ARBOR NETWORKS
The Security Division of NETSCOUT

货真价实的 DDoS保护方案

更有效, 更实惠的适合中小企业的解决方案

该是认真对待网络犯罪**的时候**了

尽管标题内容很吸引人，但绝不只是大企业和政府才是网络犯罪的受害者。网络犯罪对中小型企业(SMEs)也是垂涎欲滴 - 而且网络犯罪集团和个人也正在把他们的罪恶之手越来越多地伸向中小型企业。

网络攻击者了解大多数中小型企业不会像大企业集团那样会花巨资为他们的计算机网络提供强有力的保护，导致这种局面的原因有缺少技术，资金支持，和合格的人才配置。不过现在欣欣向荣的很多中小型企业基本上属于创新型企业或者是在某一领域有突出特长的个性化企业，因此他们的客户数据和知识产权都极具价值。黑客也希望通过攻击和进入中小型企业的供应链来获取与中小型企业的客户和供应商相关的更大和更有价值的目标。

此外，为客户或合作伙伴提供产品和服务时，越来越依赖于各种基于网络的应用也增加了遭受分布式拒绝服务攻击的风险。尤其是这种攻击的成本和技术难度都非常低，因此，这些攻击背后的动机非常分散 – 包括勒索，抗议公司作为和政策，甚至不满意公司的顾客或离职前员工的报复。

现在，由于几乎不需要专门的知识和零成本，任何一个心怀怨恨的人都可能发起攻击 - 他们的攻击有可能导致企业成长受挫，或者最坏的情况下，让企业倒闭。

对中小型企业来说，网络安全问题更具有紧迫性，这是由旨在保护顾客资料和数据的欧洲法案的性质决定的。欧洲新的通用数据保护条例将于2018年实施，根据这一条例的规定，如果有企业因为自身的安全漏洞导致他们的顾客数据和资料被泄漏或被窃取，则必须缴纳2千万欧元或者它们年度营业额的4%，以更大者为准，作为罚金。

中小型企业需要更好的DDoS保护方案，因为你不能指望你的运营商(ISP)给你提供有效的保护。

“有多达三分之二的小企业在过去两年里成为网络犯罪的受害者。”
英国小企业联合会[1]

[1] “网络弹性: 如何保护数字经济时代的小企业”，英国小企业联合会，2016年6月

负担得起的企业保护解决方案

Arbor Networks® 推出的可用性保护系统(APS)是基于预置安全解决方案的一个系统，主要通过保持网络边界的安全来维护企业各种系统和业务的连续性和可用性，并免受日益增多的DDoS攻击和其他高级威胁的侵犯。

为了能满足大企业的条件苛刻的安全防范需要，在原创开发的基础上，Arbor为它的APS2600应用集群推出了新的100M具有许可证的选项。这样，就保证了中小型企业可以享受到顶级的预置型保护，同时该选项方案的价格非常实惠，让大多数中小型企业也能负担得起，同时，该方案赖以存在的平台也非常容易配置。

它融合了复杂的攻击检测和缓解技术，能对各种网络行为实施全面的监控并实现快速修复和专家级别的阻断，因此，在各种攻击影响到各种关键应用和业务前自动让这些攻击无效。

它同样有能力扩展用户的保护范围，只要使用云信令与基于云的DDoS业务联系起来即可。之后，它会自动向上游的服务提供商发出警报，比如顾客的运营商或 Arbor云，当更大的攻击威胁到网络的可用性时，确保能在更短的时间内消除这种攻击威胁。

选择APS 2600的**五大理由**

1) 经济实惠
中小型企业使用的很多DDoS防护产品要么是其他产品的附加配置，要么省去了其他的关键功能，就是为了降低成本，让中小型企业有能力购买。

有了Arbor APS 2600，用户可以享受到企业级别的安全防护，而不会有任何功能上的阉割。100M版本的价格可以低到17,995美元，这样中小型企业有能力配置它们一直希望拥有的解决方案 – 它们也确实是中小型企业所必需的。

2) 简单
如果用户的技术能力有限，则APS 2600可称得上是用户的最佳选择。任何企业都可以配置这样一套解决方案。它的即插即用设计意味着使用缺省设置参数就可以很快地完成系统的安装。

这样用户就可以即时地为自己的企业提供保护 – 即使此时正在遭受攻击。不过，以后用户可以轻松地根据自己的企业需要对系统进行调整以便匹配企业的实际需要。

简单的设计和用户界面已经赢得了业界的认可，包括在2016年的信息安全产品指南大会上获得的年度“最佳安全防护硬件”金奖。

“Arbor APS推出的即开即用的，并且已经通过证明的攻击识别和消解解决方案几乎不用配置就可使用，即使安装期间正在遭受攻击。”
2016 信息安全产品指南大会

3) 有效
除了经济实惠和可用性外，APS2600还整合了各种企业级别的工具，这些工具有能力在各种TCP状态耗尽和应用层级的攻击影响到用户的网络和服务可用性前消弭掉这些攻击。因此，用户可以享受到与世界上最大的企业一样的保护待遇，因为系统最初开发时就是以服务世界上最大的企业为宗旨的。

