Cisco Traffic Anomaly Detector Module

The Cisco® Traffic Anomaly Detector Module is an integrated services module for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers that helps large organizations protect against distributed denial of-service (DDoS) attacks or other network attacks by enabling users to quickly initiate mitigation services and block the attacks before business is adversely affected.

Based on a unique, patented multiverification process architecture, the Cisco Traffic Anomaly Detector Module (Figure 1) uses the latest behavioral analysis and attack recognition technology to proactively detect and identify all types of online attacks. By constantly monitoring traffic destined for a protected device, such as a Web or e-commerce application server, the Cisco Traffic Anomaly Detector Module compiles detailed profiles that indicate how individual devices behave under "normal" operating conditions. If the Cisco Traffic Anomaly Detector Module detects any per-flow deviations from the profile, it considers the anomalous behavior a potential attack and responds based on user preference—by sending an operator alert to initiate a manual response, by triggering an existing management system, or by launching the Cisco Anomaly Guard Module to immediately begin mitigation services.

Figure 1.   Cisco Traffic Anomaly Detector Module

Combined with the Cisco Anomaly Guard Module, the Cisco Traffic Anomaly Detector Module contributes to the industry's most comprehensive DDoS defense system. Through the multiverification process architecture, the Cisco Traffic Anomaly Detector Module and Cisco Anomaly Guard Module detect, divert, isolate, and remove malicious attack flows without affecting legitimate transactions, delivering robust protection to networks and business-critical traffic.

How It Works

DDoS attacks represent the fastest-growing form of threats facing online businesses today. These attacks, which have evolved from simple acts of publicity-seeking vandalism to highly focused events designed to disrupt an organization's business operations, have become increasingly relentless and malicious, causing significant harm to many businesses.

Attack techniques are also growing more sophisticated. Attackers mimic valid requests, spoof source identification, and use armies of compromised "zombie" hosts to overwhelm Internet data centers and existing defenses, making identification and blocking of the malicious traffic flows virtually impossible.

The Cisco Traffic Anomaly Detector Module works with the Cisco Anomaly Guard Module to provide a complete detection and mitigation solution that protects enterprises, hosting centers, government agencies, and service provider environments from DDoS attacks. When the Traffic Anomaly Detector Module identifies potential attacks through deviations from known "normal" behavior, it alerts the Anomaly Guard Module to begin diverting traffic destined for the targeted devices—and only that traffic—for inspection. All other traffic continues to flow normally, increasing the number of devices or zones a single Anomaly Guard Module can protect.

Diverted traffic is rerouted through the Cisco Anomaly Guard Module, where it is scrutinized to identify and separate "bad" flows from legitimate transactions. Attack packets are identified and removed, while legitimate traffic is forwarded to its original destination. This helps ensure that real users and real transactions get through, and provides maximum availability.

Cisco Traffic Anomaly Detector Module Benefits

Recognition and Learning

The Cisco Traffic Anomaly Detector Module monitors a mirrored copy of selected inbound traffic flowing through the Cisco Catalyst 6500 Series or Cisco 7600 Series chassis toward destinations under protection, building detailed profiles of "normal" behavior for each protected device without consuming valuable switch or router resources.

Using sophisticated behavior-based anomaly detection technology, the Cisco Traffic Anomaly Detector Module detects any activity that deviates from those profiles at both global and detailed session levels, enabling highly accurate identification of all types of known and "day-zero" attacks. Per-connection state analysis of all packets enables fast, thorough detection and identification of the most elusive and sophisticated attacks—from subtle, low-rate server resource exhaustion attacks to large-scale attacks launched by hundreds of thousands of distributed zombies.

The Cisco Traffic Anomaly Detector Module's behavioral recognition approach eliminates the need to continually update string signatures while reducing the volume of alerts and false positives common with static signature-based approaches. In addition, the Cisco Traffic Anomaly Detector Module comes preconfigured with default profiles for immediate operation, and automated learning allows users to create specific tuning recommendations that can be reviewed by the operator.

Multigigabit Performance

The high-performance Cisco Traffic Anomaly Detector Module monitors attack flows at full gigabit line rates—and with the capacity to identify more than 100,000 sources per module in an attack, providing robust protection for large, high-volume environments against distributed attacks.

In addition, multistage analysis of fully mirrored traffic delivers fast recognition of even the stealthiest low-rate attacks. To provide the greatest possible protection, the Cisco Traffic Anomaly Detector Module can be deployed in downstream Cisco Catalyst chassis, close to protected resources in the data center, or in upstream chassis to provide more widespread coverage.

