

铨迅 Web 应用防护系统

管理员手册



南京铨迅信息技术股份有限公司
Nanjing YXLink Information Technology Co., Ltd.

未经南京铱迅信息技术股份有限公司 (Nanjing YXLink Information Technology Co.,Ltd., 简称: 铱迅信息) 的事先书面许可, 对本产品附属的相关手册之所有内容, 不得以任何方式进行翻版、传播、转录或存储在可检索系统内, 或者翻译成其他语言。

- 本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其
所提到之产品信息, 所引起直接或间接的数据流失、利益损失或事业终止,
铱迅信息不承担任何责任。
- 铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利, 而无须事
先通知。
- 本手册描述的“铱迅 Web 应用防护系统”之功能, 并非所有型号都支持, 对
于每个型号拥有的功能模块, 请咨询供货商或联系铱迅客服人员。
- 本公司已竭尽全力来确保手册内载信息的准确性和完善性。如果您发现任何
错误或遗漏, 请向铱迅信息反映。对此, 我们深表感谢。

商标信息

铱迅信息、铱迅信息的标志、铱迅 Web 应用防护系统、铱迅 WEB 服务入侵防护系统的标志为南京铱迅信息技术股份有限公司的商标或注册商标。本手册或随铱迅信息产品所附的其他文件中所提及的所有其他商标名称，分别为其相关所有者所持有的商标或注册商标。

版本历史

版本	发布时间	说明
0.9	2010 年 3 月 12 日	初稿
...		
8.0	2019 年 11 月 21 号	更换产品 logo 和截图

阅读指导

如果您是第一次使用铱迅 Web 应用防护系统，建议首先阅读如下章节：

- 3. 安装部署
- 4. 安装及初始化
- 5. 快速使用指南
- 6. 开始使用

如果您做日常入侵告警的查看和分析，建议阅读如下章节：

- 7. 系统监控
- 8. 数据中心

如果您是高级用户，建议重点阅读如下章节：

- 9. 防护设置
- 10. 网络设置
- 11. 系统维护
- 12. 其他功能
- 13. Console 功能
- 14. 复位与还原

如果您想了解产品特点及规格，建议阅读如下章节：

- 1. 简介
- 2. 产品规格

如果您有问题需要寻求答案，可阅读如下章节：

- 15. 常见问题与解答

目 录

前言.....	11
1、简介.....	13
1.1 产品介绍.....	13
1.2 技术特点.....	13
2、产品规格.....	15
2.1 面板说明.....	15
2.1.1 接口说明.....	15
3、安装部署.....	17
3.1 透明网桥模式.....	17
3.1.1 单一混合型 Web 服务部署模式.....	17
3.1.2 单一分离式 Web 服务部署模式.....	18
3.1.3 集群式/集中式 Web 服务部署模式.....	19
3.1.4 半分散式 Web 服务部署模式.....	21
3.1.5 全分散式 Web 服务部署模式.....	22
3.2 混合部署模式.....	23
3.3 混合加密部署模式.....	24
3.4 旁路反向代理模式.....	25
4、安装及初始化.....	27
4.1 打开包装箱.....	27
4.2 安装设备.....	27
4.3 选择部署方案.....	27
4.4 初始化设备.....	27
4.4.1 连接设备的 Console 口.....	27
4.4.2 连接设备的 DSI 接口.....	28
4.4.3 配置 DMI 接口网络参数.....	29
5、快速使用指南.....	32
5.1 修改密码.....	32
5.2 设置检测端口.....	32
5.3 查看系统状态.....	33
5.3.1 系统状态.....	33
5.3.2 威胁视图.....	34
5.3.3 网络状态.....	36

5.4 查看入侵记录.....	37
5.5 查看网络流量.....	37
5.6 关机和重启.....	38
6、开始使用.....	39
6.1 登录.....	39
6.1.1 登录系统.....	39
6.1.2 系统管理员登录.....	40
6.1.3 安全审计员登录.....	41
6.1.4 安全管理员登录.....	42
6.2 密码修改.....	43
6.3 欢迎界面.....	44
6.4 功能菜单.....	45
6.5 通用菜单、按钮介绍.....	47
6.5.1 保存和应用功能.....	47
6.5.2 重置和取消功能.....	48
6.5.3 刷新功能.....	48
6.5.4 多选功能.....	48
6.5.5 双击功能.....	49
6.5.6 翻页功能.....	49
6.5.7 排序功能.....	49
6.5.8 选择列功能.....	50
7、系统监控.....	50
7.1 系统状态.....	50
7.2 实时流量.....	51
7.3 设备信息.....	51
7.4 授权信息.....	52
8、数据中心.....	53
8.1 威胁监控.....	53
8.1.1 入侵记录.....	53
8.1.2 入侵查询.....	58
8.1.3 入侵统计.....	59
8.1.4 阻断日志.....	60
8.1.5 弱密码日志.....	61
8.2 网络流量.....	62

8.3 系统报表.....	62
8.3.1 报表管理.....	62
8.3.2 即时报表.....	63
8.3.3 定期报表.....	63
8.4、日志.....	64
8.4.1 系统日志.....	65
8.4.2 审计日志(仅限于安全审计员).....	66
9、防护设置.....	67
9.1 入侵防护.....	67
9.1.1 基本参数设置.....	67
9.1.2 基本访问控制.....	70
9.1.3 高级访问控制.....	77
9.1.4 HTTPS 透明防护.....	82
9.1.5 智能阻断.....	83
9.1.6 木马上传检测.....	84
9.1.7 防盗链设置.....	84
9.1.8 CSPF 防护设置.....	86
9.1.9 Flood 防护设置.....	86
9.1.10 来源 IP 解析.....	93
9.2 对象配置.....	94
9.2.1 地址对象.....	94
9.2.2 计划任务.....	94
9.2.3 重定向页面.....	96
9.2.4 蜘蛛设置.....	99
9.3 防护策略.....	100
9.3.1 自定义规则.....	100
9.3.2 内置规则.....	107
9.3.3 防护策略集.....	108
9.3.4 HTTP 请求类型过滤.....	109
9.3.5 HTTP 头防溢出设置.....	109
10、网络配置.....	110
10.1 网络接口.....	110
10.1.1 接口管理.....	110
10.1.2 虚拟 IP 设置.....	113

10.1.3 端口汇聚.....	113
10.1.4 配置网络接口为普通方式.....	113
10.1.5 配置网络接口为透明方式.....	114
10.1.6 配置网络接口为策略路由方式.....	115
10.1.7 配置网络接口为端口汇聚方式.....	115
10.2 虚拟网桥.....	116
10.3 静态路由.....	116
10.3.1 修改默认路由.....	117
10.3.2 添加普通路由.....	117
10.4 DNS 设置.....	118
10.5 BYPASS 设置.....	118
10.6 部署方式.....	119
10.6.1 配置双路进线（电信、教育网）	119
10.6.2 配置一进多出（一条线路，多台服务器）	120
10.6.3 配置策略路由.....	120
10.7 反向代理.....	121
10.7.1 反向代理设置.....	122
10.8 高可用性.....	125
10.8.1 配置同步.....	127
11、系统维护.....	128
11.1 事件管理.....	128
11.1.1 通知告警.....	128
11.1.2 SNMP.....	129
11.1.3 SNMP Trap.....	130
11.1.4 syslog.....	130
11.2 网络诊断.....	130
11.2.1 网络工具.....	130
11.2.2 抓包工具.....	132
11.3 设备维护.....	133
11.3.1 配置管理.....	133
11.3.2 授权信息.....	134
11.3.3 系统时间.....	135
11.3.4 离线升级.....	135
11.3.5 在线升级.....	135
11.3.6 日志清理.....	136

11.3.7 关机/重启.....	137
12、其他功能.....	138
12.1 主动防御.....	138
12.1.1 漏洞扫描.....	138
12.1.2 URL 自学习.....	139
12.1.3 网页防篡改.....	142
12.1.4 数据库防篡改.....	145
12.2 高级设置.....	146
12.2.1 关键字过滤.....	146
12.2.2 弱密码检测设置.....	147
12.2.3 高级防御方式.....	148
12.2.4 紧急模式.....	148
12.2.5 一键断网.....	148
12.3 访问统计.....	151
12.3.1 网站统计.....	151
12.3.2 访问记录.....	152
12.3.3 网站详情.....	153
13、Console 功能.....	153
13.1 常用命令.....	153
13.1.1 主菜单：.....	154
13.1.2 配置菜单 (configure)：.....	154
14、复位与还原.....	155
15、常见问题与解答.....	156
附录 A. 出厂默认设置.....	157
A.1. 设备设置接口(DSI 接口)初始设置.....	157
A.2. 预置账号.....	158
A.2.1. 系统管理员预置账号.....	158
A.2.2. 安全审计员预置账号.....	158
A.2.3. 安全管理员预置账号.....	158
A.2.4. Console 用户预置帐号.....	158
A.3. 默认设置.....	158
附录 B. 正则表达式入门.....	159
B.1. 简述.....	160
B.2. 历史.....	160

B.3. 入门.....	160
B.4. 表达式全集.....	161
B.5. 常用的正则表达式范例.....	165

前言

文档范围

本文将覆盖铱迅 Web 应用防护系统（也称：铱迅 WEB 服务入侵防护系统）的硬件产品规格和 Web 管理界面的所有功能特点，并详细介绍该系统的具体使用方法。

期望读者

期望了解本产品主要技术特性和使用方法的系统管理员、网络管理员、网络安全专家等。本文假设您对其下面的知识有一定的了解：

- 系统管理
- TCP/IP 协议
- HTTP 协议
- Windows 或 Linux 操作系统

内容简介

1. 简介：介绍铱迅 Web 应用防护系统（也称：铱迅 WEB 服务入侵防护系统）的产品功能
2. 产品规格：介绍本产品的硬件规格和电气特性
3. 安装部署：简明介绍本产品的安装和部署方式
4. 安装及初始化：介绍本产品的安装的一般过程
5. 快速使用指南：介绍设备的基本使用方法
6. 开始使用：介绍 Web 管理页面的内容组织和使用指南
7. 系统监控：介绍 Web 管理界面中的设备基本信息的查看
8. 数据中心：介绍 Web 管理界面中的设备高级状态的监视
9. 防护设置：介绍 Web 管理界面中的高级功能的配置
10. 网络设置：介绍 Web 管理界面中的网络接口设置
11. 系统维护：介绍系统维护相关的功能和设置
12. 其他功能：介绍其他零散的功能和设置
13. Console 功能：介绍 Console 功能的配置
14. 复位与还原：系统的复位、密码的复位与还原的方法
15. 常见问题与解答：用户常见的问题与解答

附录 A：出厂默认设置

附录 B：正则表达式入门

获得帮助

获取网络安全相关资料可以访问钰迅信息网站：<http://www.yxlink.com/>

获取钰迅 Web 应用防护系统(也称：钰迅 WEB 服务入侵防护系统)的最新相关信息可以访问网址：
<http://www.yxlink.com/products-waf.html>

如需获取更详尽的钰迅信息网络安全专业服务信息、商务信息，您可通过如下方式和我们取得联系：

地址：江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

邮编：210012

服务热线：400-097-5557

电话：025-83235296, 025-83235396, 025-58722055

传真：025-83235296, 025-83235396 转 601

网站：<http://www.yxlink.com/>

Email：info@yxlink.com

格式与名词约定

设备、产品、系统——除非特指，本手册中均表示钰迅 Web 应用防护系统（也称：钰迅 WEB 服务入侵防护系统）

防火墙、应用防火墙——除非特指，本手册中均表示钰迅 Web 应用防护系统

【A】 —— 菜单名称和按钮名称的表示方式

【A】→【B】 —— 菜单项选择的表示方式



—— 使用技巧、建议和引用信息等



—— 重要注意信息

1、简介

1.1 产品介绍

铱迅 Web 应用防护系统 (也称: 铱迅 WEB 服务入侵防护系统。英文: YXLink Web Application Firewall, 简称: YXLink WAF) 是铱迅信息结合多年在应用安全理论与应急响应实践经验积累的基础上, 自主研发的一款应用级防护系统。在提供 Web 应用实时深度防御的同时, 实现 Web 应用加速与防止敏感信息泄露的功能, 为 Web 应用提供全方位的防护解决方案。

该产品致力于解决应用及业务逻辑层面的安全问题, 广泛适用于“政府、金融、运营商、公安、能源、税务、工商、社保、交通、卫生、教育、电子商务”等所有涉及 Web 应用的各个行业。部署铱迅 Web 应用防火墙产品, 可以帮助用户解决目前所面临的各类网站安全问题, 如: 注入攻击、跨站攻击、脚本木马、缓冲区溢出、信息泄露、应用层 DoS/DDoS 攻击等常见及最新的安全问题。

1.2 技术特点

“铱迅 Web 应用防护系统 (也称: 铱迅 WEB 服务入侵防护系统)” (下文称: “YXLink WAF”) 支持多种灵活的部署方式, 如透明网桥模式、混合部署模式、旁路反向代理模式、策略路由模式。

“YXLink WAF”工作在透明网桥模式下时, 管理员可在不需要修改原网络拓扑结构的情况下进行部署, 对于标准的 Web 应用, 可以做到即插即用, 无需对“YXLink WAF”进行任何配置。同时工作在透明网桥模式下时, 设备具有软硬件 Bypass 功能 (光口 Bypass 为选配件), 具有较高的容错机制, 相当于一根网线串入当前网络中, 并对 Web 应用攻击进行防御。而混合部署模式更是在应对复杂的网络应用环境中, 提供了更加人性化的均衡部署能力。同时, “YXLink WAF”旁路反向代理模式, 完全兼容老设备的旁路反向代理模式 (或称单臂模式), 对不能采用透明网桥模式部署的用户, 提供了多种部署模式的选择。

铱迅 Web 应用防护系统 (也称, 铱迅 WEB 服务入侵防护系统) 基于先进的技术架构和高效的检测引擎, 其主要特点有:

防护能力:

- 精确和完善的预防 Web 攻击的内置策略和规则;
- 高度自由的自定义规则系统, 轻松应对各种最新黑客攻击方式;
- 支持 Unicode 完全解码, 防止攻击者采用 Unicode 变形绕过防护设备;
- 支持不小于 20MB 的报文组包, 防止攻击者采用 TCP/IP 碎片攻击绕过设备;
- 蜘蛛设置;
- 智能阻断 (部分型号支持);
- 防盗链;

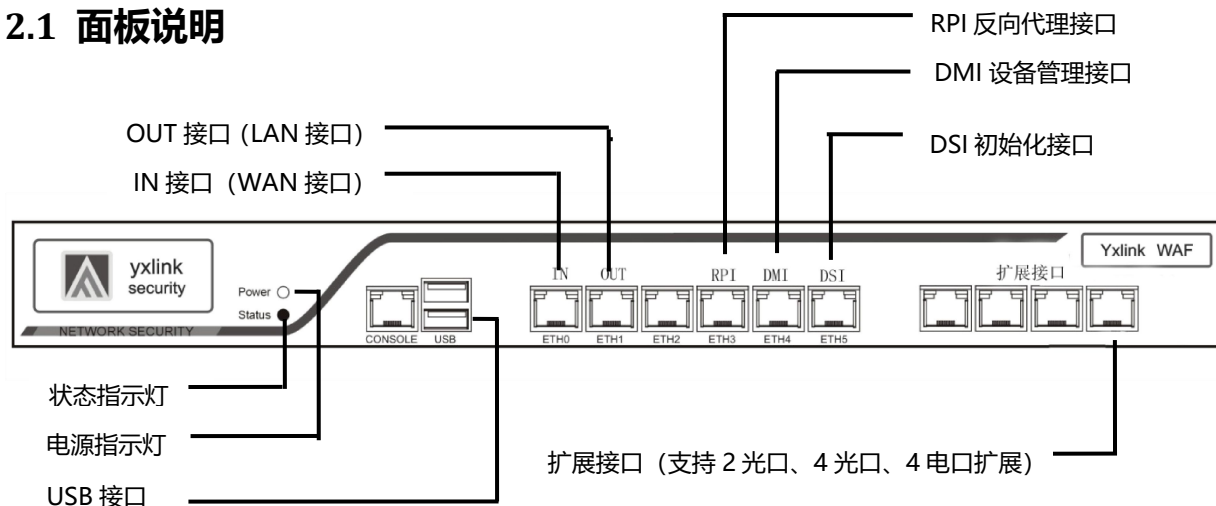
- 防扫描；
- Web 应用漏洞扫描（部分型号支持）；
- 细粒度的访问控制（部分型号支持）；
- 强大的防 CC 和抗 DDoS、DoS 攻击能力（部分型号支持）；
- 网页防篡改（部分型号支持）；
- 数据库防篡改（部分型号支持）；
- 自学习和 URL 模式（部分型号支持）；

性能及可靠性：

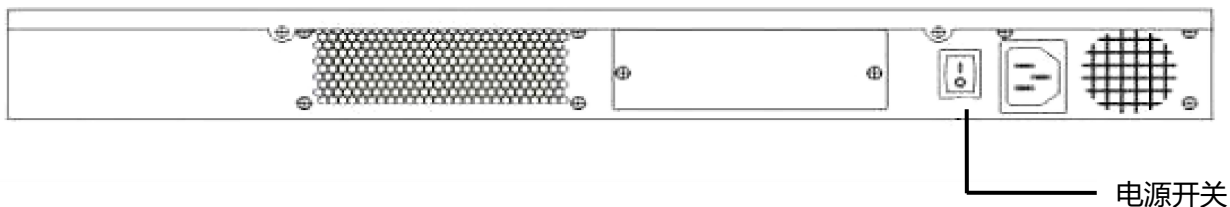
- 透明网桥模式，支持高并发连接数；
- 内置高性能解码、检测引擎；
- 支持复杂的网络环境：策略路由、VLAN 802.1Q、端口汇聚等；
- 具有硬件/软件 Bypass 功能，高可靠性 HA 架构（双机热备），保证业务稳定、长期运行；
- 完善的固件和规则升级功能，长期保证网络的安全；

2、产品规格

2.1 面板说明



面板



背板

2.1.1 接口说明



注意：DSI 接口自带 DHCP 功能，仅供直接连接计算机时使用。

切勿将其接入内部管理网络，否则会造成 DHCP 冲突。

序号	名称	说明
1	DSI 接口	设备初始化管理接口(Device Setting Interface)，直接连接计算机，供本设备初次启动时配置 DMI 接口的 IP 地址使用。在正常情况下，此接口无需连接任何网络。
2	WAN 接口	外部网络流量流入接口(WAN Interface)，也称 IN 接口。
3	LAN 接口	内部网络流量流出接口(LAN Interface)，也称 OUT 接口，连接内部设备。根据部署方式的不同，可以连接内部的 Web 服务器或交换机、路由器等网络设备。
4	DMI 接口	设备管理接口(Device Management Interface)，连接内部管理网络，管理员通过此接口登录本设备的 Web 管理页面进行日常管理工作。

5	RPI 接口	反向代理管理接口(Rreverse Proxy Interface), 连接内部的交换机。部分型号无此功能, 保留。
6	扩展接口	部分型号除了本身的基本接口外, 还可以扩展其他接口 (比如: 2 光口, 4 光口或 4 电口等)
7	电源指示灯	指示设备的电源状态, 熄灭表示断电状态。
8	状态指示灯	指示设备的磁盘读写状态。闪烁时表示正在读写磁盘。
9	USB 接口	USB 接口, 厂家检修专用。
10	电源开关	设备的电源开关。

3、安装部署

3.1 透明网桥模式

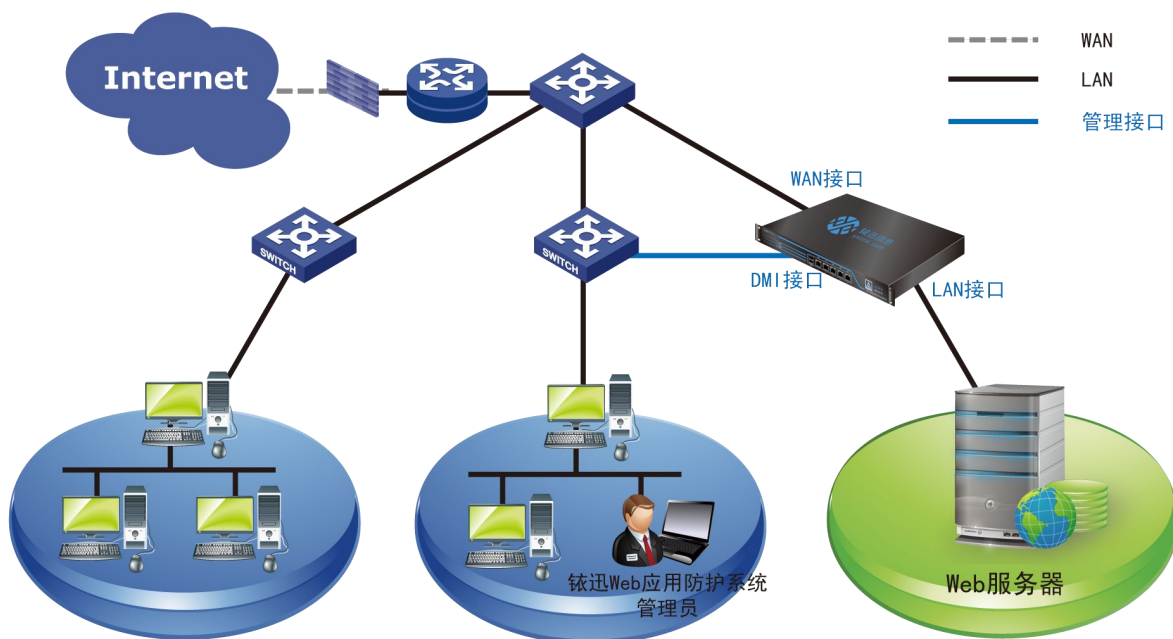
透明网桥模式指在两台运行的网络设备中间插入“钰迅 Web 应用防护系统（也称：钰迅 WEB 服务入侵防护系统）”，但是对流量并不产生影响。在透明网桥模式下，“钰迅 Web 应用防护系统”可以阻断、拦截来自 Web 应用层攻击，而让其他正常的流量通过。透明网桥部署模式的最大的特点是快速、简便，对于标准的 Web 应用（基于 80/8080 端口的 Web 应用），可做到即插即用，先部署后配置。

采用“钰迅 Web 应用防护系统（也称：钰迅 WEB 服务入侵防护系统）”透明网桥部署模式主要应用于如下五种场景：

- 单一混合型 Web 服务（Web 服务、数据库服务(以下简称 DB)在同一台服务器上)
- 单一分离式 Web 服务（Web 服务、DB 采用不同的服务器部署，但 Web 服务器只有一台)
- 集群式/集中式 Web 服务（采用集群方式的 Web 服务系统，或者多台 Web 服务器，但网络拓扑分布较为集中)
- 半分散式 Web 服务（Web 服务器分布在局域网的部分子网中)
- 全分散式 Web 服务（Web 服务器几乎分布在局域网的任何子网中)

3.1.1 单一混合型 Web 服务部署模式

单一混合型 Web 服务：采用一台服务器提供 Web 服务，并且该服务器同时提供数据库服务(DB)，这种情况主要适用于中小型企业的 Web 服务器模式。在这种网络拓扑结构下，可直接将“YXLink WAF”串接在服务器的前端，如下图显示：



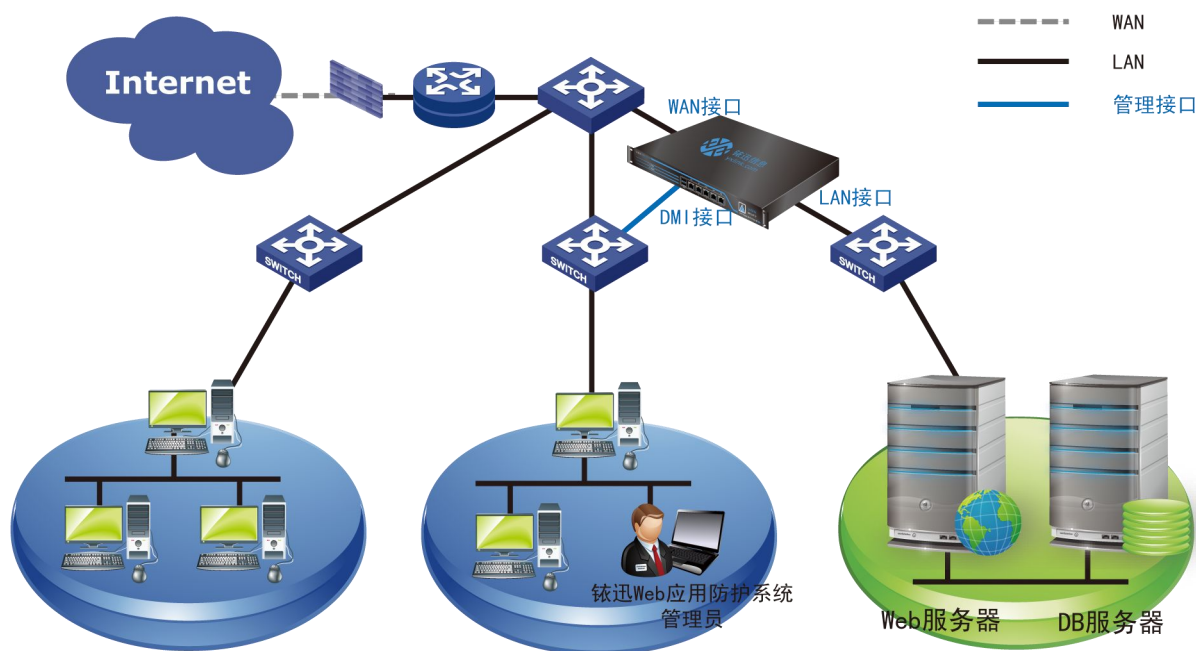
部署步骤如下：

1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 将原来接在 Web 服务器上的网线 A 从 Web 服务器上拔下；
5. 将拔下网线 A 连接在 “YXLink WAF” 的 WAF 接口；
6. 用网线连接 “YXLink WAF” 的 LAN 接口和 Web 服务器原网线 A 接插的网口上；
7. 此时，设备在硬件 Bypass 状态，再次确认 Web 服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；（如是 HA 部署方式，此时 Web 服务器无法访问）
8. 打开设备电源，等待约 120 秒；
9. 再次确认 Web 服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
11. 上述所有步骤完成后，请用网线将 “YXLink WAF” 的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.1.2 单一分离式 Web 服务部署模式

单一分离式 Web 服务：采用一台服务器提供 Web 服务，同时采用另一台服务器提供数据库服务，网站的 Web 服务和相关的数据库服务分布在不同的服务器上。这种情况主要适用于中小型企业的 Web 服务器模式。在这种网络拓扑结构下，可直接将 “YXLink WAF” 串接在 Web 服务器和 DB 服务器所在的交换机前端，如下图显示：



部署步骤如下：

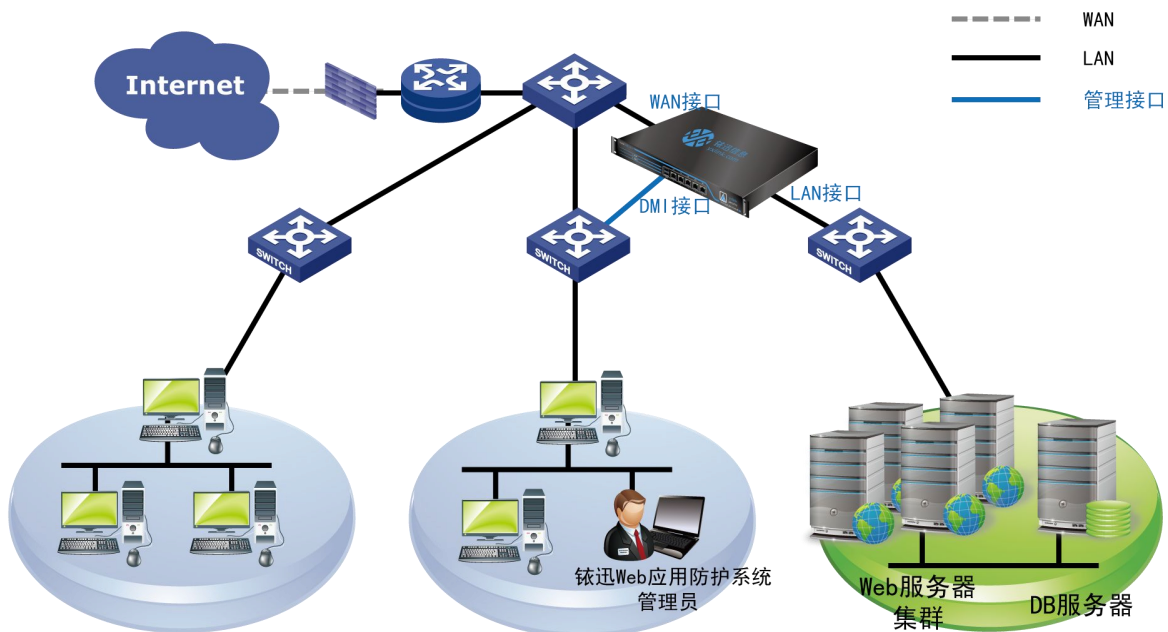
1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
5. 将拔下的网线连接在“YXLink WAF”的 WAN 接口；
6. 用网线连接“YXLink WAF”的 LAN 接口和交换机 B 的 UPLINK 网口；
7. 此时，设备在硬件 Bypass 状态，再次确认 Web 服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；（如是 HA 部署方式，此时 Web 服务器无法访问）
8. 打开设备电源，等待约 120 秒；
9. 再次确认 Web 服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
11. 上述所有步骤完成后，请用网线将“YXLink WAF”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.1.3 集群式/集中式 Web 服务部署模式

集群式/集中式 Web 服务：集群式 Web 服务采用多台 Web 服务器负荷分担提供同一 Web 服务；集中式 Web 服务主要体现在不同的 Web 服务器放置在同一网段或者相邻的网段内，但不同的 Web 服务器可能提供

多样的 Web 服务。这种情况多数应用于大中型企业的 Web 服务器模式，或者是 IDC 机房。在这种网络结构下，可直接将“YXLink WAF”串接在 Web 服务器群所在子网交换机前端，如下图显示：



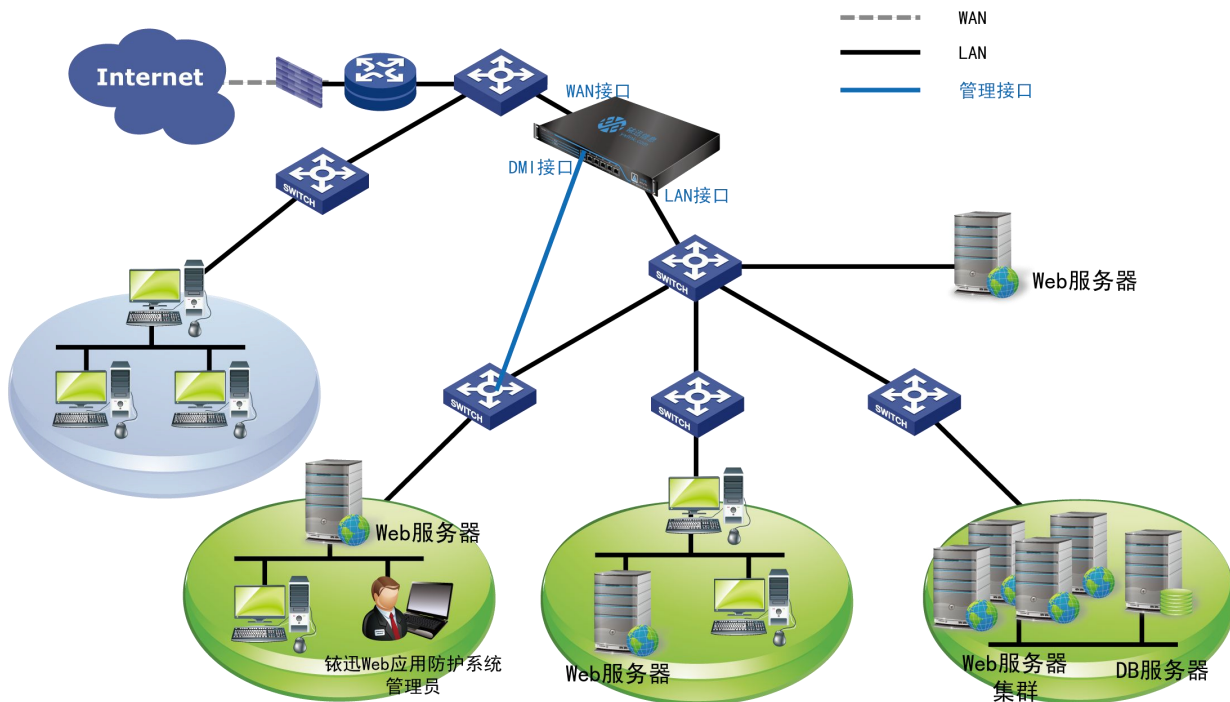
部署步骤如下：

1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
5. 将拔下的网线连接在“YXLink WAF”的 WAN 接口；
6. 用网线连接“YXLink WAF”的 LAN 接口和交换机 B 的 UPLINK 网口；
7. 此时，设备在硬件 Bypass 状态，再次确认 Web 服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；（如是 HA 部署方式，此时 Web 服务器无法访问）
8. 打开设备电源，等待约 120 秒；
9. 再次确认 Web 服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
11. 上述所有步骤完成后，请用网线将“YXLink WAF”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.1.4 半分散式 Web 服务部署模式

半分散式 Web 服务：在局域网中存在各种不同的 Web 应用服务，并且这些 Web 应用服务器分散在不同的子网中。比如：公司有整体的 Web 服务集群，同时，各个部门还有各自的 Web 服务器，而这些服务器分布在不同的子网中，如果需要对这些 Web 服务器进行保护，需要将“YXLink WAF”部署在这些 Web 服务器所在网络的边缘，如下图显示：



部署步骤如下：

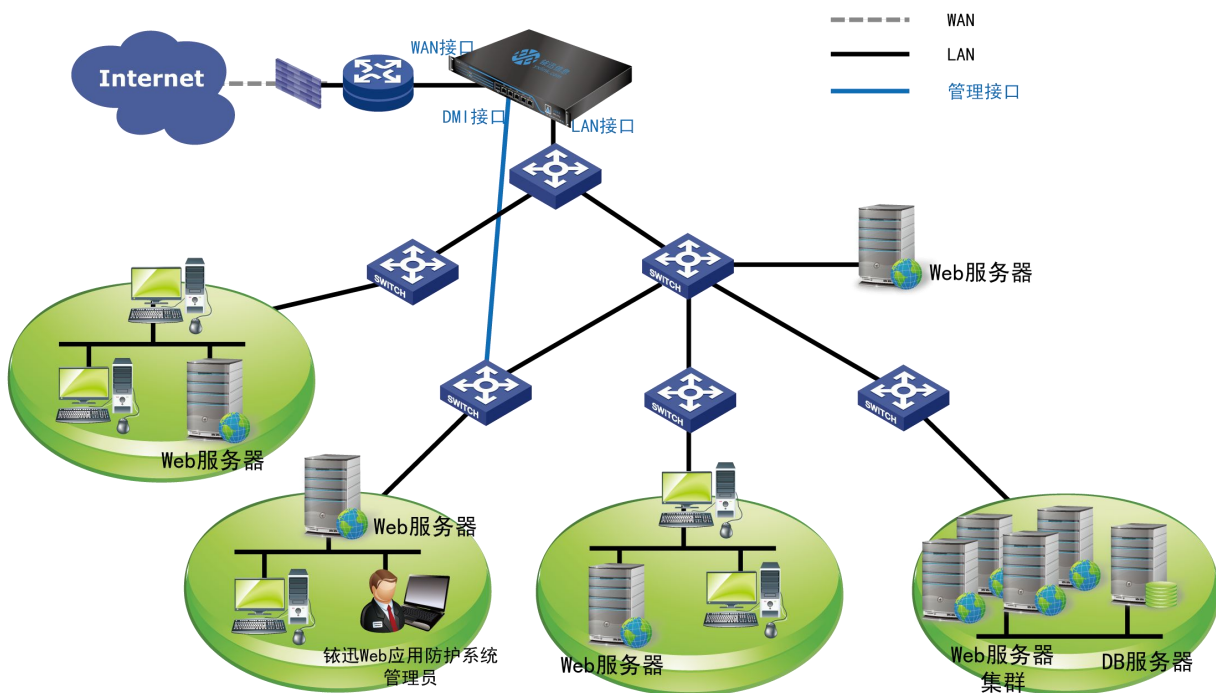
1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
5. 将拔下的网线连接在“YXLink WAF”的 WAN 接口；
6. 用网线连接“YXLink WAF”的 LAN 接口和交换机 B 的 UPLINK 网口；
7. 此时，设备在硬件 Bypass 状态，再次确认 Web 服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；（如是 HA 部署方式，此时 Web 服务器无法访问）
8. 打开设备电源，等待约 120 秒；
9. 再次确认 Web 服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；

11. 上述所有步骤完成后, 请用网线将“YXLink WAF”的 DSI 接口同一台普通的台式机网口直接连接(请勿通过局域网进行连接, DSI 带有 DHCP 功能, 可能会同您的网络环境中的其他 DHCP 设备产生冲突, 导致部分网络不可用);

请参考后续章节继续配置设备。

3.1.5 全分散式 Web 服务部署模式

全分散式 Web 服务: 在局域网中存在各种不同的 Web 应用服务, 并且这些 Web 应用服务器分散在几乎全部的子网中, 比较常见的案例: IDC 机房。此时, 需要将“YXLink WAF”部署在局域网边缘, 一般部署在主交换机同主路由器之间, 如下图显示:



部署步骤如下:

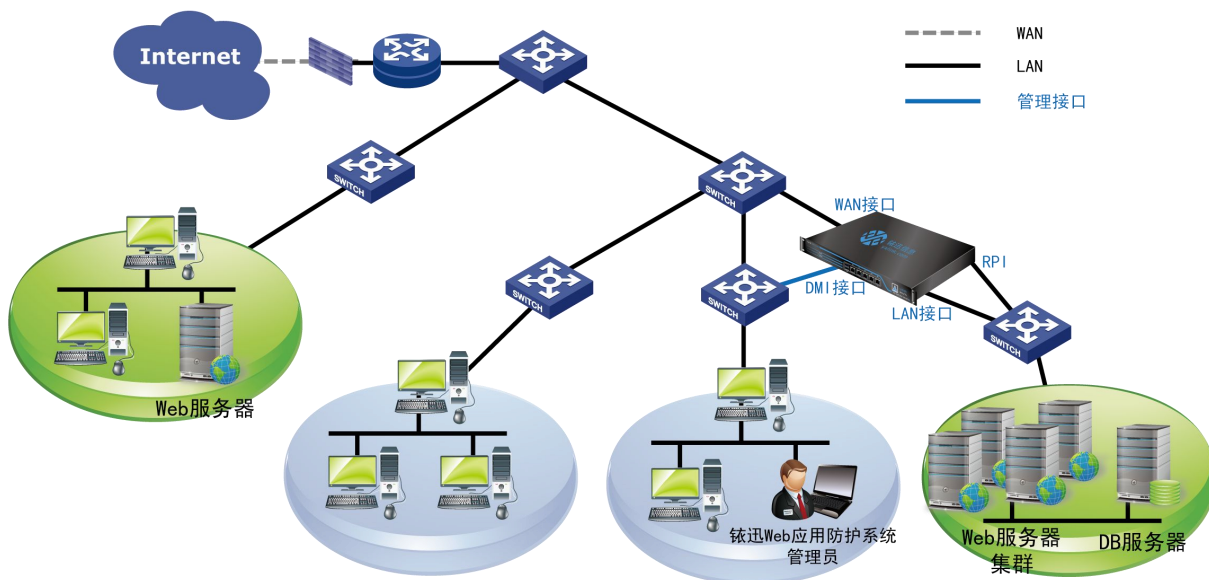
1. 在机架上选择合适的位置正确安装设备;
2. 确认设备处于断电状态;
3. 确认 Web 服务器处于正常工作状态 (从 Internet 可正常访问 Web 服务), 如工作异常, 请与 Web 服务器管理员联系, 工作正常后, 继续下一步;
4. 将原来连接在主路由器和主交换机的网线从交换机上拔下;
5. 将拔下的网线连接在“YXLink WAF”的 WAN 接口;
6. 用网线连接“YXLink WAF”的 LAN 接口和主交换机的 UPLINK 网口;
7. 此时, 设备在硬件 Bypass 状态, 再次确认 Web 服务器是否能够正常访问, 如工作状态异常, 请检查前面步骤插接的网线是否接触良好; (如是 HA 部署方式, 此时 Web 服务器无法访问)
8. 打开设备电源, 等待约 120 秒;
9. 再次确认 Web 服务器是否能够正常访问, 如工作状态异常, 请同技术服务人员联系;

10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
11. 上述所有步骤完成后，请用网线将“YXLink WAF”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.2 混合部署模式

混合部署模式：透明网桥模式和旁路反向代理模式混合的部署方式。这种方式具有部署简便，配置较为容易等特点，特别适用于具有中心机房，但同时在不同的地点分散着个别 Web 服务器的情况，设备部署位置一般同“集群式/集中式 Web 服务”，是半分散和全分散服务部署模式的替代部署模式，为管理员提供了更加人性化的管理方式。具体部署如图：



