

UNIS W2000-G 系列 Web 应用防火墙

故障处理手册

目 录

1 简介.....	1
1.1 故障处理注意事项	1
1.1 故障处理求助方式	1
1.2 故障处理流程.....	2
1.3 了解故障相关的其他信息.....	3
1.4 故障记录	3
2 故障处理	3
2.1 登录系统后，菜单栏只显示主页面	3
2.1.1 故障描述	3
2.1.2 故障排查	3
2.2 串联部署后，网络不通，服务器无法访问；	3
2.2.1 故障描述	3
2.2.2 故障处理流程	4
2.2.3 故障处理步骤	4
2.3 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
2.3.1 故障描述	4
2.3.2 故障处理流程	4
2.3.3 故障处理步骤	4
2.4 用户忘记密码或用户被锁定了	4
2.4.1 故障描述	4
2.4.2 故障处理	5
2.4.3 故障处理步骤	5
2.5 设备上线后后，部分站点或者 URL 无法正常访问.....	6
2.5.1 故障描述	6
2.5.2 故障处理流程	6
2.5.3 故障处理步骤	6
2.6 浏览器打开地址链接后显示证书存在安全问题	6
2.6.1 故障描述	6
2.6.2 故障处理流程	7
2.6.3 故障处理步骤	7
3 故障诊断命令	8
3.1 常用故障诊断命令	8

1 简介

本文档介绍 UNIS 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，以免影响其他用户正在执行的任务，避免造成任务中断，任务停止，影响其他用户使用。

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

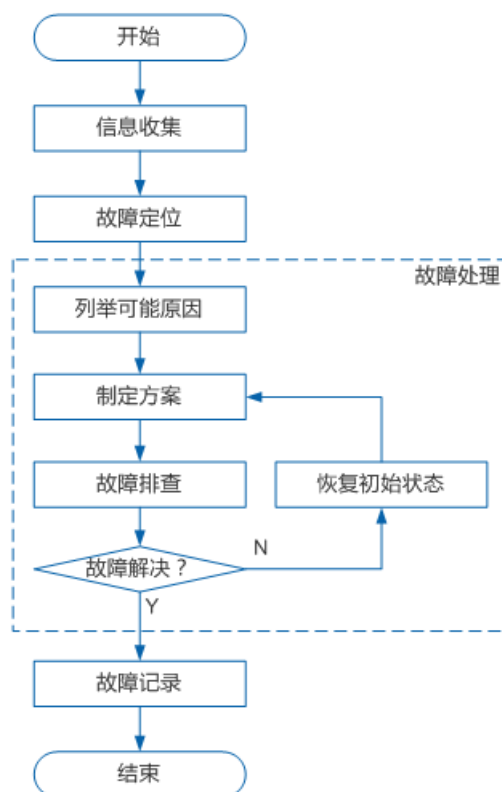
使用过程中，常见故障问题，请参考以下故障处理解决办法，若您遇到的问题不在以下故障处理范围内，或者当故障无法自行解决时，请详细记录故障信息、故障现象等，并和紫光横越公司技术支持人员沟通，进行故障定位分析，获取解决办法。

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，避免引入其他故障。
- 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 了解故障相关的其他信息

从受故障影响的用户收到报告，并收集到一些故障现象后。还需要从其他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) 设备在正常工作下的工作状态？
- (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 故障处理

2.1 登录系统后，菜单栏只显示主页面

2.1.1 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

2.1.2 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

2.2 串联部署后，网络不通，服务器无法访问；

2.2.1 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；

2.2.2 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

2.2.3 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。

2.3 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。

2.3.1 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。

2.3.2 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

2.3.3 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。

2.4 用户忘记密码或用户被锁定了

2.4.1 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2-1 用户被锁定



2.4.2 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。

2.4.3 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，如图 2-2，系统管理>账户管理，查看该账号是否在阻断用户列表中。

图2-2 开启被锁定账户



- (2) 如果在阻断用户列表中，选中该用户并点击“解除锁定按钮”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”按钮，输入新密码

图2-3 重置用户



2.5 设备上线后后，部分站点或者URL无法正常访问

2.5.1 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。

2.5.2 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

2.5.3 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) 检查日志系统>攻击日志， 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，可通过攻击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，请在系统诊断>远程支持，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2-4 一键信息收集



2.6 浏览器打开地址链接后显示证书存在安全问题

2.6.1 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2-5 浏览器访问证书问题



图2-6 浏览器访问证书问题



2.6.2 故障处理流程

点击继续浏览即可。

2.6.3 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。

3 故障诊断命令

3.1 常用故障诊断命令

命令	说明
help	帮助按钮
ifconfig	显示当前网络接口信息
ping	检查网络是否连通
reboot -R	重启
display-version	查看系统信息