Reporting and Management

The Cisco Traffic Anomaly Detector Module uses a Web-based GUI that displays information in a simple, intuitive manner, dramatically simplifying configuration, operation, and attack identification and analysis.

Multiple real-time and historical reporting levels provide network operators, security administrators, and clients with detailed information to assist in attack detection, policy setting, and mitigation

(Figure 2). Report statistics can be exported to text and Extensible Markup Language (XML) schema-formatted files for backend customization or for later review.

The Cisco Traffic Anomaly Detector Module can also be configured to proactively send alerts to network operators and to the Cisco Anomaly Guard Module to initiate rapid response to attack conditions, including automated mitigation services to quickly thwart the attack. A Simple Network Management Protocol (SNMP) MIB also makes all device-level, protected-zone-level, and attack-level statistics available to standards-based management systems.

Figure 2. Multilevel Monitoring and Reporting Provides Detailed Views into Real-Time and Historical Performance
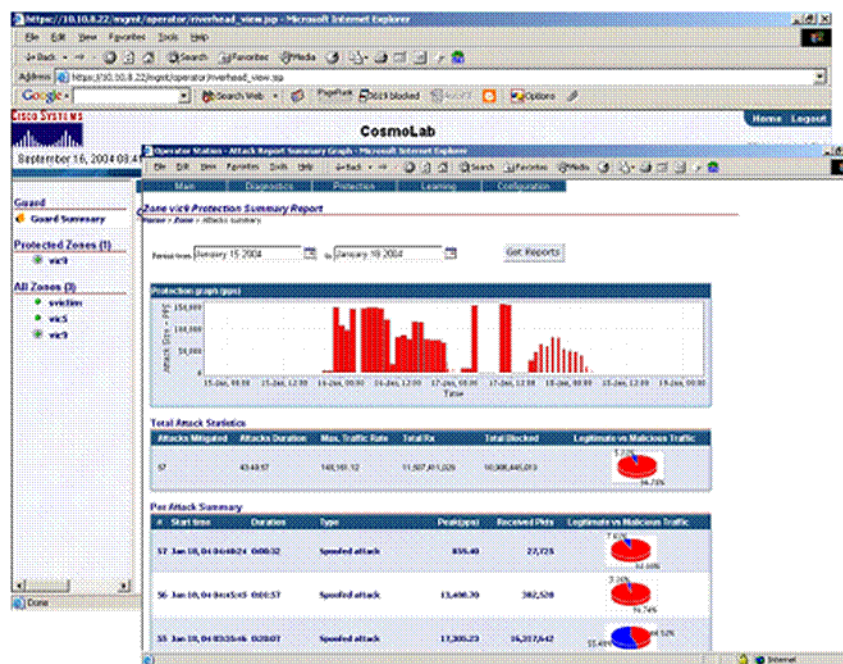
Cisco Traffic Anomaly Detector Module Performance Metrics

Table 1 provides information on the performance and capacity of the Cisco Traffic Anomaly Detector Module.

Table 1. Cisco Traffic Anomaly Detector Module Performance Metrics

Feature	Description
Performance	**Option #1: 1 Gbps** • 1 Gbps of throughput per module • 1.5 million concurrent connections • 500 protection zones (different policies and baselines [contexts]) • 90 concurrent zones in protection • Less than 1 ms latency and jitter **Option #2: 2 Gbps** • 2 Gbps of throughput per module • 3 million concurrent connections • 500 protection zones (different policies and baselines [contexts]) • 150 concurrent zones in protection • Less than 1 ms latency and jitter

Cisco Traffic Anomaly Detector Module Overall Feature Summary

Table 2 lists features of the Cisco Traffic Anomaly Detector Module.

