解决方案简介

电信

DDoS 防护

F5 BIG-IP AFM VE 和英特尔® FPGA PAC N3000 助力在云环境中实现大容量 DDoS 防护

帮助服务提供商和企业自动应对 5G 网络威胁

迁移至 5G 基础设施可能增加遭遇新型 DDoS 攻击的风险，而且这些攻击的规模、严重性和复杂性都将增加。构建 5G 基础设施的服务提供商必须制定相应的策略，以减少攻击对带宽和用户的影响。

幸运的是，使用更多虚拟化技术可以帮助服务提供商更快速、更大规模地降低 DDoS 攻击的影响力和有效性。集成英特尔® FPGA 可编程加速卡（PAC）N3000 的 F5 BIG-IP 高级防火墙管理器智能虚拟版（AFM VE）是一个很好的选择。相比当前的方法，通过将该解决方案与使用现成商用（COTS）服务器的虚拟化 5G 基础设施相结合，服务提供商网络可以自动检测并更快地抵御不断演变的容量耗尽型 DDoS 攻击，防止这些攻击影响用户对应用和其他服务的访问。

除了服务提供商，正在进行数字化转型的企业也需要应对这些新型 DDoS 攻击。本文介绍的解决方案可以为他们提供相同的保护。

该解决方案现已投产并上市，许多 1 级服务器 OEM 正在自己的服务器产品上验证。点击此处获得已验证服务器产品的列表。英特尔 FPGA PAC N3000 可进行动态配置，以加速多个工作负载，如 5G vRAN、Open vSwitch、分段路由 v6、Tungsten Fabric、5G 用户平面功能（UPF）、vBNG 和安全解决方案。服务提供商可以部署采用英特尔 FPGA PAC N3000 的服务器，根据边缘的服务需求支持多个云原生网络功能或虚拟设备。

具有破坏性的复杂 DDoS 攻击难以防御

虽然 DDoS 攻击的目的各有不同，如报复、反对、窃取、勒索或恶作剧，但它们有一个共同的结果：破坏服务的可用性，严重影响企业的日常运营。

根据技术水平的高低，他们可能使用现成的 DDoS 工具或发起定制化的复杂的攻击。一般而言，此类攻击由 4 种类型组成：

- **容量耗尽型：**泛滥式攻击（通常使用僵尸网络），可能发生在第 3、4 或 7 层
- **非对称型：**引起超时或会话状态改变
- **计算型：**消耗 CPU 和内存
- **基于漏洞型：**利用应用软件漏洞

最具破坏性的 DDoS 攻击通常将容量耗尽型攻击和针对具体应用的攻击混合在一起，以转移注意力，使真正的目标难以被评估。这种复杂攻击很难防御，而且通常预示着更高级、更长久的威胁将来临。

只有快速发现与阻止攻击，服务提供商才能提供更高的服务连续性，确保用户满意度不受影响。借助 F5 BIG-IP AFM 智能 VE，服务提供商可以提供全面的高性能第 3–7 层 DDoS 软件防护解决方案。这款高性能、状态化、全代理网络安全内部解决方案还可以与 F5 Silverline 云 DDoS 清洗服务相结合，以抵御网络、应用和容量耗尽型攻击，防止其通过最常见的协议进入网络。

攻击测试结果

在 F5 执行的测试中，相比 COTS 服务器中的软件，与英特尔® FPGA PAC N3000 相集成的 BIG-IP AFM 虚拟版（VE）能够抵御攻击力度高出 70 倍的 DDoS 攻击（TCP RST flood 攻击）。解决方案检测并拦截了“恶意”流量，同时让“正常”流量通过。[1]

配置详情请参见脚注 1。有关性能及性能指标评测结果的更完整信息，请访问：www.intel.cn/content/www/cn/zh/benchmarks/benchmark.html

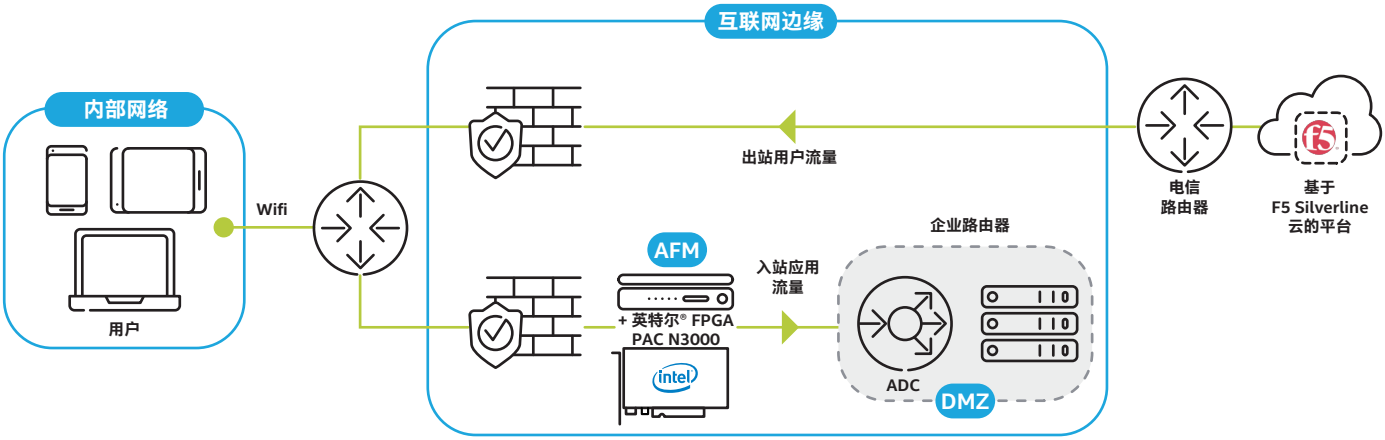

图 1. F5 解决方案能够帮助服务提供商防御复杂的 DDoS 攻击。

内部平台可以将 F5 专用软件和云清洗服务（F5 Silverline DDoS Protection）相结合，以提供主动和被动的混合 DDoS 防护。通过将攻击从数据中心迁移至基于云的防范机制，这些解决方案能够确保服务的始终可用性。

