



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.

For geographically distributed networks of large enterprises and Managed Security Service Providers (MSSPs) that provide multiple security 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 do not have qualified technical manpower to handle attacks compounds the delay. All the same, enterprises struggle to implement, monitor and control a uniform 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 enforcing distributed security. For MSSPs, the ability to implement a broad security policy across multiple clients simplifies operations while maintaining high security across client networks.

Cyberoam Centralized Threat Management

Cyberoam Central Console (CCC) offers coordinated defense against zero-hour and blended threats across distributed networks. It enables centralized, enterprise-wide implementation of corporate Internet policies. Through configuration, enforcement of global policies as well as traffic scanning for Firewall, Intrusion Prevention System, Content-Filtering, Anti-virus and Anti-spam, CCC supports the configuration of an enterprise-wide security policy that strengthens branch and remote office security while lowering operational complexity.

CCC 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 CR15i, CR25i, CR25ia, CR35ia, CR50i, CR50ia, CR100i, CR100ia, CR200i, CR300i, CR500i, CR1000i, Cr1500i.

Identity-Based Policy Implementation

The CCC 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 CCC also enables single point implementation of compliance measures for large enterprises and MSSPs. It is compliant across the board with CIPA, HIPAA, GLBA, PCI-DSS and SOX.

Alerts and Audit Logs

The CCC sends instant email alerts on device configuration changes taking place across distributed networks. This enables the administrator to take corrective actions for changes in device connectivity status, unchanged default passwords, change in CCC update repository, etc. The CCC also provides audit logs to support configuration and policy changes on distributed CR devices, support addition and removal of devices, create, modify and delete policies and rules and keep track of successful/unsuccessful log-in attempts. To view the audit log, administrators use appropriate data filters.

Features	Benefits
Centralized Configuration and Control Policy Definition and Enforcement	<ul style="list-style-type: none"> Reduces operational complexity and deployment time Minimizes errors and lowers administration cost Enables immediate action against zero-hour threats
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 IPS 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
Email alerts and audit logs	<ul style="list-style-type: none"> Email alerts enable the administrator to get notification on issues due to distributed appliances and take instant, corrective action. Audit logs provide investigative analysis as well as keep track of historical activities across the distributed network.

Centralized Device Management

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

Easy Configuration using Web Interface

The image shows a series of overlapping configuration windows. The 'Add Group' window is at the top, followed by 'Add Device', 'Create User', and 'Create Role'. Each window contains various input fields for configuration, such as 'Group Name', 'Device Name', 'User Name', 'Password', and 'Role Name'. The 'Create Role' window includes a 'Select Role' dropdown and a 'Select Devices or Groups' button.

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
CIIPA	Allow	Internet Access Policy for Children's Internet Protection Act	Apply
Categories policy	Allow	Applicable for Categories Department	Apply
Corporate Common areas 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	Deny	Deny HTTP Upload	Apply
Deny all	Deny	Deny Internet Access	Apply
Deny all chat	Deny	Deny All Chat	Apply
Deny all chat and mail	Deny	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

This block shows several overlapping configuration windows: 'Virus Scan Policy Details', 'Edit Internet Access Policy', 'Edit Bandwidth Policy', and 'Edit IDP Policy'. Each window displays detailed settings for its respective policy, including names, descriptions, and various enforcement parameters.

Instant enforcement of security policies in response to zero hour threats

Create and enforce firewall rules, custom web filter categories, custom IPS, Anti-virus 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	Service	Action	SNAT Policy	IAP	Manage	Apply
LAN - WAN (3 Rules)									
52	<input checked="" type="checkbox"/>	voipdevice1	-	-	Accept	MASQ	-	Apply	Remove
2	<input checked="" type="checkbox"/>	Any Host	Any Live User	Any Host	All Services	Accept	MASQ	User's Pol...	Apply
1	<input checked="" type="checkbox"/>	Any Host	-	Any Host	All Services	Drop	-	Apply	Remove
DMZ - WAN (2 Rules)									
51	<input checked="" type="checkbox"/>	mailserver	-	Any Host	SMTP	Accept	MASQ	-	Apply
50	<input checked="" type="checkbox"/>	Any Host	-	Any Host	All Services	Drop	-	Apply	Remove
LAN - LOCAL (1 Rules)									
*	<input checked="" type="checkbox"/>	Any Host	-	Any Host	Local ACLs	Accept	-	Apply	Remove