Table 2.   Cisco Traffic Anomaly Detector Module Features

Feature	Description
Attack Recognition	• Spoofed and nonspoofed attacks • TCP (syns, syn-acks, acks, fins, fragments) attacks • User Datagram Protocol (UDP) attacks (random port floods, fragments) • Internet Control Message Protocol (ICMP) attacks (unreachable, echo, fragments) • Domain Name System (DNS) attacks • Client attacks • Inactive and total connections attacks • HTTP Get Flood attacks • Border Gateway Protocol (BGP) attacks • Session Initiation Protocol (SIP) voice over IP (VoIP) attacks
Continuous Learning and Detection	• Can operate in continuous learning and detection mode (Release 5.0 and later) • Simultaneously adjusts thresholds and detects attacks • Switches between learning and detection modes automatically • Returns to learning mode after an attack is completed
Learns for Anomaly Guard Module	• Ability to learn traffic profiles for zones defined on guards • Ability to upload learning information to guards automatically
Traffic Analysis	• Ability to capture and packets that are traversing the guard and save them as pcap files • The GUI allows extensive analysis of the captured packets • The user may limit capture to packets with a certain decision value only (forward, drop, reply) • The user may filter the capture using a tcpdump expression
Communications Protocols	• Secure Shell (SSH), Secure Sockets Layer (SSL), File Transfer Protocol (FTP), Secure FTP (SFTP)
Management	• Console to command-line interface (CLI) • SSH to CLI • SSL to Cisco Device Manager • Simple Network Management Protocol (SNMP) MIB, MIBII, and traps
Authentication, Authorization, and Accounting (AAA) Support	• Integrates with AAA through TACACS+ • Privilege-level and command-level authorization and accounting
Security	• IP table and self-DDoS protection on management interfaces
Logging	• Comprehensive syslogging and events

Configuration and Deployment Options

The Cisco Traffic Anomaly Detector Module offers two distinct deployment options—integrated mode and dedicated mode.

In integrated mode, one or more Cisco Traffic Anomaly Detector Modules are installed in existing Cisco Catalyst 6500 Series or Cisco 7600 Series chassis deployed in the data center and residing in the normal Layer 3 data path. A copy of traffic destined for resources to be monitored for protection must be sent to the Traffic Anomaly Detector Module by Switched Port Analyzer (SPAN) sessions, by physical port or VLAN, or by VLAN access control list (VACL) capture.

In dedicated mode, the Cisco Traffic Anomaly Detector Module is installed in a dedicated Cisco Catalyst 6500 Series switch or Cisco 7600 Series router adjacent to a downstream switch or router near the devices or zones being protected, providing a more scalable solution for large and growing environments. In this configuration, a copy of traffic must be sent to the dedicated switch or router via remote SPAN or fiberoptic link splitter.

The Cisco Traffic Anomaly Detector Module can be installed in either integrated or dedicated mode, imposing either a one- or two-step packet-capture process to receive a copy of traffic for monitoring. Whether in integrated or dedicated mode, when an attack is detected, the Traffic Anomaly Detector Module responds in one of three ways—it can send an alert to initiate a manual response, it can trigger an existing management system to take action, or it can automatically launch the Cisco Anomaly Guard Module or Cisco Guard XT appliance to immediately begin mitigation services.

Applications

Cisco DDoS anomaly detection and mitigation solutions can be deployed in various topologies serving both enterprises and service provider environments (Figures 3–5).

