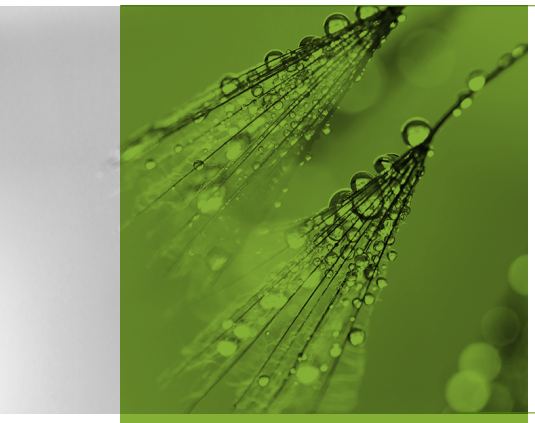

corero

瞻博网络和 CORERO：与时俱进的大规模 DDOS 防御方案

用更低的成本实时检测和缓解 DDoS 容量耗尽攻击

挑战

DDoS 攻击是当今威胁态势的重要组成部分，攻击的规模、频率和复杂度还在不断提升。利用传统的带外清洗中心和人工干预方法来解决这一不断增长的问题目前已不再可行。

解决方案

瞻博网络和 Corero 针对 DDoS 攻击开发了一种革命性的全新防御方法，通过利用不间断的数据包级监控、自动化机器分析以及基于基础架构的网络边缘实施，大规模实现实时的线速检测和缓解。

优势

- 通过在网络边缘去除恶意流量，降低 DDoS 缓解成本
- 自动化响应，在几秒内阻止 DDoS 攻击
- 利用不间断的数据包级监控提高可见性，在攻击之前、期间或之后提供详细、切实可行的的情报
- 将防护容量扩大到每秒数十 TB

自互联网问世以来，不怀好意的人就开始将分布式拒绝服务 (DDoS) 攻击作为一种抗议形式，用以制造恶作剧、破坏竞争对手以及报复那些被认为是做了坏事的人。DDoS 攻击以压倒性数量的流量淹没众多网站、网络以及云端，导致中断和服务停止，拒绝那些在日常生活的方方面面依赖服务提供商和企业网络的合法用户访问。据估算，DDoS 攻击给企业造成的平均成本在 2017 年上升到 250 多万美元[1]。

挑战

如今，几乎任何人花费不到 100 美元，就可以轻松发起一场造成严重后果的分布式拒绝服务 (DDoS) 攻击 — 不需要任何代码经验。

出租服务的出现，无论是在技术能力方面还是成本方面，都让犯罪分子执行这些攻击的门槛大大降低。随着物联网 (IoT) 的兴起，互联设备因为规模大且缺少基本的内建安全性，已成为黑客最喜欢的攻击目标。在 2016 年，Mirai 物联网僵尸网络在全球就破坏了近 100,000 台互联设备；这些设备被用来对域名系统 (DNS) 服务提供商 Dyn 发起 DDoS 攻击，其峰值容量为每秒 1.2 兆兆位 (Tbps)，从而造成四小时以上的服务中断和停机。Mirai 只是个开始，从那以后，JenX、Hajime、Satori 和 Reaper 等变种相继出现，并变得越来越复杂，越来越难以防御。

DDoS 租用服务越来越多，不受保护的物联网设备激增至数十亿，导致 DDoS 攻击数量大量增加。根据 Corero 最新的 DDoS 趋势和分析报告，在 2017 年第三季度，组织每个月平均遇到 237 次 DDoS 攻击尝试，相比上一个季度增加了 35%，相当于每天遇到 8 次攻击尝试。在采用 5G 移动网络后，可用带宽的增加会提供一个更强大的管道，这有利于遭到入侵的互联设备生成攻击流量，只会使问题变得雪上加霜。

