紫光集团 H3C
核心企业 数字化解决方案领导者

安全牛 AQNIU.COM

AI 防火墙技术白皮书

AI 防火墙技术白皮书

安全牛
AQNIU.COM

版权声明

免责声明

目录

目录

与时俱进——前言

人类社会正全面进入数字化时代——越来越多的企业、组织和政府机构旨在利用各种 5G、大数据、人工智能、物联网、云计算、区块链等一系列技术创造新价值。随着数字化新技术的应用，信息资产的范围迅速扩展到数字资产。数字资产所面临的网络攻击与威胁也随着数字化时代持续演变。攻击者积极利用机器学习、大数据、人工智能等相关先进的技术，对目标系统实施更为隐蔽的攻击。

现有基于计算机架构所开展的安全技术已经远远不能满足扩展到万物互联的网络空间安全挑战。当今所有组织机构现有安全防护措施应对新型威胁的能力正面临着严重的挑战。新一代安全技术如何与时俱进，以应对新形势下网络空间安全威胁，是当今企业、厂商乃至全社会关注的焦点。

中国具有庞大的人口以及复杂的商业模式。中国的网络空间安全市场与其他国家相比区别明显：规模庞大、区域不均衡、电子商务发达、合规与政治交织、儒家企业文化等等。中国复杂行业应用特点，意味着国内外安全厂商以及投资方都应当仔细区别对待中国市场与国外市场，包括以前瞻性为主导的网络空间安全技术研究机构。**中国网络空间安全市场将与国外网络空间安全市场齐驱并驾，必定是未来趋势。**

据此，安全牛将联合国内外技术先进的厂商，陆续发布在中国本土发生的、具有前瞻性的网络空间安全新技术指南。旨在为各类组织机构在面临网络空间安全挑战时，了解新技术的关键特点以及发展趋势，以及中国不同行业采取解决方案价值所在。

本报告为其中一份网络空间安全新技术指南系列——人工智能防火墙技术指南（简称 AI 防火墙技术指南），由安全牛与新华三联合编制。

本技术指南将从如下维度进行分析与评价。

- 【产生背景】
- 【核心能力】
- 【用户价值】
- 【未来趋势】
- 【主动安全，智能进化】

关键发现

☑ 下一代防火墙（NGFW）技术已经成熟，新一轮基于人工智能的防火墙技术革新即将开始。

☑ AI 防火墙五大特征为：

- 高速、稳定的海量业务处理性能。
- 具有智能关联分析的威胁检测引擎。
- 本地及云端的虚拟化技术。
- 具有快速的加密流量协议分析能力。
- 提供全局威胁可视的集中监测。

☑ 本地与云端结合，并提供一体化的智能网络空间安全边界防护的解决方案将是大型防火墙厂商战略部署方向。

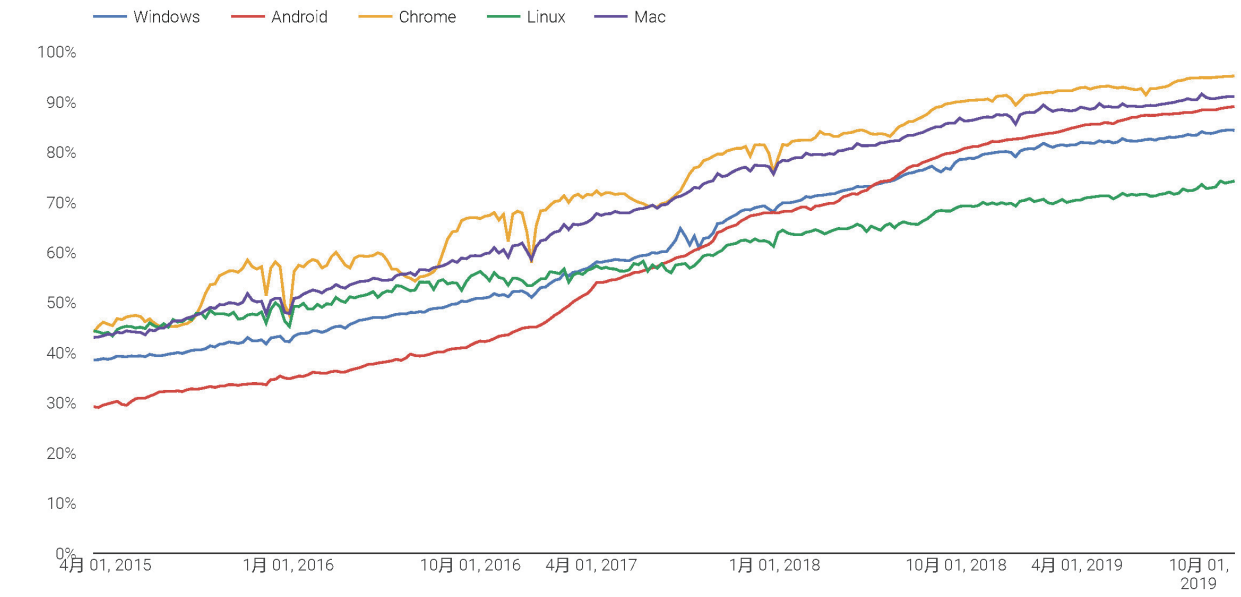
1.【产生背景】——新型网络威胁下防火墙面临的挑战

防火墙部署在内部网络和外部网络之间的边界，对外部网络屏蔽内部网络的结构和运行状况等信息，可以防止外部恶意行为对内部网络的破坏，也可以阻止内部网络中的重要信息外泄。防火墙是一个分离器，将内部和外部网络隔开，提供内部网络的安全防御；防火墙是一个采集器，收集并监测流经的网络流量；防火墙是一个分析器，通过网络流量分析内部和外部网络之间的活动；防火墙是一个控制器，基于安全策略对网络流量进行管控。

防火墙守护着网络的边界安全，是必备的网络安全产品，在整个网络安全防御体系中起着至关重要的作用。随着云计算、大数据、物联网、工业互联网、5G、区块链和人工智能等新兴技术的飞速发展，攻击者的攻击手段变得灵活多样，攻击面也不断扩大，催生了很多新型的网络威胁。这些新型的网络威胁给防火墙的安全防御提出了新的挑战。

