HHY-P-XY2-星云技术白皮书-V1.0

让安全成为IT基础属性

南京翰海源信息技术有限公司

翰海源
VULNHUNT SECURITY

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人
2014.3.24	V1.0	第一版	马以梁

翰海源
VULNHUNT SECURITY

目录

一. 网络安全正面临重大的变革

APT 攻击，特别是具有国家和组织背景的 APT 攻击，将成为伴随信息 IT 化和网络化深入到人类生活每个领域之后，人类将要遇到的最具威胁的挑战。

APT 攻击是指融合情报、黑客技术、社会工程等各种手段，针对有价值的信息资产或通过 IT 系统控制的重要系统，发起复杂而专业的攻击。由于 IT 系统复杂性，目前还没有很好的检测措施完全发现 IT 产品中的后门、漏洞以及应用运行时的可信性，利用 IT 发起的攻击已经有很长的历史了，如美国在天然气系统中植入木马引发 1985 年前苏联西伯利亚天然气大爆炸、在海湾战争中通过打印机芯片植入定位系统指导轰炸伊拉克重要目标，都成为重要的国家级作战手段。

随着 IT 深入发展，各种行业、各个企业都不可避免越来越深入的依赖于 IT 系统。利用攻入 IT 系统窃取情报与知识产权、篡改数据获取收益、监控和获取个人隐私、控制重要系统获得战略控制或大面积破坏，已经成为国家、组织和个人可以看得到的重大利益。于是 APT 在 21 世纪开始蓬勃发展起来，除了国家级的军事政治目标外，能源、公共服务、科研、大型企业、金融、大型站点等有重要信息资产的部门，都成为 APT 指向的目标，而大量 IT 系统和应用的安全漏洞与缺陷、安全意识的薄弱和攻击技术普通人难以理解、加之缺乏恶意客户判定的标准、程序的黑盒性，为 APT 攻击提供着无穷尽的弹药和成功保证，而无须非得象以前需要通过供应链来植入木马和后门。而 IT 系统的损失难以感知的特性（信息资产的可拷贝性让很多损失者不知损失，即使感知到损失，由于缺乏关联性，受害者也不一定清楚是 IT 安全问题导致的）又让受害者一直处于在安全的假象中。APT 攻击愈演愈烈，2013 年美国国会听证会上的评估，美国因为网络攻击导致的知识产权的损失（这大部分是通过 APT 攻击来获取的）每年高达 3000 亿美金。

但是伴随着 APT 攻击造成的重大损失的同时，是传统安全检测与防御手段针对 APT 攻击的无能为力。从国家级的核设施网络到美国 NASA，从世界互联网巨头 GOOGLE 到安全公司翘楚 RSA，无一不是 APT 攻击的受害者。如果说他们的安全做的不好，那世界上又有几家能说比他们的安全做的更好呢？APT 剑指之下，没有那个部门能幸免，美国前国土安全部部长 Michael Chertoff 表示“There are two types of people: those who've been hacked and

those who don't know they've been hacked”，就是这一现实的写照。试想一下，当攻击者可以肆意进出和控制军事指挥系统、核系统、能源系统、交通指挥系统、金融系统，那么除了信息的安全，我们实体的财产与生命安全，也将变得无比脆弱。

二. 下一代网络威胁如何对抗传统安全技术

APT 攻击从渗透进内网到窃取高价值信息，是一种多阶段多维度的过程。攻击者通过混合了基于网页、邮件和文档的多种攻击技术，让 APT 攻击变得难以感知。今天我们仍在使用的 Firewall、IPS、IDS、AV、上网行为管理、DLP 都不具备相应的能力可以检测到利用了 0DAY、变形木马的 APT 攻击，存在着“未知攻，焉知防”的尴尬。