F5 与英特尔携手将采用 AFM 智能 VE 的英特尔® FPGA PAC N3000 集成至现成的商用（COTS）服务器。通过将 DDOS 特定功能从 CPU 卸载至 SmartNIC FPGA，释放 CPU 资源并按照既定方式运行。用户可以对 FPGA 进行编程，以快速执行不同的任务。在未来版本的 F5 软件中，企业可以在 FPGA 中加速更多卸载功能，从而使系统灵活适应各种高性能用例。

专用软件与英特尔 FPGA PAC N3000 完美结合，BIG-IP Smart AFM VE 可为服务提供商和企业提供出色的 NFV 防火墙/DDoS 防护，确保数据中心内虚拟或基于软件的架构的安全性。该组合也可以为专用定制硬件提供相同的功能，帮助保护其服务与应用。

通过应用网络威胁情报和机器学习以及基于数据包的分析，该解决方案可以更高效、更大规模地拦截网络攻击，同时最大限度缩短计算周期，提高解决方案的 CPU 效率，降低总体拥有成本。该解决方案还可以更新黑白名单（在 SmartNIC 中实现），以便及时应对不断演变的威胁态势。

服务提供商可使用该解决方案将 DDoS 防护部署于更靠近边缘的新领域，从而监控当今技术难以发现的网络威胁与攻击。该解决方案具备出色的可视性和自动化功能，可帮助企业轻松地阻止威胁对网络的破坏，并显著降低总体拥有成本。

面向云和 5G 的 DDoS 防御

BIG-IP AFM SMART VE 能够在云环境中提供无与伦比的 DDoS 防御功能，帮助服务提供商更加轻松和自信地构建 5G 架构，进而：

- 提高服务可用性，降低延迟
- 加快从硬件到软件的迁移，同时不牺牲性能
- 提高可扩展性和 CPU 效率，从而降低运营成本，同时避免系统中断造成的收入损失

了解详细信息

有关英特尔 FPGA PAC N3000 的更多信息，请访问：**www.intel.cn/content/www/cn/zh/programmable/products/boards_and_kits/dev-kits/altera/intel-fpga-pac-n3000/overview.html**

联系 F5 安全专家 ›

关于 F5

F5（纳斯达克：FFIV）为应用提供从开发到整个生命周期的全方位支持，以便我们的客户（企业、服务提供商、政府和消费者品牌）交付差异化、高性能且安全的数字体验。如欲了解更多信息，请访问 f5.com。您还可以在 Twitter 上关注 @F5Networks 或在 LinkedIn 和 Facebook 上访问我们，以了解更多关于 F5 及其合作伙伴与技术的信息。

F5 Networks, Inc.
801 5th Avenue
Seattle, WA 98014
888-882-4447
f5.com

1. 基于 F5 内部测试，使用 Ixia 流量生成器模拟 “正常” 和 “恶意” 流量（TCP RST flood 攻击），比较了启用英特尔® FPGA PAC N3000 DDoS 防护以及仅在软件中运行 BIG-IP AFM VE 防火墙的结果。测试配置：Dell PowerEdge R740；CPU：英特尔® 至强® 银牌 4109T CPU @ 2.00 GHz（8 个内核/16 个线程）；KVM 版本：1.5.0.；基本操作系统：CentOS Linux 版本 7.4.1708（Core），1 x 英特尔® PAC N3000 SmartNIC；防火墙软件：BIG-IP 高级防火墙管理器虚拟版（VE）v15.1.0.4（Alpha 版本）。流量生成配置：恶意流量：Ixia IxExplorer IxOS 8.5.1700.5 EA.lnk.；正常流量：Ixia XT80-V2。

英特尔® 技术的特性和优势取决于系统配置，可能需要激活支持的硬件、软件或服务。性能会因系统配置的不同而有差异。没有任何产品或组件能保证绝对安全。如欲了解有关性能及性能指标评测结果的更完整信息，请访问：www.intel.cn/content/www/cn/zh/benchmarks/benchmark.html

在性能测试过程中使用的软件及工作负载可能仅针对英特尔微处理器进行了性能优化。性能测试（如 SYSmark 和 MobileMark）使用特定的计算机系统、组件、软件、操作和功能进行测量。上述任何要素的变动都有可能导致测试结果的变化。请参考其他信息及性能测试（包括结合其他产品使用时的运行性能）以对目标产品进行全面评估。更多完整信息请访问：https://www.intel.cn/content/www/cn/zh/benchmarks/benchmark.html

性能结果基于截至配置中所示日期的测试，可能并不反映所有公开发布的安全更新。请查看备用页，了解配置详情。没有任何产品或组件能保证绝对安全。结果经过估算或模拟得出。您的成本或结果可能有所差异。英特尔技术可能需要支持的硬件、软件或服务激活。

© 2020 英特尔公司版权所有。英特尔、英特尔标识和其他英特尔标志是英特尔公司在美国和/或其他国家的商标。* 其他的名称和品牌可能是其他所有者的资产。

0220/YR/CMD/PDF