360 新一代大数据智慧防火墙

技术白皮书

360网神 安全第一®

企业安全领军者

目录

1. 产品概述

在信息化飞速发展的今天，网络形势正发生着日新月异的演变，层出不穷的新型威胁冲击着现有的安全防护体系。传统的安全设备，一是以本地规则库为核心，无法有效检测已知威胁；二是没有数据智能，无法感知未知威胁；三是没有联动智能，无法对网络进行协同防御。面对诸如 0-day、APT 及未知威胁等越来越多样化和层次化的攻击，逐渐变得力不从心。归根结底，现在的安全和产品体系还在用单机的、私有的思路来解决网络的、公有的已知威胁。而面对未知的安全威胁，我们不能再孤军作战，而必须是协同共享。

360 新一代大数据智慧防火墙是 360 网神自主创新的新一代防火墙安全系统，基于 360 网神 NDR（基于网络的检测与响应）安全体系。在强劲性能与更先进架构的支撑下，集成了防火墙、VPN、应用与身份识别、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能，并完成了与 360 天眼、病毒云查杀、未知威胁感知分析等多项智能协同防御功能。是专门为政府、军队、金融、教育、运营商、企业的网络出口打造的基于协同防御体系的下一代安全防御系统。

2. 产品特色

2.1 革命性的性能提升

随着网络技术的发展，防火墙需要支持对应用层的过滤和威胁防护，如何保障开启应用层过滤和威胁防护情况下能够高效、快速、稳定运行是新一代防火墙必须面对的问题。区别于对称的多核处理结构，360 新一代大数据智慧防火墙采用自主研发且优化后的异步处理结构 AMP$^+$，突破前者处理数据的瓶颈，更大程

度上提升了防火墙的性能。更高效的性能、更快速的转发速度是防火墙的基石，让集成的多种安全防护功能，在全面启用的情况下，仍然能轻松应对，保证极快的整体转发速度。

2.2 应用层转发延迟有效降低

360 新一代大数据智慧防火墙采用完全自主研发的单引擎一次性数据包拆分和物理多核下并行虚拟计算处理技术，使得整个数据的处理，包括应用层数据的处理、入侵防护等高级功能，都在数据平面完成，不涉及数据包的拷贝，进程切换等问题，同时数据的处理在整个转发阶段都使用同一个会话，实现数据包在 4-7 层的高性能转发，有效降低应用层转发延迟。

2.3 安全隔离的虚拟系统

360 新一代大数据智慧防火墙支持通过虚拟系统功能，将防火墙虚拟成多个相互隔离并独立运行的虚拟防火墙系统，每一个虚拟系统都可以为用户提供定制化的安全防护功能，并可配备独立的管理员账号。在用户网络不断扩展时，通过虚拟系统功能不仅能有效降低用户网络的复杂度，还能提高网络的灵活性。当这些相互隔离并独立运行的虚拟防火墙系统需要通讯时，可以通过防火墙提供的虚拟接口实现，而不需要通过物理链路将它们进行连接。

2.4 基于用户、内容、行为的行为管理及策略管控

360 新一代大数据智慧防火墙提供内容过滤、URL 过滤、网络行为管理功能，从而实现对用户的网络行为进行管控。行为管控不仅支持精确到 IP 地址，更可精确到用户，并实现内容过滤及敏感信息防护。

当用户网络已经搭建了成熟的认证体系，并且业务账号如邮件账号、FTP 服务器访问账号等都与用户认证的账号统一时，防火墙可以提供基于用户行为的策略管控，在认证用户通过认证之后，基于策略用户管控功能可以检查认证用户名与邮件用户名、FTP 服务用户名是否相同，防止越权行为的发生。

2.5　基于应用层的综合安全防护能力

360 新一代大数据智慧防火墙不仅提供多达 23 种普遍的基于网络层的攻击防护，并配备入侵防护、病毒检测、地址黑白名单、域名黑白名单功能。针对 HTTP、DNS、DHCP 协议提供针对性、多级别、适用于不同场景的应用层安全防护，更提供木马专项查杀、防弱口令扫描、局域网多播广播防护等功能，覆盖用户内外网安全，精准快速定位已知威胁。

