绿盟威胁分析系统

产品白皮书

【绿盟科技】

■ **文档编号**	NSF-PROD-TAC-产品白皮书	■ **密级**	完全公开
■ **版本编号**	V1.4	■ **日期**	2018-04-09
■ **撰 写 人**		■ **批准人**	

目录

插图索引

一. 前言

如今，政府和企业同时面临着一个不断演变的网络威胁环境。最初的黑客攻击是为了获得影响力及自我满足去攻击媒体网站，而现在已演变成为了经济、政治等目的的攻击。

攻击者能够通过窃取知识产权来直接获取利益，也可以入侵、窃取客户的个人金融信息，甚至直接加密文档后进行赤裸裸的勒索，更有甚者破坏对方的服务以至国家的基础设施。动机的变化，同时也带来了攻击方式的变化。

从过去广泛、漫无目的的攻击威胁，在数年内迅速的转化为针对受害者组织将造成严重后果的高级可持续威胁（Advanced Persistent Threat）。例如勒索软件，在最近两年，呈现爆发式增长。

高级可持续威胁具备以下三个特点：

- 高级：攻击者为黑客入侵技术方面的专家，能够自主的开发攻击工具，或者挖掘漏洞，并通过结合多种攻击方法和工具，以达到预定攻击目标。
- 持续性渗透：攻击者会针对确定的攻击目标，进行长期的渗透。在不被发现的情况下，持续攻击以获得最大的效果。
- 威胁：这是一个由组织者进行协调和指挥的人为攻击。入侵团队会有一个具体的目标，这个团队训练有素、有组织性、有充足的资金，同时有充分的政治或经济动机。

APT 威胁更多的存在于国家之间的间谍活动，以及黑客团体利益驱动下的信息窃取行为。国家之间的敌对状态，获取对方的情报信息，入侵政府机密单位，获取和掌握对方的资料。公布对方的不利信息，是国家对抗在信息安全领域的主要形式。事实上带动了 APT 威胁的发展。其次，黑客团体为了获取经济利益，直接和间接的入侵政府和企业，获取敏感资料和情报，在黑客产业中进行售卖，获取利益。

APT 威胁往往可以绕过防火墙、IPS、AV 以及网闸等传统的安全机制，悄无声息的从企业或政府机构获取高级机密资料。在 2016 年 Verizon 信息外泄调查报告中可以看到，2015 年发生的重大信息数据外泄的受访组织中，有 60%是在相关执法机构告知后才知道信息外泄的情况。

IDC 在 2016 年的报告中指出：“APT 攻击成为公认的危害极大的攻击方法，其隐蔽性能够保证黑客长期窃取窃取敏感数据。国内安全厂商通过监控，判断中国为 APT 攻击主要受害国之一，基于政治、经济目的的 APT 攻击严重威胁中国政府、金融等行业的安全，因此防范 APT 攻击已经受到政府、金融行业客户的广泛关注。黑客可以借助 Email 进行鱼叉式攻击，也可以通过分析个人的行为特征，进而采取水坑式攻击，多种入侵手段对 IT 系统提出了极大的挑战”。

高级可持续威胁（APT）已经成为当今公认最具威胁的网络攻击类型。

二. 攻防的新特点

现今主流的安全防御机制，往往由防火墙或 NGFW、入侵检测、网闸以及防毒软件建构其核心检测能力，这些产品依靠已知攻击特征码进行模式匹配来检测已知的网络攻击，在一些特定情况下，也可能检测针对已知漏洞的新型攻击。

这样的解决方案，能非常有效的监测到一般的已知网络攻击，如：蠕虫、特洛伊木马、间谍软件、botnet 及基本的电脑病毒等，但针对现今最威胁的高级可持续威胁，却完全没有招架之力。在大多数情况下，APT 攻击面对传统的安全防御机制时，有如入无人之境，因为这些攻击没有特征码，故传统的防御机制无法检测攻击者在起始阶段所采取的攻击手段，最终导致网络攻击者可以任意的控制网络。

一些防护更深入的传统方案，会结合 IPS 或者 NBA 产品进行异常检测，协助找到网络攻击，这种方式虽然可以侦测到新型的 APT 威胁，但是由于经常受到误报的影响（将正常流量归为异常），因此防御效果不佳，并且也容易出现漏报的问题。

正是因为传统安全防御机制在 APT 攻击下缺乏必要的监测能力，因此近年来有大量的建立较完善传统防御机制的企业被 APT 攻击者成功得手，例如：

- 2009 年 极光行动：通过 APT 攻击 google 和其它科技公司，目的似乎是试图获取存取权限并可能尝试修改应用代码。
- 2010 年 Stuxnet ：其攻击目标是伊朗的铀浓缩基础设施，攻击首先透过 Microsoft Windows 安全漏洞散播，随后在网络中横向传播，最终到达西门子工业控制设备，

