天融信下一代防火墙（金融系列）
产品白皮书

北京市海淀区上地东路 1 号华控大厦 100085

电话：+8610-82776666

传真：+8610-82776677

服务热线：+86-4007770777

http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

目录

1 概述

2018 年 4 月 21 日，国家领导人在全国网络安全和信息化工作会议上发表讲话， 没有网络安全就没有国家安全。金融 IT 作为关键性信息基础设施，其安全性至关重要。近年，金融 IT 快速崛起，新业务、新技术大量涌现，风险敞口加大，金融 IT 安全面临极大的挑战。我国在今后一段时间内将加大金融业开放的力度，金融 IT 将直面国内外各种不同形态的网络攻击危险。从政府和行业监管机构公布的政策来看，金融机构对数据安全的重视程度正不断提升，但当前网络安全（即传统安全）仍然是金融行业最主要的需求。

防火墙作为网络安全中应用最广泛的安全产品，在金融 IT 安全中发挥着至关重要的作用。天融信下一代防火墙金融系列专为金融 IT 安全设计研发，具备高性能处理能力、高安全防护设计、高可靠设计、易于管理、支持 IPv4/v6 双栈，符合金融等保 2.0 相关要求，满足金融行业对防火墙产品的使用需求。

2 产品特点

2.1 高安全防护设计

天融信下一代防火墙产品设计之初就把安全性放在首位，从防火墙自身安全和客户业务安全进行双重保障，一方面避免产品自身安全漏洞成为系统防护的短板，另一方面提供多种业务安全防护能力，保证客户网业务安全。

2.1.1 自身安全性

为保障安全性，天融信下一代防火墙产品在发布前进行全面完整的自身安全性测评。

- **内部安全测评：**

- 漏洞查杀；
- 代码审计；
- 渗透测试；
- 组织众测；

- **权威机构测评：**

- 通过中国信息安全测评中心 EAL4+评估保障性安全认证；
- 系统安全架构、功能规范、开发安全、脆弱性等方面进行检测；
- 采用文档审核、独立性测试、穿透性测试、现场核查、回归测试、综合评估等方法进行测评；
- 通过中国信息安全测评中心国家漏洞库兼容性认证；
- 通过国家密码管理局防火墙密码检测认证；

2.1.1.1 系统管理安全

➢ **管理协议的安全性设计**

- Web 管理使用 HTTPS 安全通信协议，SSH 管理使用 SSH 安全通信协议，SNMP 管理支持 SNMPv3 协议，具备认证与加密安全机制，Web 前端和后端通信协议使用基于 SSL 机制的天融信自主交互协议；

➢ **认证与授权安全性设计**

- 管理员口令复杂度限制、密码有效期限制、连续登录失败次数限制、账号锁定时间设置、首次登录强制修改密码、密码防暴力破解；
- 支持管理员认证+密码双因子认证、支持外部认证及本地认证
- 支持管理员登录接口限制、登录接口 IP 限制、登录方式限制；
- 支持管理权限控制；

➢ **系统备份安全性设计**

- 支持多份保存配置、导出，配置丢失、错配可回滚；
- 支持多份 normal 固件系统，系统升级可回滚；
- 支持 backup 及 resume 系统，系统故障可恢复；

2.1.1.2 应用软件安全

➢ **基本代码编程安全**

- 防止程序员非授权修改代码，对代码的访问权限进行严格的权限控制；禁止在程序中添加隐藏的“恶意”的代码，防止与应用系统相关的程序员对系统的非授权修改；
- 后台检查文件与记录是否被篡改，如升级包制作时，同时产生 MD5 值，进行比对；

➢ **敏感数据的存放和传递安全**

- 敏感数据不存放在 web 页中；
- 敏感数据不存储在 cookie、隐藏字段或者潜在可能会被用户修改的地方；

➢ **系统备份安全性设计**

- 所有的输入都必须进行正确的有效性检测；
- 格式化字符串安全；
- web 编程安全；
- 具备抗网络攻击的能力及系统脆弱性分析；

2.1.1.3 数据存储和通信安全

➢ **数据存储安全**

- 程序在运行过程中所产生的临时数据（文件）、各部件及接口交互数据（文件）存储于内存文件系统中，避免过程数据泄露；
- 配置文件对称加密存储，规则库对称加密存储，管理员密码非对称加密存储，文件路径隔离，按照业务需要限制应用模块对路径的权限访问；
- 访问权限隔离，按照业务需要限制应用模块访问数据库、表格及字段的权限；
- 对外访问权限隔离，限制外部接入防火墙内部数据文件；

