ASG 概述

多功能安全设备 ASG500 / 5000

UTM发展

网络安全威胁的发展推动着安全产品的发展，产生了在一台单一设备中集成多种威胁防御系统的产品。Array统一威胁管理系统包括防火墙、VPN、入侵保护、防病毒、防恶意软件、防垃圾邮件、Web内容过滤等安全功能，可在一台单一设备中识别多种安全威胁。虽然UTM产品的大量使用使安全问题变得可以轻松应对，但因为中低端设备有限的吞吐量和低的接口密度，管理员部署设备时会受到很大的局限。

网络边界扩展

随着技术的发展，网络设备和用户的使用习惯也在不断发展，传统的安全保护措施已经不足以应对网络边界的不断扩展。笔记本电脑、支持WiFi功能的手机在提供灵活性的同时，也对访问层的安全提出更高要求。理想的网络安全解决方案应该提供线速的吞吐量和高密度的接口，以实现把局域网分区隔离为单独的安全区域；提供细粒度的安全策略和安全事件隔离，以提高网络流量和事件的可视性。

ASIC 加速多威胁安全解决方案

Array ASG500为不断成长的中小型网络提供完善的安全解决方案。通过集成的特制ASIC处理器，即ASIC网络处理器，实现在交换机速率下传输安全的流量；16个硬件加速接口(可扩展到20个)可在交换机性能下，实现在网络分区间制定防火墙策略。另一个特制的ASIC处理器，即ASIC内容处理器，可为入侵保护、病毒扫描等内容增强安全技术提供加速。AMC扩展插槽提供了更多的灵活性：可以增加ASIC加速接口、提高吞吐量或增加硬盘存储功能实现本地日志及内容归档。通过多个加速多威胁安全接口，企业可为不同部门、用户、访问方式、甚至设备创建多个安全区域，在不影响速度的前提下实现网络安全。

Array ASG5000是适用于大型企业的高性能、部署灵活的综合安全网关。Array ASG5000的成功来自于专用的ASIC芯片，高端口密度和融合了多种多种安全功能的Array OS,该设备具有万兆接口和高达40Gbps的吞吐量，完全可以满足各种环境的要求，比如虚拟系统，运计算或传统IT架构的需求。由于采用最新ASIC技术，Array ASG5000的防火墙性能可以达到40Gbps线速处理，VPN性能可以达到16Gbps。除此之外，Array ASG5000还推高了防病毒、IPS等UTM的性能。有了Array ASG5000，不用担心安全设备成为网络的瓶颈。

ArrayNetworks ASG500/5000系列

多功能安全设备

Array ASG产品系列：集成多种安全功能

Array ASG系列产品可以实现从网络层到应用层的安全防护。在不影响网络的可用性和应用的速度前提下，抵御多种复杂的攻击。Array ASG系统将ArrayOS与定制开发的ASIC芯片集成在一起，为用户提供全面的高性能的安全功能和网络功能。Array ASG可以为用户保护其网络和资产的安全，关键业务信息，实现信息安全管理。

ASIC的优势

ASIC处理器使ASG更为强大，因为专用的网络处理器和内容层处理器能够加速数据的处理，它们采用了Array独有的数字引擎。

统一安全功能特点

- 防火墙 (透明 / 路由 / NAT)
- IPSEC VPN (基于策略或者接口)
- SSL VPN (支持web和通道方式)
- 防病毒 (代理机制 / 流扫描)
- 防攻击IPS (自动隔离机制)
- 网页过滤 (动态名誉库技术)
- 垃圾邮件防御 (双向防御机制)
- DLP数据泄漏保护 (正则表达式支持)
- WAN优化传输 (缓存和压缩技术)
- 上网行为管理 (支持旁路侦听)
- 完全虚拟化支持 (会话等资源分配)
- 统一安全日志存储 (Analyzer支持)
- 统一安全管理部署 (Central Manager支持)