APT 攻击之所以能无往而不利，因为传统的安全技术主要是依靠静态签名或者是基于特征匹配的检测原理。

下面看看 APT 是如何对抗传统安全技术：

（1）防火墙：防火墙通常允许 HTTP 流量，下一代防火墙强调了对用户和应用程序的控制。下一代防火墙虽然包含了 IPS、AV、应用控制、流量控制等新功能，但依然使用的是传统的安全检测引擎，所以仍然无法使得防火墙具备检测 APT 攻击的能力。

（2）IDS、IPS：基于静态签名的检测、包检查、DNS 分析依然对使用 0DAY 漏洞利用技术的 APT 攻击是无感知的。

（3）反垃圾邮件：钓鱼网站经常使用动态域名和 URL，而反垃圾邮件的黑名单的更新往往是滞后，有数据显示钓鱼网站被关闭前平均能存活 26 个小时。

（4）杀毒软件和防毒墙：因为恶意程序、漏洞是未知的，网站本身有好的信誉，杀软和防毒墙不会对它们采取任何措施。

（5）上网行为管理：大多数出网过滤名单禁止的是成人和游戏网站，对其他类型网站很少限制。另外动态 URL、黑客自己建立的合法网站使得静态的 URL 过滤列表失去作用。

（6）DLP（数据防泄漏）：DLP 关心的是用户个人信息，比如密码、银行帐号等私密信息，但黑客在窃取信息后通常会做压缩和加密操作，然后再通过隐蔽信道发送出去，这些技术手段都是 DLP 的检测机制无法感知的。

三. 翰海源星云弥补现有安全体系的缺陷

APT 攻击本身具有复杂性、隐蔽性、持续性等特点，这些特点导致了现有安全防御体系在技术层面的对抗上就存在天然的缺陷，并且由于对 APT 攻击的认知不足，加剧了攻防之间的差距。

APT 攻击存在一个完整的生命周期，翰海源星云多维度预警系统（以下简称“星云”）针对其整个生命周期里必须使用的技术点进行监控，提供了 360 度的、多维度的未知威胁分析，覆盖从 0DAY 漏洞利用到敏感信息偷取，更加有效的防御 APT 攻击。

翰海源星云多维度预警系统（以下简称“星云”）是对现有安全防御体系的很好补充，弥补了传统安全设备无法检测 APT 攻击的缺陷。

3.1 技术原理

即使不考虑人的意识与管理制度的问题，只基于现有 IT 系统的脆弱性，我们也很难从 IT 基础架构上解决安全问题，现有 IT 基础没有客观技术标准定义恶意行为，加上大量很少考虑安全的 IT 产品的广泛部署和应用，注定 APT 攻击的检测与防御，其实是专业攻击团队与防御团队，是人和人，在技术、安全理解与智力的对抗。对于检测与防御者来说，短板在于必须兼顾用户的可用性易用性与习惯意识，并要在冲突时做出重大退让，而且企业 IT 环境的云化、移动化、软件定义化必然带来防御边界的模糊，攻击者进入路径过多，难以面面俱到，同时要考虑攻击者潜在可能的对抗手段以及后续带来的对方成本和检测成本。这就意味：难以期待一个万能的药方可以做到极致并全面解决问题，而建立一个纵深、立体的检测体系，才能适应这种环境的变化。

星云多维度检测体系，必须从如下角度来建立：

- 基于攻击生命周期的纵深检测体系

从攻击者发起的攻击生命周期角度，可以建立一个纵深检测体系，覆盖攻击者攻击的主要环节。这样即使一点失效和被攻击者绕过，也可以在后续的点进行补充，让攻击者很难整体逃逸检测。

- 基于信息来源的多覆盖检测

从攻击者可能采用的攻击路径的角度，可以建立一个覆盖广泛的检测体系，覆盖攻击者攻击的主要路径。这样避免存在很大的空区让攻击者绕过，同时增加信息的来源度进行检测。

◆ 基于攻击载体的多维度检测

针对每个具体攻击载体点的检测，则需要考虑多维度的深度检测机制，保证攻击者难以逃过检测。

综上所述：星云多维度威胁检测思想，就是由时间线（攻击的生命周期）、内容线（信息来源覆盖）、深度线（多维度检测），构成一个立体的网状检测体系，攻击者可能会饶过一个点或一个面的检测，但想全面地逃避掉检测，则非常困难。

