FortiGate®-3240C 万兆以太网综合安全设备

非官方中文译本 • 安天实验室 译注

文档信息			
原文名称	FortiGate®-3240C 10-GbE Consolidated Security Appliances		
原文作者	Fortinet	**原文发布日期**	
作者简介	Fortinet 公司成立于 2000 年,是一家美国跨国公司。本公司销售高性能网络安全产品和服务，包括其旗舰综合网络安全解决方案 FortiGate 防火墙。 http://en.wikipedia.org/wiki/FortiGate		
原文发布单位	Fortinet		
原文出处	http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-3240C.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	本译文为安天实验室针对网络资料翻译而成，并未取得原作者授权，仅供内部学习和交流使用，安天实验室不对任何可能因此导致的版权问题承担责任。		

数据表

FortiGate®-3240C

万兆以太网综合安全设备

对于大型企业网络，FortiGate-3240C 综合安全设备具有性能卓越，部署灵活以及安全的特点。由 Fortinet 全新设计 ,通过一个定制化的硬件组合(包括 FortiASIC™ 处理器，高端口密度，以及来自 FortiOS™ 操作系统的综合安全特性) 使这些设备拥有了卓越的性能。无论是保护虚拟化基础架构，云计算基础架构还是传统的 IT 架构，万兆以太网（10-GbE）端口和高达 40 Gbps 的防火墙吞吐量使这些设备非常适用于安全的，高带宽网络。

高性能硬件

通过使用创新的 FortiASIC 处理器和最新一代的通用 CPU，FortiGate-3240C 设备的防火墙性能高达 40Gbps。令人印象深刻的综合安全性能和对多种配置的支持确保你的网路的其余部分也拥有重要的安全功能。

高万兆端口密度

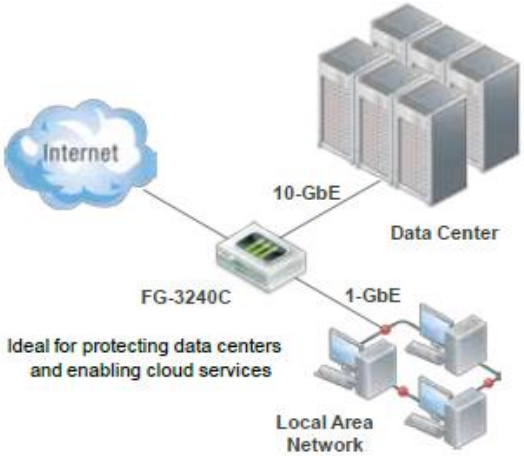
通过万兆以太网接口，你能够保护你的数据中心和其它高带宽应用。FortiGate-3240C 设备标配万兆以太网接口。每一个平台支持 SFP+，SFP 和 RJ-45 连接的系统端口，最大的提供灵活性。

综合安全能力

通过使用先进的 FortiOS 操作系统 ,FortiGate-3240C 设备可以有效的应对各种网络安全威胁。无论是被做为高性能防火墙部署还是做为综合的多重威胁安全解决方案，这些专用设备利用一些当今可用的，最有效的安全手段来对资产进行防护。

FortiGate-3240C 特点

- 优秀的万兆网络安全设备，具有同类最好的防火墙性价比
- 同类最高的万兆以太网端口密度。
- 与基于身份的强制策略相结合，全面的内容防护实现了对应用程序的控制
- IPv6 认证的平台
- 针对策略合规性的，强大的身份认证选项。



FortiGate Certifications

FortiASIC 的优势

FortiGate-3240C 设备采用最新的 FortiASIC 网络处理器（NP）和内容处理器。这些专门设计的高性能处理器使用专有的数字引擎对资源密集型安全服务进行加速。

FortiASIC NP4 内联防火墙和 VPN 功能，包括：

- 线速处理任意大小的数据包
- VPN 加速
- 基于异常的入侵防御，数据包校验和数据包碎片整理。
- 流量整形和优先级队列

FortiASIC CP8 外联直接的网络流量，提供高速的加密和内容检查服务，包括：

- 加密和解密
- 基于特征值匹配的内容检查加速

FortiGate-3240C 设备（前面板）

FortiGate-3240C 设备（背后）

FortiGuard®的安全订阅服务为 Fortinet 提供动态的自动更新。Fortinet 的全球安全研究团队提供这些更新以确保对复杂攻击的实施防御。订阅内容包括防病毒，入侵防护，网页过滤，反垃圾邮件，漏洞管理，应用程序控制和数据库安全服务。有关 FortiGuard 服务的详情，参见 www.fortiguard.com.