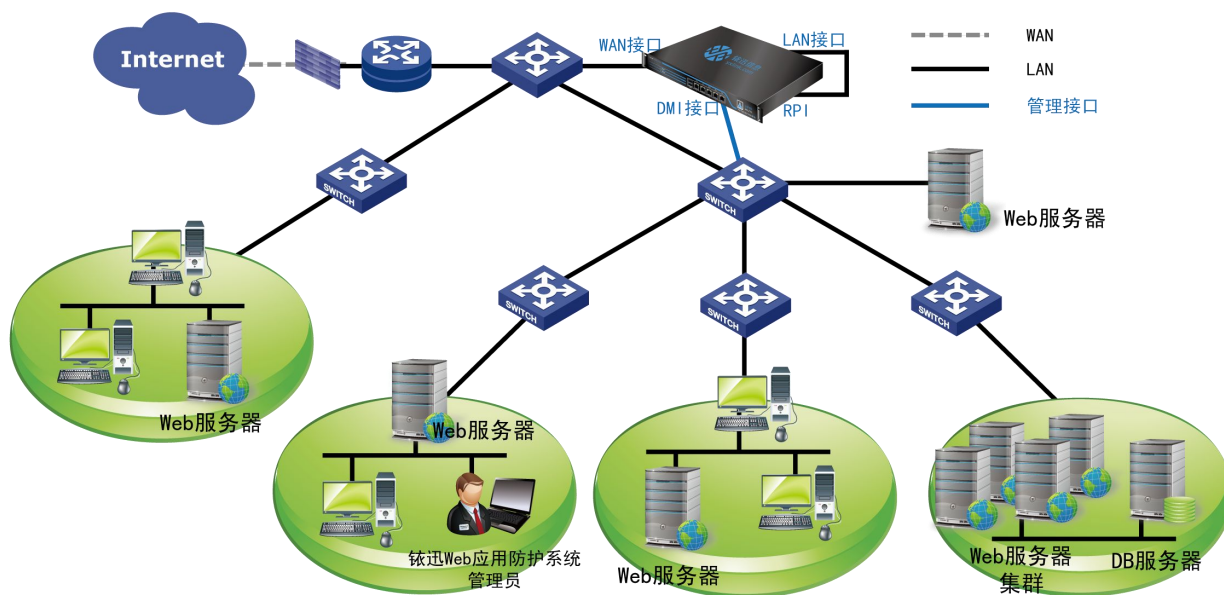
部署步骤如下：

1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
5. 将拔下的网线连接在“YXLink WAF”的 WAN 接口；
6. 用网线连接“YXLink WAF”的 LAN 接口和交换机 B 的 UPLINK 网口；
7. 此时，设备在硬件 Bypass 状态，再次确认 Web 服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；（如是 HA 部署方式，此时 Web 服务器无法访问）
8. 打开设备电源，等待约 120 秒；

- 请参考后续章节继续配置设备。

3.3 混合加密部署模式

混合加密部署模式：混合部署模式的增强形式，支持 HTTP/HTTPS。这种部署方式的特点与混合部署模式基本相同。它的工作原理是将原来由 Web 服务器完成的 SSL 加密、解密工作，现在交给“YXLink WAF”来完成，即“YXLink WAF”执行 SSL 加密、解密工作，因此需要将原来 Web 服务器上的 SSL 证书导入到“YXLink WAF”中，同时将 Web 服务器上的 HTTP 服务端口开启，比如 80 端口。具体部署如图：



部署步骤如下:

1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
5. 将拔下的网线连接在“YXLink WAF”的 WAN 接口；
6. 用网线连接“YXLink WAF”的 LAN 接口和交换机 B 的 UPLINK 网口；

7. 此时，设备在硬件 Bypass 状态，再次确认 Web 服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；（如是 HA 部署方式，此时 Web 服务器无法访问）
8. 打开设备电源，等待约 120 秒；
9. 再次确认 Web 服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 RPI 接口同交换机 A 的千兆网口相连；
11. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
12. 上述所有步骤完成后，请用网线将“YXLink WAF”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

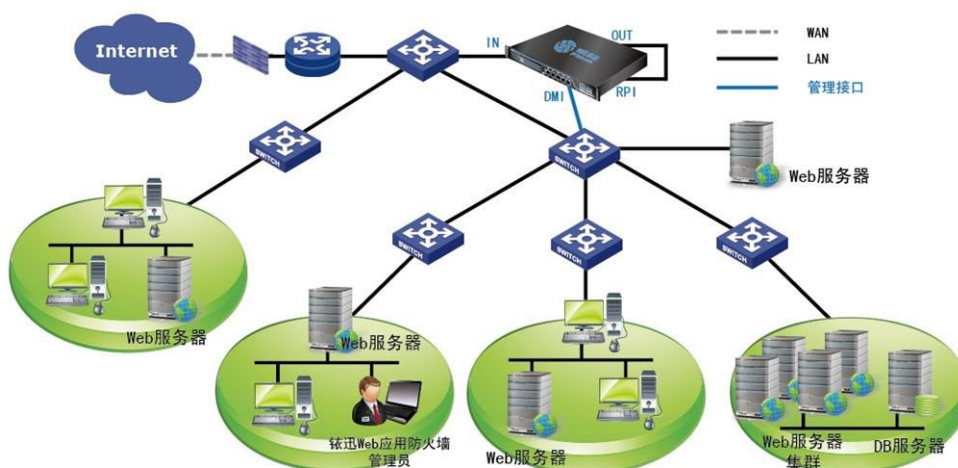


注意：

混合加密部署模式只在特定型号的设备上可用，要了解您购买的型号上是否支持此功能，请咨询供货商或者联系铱讯客服人员。

3.4 旁路反向代理模式

旁路反向代理模式：将银讯 Web 应用防护系统（也称，银讯 WEB 服务入侵防护系统）与 Web 服务器置于内网的交换机下，访问 Web 服务器的所有请求都通过“YXLink WAF”流入流出。然而，这种模式下，Web 服务器无法获取访问者的真实 IP 地址，需要借助 HTTP 报文中设置相应的字段来表示访问者 IP 地址，这样需要修改原有的 HTTP 报文。同时这种模式下将无法开启 Bypass 功能，因此除非在迫不得已的情况下，请谨慎使用旁路反向代理模式部署，推荐使用透明网桥的部署方式。旁路反向代理模式具体部署图如下：



部署步骤如下:

1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；

3. 确认 Web 服务器处于正常工作状态（局域网内的其他机器可正常访问 Web 服务），如工作异常，请与 Web 服务器管理员联系，工作正常后，继续下一步；
4. 用网线连接在“YXLink WAF”的 WAN 接口到主交换机；
5. 用网线连接“YXLink WAF”的 LAN 接口和 RPI 接口；
6. 打开设备电源，等待约 120 秒；
7. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
8. 上述所有步骤完成后，请用网线将“YXLink WAF”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。



注意：

旁路反向代理模式只在特定型号的设备上可用，要了解您购买的型号上是否支持此功能，请咨询供货商或者联系依迅客服人员。

4、安装及初始化

4.1 打开包装箱

对照物品清单检查物品，如果发现有所损坏或者任何配件短缺的情况，请及时和供货商联系。

4.2 安装设备

请使用附件箱中的耳片和螺钉将设备固定在机架上。

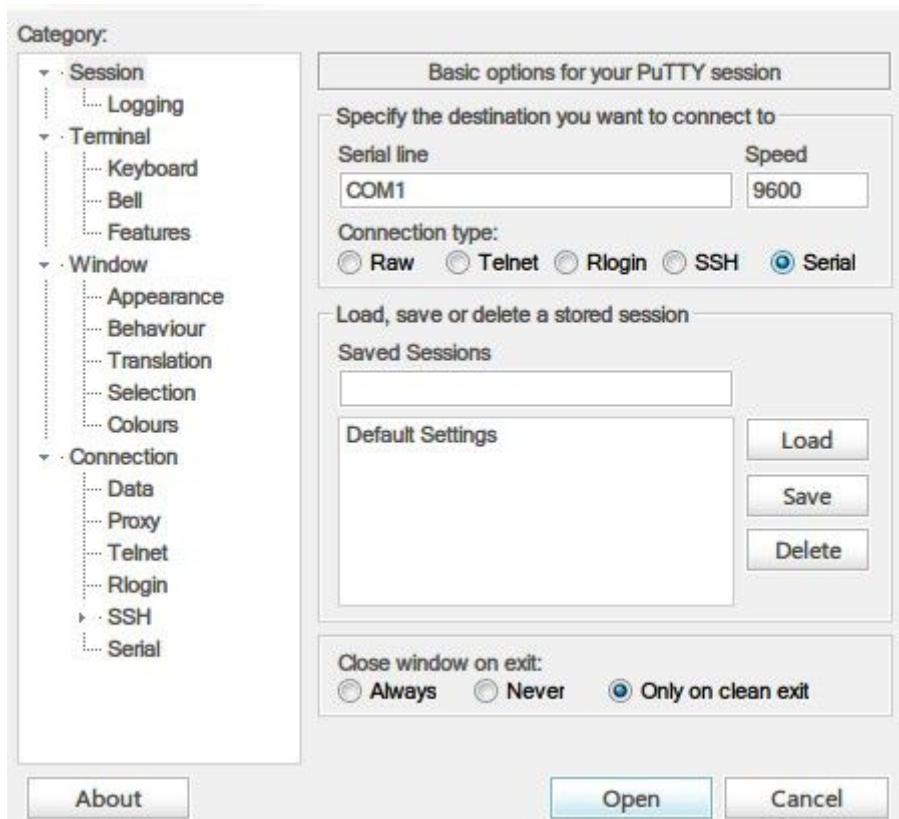
4.3 选择部署方案

参考[安装部署](#)，选择适合自己网络拓扑结构的部署方式。

4.4 初始化设备

4.4.1 连接设备的 Console 口

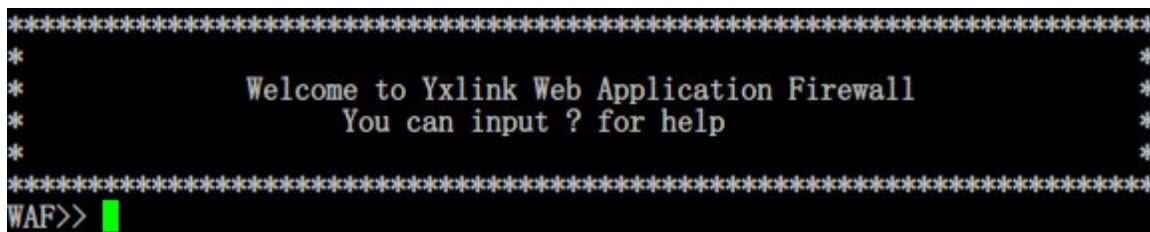
1. 用 Console 线连接 PC 机和防火墙；
2. Console 线串口一端连接 PC 机串口，另一端连接设备的 Console 口；
3. 运行支持 COM 口通讯的软件（如 PuTTY、超级终端等）连接设备，连接状态选择“串口”，波特率设置为 9600；



注意：

每台 PC 机的 COM 口设备编号可能不一样，请选择正确的 COM 口设备编号进行连接。

4. 设置好参数，点击【Open】按钮连接，输入用户名 conadmin，密码 conadmin 登陆系统，进入欢迎界面；



4.4.2 连接设备的 DSI 接口

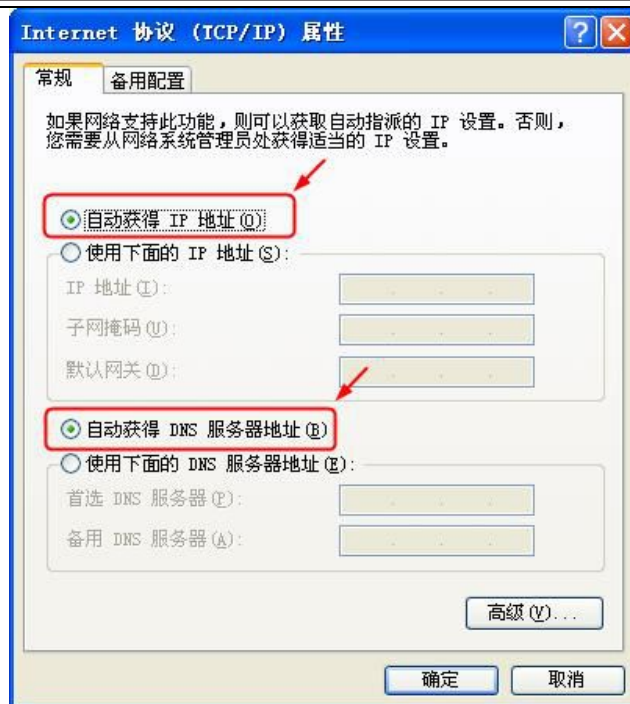
使用网线将一台计算机直接连接至本设备的 DSI 接口，（请参考[面板说明](#)）将该计算机设置为“自动获得 IP 地址”，而不要设置静态 IP 地址。

在 Microsoft Windows XP 下设置“自动获得 IP 地址”的方法如下：

- (1) 【开始】→【控制面板】→【网络连接】；
- (2) 在“本地连接”图标上点击右键，然后点击弹出的【属性】菜单。如图；
- (3) 在弹出的“本地连接 属性”对话框中选中“Internet 协议 (TCP/IP)”，然后点击【属性】；



- (4) 在弹出的“Internet 协议 (TCP/IP) 属性”对话框中，选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”，然后点击【确定】；



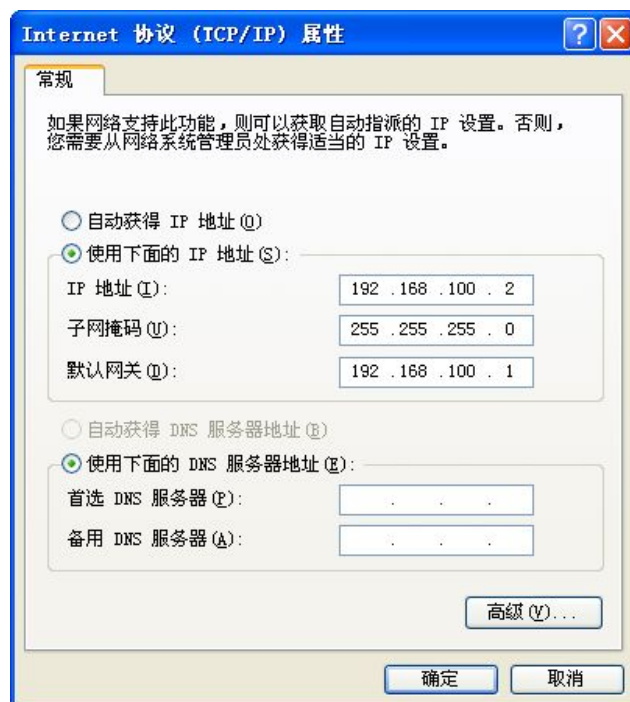
(5) 等待并确认您的计算机通过 DHCP 获得了真实有效的 IP 地址, IP 地址应为 192.168.100.xx。

提示:

如果通过步骤 (4) “自动获得 IP 地址” 无法自动获得有效的 IP 地址。

您也可以手工指定计算机的静态 IP 地址。

静态 IP 地址的设置参数如下:

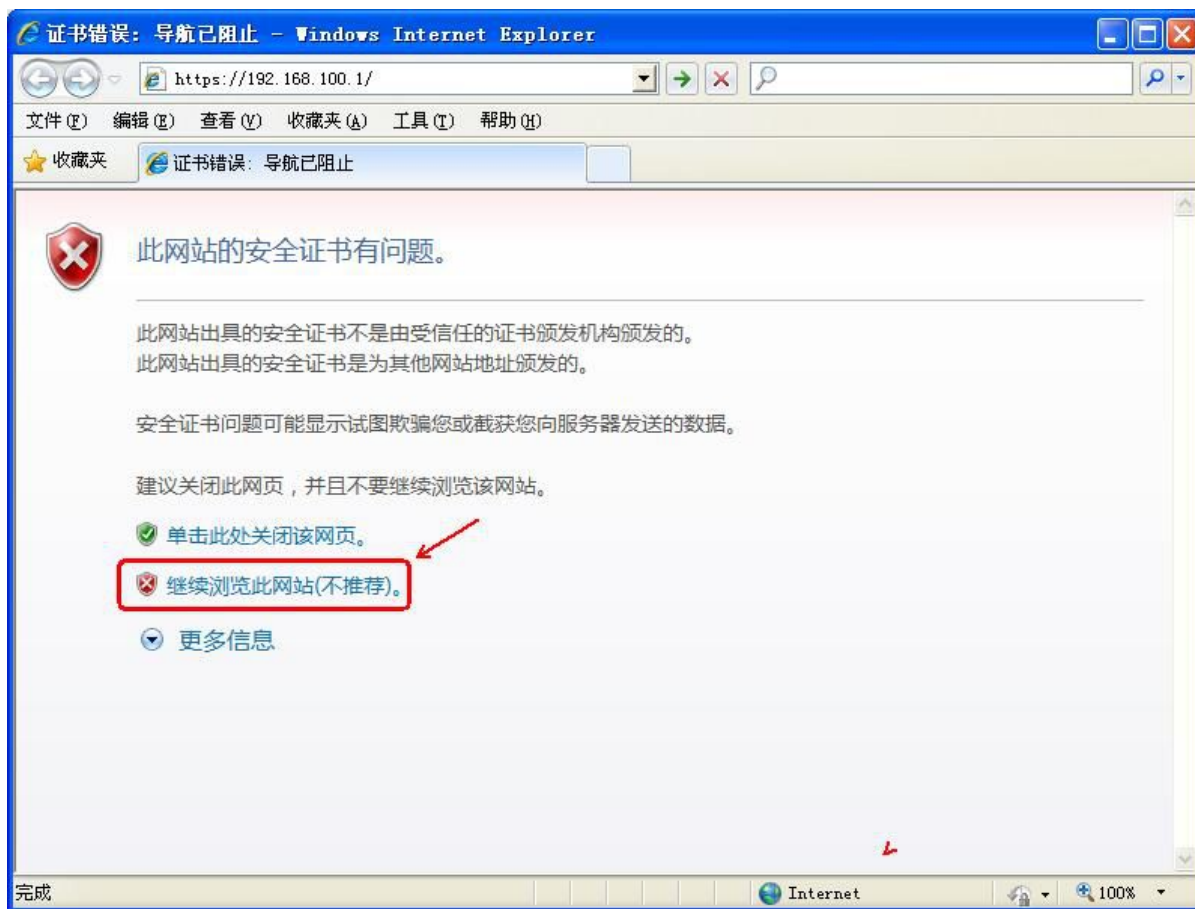


4.4.3 配置 DMI 接口网络参数

假设您已经将计算机连接至本设备的 DSI 接口, 并且通过 DSI 接口使您的计算机自动获得了 IP 地址。

下面介绍配置 DMI 接口网络参数的操作方法:

(1) 使用浏览器访问 <https://192.168.100.1>，浏览器可能会提示“此网站的安全证书有问题”，如图。



i 提示:

如果无法访问该网址，请检查计算机的防火墙设置，需要打开 443 端口才能访问此网址。

(2) 点击“继续浏览此网站（不推荐）”，然后显示系统登录页面，如图。



(3) 输入用户名和密码（设备初始用户名和密码请参看附录 A），点击【登录】按钮，进入“铱迅 Web 应用防护系统”欢迎界面。

⚠ 注意:

如果登录失败，请检查是否为以下原因引起:

- 1) 用户名输入错误;
- 2) 密码输入错误;
- 3) 没区分大小写。

如果某用户连续登录失败超过设定的次数（缺省为 3 次），则该用户将被锁定 15 分钟，15 分钟后该用户自动解锁。

建议使用 Microsoft Internet Explorer 8.0 及以上版本的浏览器，屏幕分辨率最好设置为 1024×768 及以上。

(4) 点击【网络配置】→【网络接口】，然后双击接口属性为“DMI”的网络接口进行配置（以下简称 DMI 接口，即设备管理接口），具体参数请根据内部管理网络的实际情况设置，配置完成后需要在“静态路由”配置相对应的默认网关地址。（配置方式详见[修改默认路由](#)）

物理接口 - 修改

接口名称: ETH4

是否启用: ☒ 启用 ☐ 停用

连接状态: 已连接

双工: 全双工

速度: 1000 Mbps

MAC地址: 4c:cc:6a:87:41:c0

工作方式: ☒ 普通模式 ☐ 透明网桥 ☐ 策略路由 ☐ 端口汇聚

IP地址: 192.168.5.51

子网掩码: 255.255.255.0

网关: 192.168.5.1

IPv6地址: 请填写IPv6地址

IPv6前缀: 请填写IPv6前缀

IPv6网关: 请填写IPv6网关

更多选项:
☒ DMI - 设备管理接口, 通过该接口访问设备的管理页面
☒ RPI - 反向代理接口, 该接口对外提供代理内部Web服务器 (HTTP) 的代理服务
☐ RPI2 - 反向代理接口, 该接口对外提供代理内部Web服务器的双向HTTPS代理服务

✓ 保存

↻ 刷新

✕ 取消

注意：

请联系网络管理员，以便获取正确的网络设置参数。

提示：

如果网络配置失败（包括 IP 地址填写错误，网关、DNS 配置错误等），从而无法访问设置好的网络接口的 IP 地址，请重新配置或者执行产品复位。

提示：

如果 DMI 接口的 IP 地址无法访问，请检查：

1. 确认部署环境中是否有防火墙，该防火墙中是否针对该 IP 地址进行了一些访问控制的限制；
(比如：设置了 MAC 地址绑定。)
2. 确认该 IP 地址是否已经被别的主机占用。

5、快速使用指南

5.1 修改密码

系统管理员登录“依迅 Web 应用防护系统”后，点击左边菜单栏【配置】→【用户设置】，选择 webadmin 用户，点击【修改】，重新设置密码。密码长度应该大于或等于设定的长度，且至少包含数字、大小写字母、特殊字符等。

- 系统管理员可以修改所有安全管理员和用户的密码；
- 安全审计员可以修改安全审计员的密码；
- 每个用户都可以修改自己的密码。点击右上角“欢迎您：某用户”，系统弹出该用户的密码修改对话框，如下图所示。



密码修改对话框，标题为“密码修改”，右上角有关闭按钮。对话框内显示“当前用户: webadmin”，下方有三个输入框，分别标注为“当前密码:”、“新密码:”和“新密码确认:”。底部有两个按钮，分别为“保存”和“取消”。

⚠ 注意：

出于安全的考虑，强烈建议您在初次使用时修改管理员密码。

5.2 设置检测端口

登录“依迅 Web 应用防护系统”后，点击菜单栏【防护设置】→【基本参数设置】，在“防护系统检测端口”中设置您要检测的端口，默认为“80|8080”。



检测端口设置：（指定要检测的端口，例如80端口，如有多个请用|隔开。）

*检测端口: 80|8080

💡 提示：

本设备将防护所有连接在 LAN 接口的服务器上的 Web 应用（例如 Apache, IIS 等）。因此，请将所有需要防护的 Web 应用的端口在此填写完整。如有多个端口，可以使用“|”隔开，例如填写“80|8080”。

5.3 查看系统状态

点击左侧菜单栏【布局】，在弹出的子菜单中点击【基本信息】，然后分别点击【系统状态】、【设备信息】和【系统日志】。在显示出的页面中可以分别查看当前设备的系统状态（CPU、内存和磁盘的使用情况），系统日志，设备信息，授权信息等。具体详见下面各小节。

5.3.1 系统状态

用于显示设备的当前系统状态，如图。



系统日志

操作时间	日志内容
2017-09-12 17:41:09	检测引擎启动
2017-09-11 14:20:29	从上次记录此信息以来, 累计入侵记录数超过5000
2017-09-11 14:18:16	从上次记录此信息以来, 累计入侵记录数超过5000
2017-09-11 14:02:06	从上次记录此信息以来, 累计入侵记录数超过5000
2017-09-11 13:57:14	发送入侵记录Email报警失败, 名称为: Yxlink WAF: high risk invasion alarm - 2017-09-1...
2017-09-06 17:54:04	检测引擎重启
2017-09-06 17:51:17	检测引擎重启
2017-09-06 17:50:02	检测引擎重启
2017-09-06 17:49:58	检测引擎重启
2017-09-06 17:49:28	检测引擎重启

- CPU：显示当前设备的 CPU 使用情况。
- 内存：显示当前设备的内存使用情况。
- 磁盘：显示当前设备的磁盘使用情况。当磁盘空间不足时，会向管理员发送邮件提醒，并且会自动清理磁盘。如果需要手动清理磁盘，请参考[磁盘日志清理](#)。
- 设备信息：显示当前客户名称，授权状态，有效期以及系统版本，规则版本。
- 系统日志：显示当前的操作信息。

5.3.2 威胁视图

点击左边菜单栏【布局】，在弹出的子菜单中点击【威胁视图】，然后分别点击【风险等级】、【访问记录】，【入侵记录】，【当日入侵统计】，【入侵类别 Top10】和【拦截原因 TOP10】。在显示出的页面中可以分别查看当前设备的相应状态等。具体详见下面各小节。

风险等级



入侵总数: 0

访问记录



网址	访问次数	最后访问IP	地理位置	浏览器类型	最后访问时间
没有记录					

入侵记录

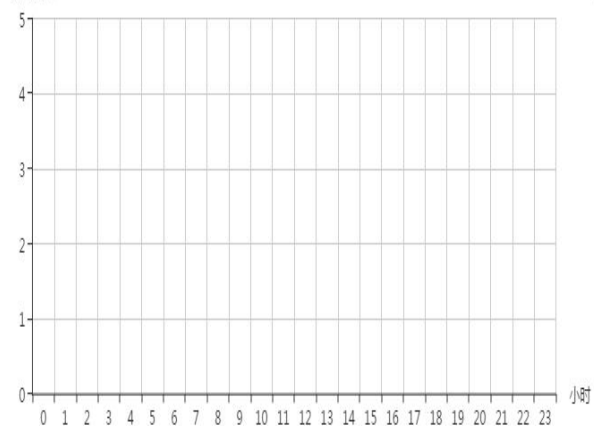


攻击时间	规则集名称	源IP地址	地理位置	拦截方式
没有记录				

当日入侵统计



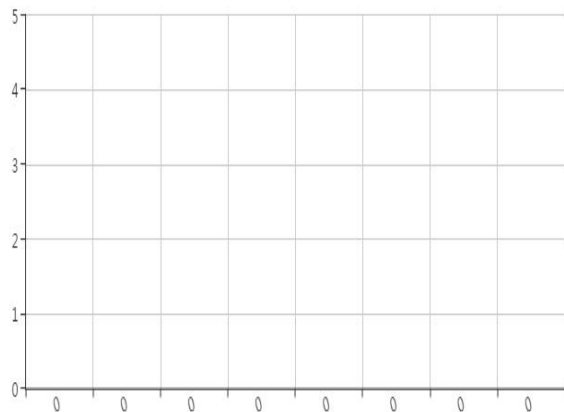
入侵次数



入侵类别Top10



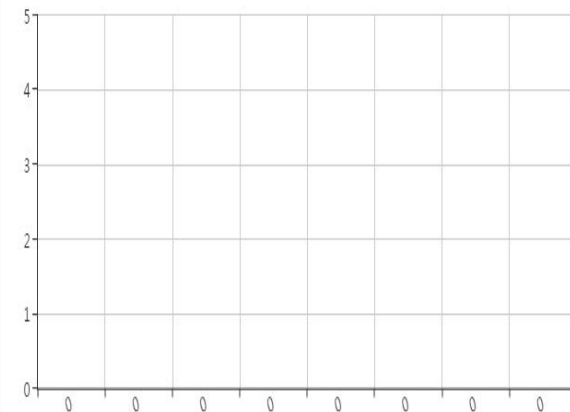
入侵次数



拦截原因Top10



拦截次数



- 分险等级：显示当前风险等级，以及当日的入侵总数。
- 当日入侵统计：显示当天的每小时的入侵统计信息。
- 入侵类别统计：显示当前拦截的入侵类别的统计信息。
- 拦截原因统计：显示当前的拦截原因的统计信息。

5.3.3 网络状态

点击左边菜单栏【布局】，在弹出的子菜单中点击【网络状态】，然后分别点击【网络接口】、【实时流量】。在显示出的页面中可以分别查看当前设备的相应状态等。具体详见下面各小节。

网络接口						
接口名称	IP地址	子网掩码	网关/下一跳地...	所属网桥	连接状态	接口属性
ETH0	192.168.100.1	255.255.255.0	*		已断开	DSI
ETH1	192.168.99.51	255.255.255.0	192.168.99.1		已连接	DMI
ETH2	192.168.1.11	255.255.255.0	192.168.1.1		已断开	RPI
ETH3					已断开	
ETH4				wafprotect	已断开	WAN
ETH5				wafprotect	已断开	LAN

实时流量							
网络接口	模式	速率	连接状态	收到的字节	发送的字节	接收速率	发送速率
ETH0	自动	自动	已断开	0B	0B	0	0
ETH1	全双工	1000 Mbps	已连接	145.47MB	31.96MB	9880	1496
ETH2	自动	自动	已断开	0B	0B	0	0
ETH3	自动	自动	已断开	0B	0B	0	0
ETH4	自动	自动	已断开	0B	0B	0	0
ETH5	自动	自动	已断开	0B	0B	0	0

- 网络接口：用于显示各个接口的 IP 地址和连接状态。
- 实时流量：用于显示各个网络接口的实时流量信息。

提示:

本设备会尽可能多的使用内存以便提高性能, 因此内存占用较大(超过 80%)是正常现象。

5.4 查看入侵记录

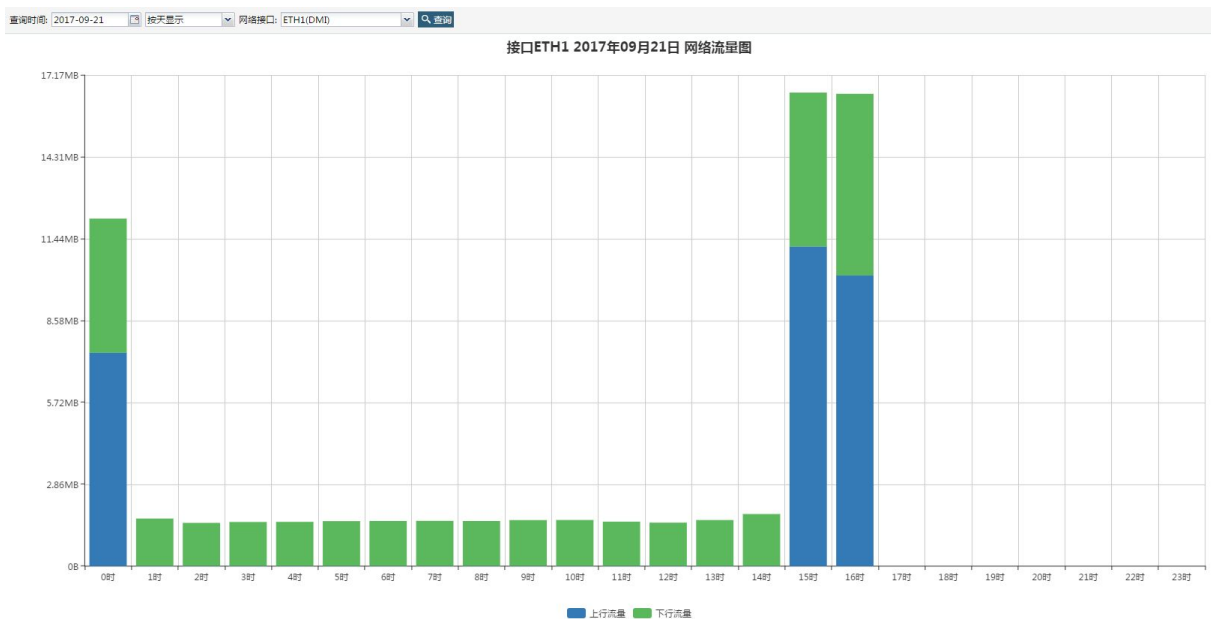
点击菜单栏【数据中心】, 点击左边菜单栏【威胁监控】→【入侵记录】, 可以查看入侵的记录。

序号	最后时间	规则编号	规则名称	危害...	源IP地址	地理位置	目的IP地址	源端...	目的...	拦截...	HTT...	次数	URL	操作
288	2017-09-21 17...	1410001	访问/读取/包含关键文件	中	192.168.99.51	LAN		247...	80	拦截	GET	13		
287	2017-09-21 17...	1310020	可疑的文件包含	低	192.168.99.51	LAN		247...	80	检测	GET	7		
283	2017-09-21 17...	1400002	XSS跨站	低	192.168.99.51	LAN		246...	80	拦截	GET	14		
269	2017-09-21 17...	1400001	下载关键文件	中	192.168.99.51	LAN		245...	80	拦截	GET	1		
268	2017-09-21 17...	1200001	SQL注入(AND/OR/XOR/HA...	低	192.168.99.51	LAN		245...	80	拦截	GET	1		
253	2017-09-21 16...	1200002	SQL注入单引号	低	192.168.99.51	LAN		223...	80	拦截	GET	4		
251	2017-09-21 16...	1200012	SQL注入(AND/OR/XOR) v3	低	192.168.99.51	LAN		223...	80	拦截	GET	4		
244	2017-09-21 16...	1410001	访问/读取/包含关键文件	中	192.168.99.51	LAN		115...	80	拦截	GET	9		
241	2017-09-21 16...	1310020	可疑的文件包含	低	192.168.99.51	LAN		115...	80	检测	GET	2		
237	2017-09-21 16...	1400002	XSS跨站	低	192.168.99.51	LAN		114...	80	拦截	GET	190		
232	2017-09-21 16...	1400006	XSS跨站(expression等关键字)	低	192.168.99.51	LAN		114...	80	拦截	GET	35		
10	2017-09-21 16...	1400001	下载关键文件	中	192.168.99.51	LAN		102...	80	拦截	GET	2		
6	2017-09-21 16...	1200002	SQL注入单引号	低	192.168.99.51	LAN		101...	80	拦截	GET	2		
4	2017-09-21 16...	1200012	SQL注入(AND/OR/XOR) v3	低	192.168.99.51	LAN		101...	80	拦截	GET	2		
2	2017-09-21 16...	1620002	phpinfo信息泄露	中	192.168.99.51	LAN		101...	80	拦截	Res...	2		

您可以选择日期查看某天的入侵记录, 也可以选择左边菜单栏的【入侵统计】查看入侵记录的统计信息。详细操作请参考《钰迅 Web 应用防护系统管理员手册》。

5.5 查看网络流量

点击左边菜单栏【网络流量】, 可以按天或者按月以折线图的形式显示某块网卡的网络流量变化趋势。



5.6 关机和重启

点击上方菜单栏【系统维护】，点击左边菜单栏【关机/重启】，在【重启】页面中可以选择“关机”和“重启”。

重新启动

点击“关机”按钮关闭本设备，点击“重启”按钮重启本设备：

 关机 重启

注意：

请您尽量避免在本设备运行的时候直接切断电源。这样可能造成数据的丢失或影响设备的使用寿命。

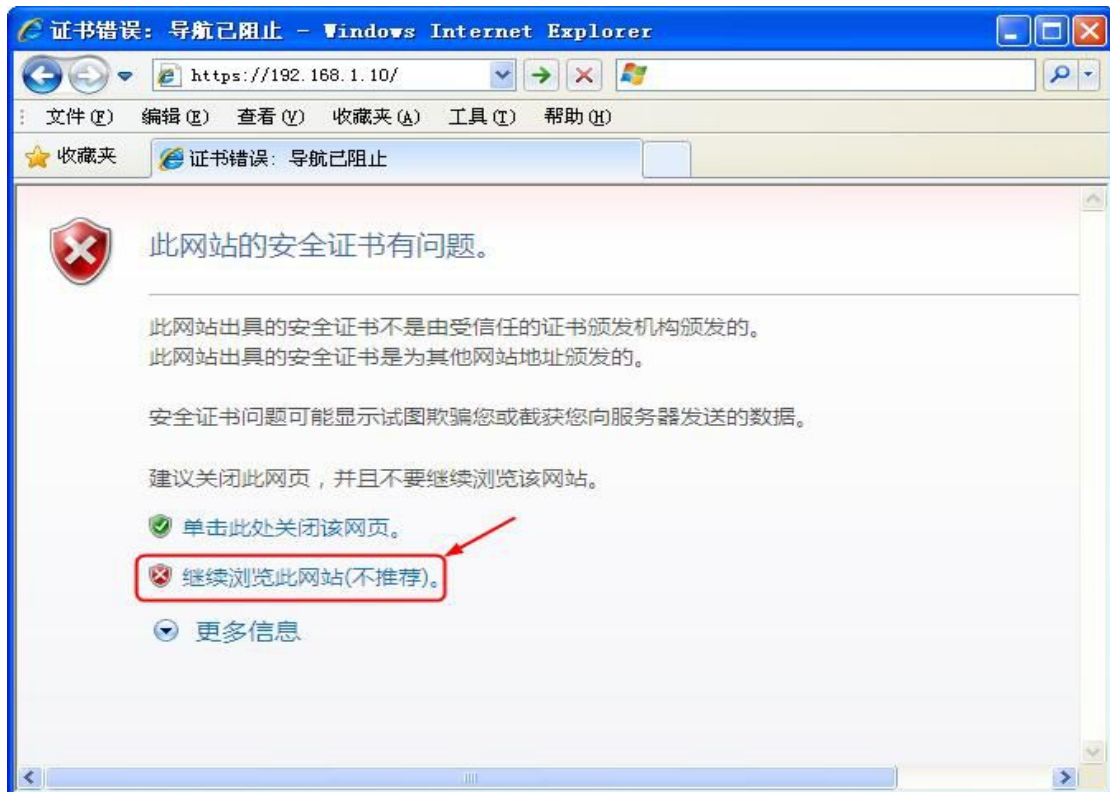
在您点击【关机】按钮，或者直接按下设备上的电源按钮后，请等待设备电源指示灯熄灭后再切断电源。设备安全关闭需要一定时间。

6、开始使用

6.1 登录

6.1.1 登录系统

在浏览器中输入您已经配置好的本设备 DMI 接口的访问地址（如：<https://192.168.1.10/>）后按回车（Enter）键，浏览器可能会提示“此网站的安全证书有问题”，如图。



点击“继续浏览此网站（不推荐）”，然后显示系统登录界面，如图。输入正确的用户名和密码，点击【登录】按钮即可登录到本设备进行操作。

提示：

如果是首次安装并使用本设备，请先仔细阅读[设备安装及初始化](#)相关章节。

关于如何配置本设备 DMI 接口的 IP 地址，具体请参考[设备安装及初始化](#)的相关章节。

出厂的默认用户名和密码请参考[附录 A](#)。

**i** 提示:

为了获得最佳的页面浏览效果,建议您使用 Microsoft Internet Explorer 8.0 及以上版本的浏览器,推荐显示分辨率 1024×768 以上。

**注意:**

如果连续登录失败的次数超过设定值(缺省为 3 次),则该用户将被锁定 15 分钟。15 分钟内不允许该用户登录。

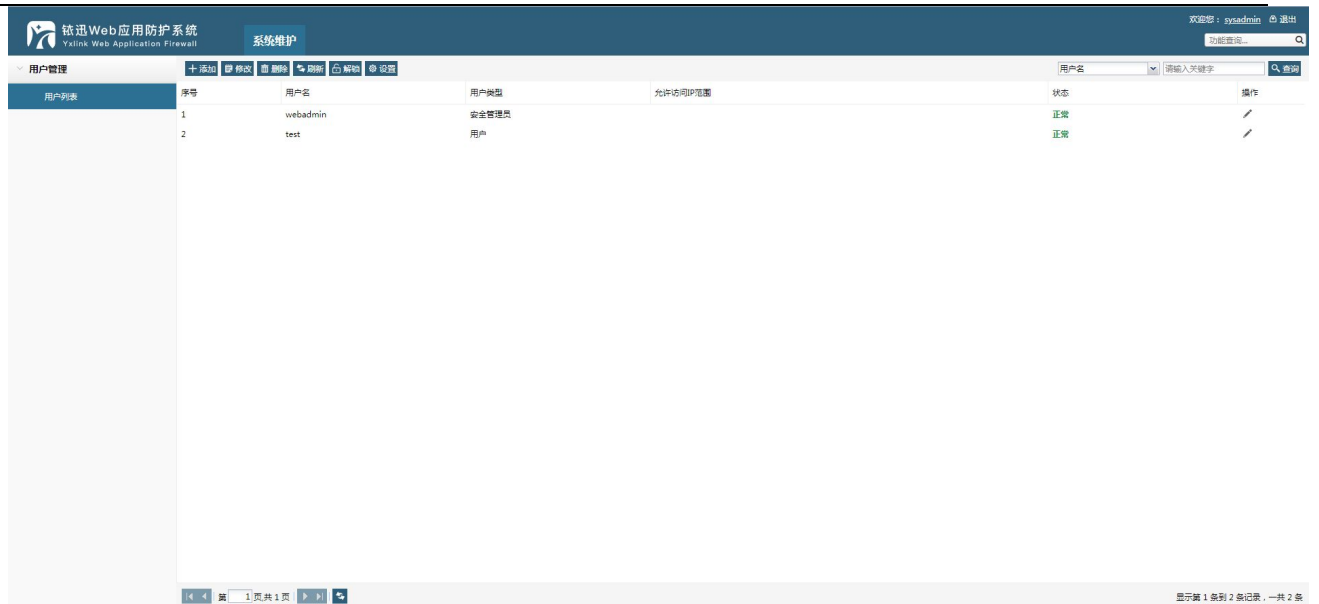
6.1.2 系统管理员登录

系统管理员为系统内置账号,可创建并管理安全管理员、普通用户的账号,除此之外无其它权限。系统管理员的所有操作行为都被记录到审计日志。内置的系统管理员账户 sysadmin 不可删除。