➢ **数据通信安全**

- 管理使用 HTTPS/SSL 等安全通信协议；
- 系统采用加密传输机制对重要信息进行传输；
- 系统采用完整性检查对业务的重要数据或敏感数据进行检查；

2.1.2 业务安全性

2.1.2.1 一体化访问控制安全设计

互联网技术的高速发展和应用模式的不断变化，打破了 Web1.0 时代网络服务使用固定、专用的协议、端口等方面的限制，代之以复用、变种、行为差异为主要特征的应用服务。同时，攻击行为呈现多层次化和多样化，攻击不再局限在网络层面和某一简单的方式，非法入侵、资源滥用、恶意代码、信息泄漏等攻击时刻威胁着网络的安全。网络安全威胁的范围和内容不断扩大和演变，网络安全形势与挑战日益严峻复杂。下一代防火墙利用深度内容检测技术实现针对应用程序、数据内容和用户三者的识别，通过对应用识别、入侵防御、防病毒、URL 过滤、数据过滤、文件过滤、流量管理、VPN 等多种安全引擎和功能的组合调用对上述多种安全威胁进行有效防御。

天融信下一代防火墙产品采用高度集成的一体化智能过滤引擎技术，通过配置一条策略，实现基于八元组的访问控制策略匹配，在此基础上融合了域名、长连接、并发连接数等要素，丰富了对网络中流量匹配、控制的要求。天融信下一代防火墙产品能够做到在一次数据拆包过程中，对数据进行并行深度检测，从而保证了协议深度识别的高效性。并且支持对会话的并发数、老化时间进行配置，使得会话管理配置简单高效，更加贴合金融客户实际需求，满足客户的使用需要。

2.1.2.2 多样安全引擎保障

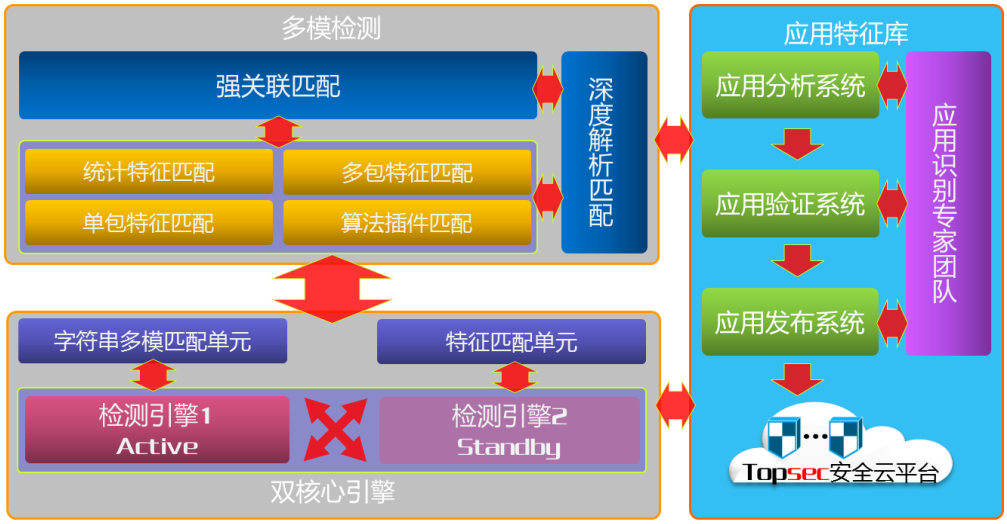
下一代防火墙作为网络安全的主要防线之一，主动适应网络威胁的变化，融合更多更有效的安全检测、防护能力。天融信推出的全新下一代防火墙，除了具备业内当前下一代防火墙的功能外，如应用识别、URL 过滤、入侵防御、病毒过滤等，还可通过异常行为分析机制实现威胁检测防御，并且增加了针对 Web 应用、DDOS 等安全威胁的防护能力。同时，通过联动机制获取 APT、IDS 等安全产品的检测结果，感知网络安全风险点，实现动态安全监控和处置，为客户提供协同防护的安全解决方案。

➢ 精准应用识别

应用识别技术从最初基于 IP、端口检测技术，到基于流特征检测技术(DFI)与深度包检测技术(DPI)，经历了前后几代的演进，而各个厂商在此基础上又纷纷开发出自己独特的应用检测技术，以满足对当前持续变化的应用流量能够进行有效识别的业务需求。当然，无论是哪一种检测技术，对应用识别的精细度、准确率与识别效率始终是衡量其检测技术优与劣的重要标准。

