Cisco Anomaly Guard Module

The Cisco® Anomaly Guard Module is an integrated services module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that delivers a powerful and extensive solution for defending online resources against massive distributed denial-of-service (DDoS) attacks. Designed to meet the performance and scalability requirements of the largest and most demanding enterprise and service provider environments, the Cisco Anomaly Guard Module delivers unprecedented levels of protection for defeating today's increasingly complex and elusive attacks.

A single Cisco Anomaly Guard Module (Figure 1) provides the platform for processing attack traffic at multigigabit line rates. The Anomaly Guard Module employs a unique "on-demand" deployment model, diverting and scrubbing only traffic addressed to targeted devices or zones without affecting other traffic. Integrated multiple layers of defense within the Anomaly Guard Module enable it to identify and block malicious attack traffic while allowing legitimate transactions to continue flowing to their original destinations. Business operations continue uninterrupted, even in the midst of attack.

Figure 1. Cisco Anomaly Guard Module

Multiple Cisco Anomaly Guard Modules, working together in a single chassis, can incrementally scale to support many times the single module rate, delivering a scalable solution that easily adapts to large and growing enterprise and service provider environments. The Anomaly Guard Module's multiprocessor architecture can support future licensed software upgrades to enhance and improve performance for defending against massive attacks.

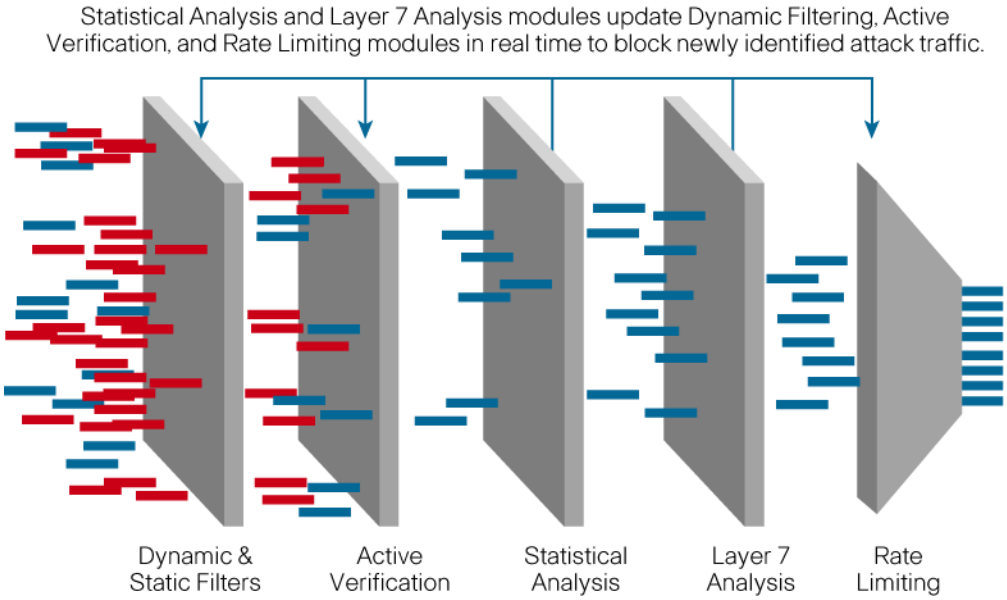
Evolving DDoS Attacks

Today's DDoS attacks are more destructive and focused than ever. These attacks can easily elude and overwhelm the most common defenses. Composed of requests that appear legitimate, massive numbers of "zombie" sources, and spoofed identities that make it virtually impossible to identify and block these malicious flows, DDoS attacks paralyze their victims and prevent them from conducting business, costing billions of dollars per year in losses—from lost transactions and customers to damaged reputations and legal liabilities.