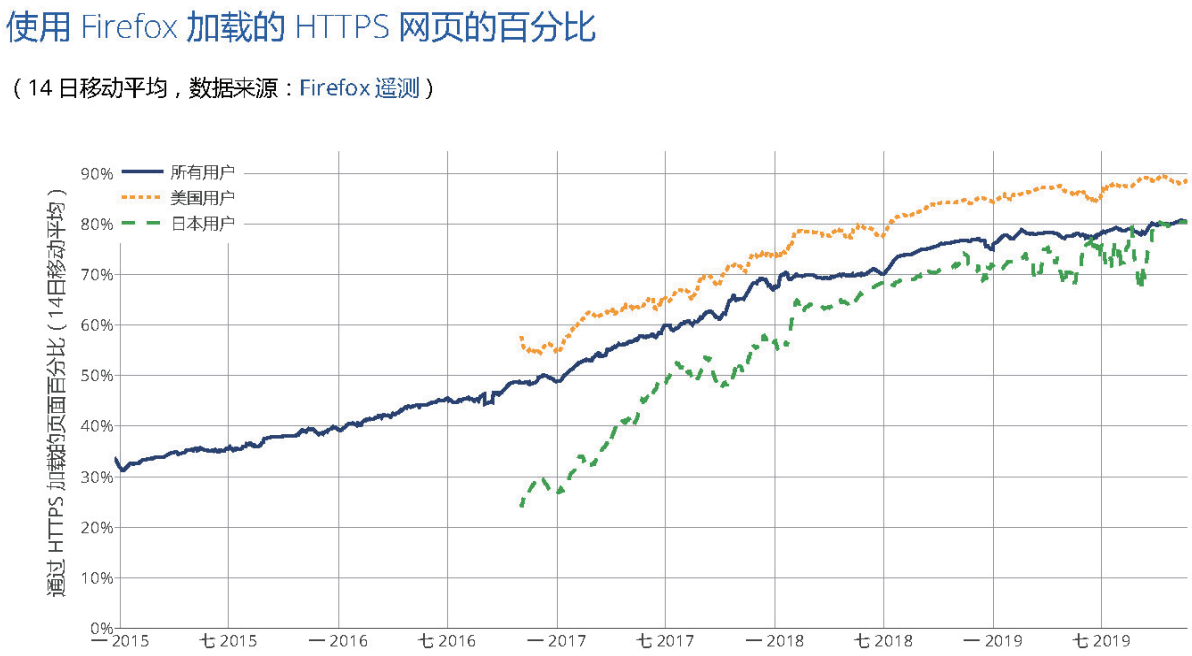
1.1. 新型 & 加密的应用使应用识别更棘手

随着互联网的发展，网络应用服务已深入到人们生活的方方面面，包括基础应用、商务交易、网络娱乐、网络金融和公共服务等。据《第 43 次中国互联网络发展状况统计报告》显示：截止到 2018 年 12 月，我国市场上的在架 APP（移动应用程序）数量约为 449 万款，其中本土 APP 超过 268 万款，占比为 59.7%，并且 2018 年全年的 APP 数量增幅超过 10%。随着 5G、物联网和虚拟现实等技术的应用和普及，网络应用服务的种类将不断增多，数量将继续增长。



[图 1.1 Chrome 中通过 HTTPS 加载的网页的百分比]

为了保护用户的隐私和应用服务的安全，越来越多的企业采用加密技术进行网络通信，网络协议逐渐由 http 协议转向 https 协议。Gartner 曾预测，2019 年将有 80% 的 web 服务采用加密协议进行数据传输。据最新的统计数据显示，全世界通过 Chrome 和 Firefox 两个浏览器访问的网页中 https 网页所占的比例已经分别超过 80% 和 90%，并且这一比例还会继续增长。



[图 1.2 Firefox 中通过 HTTPS 加载的网页的百分比]

现有的防火墙采用特征匹配和深度包检测技术进行应用的识别。在应用识别过程中，先从每款应用的网络流量中提取特征构成特征库，然后将实时流量的特征与特征库中的特征进行匹配。随着应用数量的不断增多，应用特征提取的工作量越来越大；此外，应用程序使用加密协议对网络流量进行加密，应用特征提取的难度也在不断增加。因此，现有的防火墙应用识别技术无法应对加密和新型应用的不断涌现。

1.2. 恶意加密的流量使攻击过程更隐蔽

由于越来越多的应用使用加密协议进行数据的传输，攻击者也越来越倾向于使用加密协议进行通信，以便将攻击流量隐藏于正常的加密流量中，确保攻击行为可以正常实施。Gartner 认为，2019 年有 50% 的恶意软件使用加密协议进行 C&C 通信和敏感数据外传。思科预测，2020 年将有超过 70% 的恶意软件采用加密协议来掩盖恶意软件的投递、C&C 外连和数据窃取活动。届时，将有 60% 的组织和机构不能有效的对 https 流量解密，因而失去应对加密威胁的能力。

现有的防火墙要么选择对加密流量放行，要么选择对加密流量进行解密分析再加密的操作。如果对加密流量放行，那么隐藏在加密流量中的恶意流量将躲避防火墙的检测。如果对加密流量进行解密再加密操作，那么不仅会降低防火墙的性能，还会侵犯用户的隐私。因此，急需一种对加密流量进行非解密分析的恶意软件识别方法。思科的 ETA 解决方案就是一种基于加密流量分析的恶意软件识别方法。

1.3. 人工智能的运用使攻击行为更高效

随着深度学习、对抗学习、知识图谱、强化学习等人工智能（Artificial Intelligence，AI）技术的快速发展，AI 在图像处理、语音识别、自然语言处理和自动驾驶等领域取得了突破性进展，在人脸识别、语音合成、商品推荐、网页搜索等应用场景已经达到商用水平，大大提高了应用服务质量和社会生产力。

AI 是一把双刃剑，如果被网络攻击者使用，将大大提高攻击行为的效率。以钓鱼攻击为例，攻击者利用社交媒体和电子邮件等通信工具向目标人群发送带有恶意程序或链接的内容，误导目标人员点击或者下载恶意程序。在鱼叉钓鱼攻击中，攻击者使用 AI 技术分析目标人员的社交媒体或者电子邮件内容，得到目标人员感兴趣的主题，然后依据该主题生成虚假恶意的电子邮件。经过 AI 技术生成的电子邮件，真实性和可信性都得以增强，可以躲避垃圾邮件检测，更容易误导目标人员点击或下载。在对抗钓鱼网页检测攻击中，攻击者利用机器学习模型逆向技术得到钓鱼网页分类器的部分信息，然后生成能够躲避钓鱼网页分类器的新钓鱼网页。

随着 AI 技术的发展与应用，越来越多的网络服务基于 AI 系统，AI 系统自身也逐渐成为网络攻击者的攻击对象。针对 AI 系统的攻击主要包括后门攻击、数据投毒、躲避攻击、模型盗取等。在上面所述的对抗钓鱼网页检测攻击中，对钓鱼软件分类器进行逆向的过程是模型盗取过程，生成能够躲避钓鱼网页分类器的网页的过程是躲避攻击过程。

在实际的攻击过程中，攻击者可以使用 AI 技术对 AI 系统进行攻击，这样使得攻击变得更加准确和高效。为了应对这种攻击，服务设计者可以在设计 AI 系统时考虑安全因素来增加 AI 系统的安全性，也可以使用 AI 对抗 AI。因此，在 AI 的攻防对抗中，防火墙中增加 AI 功能是一种必要的防御手段。

1.4. 新兴技术的发展使攻击目标更多元

随着云计算、物联网、工业互联网、人工智能和自动驾驶等新兴技术的快速发展，信息系统变得灵活多样，攻击者的攻击目标也变得多元化。云计算使得企业的业务转移到云端，因而攻击目标也从企业内网转向云端；

物联网的核心思想是将装有传感器和嵌入式系统的物体联网，实现“万物互联”，因而攻击目标从传统的 PC 和服务器转向联网的物体，例如网络摄像头、智能音箱等；工业互联网实现了工业设备和系统的联网，因而这些工业对象也成了攻击目标；人工智能的应用促进了诸多行业的发展，但人工智能系统本身也成为攻击对象；自动驾驶是一个复杂系统，包含各类传感器、AI 系统、云端等，其中的每个部分都可能成为攻击目标。此外，随着 5G、区块链、虚拟现实等技术的发展和应用，将催生更多应用场景，届时网络攻击的目标将变得更加多元化。

伴随着新兴技术的发展，安全防御技术也在与时俱进。例如，云安全主要保护云端的虚拟机和容器等，工控安全主要保护工业设备和系统，物联网安全主要保护各种联网的电子产品，等等。现有的防火墙源于对内网资源的保护，起初用于保护内网的 PC 和服务器。随着网络中的攻击目标越来越多元化，单一防护手段很难实现全方位、多目标的安全防护，因此需要一种协同联动的网络安全综合解决方案。

