IPS使用分析 培训

2019护网专项培训

NSFOCUS

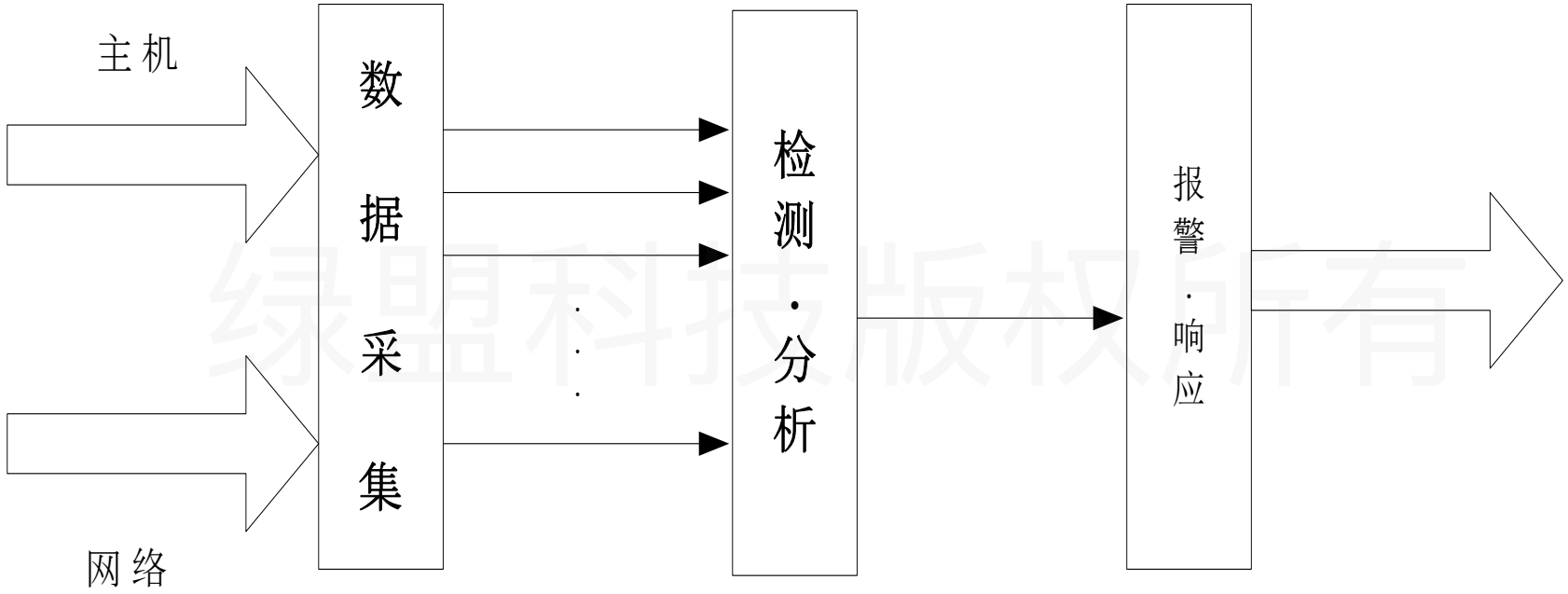
CONTENTS 目 录

- 01 工作原理
- 02 部署方式
- 03 策略配置及优化
- 04 日志分析

01

工作原理

入侵检测工作流程

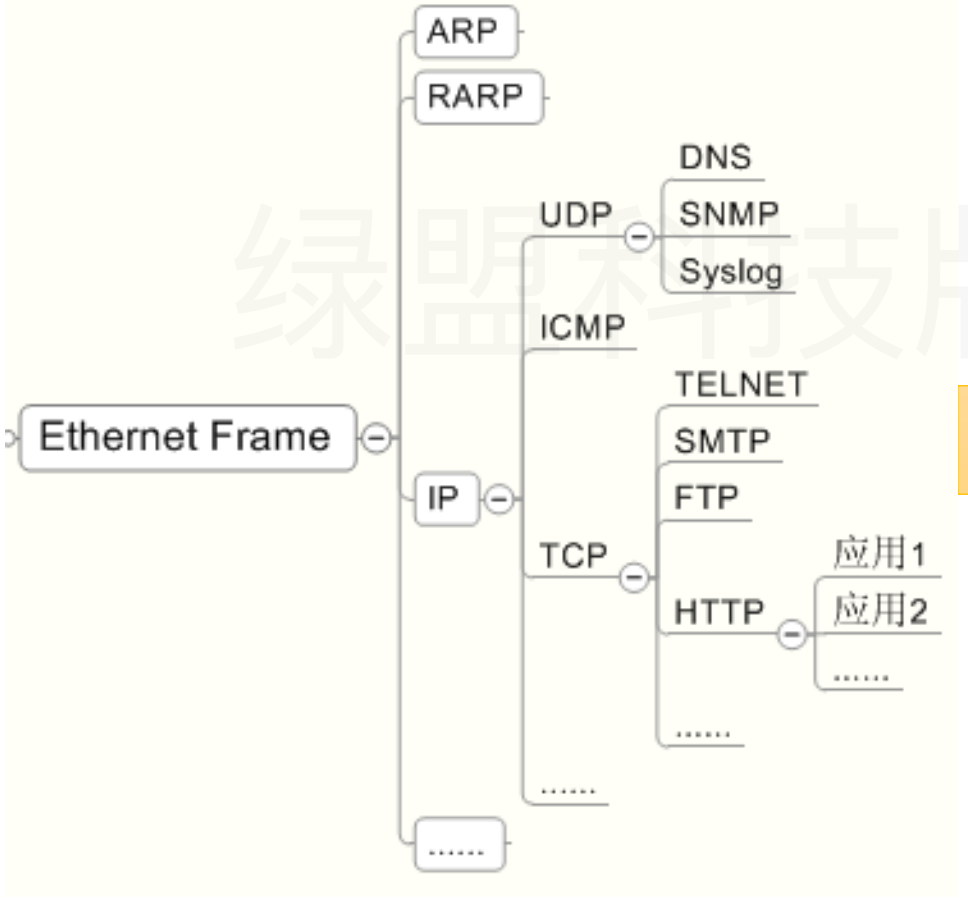


NIPS体系架构


入侵防护
抗D.o.S攻击
数据泄漏防护
高级威胁防御
信誉
URL过滤
防病毒
用户管理
应用管理
流量控制
系统规则
攻击特征库
URL分类
URL分类库
恶意网站
信誉库
安全响应模块
包丢弃
会话阻断
记录日志
报警显示
邮件报警
协议回放
互动接口
自定义命令
管理模块
账号管理
配置管理
策略管理
事件管理
日志管理
系统监控
安全引擎
（4-7层）
协议识别、分析、检测
数通引擎
（1-4层）
IP碎片重组
流汇聚
TCP状态跟踪
数据捕获
高性能多核硬件平台

