



Data Sheet

Cisco DDoS Multidevice Manager 1.0

PRODUCT OVERVIEW

The Cisco® DDoS Multidevice Manager 1.0 is a management software application that meets the growing security requirements of customer deployments that involve several guards and detectors, in geographically dispersed locations. Distributed denial of service (DDoS) attacks are increasing in severity. The Cisco DDoS Multidevice Manager 1.0 provides a powerful consolidated view of attack information across multiple guards and detectors, enabling customers to more intelligently handle them. The Cisco DDoS Multidevice Manager 1.0 application runs on a Linux server. It features an intuitive, Web-based GUI that provides easy access to a consolidated view of the size, type, and other characteristics of the attacks, both in real time and as reports that can be accessed at a later time for analysis. The DDoS Multidevice Manager 1.0 also provides the ability to distribute basic zone-level configuration to a predefined set of devices from a user-configurable master device.

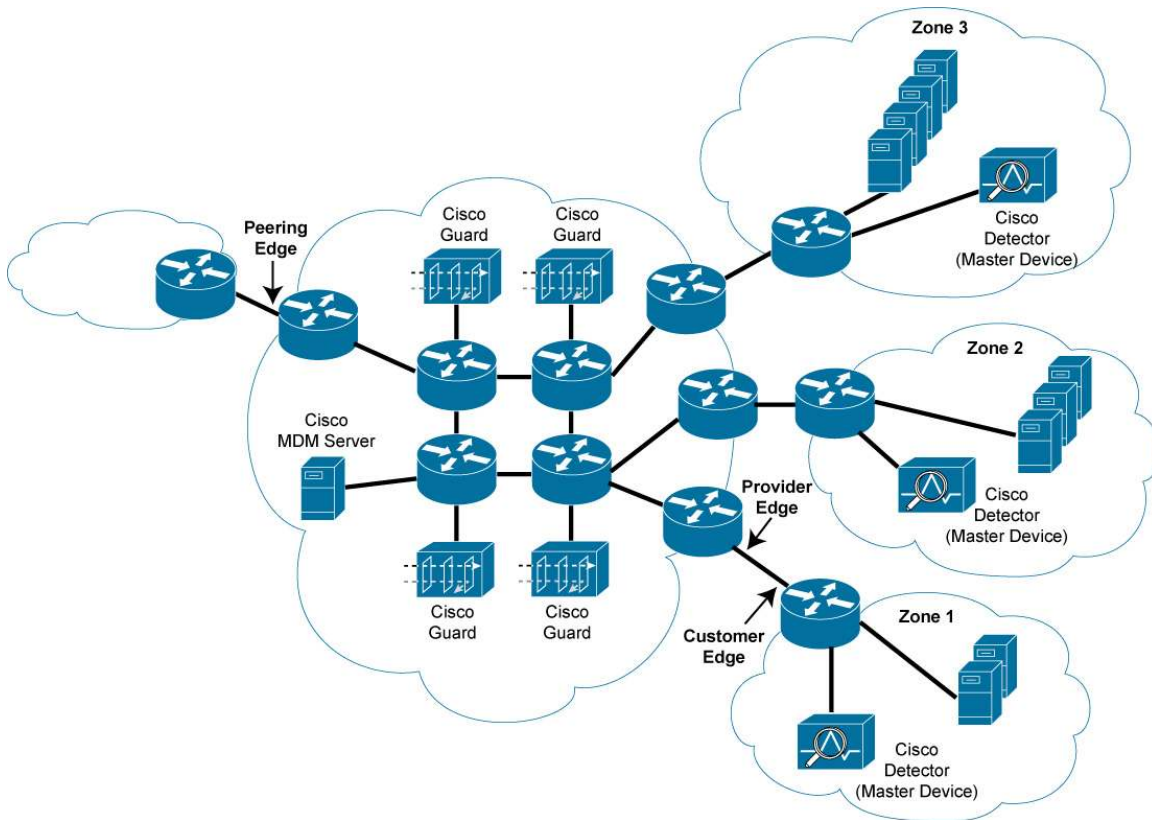
Evolution of DDoS Attacks

Today's DDoS attacks are more malicious, destructive, and distributed than ever. When these attacks are launched from different geographic locations, all attacking the same target, the attacks can be difficult to defend against.

Several customers have deployed the Cisco Guard XT as the de-facto choice to defend against these attacks, enabling businesses to defeat these attacks without compromising their mission-critical and revenue-bearing operations. However, as more of these guards are deployed in several locations, it becomes increasingly challenging to manage all the devices and consolidate information across these devices.

The Cisco DDoS Multidevice Manager 1.0 provides a way to consolidate information on counters, rates, graphs, attack reports, and event logs across all devices (both guards and detectors) in the network, significantly improving the ability of the customer to manage these devices and mitigate attacks more intelligently. Figure 1 shows the various elements in a Cisco DDoS Multidevice Manager network deployment.

Figure 1. DDoS Multidevice Manager Deployment Architecture



FEATURES AND BENEFITS

The primary features of the Cisco DDoS MultiDevice Manager 1.0 include:

- Displays a consolidated view of ongoing and past attacks on all zones
- Displays consolidated statistical information related to all zones and devices
- Creates aggregated reports
- Synchronizes zone information from one device with other devices in the network
- Activates anomaly detection on the entire set of zones on detectors in the network
- Activates zone protection (attack mitigation) on all of the guards in the network
- Activates the learning process on one or all of the zones on detectors in the network

Consolidated Information

The Cisco DDoS Multidevice Manager allows the user to monitor all DDoS detection and mitigation actions in its network from a Web GUI: all zones that are under detection, all zones that are under attack, all mitigation actions. When a zone is being protected by several guards, all information regarding the zone is consolidated to one view. Figure 2 provides a summary of all the zones that are currently under attack in the entire network, sorted by 'attack start time' (most recent in the top).