并导致其软硬件故障。

- 2011 年 RSA SecurID 攻击事件：RSA Security 收到 APT 攻击，部分 SecurID 动态密码生成器被窃取，攻击者进一步攻击使用 SecurID 双因子认证的客户，窃取其机密信息。
- 2012 年 Flame 间谍软件攻击：Flame 被认为是有史以来最精密的恶意软件，它伪装成 Microsoft 例行软件升级程序，并偷偷监控伊朗的信息网络，传回信息情报以供网络战争使用，它也是 2012 年 4 月伊朗官员无法通过网络连接石油系统终端机的攻击起因。
- 2016 年乌克兰电网 BlackEnergy 攻击：乌克兰大规模停电事件，是近年来 APT 攻击最为引人注目的安全事件。攻击范围广泛，使得乌克兰数以万计的家庭停电，而且，针对电网进行攻击，是继伊朗核设施遭受攻击后，又一起针对工业控制系统的攻击行为。调查显示，黑客利用 BlackEnergy 变种，通过鱼叉攻击，入侵乌克兰电网，实施了攻击。
- 2017 年 WannaCry 勒索病毒攻击：2017 年 5 月一种“蠕虫式”的勒索病毒软件在全球爆发，至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，影响范围覆盖到金融，能源，医疗、教育等众多行业，造成严重的危机管理问题。

通过对案例的分析，以及对信息网络广泛应用的了解，我们可以知道，无论是对政府还是对企业的攻击，都可能造成巨大的危害。

对于国家政府的 APT 攻击，可能的危害包括：

- 电力网络中断
- 银行资料泄密、篡改以至业务中断；
- 医院或者急诊室无法运作
- 军事、科技的机密外泄
- … …

对于企业的 APT 攻击可能造成的危害包括：

- 业务中断
- 竞争力丧失
- 违反合规性要求

- 声誉受损
- ……

因为 APT 对信息网络、对国家经济、政治、军事可能造成巨大的危害，各国对此积极出台政策，应对相关的变化。

勒索软件是另一类安全威胁。从 2016 年开始，勒索软件出现了井喷式的增长，并且向安卓、苹果等操作系统扩展。勒索软件在加密文档和图片等重要资料后，通常在桌面留下勒索通知，索要比特币。

勒索软件和 APT 威胁不同，APT 威胁会隐藏自己，持续盗取敏感资料；勒索软件直接告诉你已经中招。尽管表现形式不同，但其攻击手法类似，也是通过高级手段，尽量绕开传统防御方式，如防病毒，防火墙等，进行企业内网，加密文档后进行勒索。

APT 威胁和勒索软件，是高级威胁中两个重点防护对象。

三. 攻防技术发展特点

针对 APT，国内外安全界曾经提出了多种不同的检测或预防技术，安全厂商往往使用这些方法的组合来进行分析监测，这些技术包括：

一、 采用深度包检测进行网络分析，如：

a) 网络通信分析

b) 多层网络流量异常、行为检测、事件相关性

c) 枚举异常 IP 流量（如：基于 RFC 等标准）

d) 恶意主机、URL 基于文件信誉体系

e) 恶意软件的命令和控制通道检测

二、 自动文件静态分析

a) 自动分离、解析文件对象

b) 检测嵌入的可执行代码

c) 检测逃避技术，如封装、编码及加密等

三、 基于可视化、报警等进行手动分析

a) 恶意行为可视化及其分析报告

b) 可视化详细的网络流量，并关联威胁、信誉与风险级别

c) 网络流量或完整的数据包捕获上的取证分析

这些方式在使用中，被发现了各种问题，包括误报率高、大量漏报的问题、也包括对安全管理人员的要求过高，以至于大多数组织无法使产品发挥预想的检测作用，因而没有被市场广泛认可。直到以 Fireeye 为代表的基于虚拟执行技术的产品出现，易于部署管理、可以忽略的误报率、及时检测未知威胁，收到了客户的广泛认可，市场有了较快的发展。

越来越多的厂商考虑虚拟执行或模拟环境的检测方法，利用一个操作系统或浏览器实例，发起建立一个虚拟的执行容器（或者称为一个沙箱），使恶意软件在其中执行，就像在真实的用户环境一样。通过这种方式，厂商可以对整个攻击生命周期进行观察，从开始的漏洞利用，随后和命令控制服务器的通信，下载进一步的恶意可执行文件以及随后的网络回调。这种检测技术因为可以检测漏洞利用阶段的恶意软件行为，因此避免了其它只检测后期阶段活动产品的漏报（这个阶段是可以采用加密等一系列方式进行逃避），并且因为监测是基于一个高度近似真实用户环境的恶意软件的真实活动的，因此误报率极低。良好的漏报率和误报率指标，是这种基于虚拟执行环境或者沙箱的检测技术成为高级可持续威胁监测的最重要技术手段。

