安全+
SECURITY
2018/04 总第037
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

坚守在对抗DDoS攻击的第一线

绿盟ADS NX5-10000应对大流量DDoS攻击

基于SDN构建智能DDoS清洗系统

高防云清洗平台建设与运营之道

绿盟科技官方微信

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8669
传真：(010)6872 8708
网址：www.nsfocus.com

2018/04 总第 037

欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，分享您的建议和评论，或者来信nsmagazine@nsfocus.com与我们交流。

安全+ SECURITY+

© 2017 绿盟科技

本刊图片与文字未经相关版权所有人书面批准，
一概不得以任何形式、方法转载或使用。本刊保留所有版权。

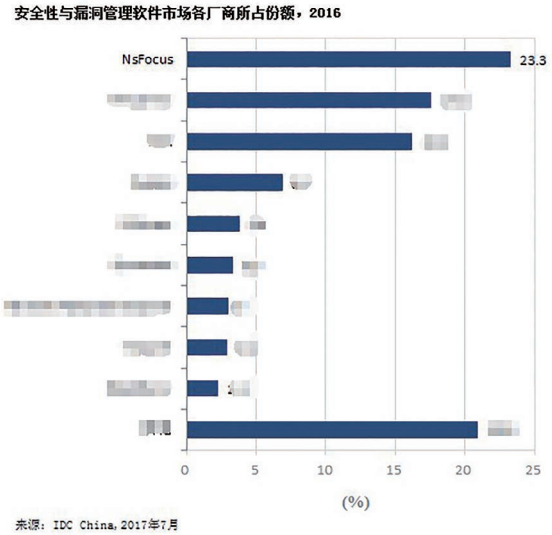
SECURITY+ 是绿盟科技的注册商标。

需要获取更多信息，请访问WWW.NSFOCUS.COM

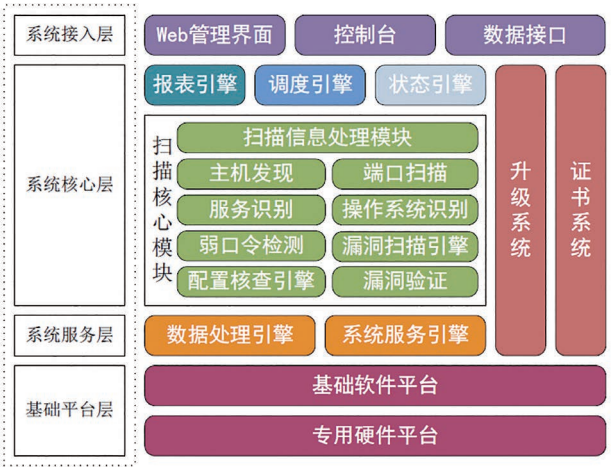
目录 CONTENTS

持续领跑
绿盟第六年蝉联漏洞管理市场第一

据 IDC 最新发布的 2016 年中国 IT 安全市场份额报告显示，绿盟科技的漏洞管理产品以 23.3% 的市场份额连续第六年领跑中国区市场。



作为国内漏洞管理市场的领导品牌，绿盟远程安全评估系统（NSFOCUS RSAS）提供准确高效的系统漏洞漏洞扫描、配置核查、web 漏洞扫描、弱口令扫描四合一功能，可部署在传统机房和虚拟化云环境，全方位满足风险合规要求。目前绿盟 RSAS 支持的系统漏洞数已超过 20000+，并依托专业的 NSFOCUS 安全小组可第一时间针对热点漏洞提供漏洞检测插件，快速帮助客户发现安全隐患。同时，为响应网络安全设备的自主可控需求，绿盟 RSAS 已实现在纯国产化 CPU 和纯国产化操作系统硬件平台上的运行，并在项目中成功实施。目前绿盟 RSAS 在金融、运营商、政府、能源等行业大

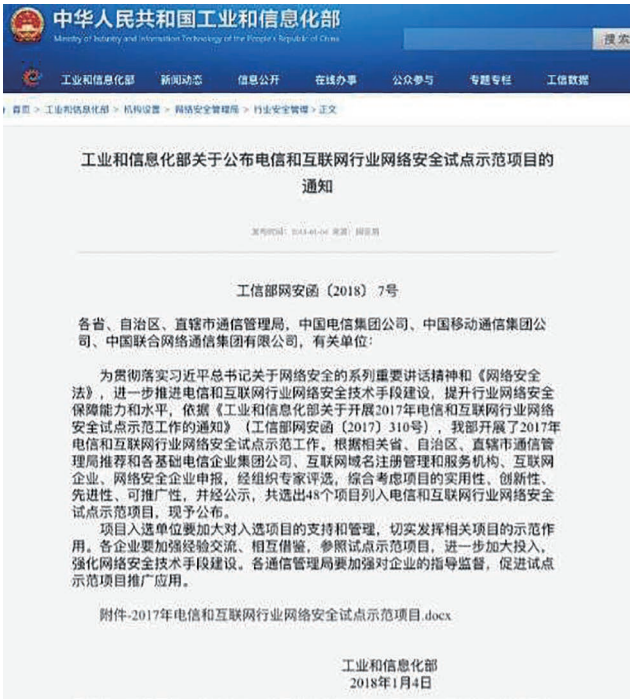


中型企业覆盖度已超过 70%，并获得客户的高度信赖和认可。

同时，针对分布式部署场景，绿盟科技创新性的推出新一代集中漏洞管理平台—基于威胁情报的绿盟威胁和漏洞管理平台（NSFOCUS TVM），跟踪分析漏洞披露事件，第一时间推送到客户侧平台，评估漏洞影响范围，协助漏洞应急响应工作，并结合对安全漏洞情报的分析，帮助客户提高漏洞加固效率，推动漏洞管理工作的落实。

工信部发布2017年网络安全试点项目，绿盟方案全部入围

近期，由工信部组织开展的“2017 年电信和互联网行业网络安全试点示范项目”已评审结束，最终从送审的 127 个项目中评审出了 48 个优秀项目，绿盟科技送审的 3 个安全解决方案项目以及与运营商客户合作的 5 个解决方案项目全部成功入选。


中华人民共和国工业和信息化部

工业和信息化部 新闻动态 信息公开 在线办事 公众参与 专题专栏 工信数据

工业和信息化部关于公布电信和互联网行业网络安全试点示范项目的通知

工信部网安函〔2018〕7号

各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司，有关单位：

为贯彻落实习近平总书记关于网络安全的系列重要讲话精神和《网络安全法》，进一步推进电信和互联网行业网络安全技术手段建设，提升行业网络安全保障能力和水平，依据《工业和信息化部关于开展2017年电信和互联网行业网络安全试点示范工作的通知》（工信部网安函〔2017〕310号），我部开展了2017年电信和互联网行业网络安全试点示范工作。根据相关省、自治区、直辖市通信管理局推荐和各基础电信企业集团公司、互联网域名注册管理和服务机构、互联网企业、网络安全企业申报，经组织专家评选，综合考虑项目的实用性、创新性、先进性、可推广性，并经公示，共选出48个项目列入电信和互联网行业网络安全试点示范项目，现予公布。

项目入选单位要加大对入选项目的支持和管理，切实发挥相关项目的示范作用。各企业要加强经验交流、相互借鉴，参照试点示范项目，进一步加大投入，强化网络安全技术手段建设。各通信管理局要加强对企业的指导监督，促进试点示范项目推广应用。

附件-2017年电信和互联网行业网络安全试点示范项目.docx

工业和信息化部
2018年1月4日

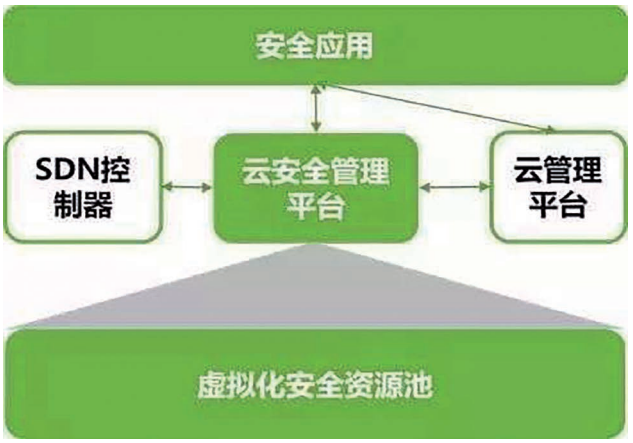
试点示范项目由工信部主导，主要目标是推广创新网络安全最佳实践，增强企业防范和应对网络安全威胁的能力，推动网络安全产业发展，提升电信和互联网行业网络安全技术防护水平。此次绿盟科技的入围，充分表明了绿盟送审项目的实用性、创新性、先进性和可推广性，以及在网络安全领域的领先优势。

绿盟科技自开启智慧安全 2.0 战略以来，不断推陈出新，提供多个在业内具备重大影响力的安全解决方案，均获得市场高度认可。本次成功入选示范项目的方案涵盖云计算、大数据、威胁漏洞管理等热门领域，已在多个行业落地为客户网络安全提供了有力的保障。

本次入围试点示范项目简介如下：

试点示范项目一：基于安全资源池的云安全服务平台

在深刻理解云计算基础上，绿盟科技开发基于虚拟安全设备的云安全平台，可以无缝融合云计算环境，为云计算租户提供自助安全服务，实现业务自动编排和能力弹性扩展。



绿盟科技的云安全方案主要由应用层，控制层和安全资源池组成。应用层为租户的自助服务入口，自行订购安全服务，实现按用户的安全业务开通和编排；控制层为云安全管理平台，对上承接应

用层业务开通指令，对下实现安全资源池的管理，通过与 SDN 控制器和云管理平台的对接完成租户流量的灵活调度，实现对南北流量和东西流量的安全防护。

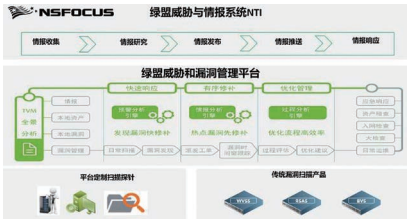
试点示范项目二：基于大数据的安全态势感知和溯源分析平台

采用大数据集中采集、分析、存储等技术，实现多维数据关联分析，应对新型复杂的安全威胁，实现对系统安全的整体展示、态势感知、攻击事件溯源及对潜在威胁的预警功能。

绿盟科技独创攻击链分析模型，完整还原整条入侵路 径，同时将机器学习算法应用到安全分析场景，对僵尸网络、蠕虫病毒、暴力破解、恶意 URL 等行为更为智能化的分析，使得分析结果更准确。

试点示范项目三：基于智能风控建模技术驱动的风险与漏洞隐患处置管理平台

结合云端专业漏洞情报和互联网资产暴露稽核能力，激活传统企业漏扫工具，建设专家级的基于智能风控建模技术驱动的风险与漏洞隐患处置管理平台一举解决安全漏洞管理和处置难的问题。同时基于漏洞威胁情报做到快速响应，基于漏洞威胁的评级做到有序推进，基于漏洞管理全流程的跟踪做



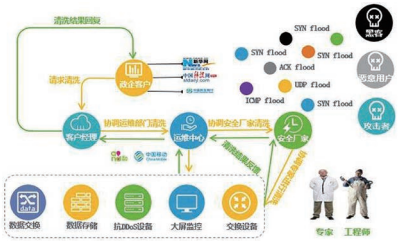
到优化管理。

不同于传统漏洞分级算法，绿盟漏洞优先级结合了威胁情报、漏洞热度、资产历史修复情况等确定漏洞在不同资产上的修复优先级，漏洞优先级会随着漏洞的情报信息和资产信息的变化而变化，贴近网络中实际漏洞修复需求。

试点示范项目四（北京移动联合申请）：基于云服务与移动互联的流量清洗统一调度处置平台

云移流量清洗平台与检测设备和清洗设备对接，实现设备统一管理，数据分析、排序、归并、整合等功能。基于移动客户端可以实现对网络流量监测、异常流量告警、事件动态告知功能，并且客户可以进行自动牵引对攻击流量进行清洗，极简运维。

北京移动通过建设云移流量清洗平台，



实现清洗设备的高效、统一管控，借助移动联网设备，实现客户自主流量清洗，为政企客户提供高水平、高质量、有偿的抗 D 安全服务，打造云移流量清洗平台及配套运营机制进一步加强北京移动的抗 D 安全保障能力。

安全服务创新联盟正式启动
绿盟科技助力中国电信共建物联网安全

2017 年 11 月 29 日，中国电信股份有限公司北京研究院（以下简称“中国电信北研院”）联合北京神州绿盟科技有限公司（以下简称“绿盟科技”）、北京安华金和科技有限公司（以下简称“安华金和”）、启明星辰信息技术有限公司（以下简称“启明星辰”）和杭州安恒信息技术有限公司（以下简称“安恒信息”），在北京举办“安全服务创新联盟暨 2017 安全帮年度发布会”，倡议发起“安全服务创新联盟”，重磅对外发布安全帮云 WAF 服务产品、2017 物联网安全研究报告、2017 数据库安全研究报告，和业界各方携手共建安全服务新生态。

“安全服务创新联盟”正式启动，
绿盟科技副总裁程斌出席并参与

中国电信集团网络运行维护事业部副总经理柏国林、中国电信北研院副院长陈运清出席发布会并致辞，参加发布会的嘉宾还有来自重要客户、互联网公司、安全公司、金融企业等 60 多家企业、高校及安全机构的代表及个人。

中国电信集团网络运行维护事业部副总经理柏国林

中国电信北研院副院长陈运清

中国电信集团网络运行维护事业部副总经理柏国林，在致辞中表示中国电信作为三大国有基础电信运营商之一，落实国家整体网络信息安全战略是义不容辞的社会责任和企业责任；中国电信将联手各方优势互补，结合自身安全能力，布局重点领域，持续推进网络和信息安全产品领域的全方位合作，为营造健康、绿色的网络环境贡献力量。

中国电信北研院副院长陈运清在致辞中表示，中国电信北京研究院作为中国电信集团的高端智库，重点聚焦网络与信息安全保障能力提升和安全服务产品研发，致力于成为中国电信安全领域技术与产品的研发及创新基地。北研院自主研发了安全帮云安全服务平台，致力于成为“SaaS 安全服务领导者”；同时积极与产业链企业联手，携手各界，齐力共建安全生态圈。

在会上，中国电信北京研究院携手绿盟科技、安华金和、启明星辰、安恒信息共同发起了“安全服务创新联盟”，以开放、协同、创新为宗旨，开展企业安全技术、产品、解决方案及标准规范的协同研究，持续深化安全服务理念创新与安全服务模式创新，不断推出满足用户需要的安全新产品和新服务，

中国电信北研院安全产品线产品总监唐洪玉

由自主创新驱动产业深度变革，逐步形成创新安全新生态。

接着，中国电信北研院安全产品线产品总监唐洪玉对“安全帮 2.0”进行了介绍，对外发布了安全帮云 WAF 安全服务产品。

会上，中国电信北研院分别与绿盟科技、安华金和发布了《2017 物联网安全研究报告》和《2017 数据库安全研究报告》，阐述了当前物联网和数据库的安全形势，剖析了物联网和数据库及数据的安全风险，给出了相应的安全防护体系和解决方案，为各企业、单位进一步加强网络和信息安全建设提供了有益的参考和借鉴。

随着万物互联时代的到来，物联网安全逐渐成为了信息安全行业的痛点，绿盟科技携手中国电信北研院为进一步加强物联网安全建设，向社会提供有关物联网安全状况的权威数据，共同发布了《2017 物联网安全研究报告》。

《2017 物联网安全研究报告》共分为四个部分：

第一部分采用分层架构思想，由底而上的分析物联网安全风险，提出各层安全需求，并对物联网典型行业应用的安全风险进行分析。

第二部分针对物联网安全状况进行分析，包括物联网资产暴露情况分析、2017 十大物联网安全事件分析、2017 十大物联网恶意软件分析，揭示物联网安全防护的必要性和紧迫性。

第三部分针对物联网安全问题，提升物联网安全总体防护水平，给出物联网安全体系架构及解决方案。

第四部分从物联网安全产业发展趋势、物联网安全新技术探索两个方面对物联网安全发展进行展望，同时给出了物联网安全建设的发展建议。

此外，绿盟科技高级安全专家进行了主

绿盟科技高级安全专家

题为“重构安全弹性的新型网络体系”的专题演讲，深入阐释了软件定义安全，探讨了如何重构安全的新型网络，为企业网络和信息安添砖加瓦、保驾护航。

绿盟科技与中国电信展开战略合作以来，为其云端安全平台的服务研发提供了全面支持，基于全套的安全态势感知服务，提供有效的安全分析模型和管理工具来融合搜集数据，可准确、高效地感知整个网络的安全状态以及发展趋势，对外部的攻击与危害行为可以及时的发现并进行应急响应，及时有效的保障信息系统安全。绿盟科技也将与中国电信携手，共同推动网络和信息安全的健康持续发展，积极营造健康发展的安全生态圈，共同开创网络和信息安全的美好未来。

绿盟云与上海联通启动云生态战略合作

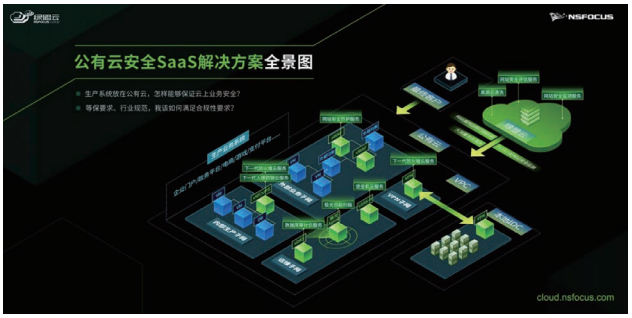
近期，上海联通云计算产品发布暨生态合作大会在全球云计算大会盛大开幕。绿盟云作为合作伙伴应邀出席，绿盟科技副总裁周凯先生参加了签约仪式并受聘成为云道学院专家。本届以“未来 • 创变——云联网”为主题的生态合作大会现场，上海联通发布了“云连接、云守护、云数聚”三大全新云产品，集中了在网络资源、数据中心、云资源池等多个层面的优势，通过自身在网络、IT、业务上的数字化转型和云化演进，携手绿盟云等 15 家云生态战略合作伙伴一起，成为企业上云的推动者、行业云业务的提供者和行业云生态的建设者。

会上，上海联通云生态重磅发布，云道学院与云道荟合作伙伴联盟正式成立。云道学院旨在汇集云计算方面的行业精英、学术专家、实践达人等，通过提供高质量的课程及分享帮助更多云计算实践人才从这里成长。绿盟科技副总裁周凯受聘成为云道学院首批专家，并分享了云计算时代企业上云方面的安全实践。

绿盟科技副总裁周凯（左一）
出席上海联通云生态战略合作签约仪式

绿盟科技副总裁周凯（右四）
受聘成为云道学院首批专家

绿盟科技副总裁周凯主题分享



绿盟云 SaaS 安全解决方案

未来，上海联通将和绿盟云将通过在云计算领域的安全合作、技术创新、行业推进方面共同为行业客户提供高品质的云计算及安全产品和服务。

同期，与上海联通云计算产品发布暨生态合作大会共舞的全球

绿盟云代表出席第四届“云鼎奖”颁奖典礼

云计算大会上，第四届云鼎奖重磅揭晓，绿盟云摘得“2016-2017 中国领先品牌”及“2016-2017 全球优秀解决方案”双料大奖。

作为每年全球云计算大会的重要项目，“云鼎奖”评选历来备受业界瞩目。此奖项旨在表彰对中国云计算做出突出贡献和具有创新精神的集体、个人或产品，进而促进云计算在中国健康、快速、有序发展，助推中国企业走向世界舞台。绿盟云凭借 17 年深耕安全领域的实践经验、中国安全技术领跑者的身份以及在云计算安全方面领先的安全创新成功摘得两个重磅奖项。

绿盟摘得“中国领先品牌”及“全球优秀解决方案”双料大奖

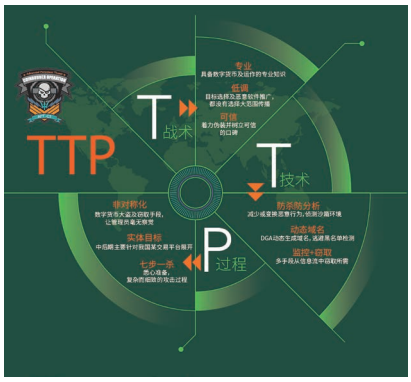
作为云安全的首倡者，绿盟云持续聚焦公有云、私有云、混合云、行业云安全，以“安全即服务（Sec-aaS）”“平台 + 生态”推进云安全落地，助力各行业用户实现业务云化转型。目前，绿盟云已经和 AWS、微软 Azure、阿里云、腾讯云、华为云等一大批国内外主流公有云达成合作，共同构建网络安全服务生态体系。

境外APT-C1组织攻击我国某互金平台

2018/01/02，绿盟科技发布报告《互金大盗背后的高级威胁组织 APT-C1》。报告首次发现并命名了境外 APT-C1 组织，他们利用“互金大盗”恶意软件攻击我国某互金平台，导致平台数字资产被窃，损失高达 150 万美元。

APT-C1 组织攻击我国互金平台

在整个攻击事件中，攻击者在战术、技术及过程三个方面（TTP）表现出高级威胁的特征，包括高度目的性、高度隐蔽性、高度危害性、高度复合性、目标实体化及攻击非对称化，在国际网络安全领域通常使用这些特征，来标识及识别高级持续性威胁（APT）攻击，同时由于其攻击主要针对我国互联网金融领域，因此将其命名为 APT-C1。

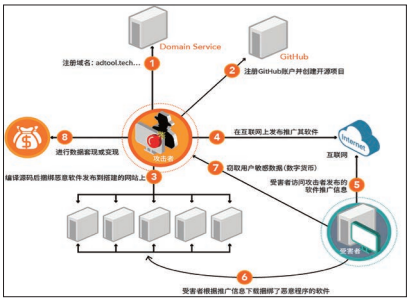


进一步分析显示，APT-C1 组织开发的“互金大盗”，从 2015 年 5 月开始，逐步聚焦到互联网金融领域，并不断收集捕获包括比特币、莱特币、以太坊、比特币现金在内的 12 种数字资产、22 个第三方钱包、8 个交易平台的敏感文件。当发现入侵目标后（我国某互联网金融交易平台），即展开持续进攻，直至进入该平台窃取凭证后，转移 150 万美元的数字资产。

APT-C1 的进攻战术隐蔽且危害性大

与其它高级威胁攻击不同，APT-C1 组织清楚的认识到，在面对互联网金融这样的大资金交易平台时，如果采用大规模感染且自动化攻击的形式，容易引起警觉很难奏效。故而攻击者长期活跃在互金社 区解答用户问题，尤其关注互金平台管理员的痛点，然后有针对性的设置“诱饵”，将“互金大盗”恶意软件捆绑到管理员工具上，并在有限范围内扩散。一旦有“鱼”上钩，就展开有针对性的攻击。

在目前发现的单个案例中，已经成功转移了数字资产，在更大范围的相关托管机构还有可能发生更为严重的“币池”资产转移，一旦投资者托管的钱包和密钥被窃取，将导致大规模数字资产失窃。目前，绿盟威胁情报中心捕获到“互金大盗”恶意软件的 29



个样本，相关域名 5 个，而这些样本在国际通行的 60 个防病毒引擎中，只有两个能察觉到。

有效应对互金大盗的攻击

APT-C1 组织的攻击较为复杂，但针对其目前使用的“互金大盗”恶意软件，绿盟威胁情报中心 NTI 已经具备了防御能力，并持续追踪相关威胁情报，客户登录该平台即可实时查询相关信息。在 NTI 支持下，还可以利用绿盟入侵防御系统 NIPS 进行网络边界防护，并利用绿盟威胁分析系统 TAC 进行内部网络的检测。

网络安全威胁月报 2017.12

关键词：高危漏洞 DDoS 攻击事件 安全会议 绿盟科技漏洞库 绿盟科技博客

摘要：绿盟科技网络安全威胁周报及月报系列，旨在简单而快速有效的传递安全威胁态势，呈现重点安全漏洞、安全事件、安全技术。获取最新的威胁月报，请访问绿盟科技博客 http://blog.nsfocus.net/

一、2017 年 12 月数据统计

1.1 高危漏洞发展趋势

2017 年 12 月绿盟科技安全漏洞库共收录 177 个漏洞，其中高危漏洞 17 个，微软高危漏洞 11 个，12 月监测到 CVE 公布高危漏洞数量为 257 个。

1.2 互联网安全漏洞

激活工具 KMSpico 内含挖矿病毒事件的分析

来源：http://blog.nsfocus.net/kmspico/

简述：近日有安全公司发布预警称“知名激活工具 KMSpico 内含挖矿病毒”，笔者对相应事件进行一番跟踪分析后发现，原作者的官方版本并不含挖矿病毒。

Weblogic WLS 组件漏洞技术分析与防护方案

来源：http://blog.nsfocus.net/weblogic-vulnerability/

简述：近日，绿盟科技应急响应团队也陆续接到来自金融、运营商及互联网等多个行业的客户的安全事件的反馈，发现 Weblogic 主机被攻击者植入恶意程序，经分析，攻击者利用 Weblogic WLS 组件漏洞 (CVE-2017-10271)，构造 payload 下载并执行虚拟币挖矿程序，对 Weblogic 中间件主机进行攻击。

美加州选民 1900 多万条信息泄露 4G 多数据包含公民个人敏感信息

来源：http://toutiao.secjia.com/california-voter-databreach

简述：一个新的、无保护的 MongoDB 数据库被发现了，内含 4G 多 1900 多万条加利福尼亚选民信息，包括每个注册选民的数据。这起事故与今年已被报道的多起选民 数据泄露 事故一样。Mongodb 数据库相关的安全问题，今年已经出现过多次。

19-YEAR-OLD TLS VULNERABILITY WEAKENS MODERN WEBSITE CRYPTO

来　源：https://threatpost.com/19-year-old-tls-vulnerability-weakens-modern-website-crypto/129158/

简述：A vulnerability called ROBOT, first identified in 1998, has resurfaced. Impacted are leading websites ranging from Facebook to Paypal, which are vulnerable to attackers that could decrypt encrypted data and sign communications using the sites' own private encryption key。

Imgur—Popular Image Sharing Site Was Hacked In 2014; Passwords Compromised

来　源：https://thehackernews.com/2017/11/imgur-data-breach.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29

简述：20 日，安全加转载 多地高校国家奖学金名单公示，泄露学生个人信息包括身份证号码 。很多人不以为然，表示“学校历来如此，还要你搞技术的提醒？”但教育部还是重视学生个人数据泄露这个事情的。

VMWare 两个高危任意代码执行漏洞 CVE-2017-4941/33 CVSS 9 分

来源：http://toutiao.secjia.com/vmware-cve-2017-4941-33

简 述：VMWare 发 布 了 6 个 补 丁， 分 别 是 针 对 ESXi, Workstations12.5.8 版，Fusion8.5.9 版以及 vCSA6.5 U1d。攻击者利用其中一些 VMware 漏洞，可以执行任意代码。其中 4 个高危漏洞的 CVE 分别是 CVE-2017-4941、CVE-2017-4933、CVE-2017-4940、CVE-2017-4943，用户请尽快安装补丁。

Samba 信息泄露漏洞 CVE-2017-15275 同时留意 CVE-2017-14746

来源：http://toutiao.secjia.com/samba-idv-cve-2017-15275

简述：上月，Samba 爆出任意代码执行漏洞 CVE-2017-14746 这个 Samba 信息泄露漏洞 是与其伴生的漏洞，攻击者可以利用这个问题获取潜在的敏感信息，获得的信息可能有助于进一步攻击。CVEID CVE-2017-15275， 只 有 Samba Samba 4.7.3 、Samba Samba 4.6.11 、Samba Samba 4.5.15 不受影响。

GoAhead httpd2.5 to 3.5 LD_PRELOAD 远程代码执行漏洞（CVE-2017-17562)

来源：http://blog.nsfocus.net/cve-2017-17562-3/

简述：GoAhead Web Server 被爆出在 3.6.5 之前的所有版本中存在一个远程代码执行漏洞（CVE-2017-17562）。该漏洞源于使用不受信任的 HTTP 请求参数初始化分叉 CGI 脚本环境，并且会影响所有启用了动态链接可执行文件（CGI 脚本）支持的用户。当与

glibc 动态链接器结合使用时，使用特殊变量（如 LD_PRELOAD）就可以实施远程代码执行。2017 年 12 月 18 日针对该漏洞利用的 PoC 公开，请受影响的用户及时更新版本进行修复。

Apache Synapse 远程代码执行漏洞（CVE-2017-15708）

来源：http://blog.nsfocus.net/cve-2017-15708/

简述：Apache Synapse 发布了新版本修复了一个远程代码执行漏洞（CVE-2017-15708）。该漏洞源于 Apache Commons Collections 组件，攻击者可以通过注入特制的序列化对象来远程执行代码。

Fastjson autotype 远程代码执行漏洞

来源：http://blog.nsfocus.net/cve-2017-15708/

简述：Fastjson 于今年 3 月份曝出一个远程代码执行漏洞，官方随后通过默认关闭 autotype 功能和开启黑名单解决了该漏洞，但近日有研究人员发现该黑名单存在一定限制，在开启 autotype 功能后可以通过改变相关类名来绕过黑名单，从而实现远程代码执行。

Microsoft Malware Protection Engine 远程代码执行漏洞

来源：http://blog.nsfocus.net/cve-2017-11937/

简述：北京时间 12 月 7 日，微软官方发布了一则通告表示其恶意软件防护引擎（Malware Protection Engine）存在一个远程代码执行漏洞（CVE-2017-11937）。

（来源：绿盟科技威胁情报与网络安全实验室）

1.3 绿盟科技漏洞库十大漏洞

声明：本十大安全漏洞由 NSFOCUS（绿盟科技）安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。

http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2017-12-22 Microsoft Malware Protection Engine 远程代码执行漏洞（CVE-2017-11937）

NSFOCUS ID: 38472

链接 :http://www.nsfocus.net/vulndb/38472

综述 :Microsoft Malware Protection Engine 是恶意程序保护引擎。Microsoft Malware Protection Engine 未正确扫描构造的文件，在实现上存在内存破坏安全漏洞。

危害 : 本地攻击者可以在 LocalSystem 帐户安全上下文中执行任意代码，控制系统

2. 2017-12-20 Linksys WVBR0-25 远程命令注入漏洞（CVE-2017-17411）

NSFOCUS ID: 38446

链接 :http://www.nsfocus.net/vulndb/38446

综述 :Linksys 是思科系统一个销售家用与小型业务用网络产品的部门。Linksys WVBR0-25 在实现上存在远程命令注入漏洞，成功利用后可使攻击者在受影响设备上下文中执行任意命令。

危害 : 远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，从而控制服务器

3. 2017-12-14 Adobe Reader/Acrobat 缓冲区溢出信息泄露漏洞 (CVE-2017-16370)

NSFOCUS ID: 38372

链接 :http://www.nsfocus.net/vulndb/38372

综述 :Adobe Reader 是 PDF 文档阅读软件。Acrobat 是 PDF 文档编辑软件。Adobe Acrobat/Reader 多个版本在实现上存在缓冲区溢出漏洞，可使攻击者利用此漏洞通过无效的指针偏移，获取敏感数据。

危害 : 攻击者可以通过诱使受害者打开恶意 pdf 文件来利用此漏洞，从而控制受害者系统

4. 2017-12-18 Google Chrome 63.0.3239.108 之前版本多个安全漏洞（CVE-2017-15429）

NSFOCUS ID: 3842

链接 :http://www.nsfocus.net/vulndb/38428

综述 :Google Chrome 是由 Google 开发的一款 Web 浏览工具。Chrome 63.0.3239.108 之前版本在实现上存在多个安全漏洞。

危害 : 远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统

5. 2017-12-14 Adobe Flash Player 远程安全漏洞 (CVE-2017-11305)

NSFOCUS ID: 38380

链接 :http://www.nsfocus.net/vulndb/38380

综述 :Flash Player 是多媒体程序播放器。Adobe Flash Player 27.0.0.187 及之前版本存在回归问题，用户清除浏览器数据时，会造成全局设置文件重置。

危害 : 攻击者可以通过诱使受害者打开恶意 swf 文件来利用此漏洞，从而控制受害者系统

6. 2017-12-13 Microsoft Edge 远程内存破坏漏洞（CVE-2017-11908）

NSFOCUS ID: 38345

链接 :http://www.nsfocus.net/vulndb/38345

综述 :Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。Windows 10 1709/ChakraCore 由于脚本引擎处理内存对象方式不当，在实现上存在安全漏洞。

危害 : 远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统

7. 2017-12-12 Google Android Media Framework 组件多个安全漏洞

NSFOCUS ID: 38307

链接 :http://www.nsfocus.net/vulndb/38307

综述 :Android 是基于 Linux 开放性内核的手机操作系统。Google Android 在实现上存在多个安全漏洞。

危害 : 攻击者利用此漏洞可获取提升的权限，执行任意代码，拒绝服务攻击

8. 2017-12-22 VMware 多个产品远程栈溢出漏洞（CVE-2017-4941）

NSFOCUS ID: 38468

链接 :http://www.nsfocus.net/vulndb/38468

综述:VMware Workstation 是一款功能强大的桌面虚拟计算机。

VMware ESXi/Workstation/Fusion 在实现上存在栈溢出安全漏洞。

危害：攻击者可以通过特定的 VNC 数据包组，造成栈溢出，在虚拟机中执行远程代码

9. 2017-12-22 Trend Micro Encryption for Email 远程代码执行漏洞（CVE-2017-11397）

NSFOCUS ID: 38465

链接 :http://www.nsfocus.net/vulndb/38465

综述 :Trend Micro Encryption for Email 是电子邮件加密解决方案。Trend Micro Encryption for Email 5.6 及更早版本在实现上存在服务 DLL 预加载漏洞。

危害：未经身份验证的远程攻击者可以在系统上执行任意代码

10. 2017-11-27 Joomla! 'com_tag' SQL 注入漏洞（CVE-2017-15946）

NSFOCUS ID: 38094

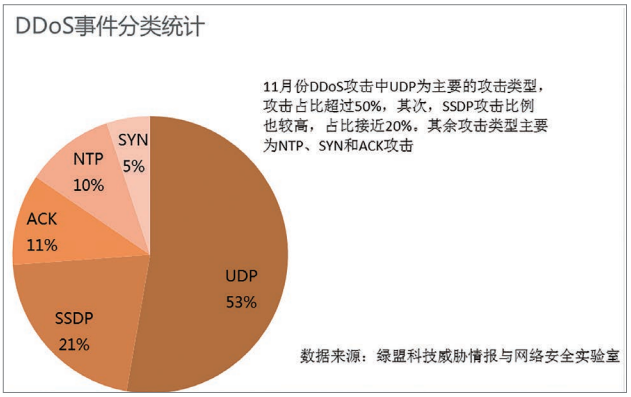
链接 :http://www.nsfocus.net/vulndb/38094

综述 :Joomla 是内容管理系统。Joomla! 'com_tag' 组件在实现上存在 SQL 注入漏洞，攻击者利用此漏洞可访问或修改数据，利用下层数据库的其他漏洞。

危害：远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，对服务器进行非授权的访问。

1.4 DDoS 攻击类型

12 月份绿盟科技科技威胁情报及网络安全实验室收集及梳理了近 6148 次攻击，与 11 月份相比，攻击次数明显降低，这个月的攻击类型分布来看，UDP 为最主要的攻击类型，其次 SSDP 攻击占都在 20% 左右，ACK、NTP、SYN 比例相对较低。



小提示

- Chargen Flood：Chargen 字符发生器协议（Character Generator Protocol）是一种简单网络协议，设计的目的是用来调试 TCP 或 UDP 协议程序、测量连接的带宽或进行 QoS 的微调等。但这个协议并没有严格的访问控制和流量控制机制。流量放大程度在不同的操作系统上有所不同。有记录称，这种攻击类型最大放大倍数是 358.8 倍。

- NTP Flood：又称 NTP Reply Flood Attack，是一种利用网络中时间服务器的脆弱性（无认证，不等价数据交换，UDP 协议），来进行 DDoS 行为的攻击类型。有记录称，这种攻击类型最大放大倍数是 556.9 倍。

- SSDP Flood：智能设备普遍采用 UPnP（即插即用）协议作为网络通讯协议，而 UPnP 设备的相互发现及感知是通过 SSDP 协议（简单服务发现协议）进行的。

攻击者伪造了发现请求，伪装被害者 IP 地址向互联网上大量的智能设备发起 SSDP 请求，结果被害者就收到了大量智能设备返回的数据，被攻击了。有记录称，这种攻击类型最大放大倍数是 30.8 倍。

更多相关信息，请关注绿盟科技 DDoS 威胁报告。

二、博文精选

OWASP TOP 10 2017 | 最新十大 WEB 安全风险你都 GET 到了吗?

