



CYBEROAM CENTRAL CONSOLE



Central Security Control for MSSPs and Distributed Enterprises

Distributed Threat Control

Zero-hour threats that spread to millions of computers within hours, outpacing traditional security solutions are threatening enterprise networks. Blended attacks in the form of viruses, worms, Trojans, spyware, phishing, pharming are compromising networks through entry at the weakest points of enterprise infrastructure - remote and branch offices - that are generally not equipped to handle complex threats.

While managing geographically distributed networks, the security infrastructure of large enterprises and Managed Security Service Providers (MSSPs) typically involves multiple devices at distributed locations. This delays attack response across networks while offering poor visibility into remote network activity. The fact that remote offices and managed client networks are not staffed with qualified technical manpower that can handle attacks instantly compounds the delay.

At the same time, enterprises struggle to implement, monitor and control a single enterprise-wide security policy, raising security, productivity and legal issues. Hence, the ability to identify impact and take rapid enterprise-wide action is a pre-requisite to enforce distributed security. In the case of MSSPs, the ability to implement a broad security policy across multiple clients can simplify operations while maintaining high security levels across client networks

Cyberoam Centralized Threat Management

Cyberoam Central Console (CCC) with its centralized management and control offers coordinated defense against zero-hour and blended threats across distributed networks. It enables enterprise-wide implementation of corporate Internet policy, ensuring high productivity and security. Through enforcement of global policies for Firewall, Intrusion Detection and Prevention and Anti-Virus scanning, it supports the creation and implementation of an enterprise-wide security policy that strengthens branch and remote office security while lowering operational complexity.

Cyberoam lowers the operating cost of deploying, upgrading and maintaining multiple devices in the enterprise, offering complete control over distributed networks from the central office or the Security Operations Center (SOC) of MSSPs. CCC supports Cyberoam CR25i, CR50i, CR100i, CR250i, CR500i, CR1000i and CR1500i.

Identity-Based Policy Implementation

The Cyberoam Central Console enables administrators to push work-profile based security policies to remote locations thus allowing implementation of enterprise wide standard security policy. This fully leverages Cyberoam's unique user identity-based security approach.

The Cyberoam Central Console also enables single point implementation of compliance measures for large enterprises and MSSPs. For example, it enables the implementation of a single CIPA compliance policy for all school districts and libraries under MSSP contract.

Features	Benefits
Centralized configuration and control	<ul style="list-style-type: none"> Reduces operational complexity and deployment time Minimizes errors and lowers administration cost
Device-Group based Roles	<ul style="list-style-type: none"> Enables the MSSPs to have different personnel for managing different customer deployments
Centralized monitoring and control	<ul style="list-style-type: none"> Enables real-time visibility of threat summary and trends for instant action
Centralized policy definition and enforcement	<ul style="list-style-type: none"> Centralized definition and real-time enforcement of security policies and custom IDP signatures enables immediate action against zero hour threats
Web based Interface and Dashboard	<ul style="list-style-type: none"> Ease of use with view of multiple devices and network status at a glance

Centralized Device Management

Cyberoam Central Console's centralized Web GUI enables remote management of all distributed Cyberoam security devices including policy management, compliance enforcement, monitoring and control. Cyberoam's easy-to-deploy and configure central console manages the task of configuring remote groups, devices, users and roles in easy steps.

Easy Configuration using Web Interface

Policy Enforcement for Compliance

Internet Access Policy Name	Default Strategy	Description	Apply
Accounting & Finance Department	Deny	to allow accounting / financial / my company websites.	Apply
Admin, Legal & Account Group policy	Deny	This is applicable for Admin, Legal and Account Departments jointly.	Apply
Administrators policy	Allow	Applicable to all system, network and data center administrators.	Apply
Allow All	Allow	Allow all Internet Access	Apply
Child Protection Act	Allow	Internet Access Policy for Children's Internet Protection Act	Apply
Categories policy	Allow	Applicable for Categories Department	Apply
Corporate Common access policy	Allow	Default policy applies to default group.	Apply
Deny AOL and ICQ chat only	Allow	Deny AOL and ICQ Chat Only	Apply
Deny HTTP Upload	Allow	Deny HTTP Upload	Apply
Deny all	Deny	Deny Internet Access	Apply
Deny all chat	Allow	Deny All Chat	Apply
Deny all chat and mail	Allow	Deny All Chat and Mail	Apply

Policy flexibility to support business requirements

Create and implement enterprise-wide policies that are in accordance with corporate human resource guidelines to maintain the same levels of productivity and security measures across enterprise. MSSPs can apply differential policies across the different enterprises whose security they manage.