检测引擎

协议分析



检测机制

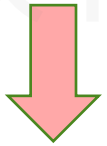
- 基于特征匹配
- 基于统计分析

匹配方式

基于特征

[50363]　Windows SMB协议用户认证失败

一段时间内达到XX次



基于统计（ddos、暴力猜测）

[20384]　Windows SMB暴力猜测用户口令

基于特征匹配举例

在http的get消息头部存在“%2F%2E%2E%2F”字段，相当于是“/../” 遍历到上一级目录，被判定为目录遍历漏洞。

```
> Frame 1: 1120 bytes on wire (8960 bits), 1120 bytes captured (8960 bits)
> Ethernet II, Src: HuaweiTe_e7:43:67 (20:f1:7c:e7:43:67), Dst: HuaweiTe_b7:37:67 (48:8e:ef:b7:37:67)
> Internet Protocol Version 4, Src: 192.168.15.234, Dst: 211.101.4.49
> Transmission Control Protocol, Src Port: 53395, Dst Port: 80, Seq: 1, Ack: 1, Len: 1066
v Hypertext Transfer Protocol
  > GET /ClinetBusiness/login2.asp?u=104003&url=%2Fclinet%5Feqa%2F%2E%2E%2Fclinetbusiness%2Fhospital%2Fmain%2Easp HTTP/1
    Host: nccl.clinet.com.cn\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://nccl.clinet.com.cn/ClinetBusiness/login2.asp?u=104003&url=%2Fclinet%5Feqa%2F%2E%2E%2Fclinetbusiness%
    Connection: keep-alive\r\n
  > [truncated]Cookie: td_cookie=2313136818; Hm_lvt_e452a20436d870d108ecce7b0f926160=1552357292,1552357451,1552379184,1
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://nccl.clinet.com.cn/ClinetBusiness/login2.asp?u=104003&url=%2Fclinet%5Feqa%2F%2E%2E%2Fcline
    [HTTP request 1/1]
```

基于统计匹配举例

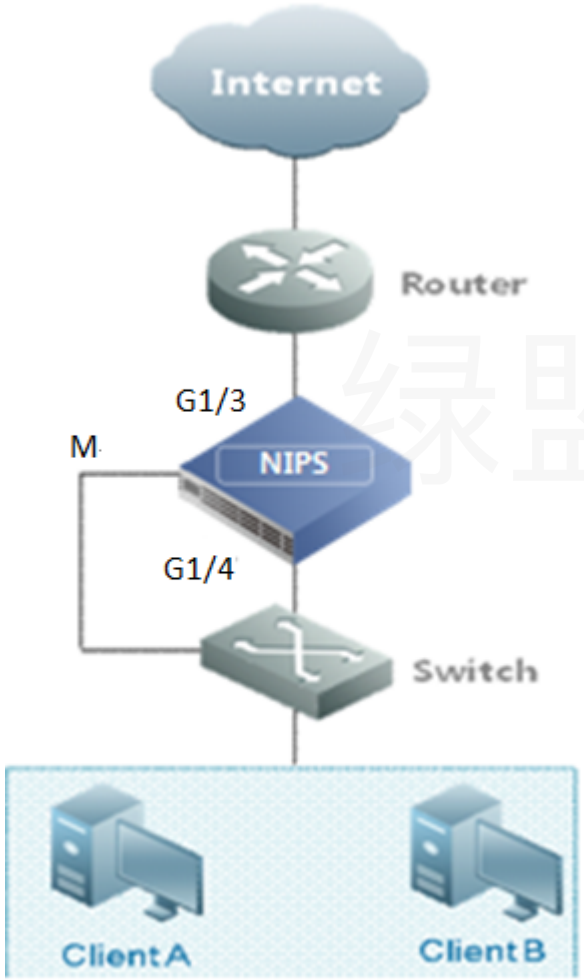
自动刷新 5 秒 手动刷新

状态	时间	事件	源	目的
	2019-04-25 14:45:32	[10115] UDP-Flood淹没拒绝服务攻击	66.225.32.219:12438	66.1.32.221:6468

