“安全区域隔离中心”通过核心交换机与多种功能模块集成来实现是思科最先提出的，方法是在不同层次上的安全技术协同，在核心处通过整合交换技术、防火墙技术、VPN 技术、防 DDOS 攻击技术、IPS/IDS 技术于一体，使用多层次的协作式防护来保证网络的安全。

“IDC 安全专区“对客户提供的个性化安全服务在“安全域隔离中心”上实现，也可以通过自建边界安全网关实现多种安全业务，但是来自内部区域通过核心交换的安全控制需求还是“安全隔离中心”实现起来简洁易行，性价比高，扩展性强！

“安全事件管理”的新高度——“速响中心”

随着安全业务开展的增多，运营者针对安全事件的响应速度成为客户体验服务质量的一个主要指标，问题接踵而来：

- 蠕虫病毒不断漫延，需要追查攻击的源头并首先阻断攻击通路
- 已部署防火墙，IPS/IDS 众多设备，却没有整体安全状态概念
- IDS，防火墙海量报警日志越存越多，无法快速理解问题所在
- 企业要求遵从 SOX 方案，人工提取网络 IT 审计报告成本太高
- 需要经常动态评估现系统安全状态，没有性价比高的实用工具

建立一个针对安全事件快速响应中心系统是保障安全业务服务质量的基础，思科推出的 MARS（Monitoring，Analysis，and Response System）正是这样一个安全监控分析和响应先进安全信息管理系统。

- 创新的端到端网络感知技术，可自动构建一个网络拓扑图，其中包括设备配置和当前安全策略，可对用户网络中的分组流建模，看图识别攻击者、攻击目标和网络热点
- 智能分析解决攻击定位、攻击路径追踪问题，提供了一个由实时热点、事故、攻击路径和具体调查组成的拓扑图，使管理员能直观的从网络拓扑图中清晰的看到攻击路径、攻击源，能完全了解事件、立即确认有效威胁
- 用户能最大的利用现有的基础设施，利用原有的投资来保证安全。MARS 能集中设备监控、集中事件库，能对网络基础设施包括路由器、交换机、防火墙、IDS、VPN 集中器和终端设备集中监控、收集信息，进行实时相互关联分析，利用现有设备准确识别和防御网络攻击

MARS“速响中心”虽然能够采集 Netflow，但主要是通过 Netflow 发现蠕虫爆发，其本身定位还是在 IDC，DCN/BOSS，企业等可以管理的内部网络系统。对于 IDC 来讲主要的功用如下：

- 托管网站之间互相攻击的监控与响应
- 蠕虫与病毒的阻断
- 实时攻击监控响应，预防与控制
- SOX 法案的遵从审计报告自动提取
- 安全事件的追踪分析报告（定位）
- 木马猜密码等自动发现

“安全第一“的目标是“安全创造业务”

运营性服务提供商分级安全模型阐述了威胁与业务关联的实现方式，三个安全中心“异常流量清洗中心”“安全区域隔离中心”“攻击事件速响中心”的技术实现为“安全创造业务”提供的了可行的方案。

如今社交网站，Web 2.0 网站，在线游戏，虚拟社区，视频，VOIP 等新应用对安全系统提出了新的挑战，进出流量的巨大差异，每秒并发的突发率与峰值越来越高，要求“安全中心”支持控制流量与数据流量异步通过（入向访问流量通过“安全中心”检测控制，出向数据业务流量不过安全中心），安全隔离中心系统每秒并发至少在 10 万以上等等，这些关键设计的把握方能将“安全保障”与“业务体验”同步提升。

“安全第一”是我们耳熟能详的一句口号，当“安全第一”与“业务开展“矛盾时，转换观念，开放思想，积极思考安全问题与“业务开展”辩证统一的关系，在可以承受的安全投入前提下，尽力实现“安全创造业务”的目标！

北京
北京市朝阳区建国门外大街2号北京银泰中心
银泰写字楼C座7-12层
邮编：100022
电话：(8610)85155000
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32-33层
邮编：200021
电话：(8621)23024000
传真：(8621)23024450

广州
广州市天河区林和西路161号
中泰国际广场A塔34层
邮编：510620
电话：(8620)85193000
传真：(8620)85193008

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86961000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn

欢迎下载电子文档，http://www.cisco.com/web/CN/products/products_netsol/security/index.html
2008 年 6 月印刷