1.5. 政策市场的需求使安全防御更重要

在数字化时代，网络空间威胁产生的危害越来越大，各个国家对网络空间安全的重视程度也越来越高，因此网络空间成为继海、陆、空、太空之后的第五空间。为了加强网络安全建设，提高应对网络攻击的能力，全球各个国家和组织纷纷加快了网络安全的制度建设。例如，中国颁布的《中华人民共和国网络安全法》和《网络安全等级保护》，美国参议院通过的《美国网络安全信息共享法案》，以及欧盟颁布的《通用数据保护条例》等。

网络安全产业规模保持高速增长。《中国网络安全产业白皮书》中指出，全球网络安全产业规模在 2018 年是 1119.88 亿美元，预计 2019 年达到 1216.68 亿美元，增长率是 11.3%；中国网络安全产业规模在 2018 年是 510.92 亿元，预计 2019 年达到 631.29 亿元，增长率接近 25%。

防火墙市场规模不断扩大。据安全牛调研统计，2018 年国内防火墙 / 统一威胁管理 / 下一代防火墙市场约为 96 亿人民币，其中下一代防火墙 (NGFW) 约占总收入的 80%、防火墙 (FW) 约占总收入的 15%、统一威胁管理 (UTM) 约占总收入的 5%。预计 2020 年国内下一代防火墙 / 防火墙 /UTM 市场约为 160 亿人民币。

在面临新型网络威胁时，攻防对抗的本质使安全防御更被动，而政策市场的需求使安全防御更重要，因此急需一种主动、智能的网络安全防御体系。在这种安全体系下，集成 AI 能力的防火墙部署在网络边界，能够起到至关重要的作用。

2.【核心能力】——AI 防火墙为网络边界防御带来希望

为了应对新型网络威胁，AI 防火墙在提供传统防火墙功能的同时还需具备以下核心能力。

2.1. AI 能力加持

AI 能力的加持是 AI 防火墙的基石，包括 AI 芯片和 AI 引擎。

AI 芯片为 AI 防火墙提供强大的计算能力。AI 芯片也被称为 AI 加速器或计算卡，是专门处理 AI 应用中大量矩阵乘法和加法的模块，主要分为 GPU 、FPGA 、ASIC 等。防火墙配备 AI 芯片后，可以在处理海量数据的同时满足性能要求，可以提升链路利用效率和用户网络访问体验，因而成为了各个防火墙厂商关注的焦点。因此，快速、高效的海量数据处理能力是 AI 防火墙的优势之一。

AI 引擎为 AI 防火墙提供灵活的计算方法。AI 引擎是一个复杂系统，包含机器学习处理的全流程，例如数据获取、数据清洗、特征分析、特征提取、模型训练、模型验证、预测等；包含有监督学习、无监督学习、半监督学习、强化学习等机器学习算法；包含流量分析、图像处理、自然语言处理、图数据处理等数据处理技术；支持基线学习、分类、聚类、回归、交互学习等场景。因此，集成了 AI 引擎的防火墙可以有效应对网络中面临的各种安全问题。

2.2. 流量应用识别

网络流量的应用识别是 AI 防火墙提供各种安全服务的必要前提。应用识别不仅要识别已知的非加密应用，还要识别未知的新型应用和加密应用。

新型应用的识别：互联网上每天都会出现大量的新型应用程序，AI 防火墙只有及时地识别这些应用程序，才能更好的对流量进行管控，并为各种安全服务提供前提条件。面对新型应用程序，无法预先知道应用的名称和流量的特征，因而无法识别应用的名称。但是，可以分析出应用中用户的行为，也可以基于用户行为和其它特征识别出应用的类别。

加密应用的识别：为了保护用户隐私和数据安全，互联网上采用加密协议进行通信的应用程序越来越多。这些加密应用不仅包含了正常的互联网应用，还包含利用加密通道进行代理访问的 VPN 软件，以及利用加密

协议进行通信的恶意软件。通过对加密应用进行识别，不仅可以评估正常应用的加密合规性，而且可以识别违规的互联网代理访问，也可以为加密恶意软件的识别提供帮助。

2.3. 加密恶意分析

对来自于恶意软件的加密流量进行分析。随着 SSL/TLS、SSH、VPN 等加密技术的广泛应用，网络中的加密流量已经超过非加密流量。恶意软件越来越倾向于采用加密协议与外部 C&C 服务器进行通信，以便将通信流量隐藏于正常的加密流量当中。AI 防火墙中的加密流量包括正常加密流量，VPN 通道加密流量和恶意加密流量。加密恶意分析是从加密流量中检测出恶意流量，并分析恶意流量的类型。此外，在分析加密恶意流量的过程中，要保证正常流量的机密性，不侵犯用户的隐私。加密恶意分析是 AI 防火墙应对新型网络威胁的必要手段。

2.4. 网络入侵防御

AI 防火墙在加持了 AI 芯片和 AI 引擎后，在原有规则匹配的基础上，**增加了智能的入侵检测和防御能力**。入侵检测系统（IDS）实时监视网络的流量数据，对异常的、可能是入侵行为的流量进行检测和报警。入侵检测系统一般通过旁路的形式部署。入侵防御系统（IPS）实时监视网络的流量数据，对攻击行为和恶意行为进行检测和防御。入侵防御系统一般串行部署在网络中，提供应对攻击行为和恶意行为的处置方法，实现网络流量的风险管控。通过集成入侵检测和入侵防御组件，AI 防火墙在原有功能的基础上还能够识别网络中的异常、威胁、攻击和恶意行为。

2.5. 安全系统协同

AI 防火墙能识别出大部分网络攻击和入侵，但是仍有部分高级持续性威胁（APT）可以绕过防火墙，成功渗透到内网。为了识别这些 APT，AI 防火墙与安全云、态势感知、边缘计算，以及其它安全系统协同，**形成一个“云 – 网 – 边 – 端”联动的一体化安全防御体系**。

AI 防火墙与安全云相结合，可以从云端获得更强大的计算能力和实时的情报信息。AI 防火墙与态势感知平台协同，可以根据收到的安全策略进行及时的阻断和告警。“云 – 网 – 边 – 端”一体化安全防御体系既可以实时了解网络的全局多维态势，识别网络中的异常、威胁、攻击等行为，还可以进行攻击溯源、调查取证、行为审计等操作。

3. 【用户价值】——AI 防火墙行业应用场景

AI 防火墙可以广泛应用在运营商、高校、金融、医疗、政府等领域，提升安全防护能力。

3.1. 运营商

运营商承载着国家的基础网络设施，提供关键的网络和通信服务。为了保证运营商的服务正常运行，确保用户的信息安全，AI 防火墙可以发挥以下作用：

- 防火墙虚拟化。随着云计算的发展，运营商将越来越多的业务迁到云端，通过虚拟机或者容器提供服务，因而针对虚拟化的安全事件不断发生。为了防护云端服务，需要采用虚拟化技术将防火墙布置在云端。

- 木马和僵尸网络监测。运营商有责任建设和执行安全规则，规避网络安全隐患。运营商基于 AI 防火墙可以建立规范的检测、分析、处置策略，主动发现僵尸、木马、蠕虫等恶意流量，提升整个网络的安全防护能力。

- 核心资产和数据保护。针对运营商的网络攻击不断增多，攻击者通过入侵服务器、盗取账号信息、伪造客户凭证等手段，实现对核心资产的攻击和重要数据的窃取。运营商基于 AI 防火墙可以有效的对重要信息基础设施和关键数据进行保护。