近几年，云、大数据、物联网、人工智能等技术广泛应用，软件开发过程引入敏捷开发和 DevOps 实现开发运维工作自动化、版本快速迭代。迅速扩张的攻击面也伴随而来，攻击者总是能找到新的攻击面。在此背景下，时隔 4 年我们再次迎来 OWASP Top 10（十大 Web 应用安全风险）的正式更新。

http://blog.nsfocus.net/owasp-top-10-2017/

恶意样本分析手册——通讯篇

传统的恶意软件一般会采用基于 TCP/UDP 的自定义协议进行通 讯，在此基础上还有利用 HTTP/HTTPS，IRC，P2P 等其他应用层协议 来进行通讯的。一般来说在调试网络通信的过程中，无论恶意软件采用何种协议均对我们所关注的内容无太多影响，只需要获取到对应的 网络通信数据即可，而且在调试方法上基本无差别，故我们将以调试 利用 TCP 通信的样本为例，讲述如何调试样本中的网络通信部分。对 于其他常见的应用层协议，我们将对其网络结构及相关的僵尸网络构 建方式和方法进行简单描述，便于读者理解

http://blog.nsfocus.net/msartele/

2017 物联网安全研究报告

中国电信安全帮携手绿盟科技联合发布《2017 物联网安全研究报告》，旨在进一步加强物联网安全建设，向社会提供有关物联网安全状况的权威数据。

http://blog.nsfocus.net/iot-security-report-2017

（来源：绿盟科技博客）

三、安全会议

安全会议是从近期召开的若干信息安全会议中选出，仅供参考。

FloCon 2018

时间：January 8-11, 2018

简介：FloCon 论坛旨在从安全运营的角度，探索大规模的下一代数据分析。FloCon 面向业务分析人员、工具开发商、研究人员、安全专业人员，以及其他有兴趣应用尖端技术分析和可视化大型数据集，进行网络系统保护和防御的专业人士。

网址：https://resources.sei.cmu.edu/news-events/events/flocon/

2017上半年Web应用攻击态势报告

潘文欣 孙叶 彭元 何坤

关键词：web 应用攻击 web 攻击方法 web 应用攻击类型 web 应用攻击防范

摘要：本文摘自《2017上半年 DDoS 与 Web 应用攻击态势报告》，由于原报告较长，本文此次主要介绍 Web 应用攻击态势。绿盟威胁情报中心 NTI 对所有攻击源 IP 的攻击广度进行了分析，发现有 19.6% 的 IP 曾经对 2 个及以上的 Web 站点发起过攻击；有 3.3% 的攻击源 IP 曾对 10 个或更多的 Web 站点发起过攻击；只攻击过一个 Web 站点的 IP 占 80.4%。

一、2017 上半年 Web 应用攻击态势

1.1 Web 应用攻击类型分析

根据我们的统计，2017上半年，针对 Web 应用的攻击占比如下图所示，其中 SQL 注入攻击占比最高，达 40.8%。其次是已知 Web 漏洞攻击，占比 24.3%。第三位是路径穿越攻击，占比 9.9%。

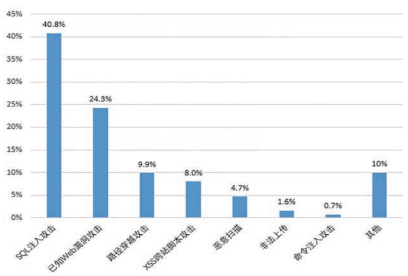


图 1.1 针对 Web 应用的各类攻击攻击次数占比

数据来源：绿盟科技可管理安全服务（MSS）

1.2 被攻击与未被攻击站点比例

2017上半年我们保护的站点中，曾遭受到 Web 应用攻击的站点达到 82%。其中已知 Web 漏洞攻击的攻击范围最广，有 79.3% 的站点遭受了已知 Web 漏洞攻击。其次是路径穿越和 SQL 注入攻击，被攻击站点率分别为 45.9% 和 44.3%。

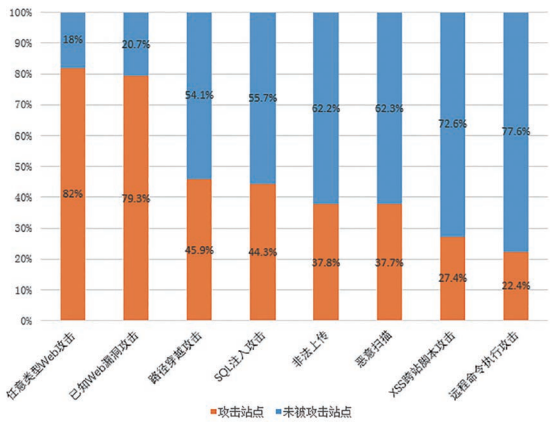


图 1.2 被攻击与未被攻击的 Web 站点比例

数据来源：绿盟科技可管理安全服务（MSS）

1.3 攻击源情况分析

1.3.1 攻击源 IP 攻击广度与其 IP 信誉

我们对所有攻击源 IP 的攻击广度进行了分析，发现有 19.6% 的 IP 曾经对 2 个及以上的 Web 站点发起过攻击；有 3.3% 的攻击源 IP 曾对 10 个或更多的 Web 站点发起过攻击；只攻击过一个 Web 站点的 IP 占 80.4%。

结合 NSFOCUS 威胁情报中心（NTI）信誉数据进行分析，发现攻击过 1 个站点的攻击源 IP 中，有 12% 的攻击源 IP 在 NTI 上有不良 IP 信誉记录，其中被标识为中、高危的占 55.2%；攻击过多个（2 个及以上）Web 站点的攻击源 IP 中，有 74.3% 的攻击源 IP 在 NTI 上有不良 IP 信誉记录，这部分源中被标识为中、高危的占比为 74.2%。表明攻击源 IP 攻击广度越高，攻击源活跃度越高，在 NTI 上被标识为异常的概率越大，属于高级别威胁的概率也越大。

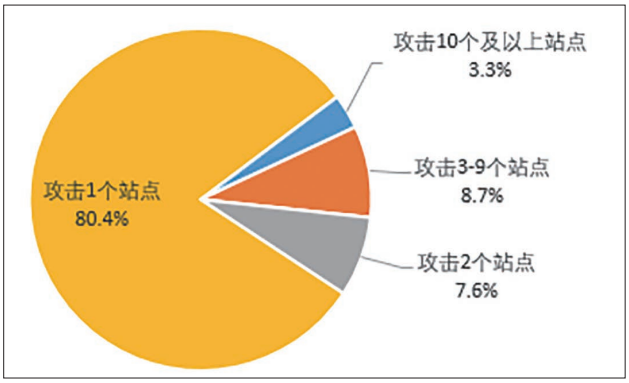


图 1.3 攻击源 IP 攻击广度

数据来源：绿盟科技威胁情报中心（NTI）

1.3.2 攻击源主机所在中国地区占比

攻击源主机数量在中国地区的分布情况如下图所示，沿海地区和发达地区的攻击源较多，山东、北京、天津排前三，分别占 22.3%、13.8%、13.8%。

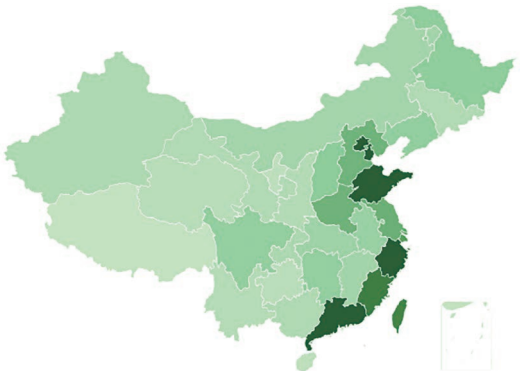


图 1.4 攻击源主机数中国地区分布

攻击源在中国地区的占比 Top 10 如下所示。

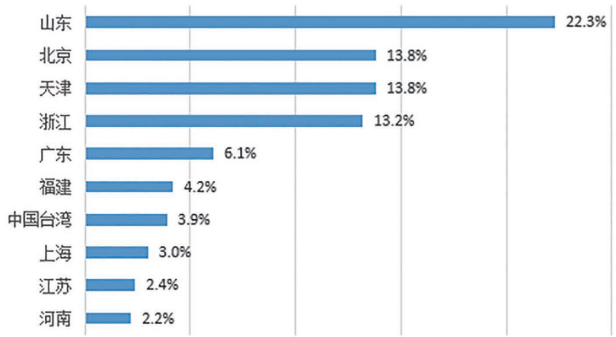


图 1.5 攻击源主机数中国地区 Top 10 占比

数据来源：绿盟科技可管理安全服务（MSS）

1.4.1 注入类攻击常见 Payload 注入位置

很多 Web 攻击者精心构造 HTTP 攻击报文，将其尽可能的伪装成正常请求并发送给攻击目标，使得目标服务器按照非正常流程运行，以达到获得系统或服务器敏感信息、上传恶意文件等目的。如 SQL 注入、路径穿越、XSS 跨站脚本、命令行注入等攻击，这些攻击最常见的攻击插入位置如下图所示，其中 URL 中的参数列表是黑客最喜欢插入攻击语句的地方，这种情况占全部攻击插入或修改位置的 47.3%。其次是 Cookie，占比 45.1%，剩下的是在 URI 处。

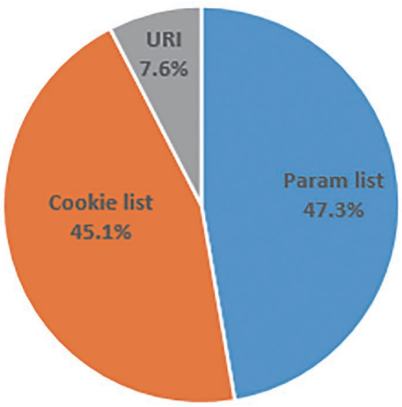


图 1.6 注入类攻击常见 Payload 注入位置

数据来源：绿盟科技可管理安全服务（MSS）

1.4.2 利用已知 Web 漏洞的攻击

在信息化的时代，企业的商业风险与其关键业务的 Web 安全威胁息息相关。而 Web 面临的安全威胁随着企业 Web 应用的数量和 Web 应用包含的漏洞数增加而迅速增加。

我们这里所说的已知漏洞包含 Web 服务器漏洞和 Web 构件漏洞。Web 服务器漏洞主要存在于 Web 服务器程序中，如：IIS、Apache、Nginx、Tomcat、lighttpd；Web 构件漏洞主要集中在 Web 应用或重要的 Web 开发框架中，如：Struts、WordPress、phpBB、EmpireCMS、Xoops、Discuz!、ShopEx、vBulletin、phpcms、ECSHOP、DedeCms、phpMyAdmin、PHPWind、Php168 以上几种使用频率比较高的论坛、cms 系统等 Web 程序。

2017 上半年，针对 Web 应用发起的攻击中利用已知 Web 相关漏洞的 Top 10 如下图所示，我们分类进行展示：

这些漏洞中，1 个为中级漏洞，其余 9 个均为高危漏洞。很多漏洞都是几年前的漏洞，但利用率仍然很高。

从图中也可看出，今年上半年针对 Web 应用的攻击利用已知漏洞 Top 10 中，Apache Struts2 相关漏洞是被利用最多的漏洞，占

全部已知漏洞 Top10 的 58.7%。Apache Struts2 是世界上最流行的 Java Web 服务器框架之一，被广泛用于政府、企业组织、金融等行业的门户网站的底层模版建设，一旦出现漏洞，影响甚广。

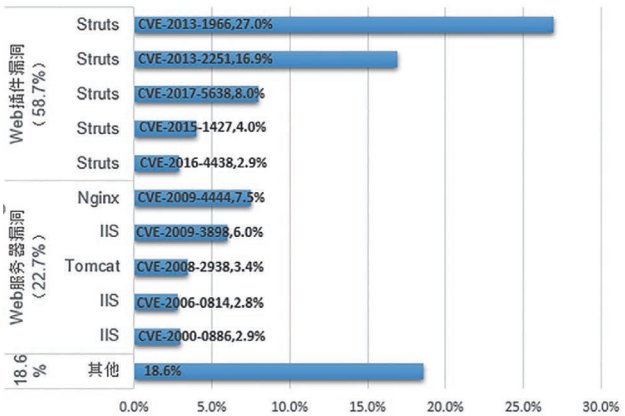


图 1.7 Web 应用攻击利用漏洞 Top 10

数据来源：绿盟科技可管理安全服务（MSS）

数据侵入系统。2017上半年，我们统计 SQL 注入攻击中黑客最常使用的 SQL 注入 Payload Top 10 如下图所示。

1、or *=* 的插入语句最为常用，占全部攻击 Payload 的

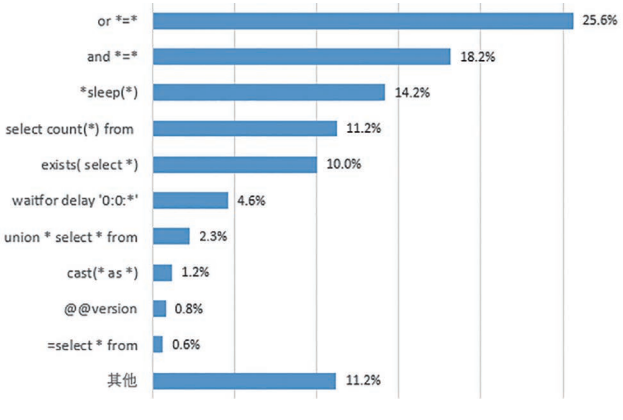


图 1.8 SQL 注入常见攻击 Payload Top 10

数据来源：绿盟科技可管理安全服务（MSS）

1.4.3 SQL 注入攻击常见 Payload

所谓 SQL 注入，是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。具体来说，它是利用现有应用程序，将恶意的 SQL 命令注入到后台数据库引擎执行，它可以通过在 Web 表单中输入恶意 SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。

其主要原因是程序没有细致地过滤用户输入的数据，致使非法

25.6%，比如：or 53=3，OR 53=35 ,OR 53=4 等均合并到此项中。其次是 and *=* ，占比达 18.2%，例如：and 1=1，and 1=2 等都合并到这个项中。

2、*sleep(*) 占比 14.2%，例如：(sleep(2);--, select pg_sleep(5)-- 等类似的语句都合并在这个选项中，常用于 MySQL、PostgreSQL 数据库基于时间的盲注，waitfor delay’ 0:0:x’ 也是这个作用，常用于 MSSQL 数据库基于时间的盲注。

3、select count(*) from，占比为 11.2%，在 SQL 注入中，常

与其他语句结合使用，用于判断某个表是否存在，或者猜测某个字段长度，猜测某个字符。

SQL 注入 Top 3 攻击 Payload 都是用于判断系统是否含有 SQL 注入漏洞的，发生在攻击初期对系统漏洞是否存在的探测踩点阶段。

1.4.4 路径穿越攻击常见 Payload

路径穿越攻击是指服务端对用户输入检查不严密，在涉及到文件路径操作时攻击者有可能利用绝对或相对路径来获取服务端关键路径访问的权限，造成攻击者获取服务端的敏感信息或系统的控制权限等。

我们统计了路径穿越攻击中常见的路径 Top 排名，如下图所示。所示。

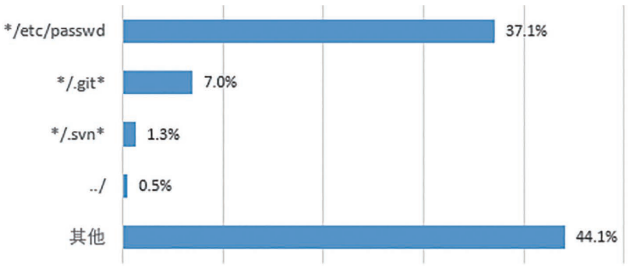


图 1.9 路径穿越攻击中常见的路径

数据来源：绿盟科技可管理安全服务（MSS）

1、*/etc/passwd 在路径穿越攻击中使用最多，占比 37.1%。在 linux 系统中，/etc/passwd 文件记录了每个用户的一些基本属性。系统管理员经常会接触到这个文件的修改以完成对用户的管理工作。这个文件对所有用户都是可读的。攻击者可以从这个文件中获取到系统的用户信息，从而加以利用。

2、其次是 */.git*，占 7.0%。Github 是开源代码库以及版本控制系统，随着越来越多的应用程序转移到了云上，Github 已经成为了管理软件开发以及获取已有代码的首选方法。.gitignore 文件是 Git 项目中用于指定哪些文件要忽略。攻击者尝试从 /git 目录下获取或修改服务端源代码或 .gitignore 文件。

3、*/.svn* 在路径穿越攻击中排名第三，占 1.3%。SVN 是 Subversion 的简称，是一个开放源代码的版本控制系统，多个人共同开发同一个项目，以达到共用资源的目的。攻击者企图通过 */.svn* 目录获取或修改服务端的资源（包括源代码）。

4、../ 在路径穿越攻击中排名第四，占 0.5%。意思是回到上一层目录，攻击者可利用相对路径进行路径穿越。

1.4.5 XSS 攻击常见 Payload

XSS 全称为 Cross Site Scripting，即跨站脚本，发生在目标网站中目标用户的浏览器层面上，当用户浏览器渲染整个 HTML 文档的过程中出现了不被预期的脚本指令并执行时，XSS 就会发生。XSS 攻击是应用层常见的典型攻击类型，攻击者可提交精心构造的 XSS 攻击代码，在页面嵌入 HTML、JS 代码，使用户的浏览器端出现恶意的 HTML 元素或执行恶意的 JS 脚本，达到窃取用户 cookie、控制用户动作等特殊目的。

我们统计了 XSS 攻击中常见的攻击 Payload Top 10，如下图所示。

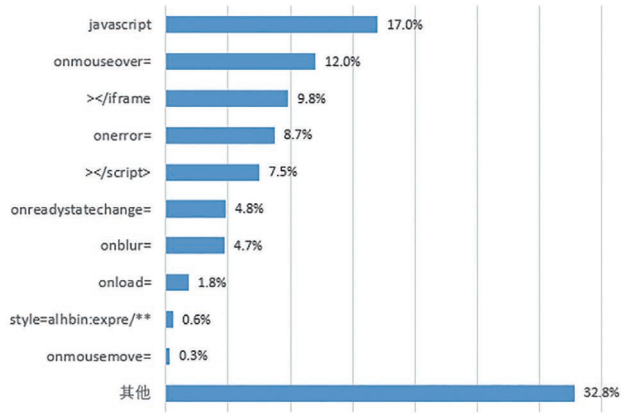


图 1.10 XSS 攻击常见攻击 Payload Top 10

数据来源：绿盟科技可管理安全服务（MSS）

1、javascript 排第一，占 17.0%。javascript 是一种网络脚本语言，广泛应用于 Web 应用开发，为网页添加各式各样的动态功能，javascript 脚本是通过嵌入在 HTML 中来实现自身的功能的。

2、onmouseover 排第二，占 12.0%。所有主流浏览器都支持 onmouseover 属性，比如攻击者可以在 <input> 元素中插入 onmouseover 属性，当用户鼠标指针移动到元素上时就会触发攻击者插入的 XSS 攻击代码。

3、></iframe 排第三，占 9.8%。所有浏览器都支持 <iframe> 标签，iframe 元素会创建包含另外一个文档的内联框架（即行内框架）。攻击者可通过在 iframe 元素中插入代码，实现 xss 攻击。

所有的 on* 事件内是可以执行 JavaScript 脚本的。

1.4.6 远程命令执行攻击常见 Payload

攻击者可通过提交经过特殊构造的系统命令，实现在服务端执行命令的目的，获得服务器的系统控制权。我们统计了远程命令执行攻击中常见的攻击 Payload Top 排名，如下图所示。

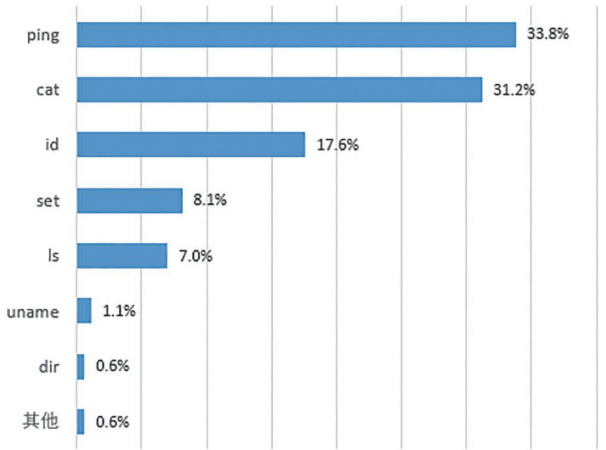


图 1.11 远程命令执行攻击常见 Payload

数据来源：绿盟科技可管理安全服务（MSS）

ping 命令常被用于测试网络中其他 IP 的联通性。

cat 命令用来显示文件内容。

Id 用于显示用户的 ID，以及所属群组的 ID。

set 命令主要是显示系统中已经存在的 shell 变量，以及设置 shell 变量的新变量值。

ls 命令在 linux 系统下用来列出目录下的文件。

uname 用于获取电脑和操作系统的相关信息。

dir 命令在 dos 系统下用来列出目录下的文件。

1.4.7 恶意扫描常见扫描器 Top 统计

端口扫描是黑客发起攻击的前置步骤，黑客发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型，从而了解到从哪里可探寻到攻击弱点。我们从告警信息中分析扫描器指纹，统计出黑客最常使用的扫描器类型占比，如下图所示。

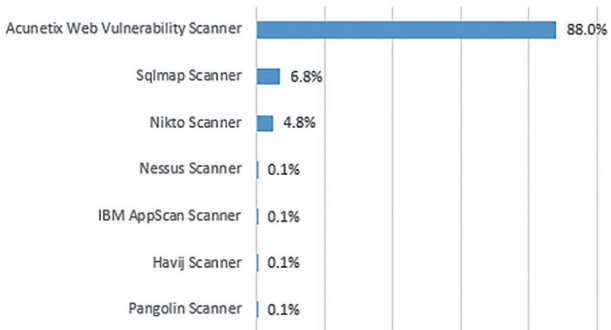


图 1.12 恶意扫描常用扫描器类型 Top 占比

数据来源：绿盟科技可管理安全服务（MSS）

1、AcunetixWeb Vulnerability Scanner 排名第一，占比高达 88%，它是一款商业的 Web 漏洞扫描程序，可以检查 Web 应用程序中的漏洞，如 SQL 注入、跨站脚本攻击、身份验证页上的弱口令长度等。它拥有一个操作方便的图形用户界面，并且能够创建专业级的 Web 站点安全审核报告。使用量 Top 1。

2、Sqlmap Scanner 是一款基于 SQLMAP 和 Charles 的被动 SQL 注入漏洞扫描工具。

3、Nikto Scanner 是一款开源的（GPL）网页服务器扫描器，它可以对网页服务器进行全面的多种扫描。

4、Nessus Scanner 是目前全世界最多人使用的系统漏洞扫描与分析软件

5、IBM AppScan Scanner。

6、Havij Scanner 胡萝卜，一款自动化的 SQL 注入工具，它能够帮助渗透测试人员发现和利用 Web 应用程序的 SQL 注入漏洞。

7、Pangolin Scanner 穿山甲，深圳宇造诺赛科技有限公司（Nosec）旗下的网站安全测试产品之一。

1.4.8 非法文件上传类型 Top 统计

攻击者为了达到长期控制网站服务器的目的，一般都会上传 Webshell 后门，排名前 3 的 ASP/PHP/JSP 都是现在最常用的 Webshell 后门格式。

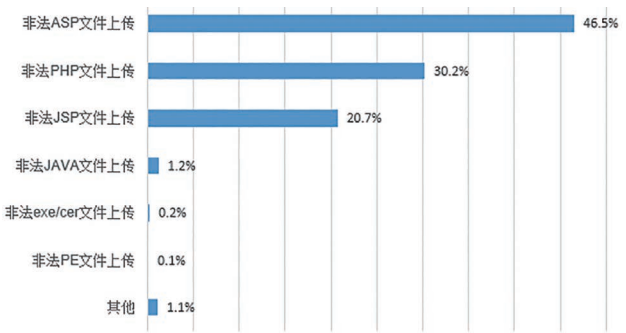


图 1.13 非法文件上传常见类型 Top 占比

数据来源：绿盟科技可管理安全服务（MSS）

扰乱者

素材提供 西南服务交付部 杨乔国

第一章 O2O 的纷乱

“老板，什么时候上菜啊？这都 20 分钟了！”客人使劲拍着桌子。

“你好，这里是维克托餐厅！你要订八号桌？好嘞！一定给你留着！”

“你好，这里是维克托餐厅，您要订 4 人桌？不好意思，只有两人桌了，行不行？那好，一定给你留着！”……

这天上午，还不到十点，维克托餐厅的订餐电话就响个不停，订餐系统也一个劲地提示，把老板维克托和助理朵儿忙得不亦乐乎。

维克托餐厅是开奥区一家开业时间不到两年的饭店。老板维克托来自外郡，他是个经商天才，不到两年的时间，他把来自东方的饮食理念做得风生水起，一套像热狗一样的食物，味道居然格外好吃。

维克托运用 O2O 的理念，线上线下皆可订餐，客人们用电话和手机都能订餐，只要订了，即可到店取，又可送上门。这么便利的运营方式，颇受年轻食客的追捧。

“今天订桌的怎么这么多？不太正常！”维克托皱着眉头说道。

“订桌的多，说明我们的店受欢迎！”朵儿得意地说，“老板，我建议你要再开几家分店了！”

“开分店我不急，我现在急的是，如何能打动你的芳心！”肥胖的维克托豆丁大的眼睛盯着朵儿那张精致的小脸。他从朵儿入职的第一天，就喜欢上这个美丽的姑娘了。

“今天这么忙，你还真有心情！”朵儿翻着白眼，继续接她的电话。

连下个星期的餐桌都被人订满，这也太不正常了。维克托再也没有撩妹的心思，他知道，一定是哪个地方出了岔子。

就在这时，楼下的服务员汤姆跑了上来：“老板，不好了！”

维克托正忧心忡忡，却被汤姆给吓了一跳：“呸呸呸，你才不好了……”

汤姆指着楼梯的方向说道：“老板，你下去看看，今天所有的桌子都被人占了！”

维克托一惊，急忙跑出办公室，顺着楼梯向下看，却被眼前的一幕惊呆了，“莫不是祖先的荣光照耀我了？”。

整个餐厅的三十张餐桌都被人占了，外面排队的还挤了一堆。

“噔噔噔噔……”肥胖的维克托却象个猴子一样跑下楼梯，来到一个秃顶的客人面前：“先生，你订桌了吗？”

“那当然！”秃顶冷冷地说道。

“你点了什么？”维克托问道。

“沙拉！”秃顶说道。

“你只点了沙拉？”

“是啊，上火！”

“要不来东方特色红酒腓力酱肘子！”维克托简直要暴走了，一份沙拉连凳子钱都不够。

维克托问了一圈，每个客人点的都是前菜，而且也都只有这一道。他明白了，今天这拨客人是有幺蛾子啊?

第二章 后门初现

深夜，餐厅已经打烊，维克托把助理、厨师和服务员都打发走，自己却瘫坐在店里的椅子上，双眼瞪着天花板。

一辆汽车戛然一声，停在维克托餐厅的门前。很快，义警布兰特走进餐厅。

看到布兰特，维克托象看到救星一样，“噌”地爬了起来。

也难怪维克托如此表现，今天一天，他就没有安生过。

中午，那些订桌的人就对着一份沙拉，愣是吃了两个多小时间，就一杯香槟，喝倒了一片人。

维克托以为晚上能会好一点，可是晚上又来了一帮人，虽然相貌和上午的人不一样，但是做派却跟上午的人无异。他们还是只点了一个前菜，然后又吃到打烊。如果一直这样下去，维克托非跳楼不可。

他希望布兰特能给他解决这个难题。

“你报的警?”布兰特一进门，就大声问道。

维克托点了点头：“是我!”

布兰特往椅子上一坐：“你说，我听听怎么回事!”

维克托就把今天的倒霉事说了一遍。

“你先把大厅的监控调出来给我看看!”布兰特说道。

“好的，请你跟我上楼!”维克托说着，把布兰特带到楼上的办公室。

看完监控之后，布兰特十分奇怪:“这些小痞子根本不是本地人。我连一个面熟的都找不出来!”

然后，布兰特又看了今天的订桌电话记录，他按照电话号码回拨过去，对方竟然是空号，而且每一个订桌电话都是空号，就连网上订桌的短信也都是空号。

“怎么会这样?”维克托简直不敢相信，“我今天早晨可是亲自接到这些电话、短信和网络订单的!”

“骗子们针对你的 O2O 订餐程序，利用网络虚拟出各种号码，并且变换出各种声音与人通话。你就是上了这个当!”布兰特解释了一下，“我需要登录你的账号，请你提供密码!”

维克托立即把他的 O2O 订餐软件的账号和密码提供给布兰特。

布兰特在电脑上操作了一会儿，却又惊讶地说道：“你的系统可能被植入了后门，我想屏蔽那些假的订餐信息，却根本无法做到。如果这个系统一直开着，那你们后面的麻烦还多着呢!”

维克托顿时慌了：“那怎么办?”

“暂时把 O2O 订餐程序给关了吧!”布兰特也没有什么好办法，然后，他又问道：“你们最近得罪过什么人没有?”

维克托不假思索地说道：“我们维克托餐厅一向与人为善，怎么可能得罪人呢?”

布兰特又说：“那可不好说，比如同行的生意竞争，是不是有人想把你们搞垮!”

维克托更傻了：“本市的酒店起码数千家，眼红我家生意好的，大有人在。上帝啊，这要是他们中的某一家做的，那可怎么查?”

布兰特说道：“我自有办法！从明天开始，你们停止营业，每个人都不要离开，以便配合我的调查！”

“停止营业？”维克托质疑道，“且不说我的损失，就是那些之前已经订餐的人怎么办，他们还不把我的店给砸了？”

布兰特摇了摇头：“有人想让你停业，你只要关门，他们应该就不会再闹！”

布兰特说得真是不错。第二天，维克托餐厅大门紧闭。虽然也有之前订餐的人来这里，但是看到餐厅歇业，闹了一通也就走了，并没有什么过激行为。

接下来的几天，维克托餐厅一直关着门。附近的市民们听说开业遥遥无期，都是十分惋惜。

第三章 愤怒服务

在维克托餐厅不远处的一栋高楼上，有一个人正通过大落地窗，用望远镜向这边看。

他叫斯图尔特，是本市斯图尔特饭馆的老板。

望着维克托餐厅那紧闭的大门，斯图尔特陷入了沉思。

两年前，斯图尔特才是这个区最红火的饭馆，他的烤肉在这个地区已经有上百年历史了。但是随着维克托餐厅的崛起，斯图尔特的生意一天不如一天。最后几个月，饭馆已经入不敷出了，传统美食的沦丧让他非常痛心与愤怒。

半个月前，斯图尔特来到附近的教堂做礼拜。这是他多年养成的习惯，每当遇到什么不顺心的事，都要到教堂里对着神自言自语，求主宽恕他的愤怒。

十多分钟之后，斯图尔特把他的心事讲完，正要离开的时候，却被一个穿着黑衣、戴着墨镜的男子拦住了。

“先生，你刚才的祈祷我都听到了。主派我来帮助你实现愿望！”黑衣男子说道。

“是吗？”斯图尔特将信将疑。

黑衣男子拿出一张名片，递给斯图尔特：“你打这个电话，就说要找阿帕特，阿帕特就会帮你达成心愿！哦，对了，电话接通后，你要说‘愿主保佑’，对方会说‘你会如愿以偿’，这就表示你是我介绍的。”说完，他与斯图尔特擦肩而过，扬长而去。

望着黑衣男子的背影，斯图尔特觉得有点虚幻。不过，他还是认真地看了看那张名片。

那张名片上，除了一组电话号码，别的什么也没有。

死马当活马医吧！斯图尔特抱着试试看的态度拨通了那个电话：“愿主保佑！”

如那个黑衣人所说，电话的那头果然清冷的回了一句：“你会如愿以偿的！”

“主听见我的心！”斯图尔特一阵狂喜，他立即说道：“阿帕特先生在吗，我找他有点事！”

“你有什么事，可以跟我说！”

“那好吧！”斯图尔特就把他的心事对着话筒讲了一遍。

助理听完，不由得冷笑一声：“这种小事情，就不用找阿帕特先生了，抱歉爱莫能助。”

斯图尔特心一沉，心想：“看来我的事要泡汤了！”

就在这时，电话里突然传来低沉的声音:“等下，你跟斯图尔特说，他的业务我接了！”看来，说话的人就在助理身边，想必他就是阿帕特。

对方接着说：“斯图尔特先生吗？你是说你的对手维克托吧，那你照我说的做！”

“好，好！”斯图尔特本来还有点半信半疑，不相信这个阿帕特有这种能力。但是他知道，即使不相信阿帕特的，自己仍然对付不了维克托。既然如此，那就信一次吧！

“我只说一遍！回家登录教堂的网站，直接输入“DDoS”，进去之后选择一个你想要的方案。不用管那些名字，你只需要选择预期的效果就行。比如要多少人去维克托的餐厅里吃饭，找哪里的人，要不要人闹事，让对方停业几天等等。还有，你要买通对手身边的一个人，让他帮忙开个‘后门’。把这些要求提交之后，你再付一千英镑，就可以坐等看戏了！”

“好的！”斯图尔特有点喜出望外，“一千英镑，不贵！”

斯图尔特挂了电话，回家做准备去了。

电话那头，一个神秘的豪华办公室内，一个年轻人问阿帕特:“老板，刚才的这个小生意并没有多少赚头，咱们很缺钱吗？”

阿帕特却笑道：“年轻人，做事要有大局观！斯图尔特的这单业务涉及到一个新领域，要不了多久，我们会从这类业务中找到更大的商机！”说到这里的时候，阿帕特想的却是自己的过往。

第四章 门中之门

转眼间，维克托餐厅已经停了十来天，但是布兰特的调查还没有头绪。眼看着开业遥遥无期，维克托都要绝望了。

这天上午，维克托正在办公室里想对策，助理朵儿走了进来:“老板，我想辞职！”

维克托简直不敢相信自己的耳朵：“朵儿，你能告诉我，为什么要走吗？你难道不知道我的心意，自从你一入职，我就喜欢你了。我还准备今年的情人节向你求婚呢！”

听维克托这么一说，朵儿的脸色有些发白，话语有些迟疑:“维克托，我知道你是好人……你志向太远大了，我配不上你！”

维克托失望透顶：“我志向哪里远大了，我就只是想把饭店搞好，当然顺便恢复一下我们家族的荣光。你是担心钱？”

“不，你的志向确实远大，你癞蛤蟆想吃天鹅肉啊”朵儿说道。

“餐厅不可能一直这样下去的，你要对我有信心！”维克托最后劝了一句。

朵儿却坚定地摇了摇头，看来她是下定决心了。

“好吧，收拾你的东西，我给你发最后一个月的薪水！”维克托说道。

朵儿收拾好她的物品，刚刚走出餐厅的大门，迎面就遇上了义警布兰特。“朵儿小姐，你要去哪里？”布兰特问道。

“不好意思，布兰特先生，我辞职了！”

“该说不好意思的是我，你现在已经走不了了！”布兰特坏笑着说道。

朵儿一慌，手中的物品差点掉在地上。“我不明白你是什么意思！”她强自镇静。

“什么意思，你心里没点儿数啊？走，跟我去维克托的办公室，

我要让你输得心服口服！”布兰特说着，抓住了朵儿的一条胳膊。这回，她就算想跑，也跑不了。

“朵儿，你怎么回来了，是回心转意了吗？”维克托看到朵儿，心中一喜，然后又看到布兰特跟在后面，“早上好，布兰特先生！”

布兰特点头示意，然后大咧咧地往椅子上一坐：“维克托先生，我有几个问题要问你！”

“你请，我一定把知道的全说出来！”

“大名鼎鼎的斯图尔特餐厅你知道吗？”

听布兰特突然提到“斯图尔特”，朵儿的脸色一变。她情不自禁地想逃出这间办公室，但是布兰特身下的椅子有滑轮，他一下子滑到门前，挡住了她的去路。

“斯图尔特餐厅？我知道的。在我的餐厅没有开业之前，斯图尔特餐厅是本地最有名的。但是自从我的餐厅开业，他的生意就一天不如一天了。”提到斯图尔特，维克托微微有点得意，“难道是？”。

“这几天，我查了你们公司所有人最近一段时间的通话和网络聊天记录，我发现朵儿小姐与斯图尔特有密切的联系。”说到这里，布兰特把目光转身朵儿，“朵儿小姐，你还不坦白吗？”

朵儿那张美丽的小脸，顿时变得煞白：“我、我，三月前，我在赌场欠了一大笔赌债，是斯图尔特替我还上的。但他的条件是，要我帮他在你的订桌系统上装个程序，然后盗走你的全部菜谱！”

维克托“腾”地站了起来：“需要钱，你为什么不跟我说？你明知道我喜欢你！”

朵儿的眼泪涌出眼眶：“你曾经跟我说过，最讨厌赌博的女人！”

维克托问布兰特：“警长先生，这件事能不能私了？”

“她既然触犯法律，就得交给法官来裁决，我可没有权力放了她！”布兰特摇了摇头，接着，他话锋一转，“不过，法官怎么判，很大程度上，要参考你这个当事人是什么态度！”

维克托问朵儿：“经过这件事，你能不能不再赌博？”

“能，一定！”朵儿重重地点头。

“那好，等你回到餐厅的那一天，等待你的将是一枚钻戒！”维克托郑重承诺。

布兰特也松了口气：“朵儿小姐，我希望，到了警局，你能把你所知道的全部说出来，我会让斯图尔特付出一定的代价！”

尾声 暴力黑幕

在阿帕特的办公室里，助理对阿帕特说道：“老板，斯图尔特被警察带走了，这件事会不会牵连到我们？”