02

部署方式

直通部署

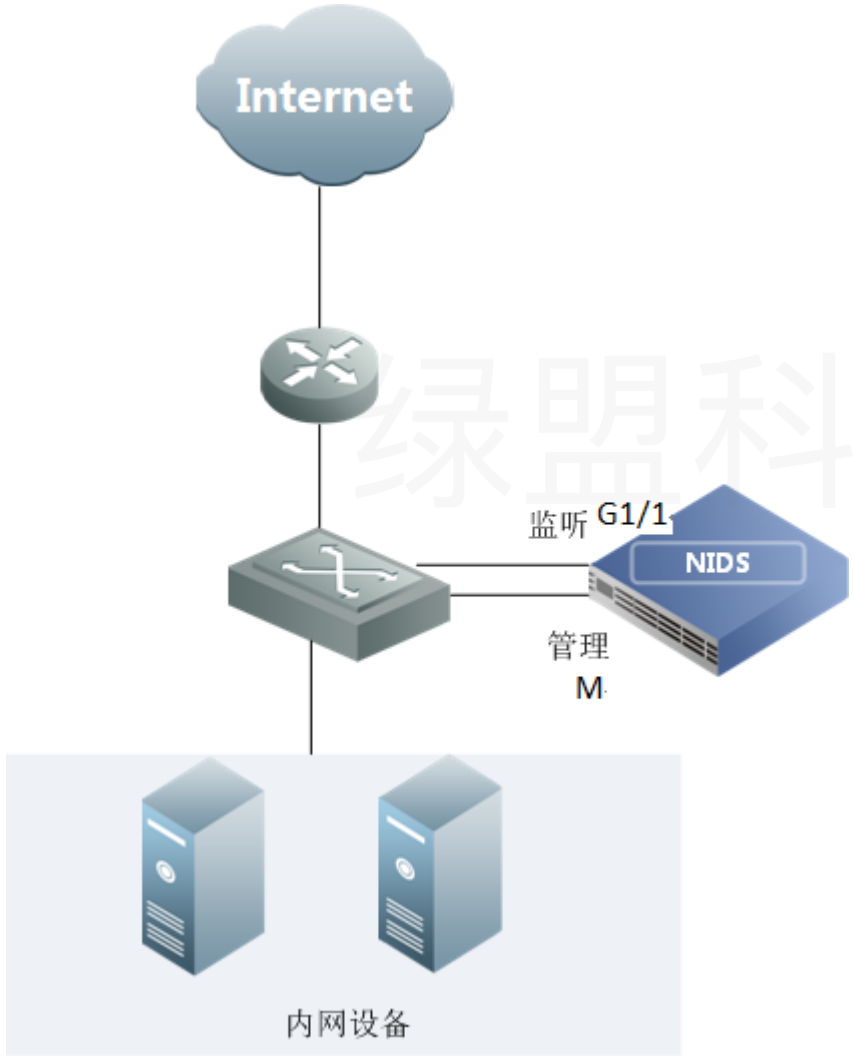


数据准备：
带外管理口地址和网关地址

配置思路：

1. 安全区配置
2. 虚拟线配置
3. 应用配置，使配置生效

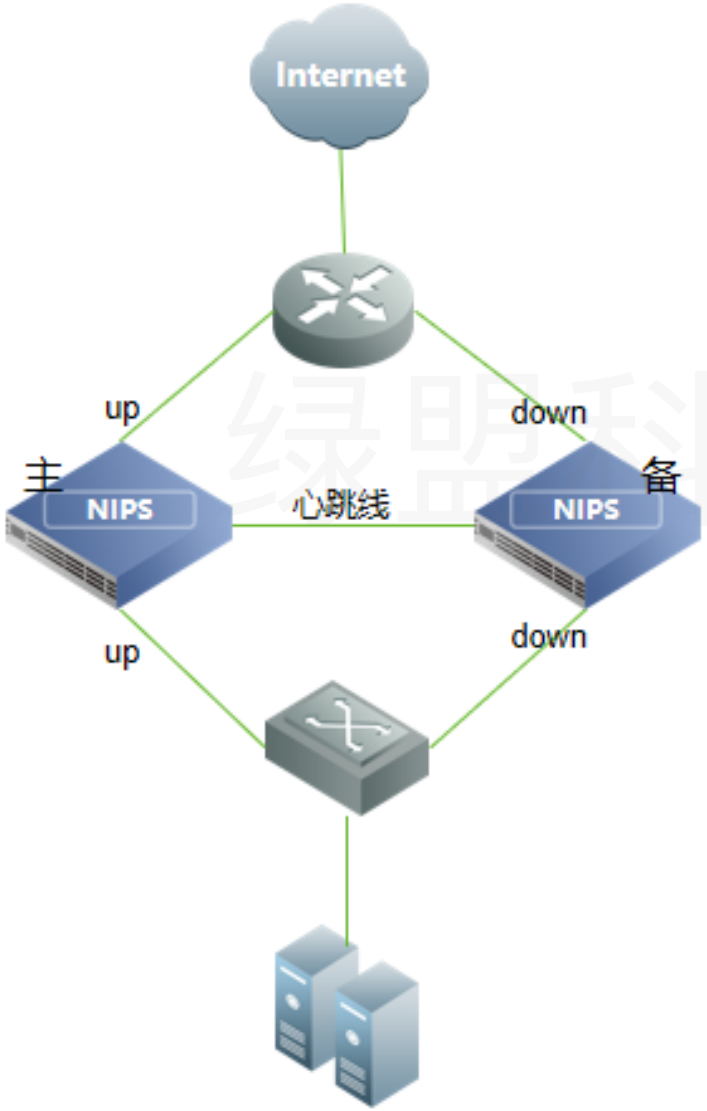
旁路部署



数据准备：
带外管理口地址和网关地址

配置思路：
1. 安全区配置
2. 接口配置
3. 应用配置，使配置生效

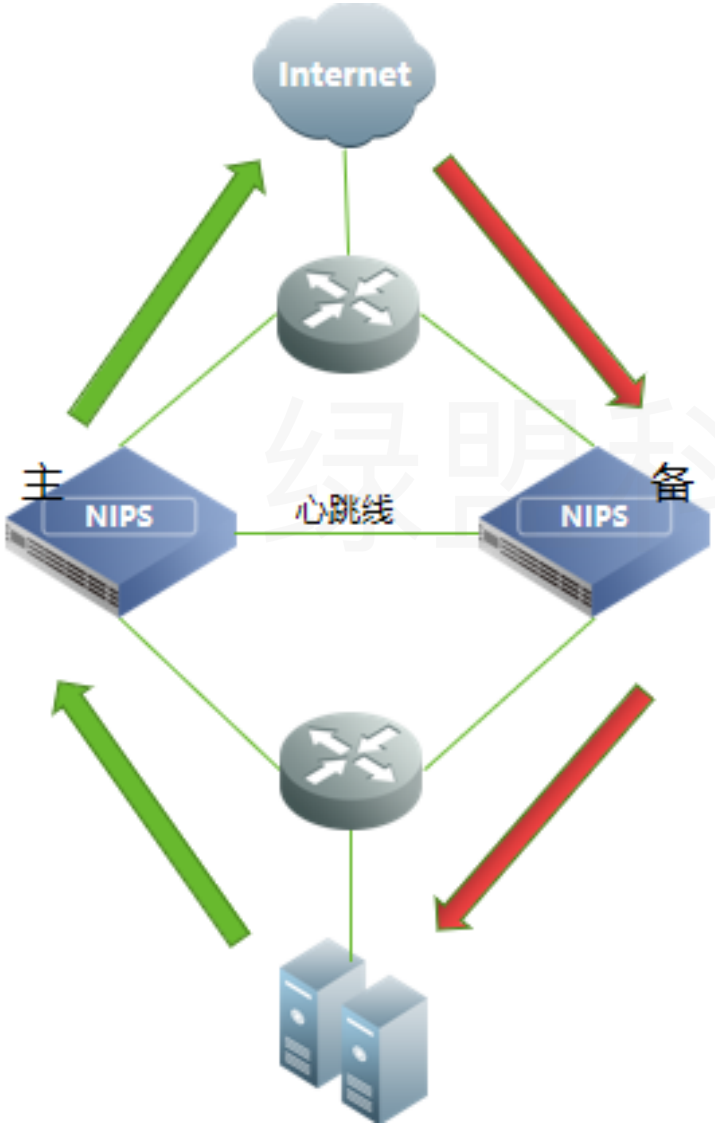
双机部署-虚拟线



数据准备：
带外管理口地址和网关地址

配置思路：
1. 安全区配置
2. 虚拟线及HA配置
3. 应用配置，使配置生效

双机部署-非对称路由



数据准备：
带外管理口地址和网关地址

配置思路：

1. 安全区配置
2. 虚拟线及HA配置
3. 应用配置，使配置生效

03

安全策略

策略配置

- 根据虚拟线的安全区建立入侵防护策略，也可以建立全局策略匹配所有安全区。由于虚拟线不区分安全区流量往返方向，所以一组虚拟线划分在一个安全区即可。

- 如果一组虚拟线两个接口配置了不同的安全区，分别建立两个方向的策略对进出流量进行检测，其实都是双向检测。

G1/1	虚拟线	IPS_test	intranet
G1/2	虚拟线	IPS_test	extranet