天融信下一代防火墙的应用识别引擎不仅可以识别出底层的承载协议（例如标准的 HTTP 协议），还能进一步区分出上层的精确应用协议类型，例如，HTTP 承载的各类 Web 视频应用（优酷视频、奇艺视频等）、各类网络邮箱（gmail、126 邮箱等）、各类网盘（115、百度网盘等）等；对于同时采用明文方式和加密方式进行通信的应用（例如 BT 应用），下一代防火墙的应用识别引擎能够将 BT 应用细化识别为不同协议类型进行区分，具体可细分为 BT HTTP 明文数据、BT 普通明文数据和 BT 加密数据等；对于同一应用的不同功能特性，下一代防火墙的应用识别引擎也将其分别划分为独立的协议类型，例如，即时通讯 QQ 可细分为登录聊天、文件传输和语音视频聊天等协议类型，从而可以更全面、更详细的了解应用产生的流量的组成；对于利用信令通道（或控制通道）协商数据通道的应用（例如 VoIP 应用的 SIP 与 H.323、FTP 应用），下一代防火墙的应用识别引擎可以通过识别信令通道提取数据通道信息，从而成功识别出无特征的数据通道流量。

天融信下一代防火墙产品的应用识别引擎综合运用单包特征识别、统计特征识别、多包特征识别等多种识别方式进行细粒度、深层次应用和协议识别，同时采用多层匹配模式与多级过滤架构，从而具有极高的应用协议识别率与精确度，可精确识别高达 98%的主流应用。此外，下一代防火墙的应用识别引擎通过拥有专利技术的加密流量识别方法，对于 SSL/TLS 加密流量，甚至是私有协议强加密流量，例如 HTTPS 流量、BT 加密流量、迅雷加密流量、网络视频加密流量或 Skype 加密流量，可实现完全识别。



下一代防火墙产品的应用识别引擎采用高效的确定型字符串多模式匹配状态机作为匹配核心，并采用 HTTP 分流、TCP/UDP 分流等状态机缩小待识别流量范围以进一步提高识别性能；同时，支持多种状态机压缩匹配方式，对于大规模规则库，可以大幅度缩减状态机内存的大小，从而避免内存的膨胀性需求，而且使得状态机可以充分利用处理器的 Cache 特性而保持较高的应用识别性能。因此，面对各种应用层出不穷和频繁升级的情形，下一代防火墙的应用识别引擎具有支持规则库规模不断增长而不损失性能的扩展能力。

- **内容深度过滤**

随着大数据时代的来临，数据已经成为了企业的核心资产，在国家对公共信息保护日益严格的情况下，数据泄露在给企业带来巨大损失的同时，还会为企业带来法律风险。所以，下一代安全技术中有必要针对数据泄露设计专门的防范措施。当前的许多数据检测都是发生在协议层的，例如 FTP，HTTP 等。而实际上，数据泄露却有着很多的渠道，许多网络应用都可以进行数据传输，例如网盘、P2P、IM 等等，这些应用都有自己独特的数据传输机制，这不是从协议层可以检测出来的。所以要进行有效的数据泄露检测，必须能够针对具体应用来进行。而这恰恰是下一代防火墙的核心能力所在。

天融信 NGFW 下一代防火墙内容过滤功能，可以防止核心数据的泄露及违规信息的传输，既能保证员工正常访问 Internet， 又可以对传输信息内容进行过滤。内容过滤是一种基于关键字对通过防火墙的应用的内容进行过滤的安全机制，对应用协议中包含的关键字进行过滤，针对基于不同协议的应用，设备过滤

的内容不同，如果是应用内容则识别出应用的类型、应用内容传输的方向；如果是文件内容则识别出承载文件的应用类型、文件类型和传输方向。

天融信 NGFW 下一代防火墙除了支持内容过滤策略外，还支持文件过滤策略。随着社会和网络技术的不断发展，病毒常感染或附着在一些文件或用户信息中，且病毒的反检测和渗透防火墙的能力越来越强，文件安全已经成为公司和个人越来越关注的问题。文件过滤是一种根据文件类型对通过防火墙的文件进行过滤的安全机制。核心数据和病毒往往存在于特定的文件类型中，比如核心数据一般保存在文档文件中，病毒信息一般附着在可执行文件中， 而管理员在 NGFW 上将文件过滤与内容过滤功能结合使用，通过阻断特定类型的文件传输，可以降低内部网络感染病毒的风险。另外，通过阻止内网用户上传文档文件和压缩文件到外网，以及阻止外网用户从内网服务器下载文档文件和压缩文件，可以降低核心数据泄露的风险。

- **Web 应用防护**

天融信下一代防火墙产品的 WAF 安全引擎通过扫描网络中的攻击行为，将数据流与 Web 应用防护特征进行比较来检测和防御攻击。Web 应用防护特征库包含了对常见攻击的防护规则，如远程代码执行、SQL 注入、XSS 攻击、跨站脚本、webshell 等，这些攻击在多种语言、多种系统中普遍存在，往往不针对特定语言、特定服务器等，覆盖面较大，涵盖了大部分攻击特征，同时包含一些针对特定 CMS 的攻击特征，如针对 phpwind、wordpress、discuz 等攻击防护规则。天融信下一代防火墙产品的 WAF 功能基于配置文件统一动作对符合 Web 应用防护特征的报文进行处理。当不需要对某些地址或应用进行检测或因特殊原因导致业务误阻断时，可以将此地址或应用加入白名单，避免业务中断。

