解决方案实践

中云网安 AI 防护者解决方案

文档版本	1.0
发布日期	2023-08-04

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 方案概述

应用场景

- 政府、金融、能源等行业门户网站及应用安全、合规要求
- HW行动-现有安全防护的补充
- 安全威胁检测与防御

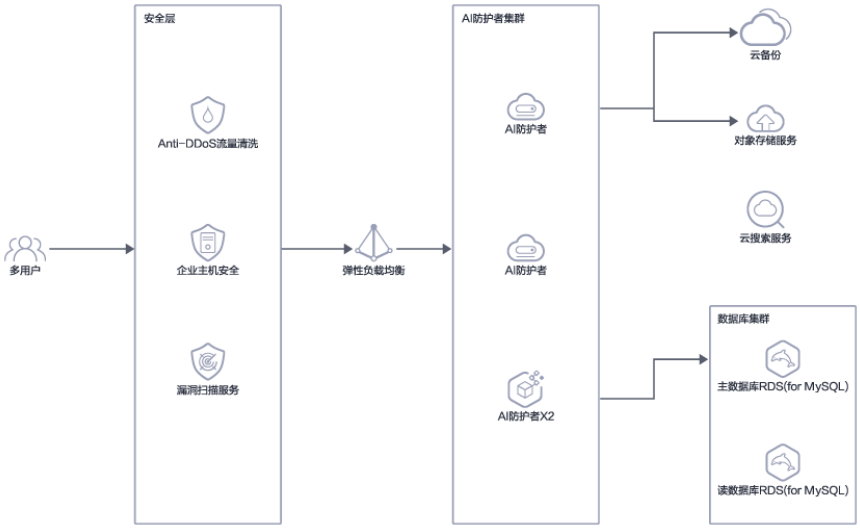
业务痛点与挑战

- 没有有效的防0-day手段，高风险的攻击大部分都是基于0-day漏洞实现。
- 安全产品多，安全运维要频繁升级特征库，对安全运维人员要求比较高，并且存在供应链攻击的风险
- 缺乏安全事件实时响应能力，系统防御能力脆弱
- 应用运维周期已过，存在未修复的漏洞
- 应用系统的复杂性，导致安全更新滞后
- 随着远程办公的发展，应用系统攻击面也随之扩大，业务持续性风险增加

方案架构

图 1-1 中云网安 AI 防护者方案架构

图 1-2 中云网安 AI 防护者部署架构



方案架构说明：

- 基线设施即服务包括：弹性云服务ECS、对象存储服务OBS、弹性负载均衡ELB以及内容分发网络CDN等。
- 技术即服务包括：云数据库 RDS for MySQL、云搜索服务CSS（集群版需要）、云容器实例CCI（集群版需要）
- 算法即服务包括：协议解析引擎、行为识别引擎、数据矩阵引擎、威胁分类引擎和多级决策引擎
- 经验能力服务包括：0-Day实时防护、AI低运维、AI威胁发现、AI规范检测、AI业务分析、实时防篡、APT联动等

中云网安的AI算法引擎不依赖于规则、签名、固定基线或训练数据。它从不断变化的数字环境中形成对每个请求和响应、URI、表单等复杂关系的多维理解，拦截非正常业务流量，并进行威胁分类和校验，生成安全告警日志。

该引擎支持Web、API、H5、APP、小程序，中云网安的AI赋能解决方案结合大数据技术和人工智能算法，实时分析业务和攻击数据，以客户网络资产为根本，智能提取安全事件，并与多种安全产品联动，为客户提供未知攻击的主动识别和防御能力。

方案优势

1. **更安全：**利用AI算法实现对已知和0-day漏洞的精准有效阻断，提升防护水平至99.99%。无需担心供应链攻击威胁，实现真实网络攻防对抗，提升网络安全对抗水平。
2. **更省钱：**运维成本降低80%以上，部署简单，无需手动更新规则库，算法减轻运维压力，无需专职运维和攻防知识，降低人员成本，覆盖多种运维场景，实现高效运营模式。
3. **主动防御：**中云网安的AI赋能解决方案专为应用安全防护设计，提供实时监测、态势感知、非嵌入式动态加固的能力，提升整体网络安全防护能力。
4. **智能学习算法：**集成自研的安全算法模型和应用学习技术，实现私有化学习，识别未知威胁和0-day攻击，实现主动防御，无感知的进化式更新，提供强大的安全防护能力。