Intranet/Extranet:共1条

编号	源地址对象	用户	目的地址对象	时间	规则模板
2	* any	any	* any	any	Default

Extranet/Intranet:共1条

编号	源地址对象	用户	目的地址对象	时间	规则模板
3	* any	any	* any	any	Default

策略配置

如果全局策略设置了具体的原和目的地址，那么策略的安全区显示为“global/global” 如果原和目的地址对象有一个是any那么策略的安全区显示为“global\any”。这只是两种显示，并没有实际意义。

global/global:共1条

编号	源地址对象	用户	目的地址对象	时间	规则模板
1	10.0.0.0-10.255...	any	172.16.0.0-172....	any	Default

global/any:共1条

编号	源地址对象	用户	目的地址对象	时间	规则模板
7	* any	any	* any	any	Default

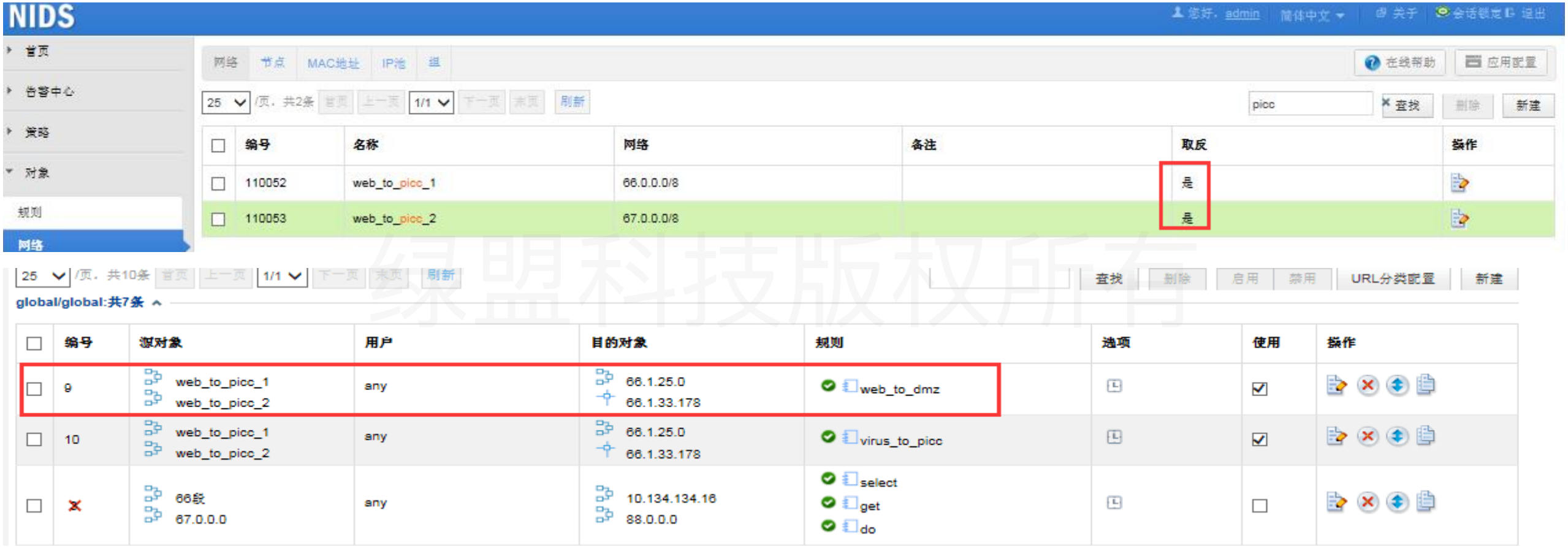
策略匹配

- 数据流进来，先匹配自身经过的安全区和策略的安全区，如果命中再匹配策略的原和目的地址，进而再匹配规则。

- 数据流会按照策略的优先级依次进行匹配，并且遍历完所有策略，遍历完之后如果所有命中执行动作为放行那么数据包会放行，如果有一个命中执行动作为阻断，数据包就会被阻断。

