



Cisco DDoS Multidevice Manager (MDM) 1.0

Product Overview

Agenda

- **Product Overview**
 - Consolidated information**
 - Synchronization of Configuration**
 - Resolving configuration conflicts**
 - Sub-Zones handling**
- **Walk through main screens**
- **Technical Specification**
 - Software architecture**
 - Communication channels**
 - Installation**

Product Overview

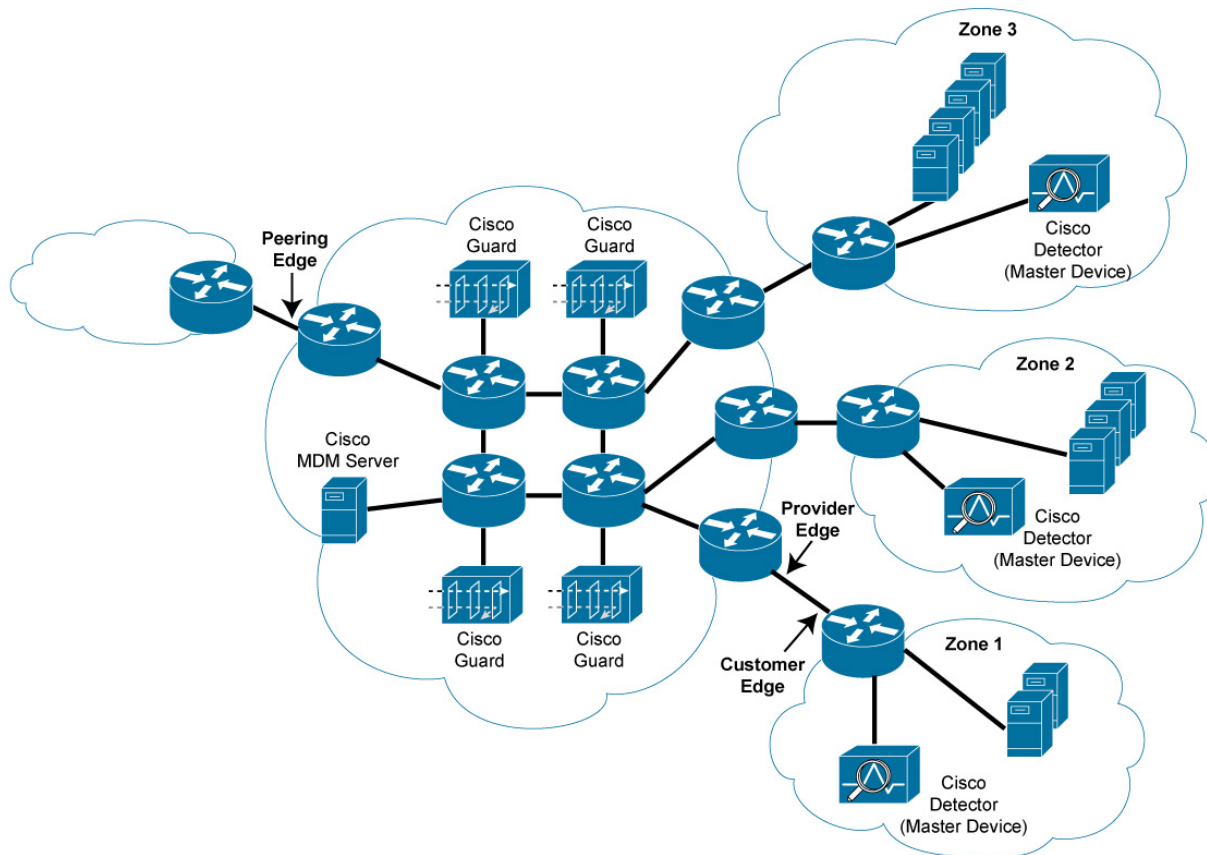
- **The DDoS MultiDevice Manager 1.0(MDM) is a software product that enables monitoring, management and reporting of several Cisco Guards and Detectors in a customer network**
- **The MDM provides a coherent and consolidated view of attack information, both in real-time and as detailed reports**
- **The MDM 1.0 runs on a Linux Server and needs to be installed on a server owned and operated by the customer**
- **MDM 1.0 requires R5.1(5) on the Guard and Detector devices**

Product Overview (Cont.)

