



PRODUCT BULLETIN

CISCO TRAFFIC ANOMALY DETECTION AND MITIGATION SOLUTIONS

Cisco traffic anomaly detection and mitigation solutions deliver the industry's most complete and powerful family of solutions for detecting and defeating complex, sophisticated DDoS attacks.

Internet attacks such as distributed denial of service (DDoS) pose a serious threat to any business with an online presence. DDoS attacks paralyze Websites by overloading servers, links, and network devices with malicious, unsolicited traffic. They can quickly overwhelm an organization, blocking legitimate transactions and preventing users—whether customers trying to complete an online purchase or employees attempting to access an internal enterprise resource planning (ERP) system—from performing mission-critical operations. Easily launched using readily available tools, DDoS attacks are costing businesses millions of dollars a month in lost revenue, compromised productivity, and tarnished reputations.

Cisco® DDoS detection and mitigation solutions, developed by Riverhead Networks (acquired by Cisco Systems in March 2004), detect the presence of DDoS attacks and identify and block malicious traffic in real time—without affecting the flow of legitimate, mission-critical transactions. As a result, the business operations of targeted organizations can continue running, even while under attack, making sure that critical corporate assets are always protected.

The Cisco DDoS family includes two different products, both of which deliver multigigabit performance for protecting the largest enterprise and service provider environments from the highest-volume, most sophisticated attacks:

Cisco Traffic Anomaly Detector XT 5600—The Cisco Traffic Anomaly Detector XT 5600 detects DDoS, worm, and other attacks, and reports on their characteristics. Detection is based on sophisticated anomaly detection capabilities that compare activity to profiles of known “normal” behavior, enabling the Cisco Traffic Anomaly Detector XT 5600 to identify even day-zero attacks that have never been seen before.

Cisco Guard XT 5650—The Cisco Guard XT 5650 performs per-flow-level attack analysis, identification, and mitigation services that block attack traffic. Alerted by the Cisco Traffic Anomaly Detector XT 5600 or other standards-based detection solutions, the Cisco Guard XT 5650 diverts traffic destined for a targeted device—and only that traffic—and subjects it to Cisco’s unique Multiverification Process (MVP) architecture. The MVP architecture imposes multiple layers of defense that identify and block the specific packets and flows responsible for the attack while allowing legitimate transactions to pass, ensuring business continuity even while under attack.

Working together, the Cisco Traffic Anomaly Detector XT 5600 and Guard XT 5650 represent the industry’s most complete, most powerful, and most accurate DDoS detection and mitigation solution.

Tables 1 and 2 highlight specific features of the Cisco Guard XT 5650 and the Cisco Traffic Anomaly Detector XT 5600 solutions.

Table 1. Cisco Guard XT 5650 Features

Feature	Description and Benefits
Performance	<ul style="list-style-type: none"> • A single Cisco Guard XT 5650 can process gigabit-level attacks at full line rates with minimal latency, keeping business operations flowing even under large, high-volume attacks • Clustering multiple Cisco Guard XT 5650 devices delivers a scalable solution that can process many times the standalone rate, sufficient for handling attacks seen by the largest enterprises and service providers • Only traffic destined for targeted victims is diverted for inspection and cleaning, allowing unaffected traffic to flow unimpeded • Legitimate traffic passes to its original destination, ensuring that customer transactions are unaffected by attacks
Attack coverage	<ul style="list-style-type: none"> • Highly sophisticated algorithms and traffic analysis enable the Cisco Guard XT 5650 to detect and defeat the largest, most advanced attacks • Zombie Killer capabilities allow a single Cisco Guard XT 5650 to identify and block more than 100,000 individual zombies in a single attack, thwarting one of the most common and difficult to defeat DDoS attack methods • Clustering increases Zombie Killer capabilities to protect against attacks launched by several hundred thousand zombies
Monitoring and reporting	<ul style="list-style-type: none"> • Multiple levels of real-time views and historical reports provide network operators, security administrators, and clients with rich, detailed information to assist in troubleshooting, policy setting, and system monitoring • Device-level views provide a high-level overview of protected zones, showing current attacks and incoming and outgoing traffic to immediately determine current status • Zone-level views provide a log of events for the selected zone, including attack history, duration, and type, helping the operator anticipate and respond appropriately to future events • Attack-level views provide details for specific events, including attack characteristics, identified zombies, and policies used to defend against the attack, allowing security experts to review and fine-tune policy thresholds • Historical reports provide visual records of attacks and associated responses over time for determining attack patterns and allowing IT administrators and service providers to verify successful protection techniques
Management	<ul style="list-style-type: none"> • Easy-to-use interface dramatically simplifies the policy setting and operational management of the Cisco Guard XT 5650 • “Interactive mode” enables users to review and approve recommended actions and policies before activation, providing manual control over attack responses • Simple Network Management Protocol (SNMP) support, including a proprietary MIB, enables the Cisco Guard XT 5650 to be easily integrated into any standards-based environment and be managed by any SNMP-compliant system • The Cisco Guard XT 5650 includes support for other interfaces such as TACACS+ authentication and syslog logging, contributing to complete, standards-based manageability

