UNIS W2000-G2 系列 Web 应用防火墙

故障处理手册

目 录

1 简介

本文档介绍 Web 应用防火墙常见故障的诊断及处理措施。

本文档适用于用户、系统管理员在产品使用过程中出现的故障处理及注意事项

注意

系统正常运行时，建议您在添加任务后，请勿进行关机重启等操作，以免影响其它用户正在执行的任务，避免造成任务中断，任务停止，影响其它用户使用。

1.1 故障处理注意事项

注意

设备正常运行时，建议您在完成重要功能的配置后，及时保存并备份当前配置，以免设备出现故障后配置丢失。建议您定期将配置文件备份至远程服务器上，以便故障发生后能够迅速恢复配置。

在进行故障诊断和处理时，请注意以下事项：

- 系统出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），收集信息越全面、越详细，越有利于故障的快速定位。
  - 记录具体的故障现象、故障时间、配置信息。
  - 记录完整的网络拓扑，包括组网图、端口连接关系、故障时间，故障功能模块。
  - 查看系统信息和诊断信息。
  - 记录设备故障时单板、电源、风扇指示灯的状态，或给现场设备拍照记录。
  - 记录现场采取的故障处理措施和后台执行操作（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
  - 记录故障处理过程中配置的所有命令行显示信息。
- 更换和维护设备部件时，请关机并摘除电源以确保您和设备的安全。
- 故障处理过程中如需更换硬件部件，请参考与软件版本对应的版本说明书，确保新硬件部件和软件版本的兼容性。

1.1 故障处理求助方式

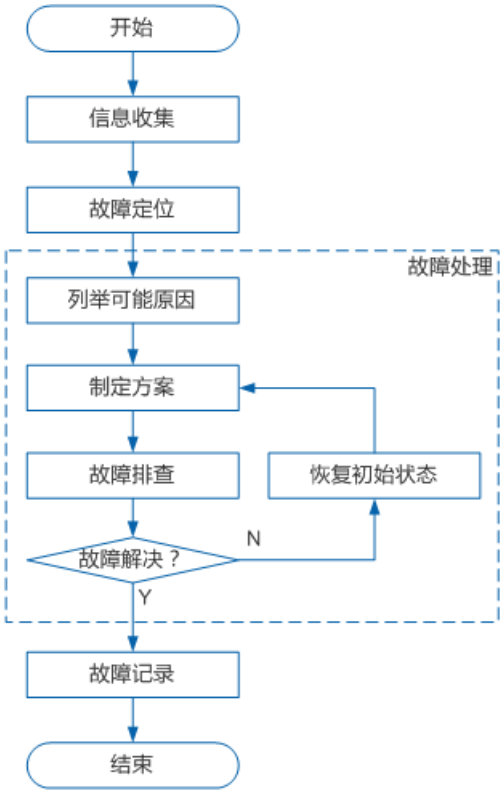
使用过程中，常见故障问题，请参考以下故障处理解决办法，若您遇到的问题不在以下故障处理范围内，或者当故障无法自行解决时，请详细记录故障信息、故障现象等，并和技术支持人员沟通，进行故障定位分析，获取解决办法。

1.2 故障处理流程

故障的处理难以根据现象直接推导出故障原因，不同原因可能会导致相同的故障现象。本节提供的故障处理流程主要用于指导用户科学地处理故障，有效地将故障范围缩小。从而达到提高故障处理效率，减少处理时间的目的。

系统化的故障处理，有利于将大型、综合、复杂的现象分隔缩小范围，从而达到对故障现象的准确定位。

图1-1 故障处理流程



- 信息收集：发生故障后应该第一时间收集故障的相关信息，而不是盲目的进行故障恢复。
- 故障定位：根据收集的故障信息，进行故障的初步定位，从而有效的缩小故障的范围。
- 列举可能原因：根据定位后的结果，列出所有的可能原因。
- 制定方案：以故障原因的可能性大小，辅助参考是否容易实施，制定故障排查的顺序，同时每种原因也要制订故障排查方案。
- 故障排查：按照方案依次进行故障的排查，根据排查结果决定是否继续排查下一个原因。
- 恢复初始状态：在排除特定故障后，如果没有解决问题，需要恢复为故障的初始状态，避免引入其它故障。
- 故障记录：完成故障处理后，需要将故障排查过程进行文档化记录，以便故障排查经验的记录和传递。

1.3 了解故障相关的其它信息

从受故障影响的用户收到报告，并收集到一些故障现象后。还需要从其它相关用户那里继续收集有用的信息，以辅助进行定位判断。通常需要确认：

(1) 发生故障时是否修改了配置？

(2) 设备在正常情况下的工作状态？

(3) 发生故障前，用户可能做了哪些操作，操作的顺序是怎样的？

1.4 故障记录

将故障处理的过程进行文档化是故障处理的最后一步，完整清晰的文字记录有助于对故障处理经验的积累和传递。记录中需要包含本次故障处理的全部信息，通常包含：

(1) 故障现象描述及收集的相关信息。

(2) 网络拓扑图绘制。

(3) 故障发生的可能原因。

(4) 对每一种可能原因制定的方案和实施结果。

2 登录故障处理

2.1 无法登录到设备Web页面

2.1.1 故障描述

WAF 的 Web 管理页面无法正常登录。

2.1.2 故障处理步骤

(1) 首先使用网络诊断工具 ping WAF 的管理地址，检查 WAF 是否存活；

(2) 如果 ping 不通，可通过串口登录 WAF 后台（登录名：admin，密码：admin），使用 bridge -S 命令查看管理桥 IP 是否丢失；若丢失，使用 MngtBridge 作为管理桥，管理 IP 为 183.1.4.230，可通过命令行 bridge -A -v MngtBridge -f 183.1.4.230 -m 255.255.255.0 -n y（注意一定要加上-n y ，否则无法登录该管理地址）将地址重新添加上；

(3) 若管理口 IP 未丢失，但是仍 ping 不通，可使用 remote -S 命令查看管理 PC 是否在信任主机权限内；若管理 PC 不在信任主机权限内，可通过 remote -A -t web -i 101.1.36.0 -m 255.255.255.0；

(4) 若可以 ping 通管理口 IP，但登录不了页面，可登录 WAF 后台，使用 websslport -G 命令查看是否 https 的端口号被修改了；如果被修改为非 443 端口，可通过 websslport -S -p 443 将其修改恢复；