- **The MDM GUI is based on the Web Based Management GUI that is currently available on the Guard and Detector devices**
- **The attack information like size, type and other characteristics are aggregated across devices and displayed on a single screen using a web based interface**
- **The MDM also supports the distribution of basic zone level configuration from a master device to a set of other devices (guards, detectors) on the network**
- **Consolidation is done on counters, rates , graphs, attack reports, events log and zone status across all devices.**

Product Overview

MDM Deployment Example



Sample MDM Deployment in a Network with Cisco Guards, Detectors

Consolidated Information

- **The MDM gives the user the ability to monitor all DDOS detection and mitigation actions in its network from a WEB GUI: all zones that are under detection, all zone 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.**
- **Consolidated information includes:**
 - Aggregate zone state in all devices (e.g. indicates whether all Guard 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 (e.g. malicious traffic and legitimate traffic across all Guards—counters aggregation does not include for Detectors)**
 - Generating attack reports that consolidate information from all Guards.**

Synchronization of Configuration

- **The MDM distributes configuration to all devices by overwriting devices' zone configuration with the master zone configuration (including all zone attributes)– this process is called synchronization.**
- **The synchronization can be triggered automatically by the following events:**
 - Before user-initiate protection**
 - Each time learning results are accepted by the user**
 - Configuration change (Configuration through the MDM)**
- **Synchronization can be also triggered manually from the menu**
- **Synchronization is not done on an active zone**

Synchronization of Configuration (Cont.)

- **The user can choose to disable the automatic synchronization:**

To avoid overwriting Global thresholds in scenarios where different Guards protecting the same zone see different portion of the traffic

When multiple Detectors are used and the zone has on each Detector a different remote-guards list

Resolving Conflicts in Configuration

- **The MDM assume that all zones are defined and configured through the MDM and that each zone has a master device.**
- **Zone which were not defined by the MDM are not presented till a conflict resolution is preformed**
- **Conflict resolution process in the MDM list all:**
 - Zones that reside only on the devices and not on the MDM db (or the MDM device list for that zone)**
 - Zones that reside in the db as defined on specific devices but do not appear on those devices (or some of them)**
 - Zones that are missing from the master device as defined in the db (a private case of the second conflict but more severe than the general case)**
 - Or any combination of the above**

Resolving Conflicts in Configuration (Cont.)

- **Each conflict has possible resolution options. For example:**
 - Zone that resides only on MDM db can be created on the devices it is missing from or removed from the db.**
- **One exception is the Sub-Zones (next slide)**


Sub-Zones

- **The Guard creates a sub-zone when it activates zone protection for a partial zone (a zone that does not include the complete IP address range of the source zone)**
- **The main use for sub-zone is when detector detect attack only on specific address in a subnet zones – it initiate protection only for the attacked address.**
- **MDM treats this zones differently:**
 - They can be viewed by MDM although not defined through it**
 - The conflict resolution does not take them into account.**
 - Their association to devices is not saved in the MDM db**
 - No master is defined (the MDM uses temporarily chosen master to display configuration)**

Walk through Main Screens

- **Network summary screen**
- **Device List Screen**
- **Create zone screen**
- **Zone home page**
- **Attack Report screen**
- **Conflict Resolution screen**

Network Summery screen



June 12, 2006 13:26

rhqaMDM.cisco.com

Home Enable Logout About

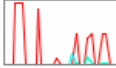
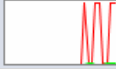
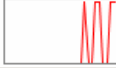


User name: admin
Privileges: admin

Network

- Network Summary
- Zones (23)**
- ✓ Vic12-App
- ✓ Vic16-J19
- ✓ Vic16-J19
- ✓ Vic16-J19
- ✓ Vic16-J19
- ✓ TestCR
- ✓ Vic11
- ✓ Vic11-1-D
- ✓ Vic12-1
- ✓ Vic12-10
- ✓ Vic12-2
- ✓ Vic12-3
- ✓ Vic12-4-1
- ✓ Vic12-5-4
- ✓ Vic12-6-1
- ✓ Vic12-7-5
- ✓ Vic12-9
- ✓ Vic12-Dac
- ✓ Vic12-J19
- ✓ Vic12-J19
- ✓ Vic16

