H3C SecPath Web 应用防火墙告警手册

目 录

1 告警简介

当设备发生故障或某些原因导致系统发生不正常的工作状态时，系统能够根据不同类型的故障及不同功能出现的故障进行分析，系统分析后将告警信息保存在设备的告警数据库中，并提供前端展示日志信息供用户查看。若配置了网管系统，则该告警信息会通过 Syslog 日志向网管系统发送，或网管系统通过 SNMP（Simple Network Management Protocol）协议进行获取。

若要查看告警信息，可以通过选择[事件/系统事件]进行查看。

按照告警的性质进行划分，告警信息分为以下三种:

- 故障告警：指由于硬件设备故障或某些重要功能异常而产生的告警。
- 恢复告警：指设备故障或异常功能恢复正常时产生的告警。
- 信息告警：指某功能模块产生的信息告警，如生成定时报表信息。

1.1 告警格式说明

1. 告警格式输出

告警信息输出格式如下：

[发生时间][等级][事件]

2. 告警字段说明

告警类型	说明
发生时间	告警事件发生时间，格式为“yyyy-mm-dd hh:mm:ss”。
等级	该告警对应事件对系统的影响程度，分警告和信息两种等级。
事件	告警发生的具体事件

1.2 告警类型说明

告警功能类别的说明如表 1 所示。

表1 告警类型说明

告警类型	说明
前端交互告警	Web前端交互告警，包括多次密码尝试、NTP时间同步、定时报表等。
设备资源监视告警	设备自身监控告警，包括CPU、内存、磁盘等状态监测。
攻击日志备份自动提醒	设备提供攻击日志自动备份功能，在数据备份后产生系统告警日志。
网络连接	指WAF设备开启端口状态检测后，当接口断开后会产生系统告警日志。
HA状态	启用HA后，WAF主备机进行协商模式，协商成功后主机工作在透明代理模式，备机工作在网桥直通状态。

1.3 告警信息说明

1. 告警解释

指该告警产生的详细说明。

2. 告警属性

指该告警的格式说明。

3. 对系统的影响

分析该告警可能产生的影响。

4. 可能的原因

用于描述产生该告警的各种原因。

5. 处理步骤

详细描述了针对告警产生的各种原因进行进一步诊断和修复的处理建议。

1.4 告警级别说明

等级（即告警级别）用于标识一条告警的严重程度，按严重程度递减分为两级：警告、信息，如所示。

表2 告警级别说明

等级	定义	说明
1	警告	该告警对应事件对系统的造成一定程度的影响。
2	信息	该告警对应事件对系统无影响。

2 前端交互告警

2.1 多次密码尝试告警

1. 告警解释

2013-05-23 13:10:01 警告 检测到 IP 192.168.12.41 以 admin 用户登录，累计出错次数超过 13 次
2013 年 5 月 23 日 13 时 10 分钟 1 秒，登录 IP 为 192.168.12.41 的用户 admin 多次登录失败。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	警告	详细事件信息，如检测到IP x.x.x.x 以 xxx 用户登录，累计出错次数超过 x 次。

3. 对系统的影响

攻击者尝试登录前端。

4. 可能原因

攻击者对前端管理页面尝试多次密码登录。

5. 处理步骤

多次密码尝试告警处理步骤如下。

(1) 登录 WAF 管理平台页面，点击[系统 / 系统设置]，用户根据实际情况设置“登录出错次数容限”次数和“登录出错锁定时间”值，WAF 默认设置分别为 5 次和 1 分钟。如图 1 所示。

