文档密级：公开

下一代防火墙

NGF

产品介绍

北京优炫软件股份有限公司

目　　录

1 产品概述

优炫下一代防火墙（Next Generation Firewall，简称 NGF）是一款可以全面应对应用层威胁的高性能防火墙。通过深入洞察网络流量中的用户、应用和内容，并借助全新的高性能单路径异构并行处理引擎，能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。

优炫下一代防火墙集成了状态检测防火墙、远程接入、网关防病毒、反间谍软件、反垃圾邮件、入侵防御系统、内容与应用程序过滤、数据泄漏防护、即时通讯管理、带宽管理、多链路管理等多种安全防护功能，并可以提供优秀的处理能力。优炫下一代防火墙是一个可扩展的架构并支持 IPv6，满足用户对未来网络的安全需求。

2 产品特性

（1）强大的加固安全操作系统

优炫下一代防火墙采用了一套智能的强大的加固安全操作系统。在此安全系统上，并行运行多种网络安全防护模块，如 IPS、网页过滤、应用程序控制、病毒扫描、Web 应用防火墙、反垃圾邮件、带宽管理等。经过优化的安全操作系统，可以在优炫软件专用多核平台上发挥其高性能的优势。

（2）基于身份识别的全面安全防护

优炫下一代防火墙提供基于身份识别的全面安全防护，以抵御当前存在的复杂的混合型威胁：蠕虫、病毒、恶意软件、数据丢失、身份盗窃、来自应用程序如即时通讯软件的威胁、隐含在 HTTPS 中的威胁等等。

（3）基于身份识别的安全管理

优炫下一代防火墙利用身份识别来提升安全性与可管理性。通过识别用户身份，管理员可以实施对应用程序的管理以及带宽的管理等多项内容，同时不会影响工作效率与连接性。

（4）提供独立的网络接口连接服务器

优炫下一代防火墙可以通过独立的网络接口连接需要访问的服务器，如网页服务器、邮件服务器、FTP 服务器等，创建 DMZ 区域保证外部的通讯访问，同时提升内部局域网络的安全。

（5）独特的融合技术，支持多种安全防护功能高效并行处理

优炫下一代防火墙采用了独特的融合技术，允许在一条防火墙策略中集成调度多种安全防护功能，如 IP 控制、用户身份验证、通讯端口控制、IPS 策略、防毒策略、网页过滤策略、应用程序过滤策略、带宽管理策略等。将多重安全保护与网络连通性相结合，可以大大地提高系统执行效率，真正实现并行数据处理。

