Unified Threat Management

Comprehensive Network Security

Emerging Internet threats External and Internal

- Viruses, Worms, Trojans
- Malware
- Spam
- Intrusions
- Spyware
- Phishing and Pharming
- Data Leakage
- Bandwidth Abuse

There's no escaping it: Enterprises, large and small are facing Internet threats not just from the external world, but from within too. While external threats are taking a targeted, blended form of attack, internal threats are creating security loopholes that leave the enterprise vulnerable to attacks. Faced with such a rapidly evolving threat environment, enterprises require multiple security features to ensure comprehensive network protection.

Enterprises that have deployed multiple security solutions face the daunting task of managing and upgrading these solutions constantly. At the same time they add to their capital and operating expenses.

Unified Threat Management

The complexity involved in managing multiple security solutions has led to unified security with multiple security features over a single platform - Unified Threat Management.

With the rise in targeted external attacks and insider threats, Unified Threat Management solutions have proven to be most effective when they extend security to encompass user identity to identify any threat whether it comes from inside or outside.

Cyberoam - Comprehensive Network Security

Cyberoam offers intelligent threat management with user identity-based controls. This approach leaves no loopholes in the network nor does it involve expensive, difficult-to-manage duplications that raise the cost of purchase, processor load and multiple, time-consuming policy settings.

Cyberoam is the only Identity-based Unified Threat Management solution that offers comprehensive network security with fine granularity through its unique user-identity based policies. Integrated High Availability feature provides protection against hardware failure to maximize network uptime and ensure uninterrupted access. Cyberoam's patent pending identity-based management offers high flexibility and ease-of-use to enterprises including corporations, educational institutions, government enterprises and more.

Cyberoam offers multi-lingual support with Chinese, Hindi, French, Turkish and English language GUIs, enhancing user experience in some of the largest and fastest growing markets.

Cyberoam's Active-Active High Availability provides efficient, continuous access to business-critical applications, information and services. Cyberoam High availability also provides continued network protection from all attacks even in the event of a device failure.

CR Series : 15i, 25i, 50i, 50ia, 100i, 100ia, 200i, 300i, 500i, 1000i, 1500i

2008 - Emerging Vendor of the Year

Features

Cyberoam offers a well-coordinated defense through tightly integrated best-of-breed solutions over a single interface. The result is a complete, dependable shield that Internet threats find extremely difficult to penetrate.

- Stateful Inspection Firewall
- Virtual Private Network (SSL VPN & IPSec)
- Gateway Anti-Virus and Anti-Spyware
- Gateway Anti-Spam
- Intrusion Prevention System - IPS
- Content & Application Filtering
- Bandwidth Management
- Multiple Link Management
- Comprehensive Reporting

Benefits

Cyberoam offers all-encompassing benefits to enterprises.

Technical Benefits

- Real-time protection against all Internet threats
- Rapid deployment
- Zero network configuration
- Single management interface - web based GUI

Financial Benefits

- Low capital expense
- Low operating expense
- High ROI

Business Benefits

- Safe business environment
- Control over legal liability
- Enhanced productivity
- Meets regulatory compliance requirements

Stateful Inspection Firewall

Cyberoam's patent pending identity-based stateful inspection firewall delivers instant visibility and consolidated security

Embeds User Identity

Cyberoam embeds user identity in the firewall rule matching criteria which eliminates the IP address as an intermediate component to identify the user offering instant visibility and proactive controls over security breaches - even in dynamic IP environments. User identity binds the security features to create a single, consolidated security unit enabling the administrator to change security policies dynamically while accounting for user movement - joiner, leaver, rise in hierarchy and more.

Unified Management

Cyberoam enables management of multiple security features from a single entry point while defining the firewall policy. This offers a unified approach to the overall security policy. It also enables easy configuration and trouble shooting.