阿帕特笑道：“都是匿名的，那帮人也跟我们没有联系，谁也抓不住我们的把柄！”

就在这时，办公室的门铃突然响了。助理立即过来开门。

门开的一刹那，助理惊喜地笑道：“是你啊，老兄！”

一个高大的汉子走近卧室，来到阿帕特的办公桌前，肩上还挎着一个很长的背包。

“事情处理得顺利吗？”阿帕特问道。

“谢谢老板的关心，一切 OK！但是，我只想说，这‘穿越者’的名字谁起的？真烂！”那汉子不屑的笑道。

直面DDoS攻击的黑幕 2018的抉择

品牌推广部 王洋

DDoS 攻击是在众多网络攻击中一种简单有效并且危害巨大的攻击方式。它通过各种手段消耗网络带宽和系统资源，导致运营方无法提供正常服务，进而对造成巨大但危害。在 2017 年里，它似乎被勒索软件给抢了风头，但在我们的观察中，DDoS 并没有停止它的脚步：

1. DOS **漏洞并没有变少**，仅绿盟科技漏洞库在 2017 年收录的 DoS 漏洞就超过 500 个，而近 18 年间已经累计超过 5000 个；

2. DDoS **技术与其它技术结合**，为了实现不同的目的，DDoS 攻击技术正在与木马、勒索软件、物联网恶意软件、垃圾邮件等技术不断结合；

3. DDoS **攻击深入行业业态**，攻击者越来越了解行业特性及运营者的弱点，从而选择合适的攻击目标及形式，尤其在运营商及游戏行业；

4. **升级至** APT **威胁态势**，DDoS 服务化乃至产业化进一步成熟，混合类型攻击呈常态，更高级的威胁源起方，让整个威胁态势呈现出 APT 特征；

然而无论 DDoS 如何变化，归根到底 DDoS 攻防就是一场资源消耗战，这种形态至今仍旧是一个世界级的难题，很难根治只能缓解。

在绿盟科技之前出版的《破坏之王 DDoS 攻击防范深度剖析》中提到，采用各种能减小 DDoS 攻击造成影响的，从而保障期服务的可能性，称之为“缓解”。缓解，这个业界通行的名字听起来并不那么有力，难道就没有有效的办法了吗？我们下面将要说到的这些观点及相关内容，会在即将发布的绿盟科技技术刊总第 37 期中精彩呈现。

年初的预测 攻守军备竞赛

在 2017 年初的文章中，绿盟科技 CTO 赵粮预测到，攻守双方的“军备竞赛”正在加剧。攻方无极限，各种攻击元素出租等“业务模式”创新将会继续。黑产已经进入更为精细化的“专业分工”，从漏洞、利用、工具开发、僵尸出租、社工库、以及各种专门服务都已经多次见诸各种安全报告。DDoS 攻击者在直接敲诈和烟幕服务等之外，提供非常低廉 DDoS as a Service(DDoS 即服务)，甚至有 5 美元起卖，还提供分销模式。

而守方则关注威胁情报，依托生态伙伴，洞察攻防前沿，避免成为跑的最慢的那一个。战场的无限扩大使得防护目标所涉及的技术和不断产生的漏洞，成为几乎“防无可防”的窘境。跟踪云物大移时代信息系统的所有环节的漏洞和攻防细节、并实时做出准确的判断，对于数十人规模的专业安全团队都是极度困难的。依托威胁情报系统和“生态伙伴”成为一种必然的选择。

年中的态势 黑产急速膨胀

毫无疑问，这一预测是成功的。根据 Nexus Guard 威胁报告显示，DDoS 攻击频率在 2017 年第一季度增长了 380%，而 CDN 服务供应商 Akamai 公司的二季度互联网安全报告显示，2017 年全球 DDoS 攻击的次数上升了 28%。然而，变化的不只是 DDoS 攻击频次。8 月，Gartner 发布了 2017 Web 应用防火墙魔力象限并指出，Web 应用防火墙（WAF）可以保护 Web 应用和 API 远离各种攻击，尤其包括注入攻击和应用层拒绝服务攻击（DoS）。它们不仅应该提供基于特征的防护，还应该支持主动安全模型及 / 或异常检测技术。

正是考虑到这一趋势，绿盟科技在 8 月份将 DDoS 攻击态势与 Web 应用攻击态势整合起来，发布《2017H1DDoS 与 Web 应用攻击态势报告》并指出，DDoS 攻击正被黑客用作实施 Web 应用攻击的烟雾弹，在 DDoS 攻击的同时，暗地里进行 Web 应用层攻击，最终达到篡改、窃取敏感信息、获取系统控制权限等目的。报告数据显示，2017 上半年仅监控到 DDoS 攻击就达 10 万余次，而 Q2 300G 以上大流量攻击上升 7 倍 。同样是这半年，攻击者对绿盟科技所防御的 Web 站点发起了 2771 万次 Web 应用层攻击。

在这些数据的另外一面，可以看到 DDoS 事件的一次次上演，让我们来看一个 DDoS 事件 timeline

1. 5 月，暗云 IV，单 IP 攻击流量达 650G ；

2. 6 月，国内多家证券金融公司、互联网金融公司接到境外黑客组织“无敌舰队 (Armada Collective)”的 DDoS 威胁恐吓邮件 ；

3. 6 月，物联网恶意软件 Persirai 攻击多国视频监控系统，可以感染 1000 多种网络摄像头，潜在影响 12 万台设备 ；

4. 8 月，DDoS 攻击木马“魔鼬”出现，6.4 万个 IP 受控制，某下载站攻击流量峰值达 632G ；

5. 8 **月**，物联网恶意软件 Rowdy 攻击我国有线电视网，感染设备涉及国内 5 家厂商，潜在影响我国 2 亿多设备；

6. 9 **月底**，幽灵小组攻击并要挟全数千家公司，要求支付 0.2 个比特币（时价约 720 美元）；

7. 10 **月中旬**，DDoS 勒索团伙 Phantom Squad 声称攻击了英国家彩票网站，导致服务下线；

8. 11 **月末**，美国运营商 Dyn 再次遭遇 Mirai 物联网恶意软件 DDoS 攻击，导致 DNS 服务瘫痪 2 小时

DDoS 即服务涌动黑产浪潮

上面这些信息都透露出一个信息，国内外的 DDoS 黑产正涌动着某种浪潮。8 月，思科 Talos 实验室在研究中发现，提供 DDoS 即服务的中文网站数量呈上升态势，并在后续的一份报告中展现了我国 DDoS 黑产形态及发展细节，从中发现大多数 DDoS 平台界面都长很像，大多来自同一套在线销售的 DDoS 平台源码，而就是这套来自海外的源码及 API，却被人发现了一个注入漏洞，可影响大多数 DDoS 平台！这表明很多购买该服务的攻击者，仍旧是被操纵的一部分。

报告中还呈现了不少销售这套源码的帖子时间是在 2017 年初或 2016 年底，这正是 DDoS 即服务兴起的时间。12 月，欧洲刑警组织发布的 2017 年网络犯罪威胁评估报告（IOCTA）认为，2017 年主要的威胁形式来自三个方面，恶意软件（含勒索软件和数据泄露）、关键基础设施攻击（含 APT）、数据泄露和网络攻击（含 DDoS）

面对攻击 我们可以还击吗

这些攻击给国内外的业务运营者们带去了灾难，大流量大规模的攻击固然能吸引注意，但更多的攻击，由于攻击行为及规模都不大，衡量攻击者的攻击行为及取证都有难度，被攻击之后该怎么办呢？好像投诉无门。这个时候有不少受害者选择反击，那“主动反击”（Hack Back）合法吗？的确，美国有这样的方案主动网络防御可靠性（ACDC）法案，但针对“主动防御”的概念存在着激烈的辩论。

• **问题 1**：网络攻击溯源准确吗？要知道攻击者有很多办法伪装自己，盲目的确定攻击源，就会卷入无辜的第三方；

• **问题 2**：被攻击方缺少能使用的资源及规模，而攻击者可供使用的手段有很多，盲目购买攻击服务，反而会被植入后门，进而再次被利用；

• **问题 3**：第三方云平台牵扯其中怎么办？想象一下，攻击者入侵了云服务提供商托管的共享服务器，利用这台服务器攻击受害者。受害者转而攻击共享服务器，影响到多家无辜公司的运营；

• **问题 4**：反击真的能实现目的吗？攻击的损失已经造成了，已经对你的业务运营造成了影响，你的反击如果不能抓获攻击者，只会导致更恶劣的报复，而你的损失也无法挽回。

如果无法妥善的解决这些问题，个人或者单位的还击行为，将可能带来更复杂和对自己更为不利的局面。所以，目前阶段我们呼吁大家，在遭遇到 DDoS 攻击之后，尽快报警并尽可能保留相关证据。

执法者们的有力回应

面对 DDoS 攻击的恶劣态势及受害者的求助，国内外的执法者们采取了积极的行动，并取得了成果。

• **年初**，广州一国资网贷平台遭受黑客网络攻击，导致官网平台一度无法访问，2 月 23 日，专案组民警在山东德州警方的大力协助下，在当地将犯罪嫌疑人李某（男，26 岁、山东陵县人）抓捕归案。

• **4 月**，20 岁黑客在英国中央刑事法庭受审，被判入狱两年。他开发的黑客程序 Titanium Stresser，曾对《我的世界》服务器以及微软和索尼等在内的公司，发动攻击超过 170 万次；

• **4 月**，江苏省某网络公司服务器频繁遭到 DDoS 流量攻击，随后一段时间，江苏省徐州警方抓获分布于全国 15 省 30 多个市的犯罪嫌疑人 58 人，包括发单人、肉鸡商、实施攻击人、出量人、担保人、黑客攻击软件作者等 DDoS 黑产链条中的各类角色；

• **8 月**，国际知名 DDoS 即服务平台 vDoS 两名嫌疑人被以色列警方起诉，调查人员表示，该平台运营者对全世界的网站上发起了超过 200 万次 DDoS 攻击，非法获利达 60 多万美金；

• **12 月**，国际知名 DDoS 即服务 PoodleCorp 组织成员被 FBI 抓捕，其运营平台也使用了 vDoS 相关 API

• **12 月**，美国司法部正式起诉三名男子，认定他们创建了 Mirai 恶意软件，并使用 Mirai 僵尸网络对互联网上的多个目标发动 DDoS 攻击。

防守者们的主动防御

同时更多的防守方，包括各行业组织及相关企业，在 DDoS 防御技术方面也采取了积极行动。11 月 16 日，中国电信发布“云堤高防”升级产品，已经具备 5000G 运营商级 DDoS 防御能力，而在在本文撰写时，绿盟科技作为中国电信的长年合作伙伴，也即将发布 ADS 10000 高性能型号，将运营商级的防护设备在性能方面再上一个台阶。

DDoS 智能防御方案

如前述，无论是哪个方面的产品进展，在面对复杂的客户业务场景时，都需要有个整合而灵活的解决方案，最终去主动的、动态的解决客户遇到的问题。绿盟科技的 DDoS 防护专家指出有效防护大流量 DDoS 攻击需要考虑以下三部分，并根据实际攻击场景进行组合及领导调配：

类型项目	本地 DDoS 防护设备	运营商清洗服务	云清洗服务
引流技术原理	企业侧部署设备，串联到网络中或者通过路由进行牵引流量。	部署在城域网，多通过路由方式进行引流，多基于 Flow 方式检测攻击。	利用 CNAME，将源站解析到新的域名，从而实现引流。

正是基于这样的设计理念，绿盟科技将 DDoS 防御与威胁情报相结合，最终诞生了 DDoS 智能混合防御方案。2017 年 3 月 30 日在欧洲 IT 和软件卓越奖庆祝晚宴和颁奖典礼上，该解决方案被授予 2017 年欧洲 IT& 软件（www.iteawards.com）年度最佳安全解决方案奖，并被提名入围“年度公共部门与公用事业解决方案”和“年度安全供应商”两项大奖的决赛。这些奖项旨在为解决客户核心问题，提供更好的服务，更清晰了解数据，以及提出更高效的 IT 解决方案。

DDoS 渗透测试及攻防演练

然而好的解决方案在进入到具体的生产环境后，并不只是面对 DDoS 攻击，还需要历经 APT 攻击的考验，用户需要在遭遇攻击之前进行有效测试，并针对测试结果进行调优。12 月，攻击模拟供应商 SafeBreach 发布了第三版“黑客手册调查报告”，该报告以独特的红队视角衡量了企业安全趋势，并指出通过模拟攻击者，可以以一个独特的视角，来了解安全将如何抵御攻击，而不是对生产环境进行测试。让自己追上攻击者的脚步，将有利于防守方的安全领导人打破攻防死环的恶性循环，并延缓攻击者的进攻。

外媒 InfoSec 曾指出，如今由于在 APT 攻击中使用了 DDoS 技术，安全专家已经建议将渗透测试与 DDoS 测试相结合。 渗透测试显示攻击者是否可以利用您的网络访问数据，DDoS 测试反过来，旨在使您的网络系统不可用，并检查他们可以处理多少工作量。这两种类型的安全测试可以独立或同时进行。在后一种情况下，渗透测试工程师可能会模拟一个 APT 攻击，而在其中采用 DDoS 攻击的作为子向量。

为解决上述应用场景的需求，绿盟科技技术团队研发了新型攻防演练平台，该平台基于绿盟科技十多年 DDoS 攻防研究，以及即将发布的 ADS NX5-10000 防护产品，还结合了多行业服务实践，实现了演练服务的自动、自助、可运营、能力云化与集中管理。

在十九大安保中的实战

无论是 DDoS 攻防研究，还是 DDoS 防护产品升级，又或者 DDoS 智能防御方案，所有这些准备，在十九大到来之时都获得了检验。在 16 天的安保过程中，绿盟科技协助客户从建流程、促呈现、细策略、控设备、自服务五个方面开展工作，DDoS 智能防御方案为北京移动圆满完成“十九大”保障工作提供了强有力的技术支持，获得了客户的高度认可，包括北京移动及其服务的新华网、人民网、中国日报等用户的肯定。这些成功也为该方案所获得的众多奖项，提供了有力的印证。

年底的抉择 正在十字路口

写到这里，正值辞旧迎新的时刻，让我们回望 DDoS 攻防资源消耗战的本质，这种形态很难根治只能缓解。据市场咨询机构 Frost&Sullivan 称，DDoS 缓解市场在 2016 年产生了 8 亿 1600 万美元的收入，预计到 2021 年，将会年复合增长 17.1% 。DDoS 缓解市场正在持续增长。

这对安全厂商们来说，或者对 DDoS 防御服务供应商来说是个好消息，但却给客户带来了挑战，特别是当客户面临庞大的架构时，每个决策及调整都面临了非常大的风险，面对 DDoS 黑产的急速膨胀和快速创新，作为防守方是该稳步慢行，还是快速调整？

无论是哪种抉择，都不意味着你可以将 DDoS 相关预算从年度预算中拿出去，大家迫切的需要从现有 DDoS 防御措施中提炼相关信息，从而为组织找到最适合的解决方案，提供决策支持。2018，是升级采购还是全新采购？绿盟科技技术刊本期文章，为您的抉择提供参考。

坚守在对抗DDoS攻击的第一线

政府技术部 庞彬彬

关键词：关键信息基础设施 重大安保 DDoS 防护 DDoS 防御 云地人机

摘要：国家某部委客户的信息系统属于关键信息基础设施，业务运行压力大、重要程度高、影响范围广，攻击者屡次三番对该信息系统进行攻击渗透但均未得逞，在此次重保中 DDoS 攻击来势汹汹，手段多变。在应急小组的统一指挥下，绿盟科技与应急保障各单位有效协作，展开“云地人机”协同作战，再次击败来犯之敌。

10 月 27 日 重保团队严阵以待

27 日，按照重要时期安全保障的总体规划，客户单位成立重保应急小组，客户信息中心主任担任应急小组总指挥，安全处处长担任应急小组副总指挥，同时作为和各保障支持成员单位之间的应急联络人。

绿盟科技作为客户应急保障成员单位，去年负责过该客户在重要时期的安全保障工作，保障经验丰富、协作沟通默契曾得到客户认可。在本次安全保障中绿盟科技担任技术咨询角色，负责重保期间客户的应急预案规划、攻击演练，与中国电信、中国联通等单位组成客户在重要时期的应急保障团队，灵活制定三方 DDoS 攻击防护策略，确保客户的关键信息基础设施在遭受攻击时，各成员单位能迅速响应，密切沟通协作保障关键基础设施安全稳定运行。

在安全保障会议上，绿盟科技代表人员向客户信息中心主任、客户安全处处长、中国电信云堤、中国联通云清洗等代表详细阐述了绿盟在拒绝服务攻击对抗中的安全经验和本次重保的安全防护思路，并根据去年保障经验和数据现场制定了详细的攻击防护策略，得到了客户和运营商代表的认可。在此基础上，中国电信云堤和中国联通云清洗将建立运营商云清洗基线。会议最后形成一致意见，对关键信息基础设施在重要时期遭受的 DDoS 攻击进行分层清洗，对于攻击者通过控制的僵尸主机并且利用运营商链路发动的攻击流量首先由运营商在本链路内进行流量清洗，清洗容量暂定 10G，如果攻击流量突破 10G，运营商将进行弹性清洗；其次，本地清洗方案则部署绿盟科技的异常流量检测系统，对客户关键基础设施的业务流量进行异常流量分析，对发现的 DDoS 攻击行为通过绿盟抗拒绝服务系统进行流量牵引，并通过本地抗拒绝服务系统的清洗矩阵做精细化的异常流量清洗，例如 CC 攻击清洗、http get flood 攻击清洗等。

重保倒计时 48 小时 初见峥嵘

重保前两天客户关键业务系统流量程上升趋势，但是流量总体

平稳，本地设备没有监测到过去 48 小时内的 DDoS 攻击流量，笔者通过沟通机制对这两天的安全保障工作向客户进行了汇报，并与中国电信和中国联通进行了沟通，两家运营商的监测结果与绿盟科技的汇报情况一致，48 小时内并没有发现 DDoS 攻击行为，但是大家都没有松懈，仍旧严阵以待。终于，考验重保团队的关键时刻到了。

11 月 1 日 突破流量清洗基线

1 日上午随着时间的推移，绿盟科技异常流量检测系统首先发现某部委客户关键信息基础设施的异常情况，绿盟科技现场保障人员将此信息及时上报到应急小组总指挥，并通过沟通机制对中国电信和中国联通发布预警通报，运营商及时调整监测策略以应对监测到的异常流量信息，在团队紧密协作下，持续观察现有流量发展态势；与此同时，应急保障团队经过分析决定一旦超过 200M 的入流量基线，则立即采取分层清洗策略。果不其然，攻击流量急速上升，流量清洗基线很快就被打破，绿盟科技按照应急预案启动清洗策略，在以运营商云清洗为主导、绿盟本地精细化清洗的配合下，有效保障了客户方重要业务系统在关键时期的顺畅运行。

持续一周 狡猾的攻击策略

从 11 月 1 日 -11 月 6 日，客户的关键业务被密集访问的过程中遭受间歇性的 DDoS 攻击，攻击总是发生在每天的正常工作时间，当天总的攻击流量不超过 20G，在 11 月 8 日也就是保障即将结束的阶段，攻击者有明显的策略转变，突然发动了持续的大流量 DDoS 攻击，根据持续监控显示，攻击流量瞬时间达到 320G。首先本地设备检测到 DDoS 攻击流量，通过沟通机制发现部分攻击流量是僵尸主机利用中国电信的链路发动的攻击行为，紧接着中国联通也发现攻击流量，三家重保单位随即对于客户遭受的 DDoS 攻击进行持续流量清洗。运营商启用本链路内的流量清洗和流量压制，非法流量被瞬间压制。但是没多久新一轮的 DDoS 攻击流量被保障团队重新检测到，基于这种情况保障团队适时而动，及时调整清洗策略，进行更为灵活且持续清洗和流量压制。绿盟本地清洗资源池启动精细化清洗策略，针对到本地的流量进行应用层清洗，保留 DDoS 攻击证据并提交给客户，以便保障会议后启动法律追责程序。最终，在保障团队通力合作下，顺利完成某部委客户重要时期的安全保障工作。

DDoS 防护 云地人机的协同

在此次重保中，某部委客户所遭受的 DDoS 攻击呈现出一定的策略性，日常攻击时间持续，攻击频率颇高，结束阶段突发大流量攻击，这样的策略性攻击在这种行业场景下也比较少见。绿盟科技在本次重保期间按照客户方统一部署，和各保障单位密切沟通合作顺利完成本次重保任务，同时也为该客户 18 年的重保服务积累宝贵经验。

近年来有组织的黑客攻击对行业客户关键信息基础设施造成严重危害，攻击手段多样化、攻击危害传播快、攻击性质商业化等特点明显，这对重要时期关键信息基础设施的保障工作提出了更高的要求。通过此次重保经历，凸显出了绿盟科技在应对 DDoS 攻击事件时“云地人机”协同作战能力的优势，也再次证明绿盟科技有能力帮助用户做好安全运营工作，有能力履行“巨人背后的安全专家，保障客户业务顺畅运行”的这一神圣而又光荣的使命。

与客户共同坚守的日子

——某移动“十九大”保障 DDoS 防护方案

北区工程部 尹沛榕

关键词：十九大安保 DDoS 防护方案 应急响应 绿盟云清洗增值自助服务平台

摘要：从 2010 年至今，某移动通过流量清洗项目 1-4 期的持续建设，具备了较强的 CMNET & IDC 侧 DDOS 防护能力，应用的相关产品均为绿盟科技产品。为了筹备今年的“十九大”安全保障，某移动在原有全网流量监控，清洗防护能力 1T 的基础上，新增了绿盟攻击态势监控系统（NTA-ATM）以及绿盟云清洗增值自助服务平台，并对接客户 ISMP 管理平台以及 EMOS 工单系统。从建流程、促呈现、细策略、控设备、自服务五个方面开展工作，整套方案为某移动圆满完成“十九大”保障工作提供了强有力的技术支持，获得了客户的高度认可。

序——午夜铃声

10 月 24 日 21:00

某移动“十九大”保障现场依旧是灯火通明，人声鼎沸。上午“十九大”已经顺利闭幕，整个保障过程中没有发生任何安全问题，大家不由得松了一口气，这口气还没喘平，客户领导莅临保障现场。

时间已经很晚了，赶到保障现场是某移动的一级经理，领导发表指示：“同志们，大家这些天都辛苦了，‘十九大’已经胜利闭幕，但是明天的新常委亮相活动非常重要，请大家振奋精神，坚守岗位，今天晚上至关重要，大家一定要盯紧了。”

这场从 11 日开始 7*24 无间断的值守，大家已经疲惫不堪了，听着领导的指示，还是抖擞精神，继续奋战。信安部门相关同事准备出发，继续追查清理伪基站；网安部门由我们配合一同保障，此时

再次确认一遍所有重保客户的实时流量情况。

10 月 25 日 01:30

所有夜班同事坚守岗位，没有休息。夜深了，白天周围嘈杂的马路，此刻听不到一点声音。看了一眼，所有重保客户流量正常，相比于白天，流量减少了很多，坐下来准备冲杯咖啡，缓解一下阵阵困意。

01:31:57

咖啡还没加上热水，NTA 上突然出现告警，一级重保用户某日报出现峰值 577M 的 ACK FLOOD 告警，要知道这个客户日常流量峰值小于 100M，要求配置的告警阈值为 350M，577M 的流量显然是异常的。

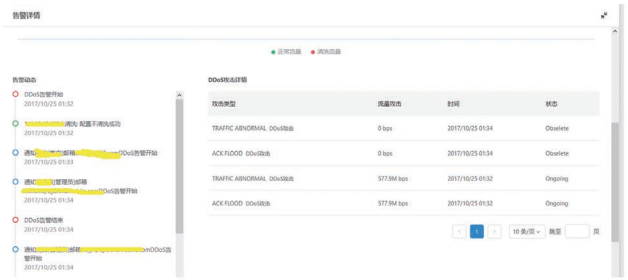
大家的瞳孔竖的和猫一样，全身绷紧，这么重要的时期，告警就这样突如其来了！！

01:31:57 的告警同步传送到 NTA-ATM 以及云清洗平台，NTA-ATM 将告警同步传送到 ISMP 管理平台，确认为一级重保客户安全事件后，同步传送到 EMOS 工单系统进行派单。

01:32:02

某移动运维人员及相关领导接到派单告警电话。午夜的电话，刺耳也格外惊心……

01:32:02 云清洗平台同步发送告警邮件以及 APP 推送消息到某日报客户以及我方所有相关协助运维人员。



此时客户、客户领导、我方所有保障人员全都在午夜时分以各种告警方式行动起来，气氛非常紧张，心脏不停狂跳，领导一直在问，到底情况如何，是否严重。

响应排查是迅速的，身后其他的保障人员都围了过来，一切的困意都被好奇心占的满满的。锁定攻击源，移动 IDC 运维人员排查攻击源，我方迅速在设备上抓包分析。然而就在抓包的同时，发现攻击告警已停止，流量开始下降。

01:35:01

客户确认攻击源为某日报电信通专线的 IP，瞬间流量突增是由于自身业务交互产生的，排除了攻击，一场虚惊，哈，一身抗 DDoS 技术还未施展。

和客户一起编写安全事件处理报告，写好之后，时间已经是凌晨两点多了，此时此刻，毫无困意，紧张的心似乎还没有减速，客户也一样。

客户表示，虽然只是虚惊一场，但通过这次告警事件，考验了我们的整个响应流程和速度，团队所呈现的状态非常到位。这样的响应流程迅速展开，离不开持续多年的抗 DDoS 能力建设。

全面的抗 DDoS 方案

2016 年 G20 峰会保障，移动集团首次提出了“五反”概念，其中反 DDOS 攻击作为重点防范内容；

2017 年网络工作计划中，移动集团明确要求 DDoS 攻击防护作为“五反”重点，应形成安全监控运营“新常态”，并在重大活动保障中实现自动化监控和一键处置能力。

2016 年两部委考核网络安全部分，明确要求数据中心（IDC）需具备防 DDoS 攻击能力；

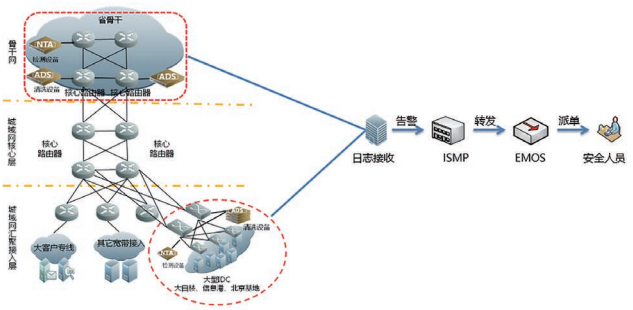
2017 年两部委考核网络安全部分，明确要求抗拒绝服务攻击手段应能够在骨干网络层面为省内的重点网站或系统提供流量清洗等抗 DDoS 攻击服务。

基于多年来移动集团以及两部委考核的相关要求，结合某移动自身安全需求、重保需求以及转型需求，某移动自 2010 年开始投入 DDoS 防护相关建设工作，一直与我司密切合作。目前具备了较强的 CMNET & IDC 侧 DDoS 防护能力，实现了全网流量监控以及清洗防护能力 1T 的 DDoS 防护能力。

2017 年，某移动为进一步将抗 D 安全能力转化为安全效益，解决流量清洗“最后一公里”问题，从**建流程**、**促呈现**、**细策略**、**控设备**、**自服务**五个方面开展工作，新增了绿盟攻击态势监控系统（NTA-ATM）以及绿盟云清洗增值自助服务平台，逐步实现了抗 DDoS 能力提升与开放，为“十九大”的安全保障工作提供了强有力的技术支持。

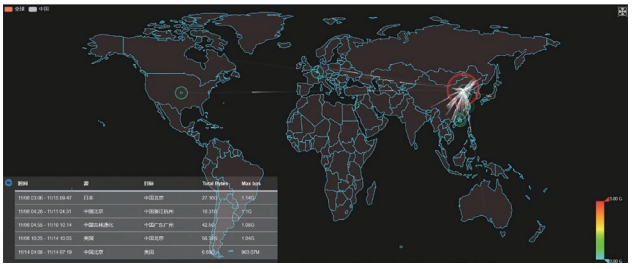
建流程

将 CMNET&IDC 侧 NTA 设备告警日志发送到 NTA-ATM 以及云清洗平台，由 NTA-ATM 汇总告警信息后通过 syslog 的传输方式发送到某移动 ISMP 监管平台，再由平台对告警信息做二次过滤，将重要安全事件告警转发给 EMOS 工单系统，系统派单给运维人员，实现了告警采集、集中监控、自动派单处理的全生命周期管理，为快速处置提供了流程依据。

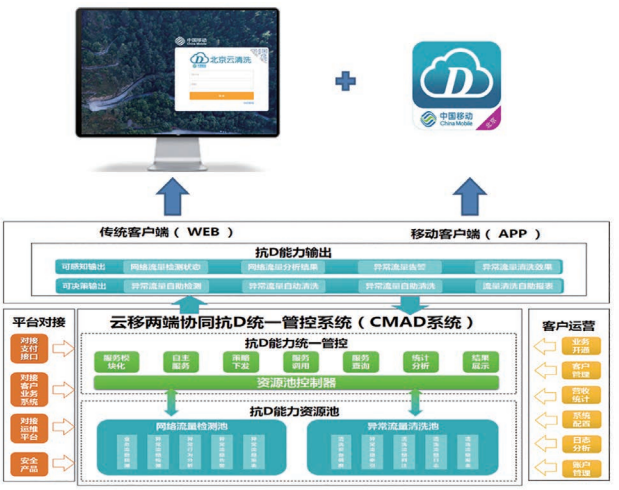


促呈现

为更加清晰地呈现安全态势，实现 DDoS 攻击实时感知与分析，部署建设了绿盟攻击态势监控系统（NTA-ATM），为网络攻击集中分析及态势感知的实现提供了数据基础。



客户清洗业务开通、统计报表等集中安全运营能力，实现云端统一管控，自助流量清洗管理。移动端架构设计：由移动手机作为终端



细策略

针对“十九大”重保期间 16 个自有网站和 15 家重保对象，细分 SYN FLOOD、ACK FLOOD、UDP FLOOD 等各类攻击防御需求，逐一制定了流量清洗策略。

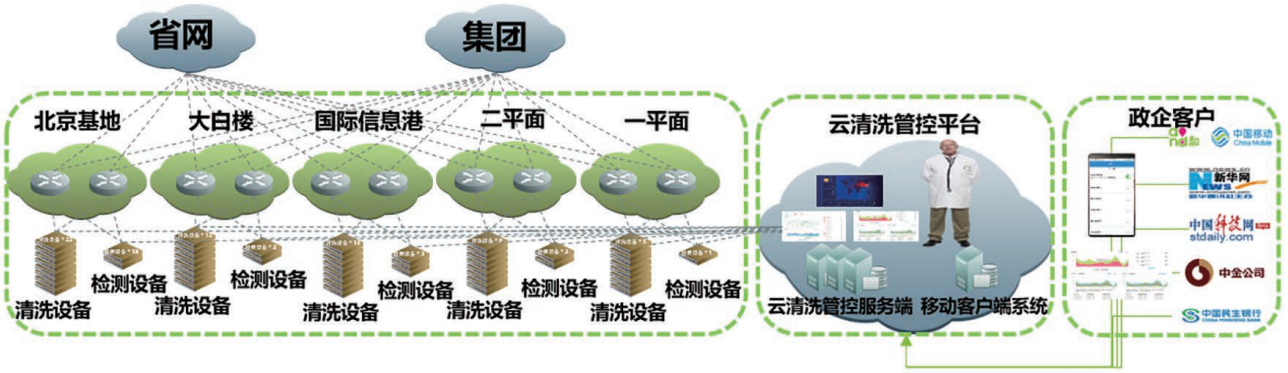
控设备

利用云清洗平台，实现对现网全量清洗设备的统一调度、集中管理。云端架构设计：流量监控和清洗的统一管控，具备可视化展示，进行接入，自有人员和政企客户可按需自助实现流量监控、清洗服务、业务可用性检测、抗 D 攻击态势监控、报表统计等服务。

自服务

利用云清洗，实现运维人员和“十九大”期间重保客户的快速自主监控和清洗，责任明晰、敏捷高效。

整套 DDoS 防护方案为某移动圆满完成“十九大”保障工作提供了强有力的技术支持，获得了客户的高度认可，同时获得了某移动



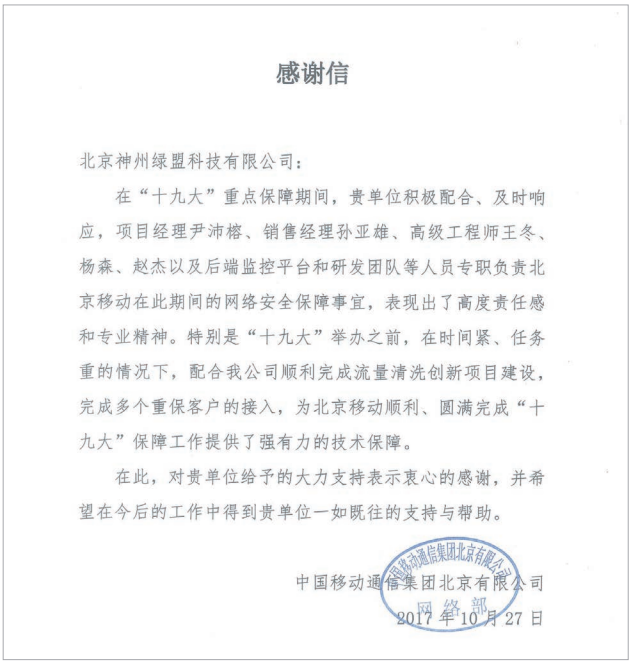
界面友好　功能全面　客户管理　自主配置　实时监控　秒级清洗

的重保客户：新华网、人民网、中国日报等用户的肯定。此方案符合战略价值的创新，能够真正实现从产品到方案到运营模式的转变，具有可复制性。

尾声

“十九大”保障就在午夜告警事件中落幕了，16 天的不间断坚守，客户对于我们的工作给予了高度评价，并寄送了感谢信。

虽然辛苦，虽然惊心动魄，“十九大”的圆满闭幕，客户系统的安全稳定，永远是我们最欣慰的事情。



感谢信

北京神州绿盟科技有限公司：

在“十九大”重点保障期间，贵单位积极配合、及时响应，项目经理尹沛榕、销售经理孙亚雄、高级工程师王冬、杨森、赵杰以及后端监控平台和研发团队等人员专职负责北京移动在此期间的网络安全保障事宜，表现出了高度责任感和专业精神。特别是“十九大”举办之前，在时间紧、任务重的情况下，配合我公司顺利完成流量清洗创新项目建设，完成多个重保客户的接入，为北京移动顺利、圆满完成“十九大”保障工作提供了强有力的技术保障。

在此，对贵单位给予的大力支持表示衷心的感谢，并希望在今后的工作中得到贵单位一如既往的支持与帮助。

中国移动通信集团北京有限公司
网络部
2017 年 10 月 27 日

DDoS攻击应急体系知多少?