[1] https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

随着 DDoS 攻击的频率、规模和复杂度不断提升，带外清洗中心和人工干预等传统防御措施已变得严重不足，并且成本高昂。发生大规模容量耗尽攻击时，将可疑流量重定向到清洗中心会增加延迟并带来巨大的财务负担，因为缓解成本与数据流量的大小直接相关。这种传统方法还需要人工分析和人为干预，这让修复过程的延迟和成本进一步增加。使用这些方法，从检测到缓解可能需要耗时 30 分钟 — 这在 DDoS 攻击几分钟内就能够使网站瘫痪的时代是不可接受的。

在这个需要不间断服务的世界，停机对任何企业而言都问题重大，服务提供商和企业必须严肃地重新审查其现有的 DDoS 保护策略，考虑采用能够以更低成本提供更快、更有效保护的新技术。IP 网络应该是解决方案的主要部分，它作为抵御容量耗尽攻击的第一道防线，而遥测、机器分析和网络编程能力能够使检测和缓解流程更加智能、自动化、有更强的适应能力。

瞻博网络和 Corero DDoS 防御解决方案

瞻博网络和 Corero Network Security 合作开发了一种用于 DDoS 防御的联合解决方案，通过在网络中的战略位置实施快速识别、精确决策、自动化缓解，结合持续监控功能，打造一个自愈型的网络（图 1）。

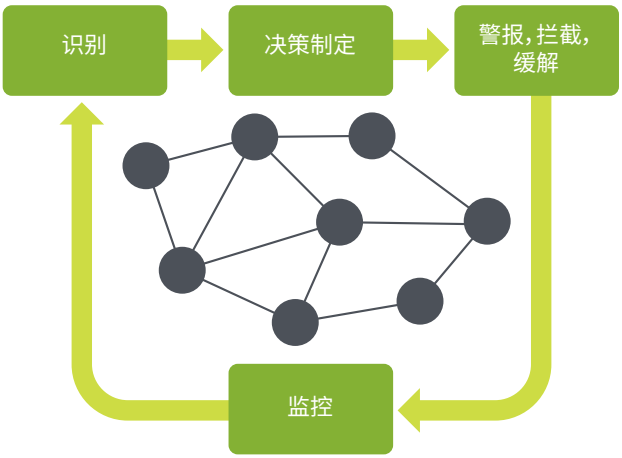

图 1：自愈网络

有效 DDoS 防御的最佳实践就是尽可能在接近源头的地方挫败攻击 — 通常就是在网络边缘。因此，三大常见的 DDoS 缓解位置就是服务提供商对等点、数据中心边缘以及用户边缘。

瞻博网络和 Corero Network Security 的 DDoS 联合解决方案是高效、自动化的解决方案，相比其它任何可用的 DDoS 解决方案，它能够以更低的成本扩展到数 TB 级的容量。它在网络的边缘发挥作用，采用以下技术来检测和缓解 DDoS 攻击（参见图 2）：

- 瞻博网络® MX 系列 5G 通用路由平台部署在网络边缘，可通过取样镜像来监视包括标头和有效负载在内的入口流量，可随着攻击动态扩展，根据威胁规模灵活调整。
- MX 系列路由器将取样镜像转发给 Corero SmartWall Threat Defense Director (TDD)，后者会检查送来的每一个数据包，结合使用基于规则的分析和机器分析，快速准确地检测到任何 DDoS 攻击流量。
- 在几秒内，TDD 就会识别到任何攻击，自动生成灵活的防火墙匹配过滤器，通过 MX 系列路由器缓解攻击。
- TDD 通过网络配置协议 (NETCONF) 自动配置 MX 系列路由器，从而安装一个可应用过滤器的短暂配置，在最接近破坏性流量源头的入口点拦截 DDoS 数据包。与此同时，允许重要的健康流量流向预期的目的地，不会降低任何转发性能。
- MX 系列路由器上的流遥测功能会将允许的/拦截的流量统计转发到 Corero SmartWall TDD。
- SmartWall TDD SecureWatch Analytics 可提供针对攻击之前、期间和之后的网络流量的全面可见性。这款由 Splunk 提供支持的应用程序能够为运维团队提供攻击汇总以及有关缓解流程有效性的其它详细、切实可行的情报。