3.2. 高校

高等院校的内网用户多，联网设备种类多、数量大，网络流量需求大，互联网出口流量动辄 10GB 以上。该应用场景中，网络攻击和入侵主要来源于互联网。为了防御外部攻击，保护内网和 DMZ，并对用户网络访问行为进行管控，AI 防火墙可以发挥以下作用：

- 高速、大流量环境下的安全防护。必须保证满足从几万个 IP 内部到外部互联网访问的源转换需求，以及具备高抗攻击能力。每秒至少数十万级别以上 TCP 或 UDP 的新建会话能力，确保在极限背景流量情况下仍可以对攻击流进行识别和阻断。

- 链路负载均衡。能自动在多条出口链路均衡分担上网流量，实现链路故障自动切换。同时可以基于应用的引流策略，开启流量控制策略，精细的控制不同对象的不同应用类型的带宽。如：基于 IP 地址的最大带

宽限制；基于 IP 地址的会话限制；基于应用的带宽管理等。

- 入侵防御及防病毒。入侵防御系统用来检测客户网络中勒索、挖矿等攻击行为，防病毒系统用来扫描传输的文件是否携带木马、蠕虫病毒等。这两个功能模块对不同校区组成的 VPN 网络进行防御，确保访问流量没有安全隐患。

- 上网行为管控。学生常常应用 P2P 协议下载软件、观看视频等，占用大量带宽，导致教育网流量难以得到保证。此外，有部分学生通过 VPN 代理软件进行违规网址访问。AI 防火墙通过应用带宽管理、URL 过滤、内容过滤等策略实现用户上网行为管控。

3.3. 金融

金融行业在遭受网络攻击时产生的危害大，因此安全需求高。银行往往有数百家分支机构，分支机构通过专线或 VPN 接入总行网络，整个网络部署上千台防火墙，员工访问控制策略非常严格。为了检测网络中的高级持续性威胁，对抗 0day 攻击，AI 防火墙可以发挥以下作用：

- 加密流量检测及精细化的策略设置。金融行业中的特定业务需要基于应用设置精细化的访问策略，同时需要防止恶意软件使用加密流量向外传输敏感数据。

- 防火墙虚拟化。大部分银行逐渐地将非核心业务迁移到云上，对于迁移到云上的业务系统采用虚拟防火墙进行隔离，并单独配置策略。

- 云端风险模型。云端可以训练风险模型，按照业务需求推荐适合的安全策略。金融行业通常对反欺诈模型、黑灰产数据分析等进行研究，以便对高风险用户及其行为进行画像。

- 核心数据保护。攻击者通过入侵网银系统、盗取用户账号、伪造客户凭证等手段，实现对金融核心数据的窃取。银行、保险、证券等金融机构基于 AI 防火墙可以对在网的用户交易数据进行实时防护。

3.4. 医疗

在医疗行业，“AI+”将催生更多的新业态，例如网上医生、远程诊断等，届时整个行业链将实现海量数

据的共享，包括医院、卫生监管机构、零售商、制药厂等，加大了个人隐私和企业涉密信息的泄露风险。为了保护个人隐私和企业的商业机密，AI 防火墙可以发挥以下作用：

▪ 核心资产和数据保护。针对医院的网络攻击不断增多，攻击者通过入侵医疗系统服务器、盗取医患信息、伪造患者凭证等手段，实现对医疗 IT 资产的攻击和医患数据的窃取。医院基于 AI 防火墙可以有效的对医疗信息基础设施和医患数据进行保护。

▪ 边界网络隔离。目前各个医疗机构采用专线方式直接接入卫生专网。如果某些医疗机构的安全防护意识较弱，个别终端感染了病毒、木马等恶意软件，那么很容易造成大范围的感染，因此必须进行边界网络隔离。

▪ 统一的入侵防范措施。卫生专网的开放性使得其容易受到各种网络攻击和入侵行为。对于网络攻击和入侵行为，各个医疗机构应该能够及时检测、有效阻断、具备对抗黑客攻击的能力。

3.5. 政府

政府网站是各级人民政府发布信息、提供在线服务，以及与公众进行互动的重要窗口。电子政务的安全不仅关系着服务的质量，还代表着政府的形象。随着智慧城市的发展，各级政府将行政、交通、经济、政治等各个方面通过先进的 IT 技术进行集成，形成一个复杂的、智慧的生态系统。在智慧城市的建设中，AI 防火墙可以发挥以下作用：

▪ 核心资产和数据保护。针对政务云的网络攻击不断增多，黑客通过入侵政务云平台、盗取智慧城市的关键信息，实现对政务系统的攻击和市民一卡通数据的窃取。政府基于 AI 防火墙可以有效的对政务云平台等 IT 基础设施和智慧城市数据进行保护。

▪ Web 安全防护。政府的 Web 网站存在着页面被篡改、业务被攻击、数据被窃取、网络被攻击等安全威胁，Web 安全防护至关重要。

▪ 多层次、全方位的安全防护。政府机构的网络安全应该涵盖网络层、传输层、应用层、系统层等多个层次，包括流量攻击、Web 攻击，以及病毒、木马、蠕虫、勒索软件等全方位的安全防护。

▪ 网络安全应急响应。在遭受到网络攻击后，要及时采取适当的措施，尽量将损失降到最小，包括阻断攻击、清理病毒、系统恢复等。整个过程要做到自动化和智能化。

4.【未来趋势】——AI 防火墙技术展望

4.1. 云端部署虚拟化

随着云计算的普及应用，企业逐渐将服务迁移到云端，通过虚拟化技术部署在虚拟机或者容器上。Gartner 指出，网络安全的未来在云端。为了保护云端部署的服务，AI 防火墙将通过虚拟化技术部署在云端。

4.2. 加密分析常态化

随着加密应用的增多，网络中的加密流量越来越多。全世界通过 Chrome 和 Firefox 访问的网页中加密网页已超过 80% 和 90%，并且还在继续增长。于此同时，各种 VPN 代理软件、恶意软件也采用加密协议传输信息。为了识别加密应用和检测恶意软件，对加密网络流量进行分析将是 AI 防火墙必备的技术。

4.3. 业务功能多样化

随着网络安全防护技术的发展，出现了很多网络安全防护产品。通过高性能的硬件设备，可以将这些产品的功能集成到一起。因此，未来的 AI 防火墙将是一个集成了 IDS、IPS、防病毒、蜜罐、应用网关、威胁检测、主动防御等多种功能的综合网络安全产品。

4.4. 防御手段智能化

随着攻击目标越来越多样化，攻击手段越来越灵活，新的网络威胁也越来越多。伴随着 AI 技术的发展，很多安全问题都可以通过 AI 算法来解决。未来 AI 防火墙需要更智能化的防御手段，综合运用监督学习、无监督学习、半监督学习、强化学习等机器学习方法。

4.5. 防护对象精细化

随着物联网、工业互联网、云计算等技术的发展，网络攻击的对象转向联网的电子产品、工业设备和系统，以及云平台中的虚拟机和容器等。为了精确地防护各类网络攻击对象，AI 防火墙的防御对象必然朝着精细化的方向发展。

■ 5. 【主动安全，智能进化】——新华三推出 AI 防火墙

紫光旗下新华三集团以“主动安全，智能进化”为理念，推出 AI 防火墙。新华三认为应对新型网络威胁的最佳手段是一个以 AI 技术为核心的集防火墙、安全云、态势感知，以及边缘计算等系统为一体的网络安全综合解决方案。在这个 AI 网络安全综合解决方案中，AI 防火墙作为网络边界的咽喉，起着关键作用。