2.6　采用全新先进的多维动态特征异常检测引擎

360 新一代大数据智慧防火墙采用全新先进的多维动态特征异常检测引擎，抛弃原有的异常行为特征码静态表达的方式，将异常行为、恶意行为特征码通过多维度提炼，动态进行表达，使得特征表达更加全面、精准、有效，极大提高了防火墙入侵防御系统的命中质量，解决了传统设备检测命中率高，但是误报率同样高的问题。

2.7　支持解密 SSL 协议并对其数据进行应用层防护

360 新一代大数据智慧防火墙支持对穿过防火墙的 SSL 协议进行解密，并对解密后的数据提供防护过滤，如攻击防护、入侵检测、病毒防护、内容过滤等。同时，对于某些重要数据，不希望防火墙进行解密，360 新一代大数据智慧防火墙也支持将指定的加密数据进行排除不解密。对 SSL 协议解密并进行过滤可以防止通过 SSL 协议加密的攻击行为从防火墙绕过。防火墙解密后的数据在过滤完毕后会再次通过 SSL 协议加密并发送，保持数据在传输的过程中加密特性不变。

2.8　全方位风险信息展示及分析

360 新一代大数据智慧防火墙为用户提供了全面的实时的风险信息展示，着重突出失陷主机、威胁事件、重点关注对象，一键直达异常行为跟踪界面。

防火墙配置威胁分析模块，可通过自定义关键字模糊检索，定位异常行为踪

迹，加之对漏洞、应用、会话、网络的全方位监控与分析，确认异常行为风险大小。

2.9 基于 NDR 安全体系下的安全联动实现全网未知威胁防御

360 新一代大数据智慧防火墙支持与 360 天眼新一代威胁感知系统、互联网威胁情报中心、云端沙箱系统、防火墙安全管理分析中心（SMAC）进行联动，构建基于全网网络数据检测与响应（NDR）的安全体系，加入了检测、响应、处置维度，为范围未知威胁形成一个防御闭环，将传统基于特征签名的初级检测防护层次升维到基于云端及本地网络数据的检测、响应、处置、防护。

2.10 配合 SMAC 实现管理、配置、分析、处置一体化

防火墙安全管理分析中心（简称 SMAC）主要适用于多台防火墙部署的应用场景，其集统一安全管理、统一设备监控、统一审计及报表展现、统一分析及可视化、快速有效处置等众多运维功能于一身的管理运维平台，实现管理、监控、审计、分析、处置统一化。