策略匹配-取反

客户的需求能实现吗？

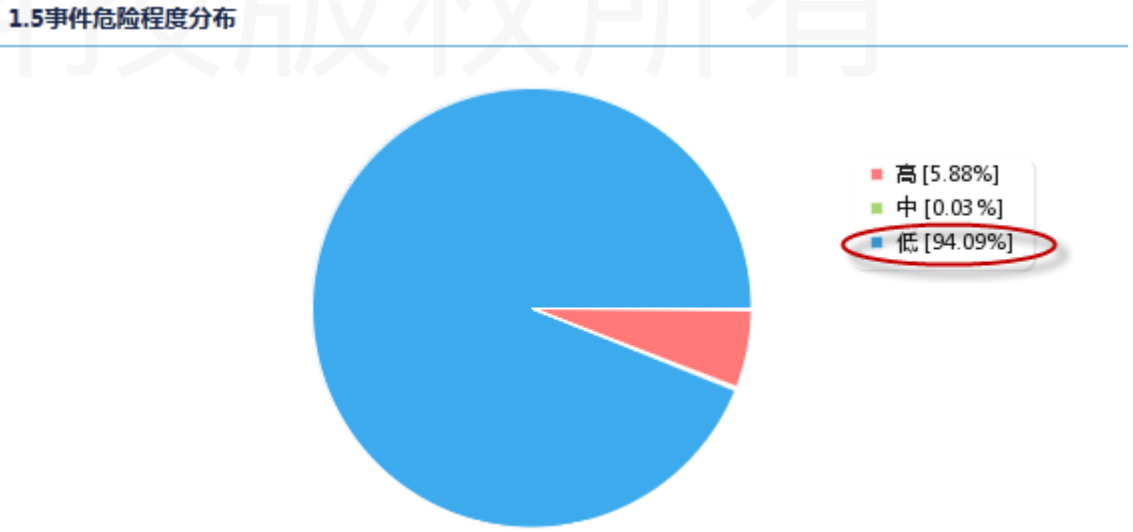


建立组对象，然后在对象组里面统一取反

策略优化-why?

- 大量的低风险事件、不关注事件、误报事件掩盖了真正的攻击事件。
- 日志分析时，用户无法从大量的告警信息中，找出真正的攻击事件，处理低风险事件浪费大量时间

排名	事件
1	HTTP协议CONNECT遂道功能连接访问
2	FTP服务普通用户认证
3	FTP服务用户弱口令认证
4	Windows SMB协议用户认证失败
5	Windows 2000 SMB建立连接
6	HTTP协议多线程文件下载
7	Windows Server服务RPC请求缓冲区溢出攻击(MS08-067)
8	Conficker 蠕虫攻击(TCP)
9	Windows XP SMB建立连接
10	通过HTTP协议下载可执行文件



策略优化-what

- ✓ 去掉（改进）误报事件
- ✓ IDS/IPS策略逐步完善

- ✓ 客户检测需求分析
- ✓ 现有事件分析

- ✓ 试运行一段时间，再进行事件分析，找出无关事件、误报事件

- ✓ 调整策略，去掉不关注事件

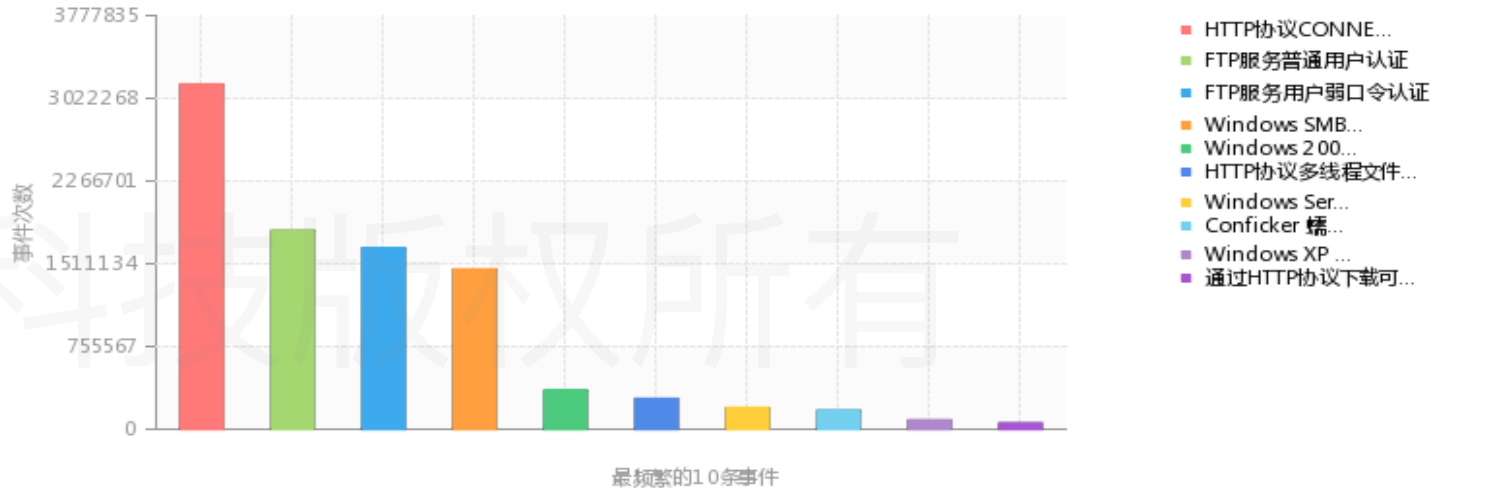
策略优化-how

找出不关注的安全事件

统计报表中，生成一段时间的报表，查看其中事件TOP10。

注意：策略中不关注事件，需要和用户沟通，确认哪些事件是不需要的。

2.1最频繁的10条事件



排名	事件	事件次数
1	HTTP协议CONNECT遂道功能连接访问	3148192
2	FTP服务普通用户认证	1814869
3	FTP服务用户弱口令认证	1654594
4	Windows SMB协议用户认证失败	1461313
5	Windows 2000 SMB建立连接	353715
6	HTTP协议多线程文件下载	278622
7	Windows Server服务RPC请求缓冲区溢出攻击(MS08-067)	195213
8	Conficker 蠕虫攻击(TCP)	172305
9	Windows XP SMB建立连接	84534
10	通过HTTP协议下载可执行文件	55445

这些事件基本不用关注

策略优化-how

屏蔽不关注事件

创建用户模板或派生模板：

- ✓ 将该事件在规则模版中设置为不告警
- ✓ 将该事件添加为例外规则

04

日志分析

日志分类

- ✓ 入侵防护、信誉
- ✓ 数据防泄漏
- ✓ 防病毒

- ✓ 设备登录记录
- ✓ 设备操作记录

- ✓ URL分类
- ✓ 应用管理

- ✓ 认证日志
- ✓ 硬件日志
- ✓ 运行日志

日志归并

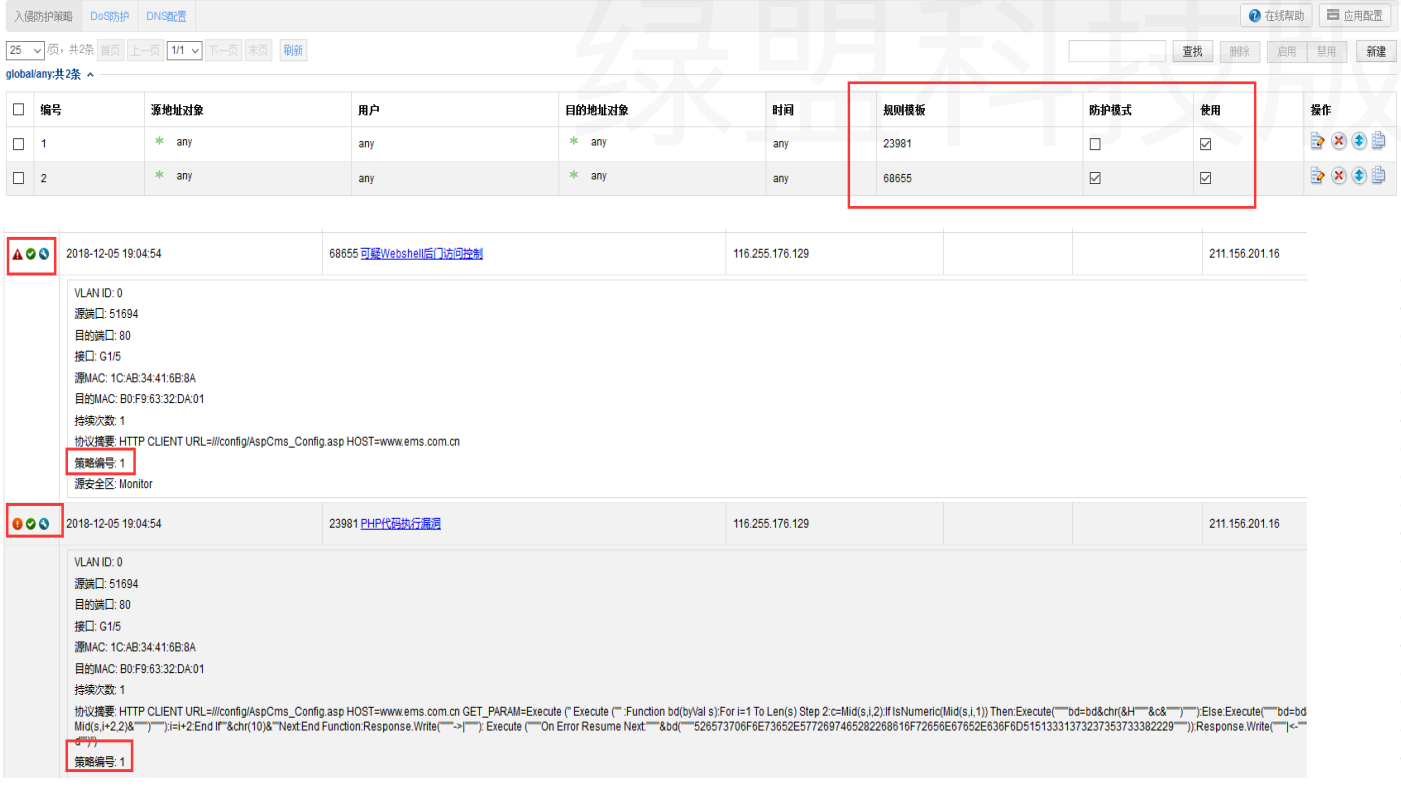
对一段时间内（缺省60分钟），同一源、目的IP地址、同一源、目的端口，同一事件的告警进行缓存，第一条正常告警，其后的告警进行缓存，只累计次数，60分钟后触发再告警。在这条告警中会显示期间发生的攻击事件次数。