系统管理员可以使用内置的 sysadmin 账号登录界面,如下图所示。



使用系统管理员账号登录成功后的欢迎界面,如下图所示。具体功能的介绍,请参见[用户设置\(系统管理员适用\)](#)。



6.1.3 安全审计员登录

安全审计员只负责对系统管理员和安全管理员的操作日志进行查看和管理，还负责管理安全审计员类型的账号。

安全审计员可以使用内置的 auditor 账号登录界面，如下图所示。



使用安全审计员账号登录成功后的欢迎界面，如下图所示。具体功能的介绍，请参见[用户设置（安全审计员适用）](#)与[审计日志\(仅限于安全审计员\)](#)。

Yxlink 系统维护					
事件管理	系统维护	系统维护	系统维护	系统维护	系统维护
审计日志	序号	用户	IP	操作时间	日志内容
用户管理	389	auditor	192.168.88.161	2019-10-25 16:05:47	登录系统
用户列表	388	sysadmin	192.168.88.161	2019-10-25 15:49:03	退出系统
	387	sysadmin	192.168.88.161	2019-10-25 15:48:08	登录系统
	386	webadmin	192.168.88.161	2019-10-25 15:46:37	退出系统
	385	webadmin	192.168.88.161	2019-10-25 15:37:14	登录系统
	384	webadmin	192.168.88.161	2019-10-25 14:48:41	登录系统
	383	webadmin	192.168.88.161	2019-10-25 13:36:09	登录系统
	382	webadmin	192.168.88.161	2019-10-25 11:32:02	登录系统
	381	webadmin	192.168.88.198	2019-10-25 11:19:30	保存基本参数设置信息，修改详情：没有修改
	380	webadmin	192.168.88.198	2019-10-25 11:19:28	应用基本参数设置信息，修改详情：停用网站统计，停用访问记录
	379	webadmin	192.168.88.198	2019-10-25 11:14:36	登录系统
	378	webadmin	192.168.88.161	2019-10-25 09:56:32	应用HTTPS透明防护配置
	377	webadmin	192.168.88.161	2019-10-25 09:56:26	添加HTTPS透明防护配置，ID：5，名称：fec00009999c101
	376	webadmin	192.168.88.161	2019-10-25 09:55:41	登录系统
	375	webadmin	192.168.88.161	2019-10-25 09:23:00	规则文件上传成功
	374	webadmin	192.168.88.161	2019-10-25 09:23:00	升级规则
	373	webadmin	192.168.88.161	2019-10-25 09:22:39	应用规则在线升级设置
	372	webadmin	192.168.88.161	2019-10-25 09:22:36	应用规则在线升级设置
	371	webadmin	192.168.88.161	2019-10-25 09:21:51	登录系统
	370	webadmin	192.168.88.161	2019-10-24 14:29:10	保存基本参数设置信息，修改详情：磁盘空间上限（%）由“8”改为“45”
	369	webadmin	192.168.88.161	2019-10-24 14:28:49	登录系统
	368	webadmin	192.168.88.115	2019-10-24 10:35:31	登录系统
	367	webadmin	192.168.88.161	2019-10-24 09:55:50	登录系统
	366	webadmin	192.168.88.115	2019-10-24 09:52:07	登录系统

6.1.4 安全管理员登录

安全管理员负责产品安全策略制定、产品配置以及日常维护等管理，不能进行审计日志的查看和管理，不能创建系统管理员、普通用户、安全审计员账号。

安全管理员可以使用内置的 webadmin 账号登录界面，如下图所示。



铱迅Web应用防护系统

Yxlink Web Application Firewall

用户名:

密码:

语言:

简体中文

登录

使用安全管理员账号登录成功后的欢迎界面，如下图所示（具体功能的介绍，请参见后面的各个章节）



6.2 密码修改

当采用系统内置用户首次登录成功后，会提示“修改初始密码”的对话框，如下：

修改初始密码

系统管理员(sysadmin)

密码:

重复密码:

安全管理员(webadmin)

密码:

重复密码:

审计员(auditor)

密码:

重复密码:

保存

密码修改有三种方式：

- 系统管理员可以修改所有安全管理员和普通用户类型账号的密码；
- 安全审计员可以修改安全审计员类型账号的密码；
- 每个用户都可以修改自己的密码。

（点击右上角“欢迎您：某用户”，系统弹出该用户的密码修改对话框，如下图所）

密码修改

当前用户: webadmin

当前密码:

新密码:

新密码确认:

保存

取消

6.3 欢迎界面

安全管理员在登录界面输入用户名和密码并通过验证后，将看到如图所示的欢迎界面。



整个界面划分为 5 个功能块，即左上侧的产品 Logo 图标，左侧的功能菜单列表，右上侧的登录信息，右侧中间的选项卡列表和右下侧的各种操作管理页面。

功能菜单列表：所有的操作管理页面都可以通过左侧的功能菜单点击进入。

1. 在【系统监控】中显示了本产品的设备型号和快捷方式，通过快捷方式，您可以快速地进入各种操作管理页面。
2. 当您打开某一个功能的页面时，页面上方会显示出当前功能所在的选项卡。
3. 当您选择换肤或者其他风格时，整个管理界面的风格和配色方案会随之改变。
4. 您可以点击【退出】按钮，以便安全退出 Web 管理页面。
5. 点击产品 Logo 图标返回【系统监控】页面。

提示：

按 F11 键可以让浏览器进入全屏浏览模式，提供更大的操作界面。

6.4 功能菜单

功能菜单主要包括以下主菜单，每个主菜单下面又有若干子菜单。

当您点击主菜单后，会弹出其下的子菜单。各个菜单的主要功能如下：

【系统监控】主菜单：

主要是方便查看系统当前的状态。

- 【快捷方式】：查看本设备的阻断日志，实时流量，入侵记录等。

【数据中心】主菜单中【威胁监控】：

- 【入侵记录】：查看本设备记录的入侵事件。可以进行查看历史入侵记录、筛选记录、导出入侵记录到文件等操作。
- 【入侵查询】：提供对入侵记录的查询，筛选，以及对查询结果生成报表，日志导出的功能。
- 【入侵统计】：查看当月和历史月份的入侵统计图，以便快速掌握不同日期遭受攻击的状况，判断攻击变化的趋势。
- 【阻断日志】：如果本设备的拦截方式是“阻断”，可以在此页面中显示当前所有被阻断的IP地址的相关信息。
- 【网页木马日志】：查看网页木马日志。
- 【Flood 防护日志】：查看本设备的DDOS日志，CC攻击日志，CC攻击阻断的IP。
- 【CSRF 防护日志】：查看CSRF相关的信息。
- 【防篡改日志】：查看本设备的防篡改日志。
- 【弱密码日志】：查看用户登录页面弱密码日志。

【数据中心】主菜单中【网络流量】：

- 【实时流量】：查看本设备所有网络接口的实时状态，以及收发数据包、速率等。
- 【历史流量】：按天或者按月显示本设备的网络流量统计图，以便快速排查异常流量情况。

【数据中心】主菜单中【系统报表】：

- 【报表管理】：查看和导出系统生成的报表。
- 【即时报表】：提供即时的生成系统报表的功能。
- 【定期报表】：提供按照设定的时间自动生成报表的功能。

【数据中心】中【系统日志】主菜单：

- 【系统日志】：查看系统日志，记录了系统相关的事件信息。

【防护设置】中【入侵防护】主菜单：

- 【基本参数设置】：设置本设备的基本防护参数。
- 【基本访问控制设置】：对防护的流量进行精确到IP、IP段、域名以及URL的细粒度的控制。
- 【高级访问控制设置】：对本设备的内置规则进行精确到IP、IP段、域名以及URL的细粒度的控制。
- 【智能阻断】：对入侵者的入侵行为进行智能拦截的功能。

- **【木马上传检测】**：开启木马上传检测可以对待检测的文件进行木马检测。
- **【防盗链设置】**：查看和设置防盗链规则。
- **【CSRF 防护设置】**：对跨站请求伪造进行防护。
- **【Flood 防护设置】**：设置 DDOS、CC 防护的基本参数以及 Flood 访问控制的基本参数设置。
- **【来源 IP 解析】**：开启后，当信任的代理地址发起的 HTTP 请求中，包含下列字段时，将使用该字段的值作为真实来源 IP 地址，常用于反向代理。

【防护设置】中【对象配置】主菜单：

- **【地址对象】**：对指定的 IP 进行防护。
- **【计划任务】**：添加计划任务的功能。
- **【重定向页面】**：设置规则的重定向页面。
- **【蜘蛛设置】**：提供对搜索引擎蜘蛛 IP 的白名单功能。

【防护设置】中【防护策略】主菜单：

- **【自定义规则】**：查看和设置用户自定义的防护规则，建议高级用户使用。
- **【内置规则】**：查看和设置本设备的内置规则。
- **【防护策略集】**：添加和删除防护策略。

【网络配置】中【网络配置】主菜单：

- **【网络接口】**：查看和设置本设备的所有网络接口。
- **【虚拟网桥】**：配置本设备的虚拟网桥。
- **【静态路由】**：配置本设备的静态路由。
- **【DNS 设置】**：设置本设备的 DNS 服务器。
- **【BYPASS 设置】**：配置设备的 BYPASS。

【网络设置】中【部署配置】主菜单：

- **【部署方式】**：透明网桥部署，反向代理部署，透明网桥/反向代理混合部署，策略路由部署，多子网防护。
- **【反向代理设置】**：设置和查看反向代理。
- **【高可用性】**：对本设备的高可用性进行相关配置。

【其他功能】中【主动防御】主菜单：

- **【漏洞扫描】**：查看和管理进行漏洞扫描的网站。
- **【URL 自学习】**：查看和管理 URL 自学习的网站。
- **【网页防篡改】**：采用定期轮询的方式，对网站数据进行监控，发现对网页进行任何形式的非法添加、修改、删除等操作时，立即进行保护，恢复数据并进行告警，同时记录防篡改日志
- **【数据库防篡改】**：查看和管理防篡改数据库。

【其他功能】中【高级设置】主菜单：

- **【关键字过滤】**：设置本设备的关键字过滤功能。

- **【弱密码检测】**：弱密码的用户名，密码，检测页面设置。
- **【备案审查】**：从页面统计中查询域名是否经过工信部备案。
- **【高级防御方式】**：TCP/IP 碎片攻击防护。
- **【防护 IP 限制】**：对指定的 IP 进行防护。
- **【紧急模式】**：流量速率超过限制时，流量将不经过检测引擎。

【其他功能】中【访问统计】主菜单：

- **【网站统计】**：查看域名被访问的次数。
- **【访问记录】**：查看访问服务器的来源地址地理位置等。
- **【网站详情】**：查看网站被访问的详细情况。

【系统维护】中【事件管理】主菜单：

- **【通知告警】**：提供发现高危攻击立即发送邮件告警的功能。
- **【SNMP Trap】**：对本设备的 SNMP Trap 功能进行配置
- **【SNMP】**：对本设备的 SNMP 功能进行相关配置。
- **【syslog】**：对本设备的 syslog 功能进行相关配置。

【系统维护】中【网络诊断】主菜单：

- **【抓包工具】**：提供对本设备接口进行数据抓包的功能。
- **【网络工具】**：提供常用的网络命令。

【系统维护】中【设备维护】主菜单：

- **【配置管理】**：导入和导出系统的配置参数或恢复出厂时的默认配置。
- **【授权信息】**：查看本设备的许可证状态，以及许可证证书的导入。
- **【系统时间】**：修改系统时间。
- **【离线升级】**：可以进行固件升级和规则升级。
- **【在线升级】**：可以在升级站点进行固件升级和规则升级。
- **【日志清理】**：对过期日志进行备份或者删除，清理磁盘空间，以便于系统良好的运行。
- **【关机/重启】**：关闭或重启本设备。

6.5 通用菜单、按钮介绍

6.5.1 保存和应用功能

如图，在许多页面中都有**【保存】**和**【应用】**按钮。

DNS配置

首选DNS服务器: 8.8.8.8

备用DNS服务器: 请输入备用DNS服务器

保存 应用

【保存】按钮的含义是保存当前的设置更改但并不立即生效。

【应用】按钮的含义是保存当前的设置更改并立即生效。



注意：

建议在每次设置更改后点击【保存】按钮。将所有设置全部配置完成以后，再点击【应用】按钮让所有设置更改生效。频繁点击【应用】按钮会降低系统的工作效率。

6.5.2 重置和取消功能

如图所示：

高级访问控制 - 添加

基本信息

拦截方式: 拦截 生效时间: 全天

是否启用: ☒ 启用 ☐ 停用 日志选项: ☒ 记录日志

说明: 请填写说明, 最长50字符

控制条件

来源与目的 防护策略 内置规则 自定义规则

来源设置 目的设置

来源: ☒ 任意IP ☐ 单IP ☐ 地址对象 目的: ☒ 任意IP ☐ 单IP

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com

保存 重置 取消

【重置】按钮的含义是清空当前窗口中用户已经输入的内容以便用户重新输入。

【取消】按钮的含义是不保存当前的用户输入并关闭窗口。

6.5.3 刷新功能

如图，【刷新】按钮的含义是从设备数据库中获取最新的数据到用户界面。当您觉得当前 Web 页面显示的信息已经过期的情况下可使用此按钮强制刷新。

接口名称	IP地址	子网掩码	网关	下一跳	是否启用	连接状态	工作方式	所属网桥	接口属性	操作
ETH0	192.168.100.1	255.255.255.0	*		已启用	已断开	保留		DSI	
ETH1	192.168.99.51	255.255.255.0	192.168.99.1		已启用	已连接	普通模式		DMI	
ETH2	192.168.1.11	255.255.255.0	192.168.1.1		已启用	已断开	普通模式		RPI	
ETH3					已停用	已断开	普通模式			
ETH4					已启用	已连接	透明网桥	wafprotect	WAN	
ETH5					已启用	已连接	透明网桥	wafprotect	LAN	

6.5.4 多选功能

如图，在大多数支持列表操作的页面中，您都可以通过按住 Ctrl 键点击以选择多条记录，或者通过按住 Shift 键选择开始记录和结尾记录以便选择一个记录范围。您也可以两种方法配合使用。

+ 添加 删除 刷新 全部开始 全部停止 显示结果						
序号	扫描地址	状态	加入时间	完成时间	说明	操作
1		未扫描	2017-12-08 00:59:16			
2		未扫描	2017-12-08 00:59:09			
3		未扫描	2017-12-08 00:58:59			
4		未扫描	2017-12-08 00:58:44			
5		未扫描	2017-12-08 00:58:35			
6		未扫描	2017-12-08 00:58:27			

6.5.5 双击功能

在大多数支持列表操作的页面中，您可以通过双击某条记录，以便快速地进行相应的操作。如图，例如您在自定义规则页面双击一条记录时，系统会自动打开该条规则的编辑页面。

+ 添加 删除 刷新			
序号	策略名称	策略说明	操作
1	默认防护策略集	出厂默认防护策略	

6.5.6 翻页功能

如图，在以列表显示的页面中，您可以通过左下角的翻页按钮来翻页：

- 表示跳到首页
- 表示上一页
- 表示下一页
- 表示跳到末页

您也可以直接在编辑框中输入页码并按回车（Enter）键来进行跳转。

13000...	Windows权限提升	在Windows下提升普通用户为管理员权限	命令... 拦截	默认提示...	记录... 已启...	2010-02-21...
14000...	下载关键文件	防止下载mdb数据库文件、*.inc文件、*.co...	信息... 拦截	默认提示...	记录... 已启...	2012-04-06...
12000...	SQL注入中使用查询、...	SQL注入中使用查询、插入、删除、更新	SQL... 拦截	默认提示...	记录... 已启...	2010-02-08...
14000...	XSS跨站	防止XSS跨站，进行挂马或者盗取用户Coo...	XSS... 拦截	默认提示...	记录... 已启...	2010-02-08...
13100...	IIS6.0文件夹、文件名...	防止访问如xxx.asp/a.jpg或者xxx.asp;aaa.j...	脚本... 拦截	默认提示...	记录... 已启...	2011-01-24...
13100...	本地文件包含	PHP中企图包含本地文件	脚本... 检测	默认提示...	记录... 已停...	2010-02-23...

第 1 页, 共 24 页

显示第 1 条到 30 条记录，一共 699 条

6.5.7 排序功能

在大多数支持列表操作的页面中，当把鼠标箭头放在列名称上时，例如：入侵记录页面的“源 IP 地址”，右侧会出现一个向上或者向下箭头。点击此箭头，在出现的菜单中可以选择“正序”或者“逆序”。

此外可以通过直接点击某个列名来快速实现列表内容按照该列“正序”或“逆序”排列，如图所示。

规则号	规则名称	说明	类别	拦截方...	重定向页面	是否...	是否...	更新时间
12000...	SQL注入(AND/OR/X...	SQL注入中用于判断	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入单引号	SQL注入中用于闭合字符串	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入关键字	SQL注入中使用的关键字, 如Select	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入使用/**/	SQL注入中使用/**/作为空格	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入中使用Union...	SQL注入中使用Union查询来获取敏感数据	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12100...	SQL注入执行存储过程...	针对MSSQL注入使用危险存储过程, 如XP...	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12200...	SQL注入导入导出文件	Mysql注入中导入、导出文件, 可以查看重...	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
13000...	添加Windows用户	在Windows下添加用户	命令...	拦截	默认提示...	记录...	已启...	2010-02-21...
13000...	Windows权限提升	在Windows下提升普通用户为管理员权限	命令...	拦截	默认提示...	记录...	已启...	2010-02-21...

6.5.8 选择列功能

在大多数支持列表操作的页面中, 当把鼠标箭头放在列名称上时, 例如: 入侵记录页面的“源 IP 地址”, 右侧会出现一个向上或者向下箭头。点击此箭头, 在出现的菜单中的“列”子菜单下, 可以根据需要选择只显示某些列, 如图。

规则号	规则名称	说明	类别	拦截方...	重定向页面	是否...	是否...	更新时间
12000...	SQL注入(AND/OR/X...	SQL注入中用于判断	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入单引号	SQL注入中用于闭合字符串	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入关键字	SQL注入中使用的关键字, 如Select	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入使用/**/	SQL注入中使用/**/作为空格	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12000...	SQL注入中使用Union...	SQL注入中使用Union查询来获取敏感数据	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12100...	SQL注入执行存储过程...	针对MSSQL注入使用危险存储过程, 如XP...	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
12200...	SQL注入导入导出文件	Mysql注入中导入、导出文件, 可以查看重...	SQL...	拦截	默认提示...	记录...	已启...	2010-02-21...
13000...	添加Windows用户	在Windows下添加用户	命令...	拦截	默认提示...	记录...	已启...	2010-02-21...
13000...	Windows权限提升	在Windows下提升普通用户为管理员权限	命令...	拦截	默认提示...	记录...	已启...	2010-02-21...
14000...	下载关键文件	防止下载mdb数据库文件、*.inc文件、*.co...	信息...	拦截	默认提示...	记录...	已启...	2012-04-06...

7、系统监控

用于查看当前设备的基本状态信息, 包括四个部分: 快捷方式、系统状态、实时流量、设备信息和授权信息。

7.1 系统状态

用于显示设备的当前系统状态, 如图



- CPU：显示当前设备的 CPU 使用情况。
- 内存：显示当前设备的内存使用情况。
- 磁盘：显示当前设备的磁盘使用情况。当磁盘空间不足时，会向管理员发送邮件提醒。并且会自动清理磁盘。如果需要手动清理磁盘，请参考[磁盘日志清理](#)。

提示：

本设备会尽可能多的使用内存以提高性能，因此内存占用较大（超过 80%）是正常现象。

7.2 实时流量

用于显示各个网络接口的实时流量信息，如图。

实时流量							
网络接口	模式	速率	连接状态	收到的字节	发送的字节	接收速率	发送速率
ETH0	自动	自动	已断开	0B	0B	0	0
ETH1	全双工	1000 Mbps	已连接	1.03GB	71.72MB	4480	0
ETH2	自动	自动	已断开	0B	0B	0	0
ETH3	自动	自动	已断开	0B	0B	0	0
ETH4	全双工	1000 Mbps	已连接	2.00GB	135.66MB	1148648	0
ETH5	全双工	1000 Mbps	已连接	136.60MB	2.00GB	0	861208

7.3 设备信息

用于显示本设备的硬件版本、固件版本、系统版本、规则版本、产品型号和产品序列号。

设备信息



许可证状态正常！

客户名称: 铱迅测试专用
授权有效期: 2019-04-12至2020-05-30
质保有效期: 2019-04-12至2022-04-12
产品型号: Yxlink WAF-5820
产品序列号: WAF0HW0B1A01
硬件版本: 2.0
系统版本: 2.6.05.0421
防护规则版本: 12.11.26.44
固件版本: 2.6



注意：

请记录下您使用产品的“产品序列号”等重要信息，以便在设备升级或出现故障的情况下，快速向铱迅客服人员请求帮助。

7.4 授权信息

用于显示本设备的授权信息。每一台铱迅 Web 应用防护系统都有唯一的许可证书，该许可证文件只能导入一次，重复导入相同证书无效。同时，许可证书不能在不同型号、同型号不同设备之间混用。

当设备没有许可证或者许可证已经过期的情况下，使用安全管理员账号登录时会显示如下页面。

授权信息

许可证已过期！

设备将在一小时内工作于检测模式（无防护能力）！
请联系设备供应商获取有效许可证书！

导入许可证

当本设备许可证是有效期授权类型的，使用安全管理员账号登录时，可以看到当前的许可证状态如下。

授权信息

许可证还有55天到期！

请尽快联系设备供应商更新许可证书！

客户名称: test
产品型号: Yxlink WAF-2810
产品序列号: WAF0HW0B1A01
授权有效期: 2018-04-02至2018-05-30

导入许可证

当设备许可证是终身授权类型的，使用安全管理员账号登录时，可以看到当前许可证状态如下。



注意：

当设备没有许可证或者许可证已经过期时，铱迅 Web 应用防护系统将在一小时之后无防护。如果遇到上述情况，请及时联系供货商或者铱迅信息以便获取有效许可证书。

8、数据中心

8.1 威胁监控

8.1.1 入侵记录

8.1.1.1 查看入侵记录

用于显示被本设备拦截的入侵记录，显示的具体内容包括：序号、攻击时间、拦截原因、规则集名称、危害等级、源 IP 地址、地理位置、目的 IP 地址、源端口、目的端口、拦截方式、HTTP 请求、URL，具体如下图所示。

入侵记录列表中不同的颜色代表了不同程度的危害等级。红色代表该条入侵记录的危害程度是严重；黄色代表该条入侵记录的危害程度是中等；白色代表该条入侵记录的危害程度是轻微。

序号	最后时间	规则编号	规则集名称	危害等级	源IP地址	地理位置	目的IP地址	源端口	目的端口	拦截方式	HTTP请求	次数	URL	操作
122...	2018-04-26 10...	1200002	SQL注入单引号	低	192.168.99.57	LAN	192.168.99.23	206...	80	拦截	GET	37		
122...	2018-04-26 10...	1200009	SQL注入关键词 (Post/Cook...	低	192.168.99.57	LAN	192.168.99.23	206...	80	拦截	POST	8		
122...	2018-04-26 10...	1410001	访问/读取/包含关键文件	中	192.168.99.57	LAN	192.168.99.23	204...	80	拦截	GET	169		
122...	2018-04-26 10...	1400001	下载关键文件	中	192.168.99.57	LAN	192.168.99.23	201...	80	拦截	GET	4		
122...	2018-04-26 10...	1420002	eWebeditor编辑器越权通...	高	192.168.99.57	LAN	192.168.99.23	201...	80	拦截	GET	1		
122...	2018-04-26 10...	1310043	通用Struts2框架远程执行代...	中	192.168.99.57	LAN	192.168.99.23	184...	80	拦截	POST	8		
122...	2018-04-26 10...	1200008	SQL注入(AND/OR/XOR) v2	低	192.168.99.57	LAN	192.168.99.23	200...	80	拦截	GET	10		

- 选择查看日期：您可以在【请选择查看日期】右侧点击日历图标，如图，在弹出的日历窗口中选择某一个日期。或者您也可以手工输入需要查看记录的日期，请注意输入日期的格式，例如：20017-11-18。



- 查询记录： 在点击选定某个日期后，可以快速查看指定日期的所有入侵记录。如果当天记录超过 30 条，会以多页的形式显示出来，可以通过翻页功能来查看指定日期的所有记录。
- 删除入侵记录： 选择一条或者多条记录后，点击【删除】按钮可以将所选择的记录删除掉。如需删除多日的入侵记录，请参考[磁盘日志清理](#)。
- 刷新： 如果需要从数据库中重新获取指定日期的入侵记录，请点击【刷新】按钮。
- 入侵记录排序： 当把鼠标箭头放在列名上时，例如：源 IP 地址，右侧会出现一个向下箭头，点击此向下箭头，在出现的菜单中可以对当前列表进行正序或逆序排序，还可以选择只显示某些列，如图。



- 查看入侵记录的详细信息： 当您双击一条记录时，会显示该记录的详细信息，如图。
- 攻击时间： 记录入侵的开始时间。
- 源 IP 地址： 记录入侵的来源 IP 地址。
- 目的 IP 地址： 记录入侵要到达的目的 IP 地址。

- 危害等级：描述入侵记录的危害程度。
- 事件描述：对该条入侵记录进行一个简单的描述和介绍。
- 解决方案：描述针对这种类型的攻击，应该采取的措施。

入侵记录 - 查看

规则集名称: 下载关键文件

规则编号: 1400001

URL: http://192.168.99.23/myinvoicer/config.inc

数据长度: 307

攻击时间: 2018-04-26 10:47:14

源IP地址: 192.168.99.57

目的IP地址: 192.168.99.23

危害等级: 中

事件描述: 防止下载mdb数据库文件、*.inc文件、*.config文件
mdb是Microsoft Access软件使用的一种存储格式,因其对数据操作的方便性,常用在一些中小型程序中;
inc一般是include文件格式,用于编写复用代码的,比如在脚本编

解决方案: 临时解决方法:
对于.mdb、.inc、.config等后缀,可在IIS中设置一个该后缀的扩展映射,将这个映射使用一个无关的dll文件来防止该后缀的文件被下载。这样不仅可以解决该漏洞问题,还可以避免其他很多安

关闭

提示:

本设备会尽可能的保存所有的历史日志，但如果保存的历史日志达到了磁盘空间的设置上限，本设备会自动执行磁盘清理，删除过期的日志。

8.1.1.2 统计视图

根据拦截原因，源 IP 地址，目的 IP 地址，目的端口对入侵记录进行合并，并统计次数，统计视图显示的入侵记录是最近的一条。

序号	最后时间	规则编号	规则集名称	危害...	源IP地址	地理位置	目的IP地址	源端口	目的...	拦截...	HTT...	次数	URL	操作
127...	2018-04-26 10...	1400002	XSS跨站	低	192.168.99.57	LAN	192.168.99.23	26996	80	拦截	GET	268		删除
127...	2018-04-26 10...	1200044	SQL注入关键字	中	192.168.99.57	LAN	192.168.99.23	26999	80	拦截	GET	5		删除
127...	2018-04-26 10...	1310022	FCkeditor编辑器存在test.h...	中	192.168.99.57	LAN	192.168.99.23	27001	80	拦截...	GET	1		删除
127...	2018-04-26 10...	1410001	访问/读取/包含关键文件	中	192.168.99.57	LAN	192.168.99.23	26993	80	拦截	GET	315		删除
127...	2018-04-26 10...	1620004	禁止访问phpmyadmin页面	低	192.168.99.57	LAN	192.168.99.23	26989	80	拦截	GET	52		删除
127...	2018-04-26 10...	1400001	下载关键文件	中	192.168.99.57	LAN	192.168.99.23	26972	80	拦截	GET	23		删除
127...	2018-04-26 10...	1200050	SQL注入关键字	中	192.168.99.57	LAN	192.168.99.23	26958	80	拦截	GET	3		删除
127...	2018-04-26 10...	1200002	SQL注入单引号	低	192.168.99.57	LAN	192.168.99.23	26959	80	拦截	GET	55		删除

8.1.1.3 筛选入侵记录

在入侵记录数量特别 大的时候，可能需要在入侵记录中筛选出符合条件的记录，以便于进一步的分析。

在【入侵记录】页面上点击【筛选】按钮，弹出【入侵记录-筛选】对话框。在此对话框中输入需要筛选的条件，点击【开始筛选】按钮后，【入侵记录】页面中将只显示符合条件的入侵记录。

如果某项内容不填写，则表示忽略该项的筛选条件。

入侵记录 - 筛选

*攻击时间: 2018-04-26

源IP地址: 请填写来源IP

目的IP地址: 请填写目的IP

起始规则编号: 请填写起始编号, 限制1000000-7999999

终止规则编号: 请填写终止编号, 限制1000000-7999999

拦截方式: ☐ 拦截并阻断 ☐ 拦截 ☐ 检测 ☐ 放行

数据长度/Byte: ☐ 大于 ☒ 等于 ☐ 小于

请填写数据长度, 限制0-65535

HTTP类型: 请选择HTTP类型

URL: 请填写URL

筛选 **重置** **取消**

用户可以在【入侵记录】页面上点击【取消筛选】按钮以恢复筛选之前的列表。

提示:

选择某条记录后点击【筛选】按钮，系统会自动将该条入侵记录的内容填充至筛选对话框中。

8.1.1.4 导出入侵记录

在【入侵记录】页面上点击【导出】按钮，将指定日期的入侵记录导出并以 csv 文件格式保存，如图。用户可以用 Microsoft Excel 等工具查看。如需导出多日的入侵记录，请参考[磁盘清理](#)。



8.1.1.5 入侵记录的右击菜单

在【入侵记录】页面右击某条入侵记录，出现如下图的右击菜单，提供各种快捷操作。针对该条入侵记录，可以进行例如：停用此条规则，设置来源 IP 直接丢弃，设置该 URL 直接放行等操作。

12794	2018-04-26 10...	1200044	SQL注入关键字	中
12793	20		t.ht...	中
12792	20			中
12791	20		页面	低
12788	20			中
12777	20			中
12772	20			低
12770	20		(关键字)	低
12754	20		件名...	低
12743	20		句	中
12727	20			中
12722	20			中
12716	2018-04-26 10...	1200003	SQL注入关键字	中

- 加入到URL自学习模式
- 设置此规则对该URL为“检测”，不记录日志
- 设置此规则对该URL为“检测”，记录日志
- 设置此规则为“检测”，不记录日志
- 设置此规则为“检测”，记录日志
- 停用此规则
- 启用此规则
- 设置来源IP为“直接丢弃”
- 设置来源IP为“放行”
- 设置目的IP为“放行”
- 设置该URL为“直接丢弃”
- 设置该URL为“放行”

该菜单提供的功能具体说明如下：

- 加入到 URL 自学习模式：此功能只针对规则集名称为“违反 URL 自学习策略”的入侵记录生效，使用此功能后，系统将学习此 URL 并添加到对应域名的 URL 模式管理中。您可以进入到“URL 自学习” - “URL 模式管理”页面进行查看。
- 设置此规则对该 URL 为“检测”，不记录日志：使用此功能会自动添加一条高级访问控制策略，将此规则对此 URL 设置为“检测”模式，并且不记录日志。您可以进入“高级” - “高级访问控制”选择添加的记录进行进一步的修改。
- 设置此规则对该 URL 为“检测”，记录日志：使用此功能会自动添加一条高级访问控制策略，将词条规则对此 URL 设置为“检测”模式，记录日志。您可以进入“高级” - “高级访问控制”选择添加的记录进行进一步的修改。
- 设置此规则为“检测”，不记录日志：使用后会将此规则设置为“检测”模式，不记录日志。您可以进入“高级” - “内置规则”或者“自定义规则”选择此规则，查看规则属性。
- 设置此规则为“检测”，记录日志：使用后会将规则设置为“检测”模式，记录日志。您可以进入“高级” - “内置规则”或者“自定义规则”选择此规则，查看规则属性。
- 停用此规则：使用后此规则将会被停用。您可以进入“高级” - “内置规则”或者“自定义规则”进行查看。
- 设置来源 IP 为“直接丢弃”：使用后将会添加一条基本访问控制策略，将此 IP 地址的设置为“直接丢弃”，阻止该 IP 地址的所有访问。您可以进入“高级” - “基本访问控制”查看详细信息。
- 设置来源 IP 为“放行”：使用后将会添加一条基本访问控制策略，将此 IP 地址的所有的访问设置为“放行”，允许该 IP 地址的所有访问，且不被检测引擎检测。您可以进入“高级” - “基本访问控制”查看详细信息。

- 设置目的 IP 为“放行”：使用后将会添加一条基本访问控制规则策略，将对此目的 IP 地址的所有的访问设置为“放行”，允许所有对此目的 IP 的访问，且不被检测引擎检测。您可以进入“高级” - “基本访问控制”查看详细信息。
- 设置该 URL 为“直接丢弃”：使用后将会添加一条基本访问控制规则策略，将对此 URL 的所有访问设置为“直接丢弃”。您可以进入“高级” - “基本访问控制”查看详细信息。
- 设置该 URL 为“放行”：使用后将会添加一条基本访问控制规则策略，将对此 URL 的所有访问设置为“放行”，所有对该 URL 的访问均会被放行，且不被检测引擎检测。您可以进入“高级” - “基本访问控制”查看详细信息。

8.1.2 入侵查询

该页面提供对入侵记录根据时间、拦截原因、规则类别、危害等级、来源 IP、源端口、目的 IP、目的端口、URL 包含、拦截方式、HTTP 请求类型进行条件组合查询的功能。同时对查询的结果，提供报表生成和日志导出的功能。

查询条件

*开始时间: 2018-04-26 00:00:00

规则编号: 请填写规则编号, 限制1000000-7999

源IP地址: 请填写来源IP

目的IP地址: 请填写目的IP

拦截方式: 不限

*结束时间: 2018-04-26 23:59:59

规则类别: 全部分类

源端口: 请填写来源端口, 限制1-65535

目的端口: 请填写目的端口, 限制1-65535

HTTP类型: 不限

危害等级: 不限

URL: 请填写URL

[开始查询](#)

序号	攻击时间	规则...	规则集名称	危害...	源IP地址	地理位置	目的IP地址	源端...	目的...	拦截...	HTT...	URL	操作
201...	2018-04-2...	1400...	XSS跨站	低	192.168...	LAN	192.168...	320...	80	拦截	GET	...	...
201...	2018-04-2...	1410...	访问/读取/包含关键文件	中	192.168...	LAN	192.168...	320...	80	拦截	GET	...	...
201...	2018-04-2...	1200...	SQL注入中使用Union查...	中	192.168...	LAN	192.168...	320...	80	拦截	GET	...	...
201...	2018-04-2...	1400...	XSS跨站	低	192.168...	LAN	192.168...	320...	80	拦截	GET	...	...
201...	2018-04-2...	1400...	XSS跨站	低	192.168...	LAN	192.168...	320...	80	拦截	GET	...	...
201...	2018-04-2...	1400...	XSS跨站	低	192.168...	LAN	192.168...	320...	80	拦截	GET	...	...

根据时间查询入侵记录：设置【开始时间】和【结束时间】，点击【开始查询】，即可查询出该日期范围内的所有入侵记录。

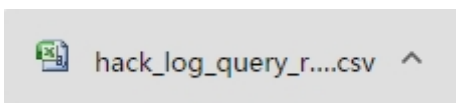
- 根据拦截原因（拦截原因为内置规则集编号或自定义规则的编号）查询入侵记录：勾选【拦截原因】，填写拦截原因例如“1900001”，点击【开始查询】，即可查询出该日期范围内的所有拦截原因为“1900001”的入侵记录。
- 根据规则类别查询入侵记录：勾选【规则类别】，在下拉菜单中选择规则类别例如“SQL 注入”，点击【开始查询】，即可查询出该日期范围内的所有规则类别为“SQL 注入”的入侵记录。
- 根据危害等级查询入侵记录：勾选【危害等级】，在下拉菜单中选择危害级别例如“严重”，点击【开始查询】，即可查询出该日期范围内的所有危害等级为“严重”的入侵记录。
- 根据来源 IP 查询入侵记录：勾选【来源 IP】，在文本框中写入来源 IP 例如“192.168.1.14”，点击【开始查询】，即可查询出该日期范围内的所有来源 IP 为“192.168.1.14”的入侵记录。
- 根据源端口查询入侵记录：勾选【源端口】，在文本框中写入源端口号，例如“5326”，点击【开始查询】，即可查询出该日期范围内的所有源端口号为“5326”的入侵记录。

- 根据目的 IP 查询入侵记录：勾选【目的 IP】，在文本框中写入目的 IP 例如 “192.168.1.15”，点击【开始查询】，即可查询出该日期范围内的所有目的 IP 为 “192.168.1.15” 的入侵记录。
- 根据目的端口查询入侵记录：勾选【目的端口】，在文本框中写入目的端口号，例如 “80”，点击【开始查询】，即可查询出该日期范围内的所有目的端口号为 “80” 的入侵记录。
- 根据 URL 包含查询入侵记录：勾选【URL 包含】，在文本框中输入 “test”，点击【开始查询】，即可查询出该日期范围内的所有入侵 URL 中包含 “test” 的入侵记录。
- 根据拦截方式查询入侵记录：勾选【拦截方式】，在下拉框中选择拦截方式例如 “阻断”，点击【开始查询】，即可查询出该日期范围内的所有拦截方式为 “阻断” 的入侵记录。
- 根据 HTTP 请求类型查询入侵记录：勾选【HTTP 请求类型】，在下拉框中选择 HTTP 请求方式例如 “POST”，点击【开始查询】，即可查询出该日期范围内的所有 HTTP 请求方式为 “POST” 的入侵记录。
- 对查询的结果使用右键加强功能：具体参考 [入侵记录的右击菜单](#)。将查询后的结果生成报表：查询出所需要的入侵记录，在下拉菜单中选择【Html 格式】或者【Doc 格式】，点击【生成报表】出现以下提示



Html 格式直接点击生成的链接就可以在浏览器中查看。Doc 格式的请点击生成的链接下载到本机后，再使用 “Microsoft Office Word” 工具打开即可查看。

- 将查询后的结果导出：查询出所需要的入侵记录，点击【导出】，在弹出的下载框中点击保存，下载完成后使用 “Microsoft Office Excel” 等工具打开即可。



- 您可以双击某条记录来查看该条记录的详细信息。

8.1.3 入侵统计

该页面以柱状图的形式显示指定月份内所发生的所有入侵事件。

月度入侵统计 攻击来源统计

月份: 2018-04 查询



您可以输入或者选择月份来查询历史月份的入侵统计，了解本设备在该月份每天所检测到的入侵事件数目，以便快速掌握不同日期遭受网络攻击的状况，判断网络攻击变化的趋势。

8.1.4 阻断日志

阻断日志会显示被智能阻断，规则阻断（当规则设置为拦截并阻断的时候）的阻断信息。如图，显示的具体内容包括：序号、IP 地址、地理位置、阻断原因、开始时间和结束时间。

请选择查看月份: 2018-04							
序号	IP地址	地理位置	阻断原因	开始时间	结束时间	备注	操作
3		LAN	规则阻断	2018-04-26 10:58:02	2018-04-26 11:08:02	阻断结束	
2		LAN	规则阻断	2018-04-26 10:47:15	2018-04-26 10:57:15	阻断结束	
1		LAN	规则阻断	2018-04-26 10:36:07	2018-04-26 10:46:07	阻断结束	

显示第 1 条到 3 条记录，一共 3 条

筛选：按时间段，阻断原因对阻断的 IP 地址进行筛选，如图。

阻断日志 - 筛选

*开始时间: 2018-04-26 00:00:00

*结束时间: 2018-04-26 23:59:59

IP地址: 请输入要查询的IP地址

*阻断原因: ☒ 智能阻断 ☒ 规则阻断

筛选

重置

取消

- 阻断状态：显示当前被阻断的 IP 地址并可对阻断的 IP 地址进行解除阻断。

阻断状态						
解除阻断 刷新						
序号	IP地址	地理位置	阻断原因	开始时间	结束时间	操作
1	192.168.99.57	LAN	规则阻断	2018-04-26 14:23:30	2018-04-26 14:33:30	

解除阻断： 选择一条阻断记录，然后点击【解除阻断】按钮，即可让该 IP 解除阻断状态，该 IP 的后续正常访问将被允许。

批量解除阻断： 选择多条阻断记录，点击【解除阻断】按钮，即可让这一组 IP 解除阻断状态，该组 IP 的后续正常访问将被允许。



注意：

实际阻断时间根据攻击行为的严重程度和基准阻断时间共同确定。

删除阻断日志后，相应的被阻断 IP 并未解除。

8.1.5 弱密码日志

该页面可以查看到弱密码检测页面中的弱密码信息。相应的弱密码检测的设置，您可以参考[弱密码检测](#)。

删除 清空 筛选 刷新						
序号	URL	用户名	密码	安全等级	时间	操作
2	192.168.1.1	admin	123***	6	2019-11-19 13:48:23	
1	192.168.1.1	admin	123***	6	2019-11-19 13:48:10	

- **删除弱密码日志：** 选择一条或者多条记录后，点击【删除】按钮可以将所选择的记录删除掉。
- **清空弱密码日志：** 点击【清空】按钮可以清空当前所有的弱密码日志，以便重新统计。
- **刷新：** 如果需要从数据库中重新获取当前最新的弱密码信息，请点击【刷新】按钮。
- **筛选弱密码日志：** 提供了对弱密码日志中 URL、用户名、密码、安全等级和时间等限制条件的筛选功能。

弱密码日志 - 筛选

URL:

用户名: <URL已删除>

密码: 192.168.99.68/admin/*

安全等级: 起始安全等级 至 终止安全等级

开始时间: 请选择或输入开始时间

结束时间: 请选择或输入结束时间

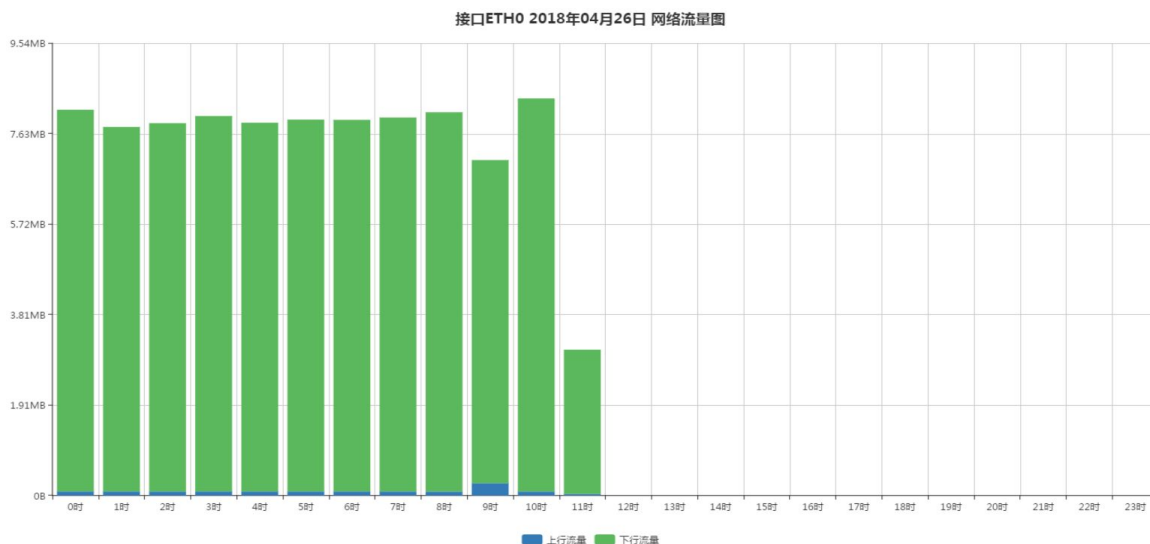
筛选

重置

取消

8.2 网络流量

该页面统计并显示 WAN 接口的网络流量，可以按天或者按月以折线图的形式显示出来。



您可以输入或者选择日期，了解本设备在该时间段内的网络流量，流量以字节（bytes）为单位。

8.3 系统报表

该模块提供按指定日期生成 Html、Doc 和 Pdf 格式报表的功能。可以对生成的报表进行管理，能够按照设置自动生成报表并且发送至管理员邮箱。

8.3.1 报表管理

该页面提供了对已经生成的报表进行管理和导出的功能。

删除	刷新	导出	报表名称	请输入关键字	查询
序号	报表名称	说明	报表类型	生成时间	操作
2	ReportView/20180426151950/report.html	即时报表	即时报表	2018-04-26 15:19:50	删除 刷新
1	ReportView/20180426151932/report.html	即时报表	即时报表	2018-04-26 15:19:32	删除 刷新