Centralized Policy Definition and Enforcement

Instant enforcement of security policies in response to zero hour threats

Create and enforce Firewall rules, custom IDP policies using custom signatures to protect your enterprise from the latest threats, update remote Cyberoam devices from the Cyberoam Central Console and protect branch, remote or distributed offices with the same technical competency as the central location.

Centralized Firewall rule definition

ID	Enable	Source	Identity	Action	SNAT Policy	IAP	Manage	Apply	Remove
LAN - WAN (3 Rules)									
52	<input checked="" type="checkbox"/>	voipdevice1	-	Accept	MASQ	-	<input type="checkbox"/>	Apply	Remove
2	<input checked="" type="checkbox"/>	Any Host	Any Live User	All Services	Accept	MASQ	User's Pol...	Apply	Remove
1	<input checked="" type="checkbox"/>	Any Host	-	All Services	Drop	-	<input type="checkbox"/>	Apply	Remove
DMZ - WAN (2 Rules)									
51	<input checked="" type="checkbox"/>	mailserver	-	SMTP	Accept	MASQ	<input type="checkbox"/>	Apply	Remove
50	<input checked="" type="checkbox"/>	Any Host	-	All Services	Drop	-	<input type="checkbox"/>	Apply	Remove
LAN - LOCAL (1 Rules)									
*	<input checked="" type="checkbox"/>	Any Host	-	Local ACLs	Accept	-	<input type="checkbox"/>	Apply	Remove

Custom IDP Signatures

Create custom IDP signatures and enforce them across the distributed networks for instant enterprise-wide security response to emerging threats.

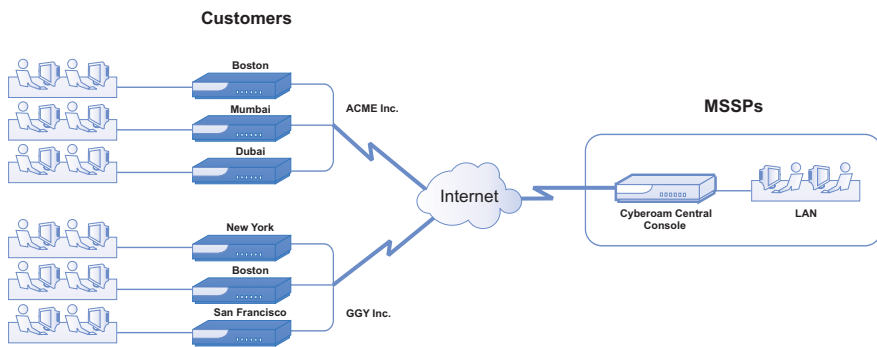
IDP Custom Signature Name	Description	Apply	Del
yahoo_adodb_exploit_1	Signature for yahoo Adodb exploit	Apply	<input type="checkbox"/>
yahoo_adodb_exploit_2	Signature for yahoo Adodb exploit variant	Apply	<input type="checkbox"/>
wmf_exploit	Signature for windows wmf exploit	Apply	<input type="checkbox"/>

Instant enterprise-wide security visibility

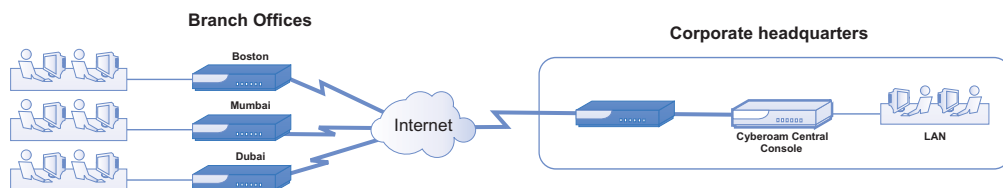
Cyberoam Central Console enables central monitoring, ensuring instant action that provides uninterrupted security across networks. Monitor the remote and distributed offices through instant visibility into their network status. Take instant action by real time enforcement of security and firewall policies to control the attack

The screenshot displays the Cyberoam Central Console interface. It features a 'Group Level Dashboard' with metrics for 'General' and 'USBranchez' groups, including Connectivity (100%), IAP Trend (100%), IDP Analysis (100%), SPAM Mails (100%), Subscription (100%), System Health (100%), CMC Version (100%), and Virus Attack (100%). A 'Device Level Dashboard' provides a detailed view of a specific device, listing metrics like IAP Trend, IDP Threat, Spam Mail, Subscription, Sys Health, Virus Attack, and Version. A 'Device Summary' panel on the right provides detailed information for the device IP 192.168.15.99, including its name (Ahmedabad), IP address, key, model (CR250), deployment mode (Route), version (9.4.2.0), and connection date (May 02, 2007 00:25:02). It also shows gateway connectivity, virus attack statistics (e.g., HTTP Virus at 0%), SPAM Mails (0%), IDP Analysis (0 threats in last 5 minutes), system health (CPU 0%, Memory 44%, Disk Usage 0%), and subscription status (29 days left for various filters).