FortiCare™支持服务为所有 Fortinet 产品和服务提供全球支持。FortiCare 的支撑可以使你的 Fortinet 产品达到最佳性能。支持计划包括 8x5 小时增强的硬件返厂和更换或 24x7 小时全天候高级硬件替换。可选项包括额外技术支持，额外 RMA 和专业服务。所有硬件产品包括 1 年有限硬件质保和 90 天有限软件质保。此外，Fortinet 专业服务能够被用于促进关键项目和初始部署。

FortiGuard 订阅服务						
产品	**防病毒**	**入侵防护**	**网页过滤**	**防垃圾邮件**	**应用控制**	**漏洞管理**
FortiGate-3240C	支持	支持	支持	支持	支持	支持

FortiOS 4.0 软件—提升品质

FortiOS 4.0：重定义网络安全

FortiOS 4.0 是 FortiGate 多线程安全平台的软件基础，专为安全，性能，可靠性而开发。它是一个利用 FortiASIC 处理器能力的专用操作系统

Fortinet 基于 ASIC 的优势

FortiASICs 是一个专用的高性能处理器系列。该处理器使用一个专用的，智能的内容扫描引擎和多种算法来对安全和网路服务进行加速。

FortiOS 安全服务

防火墙
- ICSA 认证（企业防火墙）
- NAT，PAT，透明（桥接）
- 路由模式（RIP，OSPF，BGP，Multicast）
- 基于策略的 NAT
- 虚拟域（NAT/透明模式）
- VLAN 标记（802.1Q）
- 基于组的认证和调度
- SIP/H.323/SCCP NAT 穿越
- 支持 WINS
- 支持显式代理（Citrix/TS 等）
- VoIP 安全（SIP 防火墙/RTP Pinholing)
- 细粒度的基于策略的防护配置
- 基于身份/应用策略的漏洞管理
- 支持 IPv6（NAT/透明模式）

虚拟专用网络（VPN）
- ICSA 认证（IPSec）
- PPTP，IPSec 和 SSL 专用通道道
- SSL-VPN 集中器（iPhone 客户端支持)
- 支持 DES，3DES 和 AES 加密
- SHA-1/MD5 认证
- PPTP, L2TP，VPN 客户端直通
- 支持 Hub 和 Spoke VPN
- IKE 认证证书（v1 和 v2）
- IPSec NAT Traversal
- 自动 IPSec 配置
- 失效同层检测
- 支持 RSA SecurID
- SSL 单点登陆 Bookmarks
- SSL 双因素身份认证
- LDAP 群组认证 （SSL）

网络/路由
- 支持多 WAN 链路
- DHCP 客户端/服务器
- 基于策略的路由
- IPv4 和 IPv6 动态路由（RIP ,OSPF ,BGP 和 IPv4 的组播）
- 支持多区
- 区域间路由
- 虚拟 LANs 间路由（VDOMS）
- 多链路聚合（802.3ad）
- 支持 IPv6(防火墙 ,DNS ,透明模式 ,SIP，动态路由，管理员访问，管理）
- VRRP 和链路故障控制
- sFlow 客户端

用户身份验证选项
- 本地数据库
- Windows Active Directory (AD)集成
- 外部 RADIUS/LDAP 集成
- 用于 IPSEC VPN 的 Xauth over RADIUS
- 支持 RSA SecurID
- 支持 LDAP 组