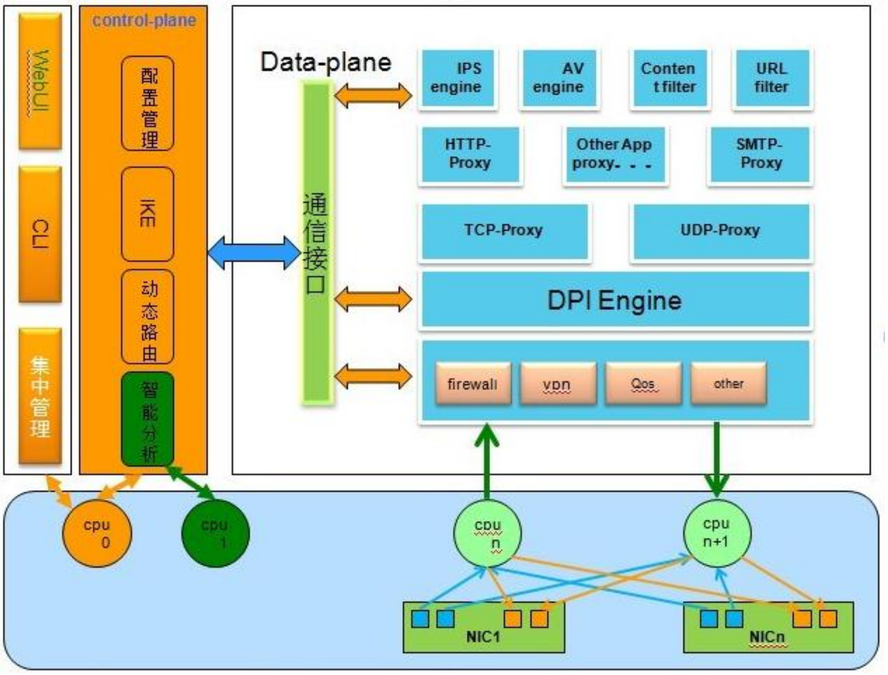
3. 技术优势

3.1 采用第三代 SecOS 系统

具备完全自主知识产权的网神第三代 SecOS 操作系统，实现了防火墙控制层和数据转发层的分离，全模块化设计，实现了独立的安全协议栈，使其突破了传统防火墙转发极限，并消除了因操作系统漏洞带来的安全性问题，以及操作系统升级、维护对防火墙功能的影响。同时也减少了因为硬件平台的更换带来的重复开发问题。先进的设计理念，使第三代 SecOS 具有更高的安全性、开放性、扩展

性和可移植性。

3.2 整体框架采用 AMP^{+}并行处理架构



🟦代表网卡收包队列

🟧代表网卡发包队列

图 3. 2　360 新一代大数据智慧防火墙整体框架

360 新一代大数据智慧防火墙的整体框架采用 AMP^{+}架构，是更加优化的多核异步并行处理架构。整体架构分为三大部分，

- 配置管理平面：由 CPU0 负责处理。
- 控制平面（control-plane）：由 CPU0 负责处理，其中智能分析功能，由 CPU1 负责处理。
- 数据平面（data-plane）：由剩余的 CPU 平均分配处理。

在 AMP^{+}架构下，多个平面负责各自不同的任务，实现了分层、独立、异步并发的工作体系。为 360 新一代大数据智慧防火墙的性能带来了革命性的提升，配置管理平面、控制平面、数据平面的三层分离，保证了防火墙的整体稳定性及可靠性。

3.3 单引擎一次性数据处理技术

传统防火墙或 UTM 技术大多以 Linux 系统为基础，数据的基本转发功能做在 Linux 系统的内核部分，高级功能（例如 IPS、防病毒、内容过滤等）都做在用户态，这样就会导致在运行高级防护时，数据需要从内核送到用户空间，处理完后再从用户空间送回内核，然后再发送出去。

这种做法总体有三大缺点：

1. 涉及到数据包频繁的上下传输。
2. 进程间频繁切换
3. 会话无法复用

而 360 新一代大数据智慧防火墙采用引擎一体化技术后，数据处理流程如下图所示：

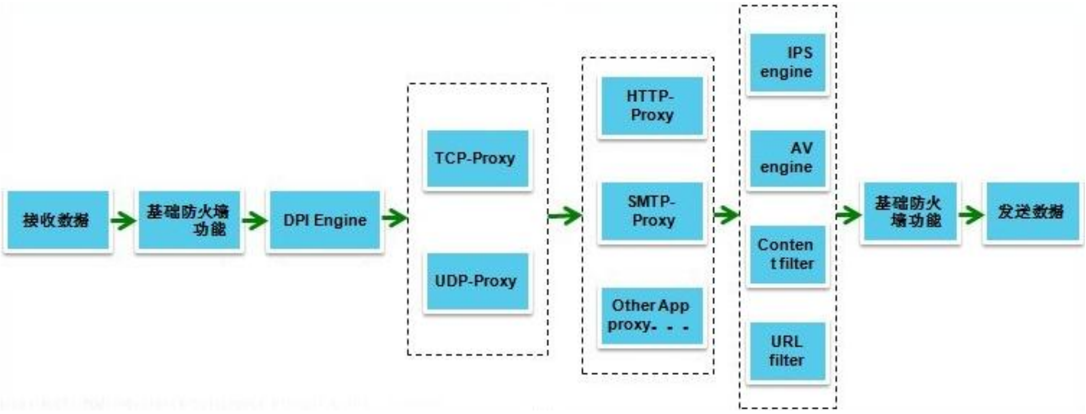


图 3. 5. 1　单引擎一次性数据处理图

从图中我们可以发现，整个数据的接收、数据的处理（包括应用层数据的处理，IPS、防病毒等高级功能），数据的发送，都在数据平面完成，不涉及数据包的拷贝，进程切换等问题。同时数据的处理在整个转发阶段都使用同一个会话。这就极大的提高了应用层的处理速度，降低了整体数据转发的延迟。