北区工程部 宣云飞

关键词：DDoS 攻击类型 DDoS 防御 应急响应体系 DDoS 攻击应急演练

摘要：本文会涉及到 DDoS 攻击应急过程中的整体策略、应急流程以及针对一些典型攻击的具体分析和应对措施，旨在分析如何在遭受 DDoS 攻击的时候更高效的组织应急工作。所以并不会深入到每一种特定 DDoS 攻击的的具体攻击方法或是应对措施的具体配置。

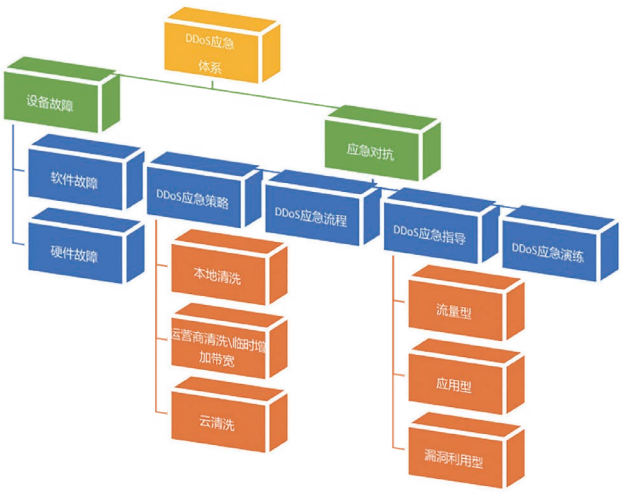
0×00、引言

近年来 DDoS 攻击事件可谓是层出不穷，从各安全厂商的 DDoS 分析报告中也不难看出，DDoS 攻击的规模及趋势正在成倍的增长。由于攻击的成本不断降低，技术门槛要求越来越低，攻击工具的肆意传播，互联网上随处可见成群的肉鸡，使得发动一起 DDoS 攻击变成了一件轻而易举的事情。各企业对于 DDoS 攻击防御的投入也是慢慢的水涨船高。高投入当然需要高回报，抗 DDoS 工作做得好不好，往往就体现在了发生 DDoS 攻击时候的应急能力。

希望通过本文可以使读者了解并且能站到一个高度全面的看待 DDoS 攻击应急的工作。当我们真的遭受到的 DDoS 攻击的时候，能游刃有余的应对，而不是手忙脚乱。

0×01、总览

一般日常运维中对于应急的定义通常都会分为两类：一类是设备本身故障的应急，另一类就是对于业务的应急。

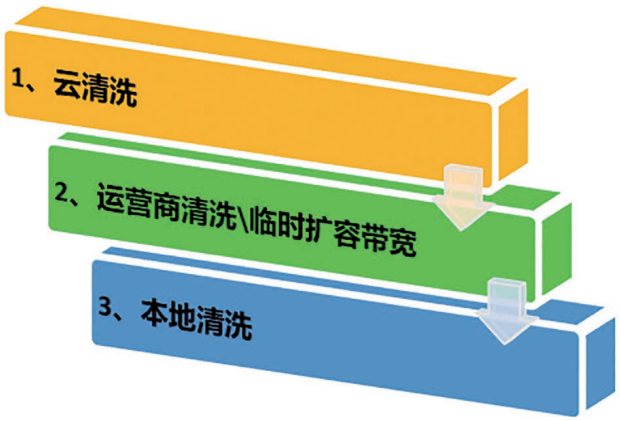


在这里，我们也把设备的故障列了出来。虽然这一块不是本文重点要讲的东西，但是如果当我们在遭受 DDoS 攻击的时候，抗 D 设备出了问题，也会使得我们空有一身力气无处使。所以在整体的应急框架里，这也是非常重要的一部分。

0×02、DDoS 攻击应急策略

DDoS 攻击应急策略总结为 8 个字就是“立体防御，层层过滤”，具体见下图。

大家都知道，DDoS 攻击最最最大的特点就是流量大，但是也有很多不需要太大流量但是同样可以达到攻击效果的方式。所以就



有了上图中的防御层次。

- 当受到 DDoS 攻击的流量还没有超过链路带宽的 80% 的时候，我们本地的抗 DDoS 攻击设备完全可以实现 DDoS 攻击的清洗。能自己搞定绝不麻烦别人。
- 当受到 DDoS 攻击的流量超过了链路带宽的 100% 的时候，这个时候就需要启动运营商的 DDoS 攻击清洗了。哎呀呀，你说刚好这条受攻击的链路运营商不提供 DDoS 攻击清洗服务怎么办？没关系，这个时候还可启用 Plan B，通知运营商临时给我们扩容一下带宽就好了。只要攻击流量没把带宽占满，本地清洗就可行。
- 当受到 DDoS 攻击的流量运营商清洗起来效果不是那么好的情况下，可以紧急启用云清洗服务来进行最后的对决。

因为大多数真正的 DDoS 攻击都是“混合”攻击（掺杂着各种不同的攻击类型），比如说：以大流量反射做背景，期间混入一些 CC 和连接耗尽，以及慢速攻击。那么这个时候很有可能需要运营商清洗

（针对流量型的攻击）先把 80% 以上的流量清洗掉，把链路带宽清出来，这个时候剩下的 20% 里面很有可能还有 80% 是攻击流量（类似慢速攻击、CC 攻击等），那么就需要本地进一步的清洗了。

0x03、DDoS 攻击应急流程

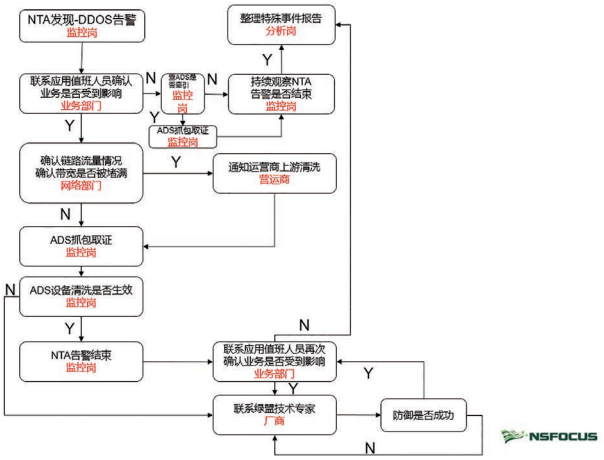
下图是一个比较适合大多数客户的对于 DDoS 攻击应急的整体流程图，其中有一些细节需要指出；

1、如果我们没有专门 24 小时现场值守的安全运维工程师的话，一般情况下是通过网管中心来发现 DDoS 告警，那么就需要和网管监控中心的监控同事有相应的合作处理机制。

2、如果我们的清洗设备并没有配置自动牵引，那么在发生攻击的时候需要手动开启。在应急状态下，这个动作由谁来做，怎么做，需要什么授权等等，这一块也是需要事前进行沟通并纳入到应急流程当中（尤其是如果在凌晨 2 点发生了 DDoS 攻击，就不会显得手忙脚乱）。

3、关于通知运营商这一块依然是需要前期就沟通确认好对应的处理机制，使得应急状态下可以顺利进行。最起码需要保证运营商的接口人的联系方式，以及双方都确认的授权方式（比如有些客户的运营商清洗的流程是需要发送盖公章的书函的传真）。

4、对于厂商的专家支持建议前期做好相关的技术交流与沟通，至少要确认在什么情况下启动此项机制，并且提前就一些基础信息的收集提供做好确认（毕竟二线支持到现场的相应是需要交通时间的，进入到应急流程以后业务恢复时间是我们不得不考虑的因素）



由于上图是一个通用的指导流程，所以会在很多细节方面没有太多的针对性（针对性太强了就没有办法通用了，这是一个很矛盾的点），所以该流程仅做参考使用，在使用过程中，还需要针对自己的事业环境因素来做相应的裁剪和优化。

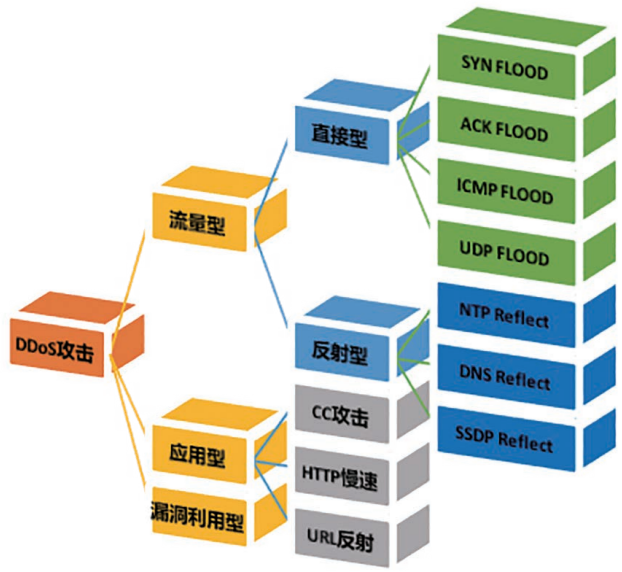
0x04、DDoS 攻击应急指导

4.1 DDoS 攻击场景

下图（如图一）为针对典型 DDoS 攻击通过攻击特征进行的分类:

转换为攻击场景：	
DDoS 攻击场景	现象
流量型（直接）	SYN\ACK\ICMP\UDP\Connection FLOOD 等 DDoS 告警

转换为攻击场景：	
流量型（反射）	NTP\DNS\SSDP\ICMP FLOOD 等 DDoS 告警
CC	流量变化可能不明显，业务访问缓慢，超时严重，大量访问请求指向同一个或少数几个页面
HTTP 慢速	流量变化可能不明显，业务访问缓慢，超时严重，大量不完整的 HTTP GET 请求，出现有规律大小（通常很小）的 HTTP POST 请求的报文
URL 反射	流量变化明显，业务访问缓慢，超时严重，大量请求的 Referer 字段相同，表明均来自同一跳转页面
各种 DOS 效果漏洞利用	入侵检测防御设备可能出现告警，DDoS 攻击检测设备告警不明显



图一

根据 DDoS 攻击防御总方针，接下来就可以对号入座的针对每一个梳理出来的攻击场景部署防御手段了。

- **流量型（直接）--- 流量未超过链路带宽 --- 本地清洗**
- **流量型（直接）--- 流量超过链路带宽 --- 通知运营商清洗 || 临时扩容 || 云清洗 --- 本地清洗**

针对 SYN、ACK、UDP、ICMP 等类型的 flood 攻击：

一般情况下：本地清洗设备的防御算法都可以轻松应对。比如说首包丢弃、IP 溯源等。

特殊情况下：可以再次基础上增加一些限速，至少就可以保证在遭受攻击的时候保持业务基本的可用性。

如果通过排查发现发生攻击源 IP 具有地域特征，可以根据地域进行限制（大量来自国外的攻击尤其适用）。

- **流量型（反射）--- 流量未超过链路带宽 --- 本地清洗**
- **流量型（反射）--- 流量超过链路带宽 --- 通知运营商清洗 || 临时扩容 || 云清洗 --- 本地清洗**

针对 NTP、DNS、SSDP 等类型的反射攻击：

一般情况下：本地清洗设备的防御算法都可以有效的进行缓解。比如说对 UDP 碎片包的丢弃，以及限速等。

特殊情况下：由于反射攻击的特征大多呈现为固定源端口 + 固定目的 IP 地址的流量占了整个链路带宽的 90%+

我们可以针对这些特征配置更加彻底的丢弃规则

- **CC--- 本地清洗 --- 本地清洗效果不佳后 ---- 云清洗**

针对 CC 攻击，如果清洗效果非常不明显，情况又很紧急可以

采用临时使用静态页面替换。

◆ HTTP 慢速 --- 本地清洗 --- 本地清洗效果不佳后 --- 云清洗

对于 HTTP body 慢速攻击，在攻击过程中分析出攻击工具的特征后，针对特征在本地防御设备进行配置。

◆ URL（反射）--- 本地清洗 + 云清洗

对于 URL 反射攻击，在攻击过程中找出反射源，在本地防御设备进行高级配置

◆ 各种 DoS 效果漏洞利用：监控入侵检测或防御设备的告警信息、做好系统漏洞修复

对于此类攻击，其实严格意义来说并不能算 DDoS 攻击，只能算是能达到效果的攻击，仅做补充场景

4.2 DDoS 攻击应急指导

4.2.1 流量型（直接）DDoS 攻击

首先我们针对流量型（直接）DDoS 攻击的判断以及清洗来做说明，此类型攻击比较有代表性的攻击有 SYN-FLOOD、ACK-FLOOD、ICM-FLOOD、UDP-FLOOD 攻击等。首先在发生 DDoS 攻击的时候在 DDoS 攻击检测设备上面就会有对应的告警，通常我们可以在检测设备上获取第一手的信息，不论是自动清洗还是手动清洗，当发生了 DDoS 攻击的时候想要对攻击进行防御，就需要把流量牵引到 DDoS 攻击的清洗设备上（串联部署除外）。不论是何种方式，当流量已经被牵引到清洗设备上以后，我们就可以通过抓包来进一步分析当前 DDoS 攻击的特征。

一般情况下，当我们抓到的数据包某类型的数据包的流量占到了整个包数的 80% 以上我们就确认攻击了。

◆ SYN-FLOOD

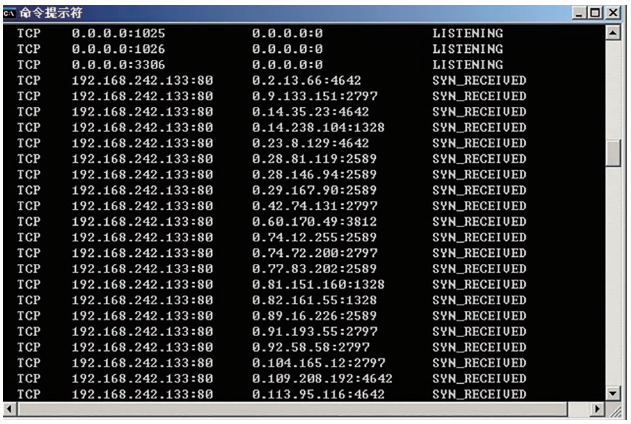
1、TCP-SYN 包的数量占到整个抓包文件的 80% 左右

No.	Time	Source	Destination	Protocol	Info
1	13:19:05.498967	110.22.126.68	5.5.5.1	TCP	56000 > http [SYN] Seq=0 Win=65535 Len=0
2	13:19:05.499017	110.22.126.68	5.5.5.1	TCP	56000 > http [SYN] Seq=0 Win=65535 Len=0
3	13:19:05.499100	45.61.110.120	5.5.5.1	TCP	15103 > http [SYN] Seq=0 Win=65535 Len=0
4	13:19:05.499106	45.61.110.120	5.5.5.1	TCP	15103 > http [SYN] Seq=0 Win=65535 Len=0
5	13:19:05.499202	168.150.250.107	5.5.5.1	TCP	53908 > http [SYN] Seq=0 Win=65535 Len=0
6	13:19:05.499207	168.150.250.107	5.5.5.1	TCP	53908 > http [SYN] Seq=0 Win=65535 Len=0
7	13:19:05.499293	70.125.205.44	5.5.5.1	TCP	21189 > http [SYN] Seq=0 Win=65535 Len=0
8	13:19:05.499298	70.125.205.44	5.5.5.1	TCP	21189 > http [SYN] Seq=0 Win=65535 Len=0
9	13:19:05.499407	21.74.6.49	5.5.5.1	TCP	61655 > http [SYN] Seq=0 Win=65535 Len=0
10	13:19:05.499412	21.74.6.49	5.5.5.1	TCP	61655 > http [SYN] Seq=0 Win=65535 Len=0
11	13:19:05.499482	87.101.237.116	5.5.5.1	TCP	26396 > http [SYN] Seq=0 Win=65535 Len=0
12	13:19:05.499487	87.101.237.116	5.5.5.1	TCP	26396 > http [SYN] Seq=0 Win=65535 Len=0
13	13:19:05.499583	134.150.46.59	5.5.5.1	TCP	44639 > http [SYN] Seq=0 Win=65535 Len=0
14	13:19:05.499588	134.150.46.59	5.5.5.1	TCP	44639 > http [SYN] Seq=0 Win=65535 Len=0
15	13:19:05.499706	21.225.58.74	5.5.5.1	TCP	34101 > http [SYN] Seq=0 Win=65535 Len=0
16	13:19:05.499711	21.225.58.74	5.5.5.1	TCP	34101 > http [SYN] Seq=0 Win=65535 Len=0

2、服务器连接数查看

netstat –an | find “SYN_RECEIVED”，检查 TCP 连接，发现大量连接处于 SYN_RECEIVED 即 SYN 半开状态下，可断定为正在遭受 SYN Flood 攻击。

netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'



```
# netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'
TIME_WAIT 16855
CLOSE_WAIT 21
SYN_SENT 99
FIN_WAIT1 229
FIN_WAIT2 113
ESTABLISHED 8358
SYN_RECV 48965
CLOSING 3
LAST_ACK 313
```

◆ ACK-FL00D

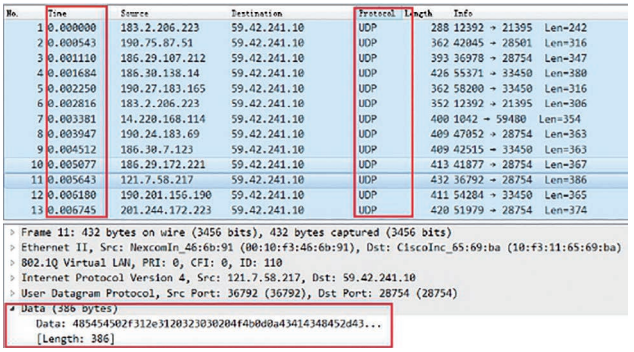
对于 ACK-FLOOD 攻击，一般情况大多数是为了消耗带宽，当我们通过分析抓包发现大量的没有建立 TCP 连接的大量的 TCP-ACK 的数据包，并且伴随着大量的重传的 TCP-ACK 的数据包的时候，基本就可以确定当前攻击为 ACK-FLOOD 攻击。

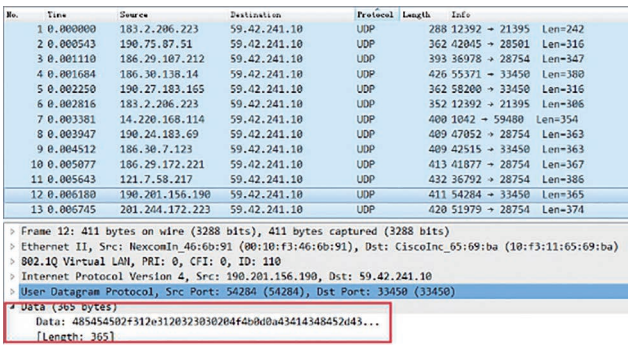
◆ ICMP-FLOOD

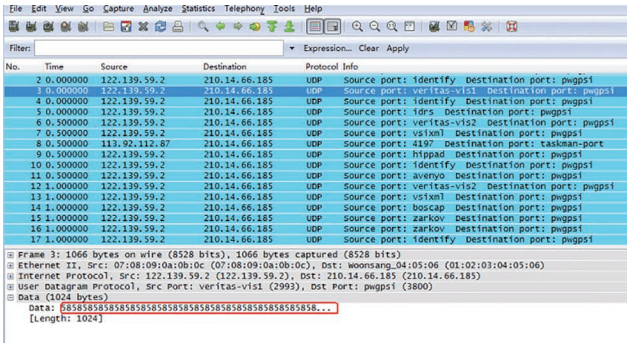
正常网络流量模型当中是会极少出现大量 ICMP 类型的数据包的，当我们抓包到的包超过 20% 的数据包为 ICMP 包的时候，有可能不是 ICMP-FLOOD 攻击，单至少表明当前网络环境中出现了问题。一个最典型的例子：当核心传输网络出现故障，某种情况下路由器会通过 ICMP 封装那些无法及时传输到目的地的数据包到服务器，导致 ICMP-FLOOD 的 DDoS 攻击告警。另外一个判断是否为真实 ICMP-FLOOD 攻击的特征是 ICMP 包的大小，一般情况 ICMP 的包大小是低于 100byte 的（除了某些特殊功能的 ICMP 探测包），那么，如果你抓的数据包中充斥这大量的 ICMP 的包，并且包大小都大于 1000byte，甚至有的时候你会发现大量的分片的 ICMP 数据包的时候，基本就可以确认是 ICMP-FLOOD 攻击了。

◆ UDP-FLOOD

由于 UDP Flood 攻击主要目的是导致带宽阻塞，单位时间内肯定会有大量的 UDP 包。同时这些 UDP 包的内容填充部分都十分相似。使用 wireshark 抓包观察，虽然 UDP 包来自于不同的源地址，访问的目的端口也不固定，但是 Data 字段部分都比较相似。







对于这类流量型（直接）DDoS 攻击，DDoS 攻击流量清洗设备的一般算法的防御效果就很好。关于设备的具体配置在这里就不做详细描述了。

4.2.2 流量型（反射）DDoS 攻击

对于流量型（反射）DDoS 攻击当前比较有代表性的攻击类型见下图：

攻击类型	放大倍数	被利用的弱点
NTP Amplification Attack	556.9	Monlist query
DNS Amplification Attack	28 to 54	Text query
SSDP Amplification Attack	30.8	SEARCH request
Charger Amplification Attack	358.8	Character generation request
SNMP Amplification Attack	6.3	GetBulk request
NetBIOS Amplification Attack	3.8	Name resolution
QOTD Amplification Attack	140.3	Quote request

大家都知道，反射型 DDoS 攻击的最大的两个特点：

1、攻击流量往往大到惊人

2、溯源困难。

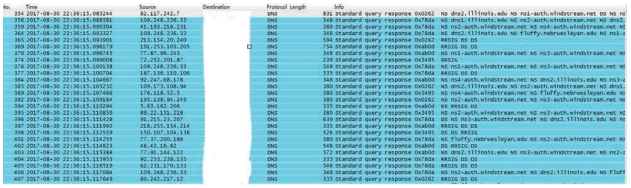
由于反射的原因，导致背后真实的攻击源（即使是僵尸网络，当然大多数也都是僵尸网络）被隐藏起来，使得使用这类攻击的攻击者往往是肆无忌惮。

对于这类攻击在排查的时候特征都很明显，就笔者以往的应急经验来说，当遭遇此类攻击的时候，不论是在清洗设备上抓包，还是在网络的探针设备上抓包。攻击流量基本都能达到整理网络流量的 90% 以上，有时候甚至达到 99%（毕竟反射型的攻击唯一的目的就是消耗网络带宽，把入口链路的带宽堵死）

此类攻击发生的时候，在 DDoS 攻击检测设备上基本出现的告警都是 UDP-FLOOD

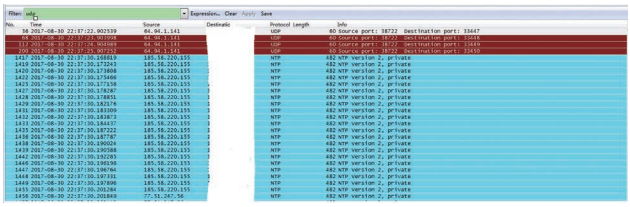
以下为此类告警抓包特征：

DNS 反射攻击



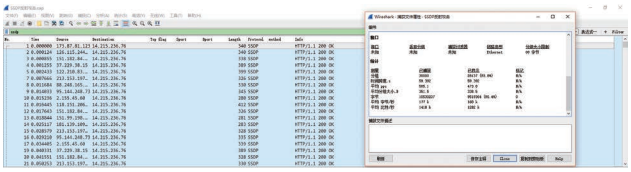
Traffic	Captured	Displayed	Marked
Packets	10000	4271	0
Between first and last packet	10143.132 sec	5.487 sec	
Avg. packets/sec	0.986	778.323	
Avg. packet size	800.381 bytes	435.261 bytes	
Bytes	8003811	1858999	
Avg. bytes/sec	789.087	338773.506	
Avg. MBit/sec	0.006	2.710	

NTP 反射攻击：



Traffic	Captured	Displayed	Marked
Packets	10000	8522	0
Between first and last packet	12.987 sec	12.305 sec	
Avg. packets/sec	769.984	692.582	
Avg. packet size	434.099 bytes	481.161 bytes	
Bytes	4340993	4100454	
Avg. bytes/sec	334249.512	333243.478	
Avg. MBit/sec	2.674	2.666	

SSDP 反射攻击：



针对这些反射型 DDoS 攻击，其实防御起来也很容易。如果攻击流量超过了链路的带宽（一般表现为带宽多少，攻击流量就多少。因为多余的流量在运营商被丢弃了，这个丢弃是基于链路带宽的最大值丢弃的，而非 DDoS 攻击防御的丢弃），此时需要通过运营商的 DDoS 攻击流量清洗服务进行。如果攻击流量没有超过链路本身的带宽，本地清洗就可以起到防御效果。还可以在边界路由器上通过 ACL 把这类流量限制掉。在本地的 DDoS 攻击清洗设备上可以配置以下策略，来彻底清洗此类反射型 DDoS 攻击的流量：

0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:65535 123:123 drop NTP Reflect

0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:65535 1900:1900 drop SSDP Reflect

0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:65535 19:19 drop CHARGEN Reflect

0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:0 0:0 drop Fragment

防护 DNS 反射攻击（DNS 反射攻击的 query 字段是 0x00ff），使用 DNS 关键字过滤防护（目前所遇到的 DNS 反射攻击，query 字段的 type，都是 0x00ff）

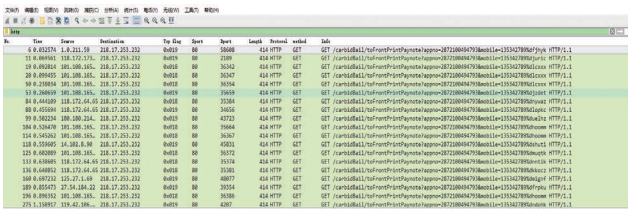
4.2.3 应用型 DDoS 攻击

对应应用型的 DDoS 攻击，最典型的还要数 CC 攻击、以及 HTTP 慢速攻击了。这两种攻击的攻击特点和流量型 DDoS 攻击最大的区别是并不需要大流量即可达到攻击效果。有些极端情况下在遭受此类攻击的时候，流量特征并没有明显的变化，业务就已经瘫痪了。

对于此类攻击，DDoS 攻击清洗设备的基础算法可以就作用没有那么明显了，需要在攻击过程中实时抓取攻击的特征，然后才好对症下药。

对于 CC 攻击来说，发生攻击时特征还是很明显的。一般情况客户在访问业务的时候不会集中在几个页面，而是比较分散的。当

发生了 CC 攻击的时候，抓包后可以很明显的发现大量的访问都集中在某几个（5-10 个）页面，那么我们可以针对这几个页面在 DDoS 攻击清洗设备上进行配置过滤。



对于 HTTP 慢速攻击来说，针对 body 慢速来说，一般的流量模型不会出现大量字节数非常小的报文。而且当发生此类攻击的时候，数据包的大小也是非常有规律的。通过分析确认这些特征后，在 DDoS 攻击清洗设备上配置对应的参数既可达到防御效果。

0x05、DDoS 攻击应急演练

为了在发生 DDoS 攻击的时候真正可以高效的开展应急工作，需要的是平时我们的不懈努力。当我们确认了 DDoS 攻击应急策略，也根据自身的特点制定了 DDoS 攻击的应急流程，并且针对各种 DDoS 攻击的具体攻击分析以及应对操作也都有了以后。就应该定期的按照以上内容进行 DDoS 攻击的应急演练，演练的形式不限于沙盘演练还是实操演练。通过演练的方式让大家熟悉我们 DDoS 攻击的应急体系，另外通过演练总结我们在 DDoS 攻击应急过程中的不足。

0x06、知己知彼，百战不殆

以下是一些针对制定 DDoS 攻击应急体系中需要或多或少考虑的问题，供大家参考。

1、所在的网络环境中，有多少条互联网出口？每一条带宽多少？

2、每一条互联网出口的运营商是否支持 DDoS 攻击清洗，我们是否购买，或可以紧急试用？当发生 DDoS 攻击需要启用运营商清洗时应急流程是否确定？

3、每一条互联网出口的运营商是否支持紧急带宽扩容，我们是否购买，或可以紧急试用？

当发生 DDoS 攻击需要启用运营商紧急带宽扩容时应急流程是否确定？

4、每一条互联网出口的线路是否都具备本地 DDoS 攻击清洗能力？

5、本地抗 DDoS 攻击设备服务商是否提供了 DDoS 攻击的应急预案？

6、所有需要我们防御的业务是否都在抗 DDoS 设备的监控范围内？

7、出现 DDoS 攻击的时候所有需要自动清洗的业务是否可以自动牵引并清洗？

8、是否有内部针对 DDoS 攻击应急的指导流程？

9、当发生 DDoS 攻击的时候如何第一时间感知？

高防云清洗平台建设与运营之道

IIS 产品管理团队 张鹏

关键词：DDoS 运营商 CDN 云清洗平台 云清洗服务

摘要： DDoSh，尤其是带宽资源的对抗。拥有海量带宽资源的运营商或 CDN 网络厂商该如何利用自身的带宽资源优势，快速建立匹配自身条件的高防云清洗平台并开展云清洗服务增值运营？本分享将逐步解析高防云清洗平台建设与运营之道。

DDoS 黑色产业链规模越来越大，客户面临 DDoS 攻击的风险日渐增大，其中政府、金融、互联网企业、游戏等客户是遭受 DDoS 攻击的高发行业。DDoS 攻击流量屡创新高。遭受攻击的客户急需有效的 DDoS 攻击清洗服务来保障自身业务安全，拥有带宽资源的服务商（如运营商、CDN 厂商等）也正在寻找新的业务增长点。云清洗服务是应对 DDoS 攻击，尤其是大流量 DDoS 攻击的关键手段。随着 DDoS 攻击频次和峰值的逐年增加，云清洗服务市场迎来了高速发展的黄金时期。但凡有一定带宽资源储备的服务商，都在积极考虑或已经在着手建设自身的高防机房和运营平台，以期能够抓住这一关键市场机遇。

不断加剧的老龄化趋势使得中国运营商告别了用户高增长的黄金时代，随着网络带宽的提速降价，数据流量增长和运营商增收不成比例。在新兴的互联网领域运营商的产业链控制地位不复存在。各种云等新兴互联网巨头通过提供带 DDoS 防护的云上主机和带宽租用，抢夺运营商的客户资源。此外，一系列监管方面的挑战使得运营商的传统业务“疆土”不断收缩。

在数字化变革的大潮中，运营商传统优势遭到侵袭的同时，也面临着变革带来的新机遇。国内运营商的当务之急是积极寻找新增市场，比如开展云清洗增值服务。运营商建设云清洗平台，开展云清洗服务在技术方案上有绝对的技术优势，运营商开展云清洗服务

面临的挑战主要来自于市场化程度不够，很多运营商都无法提供有效的 DDoS 攻击清洗服务。这里主要面临投入成本、专业的抗 DDoS 硬件设备、建设周期、安全专业人员、抗 D 技术和安全运营能力等因素的制约。

CDN 网络抗 DDoS

CDN 的全称是 Content Delivery Network，即内容分发网络。简单来说就是通过在网络各处放置节点服务器，让用户能够在离自己最近的地方访问服务，以此来提高访问速度和服务质量。业务稳定性三要素的风险从本地移到云端，从单点转换成多点分担。使用云端 CDN 进行 DDoS 防御的三大优点，包括、1 **冗余带宽和资源**；2 **平时加速，战时防御**；3、**专业的运维团队**

除此之外，相对应运营商其服务的市场化程度，客户体验，整体安全能力提供方面有优势，但其受限于牵引技术和带宽资源，服务提供有局限性。

技术流派对比

厂商	技术方案	优势	劣势
国内运营商	在国干和省干节点处建立清洗中心 BGP牵引	延时小，速度快	国内运营商： 1、多个运营商多张网，各家清洗各家 2、市场化程度不够
以BAT为主	自建高防机房（清洗中心） DNS牵引	1、云主机标配抗D服务，经济实惠适合云上客户 2、全局资源，分布式部署，清洗容量大 3、弹性计费	1、DNS牵引有一定的延时 2、直接针对目的地址的攻击很难有效防御 3、仍然有被打满的风险 4、https的防御需要上传证书和私钥，大多客户都有顾虑
CDN厂商	自建高防机房（清洗中心） DNS牵引	天生具有分布式清洗能力	1、带宽是CDN服务商的核心资源，意味着其不可能在抗D上投入太多带宽资源。DNS牵引有一定的延时 2、直接针对目的地址的攻击很难有效防御 3、仍然有被打满的风险 4、https的防御需要上传证书和私钥，大多客户都有顾虑

在未来的市场竞争中谁能够胜出，取决于谁能更好、更快地通过技术和业务创新攻克自身劣势。

绿盟云清洗平台建设思路

运营商网络：

第一步：运营商提供带宽资源和机房空间，绿盟科技提供专业抗 D 设备和实施运维团队。流量监控设备 NTA 分布式部署在骨干网中组成异常流量监控系统用于检测异常流量，一旦发现异常流量，自动联动清洗设备进行清洗。流量清洗设备 ADS 和 ADS-M 组成流量清洗系统，根据流量监控系统监控结果将异常流量牵引到清洗系统中进行清洗。运营商可以考虑分批建设，可以优先考虑骨干网，后面再逐步扩容。

第二步：在异常流量监控系统与流量清洗系统基础之上，通过部署绿盟科技云清洗中心运营平台，提供运维自动化、清洗可视化和操作简单化，极大地降低运维工作量并提升客户体验，实现规模化运营和创收的云清洗中心。同时增加业务拨测系统辅助流量监测系统提高异常流量监测准确率，与绿盟云威胁情报系统联动，将最

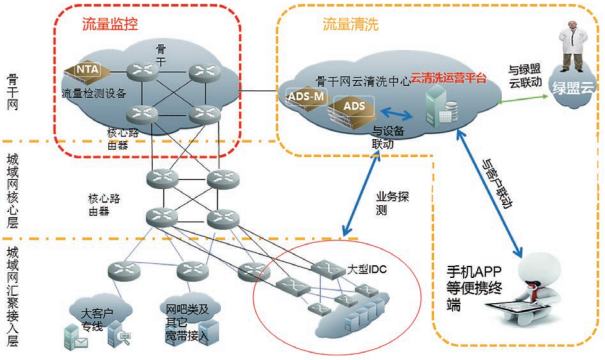


图 1.1 运营商网络云清洗平台设计方案

新的威胁情报转化成防护能力，如 IP 信誉数据有助于提高异常流量的清洗速度和性能。

CND 网络

通用节点满足日常需求、高防节点负责流量对抗；风险均摊，鸡蛋不能放一个篮子里；有更高级别的高防节点或第三方清洗资源作为最后的防线。

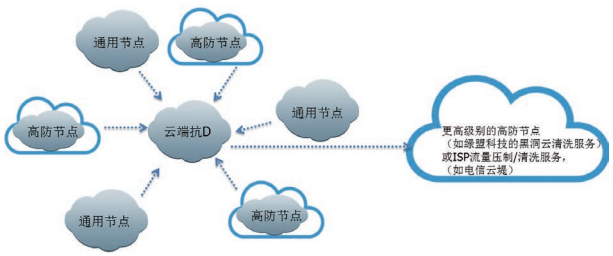


图 1.2 分散清洗，风险控制

上图中分散的抗 D 网络面临如下问题亟待解决：多点防御如何统筹？攻击点分散如何解决？服务站点多怎么办？

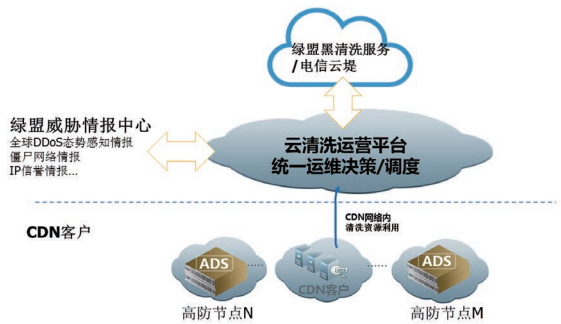


图 1.3 CDN 网络云清洗平台设计方案

CDN 防御 DDoS 需要的不是一个防护设备，需要一套统一的决策和运营系统打造一个整体防护体系。如下图所示，各高防节点通过部署绿盟科技 ADS 具备 DDoS 攻击清洗能力；通过部署绿盟科技云清洗运营平台，负责多点防御统筹，轻松解决攻击点分散问题，联动威胁情报系统和第三方清洗资源，防护能力无限度提升。

绿盟云清洗平台运营思路

运营方案架构

云端管理平台提供业务开通、监控运维、监控可视化展示、统计报表可视化展示等集中运维能力，云端管理平台可与管道侧异常流量监控系统和清洗系统联动，策略自动下发，降低人力维护投入，开放大量客户端自助服务权限，客户可灵活通过 PC、大屏和智能终端进行自助服务，如自助 / 自动清洗、手机信息实时推送、清洗流量报表和攻击溯源信息查看等。可以简单理解成云端运维，管道侧自动下发配置，客户端灵活自助的云、管、端运营架构。

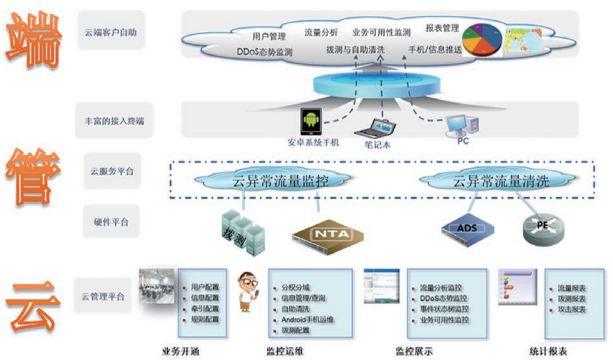


图 1.4 云清洗平台运营方案架构

运营平台系统架构

便捷的自助服务系统提升用户体验，强大的云清洗管理平台将大量运维工作自动化实现，几个人的运维团队可以搞定 10 万级规模的客户运维工作。

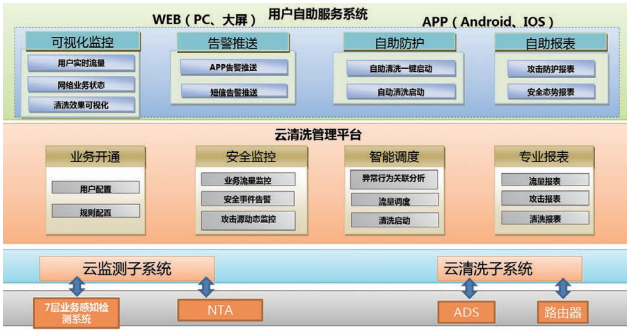


图 1.5 云清洗运营平台系统架构

攻防实践案例

2016 年 12 月 29 日晚 9 点多，珠海某 IDC 大客户受到 DDoS 攻击，申请广东某运营商的云清洗服务（绿盟科技云清洗平台解决方案成功实践客户），几分钟后运维人员通过云清洗平台为该客户开启清洗服务进行攻击防护，这个防护响应速度在没有建设云清洗平台前是不敢想象的。

同时在手机 APP 端有通知信息，显示 21 点 51 分清洗设备上开启清洗策略成功。当时攻击已经停了，并没有立即进行清洗，而是等到 22 点 54 分的时候，攻击者发起了新一波次攻击，攻击立即被检测到并成功清洗。在 30 日上午 9 点 56 分，攻击者还不死心，又发起了第二波攻击，同样无功而返。整个清洗过程无论是客户还是