- **DDoS 攻击防护**

天融信下一代防火墙产品内置异常流量检测 ADS 引擎，采用业界领先的源信誉机制，通过流量业务预警、比例抽样分析、源认证、源限速、模式过滤等多种技术手段，利用报文检测和流量监控进行防御策略匹配，精准、快速地阻断攻击流量，保护受攻击系统。天融信下一代防火墙产品能够检测与防御扫描型 DoS 攻击（如 IP 扫描、端口扫描等）、畸形报文攻击（如 Smurf、Land、Ping of death、

Winnuke 等）、特殊控制报文攻击（如 ICMP 重定向报文、Tracert 报文）、网络层 DDoS 攻击（如 IP Flood、UDP Flood、TCP Flood 等）和应用层 DDOS 攻击（如 HTTP Flood、DNS Flood、NTP Flood 等）五大类拒绝服务攻击。

- **异常行为分析**

天融信下一代防火墙具备行为分析安全功能，通过持续观察以及智能分析经过防火墙的流量行为，判断当前网络环境是否存在未知威胁攻击，并通过日志告警的方式提醒用户进行安全防范。流量行为包括当前新建连接速率、当前并发连接数以及当前流量速率。防火墙行为分析引擎通过收集记录设备初始状态，智能创建基准周期行为库和监控周期（下一个周期）的行为表现进行分析对比，并根据当前基准周期行为库和监控周期行为库自动学习生成新的基准周期行为库。若监控周期相对于基准周期的行为表现浮动比超过或低于设置的阈值，则防火墙会立即产生未知威胁日志告警，通知用户网络环境可能存在未知威胁攻击。同时，天融信下一代防火墙提供可视化的行为分析监控结果展示，可以展示行为分析策略周期内的监控行为趋势（包括新建连接、并发连接以及流量趋势），即实时值与基准值的浮动变化趋势，显示相应时间的新建连接数实时值和基准值。若实时值与基准值相差太多，超出行为分析策略设定的浮动比，则会显示超出浮动比警告。

2.1.2.3 安全资源虚拟化

随着企业网络的快速发展以及大数据时代带来的虚拟化技术普遍性发展，网络安全有了更高的要求。天融信下一代防火墙产品进一步优化功能以适应网络安全的新格局，其中包括支持 VxLAN 技术来适应网络环境的变更，支持与云管理平台对接以保证客户云业务需求,支持 RESTFUL 接口联动第三方管控平台等。

针对客户真实的环境，如较多部门划分、机房空间、网络管理复杂度等多种问题，天融信下一代防火墙产品支持划分多个虚拟系统，虚拟系统（ Virtual System）是在一台物理设备上划分出的多台相互独立的逻辑设备。管理员可以从逻辑上将一台防火墙设备划分为多个虚拟系统。每个虚拟系统相当于一台真实的设备，有自己的接口、地址集、用户/组、路由表项以及策略，并可通过虚拟系统管理员进行配置和管理。

虚拟系统具有以下特点：

- 每个虚拟系统由独立的管理员进行管理，使得多个虚拟系统的管理更加清晰简单，适合大规模的组网环境。
- 每个虚拟系统拥有独立的配置及路由表项，这使得虚拟系统下的局域网即使使用了相同的地址范围，仍然可以正常进行通信。
- 虚拟系统之间的流量相互隔离，更加安全。在需要的时候，虚拟系统之间也可以进行安全互访。

虚拟系统能够提供独立的管理界面、独立的安全策略、独立的数据展示，同时能够给每个虚拟系统分配独立的处理能力，实现了硬件资源的有效利用，节约了空间、能耗以及管理成本。

2.2 高可靠性设计

随着互联网的不断发展和进步，金融行业互联网业务扩张明显，稳定可靠的硬件架构和保障业务高可用性已成为金融行业发展的关键性需求。天融信下一代防火墙产品改进硬件结构涉及，结合多机热备及负载均衡技术，充分提高业务进程可靠性及业务不间断，保证高业务流量下的系统稳定性。