The Cisco Anomaly Guard Module defends against all types of DDoS attacks, enabling businesses to identify and block malicious traffic without compromising their mission-critical and revenue-bearing operations. Based on a unique, patented multiverification process architecture, the Cisco

Anomaly Guard Module uses advanced anomaly recognition capabilities to dynamically apply integrated source verification and antispoofing technologies in conjunction with high-performance filtering to identify and block individual attack flows while allowing legitimate transactions to pass (Figure 2). Combined with an intuitive, graphical interface and extensive multilevel monitoring and reporting designed to provide a comprehensive overview of all attack activity, the Cisco Anomaly Guard Module delivers the most comprehensive DDoS defense for protecting business operations.

Figure 2. The Cisco Anomaly Guard Module Multiverification Process Architecture



How It Works

The Cisco Anomaly Guard Module is just one part of a complete detection and mitigation solution from Cisco that protects large enterprises, government agencies, hosting centers, and service providers from DDoS attacks. The Cisco Anomaly Guard Module provides a powerful, scalable solution that enables hosting and service providers to deliver valuable managed DDoS protection services to their subscribers. Working with the Cisco Traffic Anomaly Detector Module (or other third-party alerting systems that detect the presence of DDoS attacks), the Anomaly Guard Module performs the detailed per-flow-level attack analysis, identification, and mitigation services required to prevent attacks from disrupting network and data center operations.

When the Cisco Traffic Anomaly Detector Module identifies a potential attack, it alerts the Cisco Anomaly Guard Module to begin dynamic diversion, which redirects traffic destined for the targeted resources—and only that traffic—for inspection and scrubbing. All other traffic continues to flow directly to its intended destination, delivering a low-impact, highly reliable, and economical solution that offers easy installation.

Diverted traffic is rerouted through the Cisco Anomaly Guard Module, where it is subjected to multiple layers of scrutiny to identify and separate “bad” flows from legitimate transactions. Specific attack packets are identified and removed, while “good” traffic is forwarded to its original destination, helping to ensure that real users and real transactions always get through, and providing maximum availability.

Cisco Anomaly Guard Module Benefits

Multistage Verification

The Cisco Anomaly Guard Module's innovative blocking techniques are based on Cisco's unique multiverification process architecture, which delivers multiple interactive layers of defense to identify and block all types of attacks with unparalleled accuracy. Integrated dynamic filtering and active verification technologies, driven by a sophisticated profile-based anomaly recognition engine, enable rapid, automatic protection against all types of assault—even day-zero attacks. The Anomaly Guard Module performs detailed per-flow analysis and blocking to stop attack traffic with surgical precision, while allowing legitimate transactions to flow freely.

The anomaly recognition engine uses a baseline of normal behavior that includes thorough per-flow profiles to define the normal or expected behavior specific to each protected resource. If desired, users may enhance highly accurate default profiles with automatic site-specific learning that customizes the profile for individual devices or zones.

An additional rate-limiting feature provides a mitigation alternative to blocking, as well as protection against flash floods. Static filters, comprehensive Flex filters based on the Berkeley Packet Filter that allow the creation of a deep packet inspection filter, and bypass "whitelist" filters are also available.

The Cisco Anomaly Guard Module also features "zombie killer" capabilities that defeat all types and sizes of attacks, including those launched by compromised computers known as zombies—one of the most prevalent and difficult-to-stop DDoS attack sources today. When deployed in a clustered configuration, Anomaly Guard Modules can identify and block literally hundreds of thousands of individual zombies, delivering unparalleled levels of protection for defeating the largest botnet attacks.

Multigigabit Performance

The Cisco Anomaly Guard Module features dedicated network processors that support attack analysis and cleaning at full gigabit line rates, defending against large-scale DDoS attacks, including those launched by massively distributed attackers such as compromised zombie hosts.

With Cisco Anomaly Guard Module Software Release 5.1 or lower, each module has a performance of 1 Gbps throughput. In Release 6.0, the Cisco Anomaly Guard Module will be able to operate at 3 Gbps throughput. The higher performance is achieved by turning up additional network processors on the module and can be enabled using a software license.

