

# 惠尔顿网络安全审计系统W300NM

产品名称	惠尔顿网络安全审计系统W300NM
公司名称	北京利源嘉志科技有限责任公司
价格	.00/个
规格参数	品牌:惠尔顿 型号:W300NMW480NM 产地:深圳
公司地址	北京市海淀区阜成路14号
联系电话	15110266611

## 产品详情

惠尔顿网络安全审计系统产品简介：

将惠尔顿的网络安全审计系统部署在互联网的出口，用户连接到WIFI后，无需寻找工作人员索取密码，只需关注指定的微信公众账号，即可正常上网。在节省客服人员工作量的同时，也能快速收集粉丝用户，方便后续的微信营销活动。

惠尔顿的网络安全审计系统产品可以分析用户上网行为，商家根据上网行为特征进行适当的营销活动。比如“域名TOP10排名”，“搜索引擎TOP10排名”等，通过对此类信息的分析，商家能作出更有针对性的营销决策。

惠尔顿的网络安全审计系统优化了数据库的存储，系统采用了优化的数据存储结构，将设备产生的海量监控数据通过不同的时间粒度进行分级存储，在确保了数据精度的同时，也带来了高速的数据查询汇总。分级存储的机制可以用漏桶来做形象的比喻，每个漏桶代表了一种时间粒度的数据，当一个桶里装的数据量满了之后，溢出的数据会以合并（Merge）的方式流到下一个时间粒度的桶中，这样可以保证每个桶里的数据量都是有大小限制，从而确保在每个桶里都可以进行快速的数据检索。

分类

主要规格

W600NM

W800NM

W1000NM

W1200NM

W1500NM

W2000NM

W3000NM

性能

参数

适用对象

小规模

中小型

中型企业

中型企业

中大型

大型企业

集团用户

端口RJ45

4\*1G

4\*1G

6\*1G

4\*1G

6\*1G

6\*1G

扩展光口

--

--

--

2\*SFP

4\*SFP

4\*SFP

存储容量

500G

500G

1T

1T

1T

2T

2T

建议用户数

<100

<200

<500

<1000

<1500

<2500

<5000

转发时延

<0.1ms

<0.1ms

<0.1ms

<0.1ms

建议VPN数

80

150

300

400

800

1200

2000

外观尺寸

1U

1U

1U/2U

2U

2U

设备

状态

监控

硬件环境

支持设备的CPU、内存、硬盘等硬件使用率的实时监控

网络监控

网卡的流量、吞吐量、丢包等网络状态的实时监控

系统监控

设备型号、ID、版本信息、运行时间的实时监控

网络

管理

网关模式

网关模式支持NAT、路由转发、DHCP等功能；

智能路由

网关模式时能同时连接多条外网线路，且支持多线路复用和智能选路技术

## 网桥模式

支持网桥模式，以透明方式串接在网络中；并且必须支持多路桥接功能，至少支持二进二出两网桥模式；

## 旁路模式

支持旁路模式，无需更改网络配置，实现上网行为审计；

## 路由

静态路由、策略路由

## HA高可用性

支持两台设备同时做主机的部署模式，同时支持两台设备做主备的部署模式；

## SNMP

支持标准SNMP V1、SNMP V2、SNMP V3

## ByPass

所有设备支持硬件ByPass与软件ByPass（软件故障直通不影响用户使用）

## 网络服务

DNS、DHCP Server、DHCP client、NTP

## 管理方式

安全HTTPS、HTTP、SSH、RS-232

## 用户认证

### 上线用户

直观展示、直观策略（强制下线、添加黑名单、流空策略等）

### 本地用户

支持用户的批量导入、LDAP/AD导入、内网主机自动扫描

### 用户认证

网页认证，客户端认证，Key认证

### 用户组织

根据企业的组织结构设置用户树

用户身份

绑定IP、绑定MAC、绑定Key双因素等

认证策略

支持排他性登陆策略、后登陆优先策略、并发登陆策略等

第三方认证

支持第三方的RADIUS、LADP/MS AD、POP3认证服务器

流量

对象设置

支持基于IP/用户、应用、时间段的控制

带宽保证

保障低带宽，预留固定带宽

带宽限制

限制大带宽

带宽QoS

带宽0~7共8个优先级控制

应用封堵

指定应用的封堵

免监控Key

拥有Key的用户免监控

QQ、MSN

免监控QQ、MSN、飞信、邮件帐号等网络应用白名单

邮件帐号

支持邮件收发帐号的白名单，免监控

黑名单

对实时上下行、日上下行、日总流量超过阈值的用户进行强制下线

## 网络身份

能识别网络用户使用常见网络应用（邮件地址、QQ帐号、MSN帐号、网络帐号）时的身份

## 上网报警

发送违规关键字词告警

## 邮件报警

发送违规邮件内容告警

## IM报警

发送违规使用IM告警

## HTTP识别

上网浏览、HTTP分块传输、HTTP下载、WEB音乐、WEB视频

## 行为

## 审计

### 网站审计

支持记录全部或者指定的URL的网页标题等信息；

### 网页审计

支持审计记录网页标题、网页类型、正文内容等；

### 发帖审计

支持审计用户的明文发帖内容；

### 网络搜索审计

支持常见的搜索引擎搜索习惯的审计

### Webmail审计

支持审计用户的常见的Webmail邮件外发行为，支持webmail形式发送的附件审计，并能还原成原始邮件；

### 邮件审计

支持审计用户外发Email邮件的正文及附件；

### 文件审计

支持审计用户通过HTTP、FTP、TFTP、TELNET、Email等方式外发的文件内容；

## IM审计

支持记录QQ、MSNShell、Skype、Gtalk等加密聊天内容；支持记录MSN、飞信、雅虎通等明文聊天内容；

## 应用审计

审计P2P、流媒体、炒股、网络游戏、FTP、Telnet等应用行为；

## 流量审计

记录用户在指定时间段内产生的总流量；记录用户在指定时间段内使用指定应用的总流量；

## 危险行为审计

必须能审计木马、病毒、恶意脚本和插件、端口扫描等危险行为；

## IP协议审计

支持记录其他网络行为，包括IP、端口等信息；

## 内容过滤

### URL过滤

支持内嵌url库千万级URL库，并智能分类，如：体育、教育、钓鱼网站等等

### URL库

### 定期升级

### URL自定义

自定义域名与URL的过滤或者放行

### 关键字过滤

支持网页中的关键字词

### 网页过滤

支持根据访问的URL分类进行过滤

### 发帖管理

过滤匹配关键字的网络发帖行为；支持允许用户浏览帖子但不准发帖功能；

### 外发文件告警



支持根据外发文件类型、关键字等条件的过滤告警，支持对HTTP、FTP、Email附件方式外发文件的识别、报警、过滤等管理措施；

#### 扩展名识别

支持基于外发文件的扩展名识别外发文件类型；

#### 搜索引擎过滤

支持多搜索引擎关键字词的过滤

#### 地址过滤

支持根据发件人地址过滤外发邮件；

#### 附件过滤

支持基于扩展名过滤含指定文件类型的邮件外发行为；

#### 邮件关键字过滤

过滤匹配关键字的邮件外发行为；

#### Webmail过滤

支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能；

#### 防火墙

##### 状态检测

支持线速的状态监测防火墙，支持NAT与PAT

##### 常见攻击

能封堵DOS攻击、SYN攻击、udp攻击、Tear Drop、Ping of Death、IP Spoofing 等攻击；

##### IP连接数

支持TCP、UDP、IP的并发连接数控制

##### 端口映射

VIP（端口映射），支持外网到内网的一对多负责均衡映射

##### IP映射

MIP(IP映射)，支持外网的IP池，IP映射

##### 防ARP欺骗

能防范ARP病毒欺骗、支持IP/MAC；

伪IP防护

支持内网伪IP的防护

VLAN

支持标准的802.1Q VLAN

DHCP服务

内置DHCP服务器、DHCP客户端

外发管理

邮件外发

支持邮件收件人、发件人、主题、内容的外发管理

Web外发

支持Web上传文件名、文件类型，文件大小的外发管理

QQ外发

QQ聊天外发内容管理，文件关键词、文件类型外发管理

论坛上传

论坛外发内容管理，上传文件关键词、文件类型管理

客户端准入

防火墙检查

支持客户端防火墙的安全检测

防病毒检查

支持客户端防病毒的安全检测

操作系统漏洞扫描

支持客户端操作系统的漏洞扫描

WINDOWS登录

绑定用户登录计算机，拔出Key自动锁屏

VPN专线效果

客户端连接到应用服务器后自动断开与internet的连接

禁止外设

支持禁止USB、光驱、软驱、红外、无线网络、CF卡等

进程黑白名单

支持设置进程黑白名单

网卡规则

无线网卡、网卡多IP、网卡绕过本地外联等规则准入

智能截屏

支持监控客户端的屏幕，并支持客户端截屏，支持玩游戏、违规范围时智能截屏

智能

追溯

系统

智能追溯

追溯防火墙策略丢包导致的网络不能访问的原因，追溯流量管理策略限速导致网络访问慢的原因，智能追溯防火墙攻击，系统性能，网络性能，应用性能。

日志中心

设置日志、定制日志、第三方日志

syslog

支持日志的SYSLOG转储

邮件告警

可配置将告警日志定期发送给指定邮箱，自动化、智能地定期发送。

操作日志

支持管理员的操作日志、审计员的审计等

系统日志

支持系统核心的系统日志、流量管理系统日志、上网行为记录日志

VPN访问日志

支持通过VPN访问内网的访问日志

告警日志

支持系统自定义的多种告警日志

统计报表

实时应用统计

实时统计正在使用中的应用，包括连接数排名、速度排名；每种子应用正在使用的用户；访问的目的地排名；访问的目标IP以及地址定位；

实时用户统计

实时统计在线的用户，包括连接数排名、速度排名；每个用户正在使用的应用；访问的目的地排名；访问的目标IP以及地址定位；

实时连接数统计

实时统计正在连接的连接

丢包统计

显示用户在流控策略下的效果

历史应用报表

任何时间（段）、用户15大类应用的使用流量报告

2000+应用流量统计报告；800+智能手机APP应用流量统计报告；每种应用的用户使用状况；

历史用户报告

任何时间任何用户使用的任何应用、流量报告、排名比较

用户使用习惯

常见网站使用排名；邮件发送排名、论坛发帖排名；

数据中心

支持数据中心以及数据的第三方转储