2 资源和成本规划

中云网安AI防护者应用安全防护：

表 2-1 独立部署版资源和成本规划

云资源	规格	数量	每年费用（元）
VPC	默认配置	1	00.00
Subnet	默认配置	1	00.00
安全组	根据需要开通入方向80/443/8000等端口	1	00.00
ECS	c7.xlarge.2|8vCPUs|16GB 镜像：CentOS 7.6 64Bit With X86 存储：40GB	2	27300.00
RDS	RDS for MYSQL x86通用型 | 8 vCPUs | 16 GB | 版本8.0 | 主备	1	20640.00
OBS	标准存储多AZ存储包 | 1TB	1	1161.00
ELB	应用型(HTTP/HTTPS) 小型II | 网络型(TCP/UDP) 小型I | 带宽 10M	1	17150.00
总计：62001.00			

表 2-2 集群部署版资源和成本规划

云资源	规格	数量	每年费用（元）
VPC	默认配置	1	00.00
Subnet	默认配置	1	00.00
安全组	根据需要开通入方向80/443/8000等端口	1	00.00

云资源	规格	数量	每年费用（元）
ECS	c7.xlarge.2|8vCPUs|16GB 镜像：CentOS 7.6 64Bit With X86 存储：40GB	3	40950.00
RDS	RDS for MYSQL x86通用型 | 8 vCPUs | 16 GB | 版本8.0 | 主备	1	20640.00
OBS	标准存储多AZ存储包 | 5TB	1	20611.40
ELB	应用型(HTTP/HTTPS) 小型II | 网络型(TCP/UDP) 小型I | 带宽 10M	1	17150.00
CSS	ess.spec-8u16g | 8 vCPUs | 16GB | 2T存储 | 高I/O | 5M带宽	1	20611.40
CCI	基础版资源套餐包	1	3000
总计：110455.40			

说明

本文提供的成本预估费用仅供参考，资源的实际费用以华为云管理控制台显示为准。

3 实施步骤

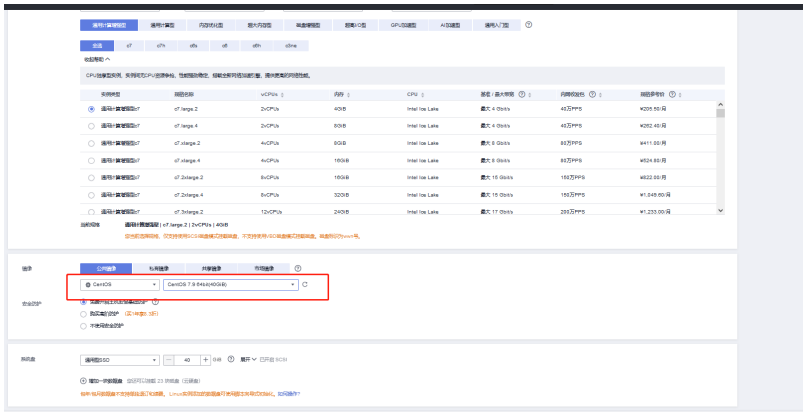
3.1 部署 AI 防护者

3.1.1 AI 防护者安装

步骤1 登录华为云管理控制台

步骤2 创建弹性云服务器（ECS），选择镜像版本为centos7，数量为3

图 3-1 AI 防护者安装 1



步骤3 登录ECS，上传AI防护者安装包

```
[root@ecs-336a ~]# ls
zyWAF-develop-9.0.3-942.centos7.x86_64.rpm
zyWAF-GM-stable-develop-9.1.0-9.1.0-810.centos7.x86_64.rpm
```