3 技术参数

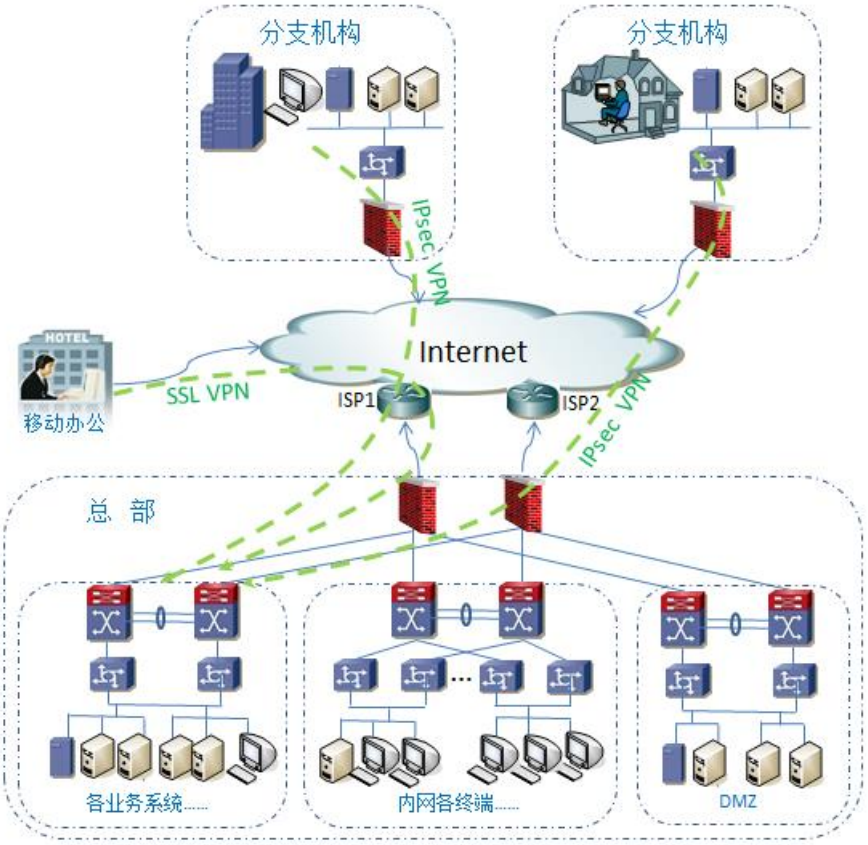
序号	技术指标	指标描述
1	状态检测型防火墙	-八层技术（用户身份）防火墙 -多安全区域规划 -基于身份的访问控制策略 -设备识别、地点识别 -访问控制条件：用户身份、源/目的区域、MAC 地址、IP 地址、服务端口 -安全策略：IPS、网页过滤、应用程序过滤、防病毒、反垃圾邮件、流量管理 -基于国家区域的流量控制 -基于时间计划的访问控制 -支持多对一、一对多、多对多、一对一的多种 NAT 模式 -H.323、SIP 的 NAT 穿越 -DoS/DDoS 攻击防御 -MAC 过滤、IP-MAC 地址捆绑 -欺骗保护
2	网络功能	-基于 WRR 的多链路负载均衡 -接口类型：桥接、链路汇聚、VLAN、TAP、WWAN -支持路由、透明、混合工作模式 -支持 USB 接口 3G/4G 无线网卡 -全功能的 DNS、DHCP 服务器 -支持 RIP、OSPF、BGP 等多种动态路由协议 -支持 ICAP，可与第三方设备集成 -支持 IPv6
3	身份认证	-支持设备本地数据库认证 -支持与 AD 域、RADIUS 服务器的远程认证 -支持基于浏览器的认证方式 -支持身份认证客户端方式 -支持免客户端认证方式 -支持单点一次性认证方式 -支持对登录用户的 IP 地址与 MAC 地址限制
4	带宽管理	-支持流量最大限制、流量最小保证 -支持最多 8 个优先级划分 -支持流量配额管理 -支持基于 IP 地址、通讯端口的流量管理 -支持基于用户身份的流量管理 -支持针对应用程序的流量管理 -支持针对网站的流量管理
5	VPN	-协议：PPTP、L2TP、IPSec、SSL

		-加密算法：DES/3DES、AES、Twofish、Blowfish、Serpent -算法：MD5、SHA-1 -认证：预共享密钥、数字证书 -支持 IPSec NAT 穿越 -支持 DPD、PFS -支持点对点互联、移动用户接入 -提供网页与隧道模式 SSL 接入
6	入侵防御	-特征库：预置 4500 余种特征，可自定义特征 -IPS 策略：预置多种基于区域的防护规则，可自定义规则 -过滤条件：按分类、危害性、平台与目标 -IPS 动作：推荐、允许包、丢弃包、禁用、丢弃会话、重置、旁路会话 -基于用户身份的策略 -特征库自动升级、手动升级 -支持工控行业的 SCADA 特征库
7	网关防病毒与反间谍软件	-发现并拦截病毒、蠕虫、木马 -间谍软件、恶意代码、钓鱼网站防御 -特征库自动升级、手动升级 -可以扫描 HTTP、HTTPS、FTP、SMTP/S、POP3、IMAP -针对用户身份定制扫描计划 -提供用户隔离区域 -基于文件大小扫描与投递 -基于文件类型拦截
8	反垃圾邮件	-进出双向垃圾邮件扫描 -实时黑名单查询（RBL） -MIME 头检测 -基于邮件头、邮件大小、发件人、收件人的过滤 -RDP 技术甄别垃圾邮件 -实时病毒邮件爆发防御 -IP 地址信誉评估 -提供用户隔离区域 -IP 地址黑白名单 -垃圾邮件通知信
9	网页过滤	-支持网页分类过滤，89 种分类，可自定义分类 -基于 URL、关键字、文件类型的过滤 -支持对 HTTP、HTTPS 的保护 -拦截恶意代码、钓鱼 URL、嫁接 URL -拦截 Java Applets、Cookies、ActiveX -兼容 CIPA -数据泄漏控制 -基于时间的控制
10	应用程序过滤	-实现 7 层（应用）与 8 层（用户身份）结合控制与可视化 -提供 2000 余种预置应用程序特征库