优势特征

功能	ASG 500	ASG 5000
硬件加速	最高20Gbps防火墙吞吐量、15Gbps VPN吞吐量，结合1Gbps IPS性能和250Mbps防病毒性能，确保不会出现性能瓶颈	支持高达40Gbps防火墙吞吐量和16GbpsVPN吞吐量，1.2G的应用层代理机制的安全检测能力
高密度接口	20 个10/100/1000M接口(可扩展至24 个)，实现网络中多个内部分区	8 个万兆接口和12个千兆接口
模块扩展，提高网络性能	可灵活的扩展四个NP加速接口或一块本地日志归档硬盘	支持WAN优化和Web Cache功能
统一安全架构	单一设备中的多种威胁保护提高了安全性，降低了部署成本	单一设备实现多种功能，提高了安全而降低了整体成本

UTM 构建安全的VPN 体系

Array ASG具有强大的防火墙和VPN功能。很多大中型企业都有分公司、办事处和移动办公用户。Array ASG的IPSec VPN功能为这类企业提供了全面的、安全的互联解决方案。IPSEC VPN支持接口和通道两种类型，主和被动两种模式。它可以实现VPN通道星形或者网状结构，并且在VPN通道上部署防火墙策略、防病毒和IPS等全面的安全解决方案。OSPF over IPSEC可以实现IPSEC通道与专线，两条IPSEC通道之间互为备份，自动切换。移动用户可以使用IPSEC客户端方式连入公司，实现家庭和远程办公，也可以采用SSL VPN这样的基于浏览器的免客户端方式连接到公司的内网。Array ASG对于企业而言，提供作为防火墙、防病毒网关、Web过滤、入侵检测和防御等功能。

虚拟域为安全服务提供商提供解决方案

虚拟域可以将Array ASG划分出若干逻辑的虚拟设备，每个虚拟设备可以单独设置路由、防火墙策略、内容层的防病毒、IPS等功能。安全服务商可以为多个企业组织部署一个Array ASG，将其划分成若干逻辑设备分配给不同的企业组织，并且为其设置相应逻辑设备的管理权限，这样每个被服务的企业可以单独地管理安全设置，查看相应的日志信息。所有Array ASG解决方案都是相同的灵活高性能架构，每个型号都有核心网络功能（比如HA）和动态路由支持，使Array ASG能够安装在分布式的和全网状网络环境。

数据中心和关键应用的高性能解决方案

在数据中心这样吞吐量大并且对实时性要求很高的环境中，新一代基于应用的攻击目标web2.0、VoIP甚至IPTV等应用，需要全面的安全战略，包括多层网络防御。

幸得是许多新型应用是需要实时的，迫使管理员在性能和安全性之间做出选择。Array ASG系列多个千兆性能解决方案提供实时的多层安全威胁防御，这些威胁主要目标是应用服务器。另外还提供新攻击类型的防御，先进的反垃圾邮件功能过滤间谍软件和安全策略不允许访问的内容。

ASG 安全功能

防火墙

ICSA认证(状态监测防火墙)
NAT / 路由, 透明模式 , 混合模式
虚拟防火墙支持(虚拟域)
标准预定义服务
(SIP,GRE,Netmeeting,h.323,OSPF等)
自定义服务 / 服务组 / 地址 / 地址组
DHCP服务器，DHCP中继
DNS转发
IP / MAC地址绑定
基于策略的NAT
VLAN标记(802.1Q)
IPV6策略和路由支持
非IP协议透明传输
ALG应用代理(SIP，H.323, TNS,
RSTP，RAS 等NAT 穿越)
服务器负载分担和健康检查
策略时间表支持
单机的会话同步支持
基于用户组的认证
细粒度的每策略保护内容表

虚拟专用网(VPN)

ICSA认证(IPSec)
PPTP, IPSec, L2TP, GRE
支持DES, 3DES, AES 256加密算法，
SHA-1 / MD5认证
SCEP简单证书登记协议
OCSP在线证书状态协议
Hub and Spoke星型VPN
DPD通道状态检测
NAT穿越，XAUTH认证
静态VPN，动态拨号VPN支持
支持子网重叠，VPN通道保持
基于策略和路由的VPN
OSPF over IPSec

反病毒

ICSA认证(网关反病毒)
包括反间谍软件和蠕虫阻断
HTTP / SMTP / POP3 / IMAP FTP / IM协议
SMTPS / IMAPS / HTTPS/POPS协议
(CP6以上硬件版本)
网络自动“推送”升级