(5) 如果按上述操作仍然无法登录 WAF 的 Web 管理页面，请搜集信息并发送给技术支持人员协助分析。

3 License 故障

3.1 无法上传License

上传 License 失败时通常会有提示信息，请根据提示信息处理。

3.1.1 故障描述

上传 License 文件时提示出错，上传失败。

3.1.2 故障处理步骤

(1) 检查确认 License 文件是否匹配设备产品信息，如设备序列号及设备硬件信息，如果有问题请重新申请 License 文件；

(2) 检查确认 License 文件是否出现损坏等情况，如果有问题请重新申请 License 文件；

(3) 检查确认 License 是否过期，如果过期请续购 License；

(4) 如果按上述操作仍然无法成功导入 License 文件，请搜集信息并发送给技术支持人员协助分析。

4 常见问题处理

4.1 Windows 防护端在server2008R2上安装后，无法探测，重装也没用

排查思路：

(1) 确认 Server2008R2 是否装了 SP1 安全补丁。如没有需要依次安装以下①②提到的补丁；

(2) 如打了 SP1 补丁，确认有无打 39029 补丁，如无打上 39029 补丁即可。

解决方法：

windows 防护端因为替换了代码签名，对 winserver2008R2 系统有要求，windows Server 2008 R2 版本没有打相应微软要求的安全补丁会导致安装驱动提示错误。

①补丁 SP1：https://www.microsoft.com/zh-cn/download/details.aspx?id=5842；

②补丁 39029：

32 位系统补丁：http://www.wosign.com/download/Windows6.1-KB3033929-x86.zip；

64 位系统补丁：http://www.wosign.com/download/Windows6.1-KB3033929-x64.zip。

注意

先要求打了 SP1 的安全补丁，再要求打 39029 补丁，如果系统本身已经是 SP1 版本的情况下，直接打 39029 补丁即可。

4.2 登录系统后，菜单栏只显示主页面

4.2.1 故障描述

登录系统后，菜单栏只显示出主页面栏，未显示相关配置等栏

4.2.2 故障排查

出现此问题原因是设备未导入授权或授权文件已过期，在主页面>许可证管理>升级许可信息，进行授权文件导入

4.3 串联部署后，网络不通，服务器无法访问

4.3.1 故障描述

在设备串联部署在交换机和服务器之间时，导致网络无法联通，服务器无法访问；

4.3.2 故障处理流程

1. 检查网络配置以及插线情况
2. 检查询问网络环境的特殊性

4.3.3 故障处理步骤

(1) 检查网桥地址是否存在冲突。地址冲突会导致流量不能正常经过 Web 应用防火墙。
(2) 检查网关配置是否有误，错误的网关地址导致流量不能正常传输。
(3) 检查网络接口是否连接有误，错误的网桥接口和插线的接口不对应导致流量不能正常传输。
(4) 检查网络环境中是否有链路聚合或者 trunk 模式环境，如果存在，需要在 WAF 上相应地配置 channel 模式或者 trunk 模式。

4.4 设备串联或旁路后，网络正常，服务器可正常访问，但是防护设备上无访问日志和攻击日志。

4.4.1 故障描述

WAF 设备上未产生防护服务器的访问日志或防护日志。

4.4.2 故障处理流程

1. 检查服务器管理配置
2. 检查防护策略配置

4.4.3 故障处理步骤

(1) 检查服务器管理中的服务器 ip 地址和服务器的端口号是否填写错误，错误的 ip 地址/端口号会导致无法防护和记录日志。

(2) 检查服务器管理中的部署模式和防护模式是否配置错误，选取错误的部署模式和防护模式会导致无法防护和记录日志。

(3) 检查服务器管理中的接口是否配置错误，选择错误的接口会导致无法防护和记录日志。

(4) 检查是否开启防护策略，未开启防护策略会导致无法记录日志。

(5) 检查访问日志是否选择开启，未开启访问日志，将不会记录日志。

(6) 上述现象都未出现，进行抓包检查流量和访问情况；若只有 arp 包，再对 Web 应用防火墙进行网络配置检查；若有正常的数据包，针对具体数据包情况进行分析。

4.5 用户忘记密码或用户被锁定了

4.5.1 故障描述

Web 界面登录用户，提示账户被锁定，请联系管理员。

图4-1 用户被锁定

4.5.2 故障处理

account 管理员登录后找到对应的用户，解除锁定或者重置密码都可。

4.5.3 故障处理步骤

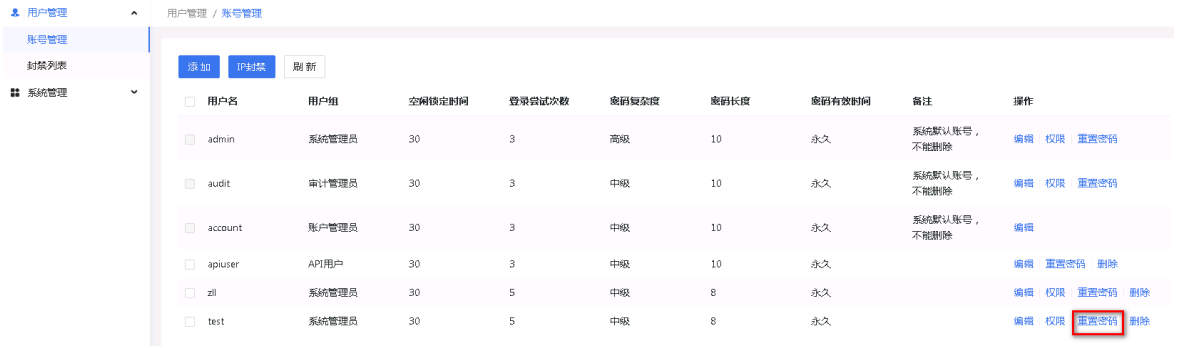
(1) account 管理员登录 Web 管理端，检查该账号是否由于输入错误的密码超过限定次数后导致，用户管理>封禁列表，查看该账号是否在封禁用户列表中。