Cyberoam Central Console Deployment- MSSP



Cyberoam Central Console Deployment- Large Enterprise



Technical Specifications	CCC 15	CCC 50	CCC 100	CCC 200
Interfaces				
CPU	Intel ULV Celeron 650MHz	Pentium 42.8GHz with 533MHz FSB and 512K L2 Cache	Pentium 42.8GHz with 533MHz FSB and 512K L2 Cache	Intel Xeon 3.2GHz with 1MB L2 Cache 1
Chipset	VIACLE266	Intel845GV	Intel845GV	Intel E7520
Memory	512MB DDRSDRAM	1GB RAM (512MB*2)	2GB RAM (1GB*2)	2GB RAM(1GB*2), DDRII ECC & REG
10/100 Ethernet ports	4	2	2	8
10/100/1000 GBE Ports	-	2	-	2
Console ports (RJ45)	-	-	-	2
SFP (Mini GBIC) Ports	-	-	-	2
COM port	2	2	2	2
USB ports	4	4	4	2
Dimensions				
Height	1.72 inches	1.72 inches	1.72 inches	3.46 inches
Width	16.8 inches	16.8 inches	16.8 inches	16.7 inches
Depth	9.1 inches	13.4 inches	13.4 inches	20.9 inches
Power				
Input Voltage	110 - 240VAC	110 - 240VAC	110 - 240VAC	90 - 264VAC
Redundant Power Supply	-	-	-	Yes
Environmental				
Operating Temperature	0 to 40 °C	0 to 40 °C	0 to 40 °C	0 to 40 °C
Storage Temperature	-20 to 80 °C	-20 to 80 °C	-20 to 80 °C	-20 to 80 °C
Relative Humidity (Non condensing)	10 to 90%	10 to 90%	10 to 90%	10 to 90%
Cooling system (40mm Fan)	2	2	4	4
No. of CR Devices Supported	15	50	100	200



Feature Specifications

System Management

- Secure Web Based User Interface
- Command line Interface
- Secure Command Shell (SSH)

Administration

- Multi-level access rights and privileges
- Configure Basic System Settings
- Restore Factory Default System Settings
- Backup and Restore option
- Audit Log

- Device Management
 - Add/Delete Devices
 - Device grouping
- Distributed Administration
 - Local Administrator Accounts
 - Device and Device Group Administrator Accounts

Centralized Remote Management

- Configure and Manage
 - Individual Devices
 - Device Groups
- Global Enforcement
 - Firewall rules and parameters
 - Host and Host Group
 - Service
 - Schedule
 - Internet Access Policy
 - Bandwidth Policy
 - IDP Policy and Custom Signatures
 - Anti-virus and Anti-spam policy
 - Custom Web Categories
 - Custom File Type Categories
 - Custom Application Category

Configuration Management

- Backup and Restore of Configuration
- Signature updates

Communication

- SSL RC4 128bit Encryption
- Mutual Authentication

Real-time Monitoring

- Dashboard
- Monitor by
 - Devices
 - Device Groups
- Track System health
- Monitor IDP Threats
- Mail and HTTP Virus attacks monitoring
- Monitor and track spam
- Web Surfing Trends
- Device Connectivity status

- View Device Information
 - Deployment mode
 - Network details
 - Appliance key and Model
 - Software Version
 - Subscription details

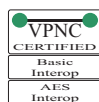
High Availability

Authentication

- Radius/AAA

Compliance

- CE
- FCC



USA - Tel: +1-978-465-8400, Fax: +1-978-293-0200

India - Tel: +91-79-66065777 | Toll Free - 1-800-301-00013

Copyright © 1999 – 2008 Ellitcore Technologies Ltd. All rights reserved. Cyberoam and Cyberoam logo are registered trademark of Ellitcore Technologies Ltd. Although Ellitcore has attempted to provide accurate information, Ellitcore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Ellitcore has the right to change, modify, transfer or otherwise revise the publication without notice.