2.2.1 硬件可靠性设计

天融信下一代防火墙产品硬件系统架构、前后端接口模块、控制器等硬件单元在结构进行了空间距离的隔离设计，避免接触带电件并采用防火防护外壳，同时，材料及原件的选用保证良好的绝缘、抗电强度和防火防护，并在电路设计上采用安全电压电路、限流电路、受限制电源及有效的过流和过热保护措施等方式，保证设备具备电击防护和防火防护能力。各硬件单元及其交互通信设施设置了部件检查程序，能够完成对产品各组成硬件进行正常工作的检测，包括 CPU、存储、网络接口、扩展部件等。

2.2.2 业务连续性保障设计

为保障金融行业业务连续性，天融信下一代防火墙产品在设备层面提供一系列可靠性设计，如支持链路备份、端口聚合、硬件 bypass、硬件告警等，保障设备发生局部硬件故障时，能自行恢复或发出告警，以便运维人员及时处理。

天融信下一代防火墙产品采用双操作系统设计来应对因升级失败、文件系统错误等系统故障而导致的设备工作异常。主用与备用系统之间采用分布式设计，设备在正常状态下产生的任何系统读写、维护等操作均在主用系统上完成，而备用系统为确保自身完整性则始终处于写保护状态。一旦主用系统发生故障，备用系统将快速、全面的接管设备工作并可实现对主用系统的系统还原。

天融信下一代防火墙产品针对不同的网络环境能够提供多种双机（或多机）部署解决方案，包括双机热备、负载均衡及连接保护模式。多样化的双机（或多机）部署模式以及良好的网络兼容性使天融信下一代防火墙产品能够快速、平滑的接入到 VRRP、RIP、OSPF 及 BGP 等多种路由协议应用场景，在保障用户业务连续性的基础上进而满足各种安全防护需求。

2.3 高效运维管理

为了便于金融用户掌握网络中安全情况以及降低运维管理工作量，天融信下一代防火墙产品提供了智能运维管理的一系列工具，包括安全监控、数据中心、安全策略管理、集中管理、第三方管理接口等。

图 3.4-1 智能安全管理和运维

- 安全策略管理：支持安全策略检查，可对冗余策略、冲突策略、包含策略进行检查；支持安全策略命中统计 ，展示策略连接信息和最后命中时间，快速定位策略有效性；支持策略检索，可对策略主要对象进行搜索，快速定位引用对象的策略；

- 安全监控：支持安全威胁统计，可对安全事件分类统计，展示攻击者、受攻击者和攻击威胁的事件信息，便于管理员了解网络安全形势；支持设备状态监控，展示各关键硬件和系统资源运行状态和趋势，便于管理员了解设备情况，排查网络问题以及合理进行安全规划；

- 安全数据中心：支持用户上网行为审计、上网流量时长审计，便于管理员详细了解用户每个行为，对安全时间进行审计溯源；支持系统、策略、管理方面的日志记录，全面覆盖用户可能需要的日志信息，便于管理员了解和追溯相关事件；支持流量、威胁、行为报表，便于管理员进行网络整体运行情况汇总统计；

- 集中管理中心：为便于对分布在不同区域的多台防火墙进行统一管理，天融信下一代防火墙支持与天融信 NGTP 平台进行对接，实现安全策略统一下发、系统统一升级、规则库统一更新、设备分布拓扑展示、安全事件统计分析等多种集中化管理能力，降低安全运维工作量，维护安全策略一致性；

- 第三方自动化管理：天融信下一代防火墙提供 Restful API 接口，能与第三方自动化运维平台实现对接，通过第三方平台对防火墙进行对象管理、策略管理、系统管理等等同于 WEB 界面的操作管理。

3 产品功能

3.1 基础功能

3.1.1 网络接入

- 支持路由、交换、虚拟线、监听及混合模式接入网络；
- 支持静态路由、动态路由（RIP、OSPF、BGP）、策略路由、ISP 路由、组播路由；
- 支持 VLAN、TRUNK、QinQ、链路聚合、子接口、路由回源、ARP 等网络特性；
- 支持 DHCP 服务器、DHCP 客户端和 DHCP 中继；
- 支持 DNAT、SNAT、双向 NAT 和 NoNAT；
- 支持 ALG，支持 FTP、TFTP、PPTP、SQLNET、H.323、SIP 及 RTSP 动态端口协议；
- 支持 ICMPv6、ND、DHCPv6、RADVD、IPv6 静态路由、RIPng、OSPFv3、IPv6 组播等；
- 支持 NAT64、NAT46、NAT66 地址转换；
- 支持 IPv6 隧道（ISATAP、6TO4 隧道、6IN4 隧道等）；
- 支持 PPPoE 接入；

3.1.2 访问控制

- 支持安全区域、五元组、源 MAC、域名、地区、用户、应用、时间等多元组一体化访问控制；

- 支持访问控制策略设置长连接时间、最大会话数限制、IPv6 选项、入侵防御、病毒过滤、WAF、URL 过滤、数据过滤、文件过滤、审计策略、邮件安全、防代理；
- 支持策略连接统计、策略冲突检测、策略冗余检测、策略包含检测等，可查看策略命中数、最后命中时间等情况；
- 支持访问记录收集，可自动生成访问控制策略；