3.4 多级冗余架构提高防火墙可靠性

在数据平面上，由于网口数据的接收和发送任务被平均分配给了每一个 CPU 进行处理，当其中一个或多个 CPU 无法工作时，余下的 CPU 可以接替他们，继

续工作，数据的接收和发送任务仍然被平均分配给了每一个当前可以工作的 CPU，在数据平面上，提高了防火墙的可靠性。

在 360 新一代大数据智慧防火墙上，允许导入两个系统，并且这两个系统彼此之间是相互独立的。当用户当前正在使用的系统出现问题时，用户可以切换到另一个系统上。这就在系统层面上，进一步提高了防火墙的可靠性。

在 360 新一代大数据智慧防火墙上，采用增强的 SGRP 路由冗余备份协议，实现双主的路由负载均衡和主备的路由冗余备份两种模式，同时支持透明环境下的 HA 冗余备份和快速切换。在整个网络结构上，更进一步的提高了防火墙的可靠性。

3.5 基于 NDR 安全体系的未知威胁闭环防御

近几年，信息价值的不断提升，让企业的数据安全面临着更多的威胁及更深的影响，传统安全手段解决已知威胁的方式并不能真正保护用户的数据安全。高级威胁往往可以透过合规数据绕过传统安全的各种防御手段并成功达到数据窃取的目的。因此，我们迫切需要一个新的安全体系来对未知威胁进行防范与跟踪。

相对于传统安全而言，360 网神在补充传统安全性能及精准度不足，提升已知威胁识别效率的同时，结合 360 大数据挖掘技术及 360 网神在数据安全分析中的积累，360 网神建立了由大数据驱动，基于网络的检测与响应的体系（简称 NDR）。从而针对未知威胁形成一套基于互联网及用户自身网络的动态数据检测、动态行为检测、动态处置响应的防御闭环。

4. 典型应用

4.1 拓扑一：高校

将 360 新一代大数据智慧防火墙部署在出口位置，实现高校环境中多个公网出口的 ISP 选路及负载功能，同时对校园内网进行智能 QoS 流量分配，保证校园网内部整体带宽的动态合理分配。并对试图进入到校园网内部的攻击进行实时防护，有效保障内部网络安全。