图4-2 开启被锁定账户

(2) 如果在封禁用户列表中，选中该用户并点击“解除封禁”即可解除锁定。

(3) 如果用户无法回忆起密码，可以选择重置密码，方法是：在用户管理中选中该用户点击“重置密码”按钮，输入新密码

图4-3 重置密码



4.6 设备上线后，部分站点或者URL无法正常访问

4.6.1 故障描述

部分站点和 url 无法正常访问/数据无法上传等现象。

4.6.2 故障处理流程

1. 检查确认是否由匹配 WAF 规则导致的

2. 如果是 WAF 规则导致的，排除/不启用误拦截的规则

4.6.3 故障处理步骤

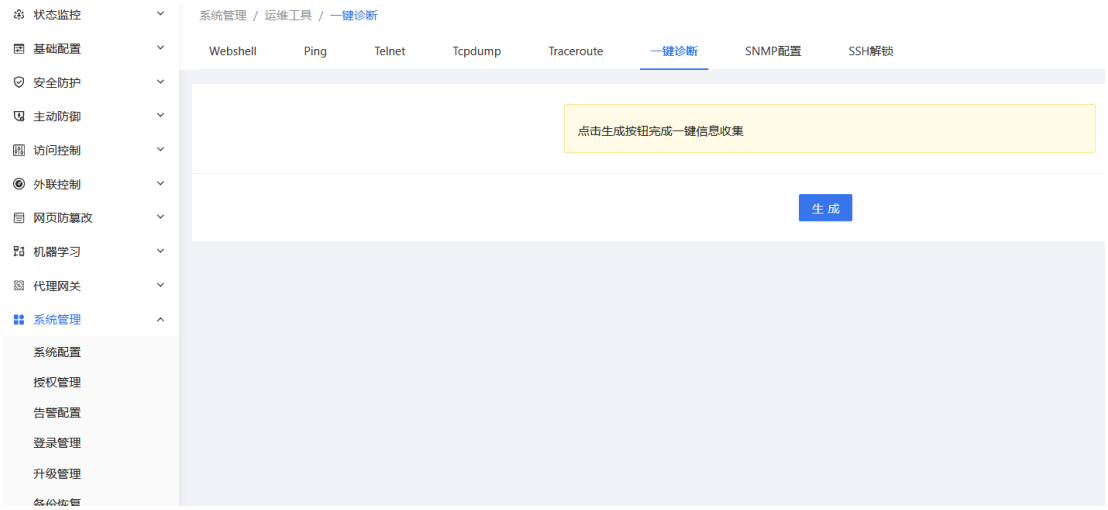
(1) 检查访问控制>黑名单/URL 黑名单是否误配了，如果是误配了，删除即可；

(2) 对站点停用 Web 防护策略，再进行访问测试，确认是否由 WAF 的 Web 防护规则导致的；

(3) 检查日志报表>防护日志， 查看是否有相应 URL 的阻断日志，若攻击日志较多或刷新较快，可通过防护日志的条件进行站点/目的 URL 过滤查询，找到相关攻击类型、处理动作、规则名称，根据规则名称/规则号在 Web 防护策略中不启用相关规则或者设置更合适的处理动作即可；

(4) 如果上述操作仍不能解决正常业务访问被 WAF 阻断的情况，请在系统管理>运维工具>一键诊断，点击“生成”按钮完成一键信息收集并发送给技术支持人员协助分析。

图4-4 一键信息收集



4.7 浏览器打开地址链接后显示证书存在安全问题

4.7.1 故障描述

浏览器访问平台链接地址后，提示此证书存在安全问题。

图4-5 浏览器访问证书问题

图4-6 浏览器访问证书问题

4.7.2 故障处理流程

点击继续浏览即可。

4.7.3 故障处理步骤

点击“继续跳转到网页”，此问题是由于产品的 HTTPS 证书不是公有证书，浏览器默认不认可私有证书导致。选择“继续”不会对浏览器有影响。

4.8 切换Bypass状态

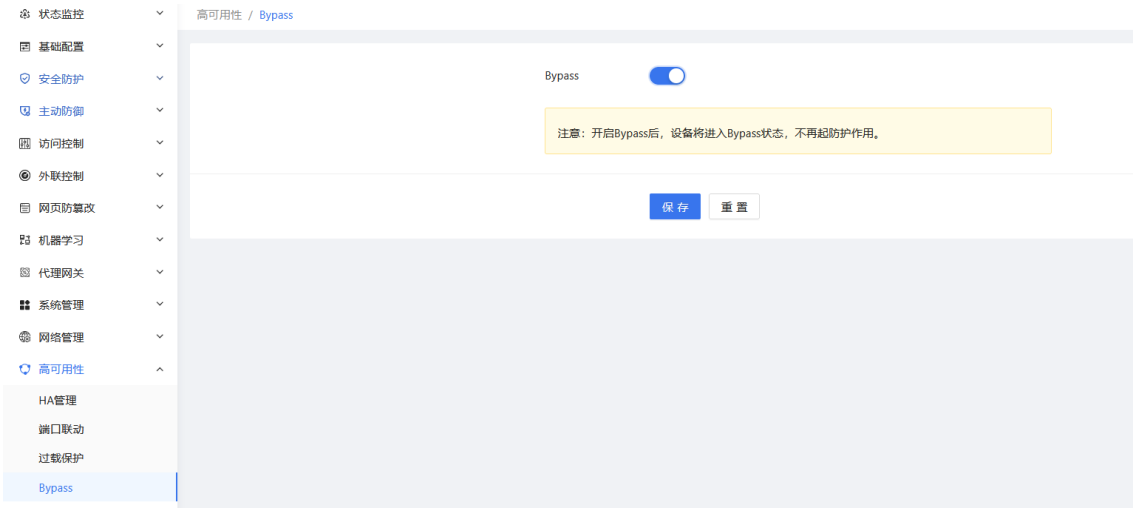
4.8.1 故障描述

WAF 部署为透明模式且进、出口使用一对 Bypass 口时，当出现网络故障时可以将 WAF 切换为 Bypass 状态，用于初步判断是否是 WAF 出现故障。当 WAF 切换到 Bypass 状态后，设备进、出两个网络接口呈短路状态，WAF 不再处理过往的流量。