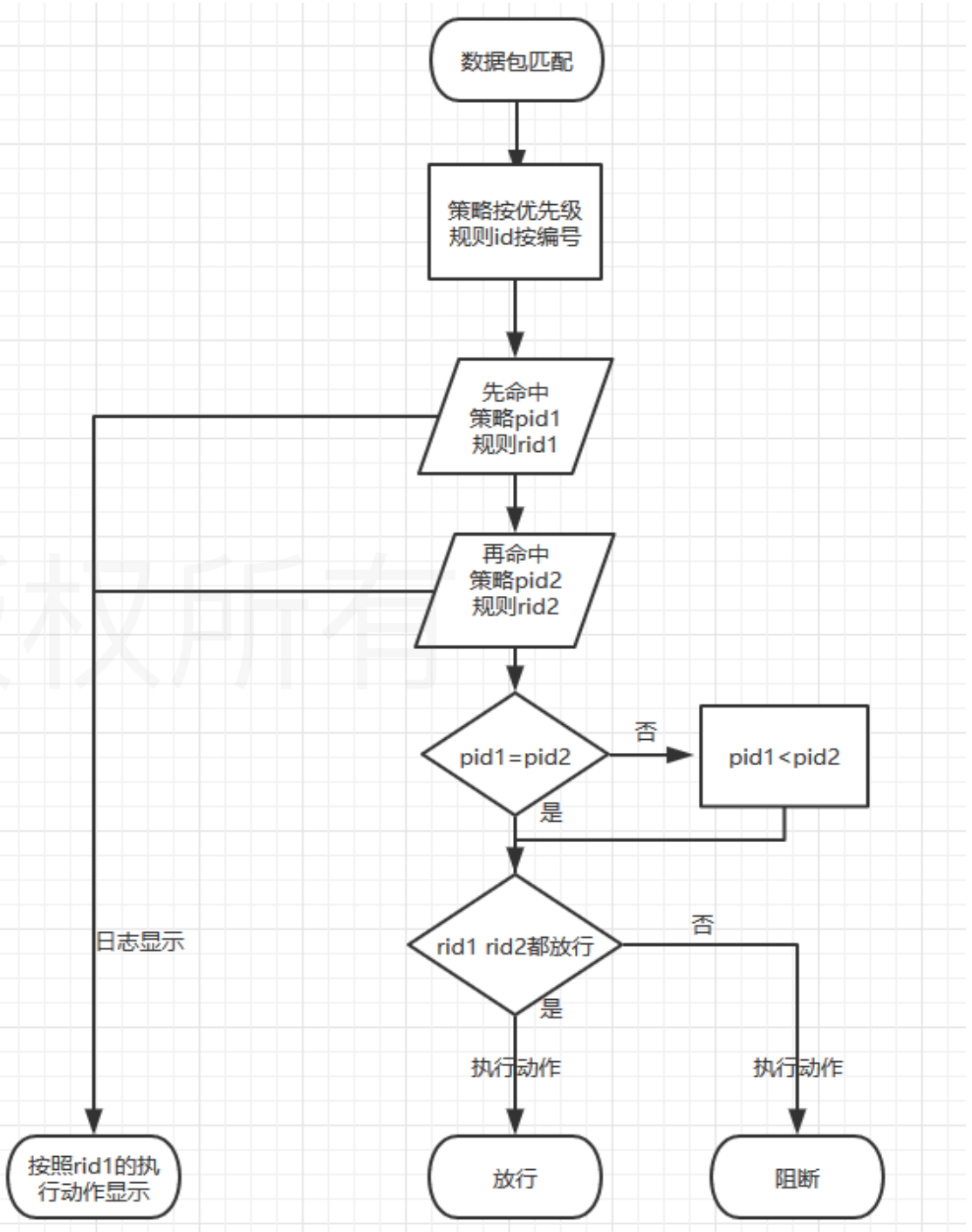
默认3600秒，0代表不归并。除非客户有特殊需求，否则不建议更改

入侵防护日志

入侵防护日志--一个包命中两条规则

现象汇总：
1 勾选了阻断，日志显示允许
2 勾选了允许，日志显示为阻断





入侵防护日志--添加例外依然有日志

用户反馈IPS针对某一规则添加了例外，但该规则依然告警
原因：开了ddos防护

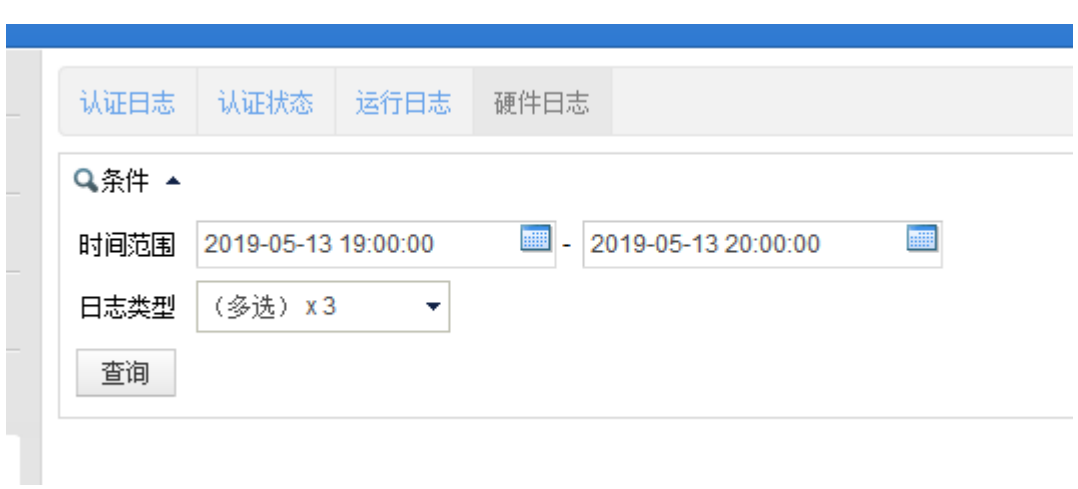
自动刷新 5 秒 手动刷新

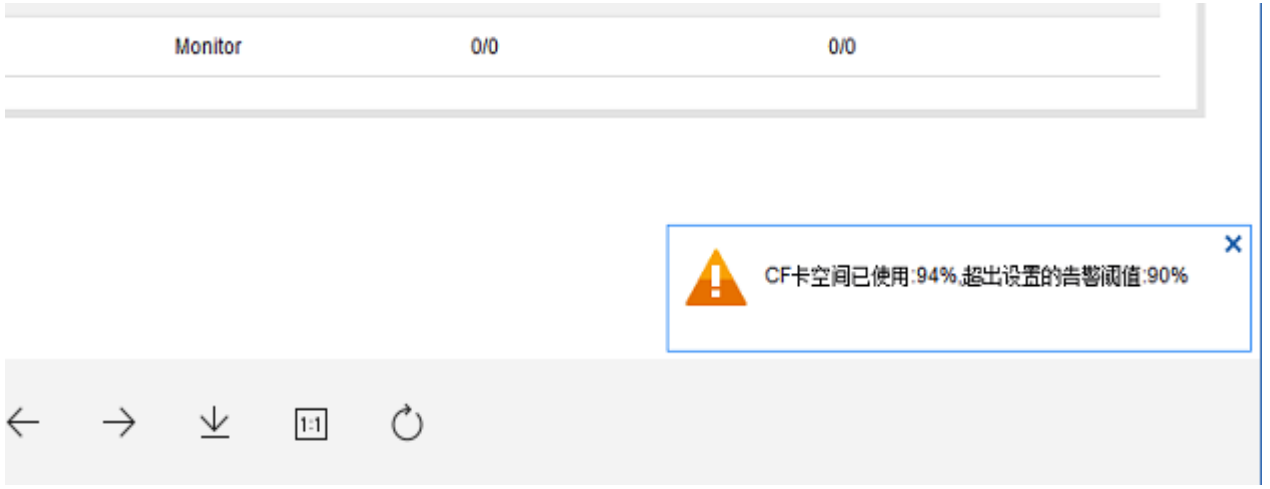
状态	时间	事件	源	目的
	2019-04-25 14:45:32	[10115] UDP-Flood淹没拒绝服务攻击	66.225.32.219:12438	66.1.32.221:6468

