Q&A

CISCO CATALYST 6500/CISCO 7600 ROUTER ANOMALY GUARD MODULE AND CISCO CATALYST 6500/CISCO 7600 ROUTER TRAFFIC ANOMALY DETECTOR MODULE PRODUCT LAUNCH

Q. What is Cisco Systems announcing with this product release?

A. With this release, Cisco® DDoS anomaly detection and mitigation solutions are now available as services modules integrated into industry-leading Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers. These services modules complement the existing appliances by providing an additional flexible, modular approach for deployment with Cisco switching and routing, as well as other Layer 4–7 network and security services.

Q. Are these new services modules similar to the existing Cisco Guard and Cisco Traffic Anomaly Detector appliances?

A. Yes. The services modules are targeted toward the same DDoS detection and mitigation applications as the existing appliances. As with the appliances, the services modules feature separate Guard and Traffic Anomaly Detector products that can be deployed individually or together as a complete solution. They offer similar capabilities and performance as the appliances, with a few platform-driven differences. Most importantly, even while integrated into Cisco Catalyst 6500 Series switches or Cisco 7600 Series routers, the Guard maintains its powerful “on-demand” scrubbing capability via routing-based dynamic diversion, rather than as a traditional, always-inline device.

Q. Will the appliance versions of Cisco Guard and Cisco Traffic Anomaly Detector still be available?

A. The current appliance versions of the Cisco 5650 Guard XT DDoS Mitigation Appliance and the Cisco 5600 Traffic Anomaly Detector XT will continue to be sold and supported. The appliances will also continue to adopt new features, for the foreseeable future.

Q. What software releases will be supported by the new services modules?

A. The first customer shipment (FCS) versions of the Cisco Anomaly Guard Module and the Cisco Traffic Anomaly Detector Module will ship with Cisco MVP Software Release 4.0. This release is specifically designed for the services modules and is equivalent to Release 3.0(8) for the appliances, with the addition of a new packet-capture feature. The appliances currently ship with Release 3.1, and the services modules will not include Release 3.1 features—enhanced TACACS+ and Extensible Markup Language (XML) formatted reports—until the next major release. This next major release (Release 5.0) will be used on both the appliances and the services modules, and will provide the same features for both (with some platform-driven differences).

To run the new DDoS detection and mitigation services modules, users will also need to upgrade their Cisco Catalyst 6500 Series switches to Cisco IOS® Software Release 12.2(18)SXD3 (currently available) or later. The Cisco 7600 Series routers will be officially certified for these new services modules with the upcoming Cisco IOS Software Release 12.2(18)SXE.

Q. Although capabilities are essentially the same, what are the platform-driven differences mentioned above?

A. The differences include the following:

First, the services modules, which have no external interfaces, connect to the Cisco Catalyst 6500 Series Switch directly via a gigabit backplane interface. Like the appliances, however, the modules can interconnect with multiple ports for configuration flexibility.

Second, routing functions are now distributed to the industry-leading Cisco IOS router in the supervisor engine; therefore, the Anomaly Guard Module does not include an integrated router (unlike the appliance version). Intrachassis routing updates for dynamic diversion are communicated via the Cisco Route Health Injection (RHI) protocol.

Third, the services modules do not include a hard disk to support extensive local report or logging storage (again, unlike the appliance). To compensate, reporting and logging data simply need to be exported more frequently via the comprehensive commands.

One additional feature of Cisco MVP Software Release 4.0 that is unique to the services modules is a new packet-capture (TCP dump) capability. Additionally, while the services modules offer the same CLI, embedded Web-based management GUIs and Simple Network Management Protocol (SNMP) management options as the appliances, they will also be supported by upcoming releases of CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch to configure setup of features such as VLANs between modules.