数据中心优化
- Web 服务器缓存
- TCP 多路复用
- HTTPS Offloading
- 支持 WCCP

反病毒/反间谍软件
包括反间谍软件和蠕虫防御：

HTTP/HTTPS	SMTP/SMTPS
POP3/POP3S	IMAP/IMAPS
FTP	IM 协议

- 基于流的反病毒扫描模式
- 自动“推送”内容更新
- 支持文件隔离
- 数据库：标准型，扩展型，极致型，流
- 支持 IPv6

WEB 过滤
- 76 个分类
- 多于 2 个的 FortiGuard 网页过滤服务分类
- 10 亿个网页
- HTTP/HTTPS 过滤
- 按时间限制的 Web 网页过滤
- URL /关键词/短语块
- URL 面屏蔽列表
- Content 简介
- 阻断 Java Applet，Cookies，Active X
- MIME 内容头过滤
- 支持 IPv6

应用控制
- 识别和控制至少 1800 种应用
- 控制使用各端口/协议的流行 App：

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

高可用性（HA）
- 主动-主动，主动-被动
- 双机热备（FW 和 VPN）
- 设备故障检测和通知
- 链路状态监控
- 链路故障切换
- 服务器负载均衡

WAN 优化
- 双向/网关到客户端/网关
- 集成的缓存和协议优化
- CIFS/FTP/MAPI/HTTP/HTTPS/通用 TCP 加速

虚拟域（VDOMs）
- 独立的防火墙/路由域
- 独立的管理域
- 独立的 VLAN 接口
- 缺省 10 VDOM（可再添加更多）

无线控制器
- 统一的 WiFi 和接入点管理
- APs 的自动配置
- 上线检测和非法接入点阻断
- 拥有不同 SSIDs 的虚拟 APs
- 多种认证模式

流量整形
- 基于策略的流量整形
- 基于应用和 IP 的流量整形
- 支持 DiffServ
- 保质/最大/优先带宽
- 通过计算和流量限额进行流量整形

入侵防御（IPS）
- ICSA 认证（NIPS）
- 至少 3000 种攻击的防御
- 协议异常防护
- 支持自定义特征
- 攻击数据库自动升级
- 支持 IPv6 Support

DATA 防泄漏（DLP）
- 数据敏感内容的识别和监控 Identification
- 内置样板库
- Built-in Pattern Database
- 用于自定义样板的正则表达式
- 可配置的动作（阻断/日志）
- 支持 IM，HTTP/HTTPS 和其他
- 支持常见的文件类型
- 支持国际字符集

反垃圾邮件
- 支持 SMTP/SMTPS，POP3/POP3S，IMAP/IMAPS
- 实时黑名单/ Open Relay Database Server
- MIME 头检测
- 关键字/词过滤
- IP 地址黑名单/免屏蔽列表
- 从 FortiGuard 网络自动实时更新

终端检测和控制
- 监视和控制安装有 FortiClient 端点的主机的安全

管理/管理选项
- 控制台接口（RS-232）
- WebUI （HTTP/HTTPS）
- Telnet/Secure Command Shell（SSH）
- 命令行接口
- 基于角色的管理
- 支持多种语言：英语，日语，韩语，西班牙语，中文（简体/繁体），法语
- 多级管理员和用户
- 通过 TFTP 和 WebUI 升级和变更
- 系统软件回退
- 可配置的密码策略
- 可选的 FortiManager 集中管理

日志/监控/漏洞
- 记录本地事件
- 远程 Syslog/WELF 服务器日志
- 图形化实时和系统监控
- 支持 SNMP
- 病毒和攻击的电子邮件告警
- VPN 隧道监控
- 可选的 FortiAnalyzer 日志/记录
- 可选的 FortiGuard 分析和管理服务

注：This list is all-inclusive and may contain FortiOS features which are not available on all FortiGate/FortiWiFi appliances.
Please consult FortiGate/FortiWiFi system documentation to determine feature availability for your appliance.