3.1.3 黑名单

- 支持静态、动态黑名单；
- 支持五元组、MAC、地址、应用、角色黑名单；

3.1.4 连接限制

- 支持基于源地址（地址、地理）、目的地址（地址、地理）、应用设置连接限制；
- 支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制；
- 支持连接限制监控，可展示限制对象、限制 IP、限制条件、被拒次数、被拒时间信息；

3.1.5 流量控制

- 支持基于上/下行区域、地址、地理、时间设置上/下行带宽；
- 链路支持通道及子通道对流量进行进一步的细化管理；
- 基于应用、角色、地址、服务、时间、地理、优先级等方式进行带宽策略定义；
- 支持针对 IP、用户设置保证带宽、限制带宽；
- 支持对地址、应用设置流量控制白名单；

3.1.6 负载均衡

- 支持基于应用、ISP 路由等方式设置路由负载；
- 支持最小带宽利用率、最小延迟等智能选路算法；
- 支持链路探测，根据链路有效性进行链路智能切换；
- 支持服务器负载均衡，提供多种负载均衡算法；

3.1.7 高可用性

- AA（负载均衡）、AS（主备模式）及 SP（连接保护）三种双机工作模式；
- 双机工作模式下，支持会话同步，支持配置实时和手工同步；
- 支持双机设备配置比较，包括运行配置比较和存盘配置比较；
- 支持抢占模式，可设置抢占延时；
- 支持 IPv6 双机配置；
- 图形化展示双机设备接口、主备和指示灯状态；
- 支持主备双系统引导；
- 支持多系统版本并存，多版本间可切换；

3.1.8 虚系统

- 支持并发、新建等系统资源虚拟化；
- 支持路由、NAT 等网络功能虚拟化；
- 支持访问控制、防病毒、WAF、入侵防御等安全功能虚拟化；
- 支持虚系统独立管理，配置单独虚系统管理员；

3.2 下一代防火墙功能

3.2.1 应用识别

- 支持对 P2P 下载、即时通讯、网络游戏、电子商务、数据库、移动应用、社交网络、网络视频等类别的应用进行识别与过滤；
- 支持电驴、BT、迅雷等加密流量进行识别过滤；
- 支持对 IM 即时通讯文件传输进行识别控制；
- 支持对向日葵、Teamview 等远程控制类软件进行识别管控；
- 支持根据协议特征对 HTTP、FTP、SMTP、POP3、Telnet 等常见标准协议进行深度识别；

3.2.2 用户管理

- 支持本地认证、RADIUS、TACACS、LDAP、MS-AD 认证；
- 支持本地认证失败锁定、密码重置限制等防暴力破解功能；
- 支持密码复杂度、密码有效性、账号接入限制等安全设置；
- 支持外部服务器用户账号同步至防火墙本地；

3.2.3 内容过滤

- 支持 HTTP 协议进行上/下行数据内容过滤；
- 支持 FTP 上/下性数据、命令进行过滤；
- 支持对 SMTP、POP3 协议收/发件人、抄送人、主题、正文、附件内容进行过滤；

3.2.4 文件过滤

- 支持对 Windows、Linux 系统常见文件类型进行过滤；
- 支持通过文件特征而非文件后缀进行文件类型识别；

- 支持对文本文件、可执行文件、压缩文件、图片文件、视频文件等识别过滤；
- 支持设置文件过滤方向；
- 支持对即时通讯、网络硬盘、标准协议等特定应用程序传输的文件进行识别过滤；

3.2.5 病毒防御

- 支持 HTTP、FTP、SMTP、POP3、IM 协议进行病毒检测；
- 支持木马病毒、蠕虫病毒、宏病毒、后门病毒查杀；
- 支持病毒库可定期更新或实时更新；

3.2.6 入侵防护

- 内置预定义入侵规则库，可本地或远程更新，支持定期更新或即时更新；
- 支持对 HTTP 攻击类、RPC 攻击类、拒绝服务类、木马类、扫描类、系统漏洞类、溢出攻击类等入侵攻击进行防护；
- 支持自定义规则库；
- 支持入侵防御白名单；
- 支持报文记录；

3.2.7 URL 过滤

- 内置预定义 URL 分类规则库，可本地或远程更新，支持定期更新或即时更新；
- 支持搜索引擎、微博、网上购物、求职招聘、婚恋交友、娱乐、旅游等常见网站类型进行过滤；
- 支持对恶意网站、赌博、色情、反动、暴力血腥、邪教迷信等非法网站类型进行过滤；

