Lippis 报告

研究纪要

Lippis 报告 158

# 保护数据中心的下一代网络安全解决方案

作者：

Lippis Consulting 总裁
Nicholas John Lippis III

2010 年 10 月

# Lippis 报告 158：保护数据中心的下一代网络安全解决方案

那些能够降低成本的 IT 项目终将成为赢家，这是当前的商业/经济周期中出现的一个显著趋势。在我 25 年的 IT 行业经历中，这个节约趋势极为重要。具体而言，这个趋势正在推动数据中心整合、服务器虚拟化和移动计算项目。当企业整合数据中心并通过虚拟化使其微型化时，云计算提供商正忙于提供新的、更低成本的 IT 交付经济模型。简而言之，一个新的计算层已经出现：终端设备是移动设备，并且应用通过公司数据中心和云计算设施提供。这种同时提高便利性和工作效率的新计算模型缺乏一个重要方面：移动终端的网络安全和数据中心安全设备跟上应用需求的能力。

跟上应用需求的步伐是 IT 业务领导者面临的最具挑战性的任务之一。在这个商业周期中，不仅信息需求剧增，而且网页形式的内容已变成动态内容，单个页面请求将打开众多连接，从不同来源抽取内容，以满足用户对实时访问信息的期望。例如，单个网页请求可以在物理和虚拟基础设施上轻松产生超过 50 个网络连接，对网络速度、延迟、可靠性和安全性提出非常高的要求。对此缺少了解的人只需使用浏览器访问下列任一网站：disney.com、cnn.com、nytimes.com 等－观察其中运行的丰富内容。在显示页面时，页面会呈现视频、照片、音频和富文本等内容，所有这些内容均通过虚拟和物理基础设施抽取自数据中心交换矩阵内的不同来源。IT 领导者正在力图解决的难题包括信息需求的大规模增长和布朗运动流量，这个难题因动态内容、拥挤的数据中心和虚拟化而产生。根据 Frost & Sullivan 的统计数据，即使借助整合和虚拟化信息/应用，需求也正在迫使数据中心整体市场规模从 2009 年的 1.08 亿平方英尺扩展到 2010 年底的预计 1.17 亿平方英尺。IT 领导者遇到的难题可通过数据中心网络交换矩阵得到解决，数据中心网络交换矩阵可安全地支持数以百万计的东-西流量和北-南流量连接/会话。

客观地看待移动性趋势，Apple 在推出 ipad 的前 3 个月销售了超过 330 万部 iPad；这是所有终端设备中的最高销量。Google 每天激活 100,000 部基于 Android 的手机。思科最近推出了基于 Android 的 CIUS 商用平板电脑，它与思科的统一通信 (UC) 和视频会议系统紧密相连。每家主要的 UC 提供商都将提供类似的设备，与此同时，传统的电脑供应商也将在未来几个季度推出基于 Android 的平板电脑。iPad 和 Android 平板电脑是一个新的计算层，它们正推动用户在有线和 VPN 网络之外通过移动和无线网络访问应用。

这正是问题所在。在当今的现代 IT 世界，应用遍布多种网络，例如有线、无线、移动和远程网络，用户在这些不同的网络接入方式之间来回转换其应用访问方式，并且期望获得相同或一致的体验。安全性对于用户体验和 IT 资产保护而言至关重要。虽然 IT 安全高管已经在公司边界内加强 IT 资产的防御措施，但是连接到公司网络和数据中心的移动终端数量呈指数级增长，带来重大的安全挑战，而不幸的是，这种情况超出 IT 的控制。

移动智能手机终端的本质是将个人与业务 IT 服务相结合，从而创造独特的用户体验。这种体验的一部分包括来自大量在线目的地的信息访问，例如公共 WIFI 热点、SaaS 应用（如 Salesforce.com、workday.com、netsuite.com 等）、公司 VPN 和涉及社交网络、银行、音乐、视频、新闻、通信等方面的个人网站。因此，对于配备移动终端的每位员工来说，安全漏洞和威胁是开放式的，除非 IT 通过网络安全解决方案减少漏洞和威胁。显然，移动设备正变得无处不在，而且提供各种安全解决方案，例如 VPN 支持、丢失后擦除数据、基于云的安全服务等。但是移动设备需要一个实时运行的安全解决方案，换句话说，它需要提供不间断的保护和全面的覆盖。

例如，需要保护移动终端（从而保护公司资产），以免用户从不安全的家庭 WIFI 网络访问公司网络和遭受黑客攻击。需要保护内部应用免遭各种攻击，例如 SQL 注入/数据泄漏、请求伪造/假冒、跨站点脚本/网络钓鱼等。需要保护 SaaS 免遭未经授权的访问，防范密码重复使用风险、第 7 层攻击等。另外，需要支持与有线用户相同的移动用户报告级别，以便确保活动/审计追踪、合规以及监管和报告。简而言之，IT 需要像在公司边界内控制设备一样对移动终端进行相同级别的控制，同时又不破坏移动体验。