四. 绿盟威胁分析系统

绿盟威胁分析系统，英文名称为 NSFOCUS Threat Analysis Center（以下简称 TAC），可有效检测通过网页、电子邮件或其他的在线文件共享方式进入网络的已知和未知的恶意软件，发现利用 0day 漏洞的 APT 攻击行为，保护客户网络免遭 0day 等攻击造成的各种风险，如敏感信息泄露、基础设施破坏等。具有如下特点：

- **具备未知威胁检测能力**：高级可持续性威胁，往往是有组织的黑客团体，对具备较高经济、科技、军事等价值的目标的持续攻击。从攻击方式上看，多采用定制化的攻击工具（木马、后门等恶意软件），其中还会使用零日漏洞，这样的攻击方式传统

的安全检测体系很难有效发现，新的监测系统应针对这种情况，需要可以检测零日漏洞、未知木马等未知威胁。

- **基于动态检测技术，不依赖传统签名技术：**要达到未知威胁检测的目的，就不能依赖传统的签名检测技术，签名检测技术依靠对已知攻击特征或漏洞特征的收集，而高级可持续威胁在危害大规模爆发前，是没有攻击样本的。基于先进的动态检测技术，即基于沙箱虚拟执行的方式，可以根据软件在虚拟环境中的代码行为特征进行实时分析，来判断是否存在攻击特征，这种检测方式不需庞大的检测签名库，同时检测已知和未知威胁，并且可以防止各种针对静态检测的逃避技术。是高级可持续威胁监测最有效的技术。
- **集成绿盟威胁情报系统：**绿盟威胁情报系统（NSFOCUS Threat Intelligence，以下简称 NTI），通过海量数据的采集，分析，验证，获得威胁信誉，包括文件安全信誉，CC 主机安全信誉，恶意 URL 安全信誉，IP 地址安全信誉等。同时，NTI 还集成了金山文件信誉系统，腾讯的 URL 信誉系统，最大程度提供广泛的信誉情报。TAC 产品，利用威胁情报，对于高级威胁，可以先通过情报引擎进行过滤，及时告警。
- **微乎其微的误报：**检测系统及时发现各种威胁，并产生报警，而威胁的消除则需要后续安全人员的响应。为了保障安全响应的及时、有效，监测系统就必须保证有极低的误报率，假设存在大量的误报，则宝贵的资源和时间有可能就消耗在对误报事件的处理当中，而真实的威胁利用这个时间差，有可能对信息系统造成巨大的损害。
- **详尽的报警信息：**为了有效的进行安全响应，还需要监测系统能够提供详尽的报警信息，使响应的安全人员可以有的放矢的开展工作。具体的报警信息可以包括：是否修改了注册表，是否新建了进程，是否尝试对外连接命令与控制服务器，是否会直接感染其它机器等等。系统应设法监测恶意软件是否有上述的活动，并作为报警的一部分输出给安全管理员。
- **开放 API 服务：**TAC 系统对外提供开放的应用开发接口 API。通过应用开发接口，可以与用户现有安全产品进行集成。TAC 作为未知威胁的分析中心，终端、网络、邮件、web 等多个安全设备或系统可以集成 TAC 可疑文件分析能力。第三方设备提交可以文件或 URL，经过 TAC 的引擎分析后，获取分析结果，第三方设备可以根据此结果进行操作，比如放行或者禁止等。

- **集成已知威胁检测技术：**攻击和监测的对抗是一个复杂的过程，应该考虑到有多种可能的攻击方式，监测系统也应该考虑到在攻击者通过没有部署监测系统的攻击路径进入网络中后，如何及时的发现。这就需要更多的检测技术，例如利用 AV 检测技术，来发现可能的木马控制流量、已知的隐秘信道传输等等。已知威胁检测技术是高级可持续威胁监测系统必要的组成部分，它可弥补动态检测的在效率上的不足之处，形成更完备的安全监测体系。
- **适配虚拟化平台：**提供虚拟化版本的 TAC 系统，适配主流虚拟化平台，支持快速扩容，实现高级威胁分析能力的快速交付。