Figure 3. Cisco DDoS Anomaly Detection and Mitigation in Enterprise or Hosting Data Center
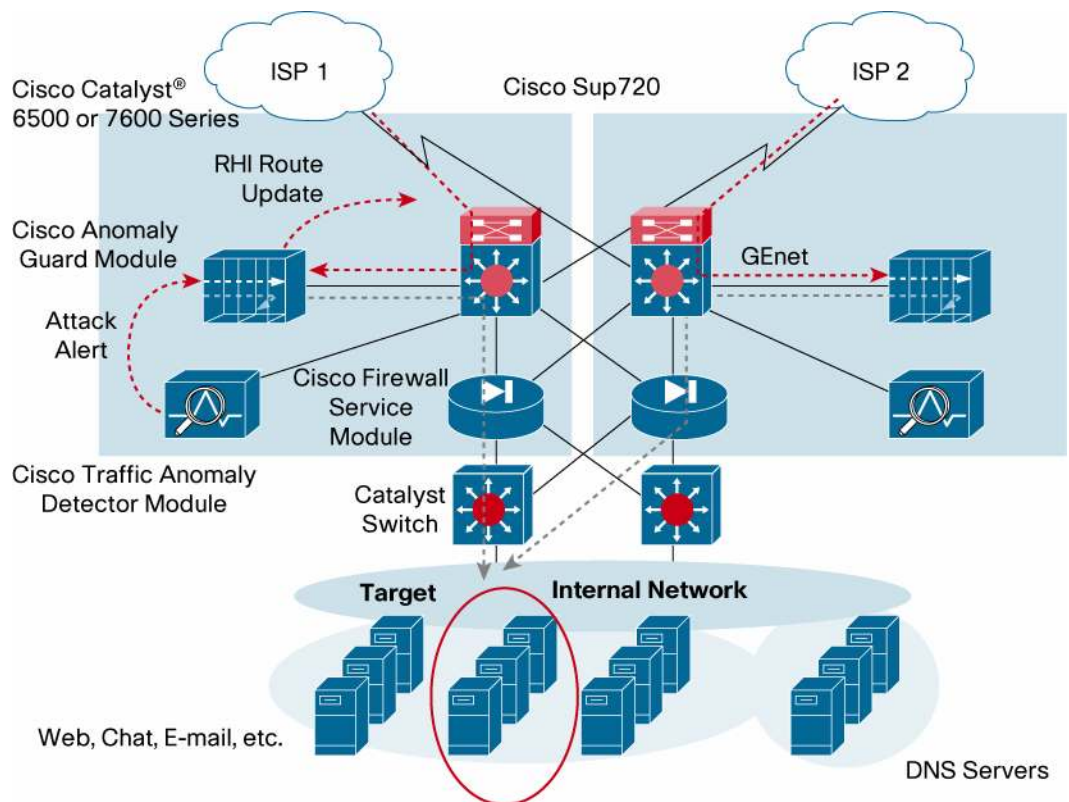
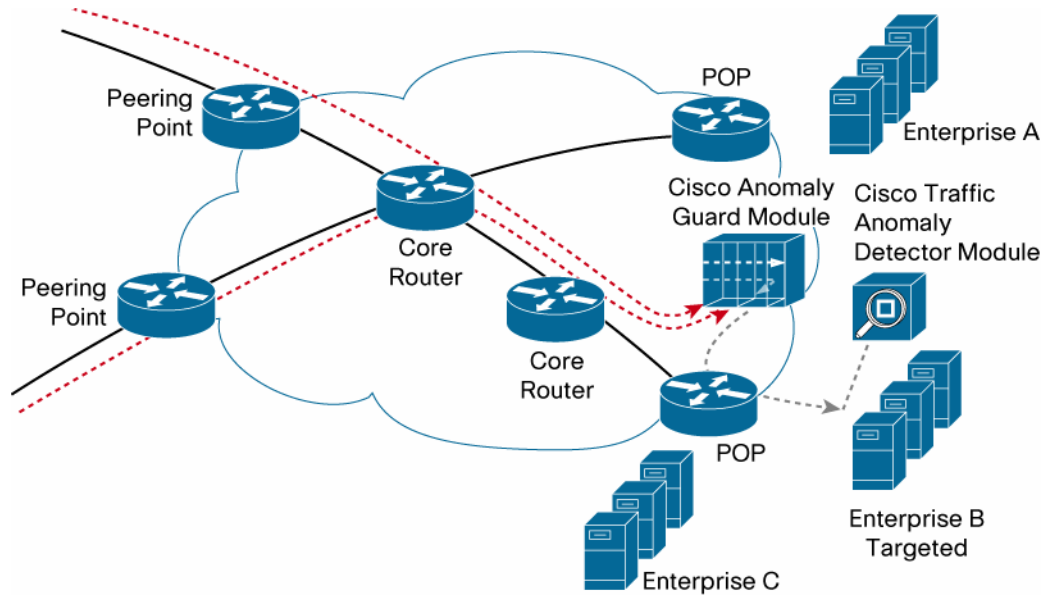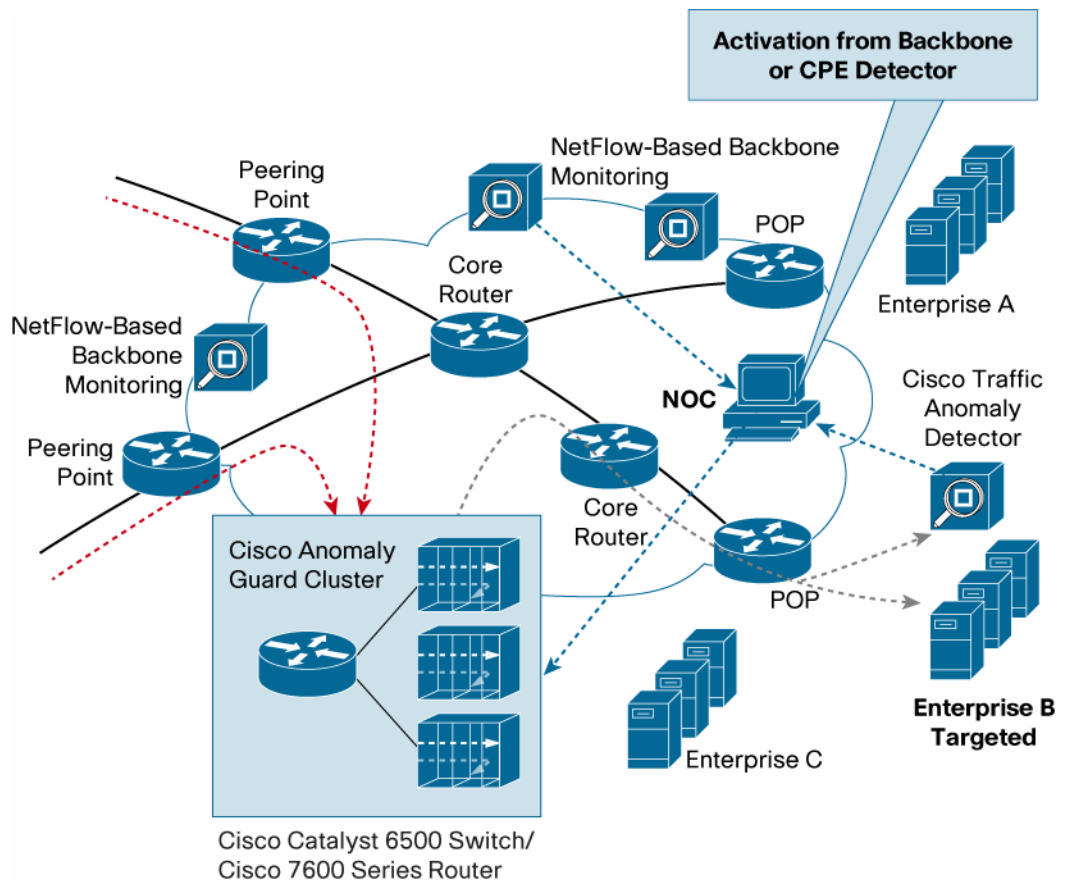**Figure 4.** Cisco DDoS Distributed/Edge Protection in a Service Provider Environment