Gateway Level Protection

Cyberoam's firewall delivers effective protection with stateful and deep-packet inspection analyzing packet headers and payloads. Cyberoam's firewall also protects networks from Denial of Service (DoS) and flooding attacks and prevents IP spoofing.

Enterprise Grade Security

Cyberoam meets enterprise level security requirement through features like High Availability, support for Virtual LAN, Dynamic Routing, Multicast Forwarding and more to ensure comprehensive security with business continuity.

Virtual Private Network (SSL VPN & IPSec)

Total Solution for Secure Remote Connectivity

SSL VPN

Location, platform and device-independent, Cyberoam UTM's on-appliance SSL VPN offers the option of secure web based VPN, delivering Anywhere-Any Device remote access in addition to client-based VPN. It enables road warriors, telecommuters, partners and customers to access the corporate network from multiple locations that include home, client networks, public kiosks, hotspots over varied devices like laptops, mobile devices and public desktops in internet cafes. Cyberoam's identity-based access policies allow administrators to limit access to pre-defined applications or offer full access based on the user identity and work profile.

IPSec VPN

Industry-standard IPSec, L2TP and PPTP VPN provide enterprises with secure connectivity with low bandwidth requirement without the fear of eavesdropping, data tampering or concerns over host and end-point and data integrity, meeting the requirements of site-to-site, host-to-host and host-to-net connectivity.

With Threat Free Tunneling technology, traffic over IPSec, L2TP and PPTP VPN is scanned for viruses, spam, intrusion attempts, inappropriate web content and unwanted network applications, preventing threats from remote users in entering the corporate network.

VPNC Certified

VPNC certified Cyberoam SSL VPN works with a variety of web portals, browsers and dynamic websites, meeting the challenges of real-world usability and compatibility and fulfills organizations' secure remote connectivity requirements. Further, the Basic and AES Interop certification from VPNC assures Cyberoam IPSec VPN's interoperability in multi-vendor environments.

Gateway Anti-Virus & Anti-Spyware

Powerful, Real-time Anti-Virus and Anti-Spyware Protection

Cyberoam offers gateway level protection from viruses, worms and malicious code through its Anti-Virus and Anti-Spyware solution, stopping threats before attack. Gateway-level scanning and blocking of HTTP, FTP, SMTP, POP3 and IMAP traffic offers a powerful coordinated web and email defense. 24x7 virus monitoring ensures rapid response to new viruses. In addition, it offers a self-service quarantine area. The Cyberoam dashboard instantly alerts network administrators to computers infected with Spyware. Simultaneously, it reports the user identity enabling network administrators to take remedial measures by immediately locating the infected systems in the Network.

Up-to-date Protection

Cyberoam's Anti-Virus feature checks viruses against its vast and regularly updated virus signature database. It's virus signature database is regularly updated to provide complete protection. Cyberoam's Anti-Virus engine supports a wide-range of file formats including password-protected attachments.

Gateway Anti-Spam

Customizable, Intelligent Anti-Spam Solution

Zero hour Defense

Cyberoam's Anti-Spam feature delivers zero-hour protection though RPD™* (Recurrent Pattern Detection) technology which provides industry's highest and best spam and threat detection capabilities. The content agnostic RPD™ technology detects and blocks emerging spam outbreaks including image, PDF, Excel spam and more with the least amount of false positives.

It is highly scalable with the ability to analyze large messaging volumes at high throughput rates. The solution reduces spyware, phishing and adware attempts and controls spam involving pornography while enhancing enterprise productivity. In addition, Cyberoam has the ability to configure White Lists and Black Lists based on user-identity, which facilitates granular mail management controls.

Early Outbreak Detection

With proactive virus detection technology, Cyberoam identifies massive e-mail borne virus outbreaks as soon as they emerge, effectively closing the early-hour vulnerability gap during which millions of users can be infected. It does so by providing a critical first layer of defense by intelligently blocking suspicious e-mails during the early stage of a virus outbreak.