Multiple Cisco Anomaly Guard Modules can be installed in a single chassis to provide incremental scaling of both packet-per-second rates and zombie defense capacities—sufficient for protecting even the largest enterprise and service provider environments against the most serious threats. These multiple modules can also be clustered to protect a single resource or zone without requiring special load balancers.

Scaling to 10-Gigabit Plus Capacity

With Cisco Anomaly Guard Module Software Release 6.0, since each Cisco Anomaly Guard Module can operate at 3 Gpbs, 10 gigabits plus performance can be achieved by clustering up to four modules in a single chassis. See the performance metrics table below for more information.

Dynamic Diversion

The Cisco Anomaly Guard Module employs a powerful on-demand scrubbing model. It is not inserted into the normal data path like traditional inline devices; rather, it uses dynamic diversion to automatically redirect traffic addressed to specific resources or zones under attack—and only that traffic—for further scrubbing. When an attack is suspected, the Anomaly Guard Module uses the Cisco Route Health Injection (RHI) protocol to insert a routing update into the supervisor engine routing tables to make the Anomaly Guard Module the next hop for any traffic destined for the targeted resource.

Once the traffic destined for the targeted device or zone has been cleaned and malicious packets blocked, legitimate transactions are forwarded on to their original destinations, helping to ensure that no critical requests are lost. By limiting diverted traffic to only those flows addressed to resources or zones currently under attack, the Cisco Anomaly Guard Module provides optimal resource utilization, transparency, and reliability for a scalable solution that can meet the needs of the largest enterprise and service provider environments. This Layer 3 insertion also enables simplified and low impact installation, as well as ease of operational maintenance and troubleshooting.

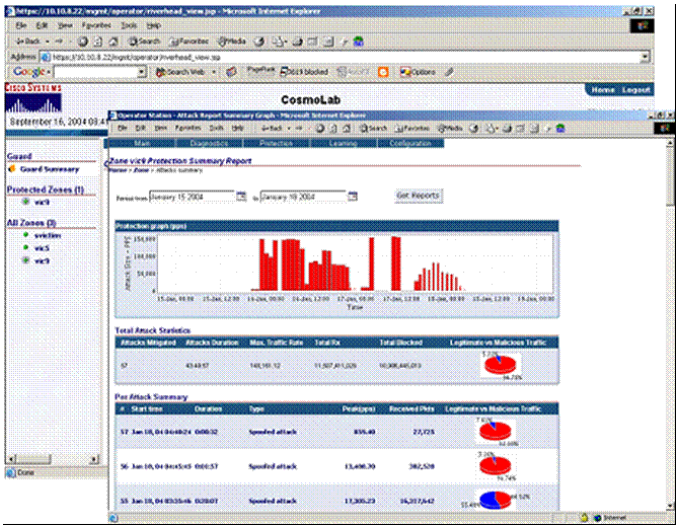
Multilevel Monitoring and Reporting

The Cisco Anomaly Guard Module features an intuitive, Web-based GUI that simplifies the policy definition, operational monitoring, and report generation processes.

Multiple monitoring and reporting levels provide network operators, security administrators, and clients with detailed real-time and historical information (Figure 5). Attack reports provide details for individual attacks, including characteristics, lists of identified zombies, and specific enforcement actions used, enabling security experts to review and tune the Cisco Anomaly Guard Module security policies.

Meanwhile, customer-level historical summaries enable service providers to easily report on successful protection against the variety, duration, and scale of attacks. In addition, an interactive mode allows users to review and approve recommended actions and policies prior to activation, providing manual control over attack responses, if desired.

Figure 3. Multilevel Monitoring and Reporting Provides Detailed Views into Real-Time and Historical Performance



The Cisco DDoS Multidevice Manager 1.0 is another management option that enables consolidating monitoring and reporting of attack information across multiple guards and detectors. More information is available at http://www.cisco.com/en/US/products/ps7020/index.html.