Main
Diagnostics
Zones

Network Summary

Zone	Attack start time	#DF	#PF	Legitimate rate (bps)	Malicious rate (bps)	Receive Rate (bps)	
Vic12-App	Jun 12, 13:18:36	3	N/A	2060772	1028941	1356067	
Vic16-J19-J17...	Jun 12, 13:16:47	1	N/A	0	205804	N/A	
Vic16-J19-J17...	Jun 12, 13:16:45	1	N/A	0	205370	N/A	
Vic16-J19-J17...	Jun 12, 13:16:42	1	N/A	0	205031	N/A	
Vic16-J19-J17	Jan 01, 02:00:00	0	N/A	N/A	N/A	697348	

Network Summary screen (cont.)

- **Display all zones that are currently under attack in the entire network, sorted according attack start time (most recent in the top)**
- **For each zone it display basic statistics (number of dynamic filters, traffic statistics)**
- **Clicking on a zone line links you to the zone home page**

Device List screen

The screenshot displays the Cisco MDM web interface. At the top left is the Cisco Systems logo. The top center shows the URL **rhqaMDM.cisco.com**. On the top right, there are navigation links: **Home Enable Logout About**. Below the header, the date and time are shown as **June 12, 2006 13:22**, and the user information is **User name: admin Privileges: admin**.

The left sidebar contains a **Network** section with a **Network Summary** link and a **Zones (23)** list. The zones listed include Vic12-App, Vic16-J19, Vic16-J19, Vic16-J19, Vic16-J19, TestCR, Vic11, Vic11-1-D, Vic12-1, Vic12-10, Vic12-2, Vic12-3, Vic12-4-1, Vic12-5-4, Vic12-6-1, Vic12-7-5, Vic12-9, Vic12-Dac, Vic12-J19, Vic12-J19, and Vic16.

The main content area has three tabs: **Main**, **Diagnostics**, and **Zones**. The **Zones** tab is active, showing the **Devices List** screen. Below the breadcrumb **Home > Device List**, there is a table of devices:

<input type="checkbox"/>	Hostname	IP Address	Type	State	Zones	Active Zones	Attacked Zones	#DF	Mem usage	Total rate (pps)
<input type="checkbox"/>	ElRom	10.56.220.61	Guard	Established	20	1	1	1	2.57%	3598
<input type="checkbox"/>	Jaffa17	10.56.36.177	Guard	Established	13	3	3	3	2.53%	1073
<input type="checkbox"/>	Suan	10.56.36.200	Guard	Established	34	0	0	0	2.67%	1
<input type="checkbox"/>	Ortal	10.56.220.62	Detector	Established	18	1	1	1	.97%	4159
<input type="checkbox"/>	Jaffa19	10.56.220.19	Detector	Established	12	1	1	0	.47%	4169

Below the table, there are four action buttons: **Add**, **Delete**, **Ping**, and **Exchange Cert.**

Device List screen (Cont.)

- **Display all devices that reside on the MDM database (defined manually by the user)**
- **Display utilization information on each device**
- **Device type (whether the device is a Guard or Detector) is retrieved at the first connection**
- **Device states:**
 - Initializing – while initiating connection (frequent during upgrade)**
 - Establish – connection established with device (most common state)**
 - Disconnected – Fail to create session with device**
 - Suspended – User disabled communication with the device**
- **Clicking on device enables to change device parameters**

Create zone screen

CISCO SYSTEMS
June 12, 2006 13:37

rhqaMDM.cisco.com

Home Enable Logout About

User name: admin
Privileges: admin

Main Diagnostics Zones

Create Zone
Home > Zones List > Create Zone

Zone Form

Name: test

Zone Template: GUARD_DEFAULT

IP Address: 2.2.2.2 IP Mask: 255.255.255.255

Devices and Master:

<input type="checkbox"/>	Hostname	IP Address	Type	State	Master	#DF	Mem usage	Legitimate rate	Malicious rate
<input checked="" type="checkbox"/>	ElRom	10.56.220.61	Guard	Establi...	<input checked="" type="radio"/>	1	2.47%	0	1
<input type="checkbox"/>	Jaffa17	10.56.36.177	Guard	Establi...	<input type="radio"/>	3	2.52%	0	4997
<input checked="" type="checkbox"/>	Suan	10.56.36.200	Guard	Establi...	<input type="radio"/>	1	2.48%	1	N/A
<input type="checkbox"/>	Ortal	10.56.220.62	Detector	Establi...	<input type="radio"/>	0	.88%	0	1358
<input type="checkbox"/>	Jaffa19	10.56.220.19	Detector	Establi...	<input type="radio"/>	3	.43%	0	1372

OK Clear Cancel

Create zone screen (Cont.)

- **The user should choose in which devices the zone should be created**
- **Choosing the devices for a zone depends on various parameters:**


The network architecture (e.g. whether the attack traffic will arrive to several Guards)

The expected attack capacity (if attacks larger than 1G are expected than several Guards should be used)

Load sharing scheme (each guard can protect concurrently on 30 zones)

- **One of the devices must be chosen as a master device**
- **If there is a detector in the device list the Detector must be the master**

Zone home page



June 12, 2006 13:16

rhqaMDM.cisco.com

Home Enable Logout About

User name: admin
Privileges: admin

Main Diagnostics Activation Learning Configuration

Network

Network Summary

Zones (20)

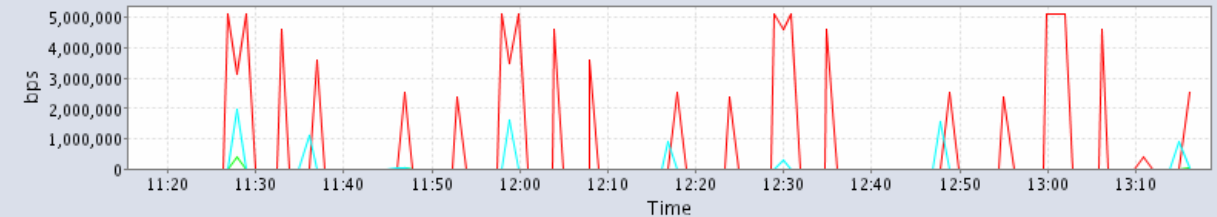
- ✓ Vic12-Appl
- ✓ Vic16-J19-J1
- ✓ TestCR
- ✓ Vic11
- ✓ Vic11-1-Det
- ✓ Vic12-1
- ✓ Vic12-10
- ✓ Vic12-2
- ✓ Vic12-3
- ✓ Vic12-4-1M
- ✓ Vic12-5-4M
- ✓ Vic12-6-128
- ✓ Vic12-7-512
- ✓ Vic12-9
- ✓ Vic12-Dad4
- ✓ Vic12-J19-1
- ✓ Vic12-J19-5
- ✓ Vic16
- ✓ Vic16-Det
- ✓ Vic16x40

Zone Vic12-Appl (automatic) - Under Attack/Under Detection

Home > Zone

Deactivate Report

Traffic Rate - bps



Legitimate rate:	Min.: 0.0	Max.: 411,834.0	Avg.: 5,567.85	Cur.: 759.0
Malicious rate:	Min.: 0.0	Max.: 5,119,898.0	Avg.: 1,037,732.54	Cur.: 83,200.0
Master Receive rate:	Min.: 0.0	Max.: 1,971,971.0	Avg.: 71,162.98	Cur.: 646.0

Zone status

<p>Detectors State: learning(0) under detection(1) attack detected(0)</p> <p>Guard State: learning(0) under protection(2) under attack(2)</p>	<p>Active Dynamic filters: 1</p> <p>Pending Dynamic filters: 0</p> <p>Last attack time: Jun 12, 13:14:38</p> <p>Activation time: N/A</p>
---	--

Zone home page (cont.)