4.8.2 故障处理步骤

可在“高可用性> Bypass”页面，打开 Bypass，并点击保存。

图4-7 启用 Bypass



4.9 如何生成技术支持文件

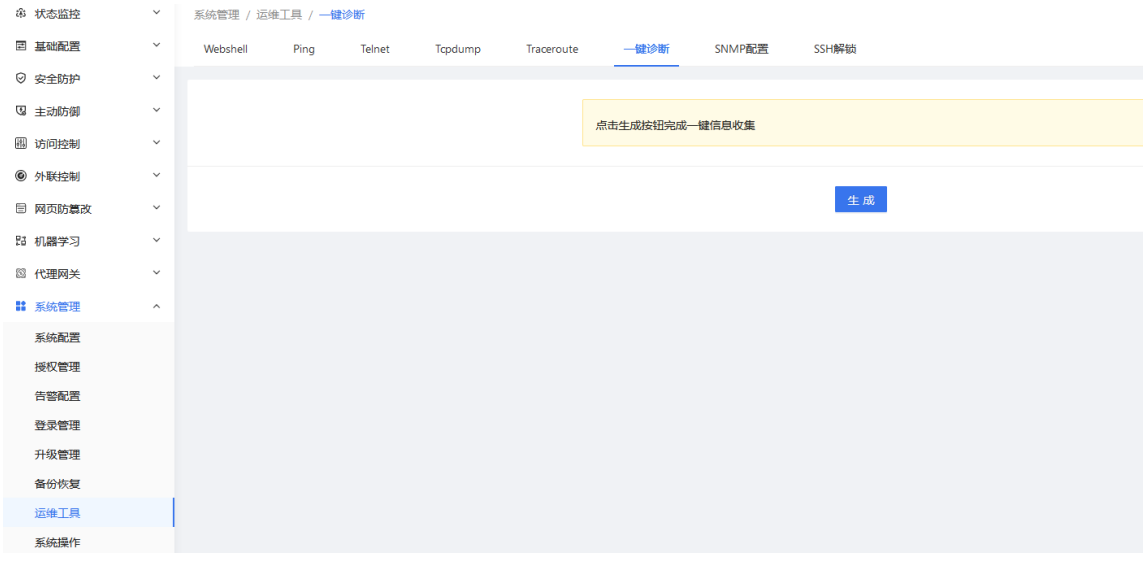
4.9.1 故障描述

当发生的问题通过排查无法解决。

4.9.2 故障处理步骤

可在“系统管理>运维工具>一键诊断”页面，点击生成按钮，待生成完成后，点击保存，将该文件发送给技术支持人员协助分析。

图4-8 WAF 生成技术支持文件



4.10 当CPU、内存较高时，可以采取哪些措施

4.10.1 故障描述

WAF 使用过程中出现 CPU、内存较高的情况。

4.10.2 故障处理步骤

由于导致 CPU 和内存较高的情况较为复杂，从 Web 页面较难分析出具体原因，因此建议按照具体情况的紧急性采取对应措施。

(1) 如果 CPU、内存较高时，导致正常业务流量受到影响，针对特别紧急且采用透明模式部署的情况，在确认链路采用 BYPASS 对接口的情况下可以直接强制 BYPASS，使 WAF 不再处理过往的流量，具体步骤可参照 4.8 小节；

(2) 如果 CPU、内存较高时，情况没有特别紧急，建议参照 4.8 小节收集技术支持文件，将该文件发送给技术支持人员协助分析。

4.11 如何在没有攻击的情况下判断WAF已生效

4.11.1 故障描述

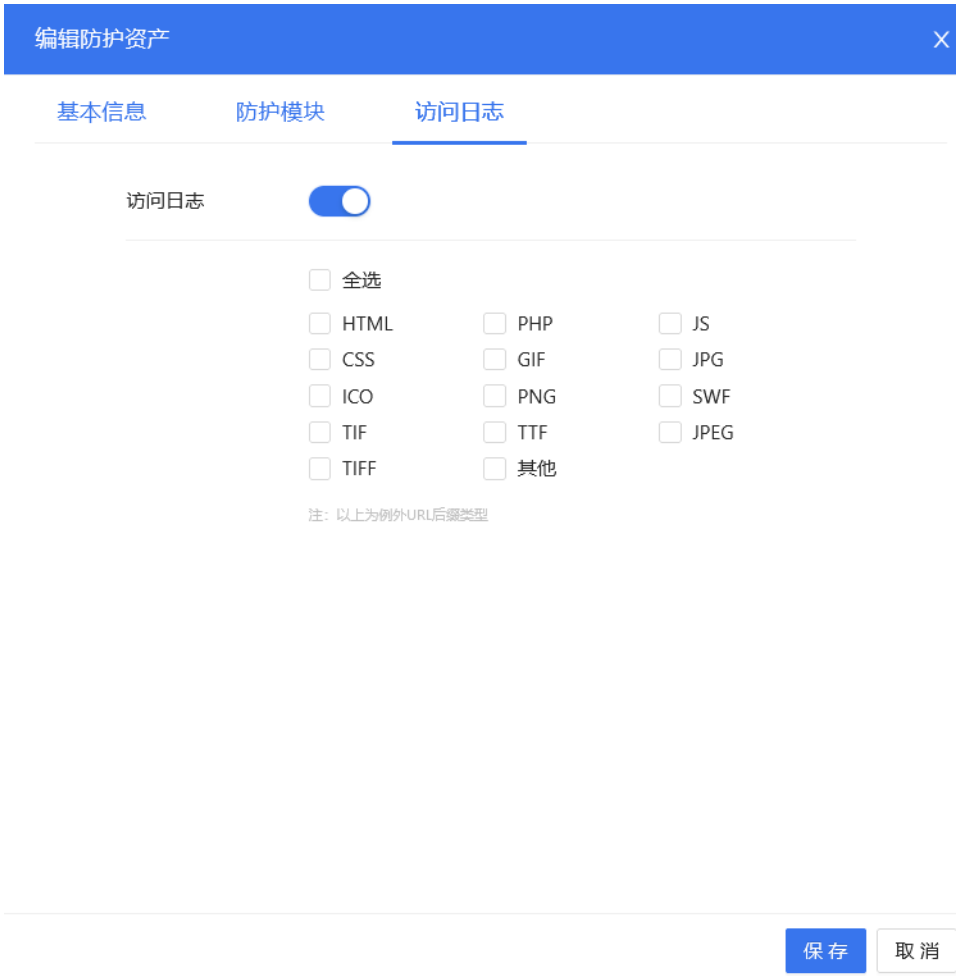
已部署、配置好 WAF，并且已配置、启用了所需的相关策略，在没有攻击的情况下如何判断 WAF 已生效。