此过程会在攻击的生命周期内持续进行，直到镜像的取样表明入口点不再受到攻击，此时 SmartWall TDD 会在 MX 系列路由器上去除过滤器，恢复正常运维。镜像的取样以及流遥测会继续从 MX 系列路由器流向 Corero 的 TDD，确保在通信流量恢复正常的同时监控下一次攻击。

这种运维模式是完全自动化的，确保企业运维完全受到保护，始终为运维团队提供可见性。

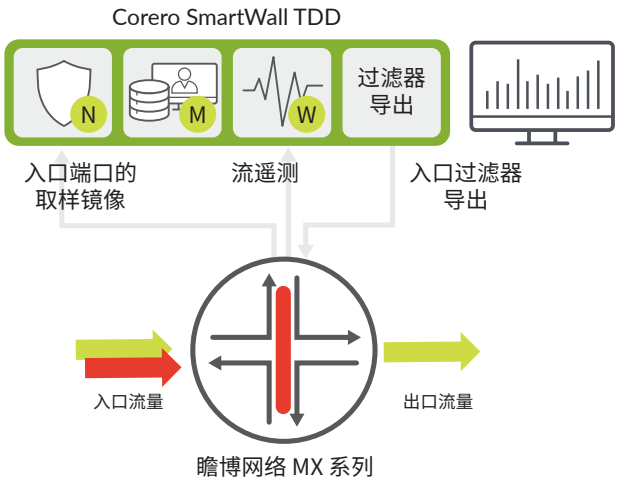

图 2：瞻博网络 + Corero DDoS 防御联合解决方案

功能与优势

瞻博网络和 Corero 的这种联合 DDoS 防御将数据包级别的流量检查优势与基于基础架构的强大实施相结合，能够以空前的数十 TB 规模对 DDoS 攻击实现实时、自动的缓解，同时成本得到显著降低。

降低 DDoS 缓解的成本

通过利用 MX 系列 5G 通用路由平台中现有的过滤功能，能够以分散的方式在网络边缘去除恶意流量。这种方法不会将所有受攻击的流量重定向到带外集中的清洗中心，也不会增加延迟和费用，从而能够帮助服务提供商和企业大大降低与此类流量相关的 DDoS 缓解服务成本，同时避免昂贵的容量升级。此外，超过 95% 的联合防御都是完全自动化的，无需任何运维人员或分析师的干预。相比依赖传统、人工密集方法的解决方案，这种方法可显著降低总拥有成本。

更快的响应和更好的客户体验

自动化意味着 DDoS 攻击能够在几秒内被识别和拦截 — 与严重依赖人工干预、需要 30 分钟或更长时间的传统方法相比，这是一个相当大的改进。速度很关键，通过选择性地只拦截攻击数据包，让合法流量继续传输，瞻博网络和 Corero 的联合解决方案可确保客户的业务即使在攻击高峰期也不受影响。

可见性、资源效率以及缓解有效性得到提升

瞻博网络和 Corero 的联合解决方案实现了数据包级别的不间断监控。与传统基于流的检测方法相比，基于数据包的检测可提高有效性，让运维人员不仅能够看到标头信息，还能够更清楚地看到有效负载数据。此外，与 IP 流信息导出 (IPFIX) 协议相比，取样镜像给路由器资源造成的负荷非常轻，因为路由器不必聚合和处理大量数据。最后，该联合解决方案不需要推倒重建；它通过一个分层的 DDoS 防御模式与现有解决方案无缝结合，其中网络周边的 IP 边缘路由器是第一道防线，卸载容量耗尽攻击流量以及使用集中的清洗资源来处理更加复杂的应用程序层攻击。

数十 TB 的可扩展性

Corero SmartWall TDD 可扩展到 40 Tbps 的线速缓解容量，无需在网络中回传 DDoS 流量。通过结合 MX 系列 5G 系列通用路由平台及其可扩展到 80 Tbps 数据包转发的能力，该联合解决方案可在目前市场上可用的单一 DDoS 缓解系统中提供出色的可扩展性。