5.1. 新华三 AI 防火墙介绍

新华三 AI 防火墙是集成了 AI 硬件和 AI 分析引擎的新一代防火墙，在有效应对传统网络安全威胁的基础上还能够：

- 识别加密和新型应用，提供更加准确、精细和灵活的安全管控策略；
- 识别恶意的加密流量，发现隐藏在正常加密流量中的恶意行为；
- 识别异常、威胁和攻击等安全风险，为应急响应提供决策和依据；
- 与云端和态势感知等平台相结合，提供全方位的协同防御。

同时，新华三认为 AI 防火墙是一个持续演进的产品，是 AI 综合网络安全解决方案中的关键部分，也是网络安全主动防御体系中的必要环节，将朝着弹性架构、加密分析、AI 赋能、协同防御的方向不断推进。

[图 5.1 新华三 AI 防火墙特性图]

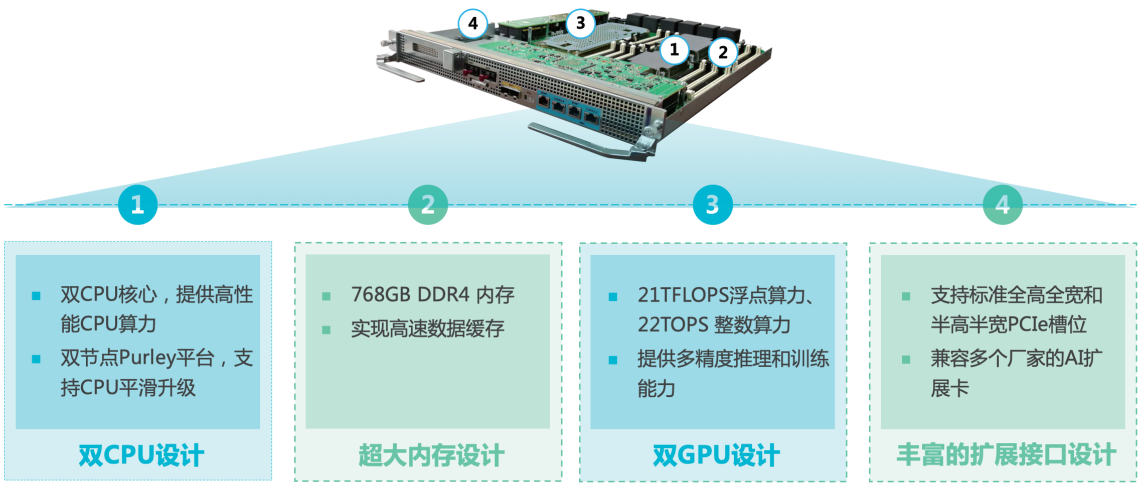
5.2. 新华三 AI 防火墙关键技术

为了应对新型网络威胁、具备 AI 防火墙的核心能力，新华三 AI 防火墙研发团队通过技术攻关，突破了以下几项关键技术。

5.2.1. 弹性智能系统架构

为了实现弹性智能的 AI 防火墙系统架构，新华三 AI 防火墙采用通用的 X86 处理器与 GPU 板卡相结合的硬件架构，同时搭载新华三 AI 引擎，实现了集 AI 硬件和 AI 引擎于一体的高性能系统架构。

弹性硬件架构：为了满足各类客户差异化业务需求，构建开放合作智能安全生态系统，新华三 AI 防火墙支持 CPU、GPU 多插卡弹性扩展，X86 CPU 业务单板采用开放 / 可扩展设计思想，GPU 板卡可兼容多个厂家的 AI 扩展卡，便于构建开放合作的智能安全生态系统；智能 SDN 控制器可灵活定义用户安全需求，实现安全业务统一编排和安全配置统一管理。新的硬件采用双节点 Purley 平台，支持 CPU 平滑升级；GPU 板卡具备超强计算能力，每秒达到 21 万亿次以上；采用超大内存设计，实现高速数据缓存；具备 100G+ 应用层性能交付能力，采用高密度 10G/40G/100G 接口设计。



[图 5.2 AI 防火墙硬件架构图]

安全 AI 引擎：为了提供智能分析技术，新华三 AI 防火墙内置高性能的安全 AI 引擎。安全 AI 引擎包含数据采集、数据清洗、特征提取、特征选择、关联分析算法、机器学习算法等一系列数据挖掘过程必备的模块，包含恶意 URL 检测、DNS 通道识别、DGA 域名识别等多种分析和检测模型，提供风险评估、异常分析、威胁检测、攻击识别、态势预测、用户审计等业务功能。

[图 5.3 安全 AI 引擎结构图]

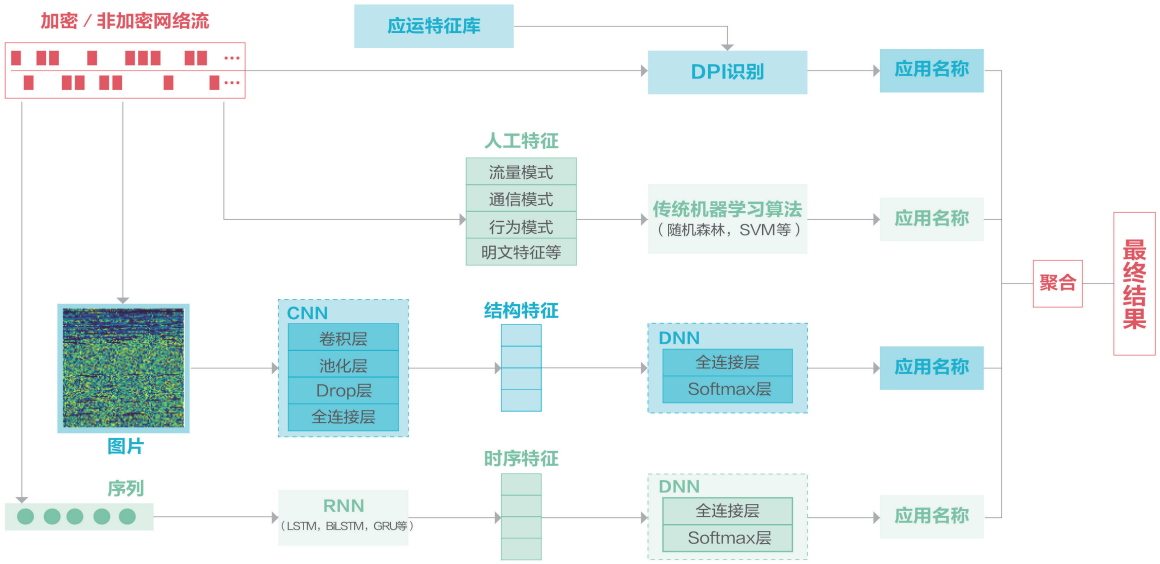
5.2.2 新型 & 加密应用识别

为了识别网络流量中的新型与加密应用，新华三 AI 防火墙研发一种先进的加密流量分析技术，采用人工和自动两种特征提取方法，运用深度包检测、传统机器学习和深度学习三类应用识别算法，实现了包含四条应用预测路径的应用识别方法。新华三 AI 防火墙不但可以识别已知非加密应用，还可以识别新型应用、加密应用和违规代理软件。