Figure 5. Cisco DDoS Anomaly Detection and Mitigation in a Centralized Provider Scrubbing Center

Benefits of Security Services Integration

Security Services Integration
The Cisco Traffic Anomaly Detector Module can be combined with other Cisco security services modules such as the Firewall Services Module (FWSM), Intrusion Detection Services Module (IDSM-2), Content Switching Module (CSM), and the Network Analysis Module (NAM-1 and NAM-2). Together, these services modules provide a complete self-defending network solution.

Deployment Flexibility
Installed inside a Cisco Catalyst 6500 Series switch or Cisco 7600 Series router, the Cisco Traffic Anomaly Detector Module integrates complete DDoS detection capabilities into the network infrastructure. Modules can be easily installed in existing switches or routers, allowing powerful DDoS protection services to be deployed where and when they are needed, without consuming any interface ports. High-density dedicated appliances or multiservice security switches can also be deployed, using any range of chassis sizes and with high-availability, DC power, and Network Equipment Building Standards (NEBS) options. Interoperable line cards help ensure media flexibility. Packet capture may be completely intrachassis, or may occur across devices using remote SPAN or fiber link splitters.

Scalability
Where high-capacity protection is required, up to four modules can be installed in a single switch to support large and rapidly expanding environments. Additionally, the Cisco Traffic Anomaly Detector Module's multiprocessor architecture and multiple gigabit backplane interfaces can support future licensed software upgrades to multigigabit performance per module.

Reliability and High Availability
The Cisco Traffic Anomaly Detector Module maintains the performance, reliability, and robust architecture of the standalone Cisco Traffic Anomaly Detector XT appliance. When deployed in a Cisco Catalyst 6500 Series switch or Cisco 7600 Series router, the Traffic Anomaly Detector Module supports highly reliable redundant configurations, including redundant supervisor engines, backplanes, power supplies, and fans. In addition, Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers offer Control Plane Policing for DDoS hardening, as well as high-availability options.

Lower Cost of Ownership
Since the modules are integrated into Cisco Catalyst 6500 Series switches or Cisco 7600 Series routers along with other services modules, there are fewer devices to manage, reducing the cost of operation. In addition, because the application software is similar to the appliance application software, training costs are minimized. With this modular approach, customers can use their existing switching and routing infrastructures for cost-effective deployment—and can do so while obtaining the highest performance available in the industry and providing secured IP services along with multilayer LAN and WAN switching and routing capabilities.