		-过滤条件：按分类、风险等级、技术特征 -基于时间的控制 -识别工控行业 SCADA 应用
11	Web 应用防火墙	-支持透明部署、反向代理部署 -防止 SQL 注入、跨站攻击、会话劫持、URL 篡改、Cookie 毒害等攻击 -Web 服务器身份隐藏 -允许过滤 HTTP 方法 -限制访问连接数量 -支持错误重定向技术 -URL 大小写验证 -SSL 卸载
12	高可用性	-支持主-被模式双机热备份 -支持主-主模式双机运行 -支持多桥组接口
13	日志与报告	-提供实时监控与历史查询 -集成 IPS、网页过滤、WAF、防病毒、反垃圾邮件、用户认证、系统与管理等上百种类型的报告 -支持 Syslog 服务器
14	设备管理	-提供基于浏览器的图形化管理界面 -支持命令行管理（Telnet、SSH、串口） -可划分管理员角色 -支持 SNMP（v1/2/3）

4 典型应用

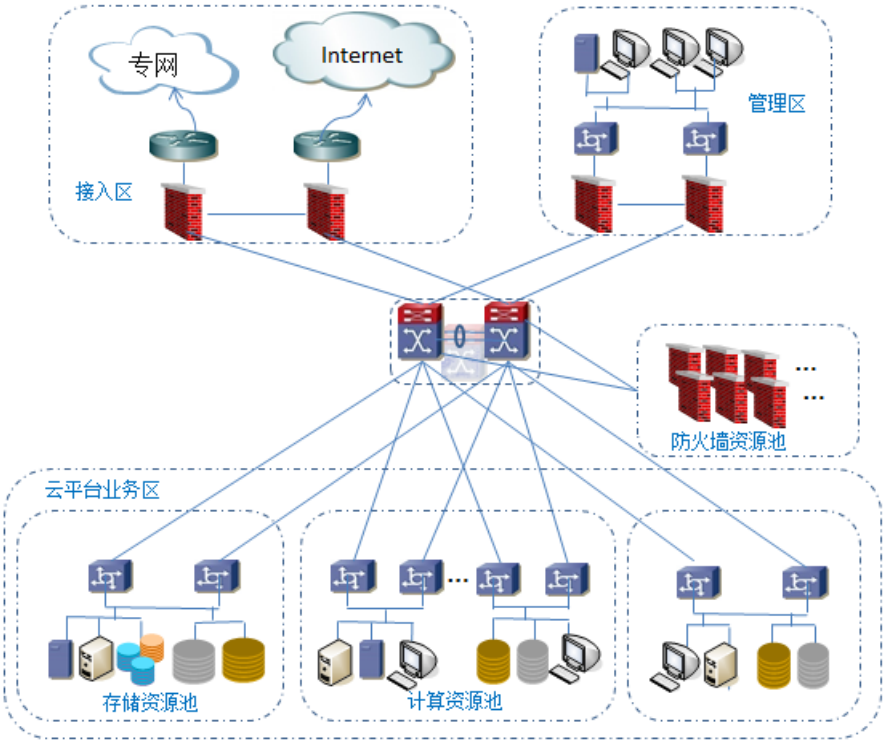
（1）企业互联网边界的应用



企业互联网边界应用示意图

优炫下一代防火墙部署在企业总部及各分支机构互联网出口，防止黑客入侵，精细控制访问权限，防止非法访问，防止企业机密信息被窃取，有效保护企业的关键业务。

（2）数据中心的应用



数据中心应用示意图

优炫下一代防火墙部署在大型数据中心的核心业务出入区，以及互联网出口、广域网边界等区域，为数据中心用户提供精细的控制访问权限，防止非法访问，防止机密信息被窃取，提供应用层安全防护，保障核心业务获取必要的带宽资源。