**移动终端策略和实施**

实时移动安全的最重要方面是策略实施，因为它将公司资产和 SaaS 访问的控制权交回 IT 的手中。策略和实施不仅可以降低将威胁从移动终端传输到公司网络的风险，还可以使移动终端成为更安全的设备，方法是提供一种像公司设备一样遵守公司策略的手段，即使移动终端是用于工作和娱乐也可以。这一点很重要，因为许多移动设备是由员工购买的，这是过去五年来一直在不断增强的一个巨大消费化趋势。IT 能够用实施的方式来管理策略，移动设备可以提供个人与业务 IT 服务。员工可以购买移动设备，但是如果他们需要访问公司 IT 网络，则终端必须遵守公司策略，并且 IT 需要采用一种手段来实施此类策略。简而言之，策略和实施使 IT 能够将公司边界扩展到移动设备周围，在 IT 资产周围创建虚拟边界。

请考虑下面的创建虚拟边界的策略和实施示例…用户可以在办公桌上访问 SaaS 应用。此流量使用关联的策略和实施穿过公司防火墙。当此用户位于公司边界之外时，他/她可以直接访问 SaaS 应用，无需公司策略或实施打开漏洞。但是，在使用移动策略和实施的情况下，此用户可以使用与位于公司边界内时提供的相同策略、实施和保护，来访问 SaaS 应用。这种情况的解决方案通常要求移动设备首先穿过公司防火墙或 IT 用来控制策略的安全云服务，然后用户才连接至 SaaS 应用。

**新的安全性能需求**

由于移动终端在公司 IT 策略和实施的控制下，这个巨大的安全漏洞现在可以得到管理和遏制。移动设备正变得无处不在，与此同时，数据中心安全设备未能跟上对信息和应用访问的巨大需求。随着更多的计算能力集中到更小的空间，流量呈指数级增长，因此安全设备需要相应地调整。请考虑网站如何呈现富媒体网页。每当用户请求某个网页时，其服务器通常需要请求 50 至 100 个不同的对象，这样做只是为了显示所请求的一个网页。现在，请考虑这样一个数据中心：它包含成千上万台服务器，每秒的请求打开 5000 个连接，每个请求产生 50 到 100 个服务器请求。服务器之间的后端东-西流量比北-南用户请求流量大一到两个数量级，两个流量的组合非常大。

**需要新的防火墙/IPS 性能指标**

从安全角度看，不仅防火墙吞吐量是一个重要的性能指标，而且“每秒连接数”正在变得更加重要。如果支持较高的“每秒连接数”，将使 IT 确信可在不延迟用户体验的情况下筛选后端服务器流量。除了每秒连接数外，另一个性能指标是每秒支持的“最大连接数”，此指标确保可以安全地提供用于呈现网页的服务器到服务器流量。吞吐量、每秒连接数和最大连接数的组合可以定义为“真正的高性能”。防火墙通常每秒可以提供几十万个连接，但是对于要求最高的数据中心来说，这个速度太慢，至少慢 2 到 3 倍。每个防火墙支持的最大同时连接数通常在几百万个左右，这个数量太小，至少小 4 到 6 倍。另外，请考虑一个更现实的吞吐量指标，而不是业界常用的一系列 UDP 数据包大小。代表流量配置文件组合的真实吞吐量性能数值是一个更好的指标，可确保引用的吞吐量就是体验的吞吐量。除了原始的安全性能外，还需要小心地管理数据中心机架空间，因为 IT 高管在整合时很快会开始用完机架空间。安全设备需要减少其占用空间，因为许多设备占用 16 到 24 个机架单元或半架空间，并且消耗更多占用空间、能源和冷却资源。我们可以期待安全设备以其 1/8 大小或 2 个机架单元高度（如果不是更小）开始实现以上性能指标。

**威胁防范**

为确保此安全基础设施以网络犯罪分子和黑客在渗透基础设施时想要达到的速度来保护 IT 资产，业界正在提供基于云的威胁防范。一些供应商已经推出基于云的安全服务，这些服务通过传感器在整个互联网和公司网络收集异常的数据、分析异常/将异常与信誉分数关联，并且当检测到新攻击的特征时，云将缓解代码/特征更新传输到公司 IPS。此过程的速度是一项竞争优势。如果安全服务每 5 分钟左右发送更新一次，将最有可能遏制网络犯罪分子发动的攻击，因为网络犯罪分子往往每小时更改 IP 地址一次以避免检测。IT 业务领导者将知道基于云的威胁防范何时变为高度可靠。正是在这个时候，供应商将开始提供“有保证的防范措施”，它包括在防范措施被渗透时对供应商进行处罚。移动设备的策略和实施创建虚拟边界，而真正的高性能使安全设备能够跟上应用需求和新的流量现实。较小的安全设备占用空间使 IT 高管可以最大限度利用数据中心空间，同时将能源和冷却资源消耗降低最低。基于云的威胁防范使安全基础设施接近实时地持续更新特征，从而缓解整个公司和虚拟边界中的威胁。简而言之，IT 业务领导者获得控制权并管理移动安全漏洞，同时快速安全地向用户提供应用，而且消耗很小的占用空间。移动、数据中心整合和虚拟化以及云计算都是强大的趋势，这些趋势基于经济效益和不断增加的信息需求。要从这些投资中获得最大价值，需要采用新的安全模型。