- **Zone status bar – the status is displayed as <Guards aggregated states> /<Detectors aggregate states>**

If the zone is active only on subset of the Guards or Detectors then the state contains “(S)” to indicate only subset of the devices are in that state


A state combination that is erroneous, where some of the Guards are under attack and other in learning state, is marked with exclamation mark

- **The rate graphs contains three lines:**
 - The received traffic as seen in the master Detector (blue line). There is not rate/counters aggregation across Detectors if several Detectors are defined.**
 - Legitimate traffic aggregated across all Guards (green line)**
 - Malicious traffic aggregated across all Guards (red line)**

Zone Home page (Cont.)

- **Dynamic filters are aggregated across all devices**
- **Events are aggregated across all devices**

Attack Report Screen



rhqMDM.cisco.com

June 12, 2006 10:53

Home Enable Logout About

User name: admin
Privileges: admin

Main
Diagnostics
Activation
Learning
Configuration

Zone Vic12-App1 (automatic) - Under Attack/Under Detection

Home > Zone > Reports > Attack Report

Attack Report #691

Attack Start Time: Jun 12, 06 10:43:21
 Attack End Time: Jun 12, 06 10:47:24
 Attack Duration: 0:04:03
 Active Devices: ElRom, Suan

Statistics Units:

i Show details for all events

Attack Statistics

	Total	Max. rate	Avg. rate	%		Total	Max. rate	Avg. rate
Received	542,002	4,982.56	2,230.46	0.00%	Dynamic filter	0	0.00	0.00
Forwarded	44,017	1,311.82	181.14	8.12%	Malformed	0	0.00	0.00
Replied	495,874	4,879.78	2,040.63	91.49%	Flex filter	2,111	19.44	8.69
Dropped	2,111	19.44	8.69	0.39%	User filter	0	0.00	0.00
					Spoofed	495,874	4,879.78	2,040.63
					Rate limiter	0	0.00	0.00

Detected Anomalies

#	Start Time	Duration	Type	Devices	Triggering Rate	Rate % thresh.	Anomaly Flow	Details
1	Jun 12 10:43	0:03:03	HTTP	ElRom, Suan	5,494.76	588.18%	dstPort=80 protocol=6 type=syns	i

Mitigated Attacks

#	Start Time	Duration	Attack Type	Devices	Triggering Rate	Rate % thresh.	Anomaly Flow	Action Flow	Dropped /Bounced	Details
1	Jun 12 10:43	0:02:10	user defined/Flex content filter	ElRom, Suan	19.44	N/A			2,111	
2	Jun 12 10:43	0:02:10	spoofed/Tcp syn (basic)	ElRom, Suan	4,879.78	N/A	protocol=6	protocol=6	495,874	

Network

Network Summary


Zones (23)

- ✓ Vic12-App1
- ✓ Vic16-J19-J17
- ✓ Vic16-J19-J17_192
- ✓ Vic16-J19-J17_192
- ✓ Vic16-J19-J17_192
- ✓ TestCR
- ✓ Vic11
- ✓ Vic11-1-Det
- ✓ Vic12-1
- ✓ Vic12-10
- ✓ Vic12-2
- ✓ Vic12-3
- ✓ Vic12-4-1M
- ✓ Vic12-5-4M
- ✓ Vic12-6-12BK
- ✓ Vic12-7-512K
- ✓ Vic12-9
- ✓ Vic12-Dad4
- ✓ Vic12-J19-17
- ✓ Vic12-J19-5u
- ✓ Vic16
- ✓ Vic16-Det
- ✓ Vic16x40

Attack Report Screen (cont.)