运维人员都能通过手机 APP 实时获取，全程掌控 DDoS 攻击和清洗情况，清洗体验超级棒。

DDoS攻击详情

全局流量趋势

DDoS告警信息

DDoS告警动态

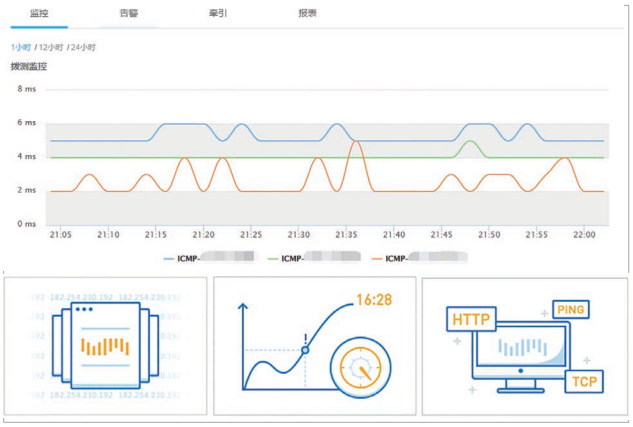
客户想了解更多有关攻击和清洗的信息，都可以通过手机 APP 或 Web 页面获取。当信息呈现到客户手机上时，直接让用户信服，立马决定采购全年的云清洗服务。

客户的价值

智能

1、攻击智能检测：

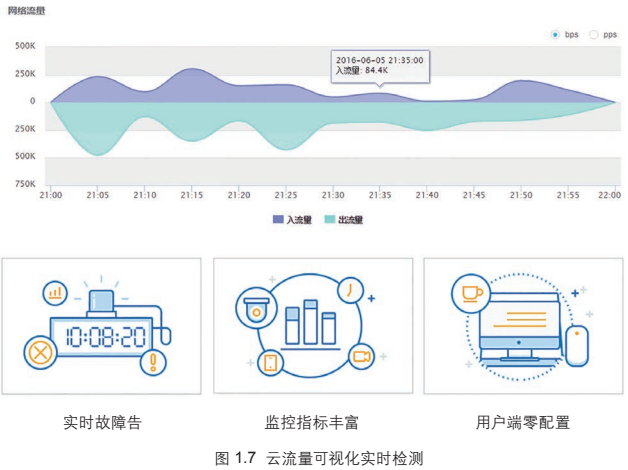
业务可视化检测 + 云流量检测双重指标保障攻击智能检测的准确率。业务可视化检测，给客户业务提供实时 “心电图”



业界领先监测网　　分钟级拨测周　　支持多种协议探

图 1.6 业务可视化检测

云流量检测，给客户提供可视化实时流量数据：



实时故障告　　监控指标丰富　　用户端零配置

图 1.7 云流量可视化实时检测

2、流量智能调度

一旦判断自动进行流量调度无需人员干预，或选择自助清洗的客户进行一键调度指令下达，流量会根据指令进行智能调度

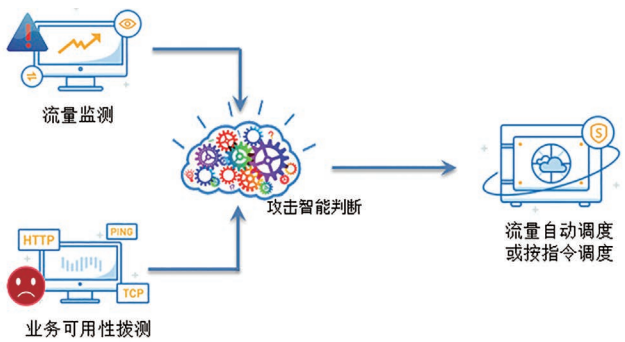


图 1.8 流量智能调度

3、威胁情报智能共享

绿盟云威胁情报中心提供最新的威胁情报给各级防护系统以提高抗 D 能力。如 IP 信誉数据、僵尸 CC 主机信息、新型 DDoS 攻击防护算法等。

敏捷

自动 / 自助清洗

自动清洗，秒级响应，一旦发现攻击，自动进行清洗，无需人工参与。同时可以按照客户要求提供自助清洗，是否清洗由客户决定，客户可以执行一键云清洗。

图 1.9 自动和自助清洗

可运营

服务可视化能力降低维护工作量，主要体现在三个方面：

1、系统概况信息呈现清晰：

24 小时概要统计：

图 1.10 24 小时概要统计

24 小时告警情况：

图 1.11 24 小时告警情况

24 小时流量清洗情况：

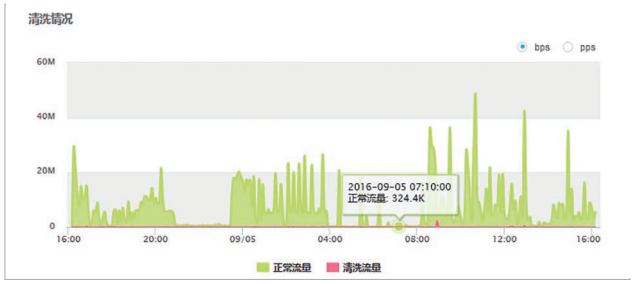


图 1.12 24 小时流量趋势图

24 小时拨测和流量监控情况：

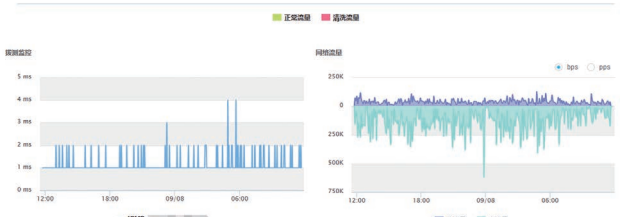


图 1.13 24 小时业务拨测和流量监控

2、业务配置可视化：

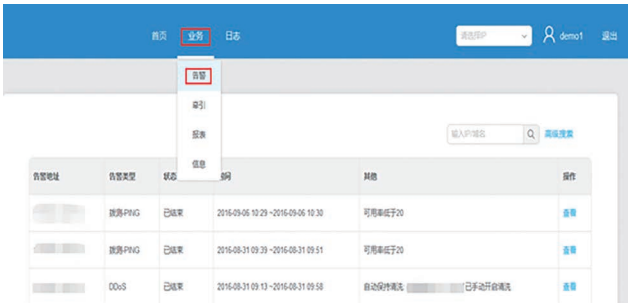


图 1.14 业务配置

可以对告警信息、牵引信息、报表信息和客户信息等业务进行快速配置。

3、APP 自服务提升客户体验，可规模化运营：

图 1.15 APP 全称自助服务

总结

绿盟科技作为国内抗 DDoS 市场的领先者，拥有过硬的抗 DDoS 产品、强大的清洗中心运维平台、完整有效的抗 DDoS 方案以及安全专家和运营经验，正在与运营商、CDN 网路厂商等资源方开展双赢合作，协助其通过业务和技术的不断创新，在云清洗市场完成其增值业务的华丽绽放。

抗DDoS安全服务体系简介

IIS技术团队 郑彬 陈裕涛

关键词：抗拒绝服务系统 抗 DDoS 服务 运营商抗 DDoS 服务 可管理安全服务
黑洞云清洗服务 云清洗运营平台

摘要：为适应不同业务场景，有效应对 DDoS 这种低成本高毁伤的攻击形式，绿盟科技抗 DDoS 安全服务体系历经多年的发展，已经覆盖了代维、服务、增值三大 DDoS 安全服务场景，且具有极高的灵活性和扩展性。本文为大家介绍这个服务体系的应用特点，便于客户结合自己的需求，进行相应的选择。

一．抗 DDoS 安全服务

随着计算机性能和网络的发展，DDoS 已经发展为一种门槛低、成本小而且能够严重影响客户业务的攻击手段。各大服务厂商都已经建立的基础的 DDoS 防护设施，为用户提供基本的安全保障。

绿盟抗拒绝服务攻击系统能够及时发现背景流量中各种类型的攻击流量，针对攻击类型迅速对攻击流量进行拦截，保证正常流量的通过。该防护设备经过了十多年的不间断技术创新和产品研发，已经成为了国内抗拒绝服务市场的领先者，广泛部署在各大银行，运营商客户，保障客户的业务安全。随着市场的发展，除了对本地抗 DDoS 的需求不断完善细化，也出现许多抗 DDoS 服务商，为客户提供简单易用的抗 DDoS 安全服务，完善抗 DDoS 整体解决方案。

抗 DDoS 安全服务是由服务提供商为其客户提供 DDoS 防护能力的手段，减少 DDoS 攻击给客户带来的影响，客户得以把注意力集中在业务发展，保证高速增长。

二．服务市场概况

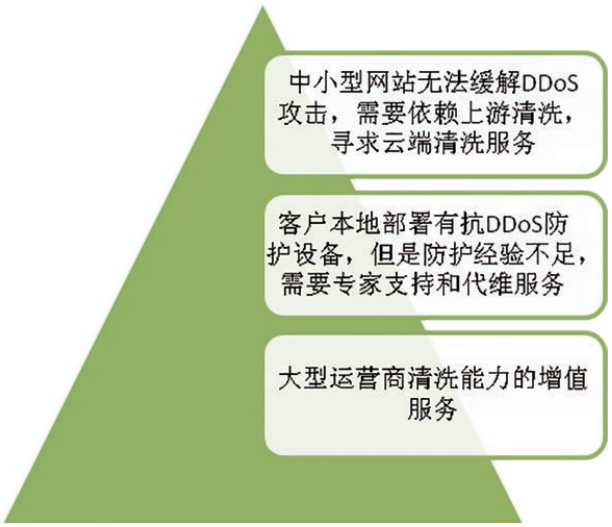
在运营商行业，各大运营商提供的服务越来越精细，对客户服务质量的保障不断促进安全能力的发展。大量的攻击流量在网络中

消耗运营商带宽，并且影响客户业务质量，网络安全整治不但是运营商自身成本的需求，更是运营商的网络服务的需求。

另一方面，客户的运维能力也在不断成熟，在购买运营商带宽的同时，也产生了安全运维的需求，希望能够运营商能够开放安全能力，帮助客户快速响应解决安全问题。DDoS 高防增值服务也成为了运营商的新一个增长点。

中小企业因自身规模小，竞争激烈，开始寻求安全服务以解决在快速增长过程中的潜在风险，DDoS 攻击更是他们的噩梦，可能导致长时间的业务不可用，造成大量的经济损失。部分企业自身会购置安全设备，但是因为安全经验缺失，需要安全代维服务，以更好的保障自身业务。

目前绿盟科技提供的 DDoS 安全服务包括可管理安全服务、黑洞云清洗服务、云清洗运营平台，全面覆盖了代维、服务、增值三大 DDoS 安全服务场景，共同组成了绿盟科技 DDoS 安全服务体系。



三．可管理安全服务

绿盟抗拒绝服务系统（可管理系列）（NSFOCUS ADS with MSS）是绿盟科技在原有 ADS 和 NTA 产品的基础上，进一步融合云安全技术，推出的 7x24 小时 DDoS 防护解决方案。ADS with MSS 可以实现将客户本地的 ADS 和 NTA 设备与绿盟安全云对接和同步，由绿盟安全专家团队协助企业实现对 DDoS 攻击全天候监视、响应、防护服务。

云监护方案由 ADS 设备及设备上云监护模块、绿盟安全云、绿盟安全专家团队组成，ADS 设备实现 DDoS 攻击流量的过滤；

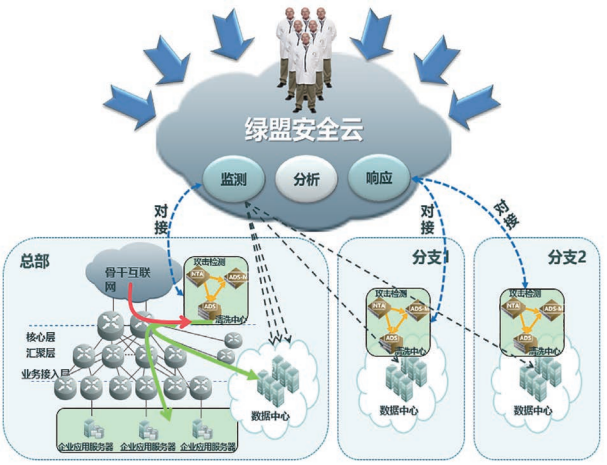
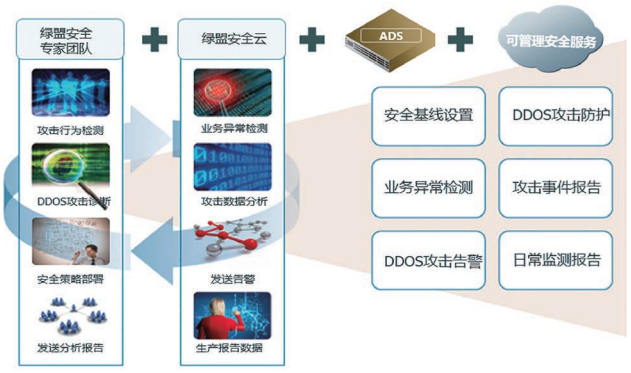


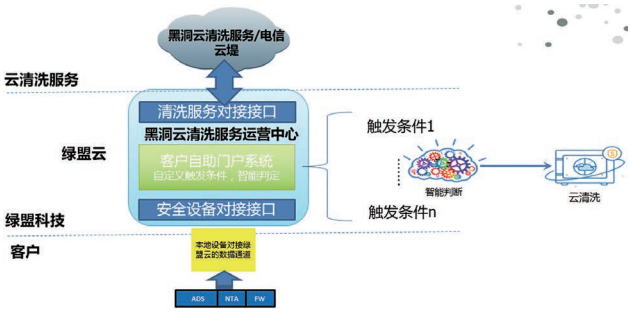
图 1 绿盟科技可管理安全服务整体架构

云监护模块实现流量日志、攻击日志信息的上传；绿盟安全云自动监测客户业务的异常，对攻击与流量日志进行数据分析，向专家呈现分析结果；绿盟安全专家团队对攻击进行诊断和分析，通过云安全中心，在 ADS 设备上部署安全策略。



四 . 黑洞云清洗服务

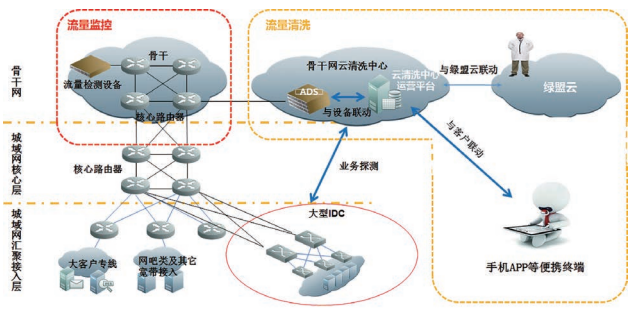
黑洞云清洗服务利用云端清洗源来有效应对突发大流量 DDoS 攻击的服务产品，该服务可以帮助客户在遭受大流量 DDoS 攻击时，将客户流量牵引到云端清洗资源进行流量清洗，清洗后的流量在回注给客户，此时即使还存在小流量的应用层 DDoS 功能，完全可以通过本地清洗设备的防护算法进行有效防御。黑洞云清洗服务是一项云清洗服务，定位于本地清洗备援服务，主要帮助客户突破本地清洗方案的局限，以最小的经济投入应对大流量 DDoS 攻击。



五 . 云清洗运营平台

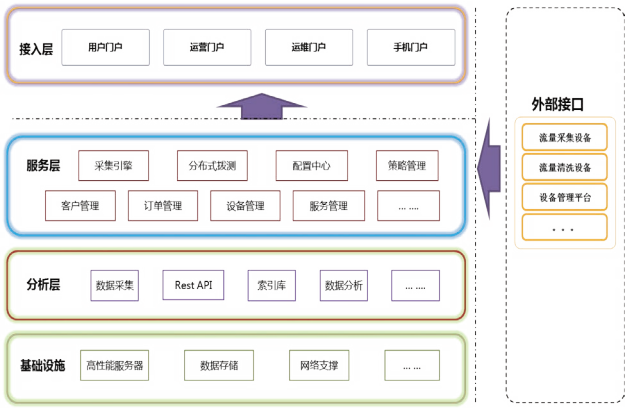
云清洗方案要解决的核心问题，是如何对 DDoS 用户进行集中化运营管理，快速响应攻击，实时呈现攻防对抗过程，以提升客户的使用体验，产生价值，从而进一步实现批量放号，规模化运营，为我们的客户产生经济效益。

基于上述考虑，我们推荐的云清洗中心的部署方案，是采用集中式的部署方案。在此方案中，关键的部件有流量采集设备（如 NTA）、流量清洗集群（如 ADS 设备集群）、设备运维管理中心（如 ADSM）、云清洗平台。通过部署 NTA 设备或者集群进行流量采集，将实时流量上传给云清洗平台，云清洗平台以客户为视角，进行流量的实时分析，识别出流量威胁之后，产生实时的告警信息推送给



相应客户，同时对流量进行合理调度，将流量牵引到合适的 ADS 设备或者集群进行清洗。等攻击事件结束之后，能够导出详细报表，发送给 DDoS 用户。

云清洗平台是云清洗中心方案中的大脑和指挥中枢，起着攻击监测、业务拨测、流量调度的重要作用，将事前监测、事中防护、事后总结的流程串接起来。平台的总体视图如下：



平台分为基础设施、分析层、服务层、接入层等平面，基于基础设施的支撑，云清洗平台提供了 web 接入、手机接入等多种接入方式，支持与流量采集设备、流量清洗集群、设备管理平台等系统进行对接。

云平台内部主要分为存储层、数据分析层、服务层、WEB 展示层这几个层次，分别负责数据存储、数据分析、后台逻辑处理、用户访问接入。为了保障业务的伸缩性，不少部件都是独立可扩展的，例如拨测模块和采集模块，随着客户数量的增加，需要消耗的性能是递增的，因此将模块单独剥离出来，支持平行扩容。

为了保障数据的安全性，同时为了减轻数据库压力，提升查询速率，数据存储也独立出来，形成了单独的高性能存储集群。

为了提升云清洗平台站点的并发访问数量，web 展示层也放在了单独的服务器上，通过负载均衡技术，可以支持横向扩展服务器数量，提升并发访问能力。

六 . 抗 DDoS 服务的发展前景

目前绿盟科技抗 DDoS 安全服务体系已经覆盖了代维、服务、增值三大 DDoS 安全服务场景，且具有极高的灵活性和扩展性，但从日益增长的各行业抗 DDoS 服务需求来看，用户还在如下领域有着不小的需求：

- 需要进行安全服务的多样化及定制化需求，以进一步贴合行业业务特点；
- 需要增强数据分析维度，从而对攻击事件进行深入分析及信息提取；
- 需要强化平台的集成化水平，以便改善对客户的服务管理及对设备的控制要求；
- 需要完善虚拟化安全设备管理，以更为灵活的平台运营适应快速发展的业务需求；

正是看到了这些需求，绿盟科技正在不断推进抗 DDoS 安全服务的创新和研发，完善在不同场景下的解决方案，为客户提供全面的安全保障，做好巨人背后的专家!

证券业金融企业网络安全建设进阶

——运用攻击者视角搭建企业防御框架

金融技术部 俞琛

关键词：企业网络安全建设措施　金融网络安全　金融行业网络安全　金融行业信息安全

摘要： 证券业拥有庞大的数据处理量，2016 年全国证券系统日均交易量达一万亿元，是中国金融市场中最活跃市场，因而其对于安全提出更高要求。本文运用攻击者视角，介绍攻击链并列举攻击者的攻击动机，并通过搭建企业防御框架，并拟定针对性的入侵防御方案，对目标进行重点防御，即在安全建设基础上提出信息对抗、技术对抗、运营对抗三方面的进阶，读者可以按需参考。

前言

开展信息安全工作其中一个主要目标就是安全保障，防止信息安全事件的发生。然而，部分企业在多年开展了网络安全建设工作后，还是会有信息安全事件发生。Nuix 公司《The Black Report》[1] 中显示，81% 的受访黑客（白帽子）表示，12 小时之内就能攻破一个目标（如一个站点），发现并窃取重要数据。相对应的，64% 的受访企业代表表示，企业明知道自己存在安全问题，却不修复。企业在攻击发生后，只有四分之一的攻击事件采取了修复措施，但也仅仅关注高危漏洞。

试问，企业网络安全现状如何？是好是坏。面对如此问题，很难准确回答。我们先来了解 2 项定义（摘自《GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南》）：

1. 信息安全事件：由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

2. 信息安全事件分类：信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等 7 个基本分类。

对于能否保证避免信息安全事件发生，业内企业安全团队通常是一片悲观情绪，认为防守方总是处于劣势。因为防守方面对的是一个开放性的安全防御难题，建设的防御体系往往如同“马其诺防线”一样被攻击者绕开。 但如果防御体系解决的是一个明确的企业物理范围和业务系统范围，即有清晰的防御目标，如明确业务范围是证券业交易 WEB 平台和交易 APP，防御目标是避免客户信息和交易记录泄露事件发生，且保障业务系统在交易时段内可用性达到 100%，且达到分钟级安全控制风险（应急响应）防护能力，那么我们的防御体系是可以做到闭环。简单说，一个问题不能犯两次，通过闭环运营让企业自身安全能力不可逆地走向更好。

笔者曾撰稿提出证券类金融企业网络安全建设思路，是首先优化网络结构，减少网络安全高危漏洞或缺陷数量，通过部署抗拒绝服务攻击、网络入侵防护和恶意程序防护措施提高基础安全水平，采取网络流量分析技术、安全意识培训、监测与防护措施等，应对高级别攻击。为了持续提升安全防护水平，满足业务发展需要和安全保障需求，在开展网络安全建设时，需要不断调整防御目标，学习理解并运用攻击者视角，搭建防御框架，达到防护能力能够囊括更多安全事件类型的进阶目的。

一．攻击者视角

为了保护低价值目标而投入过多资源是不经济的。防守方学习攻击链（攻击过程），以攻击者思维换位思考攻击目的，识别攻击者眼中的高价值目标，进而定义防御目标，才是有效应对之策。

1.1 攻击链

简单来说，攻击链就是攻击者常见攻击过程，包含信息收集、探测、渗透攻击到实施恶意行为等步骤。通常，攻击链可以图 x 形式展示。不同攻击方式的攻击过程可能不同，半数攻击者每一次都会改变具体攻击方法。

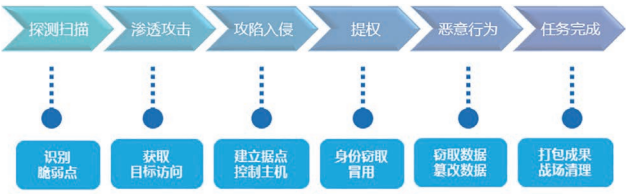


图 X 攻击链

FireEye 在 2017 年 3 月发布的《Mandiant M-Trends 2017 Report》[2] 中显示，针对金融企业的攻击者采用钓鱼邮件攻击时，会运用社会工程学辅助。为了绕过企业邮件安全网关防护，在发送含有恶意链接或恶意附件的邮件之前，通过电话与内部员工联系，获取员工信任放行收到的钓鱼邮件，完成攻击过程。这个示例攻击过程并不包含控制主机和战场清理。

1.2 攻击动机

了解你面对什么样的攻击者，可以让你理解他们的动机。

在 2017 年上半年，针对证券业的信息安全威胁主要由 DDoS 攻击、WannaCry 勒索事件、客户资料数据窃取等，需要关注事件背后的攻击动机。如果有人用脚本小子 (Script Kiddie) 取得的工具来攻击你，这可能并非严重的威胁。如果有人用新的漏洞和精心设计的恶意软件来攻击你，如绿盟公司在 2015 年发现的证券幽灵攻击，潜伏最长十多年，默默窃取交易数据，那就要重点关注了。他们的能力可能也反映了他们的意图。例如，故意破坏（如篡改网站）比较可能是激进黑客，或许是政治目的攻击活动。但大多数攻击的目标是窃取信息，有时可能是可以马上换钱的金融信息，如支付凭证。有时可能是更加敏感的信息，如公司机密。《Mandiant M-Trends 2017 Report》中显示，较之欧洲、美洲区域，亚洲金融行业是全世界黑客主要攻击目标，针对金融企业的攻击复杂性逐步增加，攻击特点是不摧毁，更贪婪。

二．防御框架

理解和分析攻击链是关键，可以帮助企业在必要阶段部署适当的防御控制。运用攻击者视角，搭建企业防御框架。笔者建议防御策略包含明确防御目标、开展信息对抗、技术对抗、运营对抗三方面进阶建设。

明确防御目标，莫过于确认攻击者的动机，然后根据此动机判断入侵最可能发生的节点以及攻击方式，并拟定针对性的入侵防御方案，对目标进行重点防御。

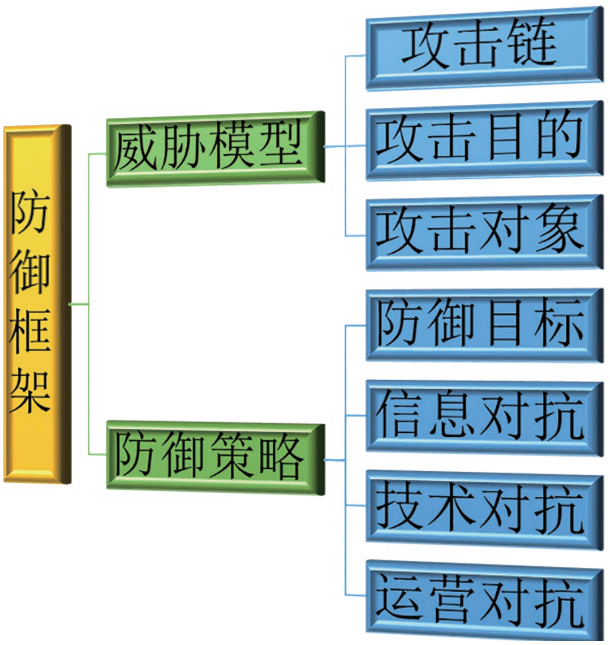


图 X 防御框架

2.1 信息对抗

信息对抗，目的是知己知彼，提供针对性设防的有效信息，并在事件发生时持续监控，获取攻击者攻击行为的信息。威胁情报就是有效信息，还原已发生的攻击事件、预测未发生的攻击威胁和提供应对建议，通常包含 IP 信誉库、漏洞库、武器库等，可为企业安全团队提供如何响应威胁或危害的决策信息。信息对抗关注信息的时效性和行业属性，如网络游戏行业、政府、金融企业的攻击者和

攻击动机差异很大。

证券业对外服务的重要系统以交易 WEB 平台和交易 APP 为主，通过收集威胁情报，掌握国内外已发生的特定信息安全事件所利用的已知漏洞，是否与企业交易 WEB 平台存在的漏洞，或交易 APP 某项业务流程缺陷有关联，从而提出漏洞缺陷修补优先级。威胁风险分析过程需要将信息资产、存在漏洞信息、威胁信息综合分析，得出风险高低结果。

目前，已有国内安全厂商可提供威胁情报平台，支撑企业威胁风险分析和决策。

2.1.1 IP 信誉库

IP 信誉库提供攻击源信息，通过配合设备指纹、时间属性来锁定攻击者的身份和物理位置。对于企业来说，一旦攻击者实施了恶意行为，如盗取第三方企业数据，就可以根据溯源结果进入法律程序。

通常，为了方便使用，提高溯源和运营效率，IP 信誉库信息以攻击类型进行分类。

IP信誉库的攻击类型列表

分类id	分类值	中文名称
0	Other	恶意
1	DDos	DDoS攻击
2	Exploits	安全漏洞
3	Spam Sourc	垃圾邮件
4	Web Attacks	Web攻击
5	Scanners	扫描源
6	Botnets	Botnet客户端
7	malware	恶意软件
8	phishing	钓鱼

图 X IP 信誉库分类表

2.1.2 漏洞库

Struts2 依靠连续 5 个漏洞成为 2017 上半年的一个焦点。在 S2-045 爆发的一周内，绿盟科技威胁情报中心监测到 19,396 次针对该漏洞的攻击尝试。针对 Struts2 利用的攻击次数超过所有框架及应用漏洞攻击总次数的 80%。当有关键业务运行于 Struts2 框架之上时，24x7 的漏洞监视机制、小时级的通报响应机制变得尤其重要。

2.1.3 武器库

武器库提供攻击者攻击方式的有效信息。以 XSS 攻击为例，XSS 是 WEB 应用攻击威胁，又叫 CSS (Cross Site Script)，跨站脚本攻击。它指的是攻击者往 Web 页面里插入恶意脚本代码，而程序对于用户输入内容未过滤，当用户浏览该页之时，嵌入其中 Web 里面的脚本代码会被执行，从而达到恶意攻击用户的特殊目的。跨站脚本攻击的危害通常是窃取 cookie、放蠕虫、网站钓鱼等。利用过

图 X XSS 攻击核心步骤

程即攻击者找出站点内动态表单页面，如含有富文本编辑器（自定义样式）的注册页面，通过插入特征文本、构造 XSS 代码、猜测过滤规则、用等价代码替换实施攻击。之后，只要用户注册该平台会员账号，这个包括恶意脚本的页面就被其本地浏览器执行，攻击者就可能获得该用户终端浏览器当下进程的注册信息（cookie）。整个过程未控制主机，仅是植入恶意脚本，即实现数据窃取的恶意行为。图 X 是 XSS 攻击核心步骤展示。

2.1.4 威胁处置效率

为了有效地应对挑战，需要快速适应信息安全管理理念的变革，那就是将传统安全投入只注重防护”Prevent”，不断向检测、响应、预测和持续监控转移，实现动态适应。只有化被动安全为主动安全，才能及时检测正在发生的威胁，甚至预测即将发生的威胁，快速地响应将成为安全团队新的聚焦点。

威胁处置效率，从被攻陷到处置的耗时，是衡量最高级别威胁处置效率的指标。平均检测时间 (MTTD) 和平均响应时间 (MTTR) 作为两个衡量企业安全能力的关键指标，已经被更多企业采纳。MTTD 是企业识别出影响公司的威胁所需的平均时间。这些威胁表现出实际的风险，需要进一步的分析和响应工作来验证。 MTTR 是企业完全分析威胁并控制和解除威胁所需的平均时间。MTTD 可被计为企业信息环境中第一次证明 (收集到的) 的威胁到其真正被安全团队发现的这段时间。 MTTR 可被计为从威胁被检测确认到最终锁定存在风险或解除风险的这段时间。根据 2016 年 FireEye(火眼) 公司发布的报告, 企业从被攻陷到发现的平均时间 (MTTD) 是 146 天。而平均 MTTR 是 30 天。

不难看出，降低 MTTD 和 MTTR 必须建立有效的威胁检测和响应生命周期。 而在这个检测与响应的每个阶段，能够以威胁情报驱动，并不断优化每个阶段的安全操作流程有效性的公司可以实现 MTTD 和 MTTR 的显着改进。

2.2 技术对抗

通过部署抗拒绝服务攻击、网络入侵防护和恶意程序防护措施提高基础安全水平。以信息安全经理思路开展安全建设，可参考笔者编写的《证券类金融企业网络安全建设方法与思路》。结合证券业现状，笔者补充了对于证券业适用的漏洞管理问题、客户资料泄露应对、互联网资产暴露检查方法。

2.2.1 漏洞管理

通常，证券业金融企业自身拥有互联网信息系统和内部信息系统，防护对象重心是互联网侧系统。WannaCry 勒索事件，证明内网不是绝对的安全。攻击者利用已知高危漏洞，采用蠕虫传播恶意木马，对内部信息系统（办公终端）发起攻击。

如何在种类繁杂数量众多的漏洞中，明确修补加固优先级。笔者建议，首先梳理资产，识别哪些是核心系统。证券业的核心业务大致是开户 APP、交易 APP、理财 APP 及门户网站。之后，明确每个系统的责任人。通常，系统的拥有者就是第一责任人。然后，设定漏洞管理安全红线，通过梳理历史漏洞，采用清单列表形式将必须加固整改的漏洞列示出来。

漏洞整改清单，是将漏洞分为三类：厂商补丁、配置管理、操作

类。厂商补丁修复方法可能为打厂商补丁或升级软件版本，配置管理类修复方法可能为修改配置文件，操作类漏洞修复方法可能为执行某操作。各系统管理员对服务器的漏洞进行修复时，对清单中漏洞风险等级“高”，必须修复，并明确修复时间计划。其中，对涉及打补丁、升级版本的修复方法，首先按要求确认安全处是否发布补丁或版本，如未发布，可不修复；如已发布，可在变更时间内修复该漏洞，并明确修复时间计划。漏洞检测和加固的可选方式如下说明。

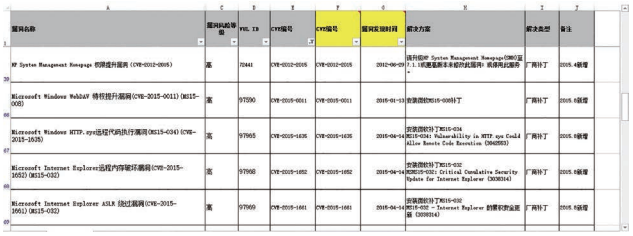


图 X 漏洞整改清单示例

■ 漏洞检测

- 在线检测，输入互联网应用 URL，在线检测 WEB 应用漏洞
- 日常检测服务，由第三方安全厂商提供服务，如绿盟网站监测服务包含漏洞扫描与验证服务
- 扫描器检测，采购或租用漏洞扫描工具，由企业自有团队开展定期漏洞检测工作，可使用绿盟 RSAS 和 WVSS 对 Web 应用进行扫描

■ 漏洞加固

- 补丁修复，下载官方补丁并安装
- 临时方法，如暂时无法升级 Struts 框架，可以采用禁用 XML 请求
- 纵深防御，互联网接入区部署入侵防御系统 IPS

2.2.2 客户资料泄露应对

多数情况下企业仅凭依赖其IT部门来完成防护重点对象的确认，但实际上重点防护对象不仅限于 IT 部门所管辖的 IT 资产。

应对数据泄露的安全防护方案是个大课题，本节介绍在明确系统范围和特定数据（客户姓名、手机号码、交易账号）场景下的安全分析思路。基于此，后续扩大范围覆盖，逐步提高数据防护能力。

证券业客户开户 APP 和在线交易 APP，梳理 APP 重要数据流，找出相关系统处理客户信息（手机号码、交易账号）的所有场景，包含数据生成、存储、传输、使用、导出 / 下载、删除，评估结果是提交关注数据存在泄露风险点，并对高危风险点提出整改建议。

2.2.3 互联网资产暴露检查

攻击者探测扫描攻击对象，暴露在互联网资产每天被上百次扫

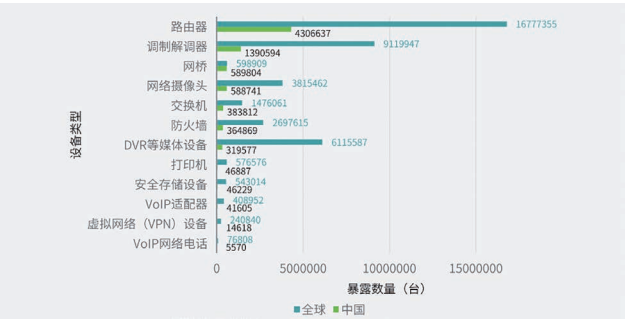


图 X 全球和国内物联网相关设备暴露情况

描司空见惯。绿盟科技《2017上半年网络安全观察》中显示，全球和国内物联网相关设备暴露情况，路由器、网络摄像头等设备的暴露数量统计。

证券业广泛采用CDN技术在全国设置多个分节点，提供用户通过互联网连接访问。新上线业务开通审批相对严格，但一段时间后，业务的使用状况、端口开放情况就基本失控了。结合行业互联网资产在物理位置上的分散部署，更有必要开展暴露资产检查。梳理企业自身所有互联网IP地址段和域名（如能提供尽可能完整的二级域名信息会更好），通过工具检查可以发现企业安全团队未知的互联网存活资产。绿盟NTI平台提供互联网资产稽查服务，在2017厦门金砖会议安全保障期间广泛使用，评估结果对于重保和迎检很有价值，且传统的服务中较少涉及，是比较独特的价值。

2.3 运营对抗

运营对抗是真正意义上的攻击者与防守方之间的综合比拼，与人、规范化、自动化工具、有效度量和优化息息相关。这些方面的组合就是能力体现。笔者在此简要列举三个安全运营能力供读者参考。

首先，企业监控预警能力高低，企业越早检测到攻击，就越可能阻止攻击。其次，企业漏洞管理能力强壮与否，如足够健全，就能降低发生安全事件风险。再次，通过对漏洞规则重新按照事件的攻击链划分，结合告警日志分析，利用智能化的势态分析工具，准确还原出攻击的整个过程，就能对攻击做出响应，减少攻击带来的损失和对业务运维的影响。

三．结语

何为网络安全建设进阶？笔者认为，证券业金融企业的信息安全经理和安全团队构成了防守方，最初选择分阶段的安全建设思路，让企业有一个最基础的安全保障。之后，运用攻击者视角，发现当下安全威胁趋势，开展如漏洞管理、客户资料泄露应对、互联网资产暴露检查等工作。伴随安全建设持续调整防御目标，逐步具备威胁情报管理、监控预警、应急响应处置能力。此过程中，可以结合第三方安全能力，依托其大规模的安全情报系统和专业、智能的大数据分析模块相互融合，协助提升企业的综合安全运营能力。