Multi-tier Filtration

Cyberoam's granular policies use sender or recipient name, IP address, mime header and message size as their scanning parameters. This ensures that policies are finetuned as per business and compliance needs. Cyberoam supports the full protocol spectrum which consists of SMTP, POP3 and IMAP, offering comprehensive protection.

Flexible Options

Based on configuration, Cyberoam's Anti-Spam offers flexible options to deliver spam to the original address or delete/redirect spam to a pre-defined address e.g. Administrator, department head or others. In addition, Cyberoam provides user-wise self-service quarantine area where mails identified as spam can be quarantined. This gives the flexibility to the administrator and the users to self manage their quarantined e-mails. This also reduces the risk of losing legitimate business communication messages.

*Commtouch Software Ltd.

Net Facts - Internal Threats

- 50% of security problems originate from internal threats
- IM Threats are growing at 50% per month
- One in three instant message users have received SPIM spam over IM
- 51% of executives say they do personal surfing during business hours
- Financial losses from unauthorized access to data and theft of proprietary information has gone up

Source: CSO Metrics, Yankee group

Intrusion Prevention System - IPS

Cyberoam's IPS protects against threats by blocking Internet attacks before they impact the network. With its unique identity-based policy and reporting support, it provides advanced Intrusion Detection and Prevention, cutting down false positives drastically. Cyberoam IPS blocks intrusion attempts, DoS attacks, malicious code transmission, backdoor activity and blended threats without degrading network performance.

Comprehensive Protection

With one of the largest signature databases, Cyberoam's IPS instantly detects potentially malicious traffic based on policy settings bringing intelligence into the IPS mechanism. It offers blended protection through multiple analysis, stateful detection and individual user identity-based policies rather than blanket policies providing application and network-layer protection.

Identity-based Protection

Cyberoam's user identity-based policies deliver granular protection in addition to identifying attackers within the network and alerting administrators enabling real-time corrective action. Visibility into applications by user with period and extent of usage, enables IT administrators to zone in on rogue users and systems.

Custom IPS Signatures

Cyberoam's IPS supports custom signatures, allowing enterprises to create their own signatures, delivering zero-hour protection against emerging threats. The IPS signature database includes HTTP proxy signatures that prevent masking of user surfing through an anonymous open proxy. Cyberoam IPS signatures instantly uncover existing Spyware infections when the Spyware starts to 'phone home' about its findings.

Online Updates

Updates are delivered online allowing automatic updates for protection against vulnerabilities before they are exploited.

Content & Application Filtering

Indiscriminate surfing is the leading factor attracting Internet threats

Comprehensive Site Database

Cyberoam delivers dependable content filtering through WebCat, Cyberoam's web categorization engine. With a comprehensive database of millions of region-specific popular sites across the globe grouped in 82+ categories, it delivers great value-for-money and dependability. The comprehensive database ensures the safety and security of minors online supporting CIPA compliance for schools and libraries.

HTTPS URL Filtering

Cyberoam can also control access to websites hosted over HTTPS by categorizing the domain names using the comprehensive website database. This feature helps the administrator to block access to unauthorized or unsafe websites like anonymous proxies and malware hosting websites, hosted over HTTPS.

Granular Controls

Cyberoam breaks free from static IP-based and blanket policies with its granular, user-identity based policy capability to apply pre-defined surfing policies to any user, anywhere in the network. Enterprises can define and apply user, group and application-based policies by hierarchy, department or any combination with access restriction to certain sites during specific time of the day.

IM-P2P Traffic

Cyberoam's surfing security extends beyond standard Web traffic to include IMs (instant messaging) like Yahoo, MSN, Skype as well as P2P (peer-to-peer) exchanges. It offers a complete view and user based controls to match the dynamic threat scenario.

Bandwidth Management

Bandwidth management controls threat to enterprise productivity

Cyberoam offers a high degree of customization in assigning bandwidth with the facility to define groups, subgroups and departments for policy setting over an easy-to-use GUI.