- 删除：选择某条记录，点击【删除】，在弹出的对话框点击【确定】即可删除此条报表。

- 刷新：点击“刷新”按钮，即可刷新该页面。
- 导出：选择某条记录，点击【导出】，即可导出该条记录所对应的报表。双击选中的记录，也能够导出该条记录所对应的报表。
- 快速查询：可以输入任意字符，对报表名称进行匹配查询操作。

8.3.2 即时报表

该页面能够按照选择的报表类型、日期范围、输入格式立刻生成对应的报表。

即时报表

*报表内容: ☒ 攻击报表 ☒ Webshell分析报表 ☒ 流量报表 ☒ 访问报表

时间范围:

报表格式:

报表说明:

- 攻击报表：针对入侵记录生成的攻击行为分析报表。
- Webshell 分析报表：针对系统检测到的 Webshell 攻击分析，分析出这些行为的一些相关信息。
- 流量报表：针对系统端口的流量生成的流量报表。
- 访问报表：针对 web 应用的访问信息进行统计分析得出的访问报表。（此功能必须打开访问统计功能，具体参照[其他设置](#)）
- 日期范围：可以选择最近一个月，最近一周，当天，或者自定义统计范围。
- 输入格式：可以选择 html、doc、pdf 的格式。
- 说明：可以为生成的报表填写相关说明信息。



注意：

点击【生成报表】，会在该表单下方显示出该报表的链接，点击即可进行打开操作。报表也会自动保存至“报表管理”页面，可以进入“报表管理”页面进行导出操作。

8.3.3 定期报表

该页面提供了对定期报表进行配置的功能。设置自动生成报表的类型、时间、格式、是否邮件发送等配置信息。

定期报表

*报表内容: ☒ 攻击报表 ☒ Webshell分析报表 ☒ 流量报表 ☒ 访问报表

生成时间: 每月第一天的凌晨1点 报表格式: Html格式

*报表说明: WAF Report

邮件发送: ☒ 开启邮件发送

保存

应用

- 报表包含的日志类型：可以根据需要选择不同的报表类型。
- 选择日期：每天（默认在每天的一点钟生成），每周（默认在每个星期日的一点钟生成），每月（默认在每月的第一天的一点钟生成）。
- 选择邮件发送：如果开启将会自动将报表发送至管理员邮箱。
- 输出格式：可以选择 Pdf, Doc, Html。
- 说明：可以填写定期报表的说明。



注意：

如果需要开启邮件发送的功能，请先配置好邮件通知，具体请参照：[通知设置](#)。

8.4、日志

系统在磁盘日志空间使用率将满或者已满的情况下，系统有三种提示用户的方式。

记录到系统日志，如下图：

序号	操作时间	日志内容	操作
186	2018-04-26 09:38:16	从上次记录此信息以来，累计入侵记录数超过5000	删除
185	2018-04-26 09:33:11	检测引擎重启	删除

- 2、邮件通知：如果用户使用了通知设置，在日志将满或者已满时，会收到相关邮件，如图：

尊敬的管理员，您好！
钰迅Web应用防护系统磁盘空间不足！
设备DMI接口的IP地址： 192.168.1.10
请尽快登录此设备备份日志或进行磁盘清理！

- 3、登录提示：在安全管理员登录时，系统自动弹出一个提示对话框，如图：

磁盘清理
当前磁盘使用率超过上限，已执行日志清理！

若点击“确定”按钮，则自动跳转到“磁盘日志清理”页面，具体请参考[手动磁盘清理](#)。若点击“取消”按钮，不做清理，就会出现一个系统提示，如图：

系统提示
您选择暂不清理日志信息，如果磁盘使用率超过设置上限，系统将自动清理！

系统在磁盘空间使用率已满的情况下，自动做磁盘清理操作，自动磁盘清理日志会记录到系统日志当中，如图所示：

序号	操作时间	日志内容	操作
18	2018-04-26 15:48:30	发送邮件通知	
17	2018-04-26 15:48:29	磁盘使用率（日志）超过上限，执行磁盘清理	

8.4.1 系统日志

系统日志页面显示了本设备上的系统事件，如图，您可以通过查询日志了解本设备上所发生的所有系统事件。

序号	操作时间	日志内容	操作
18	2018-04-26 15:48:30	发送邮件通知	
17	2018-04-26 15:48:29	磁盘使用率（日志）超过上限，执行磁盘清理	
16	2018-04-26 15:48:26	检测引擎启动	
15	2018-04-26 14:11:17	检测引擎重启	
14	2018-04-26 13:51:30	许可证书导入成功	
13	2018-04-26 00:00:00	许可证书已过期，设备将在一小时内工作于放行模式（无防护能力）	
12	2017-11-14 11:27:09	固件升级成功，版本号：2.6.04.9296	
11	2017-11-14 11:26:03	检测引擎重启	
10	2017-11-14 11:24:55	检测引擎重启	
9	2017-11-14 11:24:51	检测引擎停止	
8	2017-11-14 11:24:49	开始固件升级，请稍等	
7	2017-11-14 11:22:05	检测引擎重启	
6	2017-11-14 11:22:03	许可证书导入成功	
5	2017-11-14 11:19:30	许可证书已过期，设备将在一小时内工作于放行模式（无防护能力）	
4	2017-11-14 11:19:28	检测引擎启动	

- 系统事件查询：在右上侧选择或者输入指定日期，点击【快速查询】按钮，可以查询指定日期的系统日志。
- 导出日志：选择某个日期，点击【导出日志】按钮，导出指定日期的日志信息，以 csv 文件形式保存，您可以选择用 Microsoft Excel 等工具查看导出的系统日志文件。
- 日志筛选：点击【筛选】按钮，弹出【系统日志-筛选】对话框，如图。您可以组合日期和日志包含内容条件，筛选出需要查看的系统日志。

系统日志 - 筛选

*开始日期: 2018-04-26
*终止日期: 2018-04-26
日志内容: 请输入日志包含的内容

筛选

重置

取消

- 取消筛选: 点击【取消筛选】按钮, 可以取消已经筛选出的日志列表, 恢复到正常状态。
- 删除日志: 选择一条或者多条系统日志, 点击【删除】按钮, 这些系统日志将被从系统中删除。

 注意:

系统会根据当前的磁盘空间上限设置, 自动定期执行日志清理工作。如果需要保留日志, 请参见[磁盘日志清理](#)。

8.4.2 审计日志(仅限于安全审计员)

审计日志用于安全审计员审查设备的使用情况, 用户对设备配置所作的修改操作都将被记录到审计日志中。

 刷新  筛选  导出  设置 请选择查看日期:				
序号	用户	IP	操作时间	日志内容
25	auditor	192.168.88.144	2018-04-26 16:11:03	登录系统
24	webadmin	192.168.88.144	2018-04-26 16:10:46	退出系统
23	webadmin	192.168.88.144	2018-04-26 16:09:41	应用基本参数设置信息, 修改详情: 全局拦截方式由“拦截并阻断”改为“高级模式”
22	webadmin	192.168.88.144	2018-04-26 16:06:08	登录系统
21	webadmin	192.168.88.144	2018-04-26 15:48:57	登录系统
20	webadmin	192.168.88.144	2018-04-26 15:47:01	登录系统
19	未知用户	192.168.88.144	2018-04-26 15:46:56	尝试登录系统, 尝试用户名为webadmin
18	webadmin	192.168.88.144	2018-04-26 15:46:50	退出系统
17	webadmin	192.168.88.144	2018-04-26 15:43:32	登录系统
16	webadmin	192.168.88.144	2018-04-26 15:43:26	退出系统
15	webadmin	192.168.88.144	2018-04-26 15:30:50	登录系统
14	webadmin	192.168.88.144	2018-04-26 15:06:18	登录系统
13	webadmin	192.168.88.144	2018-04-26 14:11:16	应用基本参数设置信息, 修改详情: 全局拦截方式由“高级模式”改为“拦截并阻断”
12	webadmin	192.168.88.144	2018-04-26 13:51:29	许可证验证通过
11	webadmin	192.168.88.144	2018-04-26 13:51:28	许可证上传成功
10	webadmin	192.168.88.144	2018-04-26 13:51:13	登录系统

第 1 页共 1 页

显示第 1 条到 25 条记录, 一共 25 条

- 审计日志查询: 在右侧选择或者输入指定日期, 点击【快速查询】按钮, 可查询指定日期的审计日志。
- 导出日志: 选择某个日期, 点击【导出日志】按钮, 导出当天的日志信息, 以 csv 文件形式保存, 您可以选择用 Microsoft Excel 等工具查看导出的审计日志文件。
- 日志筛选: 通过筛选功能, 可以快速筛选出需要查看的审计日志。点击【筛选】按钮, 弹出【审计日志-筛选】对话框, 如图。您可以组合日期和日志包含内容条件, 筛选出需要查看的日志。

审计日志 - 筛选

✕

*开始日期: 2018-04-26

*终止日期: 2018-04-26

用户: 请输入用户名

IP: 请输入操作IP

日志内容: 请输入日志包含的内容

筛选

重置

✕ 取消

取消筛选：点击【取消筛选】按钮，可以取消已经筛选出的日志列表，恢复到正常状态。

9、防护设置

9.1 入侵防护

9.1.1 基本参数设置

基本参数设置页面用于配置本设备的一些基本防护参数，如图。具体参数的设置详见各小节。

全局拦截方式设置

全局拦截方式: ☐ 拦截并阻断-----拦截尝试入侵的数据报文并记录日志，在一段时间内拒绝该IP的访问。

☐ 拦截-----拦截尝试入侵的数据报文并记录日志。

☐ 检测-----检查尝试入侵的数据报文并记录日志，但不拦截。

☐ 放行-----对所有数据报文一律放行，不记录日志。

☒ 高级模式-----拦截方式由规则和高级访问控制共同确定，适用于高级用户。

检测端口设置: (指定要检测的端口，例如80端口，如有多个请用|隔开。)

*检测端口: 80|8080

功能设置

HTTP返回报文检测: ☒ 开启后，将对HTTP返回的数据报文进行检查，防止服务器泄露信息的泄露。

重定向页面: ☒ 开启重定向页面后，对于需要拦截的HTTP请求，将直接返回设置好的重定向页面。

网站统计: ☐ 开启网站统计功能后，将统计所有网站的请求和被攻击次数。

访问记录: ☐ 开启访问记录功能后，将按照不同URL统计所有被访问URL的请求次数。

网站隐身: ☐ 开启网站隐身功能后，将防护网站的Web服务器信息隐藏，例如：Apache。

双向检测: ☐ 开启双向检测后，将检查所有流入WAN、LAN接口的数据报文。关闭时，系统只检查WAN接口。

端口镜像检测: ☐ 开启端口镜像检测后，将对设置为镜像端口上的数据报文进行检测，但不进行拦截或阻断。

X-Real-IP获取: ☐ 开启后，当请求中包含X-Real-IP或X-Forwarded-For字段时，将使用该字段作为来源IP地址，用于反向代理。

IPv6协议支持: ☐ 开启后，系统将对IPv6的数据报文进行检测。关闭时，只支持对IPv4报文的检测。

其他设置

入侵阻断时间: ☐ 高 ☐ 中 ☒ 低 ☐ 自定义/秒

*磁盘空间上限/%: 80 在磁盘空间使用接近上限时，系统会发出邮件通知。如果超过上限，自动启动磁盘清理。

保存

应用

9.1.1.1 防护系统拦截方式设置

设置本设备的全局拦截方式。

全局拦截方式设置

全局拦截方式: ☐ 拦截并阻断-----拦截尝试入侵的数据报文并记录日志，在一段时间内拒绝该IP的访问。

☐ 拦截-----拦截尝试入侵的数据报文并记录日志。

☐ 检测-----检查尝试入侵的数据报文并记录日志，但不拦截。

☐ 放行-----对所有数据报文一律放行，不记录日志。

☒ 高级模式-----拦截方式由规则和高级访问控制共同确定，适用于高级用户。



注意：

基本访问控制在防护系统拦截方式设置为“放行”时不生效。

高级访问控制在防护系统拦截方式设置为“拦截并阻断”，“拦截”，“检测”和“放行”模式下时不生效。拦截方式完全由这里的全局拦截方式确定。

内置规则和自定规则的拦截方式在防护系统拦截方式设置为“拦截并阻断”，“拦截”，“检测”和“放行”模式下时不生效。拦截方式完全由这里的全局拦截方式确定。不过，您仍然可以在内置规则和自定义规则的页面进行规则的启用或者停用操作。

9.1.1.2 防护系统检测端口设置

设置本设备需要拦截的端口，如果连接在本设备 LAN 接口的 Web 服务器使用的端口各不一样，则需要全部添加进来。端口之间用“|”符号隔开。

检测端口设置：（指定要检测的端口，例如80端口，如有多个请用|隔开。）

*检测端口: 80|8080

例如：在您的网络环境下，连接在本设备 LAN 接口的 Web 服务器有 3 台（透明网桥模式），分别为服务器 A、服务器 B 和服务器 C。服务器 A 使用 80 端口作为 HTTP 访问端口，服务器 B 使用 80 和 8080 端口作为 HTTP 访问端口，服务器 C 使用 80 和 9080 端口作为 HTTP 访问端口。则此时的端口设置内容为：80|8080|9080。

9.1.1.3 功能设置

常用的功能开关设置。

功能设置

HTTP返回报文检测: ☒ 开启后，将对HTTP返回的数据报文进行检查，防止服务器出错信息的泄露。

重定向页面: ☒ 开启重定向页面后，对于需要拦截的HTTP请求，将直接返回设置好的重定向页面。

网站统计: ☐ 开启网站统计功能后，将统计所有网站的请求和被攻击次数。

访问记录: ☐ 开启访问记录功能后，将按照不同URL统计所有被访问URL的请求次数。

网站隐身: ☐ 开启网站隐身功能后，将防护网站的Web服务器信息隐藏，例如：Apache。

双向检测: ☐ 开启双向检测后，将检查所有流入WAN、LAN接口的数据报文。关闭时，系统只检查WAN接口。

端口镜像检测: ☐ 开启端口镜像检测后，将对设置为镜像端口上的数据报文进行检测，但不进行拦截或阻断。

X-Real-IP获取: ☐ 开启后，当请求中包含X-Real-IP或X-Forwarded-For字段时，将使用该字段作为来源IP地址，用于反向代理。

IPv6协议支持: ☐ 开启后，系统将对IPv6的数据报文进行检测。关闭时，只支持对IPv4报文的检测。

● HTTP 返回报文进行检测：

开启后，将对 HTTP 返回报文进行相应“内置规则”和“自定义规则”的匹配。HTTP 返回报文检测通常用于检查 Web 服务器或数据库出错导致的信息泄露，以及 Webshell 的特征等。

● 重定向页面：

重定向页面总开关，勾选后，系统将开启本设备的重定向页面功能（此时，规则中的重定向页面设置生效）。未勾选时，页面重定向功能完全不工作。

● 网站统计：

勾选后，系统将开启本设备的网站统计功能，统计每个网站的累计访问次数、攻击次数。

- 页面统计：

勾选后，系统将开启本设备的页面统计功能，统计每个页面的累计访问次数，同时记录每个页面的最后访问 IP、最后访问端口、浏览器类型、最后访问时间。

- 网站隐身：

勾选后，系统将开启网站隐身功能，将防护网站的 Web 服务器信息隐藏。

- 双向检测：

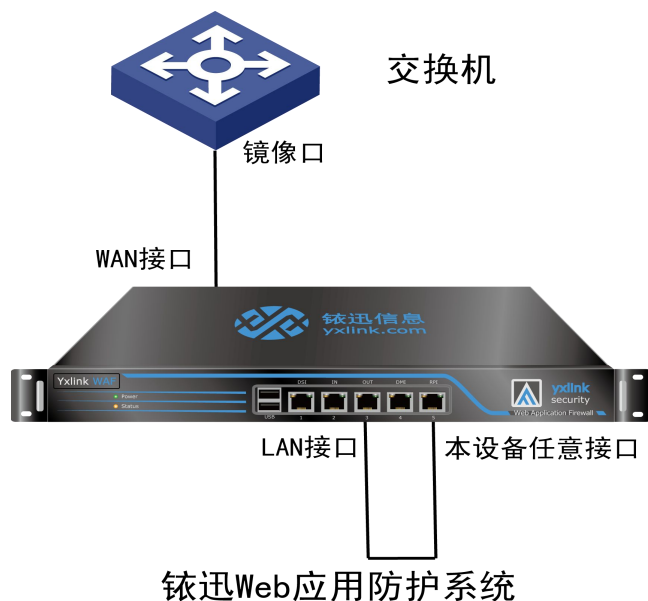
勾选时为开启双向检测，在双向检测方式下，所有流入 WAN 接口和 LAN 接口的 HTTP 请求都将通过检测引擎模块。

默认为关闭，这时防护系统只将流入 WAN 接口的 HTTP 请求通过检测引擎模块，也称为单向检测。

- 端口镜像检测：

本设备支持端口镜像，端口镜像只能对镜像的流量进行检测，不能真正防护 Web 服务器，您可以参照以下方式进行部署。

1. 勾选“是否开启端口镜像检测”，点击“保存”；
2. 按照下图方式进行部署。



i 提示：

端口镜像功能只能对镜像端口的数据报文进行检测，不能进行拦截或者阻断。

9.1.1.4 其他设置

在其他设置框中，可以对入侵阻断时间，磁盘空间上线限制。

其他设置

入侵阻断时间: ☐ 高 ☐ 中 ☒ 低 ☐ 自定义/秒

*磁盘空间上限/%: 在磁盘空间使用接近上限时, 系统会发出邮件通知。如果超过上限, 自动启动磁盘清理。

● 设置入侵阻断时间:

高: 10 小时, 中: 1 小时, 低: 10 分钟。

此选项仅在防护系统拦截方式设置为“拦截并阻断”或“高级模式”方式下工作。入侵阻断时间表示禁止入侵 IP 访问 Web 服务器的时间, 在阻断时间内, 无论其访问请求是正常行为, 还是入侵行为, 该 IP 都将无法访问 Web 服务器。

● 磁盘空间上限 (默认为 80%) :

当接近设置上限的时候, 系统自动执行磁盘清理工作。

磁盘空间上限的允许设置范围介于 45%至 95%之间。

磁盘空间使用率接近设置上限 90%的时候, 系统会以邮件提醒管理员进行手工清理。

9.1.2 基本访问控制

基本访问控制针对来源 IP、目的 IP、目的域名及目的 URL 提供了细粒度的控制管理功能。该功能能够对用户的访问进行精细控制, 甚至实现了在特定的时间范围内是否允许特定用户进行访问的功能。

+ 添加 删除 ▶ 启用 停用 ↑ 上移 ↓ 下移 刷新 还原 备份 ✓ 应用							
序号	来源IP	目的	拦截方式	是否启用	说明	生效时间	操作
1			直接丢弃	已启用	demo使用的漏洞网站	全天	/ 删除 上移 下移
2			放行	已启用	漏扫	全天	/ 删除 上移 下移
3			继续检测	已启用	漏扫	全天	/ 删除 上移 下移
4			直接丢弃	已启用	邮箱管理, 不允许外网访问	全天	/ 删除 上移 下移
5			放行	已启用	漏扫	全天	/ 删除 上移 下移
6			直接丢弃	已启用	漏扫	全天	/ 删除 上移 下移

9.1.2.1 添加基本访问控制策略

点击【添加】按钮, 弹出“基本访问控制设置-添加”对话框;

基本访问控制 - 添加

拦截方式: 直接丢弃

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

说明: 请填写说明, 最长50字符

来源: ☒ 任意IP ☐ 单IP ☐ 地址对象

目的: ☒ 任意IP ☐ 单IP ☐ 地址对象

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以"/"结束。
URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

✓ 保存

↺ 重置

✕ 取消

选择【拦截方式】：即如果匹配到此条策略所做的操作，例如“放行”；

基本访问控制 - 添加

拦截方式: 直接丢弃

生效时间: 直接丢弃

是否启用: 放行

说明: 请填写说明, 最长50字符

选择【生效时间】：用来表示这条策略的生效时间，生效时间是在计划任务中添加的，添加方法具体参考[计划任务](#)；

基本访问控制 - 添加

拦截方式: 直接丢弃

生效时间: 全天

是否启用: 全天

说明: 工作时间

说明: 下班时间

选择【是否启用】：是否启用此条规则；

基本访问控制 - 添加

拦截方式: 直接丢弃

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

填写【说明】：对此条规则的说明；

基本访问控制 - 添加

拦截方式: 放行

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

说明: 测试

【来源设置】：提供对来源 IP 的设置。这里我们选择单 IP（192.168.1.230），您可以根据您的需求自行选择添加；

基本访问控制 - 添加

拦截方式: 放行

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

说明: 测试

来源: ☐ 任意IP ☒ 单IP ☐ 地址对象

*来源IP: 192.168.1.230

目的: ☒ 任意IP ☐ 单IP ☐ 地址对象

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以"/*"结束。
URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

【目的设置】：提供对目的 IP 或者 URL 的设置。这里我们选择单一 IP（192.168.1.4），您可以根据您的需求自行添加；

目的: ☐ 任意IP ☒ 单IP ☐ 地址对象

*目的IP: 192.168.1.4

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以"/*"结束。
URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

点击【保存】按钮，该条访问控制策略被保存并返回上一级页面；

+ 添加 删除 启用 停用 上移 下移 刷新 还原 备份 应用							
序号	来源IP	目的	拦截方式	是否启用	说明	生效时间	操作
1	地址组 (192.168.9.1-192)	任意IP	直接丢弃	已启用	内部网络	全天	编辑删除
2	单IP (192.168.99.57)	任意IP	放行	已启用	非法用户	全天	编辑删除
3	单IP (192.168.99.23)	单IP (192.168.99.68)	继续检测	已启用	内部OA系统	全天	编辑删除
4	任意IP	任意IP	直接丢弃	已启用	邮箱管理	全天	编辑删除
5	任意IP	任意IP	放行	已启用	测试	全天	编辑删除
6	任意IP	任意IP	直接丢弃	已启用	测试	全天	编辑删除

在【基本访问控制设置】页面点击【应用】按钮，让当前更改立即生效。

9.1.2.2 删除基本访问控制策略

选中选定某条基本访问控制策略；

点击【删除】，在弹出的对话框中选择【确定】。

9.1.2.3 修改基本访问控制策略

选中选定某条基本访问控制策略；

点击【修改】弹出【基本访问控制-修改】界面；

基本访问控制 - 修改

拦截方式: 继续检测

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

说明: 内部OA系统

来源: ☐ 任意IP ☒ 单IP ☐ 地址对象

*来源IP: 192.168.1.230

目的: ☐ 任意IP ☒ 单IP ☐ 地址对象

*目的IP: 192.168.1.4

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以"/*"结束。
URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

✓ 保存

✕ 取消

修改完毕后点击【保存】。

9.1.2.4 基本访问控制策略的匹配顺序

本系统对于所有基本访问控制的策略，采取顺序匹配的原则，由上至下顺序匹配，按顺序匹配到的第一条策略进行访问控制，比如系统中存在两条或者多条来源以及目的 IP 相同的策略，则按匹配到的第一条策略进行控制，例如下图：

序号	来源IP	目的	拦截方式	是否启用	说明	生效时间	优先级	操作
1	单IP (192.168.9.230)	任意IP	直接丢弃	已启用	内部网络	全天	0	
2	单IP (192.168.9.230)	任意IP	放行	已启用	非法用户	全天	1	
3	单IP (192.168.9.230)	任意IP	继续检测	已启用	内部OA系统	全天	2	

如果我们想对来源 IP：192.168.9.230 放行，则实际采取的动作是直接丢弃，因为第一条策略被优先匹配到。策略的优先级顺序可以通过每条策略最后的 按钮来进行调整或者点击 手动修改优先级。您也可以停用第 1，2 条规则来使第 3 条规则生效。

9.1.2.5 基本访问控制策略应用示例

示例一：例如 192.168.9.2 是系统管理员计算机的静态 IP 地址，需要对网站进行定期更新，并且确认该计算机是安全的。在这种情况下，不需要对其访问进行任何拦截，可以参照如下方式添加控制策略：

1. 【动作】选择“放行”；

2. 【生效时间】选择“全天”；
3. 【是否启用】选择“启用”；
4. 【说明】填写“管理员 IP”；
5. 【来源设置】选择【单 IP】填写“192.168.9.2”；
6. 【目的设置】选择“任意”；
7. 点击【保存】；
8. 点击【应用】。

基本访问控制 - 添加
×

拦截方式: 放行

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

说明: 管理员IP

来源: ☐ 任意IP ☒ 单IP ☐ 地址对象

*来源IP: 192.168.9.2

目的: ☒ 任意IP ☐ 单IP ☐ 地址对象

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以/*结束。

URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

✓ 保存
↺ 重置
✕ 取消

提示:

对某 IP 段不进行拦截请将示例第三步中【来源设置】选择【IP 段】，填写不需要的进行防护的 IP 段起始和结束地址即可。

如果您不允许某来源 IP 访问，请将示例第一步中的【动作】选择为“直接丢弃”。

- 示例二: 例如 IP 为 192.168.1.4 的服务器是图片服务器不需要进行防护, 可以按如下方式添加控制策略:

1. 【动作】选择“放行”；
2. 【生效时间】选择“全天”；
3. 【是否启用】选择“启用”；
4. 【说明】填写“图片服务器 IP”；
5. 【来源设置】选择“任意”；
6. 【目的设置】选择【单 IP】填写“192.168.1.4”；
7. 点击【保存】；

8. 点击【应用】。

基本访问控制 - 添加
X

拦截方式: 放行

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

说明: 图片服务器IP

来源: ☒ 任意IP ☐ 单IP ☐ 地址对象

目的: ☐ 任意IP ☒ 单IP ☐ 地址对象

*目的IP: 192.168.1.4

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以"/*"结束。
URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

i提示:

对某 IP 段的服务器不进行防护, 请将示例第四步中【目的设置】选择【IP 段】, 填写入您所部需要的进行防护的 IP 段起始和结束地址即可。

如果您不允许某 IP 被访问, 请将示例第一步中的【动作】选择为“直接丢弃”。

示例三：

例如域名为 <http://www.photo.com> 的网站是图片站不需要进行防护，可以参照如下方式添加控制策略：

1. 【动作】选择“放行”；
2. 【生效时间】选择“全天”；
3. 【是否启用】选择“启用”；
4. 【说明】填写“图片站”；
5. 【来源设置】选择“任意”；
6. 【目的设置】选择【URL】填写“<http://www.photo.com/>”；
7. 点击【保存】；
8. 点击【应用】。

基本访问控制 - 添加

×

拦截方式: 放行

生效时间: 全天

是否启用:

☒ 启用

☐ 停用

说明: 图片站

来源:

☒ 任意IP

☐ 单IP

☐ 地址对象

目的:

☒ 任意IP

☐ 单IP

☐ 地址对象

*目的URL:

<http://www.photo.com/>

格式说明: 域名: http://*.test.com/, 必须以“/”结束。

URL: <http://www.test.com/test.asp>, 其中“*”匹配任意内容。

✓ 保存

↺ 重置

✕ 取消

i提示:

对二级域名进行控制可以将示例中的第四步的参数写成“http://*.test.com/”。

对具体的 URL 例如 <http://www.test.com/news.asp> 进行访问控制可以将示例中第四步的参数写成“<http://www.test.com/news.asp>”。

如果该 URL 带有参数，例如 <http://www.test.com/product.asp?id=1> 这个页面，可以将示例中第四步的参数写成“<http://www.test.com/news.asp>”。

- 示例四：例如 IP 为 192.168.1.14 的服务器在工作时间允许被访问，下班后不允许访问，可以参照如下方式添加控制策略：

1. 参照示例二，添加两条策略，如下图：

+ 添加 ✕ 删除 ▶ 启用 ⏸ 停用 ↑ 上移 ↓ 下移 ↻ 刷新 ↶ 还原 📁 备份 ✓ 应用							
序号	来源IP	目的	拦截方式	是否启用	说明	生效时间	操作
1	任意IP	单IP (192.168.1.4)	直接丢弃	已启用	下班不允许访问	下班时间	✎ ✕ ▶ ⏸ ↑ ↓
2	任意IP	单IP (192.168.1.4)	放行	已启用	全天允许访问	全天	✎ ✕ ▶ ⏸ ↑ ↓

- 将【拦截方式】为“直接丢弃”，【生效时间】为“下班时间”通过【优先级操作】调整到【拦截方式】为“继续检测”、【生效时间】为“全天”的策略上面；
- 点击【应用】。

提示:

访问控制策略是由上到下按照顺序匹配到由第一条匹配到的策略进行工作的。如果您在使用该功能的过程中出现问题请检查访问策略的顺序问题，并通过【优先级操作】进行策略顺序的调整。如果仍然有问题请删除访问控制策略重新配置。

注意:

“放行”是个危险的操作，如果启用“放行”那么所有的攻击行为都将会被“放行”并且不会被记录到入侵记录中，如非必要请勿使用。

“直接丢弃”是个危险的操作，如果启用“直接丢弃”那么所有匹配该策略的行为都不能够进行访问，如果您需要该功能，请谨慎使用。

9.1.3 高级访问控制

高级访问控制针对内置规则或者自定义规则，提供细粒度的控制。针对来源 IP、目的 IP、域名、URL 和规则（集）进行精细控制。例如：某个规则只对特定的 URL 产生误报，则可以对该特定的 URL，设置此规则为检测；而对于其他情况，仍然采取缺省动作。

+ 添加 ✕ 删除 ▶ 启用 ⏸ 停用 ↑ 上移 ↓ 下移 ↻ 刷新 ↶ 还原 📁 备份 ✓ 应用									
序号	相关规则	来源IP	目的	拦截方式	日志选项	是否启用	说明	生效时间	操作
1	1200001	任意IP	...	检测	记录日志	已启用		全天	✎ ✕ ▶ ⏸ ↑ ↓
2	1200002	任意IP	...	检测	记录日志	已启用		全天	✎ ✕ ▶ ⏸ ↑ ↓
3	1200003	任意IP	...	检测	记录日志	已启用		全天	✎ ✕ ▶ ⏸ ↑ ↓
4	1200004	任意IP	...	检测	记录日志	已启用		全天	✎ ✕ ▶ ⏸ ↑ ↓
5	1200005	任意IP	...	拦截	记录日志	已启用		全天	✎ ✕ ▶ ⏸ ↑ ↓
6	1210001	任意IP	...	放行	记录日志	已启用		全天	✎ ✕ ▶ ⏸ ↑ ↓

9.1.3.1 添加高级访问控制策略

点击【添加】按钮，弹出【高级访问控制设置-添加】对话框，再点击【防护策略集】；

高级访问控制 - 添加

基本信息

拦截方式: 拦截

生效时间: 全天

是否启用: 启用 停用

日志选项: 记录日志 不记日志

说明: 请填写说明, 最长50字符

控制条件

来源与目的

防护策略集

内置规则

自定义规则

+ 添加

删除

刷新

策略名称	策略说明	操作
默认防护策略集	出厂默认防护策略	

第 1 页, 共 1 页

显示第 1 条到 1 条记录, 一共 1 条

保存

重置

取消

点击【添加】，弹出【防护策略集-添加】，规则编号您可以在内置规则中获得，例如 1200001。（您如果想填写多条规则编号，在填写【策略名称】后，可以在规则列表中选择多条规则）。

防护策略集 - 添加

基本信息

*策略名称: 策略名称无效, 最长20字符, 且不可以空格开头或结尾!

策略说明: 请填写策略说明, 最长50字符

规则配置

内置规则 (3)

自定义规则

规则分类

所有分类

HTTP状态码

SQL注入

URL自学习

XSS攻击

信息泄露

合规性检查

命令执行

扫描行为

挂马检测

程序上传

缓冲区溢出

脚本上传

脚本执行

规则列表

刷新

应用

规则号

请输入关键字

查询

规则号	规则名称	拦截方式	重定向页面	是否...	是否...	更新时间	
☒	1200001	SQL注入(AND/OR/XOR/HA...	拦截	默认提示页面	记录...	已启用	2010-02-21 16:25...
☒	1200002	SQL注入单引号	拦截	默认提示页面	记录...	已启用	2010-02-21 16:25...
☒	1200003	SQL注入关键字	拦截	默认提示页面	记录...	已启用	2010-02-21 16:25...
☐	1200004	SQL注入使用/**/	拦截	默认提示页面	记录...	已启用	2010-02-21 16:25...
☐	1200005	SQL注入中使用Union查询	拦截	默认提示页面	记录...	已启用	2010-02-21 16:25...
☐	1210001	SQL注入执行存储过程 v1	拦截	默认提示页面	记录...	已启用	2010-02-21 16:25...

第 1 页, 共 24 页

显示第 1 条到 30 条记录, 一共 705 条

保存

重置

取消

选择【拦截方式】，即如果匹配到此条策略所做的操作，例如“检测”；

公司网址: <http://www.yxlink.com/>

78

密级: 公开

基本信息

拦截方式: 检测

是否启用: 检测

说明: 拦截
拦截并阻断
放行

生效时间: 全

日志选项: 记录日志

控制条件

选择是否记录日志，例如“记录日志”；

基本信息

拦截方式: 检测

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

日志选项: ☒ 记录日志 ☐ 不记日志

说明: 请填写说明，最长50字符

选择【生效时间】，用来表示这条策略的生效时间，生效时间是在计划任务中添加的，添加方法具体参考[计划任务](#)；

生效时间: 全天

日志选项: 全天
工作时间
下班时间

选择【是否启用】，用来说明这条规则是否生效；

是否启用: ☒ 启用 ☐ 停用

填写【说明】，给这条规则添加说明信息；

说明: 请填写说明，最长50字符

【来源设置】：提供对来源 IP 的设置。这里我们选择单 IP（192.168.1.230），您可以根据您的需求自行选择添加；

来源设置

来源: ☒ 任意IP ☐ 单IP ☐ 地址对象

【目的设置】：提供对目的 IP 或者 URL 的设置。这里我们选择单一 IP（192.168.1.14），您可以根据您的需求自行选择添加；

目的设置

目的: ☒ 任意IP ☐ 单IP ☐ 地址对象

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以"/"结束。
URL: http://www.test.com/test.asp*, 其中"*"匹配任意内容。

点击【保存】按钮，该条访问控制策略被保存并返回上一级页面；

+ 添加 删除 ▶ 启用 停用 ↑ 上移 ↓ 下移 刷新 还原 备份 应用									
序号	相关规则	来源IP	目的	拦截方式	日志选项	是否启用	说明	生效时间	操作
1	全部规则	任意IP	任意IP	检测	记录日志	已启用		全天	
2	全部规则	任意IP	单IP (192.168.1.4)	检测	记录日志	已启用		全天	
3	1200003	任意IP	任意IP	检测	记录日志	已启用		全天	
4	1200003,12000...	单IP (192.168.9.230)	单IP (192.168.1.4)	检测	记录日志	已启用	Test	全天	
5	全部规则	任意IP	任意IP	拦截	记录日志	已启用		全天	

在【高级访问控制设置】页面点击【应用】按钮，让当前更改立即生效。

9.1.3.2 删除高级访问控制策略

选中选定某条高级访问控制策略；

点击【删除】，在弹出的对话框中选择【确定】。

9.1.3.3 修改高级访问控制策略

选中选定某条高级访问控制策略；

点击要修改策略的右侧对应图标，如图，

+ 添加 删除 ▶ 启用 停用 ↑ 上移 ↓ 下移 刷新 还原 备份 应用									
序号	相关规则	来源IP	目的	拦截方式	日志选项	是否启用	说明	生效时间	操作
1	全部规则	任意IP	任意IP	检测	记录日志	已启用		全天	

弹出【高级访问控制-修改】界面；

高级访问控制 - 修改

基本信息

拦截方式: 检测

生效时间: 全天

是否启用: ☒ 启用 ☐ 停用

日志选项: ☒ 记录日志 ☐ 不记日志

说明: Test

控制条件

来源与目的 策略集 (0) 内置规则 (2) 自定义规则 (0)

来源设置

目的设置

来源: ☐ 任意IP ☒ 单IP ☐ 地址对象

*来源IP: 192.168.9.230

目的: ☐ 任意IP ☒ 单IP ☐ 地址对象

*目的IP: 192.168.1.4

目的URL: 请填写目的URL

格式说明: 域名: http://*.test.com/*, 必须以/*结束。
URL: http://www.test.com/test.asp*, 其中**匹配任意内容。

✓ 保存

✕ 取消

修改完毕后点击【保存】。

9.1.3.4 高级访问控制策略的匹配顺序

本系统对于所有高级访问控制的策略，采取顺序匹配的原则，由上至下顺序匹配，按顺序匹配到的第一条策略进行访问控制，比如系统中存在两条或者多条来源以及目的 IP 相同的策略，则按匹配到的第一条策略进行控制，例如下图：

序号	相关规则	来源IP	目的	拦截方式	日志选项	是否启用	说明	生效时间	操作
1	全部规则	任意IP	任意IP	拦截并阻断	记录日志	已停用		全天	   
2	全部规则	任意IP	任意IP	拦截	记录日志	已启用		全天	   
3	全部规则	任意IP	任意IP	检测	记录日志	已启用		全天	   

来源 IP 192.168.1.230 的地址进行攻击的话，则实际采取动作是拦截并阻断，因为第一条策略被匹配到。

策略的优先级顺序可以通过每条策略最后的   按钮来进行调整。

9.1.3.5 高级访问控制策略应用示例

- 示例一：例如 URL 为 <http://www.test.com/addnews.asp> 这个页面在添加新闻的时候被 1300004 命令执行关键词这个规则误拦截，需要将这个页面针对这条规则设置为放行。您可以参照以下步骤进行添加高级访问控制策略：

1. 规则编号填写 1300004
2. 拦截方式：放行
3. 是否记录日志：不记录
4. 生效时间：全天
5. 是否启用：启用
6. 说明：addnew.asp 停用 130004 规则
7. 来源 IP 任意
8. 目的 IP 任意
9. URL 填写 <http://www.test.com/addnews.asp>*

高级访问控制 - 修改

基本信息

拦截方式：

放行

是否启用：

启用

停用

说明：

addnew.asp停用1300004规则

生效时间：

全天

日志选项：

记录日志

不记录日志

控制条件

来源与目的

策略集 (0) 内置规则 (1) 自定义规则 (0)

来源设置

来源：

任意IP

单IP

地址对象

目的设置

目的：

任意IP

单IP

地址对象

目的URL：

http://www.test.com/addnews.asp*

格式说明：域名：http://*.test.com/*，必须以/**结束。

URL：http://www.test.com/test.asp*，其中**匹配任意内容。

保存

取消

公司网址：<http://www.yxlink.com/>

81

密级：公开



提示:

- 1, 如果还需要精确到来源和目的 IP 进行放行操作的话, 只需要在对应位置进行设置即可。
- 2, 如果高级访问控制匹配的【URL】中包含“//”, 请用“/”或者“?”代替“//”, 如需匹配:
“<http://www.test.com/portal/?id=26162&link=http://www.baidu.com>” 替换 URL 为:
“<http://www.test.com/portal/?id=26162&link=http://www.baidu.com>” 或
“<http://www.test.com/portal/?id=26162&link=http://www.baidu.com>”。

9.1.4 HTTPS 透明防护

HTTPS 透明防护是依赖透明网桥来进行 HTTPS 防护,当出现对防护的网站进行 https 攻击时,设备会阻碍攻击并产生入侵记录。配置 HTTPS 透明防护首先需要配置防护端口, HTTPS 防护引擎数等信息。配置信息如下图:

HTTPS透明防护 - 设置

是否启用: ☒ 启用 ☐ 停用

*防护端口: 443

提示: 端口限制1-65535, 多个端口请用“|”隔开。

*HTTPS防护引擎数: 1

生效网桥: ☒ wafprote... ☐ xxx ☒ test ☐ proxy

保存 关闭

注意: HTTPS 防护仅对已选的“生效网桥”生效。

HTTPS 透明配置需要配置证书, 证书的方式有两种, 一种是系统生成证书, 另一种是用户上传证书。包含域名则是需要防护的网址, 可填写 IP 地址或 URL。系统生成证书方式配置如下:

HTTPS透明防护设置 - 修改

*名称: test

是否启用: ☒ 启用 ☐ 停用

证书设置: ☐ 上传证书 ☒ 系统生成证书

包含域名: 192.168.99.23

保存 刷新 取消

上传证书方式如下：

HTTPS透明防护 - 修改
✕

***名称:**

是否启用: ☒ 启用 ☐ 停用

证书设置: ☒ 上传证书 ☐ 系统生成证书

证书公钥:

证书私钥:

证书密码:

***包含域名:**

注意: HTTPS透明防护仅对配置了IP的网桥生效, 与反向代理的HTTPS2、HTTPS功能冲突, 请不要同时开启!