Cisco Anomaly Guard Module Performance Metrics

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

Table 1. Cisco Anomaly Guard Module Features

Feature	Description
Performance	**Option #1: 1 Gbps** • 1 Gbps of throughput per module • Up to 150,000 dynamic filters • 1.5 million concurrent connections • 500 protection zones (different policies and baselines [contexts]) • 30 concurrent zones in protection • Less than 1 ms latency and jitter **Option #2: 3 Gbps** • 3 Gbps of throughput per module • Up to 150,000 dynamic filters • 4.5 million concurrent connections • 500 protection zones (different policies and baselines [contexts]) • 50 concurrent zones in protection • Less than 1 ms latency and jitter
Clustering	**Option #1: Clustering 1-Gbps modules** • Uses equal-cost multipath routing • No special load balancers required • Up to 6 modules in a Cisco Catalyst 6509/Cisco 7609 chassis • Up to 10 modules in a Cisco Catalyst 6513/Cisco 7613 chassis **Option #2: Clustering 3-Gbps modules** • Uses equal-cost multipath routing • No special load balancers required • Up to 6 modules in a Cisco Catalyst 6509/Cisco 7609 chassis • Up to 10 modules in a Cisco Catalyst 6513/Cisco 7613 chassis

Cisco Anomaly Guard Module Overall Feature Summary

Table 2 lists features of the Cisco Anomaly Guard Module.

Table 2. Cisco Anomaly Guard Module Features

Feature	Description
Attack Protection	• Spoofed and non-spoofed 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 Protection	• Can operate in continuous learning and protection mode (Release 5.0 and later) • Simultaneously adjusts thresholds and protect from attacks • Switches between learning and protection modes automatically • Returns to learning mode after an attack is completed

Feature	Description
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.
Signature Extraction—Deep Packet Inspection	• Ability to find prominent patterns in the payload of captured packets • Automated algorithm analyzes packet capture to extract a signature found only in malicious packets • Content-based filter can be applied for extracted signature
Content-Based Filter	• Provides ability to look for patterns in the payload • Can define multiple content-based filters • Can be configured to either just count packets, or drop them
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 Guard 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 Anomaly Guard Module offers two distinct deployment options—integrated mode and dedicated mode.

In integrated mode, one or more Cisco Anomaly Guard 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. When an attack is detected, suspicious traffic is dynamically diverted across the Cisco Catalyst backplane to the Anomaly Guard Module for analysis and cleaning, before it is forwarded to the normal next downstream device.

In dedicated mode, the Cisco Anomaly Guard Module is installed in a dedicated Cisco Catalyst 6500 Series switch or 7600 Series router—for example, in a “scrubbing center,” where multiple Cisco Anomaly Guard Modules can be clustered for high-capacity protection. When an attack is detected in dedicated mode, affected traffic is diverted from an upstream switch or router to the dedicated Cisco Catalyst switch, using any supported Cisco IOS® Software routing protocol. Within the dedicated chassis, the Cisco Anomaly Guard Modules are the next hop for the diverted traffic forwarded by the routing process of the supervisor engine, where it is scrubbed and malicious traffic is removed. The Anomaly Guard Module returns legitimate traffic to the network, where it continues on to its original destination.

The Cisco Traffic Anomaly Detector Module can also be installed in either integrated or dedicated mode, imposing either a one- or two-step packet capture process (versus routing) to receive a copy of traffic for monitoring.

Whether in integrated or dedicated mode, when an attack is detected, the Cisco Anomaly Guard Module is typically enabled to initiate the diversion process upon activation. The Anomaly Guard Module accomplishes this by using the Cisco RHI protocol within the Cisco Catalyst chassis to dynamically insert a routing update in the supervisor engine that makes the Anomaly Guard

Module the next hop. In dedicated mode, the routing process in the supervisor engine is typically configured to redistribute the route update to the upstream device. Other diversion options include operator-entered route updates or permanent static routes.