3.2 主要功能

威胁检测功能

（1）多维度检测机制

从已知签名检测、无签名的深度内容检测、动态行为检测及事件关联分析等维度，对各类威胁进行深度检测并在漏洞利用、后门植入、窃密等攻击环节上形成纵深检测体系。

（2）动态行为分析

不仅让用户知道发生了真实攻击，更让用户了解攻击的危害行为。星云提供了沙盒动态行为分析引擎，实时分析恶意程序的行为，为用户展现程序读写的文件、注册表、网络通讯情况，并对其行为进行判断（正常或者恶意）。

（3）全面覆盖威胁载体

针对网络中的 URL、文档文件、可执行程序、邮件、网络通道、流量等威胁载体进行检测，全面阻击 APT 可能存在的载体。

（4）云防御

在用户授权下，利用云平台的特性，实现威胁信息和专业团队共享，在端点设备上提供协同响应能力，实现单点识别，全局防御。

（5）多种部署模式

支持网关旁路监听模式，实现在线检测和实时防御。

支持邮件网关模式，特别针对钓鱼邮件的攻击方式，从邮件层面进行专项防御。

威胁管理功能

（1）告警管理

告警信息提供了攻击事件的完整信息：攻击发生时间范围、事件名称、事件类别、所属服务、源网络范围、目的网络范围、触发探测器、攻击结果、事件动作

（2）多视图展示

提供事件视图，样本视图，攻击源视图，受害者视图等多视图展示，全方位快速展示攻击事件背后的信息。

（3）多样化的综合报表

报表系统提供了详细的综合报表，支持生成：日、周、月、季度、年度综合报表。报表支持 MS WORD、HTML、PDF 格式导出，同时支持定时通过电子邮件发送报表至系统管理员。

（4）丰富的响应方式

提供丰富的响应方式，包括：邮件报警、界面显示、日志数据库记录等，同时提供标准 syslog 接口，可接受第三方管理平台的安全事件集中监控、报告和管理。

（5）联合运维

为解决用户“设备报了警后，如何判断是真假？成千上百的警告，如何运维？”等问题，星云提出了联合运维模式。利用翰海源专家团队，在云端帮忙客户确认样本的真实危害性，大大减轻用户的运维压力。

3.3 技术优势

（1）智能协议识别和分析

采用独有的智能协议识别技术，通过动态分析网络报文中包含的协议特征，发现其所在协议，然后递交给相应的协议分析引擎进行处理，能够在完全不需要管理员参与的情况下，高速、准确地检测出通过动态端口识别出协议。

（2）基于签名特征检测

装载权威的专家知识库，提供高品质的攻击特征介绍和分析，基于高速、智能模式匹配方法，能够精确识别各种已知攻击，包括病毒、特洛伊木马等，并通过不断升级攻击特征，保证第一时间检测到攻击行为。

（3）基于漏洞特征检测

漏洞特征检测是在了解漏洞触发原理的基础上，去检测和识别该漏洞触发条件。能够通过一个漏洞特征就识别成千上万利用该漏洞的各种攻击事件。

翰海源拥有的业界权威安全漏洞研究团队代码审计实验室（Code Audit Labs），致力于分析来自于全球的各类攻击威胁，并努力找到各种漏洞的修补方案，形成解药，融于星云攻击特征库，以保持产品持续、先进的攻击防护能力。

（4）未知恶意代码检测

当前传统安全产品（如 IDS，IPS，UTM）对未知漏洞（零日攻击）/未知恶意代码无能为力，翰海源星云通过多年研究，采用基于攻击特征的无签名检测算法和基于动态行为分析的自动化恶意判断来识别未知恶意代码，对其具有出色的精确检测效果。

