

# 思科 XT 5600 流量异常检测器



## 产品概述

思科系统®公司推出的 Cisco® XT 5600 流量异常检测器是一种完整的解决方案，能够帮助大型机构预防分布式拒绝服务 (DDoS) 或其它计算机攻击。利用它，用户能够快速启动抵御服务，在业务受到影响之前就制止攻击。

Cisco XT 流量异常检测器采用了已获专利的独特的多重验证处理 (MVP) 体系结构，以及最新的行为分析和攻击识别技术，能够主动检测和识别各种计算机攻击。

Cisco XT 流量异常检测器能够持续监控去往受保护设备的流量，例如 Web 或电子商务应用服务器，并详细记录各种设备在“正常”操作条件下的情况。如果 Cisco XT 流量异常检测器检测到哪股流量与正常情况不同，就会怀疑这种异常行为可能来自攻击，然后按照用户的喜好作出反应：向操作员发出警报，启动人工反应流程；触发现有的管理系统；或者启动 Cisco Guard XT DDoS 防护设备，立即开始抵御服务。

如果与 Cisco Guard XT 配合使用，Cisco XT 流量异常检测器堪称业界最全面的 DDoS 防御系统。利用 MVP 体系结构，Cisco XT 流量异常检测器和 Cisco Guard XT 能够检测、隔离和删除恶意攻击流量，而且不会影响合法事务处理，因而能有效保护网络流量和关键业务流量。

## 应用

计算机攻击方兴未艾，而 DDoS 攻击又是当今网络业面临的发展最快的威胁。这些攻击已经从试图引起公众关注的简单破坏行为发展成目的性极强的旨在破坏某企业业务运作的恶意行为，针对性和破坏力都越来越强，很多企业都因此而惨遭破产。

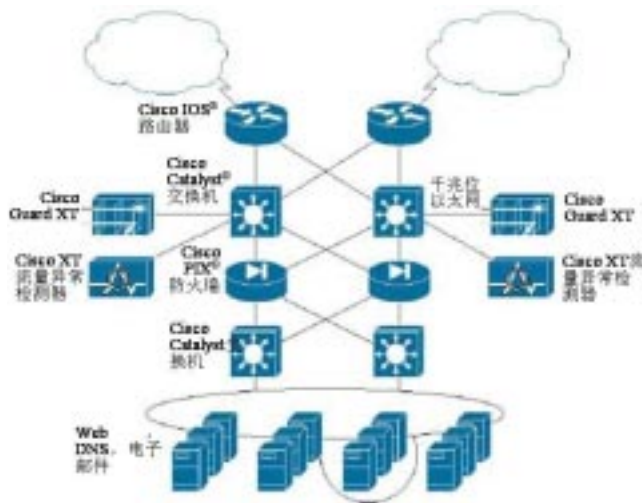
与此同时，攻击技术也变得越来越先进。攻击者能够模仿合法请求，伪造源身份，并利用众多受感染的“非正常”主机攻击互联网数据中心，穿越现有防线，使恶意流量的识别和阻止变得异常困难。

Cisco XT 流量异常检测器与 Cisco Guard XT 配合使用，能够提供完整的检测和防护解决方案，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。当 XT 流量异常检测器发现某流量不同于“正常”行为时，将向 Guard XT 发出警报，让它开始监控而且只监控去往目标设备的流量。由于所有流量都能继续顺畅地流动，因而既能够减小对整体业务运作的影响，又能增加每台 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。受监控的流量将接受严格检查，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。

# 思科 XT 5600 流量异常检测器

图 1



## 主要特点和优点

### 识别与学习

Cisco XT 流量异常检测器驻留在关键路径以外，能够以真正的千兆位线速监控映射流量，为每台受保护的设备建立详细的“正常”行为档案，而且不会消耗宝贵的交换机或路由器资源。

Cisco XT 流量异常检测器采用了基于行为的先进异常检测技术，能够同时在宏观和微观对话水平上检测异常行为，从而高度准确地识别到各类已知攻击和“零天”攻击。利用精细的对所有分组都执行的单连接状态分析，可以快速、彻底地检测和发现最隐蔽、最先进的攻击——从微小的低速服务器资源消耗攻击到由数十万台分布式“非正常”机器发动的大型攻击。

另外，XT 流量异常检测器还包括行为识别引擎，这种引擎不但不需要持续更新概况信息，还能够减少静态签名方法所固有的大量警报和错误提示。另外，Cisco XT 流量异常检测器还预先配置了默认概况信息，因而可以立即投入使用，并启动自动学习功能，帮助用户提出特殊调整建议，供操作员参考。

最后，还可以通过对话状态识别合法对话流量，发现对话滥用攻击，抵御恶意行为。

### 高性能

高性能的 Cisco XT 流量异常检测器能够以真正的千兆位线速监控攻击流量，即在一次攻击中，能够为每台设备识别 100,000 多个来源，因而能够为大型大容量环境提供强大的保护，抵御分布式攻击。

另外，对完全映射流量的多阶段分析还有助于快速识别最隐蔽的低速攻击。为提供最可靠的保护，Cisco XT 流量异常检测器可以部署在下游——靠近数据中心的受保护资源，也可以部署在上游——靠近 Cisco Guard XT，增大覆盖范围。

### 报告和管理

Cisco XT 流量异常检测器使用了基于 Web 的图形用户界面 (GUI)，能够以简单、直观的方式显

# 思科 XT 5600 流量异常检测器

示信息，并大大简化配置、运作和攻击的识别和分析。

Cisco XT 流量异常检测器提供多种实时和历史报告，利用这些报告，网络操作员、安全管理员和客户能够通过详细信息检测攻击、制定策略并抵御攻击。另外，还可以将报告统计数据输出为文本文件，供后端定制或后续查看。

通过配置，Cisco XT 流量异常检测器还可以主动将警报发送给网络操作员和 Cisco Guard XT，以便对攻击作出快速反应，包括自动启动抵御服务，快速抵御攻击。利用简单网络管理协议 (SNMP) 管理信息库 (MIB)，还可以向基于标准的管理系统提供所有设备信息、受保护区域信息和攻击信息。

## 总结

Cisco XT 流量异常检测器是为大型托管中心和网上企业设计的，如果与 Cisco Guard XT DDoS 防护设备配合使用，将能够提供有效的安全解决方案，即使遇到最恶意的攻击，也能够保证业务的不间断运作。对于用户，由于能获得无与伦比的可用性，并有效保护宝贵的企业资源，因而能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"><li>• 欺诈攻击和非欺诈攻击<ul style="list-style-type: none"><li>- TCP (syns, syn-acks, acks, fins, 分段)</li><li>- UDP(随机端口洪泛, 分段)</li><li>- ICMP (不可到达, 回声, 分段)</li><li>- DNS</li></ul></li><li>• 客户机攻击<ul style="list-style-type: none"><li>- 被动连接和总连接</li><li>- HTTP Get 洪泛</li></ul></li><li>• BGP 攻击</li></ul>

欲知详情，请访问：[http://www.cisco.com/en/US/products/svcs/ps3034/serv\\_category\\_home.html](http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html)



## 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。