Summary
Working in concert with the Cisco Anomaly Guard Module, the Cisco Traffic Anomaly Detector Module contributes to a complete security solution that helps ensure uninterrupted business operations, even in the face of the most malicious DDoS attacks. This translates into a significant

competitive advantage, providing uncompromised availability and unparalleled protection of the most valuable business assets.

System Requirements

- Cisco Traffic Anomaly Detector Module Software Release 5.03 or later.
- Cisco Catalyst 6500 Series Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) or Cisco Catalyst 6500 Series Supervisor Engine 720 (Cisco Catalyst 6500 Series Supervisor Engine 1 not supported).
- Switch Fabric Module (SFM) required on the Supervisor Engine 2 to process more than 1 Gbps of traffic.
- On the Cisco Catalyst 6500 Series switch, IOS support is only upto IOS® Software Release 12.2(18)SXE..
- On the Cisco 7600 Series routers, IOS support is on Software Release 12.2(18)SXE and also on the 12.2(33)SRA/SRB release.
- Occupies one slot in a Cisco Catalyst 6500 Series switch or Cisco 7600 Series router.
- Up to 6 Cisco Traffic Anomaly Detector Modules may be deployed in a single 9 slot chassis, either protecting the same destinations in load-sharing mode or different destinations. If deploying Cisco Anomaly Guard Modules and Cisco Traffic Anomaly Detector Modules in the same chassis, a combined total of eight modules may be installed. For nonstandard installations, consult the release notes or your Cisco technical support representative.
- Redundant supervisor engines must be used in Nonstop Forwarding (NSF) with Stateful Switchover (SSO) mode (not Route Processor Redundancy [RPR] or RPR+).

Product Specifications

Table 3 provides product specifications for the Cisco Traffic Anomaly Detector Module.

Table 3.   Product Specifications

Specification	Description
Memory	7 GB DDRAM, 1 GB Compact Flash
Weight	- Minimum: 3 lb (1.36 kg) - Maximum: 5 lb (2.27 kg)
Height	1.18 in. (30 mm)
Width	15.51 in. (394 cm)
Depth	16.34 in. (415 cm)
Power Requirements	- 168 Watts
Operating Temperature	32 to 104°F (0 to 40°C)
Nonoperating Temperature	–40 to 167°F (–40 to 75°C)
Humidity	10 to 90 percent, noncondensing
Management	- Secure Web-based GUI - CLI: Console, Telnet, SSH - Cisco (Riverhead) SNMP MIB and MIB II - TACACS+ - Syslog
Certifications	- UL-recognized - CE - FCC Rules Part 15-compliant

Ordering Information

Table 4 provides ordering information for the Cisco Traffic Anomaly Detector Module.

Table 4.   Ordering Information

Product Name	Part Number	Cisco SMARTnet Number
Cisco Catalyst 6500 Series/Cisco 7600 Series Traffic Anomaly Detector Module	WS-SVC-ADM-1-K9	CON-SNT-WSADMK9
Cisco Catalyst 6500 Series/Cisco 7600 Series Traffic Anomaly Detector Module (spare)	WS-SVC-ADM-1-K9=	CON-SNT-WSADMK9
Cisco Catalyst 6500 Series/Cisco 7600 Series Traffic Anomaly Detector Module Software Release 5.1	SC-ADM-5.1-K9	–
Cisco Catalyst 6500 Series/Cisco 7600 Series Traffic Anomaly Detector Module Software Release 6.0 1G	SC-ADM-6.0-1G-k9	–
Cisco Catalyst 6500 Series/Cisco 7600 Series Traffic Anomaly Detector Module Software Release 6.0 2G	SC-ADM-6.0-2G-k9	–
License for Cisco Catalyst 6500/Cisco 7600 Router Traffic Anomaly Detector Service Software Release 6.0 2G	LIC-ADM-2G-k9	–
License for Cisco Catalyst 6500/Cisco 7600 Router Traffic Anomaly Detector Service Software Release 6.0 2G (spare)	LIC-ADM-2G-k9=	–

To place an order, visit the Cisco Ordering Home Page.

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity

Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet® support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades (SAS/SASU)

For more information about support services, visit
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html.

For More Information

For more information about the Cisco Traffic Anomaly Detector Module, visit
http://www.cisco.com/en/US/products/ps6236/index.html or contact your local account
representative.