图1 系统设置图

(2) 设置完成后，点击[保存]按钮。

(3) 验证设置是否有效。模拟攻击者对前端管理页面尝试 5 次密码错误登录，1 分钟内第 6 次输出正确的用户名和密码显示该 IP 和用户被锁定，无法登录。

(4) 查看右上角的未读消息如图 2 所示，查看多次密码尝试告警日志，如图 3 所示。

图2 未读消息

图3 多次密码尝试告警日志

(5) 用户可以根据告警日志确认是否为攻击行为，如为攻击行为，可将该 IP 禁止访问；如不是攻

击行为，如正常用户忘记密码等，WAF 会在一定时间后（图中为 1 分钟后）解锁该用户。

6. 告警清除

选择右上角的未读消息按钮，如 5. (4)图 2 所示。点击“以上已读”即可清除，如图 4 所示。

图4 点击[以上已读]按钮

2.2 NTP同步告警

1. 告警解释

2013-05-23 13:10:01　信息　NTP 时间同步成功，目标服务器 10.10.10.11

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 启用 NTP 时间动态同步成功。

2013-05-23 13:10:01　警告　NTP 时间同步出错，无法链接到目标服务器 10.10.10.11

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 启用 NTP 时间动态同步失败。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	NTP时间同步成功，目标服务器x.x.x.x 。
格式为 yyyy-mm-dd hh:mm:ss	警告	NTP时间同步出错，无法链接到目标服务器x.x.x.x。

3. 对系统的影响

设备系统时间的更新。

4. 可能原因

产生设备资源监视告警的可能原因如下。

- WAF 管理口网络异常。
- NTP 服务器网络异常。

5. 处理步骤

NTP 同步告警处理步骤如下。

(1)　检查 WAF 管理口与 NTP 服务器连接异常。

(2)　检查 NTP 同步服务器是否异常。

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

2.3 生成定时报表

1. 告警解释

2013-05-23 13:10:01　信息　生成定时报表

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 生成了定时报表。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	生成定时报表。

3. 对系统的影响

无。

4. 可能原因

WAF 设备启用了定时报表生成。

5. 处理步骤

无需处理。

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

3 设备资源监视告警

3.1 CPU、内存、磁盘状态告警

1. 告警解释

2013-05-23 13:10:01　告警　CPU 使用率超过 80%

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的 CPU 使用率超过 80%。

2013-05-23 13:10:01　告警　内存使用率超过 80%

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的内存使用率超过 80%。

2013-05-23 13:10:01　告警　磁盘使用率超过 80%

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的磁盘使用率超过 80%。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	警告	CPU使用率超过80%。
格式为 yyyy-mm-dd hh:mm:ss	警告	内存使用率超过80% 。
格式为 yyyy-mm-dd hh:mm:ss	警告	磁盘使用率超过80% 。

3. 对系统的影响

系统响应变慢。

4. 可能原因

产生设备资源监视告警的可能原因如下。

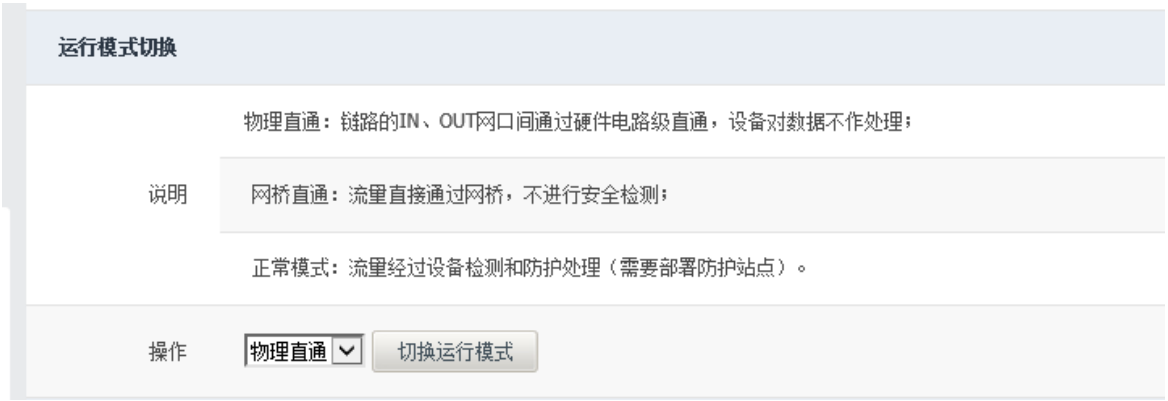
- 设备自身被攻击。
- 被防护对象遭受攻击或突发流量很大，设备长时间处于资源使用过高的状态。

