



FortiAnalyzer®

集中日志、分析和报表

提高网络透明度

FortiAnalyzer 集成了网络日志、分析和报表于一体，让网络管理员以最快速度知道网络安全事件。它具有集中化日志分析、相关性分析、报表、内容归档、数据挖掘、病毒文件隔离，漏洞评估等功能。FortiAnalyzer 可以根据地理和时间，对来自 Fortinet 产品和第三方产品的日志进行关联分析，从而让管理员能够对整个安全状态全面的了解。

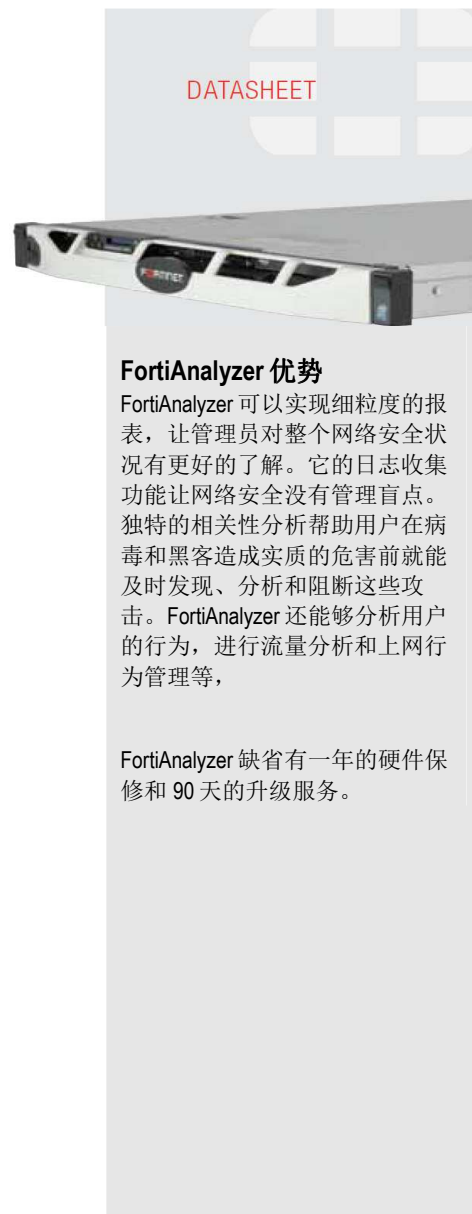
FortiAnalyzer 能够帮助分析安全策略的使用情况，比如识别某种类型的攻击，然后再对安全策略进行细调。除此之外，FortiAnalyzer 还可以对数据包进行捕捉，以帮助相关性分析，和对国家安全条例的审查要求。

安全事件的集中管理

网络管理员部署 FortiAnalyzer 到已有的网络安全体系中，可以对安全事件、内容归档和漏洞评估等安全信息统一管理。FortiAnalyzer 平台可以接收 Fortinet 解决方案中任何日志，比如流量、时间、攻击、内容过滤和邮件过滤日志。使用 FortiAnalyzer 可以减少人工查询日志，或者因为相关性分析和网络监听而手工切换不同的平台，等导致的人力和时间的浪费。FortiAnalyzer 还可以实现集中的日志归档，文件隔离和漏洞评估等功能，让管理员最大程度地掌控企业和组织的网络行为分析。

漏洞管理

FortiAnalyzer OS 4.0 增加了漏洞扫描功能，采用一套特征值库来检测 PC 和服务器的系统漏洞，并且给出解决方案。所增加的功能包括，设备的自动发现，映射，资产定义，资产优先级和报表的定制化。另外，漏洞扫描功能还包含漏洞库的升级服务，如果购买该服务，则漏洞库可以直接与 FortiGuard 服务器相连获得最新的升级。



FortiAnalyzer 优势

FortiAnalyzer 可以实现细粒度的报表，让管理员对整个网络安全状况有更好的了解。它的日志收集功能让网络安全没有管理盲点。独特的相关性分析帮助用户在病毒和黑客造成实质的危害前就能及时发现、分析和阻断这些攻击。FortiAnalyzer 还能够分析用户的行为，进行流量分析和上网行为管理等，

FortiAnalyzer 缺省有一年的硬件保修和 90 天的升级服务。

功能	优点
网络事件汇总	网络管理员可以迅速发现网络安全问题，迅速响应并解决该问题。
图形化报表	从 FortiGate 和第三方设备收集数据，产生事件、行为和趋势方面的报表
性能和容量的可扩展性	FortiAnalyzer 系列可以支持上千个 FortiGate 和 FortiAnalyzer
多种类型日志的集中处理	涵盖了流量、事件、病毒、攻击、web 过滤和通信活动和数据
与 Fortinet 产品的无缝集成	紧密地集成，提高了整体性能，FortiGate 和 Fortimanager 可以直接通过界面访问 FortiAnalyzer 上的资源