解决方案组件

Corero SmartWall Threat Defense Director

Corero SmartWall TDD 代表了实时容量耗尽攻击 DDoS 防御技术的突破，提供了以下功能：

- 可扩展到数十 TB 的容量耗尽攻击的监控和缓解
- 数据包级检查可准确检测容量耗尽攻击 DDoS
- 通过机器分析执行自动过滤，实现智能缓解
- 实时响应，缓解时间缩短为几秒
- 闭环反馈可避免误报
- 数秒、数分钟、数天、数周、数月和数年的详细日志解析
- 允许的流量和拦截流量的数据包取样取证
- 由 Splunk 提供支持的分析、报告、警报和自动化
- 开放式集成 API 实现自动响应和安全运维
- 通过 BGP、NETCONF、Representational State Transfer (REST)、JavaScript Object Notation (JSON) 以及云发出缓解信令

瞻博网络 MX 系列 5G 通用路由平台

MX 系列平台提供了强大的路由器 (支持 SDN) 产品组合，可提供以下功能：

- 无与伦比的系统容量、密度、安全性和性能
- 行业领先的内联数据平面安全性，吞吐量性能无影响
- 无限的可编程性为未来创新提供渐进式支持
- 利用自动化加快服务交付
- 多服务网络和节点切片功能可提供高达 40% 的总拥有成本节约
- 利用 Junos® Continuity 和统一不中断服务软件升级 (统一 ISSU) 降低停机风险
- 借助丰富的弹性功能实现无与伦比的网络和服务可用性
- 能够利用深度包检测 (DPI) 按应用处理流量
- 通过 Junos 遥测接口 (JTI) 将组件级别数据流传输到监控和分析工具
- 无比的空间效率和能效

总结 — 与时俱进的大规模、低成本 DDoS 实时防御方案

在多云、物联网和 5G 时代，网络安全威胁不断在演变。特别是 DDoS 攻击的规模、频率和复杂度仍在不断提升，服务提供商和企业都必须探索能够以更低成本提供更快、更有效保护的解决方案来扩大现有的防御。

IP 网络是现代安全解决方案的重要组成部分，是抵御容量耗尽攻击的第一道防线。遥测、机器学习分析和网络可编程性能够使检测和缓解流程更加智能、自动化以及更具适应性。

瞻博网络和 Corero 的这种联合 DDoS 防御解决方案将数据包级别的流量检查优势与基于基础架构的强大实施相结合，能够以空前的数十 TB 规模对 DDoS 攻击实现实时、自动的缓解，同时成本得到显著降低。

后续举措

如需了解有关瞻博网络和 Corero 如何帮助您的公司保护网络免受恶意 DDoS 攻击的更多信息，请联系您的瞻博网络或 Corero 销售代表。

关于 Corero

Corero Network Security 是一家专注于实时、高性能 DDoS 防御解决方案的领先企业。服务提供商、托管提供商以及在线企业依靠 Corero 备受赞誉的技术，通过自动检测和缓解攻击，同时结合全面的网络可见性、分析和报告功能来消除 DDoS 攻击对其环境的威胁。这种行业领先的技术可在最复杂的环境中针对 DDoS 攻击提供经济有效、可扩展的防御功能，相比先前提供的防御模式更具成本效益，更加经济划算。更多详情，请访问 www.corero.com。

关于瞻博网络

瞻博网络将简单性融入到全球互联的产品、解决方案和服务之中。通过工程创新，我们消除了云时代网络的限制和复杂性，可应对我们的客户和合作伙伴日常面临的的严苛挑战。在瞻博网络，我们坚信，网络是分享知识和实现人类进步的资源，它将改变这个世界。我们致力于开创具有突破性的方式，以提供与业务发展速度相匹配的自动化、可扩展且安全的网络。

公司和销售总部
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737)
或 +1.408.745.2000
传真：+1.408.745.2100
www.juniper.net

亚太地区及欧洲、中东和非洲地区总部
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.0.207.125.700
传真：+31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity