

思科 Guard XT 5650

产品概述

思科系统®公司推出的Cisco®Guard XT 5650 DDoS 防护设备是一种功能强大、用途广泛的拒绝服务 (DDoS) 防护系统。Cisco Guard XT 的目标是满足要求最高、规模最大的企业环境提出的性能和扩展能力要求,它能够抵抗当今最复杂、最隐蔽的攻击,有效保护企业的网络环境。



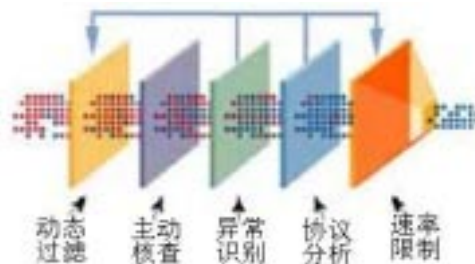
Cisco Guard XT 配有两个千兆位以太网接口,能够以真正的千兆位线速处理攻击流量。如果组合使用多台 Cisco Guard XT,还可以支持数 Gbps 速率,为大型发展中企业环境提供可以不断扩展的解决方案。

DDoS 攻击的发展

当今的 DDoS 攻击更恶毒、传染性更强、破坏力更大、目的性也更强。这些攻击一般由心怀不满的用户或不讲道德的企业发起,目的是攻击某些网站或竞争对手,由于技术高明,很容易越过多数普通的防御系统。很多病毒看似有合法的外观和身份,使人很难发现并阻止这些恶意流量。DDoS 攻击会使受害系统瘫痪,令企业无法正常开展业务,并使企业每年遭受数十亿美元的损失。

Cisco Guard XT 能够预防这种新的 DDoS 攻击,帮助企业预防此类攻击,有效保护其关键业务和盈利业务。Cisco Guard XT 采用了独特的多重验证过程 (MVP) 体系结构、最先进的异常识别、源核查和防欺诈技术,能够有效发现并阻止攻击流量,并保证合法事务处理流量通过。另外,Cisco Guard XT 还采用了直观的图形用户界面 (GUI) 和多层监控和报告,以便综合了解所有攻击行为,提供强有力的全面 DDoS 防御,有效保护业务的正常运作。

图 1
Cisco Guard XT MVP
的体系结构



应用

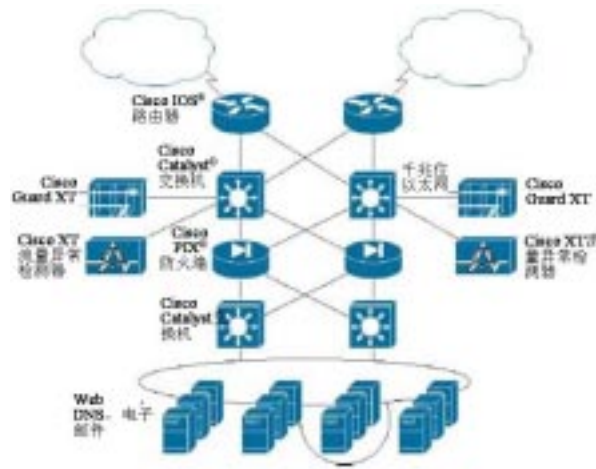
Cisco Guard XT 是完整的探测和预防技术,能够有效防止企业、托管中心、政府机构和服务供应商的环境遭受 DDoS 攻击。如果与用于探测 DDoS、蠕虫及其它攻击的 Cisco XT 流量异常探测器配合使用,Cisco Guard XT 能够执行详细的流量级攻击分析、识别和预防服务,防止恶意攻击危害到网络运作。

当 Cisco XT 流量异常探测器发现潜在的攻击后,它将向 Cisco Guard XT 报警,提示 Cisco Guard XT 开始监控而且只监控去往目标设备的流量。由于所有其它流量都可以继续顺畅地流动,因此,

这种方式不但可以减小对整个业务运作的影响，还可以增加每台 Cisco Guard XT 可以保护的设备或区域的数量。

受监控的流量将通过 Cisco Guard XT 重新路由，通常会令其脱离网络上的关键路径——从企业入口接入点到离开 ISP 骨干网的对等点。受监控的流量将受到严格检查，以便将“坏”流量与合法的事务处理流量分开。攻击分组将被识别并删除，合法流量则将转发到初始目的地，以保证实际用户和实际事务处理能够顺利通过，最终实现最高的可用性。