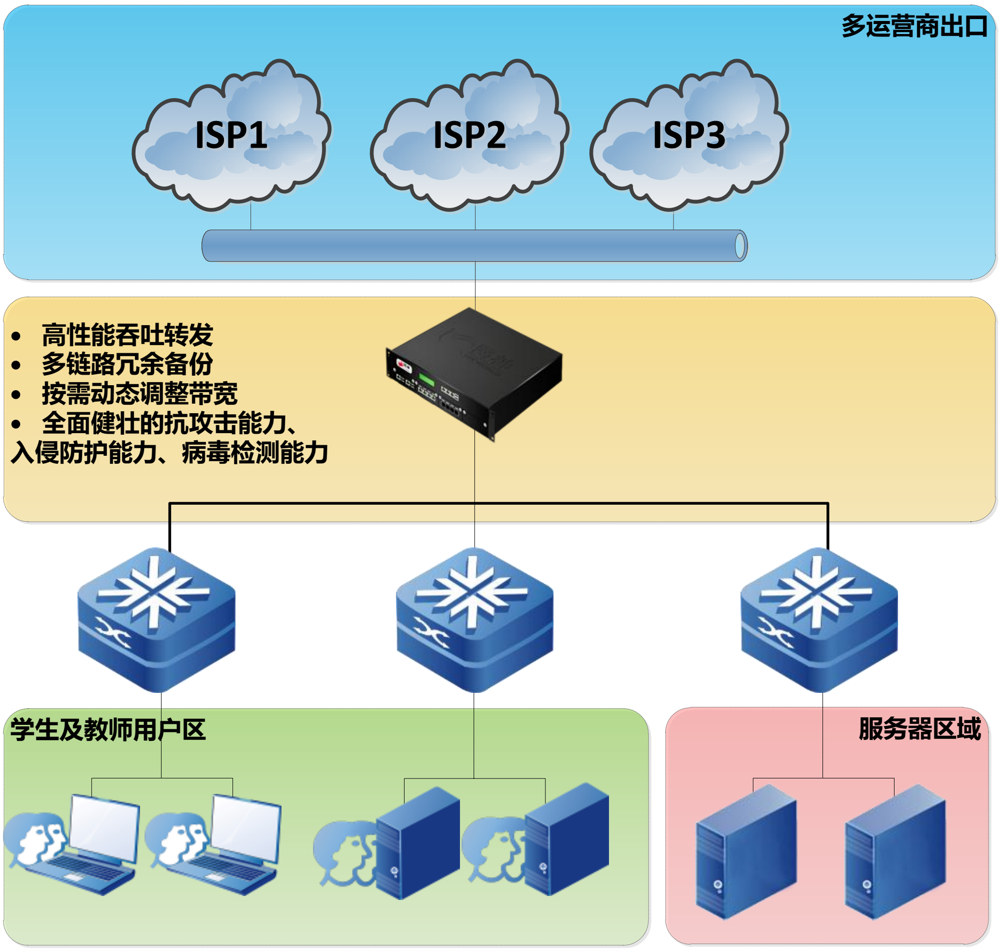


图 4.1　360 新一代大数据智慧防火墙典型应用拓扑图一

4.2 拓扑二：政府

将 360 新一代大数据智慧防火墙采用双机热备部署在数据中心核心层提高

数据中心的可靠性。并与分支机构建立 IPSec VPN，实现内网办公数据与公网出口数据的分离，保证办公数据的保密性。并对试图进入到办公网内部的攻击进行实时防护，有效保障内部网络安全。