防火墙

Fortinet 防火墙技术通过与具有一整套强大的安全功能的状态检查相结合，提供了完整的内容和网络防护。应用控制，病毒，网页过滤和 VPN，以及先进功能（例如，端威胁数据库，漏洞管理，基于流的检测和主动分析）协调工作，共同辨识和消除最新的复杂安全威胁。强化安全的 FortiOS 操作系统与专用 FortiASIC 处理器协同工作来加速检测的吐量和对恶意软件的辨识。

特性
NAT，PAT 和透明（桥接）
基于策略的 NAT
SIP/H.323/SCCP NAT 穿越
VLAN 标记（802.1Q）
漏洞管理
支持 IPv6

吞吐量	
1518 Byte Packets	40 Gbps
512 Byte Packets	40 Gbps
64 Byte Packets	40 Gbps

入侵防御

IPS 技术可以防御现有和新兴的网络层威胁。除了基于签名的威胁检测，IPS 还进行基于异常的检测，它能够针对任何与攻击行为特性相匹配的流量向用户告警。Fortinet 威胁研究团队分析可疑行为，辨别和归类新出现的威胁，生成新的特征以及 FortiGuard 服务更新。

特性
自动数据库更新
支持异常协议
IPS 和 DoS 攻击防护传感器
支持 IPv6

吞吐量
IPS

防病毒/防间谍软件

反病毒内容检测技术可以防止病毒，间谍软件，蠕虫和其他形式的，能够感染网络基础设施和端点设备的恶意软件。通过拦截和检测基于应用的流量和内容，反病毒防护措施可以确保将隐藏在合法应用内容中的恶意代码威胁辨识出来，并在其产生危害前将其从数据流中移除。FortiGuard 订阅服务能使 FortiGate 设备更新为最新的恶意代码特征，以确保高水平的检测和移除。

特性
自动数据库更新
基于代理的防病毒
基于流的防病毒
文件隔离
支持 IPv6

吞吐量	
防病毒（基于代理）	2.6 Gbps
防病毒（基于流）	5 Gbps

VPN

Fortinet 的 VPN 利用 SSL 和 IPsec VPN 技术提供多个网络和主机间的安全通信。这两种服务采用我们定制化的 FortiASIC 处理器来加速加密和解密步骤。FortiGate 的 VPN 服务增强了完整内容检查和多威胁防护（包括，防病毒，入侵防护和网页过滤）的能力。流量优化为通过 VPN 隧道的关键通信提供了优先级划分。

特性
IPSec 和 SSL VPN
DES，3DES，AES 和 SHA-1/MD5 认证
PPTP，L2TP，VPN 客户端 SSL 直通
登陆书签
双因素身份认证

吞吐量	
IPSec VPN 吞吐量	17 Gbps
SSL VPN 吞吐量	1 Gbps

WAN 优化

广域网（WAN）优化加速了位于物理上分散的网络中的应用，同时确保了全网流量的多威胁检测。广域网优化消除了不必要的和恶意的流量,优化了合法的流量,并减少了应用程序和服务器间传输数据所用的带宽。应用程序性能的提高和交付的网络服务减少了对带宽和基础设施的需求和相关开支。

特性

网关到网关的优化
双向网关到客户端的优化
Web 缓存
安全隧道
透明模式

SSL-加密流量检测

SSL-加密流量检查使客户端 ,Web 和应用服务器免受隐藏威胁的侵害。SSL 检测拦截加密流量，在将它们路由至他们的目的地之前检测它们是否含有威胁。该检测可以被应用于面向客户端的 SSL 流量（例如 ,连接到基于云的 CRM 站点的用户）,以及入站 Web 和应用服务器流量。SSL 检测使你能够在加密的网站内容上施行合适的使用策略，并且使服务免受可能隐藏在加密流量内部的威胁的侵害。

特性

支持的协议：
HTTPS，SMTPS，POP3S，IMAPS
支持的监测：
防病毒，网页过滤，反垃圾邮件，数据防泄漏， SSL 卸载

端点 NAC

端点 NAC 可强制使连接企业网络的用户使用 FortiClient 端点安全。端点 NAC 在允许网络访问之前验证 FortiClient 终端安全产品的安装，防火墙的运行和反病毒特征的更新。不符合要求的端点（例如，运行违反安全策略的应用程序的端点）可以被隔离或者被治理。