Applications

Cisco DDoS anomaly detection and mitigation solutions can be deployed in various topologies serving both enterprise and service provider environments (Figures 4–6).

Figure 4. Cisco DDoS Anomaly Detection and Mitigation in Enterprise or Hosting Data Center

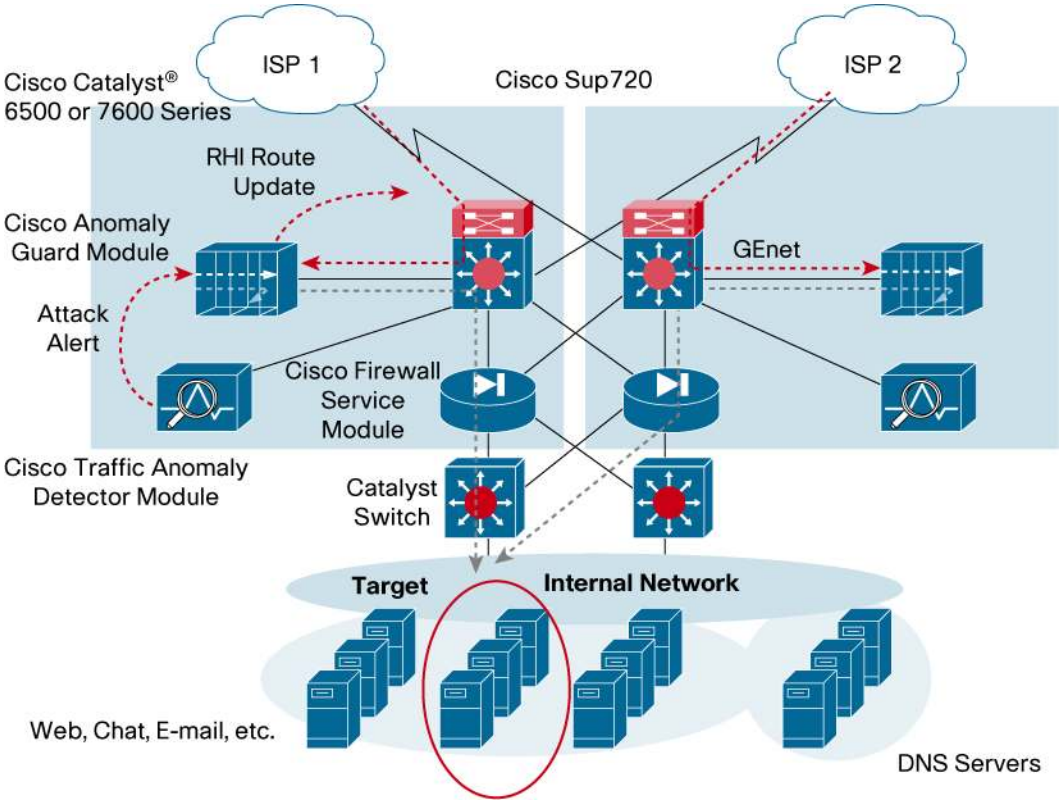


Figure 5. Cisco DDoS Distributed/Edge Protection in a Service Provider Environment