✓ 保存
↻ 刷新
✕ 取消

注：包含域名可以填写 ip，也可以填写服务器 443 端口的域名

9.1.5 智能阻断

智能阻断是系统提供的动态识别黑客攻击行为的高级功能。而智能数据挖掘是对入侵记录较智能阻断更深入的分析，挖掘出隐藏在其中的黑客，并对他进行阻断。一般来说，当黑客发起攻击时，会尝试从多个方面来攻击 Web 服务器，因此它与普通用户无意触发告警的行为有一定的差异性。黑客恶意攻击的危害性较大，因此我们需要尽可能快的将隐藏在正常用户中间的黑客挖掘出来，然后将其 IP 加入到阻断列表中，禁止该 IP 在一段时间内访问任何被本设备防护的 Web 服务器。

智能阻断设置

智能阻断: ☒ 开启 (启用后, 系统将根据设定条件, 识别频繁攻击的来源IP地址, 在一段时间内拒绝该IP地址的访问。)

*统计周期/秒:

*入侵次数:

触发多个URL: ☒ 触发2个或以上数目的不同URL (包含参数)

*触发规则 (集) 数:

智能数据挖掘设置

数据挖掘: ☒ 开启 (启用后, 系统将根据入侵记录的历史日志, 分析黑客的持续攻击行为, 加以惩罚性阻断。)

灵敏度: ☐ 高 ☒ 中 ☐ 低

说明: 灵敏度越高, 阻断能力越强, 请根据实际情况选择。

基准阻断时间: ☐ 高 ☒ 中 ☐ 低 ☐ 自定义/秒

说明: 实际阻断时间根据攻击行为的严重程度和基准阻断时间共同确定。

💾 保存
✓ 应用

是否启用：智能阻断的开关。勾选上点击【应用】将会启用智能阻断模块。

- 统计周期：设定入侵记录的统计周期。在该周期内满足触发阻断条件，将会将入侵 IP 添加到阻断列表中。
- 入侵次数：设定触发智能阻断需要满足的入侵次数。如果在统计周期内入侵次数超过此处设定的次数，该入侵 IP 将会被加入到阻断列表中。
- 触发 2 个以上不同的 URL（包含参数）：选中后必须满足在统计周期内入侵次数超过设定的次数，且入侵的 URL 数目必须大于或等于 2 个，入侵 IP 才会被加入到阻断列表中。
- 触发的规则（集）数目：设定在智能阻断需要触发的规则集数目，满足在统计周期内，入侵次数大于设定次数，触发的规则集大于设定的值，则该入侵 IP 才会被加入到阻断列表中。
- 数据挖掘：数据挖掘的开关，勾选上点击【应用】将会启用智能数据挖掘模块。
- 灵敏度：智能数据挖掘的灵敏度设置，设置为高的时候，可能会产生误报。
- 基准阻断时间：基准阻断时间设置，高：10 小时，中：1 小时，低：10 分钟。实际阻断时间根据攻击行为的严重程度和基准阻断时间共同确定。



注意：

应用防扫描功能需在内置规则中开启对应的防扫描规则。

9.1.6 木马上传检测

开启木马上传检测功能可以有效的检测后端服务器是否有木马上传入侵，防止木马入侵后端服务器。

木马上传检测

木马上传检测: ☒ 开启木马上传检测

*检测文件大小上限/字节: 2048000

超过上限执行动作: 放行

检测文件类型: *

说明: 文件类型用'|'隔开, '*'匹配任何文件类型。常见文件类型为: php|asp|aspx|jsp|jpg|gif|png|rar|zip|pdf|doc。

脚本文件上传处理方式: ☒ 直接拦截 ☐ 智能识别

说明: 脚本文件是指后缀名为php|asp|aspx|jsp的文件。

检测灵敏度: ☒ 高 ☐ 中 ☐ 低

说明: 灵敏度越高, 漏报越少, 但可能会引起误拦截。请根据实际情况选择。

保存

应用

9.1.7 防盗链设置

防止未经授权的网站盗用设备所防护网站的资源，并跳转到指定的重定向页面；允许信任的网站（referer）访问受保护的资源。

防盗链工作原理如下：

用户访问某 URL 的时候，如果该 URL 是受保护的，则去判断 Referer 是否是信任的，如果是信任的，则允许访问；如果 Referer 不是信任的，则不允许访问受保护的资源，但可以访问未受保护的资源；当 Referer 为空的时候，则根据【Referer 为空时访问】的设置判断是否允许访问；当不允许访问且设置重定向页面的时候，跳转到指定的重定向页面。

公司网址：<http://www.yxlink.com/>

84

密级：公开

+ 添加 删除 启用 停用 上移 下移 刷新 应用 保护的URL 请输入关键字 查询							
序号	保护的URL	信任的Referer	保护的资源类型	Referer为空时	重定向页面	是否	说明
1	http://www.test.com/*	http://baidu.com/*	jpg gif bmp avi flv rmvb mp3...	允许访问	<无>	已启...	
2	http://yxlink.com/*	http://www.google.com/*	jpg gif bmp avi flv rmvb mp3...	允许访问	<无>	已启...	

- **【添加】**：可以填写保护的 URL，是否启用，说明，信任的 Referer，保护的资源类型，Referer 为空时是否允许访问，以及违反防盗链规则的重定向页面，点击**【添加】**，弹出**【防盗链-添加】**页面。

防盗链设置 - 添加

*保护的URL: 请填写保护的URL，最长1024字符
 格式: http://www.test.com/*，其中 "*" 匹配任何内容。

是否启用: ☒ 启用 ☐ 停用

说明: 请填写说明，最长50字符

*信任的Referer: 请填写信任的Referer
 格式: http://www.123.com/*，其中 "*" 匹配任何内容。支持多个referer，每个referer各占一行。

*保护的资源类型: jpg|gif|bmp|avi|flv|rmvb|mp3|wma|rar|zip
 说明: 用 "|" 隔开， "*" 匹配任何资源类型。默认保护的资源类型为: jpg|gif|bmp|avi|flv|rmvb|mp3|wma|rar|zip。

Referer为空时: ☒ 允许访问 ☐ 禁止访问

重定向页面: <无>

保存

重置

取消

【保护的 URL】：需要保护的 URL。

【是否启用】：该条规则是否启用。

【说明】：对该条规则的说明。

【信任的 Referer】：信任的 Referer 可以访问受保护的资源。

【保护的资源类型】：防止盗用的资源类型。

【Referer 为空时访问】：Referer 为空时是否允许访问。

【重定向页面】：触发防盗链规则时指向的重定向页面。

- **【修改】**：对已经添加的防盗链规则进行“修改”操作。
- **【删除】**：“删除”已经添加的防盗链规则。
- **【启用】**：“启用”某条防盗链规则。
- **【停用】**：“停用”某条防盗链规则。
- **【刷新】**：“刷新”这个页面。
- **【应用】**：点击“应用”按钮以便使您的设置立即生效。

9.1.6.1 防盗链添加示例

某 Web 服务器的图片被其他网站盗链，造成服务器负荷过大，可配置如下防盗链规则，防止未经授权的网站盗用图片资源。

防盗链设置 - 添加

*保护的URL:

格式: http://www.test.com/*, 其中 "*" 匹配任何内容。

是否启用: ☒ 启用 ☐ 停用

说明:

*信任的Referer:

格式: http://www.123.com/*, 其中 "*" 匹配任何内容。支持多个referer, 每个referer各占一行。

*保护的资源类型:

说明: 用 "|" 隔开, "*" 匹配任何资源类型。默认保护的资源类型为: jpg|gif|bmp|avi|flv|rmvb|mp3|wma|rar|zip。

Referer为空时: ☒ 允许访问 ☐ 禁止访问

重定向页面:

✓ 保存

↺ 重置

✕ 取消

- 保护的 URL: http://www.test.com/*;
- 是否启用: 启用;
- 说明: 防止 www.test.com 网站的图片被盗链;
- 信任的 Referer: http://www.baidu.com/*(允许 www.baidu.com 链接本站图片资源) ;
- 保护的资源类型: jpg|gif|bmp;
- Referer 为空时访问: 允许;
- 重定向页面: 默认提示页面。

9.1.8 CSPF 防护设置

9.1.9 Flood 防护设置

DoS 攻击——拒绝服务 (Denial of Service) 攻击, 基本原理是: 攻击者使用个人电脑向服务器发送大量的垃圾信息, 拥堵服务器的网络, 并加大服务器处理数据的负担, 降低服务器 CPU 和内存的工作效率。但随着技术的进步, 服务器的性能远远的超越了普通的个人电脑, 所以像 DoS 这样一对一的攻击已经起不到任何作用了, 于是出现了 DDoS 攻击——分布式拒绝服务 (Distributed Denial of Service) 攻击。其实原理还是一样, 只不过变成了多对一, 可能是数以万计的个人电脑去同时使用 DoS 方式攻击一台服务器, 最终导致服务器瘫痪。

攻击者借助代理服务器生成指向受害主机的合法请求, 实现 DOS(Denial of Service)和伪装一般称之为 CC(Challenge Collapsar)。CC 攻击跟 DDOS 攻击本质上是一样的, 都是以消耗服务器资源为目的, 目前看来, 它们主要针对 Web 应用程序比较消耗资源的地方进行疯狂的 HTTP 请求。

本设备可以有效的过滤这些攻击的流量, 维持服务器的性能, 防止服务器瘫痪。

9.1.8.1 DDOS 日志

该页面记录了所有的 DDOS 攻击事件，您可以通过本页面了解所有发生的 DDOS 攻击事件，可以实时的看到被加入黑名单中的 IP。

DDOS防护日志 CC攻击日志 CC阻断状态

删除 清空 刷新 筛选 导出 请选择查看日期: 请选择查看日期

序号	时间	日志内容	操作
13	2018-04-27 14:02:42	发生TCP Flood (SYN)攻击, 正在清洗DDOS流量	删除
12	2018-04-27 14:02:42	全部DDOS攻击已经消退	删除
11	2018-04-27 14:02:42	ICMP Flood攻击已经消退	删除
10	2018-04-27 14:02:05	发生ICMP Flood攻击, 正在清洗DDOS流量	删除
9	2018-04-27 14:02:05	全部DDOS攻击已经消退	删除
8	2018-04-27 14:02:05	TCP Flood攻击已经消退	删除
7	2018-04-27 14:00:51	发起了SYN Flood攻击, 加入黑名单	删除
6	2018-04-27 13:59:00	发生TCP Flood (SYN)攻击, 正在清洗DDOS流量	删除
5	2018-04-27 13:59:00	全部DDOS攻击已经消退	删除
4	2018-04-27 13:59:00	UDP Flood攻击已经消退	删除
3	2018-04-27 13:57:09	发起了UDP Flood攻击, 加入黑名单	删除
2	2018-04-27 13:57:09	发生UDP Flood攻击, 正在清洗DDOS流量	删除
1	2018-04-27 13:56:32	DDOS检测引擎启动	删除

- 删除：选中某条记录，点击【删除】即可删除该条记录。
- 筛选：根据日志内容和时间进行筛选。例如查找所有 192.168.1.15 在 2011 年 1 月 24 日的相关的 CC 日志，点击【筛选】就可以筛选出所有的符合条件的 CC 日志。
- 快速查询：可以选择一个指定的日期，查询到此日期的 DDOS 攻击日志。
- 导出日志：分别选择开始日期和结束日期，可以导出 CSV 格式的日志文件，记录了该段日期内的 DDOS 攻击日志。

DDOS防护日志 - 导出

*开始时间: 2018-04-27

*结束时间: 2018-04-27

导出 关闭

9.1.8.2 DDOS 防护设置

本页面设置与 DDOS 防护相关的参数。如图。

DDoS阈值设置

DDoS防护: ☒ 开启DDoS防护

*网络流量/Mbps: 100

*总流量触发阈值/pps: 10000

*TCP包触发阈值/pps: 10000

*SYN Flood触发阈值/pps: 10000

*SYN Flood比例触发阈值/%: 5

*ACK Flood触发阈值/pps: 10000

*RST Flood触发阈值/pps: 10000

*其他TCP Flood触发阈值/pps: 10000

*UDP包触发阈值/pps: 10000

*ICMP包触发阈值/pps: 1000

分布式SYN Flood防护: ☒ 开启分布式SYN Flood防护

*防御等级: 4

防御等级说明: 默认为4; 等级越小, 防御能力越强, 但可能误拦截; 较大的等级适合网络延迟比较大的环境。

阈值设定: ☐ 使用推荐值 ☒ 自定义

*单IP 总流量触发阈值/pps: 1000

*单IP TCP包触发阈值/pps: 1000

*单IP SYN Flood触发阈值/pps: 100

(SYN数据包占总数据包的百分比。)

*单IP ACK Flood触发阈值/pps: 1000

*单IP RST Flood触发阈值/pps: 1000

*单IP 其他TCP Flood触发阈值/pps: 1000

*单IP UDP包触发阈值/pps: 1000

*单IP ICMP包触发阈值/pps: 100

禁止UDP数据包

禁止UDP数据传输: ☐ 开启 (启用后, 所有使用UDP协议的通信将被禁止, 包括使用UDP协议的DNS解析服务。)

禁止ICMP数据包

禁止ICMP数据传输: ☐ 开启 (启用后, 所有使用ICMP协议的通信将被禁止, 包括使用ICMP协议的PING请求。)

禁止ICMP报文分组: ☐ 开启 (使用此功能需要同时开启DDoS防护功能。)

禁止大于1024字节的ICMP报文: ☐ 开启 (使用此功能需要同时开启DDoS防护功能。)

- DDoS 设置: 可以根据您的网络环境流量大小来进行设定, 您只需要在网络流量选择中输入当前网络流量的大小 (可以输入 1--10000Mbps), 再点击“推荐阈值”, 系统会根据您设定的网络流量数值自动生成最适合您网络环境的的阈值信息, 当然您也可以对每一个阈值进行单独设定。
- 勾选【禁止所有 UDP 协议的通信】后, 所有经过本设备的 UDP 协议的网络数据将会不允许通过。
- 勾选【禁止所有 ICMP 协议的通信】后, 所有经过本设备的 ICMP 协议的网络数据将会不允许通过。
- 勾选【禁止 ICMP 报文分组】后, 所有经过本设备的分组的 ICMP 报文将会不允许通过。
- 勾选【禁止大于 1024 字节的 ICMP 报文】后, 所有经本设备的大于 1024 字节的 ICMP 报文将会不允许通过。

注意:

在网络正常的情况下, 请不要勾选【禁止所有 UDP 协议的通信】和【禁止所有 ICMP 协议的通信】。因为禁止所有 UDP 协议的通信可能会使得一些服务工作不正常, 例如 DNS 解析服务。而【禁止所有 ICMP 协议的通信】则会导致一些基于 ICMP 的程序工作不正常, 例如无法使用 PING 来探测主机网络是否可达。

9.1.8.3 CC 攻击日志

该页面记录了所有的 CC 攻击事件, 您可以通过本页面了解所有发生的 CC 攻击事件。

公司网址: <http://www.yxlink.com/>

88

密级: 公开

DDoS防护日志 CC攻击日志 CC阻断状态

删除 解除阻断 筛选 清除筛选 刷新 清空			
序号	时间	日志内容	操作
5	2018-04-27 14:45:12	来自www.ttt.com，链接了本地资源，超过referer访问速率限制，已被阻止。	删除
4	2018-04-27 14:44:21	来自www.test.com，链接了本地资源，超过referer访问速率限制，已被阻止。	删除
3	2018-04-27 14:37:26	来源IP地址：■■■■■■■■■■，超过访问速率限制，已被阻止。	删除
2	2018-04-27 14:24:39	来源IP地址：■■■■■■■■■■，超过访问速率限制，已被阻止。	删除
1	2018-04-27 14:20:52	来源IP地址：■■■■■■■■■■，超过访问速率限制，已被阻止。	删除

第 1 页, 共 1 页
显示第 1 条到 5 条记录，一共 5 条

下面介绍一下防 CC 日志页面的主要功能菜单：

- 删除：选中某条记录，点击【删除】即可删除该条记录。
- 清空：点击【清空】，可以清空所有的 CC 攻击日志。
- 筛选：根据日志内容和时间进行筛选。例如查找所有 192.168.1.15 在 2011 年 1 月 24 日的相关的 CC 日志，点击【开始筛选】就可以筛选出所有的符合条件的 CC 日志。

CC攻击日志 - 筛选

时间: 2018-04-27

日志内容: 请输入包含的日志内容

筛选
重置
取消

9.1.8.4 CC 阻断状态

该页面用于显示系统当前正在阻止的 IP，Referer 的 URL 以及阻止的起始、终止时间等信息。您可以根据需要，解除正在被阻止的 IP 以及 Referer 的 URL。

DDoS防护日志 CC攻击日志 CC阻断状态

[解除阻止](#) [刷新](#)

序号	阻断原因	内容	开始时间	结束时间	操作
1	Referer的URL	www.ttt.com	2018-04-27 15:05:35	2018-04-27 15:06:35	解除阻止

第 1 页共 1 页

显示第 1 条到 1 条记录，一共 1 条

- 解除阻止：选择一条阻止记录，然后点击【解除阻止】按钮，即可让该 IP 或者 URL 解除阻断状态，该 IP 或者 URL 的后续正常访问将被允许。
- 批量解除阻止：选择多条阻止记录，点击【解除阻止】按钮，即可让这一组 IP 或者 URL 解除阻止状态，该组 IP 或者 URL 的后续正常访问将被允许。

9.1.8.5 CC 防护设置

基本设置

基本设置

*阻止访问时间/秒: 600

可以设置被阻止的 IP、Referer 的 URL 被阻止访问的时间长度。例如：来自于 192.168.1.19 主机的 CC 攻击被拦截，则所有来自于 192.168.1.19 主机的后续正常访问将会被阻止 60 秒，60 秒后自动恢复正常访问。

来源 IP 防 CC 设置

来源IP防CC

来源IP地址访问速率限制: ☒ 开启 (启用后，来源IP地址对目的URL的访问次数超过设定上限的，禁止该IP地址的任何后续访问)

*统计周期/秒: 10

*请求次数上限: 3

可以选择来源 IP 防 CC 功能的开启和关闭，设置统计的周期和统计周期内允许 Http 请求次数的上限。例如：开启该功能后，来源 IP 地址 192.168.1.19 在统计周期内（10 秒）对被防护网站服务器的请求次数超过上限（500 次），则 192.168.1.19 的所有后续正常访问将被阻止，并且记录到防 CC 日志中，直到阻止访问时间结束。

Referer 防 CC 设置

Referer防CC

Referer访问速率限制: ☒ 开启 (启用后, 对于Referer中相同的URL, 累计访问次数超过设定上限的, 禁止具有相同Referer URL的任何来源IP地址的访问)

*统计周期/秒: 10

*请求次数上限: 500

可以选择 Referer 防 CC 功能的开启和关闭, 设置统计的周期和统计周期内允许 Referer 请求次数的上限。例如: 开启该功能后, 来自于 www.fromcc.com 网站的引用请求 (例如: http://www.fromcc.com/news/view.htm) 在统计周期内的访问次数 (10 秒) 超过请求次数上限 (100 秒), 则所有 Referer URL 为 http://www.fromcc.com/news/view.htm 的访问将被阻止, 并且记录到防 CC 日志中, 直到阻止访问时间结束。

特定 URL 防 CC 设置

特定URL防CC

目的URL访问速率限制: ☒ 开启 (启用后, 来源IP地址的访问次数超过设定上限的, 禁止该IP地址的任何后续访问)

*统计周期/秒: 10

目的URL列表

[+ 添加](#) [删除](#) [刷新](#)

序号	目的URL	周期内请求次数上限	操作
1	http://*.test.com/test.asp*	500	编辑 删除

可以选择特定目的 URL 防 CC 功能的开启和关闭, 设置统计的周期和统计周期内该页面允许被请求次数的上限, 相对于来源 IP 防 CC, 这里进行了更加精细的控制。例如: 开启该功能后, 某一个 IP 对 http://www.test.com/test.html 在统计周期内的访问次数超过请求次数上限, 则该 IP 地址 192.168.1.19 的所有后续正常页面访问将被阻止, 并且记录到防 CC 日志中, 直到阻止访问时间结束。

9.1.8.6 Flood 访问控制

对防 CC 功能进行细粒度的控制, 设置允许和禁止的 IP 以及 URL。

DDOS防护设置 CC防护设置 Flood访问控制

[+ 添加](#) [删除](#) [刷新](#) [应用](#)

序号	访问控制类型	内容	操作
1	DDOS, 允许的来源IP	192.168.9.17	编辑 删除
2	CC, 禁止Referer的URL	http://www.test.com/	编辑 删除
3	CC, 禁止的来源IP	192.168.9.22	编辑 删除

添加策略

1. 点击【添加】，选择【访问控制类别】例如：允许来源的 IP；



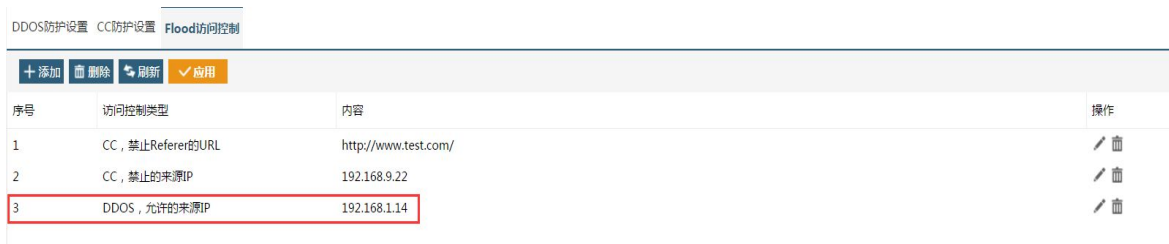
The dialog box titled "Flood访问控制 - 添加" contains a dropdown menu for "访问控制类型" (Access Control Type) with the following options: "CC, 禁止的来源IP", "CC, 允许的来源IP", "CC, 禁止Referer的URL", "CC, 允许Referer的URL", "DDOS, 允许的来源IP", and "DDOS, 禁止的来源IP". The "内容" (Content) field is currently empty.

2. 填写【内容】，例如：192.168.1.14；



The dialog box titled "Flood访问控制 - 添加" shows the "访问控制类型" (Access Control Type) set to "DDOS, 允许的来源IP" and the "内容" (Content) field filled with "192.168.1.14". At the bottom, there are three buttons: "保存" (Save), "重置" (Reset), and "取消" (Cancel).

3. 点击【保存】，添加成功，如下图：



The screenshot shows the "Flood访问控制" (Flood Access Control) settings page. It features a table with the following data:

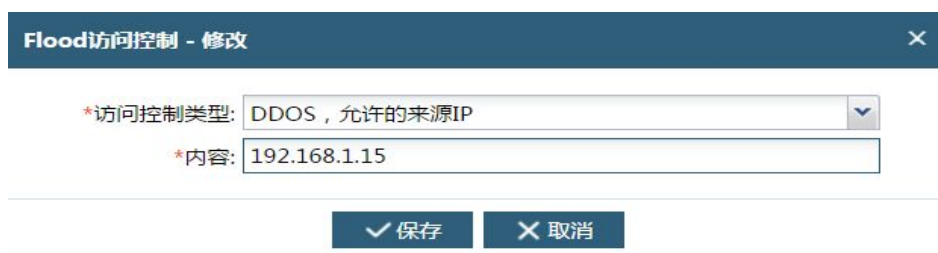
序号	访问控制类型	内容	操作
1	CC, 禁止Referer的URL	http://www.test.com/	✎ ✖
2	CC, 禁止的来源IP	192.168.9.22	✎ ✖
3	DDOS, 允许的来源IP	192.168.1.14	✎ ✖

Buttons at the top: + 添加, 删除, 刷新, 应用.

4. 点击【应用】，使添加的规则生效。

修改策略

1. 选中要修改的策略，点击右侧【修改】图标；



The dialog box titled "Flood访问控制 - 修改" shows the "访问控制类型" (Access Control Type) set to "DDOS, 允许的来源IP" and the "内容" (Content) field filled with "192.168.1.15". At the bottom, there are two buttons: "保存" (Save) and "取消" (Cancel).

2. 修改完毕后点击【保存】；
3. 点击【应用】，使修改后的策略生效。

删除策略

1. 选中要修改的策略，点击【删除】；

操作确认



是否确认删除数据？

是

否

2. 点击【是】删除该条规则；
3. 点击【应用】，使原有的策略生效。

9.1.8.7 防扫描设置

防扫描功能能拦截扫描器对设备所防护的 Web 服务器的扫描行为，对主流的扫描器如：Appscan, WVS 等具有较好的防护效果。

在内置规则中，编号为 1950001 和 1950002 的规则对应本功能设置，如果两条规则都没有启用，则防扫描功能不生效。基本访问控制和高级访问控制对防扫描功能有效。

防扫描设置

防扫描：☒ 开启防扫描（启用后，系统将根据设置的灵敏度，阻止各种恶意的扫描行为。）

灵敏度：☐ 高 ☒ 中 ☐ 低

说明：灵敏度越高，防扫描能力越强。针对低速扫描行为，设置为高；当有误拦截时，设置为低。

保存

应用

防扫描：启用，停用防扫描功能。

灵敏度：对检测的灵敏度设置，灵敏度越高，防扫描能力越强。针对低速扫描行为，设置为高；当有误拦截时，设置为低。



注意：

应用防扫描功能需在内置规则中开启对应的防扫描规则。

9.1.10 来源 IP 解析

只对信任的代理地址发起的 HTTP 请求，进行真实来源 IP 地址的解析。一般作为 CDN 白名单来使用，可填写信任的 CDN 代理服务器的 IP 地址。

序号	起始IP	终止IP	是否启用	说明	操作
1	0.0.0.0	255.255.255.255	启用	全部地址范围	
2	::	:::ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	启用	全部IPv6地址范围	

- 添加：输入需要解析的起始，终止 IP 地址，点击【应用】按钮。

9.2 对象配置

9.2.1 地址对象

地址对象可以手动添加 IP/IP 段，基本访问控制和高级访问控制可直接调用一个或多个地址对象。同时地址对象可以自定义来源地理位置。

+ 添加 删除 刷新					名称	请输入关键字
序号	名称	IP/IP段	描述	地理位置	操作	
1	内部	192.168.5.4-192.168.5.100		内部	✎ 删除	
2	服务器	192.168.9.1/24		99网络服务器	✎ 删除	
3	192.168.88.1	192.168.8.1			✎ 删除	

点击【添加】

填写 IP/IP 段、名称、描述、地理位置，点击【保存】

地址对象 - 修改

*IP/IP段: 192.168.5.4-192.168.5.100

*名称: 内部

描述: 内部网络

地理位置: 来自内部

✓ 保存

✕ 取消

9.2.2 计划任务

本页面提供查看、添加和修改计划任务的功能。在防篡改和高级访问控制功能中需要使用计划任务。

+ 添加 删除 刷新				
序号	名称	说明	类型	操作
1	全天	每天, 00:00 - 24:00	每天	✎
2	工作时间	启动任务的时间为：工作日 08:00-17:00。	每周	✎ 删除
3	下班时间	启动任务的时间为：工作日 00:00-08:00和17:00-24:00，周六和周日 00:00-24:00。	每周	✎ 删除

第 1 页共 1 页

显示第 1 条到 3 条记录，一共 3 条

9.2.2.1 添加计划任务

点击【添加】；

计划任务 - 添加

基本信息

*名称: 测试任务

说明: 测试任务

时段设置

类型: ☒ 每天

☐ 每周

*每天: 请填写每天时段设置



✓ 保存

↺ 重置

✕ 取消

填入【名称】和【说明】，点击【“+”按钮】；

添加时间段 - 每天

08:30



至

17:30



✓ 确定

✕ 取消

选择起始时间和开始时间，点击【确定】；

计划任务 - 添加

基本信息

*名称: 测试任务

说明: 测试任务

时段设置

类型: ☒ 每天

☐ 每周

*每天: 08:30-17:30



✓ 保存

↺ 重置

✕ 取消

点击【保存】，计划任务添加成功，您可以在添加防篡改和访问控制的时候选择它，具体参照[防篡改设置](#)与[添加访问控制规则](#)。

9.2.2.2 修改计划任务

选中要修改的计划任务，点击【修改】；

计划任务 - 修改



基本信息

*名称: 下班时间
说明: 启动任务的时间为: 工作日 00:00-08:00和17:00-24:00, 周六和周日

时段设置

类型: ☐ 每天 ☒ 每周

*周日: 00:00-24:00 +
*周一: 00:00-08:00,17:00-24:00 +
*周二: 00:00-08:00,17:00-24:00 +
*周三: 00:00-08:00,17:00-24:00 +
*周四: 17:00-24:00,00:00-08:00 +
*周五: 00:00-08:00,17:00-24:00 +
*周六: 00:00-24:00 +

✓ 保存

✕ 取消

修改完毕后点击【保存】。

9.2.2.3 删除计划任务

选中要删除的计划任务，点击【删除】，弹出确定对话框；

操作确认



是否确认删除数据？

是

否

点击【是】，删除成功。

i 提示：

系统提供 3 个默认的计划任务。名称为“全天”的计划任务是不可以删除的。时间段的添加支持多个时间段，例如：00:00-08:00,17:00-24:00。您可以根据您的需要自由添加。

9.2.3 重定向页面

此功能主要实现在本设备拦截掉用户访问的时候能够给予用户特定的重定向页面。便于管理员定位拦截的记录或者给予用户所对应的提示信息。

+ 添加 删除 刷新 应用 名称 请输入关键字 查询				
序号	名称	描述	更新时间	操作
1	默认提示页面	返回拦截的事件id给浏览器	2012-08-09 14:45:34	/ o
2	301跳转页面	跳转到一个指定的网页	2012-06-28 14:39:11	/ o
3	404页面不存在	模仿Apache的页面不存在	2012-06-28 14:44:23	/ o
4	服务器错误页面	返回模仿的服务器错误页面	2012-06-28 14:49:25	/ o

重定向页面有如下功能：

1. 使得拦截显示更友好的提示页面。
2. 可以自定义跳转到预先设置的页面。

当使用“默认提示页面”时，可以方便的辅助管理员排除误报。“默认提示页面”会返回拦截的事件 id 给浏览器，管理员可以根据这个 id 快速定位到入侵记录中的数据。方便进一步排查问题。

9.2.3.1 添加重定向页面

点击【添加】按钮，弹出【重定向页面-添加】对话框

- 名称：重定向页面的名称。
- 描述：对重定向页面的描述。
- HTTP 状态码：Web 服务器 HTTP 返回的三位状态码。
- 服务器名：Web 服务器名称。
- 额外信息：用于在 HTTP 返回头部中添加额外的头部信息，比如 Cookie 和 Location 等。当使用 301 重定向时，需要在此处通过 Location 指定跳转的页面。
- 页面返回内容：返回的 HTTP 协议头部之外的页面内容，此部分内容可以在浏览器中显示。

9.2.3.2 重定向页面添加示例

为规则指定重定向页面，当规则被触发后，跳转到指定的页面，为用户提供更良好的体验。

重定向页面 - 添加

基本信息

*名称: 301跳转页面

描述: 跳转到一个指定的网页

头部信息

*HTTP状态码: 200 OK

*服务器名: Microsoft-IIS/6.0

额外信息: Location: http://www.yxlink.com/

页面返回内容

HTML代码: 请填写页面HTML代码

预览

保存

重置

取消

1. 名称: 301 跳转页面;
 2. 描述: 跳转到一个指定的网页;
 3. HTTP 状态码: 301 Moved Permanently;
 4. 额外信息: Location: http://www.yxlink.com;
 5. 点击【保存】;
 6. 打开“内置规则”;
- 修改: 选中需要修改的重定向页面, 或双击需要修改的重定向页面, 弹出【重定向页-修改】。

重定向页面 - 修改

基本信息

*名称: 301跳转页面

描述: 跳转到一个指定的网页

头部信息

*HTTP状态码: 200 OK

*服务器名: Microsoft-IIS/6.0

额外信息: Location: http://www.yxlink.com/

页面返回内容

HTML代码: 请填写页面HTML代码

预览

保存

取消

- 删除：选中需要删除的重定向页面，点击【删除】，即可删除该重定向页面。号为 1,2,3,4 的内置重定向页面不能被删除。
- 刷新：点击【刷新】，当前页面的数据被刷新。
- 应用：使当前重定向页面设置生效。
- 页面预览：对重定向页面进行预览。

9.2.4 蜘蛛设置

蜘蛛设置功能能够对搜索引擎的网页抓取行为进行“放行”操作，避免搜索引擎的蜘蛛被设备误拦截。设备中已经内置了一些常见的搜索引擎蜘蛛的 IP 地址。

+ 添加 修改 删除 启用 停用 刷新 应用 输入条件： 查询				
IP地址	说明	类型	是否启用	更新时间
类型: 163蜘蛛(9 条记录)				
202.108.36.0 - 202.108.36.255	北京市 163蜘蛛 (联通)	163蜘蛛	启用	2012-04-28 09:34:33
202.108.44.0 - 202.108.45.255	北京市 163蜘蛛 (联通)	163蜘蛛	启用	2012-03-14 10:21:25
202.108.5.0 - 202.108.5.255	北京市 163蜘蛛 (联通)	163蜘蛛	启用	2012-03-14 10:21:25
202.108.9.0 - 202.108.9.255	北京市 163蜘蛛 (联通)	163蜘蛛	启用	2012-03-14 10:21:25
220.181.31.0 - 220.181.31.255	北京市 163蜘蛛 (电信)	163蜘蛛	启用	2012-03-14 10:21:25
222.185.245.0 - 222.185.245.255	常州市 163蜘蛛 (电信)	163蜘蛛	启用	2012-03-14 10:21:25
202.106.186.0 - 202.106.186.255	北京市 163蜘蛛 (联通)	163蜘蛛	启用	2012-03-14 10:21:25
220.181.12.0 - 220.181.15.255	北京市 163蜘蛛 (电信)	163蜘蛛	启用	2012-03-14 10:21:25
220.181.28.0 - 220.181.28.255	北京市 163蜘蛛 (电信)	163蜘蛛	启用	2012-03-14 10:21:25
类型: 3721蜘蛛(1 条记录)				
类型: Baidu蜘蛛(13 条记录)				
类型: Bing蜘蛛(1 条记录)				
类型: Google蜘蛛(21 条记录)				
类型: MSN蜘蛛(8 条记录)				

添加：可以填写单独的 IP、IP 段、是否启用、蜘蛛类型、说明，来添加相关的蜘蛛信息。（注意：您可以在蜘蛛类型后直接输入新的蜘蛛类型以便添加一个新的蜘蛛类型。）

蜘蛛设置 - 添加

单IP

IP段

 -

是否启用:

启用

停用

蜘蛛类型:

请选择类型

说明:

标记为蜘蛛的来源IP或者IP地址段将被直接放行，对数据报文不做检测。

保存

重置

取消

- 修改：对已经添加的蜘蛛 IP 进行“修改”操作。
- 删除：“删除”已经添加的蜘蛛 IP。
- 启用：“启用”某条蜘蛛的 IP。
- 停用：“停用”某条蜘蛛的 IP。
- 刷新：“刷新”这个页面。

- 应用： 当您修改了这个页面的内容后，可以点击“应用”按钮以便使您的设置立即生效。

9.3 防护策略

9.3.1 自定义规则

9.3.1.1 查看自定义规则

本页面设置用户自定义的规则，适合高级用户使用。通过完全自由的自定义规则框架，您可以根据实际的网络攻击情况对规则进行最大限度的定制。

+ 添加 修改 删除 刷新 ▶ 启用 停用 ✓ 应用 规则ID 请输入关键字 查询									
序号	规则ID	规则名称	说明	拦截方式	是否记录	是否启用	更新时间	重定向页面	操作
1	2000000	test	test	拦截	记录日志	已启用	2017-09-04...	301跳转页面	

- 添加自定义规则： 点击【添加】按钮，出现【自定义规则-添加】对话框。具体操作请参见下一节自定义规则的添加和修改。
- 修改自定义规则： 选择一条规则然后点击【修改】按钮，出现【自定义规则-修改】对话框。双击某条规则也可以直接打开【自定义规则-修改】对话框。具体操作请参见下一节自定义规则的添加和修改。
- 删除自定义规则： 选择一条或者多条自定义规则，然后点击【删除】按钮，则删除所选自定义规则。
- 启用自定义规则： 选择一条或者多条自定义规则，然后点击【启用】按钮，则启用所选自定义规则。
- 停用自定义规则： 选择一条或者多条自定义规则，然后点击【停用】按钮，则停用所选自定义规则。
- 查询自定义规则： 当用户自定义规则比较多时，输入名称并点击【快速查询】按钮，可以根据名称快速筛选出包含输入名称的自定义规则。
- 立即生效： 点击【应用】按钮后当前更改立即生效，建议在所有设置全部配置完成以后，点击【应用】按钮。

9.3.1.2 自定义规则的添加和修改

自定义规则的添加和修改界面如图。自定义规则支持简单的字符串匹配和高级的 PCRE 正则表达式匹配算法。关于 PCRE 正则表达式的介绍，请参见[附录 B 正则表达式入门](#)。

自定义规则 - 添加

规则基本信息

*规则ID: 请填写规则ID, 限制2000000-7999999

*规则名称: 请填写规则名称, 最长50字符

说明: 请填写说明, 最长100字符

*危害等级: 中等

*拦截方式: 检测

是否启用: ☒ 启用 ☐ 停用

是否记录: ☒ 记录日志 ☐ 不记日志

HTTP数据类: ☒ HTTP请求 - ☐ HTTP响应 -

型: Request Response

*HTTP请求: GET

重定向页面: <空>

类型:

特征生成

*特征关键字: 请填写特征关键字, 最长50字符

匹配算法: 字符串匹配

关系: AND

*匹配内容: ☒ URL ☐ POST ☐ COOKIE

插入特征

字符串特征

PCRE特征

? 测试规则 ✓ 保存 ↺ 重置 ✕ 取消

- 编号： 自定义规则的用户指定编号。此编号应该介于 2000000 和 9999999 之间，并且不允许重复。如果您输入的编号不在允许范围内，系统会提示您重新输入编号。
- 名称： 自定义规则的中文或者英文名称。建议名称尽量简洁并能反映该条规则的真实含义。
- 说明： 关于该条规则的备注信息，您可以在此处添加说明性的文字。
- 危害等级： 关于该条规则的警告等级。
- 是否启用： 该条规则保存后是否启用。
- 拦截类型： 匹配到选择该条规则所执行的动作。
- 是否记录日志： 匹配到后是否记录日志。
- HTTP 数据类型： Request 为用户请求的数据，Response 为服务器返回的数据。
- HTTP 请求类型： 选择匹配的 HTTP 请求类型（或称为请求方式）。
- 重定向页面： 匹配到该条规则后返回所设置的重定向页面。

- 特征关键字：填写用于字符串匹配或者 PCRE 匹配的内容。
- 匹配算法：选择匹配所采用的算法。字符串匹配用于简单的字符串匹配，PCRE 匹配用于较复杂的正则表达式匹配。
- 关系：选择两个特征之间的逻辑关系， AND 表示逻辑与，OR 表示逻辑或。
- 匹配内容：选择要匹配的 HTTP 协议各部分的内容，可多选。例如：
 - 1) URL 表示需要匹配 HTTP 协议中的 Request-URI 部分的内容；
 - 2) POST 表示需要匹配 HTTP 协议中的 POST 请求类型中的 HTTP body 部分；
 - 3) COOKIE 表示需要匹配 HTTP 协议中的 Cookie 部分的内容。
- 插入特征：每填写好一组“特征生成”的内容后，点击【插入特征】按钮将特征插入下面对应文本框。
- 字符串特征：用于显示已经插入的字符串匹配的内容。用户也可手动编辑。
- PCRE 特征：用于显示已经插入的 PCRE 匹配的内容。用户也可手动编辑。说明：字符串特征和 PCRE 特征是逻辑与的关系，两个特征必须同时满足才能匹配成功。
- 测试规则：当规则编辑好后，可以点击测试，查看规则语法是否正确。

操作步骤提示：

- 1) 先输入特征关键字，选择合适的 HTTP 数据类型、HTTP 协议、匹配算法、关系以及匹配内容，然后点击【插入特征】按钮；
- 2) 重复步骤 1，直到您已经将所有需要特征插入完毕；
- 3) 点击【测试规则】按钮，查看编写的规则是否规范，如果提示错误，重复步骤 1-2 进行修改，直到提示正确；
- 4) 点击【保存】按钮，保存该条自定义规则。

9.3.1.3 自定义规则举例

- 示例一（字符串匹配）：

某网站 A 存在一个论坛，有恶意用户在论坛上传图片，并在多家流量很大的网站引用，导致网站 A 流量猛增，影响了该网站正常用户的访问，可以添加一条自定义规则拦截所有对上传图片的访问，例如，图片名称是：image1.jpg，image2.jpg。

操作步骤：

1. 编号填写：2000020；
2. 名称填写：防止图片恶意访问；
3. 备注填写：防止图片恶意访问；
4. 危害等级选择：轻微；
5. 选择启用；
6. 拦截方式选择：拦截；
7. 是否记录日志选择：不记录；

8. HTTP 数据类型选择: HTTP 请求数据;
9. HTTP 请求类型选择: GET;
10. 特征生成, 首先添加 image1.jpg 的特征:
11. 先输入特征关键字 "image1.jpg" ;
12. 匹配算法选择 "字符串匹配" ;
13. 关系选择 "AND" ;
14. 匹配内容选择 "URL" ;
15. 然后点击【插入特征】按钮。
16. 重复步骤 5, 添加 image2.jpg 的特征;
17. 到这一步, 规则生成初步完成, 生成后的规则如图所示;

自定义规则 - 添加
×

规则基本信息

*规则ID: 2000020

*规则名称: 防止图片恶意访问

说明: 防止图片恶意访问

*危害等级: 轻微

是否启用: ☒ 启用 ☐ 停用

HTTP数据类: ☒ HTTP请求 - 型: Request ☐ HTTP响应 - Response

*HTTP请求类型: GET

*拦截方式: 拦截

是否记录: ☒ 记录日志 ☐ 不记日志

重定向页面: 默认提示页面

特征生成

*特征关键字: image2.jpg

匹配算法: 字符串匹配 关系: OR

*匹配内容: ☒ URL ☐ POST ☐ COOKIE + 插入特征

字符串特征

content:"image2.jpg";on:"UO";

PCRE特征

? 测试规则
✓ 保存
↺ 重置
✕ 取消

18. 点击【测试规则】按钮, 查看编写的规则是否符合规范;