4.1 体系架构

TAC 系统采用多核、虚拟化平台，通过并行虚拟环境检测及流处理方式达到更高的性能和更高的检测率。

系统共四个核心检测组件：信誉检测引擎、病毒检测引擎、静态检测引擎（包含漏洞检测及 shellcode 检测）和动态沙箱检测引擎，通过多种检测技术的并行检测，在检测已知威胁的同时，可以有效检测 0day 攻击和未知攻击，进而能够有效地监测高级可持续威胁。参见下图：

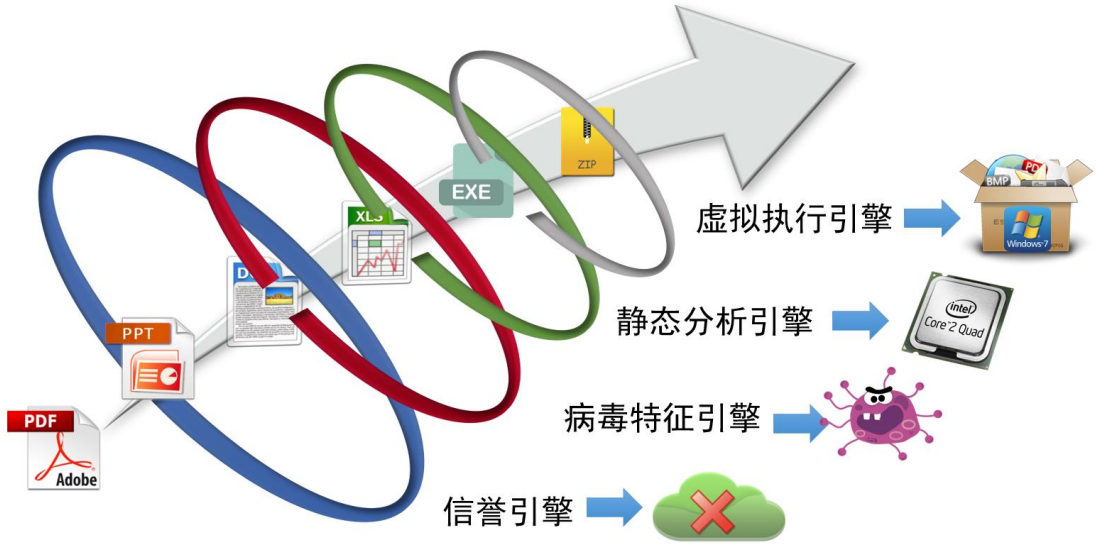

图 4.1 绿盟威胁分析系统文件处理流程

4.2 主要功能

◆ **多种应用层及文件层解码**

从高级可持续威胁的攻击路径上分析，绝大多数的攻击来自与 Web 冲浪，钓鱼邮件以及文件共享，基于此监测系统提供以上相关的应用协议的解码还原能力，具体包括：HTTP、SMTP、POP3、IMAP、FTP。

为了更精确的检测威胁，监控系统考虑到高级可持续威胁的攻击特点，对关键文件类型进行完整的文件还原解析，系统支持了以下的文件解码：

- Office 类：Word、Excel、PowerPoint…
- Adobe 类：.swf、.pdf…
- 不同的压缩格式：.zip、.rar、.gz、.tar、.7z，.bz…
- 图片类：jpg、jpeg、bmp….

