紫光集团 核心企业 | H3C 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

- AI 防火墙技术白皮书（以下简称为“白皮书”）为安全牛与紫光旗下新华三集团联合发布，版权为双方共有，其数据与结论谨代表双方观点。白皮书仅限于安全牛与新华三全权使用。未经双方同意审核、确认及书面授权，获得白皮书的客户不得以任何方式，在任何媒体上（包括互联网）公开引用本白皮书的观点和数据，
- 不得以任何方式将白皮书的内容提供给其他单位或个人。否则引起的一切法律后果由该客户自行承担，同时安全牛亦认为其行为侵犯了安全牛的著作权，安全牛有权依法追究其法律责任。

- 白皮书中未注明来源的所有图片、表格及文字内容的版权归安全牛与新华三所有。有侵权行为的个人、法人或其它组织，必须立即停止侵权并对其因侵权造成的一切后果承担全部责任和相应赔偿。否则安全牛将依据中华人民共和国《著作权法》、《计算机软件保护条例》等相关法律、法规追究其经济和法律责任。

- 本声明未涉及的问题参见国家有关法律法规，当本声明与国家法律法规冲突时，以国家法律法规为准。

免责声明

- 本白皮书中部分图表在标注有数据来源的情况下，版权归属原数据公司。安全牛取得数据的途径来源于厂商调研、用户调研、第三方购买、国家机构、公开资料。如不同意安全牛引用，请作者来电或来函联系，我们协调给予处理（或删除）。

- 白皮书有偿提供给限定客户，应限于客户内部使用，仅供客户在开展相关工作过程中参考。如客户引用白皮书内容进行对外使用，所产生的误解和诉讼由客户自行负责，安全牛不承担责任。

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。

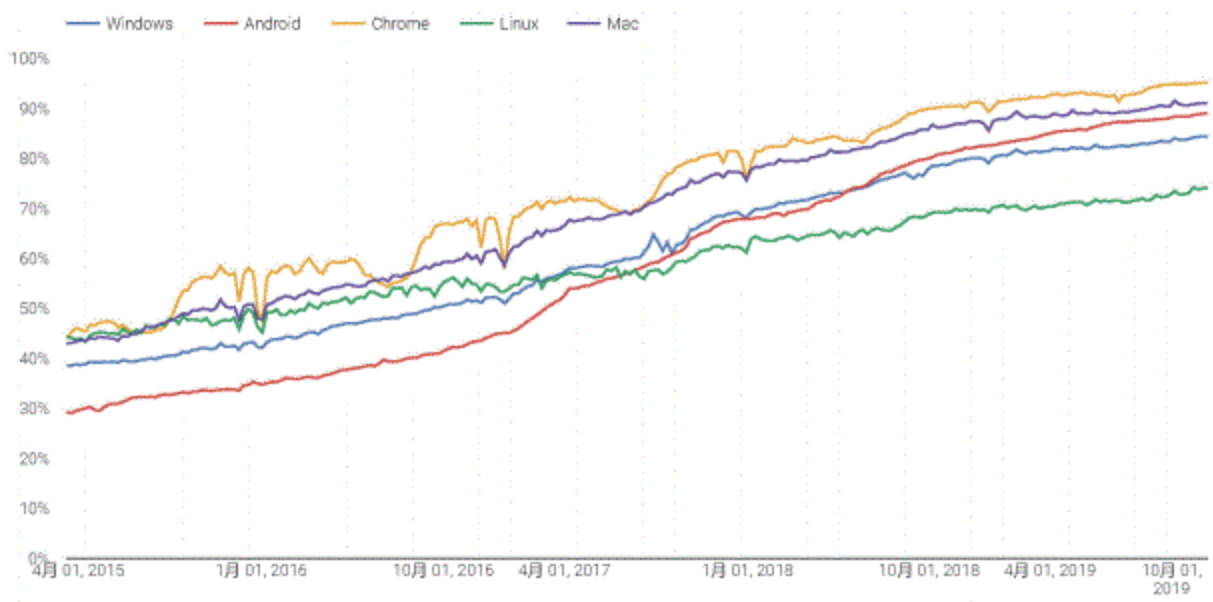
1.【产生背景】——新型网络威胁下防火墙面临的挑战

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。