19. 点击【保存】按钮，保存该条自定义规则。

● 示例二（PCRE 匹配）：

PHP 脚本语言的 webshell，通常用 base64_decode 函数解密一个经过加密的恶意代码，然后通过 eval 来执行。如果入侵者上传的这个 webshell 能被自己编写的自定义规则拦截，则可以有效防止因 Web 代码问题而造成的入侵危害。

参考附录 B，经过分析，可以写出一个拦截上传 PHP 语言 webshell 木马的 PCRE 正则表达式：

`"\beval\s*(\s*base64_decode\b"`。

操作步骤：

1. 编号填写：2000021；
2. 名称填写：防止上传 PHP 木马；
3. 备注填写：防止上传 PHP 木马；
4. 危害等级选择：严重；
5. 选择启用；
6. 拦截方式选择：拦截；
7. 是否记录日志选择：记录日志；
8. HTTP 数据类型选择：HTTP 请求数据；
9. HTTP 请求类型选择：POST；
10. 添加上述特征；
11. 先输入特征关键：`"\beval\s*(\s*base64_decode\b"`；
12. 匹配算法选择“PCRE 匹配”；
13. 关系选择“AND”；
14. 匹配内容选择“POST”；
15. 然后点击【插入特征】按钮。
16. 到这一步，规则生成初步完成，生成后的规则如图所示；

自定义规则 - 添加

规则基本信息

*规则ID: 2000021

*规则名称: 防止上传PHP木马

说明: 防止上传PHP木马

*危害等级: 严重

*拦截方式: 拦截

是否启用: ☒ 启用 ☐ 停用

是否记录: ☒ 记录日志 ☐ 不记日志

HTTP数据类: ☒ HTTP请求 - 型: Request ☐ HTTP响应 - Response

*HTTP请求类型: POST

重定向页面: 默认提示页面

特征生成

特征关键字: \beval\s(\s*base64_decode\b

匹配算法: PCRE匹配

关系: AND

*匹配内容: ☒ URL ☐ POST ☐ COOKIE

插入特征

字符串特征

PCRE特征

```
pcre:"\beval\s*(\s*base64_decode\ ) b";on:"UA";
```

? 测试规则

✓ 保存

↺ 重置

✕ 取消

17. 点击【测试规则】按钮，查看编写的规则是否符合规范；

18. 点击【保存】按钮，保存该条自定义规则。

● 示例三（字符串匹配+PCRE 匹配）：

在 ASP 网站里，COOKIE 注入一直是一类让广大管理员头疼的问题，如果能有效解决 COOKIE 注入，则可以很大程度地提高网站的安全性。经过分析，如果要进行 COOKIE 注入，一般会出现 and 或者 select 等特殊字符，结合使用自定义规则的字符串匹配和 PCRE 匹配，则可以防止此类 COOKIE 注入问题。

操作步骤：

1. 编号填写：2000022；
2. 名称填写：防止 COOKIE 注入；
3. 备注填写：防止 COOKIE 注入；
4. 危害等级选择：轻微；
5. 选择启用；
6. 拦截方式选择：拦截；
7. 是否记录选择：记录日志；
8. HTTP 数据类型选择：HTTP 请求数据；

9. HTTP 请求类型选择: ALL;
10. 选择重定向页面: “默认提示页面”;
11. 特征关键字, 输入如下内容: “(and|or|xor|union)[^\n]*\bselect\b”;
12. 匹配算法选择 “PCRE 匹配”;
13. 关系选择 “AND”;
14. 匹配内容选择 “URL”;
15. 然后点击【插入特征】按钮。
16. 字符串特征输入如下内容: “content: *select*;on:*UA;”;
17. 再输入 PCRE 特征: “pcre:*(and|or|xor|union) [^\n]*\bselect\b;on:*UA;”;
18. 然后点击【插入特征】按钮;
19. 到这一步, 规则生成初步完成, 生成后的规则如图所示;

自定义规则 - 添加

规则基本信息

*规则ID: 2000022

*规则名称: 防止COOKIE注入

说明: 防止COOKIE注入

*危害等级: 轻微

*拦截方式: 拦截

是否启用: ☒ 启用 ☐ 停用

是否记录: ☒ 记录日志 ☐ 不记日志

HTTP数据类: ☒ HTTP请求 - ☐ HTTP响应 -

型: Request Response

*HTTP请求类型: ALL

重定向页面: 默认提示页面

特征生成

特征关键字: (and|or|xor|union)[^\n]\bselect\b

匹配算法: PCRE匹配

关系: AND

*匹配内容: ☒ URL ☐ POST ☐ COOKIE

插入特征

字符串特征

content : *select*;on:*UA;

PCRE特征

pcre:*(and|or|xor|union) [^\n]*\bselect\b;on:*UA;

测试规则

保存

重置

取消

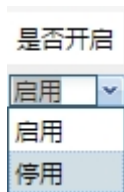
20. 点击【测试规则】按钮，查看编写的规则是否符合规范；
21. 点击【保存】按钮，保存该条自定义规则。

9.3.2 内置规则

本页面显示钰迅 Web 应用防护系统在出厂时已经内置好的防护规则集。页面具体如图所示，显示的详细内容包括：序号、编号、名称、备注、是否启用和更新时间。您可以根据实际情况，设置启用与停用某个内置规则集。

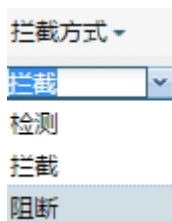
规则分类		规则列表							
所有分类		规则号	规则名称	说明	类别	拦截方式	重定向页面	是否记录	是否启用
• HTTP 状态码		1500007	明鉴WEB应用漏洞扫描器的扫描行为	明鉴WEB应用漏洞扫描器为一款Web渗透测试工具	扫描行为	阻断	默认提示页面	记录日志	已启用
• SQL注入		1500008	明鉴WEB应用漏洞扫描器的扫描行为	明鉴WEB应用漏洞扫描器为一款Web渗透测试工具	扫描行为	阻断	默认提示页面	记录日志	已启用
• URL黑学习		1500009	绿盟远程安全评估系统的扫描行为	绿盟远程安全评估系统为一款Web渗透测试工具	扫描行为	阻断	默认提示页面	记录日志	已启用
• XSS攻击		1500010	绿盟远程安全评估系统的扫描行为	绿盟远程安全评估系统为一款Web渗透测试工具	扫描行为	阻断	默认提示页面	记录日志	已启用
• 信息泄露		1950001	发现扫描器扫描行为（请求特征）	发现漏洞扫描器扫描网站的行为。	扫描行为	阻断	默认提示页面	记录日志	已启用
• 会话劫持		1950002	发现扫描器扫描行为（返回特征）	发现漏洞扫描器扫描网站的行为。	扫描行为	阻断	<无>	记录日志	已启用
• 命令执行		1500011	禁止Sqlmap注入攻击	Sqlmap是一款被黑客广泛使用的Web注入攻击工具，具有较强的危害性	扫描行为	阻断	默认提示页面	记录日志	已启用
• 扫描行为		1500012	发现Jsky扫描器行为	Jsky是一款国内的Web渗透测试工具，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用
• 挂马检测		1500013	Nsauditor网络安全扫描器的扫描行为	Nsauditor是一款网络安全扫描器，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用
• 程序上传		1500014	禁止Netsparker扫描	Netsparker是一款国外的Web渗透测试工具，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用
• 缓冲区溢出		1500015	禁止Grendel-Scan扫描	Grendel-Scan是一款国外的Web渗透测试工具，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用
• 脚本上传		1500016	禁止w3af扫描	w3af是一款国外的Web渗透测试工具，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用
• 脚本木马		1500017	禁止Nikto扫描	Nikto是一款国外的Web渗透测试工具，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用
• 请求类型		1500018	禁止Havij注入攻击	Havij是一款被黑客广泛使用的Web注入攻击工具，具有较强的危害性	扫描行为	阻断	默认提示页面	记录日志	已启用
		1500019	禁止BurpSuite扫描	BurpSuite是一款国外的Web渗透测试工具，具有较强的攻击能力、漏洞发现能力	扫描行为	阻断	默认提示页面	记录日志	已启用

- 启用停用规则集：选择一条规则集然后点击如图所示位置；



出现下拉菜单，选择是否启用，则可启用停用所选内置规则集。

- 设置规则集动作类型：选择一条内置规则然后点击如图所示位置；



选择所要设置的动作类型，即可设置所选规则集的动作类型。

- 选择重定向页面：选择一条内置规则然后点击如图所示位置；



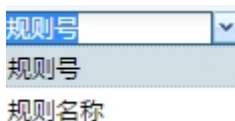
重定向页面的记录来自重定向页面设置，参见[重定向页面](#)。

- 启用停用记录日志：选择一条内置规则然后点击如图所示位置；



选择是否记录日志，即可设置是否记录日志。

- 查询规则集：在右边的输入名称框中输入需要查询的规则集名称，点击【快速查询】按钮，系统查询出所有规则集名称中包含该文字的内置规则集或者输入规则号查询；



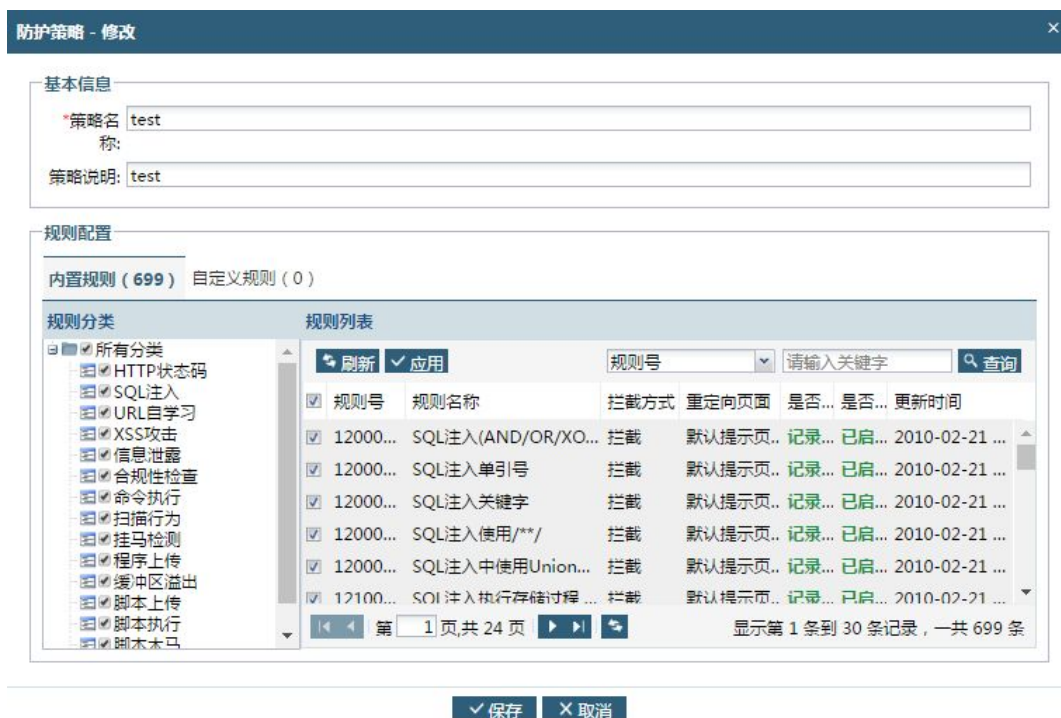
注意：

所有内置规则集都经过厂家的严格测试，保证最小程度的误拦截。除非您完全清楚正在进行的操作，否则不要停用任何内置规则集。

9.3.3 防护策略集

添加防护策略集：输入策略名称，策略说明，选中要添加的规则，点击保存。

添加内置规则：如下图左右



添加自定义规则：如下图左右（需要先定义自定义规则后添加），最后点击保存即可。

防护策略 - 修改

基本信息

策略名称: test
策略说明: test

规则配置

内置规则 (0) 自定义规则 (1)

+ 添加
修改
删除
刷新
启用
停用
应用

规则ID
请输入关键字
查询

规则ID	规则名称	说明	拦截方式	是否记录	是否启用	更新时间	重定向页面	操作
2000000	test	test	拦截	记录日志	已启用	2017-09...	301跳转页...	

第 1 页, 共 1 页

显示第 1 条到 1 条记录, 一共 1 条

保存
取消

9.3.4 HTTP 请求类型过滤

本页面设置是否对 HTTP 请求类型进行拦截, 您也可以在“内置规则”页面完成相同的功能。

HTTP请求类型过滤

禁止的HTTP请求类型:

☐ CHECKIN	☐ CHECKOUT	☐ CONNECT	☒ COPY	☒ DEBUG	☒ DELETE	☐ GET
☐ HEAD	☐ LINK	☐ LOCK	☐ MKCOL	☒ MOVE	☐ OPTIONS	☐ POST
☐ PROPFIND	☐ PROPPATCH	☒ PUT	☐ SEARCH	☐ SPACEJUMP		
☒ TRACE	☒ TRACK	☐ UNLINK	☐ UNLOCK	☐ <其他类型>		

☒ 全选
☐ 反选
☐ 不选

9.3.5 HTTP 头防溢出设置

本页面设置和显示 HTTP 协议各部分内容的最大允许长度, 您可以根据实际情况修改相应部分的最大长度。如果一个 HTTP 连接请求超过某个最大允许长度, 例如: URL 部分的最大允许长度, 则该连接请求将被禁止同时记录到入侵记录中。

列表中为本设备目前所支持并检测的协议字

HTTP头防溢出设置

*Accept长度:	2048
*Accept-Charset长度:	2048
*Accept-Encoding长度:	2048
*Authorization长度:	2048
*Cookie长度:	32767
*Host长度:	2048
*Post长度:	10000000
*Proxy-Authorization长度:	2048
*Referer长度:	2048
*URL长度:	2048
*User-Agent长度:	2048
*Connection长度:	64
*Cache-Control长度:	128
*Server长度:	1024

- 修改：在文本框中输入指定的数值然后点击【保存】按钮。
- 立即生效：点击【应用】按钮后当前更改立即生效。



注意：

防溢出功能能够被单独关闭，您可以到高级-内置规则中“启用”“停用”相关防溢出规则。

10、网络配置

10.1 网络接口

该页面列出了设备所有网络接口的工作状态，包括 IP 地址、子网掩码、网关、是否启用、工作方式、接口属性等信息。

接口名称	IP地址	子网掩码	网关	下一跳	是否启用	连接状态	工作方式	所属网桥	接口属性	操作
ETH0	192.168.1...	255.255.2...	*		已启用	已断开	保留		DSI	
ETH1	192.168.9...	255.255.2...	192.168.9...		已启用	已连接	普通模式		DMI	
ETH2	192.168.1...	255.255.2...	192.168.1.1		已启用	已断开	普通模式		RPI	
ETH3					已停用	已断开	普通模式			
ETH4					已启用	已断开	透明网桥	wafprotect	WAN	
ETH5					已启用	已断开	透明网桥	wafprotect	LAN	

选择某个网络接口，点击【修改】，弹出【网络接口-修改】对话框，对该网络接口进行配置。

10.1.1 接口管理

此处提供系统初始化接口（DSI），设备管理接口（DMI），反向代理口（RPI）的接口配置功能。

10.1.1.1 配置系统初始化接口 (DSI)

DSI 是初始化接口，在设备初始配置时使用。如果一个网络接口的接口属性被配置为 DSI，通常简称为 DSI 接口，该接口的工作模式和接口属性都不能被修改。

DSI 接口提供 DHCP 服务，您可以在这里设置 DHCP 服务分配的起始和结束 IP 地址。

如果您在【网络接口】页面修改了 DSI 接口的 IP 地址，请相应地修改 DHCP 服务器的起始、结束地址，否则 DHCP 服务将无法正常工作。

物理网口 - 修改

接口名称: ETH0

是否启用:

☒ 启用
☐ 停用

连接状态:

● 已断开

双工:

自动

速度:

自动

MAC地址:

00:0c:29:55:6f:8b

工作方式:

☒ 保留

IP地址:

192.168.100.1

子网掩码:

255.255.255.0

网关:

*

DHCP服务:

初始化接口提供DHCP服务。

*起始地址:

192.168.100.10

*结束地址:

192.168.100.100

更多选项:

☐ DMI - 设备管理接口，通过该接口访问设备的管理页面
☐ PI - 反向代理接口，设备通过该接口对外提供反

✓ 保存

↻ 刷新

✕ 取消

10.1.1.2 配置设备管理接口 (DMI)

DMI 是设备管理接口，通过该接口访问设备的管理页面。如果一个网络接口的接口属性被配置为 DMI，通常简称为 DMI 接口。在更多选项中，选择是否开启 DMI 口，点击保存即可。

物理网口 - 修改

接口名称: ETH4

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已连接

双工: 全双工

速度: 1000 Mbps

MAC地址: 4c:cc:6a:87:41:c0

工作方式: ☒ 普通模式 ☐ 透明网桥 ☐ 策略路由 ☐ 端口汇聚

IP地址: 192.168.1.1

子网掩码: 255.255.255.0

网关: 192.168.1.1

IPv6地址: fec0:0:0:9::

IPv6前缀: 64

IPv6网关: fec0:0:0:9::

更多选项: ☒ DMI - 设备管理接口, 通过该接口访问设备的管理页面
☒ RPI - 反向代理接口, 该接口对外提供代理内部Web服务器 (HTTP) 的代理服务
☐ RPI2 - 反向代理接口, 该接口对外提供代理内部Web服务器的双向HTTPS代理服务



注意:

只有工作模式为普通, 且不是 DSI 接口的网络接口才能配置为管理接口。

系统允许配置多个设备管理接口。

10.1.1.3 配置反向代理口 (RPI)

RPI 是反向代理接口, 设备通过该接口对外提供反向代理服务。如果一个网络接口的接口属性被配置为 RPI, 通常简称为 RPI 接口。在更多选项中, 选择是否开启 RPI 口, 点击保存即可。

物理网口 - 修改

接口名称: ETH4

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已连接

双工: 全双工

速度: 1000 Mbps

MAC地址: 4c:cc:6a:87:41:c0

工作方式: ☒ 普通模式 ☐ 透明网桥 ☐ 策略路由 ☐ 端口汇聚

IP地址: 192.168.1.1

子网掩码: 255.255.255.0

网关: 192.168.1.1

IPv6地址: fec0:0:0:9::

IPv6前缀: 64

IPv6网关: fec0:0:0:9::

更多选项: ☒ DMI - 设备管理接口, 通过该接口访问设备的管理页面
☒ RPI - 反向代理接口, 该接口对外提供代理内部Web服务器 (HTTP) 的代理服务
☐ RPI2 - 反向代理接口, 该接口对外提供代理内部Web服务器的双向HTTPS代理服务



注意:

只有网络接口工作于普通方式, 且不是 DSI 接口的才能配置为反向代理接口, RPI 接口与 DMI 接口可以共存于同一个网络接口上。系统只能允许配置一个 RPI 接口。

10.1.2 虚拟 IP 设置

本设备支持在同一物理网卡下设置多个 IP 地址。

- 添加：添加一个虚拟 IP，在[网络接口](#)里面可以对添加的虚拟 IP 进行配置。

物理接口 - 修改

接口名称: ETH4

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已连接

双工: 全双工

速度: 1000 Mbps

MAC地址: 4ccc6a87:41:c0

工作方式: ☒ 普通模式 ☐ 透明网桥 ☐ 策略路由 ☐ 端口汇聚

IP地址:

子网掩码:

网关:

IPv6地址:

IPv6前缀:

IPv6网关:

更多选项:

☐ DMI - 设备管理接口，通过该接口访问设备的管理页面
☒ RPI - 反向代理接口，该接口对外提供代理内部Web服务器（HTTP）的代理服务
☐ RPI2 - 反向代理接口，该接口对外提供代理内部Web服务器的双向HTTPS代理服务

✓ 保存

↻ 刷新

✕ 取消

- 删除：选中一条虚拟 IP 记录，点击“删除”，即可删除该虚拟 IP，如果此虚拟 IP 具有 DMI 属性，则需去掉 DMI 属性后才能删除。

ETH1:0	1.1.1.1	255.255.255.0	*	已启用	● 已...	普通...	✎
--------	---------	---------------	---	-----	--------	-------	---

10.1.3 端口汇聚

本设备支持端口汇聚功能，如果您需要绑定多个网络接口，请开启该功能。

combo0	1.1.1.1	255.255.255.0	*	已启用	● 已...	普通...	✎
combo1	2.2.2.2	255.255.255.0	*	已启用	● 已...	普通...	✎

提示：

关于端口汇聚算法，需要配合已有环境进行选择，如果算法不对将造成端口汇聚效果降低或者无法工作。

10.1.4 配置网络接口为普通方式

1. 双击需要修改的网络接口，比如：ETH3，弹出【网络接口-修改】对话框；

物理网口 - 修改

接口名称: ETH4

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已连接

双工: 全双工

速度: 1000 Mbps

MAC地址: 4c:cc:6a:87:41:c0

工作方式: ☒ 普通模式 ☐ 透明网桥 ☐ 策略路由 ☐ 端口汇聚

IP地址:

子网掩码:

网关:

IPv6地址:

IPv6前缀:

IPv6网关:

更多选项: ☐ DMI - 设备管理接口, 通过该接口访问设备的管理页面
☒ RPI - 反向代理接口, 该接口对外提供代理内部Web服务器 (HTTP) 的代理服务
☐ RPI2 - 反向代理接口, 该接口对外提供代理内部Web服务器的双向HTTPS代理服务

✓ 保存

↻ 刷新

✕ 取消

2. 选择接口状态为“启用”；
3. 选择工作方式为“普通”；
4. 填写“IP 地址”，“子网掩码”；
5. 如果该接口有相应的网关，请填写网关。如果没有，可以留空不填写；
6. 点击【应用】按钮，该设置生效并返回上一级页面。

10.1.5 配置网络接口为透明方式

1. 双击需要修改的网络接口，比如：ETH3，弹出【网络接口-修改】对话框；

物理网口 - 修改

接口名称: ETH3

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已断开

双工: 自动

速度: 自动

MAC地址: 00:50:56:34:b7:3a

工作方式: ☐ 普通模式 ☒ 透明网桥 ☐ 策略路由 ☐ 端口汇聚

接口属性: ☒ LAN ☐ WAN

*绑定网桥:

更多选项: ☐ DMI - 设备管理接口, 通过该接口访问设备的管理页面
☐ RPI - 反向代理接口, 设备通过该接口对外提供反

✓ 保存

↻ 刷新

✕ 取消

2. 选择接口状态为“启用”；
3. 选择工作方式为“透明”；

- 1) 选择接口属性为“WAN”或者“LAN”。系统默认只检测流入 WAN 接口的数据包，如果需要检测 LAN 接口的数据包请到【配置】->【基本参数设置】打开双向检测功能；
- 2) 选择“所属虚拟网桥”，如果需要加入的网桥不存在，可以在【虚拟网桥】页面添加；
- 3) 点击【应用】按钮，该设置生效并返回上一级页面。

10.1.6 配置网络接口为策略路由方式

1. 双击需要修改的网络接口，比如：ETH3，弹出【网络接口-修改】对话框

物理网口 - 修改
×

接口名称: ETH3

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已断开

双工: 自动

速度: 自动

MAC地址: 00:50:56:34:b7:3a

工作方式: ☐ 普通模式 ☐ 透明网桥 ☒ 策略路由 ☐ 端口汇聚

接口属性: ☒ LAN ☐ WAN

IP地址:

子网掩码:

下一跳:

更多选项: ☐ DMI - 设备管理接口，通过该接口访问设备的管理
☐ 反向代理接口，设备通过该接口对外提供反

✓ 保存
↻ 刷新
✕ 取消

2. 选择接口状态为“启用”；
3. 选择工作方式为“策略路由”；
 - 1) 选择接口属性为“WAN”或者“LAN”；
 - 2) 填写“IP 地址”和“子网掩码”；
 - 3) 点击【应用】按钮，该设置生效并返回上一级页面；
 - 4) 配置为“策略路由”工作方式的网络接口，将会出现在【策略路由】页面，在该页面进行策略路由的进一步配置。

10.1.7 配置网络接口为端口汇聚方式

1. 双击需要修改的网络接口，比如：ETH3，弹出【网络接口-修改】对话框；

物理网口 - 修改

接口名称: ETH3

是否启用: ☐ 启用 ☒ 停用

连接状态: ● 已断开

双工: 自动

速度: 自动

MAC地址: 00:50:56:34:b7:3a

工作方式: ☐ 普通模式 ☐ 透明网桥 ☐ 策略路由 ☒ 端口汇聚

*绑定端口汇聚:

更多选项: ☐ DMI - 设备管理接口, 通过该接口访问设备的管理页面 ☐ P1 - 反向代理接口, 设备通过该接口对外提供反

2. 选择接口状态为“启用”；
3. 选择工作方式为“端口汇聚”；
 - 1) 选择工作方式为“端口汇聚”。
 - 2) 选择对应的虚拟设备。（此虚拟设备需要在端口汇聚中添加，具体参照端口汇聚。）

 注意：

添加后的 combo 设备和普通网卡一样，可以配置为普通，透明，策略路由模式。

10.2 虚拟网桥

工作于透明模式的网络接口必须从属于某个虚拟网桥，在本页面可以查看虚拟网桥的数量、名称、每个虚拟网桥拥有的网络接口，您也可以在此页面添加、删除、修改虚拟网桥。在配置高可用性功能时，根据您的网络环境中的交换机配置，选择是否开启 STP，以及相关的 STP 参数的设置。

序号	名称	相关接口	IP	子网掩码	网关	IPv6地址	IPv6前缀	IPv6网关	老化时间/秒	HTTPS防护	链路联动...	生成树协...	优先级	转发延时...	Max-Age...	Hello-Tim...	操作
1	wafprotect	ETH0,ETH1								已启用	已停用	已停用					

 注意：

虚拟网桥所允许的最大数量与设备型号有关，具体请联系钰迅信息或者供货商。

10.3 静态路由

用于配置系统当前的静态路由表，具体界面如下图。您可以添加、修改、删除静态路由。配置完成后，必须点击【应用】按钮以使配置生效。

+ 添加 修改 删除 刷新 应用					
序号	网络接口	目的地址	子网掩码	网关	操作
1	ETH1	0.0.0.0	0.0.0.0	192.168.99.1	

只能为工作于普通方式的网络接口配置静态路由。

如果您配置了防篡改或者反向代理的功能，请在这里添加相应的静态路由。

10.3.1 修改默认路由

例如：序号为 1 的记录为默认路由，双击该记录，弹出【静态路由-修改】对话框；

选择“接口名称”：即对应的网络接口名称，可以修改默认路由所在的接口，比如从 ETH1 改到 ETH4；

勾选“设置为默认路由”；

1. 填写“网关”，这里添加的网关必须与【网络接口】页面中该网络接口的网关一致；并且默认路由的网关不能为空；
2. 点击【保存】按钮，返回上一级页面。

 注意：

系统只能有一条默认路由，可以修改默认路由，但不能添加多条默认路由。

10.3.2 添加普通路由

您可以添加到主机或者某一网段的路由，请务必保证目的地址与子网掩码的正确有效。此处的网关是到达目的地址的路由的下一跳地址；因此可以与该网络接口的网关不一致。

1. 点击【添加】，弹出添加【静态路由-添加】对话框；

静态路由 - 添加

*网络接口: ETH4

默认路由: ☐ 设置为默认路由

目的地址: 192.168.8.1

子网掩码: 255.255.255.0

网关: 192.168.9.1

IPv6默认路由: ☐ 设置IPv6为默认路由

IPv6目的地址: 请填写IPv6目的地址

IPv6前缀: 请填写IPv6前缀

IPv6网关: 请填写IPv6网关

✓ 保存

↺ 重置

✕ 取消

2. 选择“接口名称”，即对应的网络接口名称；

- 1) 填写“目的地址”，“子网掩码”。如果是添加到主机的静态路由，子网掩码可以为 255.255.255.0；
- 2) 填写“网关”，此处可以留空或者填写路由的下一跳地址。如果填写了网关，必须保证该网络接口到该网关的 IP 地址是可到达的；
- 3) 点击【保存】按钮，返回上一级页面。

10.4 DNS 设置

设置 DNS 服务器地址，系统的邮件通知、漏洞扫描等功能依赖于 DNS 设置，因此建议您最好配置 DNS 服务器地址。

DNS配置

首选DNS服务器:	8.8.8.8
备用DNS服务器:	114.114.114.114
首选IPv6DNS服务器:	请输入首选IPv6DNS服务器
备用IPv6DNS服务器:	请输入备用IPv6DNS服务器

提示:

如果您不清楚 DNS 服务器地址，请联系网络管理员获得。

10.5 BYPASS 设置

BYPASS配置

开启BYPASS

开启BYPASS后，每对WAN/LAN接口在物理上直接连通，流量不经过设备，一般用于网络故障排除。

关闭BYPASS

关闭BYPASS后，流量经过设备，恢复到正常状态。

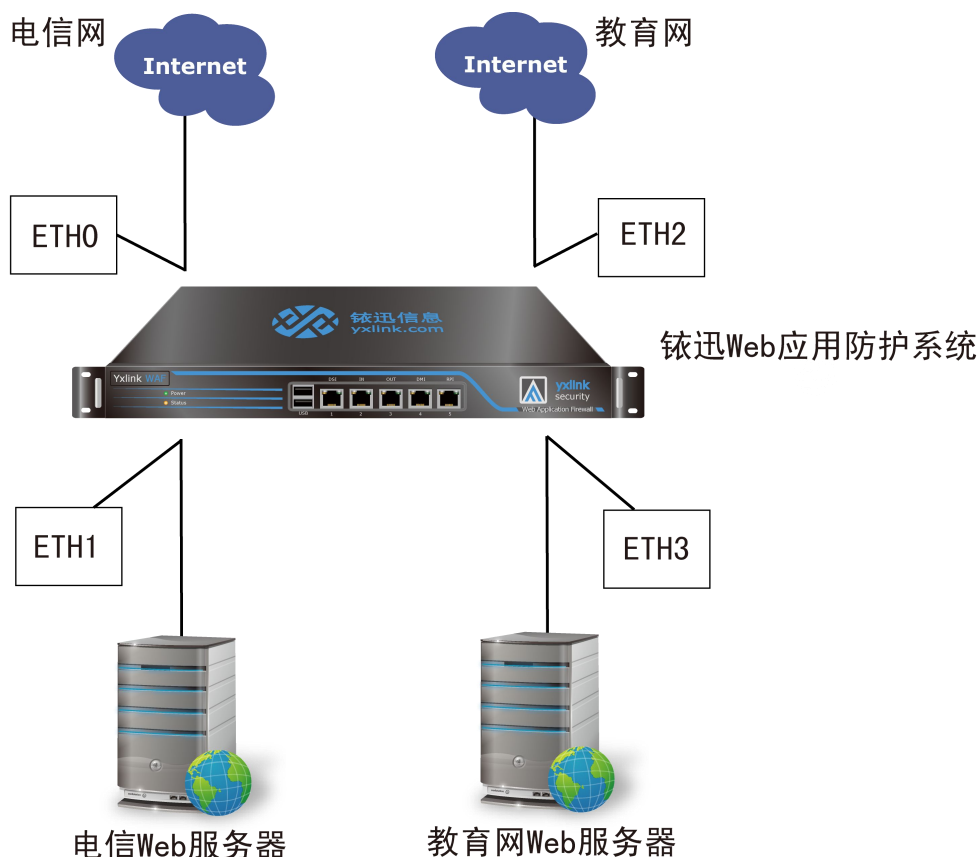
【开启 BYPASS】：开启 BYPASS 后，设备不检测经过设备的流量。

【关闭 BYPASS】：关闭 BYPASS 后，设备检测经过设备的流量。

10.6 部署方式

10.6.1 配置双路进线（电信、教育网）

如果您的网络环境是双路进线，一路是电信线路，另一路是教育网线路，并且同时都需要 WAF 防护，可以参考本实例。



配置步骤如下：

1. 进入到【虚拟网桥】页面添加一个虚拟网桥，例如 wafprotect；
2. 进入到【网络接口】页面，将 ETH4 和 ETH5 配置工作于透明方式，选择虚拟网桥为 test1，配置结果如下图；

接口名称	IP地址	子网掩码	网关	下一跳	是否启用	连接状态	工作方式	所属网桥	接口属性	操作
ETH0	192.168.100.1	255.255.255.0	*		已启用	● 已连接	保留		DSI	
ETH1	192.168.99.75	255.255.255.0	192.168.99.1		已启用	● 已连接	普通模式		DMI	
ETH2					已启用	● 已断开	透明网桥	wafprotect	WAN	
ETH3					已启用	● 已断开	透明网桥	wafprotect	LAN	
ETH4					已启用	● 已断开	透明网桥	test1	WAN	
ETH5					已启用	● 已断开	透明网桥	test1	LAN	

说明：虚拟网桥 test1 为一条线路，接电信，包含两个接口，即 ETH4 和 ETH5，其中 ETH4 是 WAN 接口，ETH5 是 LAN 接口。

虚拟网桥 wafprotect 为另一条线路，接教育网，也包含两个接口，即 ETH2 和 ETH3，其中 ETH2 是 WAN 接口，ETH3 是 LAN 接口。

至此，双路进线配置完成。



注意：

如果提示虚拟网桥数量达到最大值，请确认该设备是否支持双路或者多路。

10.6.2 配置一进多出（一条线路，多台服务器）

如果您的网络环境是一条线路，但是有多个 Web 服务器，比如：2 台。您可以将本设备配置为一条进线、多路出线的方式，此时本设备相当于一台交换机。

配置步骤如下：

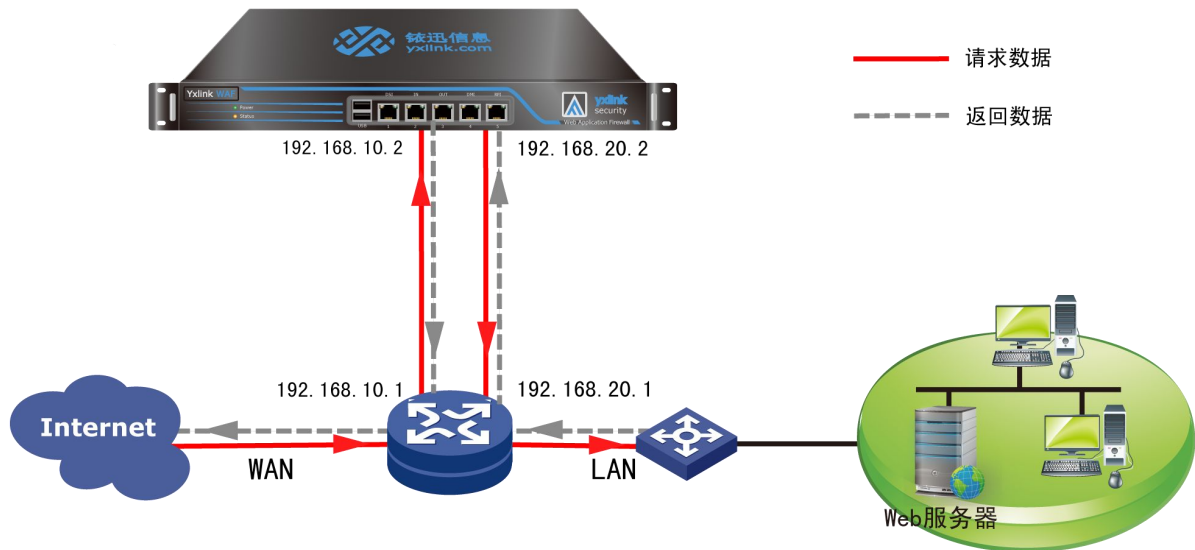
- 进入到【网络接口】页面，配置 3 个网络接口为透明方式，选择同一个虚拟网桥 wafprotect，其中 ETH2 的接口属性为 WAN，ETH3 和 ETH4 接口属性为 LAN，如下图；

接口名称	IP地址	子网掩码	网关	下一跳	是否启用	连接状态	工作方式	所属网桥	接口属性	操作
ETH0	192.168.100.1	255.255.255.0	*		已启用	● 已连接	保留		DSI	
ETH1	192.168.99.75	255.255.255.0	192.168.99.1		已启用	● 已连接	普通模式		DMI	
ETH2					已启用	● 已断开	透明网桥	wafprotect	WAN	
ETH3					已启用	● 已断开	透明网桥	wafprotect	LAN	
ETH4					已启用	● 已断开	透明网桥	wafprotect	LAN	
ETH5					已启用	● 已断开	透明网桥	test1	LAN	

- 将网络进线接到网络接口 ETH2 上；
- 用网线将 ETH3、ETH4 分别接到 2 台 Web 服务器的网口上；
- 至此，一进多出部署方式配置完成。

10.6.3 配置策略路由

如果您需要策略路由部署方式，可以参照本配置实例。网络拓扑如下图：



配置策略路由的步骤如下:

1. 配置路由器, 首先请参考路由器说明文档;
2. 进入【网络接口】页面, 配置网络接口 ETH2、ETH3 的工作模式为策略路由, 结果如下图;

接口名称	IP地址	子网掩码	网关	下一跳	IPv6地址	IPv6前缀	IPv6网关	IPv6下一跳	是否启用	连接状态	工作方式	所属网桥	接口属性
ETH0									已启用	已连接	透明网桥	wafprotect	WAN
ETH1									已启用	已连接	透明网桥	wafprotect	LAN
ETH2	192.168.10.2	255.255.255.0		192.168.20.1					已启用	已断开	策略路由		WAN
ETH3	192.168.20.2	255.255.255.0		192.168.10.1					已启用	已断开	策略路由		LAN

3. 进入【策略路由】页面, 配置网络接口的下一跳地址, 结果如下图;

物理网口 - 修改

接口名称: ETH2

是否启用: ☒ 启用 ☐ 停用

连接状态: ● 已断开

双工: 自动

速度: 自动

MAC地址: 4c:cc:6a:87:41:be

工作方式: ☐ 普通模式 ☐ 透明网桥 ☒ 策略路由 ☐ 端口汇聚

接口属性: ☐ LAN ☒ WAN

IP地址:

子网掩码:

下一跳地址:

IPv6地址:

IPv6前缀:

IPv6下一跳地址:

更多选项: ☐ DMI - 设备管理接口, 通过该接口访问设备的管理页面
☐ RPI - 反向代理接口, 该接口对外提供代理内部Web服务器 (HTTP) 的代理服务
☐ RPI2 - 反向代理接口, 该接口对外提供代理内部Web服务器的双向HTTPS代理服务

✓ 保存

↻ 刷新

✕ 取消

4. 填写“下一跳地址”。策略路由需要配置为一对，例如这里配置的 ETH2 和 ETH3，即所有从 ETH2 流入的数据包将从 ETH3 流出，所有从 ETH3 流入的数据包将从 ETH2 流出。所以 ETH3 设置的下一跳地址应该与 ETH2 的地址处于同一网段，反之，ETH2 设置的下一跳地址应该与 ETH3 的地址处于同一网段；
5. 至此，策略路由部署方式配置完成。

10.7 反向代理

本设备可以作为反向代理（Reverse Proxy）服务器，接受 Internet 用户的连接请求，然后将请求转发给内部网络中的 Web 服务器，并将从 Web 服务器上得到的结果返回给 Internet 上请求连接的用户。所有流入流出本设备 RPI 接口的网络流量都将被检测，并根据设定的拦截方式，进行相应的拦截。这种模式下，Web 服务器无法获取访问者的真实 IP 地址，需要借助 HTTP 报文中设置相应的字段来表示访问者的 IP 地址，这样需要修改原有的 HTTP 报文。具体部署方式请参考[旁路反向代理模式](#)。

本设备支持 HTTPS/SSL 的反向代理，即对采用 HTTPS 加密通信（一般为 443 端口）的 Web 应用同样可以进行防护。它的工作原理是将原来由 Web 服务器完成的 SSL 加密、解密工作，现在交给本设备来完成，即本设备执行 SSL 加密、解密工作，因此需要将原来 Web 服务器上的 SSL 证书导入到本设备中，同时将 Web 服务器上的 HTTP 端口开启，一般为 80 端口。



注意：

本设备通过 RPI 接口提供反向代理的服务。对于添加的反向代理，建议您在【静态路由】页面专门添加 RPI 接口到该主机的静态路由。

10.7.1 反向代理设置

本页面显示和设置反向代理的列表，如图。

+ 添加 修改 删除 启用 停用 应用 刷新 参数设置 服务器状态 导入 导出										
序号	主机头	协议	本地监听接口	证书公钥	证书私钥	是否启用	数据缓存	状态检查	代理IP及端口	操作
1	www.test.com	HTTP	ETH2的80端口			已启用	已停用	已停用	192.168.9.221:80	编辑

本页面需要设置的参数如下：

主机头名：也称主机域名，也就是需要被代理的网站域名。

协议：需要被代理的 HTTP 协议类型。其中，HTTP 表示明文的 HTTP 协议，对应本地监听端口一般为 80 端口；另一个为 HTTPS，表示加密的 HTTPS/SSL 协议，对应本地监听端口一般为 443 端口。

本地监听端口：本设备 RPI 接口的本地监听端口。DNS 将 Internet 用户访问的域名解析为 RPI 接口的 IP 地址后，连接请求将被发送到此监听端口。

证书公钥：Web 服务器提供给浏览器下载的 SSL 证书的公钥，浏览器用它来验证 Web 服务器的合法性。如果验证成功，浏览器随机生成一个对称密钥并使用接收到的 SSL 证书的公钥进行加密并发送给 Web 服务器。

证书密钥：Web 服务器通过 SSL 证书的密钥对收到的信息进行解密并得到浏览器随机生成的对称密钥，最后 Web 服务器和浏览器都通过这个对称密钥进行加密通讯。

开启缓存：开启页面缓存的功能。开启后，设备将会根据设置保存 Web 服务器返回的页面，当浏览器再次请求时，将直接返回缓存的内容。

启用状态检查：开启状态检测功能。开启之后，设备能判断被代理的服务器是否在线。

本地监听端口：本地监听接口的监控类型为 IPv4 时，代理 IP 只能添加 IPv4 地址。本地监听接口的监控类型为 IPv6 时，代理 IP 可以添加 IPv4 或 IPv6 地址。