参考文献

[1]Nuix公司《The Black Report》，在2016年召开的BlackHat黑帽美国大会与DEF CON 24上，针对已知黑客人员（专业术语称为渗透测试人员）进行了一番调查，旨在了解其使用的攻击方法、偏好选择的漏洞以及在实际操作中发现哪些防御措施最具成效等问题。

原报告地址：https://www.nuix.com/white-papers/black-report

[2]《Mandiant M-Trends 2017 Report》，FireEye

Windows 10 Fall Creators Update安全新特性之WDEG

高级安全研究部　张云海

关键词：Win10　WDEG　秋季创意者版本

摘要：本文对 Windows 10 Fall Creators Update 更新中的新安全特性 WDEG 进行介绍，并分析其中攻击防护功能的实现。

一、概述

微软于 2017 年 10 月 17 日正式发布了 Windows 10 的新版本 Fall Creators Update（RS3）。

在此次更新中，微软将其缓解工具集 EMET（The Enhanced Mitigation Experience Toolkit）的功能集成到操作系统中，推出了 WDEG（Windows Defender Exploit Guard）。

WDEG 主要实现以下四项功能：

- **攻击防护**（Exploit protection）

通过应用缓解技术来阻止攻击者利用漏洞，可以应用于指定的程序或者系统中所有的程序。

- **攻击面减少**（Attack surface reduction）

通过设置智能规则来减少潜在的攻击面，以阻止基于 Office 应用、脚本、邮件等的攻击。

- **网络保护**（Network protection）

扩展 Windows Defender SmartScreen 的范围，为所有网络相关的操作提供基于信誉的防护。

- **受控制文件夹的访问**（Controlled folder access）

协助保护系统中的重要文件，使其不会被恶意软件（尤其是加密文件的勒索软件）修改。

二、攻击防护

攻击防护功能由系统的缓解措施与 EMET 的增强功能发展而来，通过阻止漏洞利用中的关键技术来进行防护。

2.1 设置

攻击防护可以通过 Windows Defender 安全中心进行设置：

攻击防护的设置有系统设置与程序设置两类：

2.1.1 系统设置

系统设置用于设置全局性的策略，包含以下项目：

- 控制流保护（CFG）

确保间接调用的控制流完整性。

默认设置为打开。

- 数据执行保护（DEP）

阻止代码从仅数据内存页中运行。

默认设置为打开。

- 强制映像随机化（强制性 ASLR）

强制重定位未用 /DYNAMICBASE 编译的映像。

默认设置为关闭。

- 随机化内存分配（自下而上 ASLR）

随机化虚拟内存分配位置。

默认设置为打开。

- 验证异常链（SEHOP）

确保调度期间异常链的完整性。

默认设置为打开。

- 验证堆完整性

检测到堆损坏时终止进程。

默认设置为打开。

2.1.2 程序设置

程序设置用于对特定程序进行自定义设置，包含以下项目：

- 任意代码保护（ACG）

阻止非映像支持的可执行代码和代码页修改。

可选设置有：允许线程退出、审核。

● 阻止低完整性映像

阻止加载标记低完整性的映像。

可选设置有：审核。

● 阻止远程映像

阻止从远程设备加载映像。

可选设置有：审核。

● 阻止不受信任的字体

阻止加载系统字体目录中未安装的任何基于 GDI 的字体。

可选设置有：审核。

● 代码完整性保护

只允许加载由 Microsoft 签名的映像。

可选设置有：同时允许加载由 Windows 应用商店签名的映像、审核。

● 控制流保护（CFG）

确保间接调用的控制流完整性。

可选设置有：使用严格 CFG。

● 数据执行保护（DEP）

阻止代码从仅数据内存页中运行。

可选设置有：启用 ATL 形式转换模拟。

● 禁用扩展点

禁用各种允许 DLL 注入到所有进程的可扩展机制，如窗口挂接。

● 禁用 Win32k 系统调用

阻止程序使用 Win32k 系统调用表。

可选设置有：审核。

● 不允许子进程

阻止程序创建子进程。

可选设置有：审核。

● 导出地址筛选（EAF）

检测由恶意代码解析的危险导出函数。

可选设置有：验证通常被攻击滥用的模块的访问权限、审核。

● 强制映像随机化（强制性 ASLR）

强制重定位未用 /DYNAMICBASE 编译的映像。

可选设置有：不允许去除的映像。

● 导入地址筛选（IAF）

检测由恶意代码解析的危险导入函数。

可选设置有：审核。

● 随机化内存分配（自下而上 ASLR）

随机化虚拟内存分配位置。

可选设置有：不使用高熵。

● 模拟执行（SimExec）

确保对敏感函数的调用返回到合法调用方。

可选设置有：审核。

● 验证 API 调用（CallerCheck）

确保由合法调用方调用敏感 API。

可选设置有：审核。

● 验证异常链（SEHOP）

确保调度期间异常链的完整性。

● 验证句柄使用情况

对任何无效句柄引用引发异常。

● 验证堆完整性

检测到堆损坏时终止进程。

● 验证映像依赖项完整性

对 Windows 映像依赖项加载强制执行代码签名。

可选设置有：审核。

● 验证堆栈完整性（StackPivot）

确保未对敏感函数重定向堆栈。

可选设置有：审核。

2.2 实现

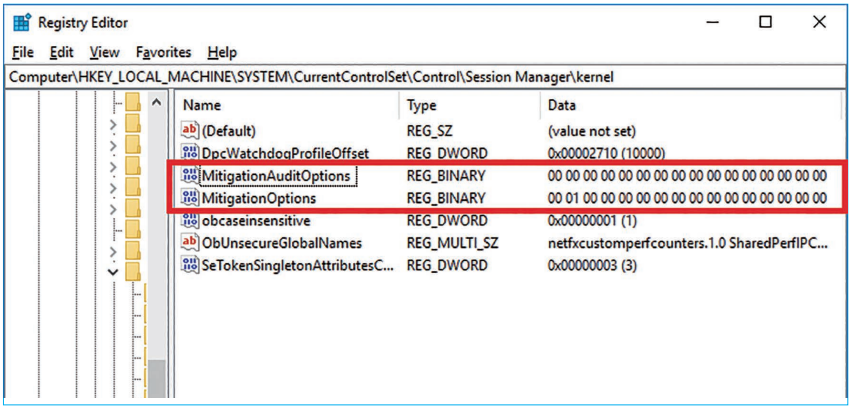
2.2.1 加载系统设置

攻击防护的系统设置保存在注册表中 HKLM\System\CurrentControlSet\

Control\Session Manager\kernel 项下:(如图一)

系统启动时,在初始化过程中会调用 nt!CmGetSystemControlValues 函数来获取注册表中保存的设置:(如图二)

其中,MitigationOptions 的值保存到 nt!PspSystemMitigationOptions 中,MitigationAuditOptions 的值保存到 nt!PspSystemMitigationAuditOptions 中(如图三)



图一

```
 # Child-SP          RetAddr           Call Site
00 fffff803`ff06b360 fffff803`fd6ab55f nt!CmGetSystemControlValues
01 fffff803`ff06b590 fffff803`fd2a5803 nt!InitBootProcessor+0x1bf
02 fffff803`ff06b7d0 fffff803`fd2a41cf nt!KiInitializeKernel+0x433
03 fffff803`ff06bad0 00000000`00000000 nt!KiSystemStartup+0x1bf
```

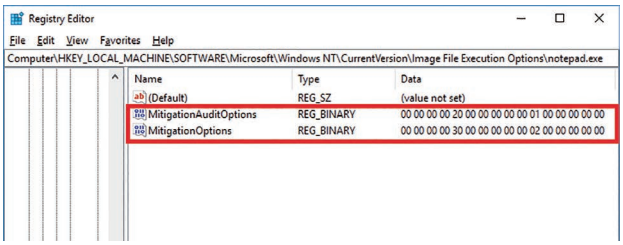
图二

```
0000140869490           dq offset aSessionManager_10 ; "Session Manager\\Kernel"
0000140869498           dq offset aMitigationopti_0 ; "MitigationOptions"
00001408694A0           dq offset PspSystemMitigationOptions
00001408694A8           dq offset PspSystemMitigationOptionsLength
00001408694B0           dq 0
00001408694B8           dq offset aSessionManager_10 ; "Session Manager\\Kernel"
00001408694C0           dq offset aMitigationaudi ; "MitigationAuditOptions"
00001408694C8           dq offset PspSystemMitigationAuditOptions
00001408694D0           dq offset PspSystemMitigationAuditOptionsLength
00001408694D8           align 20h
```

图三

2.2.2 加载程序设置

攻击防护的程序设置保存在对应程序的 IFEO（Image File Execution Options）项中：



系统创建新的进程时，将调用 nt!PspAllocateProcess 函数：

```
00 ffff9081`81852e48 fffff803`fd31f657 nt!PspAllocateProcess
01 ffff9081`81852e50 fffff803`fcff8d53 nt!NtCreateUserProcess+0x723
```

nt!PspAllocateProcess 函数调用 nt!PspReadIFEOMitigationOptions 函数以及 nt!PspReadIFEOMitigationAuditOptions 函数来读取 IFEO 中保存的程序设置：

```
IFEOMitigationOptions = 0ui64;
PspReadIFEOMitigationOptions(a11, &IFEOMitigationOptions, v80, IFEOMitigationOptionsLength);
_mm_store_si128(&v180, IFEOMitigationOptions);

IFEOMitigationAuditOptions = 0ui64;
PspReadIFEOMitigationAuditOptions(a11, &IFEOMitigationAuditOptions, v82, IFEOMitigationAuditOptionsLength);
_mm_store_si128(&v182, IFEOMitigationAuditOptions);
```

2.2.3 应用设置

然后，nt!PspAllocateProcess 函数调用 nt!PspInheritMitigationOptions 函数合并系统设置与程序设置，得到需要应用的设置：

```
MitigationOptions = PspSystemMitigationOptions;
PspInheritMitigationOptions(&MitigationOptions, &v180, &IFEOMitigationOptions);

MitigationAuditOptions = PspSystemMitigationAuditOptions;
PspInheritMitigationAuditOptions(&MitigationAuditOptions, &v182, &IFEOMitigationAuditOptions);
```

最后，nt!PspAllocateProcess 函数调用 nt!PspApplyMitigationOptions 函数来应用设置：

```
PspApplyMitigationOptions(pEProcess, pParentEProcess, &IFEOMitigationOptions, &IFEOMitigationAuditOptions, v85);
```

nt!PspApplyMitigationOptions 根据 MitigationOptions 与 MitigationAuditOption 的值来设置 EPROCESS 的 MitigationFlags 与 MitigationFlags2 对应的标志位：

```
+0x828 MitigationFlagsValues : <unnamed-tag>
   +0x000 ControlFlowGuardEnabled : Pos 0, 1 Bit
   +0x000 ControlFlowGuardExportSuppressionEnabled : Pos 1, 1 Bit
   +0x000 ControlFlowGuardStrict : Pos 2, 1 Bit
   +0x000 DisallowStrippedImages : Pos 3, 1 Bit
   +0x000 ForceRelocateImages : Pos 4, 1 Bit
   +0x000 HighEntropyASLREnabled : Pos 5, 1 Bit
   +0x000 StackRandomizationDisabled : Pos 6, 1 Bit
   +0x000 ExtensionPointDisable : Pos 7, 1 Bit
   +0x000 DisableDynamicCode : Pos 8, 1 Bit
   +0x000 DisableDynamicCodeAllowOptOut : Pos 9, 1 Bit
   +0x000 DisableDynamicCodeAllowRemoteDowngrade : Pos 10, 1 Bit
   +0x000 AuditDisableDynamicCode : Pos 11, 1 Bit
   +0x000 DisallowWin32kSystemCalls : Pos 12, 1 Bit
   +0x000 AuditDisallowWin32kSystemCalls : Pos 13, 1 Bit
   +0x000 EnableFilteredWin32kAPIs : Pos 14, 1 Bit
   +0x000 AuditFilteredWin32kAPIs : Pos 15, 1 Bit
   +0x000 DisableNonSystemFonts : Pos 16, 1 Bit
   +0x000 AuditNonSystemFontLoading : Pos 17, 1 Bit
   +0x000 PreferSystem32Images : Pos 18, 1 Bit
   +0x000 ProhibitRemoteImageMap : Pos 19, 1 Bit
   +0x000 AuditProhibitRemoteImageMap : Pos 20, 1 Bit
   +0x000 ProhibitLowILImageMap : Pos 21, 1 Bit
   +0x000 AuditProhibitLowILImageMap : Pos 22, 1 Bit
   +0x000 SignatureMitigationOptIn : Pos 23, 1 Bit
   +0x000 AuditBlockNonMicrosoftBinaries : Pos 24, 1 Bit
   +0x000 AuditBlockNonMicrosoftBinariesAllowStore : Pos 25, 1 Bit
   +0x000 LoaderIntegrityContinuityEnabled : Pos 26, 1 Bit
   +0x000 AuditLoaderIntegrityContinuity : Pos 27, 1 Bit
   +0x000 EnableModuleTamperingProtection : Pos 28, 1 Bit
   +0x000 EnableModuleTamperingProtectionNoInherit : Pos 29, 1 Bit

+0x82c MitigationFlags2Values : <unnamed-tag>
   +0x000 EnableExportAddressFilter : Pos 0, 1 Bit
   +0x000 AuditExportAddressFilter : Pos 1, 1 Bit
   +0x000 EnableExportAddressFilterPlus : Pos 2, 1 Bit
   +0x000 AuditExportAddressFilterPlus : Pos 3, 1 Bit
   +0x000 EnableRopStackPivot : Pos 4, 1 Bit
   +0x000 AuditRopStackPivot : Pos 5, 1 Bit
   +0x000 EnableRopCallerCheck : Pos 6, 1 Bit
   +0x000 AuditRopCallerCheck : Pos 7, 1 Bit
   +0x000 EnableRopSimExec : Pos 8, 1 Bit
   +0x000 AuditRopSimExec : Pos 9, 1 Bit
   +0x000 EnableImportAddressFilter : Pos 10, 1 Bit
   +0x000 AuditImportAddressFilter : Pos 11, 1 Bit
```

MitigationFlags 对应系统的缓解措施，设置对应的标志位之后即可生效。

MitigationFlags2 对应增强的缓解措施，需要加载动态库 PayloadRestrictions.dll 来实现。

2.2.4 加载 Payload Restriction

完成进程创建之后，将调用 ntdll.dll 的 LdrInitializeThunk 函数进行初始化。

初始化过程中，将逐步调用到 ntdll!LdrpInitializeExecutionOptions 函数：

```
00 00000031`9b18f388 00007ff8`39ea469d ntdll!LdrpInitializeExecutionOptions
01 00000031`9b18f390 00007ff8`39e975b3 ntdll!LdrpInitializeProcess+0x381
02 00000031`9b18f7d0 00007ff8`39e4920b ntdll!_LdrpInitialize+0x4e393
03 00000031`9b18f850 00007ff8`39e491be ntdll!LdrpInitialize+0x3b
04 00000031`9b18f880 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

ntdll!LdrpInitializeExecutionOptions 函数检查 PEB 的 NtGlobalFlag 是否设置了 FLG_HEAP_PAGE_ALLOCS 或 FLG_APPLICATION_VERIFIER 标志位，同时调用 ntdll!LdrpPayloadRestrictionMitigationsEnabled 函数来判断是否启用了 Payload Restriction 的缓解措施：

```
if ( Peb->NtGlobalFlag & 0x2000100 || LdrpPayloadRestrictionMitigationsEnabled() )
{
  status = LdrpInitializeApplicationVerifierPackage(ImagePathName, Peb);
  if ( status >= 0 )
    goto LABEL_174;
  LdrpDebugFlags_ = LdrpDebugFlags;
  if ( LdrpDebugFlags & 3 )
  {
    LdrpLogDbgPrint("minkernel\\ntdll\\ldrinit.c", 54);
    LdrpDebugFlags_ = LdrpDebugFlags;
  }
  if ( LdrpDebugFlags_ & 0x10 )
    __debugbreak();
}
```

满足任一条件时，将调用 ntdll!LdrpInitializeApplicationVerifierPackage 函数来初始化 ApplicationVerifier；后者将调用 ntdll!AvrfMiniLoadDll 函数来加载动态库 verifier.dll：

```
00 000000ad`dfe7c1a0 00007ffb`6ea4a95b ntdll!AvrfMiniLoadDll
01 000000ad`dfe7c6d0 00007ffb`6ea431c1 ntdll!AVrfInitializeVerifier+0xa4b
02 000000ad`dfe7d7e0 00007ffb`6ea44237 ntdll!LdrpInitializeApplicationVerifierPackage+0x105
03 000000ad`dfe7dc90 00007ffb`6ea4469d ntdll!LdrpInitializeExecutionOptions+0xd4b
04 000000ad`dfe7eff0 00007ffb`6ea375b3 ntdll!LdrpInitializeProcess+0x381
05 000000ad`dfe7f430 00007ffb`6e9e920b ntdll!_LdrpInitialize+0x4e393
06 000000ad`dfe7f4b0 00007ffb`6e9e91be ntdll!LdrpInitialize+0x3b
07 000000ad`dfe7f4e0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

verifier.dll 进行初始化时，将调用 verifier!MitLibInitialize 函数：

```
if ( NtGlobalFlag & 0x2000100 )
{
  v38 = 0;
  if ( MitLibQueryMitigations(&v38) >= 0 && v38 == 1 )
    DbgPrintEx(
      93i64,
      1i64,
      "AVRF: Ignoring payload restriction mitigation options since App Verifier or Pageheap are enabled. \n");
}
else if ( AVrfSystemDllBase && MitLibInitialize(Module, *&fdwReason, lpvReserved) < 0 )
{
  return 0;
}
```

verifier!MitLibInitialize 函数完成动态库 PayloadRestrictions.dll 的加载：

```
RtlInitUnicodeString(&DestinationString, L"PayloadRestrictions.dll");
status = LdrLoadDll(0x4081i64, 0i64, &DestinationString, &MitLibHandle);
```

2.2.5 应用 Payload Restriction

PayloadRestrictions.dll 进行初始化时，将调用 ntdll!LdrRegisterDllNotification 函数来注册回调函数 PayloadRestrictions!MitLibDllNotification：

```
LdrRegisterDllNotification = 0i64;
RtlInitAnsiString(&DestinationString, "LdrRegisterDllNotification");
status = LdrGetProcedureAddress(ntdll, &DestinationString, 0i64, &LdrRegisterDllNotification);
if ( status >= 0 )
  status = LdrRegisterDllNotification(0i64, MitLibDllNotification, 0i64, &v28);
```

此后加载、卸载模块时，系统会调用 PayloadRestrictions!MitLibDllNotification 函数进行通知：

```
char __fastcall MitLibDllNotification(ULONG NotificationReason, LPVOID NotificationData)
{
  JUMPOUT(NotificationReason != 1, MitLibHandleDllUnloadEvent);
  return MitLibHandleDllLoadEvent((__int64)NotificationData);
}
```

加载模块时，PayloadRestrictions!MitLibHandleDllLoadEvent 为该模块注入相应的防护机制：

```
char __fastcall MitLibHandleDllLoadEvent(LPVOID NotificationData)
{
  char v2; // r12
  __int64 v3; // rcx
  __int64 v4; // rdx
  __int64 v5; // rcx
  int status; // eax
  int v17; // [rsp+88h] [rbp+10h]

  v2 = 0;
  RtlAcquireSRWLockShared(&g_MitLibLock);
  MitLibIAFProtectModule(v3, *((_QWORD *)NotificationData + 3), *((unsigned int *)NotificationData + 8));
  v4 = *((_QWORD *)NotificationData + 3);
  v5 = *((_QWORD *)NotificationData + 2);
  LOBYTE(status) = RtlReleaseSRWLockShared(&g_MitLibLock, v4);
  if ( v2 == 1 )
  {
    status = MitLibAddProtectedModule(
               *((_QWORD *)NotificationData + 3),
               *((_QWORD *)NotificationData + 2),
               *((_QWORD *)NotificationData + 1),
               (unsigned int *)&v17);
    if ( status >= 0 )
      LOBYTE(status) = 0;
  }
  return status;
}
```

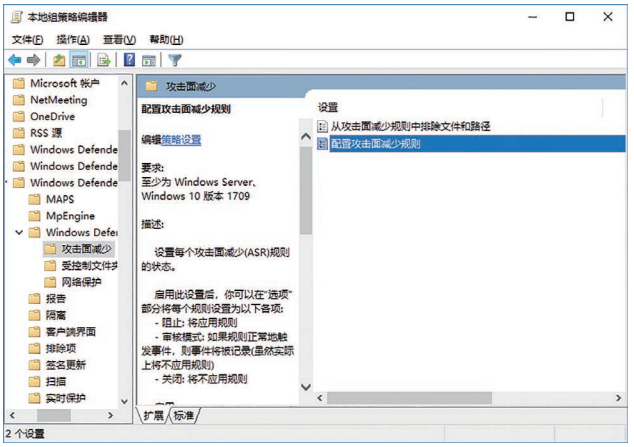
三、攻击面减少

攻击面减少用于阻止 Office 应用、脚本、邮件的一些特性被攻击者滥用，包括：

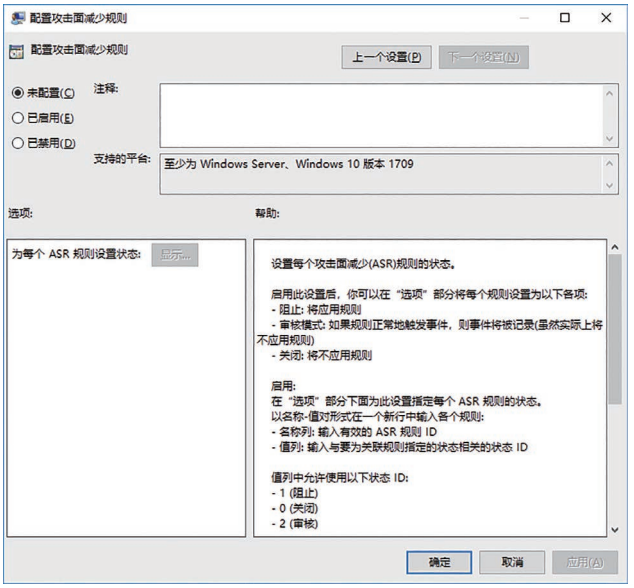
- 在 Office 应用或 Web Mail 中执行程序或脚本来下载或执行文件；
- 执行混淆的可疑脚本；
- 其他在正常的日常工作中不太可能出现的行为；

攻击面减少可以通过组策略编辑器来设置，其路径为“计算机配置 > 管理模板 > Windows 组件 > Windows Defender 防病毒程序 > Windows Defender 攻击防护 > 攻击面减少”：（见图一）

攻击面减少规则由 GUID 来标识，启用后可以设置每个规则的状态（1 表示阻止，0 表示关闭，2 表示审核）。（见图二）



图一

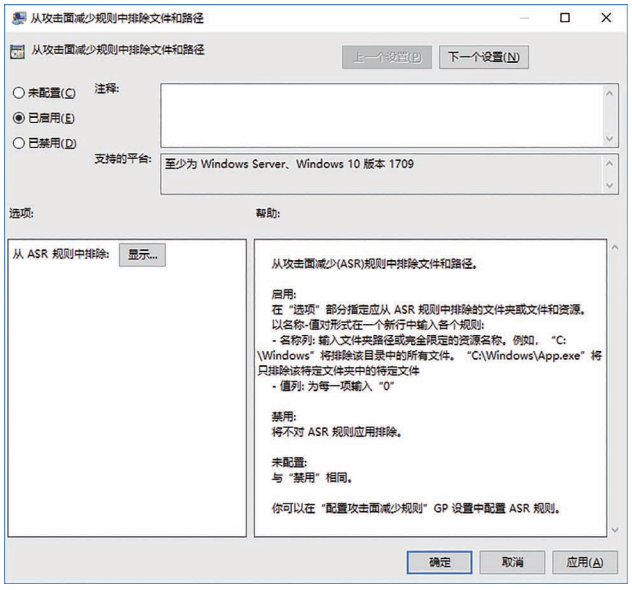


图二

目前支持的规则如下：

规则 ID	说明
BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550	阻止从邮件中执行内容
D4F940AB-401B-4EFC-AADC-AD5F3C50688A	阻止 Office 应用创建子进程
3B576869-A4EC-4529-8536-B80A7769E899	阻止 Office 应用创建可执行内容
75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84	阻止 Office 应用向其他进程注入代码
D3E037E1-3EB8-44C8-A917-57927947596D	阻止脚本执行下载的内容
5BEB7EFE-FD9A-4556-801D-275E5FFC04CC	阻止执行混淆的脚本
92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B	阻止在宏中调用 Win32 API

同时，可以指定从上述规则中排除的文件和路径：



攻击面减少的规则保存在注册表中

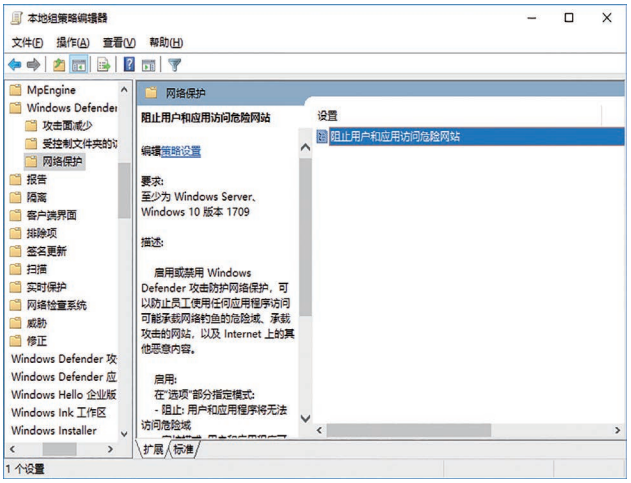
HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{EE798E8D-335D-4D47-9C4B-ECDF73662A1F}Machine\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules 项下。

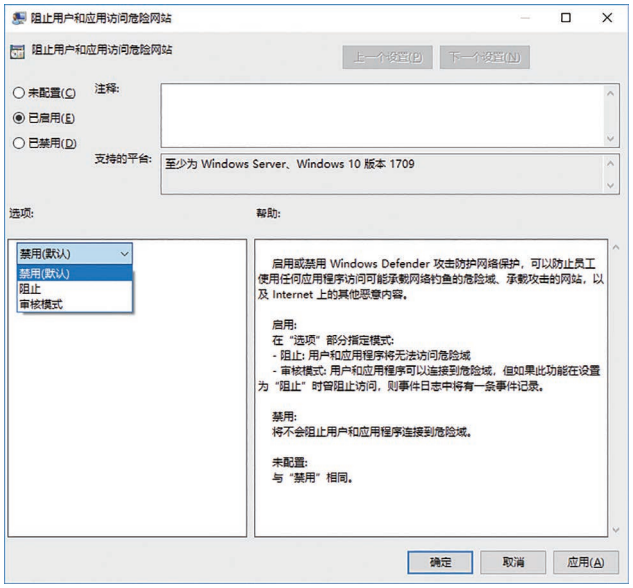
四、网络保护

网络保护通过阻止任意程序访问危险的网站（可能包含钓鱼诈骗、漏洞利用等恶意内容）来减少基于网络的攻击面。

网络保护扩展了 Windows Defender SmartScreen 的范围，将阻断全部试图连接低信誉目标的 HTTP / HTTPS 流量。

网络保护可以通过组策略编辑器来设置，其路径为“计算机配置 > 管理模板 > Windows 组件 > Windows Defender 防病毒程序 > Windows Defender 攻击防护 > 网络保护”：





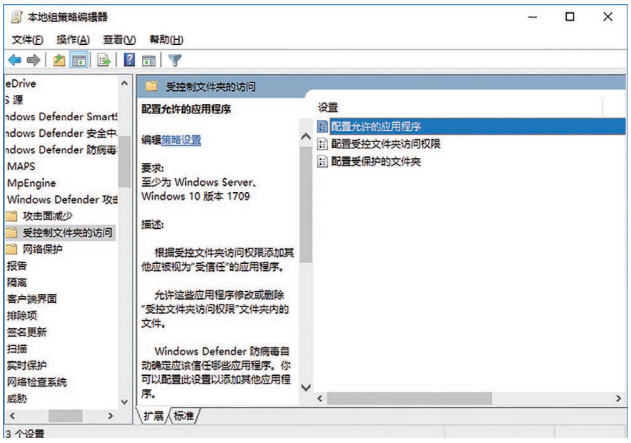
网络保护的规则保存在注册表中

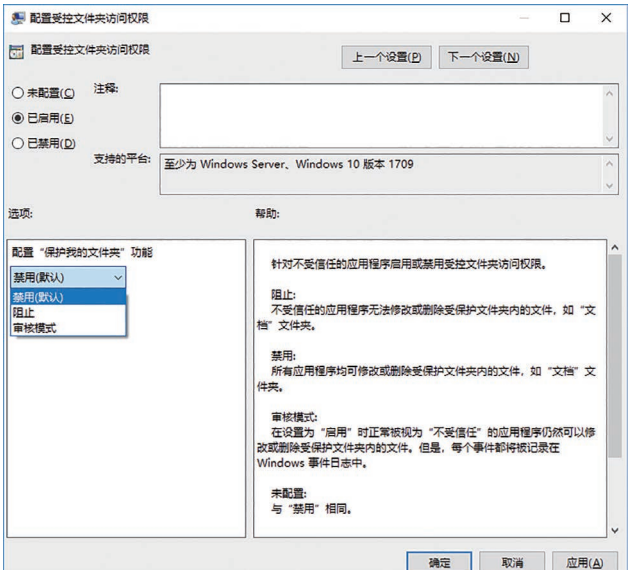
HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{EE798E8D-335D-4D47-9C4B-ECDF73662A1F} Machine\Software\Policies\Microsoft\Windows Defender\ Windows Defender Exploit Guard\ Network Protection 项下。

五、受控制文件夹的访问

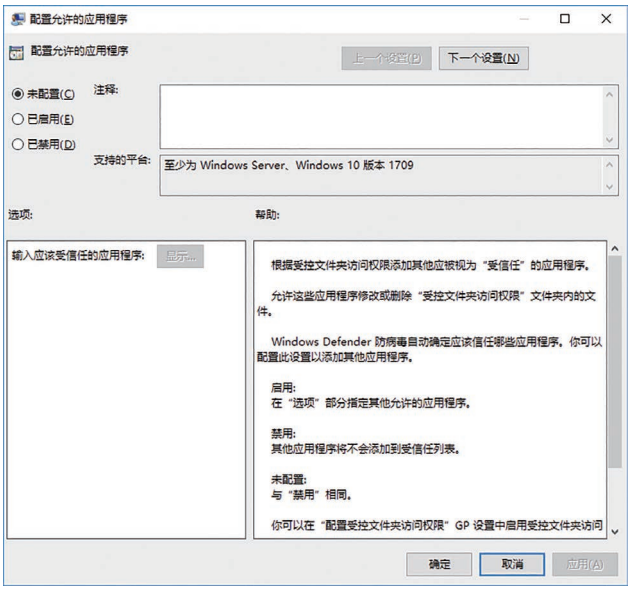
受控制文件夹的访问用于阻止恶意应用（如勒索软件）修改重要的文件，只有 Windows Defender 防病毒程序评估为安全的应用才被允许修改受控制文件夹中的文件。

受控制文件夹的访问可以通过组策略编辑器来设置，其路径为“计算机配置 > 管理模板 > Windows 组件 > Windows Defender 防病毒程序 > Windows Defender 攻击防护 > 受控制文件夹的访问”：





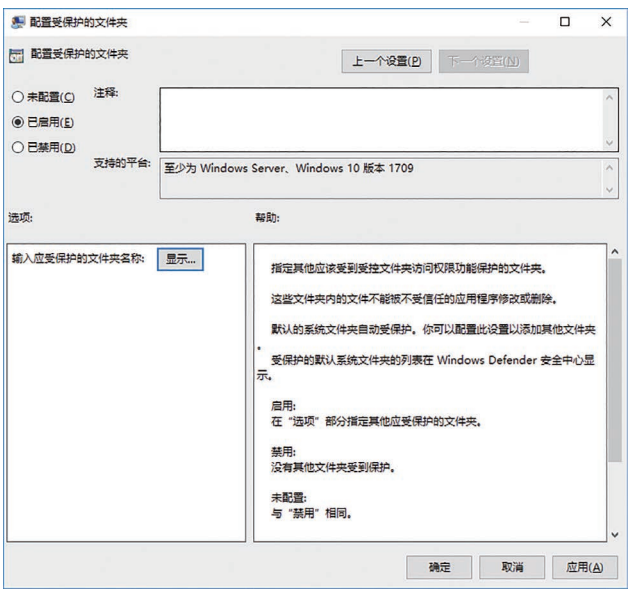
可以通过配置允许的应用程序，将受信任的程序加入白名单：



缺省情况受保护的只有系统文件夹，可以通过配置受保护的文件夹来添加应该受到该功能保护的文件夹：

受控制文件夹的访问的规则保存在注册表中

HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{EE798E8D-335D-4D47-9C4B-ECDF73662A1F}Machine\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ Controlled Folder Access 项下。



六、总结

Windows 10 Fall Creators Update 更新中的 WDEG 提供了全面而强大的漏洞利用防护功能。

然而，安全与便捷往往不可兼得，为了不过多的影响用户体验，WDEG 中的许多功能缺省并未开启。

系统管理员应当根据其实际情况来设置组策略，以便更好的利用 WDEG 来进行防护。

HTTPS的DDoS攻击防护思路

IIS技术团队 李明　系统架构部 李凯

关键词：HTTPS　DDoS 防护　SSL/TLS

摘要： 随着越来越多的网络业务由明文 HTTP 转向加密 HTTPS 协议，针对 HTTPS 的 DDoS 攻击也呈快速增长趋势，包括针对 SSL/TLS 握手交互的攻击和针对 HTTPS 业务的攻击。HTTPS 的 DDoS 防护一直是业界的一个难题，本文介绍 HTTPS 的 DDoS 攻击原理和危害，并给出防护思路和防护实践

一、引言

DDoS（Distributed Denial of Service，分布式拒绝服务）攻击的主要目的是让指定目标无法提供正常服务，甚至从互联网上消失，是目前最强大、最难防御的攻击之一。DDoS，常见网络和应用层的攻击，经过长时间的对抗研究，对协议和报文内容的分析，已经形成了成熟的解决方案。

但随着用户对安全性要求的增强，以及一些政策性的强制性要求（比如苹果 appstore 对 HTTPS 的强制要求），越来越多的网络服务主动或被动的将自己的服务由 HTTP 切换到 HTTPS。HTTPS 协议在网络上传输加密的报文，传统的内容检测技术失去了效果；由于处理 HTTPS 连接的巨大资源消耗，让 HTTPS 的 DDoS 攻击成本较低，危害性却较大。

本文介绍常见的针对 HTTPS 的 DDoS 攻击原理，它通过 HTTPS 的原理介绍攻击的特别之处；给出常见的防护思路和针对性防护实践。

二、HTTPS 的 DDoS 攻击原理

2.1 HTTPS 协议简介

传统的 HTTP 协议采用明文传输信息，存在被窃听和篡改的风险；SSL/TLS 提供了身份验证、信息机密性和完整性校验功能。HTTPS 基于 HTTP 开发，使用 SSL/TLS 进行加密的信息交互，在交互协议上使用了 TCP、SSL/TLS 和 HTTP 三种常见的协议。

针对 HTTPS 的 DDoS 攻击也主要从 TCP 协议、SSL/TLS 协议和 HTTP 协议三个方面来进行的，下面分别介绍。

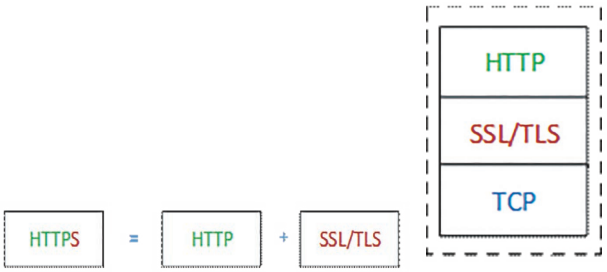


图 2.1 HTTP 协议示意图

2.2 TCP 协议的攻击

此类攻击比较常见，即是普通的针对 HTTPS 服务器发起的 SYN-Flood、ACK-Flood 等，用以消耗服务器的 TCP 连接等资源。这类攻击不涉及 HTTPS 特有的协议，所有承载在 TCP 协议之上的服务都可能收到此类攻击。

2.3 SSL/TLS 协议的攻击

SSL/TLS 握手过程涉及非对称加密算法，对称加密算法和散列算法，其中非对称加解密是非常重量的计算消耗性工作。而大部分非对称加密算法在实际使用中，服务器的计算量远大于客户端，下面以最常使用的非对称加密算法 RSA 介绍，其原理如下：

1. 选择一对不同的、位数差不多且足够大的素数 p 和 q；
2. 计算 n=p*q；
3. 计算 φ(n)=(p – 1)(q – 1);
4. 取一个与 φ(n) 互质的数 e，1<e<φ(n);
5. 计算 d，使得 d*e ≡ 1modφ(n)；
6. 公钥为（n，e），私钥为（n，d）；
7. 消息 m 加密 c=m^e mod n, 解密为 m=c^d mod n