新型应用的识别：面对未知新型应用，虽然无法准确识别应用的名字，但是可以识别出该应用的大类。例如，当遇到一款新的即时通讯应用时，虽然无法识别其具体名称，但是可以将其归类为即时通讯。虽然每个应用都有自己的流量模式、通信模式和行为模式等统计特征，但是同一大类应用往往具有相似的功能，它们的统计特征值也往往相近。因此，对于新应用的识别，虽然机器学习模型的训练数据中没有该应用的训练数据，仍然可以利用同一应用大类中其它应用的训练数据作为应用大类的判断依据。

加密应用的识别：加密通信协议通常包含密钥交换和密文传输两个阶段。密钥交换阶段一般传输的是明文，可以提取密码套件、证书等特征；密文传输阶段传输的是密文，可以提取通信双方的流量模式、通信模式和行为模式等统计特征。对于已知的加密应用，采集大量的加密流量用作训练样本，应用机器学习方法进行加密应用的识别。

违规代理软件的识别：违规代理软件（又称翻墙软件）通常采用 VPN 加密通道与 VPN 服务器建立连接，由 VPN 服务器代理翻墙软件访问敏感的海外网站。由于翻墙软件和 VPN 服务器之间的通信是加密的，因此容易绕过网络设备的访问控制约束。将每种翻墙软件都视为一款应用，依据上述加密应用识别方法可以识别翻墙软件。



[图 5.4 应用识别方法原理图]

5.2.3 加密恶意软件识别

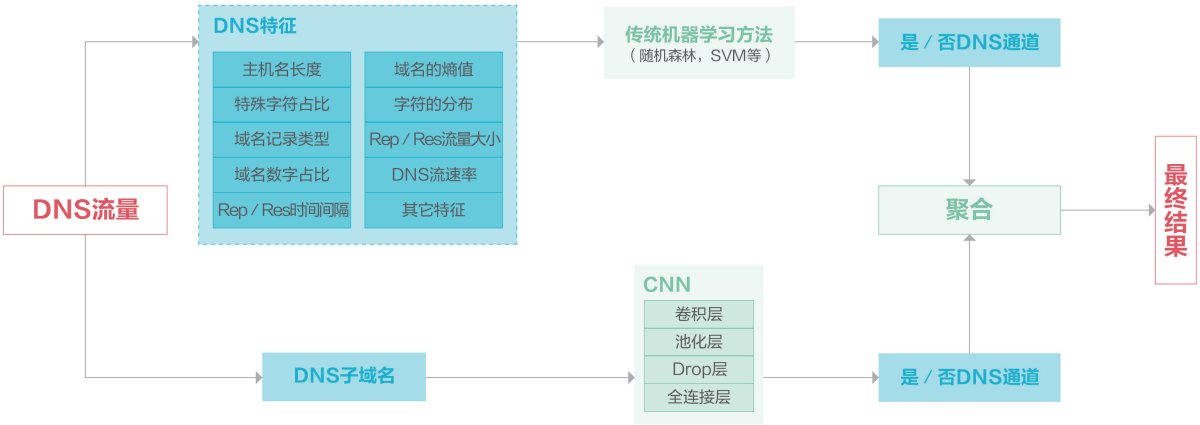
为了识别网络中的加密恶意软件，新华三 AI 防火墙基于恶意加密流量、DNS 通道、DGA 域名外连三种方式，实现了三种加密恶意软件识别方法。

恶意加密流量识别：相对于白样本而言，黑样本数量极少，并且很难获取。通过收集公开样本，购买合作伙伴数据和构建测试样本三种方法获取真实黑样本，同时采用 GAN 自动生成对抗黑样本。采用人工方式提取密钥交换阶段的明文特征和数据流的统计特征，采用 CNN 提取网络流的结构特征，采用 RNN 提取网络流的

时序特征。使用传统机器学习算法对加密流量的人工特征进行处理，用于恶意加密流量的检测；使用 GAN 生成有标记的对抗样本；使用 CNN 对加密网络流提取的图片格式进行处理，得到自动结构特征；使用 RNN 对加密网络流提取的序列格式进行处理，得到自动序列特征；使用 DNN 进行自动特征后续的恶意流量检测。

[图 5.5 恶意加密流量识别方法原理图]

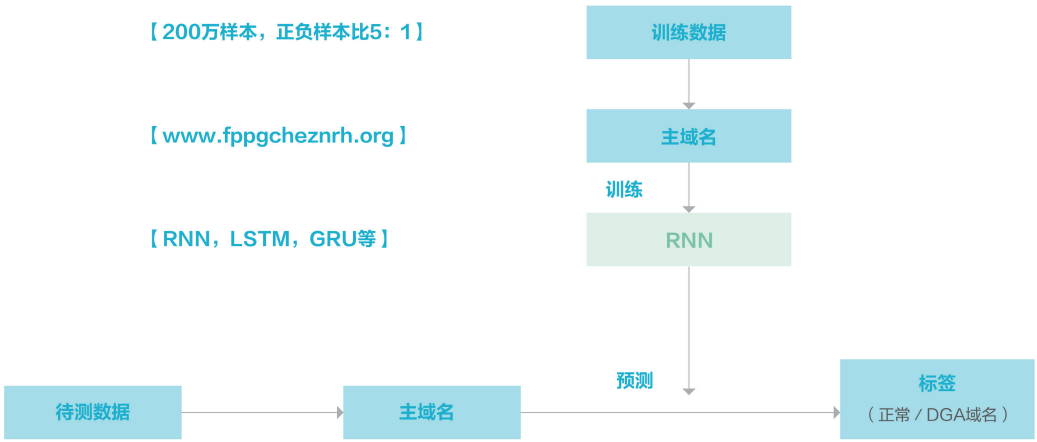
DNS 通道检测：越来越多的恶意软件采用隐蔽通道与外部主机进行通信，例如 DNS 通道。新华三 AI 防火墙对网络中的 DNS 流量进行分析，实现了基于传统机器学习算法和卷积神经网络的 DNS 通道检测方法。针对 DNS 流量，提取主机名长度、域名的熵值、特殊字符占比、字符的分布、请求 / 响应流量大小、请求 / 响应时间间隔、DNS 流速率等特征，采用随机森林、SVM 等对 DNS 流量的特征向量进行分类，从而判断该 DNS 流量是否为 DNS 通道。针对 DNS 请求中的子域名，采用一维 CNN 及相关模块对子域名进行分析，自动提取子域名中的特征，然后用全连接神经网络预测该子域名对应的 DNS 流量是否为 DNS 通道。



[图 5.6 DNS 通道检测方法原理图]

DGA 域名检测：恶意软件除了采用 DNS 通道与外部主机进行通信外，还可以通过 DGA 生成域名与

C&C 服务器建立连接并进行通信。新华三 AI 防火墙基于海量的 DGA 域名和 Alexa 正常域名，采用 RNN 算法实现 DGA 域名检测。通过分析已有的 DGA，生成大量的 DGA 域名作为黑样本，同时应用 Alexa 正常域名作为白样本。将每个主域名看作一个字符序列，采用 RNN 对主域名进行分析得到嵌入向量，然后应用全连接网络进行 DGA 域名的检测。此外，为了应对误报数据，加入了中文单词的拼音首字母组合，以及部分 DGA 为对抗检测采用的单词组合的域名生成方法等特征，实现了对 DGA 域名的准确检测。