特别是，它会源源不断地收到Arbor的ATLAS智能聚合系统提供的最新的威胁信息。由于发现了新的攻击动态，关于攻击的信息会自动发送给所有的Arbor产品，让这些产品了解新的威胁以便能及时阻断和消弭最新的各类攻击或高级威胁 – 在用户企业被侵害前。

没有其他方案能做到这一点!

选择APS 2600的**五大理由**

4) 可扩展

APS 2600针对中小企业推出的版本是我们最小的设备，不过它依旧有能力处理多达100兆比特每秒的已经检测到的在线吞吐量能力。

不过，如果是可负担得起的月度订阅用户，它还是能无缝地与Arbor的基于云的DDoS服务对接。之后这将自动地快速防范巨量的DDoS攻击(这些攻击由于体量过于巨大以至于无法通过预置形式加以消除)，因此不会影响到对用户的各种应用和服务的访问。

这使得用户可以处理各种规模的攻击，不会让用户的现在防护措施被攻击所压制，而且不用等待用户自己的安全解决方案供应商手动启动其他的基于云的防护措施。

“混合解决方案是处理各种巨量的应用层级攻击的唯一有效方法。”

弗若斯特沙利文咨询公司[2]

这种方法是最佳的行业做法。为了阻止最新的DDoS和各种高级威胁，行业分析师推荐了一种综合的，多层级的方法，旨在以更快，更智能的方式检测和阻止各种攻击并对这些攻击做出响应。

5）综合

了解DDoS检测和DDoS保护解决方案之间的差异具有非常重要的意义。一些技术，尤其以防火墙附加配置出售的那些技术方案，其设计的目的仅仅是在企业成为DDoS攻击的目标后用于检测可能出现的攻击，却不具备保护或消除攻击的功能。

通过全面的比对，Arbor提供的防护产品和服务完全融合了云端和本地防护功能，并且一直得到全球威胁情报的支撑。

行业中还没有另外一家公司能提供这样全面的DDoS保护方案，这也是Arbor成为运营商，企业和无线市场上DDoS防护装备的第一供应商的理由[3]。

通过为用户的数据保护需要提供全面的解决方案，我们实现了为用户企业的网络安全承担全面责任的目的 – 因此，用户无需浪费时间去管理各种关系，而且责任非常明确，再无需在出现问题时“诿过于人”。

用户同样可以有机会使用迄今为止最高等级的专业技术。Arbor 安全工程和响应团队(ASERT)是具有全球声誉的由安全工程师和研发人员组成的团队，专门从事全天候的互联网威胁监控工作。由于ASERT的存在，各个单位能获得所需的专业服务来加强他们的业已疲惫不堪的安全响应团队的力量并对用户的整个网络基础架构实现优化。

是采取行动**的时候**了

由于DDoS攻击的体量和复杂程度越来越呈现上升趋势，所有的企业几乎不可避免地要受到攻击 – 攻击将会给用户的盈利，顾客关系，声誉和企业成长带来巨大的危害并造成严重的后果。

APS 2600为用户提供了企业级别的保护，而价格却是中小企业能负担得起，因此你真的不想在自己的经济承受能力内拥有这样一套系统?

[2] “解密日益红火的DDoS攻击阻断市场”，弗若斯特沙利文咨询公司，2014年8月。
[3] “DDoS防护设备: 半年度市场跟踪系统”。 IHS Infonetics，2016年6月

ARBOR NETWORKS
The Security Division of NETSCOUT

关于ARBOR网络

Arbor Networks，NETSCOUT的网络业务部门，让世界上最大的企业和服务提供商网络免受DDoS攻击和高级威胁的侵扰。根据Infonetics Research的报告，Arbor是全球领先的DDoS防护装备和服务的供应商，其产品和服务主要针对企业，运营商和无线市场。Arbor Networks Spectrum™的高级威胁解决方案利用抓包和NetFlow技术能对整个网络实现无死角的监控，从而能快速检测到各种攻击活动，恶意软件和恶意内幕人并予以阻断。Arbor力争成为“力量倍增器,” 让网络和安全团队更加专业。我们的目标是为网络提供更丰富的场景和更加安全的环境，使得顾客能更快地解决他们的问题并降低他们企业的风险。

欲了解更多的关于Arbor产品和服务的信息，请登录我们的网站arbornetworks.com或关注我们的推特Twitter @ArborNetworks.