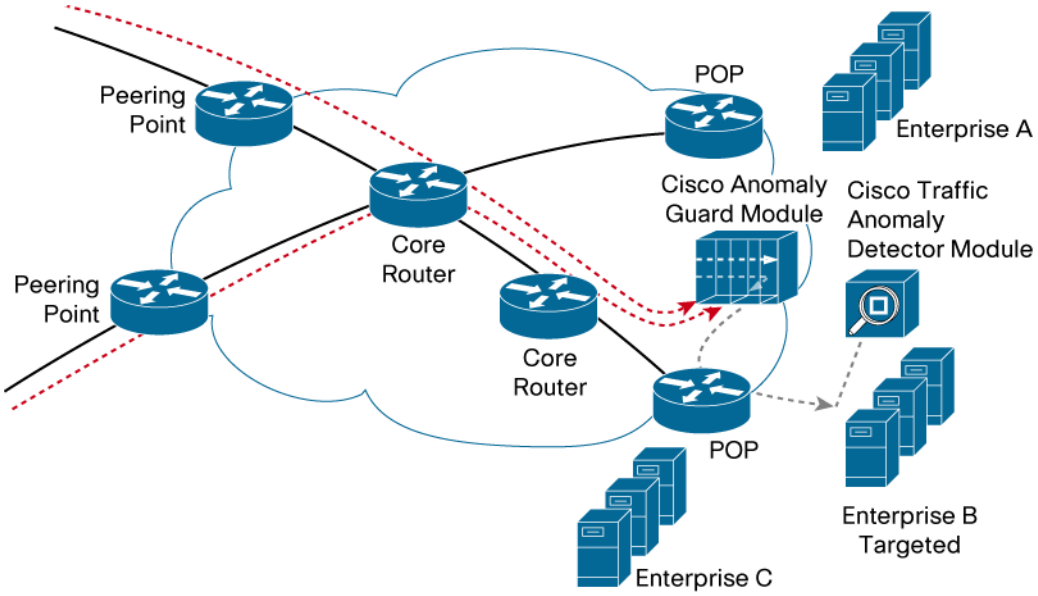
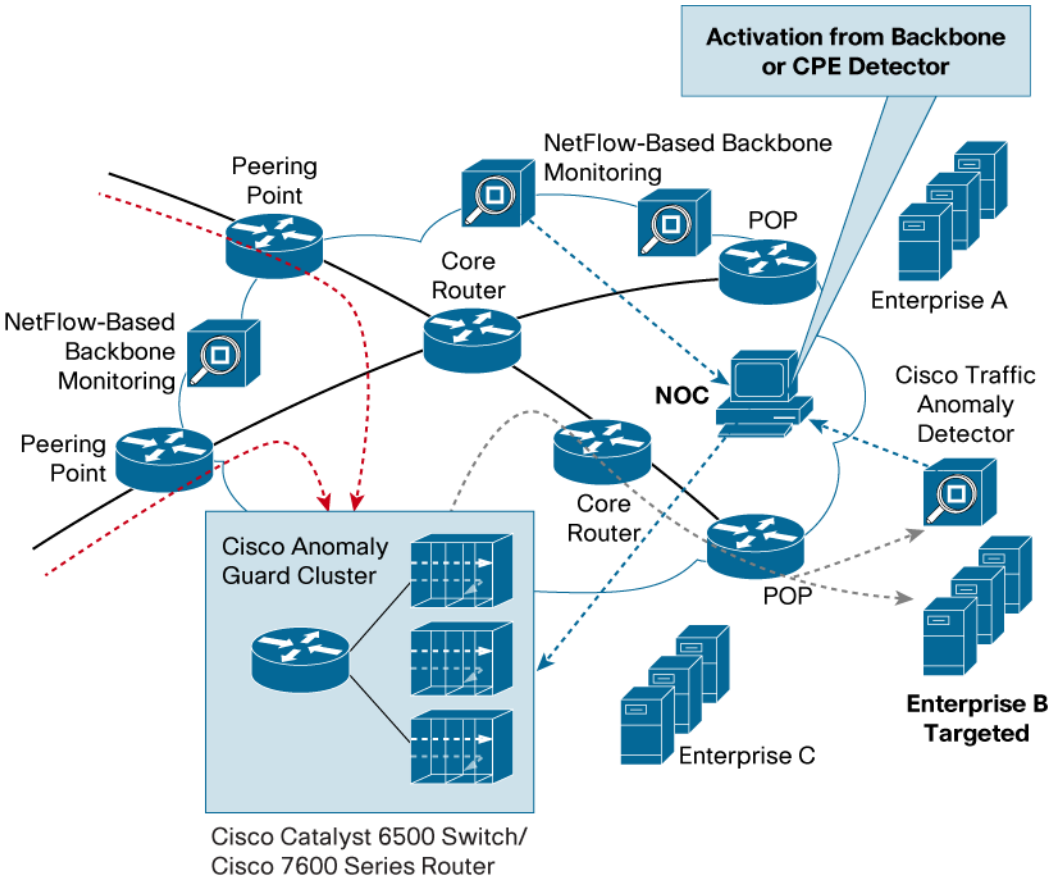