特性	FortiAnalyzer 100C	FortiAnalyzer 400B	FortiAnalyzer 1000C	FortiAnalyzer 2000B	FortiAnalyzer 4000B
硬件参数					
专有的硬件平台	支持	支持	支持	支持	支持
10/100/1000 以太网接口	2	4	4	6	2
10/100 以太网接口	1	0	0	0	0
1GbE SFP	0	0	0	0	2
硬盘的数量	1	1, 可加 1 个	1, 可加 3 个	2, 可加 4 个	6, 可加 18 个
硬盘的总容量	1TB	500GB,可扩到 1TB	1.0TB(可扩到 4.0TB)	2.0TB(可扩到 6.0TB)	6.0TB(可扩展到 24TB)
RAID	没有	没有(可选 0,1)	没有(可选 0,1,10)	0,1,5,10,50	0, 1, 5, 10, 50, 60, 缺省 50
热插拔冗余电源	没有	没有	没有	有	有
系统性能					
日志记录(数量/秒)	最大 200	最大 500	最大 1000	最大 3000	最大 6000
数据接收速度	800Kbps	2Mbps	4Mbps	12Mbps	24Mbps
授权的网络设备数量**	100	200	500	2000	2000
授权的 FortiClient 数量	100	2000	5000	无限制	无限制
支持 FortiGate 型号	所有型号	所有型号	所有型号	所有型号	所有型号
物理参数					
尺寸(高、宽、长)	4.4×38×16 cm	4.3×43.8×36.8 cm	4.3×43.4×62.7cm	8.6×44.3×68.1 cm	17.5×48.5×69 cm
重量	1.8 kg	4.5kg	15.9kg	26.1kg	43kg
是否支持机架	否	是	是	是	是
环境要求					
输入电压	100-240VAC	100-240V AC	100-240V AC	100-240VAC	100-240V AC
最大输入电流	1.5A	4.0A	7A	8A	5.5A~11.5A
平均功率	24W	121W	189W	152W	420W(配 6 个硬盘)
工作温度	0~40°C(所有型号, 除 1000C), 0-35°C(1000C)				
存储温度	-25~70°C				
湿度	5 到 95%非凝结				
规范	FCC Class A 15,UL/CUL,C Tick, CE, VCCI				
** 这里网络设备是指:					
1、 没有启动虚拟域的 FortiGate					
2、 如果启用了虚拟域, 那么这里指的就是虚拟域					
3、 第三方的兼容 Syslog 的设备					

图形化报表

FortiAnalyzer 系统对于网络管理员来说是一个强大工具, 他可以充分地发挥 FortiAnalyzer 作用生成详尽的报表。FortiAnalyzer 本身提供一整套报表功能, 而且还支持用户自行定义报表。网络信息被归档, 过滤和挖掘, 以满足审计需求。

细粒度信息

FortiAnalyzer 图形化界面能够有效地帮助管理员深入到数据的每个细节, 充分挖掘可用信息, 生成直观漂亮的报表, 从而让管理员能够了解到网络中究竟发生什么事情。查看历史记录和当前信息, 比如流量日志, 能够分析网络状况和内容层信息。相关性分析能够从网络层到应用层跟踪和分析用户的行为。

实时日志监控

实时监控网络、流量和用户事件, 对于管理员来说是非常重要的, 他能够及时发现网络安全问题, 及时采用采用手段予以应对。

支持的型号

- 所有 FortiGate 型号
- 所有 Fortimail 型号
- FortiClient
- FortiManager
- Syslog 兼容设备

FortiAnalyzer OS 4.1 功能

系统

- 基于权限表的管理员设置
- 加密的Web界面
- FortiAnalyzer 和 FortiGate设备之间通讯的加密与认证
- 邮件报警
- FortiAnalyzer的连接与同步
- SNMP Traps
- 支持Syslog
- RAID配制、修改和查看
- 支持NAS
- 可以加载管理模块
- 可以加载管理命令窗口
- 基本的系统配置
- 在线帮助
- 添加、修改和删除 FortiGate设备
- 查看设备组
- 查看被阻断设备
- 查看报警, 报警事件
- 报警信息窗口
- 查看FortiManager连接状况
- 查看系统信息和资源
- 查看统计信息
- 查看操作历史记录
- 查看会话信息
- 备份和恢复
- 恢复到出厂状态
- 格式化日志硬盘
- 在FortiAnalyzer间迁移数据
- 每个-ADOM的仪表盘