（5）C&C 的检测

为解决用户想知道哪些机器受攻击，更想知道哪些机器中招的需求，通过沙盒动态分析引擎动态提取恶意程序运行后的特征，例如 C&C 的检测。

这样就能区分网络中哪些机器只是受到了攻击（例如只是下载了个攻击文件，没有运行），哪些中招。用户就可以分别对待和处理哪些机器。

（6）全面检测新一代威胁恶意对象

检测恶意 URL，恶意文档文件，恶意可执行文件，恶意木马/后门网络通道，C&C，流量异常等；对通过邮件附件传播恶意代码攻击方式(此方式为定向攻击主要方式）及邮件正文中内嵌的恶意 URL 具有精确检测能力。

（7）业界领先的安全漏洞研究团队

翰海源拥有著名的安全研究部门代码审计实验室（Code Audit Labs），已经独立发现了 30 多个 Microsoft、HP、Oracle、SUN、Juniper 等国际著名厂商的重大安全漏洞，保证了星云技术的领先和规则库的及时更新，在受到攻击以前就能够提供前瞻性的保护。

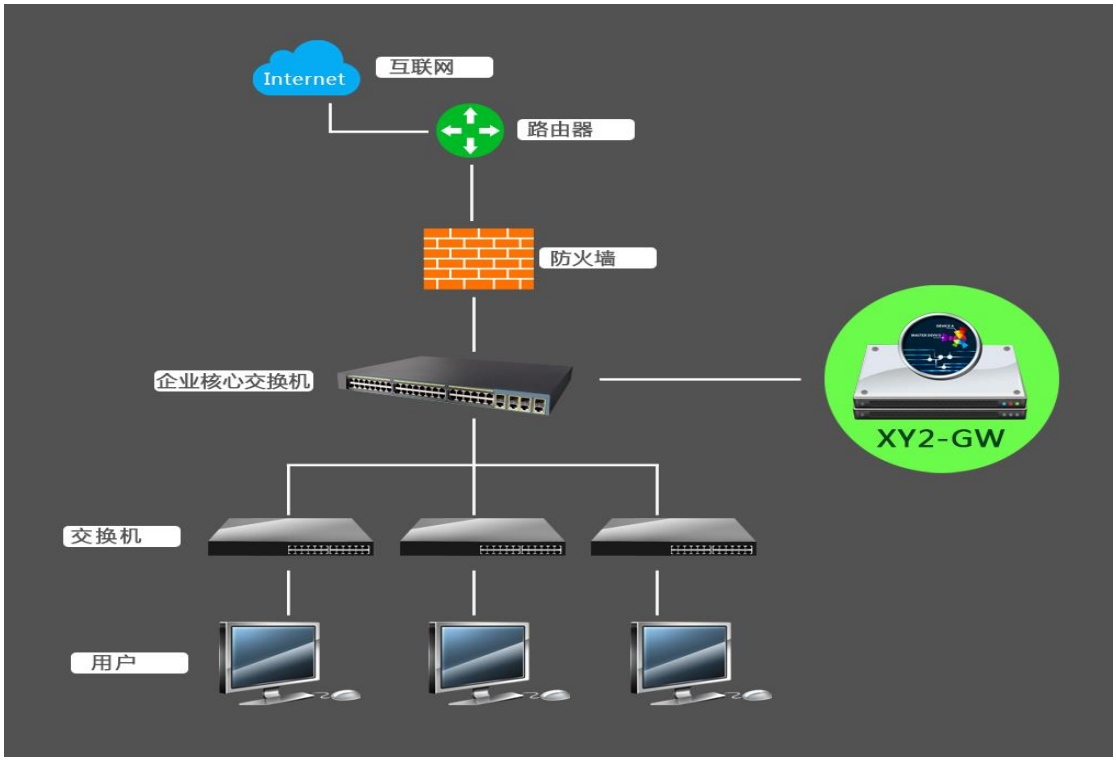
3.4 产品部署

星云支持旁路模式流量检测，在实现监控检测功能的同时，完全不需改变用户的网络环境，避免设备对用户网络造成中断的风险。在旁路模式下，星云分别支持 SPAN 和 TAP 部署方式。