Preventing Bandwidth Congestion

Cyberoam delivers a powerful productivity tool, reducing bandwidth congestion through control over bandwidth of non-critical applications and recreational traffic like audio-video downloads, gaming, tickers, ads, etc.

Prioritizing Bandwidth by Applications & Category

Committed and burstable bandwidth can be assigned to bandwidth-sensitive applications. Cyberoam implements policies by assigning bandwidth based on time, web category and business criticality.

Bandwidth Scheduling

Cyberoam allows administrators to schedule and regulate bandwidth on time basis to users and host groups. This enables precise bandwidth allocation based on usage and time of the day with a defined data transfer.

Capacity Planning

Detailed bandwidth usage reports allow enterprises to plan capacity enhancements and make optimum use of resources.

Multiple Link Management

Optimum use of multiple links for dependable connectivity

Cyberoam Multi-Link Management controls traffic over multiple WAN links with a single Cyberoam installation. It delivers comprehensive traffic management capability, optimizing links and offering high-speed connectivity while maximizing ROI.

Load Balancing

Multi-Link Management maximizes reliability of enterprise connectivity by managing outbound Internet traffic over multiple ISP links. It load balances traffic based on a weighted round robin distribution offering a dynamic traffic management system.

Gateway Failover

Multi Link Manager monitors link availability of multiple WAN connections and transfers traffic from a failed to an operational link delivering seamless connectivity for business continuity.

Comprehensive Reporting

Traffic and analytical reports to identify pattern changes in usage

Comprehensive Analytical Reports

Cyberoam's analytical reports enable IT managers to identify pattern changes in Internet usage and fine tune enterprise policies. Cyberoam reports also provide details of HTTP upload activity carried out by each user. Cyberoam can store logs locally or send logs to multiple external syslog servers for archival .

Compliance Reports

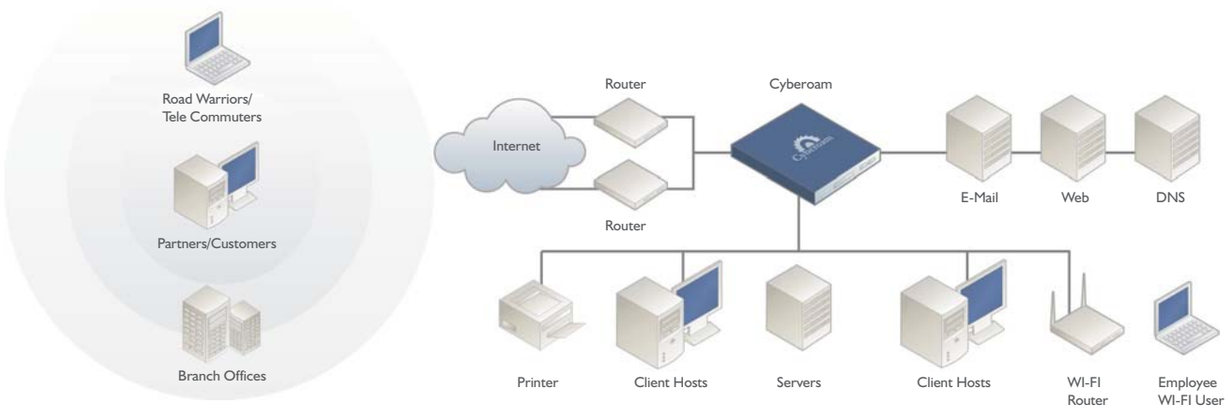
Cyberoam reporting includes 45 compliance reports aiding SOX, HIPAA, PCI-DSS, FISMA, GLBA and CIPA compliance. Reports enable corporations and educational institutions to meet regulatory compliance needs and also reduces audit time.