还可以进一步将 360 新一代大数据智慧防火墙部署在数据中心接入层，为数据中心的服务器提供独立的安全防护功能。

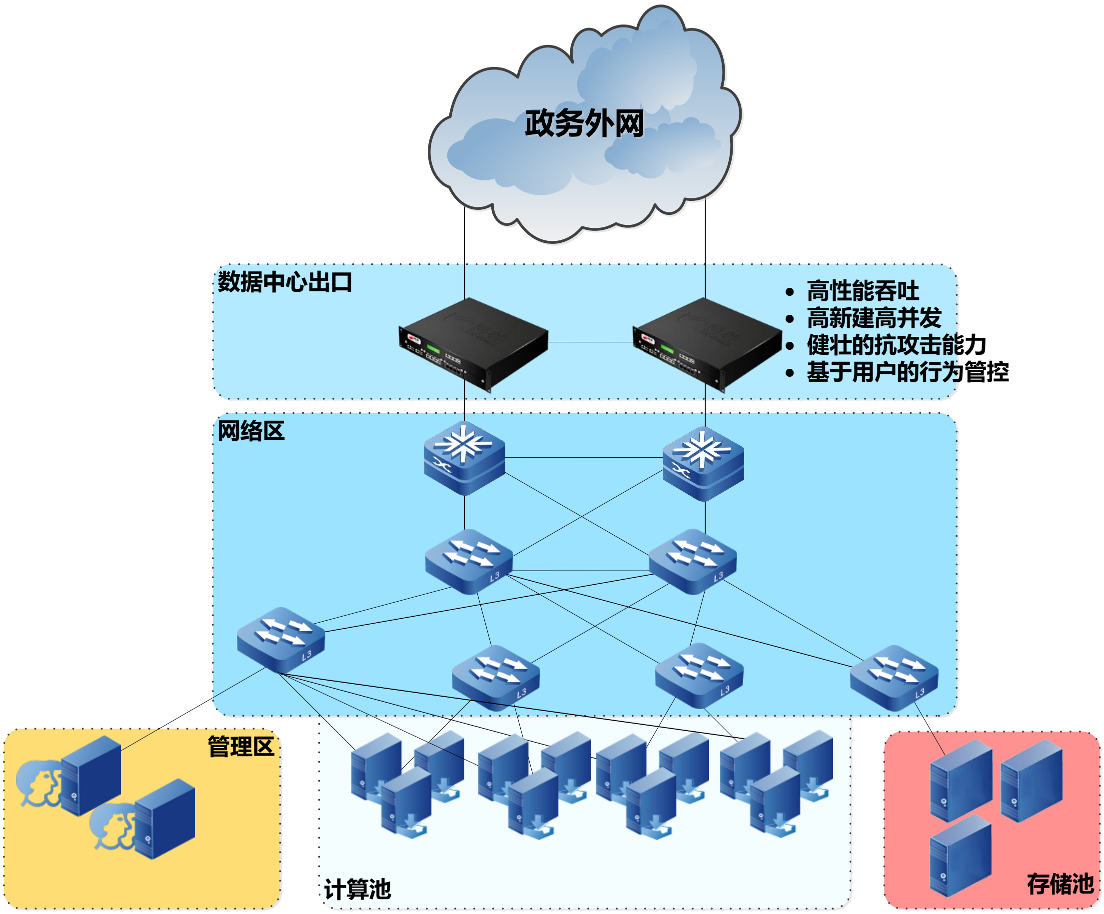


图 4. 2　360 新一代大数据智慧防火墙典型应用拓扑图二

4.3 拓扑三：运营商

将 360 新一代大数据智慧防火墙部署在出口位置，作为大流量出口的承载设备。并提供服务器负载均衡功能，提高服务器的可靠性及服务效率。同时针对多个公网出口提供 ISP 选路及负载功能，保证路由的健壮性。并对试图进入到运营商内部，针对内网的攻击进行实时防护，有效保障内部网络安全。