代理 IP 及端口：需要被代理的内部 Web 服务器的 IP 地址和端口，如有多个则表示自动进行负载均衡。

在完成反向代理的配置后，您还需要更改 DNS 服务器的域名解析，即由原来指向内部 Web 服务器的 IP 地址更改为指向 RPI 接口的 IP 地址。

下面介绍一下反向代理设置页面的主要功能：

- 添加反向代理： 点击【添加】按钮，弹出【反向代理设置-添加】对话框，如图。

1. 如果选择 HTTP 协议类型，则出现如下对话框。输入主机头名、选择监听类型、输入本地监听端口、填写代理 IP 及端口（如不指定端口，缺省采用 80 端口）后保存退出。

2. 如果选择 HTTPS 协议类型，则显示如下的对话框。输入主机头名、本地监听端口默认为 443、选择证书公钥、选择证书密钥、选择监听类型、填写代理 IP 及端口（如不指定端口，缺省采用 80 端口）后保存退出。

反向代理设置 - 修改

*主机头:

协议: ☐ HTTP ☒ HTTPS

证书公钥:

证书私钥:

是否启用: ☒ 启用 ☐ 停用 数据缓存: ☐ 启用 ☒ 停用

状态检查: ☒ 启用 ☐ 停用 强制HTTPS: ☒ 启用 ☐ 停用

负载均衡: ☒ 轮询 ☐ IP哈希 ☐ X-Real-IP获取

本地监听接口

监听类型: ☒ IPv4 ☐ IPv6

+ 添加 修改 删除

☐ RPI接口	端口
☒ ETH4:0	443

代理IP及端口

+ 添加 修改 删除

☐ IP地址	端口	权重
☒ 192.168.98.181	80	1

如需负载均衡, 在“代理IP及端口”可添加多条记录, 则自动进行负载均衡。本地监听接口的监听类型为IPv4时, 只能添加IPv4地址。

✓ 保存

↻ 刷新

✕ 取消

- 修改反向代理：选择一条已有的反向代理然后点击【修改】按钮，弹出【反向代理设置-修改】对话框，您就可以编辑该条记录。您也可以双击一条记录直接进入修改对话框。
- 删除反向代理：选择一条或多条反向代理然后点击【删除】按钮，则被选中的反向代理将被删除。
- 参数设置：对被代理的 Web 服务器参数进行设置，此设置对所有被代理的 Web 服务器生效。可以对被代理的服务器超时时间，上传文件的大小，全局缓存大小，服务器状态检查、SSL 协议等信息进行设置，如图。

反向代理设置 - 参数设置

代理设置

*代理服务器超时/秒: 90

*上传大小限制/MB: 32

缓存设置

占用内存上限/MB: 200

缓存超时时间/天: 1

占用磁盘上限/GB: 9

清除缓存

状态检查

检测周期/秒: 15

正常状态判定次数: 2

异常状态判定次数: 5

检测超时时间/秒: 3

SSL协议

SSL协议类型: ☐ TLSv1 ☐ TLSv1.1 ☐ TLSv1.2
☐ SSLv2 ☐ SSLv3

保存 **关闭**

- 服务器状态：开启服务器状态检查后，可以看到被代理的服务器是否在线，如图。

服务器状态					
刷新		主机头名	请输入关键字	查询	
序号	主机头名	后端服务器	状态	检查成功次数	检查失败次数
1	123.com	192.168.1.70:80	正常	6	0

- 查询反向代理：输入需要查找的文字，点击【快速查询】按钮，系统会查询出所有主机头名中包含该文字的反向代理。
- 立即生效：点击【应用】按钮后当前更改立即生效，建议在所有设置全部配置完成以后，点击【应用】按钮。

10.8 高可用性

高可用性（High Availability）提供了一种最小化网络中由于单点故障而带来的风险的方法。对于部署 Web 应用防火墙的企业，从网络安全方面考虑，所有进出的网络流量都必须经过 Web 应用防火墙。如果 Web 应用防火墙出现故障，这时候 Web 应用防火墙就是一个单点故障。对于很多企业来说，长时间的服务中断是不可接受的。

本设备具有高可用性功能，俗称双机热备，可以将本设备带来的单点故障最小化，提高网络的高可靠性。高可用性需要双机协同工作，当出现主设备（master）宕机，备用设备(slave)主动接管主设备的一切工作，待主设备恢复正常后，再次切换到主设备上运行。

如果需要使用 HA 功能，请确认您有两台相同型号的设备，并且配置完全正确。

高可用性配置

工作模式: ☐ 停止 ☒ 主模式 ☐ 备模式

工作状态: 工作中

*本端心跳口: ETH2(192.168.10.2)

*对端心跳口地址: 192.168.10.3 测试连接

网口列表:

接口名称	设备类型
ETH0	物理网口
ETH1	物理网口

注意: 设备将监控列表中的所有网口, 任意网口断开都将触发主从切换。

- 高可用性: 您可以勾选它来决定是否启用高可用性这项功能。

- 工作状态: 用来显示当前本设备的工作状态。

工作中 (Active): 表示本设备正在工作。

备用中 (Suspending): 表示本设备正在待机, 如果检测到主设备出现问题, 备用设备自动接管主设备的工作同时切换到活动中 (active) 状态。

- 设备角色: 选择本设备的工作角色。

主设备(Master): 表示本机是主设备。

从设备 (Slave): 表示本机是备用设备。

- 本设备名称与对端设备名称: 注意本设备名称不能和对端设备名称相同, 并且对端设备的设置的配置需要与本设备对应。

- 心跳线网络设置: 心跳线是用于连接主设备和备用设备两台服务器间的网线。用来实时监测对方的运行状态。本系统提供两个心跳线的接口, HA1 与 HA2, 双心跳线配置用于降低心跳线出现问题而带来网络故障的风险。具体配置可以参考下图。

主设备配置:

高可用性配置

工作模式: ☐ 停止 ☒ 主模式 ☐ 备模式

工作状态: 工作中

*本端心跳口: ETH2(192.168.10.2)

*对端心跳口地址: 192.168.10.3 测试连接

网口列表:

接口名称	设备类型
ETH0	物理网口
ETH1	物理网口

注意: 设备将监控列表中的所有网口, 任意网口断开都将触发主从切换。

保存 应用

从设备配置:

高可用性配置

工作模式: ☐ 停止 ☒ 主模式 ☐ 备模式

工作状态: 备用中

*本端心跳口:

*对端心跳口地址: [? 测试连接](#)

网口列表:

接口名称	设备类型
☒ ETH1	物理网口

[+ 添加](#) [- 删除](#)

[保存](#) [应用](#)

选择接口：设备中启用并且工作在普通状态下的接口（设备初始化接口 DSI 口除外）都可以被选择为心跳线接口。接口的 IP 和工作方式的设定，您可以查看[网络接口](#)中的相关内容。

配置后点击测试连接，测试成功表明心跳线工作正常，如果测试失败请检查网线连接是否正确，【设备角色】，【设备名称】是否填写正确。

 **注意：**

1.如果开启 HA 功能，需要保证两台设备工作状态分别为：主设备为活动中（active）、备用设备为待机（Suspending）后，再行接入到您的实际网络环境中，否则会造成网络环路，引起网络故障。

10.8.1 配置同步

高可用性中，主设备与从设备的配置等数据实时同步的功能，当出现主设备宕机，备用设备主动接管主设备的一切工作时，从设备上的配置将和主设备完全一致，不会对您的网站安全性产生任何影响。同时开启该功能后，您也只需要对主从设备中的任意一台进行配置，就可同步到对端设备。

配置同步

工作方式: ☐ 停止 ☒ 自动同步 ☐ 手动同步

*同步接口:

本设备IP地址: 192.168.1.11

本设备掩码: 255.255.255.0

*对端设备IP地址:

*同步识别码: [随机生成](#)

[保存](#) [? 测试](#) [应用](#) [从对端同步](#)

- 开启配置同步：您可以勾选它来决定是否开启配置同步的功能，开启后处于高可用性状态下运行的 2 台设备会自动同步配置等数据。
- 同步接口：设备中启用并且工作在普通状态下的接口（设备初始化接口 DSI 口除外）都可以被选择为同步接口。接口的 IP 和工作方式的设定，您可以查看[网络接口](#)中的相关内容。
- 配置同步识别码：2 台配置同步的设备，同步识别码必须相同，您可以在一台设备上生成后复制到对端设备，进行同步测试，测试成功后保存识别码。
- 从对端设备同步：该功能可以让没有开启自动同步的主从设备通过手动的操作，实现配置的同步。



注意：

- 1.配置同步功能必须要 2 台设备工作在 HA 状态下才可以生效。
- 2.开启了自动同步功能的主从设备，不可以使用从对端设备同步的功能，如必须使用需停用配置自动同步的功能。
- 3.升级操作只有在配置同步功能关闭时才允许进行。

11、系统维护

11.1 事件管理

11.1.1 通知公告

本页面设置用于发送通知邮件的邮箱信息，包括发送邮件的 SMTP 服务器信息，以及接收通知的邮箱地址。

邮件通知配置	
*发件人邮箱:	support@test.com
*发件人账号:	support
*发件人密码:	*****
*SMTP服务器地址:	smtp.test.com
*SMTP服务器端口:	25
*收件人邮箱:	support@test.com

SMTP 设置：

- 发件人邮箱：用于发送邮件的邮箱。
- 发件人账号：用于发送邮件的账号名称。
- 发件人密码：用于发送邮件的邮箱密码。
- SMTP 服务器地址：用于发送邮件的 SMTP 服务器地址。
- SMTP 服务器端口：用于发送邮件的 SMTP 服务器端口。

通知邮箱设置：

- 收件人邮箱：用于接收通知邮件的邮箱。



提示：

当本设备磁盘空间使用率接近设置上限的 90%的时候，本设备将自动发送邮件提醒管理员。

11.1.1.1 Email 报警

该功能可以在发现高危的入侵记录时立即给管理员发送 Email 报警，并且可以在指定的统计周期内当入侵记录达到阈值时，自动给管理员发送通知邮件。

☒ 开启入侵记录的Email报警功能。(备注：开启后如有报警信息，信息将会发送到您的Email邮箱。)

立即报警：☒ 发现高危入侵记录时，立即发送Email报警。

发送周期： Email报警的发送间隔，单位：小时。

入侵记录阈值： 在发送周期内的入侵记录达到阈值，则发送Email报警。

计划任务： 在计划任务的时间范围内发送Email。

[? 测试发送](#)[保存](#)[应用](#)

- 入侵记录：是否开启该功能的选项。
- 立即报警：发现高危入侵时是否立即发送 Email 报警。
- 发送周期：设置统计周期。
- 入侵记录阈值：设置在该统计周期内入侵记录的阈值，达到该值发送 Email 报警。
- 计划任务：设置该功能的生效时间。

11.1.1.2 SNMP

简单网络管理协议（SNMP）是目前 TCP/IP 网络中应用最为广泛的网络管理协议

SNMP服务器1

IP:

共同体:

SNMP服务器2

IP:

共同体:

SNMP服务器3

IP:

共同体:

[保存](#)[应用](#)

i 提示：

具体配置请询问您的网络管理员，本设备最多支持同时向 3 台服务器发送日志。

11.1.3 SNMP Trap

SNMP Trap：本设备可以通过 SNMP Trap 的方式发送系统

SNMP Trap版本
 SNMP Trap版本:

SNMP服务器1
 IP:
 端口:
 共同体:

SNMP服务器2
 IP:
 端口:
 共同体:

SNMP服务器3
 IP:
 端口:
 共同体:

11.1.4 syslog

syslog 常被称为系统日志或系统记录，是一种用来在互联网协议（TCP/IP）的网络中传递存档信息的标准。本系统支持 syslog 日志的发送。

syslog 服务器1
 IP:
 端口:
 日志方式:

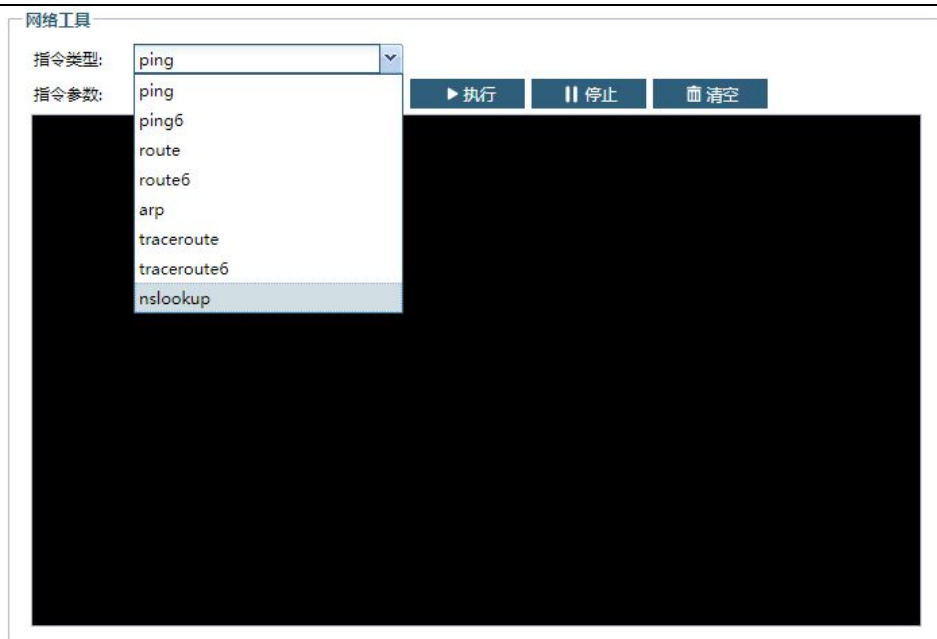
syslog 服务器2
 IP:
 端口:
 日志方式:

syslog 服务器3
 IP:
 端口:
 日志方式:

11.2 网络诊断

11.2.1 网络工具

本设备内部添加的一个包含有 ping、ping6、route、route6、arp、tracert、tracert6 和 nslookup 的网络工具。



- 指令类型：点击下拉菜单，可以选择 8 条常用指令中的一条。
- 指令参数：相应指令所对应的参数，比如 ping 指令可以设定参数为域名或 IP 地址。
- 执行：执行选择的操作指令。
- 停止：一些操作指令需要手动停止，比如 ping。
- 清空：清除界面上显示的信息。

使用 ping 指令：可以检测本设备的网络连接状况

选择指令类型为 ping, 指令参数设定为 192.168.9.1, 点击执行, 出现如下信息。其他指令您可以参照 windows 下命令行的相对应指令信息使用。

网络工具

指令类型:

指令参数:

▶ 执行

|| 停止

🗑 清空

```
PING 192.168.99.67 (192.168.99.67) 56(84) bytes of data.  
64 bytes from 192.168.99.67: icmp_seq=1 ttl=64 time=0.024 ms  
64 bytes from 192.168.99.67: icmp_seq=2 ttl=64 time=0.022 ms  
64 bytes from 192.168.99.67: icmp_seq=3 ttl=64 time=0.022 ms  
64 bytes from 192.168.99.67: icmp_seq=4 ttl=64 time=0.019 ms  
64 bytes from 192.168.99.67: icmp_seq=5 ttl=64 time=0.020 ms
```

11.2.2 抓包工具

该页面用于对本设备的各个接口进行数据抓包的操作。

抓包设置

物理接口:

抓包数目:

数据包长度:

来源IP:

目的IP:

目的端口号:

🔍 开始抓包

抓包文件列表

🔄 刷新 🗑 删除 || 停止抓包

序号	文件名称	状态	操作
1	ETH1_20191028_110932.cap	完成	下载
2	ETH2_20191017_143747.cap	完成	下载
3	ETH1_20191016_132526.cap	完成	下载

11.2.1.1 对指定接口进行抓包

1. 在抓包设置填写接口名称，比如：ETH0，抓包数目、数据包长度、来源 IP、目的 IP 以及目的端口号等信息，点击【开始抓包】；

抓包设置

物理接口:

抓包数目:

1000

数据包长度:

68

来源IP:

目的IP:

目的端口号:

开始抓包

2. 【抓包文件列表】出现抓包的文件名，抓包状态，操作的信息；

抓包文件列表

刷新

删除

停止抓包

序号	文件名称	状态	操作
1	ETH1_20170904_165939.cap	完成	下载

3. 您可以单击【刷新】按钮来查看当前抓包的最新状态，如果抓包时间过长，可以点击【停止抓包】按钮停止此次抓包；
4. 当抓包状态为【完成】时，您可以点击【下载】操作来下载此次的抓包文件。下载后使用“wireshark”等分析软件打开此文件。

11.3 设备维护

11.3.1 配置管理

用于备份和还原当前系统的设置，这些设置包括网络设置、基本参数设置、访问控制、通知设置、关键字过滤拦截、HTTP 类型过滤和防溢出设置等等。

备份配置

说明: 点击“备份配置”按钮备份当前数据库配置。

备份配置

还原配置

备份文件: 请选择备份文件

排除配置: ☐ 网络配置 ☐ 静态路由 ☐ 虚拟网桥 ☐ 用户

☐ 高可用配置 ☐ 配置同步

说明: 选择备份文件, 点击“还原配置”按钮恢复之前配置。

还原配置

恢复默认配置

说明: 点击“恢复默认配置值”按钮恢复本设备默认配置。

恢复默认配置值

- 备份配置： 点击【备份配置】按钮，按照提示将备份配置文件保存到计算机的指定目录中。
- 还原配置： 选择还原配置文件后，点击【还原配置】按钮，将备份文件导入到设备，恢复之前保存的配置。选择排除配置，勾选的功能将不会导入设备。
- 恢复默认配置值： 点击【恢复默认配置值】按钮，则本设备的基本参数设置、关键字过滤、HTTP 类型过滤和防溢出设置将会被恢复为默认值。

⚠注意：

1. 只有从本设备导出的配置文件才可导入，系统不支持导入从其他设备导出的配置文件。
2. 请不要手动修改导出的配置文件，以免造成无法导入。
3. 建议您在配置好本设备后就导出一份配置文件并存放于安全的地方，以便日后需要时导入使用。

11.3.2 授权信息

用于显示本设备的授权信息。每一台锐迅 Web 应用防护系统都有唯一的许可证书，该许可证文件只能导入一次，重复导入相同证书无效。同时，许可证书不能在不同型号、同型号不同设备之间混用。

当设备没有许可证或者许可证已经过期的情况下，使用安全管理员账号登录时就会出现如下页面。

授权信息

许可证已过期！

设备将在一小时内工作于检测模式（无防护能力）！
请联系设备供应商获取有效许可证书！

导入许可证

当本设备许可证是有效期授权类型的，使用安全管理员账号登录时，可以看到当前的许可证状态如下。

授权信息

许可证状态正常！

客户名称: 锐迅测试专用

产品型号: Yxlink WAF-5820

产品序列号: WAF0HW0B1A01

授权有效期: 2017-04-13至2019-05-30

导入许可证

注意：

公司网址：<http://www.yxlink.com/>

134

密级：公开

当设备没有许可证或者许可证已经过期，铱迅 Web 应用防护系统将在一小时之后无防护。如果遇到上述情况，请及时联系供货商或者铱迅信息以便获取有效许可证书。

11.3.3 系统时间

本页面设置设备的系统时间。设置好时间后，点击【应用】按钮，完成系统时间设定。您也可以设置时间同步服务，系统缺省的服务器地址 210.72.145.44 为中国国家授时中心的 NTP 服务器的 IP 地址。

时间设置

*当前时间: 2017-09-04 17:24:11

与本机同步 应用

时间同步服务 (NTP)

服务器地址1: 210.72.145.44

服务器地址2: 请选择或输入服务器地址

服务器地址3: 请选择或输入服务器地址

同步时间

11.3.4 离线升级

通过固件升级，您可以获得最新的产品功能或者加固的产品安全性能。请联系铱迅信息客服人员，然后提交产品序列号，根据您所购买的产品型号获取相应的固件升级文件，在本页面选择升级文件后，点击【升级】按钮，完成产品升级。

升级后，请进入【系统日志】页面查看相关系统日志。

固件升级 规则升级

固件升级

*固件升级，请先选择升 请选择升级文件

级文件:

升级 重置

通过升级内置规则，可以使本设备具备抵御各种最新入侵行为的能力。请联系铱迅信息客服人员，提交产品序列号，然后根据您所购买的产品型号获取相应的规则升级文件，在本页面选择升级文件后，点击【升级】按钮，完成内置规则升级。

升级后，请进入【系统日志】页面查看相关系统日志。

规则升级

*规则升级，请先选择升 请选择升级文件

级文件:

升级 重置

11.3.5 在线升级

在线升级可以实现产品的自动升级，既可以选择固件在线升级还可以选择规则在线升级。

在线升级设置

升级类型:

*升级站点:

升级方式: ☐ 自动升级到最新版本
☐ 不自动升级,有更新时提醒我
☒ 关闭自动升级

检查时间:

代理设置: ☐ 启用HTTP代理

*站点:

*端口:

用户名:

密码:

✓ 应用 ✓ 立即检查

在线升级设置

升级类型:

*升级站点:

升级方式: ☐ 自动升级到最新版本
☐ 不自动升级,有更新时提醒我
☒ 关闭自动升级

检查时间:

代理设置: ☐ 启用HTTP代理

*站点:

*端口:

用户名:

密码:

✓ 应用 ✓ 立即检查

11.3.6 日志清理

系统运行会产生各种日志信息,但过多的日志信息会影响系统的正常运行,建议用户定期对磁盘中的日志进行清理。

自动磁盘清理

系统会在磁盘空间使用率达到设置上限时自动执行磁盘清理工作。设备的“自动清理”会从最早的日志记录开始清理,直到磁盘空间的使用率低于设置值,所以请您记得定期备份日志。

手动磁盘清理

除了系统自动清理功能,您还可以手动进行磁盘清理,在手动清理时,建议您先将日志导出后再删除。

当前磁盘状态

磁盘总大小: 18.82GB, 已使用: 2.69GB, 磁盘空间使用率为: 14%。

选择日志类型

☐ 入侵记录 ☒ 系统日志

选择时间范围

☒ 日期早于

☐ 日期范围

导出 删除

- 当前状态：显示磁盘当前的使用情况，用户可根据磁盘使用率来决定是否进行清理。
- 日志类型选择：选择要处理的日志类型，包括入侵记录、流量记录、系统日志和审计日志。
- 操作日期选择：可选择某个日期之前的所有记录或者选择一个日期的范围。
- 导出日志：首先选择需要导出的日志类型和时间范围，点击【导出】按钮，导出的格式为 csv 文件。请用 Microsoft Excel 等软件查看。导出的日志将无法再导入到设备中。
- 删除日志：首先选择需要删除的日志类型和时间范围，点击【删除】按钮，则指定的日志被直接删除。



注意：

日志删除后不可以恢复，请您确认不再需要查看所选的日志后再决定将其删除。建议您在删除前将日志导出以便日后查看。

11.3.7 关机/重启

本页面用于对设备进行“关机”与“重启”操作。

重新启动

点击“关机”按钮关闭本设备，点击“重启”按钮重启本设备：



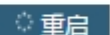
- 关机：点击【关机】按钮，稍后将会安全关闭设备。
- 重启：点击【重启】按钮，将会重新启动设备。

重启数据库

本页面点击 重启 按钮，即可重启数据库。

重启数据库

点击“重启”按钮重启数据库：



注意：

1. 请您尽量避免在本设备正常运行时直接切断电源。
(这样可能造成数据的丢失或者影响设备的使用寿命)
2. 在您点击【关机】按钮，或者直接按下本设备上的电源按钮后，请等待电源指示灯熄灭后再切断电源，设备安全关闭需要一定时间。

12、其他功能

12.1 主动防御

12.1.1 漏洞扫描

本设备的漏洞扫描是基于漏洞数据库，通过扫描手段，对指定的 Web 服务器的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）功能。主要可以扫描以下漏洞信息：SQL 注入、CGI 漏洞、XSS 漏洞、上传漏洞等漏洞信息。

对需要扫描的网站进行添加、删除、开始扫描以及停止扫描等操作。

+ 添加 删除 刷新 全部开始 全部停止 显示结果						
序号	扫描地址	状态	加入时间	完成时间	说明	操作
1	1.1.1.1	未扫描	2017-09-05 09:54:54		服务器地址	编辑 删除
2	www.baidu.com	正在扫描	2017-09-05 09:54:15		扫描百度网站	编辑 删除

- 添加漏洞扫描的网站：点击【添加】按钮，弹出“漏洞扫描-添加”对话框，输入扫描地址和描述信息，点击“保存”，添加成功。

漏洞扫描 - 添加

*扫描地址: 1.1.1.1

说明: test

✓ 保存

↺ 重置

✕ 取消

- 删除漏洞扫描的网站：选择需要删除的记录，点击【删除】按钮，在弹出的确认对话框中点击“是”，删除成功。
- 执行扫描：选中需要开始扫描的记录，点击【全部开始】按钮，在弹出的对话框中选择是即可。

系统提示

?

确认要全部开始扫描吗？

是

否

- 停止扫描：点击【全部停止】按钮，所有正在扫描的任务都将停止。



注意：

如果扫描状态显示为无法访问，请检查“网络配置” - “静态路由”与“网络配置” - “DNS 设置”是否配置正确，配置正确后再次“执行扫描”即可。

12.1.1.1 扫描记录

查看扫描到的漏洞信息，您可以通过本页面显示结果查看扫描到的网站漏洞信息，并导出文件。

显示结果					
删除 清空 刷新			导出		
序号	URL	漏洞类型	域名	详细信息	操作
1	http://baidu.com/IDSWebApp/IDSjsp/Login.jsp	CGI漏洞	baidu.com	Tivoli Directory Server Web Admin...	删除

- 查看扫描任务扫描到的漏洞信息：“漏洞扫描任务”下拉菜单中选择需要查看的任务，点击【显示扫描结果】按钮，即可查看到该任务扫描的漏洞信息。
- 删除漏洞：选中需要删除的漏洞记录，点击【删除】按钮，即可删除该条漏洞。
- 清空漏洞：点击【清空】按钮，即可清除该任务的所有漏洞信息。
- 导出日志：首先查看扫描到的漏洞信息，然后点击【导出日志】按钮，即可将扫描到的漏洞信息导出为 Excel 格式的文件。

12.1.2 URL 自学习

一般来说，Web 应用在不同页面间传递参数，例如：<http://host/test.asp?arg1=samp1&arg2=sample2>，通过这样的 URL 请求(即网址)来传递参数。这类带参数的 URL 请求的作用就是通过 URL 后面附加内容信息来传递相关信息给远程 Web 服务器，并在 Web 服务器进行适当处理后将结果返回给客户端，从而达到网页交互的目的，并实现网页内容动态化。而黑客经常通过篡改这些参数来进行 SQL 注入、XSS 跨站等攻击，威胁 Web 服务器的安全。

本设备的 URL 自学习功能基于正向安全模型，自动学习并构建 Web 服务器的 URL 模型，禁止违反现有模型的尝试行为，这样不仅对于已知类型的攻击行为具有很好的防护效果，而且对于任意未知类型的攻击行为，同样具有非常好的防护效果。

URL 自学习功能，采用主动与被动学习相结合的方式，对 Web 服务器的 URL 参数模式进行学习及识别。在学习完成后，自动检查所有用户访问 Web 服务器的行为，对于违反现有 URL 参数模式的访问行为，按照设定动作进行检测或拦截。

12.1.2.1 URL 自学习

本设备的 URL 主动学习功能通过网页蜘蛛爬虫主动抓取网站的 URL，然后学习 URL 的参数模式。

URL 参数的模式有四种：number-数字、alpha-字母、combination-数字和字母的组合、mixed-混合类型(其他剩余情况)。例如：

<http://www.test.com/test.asp?id=1&id2=sd&id3=ds2&id4=test.exe>，这个 URL 被学习到的 URL 模式为：

[http://www.test.com/test.asp?id=\(number\)&id2=\(alpha\)&id3=\(combination\)&id4=\(mixed\)](http://www.test.com/test.asp?id=(number)&id2=(alpha)&id3=(combination)&id4=(mixed))

当用户提交非法的 URL 请求，例如：

http://www.test.com/test.asp?id=1%20selcet%20*%20from%20admin%20where%201=1&id2=sd&id3=ds2&id4=test.exe

说明：id 的参数原来是数字型，现在被恶意的修改为混合型。

系统将会拦截这种非法的 URL 请求，如下图：

序号	攻击时间	规则编号	规则名称	危害等级	源IP地址	地理位置	目的IP地址	源端口	目的端口	拦截方式	HTTP类...	URL	操作
5	2018-03-15 14:40:11	1920001	违反URL自学习策略	低	192.168.88.83	LAN	192.168.99.69	64694	80	拦截	GET	http://192.168.99.69/downloadshow.asp?id=ufjkaif	自 查
4	2018-03-15 14:40:11	1920001	违反URL自学习策略	低	192.168.88.83	LAN	192.168.99.69	64693	80	拦截	GET	http://192.168.99.69/downloadshow.asp?id=ufjkaif	自 查

本页面提供添加、删除已经学习的域名、查看学习状态、重新学习的功能。

序号	域名	状态	操作
1	192.168.99.69	学习成功	✎
2	www.baidu.com	正在学习，预期完成时间2017-09-05 17:26:44	✎

- 添加需要学习的域名：点击【添加】按钮，弹出“URL 自学习--添加”对话框，输入域名，选择协议：http/https，点击【保存】，自动开始自学习。

URL自学习 - 添加

*域名:

协议:

被动学习: ☒ 开启 (开启后将在指定时间内被动学习未知的URL)

*自动停止时间/小时:

排除文件列表:

✓ 保存

↺ 重置

✕ 取消

- 删除：选中需要删除的域名，点击【删除】按钮，在弹出的对话框中点击【确定】，即可删除。说明：该域名下的所有已学习内容将一起被清理掉。
- 重新学习：选中需要重新学习的域名，点击【重新学习】按钮，自动开始学习。
- 快速查询：输入需要查询的域名，点击【快速查询】，即可查询到相应的域名。



注意：

如果 URL 自学习的状态显示为“学习失败”，则可能是设备无法访问该域名。请从两个方面来排查问题：

1. 进入“网络设置” - “DNS 设置”，检查 DNS 解析服务器，
2. 进入“网络设置” - “静态路由”，检查静态路由是否正确。

12.1.2.2 URL 模式管理

对已经学习到的 URL 模式进行管理，提供手动学习、删除 URL 和删除域名等功能。

[域名详情](#) | [URL模式详情](#) | [URL Cookie](#)
URL列表
[+ 批量学习](#) | [+ 添加](#) | [删除](#) | [▶ 启用](#) | [|| 停用](#) | [刷新](#) | [应用](#)

序号	URL模式类型	URL	是否启用	操作
1	普通URL	http://192.168.99.69/favicon.ico	停用	
2	普通URL	http://192.168.99.69/uppic/200837151032.jpg	停用	
3	普通URL	http://192.168.99.69/uppic/20089241182li.jpg	停用	
4	普通URL	http://192.168.99.69/uppic/2008816134346410.jpg	停用	
5	普通URL	http://192.168.99.69/images/ggwzz.swf	停用	
6	普通URL	http://192.168.99.69/images/pixviewer.swf	停用	
7	普通URL	http://192.168.99.69/images/tit_bg.gif	停用	
8	普通URL	http://192.168.99.69/images/no_list_bg_1.gif	停用	
9	普通URL	http://192.168.99.69/images/topline_botbg.gif	停用	
10	普通URL	http://192.168.99.69/images/bottom.gif	停用	
11	普通URL	http://192.168.99.69/images/gaobei_top2.gif	停用	
12	普通URL	http://192.168.99.69/images/menu-hbg.gif	停用	
13	普通URL	http://192.168.99.69/images/1.gif	停用	
14	普通URL	http://192.168.99.69/images/article_ico_1.gif	停用	

- 查看学习到的 URL 模式：点击【刷新域名列表】，在下拉菜单中选择需要查看的域名。
- 删除域名：点击下拉菜单中的域名，点击【删除域名】按钮，则此域名学习到的所有 URL 模式都将被删除。
- 勾选框【只显示含参数的 URL 地址】：勾选上后只显示带参数的 URL 模式，不勾选将显示所有学习到的 URL 模式。
- URL 模式列表：点击【添加】按钮，弹出“URL 模式详情”对话框：

URL列表 - 添加

提示: 如果您不知道如何填写, 建议先使用URL列表的批量学习功能。

配置项: 192.168.99.69

URL模式类型: ☒ 普通URL ☐ Rewrite URL

是否启用: ☒ 启用 ☐ 停用

*URL路径:

在“需检测 URL 格式”输入需要检测的 URL，在“合法 URL 格式”输入合法格式，然后点击【保存】按钮。

- 删除 URL：选中某条 URL 记录，点击【删除 URL】按钮，弹出确认对话框：

操作确认

×



是否确认删除数据？

是

否

如果勾选【删除该 URL 下所有的参数模式】，则该 URL 的所有参数模式都将被删除。否则，仅仅删除该条 URL 参数模式。

- 批量学习模式：点击后，引擎重新加载所有的 URL 模式。



提示：

对于 <http://www.test.com/test.asp?id=1&id=sa> 这种重复的参数模式，本设备采取的是参数覆盖的模式，最后获取到的参数模式为 [http://test/test.asp?id= \(alpha\)](http://test/test.asp?id=(alpha))。

URL 自学习会将学习到的参数名称进行排序，所以参数顺序的改变不会影响该功能的使用，<http://name/a.asp?id=1&id1=a> 与 <http://name/a.asp?id1=a&id=1> 是相同的 URL 模式。

对于没有被学习到的 URL 参数模式，分为 2 种情况来处理：

- 1、该 URL 从来都没有被学习过，那么该 URL 的所有访问均不会被认为违反 URL 自学习规则，因为该 URL 不存在任何已知的参数模式。
- 2、该 URL 已经存在其它的 URL 参数模式，那么没有被学习到的 URL 参数模式的访问将会被认为违反 URL 自学习规则，最终结果是该 URL 参数模式将被拦截。

对于没有违反 URL 自学习规则，但是包含了攻击行为的 URL，例如：

<http://www.test.com/upfile.asp?id=1.txt> and select * from admin，该 URL 请求符合

[http://www.test.com/upfile.asp?id= \(mixed\)](http://www.test.com/upfile.asp?id=(mixed)) URL 参数模式，仍然会被其他规则检测到并被拦截。

12.1.3 网页防篡改

本设备的网页防篡改功能，采用定期轮询的方式，对网站数据进行监控，发现对网页进行任何形式的非法添加、修改、删除等操作时，立即进行保护，恢复数据并进行告警，同时记录防篡改日志。

在进行正确的防篡改设置后，系统进行网站备份，将网站文件备份到本设备中，备份结束后，自动启动防篡改功能，使被设置为防篡改的网站处于监控状态，达到防篡改的目的。

一般来说，我们都需要定期对网站进行更新。在部署了网页防篡改以后，网站更新的流程如下：

- 在对网站的内容进行更新之前，必须先停止对防篡改网站的监控功能；
- 然后正常进行网站内容的更新；
- 在完成网站内容的更新后，进入本设备的防篡改页面，再次执行网站的重建备份。在重建备份完成后，系统将再次启动对该网站的防篡改监控。

本设备支持两种文件传输的形式，即 FTP 和 SFTP 协议。FTP 为普通的文件传输协议，SFTP 为支持 SSH 的加密文件传输协议。您可以根据实际情况选择其中一种，然后在网站服务器上安装相应的 FTP、SFTP 服务程序。



注意:

本设备缺省选择从 DMI 接口进行防篡改网络数据包的传输，您可以在【静态路由】页面配置特定接口用于防篡改功能。对于添加的防篡改网站，建议您在【静态路由】页面专门添加 DMI 接口到该网站的静态路由。

本页面显示了防篡改的所有相关配置功能菜单，包括添加、删除和修改网页防篡改的网站记录。针对已经配置好的网站记录，可以进行启动监控、停止和重建备份的操作。

序号	网站名称	网站IP地址	是否启用	连接类型	当前状态	计划任务	说明	操作
1	192.168.88.132	192.168.88.132	已启用	FTP	监控中	全天		

下面介绍一下防篡改设置页面的主要功能菜单：

- 添加防篡改：点击【添加】按钮，弹出【防篡改设置-添加】的对话框，按照下面提供的详细步骤，在输入完成后点击保存。则一条防篡改的网站记录被加入到防篡改列表中，同时自动启动该网站的备份过程。

网页防篡改 - 修改

基本信息

*网站名称: 192.168.88.132

说明: 请填写说明, 最长100字符

是否启用: ☒ 启用 ☐ 停用

计划任务: 全天

连接设置

*网站IP地址: 192.168.88.132

*连接用户: Administrator

*连接类型: FTP

*网站相对路径: /

默认编码: gbk

连接密码:

*端口: 21

*并发连接数: 5

监控设置

*监控检查间隔/秒: 120

*监控文件大小限制/B: 10240000

忽略文件列表: 填写要忽略的文件/文件夹, 一行一个, 不可包含竖线。如:
*.jpg
test.html

? 测试连接

✓ 保存

✕ 取消

- 点击【添加】按钮，弹出【防篡改设置-添加】对话框，如图；
- 输入网站名称，在说明框中，可以根据需要输入描述信息；
- 输入网站的 IP 地址；
- 网站路径编码可以选择 gbk 或者 utf8。对于 windows 服务器，请选择 gbk，对于 linux 服务器，请选择 utf8；

- 在连接用户和密码框中输入相应的 FTP/SFTP 的用户名和密码，建议密码长度至少为 10 位，强度至少为数字、字母和标点符号的组合。注意，此用户必须对 FTP/SFTP 服务中的网站相对目录具有除了执行以外的所有控制权限，比如读、写、新建、删除等权限；
- 在连接类型中可以选择 FTP 或者 SFTP；
- 填入连接的端口号（例如：FTP 端口号默认为 21，SFTP 端口号默认为 22）；
- 输入网站文件所在目录，它是相对于 FTP/SFTP 根目录的路径（例如：FTP 根目录为 D:/web，网站路径为 D:/web/www，则所在目录可以填写为 “/www” ）；
- 并发连接数的值为 1~100，缺省为 5；
- 监控检查间隔：输入 FTP 的轮询间隔，比如：60 秒。此值不宜设置过小，不然会增加本设备和网站服务器的负担，推荐设置为 120 秒；
- 设置监控文件的大小，此处留空表示不对文件大小做任何限制；
- 在不做监控的文件类型中可以设置文件类型，其中不同的类型之间用 “|” 隔开，支持文件和目录名称的通配符（例如：**aaa/bbb/*|aaa/a.jpg|aaa/*/ccc.jpg|*.zip**）；
- 点击 ‘测试连接’，检查当前设置的网站是否可以连接。然后保存退出对话框。
- 修改防篡改：选择一个防篡改记录，然后点击【修改】按钮，出现【防篡改设置-修改】对话框。双击防篡改网站也可以直接打开【防篡改设置-修改】对话框。
- 删除防篡改：选择一条防篡改记录，然后点击【删除】按钮，则删除所选防篡改网站。
- 启动监控：选择一条防篡改记录，然后点击【启用监控】按钮，所选防篡改网站将处于监控状态。如果该网站创建备份还没有完成，则启动重建备份的过程。
- 停止：选择一条防篡改记录，然后点击【停止】按钮，则停止对该网站的监控。如果该网站正处于创建备份的过程中，则停止创建备份的过程，此时备份网站处于中间状态，建议您删除该网站后重新添加。
- 重建备份：一般用于网站内容更新以后，防篡改对网站内容的重新备份，也就是将网站更新的内容再次备份到本设备中。在重新创建备份前必须保证网站防篡改监控已经被停止。当然，如果在第一次自动创建网站备份失败的情况下，您也可以手动点击【重建备份】按钮，强制执行网站创建备份的过程。注意：在重建备份之前，请确认网站内容已经被更新并正常工作。
- 查询防篡改记录：输入名称并点击【快速查询】按钮，可以根据名称快速筛选出包含输入名称的防篡改网站。

12.1.3.1 防篡改日志

本页面显示防篡改日志。根据防篡改日志，您可以了解在开启防篡改功能的情况下，网站被非法篡改操作的详细信息。

ID	名称	IP地址	日志内容	日志类型	时间	操作
4	192.168.88.132	192.168.88.132	文件【test.html】被删除，已经恢复！	非法文件删除	2018-03-15 11:19:41	删除
3	192.168.88.132	192.168.88.132	网页防篡改创建备份完成，网站名称：192.168.88.132	系统日志	2018-03-15 11:15:39	删除
2	192.168.88.132	192.168.88.132	新增文件【test.html】，备份成功！	网站备份	2018-03-15 11:15:39	删除
1	192.168.88.132	192.168.88.132	网页防篡改开始创建备份，网站名称：192.168.88.132	系统日志	2018-03-15 11:15:38	删除

- **删除日志：**选择一条或者多条防篡改日志，点击【删除】按钮，这些防篡改记录将被从防篡改日志中删除。
- **清空日志：**点击【清空】按钮，所有的防篡改日志将被删除。
- **日志筛选：**点击【筛选】按钮，弹出【防篡改日志-筛选】对话框，如图。您可以组合篡改类型、网站名称、网站 IP 地址和日志内容，筛选出需要查看的防篡改记录。

防篡改日志 - 筛选

时间:

🔍

日志类型:

▼

名称:

IP地址:

日志内容:

筛选

重置

取消

- **取消筛选：**点击【取消筛选】按钮，可以取消已经筛选出的日志列表，恢复到正常状态，如图。

ID	名称	IP地址	日志内容	日志类型	时间	操作
4	192.168.88.132	192.168.88.132	文件【test.html】被删除，已经恢复！	非法文件删除	2018-03-15 11:19:41	删除
3	192.168.88.132	192.168.88.132	网页防篡改创建备份完成，网站名称：192.168.88.132	系统日志	2018-03-15 11:15:39	删除
2	192.168.88.132	192.168.88.132	新增文件【test.html】，备份成功！	网站备份	2018-03-15 11:15:39	删除
1	192.168.88.132	192.168.88.132	网页防篡改开始创建备份，网站名称：192.168.88.132	系统日志	2018-03-15 11:15:38	删除

12.1.4 数据库防篡改

数据篡改即是数据篡改,增加或删除，造成数据破坏。

数据库关键数据的防篡改检验方法，包括以下步骤：在数据库的记录中设置检验码，校验码根据记录中的关键数据生成；当校验时，生成关键数据的密文；将密文与检验码进行比较，根据比较结果确定关键数据是否被篡改。