特性

监测和控制运行 FortiClient 的主机
网络节点的漏洞扫描
隔离入口
应用程序检测和控制
内嵌应用程序数据库

防数据泄漏

即便应用程序加密了它们的通信，DLP 也可以采用先进的模式识别引擎来辨识和阻断敏感信息被传送出你的网络边界，除了保护你的企业的关键数据，Fortinet DLP 提供了审计线索以有助于策略合规性。你可在多种可配置的操作中进行选择，来记录、阻断和归档数据，以及隔离和禁止用户。

特性

识别和控制移动中的数据
内嵌样板库
基于正则表达式的匹配引擎
通用文件格式检测
支持国际字符集
基于流量的 DLP

Web 过滤

Web 过滤通过阻止用户访问已知钓鱼站点和恶意软件源来保护终端 ,网络和敏感数据免收基于 Web 威胁的侵害。此外，管理员可以通过强制实行基于 Web 站点分类的策略来很容易的阻止用户访问不合适的内容，以及使非法流量阻塞网络。

特性

HTTP/HTTPS 过滤
URL/关键字/词阻断
阻断 Java Applet，Cookies 或 Active X
MIME 内容头过滤
基于流的 Web 过滤
支持 IPv6

日志，报告和监控

FortiGate 综合安全设备为流量，系统和网络防护功能提供了广泛的日志纪录能力。他们还允许你形成来自详细日志信息的，drill-down 的和图形化的报告。报告可以提供针对网络行为的，历史的和当前的分析，以帮助辨识安全问题并防止网络的滥用和误用。

特性

内置日志存储和报告生成
图形化实时和历史监控
支持图形化报表
图形化 Drill-down 图表
可选的 FortiAnalyzer 日志（包括每一个 VDOM）
可选的 FortiGuard 分析和管理服务

高可用性

高可用性（HA）配置通过将多个 FortiGate 设备聚合为一个单一实体，增强了可靠性并提高了性能。FortiGate 高可用性支持主动-主动，主动-被动选项，为 HA 集群中成员的利用提供了最大的灵活性。HA 功能是 FortiOS 操作系统的一部分，大多数 FortiGate 设备拥有该功能。

特性

主动-主动以及主动-被动
双机热备（FW 和 VPN）
链路状态监控和故障切换
设备故障检测和通知
服务器负载均衡

应用控制

应用控制使你可以定义策略并将策略施加于上千台跨网运行的设备上， 无论这些设备采用什么端口或协议来通信。如今，新的基于网络的和 Web 2.0 的应用程序轰炸着网络，这使得应用控制变的非常重要 ,因为对传统的防火墙来说，大多数应用程序流量看起来像是普通的 Web 流量。Fortinet 应用控制提供了对应用的细粒度控制，以及流量整形和基于流的检测选项。

特性

识别和控制超过 1,800 种应用程序
流量整形（每一应用程序）
控制使用各种端口/协议的流行 Apps：

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

及其他

虚拟域

虚拟域（VDOMs）能够使单个的 FortiGate 系统起到多个独立的虚拟 FortiGate 系统的功能。每一个 VDOM 有他自己的虚拟界面，安全配置文件，路由表，管理系统，以及许多其他功能。通过在 FortiGate 平台上虚拟安全资源，FortiGate VDOMs 减少了保护不同网络安全的复杂性。与多点产品相比，大大减少了功耗和空间占用。适用于大型企业和托管服务提供商。

特性
独立的防护墙/路由域
独立的管理域
独立的 VLAN 界面
最多 VDOMs：250
缺省 VDOMs：10

安装/配置选项

Fortinet 为管理员提供了多种方法和向导，以帮助其在部署过程中配置 FortiGate 设备。从易于使用的 Web 界面到高级功能的命令行界面，FortiGate systems 提供了简单灵活的形式以满足你的需求。

特性
基于 Web 的用户界面
基于串口的命令行界面
通过 USB 口的预配置设置

无线控制器

所有 FortiGate 和 FortiWiFiTM 综合安全平台有一个集成的无线控制器，它可以集中管理 FortiAPTM 安全接入点和无线 LANs。阻断未经授权的无线流量，允许经受住身份感知防火墙策略和多重威胁安全检测的流量通过。你可以从一个单个控制台控制网络接入，更新安全策略，启用非法接入点的自动识别和压制。