Q. What are the advantages of the new modules?

A. The advantages of the new DDoS detection and mitigation services modules include the following:

Deployment flexibility:

- The modules can be installed in and connected to existing switches and routers without consuming any interface ports
- The modules can be deployed in dedicated chassis of any size
- The modules offer the full range of media options for interfaces
- The modules include high availability, as well as DC power and Network Equipment Building Standards (NEBS) options
- Cisco IOS routing provides extensive routing and tunneling protocol support for diversion and injection of traffic, which may take place completely within the chassis

Scalability:

- Eight or more modules can be installed in a single chassis to support future growth
- Platforms can support future licensed software upgrades that enhance performance

Reliability and high availability:

- Modules maintain the solution's on-demand scrubbing architecture using routing updates with failover
- Platforms offer high-availability options and Control Plane Policing for DDoS hardening

Lower cost of operation:

- Integration with routing and switching functions, as well as other services, lowers overall costs of operation
- Consistency between appliance and services module versions helps ensure compatibility moving forward

Q. What deployment options are available with the services module versions of the DDoS detection and mitigation solutions?

A. The Cisco DDoS detection and mitigation services modules offer two distinct deployment options—integrated mode and dedicated mode. The Anomaly Guard Module will be used to illustrate each mode in the following examples.

In integrated mode, Cisco Anomaly Guard modules reside in a Cisco Catalyst 6500 Series or Cisco 7600 Series chassis that is in the normal Layer 3 data path—for example, one or two modules installed in existing switches deployed in the data center. If an attack is detected, traffic is diverted across the Cisco Catalyst backplane to the Anomaly Guard Module for analysis and cleaning before being forwarded to the next regular hop after the supervisor engine.

In appliance mode, multiple Cisco Anomaly Guard modules are installed in a dedicated Cisco Catalyst 6500 Series switch or Cisco 7600 Series router chassis adjacent to an upstream switch or router—for example, a scrubbing center where Cisco Anomaly Guard modules would be clustered in a single, dedicated chassis for high-capacity applications. When an attack is detected in dedicated mode, affected traffic is diverted using any supported routing protocol from the upstream switch or router to the adjacent switch. Within the switch itself, the Cisco Anomaly Guard (or guards) are the next hop for scrubbing after the supervisor engine. Once the attack traffic has been removed, the legitimate traffic is returned to the network, where it continues on to its original destination.

The Cisco Traffic Anomaly Detector Module can also be installed in either mode, in this case implying either a one- or two-step spanning (versus routing) process to receive a copy of traffic for monitoring.

Q. Are there specific applications for which the services modules are particularly attractive?

A. As with other product suites that offer both appliances and services module offerings, customers must consider several issues to decide which is best for them. In general, however, the DDoS services modules might be particularly well suited for the following types of installations:

- Applications where only one or a few modules are required in data centers where existing chassis with available slots currently reside
- Deployments where multiple integrated services are desired, such as DDoS along with firewall, Secure Sockets Layer (SSL), and content switching services
- Deployments of high-density Anomaly Guard scrubbing centers, especially if physical density is a consideration and a dedicated "guard router" is desired to perform load-leveling services

Q. Are these solutions only applicable to the largest enterprise environments?

A. These solutions can provide DDoS protection for all enterprises, from the largest global corporations to small enterprises.

The largest enterprises can easily deploy and manage these solutions in their own data centers. However, if the bandwidth connecting the enterprise data center to the provider(s) is less than 500 Mbps to 1 Gbps, large DDoS attacks may exceed this and still result in blocked availability. Customers of this size need to consider their historical and predicted sizes of attacks. An enterprise may still want an alternative to purchasing and managing devices directly, especially where last-mile bandwidth may constrain the protection of an enterprise-deployed solution. Managed DDoS services are available from AT&T, Sprint, C&W, and many other service providers. More importantly, in addition to the benefits of outsourcing, an upstream provider-based solution protects the last-mile bandwidth and the business, even against attacks that can be several multiples larger than currently provisioned access bandwidth.

For enterprises that outsource their e-commerce or Web presence to hosting providers, there are also managed DDoS services available from Datapipe, Rackspace, The Planet, Website Source, and many other hosting providers for integrated protection.

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

204177.s_ETMG_MH_1.05

Printed in the USA