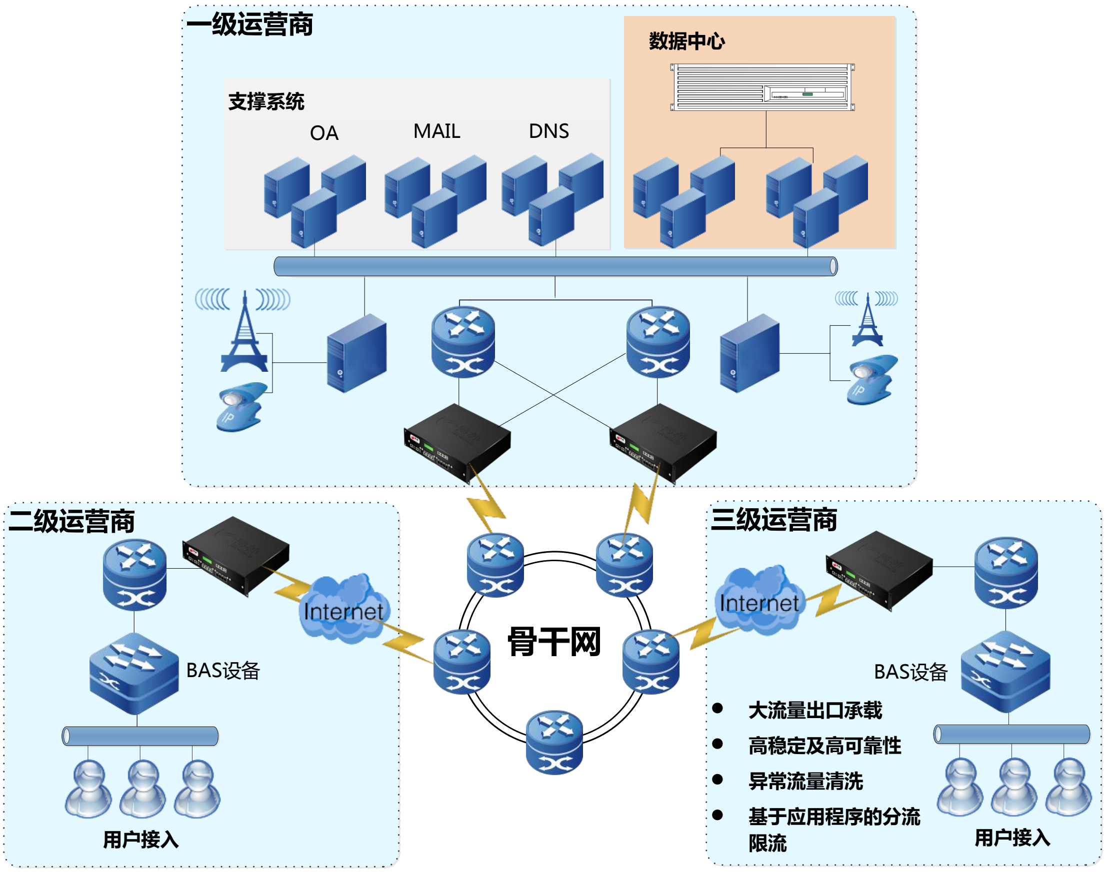


图 4. 3　360 新一代大数据智慧防火墙典型应用拓扑图三

4.4 拓扑三：数据中心（结合 SMAC）

将 360 新一代大数据智慧防火墙部署在数据中心出口位置，作为数据中心出口的承载设备，可为数据中心提供强大性能支撑。而在安全方面，数据中心安全要求高涉及业务杂，传统安全无法满足数据中心严格降低风险的要求。未知威胁可以轻易穿透传统安全手段渗入数据中心内部。因此，360 网神为数据中心提供了防范已知威胁与未知威胁的协同防御解决方案，结合传统安全防范已知威胁的手段，加之全球威胁情报分析中发现未知威胁的手段，防火墙可以为数据中心的安全提供精准的已知威胁拦截能力、有效的未知威胁防御能力。搭配 360 网神安全管理分析中心（SMAC），将分析中心转移到 SMAC 上，可为防火墙减轻分析压力并极大提高基于全网关联分析的威胁行为发现效率。

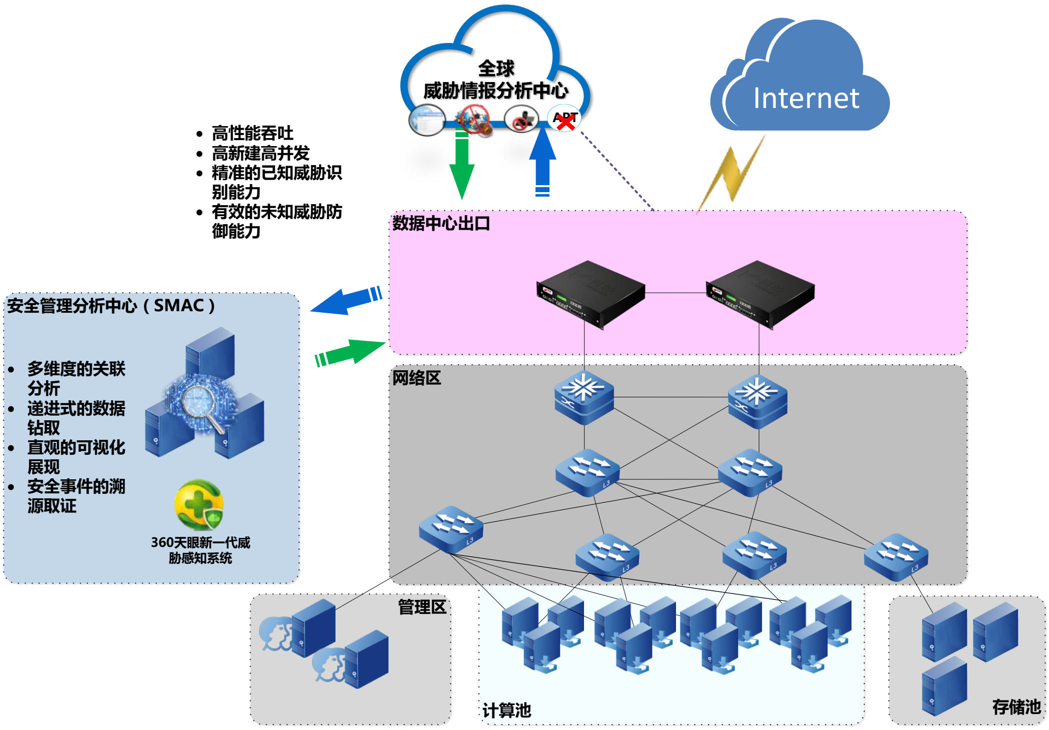


图 4.4　360 新一代大数据智慧防火墙典型应用拓扑图四