◆ **独特的信誉设计**

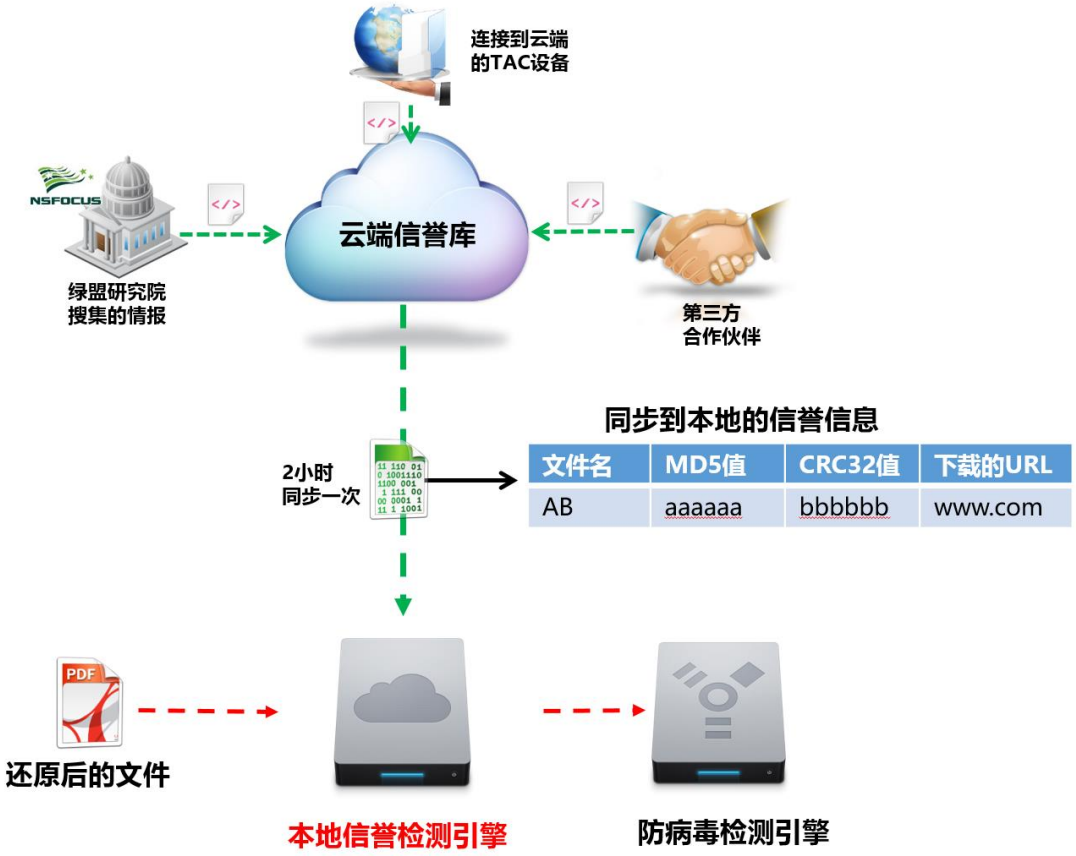

图 4.2 NSFOCUS TAC 信誉交互过程图

TAC 利用广阔的全球信誉，让检测更加高效、精准，当文件被还原出来后，首先进入信誉检测引擎，利用全球信誉库的信息进行一次检测，如果文件命中则提升在非动态环境下的检测优先级但不放到动态检测引擎中进行检测，如有需求可手动加载至动态检测引擎用以生成详细的报告。目前的信誉值主要有文件的 MD5、CRC32 值，该文件的下载 URL 地址、IP 等信息；

◆ **集成多种已知威胁检测技术：AV、基于漏洞的静态检测**

系统为更全面的检测已知、未知恶意软件，同时内置 AV 检测模块及基于漏洞的静态检测模块。

AV 模块采用启发式文件扫描技术,可对 HTTP、SMTP、POP3、FTP 等多种协议类型的百万种病毒进行查杀,包括木马、蠕虫、宏病毒、脚本病毒等,同时可对多线程并 发、深层次压缩文件等进行有效控制和查杀。

静态漏洞检测模块，不同与基于攻击特征的检测技术，它关注与攻击威胁中造成溢出等漏洞利用的特征，虽然需要基于已知的漏洞信息，但是检测精度高，并且针对利用同一漏洞的不同恶意软件，可以使用一个检测规则做到完整的覆盖，也就是说不但可以针对已知漏洞和恶意软件，对部分的未知恶意软件也有较好的检测效果。

- **智能 ShellCode 检测**

恶意攻击软件中具体的攻击功能实现是一段攻击者精心构造的可执行代码，即 ShellCode。一般是开启 Shell、下载并执行攻击程序、添加系统账户等。由于通常攻击程序中一定会包含 ShellCode，所以可以检测是否存在 ShellCode 作为监测恶意软件的依据。这种检测技术不依赖与特定的攻击样本或者漏洞利用方式，可以有效的检测已知、未知威胁。

需要注意的是由于传统的 ShellCode 检测已经被业界一些厂商使用，因此攻击者在构造 ShellCode 时，往往会使用一些变形技术来规避。主要手段就是对相应的功能字段进行编码，达到攻击客户端时，解码字段首先运行，对编码后的功能字段进行解码，然后跳到解码后的功能字段执行。这样的情况下，简单的匹配相关的攻击功能字段就无法发现相关威胁了。

系统在传统 ShellCode 检测基础上，增加了文件解码功能，通过对不同文件格式的解码，还原出攻击功能字段，从而在新的情势下，依然可以检测出已知、未知威胁。在系统中，此方式作为沙箱检测的有益补充，使系统具备更强的检测能力，提升攻击检测率。

- **动态沙箱检测（虚拟执行检测）**

动态沙箱检测，也称虚拟执行检测，它通过虚拟机技术建立多个不同的应用环境，观察程序在其中的行为，来判断是否存在攻击。这种方式可以检测已知和未知威胁，并且因为分析的是真实应用环境下的真实行为，因此可以做到极低的误报率，而较高的检测率。