- 支持自定义 URL 分类和地址；
- 支持 URL 黑/白名单；
- 支持自定义阻断页面；

3.2.8 WAF

- 内置预定义 WAF 规则库，可本地或远程更新，支持定期更新或即时更新；
- 支持 XSS 注入、SQL 注入、信息泄露、Webshell 防护等 Web 应用安全防护功能；
- 支持自定义规则库；
- 支持 Web 应用防护白名单；
- 支持报文记录；

3.2.9 DDoS 防护

- 基于 IP、ICMP、TCP、UDP、HTTP、NTP、DNS 等协议的 DDoS 攻击防护；
- 支持单包防御，包含 IP 扫描、端口扫描、畸形报文防御、特殊控制报文防御；
- 支持动态黑名单、阈值限流、认证等防护手段；
- 支持添加静态白名单地址；

3.2.10 邮件安全

- 基于发件人、收件人、邮件主题、邮件附件名称等方式对邮件进行过滤；
- 支持邮箱防暴力破解；
- 支持邮件泛洪攻击防护；
- 支持邮件黑、白名单检测；

3.2.11 行为审计

- 支持网站访问、邮件收发、FTP 协议审计；
- 支持上网流量时长审计；
- 支持白名单，对指定的 IP 地址、 URL、 应用的报文不进行审计；

3.2.12 远程接入

- IPSEC VPN、SSL VPN、GRE 多种隧道接入技术；
- IPSEC VPN 支持“预共享密钥”和“数字证书”两种认证方式，支持 DES/3DES/AES 等标准加密算法及 MD5/SHA1 等标准 HASH 算法；
- SSL VPN 支持 PC 端免客户端认证接入，移动端支持 Android、IOS 系统安装客户端认证接入；

3.2.13 异常行为分析

- 支持行为分析，对新建连接数、并发连接数、流量等数据进行统计分析，建立安全行为基线，对异常行为进行告警；
- 支持行为分析监控展示，可展示不同行为分析策略的统计趋势信息；

3.3 安全管理和运维

3.3.1 系统管理

- Web 界面与命令行方式进行系统管理；
- 支持 SSH、HTTPS 安全协议进行管理，支持管理端口自定义；
- 支持 SNMPV1、V2、V3 协议；
- 支持 Restful API 接口，与第三方管理平台进行对接；
- 支持集中管理，通过 NGTP 对防火墙设备状态、系统升级、策略下发等进行统一管理；

- 支持管理员本地认证、外部认证，支持双因子认证；
- 支持管理角色预定义和自定义；
- 支持密码强度、验证码、账号锁定、管理员在线数设置；
- 支持系统资源、硬件状态、网络流量、安全事件的可视化监控；
- 支持报警，支持邮件、声音、本地、控制台、TP、SNMP、短信等多种报警方式；
- 支持日志配置，支持日志本地保存，可设置日志存储空间、日志级别；
- 支持日志外发至多个服务器，支持 Syslog、welf 两种日志格式，支持分级和按类型输出以及日志加密传输；

3.3.2 系统维护

- 支持配置本地保存、外部保存，支持配置导入导出；
- 支持保存全部配置和部分配置；
- 支持保存多份配置；
- 支持配置加密保存和定时保存；
- 支持报文调试功能及系统健康记录，支持端口镜像；
- 支持 PING、Traceroute、TCP、DNS、HTTP 方式进行网络诊断；
- 支持 WEB 抓包，可设置接口、IP、协议、端口、抓报数量等过滤参数，抓包文件可导出；
- 支持多系统版本，多个系统版本之间可进行切换；
- 支持规则库本地升级、FTP/HTTP 远程升级，支持立即升级或周期性升级；
- 支持设备远程重启；

3.3.3 数据中心

- 支持日志查看，可查看管理日志、策略日志、系统日志等；
- 内置预定义报表模板，支持根据通信流量、上网行为、威胁统计等来源自定义报表模板；
- 支持设置报表生成时间和报表本地保存时间、数量；
- 支持周期性和一次性报表生成；
- 支持报表在线查看和导出，支持按照 PDF、WORD 及 EXCEL 格式导出；
- 支持上网行为审计，可对用户访问网站、收发邮件等行为进行审计；
- 支持对用户上网流量和时长进行审计；