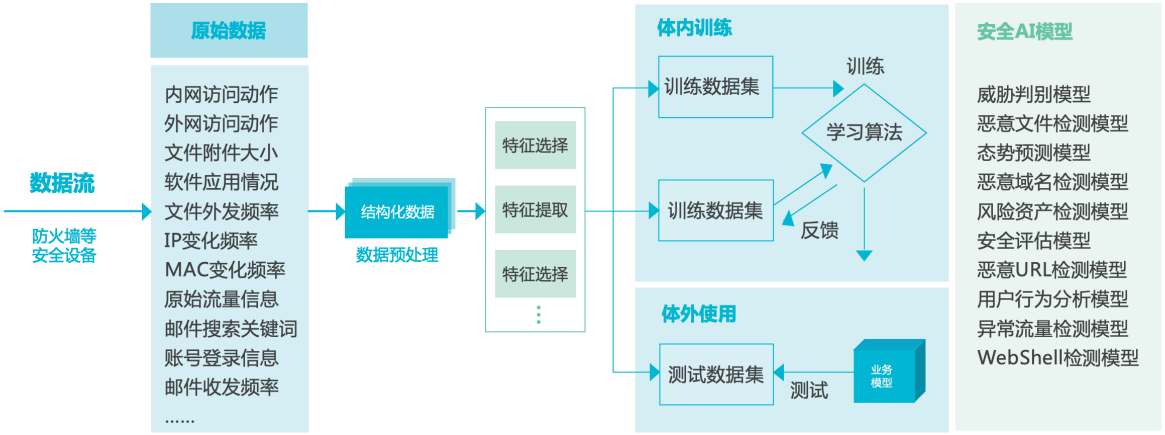


[图 5.7 DGA 域名检测方法原理图]

5.2.4. 异常流量 & 行为分析

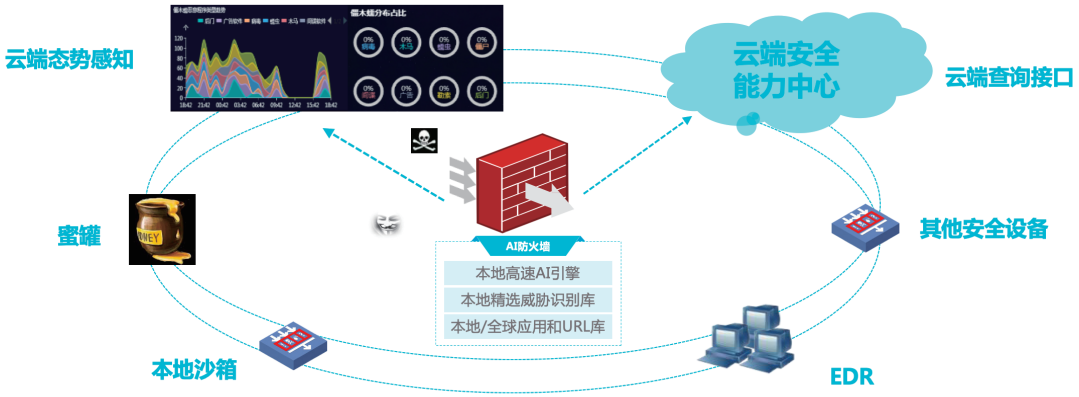
为了对抗网络安全风险，新华三 AI 防火墙对网络攻击的各个阶段进行深度的分析、检测和识别，实现了网络异常流量分析和异常行为分析。

异常流量分析：为了有效应对各类复杂高效的网络攻击，新华三 AI 防火墙提供多维度全栈分析功能，利用机器学习等人工智能算法，能够对网络攻击的各个阶段进行持续监视和关联分析，及时发现网络中的安全风险，给出告警信息。通过用户行为的持续监视，对用户行为进行智能画像，及时检测发现用户的异常行为；通过对各类异常流量训练出异常流量检测模型，检测各类隐蔽恶意流量通道，及时关闭恶意通信流量通道等；通过本地和云端沙箱进行智能行为分析，检测隐藏在应用中的各类恶意行为，及时阻止恶意应用下载等；通过云端情报综合智能分析，提升各类已知威胁、变种和未知威胁的检测能力；最后，通过将用户、应用、流量、情报等多种异常行为进行多维度关联分析，可还原整个攻击链条，同时通过云端大数据智能分析，不断优化调整识别模型，实时发现网络攻击。



[图 5.8 异常流量分析方法原理图]

异常行为分析：新一代的网络攻击仅仅依靠对流量和内容的检测识别已经不能够应对，防火墙已经开始通过本地和云端沙箱技术对各类应用的行为进行检测分析。新华三 AI 防火墙可以对各类用户进行用户行为智能画像，从而对各类合法和非授权用户进行持续行为监视和智能分析，同时通过本地和云端沙箱环境对各类应用行为进行过程监视和异常判别。用户行为智能画像可以关联应用行为智能分析结果，与网络流量和内容智能分析一起实现对各类异常行为的识别。

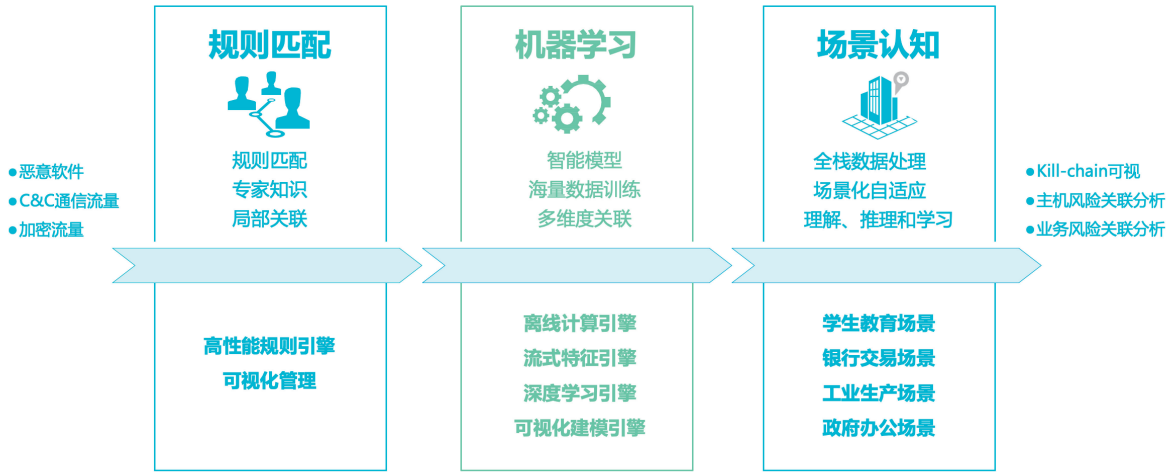


[图 5.9 异常行为分析方法架构图]

5.2.5. 智能高级威胁检测

为了检测网络中的高级威胁，新华三 AI 防火墙与安全云和态势感知相协同，实现了智能的高级威胁检测方法。

智能高级威胁检测：高级持续性威胁（APT）是有组织的，精心策划的、极具隐蔽性和耐心的网络攻击行为，这类网络攻击具有极强的隐蔽性，不易被检测发现，现有防火墙技术已经不能够有效应对。新华三 AI 防火墙通过内嵌智能本地 AI 分析引擎和云端大数据智能分析，来实现领先的高级威胁有效检测能力。高级威胁行为虽然难以被检测，但是并非无迹可寻，其行为和属性仍然具有普通恶意行为的特点，只是其各阶段的行为分布在一个广泛时间尺度范围内，使得其不容易被发现。新华三 AI 防火墙能够对各类用户行为、应用行为、网络流量和内容进行持续监视和智能分析，快速发现并记录各类恶意行为，对历史异常数据记录进行长时间多维度关联分析，还原并检测出潜在的高级威胁。