SSL/TLS 使用 RSA 算法进行密钥交换的过程如下（图 2.2）：

客户端加密随机数 m，计算 c=m^e mod n 并将 c 发送给服务器，服务器解密随机数 m=c^d mod n；如果 e 和 d 大小差不多的话，那么客户端和服务器的计算量是基本对等的。但现实中 e 和 d 大小差别很大，e 一般是一个固定的小素数，当前普遍使用 65537(0x10001)，而根据 e 计算出来的 d 就是一个很大的值，如下

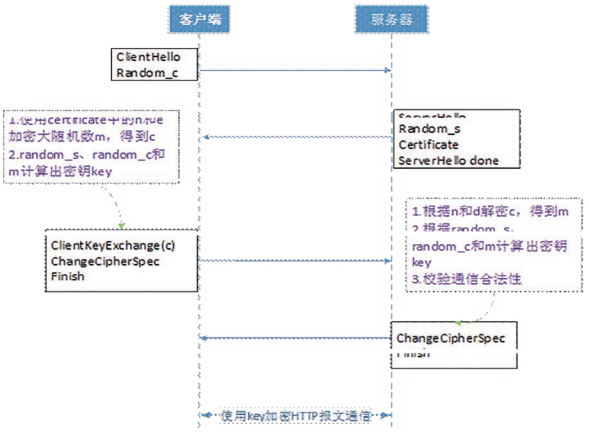


图 2.2 RSA 密钥交换过程

图 RSA2048 做出的证书(modules 表示 n, publicExponent 表示 e, privateExponent 表示 d)。

根据 RSA 算法第 7 步流程，服务器的解密消耗远大于客户端。一方面基于历史原因，e 不能设置的过大（最大为 32 位数）；另一方面为了安全性考虑，d 又不能选择的太小，一般和 n 的位数差不多 [1]。

虽然有算法来大量减小服务器计算 m 的 CPU 消耗 [2]，但经过实际测试，使用 RSA2048 作 SSL/TLS 密钥交换算法时，服务器在 SSL/TLS 握手阶段的 CPU 消耗大约是客户端的 6 倍。

根据上面描述的握手不对称性，攻击者通过不断与服务器新建 SSL/TLS 握手，或建立 SSL/TLS 后不断的重协商密钥（比如著名的 THC-SSL-DOS），即可以较小代价将服务器打瘫。更严重者，客户端可以不用计算 c，而是提前准备一个 c'，让服务器做大量无效但昂贵的计算后，才发现本次 SSL/TLS 通信失败。这种情况下，极

```
Private-Key: (2048 bit)
modulus:
    00:b3:41:c5:04:3d:1c:f6:96:63:c2:a2:03:a8:b6:
    56:9d:21:e8:78:25:ba:66:74:49:5a:b1:0a:ac:fd:
    c8:82:b8:82:f2:c5:15:ac:3c:3a:0c:ab:ca:ef:6f:
    b8:59:95:a1:cb:e2:4b:d0:bc:fd:93:fa:d9:09:58:
    69:dc:b9:80:e0:68:8d:e1:bc:85:36:39:5f:d2:2f:
    67:f1:2c:2f:04:93:c3:da:6b:a2:b0:6d:60:d9:83:
    de:6a:1b:f0:ac:51:a0:7c:32:9d:3b:09:df:2e:c4:
    07:41:52:d9:f6:93:5d:6e:d0:62:d1:3b:b5:06:7d:
    ad:59:e1:68:cf:77:f8:6e:ae:ce:5f:09:e6:7f:5d:
    51:5e:26:f3:d0:46:7f:b1:ff:87:f0:ad:05:f8:04:
    58:b1:64:6e:47:db:3c:20:a1:49:03:ff:d4:d0:10:
    cf:99:fc:79:54:04:c1:47:e2:23:bf:b3:e1:40:88:
    0c:7f:cf:4b:9e:7a:6b:97:f2:26:e2:d5:fa:16:26:
    04:c3:a2:77:e6:ad:33:99:55:57:b0:6e:0d:c0:21:
    6f:a5:3b:bd:57:c8:74:b5:81:f7:6c:66:dd:05:9e:
    94:c9:9a:8f:60:3a:7d:f5:c5:9f:7f:79:b2:bc:5e:
    5f:46:a1:42:65:12:67:cc:ff:da:dc:37:75:ad:9a:
    eb:13
publicExponent: 65537 (0x10001)
privateExponent:
    00:87:6c:e0:d3:5a:f8:4e:b3:3f:9b:03:9b:90:12:
    71:4d:35:18:d3:ec:6c:ee:8a:5c:00:d0:50:28:71:
    72:d2:8f:63:1e:d6:16:91:90:ce:aa:53:ff:74:f5:
    0a:69:63:ca:60:a6:0e:71:1c:d6:d6:bd:64:ca:d2:
    a8:e7:c0:9d:c4:ec:38:84:9a:50:69:ae:de:dd:84:
    43:1a:c9:2e:9c:5e:a6:50:95:90:cb:89:56:e9:fd:
    de:42:7b:e9:4f:c6:3b:60:99:3c:80:25:ed:1e:ff:
    aa:1b:87:e4:73:8c:d1:c1:ae:5d:79:85:8a:35:e5:
    2c:da:02:99:94:64:26:a4:36:d7:e7:65:d7:c2:71:
    e6:8e:71:8b:ce:59:20:59:43:ce:c9:1d:45:e3:62:
    41:10:06:d9:a3:a3:1b:bf:7b:ac:39:9d:43:a3:ea:
    fa:d9:8e:93:15:83:c0:a7:45:33:be:cf:db:4d:ec:
    d6:1e:a9:74:6d:89:75:f4:88:a5:41:20:d0:4e:ee:
    4d:44:fa:03:e5:27:e9:94:00:30:af:0e:25:41:d4:
    70:2e:62:3a:0a:d7:a8:c8:2c:c2:c9:40:ca:b6:b4:
    e4:12:e1:3f:cb:18:35:97:4c:70:68:5f:25:a6:70:
    d4:26:a3:b4:a4:da:90:87:4d:eb:a5:35:44:69:00:
    b4:c1
```

图 2.3 RSA 证书公私钥参数

少量的攻击者即可让服务器假死。

2.4 HTTP 协议的攻击

针对 HTTP 协议的攻击涉及两个方面：一方面通过发送大量加密或提前准备的垃圾 HTTP 加密报文，以消耗服务器对称解密性能；另一个方面消耗服务器处理 HTTP 连接或附加的其他数据库等资源；

三、HTTPS 的 DDoS 防护思路

3.1 HTTPS 防护概述

根据第二章介绍常见的针对 HTTPS 的 DDoS 攻击，HTTPS 的 DDoS 防护也先从 TCP、SSL/TLS 和 HTTPS 协议三个方向来讨论。另外，HTTPS 防护是一个系统性的工程，涉及到 SSL 证书管理等工作，下面分别介绍。

3.2 TCP 协议攻击的防护

经过多年的防护积累，业界针对 TCP 协议的 DDoS 攻击有比较丰富的防护算法。针对 TCP-Flood，绿盟科技抗 DDoS 产品有自研的反向探测算法，不用断正常流量的连接，也能有效识别虚假源。针对肉鸡发起的攻击可通过针对源限速或根据绿盟科技的威胁情报做过滤。

3.3 SSL/TLS 协议攻击的防护

SSL/TLS 攻击通常是攻击源已经通过了 TCP 协议防护，是一个真实的客户端。单独考虑 SSL/TLS 协议的计算型攻击，没有太好的办法。在 DDoS 防护设备上，可根据客户端发起密钥交换的次数来识别异常客户端，此方法对 THC-SSL-DOS 还比较有效。

3.4 HTTP 协议攻击的防护

针对 HTTP 协议的攻击，业界有一些通用的 HTTP 防护算法，比如 302 跳转、JavaScript 验证和图片验证等，以将正常用户和肉鸡程序区分。但 HTTP 防护算法需要得到解密后的 HTTP 明文信息，防护设备需要跟踪与客户端的每个 HTTPS 连接，最终还是回到 SSL/TLS 性能问题。

3.5 通用 HTTPS 防护的问题

当前针对 HTTPS 使用的 SSL/TLS 协议及之上的 DDoS 防护一般是做代理防护，比如 CDN 厂商，通过庞大的集群，消化掉攻击流量。待防护的 HTTPS 服务器将证书和私钥交给 DDoS 防护代理方，客户端对服务器的访问转化为：客户端访问防护代理方，然后防护代理方再访问服务器（HTTPS 或 HTTP 都可），客户端和服务器的通信内容在防护代理方是明文的，防护代理方可以通过报文内容分析做进一步的防护。这种防护方法存在的问题在于：

（1）用户需要将自己服务器使用的证书和私钥提供给防护代理方；

（2）客户端和服务器的通信内容对防护代理方是明文可见的，失去了 HTTPS 的机密性原则。

3.6 优化的 HTTPS 防护

本节从 HTTPS 的整理业务逻辑考虑，绿盟科技抗 DDoS 防护设备（简称为 ADS）作为代理处理客户端发起的 TCP 和 SSL/TLS 握手，通过丰富的 HTTP 协议验证算法单次验证客户端的合法性。将有 HTTPS 业务交互，并通过 HTTP 算法交互验证的客户端识别为合法用户，其后续报文直接放行。

HTTPS 服务器提供的是应用层服务，SSL/TLS 连接只是 HTTP 业务访问之前的中间步骤，正常用户不会只做 SSL/TLS 连接，而不进行后续的 HTTP 加密报文交互。对于多次 SSL/TLS 连接后，仍不能通过 HTTP 算法验证的客户端，后续报文直接丢弃或将其加入黑名单。通过这种 HTTPS 交互全局视图，将攻击者逐步排除。

验证流程如下：客户首先在 ADS 设备上导入需防护 HTTPS 服务器的 SSL 证书和私钥（一般导入一对和服务器上不一样的证书私钥，不导入的话，将使用 ADS 自带的缺省 SSL 证书私钥）；当 HTTPS 攻击发生时，ADS 截获客户端的 HTTPS 连接，通过 SSL 和 HTTP 算法验证客户端的合法性；验证通过的合法客户端后续报文，ADS 直接放行其与服务器通信。

相对于完全代理方式，ADS 针对 HTTPS 的 DDoS 防护的优点：

（1）ADS 可以对 HTTPS 业务报文解密后，基于现有丰富的 HTTP 算法来防护 HTTPS 攻击；

（2）客户导入的证书，只是为了让浏览器不告警，客户可以导入一个和服务器上不一样的证书，比如域名验证 (DV) 证书，这样即可规避一些法律政策问题；

（3）ADS 也可只做客户端合法性验证，不对流量进行解密防护。

3.7 扩展防护思路

针对 HTTPS 连接在客户端和服务器的计算差异，提高客户端的计算消耗量，以减小攻击者在单位时间内能发起的访问请求，可以一定程度遏制攻击企图。Client Puzzle 协议（CPP）[3] 是一个很好的参考，服务器发送一个数学问题给客户端，在得到客户端发送过来的答案之前，不允许客户端的下一步操作，客户端需要花费大量 CPU 来解决此数学问题。

四、结束语

HTTPS 防护是业界的一大难题，本文介绍了 HTTPS 的 DDoS 攻击场景和防护难点，给出常见的防护 HTTPS 的 DDoS 攻击思路，并介绍了绿盟科技 ADS 技术团队在防护 HTTPS 攻击上的思路和实践。

高性能Flow负载均衡及其应用

IIS技术团队　陈涛 苗宇 何坤

关键词：高性能　流量分析　DDoS 检测　负载均衡

摘要：基于 Flow 的攻击检测是 DDoS 清洗服务中非常重要的一环，而随着互联网的发展，网络承载的信息越来越多，流量越来越大，单台 Flow 分析设备 (NTA) 的能力逐渐满足不了 DDoS 攻击检测任务。本文分析了 NTA 设备目前遇到的诸多挑战，描述了高性能 Flow 负载均衡设备的工作原理及其应用场景。

一、引言

NetFlow/SFlow 是网络流量统计的标准协议，与 DPI 技术相比，基于 Flow 的检测技术处理速度更快、配置部署更方便快捷、维护成本更低，因此被广泛应用在网络流量分析、DDoS 攻击检测、攻击溯源等多个方向。

表一　常用的几种 Flow 协议

Flow 名称	代表厂商	主要版本	备注
NetFlow	Cisco	V5、V9	应用最广
sFlow	Foundry、HP、Alcatel、NEC、Extreme 等	V4、V5	实时性较强，具备突出的第二~ 七层信息描述能力
NetStream	华为	V5、V8、V9	与 NetFlow 相同
IPFIX	IETF 标准规范	RFC 3917	以 NetFlow V9 为蓝本相当于 Netflow V10

随着互联网的快速发展和移动互联网的普及，网络流量的种类和数量都在发生着变化，对网络流量分析设备也提出了很多新的要求。下面我们将分析下 NTA 流量分析设备在几种应用场景下可能存在的挑战，再介绍 Flow 负载均衡设备的原理和主要技术要点，以负载均衡方式给出当前问题的方案。

二、Flow 流量分析设备的挑战

2.1 对处理性能的挑战

现在骨干网络带宽动辄达到几十 T，且每年以 50% 以上速度进行增长，其中一台核心路由器的输出 Flow 就可达到 300w Flow/s 甚至更高，传统单台 NTA 设备遇到性能挑战，需要采用集群方式组网，配置比较复杂。

2.2 对部署的挑战

某些网络环境下，特别是运营商环境，需要从不同网络层级对业务流量进行分析，如下图所示，在骨干网需要采集全网流量进行分析，而各个接入层分析本网络内的流量。从流量大小来看，一台 NTA 应对较为困难，部署多台 NTA 时也需要在各层级网络设备上分别配置，以输出到不同的 NTA，网络的变化也会给部署带来很多不便的麻烦。

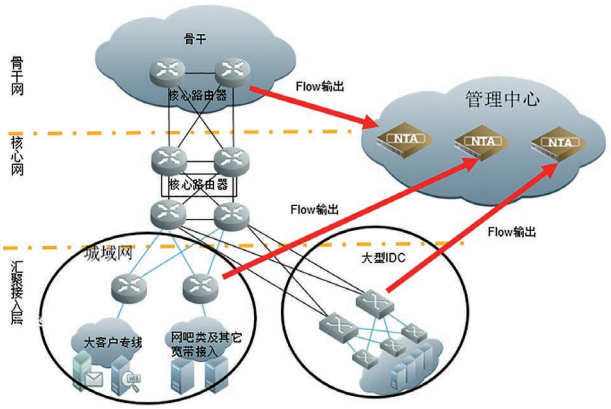


图 1 多层级网络流量分析

2.3 对复制转发的挑战

一些第三方产品也需要对 Flow 进行分析，例如绿盟科技溯源系统通过 NetFlow 做攻击溯源，通管局的合规要求等。因此 NTA 除了自身的流量分析和攻击检测以外，还承担着 Flow 的复制和转发任务，流量的增大和转发对象增多都会导致 NTA 分析检测能力下降。

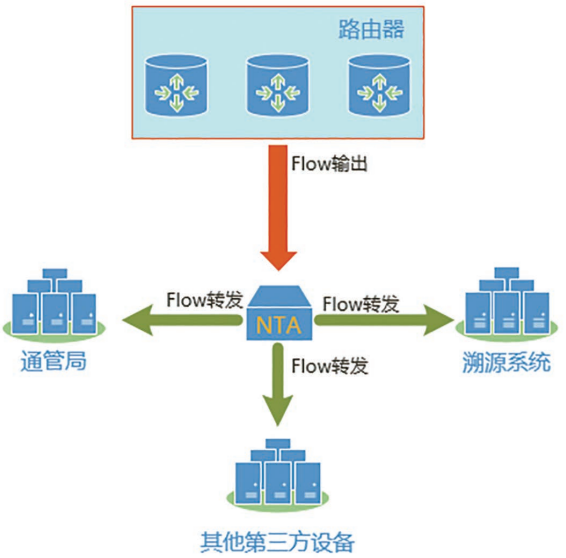


图 2 Flow 转发场景

2.4 对可靠性方案的挑战

客户的流量是至关重要的，流量分析设备在工作过程中的异常会导致信息丢失，期间发生的攻击也会被漏检测，目前的 NTA HA 主备方案解决的就是这类问题，如图 3 所示。此方案的缺点是备份

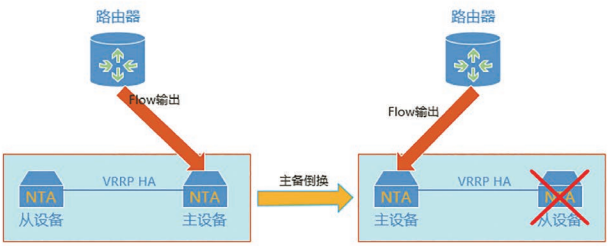


图 3 NTA 主备倒换示意图

设备始终不承担任何业务，资源存在一定程度的浪费，有些预算紧缺的客户可能无法接受。

三、Flow 负载均衡设备

为解决上述市场需求，绿盟科技新研发了 Flow 负载均衡设备 (Flow Load Balancer，以下简称 FLB)，与其他通用的负载均衡设备不同的是，该设备专门针对 Flow 数据进行负载均衡，包括 NetFlow v5/v9、NetStream v5、SFlow v4/v5、IPFIX(以下以 xFlow 统称所有 Flow 类型)。其支持二三层接入方式，提供基于路由器、基于业务域和基于目的 IP 多个维度的负载均衡模式。

典型拓扑图，FLB 设备接受来自路由器输出的 xFlow 报文，根据配置的策略以负载均衡或复制方式转发给不同的 Flow 采集器，支持同时对多个采集器集群进行负载均衡和复制转发

3.1 路由转发方式

FLB 转发的目的设备可以与 FLB 在一个二层网络，也可以是路由可达的三层网络。

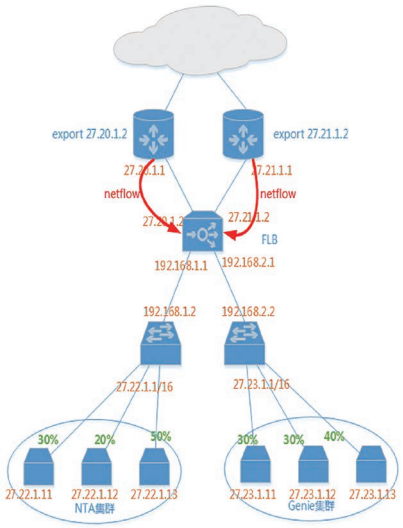


图 4 三层路由转发方式

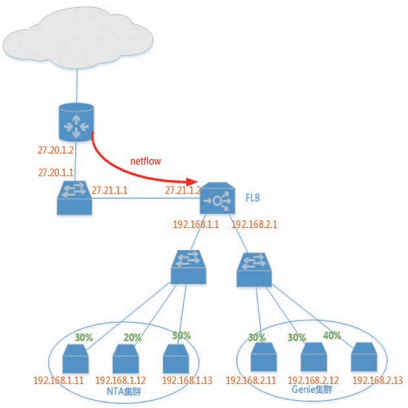


图 5 二层转发方式

3.2 多维度的负载均衡算法

如下图，以设备组的形式管理各个路由器和 Flow 采集器，在路由器组和采集器组之间建立负载均衡映射关系，且可以同时配置多个负载均衡映射对象。

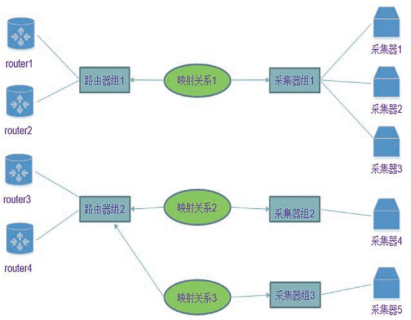


图 6 负载均衡映射关系

主要支持四种负载均衡策略算法：

■ 基于目的 IP 均衡的策略

将相同目的 IP 的 Flow 数据转发到同一台采集器。

■ 基于业务域均衡的策略

按照目的 IP 按照所属业务域分组，确保相同业务域的 Flow 数据转发到同一台采集器。

■ 基于路由器自动均衡的策略

根据 Flow 报文的源 ip(即路由器地址) 决定转发给哪个采集器，确保相同路由器的 Flow 数据转发到同一台采集器。系统根据采集器的状态自动生成路由器和采集器的对应关系，当采集器掉线时，其映射的路由器自动负载均衡到其他活跃的采集器上。如下图，router1 的 Flow 数据转发给采集器 1，router2 转发给采集器 2，router3 转发给采集器 3，router4 转发给采集器 1。当发现采集器 2 掉线时，router2 会自动映射到采集器 3 上。

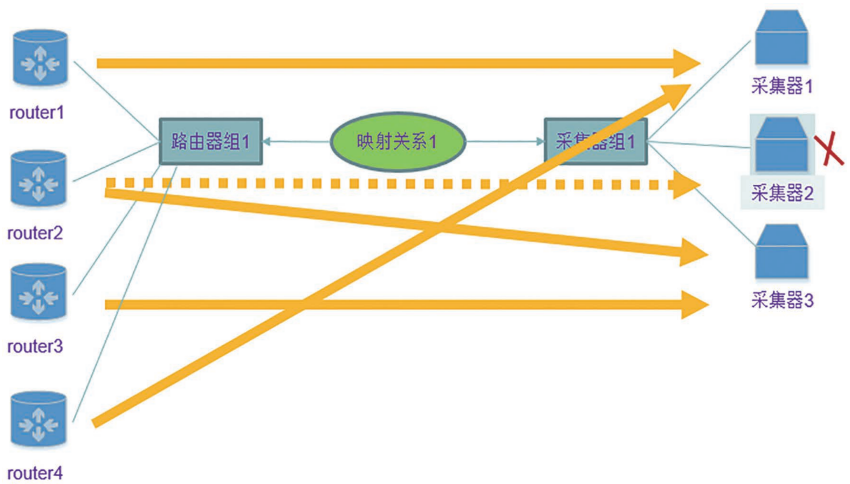


图 7 采集器掉线后的重映射图

■ 基于路由器手动均衡的策略

与基于路由器自动均衡的方式一样，不同的是路由器和采集器的对应关系由人工配置，且即使采集器掉线，映射关系也不发生变化。

3.3 高可靠性设计

FLB 设备位于 Flow 网络的关键路径，对可靠性的要求非常高。

FLB 提供了 HA 主备功能。当主 FLB 设备检测到自身关键业务进程异常或恢复时，通过 VRRP 协议交互通知对端进行主备切换，切换时间在 1-2 秒范围内，切换后业务照常运行，整个过程对用户几乎无感知。

除此之外，FLB 还会实时监控采集设备的状态，支持使用 ping 和 webapi 方式探测采集设备是否存活以及功能是否正常，以此保证采集器异常时能够将 Flow 数据快速切换到其他正常的采集设备上。

四、结束语

结合本文提出的 Flow 负载均衡设备，能解决大部分大流量和复杂环境下的 NTA 部署问题，使 NTA 能适用于更多的解决方案场景，充分发挥其市场价值。另外值得一提的是，绿盟科技的 FLB 设备具备更高的处理性能和更全面的负载均衡策略。

绿盟ADS NX5-10000 应对大流量DDoS攻击

产品管理团队 汤湘君

关键词：大流量 DDoS 防护 ddos 防护高端产品 抗 ddos 产品 抗 ddos 设备

摘要：DDoS 攻击频次及峰值流量不断刷新纪录，面对这样的挑战，一方面客户需要大流量防护，另一方面运营商需要增值运营服务，绿盟科技推出 ADS NX5-10000 高端型号，以满配 240G 的高性能清洗能力，定位高端市场。本文介绍了新产品特性及应用场景。

前言

在纷繁复杂的网络攻击种类里，DDoS 主要属于资源消耗型的一类。通过利用大量分散的攻击源对目标带宽、基础网络设施或服务器等进行消耗，造成业务异常。攻击端能够调用的资源越多，对目标造成的伤害也就越大。因此，防守一方想要实现绝对的拦截和清洗，也要有势均力敌的防护资源才能与之抗衡。随着互联网带宽的高速扩容，DDoS 攻击的发展态势和行业需求也在不断变化。变的是不断刷新历史纪录的攻击量级，而不变的是对高性能资源的持续要求与渴望。

DDoS 攻击频次及峰值流量不断刷新纪录

近几年观察到的 DDoS 攻击流量趋势和案例表明，大流量 DDoS 攻击更新速度加快。物联网的兴起使 DDoS 可调用的攻击资源得到了极大的延展，从传统 PC 到移动设备，再到 IoT 物联网终端，都成了培育 DDoS 僵尸的温床。据 DDoS 威胁报告统计，2016 年我国境内发生的攻击次数与去年同期相比增长 18.6%，攻击总流量同比增长 25%。2017 依然延续着这个增长趋势。

除了攻击次数和流量总和发生增长，大流量 DDoS 攻击的事件占比和单次攻击峰值也大幅刷新了历史纪录。2017 上半年，超 300Gbps 的超大流量 DDoS 攻击共发生 46 次。峰值超过 300G 的 DDoS 攻击事件在前几年依然是震惊行业的特大号新闻，而今已见怪不怪了。更有甚者，单次峰值超过 600G 的 DDoS 攻击已经成为事实。攻击者用直白的数字证明了他们的存在与实力，并向所有人宣战：带宽扩容不是抵抗 DDoS 的方法，只会引起更强劲的攻击。作为安全厂商，我们要直面攻击，坚决应战，打好每一场攻防的硬仗。

客户需要大流量防护 运营商需要增值运营服务

运营商一直是 ADS 采购的主力行业。抗 DDoS 设备在移动集采和电信项目中的需求一直很旺盛，而移动集采在 2017 年也提出了单体 100G 的防护要求。从方案建设来看，电信云堤、移动和联通

增值业务的发展离不开高性能设备的采购和部署。低端型号虽然可以通过集群方案来实现大流量防护节点的建设，但是一方面存在集群部署的瓶颈，做不到无限堆叠，另一方面增加了部署的难度和运营复杂度，而高性能设备能够更好的解决这些问题。

从防护需求来看，全国各地的骨干网正在紧锣密鼓的开展流量清洗服务，集团也提出了大流量清洗平台的发展规划。广东、福建和江苏等地的带宽发展和 DDoS 防护体量呈正比增长，短期目标计划已经超过 T 级容量。这么大的防护体量既是自身业务防护、基础设施安全的需求，同时也是打造增值业务的重要条件。

从运营商自身的业务发展来看，大流量防护的增值运营发展态势良好。一是源于大流量 DDoS 攻击下，子一级客户对云清洗防护的采购需求；二是金融客户作为 DDoS 攻击的重点受灾对象，由于运营能力有限，不得不频繁向上一级运营商求助的需求场景。

2017 年 6 月，黑客组织匿名者向全球超过 140 个金融机构发起了新一轮的攻击行动，中国人民银行、香港金融办理局在内的全球近 140 家金融机构均在其公布的攻击列表中。鉴于金融行业流量的涉密性以及安全要求，在遭受 DDoS 攻击时主要通过运营商的清洗服务进行防护。此外，游戏行业的也是 DDoS 攻击的重灾区。中国的游戏市场已经进入繁荣发展期。不管是网游、页游、端游，还是手游，尤其是手游得到爆发式增长。游戏行业遭受 DDoS 攻击的主要原因是行业恶性竞争，黑客恶意骚扰。其中，90% 的游戏业务在被攻击后的 2-3 天内彻底下线，攻击持续时间超过 2-3 天，玩家一般会从几万人调到几百人。攻击导致的用户数量下降是对游戏厂商最大的威胁。阿里云报告显示，2017 年 1 月至 6 月，游戏行业大于 300G 以上的攻击超过 1800 次；游戏公司每月平均被攻击次数为 800 余次。2017 年 2 月 27 日 02 点 28 分，某游戏公司遭遇峰值高达 700+Gbps 的 DDoS 攻击。300G 以上的 DDoS 攻击，在游戏行业已是“家常便饭”。面对高频大流量的 DDoS 攻击，多数游戏场景由于缺少足够的带宽容量进行防御抵抗，只能向上一级运营商节点求助。业务市场的强烈需求加快推动了运营商高性能清洗节点的建设步伐。

ADS NX5-10000 优势 接口丰富、扩展灵活

绿盟抗拒绝服务系统 ADS NX5-10000 的产品优势主要从两个角度进行分析：对比自身和外部竞争。与 ADS 的现有型号相比（以 ADS NX5-8000 为例），ADS NX5-10000 主要有如下四点差异。

- **硬件架构**

ADS NX5-8000 为 2U 的盒式设备，由接口网卡和机体组成。ADS NX5-10000 采用 6U 的机框式平台，产品构成包括机框、接口板和业务板。这样看来，ADS 10000 的组成更为灵活，符合高性能平台的架构特点，便于后续扩容和部件复用。

- **网络接口**

ADS 产品其他型号多数只支持千兆口和万兆口，而 ADS 10000 能够支持 40GE 接口和 100GE 接口，符合运营商网络的改造趋势。并且一块网卡就能同时满足 10GE、40GE 和 100GE 三种接口类型，

适配性强，节约成本，即使未来发生网路改造也不需要再额外采购和更换接口板。

● 防护性能

绿盟抗拒绝服务系统 ADS NX5-8000 单机最大 40G 的防护能力，ADS NX5-10000 能够实现满配 240G 的清洗量级。符号高端型号市场的需求，延伸产品线，有利于提升绿盟抗 DDoS 产品的市场份额。

● 扩容方式

采用盒式设备供货的 ADS 产品通过证书授权的方式实现防护能力扩容，而 ADS NX5-10000 的清洗能力与业务板关联。因此，ADS NX5-10000 在进行扩容时需要同时扩容证书和业务板。

● 运行平稳

ADS NX5-10000 作为一款电信级的产品，其稳定性在各类业务环境中得到了全面检验。硬件质量在变化的冷度、热度、湿度以及循环温度下进行长期压力测试，电源、CPU、接口等各部件全部满足持续正常运行。软件功能在流量达到最大处理性能时依然保持高可靠性。满足质量验收标准，用实力赢得了用户的口碑。

对比 ADS NX5-10000 与其他 ADS 型号的差异，可以明显看出高端平台的特点，以及该型号与大流量部署场景的高度适配性。在大体量的项目中，ADS NX5-10000 能够更好的发挥防护软实力，体现产品优势。中低端型号在大流量节点通常采用集群的部署方式，且无法满足对 40GE、100GE 接口的使用要求，在大型节点的项目方案中存在不足。而 ADS NX5-10000 的性能表现力，以及产品软实力对 DDoS 攻防经年累月的研究与实战经验，让我们在现有客户市场获得口碑，并且在大型和超大型客户项目中大展拳脚。加速扩大市场占有率，打造绿盟抗 DDoS 坚守以技术为核心，持续改革发展的活力产品形象。

绿盟抗 DDoS 的未来——贴合市场、持续发展

对于运营商这样超大体量的客户而言，防护节点的清洗能力要与带宽扩容相匹配，打造 T 级的防护节点早已具备成熟方案。其他大型客户的防护规格，尤其是采用按需防护的部署模式，可能会根据常见的 DDoS 攻击体量来考虑节点的清洗能力。绿盟发布的 DDoS 态势报告全面直观地展示了攻击的发展趋势和规模分布，峰值在 200G 以下的 DDoS 攻击在数量上依然占有较大比重。针对这个体量的 DDoS 攻击防护，绿盟 ADS NX5-10000 一台搞定!

市场的需求在变，产品的发展也在变。为了确保产品活力和市场占有率，我们需要了解当前的市场痛点，更要运用发展的眼光看待市场。通过交叉分析，把握未来的需求走向。攻击的发展趋势表明，DDoS 流量的量级依然会持续增长，而业务带宽的快速扩容预示着市场的不竭需求。为了实现供需双方的高度契合，绿盟抗拒绝服务系统 ADS 一方面通过大量的实战积累和对复杂多变的业务场景进行总结提炼，不断提升防护实力，确保技术先进性；另一方面加强对硬件高性能平台的调研和引入，使产品灵活应对各类业务场景的部署需求和使用条件，确保绿盟抗 DDoS 产品及方案在未来市场上依旧独领风骚。

东西向流量牵引小结

创新中心 江国龙

关键词：流量牵引　SDN 引流　API 接口引流　代理引流　微代理引流

摘要：东西向流量的安全检测和防护，在云安全体系中占据了重要的位置，如何有效的进行东西向流量的防护，成为了云安全研究的重要内容。本文从网络层面，详细总结了在对东西向流量进行防护时的多种流量牵引方法，并且结合业界一些主流的方案进行对比分析。

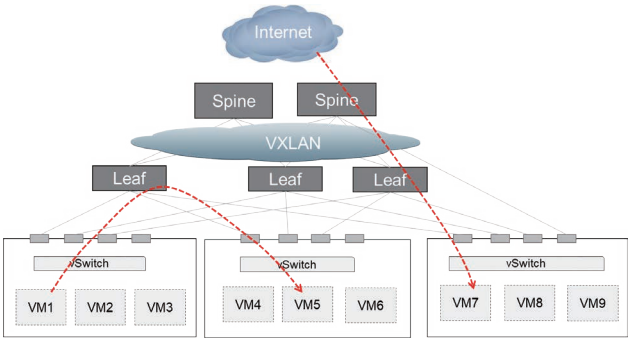
1、什么是东西向流量

通常在数据中心中，我们将其网络流量分为两种类型，一种是数据中心外部用户和内部服务器之间交互的流量，这样的流量称作南北向流量或者纵向流量；另外一种就是数据中心内部服务器之间交互的流量，也叫东西向流量或者横向流量。

早期数据中心的流量，80% 为南北向流量，现在已经转变成 80% 为东西向流量。数据中心网络流量由“南北”为主转变为“东西”为主，主要是随着云计算的到来，越来越丰富的业务对数据中心的流量模型产生了巨大的冲击，如搜索、并行计算等业务，需要大量的服务器组成集群系统，协同完成工作，这导致服务器之间的流量变得非常大。

伴随着这种由业务引发的流量特性的变化，数据中心的网络架构也由典型的三层树型结构，转变为 CLOS 或者 Spine-Leaf 等大二层结构。这种大二层概念甚至不再局限于一个数据中心内部，而在数据中心之间也是逻辑上二层互通。

本文中我们谈到的东西向流量，更多的是指云计算系统内部的



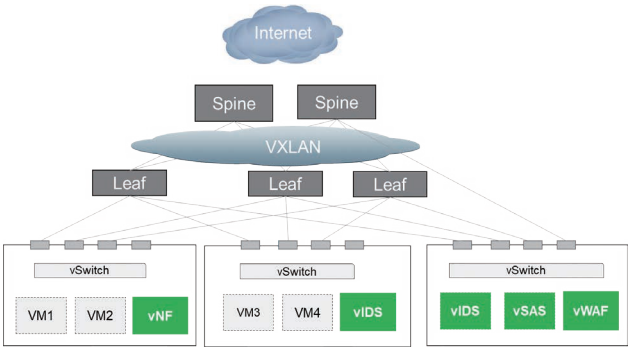
流量，也就是云中虚拟机之间通信的流量。这种流量既包括同一租户、同一子网内虚拟机之间的流量；也包括同一租户，不同子网间的流量；当然还可能是不同租户之间的通信流量。这里的云计算系统主要是指私有云，对于公有云，在原理上都是一样的。

2、为什么要进行东西向的流量牵引

这里提到的对东西向流量进行牵引，主要是解决云安全的问题。正如前文所描述的那样，云计算的数据中心，80% 的流量为东西向流量，而传统的安全解决方案，通常是基于固定物理边界的安全防护，那么对应到云计算数据中心，也就是只解决了南北向流量的安全防护问题，对于东西向流量的安全防护，基本上是无能为力的。

这种无能为力可以概括为两个方面：一方面是“看不到”，比如同一宿主机内的两台虚拟机之间的流量；另一方面是“不认识”，比如封装了 vxlan 等隧道包头的数据流量。具体可参考“附录：1 基于 SDN/NFV 的云安全实践”一文。

面对这个问题，当前厂商主要存在两种解决思路，一种就是把安全设备“放进去”，也就是将传统的“安全设备盒子”进行虚拟化，部署到云计算系统内部，这样就能够“触摸到”并且能够进行相应的安全防护；另一种思路就是把流量“引出来”，将需要检测和防护的流量，从云计算系统中牵引出来，经过相应安全设备的“清洗”之后，再将流量回注到业务系统之中。具体可参考”附录：2 云来了，安全盒子怎么办？”一文。



无论是采用上述哪种方案进行东西向流量的安全防护，都不可避免的需要对业务流量进行牵引调度，使相应的流量通过对应的防护设备。这样的话，东西向流量的安全防护问题就从安全设备无法“看见”、无法“认识”流量，转化为如何动态高效的对东西向流量进行牵引调度。

据笔者的了解，现在国内主流安全厂商的东西向安全方案，均是通过这种流量牵引的方式实现安全防护。

3、流量牵引痛点

对于云计算 IaaS 层面的服务，其核心主要是提供相应的计算、

存储、网络资源。对比这三大主要部分，计算和存储资源的虚拟化技术已经相对比较成熟和完善，但是网络的虚拟化相对来讲比较滞后。

因此，各云服务商（Cloud Service Provider，CSP）也就根据各自的特点，推出了多种不同类型的网络方案。比如 VMware 通常会使用虚拟交换机的原生模式，也有使用 NSX 的 SDN 方案。基于 OpenStack 的一些传统 CSP 可能会使用网络虚拟化的 Neutron 组件，激进一些的 CSP 甚至可能会使用 DragonFlow、OpenDove 等与 Neutron 集成的 SDN 方案。还有一些厂商会引入第三方独立的网络虚拟化和 SDN 方案。说的夸张一些，甚至可以说有多少家 CSP，可能就有多少种虚拟化的网络方案。