- **The attack report list all Guards that participate in detection and mitigation of the zone attack**
- **Attack counters/rates statistics is aggregated across all Guards**
- **All mitigation actions are aggregated across all Guards**

Conflict Resolution Screen



June 12, 2006 13:33

rhqMDM.cisco.com

Home Enable Logout About

User name: admin
Privileges: admin

Network

- Network Summary
- Zones (26)
 - ✓ Vic12-App1
 - ✓ Vic16-J19-J17
 - ✓ Vic16-J19-J17_192
 - ✓ Vic16-J19-J17_192
 - ✓ Vic16-J19-J17_192
 - ✓ test-k
 - ✓ test-k2
 - ✓ test-k3
 - ✓ TestCR
 - ✓ Vic11
 - ✓ Vic11-1-Det
 - ✓ Vic12-1
 - ✓ Vic12-10
 - ✓ Vic12-2
 - ✓ Vic12-3
 - ✓ Vic12-4-1M
 - ✓ Vic12-5-4M
 - ✓ Vic12-6-128K
 - ✓ Vic12-7-512K
 - ✓ Vic12-9
 - ✓ Vic12-Dad4
 - ✓ Vic12-J19-17
 - ✓ Vic12-J19-Su
 - ✓ Vic16
 - ✓ Vic16-Det
 - ✓ Vic16x40

Main
Diagnostics
Zones

Conflicts Resolution

Home > Conflicts Check

Exist on Unassociated Devices

<input type="checkbox"/>	Zone Name	ElRom	Jaffa17	Suan	Ortal	Jaffa19
<input type="checkbox"/>	Z215-no_SIP			X		
<input type="checkbox"/>	autotest_vic11			X		
<input type="checkbox"/>	IXIA250-SIP			X		
<input type="checkbox"/>	Z215-no_SIP2			X		
<input type="checkbox"/>	IXIA250			X		
<input type="checkbox"/>	Conflict-319					X
<input type="checkbox"/>	SIP215			X		
<input type="checkbox"/>	llat-test	X		X	X	
<input type="checkbox"/>	IXIA4567			X		

Associate Remove Rename & Create

Missing from Devices

<input type="checkbox"/>	Zone Name	ElRom	Jaffa17	Suan	Ortal	Jaffa19
<input type="checkbox"/>	test-k			X		
<input type="checkbox"/>	test-k2			X		

Add Disassociate Delete

Missing from Master

<input type="checkbox"/>	Zone Name	ElRom	Jaffa17	Suan	Ortal	Jaffa19
<input type="checkbox"/>	test-k3			X		

Select Master Restore

Conflict Resolution Screen (Cont.)

- **The conflicts are grouped according to the conflict type**
- **Only zones with conflicts appears**
- **Sub zones are ignored**

Technical Specifications

- **Software Architecture**
- **Communication Channels**
- **Installation**

Software Architecture (cont.)

- **Communication between back-end and devices is over SSL**
- **Logs event are sent over UDP (syslog port) from all devices to the MDM**
- **The Agent (AKA RA) on the Device is part of the MDM (can be upgraded by the MDM with no need for version upgrade in the device). The Device image only contains an upgradeable agent stub.**
- **The MDM database is a “thin” database. Holds the list of known devices and for each zone the list of devices it is was defined on. Does not hold zones configuration.**
- **The displayed zone configuration in the MDM is the zone configuration as defined in the master. The zone configuration in the master device is distributed to the other devices in the zone device list.**

MDM Communication Channels

- **Open ports to the MDM**
 - https (443/tcp) – for WEB GUI clients**
 - SSH (22/tcp) – Key exchange with the devices**
 - Syslog (514/udp) – MDM log consolidation functionality**
- **Open ports from the MDM**
 - Device Remote Agent (1334/tcp)**
 - NTP (if installed)**
 - TACACS (if installed)**

Installation

- **HW requirements:**

minimum: CPU 1GHz, RAM 512M, hard disk 2G

Recommended: CPU 2GHz, RAM 1GB, hard disk 2G

- **Server Software requirement:**

RedHat Enterprise Linux version 3 and 4

“Clean” machine – no mySQL, no tomcat installed

- **Device Software Requirements: R5.1(5) or later**

- **Device should be configured in the MDM and for each device the user should initiate a key exchange between the MDM and the device (through the MDM GUI)**

- **Conflict resolution is required after installation to integrate already defined zones**

CISCO SYSTEMS