Figure 6. Cisco DDoS Anomaly Detection and Mitigation in a Centralized Provider Scrubbing Center



Benefits of Security Services Integration

Security Services Integration

The Cisco Anomaly Guard Module can be combined with other Cisco security services modules such as the Firewall Service 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 Anomaly Guard Module integrates complete DDoS protection 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 scrubbing 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. Diversion may be completely intrachassis, or may occur across devices using the full range of the supervisor engine's Cisco IOS Software routing and tunneling protocol support.

Scalability

Where high-capacity protection is required, eight modules can be installed in a single switch to support large and rapidly expanding environments. Additionally, the Cisco Anomaly Guard 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 Anomaly Guard Module maintains a powerful on-demand scrubbing architecture via routing-based dynamic diversion with robust failover protection. This capability offers ease of installation, operational reliability, and transparency not found in traditional inline solutions required for active mitigation. 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 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

Designed for service providers, hosting centers, and online enterprises, the Cisco Anomaly Guard Module does what no other DDoS mitigation solution can—help ensure uninterrupted business operations, even in the face of the most malicious assaults. This translates into a significant competitive advantage, providing uncompromised availability and unparalleled protection of the most valuable business assets.

System Requirements

- Cisco Anomaly Guard Module Software Release 5.0 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.
- Supervisor Engine 720 module that supports Multiprotocol Label Switching (MPLS) (WS-SUP720-3B or WS-SUP720-3BXL) is required to configure return injection of legitimate traffic to the supervisor engine using VPN Routing and Forwarding (VRF).
- 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 10 Cisco Anomaly Guard modules may be deployed in a single 13 slot chassis, either protecting the same destinations in load-sharing mode or different destinations. If deploying both Cisco Anomaly Guard Modules and Cisco Traffic Anomaly Detector Modules in the same chassis, a combined total of 10 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 specification of the Cisco Anomaly Guard 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)
Non Operating 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 Anomaly Guard Module.

Table 4. Ordering Information

Product Name	Part Number	SMARTnet Number
Cisco Catalyst 6500 Series/Cisco 7600 Series Anomaly Guard Module	WS-SVC-AGM-1-K9	CON-SNT-WSAGMK9
Cisco Catalyst 6500 Series/Cisco 7600 Series Anomaly Guard Module (spare)	WS-SVC-AGM-1-K9=	CON-SNT-WSAGMK9
Cisco Catalyst 6500 Series /Cisco 7600 Series Anomaly Guard Module Software Release 5.1	SC-AGM-5.1-K9	–
Cisco Catalyst 6500 Series/Cisco 7600 Series Anomaly Guard Module Software Release 6.0 1G	sc-agm-6.0-1g-k9	–
Cisco Catalyst 6500 Series/Cisco 7600 Series Anomaly Guard Module Software Release 6.0 3G	sc-agm-6.0-3g-k9	–
License for Cisco Catalyst 6500 Series/Cisco 7600 Series Anomaly Guard Module Software Release 6.0 3G	lic-agm-3g-k9	–
License for Cisco Catalyst 6500 Series/Cisco 7600 Series Anomaly Guard Module Software Release 6.0 3G (spare)	lic-agm-3g-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 Anomaly Guard Module, visit http://www.cisco.com/en/US/products/ps6235/index.html or contact your local account representative.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-386402-03 7/07