步骤4 安装AI防护者计算节点

进入安装包所在目录rpm -ivh / “安装包名称”

```
[root@ecs-336a ~]# rpm -ivh ./zyWAF-develop-9.0.3-942.centos7.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
1:zyWAF-9.0.3-942.centos7         ################################# [100%]
---------- Creating the MariaDB system databases and tables
---------- Starting the server..Done
---------- Creating/updating users
---------- Stopping the server.Done
---------- Starting the server..Done
---------- Creating zyWAF databases
---------- Stopping the server.Done
***** Starting upgrade at Fri Jul 28 10:31:31 2023
----- Info: Skipping bin/cvt-settings -f "/usr/local/waf/etc/my.cnf"
----- Info: Skipping conversion of logs/alerts.db
----- Info: Skipping conversion of logs/audit.db
***** Finishing upgrade at Fri Jul 28 10:31:31 2023
```

步骤5 安装AI防护者管理节点

进入安装包所在目录rpm -ivh / “安装包名称”

```
[root@ecs-336a ~]# rpm -ivh zyWAF-GM-stable-develop-9.1.0-9.1.0-810.centos7.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
1:zyWAF-GM-9.1.0-810.centos7      ################################# [100%]
---------- Creating the MariaDB system databases and tables
---------- Starting the server..Done
---------- Creating/updating users
---------- Stopping the server.Done
---------- Starting the server..Done
---------- Stopping the server.Done
```

步骤6 启动管理节点、计算节点

```
[root@ecs-336a ~]# systemctl start zywaf
[root@ecs-336a ~]# systemctl start zygm
[root@ecs-336a ~]# systemctl status zygm
● zygm.service - zyProtect Web Application Firewall Global Manager
Loaded: loaded (/usr/lib/systemd/system/zygm.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2023-07-28 10:36:20 CST; 1min 49s ago
Docs: https://www.zyprotect.com/zywaf-en/
Process: 29465 ExecStartPost=/usr/bin/sleep 0.2 (code=exited, status=0/SUCCESS)
Process: 29463 ExecStart=/usr/local/waf-gm/bin/zygm $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 29464 (zygm)
Tasks: 1
Memory: 74.1M
CGroup: /system.slice/zygm.service
└─29464 /usr/local/waf-gm/bin/zygm
Jul 28 10:36:19 ecs-336a systemd[1]: Starting zyProtect Web Application Firewall Global Manager...
Jul 28 10:36:20 ecs-336a systemd[1]: Started zyProtect Web Application Firewall Global Manager.
[root@ecs-336a ~]# systemctl status zywaf
● zywaf.service - zyProtect Web Application Firewall
Loaded: loaded (/usr/lib/systemd/system/zywaf.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2023-07-28 10:31:31 CST; 6min ago
Docs: https://www.zyprotect.com/zywaf-en/
Main PID: 28101 (wafmanager)
Tasks: 16
Memory: 94.5M
CGroup: /system.slice/zywaf.service
├─28101 /usr/local/waf/bin/wafmanager
└─28118 /usr/local/waf/bin/waf --no-daemon --no-rastate --no-crawl -path /usr/local/waf
```

```
Jul 28 10:31:31 ecs-336a systemd[1]: Starting zyProtect Web Application Firewall...
Jul 28 10:31:31 ecs-336a systemd[1]: Started zyProtect Web Application Firewall.
```

----结束

3.1.2 AI 防护者激活

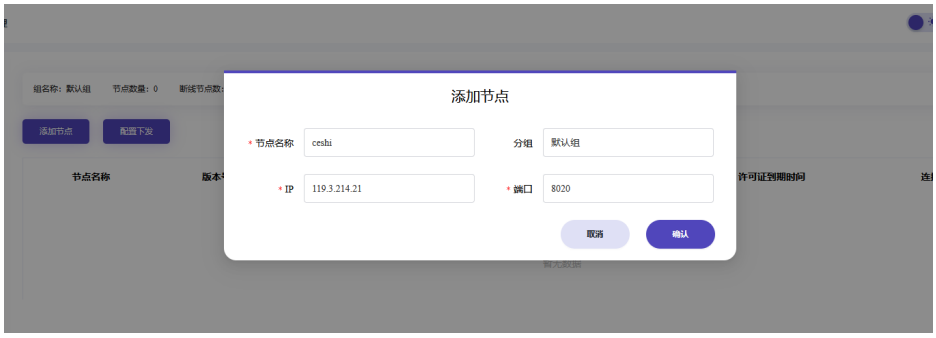
步骤1 通过浏览器访问管理节点，URL地址为“https://<管理节点IP>：8000”

步骤2 登录管理平台，首次登录需修改密码，默认账户密码admin/Admin123

步骤3 管理平台添加管理节点，集群管理>添加节点>节点信息>确定

节点信息：名称可自定义，IP为计算节点IP地址，端口8020

图 3-2 AI 防护者激活 1



步骤4 添加许可证，输入密钥点击确认

图 3-3 AI 防护者激活 2

步骤5 许可证激活，选择节点点击确定，通过页面可查看许可证状态

图 3-4 AI 防护者激活 3

----结束

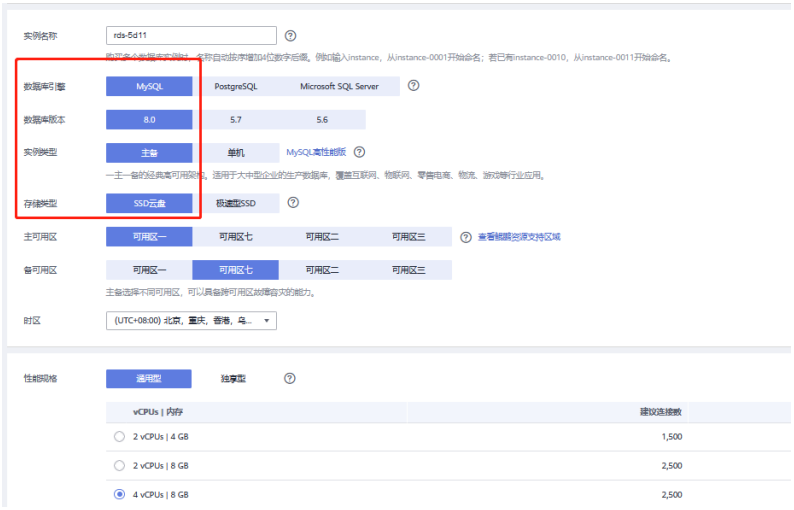
3.2 RDS、CSS 部署

3.2.1 RDS 部署

步骤1 登录控制台

步骤2 创建RDS for mysql，版本选择8.0，存储类型选择SSD

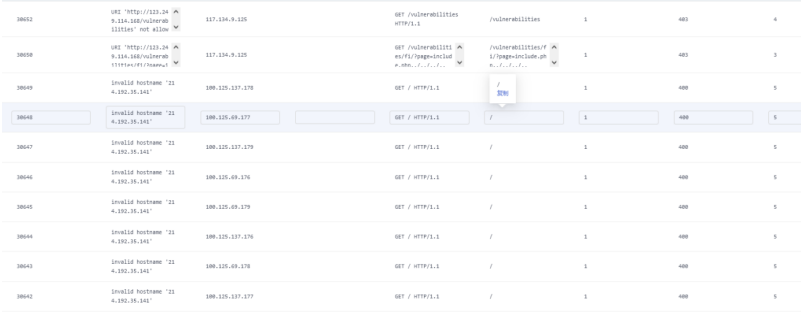
图 3-5 RDS 部署 1



步骤3 配置数据库连接，查看数据是否成功入库

图 3-6 RDS 部署 2

图 3-7 RDS 部署 3



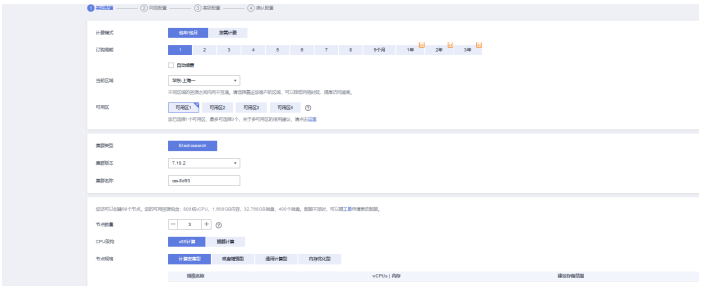
----结束

3.2.2 CSS 部署

步骤1 登录控制台

步骤2 创建CSS

图 3-8 CSS 部署 1



步骤3 CSS集群配置，查看数据是否正常

图 3-9 CSS 部署 2

----结束

3.3 添加站点

3.3.1 添加保护站点

步骤1 登录AI防护者管理页面，URL地址为“https://<管理节点IP>：8000”

步骤2 添加保护站点，安全防护设置>保护站点设置>添加服务器>输入配置信息>应用

图 3-10 添加保护站点 1

----结束

3.3.2 配置 ELB

步骤1 登录控制台

步骤2 创建ELB

步骤3 ELB配置，创建后端服务器组

图 3-11 配置 ELB1

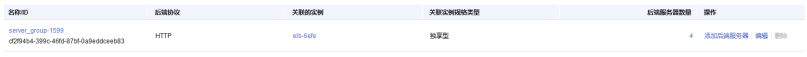
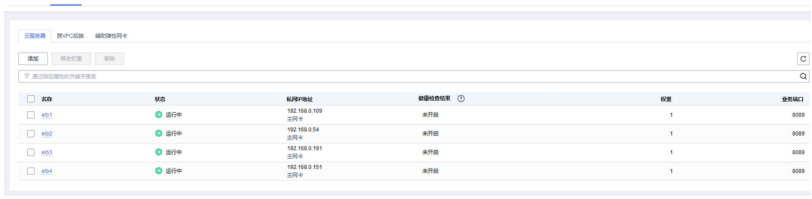


图 3-12 配置 ELB1



----结束

3.4 AI 防护者初始化

3.4.1 AI 防护者初始化

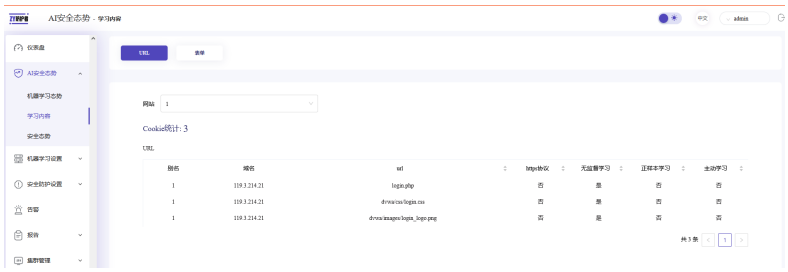
步骤1 登录AI防护者管理页面，URL地址为“https://<管理节点IP>：8000”

步骤2 启用主动学习，机器学习设置>主动学习>选择网站>应用

图 3-13 AI 防护者初始化 1

步骤3 查看学习内容

图 3-14 AI 防护者初始化 2



----结束

3.5 测试 AI 防护链路

3.5.1 测试 AI 防护者链路

步骤1 访问保护站点，查看是否访问成功

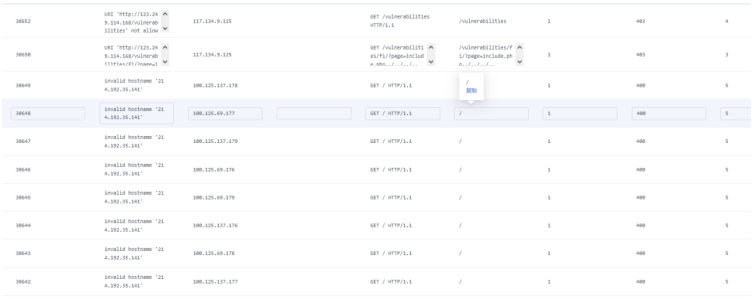
图 3-15 测试 AI 防护者链路 1

步骤2 登录AI防护者节点，查看仪表盘请求数量

图 3-16 测试 AI 防护者链路 2

步骤3 登录RDS，查看是否数量是否正常入库

图 3-17 测试 AI 防护者链路 3



----结束

3.6 删除 ECS、RDS、CSS、ELB

3.6.1 删除 ECS、RDS、CSS、ELB

步骤1 登录控制台

步骤2 进入ELB控制台，删除ELB

图 3-18 删除 ELB

步骤3 进入CSS控制台，删除CSS

图 3-19 删除 CSS

步骤4 进入RDS控制台，删除RDS

图 3-20 删除 CSS

步骤5 进入ECS控制台，删除ECS

图 3-21 删除 CSS

----结束

4 修订记录

表 4-1 修订记录

发布日期	修订记录
2023-08-08	第一次正式发布。