数据库防篡改 - 添加

*名称: 请填写名称, 最长50字符

*数据库IP地址: 请填写与数据库IP地址

*数据库用户: sa

触发式检测: ☒ 启用

*数据库类型: Sql Server2000

*检查间隔: 60 (秒):

连接状态: 就绪

是否开启监控: ☒ 启用 ☐ 停用

*数据库端口: 1433

数据库密码: 请填写与数据库密码

*本地代理端口: 请填写与本地代理端口, 限制1-65535

*备份后缀: _bak

计划任务: 全天

测试连接

数据库列表

刷新

sa@%:1433

保存

重置

取消

系统提供数据库防篡改的添加, 删除操作。

12.2 高级设置

12.2.1 关键字过滤

本页面设置和显示需要被拦截的关键字。开启关键字拦截功能后, 与关键字匹配的文字将被替换为 “*”。

关键字过滤

关键字过滤: ☒ 开启关键字过滤功能。(启用后, 系统自动将下面设置的关键字替换为*)

过滤用户请求: ☒ 开启

*端口设置: 80|8080 ☐ 与防护系统检测端口相同

过滤网站响应: ☒ 开启

*端口设置: 80|8080 ☐ 与防护系统检测端口相同

*过滤内容: 法轮功|李洪志|大纪元|真善忍|新唐人|毛一鲜|黎阳平|张小平|戴海静|赵紫阳|胡耀邦|六四事件|退党|天葬|禁书|枪决现场|疆独|藏独|反共|中共|达赖|班禅|东突|台独|台海|肉棍|淫靡|淫水|迷药|迷管药|色情服务|成人片|三级片|激情小电影|黄色小电影|色情小电影|援交|打炮|口活|吹箫|打飞机|冰火|毒龙|全身漫游|休闲按摩|丝袜美女|推油|毛片|淫荡|强奸|熟女|成人电影|换妻|丝袜美足|走光|摇头丸|海洛因|白面|迷幻|麻醉|春药|催情|三唑仑|麻醉乙醚|遗忘药|佳境安定片|蒙汗药粉|麻醉药|买卖枪支|出售枪支|投毒杀人|手机复制|麻醉钢枪|枪支弹药|鬼村|雷管|古方迷香|陈效失忆药|迷奸药|代考|考研枪手|墓碑|印章|办证|证件集团|办理证件|窃听器|汽车解码器|汽车拦截器|开锁枪|侦探设备|远程偷

保存

应用

- 是否开启: 当勾选开启关键字拦截功能并应用生效以后, 数据包中所有被匹配到的关键字将被替换为一个或多个 “*” 符号。
- 过滤用户提交的数据: 当勾选后, 所有用户提交的数据包将被过滤。您可以手工指定需要过滤的端口, 或者直接与防护系统检测端口绑定。
- 过滤网站返回的数据: 当勾选后, 所有网站返回给用户的数据包将被过滤。您可以手工指定需要过滤的端口, 或者直接与防护系统检测端口绑定。
- 当把端口设置全部删除时, 是匹配任意端口。
- 添加和删除关键字: 您可以在文本框中添加或者删除关键字, 关键字之间用 “|” 符号隔开。

- 保存： 点击【保存】按钮后将保存当前更改到数据库。
- 应用： 点击【应用】按钮后将保存当前更改并且立即生效。建议您将所有的更改完成以后再点击【应用】按钮。
- 编码方式： 支持 UTF-8、GBK 等编码方式。不支持通配符等特殊符号。

⚠注意：

开启关键字过滤功能，可能导致包含关键字的文件在传输时，文件的内容被修改。建议您只勾选“过滤用户提交的数据”而不要勾选“过滤网站返回的数据”，并设置好 Web 服务器的端口。这样，系统将只检查上传至 Web 服务器的流量，对于用户下载的内容将不作检查。

⚠提示：

本设备不支持对采用 gzip 等方式压缩的网站返回数据进行关键字过滤。

12.2.2 弱密码检测设置

本页面提供了对防护页面中的用户名和密码字段检测的相关功能，您可以设定密码检测的字段、密码检测的等级和需要检测的页面。

12.2.2.1 弱密码检测设置

开启弱密码检测设置，需要添加 URL 和检测等级信息，点击保存，保存配置信息。

12.2.2.2 检测页面列表

+ 添加 删除 刷新 设置 应用 弱密码检测状态: 已开启			
序号	URL	检测等级	操作
1	http://192.168.98.180/admin*	98	✎
2	https://www.test.com/*	20	✎

- 添加：添加一条检测页面，可以设定检测等级。检测等级越高可以检测更复杂的用户名和密码的字段内容。

- 修改：选择一条页面，单击修改，可以更改 URL 内容和设定的检测等级。

- 删除：可以选择一条或多条页面，点击删除，就可以删掉选定的页面内容。

12.2.3 高级防御方式

高级防御方式可以防御 TCP/IP 碎片攻击。TCP/IP 碎片攻击是攻击者在攻击报文前构造大量的正常报文，用以达到绕过检测的目的，正常情况下请勿修改缺省值。高级防御方式主要设置组包大小设置和最大检测长度设置。

网站防护方式设置：勾选网站防护，一键提升网站防护等级，在重大安保期间可大幅度提升网站的防护。

高级防御方式设置

TCP/IP碎片攻击防护: ☒ 启用TCP/IP碎片攻击防护

组包大小设置/KB:

说明: TCP/IP碎片攻击是攻击者在攻击报文前构造大量的正常报文，用以达到绕过检测的目的，正常情况下请勿修改缺省值。

最大检测长度/KB:

说明: 最大检测长度指设备对POST等报文最大的检测大小，超过该大小的内容将不进行检测以节省系统资源。

网站防护方式设置

网站防护: ☐ 启用网站防护等级提升

12.2.4 紧急模式

紧急模式通过设置流量阈值来控制过设备的流量。流量速率超过此设置数值时，启动紧急模式，此时流量将不经过检测引擎

紧急模式

紧急模式: ☐ 启用紧急模式

*流量阈值/Mbps:

说明: 流量速率超过此设置数值时，启动紧急模式，此时流量将不经过检测引擎。

12.2.5 一键断网

一键断网功能可用于手机微信端快捷操作断网请求。发送断网请求所填的 IP/IP 段/域名或全部断网，服务器将无法访问，返回重定向页面。微信端还提供一键恢复、设备 Web 密码复位、一键提升网站防护等级、解绑等功能。

绑定步骤：

1. 关注公众号：进入 WAF 一键断网页面：其他功能-->高级防御-->一键断网，用手机扫描【公众号】二维码关注“铱迅安全港”。

2. 绑定设备：在微信端点击【产品服务】--【WAF 一键断网】--【+绑定设备】

在 WAF 一键断网界面点击【设备信息】按钮生成设备信息二维码。

在微信端点击【扫一扫】，扫描设备信息二维码，微信端自动生成填写序列号、二维码。

设备别名：手动输入设备名称

手机号码：填写绑定的手机号

验证码：点击【获取验证码】，输入获取到的验证码

点击【绑定】，绑定成功！

3.验证是否绑定成功

微信端会收到设备绑定成功通知

设备绑定成功通知
19/10/09 17:33

设备ID : WAF0HW0B1A01
设备名称 : 98.50
绑定时间 : 2019年10月09日 17:34
备注 : 现在你可以用你的微信来对WAF设备【一键断网】了

在 WAF 界面上【一键断网】--【绑定查询】查看有无绑定信息。

注意：一个手机可以绑定多台 WAF，一台 WAF 支持多个手机绑定。

微信端发送一键断网请求

首先在 WAF【一键断网】页面点击【启用】



在微信端点击绑定的设备下拉框，选择【一键断网】

类型：选择 IP/IP 段/域名，需要手动输入需要网段的服务器的地址或域名，支持 IP/IP 段/域名 3 种格式书写

重定向页面：无重定向页、默认页面、自定义页面 3 种可选择

点击【一键断网】按钮，输入获取的验证码，断网操作成功，微信端会收到执行结果通知

执行结果通知
19/10/08 17:31

任务主机 : 【98.51】
任务名称 : 一键断网
【192.168.1.1】
执行状态 : 执行成功
执行时间 : 2019-10-08 17:31:47
备注 : 如有疑问，请联系钰迅技术支持

同时 WAF 界面上会显示一条断网条目

序号	断网方式	断网内容	重定向页面	是否启用	添加时间	操作
1	全部断网		默认页面	已停用	2019-10-30 13:50:35	面
2	IP	192.168.1.1	自定义页面	已停用	2019-10-31 14:17:29	面
32	IP	192.168.1.1	默认页面	已启用	2019-10-31 14:17:40	面

访问所添加的服务器地址会返回选择的重新定向页面

例如默认重新定向页面显示如下

访问禁止

- 确保浏览器的地址栏中的地址拼写和格式正确无误；
- 单击后退返回上一页；
- 如有任何疑问，请与管理员联系。

○ 详细>>

检测到可疑访问，事件编号：18446744073709551615

若类型选择全部断网，微信端会发送全部断网执行结果通知

执行结果通知

19/10/09 17:48

任务主机：【98.50】

任务名称：全部断网

执行状态：执行成功

执行时间：2019-10-09 17:49:09

备注：如有疑问，请联系锐迅技术支持

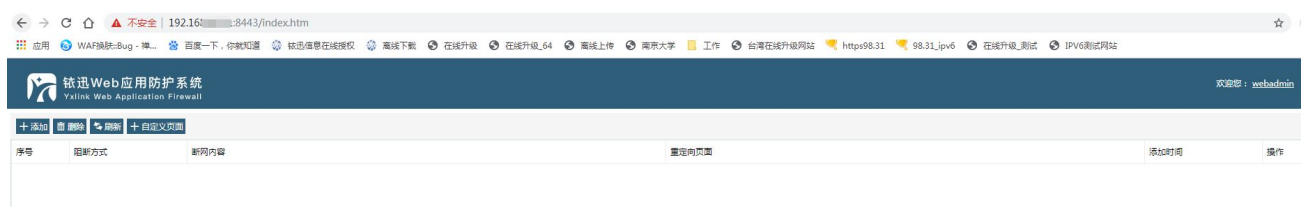
同时 WAF 界面上会显示一条断网条目

序号	断网方式	断网内容	重定向页面	断网结果	添加时间	操作
1	全部断网	默认页面		已断网	2019-11-07 15:59:37	管理

访问所有的服务器都会返回重定向页面，全部断网操作成功。

设备的 8443 端口也提供一键断网条目添加、删除以及自定义页面添加。访问 DMI 口的 8443 端口：

<https://192.168.xx.x:8443> webadmin 用户登录即可。显示页面如下图



服务器列表

未断网页面：记录未断网的服务器，可点击【断网】按钮执行断网操作；

已断网页面：记录已断网的服务器，可点击【恢复】按钮执行恢复操作；

设备 Web 密码复位

点击设备 Web 密码复位，输入验证码，设备密码复位成功。

密码恢复默认 用户名：webadmin 密码：webadmin

微信端收到执行结果通知

一键提升网站防护等级

点击【开】，一键提升网站防护等级功能开启

自动启用 8 条规则： 1334096-1334102、1930500

自动开启智能阻断、防扫描、木马上传检测功能；

点击【关】，一键提升网站防护等级功能关闭

8 条规则： 1334096-1334102、1930500 恢复到开启前状态；

智能阻断、防扫描、木马上传检测功能恢复到开启前状态；

解绑

点击【解绑】，输入验证码，解绑成功。

微信端收到执行结果通知

设备解绑通知

19/10/09 17:33

设备ID： WAF0HW0B1A01

设备名称： 98.51

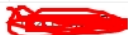
解绑时间： 2019年10月09日 17:34

备注： 感谢您的使用

12.3 访问统计

12.3.1 网站统计

用于显示被本设备所防护网站每天的访问量和攻击数，如下图所示。

删除 清空 筛选 刷新 请选择查看日期: 2017-09-06				
序号	域名	总访问量	总攻击数	操作
1		26	1	

- 选择查看日期：您可以在【请选择查看日期】右侧点击日历图标，如图，在弹出的日历窗口中选择某一个日期。或者您也可以手工输入需要查看记录的日期，请注意输入日期的格式，例如：2017-09-06

请选择查看日期: 2017-09-06

九月 2017

日	一	二	三	四	五	六
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

今天

- 筛选：当域名较多的时候，可以筛选功能筛选出符合条件的记录。
选择统计时间，输入主机头名，即可查询出符合条件的记录，如图。

访问记录 - 筛选

*统计月份: 2017-09

网址: http://s.f.360.cn/scan

最后访问IP: 请填写最后访问IP 最后访问端口: 请填写访问端口, 限制1-65535

目的IP: 请填写目的IP 目的端口: 请填写目的端口, 限制1-65535

筛选 重置 取消

筛选出的记录，如下图所示。

序号	网址	访问...	最后访问...	地理位置	最后访问...	目的IP	目的端口	浏览器类...	最后访问时...	操作
1	http://s.f.360.cn/scan	2	192.168...	LAN	3945	180.163...	80		2017-09-0...	

- 刷新：点击【刷新】按钮，刷新当前页面显示的数据。

12.3.2 访问记录

该页面统计并显示每个 Web 页面的访问次数、最后访问时间、浏览器类型等信息，用户可以按月份查看该月的页面访问信息。如需打开此功能请参照：[其他设置](#)

删除 清空 筛选 刷新 导出

请选择查看月份: 2017-09

序号	网址	访问...	最后访问IP	地理位置	最后访问端口	目的IP	目的端口	浏览器类型	最后访问时间	操作
1	http://s.f.360.cn/scan	2	192.168.99.70	LAN	3945	180.163.222.2...	80		2017-09-05 15:5...	
2	http://www.download...	2	192.168.99.70	LAN	3802	222.186.137.2...	80	Microsoft-Cry...	2017-09-05 15:4...	
3	http://www.download...	2	192.168.99.70	LAN	3802	222.186.137.2...	80	Microsoft-Cry...	2017-09-05 15:4...	
4	http://update.gouwu.s...	2	192.168.99.70	LAN	3091	221.228.218.1...	80	Mozilla/5.0 (W...	2017-09-05 15:3...	
5	http://update.gouwu.s...	2	192.168.99.70	LAN	3091	221.228.218.1...	80	Mozilla/5.0 (W...	2017-09-05 15:3...	
6	http://linnotechx.com/...	2	192.168.99.70	LAN	3712	106.75.114.232	80	Mozilla/5.0 (W...	2017-09-05 15:4...	
7	http://imp.ad-plus.cn/2...	2	192.168.99.70	LAN	3500	101.227.172.23	80	Mozilla/5.0 (W...	2017-09-05 15:3...	
8	http://images.sohu.com...	2	192.168.99.70	LAN	3422	221.228.218.2...	80	Mozilla/5.0 (W...	2017-09-05 15:3...	
9	http://xjd.com/exsites?...	2	192.168.99.70	LAN	3468	36.110.181.246	80	Mozilla/5.0 (W...	2017-09-05 15:3...	
10	http://vinci.ie.sogou.co...	22	192.168.99.70	LAN	2972	220.181.124.50	80	Mozilla/5.0 (W...	2017-09-05 15:3...	
11	http://update.gouwu.s...	2	192.168.99.70	LAN	3087	221.228.218.1...	80	Mozilla/5.0 (W...	2017-09-05 15:3...	

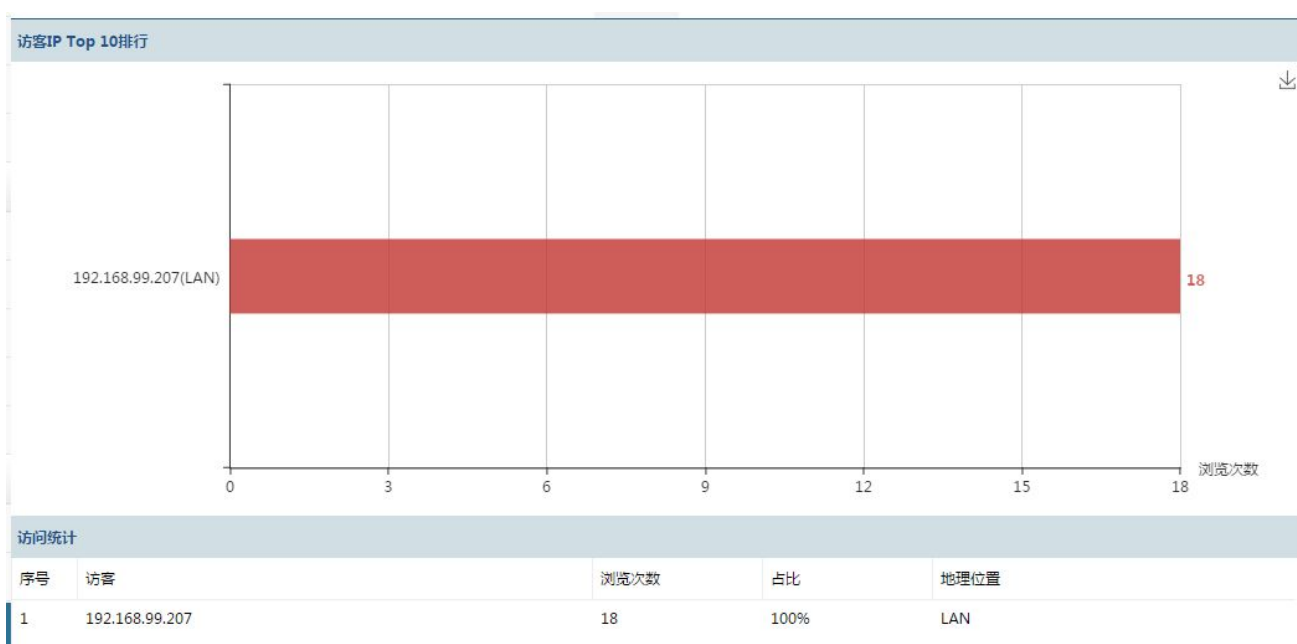
- 同步最新访问页面数据：页面访问信息的数据将定期自动更新，您也可以点击【同步最新数据】按钮强制更新并查看最新页面访问数据。

- 清空页面访问记录： 点击【清空】按钮可以清空当前选定月份的页面统计数据，以便重新统计。
- 刷新： 点击【刷新】按钮，刷新所显示的页面访问记录。与【同步最新数据】不同的是，【刷新】仅从数据库中获取数据，若想查看最新页面访问数据，请使用【同步最新数据】按钮。
- 历史访问记录查询： 选择指定月份后，点击【快速查询】按钮可以快速查看该月的页面统计信息。
- 复制网址到剪贴板： 直接双击某条记录便可以把该条记录的网址复制到剪贴板中。

12.3.3 网站详情

网站详情界面提供了访问记录统计，浏览器统计，操作系统统计，来源页面统计，搜索引擎统计，关键词统计，访问统计，单日访问统计等记录查询。

访问统计，如下图所示：



13、Console 功能

Console 口可以对设备进行常用配置，特别是当设备无法通过 Web 方式进行正常的管理维护的时候，可以通过 Console 功能，对设备进行管理，查看设备的状态，对设备进行配置、复位或还原等操作。

- 登录：用 PC 连接设备 Console 口，输入用户名：conadmin 密码：conadmin。

```
*****
*                                     *
*      Welcome to Yxlink Web Application Firewall      *
*      You can input ? for help                       *
*                                     *
*****
WAF>> █
```

- 帮助：输入 “?” 或者 “help”。

13.1 常用命令



注意：

所有的参数请根据实际情况输入。

13.1.1 主菜单:

在主菜单界面输入 “?” 显示“主菜单目录”，主菜单提供常用的网络命令，ping, route, traceroute, nslookup, 查看设备信息以及关机重启等操作。

```
WAF>>
configure      Enter configure model
show           Show all information
arp            Display Arp table
ping           Send echo messages
route          Display the IP routing table
traceroute     Trace route to destination
nslookup       Query Internet name servers
reboot         Reboot the system
shutdown       Shutdown the system
help           List all available commands
exit           Quit the console
WAF>>
```

主菜单常用命令

显示接口信息:

WAF>> show interface

显示设备信息:

WAF>> show wafinfo

显示网卡 MAC 地址:

WAF>> show macaddress

显示 ARP 信息:

WAF>> arp

重启:

WAF>> reboot

关机:

WAF>> shutdown

13.1.2 配置菜单 (configure) :

在主菜单输入: *configure* 进入配置菜单, 在配置主菜单界面输入 “?” 显示配置菜单目录, 配置菜单可以配置 DMI, DSI, DNS, DHCP, 还原, 复位等操作。

```
WAF>> configure
WAF(configure)#
system      Set the system information
show        Display some configuration
restore     Restore the software
reset       Reset the device
help        List all available commands
exit        Exit from configure mode
```

配置菜单常用命令:

参数说明:

netmask 子网掩码

gateway 网关

ip_begin DHCP 起始 IP

ip_end DHCP 结束 IP

配置 DMI:

WAF(configure)#system interface DMI ip 192.168.9.10 netmask 255.255.255.0 gateway 192.168.9.1

配置 DSI:

WAF(configure)#system interface DMI ip 192.168.100.2 netmask 255.255.255.0 gateway 192.168.100.1

配置系统时间:

WAF(configure)#system clock 2012-09-12

配置首选 DNS:

WAF(configure)#system dns1 8.8.8.8

配置备用 DNS:

WAF(configure)#system dns2 9.9.9.9

配置 DHCP:

WAF(configure)#system dhcp ip_begin 192.168.9.10 ip_end 192.168.9.100

修改密码:

WAF(configure)#system passwd 123456789

显示系统时间:

WAF(configure)#show clock

显示 DMI:

WAF(configure)#show DMI

显示 DSI:

WAF(configure)#show DSI

显示 DHCP:

WAF(configure)#show dhcp

显示 DNS:

WAF(configure)#show dns

还原:

WAF(configure)#restore

复位:

WAF(configure)#reset

返回上级菜单:

WAF(configure)#exit

14、复位与还原

如需对设备复位,必须先断开 DMI 接口的网络连接,并通过 DSI 接口连接本设备。然后通过浏览器访问页面 https://192.168.100.1/product_reset.htm。此处的 192.168.100.1 可能根据您的具体设备有所不同,请参考[附录 A.1. 设备设置接口\(DSI 接口\)初始设置](#)。

铱迅Web应用防护系统复位

请确认您已经断开DMI接口的网络连接，并通过DSI接口的网络连接进入这个页面，否则无法执行复位。

注意：请提前备份系统配置，在复位后，本设备的配置和运行数据将全部复位到出厂状态。

请选择操作

系统复位

系统还原

点击【系统复位】将会使本设备的所有设置恢复到出厂值，所有的入侵记录和页面统计数据等日志数据将被清空，用户账户和密码将恢复到出厂值。

点击【系统还原】后，除了执行【系统复位】的操作外，还将会使设备固件恢复到出厂版本。只有在固件升级失败和系统异常时才可以使用。



注意：

请提前备份系统配置并且导出重要的日志数据。在设备复位或还原后，本设备的配置和运行数据将全部恢复到出厂状态。

15、常见问题与解答

问题：选择某个日期后，查看不到任何入侵记录？

解答：当天没有任何入侵事件产生，所以没有记录。如果您选择的是一个很早的日期，有可能这个日期的入侵记录日志已经被清理掉。

问题：如何知道本系统处于正常工作状态？

解答：可以向被本设备防护的 Web 服务器发送测试攻击报文，查看入侵记录中是否记录下该次攻击行为。例如，在浏览器中输入：<http://www.test.com/aaa.mdb>，其中 www.test.com 需要替换为 Web 服务器上的实际域名。

问题：修改某个设置后，好像没有生效？

解答：请点击该页面的【应用】按钮后等待 1 分钟左右，设置生效需要一定时间。

问题：如何正常关闭设备？

解答：按下本设备背面的电源按钮或者进入【重新启动】页面后点击【关机】按钮。安全关闭设备需要一定时间，前面板的 Power 灯熄灭后，设备正常关闭。

问题：使用本设备后，部分网页访问不正常？

解答：

- (1) 请检查自定义规则，是否是由于您写的自定义规则导致数据包被误拦截。
- (2) 请检查关键字设置中是否包含了会造成大量数据包内容被替换的字符，如您将关键字设置为单个字符，系统点击保存时，系统将会，自动去除单个字符。
- (3) 如果仍然出现此问题，请检查是否由内置规则误拦截引起。如果是，请停用此内置规则。

问题：无法进入 Web 管理页面怎么办？

解答：

- (1) 请先确认计算机能和本设备进行正常通讯（如果计算机开启了防火墙，请将 443 端口打开）。
- (2) 如果仍然无法进入 Web 管理页面，请尝试从 DSI 接口连接。
- (3) 如果从 DSI 接口仍然无法进入 Web 管理页面，请参考问题 7。

问题：忘记管理员密码怎么办？

解答： 方法一：可以通过密码复位功能重置管理员密码。首先，拔下 DMI 接口的网线，从 DSI 接口用网线连接计算机，并参考《铱迅 Web 应用防护系统安装部署手册》设置您的计算机网络参数。在浏览器中访问 https://192.168.100.1/product_reset.htm，根据提示进行产品密码复位。

方法二：手机微信端关注“铱迅安全港”，产品服务-->WAF 一键断网-->绑定设备-->设备 Web 密码复位，通过短信验证进行复位。

问题：规则升级失败怎么办？

解答：如果规则升级失败，系统会自动进行规则回滚操作，因此您不用担心规则升级失败。在确认升级文件正确的情况下，如果再次升级失败，请联系铱迅客服人员。

问题：固件升级失败怎么办？

解答：如果升级失败，请首先检查设备是否工作正常。如果一切正常，请忽略此失败事件。如果不正常，请参考问题 7 进行产品复位。如果仍然无法解决此问题，请联系铱迅客服人员。

附录 A. 出厂默认设置

A.1. 设备设置接口(DSI 接口)初始设置

IP 地址	192.168.100.1
子网掩码	255.255.255.0

A.2. 预置账号

A.2.1. 系统管理员预置账号

用户名	sysadmin
密 码	sysadmin

A.2.2. 安全审计员预置账号

用户名	auditor
密 码	auditor

A.2.3. 安全管理员预置账号

用户名	webadmin
密 码	webadmin

A.2.4. Console 用户预置帐号

用户名	conadmin
密 码	conadmin

A.3. 默认设置

设置项	值
防护系统检测端口	80 8080
防护系统检测方向	不开启双向检测
HTTP 返回报文检测:	开启
重定向页面	开启
网站统计	开启
页面统计	不开启
网站隐身	不开启
端口镜像检测	不开启
入侵阻断时间	低
磁盘空间上限	80%
关键字拦截	不开启

HTTP 请求类型	不勾选 GET、POST、HEAD
定期报表	开启每月报表邮件发送
HTTP 返回报文检测	开启
防护系统拦截方式	高级模式
Email 报警	开启入侵记录 Email 报警 开启高危入侵报警
防溢出设置	Accept 长度：2048 Accept-Charset 长度：2048 Accept-Encoding 长度：2048 Authorization 长度：2048 Cookie 长度：32767 Host 长度：2048 Post 长度：10000000 Proxy-Authorization 长度：2048 Referer 长度：2048 URL 长度：2048 User-Agent 长度：2048 Connection 长度：64 Cache-Control 长度：128 Server 长度：1024
防扫描设置	不开启
智能阻断设置	开启
数据挖掘设置	不开启
HTTP 请求类型设置	勾选 PUT、DEBUG、DELETE、TRACE、COPY、MOVE、TRACK
备案审查	不开启
DDOS 防护设置	不开启
CC 防护设置	不开启
IPv6 协议支持	开启
单网口模式	不开启
固件在线升级	不自动升级，有更新是提醒我
规则在线升级	自动升级到最新版本
一键断网	不开启

附录 B. 正则表达式入门

B.1. 简述

正则表达式 (英文: Regular Expression) 在计算机科学中, 是指一个用来描述或者匹配一系列符合某个句法规则的字符串的单个字符串。

在编写处理字符串的程序或网页时, 经常会有查找符合某些复杂规则的字符串的需要。正则表达式就是用于描述这些规则的工具。换句话说, 正则表达式就是记录文本规则的代码。

很可能您使用过 Windows/Dos 下用于文件查找的通配符(wildcard), 也就是*和?。如果您想查找某个目录下的所有的 Word 文档的话, 您会搜索*.doc。在这里, *会被解释成任意的字符串。和通配符类似, 正则表达式也是用来进行文本匹配的工具, 只不过比起通配符, 它能更精确地满足您的需求。当然, 代价就是更复杂。例如您可以编写一个正则表达式, 用来查找所有以 0 开头, 后面跟着 2-3 个数字, 然后是一个连字符号 "-", 最后是 7 或 8 位数字的字符串(像 025-12345678 或 0513-7654321)。

B.2. 历史

最初的正则表达式出现于理论计算机科学的自动控制理论和形式化语言理论中。在这些领域中有对计算 (自动控制) 的模型和对形式化语言描述与分类的研究。1940 年代, Warren McCulloch 与 Walter Pitts 将神经系统中的神经元描述成小而简单的自动控制元。在 1950 年代, 数学家斯蒂芬·科尔·克莱尼利用称之为「正则集合」的数学符号来描述此模型。肯·汤普逊将此符号系统引入编辑器 QED, 然后是 Unix 上的编辑器 ed, 并最终引入 grep。自此, 正则表达式被广泛地使用于各种 Unix 或者类似 Unix 的工具, 例如 Perl。

Perl 正则表达式源自于 Henry Spencer 写的 regex, 它已经演化成了 pcre (Perl 兼容正则表达式, Perl Compatible Regular Expressions), 一个由 Philip Hazel 开发的, 为很多现代工具所使用的库。

B.3. 入门

学习正则表达式的最好方法是从例子开始, 理解例子之后再自己对例子进行修改、实验。下面给出了一个简单的例子, 并对它们作详细的说明。

假设您书写自定义规则的时候, 想检测用户提交的数据里有没有注入语句是否包含 or, 于是查找 or, 您可以使用正则表达式 or 来匹配。2 个英文字母的匹配, 太简单了; 可是, 要是用户提交的是大写的 OR 呢, 或者是大小写混编的 Or、oR 呢, 幸运的是, 正则表达式提供了忽略大小写的选项。

然而, 不久您可能又会发现, 虽然大小写都能检测了, 但也匹配到了很多不应该匹配的单词, 例如 door, report, organization, word, 如果用 or 来匹配, 所有包含 or 的单词都会被匹配出来, 这显然不是您想要的。这时如果要精确地匹配 or 这个单词的话, 您应该使用\b or\b。

`\b` 是正则表达式规定的元字符，代表着单词的开头或结尾，也就是单词的分界处。虽然通常英文的单词是由空格，标点符号或者换行来分隔的，但是 `\b` 并不匹配这些单词分隔字符中的任何一个，它只匹配一个位置。

接着，如果您觉得 `and` 也需要检测，而不仅仅是 `or`，在正则表达式里，您可以轻松的做到：`\b(or|and)\b`，在正则表达式里，`|` 竖直接分隔符代表选择；当然，您也可以这么写：`(\bor\b|\band\b)`。

写了这么多了，也许匹配的还不是太精确，也许您还想加上 `select` 关键词，于是您应该用上

`\b(or|and)\b.*\bselect\b`。

这里，`.` 是另一个元字符，匹配除了换行符以外的任意字符。`*` 同样是元字符，不过它代表的不是字符，也不是位置，而是数量——它指定 `*` 前边的内容可以连续重复使用任意次以使整个表达式得到匹配。因此，`*` 连在一起就意味着任意数量的不包含换行的字符。现在 `\b(or|and)\b.*\bselect\b` 的意思就很明显了：匹配含有 `or` 或者 `and`，并且之后（无换行符）含有 `select` 的所有字符串。换行符就是 `'\n'`，ASCII 编码为 10（十六进制 0x0A）的字符。

如果同时使用其它元字符，您可以构造出功能更强大的正则表达式。比如咱们来看一个 IP 匹配的例子：一般的 IPv4 下的 IP 是类似这么写的：192.168.200.100，您想匹配这个 IP，可以这样写正则表达式：

`\d\d\d\d\d\d\d\d\d\d\d\d\d\d`

三个数字加一个点加三个数字加一个点加三个数字加一个点加三个数字，这样是能匹配到例子里的 IP，可是要是 IP 其中一位换成 1 个或者 2 个数字，就匹配不到了。

这里的 `\d` 是个新的元字符，匹配一位数字（0，或 1，或 2，或.....）。由于 `.` 是正则表达式的元字符，因此您必须在之前加上 `\` 对 `.` 进行转义。`\` 可以取消元字符的特殊意义，使其变成原始的字符串。例如，要查找 `.` 与 `*`，您应该使用 `\.` 和 `*`。当然，要查找 `\` 本身，您也得用 `\\`。

为了避免那么多烦人的重复，您可以改写上面的表达式：`\d{3}\d{3}\d{3}\d{3}`。这里 `\d` 后面的 `{3}` 的意思是前面 `\d` 必须连续重复匹配 3 次，既然可以设置重复三次，是否觉得上面的写法太过冗余了，于是这么改：`(\d{3}\.){3}\d{3}`，这样做精简了正则表达式的代码，但是还是没能解决 IP 某一位是 1 个或者 2 个数字的问题，在正则里 `{3}` 代表重复三次，`{1,3}` 代表可以重复一到三次，综上所述，一个简单的 IP 地址匹配的正则表达式就出来了：`(\d{1,3}\.){3}\d{1,3}`。

B.4. 表达式全集

字符	描述
<code>\</code>	将下一个字符标记为一个特殊字符、或一个原义字符、或一个向后引用、或一个八进制转义符。例如， <code>「n」</code> 匹配字符 <code>「n」</code> 。 <code>「\n」</code> 匹配一个换行符。序列 <code>「\\」</code> 匹配 <code>「\」</code> 而 <code>「\」</code> 则匹

	配「(」。
^	匹配输入字符串的开始位置。如果设置了 RegExp 对象的 Multiline 属性, ^也匹配「\n」或「\r」之后的位置。
\$	匹配输入字符串的结束位置。如果设置了 RegExp 对象的 Multiline 属性, \$也匹配「\n」或「\r」之前的位置。
*	匹配前面的子表达式零次或多次。例如, zo*能匹配「z」以及「zoo」。*等价于{0,}。
+	匹配前面的子表达式一次或多次。例如,「zo+」能匹配「zo」以及「zoo」,但不能匹配「z」。 +等价于{1,}。
?	匹配前面的子表达式零次或一次。例如,「do(es)?」可以匹配「do」或「does」中的「do」。 ?等价于{0,1}。
{n}	n 是一个非负整数。匹配确定的 n 次。例如,「o{2}」不能匹配「Bob」中的「o」,但是能匹配「food」中的两个 o。
{n,}	n 是一个非负整数。至少匹配 n 次。例如,「o{2,}」不能匹配「Bob」中的「o」,但能匹配「foooooo」中的所有 o。「o{1,}」等价于「o+」。「o{0,}」则等价于「o*」。
{n,m}	m 和 n 均为非负整数,其中 n<=m。最少匹配 n 次且最多匹配 m 次。例如,「o{1,3}」将匹配「foooooo」中的前三个 o。「o{0,1}」等价于「o?」。请注意在逗号和两个数之间不能有空格。
?	当该字符紧跟在任何一个其他限制符 (*,+,?, {n}, {n,}, {n,m}) 后面时,匹配模式是非贪婪的。非贪婪模式尽可能少的匹配所搜索的字符串,而默认的贪婪模式则尽可能多的匹配所搜索的字符串。例如,对于字符串「oooo」,「o+?」将匹配单个「o」,而「o+」将匹配所有

	「o」。
.	匹配除「\n」之外的任何单个字符。要匹配包括「\n」在内的任何字符，请使用像「[\n]」的模式。
(pattern)	匹配 pattern 并获取这一匹配。所获取的匹配可以从产生的 Matches 集合得到，在 VBScript 中使用 SubMatches 集合，在 JScript 中则使用 \$0...\$9 属性。要匹配圆括号字符，请使用「\」或「\)」。
(?:pattern)	匹配 pattern 但不获取匹配结果，也就是说这是一个非获取匹配，不进行存储供以后使用。这在使用或字符「()」来组合一个模式的各个部分是很有用。例如「industr(?:y ies)」就是一个比「industry industries」更简略的表达式。
(?=pattern)	正向预查，在任何匹配 pattern 的字符串开始处匹配查找字符串。这是一个非获取匹配，也就是说，该匹配不需要获取供以后使用。例如，「Windows(?:=95 98 NT 2000)」能匹配「Windows2000」中的「Windows」，但不能匹配「Windows3.1」中的「Windows」。预查不消耗字符，也就是说，在一个匹配发生后，在最后一次匹配之后立即开始下一次匹配的搜索，而不是从包含预查的字符之后开始。
(?!pattern)	负向预查，在任何不匹配 pattern 的字符串开始处匹配查找字符串。这是一个非获取匹配，也就是说，该匹配不需要获取供以后使用。例如「Windows(?:!95 98 NT 2000)」能匹配「Windows3.1」中的「Windows」，但不能匹配「Windows2000」中的「Windows」。预查不消耗字符，也就是说，在一个匹配发生后，在最后一次匹配之后立即开始下一次匹配的搜索，而不是从包含预查的字符之后开始
x y	匹配 x 或 y。例如，「z food」能匹配「z」或「food」。「(z f)ood」则匹配「zood」或「food」。
[xyz]	字符集合。匹配所包含的任意一个字符。例如，「[abc]」可以匹配「plain」中的「a」。
[^xyz]	负值字符集合。匹配未包含的任意字符。例如，「[^abc]」可以匹配「plain」中的「p」。

[a-z]	字符范围。匹配指定范围内的任意字符。例如，「[a-z]」可以匹配「a」到「z」范围内的任意小写字母字符。
[^a-z]	负值字符范围。匹配任何不在指定范围内的任意字符。例如，「[^a-z]」可以匹配任何不在「a」到「z」范围内的任意字符。
\b	匹配一个单词边界，也就是指单词和空格间的位置。例如，「er\b」可以匹配「never」中的「er」，但不能匹配「verb」中的「er」。
\B	匹配非单词边界。「er\B」能匹配「verb」中的「er」，但不能匹配「never」中的「er」。
\cx	匹配由 x 指明的控制字符。例如，\cM 匹配一个 Control-M 或回车符。x 的值必须为 A-Z 或 a-z 之一。否则，将 c 视为一个原义的「c」字符。
\d	匹配一个数字字符。等价于[0-9]。
\D	匹配一个非数字字符。等价于[^0-9]。
\f	匹配一个换页符。等价于\x0c 和\cL。
\n	匹配一个换行符。等价于\x0a 和\cJ。
\r	匹配一个回车符。等价于\x0d 和\cM。
\s	匹配任何空白字符，包括空格、制表符、换页符等等。等价于[\f\n\r\t\v]。
\S	匹配任何非空白字符。等价于[^\f\n\r\t\v]。

\t	匹配一个制表符。等价于\x09 和\cI。
\v	匹配一个垂直制表符。等价于\x0b 和\cK。
\w	匹配包括下划线的任何单词字符。等价于「[A-Za-z0-9_]」。
\W	匹配任何非单词字符。等价于「[^A-Za-z0-9_]」。
\xn	匹配 n，其中 n 为十六进制转义值。十六进制转义值必须为确定的两个数字长。例如，「\x41」匹配「A」。「\x041」则等价于「\x04&1」。正则表达式中可以使用 ASCII 编码。.
\num	匹配 num，其中 num 是一个正整数。对所获取的匹配的引用。例如，「(.)\1」匹配两个连续 的相同字符。
\n	标识一个八进制转义值或一个向后引用。如果\n 之前至少 n 个获取的子表达式，则 n 为向后 引用。否则，如果 n 为八进制数字（0-7），则 n 为一个八进制转义值。
\nm	标识一个八进制转义值或一个向后引用。如果\nm 之前至少有 nm 个获得子表达式，则 nm 为 向后引用。如果\nm 之前至少有 n 个获取，则 n 为一个后跟文字 m 的向后引用。如果前面的 条件都不满足，若 n 和 m 均为八进制数字（0-7），则\nm 将匹配八进制转义值 nm。
\nml	如果 n 为八进制数字（0-3），且 m 和 l 均为八进制数字（0-7），则匹配八进制转义值 nml。
\un	匹配 n，其中 n 是一个用四个十六进制数字表示的 Unicode 字符。例如，\u00A9 匹配版权符 号（©）。

B.5. 常用的正则表达式范例

1) 用户名

```
/^[a-z0-9_-]{3,16}$/
```

2) 密码

```
/^[a-z0-9_-]{6,18}$/
```

3) 十六进制值

```
/^#?([a-f0-9]{6}|[a-f0-9]{3})$/
```

4) 电子邮箱

```
/^([a-z0-9_\-\.]+)@([a-z\.-]+)\.([a-z\.-]{2,6})$/
```

5) URL

```
/^(https?:\/\/)?([a-z\.-]+)\.([a-z\.-]{2,6})([a-z\.-]*)*\/?$/
```

6) IP 地址

```
/^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$/
```

7) HTML 标签

```
/^<([a-z]+)([^\<]+)*(?:>|<\/1>|<\/s+\/>)$/
```

8) Unicode 编码中的汉字范围

```
/^[u4e00-u9fa5],{0,}$/
```

9) SQL 注入

```
^w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/i
```

10) XSS 攻击

```
/((\%3C)|<)/i
```



注意：

依迅 Web 应用防护系统在用户自定义规则功能里已经对 PCRE 的大小写选项等进行了预处理，因此如果您需要添加自定义的 PCRE 规则，只需添加两个 “/” 之间的内容即可。例如：您要添加一个通用的防 XSS 规则，在【自定义规则-添加】对话框里，“特征关键字” 文本框里填上：`((\%3C)|<)`，然后点击【插入特征】即可。

参考资料：

1. 正则表达式:

<http://zh.wikipedia.org/wiki/%E6%AD%A3%E5%88%99%E8%A1%A8%E8%BE%BE%E5%BC%8F>

2. 正则表达式 30 分钟入门教程:

<http://deerchao.net/tutorials/regex/regex.htm>

铱迅信息(YXLink)

未获得南京铱迅信息技术股份有限公司的书面许可，不可擅自以任何形式复制此说明书的全部或部分内容（评价或介绍文章的简单引用除外）。

南京铱迅信息技术股份有限公司

江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

Nanjing YXLink Information Technology Co., Ltd.