图 4.3 NSFOCUS TAC 虚拟执行过程图

检测系统具备指令级的代码分析能力，可以跟踪分析指令特征以及行为特征。指令特征包括了堆、栈中的代码执行情况等，通过指令运行中的内存空间的异常变化，可以发现各种溢出攻击等漏洞利用行为，发现 0day 漏洞。 系统同时跟踪以下的行为特征，包括：

- 进程的创建中止，进程注入；
- 服务、驱动
- 注册表访问、改写
- 文件访问、改写、下载
- 程序端口监听
- 网络访问行为
- … …

系统根据以上行为特征，综合分析找到属于攻击威胁的行为特征，进而发现 0day 木马等恶意软件。

系统发现恶意软件后，会持续观察其进一步的行为，包括网络、文件、进程、注册表等等，作为报警内容的一部分输出给安全管理员，方便追查和审计。而其中恶意软件连接 C&C 服务器（命令与控制服务器）的网络特征也可以进一步被用来发现、跟踪 botnet 网络。

◆ **完备的虚拟环境**

图 4.4 NSFOCUS TAC 虚拟环境图

目前典型的 APT 攻击多是通过钓鱼邮件、诱惑性网站等方式将恶意代码传递到内网的终端上，绿盟 TAC 支持 http、pop3、smtp、imap、smb 等典型的互联网传输协议。受设备内置虚拟环境有限影响，会存在部分文件无法运行，绿盟 TAC 内置静态检测引擎，通过模拟 CPU 指令集的方式来形成轻量级的虚拟环境，以应对以上问题。

很多 APT 安全事件都是从防御较薄弱的终端用户处入手，绿盟 TAC 支持 WINXP、WIN7、安卓（即将发布）等多个终端虚拟操作系统；

◆ **多核虚拟化平台**

系统设计在一台机器上运行多个虚拟机，同时利用并行虚拟机加快执行检测任务，以达到一个可扩展的平台来处理现实世界的高速网络流量，及时、有效的进行威胁监测。

通过专门设计的虚拟机管理程序来执行威胁分析的检测策略，管理程序支持大量并行的执行环境，即包括操作系统、升级包、应用程序组合的虚拟机。每个虚拟机利用包含的环境，识别恶意软件及其关键行为特征。通过这种设计，达到了同时多并发流量、多虚拟执行环境的并行处理，提高了性能及检测率。

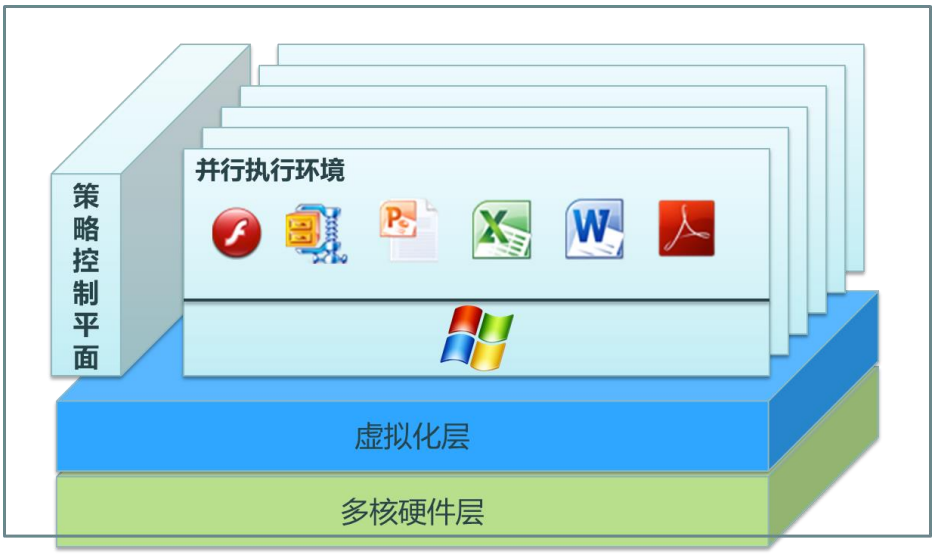

图 4.5 NSFOCUS TAC 多核平台结构图

4.3 部署场景

绿盟科技威胁分析系统产品，通常部署在互联网接入口，检测进出网络的流量，发现企图进入内网的恶意软件，以及试图往外网链接的木马。根据需求，TAC 产品有以下三种部署场景：镜像模式、邮件代理模式和联动模式。