Network and Application Monitoring

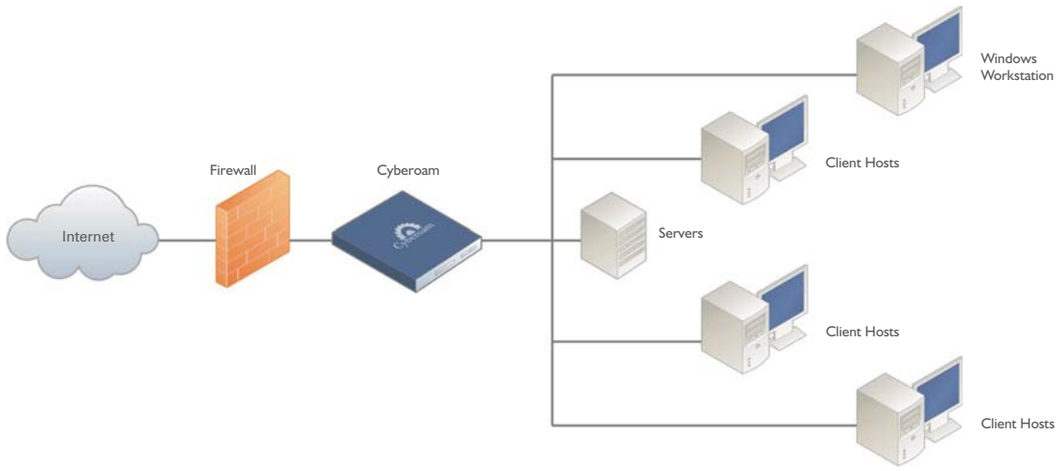
This offers information on current traffic movement alerting administrators to unproductive usage and threat incidents as they happen. They can take instant action by isolating system threats and controlling access to users who are choking bandwidth..

Cyberoam Deployment Scenarios

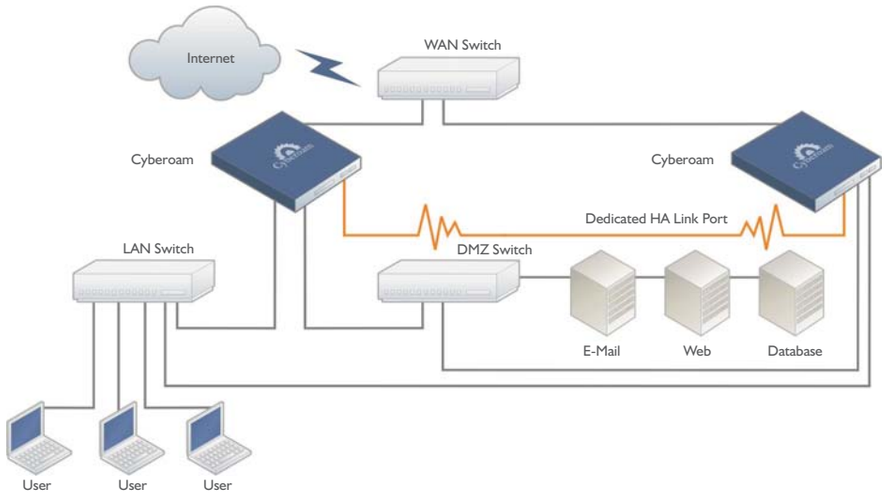
Gateway Mode



Bridge Mode
With Existing Firewall



High Availability
Active-Active



www.elitecore.com | www.cyberoam.com

North America
Cyberoam
Elitecore Technologies
600 West Cummings Park, Suite 1375
Woburn MA 01801. USA.
Tel: +1-781-460-2080
Fax: +1-978-293-0200

Toll Free Numbers
USA : +1-877-777-0368
India : 1-800-301-00013
APAC/MEA : +1-877-777-0368
Europe : +44-808-120-3958

Email
sales@cyberoam.com
support@cyberoam.com

Copyright © 1999 - 2009 Elitecore Technologies Ltd. All rights reserved.
Cyberoam and Cyberoam logo are registered trademark 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. Trademark under licence from NeoAccel.

10-96000-09-04-13