Figure 2. Networkwide Attack Summary View



Consolidated information includes:

- Aggregate zone state in all devices (indicates whether all guards detected the attack or subset)
- Aggregating all dynamic filters across all devices to one list
- Aggregating all log events from all devices to one log file sorted by time in devices level and zone level
- Aggregating counters and rates (malicious traffic and legitimate traffic across all guards; counter aggregation does not include detectors)
- Generating attack reports that consolidate information from all guards.

Synchronization of Configuration

The Cisco DDoS Multidevice Manager distributes configuration to all devices by overwriting devices' zone configuration with the master zone configuration (including all zone attributes). This process is called synchronization.

Synchronization can be triggered automatically by the following events:

- Before user-initiated protection
- Each time learning results are accepted by the user
- Configuration change (through the Multidevice Manager)

The user can choose to disable the automatic synchronization.

Conflict Resolution

Using the Cisco DDoS Multidevice Manager is the preferred way to create zones and distribute that information to the guard and detector devices in the network. The Cisco DDoS Multidevice Manager is capable of importing zone information from devices that have already been configured in the network as well.

Every time the Cisco DDoS Multidevice Manager sees a mismatch between the zone information in its database and that on the devices in the network, it will flag a conflict and provide several options to resolve that conflict.

In the conflict resolution process, the Cisco DDoS Multidevice Manager lists all:

- Zones that reside only on the devices (detectors, guards) and not in the Cisco DDoS Multidevice Manager database (or the device list for that zone)
- Zones that reside in the Cisco DDoS Multidevice Manager database as defined on specific devices but that do not appear on those devices (or some of them)
- Zones that are missing from the master device as defined in the database (a private case of the second conflict but more severe than the general case)

Or any combination of the above.

Depending on the conflict, the Cisco DDoS Multidevice Manager will recommend the appropriate resolution option; examples include associating a zone, disassociating a zone, or deleting the zone.

Figure 3 shows a sample of a conflict resolution screen.

Figure 3. Zone Configuration Conflict Resolution Screen

The screenshot displays the 'Conflicts Resolution' screen in the Cisco DDoS Multidevice Manager. The interface includes a navigation menu on the left with 'Zones (26)' expanded, showing a list of zones like 'Vic12-App1', 'Vic16-319-317', etc. The main content area has tabs for 'Main', 'Diagnostics', and 'Zones'. The 'Zones' tab is active, showing three sections:

- Exist on Unassociated Devices:** A table with columns 'Zone Name', 'ElRom', 'Jaffa17', 'Suan', 'Ortal', and 'Jaffa19'. It lists zones like 'Z215-no_SIP', 'autotest_vic11', 'IXIA250-SIP', etc., with checkboxes and 'Associate', 'Remove', and 'Rename & Create' buttons.
- Missing from Devices:** A table with the same columns, listing zones like 'test-k' and 'test-k2' with checkboxes and 'Add', 'Disassociate', and 'Delete' buttons.
- Missing from Master:** A table with the same columns, listing zones like 'test-k3' with checkboxes and 'Select Master' and 'Restore' buttons.

TECHNICAL SPECIFICATIONS

Cisco DDoS Multidevice Manager communication channels:

- Back end and devices communicate over Secure Sockets Layer (SSL).
- Event logs are sent over User Datagram Protocol (UDP) (syslog port) from all devices to the Cisco DDoS Multidevice Manager.
- The agent on the device is part of the Cisco DDoS Multidevice Manager (can be upgraded by the Cisco DDoS Multidevice Manager with no need for version upgrade in the device). The device image only contains an upgradable agent stub.
- The Cisco DDoS Multidevice Manager database is a “thin” database. It holds the list of known devices and, for each zone, the list of devices it is defined on. It does not hold zone configuration.
- The displayed zone configuration in the Cisco DDoS Multidevice Manager is the zone configuration as defined in the master device. The zone configuration in the master device is distributed to the other devices in the zone device list.

Open ports to the Cisco DDoS Multidevice Manager:

- HTTPS (443/tcp) – For Web GUI clients
- SSH (22/tcp) – Key exchange with the devices
- Syslog (514/udp) – Cisco DDoS Multidevice Manager log consolidation

Open ports from the Cisco DDoS Multidevice Manager:

- Device remote agent (1334/tcp)
- Network Time Protocol (NTP) (if installed)
- TACACS (if installed)

SYSTEM REQUIREMENTS

Hardware Requirements

	Minimum	Recommended
CPU	1 GHz	2 GHz
RAM	512 MB	1 GB
Hard Disk	2 GB	2 GB

Server software requirements:

- RedHat Enterprise Linux version 3 and 4

Prerequisite: Must NOT contain any MySQL or Tomcat installation.

Device Software Requirements:

- Cisco Guard XT: Guard Software Release 5.1(5)
- Cisco Traffic Anomaly Detector XT: Detector Software Release 5.1(5)

TECHNICAL SUPPORT SERVICES

Whether your company is a large organization, a commercial business, or a service provider, Cisco Systems® 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

For more information, visit:

http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/serv_category_home.html

ORDERING INFORMATION

The Cisco DDoS Multidevice Manager can be downloaded from Cisco.com at no charge. To download the software, visit:

<http://www.cisco.com/en/US/products/ps7020/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.com 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 © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered 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. (0601R)