1.1.1 镜像模式

TAC 镜像部署模式，与 IDS 相类似，可以通过交换机镜像端口，或者通过分光器 TAP 进行流量监听。

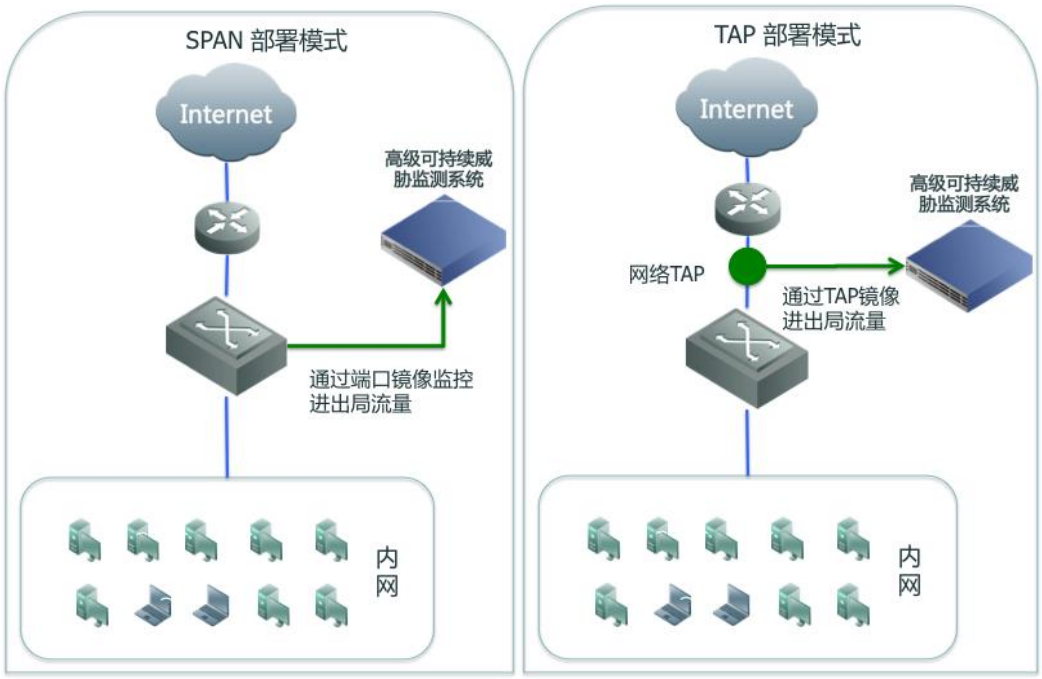

图 4.6 NSFOCUS TAC SPAN 和 TAP 部署方案

镜像模式部署，优势是 TAC 可以监听所有网络协议，进行文件还原，然后依次通过 TAC 的系列安全检测引擎进行检测。

1.1.2 邮件代理模式

TAC 邮件代理模式，部署在邮件安全网关和邮件服务器之间，监控和过滤邮件中的高级恶意软件。

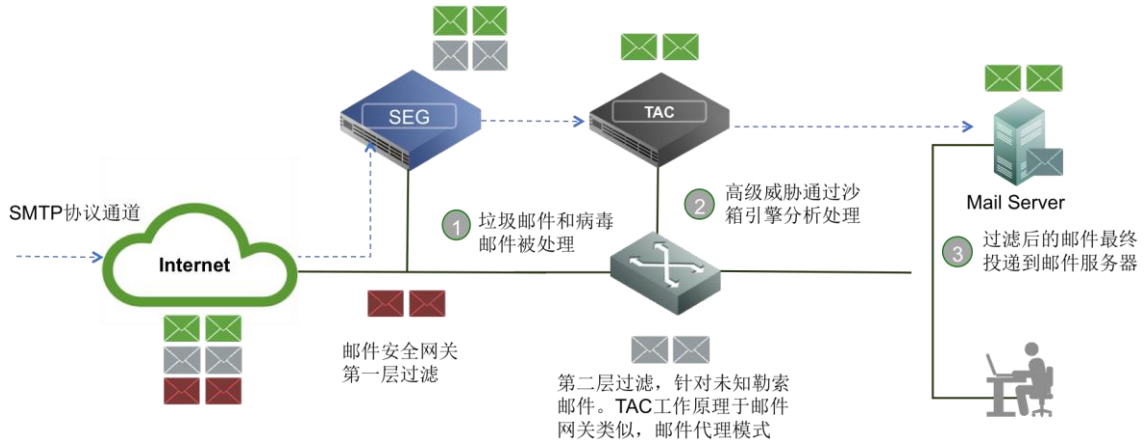

图 4.7 NSFOCUS TAC 邮件代理部署方案

TAC 邮件代理部署，直接在 SMTP 协议中，参与邮件接收和转发，再此过程中，对邮件正文的恶意 URL，文件附件进行恶意行为分析。邮件代理模式，根据策略，可以设置监控模式和阻断模式，前者只对恶意软件进行告警，后者实现告警的同时，对邮件进行隔离或者删除。

1.1.3 API 联动模式

TAC 提供开放 API，可以与网关设备（IPS / FW）一起协同防护。其原理为，网关设备提交文件到 TAC 进行安全检测，然后返回检测结果，形成本地安全信誉，实现安全阻断。借助 TAC 产品，网关设备具有了对未知威胁的感知能力。TAC 也借助网关设备，实现了安全检测与阻断的闭环。

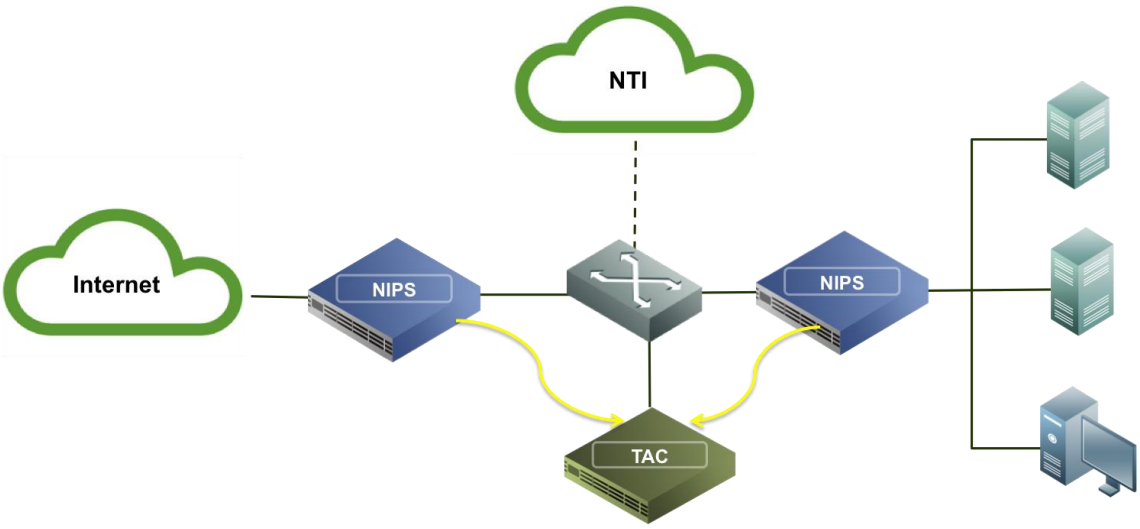

图 4.8 NSFOCUS TAC API 联动部署方案

1.1.4 虚拟化模式

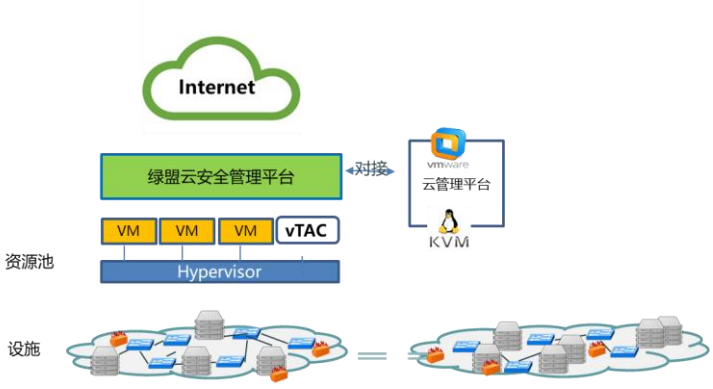

图 4.9 NSFOCUS TAC 虚拟化模式部署方案

TAC 提供虚拟化版本（vTAC），支持 KVM 及 VMWARE 平台，系统部署方便，易于扩展，可快速在用户云环境中提供高级威胁分析能力。

五. 结论

过往的安全事件早已证明，传统的安全防护手段（防病毒或者 IPS），是必不可少的安全设施，但存在不足，即基于 Signature 攻击签名的防护手段，对 APT 这种高级可持续性攻击，无能为力。分析 APT 攻击的技术特点、传统检测技术的差距，我们亟需新一代高级可持续威胁监测产品。

绿盟威胁分析系统/NSFOCUS Threat Analysis Center（TAC）提供了业界领先的未知威胁检测能力，通过新一代的威胁分析检测技术，绿盟科技的产品和技术能够有效检测通过网页、电子邮件或其他的在线文件共享方式进入网络的已知和未知的恶意软件，发现利用 0day 漏洞的 APT 攻击行为，保护客户网络免遭 0day 等攻击造成的各种风险，如敏感信息泄露、基础设施破坏等。这对于保障业务系统的运行连续性和完整性有着极为重要的意义。