ASG 安全功能

根据文件尺寸和类型阻断
可定义的服务端口，服务超时控制
支持病毒阻拦和监视模式
多层压缩文件扫描
支持Tar /gzip/ rar/ lzh/ cab/ arj /zip /bzip /bzip2/ msc /UPX
支持文件大小限制文件类型限制
病毒隔离支持(需要本地硬盘或Analyzer日志服务器)
支持NAC，可以隔离病毒发送者和病毒来源接

WEB过滤

82种Web过滤类别，超过20亿个Web页面
自定义URL地址，域名过滤
基本于分值的网页关键词阻断规则
自定义分类库，基于用户认证的分类库控制
URL地址 / 域名黑白名单
阻断Java Applet, Cookies, Active X

反垃圾邮件

支持SMTP / POP3 / IMAP协议
支持SMTPS / POPS / IMAPS协议(CP6硬件版本)RBL / ORDBL
Guard垃圾邮件库动态更新
MIME头检查、关键字 / 短句过滤
IP地址和Email黑名单 / 免屏蔽
返回地址DNS检查
支持邮件阻断或者标记
支持用户自定义反垃圾邮件阈值

应用控制

超过1000种应用程序，分成以下类别：
备份软件类，如IBM Tivoli, CA MQ等
商务软件，如指南针，证券之星，分析家
数据库，如DB2, MySQL, Oracle等
文件传输类，如DuDu，纳米盘等
游戏，如赤壁、劲舞团、联众、魔兽等
即时通讯，如MSN、QQ、新浪UC、飞信等
媒体类，如土豆、酷6、PPS 网络电视等
网络服务，如BGP、ISCSI、QUAKE等
P2P，如电驴、迅雷、VeryCD
协议命令类，如ftp 命令，sip命令
代理软件，如无界、Tor等
远程控制软件，如VNC、Pcanywhere等
工具条，如Google、yahoo、MSN工具条等
升级程序，如各种杀毒软件升级，firefox 升级
VoIP，如Sip，netmeeting, net2phone等
网站与论坛，如网易论坛、QQ论坛等
Web Mail，如126mail、hotmail、QQmail等
可以对以上应用进行日志和阻断

数据泄露防护(DLP)

HTTP / SMTP / POP3 / FTP / NNTP / IM协议支持
SMTPS / IMAPS / HTTPS / POPS协议(CP6以上硬件版本)
支持对压缩文件的扫描和存档(Tar /gzip/ rar/ lzh/ cab/ arj /zip /bzip /bzip2/ msc /UPX)
支持TXT、PDF和Word类型文档
以动机确认和控制敏感信息
内建模式匹配库
正则表达式匹配引擎　　SMTP / POP3 / IMAP可检测邮件头、主题、内容、附件和用户名等
FTP可检测GET / PUT的文件、服务器、用户名等
HTTP可检测GET / POST、html头、URL、CGI、Cookie、内容和用户等
IM可检测传输文件、内容、发送者、用户等
NTTP可检测传输文件、内容、用户等
可配置的行为方式(阻断 / 记录日志)

终端控制(NAC)

监控运行Client终端安全的主机
检查PC主机是否安装如下安全软件：
防火墙、防病毒、web过滤
可定制强制分发Client安全软件
检查PC主机的操作系统和补丁
可定制监控PC主机安装软件

入侵防御系统(IPS)

ICSA认证(NIPS)
DOS和DDOS攻击控制
4000+多种攻击特征
自定义攻击特征
自动升级攻击特征库
源地址 / 目的地址TCP / UDP会话控制
自定义攻击传感器，
支持基于策略的攻击防御
基于系统，协议，威胁等级的特征库管理
支持NAC攻击源自动隔离
可以按时间自动隔离攻击者的Ip，攻击者和被攻击者的IP，攻击者的接口。

ASG 网络功能

网络/路由
支持多WAN链路，多链路负载均衡网关健康检测
静态地址 / DHCP / PPPOE / DDNS域名
DHCP服务器/中继
静态路由，策略路由
基于TOS的路由
基于用户认证的路由
动态路由RIP v1 & v2, OSPF, BGP
Multicast组播(PIM parse, PIM Dense)
支持多区域
安全区域间路由VDOM虚拟域间路由
多链路聚合(802.3ad)
支持IPv6路由和策略控制
多个二级地址支持
USB 3G modem支持
VLAN子接口支持***