特性
统一的 WiFi 和接入点管理
APs 的自动配置
上线检测和非法接入点阻断
支持拥有不同 SSIDs 的虚拟 APs
支持多种认证模式

Technical Specifications	FortiGate-3240C
接口和模块	
总网络接口	30
硬件加速万兆 SFP+接口	12
硬件加速千兆 SFP 接口	16
非硬件加速接口（10/100/1000）	2
收发器	2x SR SFP+
本地固态磁盘存储	64 GB SSD
USB 接口（客户端/服务器）	1 / 1
RJ45 串口控制台	1
系统性能	
防火墙吞吐量（1518/512/64 字节 UDP）	40/40/40Gbps
防火墙延迟（64 字节 UDP）	4µs
防火墙吞吐量（Packets Per Second）	64Mpps
并发会话（TCP）	1000 万
新建会话数/秒（TCP）	200,000
防火墙策略	100,000
IPSec VPN 吞吐量（512 byte packets）	17Gbps
IPSec VPN 通道（网关到网关）	10,000
IPSec VPN 通道（客户端至网关）	64,000
SSL-VPN 吞吐量	1 Gbps
并发 SSL-VPN 用户数（建议最大）	30,000
IPS 吞吐量	8 Gbps
防病毒吞吐量（基于代理/流）	2.6/5Gbps
虚拟域（缺省/最大）	10/250
最大 FortiAPs 数	1,024
最大 FortiTokens 数	5,000
高可用性配置	主动/主动，主动/被动，集群
不限用户数	Yes
尺寸和功耗	
长 x 宽 x 高	3.5 x 17.4 x 21.9 in (8.8 x 44.2 x 55.5 cm)
重	40 lb (18.2 kg)
机架安装	耳朵+导轨（选配）
交流电源	100-240 VAC, 50-60Hz, 3.50-1.75A（最大）
功耗（平均/最大）	315/378 W
散热	1290 BTU/h
直流电源（FG-3240C-DC）	-48V VDC
冗余电源（热插拔）	Yes
运行环境和认证	
工作温度	摄氏 0–40 度
存储温度	摄氏-35–70 度
湿度	20 to 90% 非饱和
规范	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
认证	ICSA：防火墙，IPSec，IPS，防病毒，SSL VPN

FortiGate-3240C 综合安全设备还包括：

- 便于安装的多种部署模式（透明/路由）
- 实现低延迟的集成交换矩阵
- 用于数据中心流量优化的高级 Layer-2/3 路由
- 实现最大运行时间的高可用性（主动/主动，主动/被动，集群）
- 用于多租户环境的虚拟域（VDOMs）
- 流量整形和优先级队列以确保关键流量的性能
- 提高性能和降低功耗的广域网优化和 Web 缓存
- 用于合规性和审计的本地事件日志和报告

管理选项

- 本地基于 Web 的管理界面
- 命令行管理界面（CLI）
- 通过 FortiManager 和 FortiAnalyzer 实施的集中管理和分析

主：所有性能与系统配置相关。防病毒性能是以 44Kbyte HTTP 文件测出的。IPS 的性能是使用 1Mbyte HTTP 文件测出的

订购信息	
产品	**SKU**
FortiGate-3240C	FG-3240C
FortiGate-3240C-DC	FG-3240C-DC
可选配件	**SKU**
10-Gig 收发器，适用于 FortiGate 所有模块的 Short Range SFP+模块，带 SFP+接口	FG-TRAN-SFP+SR
10-Gig 收发器，适用于 FortiGate 所有模块的 Long Range SFP+模块，带带 SFP+接口	FG-TRAN-SFP+LR

全球总部
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
电话：+1.408.235.7700
传真：+1.408.235.7737
www.fortinet.com/sales

EMEA 销售办公室–法国
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
电话：+33.4.8987.0510
传真：+33.4.8987.0501

亚太地区销售办公室–新加坡
Fortinet Incorporated
300 Beach Road #20-01
The Concourse,
Singapore 199555
电话：+65-6513-3734
传真：+65-6295-0015