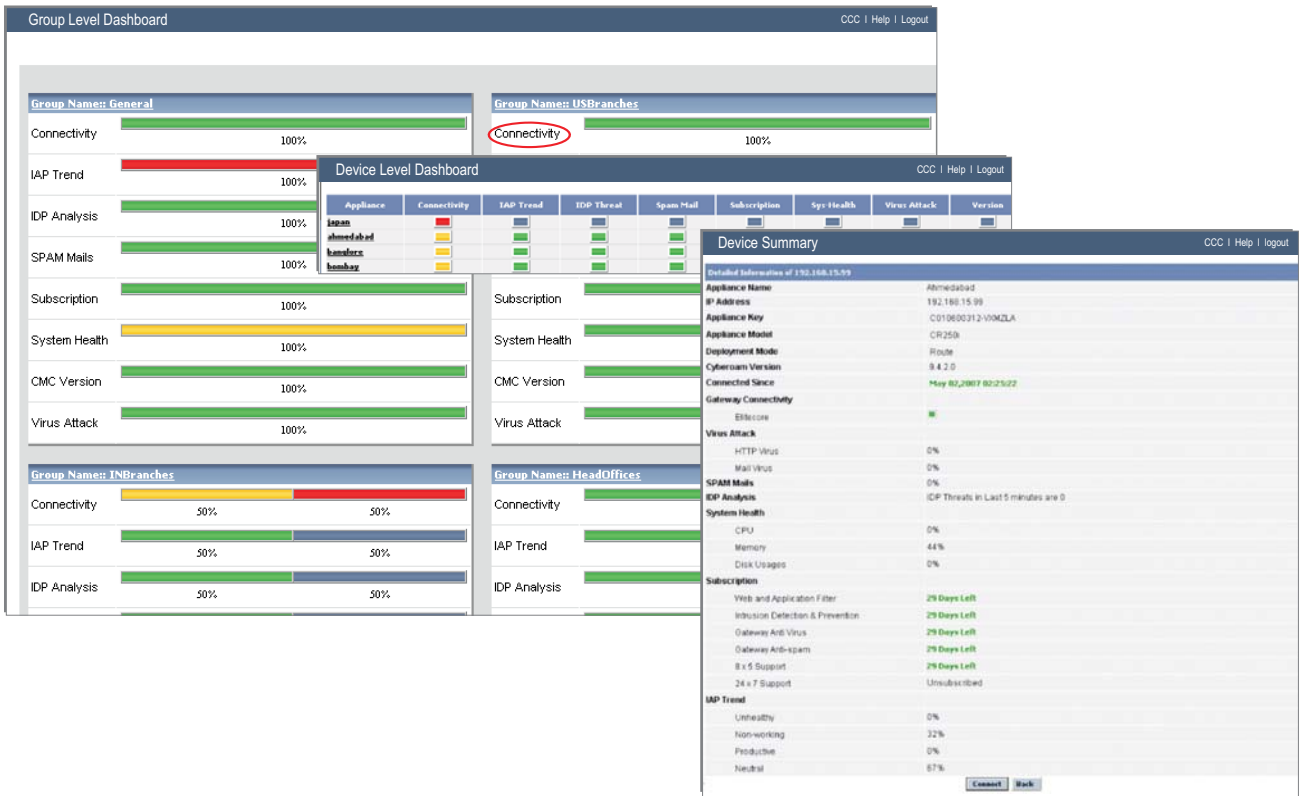
Custom IPS Signatures

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

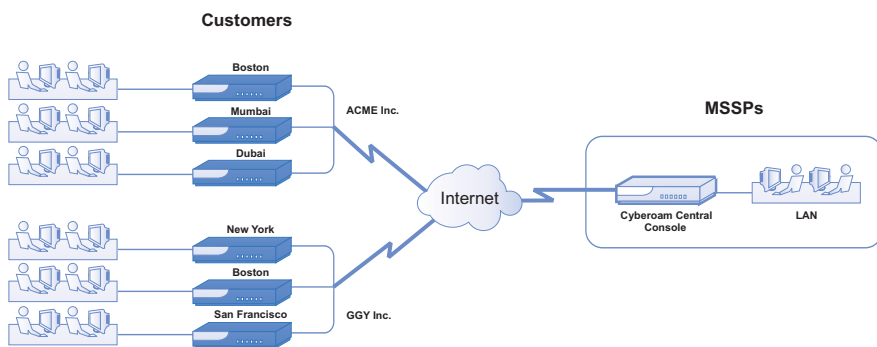
IDP Custom Signature Name	Description	Apply	Del
yahoo_adodb_exploit_1	Signature for yahoo Adodb exploit	Apply	<input type="checkbox"/>
yahoo_adodb_exploit_2	Signature for yahoo Adodb exploit variant	Apply	<input type="checkbox"/>
wmf_exploit	Signature for windows wmf exploit	Apply	<input type="checkbox"/>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

Instant enterprise-wide security visibility

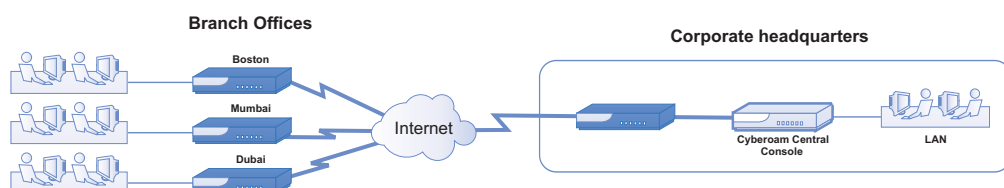
Cyberoam Central Console enables central monitoring, ensuring instant action that provides uninterrupted security across networks. Monitor the remote and distributed offices through instant visibility into their network status. Take instant action by real time enforcement of security and firewall policies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



Cyberoam Central Console Deployment- MSSP



Cyberoam Central Console Deployment- Large Enterprise



Technical Specifications	CCC 15	CCC 50	CCC 100	CCC 200
Interfaces				
10/100/1000 GBE Ports	6	6	6	10
Console Ports (RJ45)	1	1	1	1
SFP (Mini GBIC) Ports	-	-	-	2
COM Port	-	-	-	-
USB Ports	2	2	2	2
Dimensions				
Height	1.7 inches	1.7 inches	1.72 inches	3.46 inches
Width	16.8 inches	16.8 inches	16.8 inches	16.7 inches
Depth	10.3 inches	10.3 inches	13.4 inches	20.9 inches
Power				
Input Voltage	115-230VAC	115-230VAC	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)	0 to 90%	0 to 90%	10 to 90%	10 to 90%
Cooling System (40mm Fan)	2	2	4	7
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