3.4.1 旁路模式 SPAN 部署方式

部署方式：

核心交换机与出口路由器之间只有唯一的一条物理通路，所有内网与外网之间的数据流都要流经这条通路。将交换机数据端口的流量镜像至监控端口的星云设备。



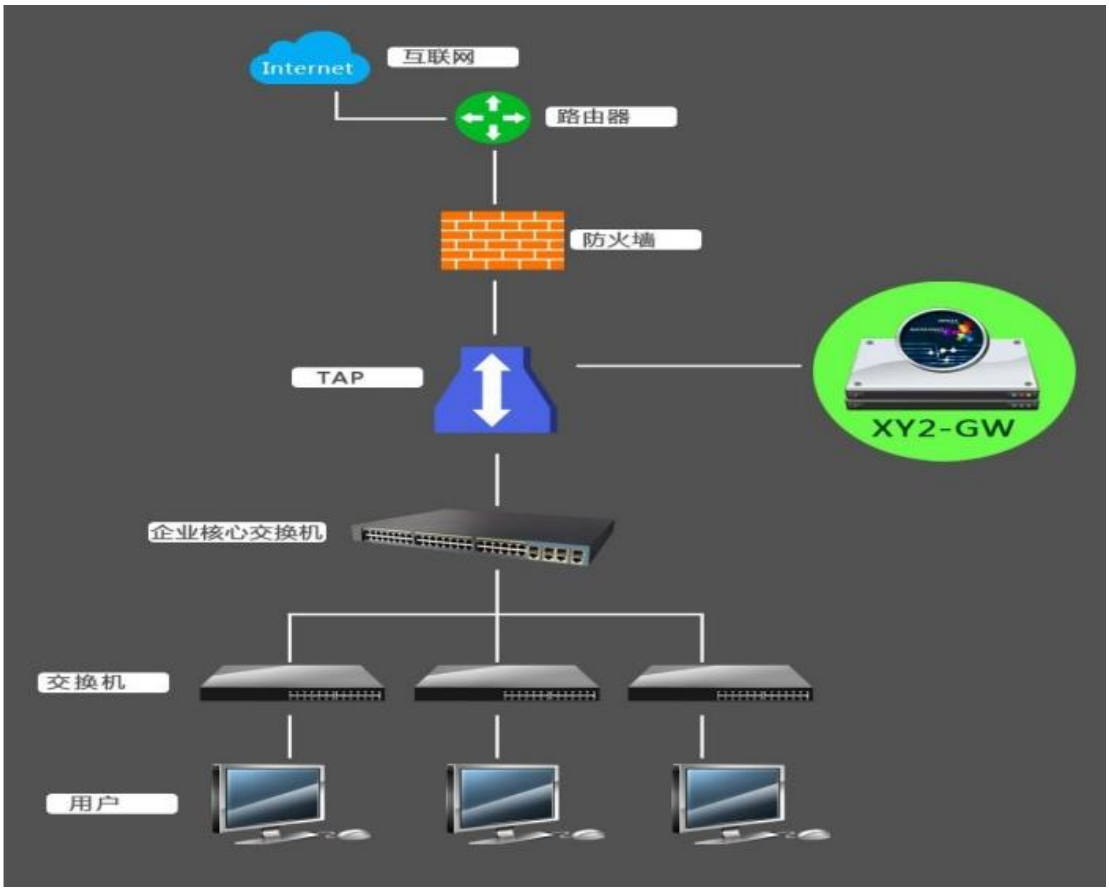
特点：

可以对网络数据进行实时监控，能够及时筛选侦测可疑网络入侵、攻击数据，尽早检测到新的和已知零日攻击，并且完全不需要改变用户的网络环境，避免设备对用户网络造成中断。

3.4.2 旁路模式 TAP 部署方式

部署方式：