运维日志--硬件

运维日志--硬件件

2019-05-05 16:01:58	主板温度日志	主板温度为47.0,超过阀值
2019-05-05 16:00:08	主板温度日志	主板温度为48.0,超过阀值
2019-05-05 15:58:15	主板温度日志	主板温度为49.0,超过阀值
2019-05-05 15:56:24	主板温度日志	主板温度为51.0,超过阀值
2019-05-05 15:54:34	主板温度日志	主板温度为51.0,超过阀值
2019-05-05 15:52:43	主板温度日志	主板温度为52.0,超过阀值





运行日志--开机

	高可用性日志	2019-05-06 10:18:47	运行日志	3	server_0 register successful.
	高可用性日志	2019-05-06 10:18:47	运行日志	2	Bypass initialization is complete.
	bypass日志	2019-05-06 10:18:45	警告日志		Set 0-0 poweron bypass state to nobypass
	bypass日志	2019-05-06 10:18:42	警告日志	1	Set 0-0 poweroff bypass state to nobypass
	bypass日志	2019-05-06 10:18:40	警告日志		Set 0-0 runtime bypass state to nobypass
	bypass日志	2019-05-06 10:18:39	警告日志		Set portwell 8ge_b gloable switch disable status

1 设备的bypass交由软件接管，变成非bypass状态

2 bypass初始化成功

3 设备引擎加载成功

运行日志--内存和CPU

⚠	系统日志	2019-05-07 06:28:10	警告日志	warning: cpu usage is higher than 90 percent
!	接口状态	2019-05-07 05:02:12	警告日志	G2/2 Link Status:UP S:10Mb/s D:Full--> UP S:1000Mb/s D:Full
!	接口状态	2019-05-07 05:02:10	警告日志	G2/2 Link Status:UP S:1000Mb/s D:Full--> UP S:10Mb/s D:Full

⚠	系统日志	2019-05-13 10:31:48	警告日志	warning!!! free memory is lower than 20 percent
⚠	系统日志	2019-05-13 10:31:44	警告日志	warning!!! free memory is lower than 20 percent

内存和CPU异常告警，大量资源被占用，请及时联系工程师

运行日志--bypass

2019-05-10 01:34:03	bypass	1	3	Set 0-0 runtime bypass state to nobypass
2019-05-10 01:34:02	bypass	1	3	Start bypass wdt, timeout: 30.
2019-05-10 01:34:00	bypass	1	3	Set 0-0 poweron bypass state to bypass
2019-05-10 01:33:59	bypass	1	3	Set 0-0 poweroff bypass state to bypass
2019-05-10 01:33:57	bypass	1	3	Set 0-0 wdt-timeout bypass state to bypass
2019-05-10 01:33:55	bypass	1	3	Set portwell 8ge_b gloable switch enable status
2019-05-09 13:32:06	interface	1	2	Logic G1/1 link changed: curLink yes; curDuplex 1; curSp...
2019-05-09 10:23:03	interface	1	2	G1/1 Link Status:DOWN S:Unknown! D:Unknown!--> UP ..
2019-05-09 10:23:01	interface	1	3	RX or TX errors appear in NIC G1/1 and maybe negotiatio..
2019-05-09 10:23:01	interface	1	2	PHY G1/1 changed to up: Duplex 1; Speed 1000
2019-05-09 10:23:01	interface	1	2	Logic G1/1 link changed: curLink yes; curDuplex 1; curSp...
2019-05-09 10:22:59	interface	1	2	Logic G1/1 link changed: curLink no; curDuplex -1; curSpe..
2019-05-09 10:22:58	interface	1	2	Logic G1/1 link changed: curLink yes; curDuplex 1; curSp...
2019-05-09 10:22:57	bypass	1	3	Set 0-0 runtime bypass state to nobypass
2019-05-09 10:22:57	interface	1	2	PHY G1/1 changed to down: Duplex -1; Speed -1
2019-05-09 10:22:56	interface	1	2	G1/1 Link Status:UP S:1000Mb/s D:Full--> DOWN S:Unkn..
2019-05-09 10:22:55	bypass	1	3	Start bypass wdt, timeout: 30.

看门狗超时，自动进入bypass

运行日志--接口

收发错误

接口状态	2019-05-07 17:04:03	警告日志	RX or TX errors appear in NIC G1/3 and maybe negotiation abnormal
接口状态	2019-05-07 17:02:59	警告日志	RX or TX errors appear in NIC G1/3 and maybe negotiation abnormal
接口状态	2019-05-07 17:01:55	警告日志	RX or TX errors appear in NIC G1/3 and maybe negotiation abnormal
接口状态	2019-05-07 17:00:51	警告日志	RX or TX errors appear in NIC G1/3 and maybe negotiation abnormal

接口状态	2019-05-09 17:40:32	警告日志	G1/6 Link Status:DOWN S:Unknown! D:Unknown!--> UP S:1000Mb/s D:Full
接口状态	2019-05-09 17:40:32	警告日志	G1/5 Link Status:DOWN S:Unknown! D:Unknown!--> UP S:1000Mb/s D:Full
接口状态	2019-05-09 17:40:32	警告日志	G1/4 Link Status:DOWN S:Unknown! D:Unknown!--> UP S:1000Mb/s D:Full
接口状态	2019-05-09 17:40:31	警告日志	G1/3 Link Status:DOWN S:Unknown! D:Unknown!--> UP S:1000Mb/s D:Full
接口状态	2019-05-09 17:40:31	警告日志	G1/2 Link Status:DOWN S:Unknown! D:Unknown!--> UP S:1000Mb/s D:Full
接口状态	2019-05-09 17:40:31	警告日志	G1/1 Link Status:DOWN S:Unknown! D:Unknown!--> UP S:1000Mb/s D:Full
接口状态	2019-05-09 17:40:30	警告日志	G1/5 Link Status:UP S:1000Mb/s D:Unknown!--> DOWN S:Unknown! D:Unknown!
接口状态	2019-05-09 17:40:29	警告日志	G1/4 Link Status:UP S:1000Mb/s D:Full--> DOWN S:Unknown! D:Unknown!
接口状态	2019-05-09 17:40:28	警告日志	G1/3 Link Status:UP S:1000Mb/s D:Full--> DOWN S:Unknown! D:Unknown!

接口闪断

谢谢！

NSFOCUS