4.11.2 故障处理步骤

由于 WAF 对于 Web 访问行为的记录是与“防护资产”关联的，因此，可以通过开启访问日志记录并查看是否产生访问日志来判断 WAF 是否已生效。

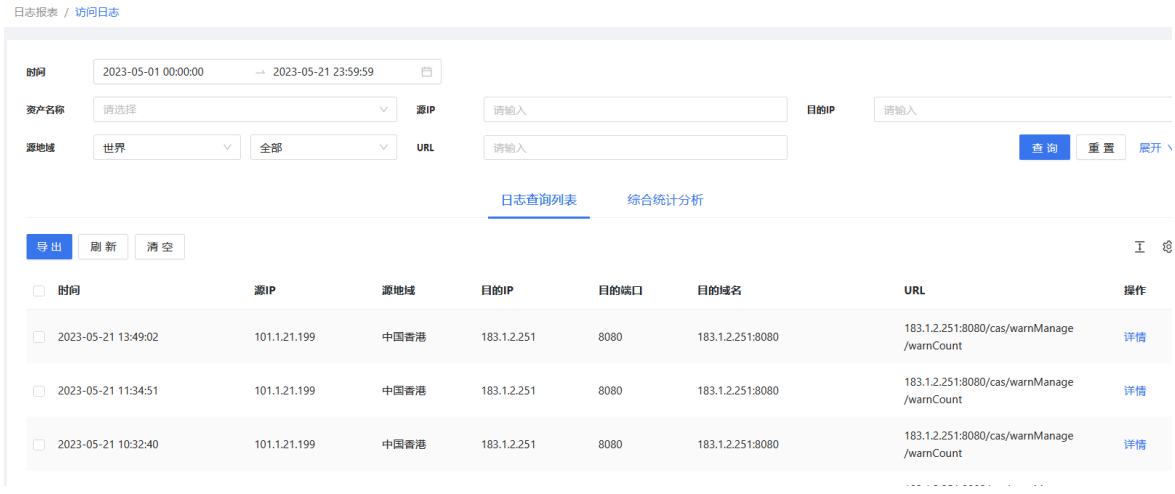
(1) 在“基础配置>防护资产”中，编辑相应的防护资产，访问日志选择开启，并点击保存；

图4-9 启用记录 Web 访问日志



(2) 当有访问流量经过 WAF 时，点击“日志系统>访问日志”进行查看，如果产生了访问日志，说明 WAF 的防护功能已经生效。

图4-10 查看访问日志



4.12 当业务经WAF设备转发存在丢包故障时应如何排查

4.12.1 故障描述

业务经 WAF 设备转发时存在丢包故障。

4.12.2 故障处理步骤

(1) 分别在停用、启用策略情况下，在业务的流入和流出口进行抓包对比，查看是否是硬件、组网等非软件问题导致的；

(2) 抓包方法：点击“系统管理>运维工具>>tcpdump”页面，选择需要抓包的协议类型、数据条目、接口、类别、主机 IP/域名，点击启动，抓包完成后点击停止按钮，并点击保存按钮导出抓包文件进行查看；

图4-11 使用 tcpdump 抓包

(3) 分析抓包文件后，如果确认是某些策略开启导致的，可逐个关闭相应策略，缩小问题范围，最终定位问题原因；

(4) 如果按上述操作仍然排查不出丢包故障的原因，请搜集信息并发送给技术支持人员协助分析。

4.13 当正常的业务访问被WAF阻断时应如何排查

4.13.1 故障描述

正常的业务访问被 WAF 阻断。

4.13.2 故障处理步骤

(1) 针对特别紧急且采用透明模式部署的情况，在确认链路采用 BYPASS 对接口的情况下可以直接强制 BYPASS，使 WAF 不再处理过往的流量，具体步骤可参照 4.8 小节；

(2) 针对不是特别紧急的情况，可以在日志中使用条件选项进行过滤查询，可以根据时间、IP 等选项进行过滤，查看对应日志；

图4-12 在日志中过滤查询

(3) 在过滤后的日志中查看是否有阻拦动作的日志，如果有，可以根据该日志条目的攻击类别进行例外添加或功能关闭，再进一步查看业务状态是否正常；

(4) 如果按上述操作仍不能解决正常业务访问被 WAF 阻断的情况，请搜集信息并发送给技术支持人员协助分析。

5 硬件故障问题

5.1 万兆插卡无法up

4 端口万兆光或 4 端口万兆光（带 2 对 bypass，多模）可能会出现光口无法 up 问题，需通过升级插卡固件版本解决。

所需工具：

- 需要 8G 以上 U 盘；
- 带 USB 口的键盘与显示器；（若无显示器和键盘，可直接连接串口）
- 固件升级包，请在官网 R6203 版本路径下获取：
  - 用于制作 U 盘镜像：FW8.15 Linux 盘 USB-密 12345678.img
    MD5：60B4C68D38765266E33430013BF43390
  - 用于制作 U 盘软件包：usbit.zip
    MD5：51FC107634689D18E909AD91B475238F