数据归档和挖掘

- 日志分析和报表的所有功能
- 检测和分析数据丢失
- 查看流量类型
- 查看http,ftp,email和及时通讯协议传输的内容
- 查看安全事件概况

- 查看流量概况
- 查看最大流量制造者

网络分析

- 实时网络流量查看器
- 历史网络流量查看器
- 定制化的流量分析器
- 查找网络流量日志

日志分析与报表

- 查看、查找和管理日志
- 自动日志检查
- 基于内容表的报表
- 300多个预定义的报表
- 预定义报表:
 - 攻击: 根据设备、每小时、类型和最大源来统计
 - 病毒: 根据检测量和协议来统计
 - 事件: 根据防火墙, 所有触发事件, 按天等来统计
 - 邮件使用率: 流入和流出的最大邮件用户
 - Web使用率: 最大Web用户, 最多被阻断的网址, 试图访问被阻断网址的用户等统计信息
 - 带宽使用率: 最大带宽占用者, 按天或小时统计带宽, 按协议统计带宽使用率
 - 协议: 使用的最大协议, 最大FTP用户, 最大Telnet用户
 - 广域网优化信息
- 日志汇聚到FortiAnalyzer
- FortiClient定制的报表
- 集成SQL数据库
- SQL支持所有功能, 比如报警、仪表盘、日志查看, FortiClient和FortiMail

中心隔离

- 配置隔离设置
- 查看隔离文件列表
- 隔离文件释放 API
- 隔离文件会显示文件类型、隔离原因和检测次数, 第一次和最后一次检测到的时间

相关性分析

- E-Discovery
- 根据用户名、邮件地址和IM名称来跟踪用户行为
- 支持FortiGuard Web过滤报表
- 显示访问的网站和被阻断的网址
- 每用户统计
- 可配制报表参数, 比如内容表、设备、范围、类型、格式、时间表和输出
- 定制输出的格式
- 按需生成报表
- 报表浏览

日志浏览器和实时日志浏览器

- Web 2.0 风格的, 实时日志浏览器
- 历史和定制化的日志浏览器
- 日志过滤、查找和滚动
- 查看Web、Email和FTP流量
- 查看即时通信和P2P流量
- 过滤流量概况
- 设备概况
- 流量报表涵盖: 事件(管理员审计), 检测到的病毒, 攻击, Web内容过滤, 邮件过滤, 内容(Web, Email, IM)

漏洞扫描和条例管理

- 涵盖了基本漏洞库
- 可以购买升级服务
- 检测漏洞, 推荐解决方案
- 基于资产的报表和分组
- 符合CVE命名规范
- PCI DSS 扫描和报表

标准FortiGuard升级服务

包含以下内容(一个月):

- 病毒库升级
- IPS入侵库升级
- Web分类过滤升级, 包括82个Web类别, 涵盖了2900万个域名和20亿个网页
- 反垃圾邮件(AntiSpam)库升级, 提供实时的垃圾邮件库查询, 确保准确过滤垃圾邮件

Fortinet的全球威胁科研团队负责更新FortiGuard服务, 专家团队24x7的在世界各地保障用户的安全。提供了完整的多重威胁保护, 包括零日攻击等最新威胁响应。针对用户对于可疑恶意软件威胁保证响应时间的需求, Fortinet还可以提供FortiGuard防病毒安全订阅服务的“高级响应”服务级别。与用户购买的服务保证协议(SLA)一起, 这种高级服务合同可为用户提供一个直接联系Fortinet全球威胁科研团队的渠道。

标准FortiCare支持服务

包括以下服务内容:

- 1年的硬件保修
- 90天的FortiCare Web技术支持
- 90天的软件升级

售后支持指南请参阅 <http://support.fortinet.com.cn/support/support/support.html>



飞塔信息科技(北京)有限公司
地址: 北京市海淀区北四环西路52号方正国际大厦12层 邮编: 100080
电话: (010) 6296 0376
传真: (010) 6296 0239
售后: support_cn@fortinet.com

飞塔信息科技(北京)有限公司
上海分公司
地址: 上海市黄浦区南京西路338号天安中心1404室 邮编: 200021
电话: (021) 6120 2836
传真: (021) 6120 2856
<http://www.fortinet.com.cn>

飞塔信息科技(北京)有限公司
广州销售办公室
广州市天河区体育西路101号维多利广场B塔1205室 邮编: 510620
电话: (020) 2885 8303
传真: (020) 2885 8378

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale,
CA 94086 USA
Tel: +1-408-235-7700
Fax: +1-408-235-7737