TAP 部署方式即将高性能网络分流器部署在核心交换机与出口路由器之间。网络分流器对所有数据流量进行复制并均衡输出到多个星云设备。



特点：

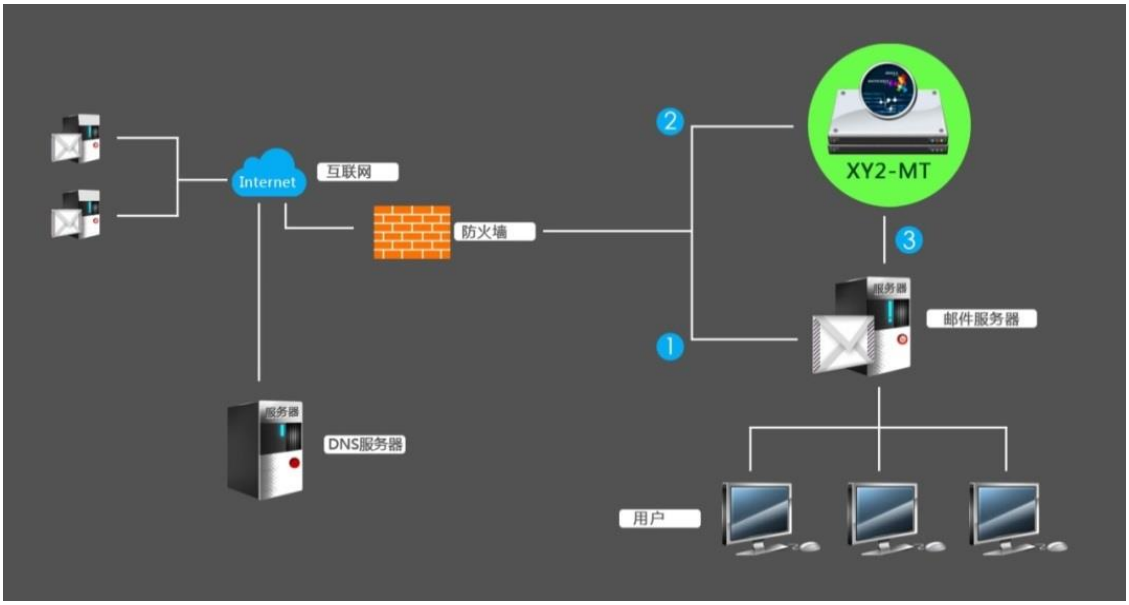
对数据流量较大的网络可以使用多台星云设备进行监控，避免因星云性能瓶颈而无法处理大流量的网络数据。

3.4.3 MT 邮件网关部署方式

星云 MT 系统将检测所有由外部发往邮件服务器的邮件的附件、展示图片及正文 URL 等信息。根据客户的邮件服务器的部署方式，星云将提供多种部署方式。主要有 2 种部署方式。