运营商“ 安全创造业务”新思维的技术实现

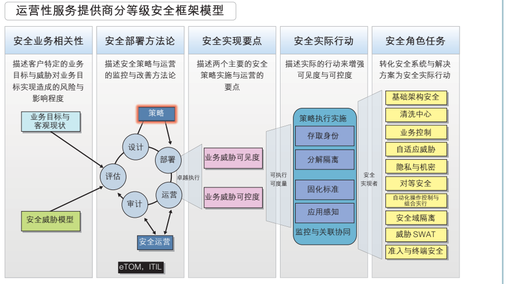
〈思科安全技术部门〉

中心观点

改变“安全是业务障碍”的传统观念，推进“安全创造业务”的新思维。提出三个安全中心——“异常流量清洗中心”“安全区域隔离中心”“攻击事件速响中心”的技术实现与创造业务的设计原理。阐述“安全第一” 的核心观念是平衡成本，在可以承受的安全成本投入下并实现 “安全创造业务“的目标！

运营性服务提供商分级安全模型

Service Provider 本意是服务提供商，任何针对信息的威胁对于运营商的挑战就是如何将威胁与其核心的业务关联起来，思科提出的针对运营性服务提供商的分级安全模型中分为 5 个阶段去展现将威胁问题转化为增值业务的过程，参见下图：



- 安全业务相关性： 定位客户特定的业务目标与威胁对业务目标实现造成的风险与影响程度
- 安全部署方法论： 确定安全策略与运营的监控与改善方法论
- 安全实现要点：关注两个主要的安全策略实施与运营的要点
- 安全实际行动：四个实际的行动来增强可见度与可控度
- 安全角色任务：努力转化安全系统与解决方案为安全实际行动

“安全创造业务”的新概念——清洗中心

近年来利用分布式拒绝服务（以下简称 DDOS）攻击的网络敲诈活动愈演愈烈，对正常的网络应用、服务和经济活动造成了严重影响。由于种种原因导致实施 DDOS 攻击的成本非常低，但处理 DDOS 攻击、追踪攻击的代价却很高。鉴于互联网的互联性和无边界性，溯源的过程涉及到的技术、管理、法律、执法等多方问题目前都不能妥善解决，溯源成本远远大于攻击成本。

应对 DDOS 拒绝服务攻击正是运营商发挥作用的契机，而且只有运营商有条件控制全网的异常流量。过去简单的将用户服务设备路由设为“黑洞路由”使恶意流量无法访问的方法已不能适应新阶段客户的期望，如何有效的缓解 DDOS 攻击，快速检测攻击，从合法业务流量中分离出恶意数据包，提供以秒计而不是以小时计的快速 DDOS 响应，需要一个全新的技术实现方案。

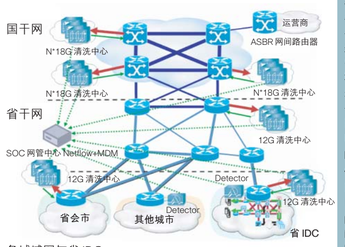
旁路的“清洗中心”成为公认的最佳选择，它部署在关键路由器和交换机附近，消除了单个故障点问题，且不影响任何现存的网络部件的性能和可靠性。

思科 Guard 清洗中心与 Detector 检测器配合的整体 Anti-DDOS 解决方案如下：

- Anti-DDOS清洗中心：清洗中心是创新的DDOS解决方案的核心——它是一个高性能可扩展的DDOS攻击缓解系统，不仅能部署在上游的运营商与数据中心，还可以部署在一个大企业内部来保护网络和数据中心资源。当DDOS清洗中心被通知有一个目标处于被攻击状态时，指向目标的业务将被转移到与该目标设备相连的清洗中心。然后业务将通过七层分析和过滤，以除去所有恶意业务使得好的数据包能继续传送。清洗中心位于一个单独网络接口处的路由器或交换机附近，在不影响其他系统的数据业务流情况下实现按需保护。由于它的位置靠上游，清洗中心可同时保护多个可能的目标，包括路由器、防火墙，四层交换机，Web/DNS 服务器、LAN 和 WAN 带宽等。
- DDOS检测探测器：作为清洗中心的配套报警系统，探测器提供对最复杂DDOS攻击的深入分析。探测器被动监测网络业务，搜寻与“正常”行为的偏差或DDOS攻击的基本行为。攻击被识别后，检测器发报警给清洗中心，提供详细的报告和具体报警来快速响应该威胁。例如，即使在没有超出总阈值界限的情况下，检测器也需要能观测到从单个源头来的 UDP 包速率是否超出了范围。

下面我们给出运营商提供 Anti-DDOS 服务的整体三级部署架构图:

经典城域网 / IDC 清洗中心 三级部署



各城域网与省 IDC

国干网：Core N*18G；防护基础架构与 VIP

省干网：建立一个（或备份一个）12G 清洗中心；防护基础架构（DNS，AAA，特定 IP）与省会城市以外的其他地市城域网及省 IDC

城域网：建立一个（或备份一个）12G 清洗中心；保护 VIP 网吧，专线用户以及 IDC 出口的带宽

IDC：建立一个 12G 清洗中心；保护托管业务

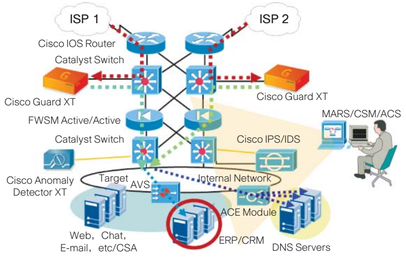
网间部署：对等部署控制网间异常流量的费用

DDOS 检测与网管：广域网 Netflow 技术，MSS/IDC 部署 Detector

运营商通过全网部署 DDOS 防御体系提供增值服务的方式形成商业良性循环，即保护自己的网络又提供增值的服务，DDOS 攻击防护需要运营商抓住机遇也只有运营商能从根本上缓解 DDOS 攻击的危害。清洗中心部署在上游截流缓解最有效果，此外还有集群式部署，分布式部署，Peer 对等部署，MultiCast 冗余等多种部署方式。

在数据中心IDC中清洗中心被布署在数据中心的分发层，保护下游的链路和服务器。清洗中心连接到分发交换机并且支持冗余配置的防护架构图如下：

数据中心 DDOS 防护部署图



清洗中心应该部署在防火墙的上层，这样可以有效防护外部攻击防火墙引起防火墙连接拥塞的可能性，如果部署在防火墙后面，就无法防护防火墙，IPS，四层交换机等由于 Session 表冲满导致的中断问题，从而失去保护网络的意义。

清洗中心通过创新的 BGP 旁路牵引与按需防护技术成为引领 DDOS 防护的主流技术解决方案，思科 Guard专利的自学习基线－攻击检测－攻击防护三阶段闭环设计与全动态自调整策略防护机制是核心技术，开放的DDOS安全服务报表输出与自动抓包取证的一体化思路是DDOS防护业务服务化的基础。清洗中心与多种检测协同工作不仅能检测最复杂的网络层DDOS攻击，也能提供阻断日益复杂和难于检测的应用层攻击，在清洗DDOS恶意流量同时不影响合法业务的正常通过，它自动检测恶意流量特征并去除恶意业务，只允许信任的数据包通过，确保了客户业务的持续性和完整性，是新形式下有效防护大规模互联网 DDOS 突发事件的最佳实践。

“清洗中心”概念的引入是缘于防护 DDOS 攻击的缘故，思科新一代“清洗中心”将针对 DDOS，异常流量，蠕虫攻击，应用层攻击等安全问题创造出与时俱进的新一代 “安全中心”!

“安全域划分”的经典设计——隔离中心

互联网数据中心IDC业务发展迅速，有调查显示，70%以上的用户有IDC使用需求，需求主要集中在基础服务、管理服务、互联网增值服务、咨询服务及企业应用服务等。目前IDC提供的业务仍停留在基础主机托管业务上，没有专门的安全防护设备来为托管主机进行安全防护，存在较大的安全隐患。同时随着竞争的加剧，以恶意竞争为目的的攻击行为层出不穷，严重影响了托管主机业务的正常进行。“IDC安全专区“成为运营商新的经济增长点，如何在IDC核心部署安全隔离系统为托管用户提供个性化的安全服务呢?

IDC 的 Internet 接入通过申请上游的“清洗中心“或自建的”安全中心“防护来自外部 DDOS，网络入侵，蠕虫病毒等的恶意攻击，守好 IDC 对外的第一道门!

当然来自内部的攻击危害更大，所以内部各安全区域之间的隔离尤为重要，隔离策略的好坏直接影响内部威胁的蔓延。病毒蠕虫变种传播，垃圾邮件泛滥，数据泄露损坏，开源代码的安全等新威胁问题层出不穷。还有企业远程移动存取 IDC 内部数据的安全问题等等……

完善的安全域隔离系统将涵盖五个层面：

- 物理层隔离：通过将广泛种类与数量的物理端口划开各安全域（10GE，POS，GE，FE 等），在物理上隔开各安全域
- 逻辑层隔离：通过 VLAN，虚拟防火墙功能，同一物理口上可逻辑上划开各安全域之间通过虚拟防火墙控制
- 策略层隔离：通过足够的策略数在不同的安全 Zone 之间，策略上划开各安全域之间的防护等级
- 应用层隔离：通过 DPI 应用检测技术，能够区分出流量内容，控制各安全域之间的业务应用
- 准入层隔离：通过网络准入控制技术，能够根据接入端点的系统安全状况，接入不同等级的安全域

安全区域划分边界是水平分域的方式，垂直层面描述的是各安全域之间隔离的层次程度。如下图：