5. 处理步骤

设备资源监视告警处理步骤如下。

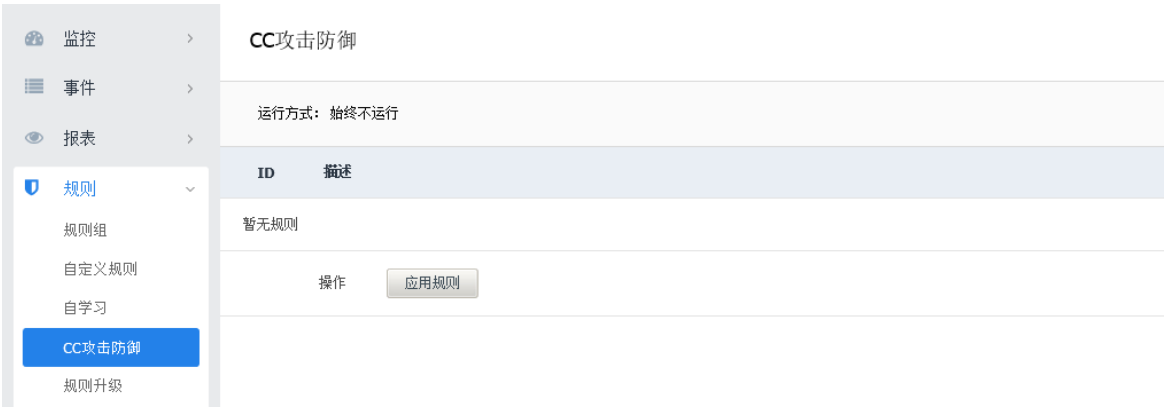
(1) 设备自身被攻击，WAF 的 CPU 或内存过高时，登录 WAF Web 管理平台，选择[系统/系统维护/运行模式切换]，将 WAF 运行模式手工切换到物理直通模式。如 3.1 5. (1)图 5 所示。

图5 运行模式切换



(2) 分析是什么类型攻击，如应用层 DDOS/CC 攻击，则建议 WAF 开启应用层 DDOS/CC 防护模块。选择[规则/CC 攻击防御]”，创建防护 CC 的规则，如所示。然后选择右上角的应用更改进入应用更改页面，点击[应用更改]进行生效。

图6 CC 防护模块



(3) 选择“[配置/资源监控/设备自身监控]启用”，将检测到异常后的动作改为“告警并物理直通”，如所示。然后点击<保存>，选择右上角的应用更改进入应用更改页面，点击[应用更改]进行生效。

图7 设备资源监控—告警并物理直通

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

3.2 自动切换模式

1. 告警解释

2013-05-23 13:10:01 告警 [设备自身监控] 切换到网桥直通模式

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的设备自身监控设置为网桥直通模式。即，当 CPU、内存、磁盘资源使用出现异常后，WAF 将进行告警并网桥直通动作。

2013-05-23 13:10:01 告警 [设备自身监控] 切换到物理直通模式

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的设备自身监控设置为物理直通模式。即，当 CPU、内存、磁盘资源使用出现异常后，WAF 将进行告警并物理直通动作。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	警告	[设备自身监控] 切换到网桥直通模式。
格式为 yyyy-mm-dd hh:mm:ss	警告	[设备自身监控] 切换到物理直通模式。

3. 对系统的影响

自动切换模式告警对系统影响如下。

- 系统响应变慢。

- 设备长时间在资源使用过高的状态会自动切为 bypass 状态，站点失去防护。

4. 可能原因

自动切换模式告警的可能原因如下。

- 设备自身被攻击。
- 被防护对象遭受攻击或突发流量很大，设备长时间处于资源使用过高的状态。

5. 处理步骤

自动切换模式告警处理步骤如下。

(1) 设备自身被攻击，WAF 的 CPU 或内存过高时，设备将自动切换到物理直通/网桥直通模式。操作步骤同 3.1 设备资源监视一样。

(2) 分析是什么类型攻击，如应用层 DDOS/CC 攻击，则建议 WAF 开启应用层 DDOS/CC 防护模块。操作步骤同 3.1 设备资源监视一样。

(3) 如突发流量很大时，设备自动切为 bypass。待流量恢复正常值则重新切换工作模式，通过[系统 / 系统维]将运行模式切换为透明代理模式。

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

4 攻击日志自动备份提醒

4.1 攻击日志自动备份

1. 告警解释

2013-05-23 13:10:01　信息　告警日志自动备份

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 告警日志进行了自动备份。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	告警日志自动备份。

3. 对系统的影响

自动备份后会清理已备份的攻击日志，这样已备份的攻击日志无法通过[事件/应用防护]进行查看。

4. 可能原因

设备默认开启攻击日志自动备份功能。

5. 处理步骤

无需处理

6. 告警清除

选择右上角的未读消息按钮，如 2.1　5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1　6. 图 4 所示。

4.2 攻击日志自动备份清理

1. 告警解释

2013-05-23 13:10:01　信息　告警日志自动备份清理

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 将自动备份的告警日志进行了清理。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	告警日志自动备份清理。

3. 对系统的影响

攻击日志自动备份清理告警对系统影响如下。

- 释放磁盘空间。
- 自动备份后会清理已备份的攻击日志，这样已备份的攻击日志无法通过“日志 > 攻击日志”进行查看。

4. 可能原因

设备默认开启攻击日志自动备份清理功能。

5. 处理步骤

无需处理

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

4.3 攻击日志自动备份下载

1. 告警解释

2013-05-23 13:10:01 信息 告警日志自动备份已接近最大保留个数，请注意下载备份

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 提示告警日志自动备份已接近最大保留个数，需注意下载备份。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	告警日志自动备份已接近最大保留个数，请注意下载备份。

3. 对系统的影响

影响磁盘空间。

4. 可能原因

影响磁盘空间。

5. 处理步骤

无需处理

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

5 网络连接

1. 告警解释

2013-05-23 13:10:01 信息 接口 eth1 没有连接网线

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的接口 eth1 没有连接网线。

2. 告警属性

发生时间	等级	事件
格式为	信息	接口eth1没有连接网线。

发生时间	等级	事件
yyyy-mm-dd hh:mm:ss		

3. 对系统的的影响

网络断开后会造成断网，设备会自动切换到物理直通模式。

4. 可能原因

设备物理链路断开。

5. 处理步骤

网络连接告警处理步骤如下。

(1) 检测连接设备的物理链路是否连接正常。

(2) 检测 WAF 设备的物理链路，可查看 eth 口的 link 灯是否常亮。

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。

6 双机热备状态

6.1 协商工作模式

1. 告警解释

2013-05-23 13:10:01　信息　[HA 状态]协商工作模式

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的 HA 状态为协商工作模式。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	[HA状态]协商工作模式。

3. 对系统的影响

系统正在协商工作模式，此时保护站点无防护。

4. 可能原因

主备机正在协商工作模式。

5. 处理步骤

确保有持续不断的流量访问。

6. 告警处理

选择右上角的未读消息按钮，如 2.1　5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1　6. 图 4 所示。

6.2 工作中

1. 告警解释

2013-05-23 13:10:01　信息　[HA 状态]主机工作中，备机状态正在检测

2013 年 5 月 23 日 13 时 10 分钟 1 秒，WAF 的 HA 状态为主机工作中，备机正在检测中。

2. 告警属性

发生时间	等级	事件
格式为 yyyy-mm-dd hh:mm:ss	信息	[HA状态]主机工作中，备机状态正在检测。

3. 对系统的影响

已完成协商，主机工作为透明代理模式，备机工作为网桥直通模式。

4. 可能原因

已完成协商。

5. 处理步骤

无需处理

6. 告警清除

选择右上角的未读消息按钮，如 2.1 5. (4)图 2 所示。点击“以上已读”即可清除，如 2.1 6. 图 4 所示。