4 产品参数及规格

型号	NGFW4000-UF
PN 码	NG-86142-FI
防火墙吞吐	26G
最大并发连接数	1000 万
新建并发连接	30 万/s
IPS 吞吐	7Gbps
AV 吞吐	5Gbps
IPsec VPN 吞吐	12Gbps
IPSec VPN 隧道数	20000 个
SSL VPN 最大用户数	10000 个
SSL VPN 用户数标配	8 个
固定接口	4 个 10/100/1000 自适应电口（包含一对 Bypass 接口） 4 个 SFP 接口 2 个万兆 SFP+接口 最大支持 40 个千兆接口（36 个千兆电口、36 个千兆光口）或者 10 个万兆接口 每个接口可划分到不同安全域实现各接口间的安全隔离 支持扩展 bypass 接口，最大可扩展 16 个 bypass 接口。
RJ45 串口	1
HA 口	1
MGT 口	1

AUX 口	1
扩展插槽	4
USB	2
产品形态	2U
尺寸（宽深高）	640*570*245mm
冗余电源	是
净重	12.42Kg
毛重	16Kg
电压	100~240V AC
频率	50~60HZ
电流	5-2.5A
功率	300W
环境	运行温度：0~45 摄氏度 存储温度：-20~70 摄氏度 相对湿度：5~95%，非冷凝

5 产品资质

证书名称	认证机构
计算机信息系统安全专用产品销售许可证	中华人民共和国公安部
计算机信息系统安全专用产品销售许可证（第二代防火墙）	中华人民共和国公安部
电信设备进网许可证	中华人民共和国工业和信息化部
国家信息安全测评信息技术产品安全测评证书	中国信息安全测评中心
国家信息安全漏洞库兼容性资质证书	中国信息安全测评中心
中国国家信息安全产品认证证书	中国网络安全审查技术与认证中心
防火墙产品密码检测证书	国家密码管理局商用密码检测中心
IPv6 Ready 产品测试认证	全球 IPv6 测试中心
信息安全产品自主原创证明	中国信息安全测评中心

6 应用场景

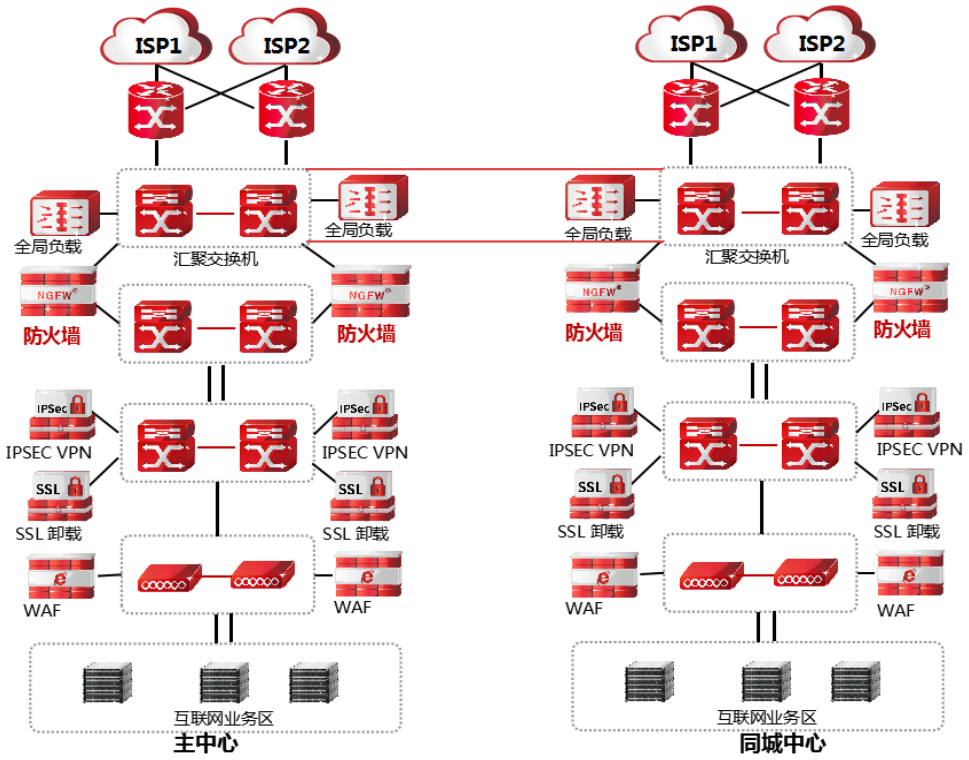


图 7-1 数据中心互联网接入应用场景

安全价值：

- 为用户提供整网安全的第一道防线，在网络关键位置建立安全控制点；
- 提供内部业务服务器地址和服务映射，保障业务正常访问，同时隐藏内部网络；
- 通过多维的访问控制和安全防护能力，对各安全域之间通信流量进行安全检测，实时阻断非法访问；
- 通过与用户网络内的 IDS、APT 等安全产品联动，实现安全设备间协同防护，提升安全有效性。

声明

1．本文档所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2．本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。

3．本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。

RELIABLE NETWORK
SAFE WORLD
TOPSEC