	0	0	0	0	0	0	0	0	0	0	0

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	用户	动作	内容安全	命中次数	流量	统计	启用	编辑
12	Any	Any	IPv4	8		Any	Any	Any	Any	允许		0	0.008	☑	☑	

过程分析

旁路部署镜像需要配置inline黑洞，不然设备不转发流量，所以策略中没有命中次数

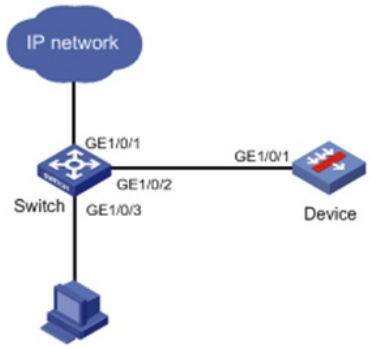
解决方法

配置Inline黑洞解决，配置方法如下

如图-1所示，Device旁挂在网络出口设备Switch上，Switch将流量镜像到Device上进行安全业务的处理，Device对报文的收发均为一个接口。现需配置Inline黑洞转发功能，使Device对收到的报文处理后直接丢弃，并对Switch上接收的流量进行入侵防御检测。

图-1 Inline黑洞转发配置组网图

图-1 Inline黑洞转发配置组网图



配置思路

Switch上需要配置的内容：镜像功能，将接收到的流量镜像到Device上进行安全业务的处理。

Device上需要配置的内容：

· 配置Inline黑洞转发功能。

· 配置安全业务（本举例中以入侵防御功能为例）。

配置步骤

配置Switch

1. 配置接口和Vlan

创建VLAN。

<Switch> system-view

[Switch] vlan 2

[Switch-vlan2] quit

配置接口GigabitEthernet1/0/1为二层转发口，并允许VLAN 2通过。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/3] port link-mode bridge

[Switch-GigabitEthernet1/0/3] port access vlan 2

[Switch-GigabitEthernet1/0/3] quit

配置与Device相连的GigabitEthernet1/0/2为二层接口，并允许VLAN 2通过。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/1] port link-mode bridge

[Switch-GigabitEthernet1/0/1] port access vlan 2

配置GigabitEthernet1/0/3为二层转发口，并允许VLAN 2通过。

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] port link-mode bridge

[Switch-GigabitEthernet1/0/3] port access vlan 2

[Switch-GigabitEthernet1/0/3] quit

2. 配置镜像组和源目的镜像口

配置本地镜像组1。

[Switch] mirroring-group 1 local

配置接口GigabitEthernet1/0/1为镜像组1的源端口，对收发的报文都进行镜像。

[Switch-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both

[Switch-GigabitEthernet1/0/1] quit

配置接口GabitEthernet1/0/2为镜像组1的监控端口。

[Switch-GigabitEthernet1/0/2] mirroring-group 1 monitor-port

[Switch-GigabitEthernet1/0/2] quit

配置Device

1. 创建VLAN

选择“网络 > 链路 > VLAN”，进入VLAN配置页面。

单击<新建>按钮，进入新建VLAN页面。配置VLAN列表为2。

2. 配置接口工作在二层模式并加入VLAN

选择“网络 > 接口 > 接口”，进入接口配置页面。

单击接口GE1/0/1右侧的<编辑>按钮，进入修改接口设置页面，配置如下。

- 工作模式：二层模式。
- 链路类型：Access。