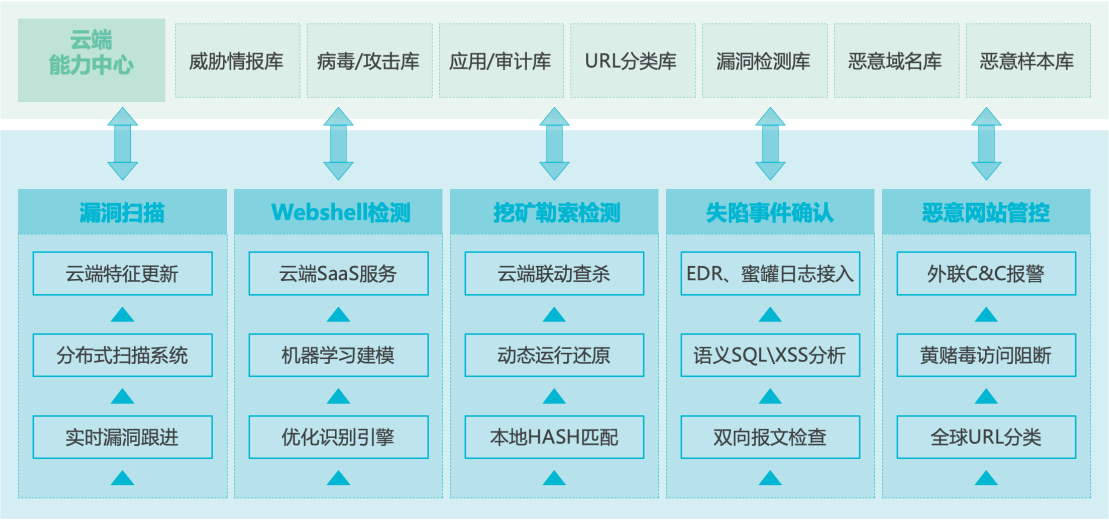
[图 5.10 智能高级威胁检测方法原理图]

5.2.6.“云 – 网 – 边 – 端”协同联动

为了构建“云 – 网 – 边 – 端”联动的一体化安全防御体系，新华三 AI 防火墙与安全云、态势感知、边缘计算等系统相结合，实现情报共享、算力提升、关联分析、协同联动等功能。

AI 防火墙与安全云平台协同联动：新华三 AI 防火墙大幅增强云端智能能力。通过云端威胁情况的共享、分析与服务，新华三 AI 防火墙可以共享所有来源的威胁情报，迅速响应各类漏洞和威胁，及时阻止各类攻击行为的传播。威胁情报不仅仅限于新华三自身搜集的情报，还包括新华三所有生态合作伙伴的威胁情报来源。

同时，新华三所有 AI 防火墙可以共享部署策略，通过云端的智能策略分析，可以为各行各业的客户提供最优的部署策略推荐，大大简化部署和运维。除此之外，本地防火墙将潜在威胁数据上传至云端，通过云端大数据分析，获取机器学习模型，再将模型参数下放到本地进行本地智能检测分析，实现云端一体化智能联动。



[图 5.11 云端能力感知结构图]

AI 防火墙与态势感知系统协同联动：为了满足多方面、多维度的安全检测需求，新华三 AI 防火墙提供多元智能感知引擎，全面提升威胁风险的检测、判断、识别、预测和告警能力。根据业务场景，在弹性智能硬件架构支持下，将机器学习引入多业务感知引擎，可以对海量的安全信息进行自动分析与深度挖掘，不同业务引擎间可模块化组合，协同完成终端可信接入、用户异常行为检测、恶意应用软件检测、加密流量免解密识别、应用流量内容识别等智能感知功能。

[图 5.12 态势感知系统感知环境层次图]

5.3. 新华三 AI 防火墙特点

5.3.1. 弹性架构

新华三 AI 防火墙采用 X86 硬件架构，业务单板支持多个 CPU 和 GPU 的弹性扩展，GPU 板卡可兼容多个厂家的 AI 扩展卡，是一种开放、可扩展的弹性架构。弹性架构便于构建开放的智能安全生态系统，可以集成各种第三方应用， 实现硬件资源的统一管理和业务功能的统一编排，最大程度满足客户业务的弹性需求，降低客户业务的部署成本。

5.3.2. AI 赋能

新华三 AI 防火墙集成了 AI 硬件与 AI 分析引擎，AI 分析引擎内置了大量人工智能算法，主要用于网络中各个安全场景的智能分析，包括: 加密和新型应用的识别，违规网络代理软件的识别，恶意软件加密流量的识别，恶意软件 DGA 域名检测和 DNS 通道检测，用户、应用和主机的行为智能分析；恶意 URL 的在线实时检测等。

5.3.3. 加密分析

新华三 AI 防火墙基于先进的加密流量分析技术，可以分析各种软件产生的加密流量。可以识别加密应用，用于加密应用的管控和加密合规性检查；可以识别 VPN、加密通道，以及其它违规代理软件，实现网页的合规访问；也可以识别出恶意软件的加密 C&C 连接，从而发现网络中的失陷主机。

5.3.4. 协同防御

新华三基于协同防御的思想，将防火墙与云端和态势感知等平台相结合，实现 AI 网络安全解决方案。云端强大的计算能力，可以解决 AI 防火墙的计算力不足问题；云端强大的数据采集和智能分析技术，可以实现威胁情报的实时更新和安全策略共享。态势感知平台通过对多源异构数据进行智能分析，可以实现安全风险全过程的检测、跟踪、展示和预测，为应急响应和溯源取证提供依据。

研究方法

资料与参考收集

- 研究网络空间安全行业 71 个细分领域，300 多家安全企业。
- 收集超过 10 家国内外防火墙安全企业调查，甄选 4 家企业详细调研。
- 涉及视频安全、移动应用安全、DLP、UTM、SIEM 等安全领域扩展调研。
- 技术参考材料超过 50 份相关材料。

法律合规与监管

- 美国、欧盟相关法律法规约 10 份。
- 国内法律、法规及监管要求超过 20 份。

数据来源与分析

- 国外：Gartner、IDC、IHS Markit 、LVD 、高盛公司发布的相关报告。
- 国内： ICS CERT、 CNVD、国家质监总局、安全企业发布的相关研究报告。

安全牛已发布报告


数据脱敏
应用指南报告


下一代防火墙 (NGFW)
应用指南报告


数字品牌保护 (DBP)
业务应用指南报告


UEBA
客户使用指南报告


数据防泄密（DLP）
应用指南报告


移动业务安全架构 (SAME)
应用指南报告


在线交互安全
应用指南


信息资产风险与合规管理 (ITARC)
应用指南报告


视频监控安全
应用指南报告


威胁情报
技术指南 • 市场指南


新一代SOC研究报告
技术指南 • 市场指南


数据库安全技术
应用指南


工控态势感知
技术指南 • 市场指南


反欺诈
技术指南


移动业务安全架构
(SAME)
技术指南


国内云安全服务和市场
调研报告
安全牛
AQNIU.COM


工业控制系统安全
技术及市场分析

垂询及订阅请联系

电话 /Tel：+86-10-51626974

邮箱 /E-mail：xurongrong@aqniu.com

安全牛网址：http://www.aqniu.com

新华三集团

杭州总部
杭州市滨江区长河路 466 号
邮编 :310052
北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编 :100102
网址：www.h3c.com

CN-173X30-20190909-BR-HZ-V1.0

垂询及订阅请联系

安全牛

电话 /Tel：+86-10-51626974

邮箱 /E-mail：xurongrong@aqniu.com

安全牛网址：http://www.aqniu.com