图 2



主要特点和优点

多级验证

Cisco Guard XT 能够对每股流量进行非常详细的分析，以高精度度阻止攻击流量，同时允许合法事务处理流量顺利流过。

为精确识别并阻止各类攻击，思科系统公司提供了多个防御交互层次。利用由基于概况的先进异常识别引擎支持的集成式动态过滤和主动核查技术，能够快速、自动预防各类攻击，甚至包括以前从未出现过的“第零天”攻击。借助其它协议分析和速率限制特性，可以只允许合法流量通过，而且数量不会使下游设备过载。

另外，Cisco Guard XT 还采用了集成式“杀手”技术，能够发现并阻止各种类型和大小的攻击，包括由数十万台分布式“非正常”主机发动的攻击，这是目前最盛行、最难抵御的一种 DDoS 攻击。

多 GB 性能

每台 Cisco Guard XT 采用了网络专用处理器，这种处理器能够在独立模式下以真正的千兆位线速执行攻击分析和清除，从而预防大型 DDoS 攻击，包括由大量分布式攻击者发动的攻击，例如危害极大的“非正常”主机。

另外，Guard XT 还支持独特的集群体系结构，即能够逐级提高攻击处理速率和“非正常”主机防御功能，即使是最大的企业和服务供应商环境，也可以通过扩展防止其遭受最严重的攻击。

Cisco Guard XT 能够避开关键路径作为路由对等物部署，因而可以提供最高的可靠性和直接安装。Cisco Guard XT 只转移和清除去往目标区域的流量，因而能经济有效地利用资源并进行扩展。

多级监控和报告

Guard XT 采用了基于 Web 的直观 GUI，以简化策略定义、运作监控和报告生成过程。

多级监控和报告能够为网络操作员、安全管理员和客户多种详细的实时信息和历史信息。攻击报告提供每次攻击的详细内容，包括特征、识别到的“非正常”表以及采取的特定措施等，以帮助安全专家审核和调整 Cisco Guard XT 的安全策略。

与此同时，利用客户级历史信息汇总，服务供应商不但可以报告攻击的数量、期限和影响力，还可以报告成功的抵御方法。另外，用户还可以在激活前利用交互模式查看和审核系统推荐的各项措施和策略，如果需要，还可以请求人工帮助。

总结

利用 Cisco Guard XT，即使遭遇到了最恶意的攻击，服务供应商、托管中心和网上企业也可以实现不间断业务运作。利用它，用户不但可以实现无与伦比的可用性，还可以有效保护最宝贵的企业资源，因而可以获得极高的竞争优势。

产品规格

表 1 产品规格

描述	规格
内存	2GB DDRAM
硬盘驱动器	80GB
接口	两个千兆位以太网 两个 100BASE-T (管理)
电源	双 110-220V, 350W
重量	62 lbs/28.2 kg
高度	3.36 in. / 8.53 cm
宽度	17.5 in. / 44.5 cm
深度	27.5 in. / 69.9 cm
是否可用机架安装	是
管理	基于 Web 的安全 GUI CLI: 控制台, Telnet, SSH Cisco (Riverhead) SNMP MIB 和 MIB II TACACS+ Syslog
认证	通过了 UL 认证 CE 遵守 FCC 规定第 15 部分
预防攻击	<ul style="list-style-type: none">• 欺诈攻击和非欺诈攻击<ul style="list-style-type: none">- TCP (syns, syn-acks, acks, fins, 分段)- UDP(随机端口洪泛, 分段)- ICMP (不可到达, 回声, 分段)- DNS• 客户机攻击<ul style="list-style-type: none">- 被动连接和总连接- HTTP Get 洪泛• BGP 攻击



思科系统（中国）网络技术有限公司

北京

北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19~21层
邮编: 100738
电话: (8610)65267777
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)33104777
传真: (8621)53966750

广州

广州市天河北路233号
中信广场43楼
邮编: 510620
电话: (8620)87007000
传真: (8620)38770077

成都

成都市顺城大街308号
冠城广场23层
邮编: 610017
电话: (8628)86758000
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>

思科系统（中国）网络技术有限公司版权所有。

2004 ©思科系统公司版权所有。该版权和其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌, 名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。