广域网优化
双向优化支持：网关与客户端之间/网关之间
支持A-P 和P-P模式
支持透明或代理方式的Web Cache
支持通道模式和SSL加密通道
支持对SSL加密流量的优化
集成缓存和协议优化技术
加速 CIFS / FTP / MAPI / HTTP / HTTPS / TCP
需要带硬盘的ASG设备

流量整形
基于策略的流量管理
Diffserv服务等级设置
最大 / 最小 / 优先带宽控制
DSCP服务级别设置
上行下行双向流量控制

高可靠性（HA）
主-主，主-
状态失败恢复(FW和VPN)
支持全网状HA
设备失败检测和通告
链路状态监控
链路失败恢复
服务器负载均衡
透明 / NAT / 路由模式支持

ASG管理功能

配置与管理
Console接口(RS-232)
支持多种语言Web管理
支持Telnet, SSH, HTTP,HTTPS管理
多级管理员基于角色的权限配置
可信主机控制
基于Radius的管理员认证
PKI证书管理员认证
分区系统软件存储，支持版本回退
USB
系统软件升级，配置文件自动上载
集中管理、策略下发、集中管理平台
CentralManager

日志与监控
分类日志事件，流量，攻击，病毒，网页
过滤，垃圾邮件，VOIP，IM、内容存档等
内部日志，
远程Syslog / WELF
服务器日志
可选的Analyzer
日志平台，支持丰富的图形实时和历史数据显示、查询，300 种以上自定义报表
本地显示远程Analyzer日志系统管理
SNMPv1 / v2 / 支持Email
事件告警
可选的Guard
分析与管理服务

防火墙用户认证
本地数据库
Windows AD认证
RADIUS / LDAP认证
TACACS+ / PKI
IP / MAC地址绑定
IPSEC VPN Xauth扩展认证
RSA SecurID认证
FSAE一次性认证支持

UTM管理界面定义
自定义基于WEB的管理菜单

设备规格

	ASG 500	ASG 5000
接口	20可扩到24 10/100/1000接口数(铜口)	总接口数：20 硬件加速万兆SFP+接口：8 硬件加速千兆SFP 接口：10 非硬件加速接口(10/100/1000M)：2 缺省配置的模块：2个SR SFP+ FSM扩展插槽：4 USB Server：2 RJ45串口：1
防火墙吞吐量	20Gbps	40Gbps
IPSec VPN吞吐量	15Gbps	16Gbps
IPS吞吐量	1Gbps	1.6Gbps
IPSec VPN通道数	20,000	64,000
IPSec通道(网关到网关) (系统 / vdom)		10,000/5,000
防病毒吞吐量	350Mbps	1.2Gbps
并发会话	1,000,000	4,000,000
新建会话数/秒	25,000	100,000
策略数	100,000	每虚拟域/系统：50,000/100,000
虚拟域(最大/缺省)		250/10
高/宽/长	4.5cm/43.2cm/39.4cm	8.8cm/44.2cm/55.5cm
重	9.1kg	15.88kg
供电要求	90–240 VAC, 50–60 Hz, 8.0Amp(最大)	100–240VAC, 50–60Hz,3.2–6.3A(最大),
功率(平均)	225W	366W
工作温度	0–40° C	0–40° C
存储温度	–35～70℃	–35～70℃
湿度	20到90%非饱和	20到90%非饱和
电气标准	FCC class A part 15, UL/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CUL, C Tick, VCCI

Array NETWORKS

www.arraynetworks.com.cn
www.arraynetworks.net

Array Networks（中国）有限公司

地　　址：北京市朝阳区亮马桥路甲40号 二十一世纪大厦B座1001室
邮　　编：100125
电　　话：010–84446688
传　　真：010–84447566
资料索取：marketing@arraynetworks.com.cn
渠道支持：channel@arraynetworks.com.cn
售后支持：support@arraynetworks.com.cn

上海办事处

地　　址：上海市浦东新区花园石桥路33号 花旗银行集团大厦20楼2011室
邮　　编：200120
电　　话：021–68877222
传　　真：021–68878216

广州办事处

地　　址：广州市林和西路161号 中泰国际广场A1502
邮　　编：510620
电　　话：020–38251185
传　　真：020–38251123