Table 2. Cisco Traffic Anomaly Detector XT 5600

Feature	Benefit
High-performance detection	<ul style="list-style-type: none"> • Detects and identifies the sources of even the most elusive and sophisticated DDoS attacks, including massive botnet attacks launched by legions of zombies • Monitors copies of individual traffic flows entering protected zones, enabling rapid, accurate, and precise detection of all types of attacks • Processes traffic flows at full Gigabit Ethernet line rates, delivering performance sufficient for the largest and most demanding environments • Uses Cisco's MVP-based anomaly recognition technology to identify deviations from "normal" behavior that indicate an attack, allowing detection of attacks that had never been seen before without relying on signature updates • Session state context allows the Cisco Traffic Anomaly Detector XT 5600 to recognize validated session traffic and identify session-abusive attacks, providing additional protection against malicious activity • Scheduled learning sessions gather performance data to suggest thresholds and policies that can be accepted, modified, or rejected • Can be deployed downstream close to protected zones or resources, or upstream closer to the Cisco Guard XT 5650 to provide wider coverage
Leading management and reporting	<ul style="list-style-type: none"> • A single Cisco Traffic Anomaly Detector XT 5600 can monitor a Gigabit link and can detect attacks on thousands of protected IP addresses, providing a scalable solution for large and expanding environments • Resides off the critical network path and does not require network device statistics collection that might interfere with network operations while under attack • Automatically sends alerts to network operators, management systems, and the Cisco Guard XT 5650 to initiate rapid response and attack mitigation • Preconfigured default thresholds can be automatically tuned by self-learning, eliminating the need for manual tuning or technical expertise • Web-based interface dramatically simplifies Cisco Traffic Anomaly Detector XT 5600 management, configuration, and operation • Proprietary SNMP MIB enables integration with other standards-based management systems

Table 3. Availability and Ordering Information

Product Name	Part Number
Cisco Traffic Anomaly Detector XT 5600 with 10/100/1000BASE-T Ethernet ports, dual AC power, Redundant Array of Independent Disks (RAID)	ADXT-5600-GET-A-K9
Cisco Traffic Anomaly Detector XT 5600 with 1000BASE-SX multimode fiber-optic ports with LC connectors, dual AC power, RAID	ADXT-5600-MMF-A-K9
Cisco Traffic Anomaly Detector XT 5600 MVP-OS Release 3.08	SC-ADXT-3.0.8-K9
Cisco Guard XT 5650 with 10/100/1000BASE-T Ethernet ports, dual AC power, RAID	AGXT-5650-GET-A-K9
Cisco Guard XT 5650 with 1000 BASE-SX multimode fiber-optic ports with LC connectors, dual AC power, RAID	AGXT-5650-MMF-A-K9
Cisco Guard XT 5650 MVP-OS Release 3.0.8	SC-AGXT-3.0.8-K9

General orderability (still with new product hold) and first customer shipment (FCS) are scheduled for July 2004. Until then, the Cisco Traffic Anomaly Detector XT 5600 and Guard XT 5650 are on limited orderability.

PRODUCT INFORMATION

For more information about the Cisco Traffic Anomaly Detector XT 5600, visit <http://www.cisco.com/en/US/products/ps5887/index.html>

For more information about the Cisco Guard XT 5650, visit <http://www.cisco.com/en/US/products/ps5888/index.html>



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

BG/LW6509 06/04