注意：若是暂时没有条件进行固件升级时，可以先在 waf 物理口上插上光模块和光纤保证物理可通后，启动 waf 设备 。

5.1.1 故障描述

4 端口万兆光或 4 端口万兆光（带 2 对 bypass，多模）可能会出现光口无法 up 问题。

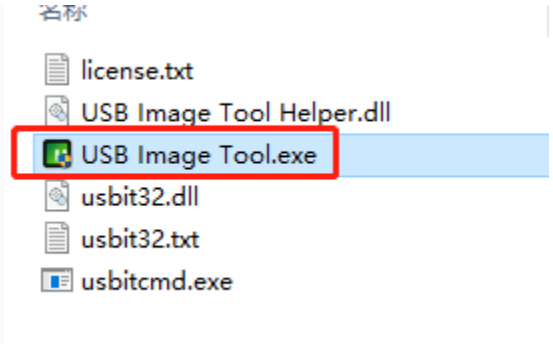
5.1.2 故障处理步骤

1. 可以尝试断电重启，如果仍无法解决，则建议进行如下 2、3 步骤，升级固件。

2. Linux 环境准备

(1) 进入文件夹 usbit，双击运行 USB Image Tool.exe。

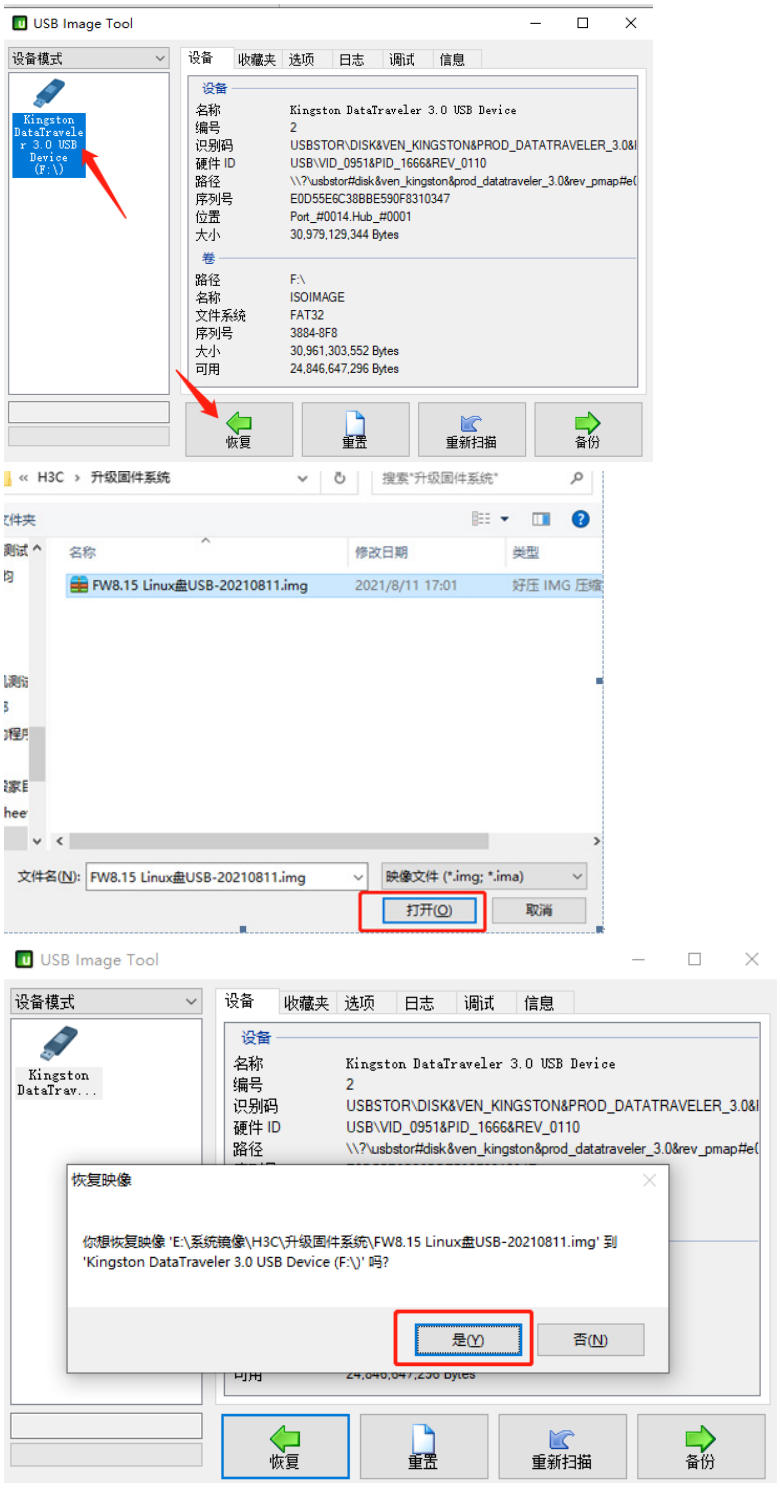
图5-1 运行 USB Image Tool



(2) 将需要做系统的 U 盘插在设备上（U 盘需要 8GB 以上）。

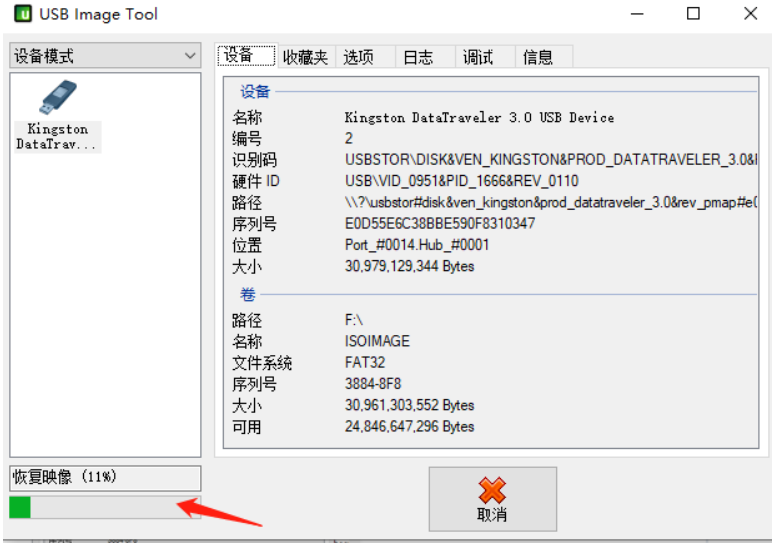
(3) 出现下图，选中 U 盘，然后点击恢复按钮选择镜像“FW8.15 Linux 盘 USB-密 12345678.img”，选择打开，然后点击“是”按钮。注：图片中镜像仅为举例，以实际镜像为准。

图5-2 安装运行 USB Image Tool



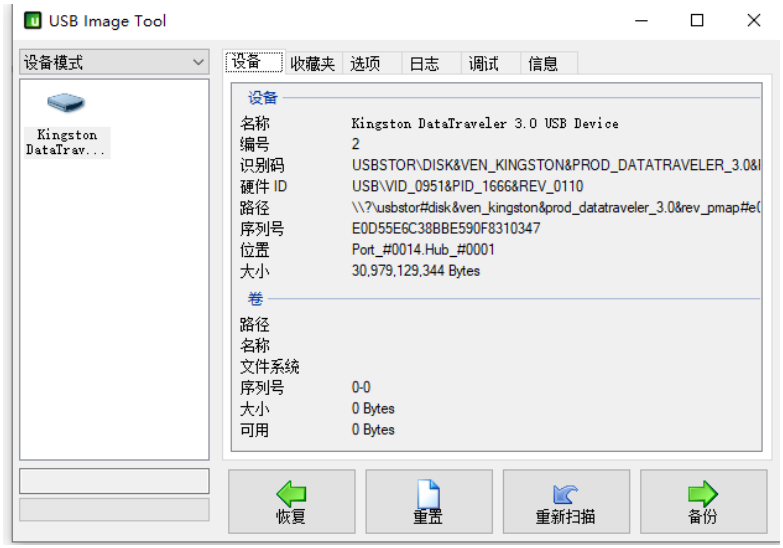
下图是正在恢复镜像中... 等待进度条走完即可。

图5-3 安装中



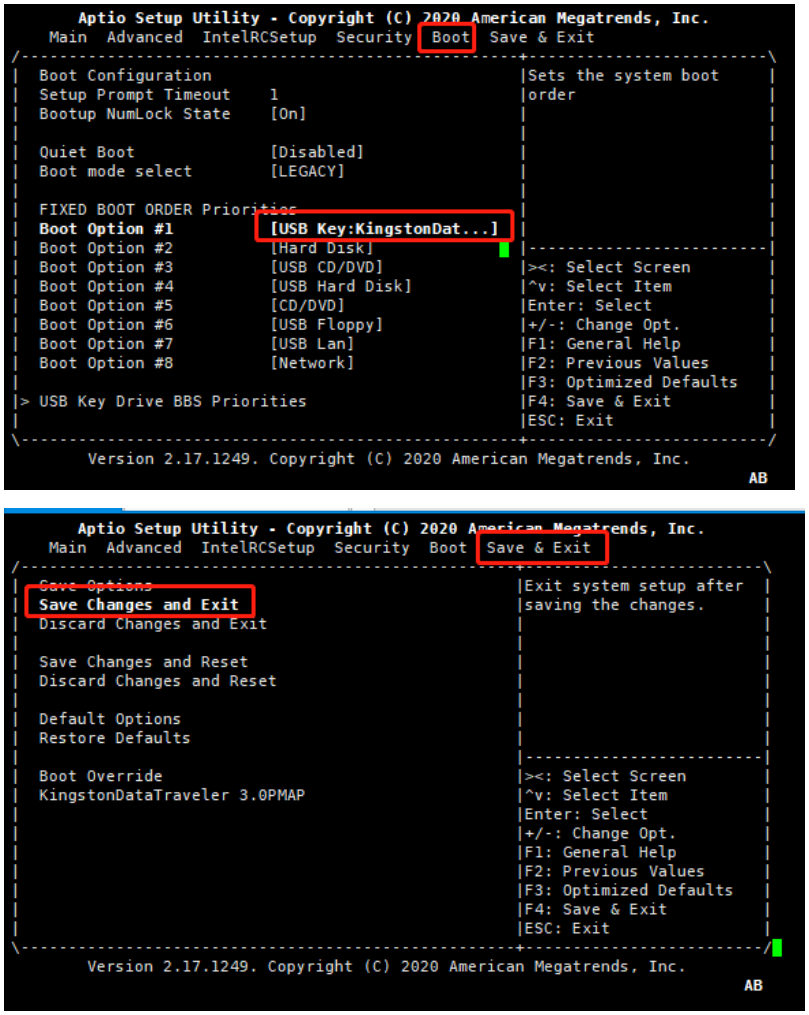
如下图，表示 U 盘系统做完。拔掉 U 盘，将 U 盘插上设备的 USB 口上，开机按键盘“Del”进 BIOS。

图5-4 安装完成



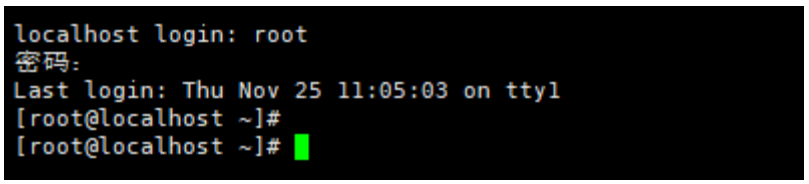
(4) 插入键盘和显示器（或直接连接串口，波特率是 115200），启动设备后点击 delete 键进入 bios 界面，如下图是 BIOS 页面，使用左右上下箭头进行切换，在 boot 那一列选择 BOOT Option1 为 USB 的 U 盘启动，最后按键盘 F4 或者选择 BIOS 下 Save & Exit 的 Save Changes and Exit。保存退出。设备自动重启从 U 盘启动进系统。