1. MX 记录优先部署方式

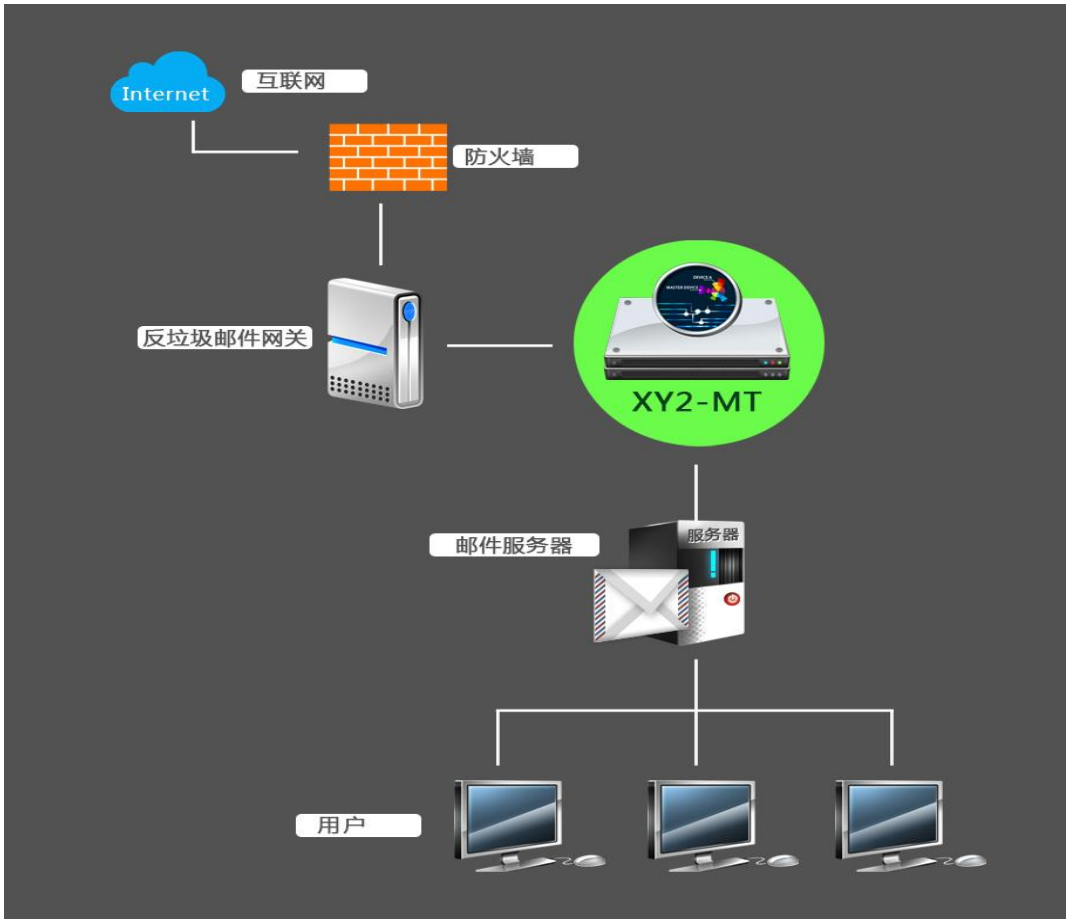
在此种部署方式中，邮件服务器直接拥有公网 IP，通过 MX 记录把域名和 IP 进行了绑定。MX 记录是 DNS 服务器上的一组数据。邮件服务器在传送信件之前，会先向 DNS 询问邮件服务器的地址。电子邮件传送简略流程如下：



在添加星云 MT 系统之后，所有的电子邮件将会先经过星云 MT 系统的扫描，再传送到后方的邮件服务器中。

2. 接管模式

在此种部署方式中，邮件服务器通过防火墙做了 SMTP 端口的端口映射。邮件服务器部署在企业内网中，不具有公网 IP。此种方法下，将星云 MT 系统与企业网络简单连接即可。



此种部署方式中，星云 MT 系统将处于原有的防护体系的最后一层。

四. 用户价值

- 全面感知 APT 攻击行为（如 0DAY 漏洞攻击、高级特马、隐蔽信道）。
- 威胁动态行为可视化，将未知恶意代码识别能力交给用户
- 第一时间确认内网中招主机，将威胁感染可控化，使用户损失降到最低。
- 统一威胁云实现大数据关联分析，提供 APT 攻击事件确认。
- 为用户提供专业的技术团队支持。

五. 联系我们

VULNHUNT

产品与服务联系热线

电话：400-086-9086

025-82211581-903/907/908

邮箱：support@vulnhunt.com

地址：南京市雨花台区雨花大道邦宁科技园 101 室