而无论是云服务商，还是第三方独立的虚拟化网络厂商，在对其标准产品的云网络进行设计的时候，通常仅仅考虑到相应的业务需求，几乎很少有对安全产品如何接入进行设计。

我们再从用户的角度来看，通常用户在将其业务进行虚拟化上云的时候，第一步往往考虑的仅是其业务系统虚拟化，很少考虑安全问题，尤其是早期建设的一些私有云，基本上没有任何安全方面的设计，甚至网络的配置很多还都没有实现自动化。

那么对于这样的私有云如果要进行东西向流量的安全防护，实现东西向流量的牵引，必然会牵扯到对其现有网络方案的改动，那么假如碰巧网络方案又是第三方厂商提供的，那么就出现了云服务商、网络厂商、安全厂商共同来重构这个云网络，因此“三个和尚没水喝”的故事基本上很容易上演。

4、如何进行流量牵引

痛点归痛点，虽然东西向的流量牵引调度确实存在各种各样的难题，但是其安全防护也是无法逃避的，那么在标准化的方式出来之前（相信随着技术的发展，会有一种标准化的方式提出），各家厂商也根据各自的特点，相继提出了多种的流量牵引方案。

下面本文就结合业界主流的方案以及绿盟科技在东西向安全防护的经验积累，详细介绍几种流量牵引方案。

4.1 SDN 引流

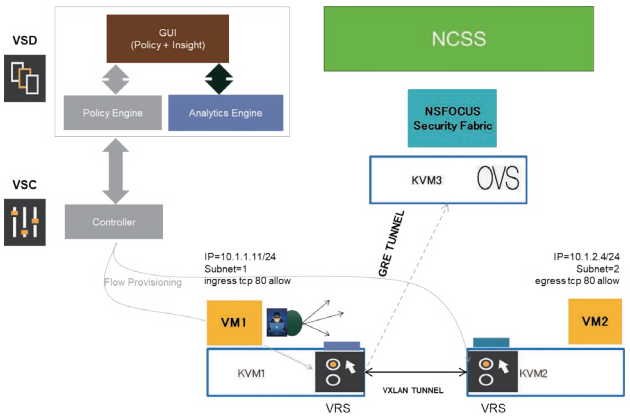
软件定义网络提出了一种将控制平面和数据平面分离的网络架构，在云计算环境中，SDN 也越来越多的得到部署应用，比如典型的开源组合方案 OpenStack+OpenDaylight。传统的通信 / 网络厂商，比如 Nokia、Juniper 等也推出了自己的一整套云计算网络 SDN 方案，SDN 初创公司也有类似的全套方案，比如 BigSwitch 的 BCF（Big Cloud Fabric）以及云杉网络的 DeepFlow。

SDN 逻辑上集中的控制器，有着全局的网络视图以及相应的流量信息，那么对于云内需要进行检测和防护的流量，可以通过 SDN 控制器自动化的进行流表项的下发，完成流量的牵引。

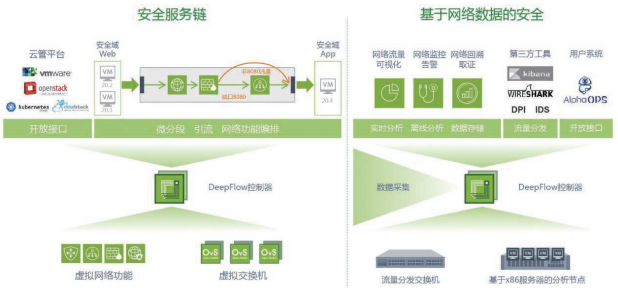
下面将以 Nokia Nuage 的 SDN 方案进行详细描述。下图中的 VRS、VSC 和 VSD 共同组成了其云网络的数据平面和控制平面，其中 VRS 是虚拟交换机，宿主机上的所有虚拟机全部挂在这个虚拟交换机上，宿主机之间的 overlay 网络则是通过 vxlan 实现，VSC 和 VSD 组成了其整个网络的控制平面。

当需要对 VM1 和 VM2 之间的流量进行检测和防护时，用户可以在 NCSS（NSFOCUS Cloud Security System）的安全控制平台发出防护请求，NCSS 根据防护请求，将对应的流量牵引命令发送给 VSC，VSC 根据这个流量牵引请求，下发相应的流表项并进行流量牵引的配置，图示的流量牵引是通过 GRE 隧道实现的。这样就完成了东西向流量的牵引工作。

Nokia Nuage 这种基于 SDN 的东西向流量牵引方案已经在运营商行业有不同程度的落地应用。



下图是国内的 SDN 初创公司云杉网络推出的基于 SDN 的东西向流量防护方案，方案同样是基于 SDN 网络架构，通过 SDN 控制器的全网控制能力，实现流量监控以及流量牵引调度，结合绿盟科技等第三方安全厂商的专用安全设备，实现深度的安全监测和防护。由于方案在原理上存在相似之处，这里就不再展开介绍了。



4.2 API 接口引流

API 接口引流主要是指通过调用云计算系统的标准引流 API，实现东西向流量的牵引调度。它和基于 SDN 引流的不同之处在于，基于 SDN 的网络厂商在为云计算系统提供网络设计和规划时，通常其标准方案和接口里，是不包含这种为了安全防护而存在的引流 API 的。那么如果要在 SDN 网络里实现通过 API 接口自动的进行流量牵引，需要 SDN 网络厂商与安全厂商进行一定程度的适配开发，从而实现整个引流过程的自动化。

这里的 API 接口引流，通常是通过云服务商提供的标准引流 API 实现的，典型的就是 VMware 提供的引流接口。云安全平台通过与 Vmware 的引流接口进行适配，实现整个东西向流量的牵引防护自动化。当然这种自动化的引流在 VMware 中典型的实现也是基于其 SDN 控制器 NSX 的。

当然，如果其 VMware 云平台不包括 NSX，也可以通过手动配

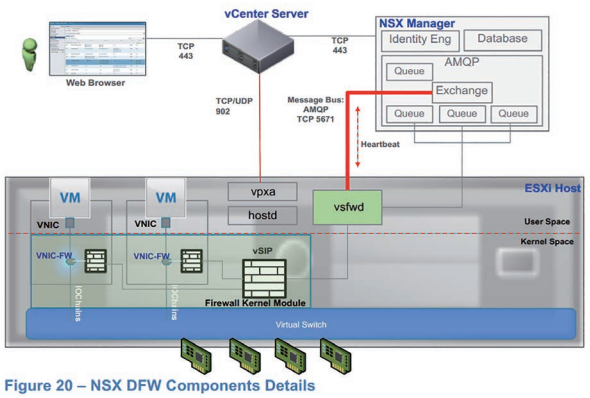
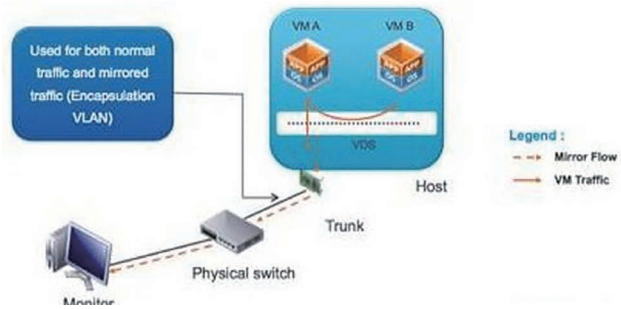


Figure 20 – NSX DFW Components Details

置实现对东西向流量向安全资源池的牵引调度，具体可以参考“附录：3 硬件盒子在云中获取网络流量的方法”

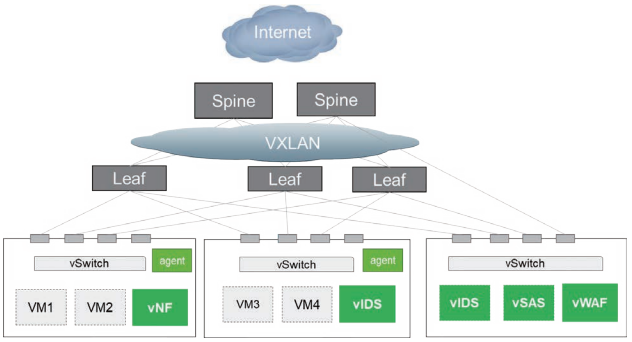


4.3 代理引流

对于云网络为非 SDN 网络的情况，如何实现东西向流量的牵引调度。这里主要介绍本节的代理引流和下节的微代理引流两种方式。

代理引流，顾名思义就是在云计算系统中，添加一个引流的代理，当然也有将其称作引流引擎、或者引流平台，其实实现的功能都是一样的。对于 SDN 网络中 SDN 控制器所做的相关引流操作，在这里完全由这个代理来实现。

安全控制平台将相应的引流请求发送至这个引流代理，引流代理根据虚拟机所在宿主机的位置以及虚拟机当前的网络情况，下发相应的引流指令，并且完成对应的网络配置，实现流量牵引。



这种引流方式，从原理来看，很容易理解。但是在实现上，也存在着很大的难度。因为引流代理在进行引流操作时，需要对云计算系统有着深入的理解和操作权限，这样每种代理对于云计算平台的耦合度就比较高，可移植性和可复制性比较差。

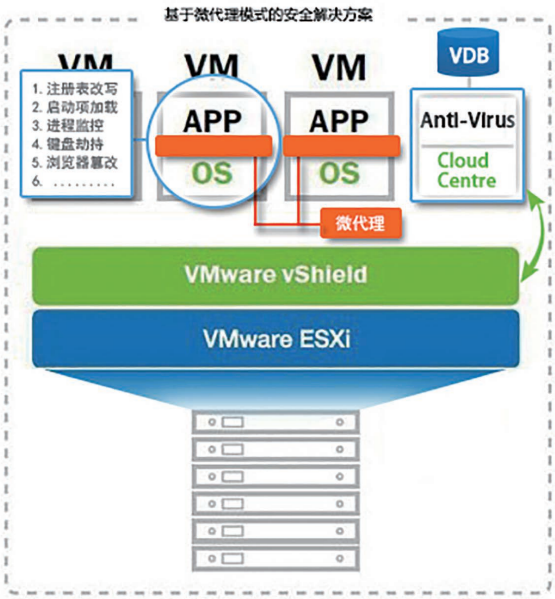
这种引流代理主要是为了实现东西向流量的安全防护而部署的，那么这个代理通常由安全厂商来提供，而代理所做的工作却是要对云计算系统的网络进行更改和操作，因此需要安全厂商和网络厂商有着紧密的合作才能够完成准确高效的流量牵引工作。

4.4 微代理引流

微代理和代理的区别主要体现在，代理是部署在计算节点的宿主机上，通过改变虚拟网络的相关配置，进而完成对应流量的牵引

调度。微代理则是像传统的终端安全软件一样，部署在虚拟机内部，那么这个微代理就可以在虚拟机的网络协议栈或者网卡等层面对数据包进行修改或者标记，完成流量牵引的工作。代表性的厂商比如 Kingsoft、Fortinet。

这种方式的优点在于，一方面不会对云计算系统的虚拟化网络做适配和修改，就可以完成流量牵引；另一方面，可以充分利用虚拟机的计算能力，无需额外增加安全相关的虚拟机投入。



这种方式，需要在客户的虚拟机内安装代理，那么会存在相应的信任问题，如果客户的数据比较敏感或者秘密等级比较高，通常不太会选择接受这样的方案。

5、总结

对于云计算中的东西向流量，引流防护已经成为了一种趋势，那么究竟该如何进行流量牵引，是一个难题。本文主要介绍了几种常见的引流方式和厂商的方案。

从本文的介绍可以看出，厂商在选择方案时，根据各自的技术积累和产品特性，会有不同的倾向性。比如云服务商，它可以决定整个云计算系统的设计，通常会选择 API 引流支持；对于网络厂商，它的优势在于有着云网络的设计和控制权，因此通常会选择 SDN 引流的支持；对于传统的杀毒厂商，它的技术积累主要存在于终端设备，那么它的方案可能会更倾向于微代理的方式。

比较尴尬的就是传统的安全厂商，所以安全厂商的方案通常是既支持 SDN 方式的引流，同时也可以做 API 引流的适配，如果云网络不是 SDN 的话，也可以通过代理或者微代理的方式。总结起来就是，既然安全厂商没有云计算系统的控制权，那么就会低姿态的进行多种支持和适配，凭借其专业的安全检测和防护优势，为云上的东西向流量提供安全保障。

附录

1、基于 SDN/NFV 的云安全实践

https://mp.weixin.qq.com/s/n03ZnkNPY8YKOA2cH7djmg

2、云来了，安全盒子怎么办？ http://blog.nsfocus.net/cloud-safe-box/

3、硬件盒子在云中获取网络流量的方法 http://blog.nsfocus.net/hardware-box-network-traffic-cloud/

基于SDN构建智能DDoS清洗系统

IIS技术团队 赵跃明 系统架构部 李凯

关键词：DDoS 清洗 SDN 技术 智能防护

摘要： 传统的 DDoS 防护方案在满足弹性、可调度和增值服务等需求。SDN 技术的出现，特别是与网络虚拟化结合，给安全设备的部署模式提供了一种新的思路。本文提出的基于 SDN 网络的智能清洗系统能够从 DDoS 攻击的识别，到清洗策略的制定，以及清洗资源的选择，实时最优匹配，达到按需清洗，智能清洗的目的，有效防护 DDoS 攻击。

一、背景

1.1 DDoS 攻击趋势

DDoS 攻击技术呈现两极分化的局面，大流量攻击不断增长，按照此趋势足以对互联网骨干网络造成威胁，并开始走向云端攻击的形式；与此同时，中小流量技巧型攻击也在暗地持续的发展，主要针对各行业中的业务设计不合理的环节，这些攻击很容易导致用户的业务缓慢甚至无法进行。现有越来越多的攻击者混合使用流量型和技巧型攻击手法，让用户防不胜防；

1.2 SDN 技术

软件定义网络（Software Defined Networking，SDN）提出了一种全新的网络架构，能够通过逻辑上集中的控制平面，实现网络管理、控制的集中化、自动化。基于 SDN 网络技术实现的网络集中控制，流量实时调度技术已经广泛应用到数据中心，云服务，NFV 等众多的场景。

本系统结合 DDoS 防护和 SDN 的技术原理，通过安全数据平面与控制平面分离，对物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行了解耦，底层抽象为安全资源池里的资源，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现一种灵活的安全防护。

二、传统 DDoS 清洗面临的挑战

2.1 独立清洗节点面临的挑战

在独立清洗节点部署的情况下，主要有如下三个方面的挑战：

- 单节点的清洗容量上限被突破后，束手无策；

对于用户，面对未知大小的攻击流量，往往不能准确定义对清洗设备容量的需求，一旦发生攻击流量大于清洗设备的防护能力，将导致用户业务无法正常开展。

- 单节点的防护能力类型集成度过高，统一处理组合攻击效率较低；

单个清洗盒子为了适应日益复杂个攻击场景，几乎涵盖了所有常

用攻击的防护算法，导致清洗盒子的软件复杂度越来越高。而实际发生的 DDoS 攻击，常常都是某种，或者某几种固定的攻击的组合，复杂的软件模型往往导致 CPU 和内存的有效利用率偏低。

- 单节点部署在线防护业务可靠性不足

可靠性方面，单个清洗设备，一旦发生软硬件故障，或者需要升级维护，都将不能持续保护用户的业务，导致用户业务面临被攻击的危险。

2.2 集群清洗面临的挑战

面对单个清洗设备清洗能力不足时，人们往往想到把多台清洗设备组成集群，来扩大清洗防御能力，但是由于集群清洗的负载均衡模型限制，通常要求参与到清洗集群的清洗设备的性能和特性一致。而实际上，随着清洗设备的演进，清洗设备间的能力差异很大，清洗特性方面也很难一致，比如有的清洗设备支持硬件加解密，有很好的 HTTPS 防护性能，而较老的清洗设备则没有该功能。这些限制导致集群组网的各种约束，甚至是部分清洗设备的更新淘汰，用户资产利用率低。

三、基于 SDN 原理的智能清洗系统

3.1 系统部署视图

本系统分的部署分为管理域和业务域两个部分：

管理域为智能清洗平台和流量控制器（WITCH SDN）、流量监测设备（NTA）以及清洗节点集群间的指令传递；

业务域是当流量监测设备检测到攻击发生时，上报攻击和流量信息到智能清洗平台，智能清洗平台发送流量牵引和流量调度指令把攻击流量指向 SDN 交换机的入口，SDN 交换机和上端的交换机直连，实现攻击流量的被动引入和合法流量回注过程，所有的清洗设备直接和 SDN 交换机直连，实现流量的被动清洗和流量回注。

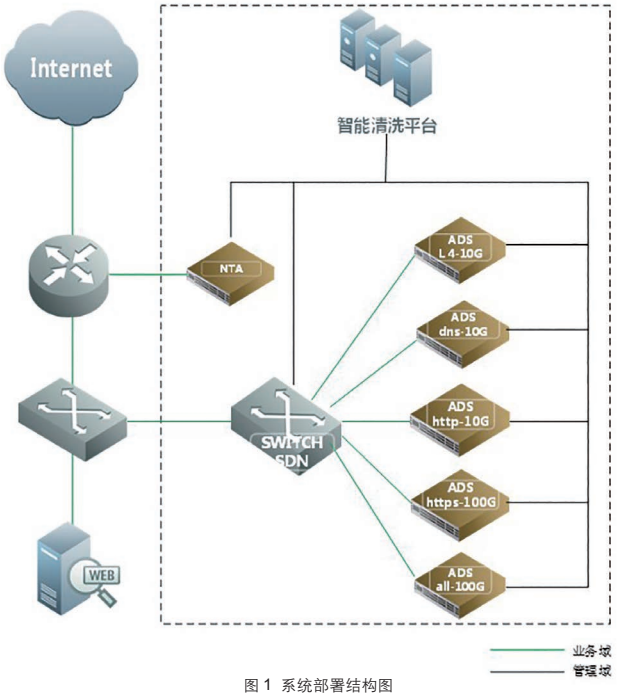


图 1 系统部署结构图

3.2 系统架构（如图 2）

3.2.1 智能清洗平台北向接口

智能清洗平台提供如下北向接口：

- 业务受理，接收被保护服务器信息，初步逻辑运算，如果智能清洗平台性能或者特性不能满足，返回出错提示，否则下发流量

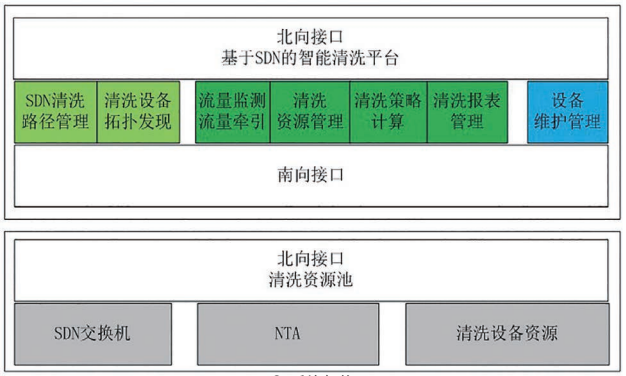


图 2 系统架构图

监控请求到 NTA 设备；

- 清洗报表，智能清洗平台提供被保护服务器的 DDoS 攻击防护效果的多维报表；
- 设备维护，提供智能清洗平台的设备维护接口，如常用的版本升级，设备上下线操作等；

3.2.2 SDN 路径管理

智能清洗平台通过 OpenFlow 协议，下发特定的转发表，可以动态实时定义待清洗的流量的转发的目的端口，达到定义待清洗流量进入匹配的清洗设备清洗的目的。

3.2.3 清洗设备拓扑发现

随着清洗中心的规模逐渐扩大，接入清洗中心的清洗设备越来越多，传统的依靠技术工程师手工配置维护网络设备的工作量越来越大，而且容易出错。

采用标准的 LLDP 协议，网络设备通过相互通告之恋的链路层信息，通过计算，最终形成网络拓扑结构。

LLDP 简介

LLDP（LLDP，Link Layer Discovery Protocol，链路层发现协议）是 IEEE 802.1AB 中定义的第二层发现协议，它提供了一种标准的链路层发现方式。LLDP 协议使得接入网络的一台设备可以将其主要的能力，管理地址，设备标识，接口标识等信息发送给接入同一个局域网络的其它设备。通过采用 LLDP 技术，在网络规模迅速扩大时，网管系统可以快速掌握二层网络拓扑信息和拓扑变化信息。

通过在 SDN 交换机以及接入的清洗设备上启用 LLDP 协议，可以自动发现接入 SDN 交换机的清洗设备的网络拓扑。

3.2.4 流量监控流量牵引

智能清洗平台通过 NTA 设备实现被保护 IP 的实时流量监控，当被保护 IP 的实时流量超过设定阈值时，NAT 设备主动向智能清洗平台告警，智能清洗平台通过防护策略计算后，下发流量牵引指令到 NTA 设备，实现流量的实时监控和流量牵引。

3.2.5 清洗资源管理

清洗设备接入智能清洗平台的管理网络后，主动上报清洗设备清洗能力和清洗特性；智能清洗平台实时计算清洗设备的清洗资源，如总的清洗能力，已经使用的清洗能力等；当新的攻击发生时，智能清洗平台通过对攻击流量的大小和分类识别，选取匹配的清洗资源，并刷新清洗资源池；

3.2.6 清洗策略计算

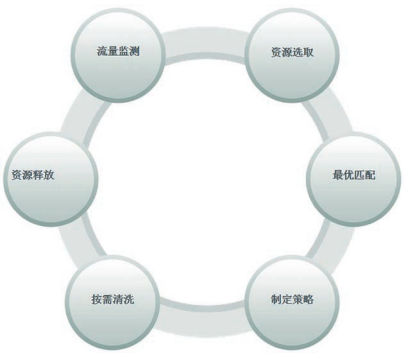
智能清洗平台通过对攻击的分类识别，计算出最匹配的防护算

法，下发到选中的清洗设备资源上；当攻击流量变化时，或者防护效果不佳师，重新计算防护算法，并下发到清洗设备上，实现清洗策略的实时计算，动态更新；

四、智能清洗系统的价值

4.1 智能清洗系统的防护闭环

智能清洗系统能够进行网络流量监控，合适资源选取，实时最优匹配，下放制定的策略，对攻击流量进行按需清洗，当攻击停止时，自动的进行资源释放，形成了防护闭环；



4.2 智能清洗系统的优势

智能清洗系统有如下方面的优势：

● 对清洗设备减负

清洗设备只关注清洗算法等防护特性，BGP 牵引，WEB 网管等可以由智能清洗平台接管，并减少了软件的复杂度的同时，有效利用的清洗设备的硬件资源；

● 有效保护用户资产

允许清洗设备在清洗特性和清洗容量上的差异，充分发挥清洗设备资产的清洗能力；

● 网络维护工程师减负

清洗设备通过链路层发现协议，把设备直连的邻居信息上报给智能清洗平台，最终实现清洗设备网络拓扑自动发现，真正的即插即用；

● 大幅提高防护性能

利用硬件特性，增强防护性能，充分利用交换机的硬件特性，如交换芯片的 ACL 资源，把通过清洗设备算法产生的黑白名单终端信息上报到智能清洗平台，智能清洗平台生成 ACL 表下发到 SDN 交换机的硬件，将大大提供转发性能的同时，清洗设备只关注未知终端的流量，提高了防清洗设备的防护性能；

● 防护资源最大效率利用

防护策略自动下发，当检测到攻击时，智能清洗平台通过实时计算选取匹配的防护设备，制定有效的防护策略，并自动下发到对应清洗设备。攻击流量自动调度，当策略下发完成后，智能清洗平台通告 NTA 设备实施流量远程调度，并同时打开 SDN 交换机的连接选中的清洗设备的对应端口，实现流量实时智能调度；

● 硬件维护智能化

清洗设备代为维护，清洗资源设备都通过智能清洗平台代为维护。智能清洗平台可以根据清洗设备的繁忙程度，定制对用户业务无影响的升级维护计划，用户业务不会由于清洗设备的升级维护而脱离保护；智能清洗平台采用多机集群方式，有效防止清洗智能平台的单点故障；

五、参考文献

《基于 SDN/NFV 的云安全实践》

《2017 上半年 DDoS 与 Web 应用攻击态势报告》

DDoS攻防演练平台

系统架构部:李凯　IIS技术团队:陈裕涛　何坤

关键词：DDoS 防护　清洗服务　增值服务

摘要： 传统的 DDoS 的增值服务方案由于 DDoS 威胁事件频度低，防护服务感知不高，导致客户满意度低，增值服务推广面过窄。抗 D 技术团队结合运营商和 IDC 服务运营经验，重点在客户威胁感知和价值体验上进行深挖，开发 DDoS 攻防演练平台。完成“能力推广 --- 业务开通 --- 增值运营 --- 价值呈现”增值服务的闭环，践行绿盟科技智慧安全 2.0 战略。

一、平台简介

随着移动互联网的快速发展，消费者的心理需求和行为结构均发生了很大的变化，曾经“广告和推销”的传统营销模式的时代一去不复返，体验和感知成为市场的关键因素，体验式营销开始为企业广泛使用；

DDoS 防护领域中，由于 DoS 攻击发起的不定时性、攻击技术较复杂以及防护技术门槛较高，使客户对 DDoS 攻击及防护的认知还是停留在技术人员提供的晦涩难懂的报表和一些攻击新闻层面，客户无法感知攻击对业务威胁的程度和清洗服务价值，以帮助其作出最佳的选择；

攻防演练平台通过部署分布式架构的 DDoS 攻击仿真系统，基于业务流量和业务健康的监控系统，结合单体百 G 清洗能力的清洗设备，配合开发的演练管理平台与移动端 APP，为存在流量清洗服务需求的客户提供真实直观的攻防体验；

二、面临的挑战

2.1 攻击的威胁感知滞后

由于不同客户对 DDoS 领域及技术的了解程度不同，对于 DDoS 的威胁感知的程度和需求，也是有较大的差别。

- 客户业务处于创业期，业务规模较小时，抱着“咱不惹事，也不出名，不会被盯上”的侥幸心理，**对 DDoS 的潜在风险认识不足**；
- 客户的业务处于发展阶段，遭受过一定程度的 DDoS 攻击，通过服务能力增强和带宽扩容，暂时的缓解了 DDoS 的威胁；**对激增的攻击预估和演练缺乏必要的手段**。
- 客户的业务处于规模较大的阶段时，则认为“万能的防火墙 / IPS”能够解决 DDoS 的威胁，但防火墙 /IPS 是高强度的检查为代价来进行防护的；一旦大流量攻击发生，**传统常规的防护设备也会陷入束手无策的被动状态**。

2.2 防护能力的体验不足

- DDoS 攻击发生的时间存在随机性和不可预估性，客户往往很难有机会亲身经历攻击发生和防护缓解的全过程，**攻防过程的参与感不足**。
- 客户对 DDoS 攻击的对业务影响的维度和程度缺乏标准指标的了解和跟踪，也就不**能对防护效果和防护能力优劣进行准确判断**，无法选择适合自己的防护解决方案；
- DDoS 攻防过程展示本身就是向客户传递价值最直接的方式，**如何将实时对抗过程可视化，将防护价值最直接的展示在客户面前，是体验式营销的关键**。

总而言之，如何让客户直观真实体验到 DDoS 攻击给业务系统带来的危害及损失，让客户对 DDoS 威胁产生直观的感受，并提供防护能力可视化体验，达到体验式营销的目的，是 DDoS 防护业务推广的当务之急。

三、平台架构及实现

为解决上述应用场景的需求，抗 D 技术团队新研发了攻防演练平台，该平台基于绿盟十多年 DDoS 攻击研究经验、成熟防护产品和运营服务实践的积累，实现演练服务的自动、自助、可运营、能力云化与集中管理。

平台的架构如图一所示。

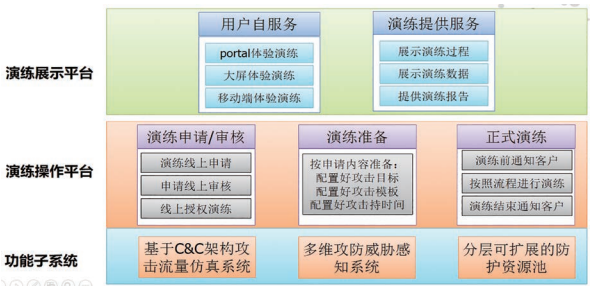


图 1 攻防演练平台架构

3.1 基于 C&C 架构攻击流量仿真系统

攻防演练平台依据真实网络中最常见的 C&C（Command and Control Server）的架构来沟通攻击流量仿真系统，其构建过程主要分为如下步骤：

1. 部署一台 C&C 服务器（主控）和多台发包机（受控），并保证 C&C 服务器能够通过控 制账号访问发包设备。

2.C&C 服务器将受控的发包工具自动化的部署到发包机上，并获取所有发包机初始的发包资源（CPU 和带宽资源），形成统一的攻击集群。

3. 平台将用户在平台上定义的攻击流量及演练时长，智能均衡的将其转换为每台发包设备的发包指令（类型、大小），并统一控制演练时间。

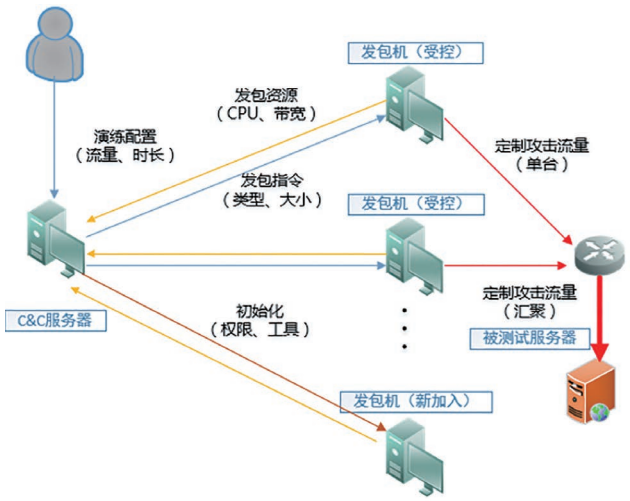


图 2 攻击流量仿真系统架构

本系统相比传统发包仪器（比如 IXIA），有如下方面的优势：

	攻击仿真系统	IXIA等测试仪器
流量带宽	弹性扩容，攻击流量可上T	型号固定，最大100G
流量类型	全系列DDoS类型	基于协议行为构造困难
成本	普通硬件及虚拟化平台	昂贵专业仪器
网络部署	一键接入，智能负载均衡	专门机架和牵线

图 3 攻击仿真系统和 IXIA 对比

3.2 分层可扩展的防护资源池

DDoS 的防护，本质上是资源的对抗，在不同量级的流量攻击下，其防护技术和方法也是不同的，所以需要建立分层的可扩展防护资源池，以便达到根据攻击流量量级适配最有效的防护方法。

分层的可扩展防护资源按照流量的量级及对应技术主要分为如下三类：

1. 攻击流量在业务带宽范围内，采用清洗的方式进行防护，目前基于 HTCA 架构的 ADS NX5-10000 的设备，单台满载板卡的清洗能力能够达到 240G 的清洗容量，采用集群能够轻松的扩展部署 T 级别的清洗容量。

2. 流量超过得了业务带宽范围，则需要通过联动上游的路由器协同处理，将流量过大的目的 IP 的流量，通过 FLOWSPEC 的技术，将其限速和过滤规则传递给上游路由器处理，使流量降低到带宽范围内后，再进行清洗。

3. 当出现超大流量，大规模影响网络基础设施时，则需要协调运营商，并调用运营商接口进行源端压制，以保证基础网络的安全。

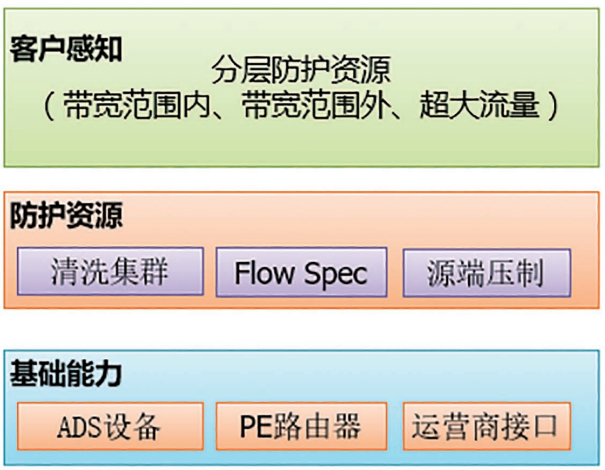


图 4 分层可扩展的防护资源池

3.3 多维攻防威胁感知系统

为了达到客户能够更好的感知攻击的威胁和体验我司技术防护能力的目的，对攻击威胁指标进行量化，并通过攻防过程实时跟踪其指标数据的变化，建立了多维的攻防威胁感知系统。

系统主要从如下三个维度进行威胁跟踪和展示：

1. 网络带宽资源状态，通过 NTA 设备监控业务 IP 的实时流量，结合业务 IP 的业务带宽，从网络层的带宽占用比来进行度量。

2. 系统资源状态，通过周期性的获取服务器的资源接口，定期获取 CPU 和内存以及进程状态数等信息，对系统的健康度进行全面的监控。

3. 业务服务状态，通过网络连通性（ping）、网络层拨测（TCP、SSL）、业务拨测（业务访问成功率）等技术的利用，对业务的可用性进行标识。

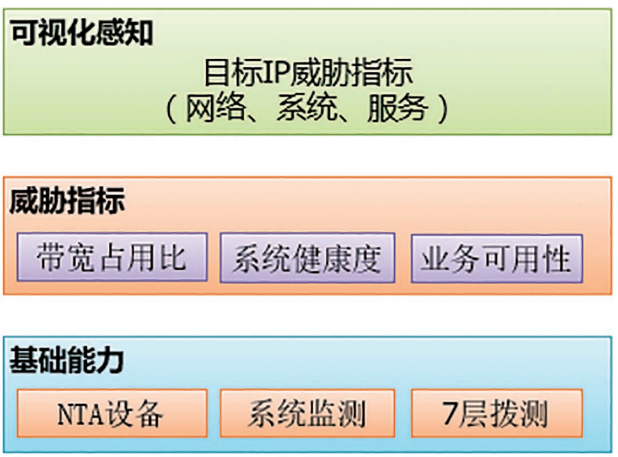


图 5 多维攻防威胁感知系统

该威胁系统相比传统的攻击检测方式，有如下优势：

- 将攻击事件事后被动投诉的被动局面，转换为事件主动 APP 推送，让移动运维成为可能。
- 检测感知事件从原先的 10min 级别提升到 10s 级别，缩短了对攻击事件响应周期。
- 从单一的流量激增检测方式，扩展为多维的威胁指标（网络、

系统、服务）的综合判断，降低了攻击事件的误判率。

3.4 演练平台用户界面

演练平台的用户操作主要包含如下三个部分：

■ 演练定义

客户在新增演练时，需要定义演练名称，演练客户权限引用（受控权限校验），演练 IP 地址，攻击流量定义（类型、大小和演练时间）。

■ 演练过程展示

演练过程分为“攻击开始 ---> 业务受损 ---> 清洗开始 ---> 业务恢复 ---> 攻击结束”五个阶段，且对于每个阶段的耗费时间有明确的进度条展示；

每个阶段都有通过业务带宽占用率 \ 业务拨测监控趋势图、实时告警、攻击类型分布和清洗攻击流量趋势等图，实时对攻击威胁和防护体验进行可视化的展示，其过程也能够通过手机 APP 对客户进行实时传递信息；

图 6 攻防演练平台主界面

■ 演练中止和结束

提供用户临时中止演练的接口，当然演练也可按照既定演练时间结束，结束之后提供整个演练过程的攻击和缓解的详细报表，记录和证明演练的对抗细节和结论。

演练平台的用户操作主界面如上图所示（如图 6）：

四、平台价值

本文提出的攻防演练平台，通过部署分布式架构的 DDoS 攻击仿真系统，利用基于业务流量和业务健康监控系统，结合百 G 级别清洗能力的 ADS 防护集群，配合开发的演练管理平台与移动端 APP，为存在流量清洗服务需求的潜在客户提供真实直观的攻防体验，开发了具有一定规模、攻防兼备、以攻促防的攻防演练平台；为云清洗的市场推广打下了坚实的基础，完成了“能力推广 --- 业务开通 --- 服务运营 --- 价值呈现（报表）”增值服务的闭环；使客户对绿盟的印象从卖盒子真正改变为平台创新型厂家，践行了绿盟科技智慧安全 2.0 战略。

NSFOCUS绿盟科技

THE EXPERT BEHIND GIANTS

巨 人 背 后 的 专 家

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS ADS
绿盟抗拒绝服务系统

T级 DDoS 防护
只等你来试！

能挣钱！运营商增值服务、10多个大型项目　**看实效！**高防云清洗平台、数分钟立竿见影　**易上手！**APP+Web可视化、效果实时掌控

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS绿盟科技