- Roll based Administration
- 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

■ Alerts

- Schedule Email Alerts
- Device or Device Group based Alerts
- Unchanged default passwords for Administrative consoles
- Unregistered Device
- Subscription expired
- Device version Upgrade required
- Successful Device Version upgrade
- Change in Device connectivity status
- Device System Health
- Device Virus threats
- Unhealthy traffic
- IPS attack
- Spam attack
- Signature - Antivirus and IPS Upgrade required
- Filtering Categories Upgrade required

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
 - IPS 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
- SNMP (v1, v2c, v3)
- Syslog settings
- NTP server support
- Communication
 - SSL RC4 128bit Encryption
 - Mutual Authentication

Real-time Monitoring

- Dashboard
- Monitor by
 - Devices
 - Device Groups
 - Device and Device group Information Notifications

- Track System health
- Monitor IPS 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

Authentication

- User Authentication
 - Local Authentication
 - Active Directory Integration
 - External LDAP/RADIUS Integration

Compliance

- CE
- FCC

Upgrade Manager

- Upgrade AV and IPS signatures
- Upgrade Content filtering Categories
- Upgrade Devices

Toll Free Numbers

Thailand : +66-2-331-6491, Fax: +66-2-331-648

USA : +1-877-777-0368 | India : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958

Copyright © 1999-2010 Elitecore Technologies Ltd. All Rights Reserved. Cyberoam and Cyberoam logo are registered trademarks of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice. 1.0-20100128