图5-5 设置 USB 的 U 盘启动



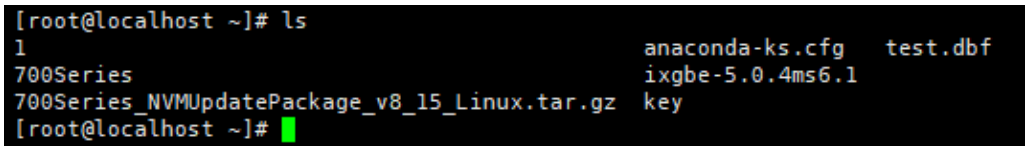
(5) 进入系统后，系统用户名 root，密码 12345678。

图5-6 登录设备



(6) 输入 ls 查看系统下文件如下图。

图5-7 查看系统文件



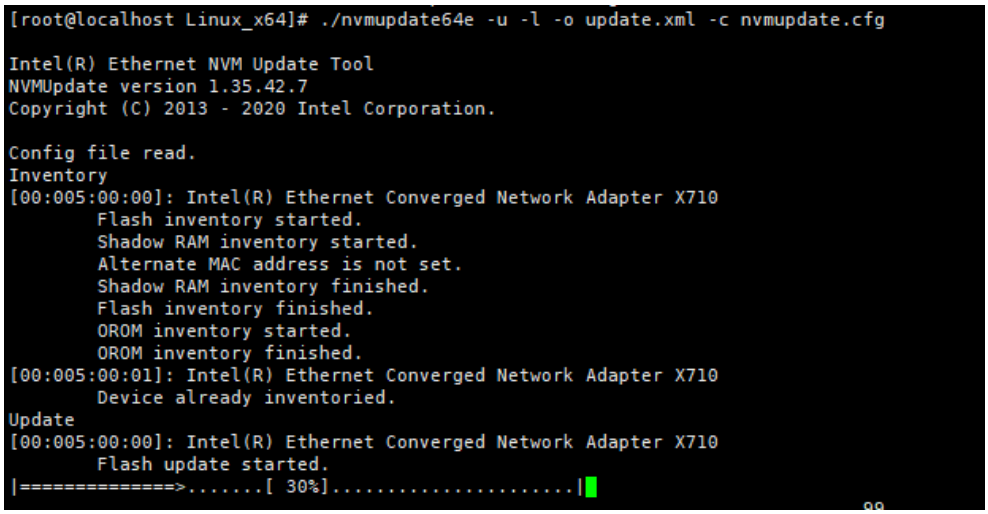
(7) 插上需要被升级的 4 端口以太网万兆光口卡。

3. linux 环境升级步骤

(1) 输入 cd 700Series/Linux_x64 进入/700Series/Linux_x64 路径下。

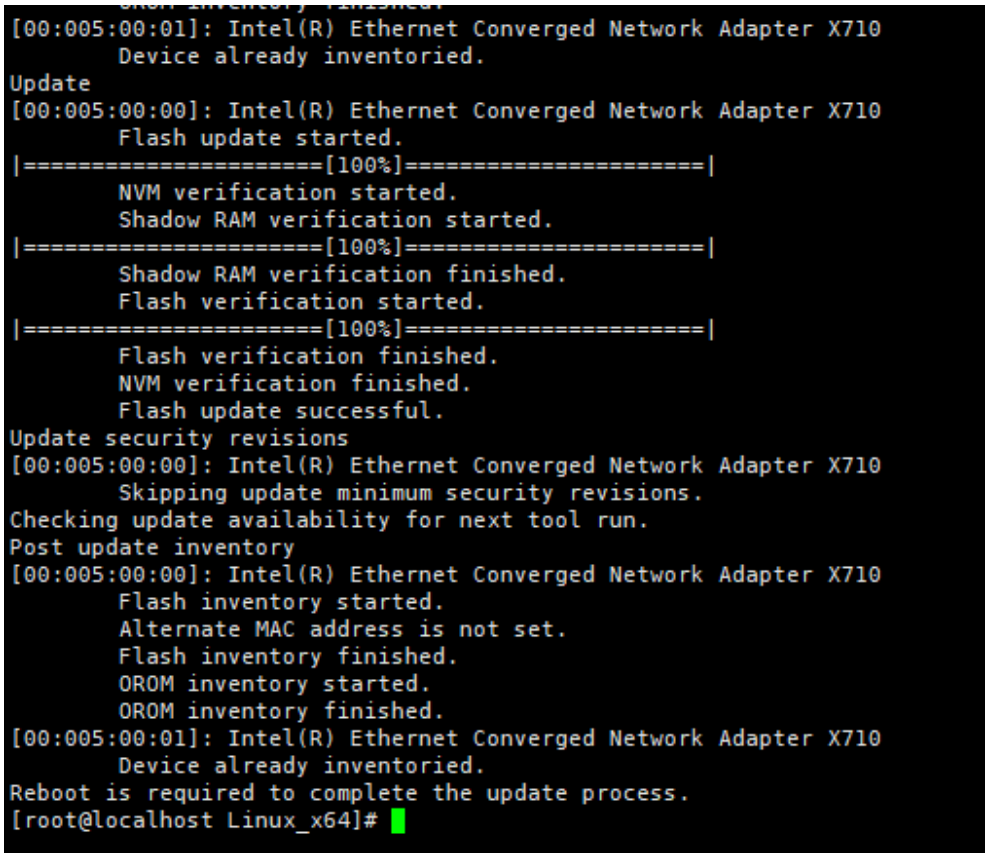
(2) 执行# ./nvmupdate64e -u -l -o update.xml -c nvmupdate.cfg 如下图。

图5-8 执行# ./nvmupdate64e -u -l -o update.xml -c nvmupdate.cfg



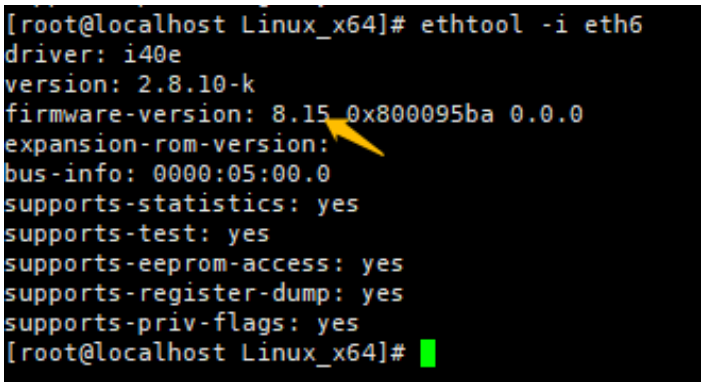
(3) 当出现下图界面表示升级成功。之后 reboot 系统。

图5-9 准备重启



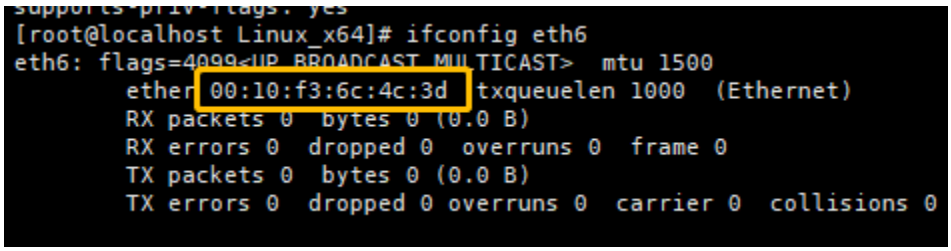
(4) 重启后找到万兆网卡对应网卡的网口名字，”ethtool -i 网口号”查看 firmware-version 版本号。如下图显示升级到 8.15 版本 OK。

图5-10 升级到 8.15 版本



(5) 复验下 MAC 地址是否有在。

图5-11 复验下 MAC 地址



(6) 确认 OK，则表示使用 linux 环境升级 firmware 固件成功。

5.2 双电源插槽，PWR1无法插入

5.2.1 故障描述

双电源插槽，PWR1 无法插入。

5.2.2 故障处理步骤

(1) 如果 PWR1 无法插入，建议使劲用力插入，或者从电源模块的上边框或者下边框 45 度方向用力使劲推入。

6 故障诊断命令

6.1 常用故障诊断命令

命令	说明
help	命令说明帮助按钮
bridge –S和port-S	显示当前网络接口信息
ping	检查网络是否连通
route -S	检查路由信息
reboot -R	重启
display-version	查看系统信息