



Cyberoam UTM
(CR Series)

Vs.

SonicWALL UTM
(TZ and Pro Series)

SonicWALL UTM does
not have
Anti Spam
Security Solution

Cyberoam UTM won certifications from:

**Checkmark Certification
UTM Level 5**

Categories:

- Enterprise Firewall
- VPN
- Anti-Virus Gateway
- Anti-Spyware Gateway
- Anti-Spam
- URL Filtering
- IPS



ICSA

Category:

Corporate Firewall



**2007 Global Product Excellence Awards -
Customer Trust**

Category:

- Winner of Excellence in Integrated Security Appliance
- Winner of Excellence in Security Solution for Education
- Winner of Excellence in Unified Security



SC Magazine

Cyberoam UTM Overall Rating:

★★★★★ - 5 Stars



Cyberoam UTM was a finalist in:

The American Business Awards

Category:

**Best New Product or Service - Computer
Hardware or Services**



**Network Middle East Innovation Awards
2007**



Cyberoam UTM is a member of:

Virtual Private Network Consortium (VPNC)

- Basic Interop
- AES Interop



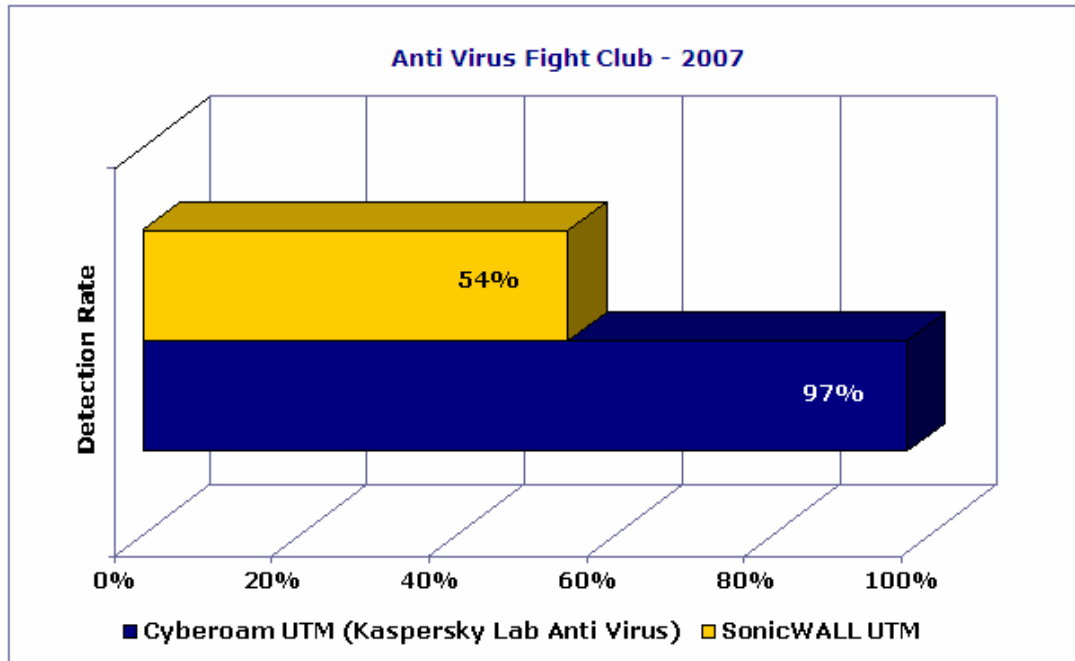
Cyberoam's Anti Virus vs. SonicWALL Anti Virus:

Cyberoam has an OEM with Kaspersky Lab for Gateway Anti Virus, which is one of the industries leading Anti Virus Solution.

SonicWALL has a proprietary gateway anti virus engine for HTTP and FTP scanning.

On August 8th 2007, at LinuxWorld, an all-out public test of different anti-virus vendors to see how they really compare took place. 10 antivirus products were confronted with 25 viruses, many submitted by members of the audience. The goal: to see whether the AV tools would catch them all.

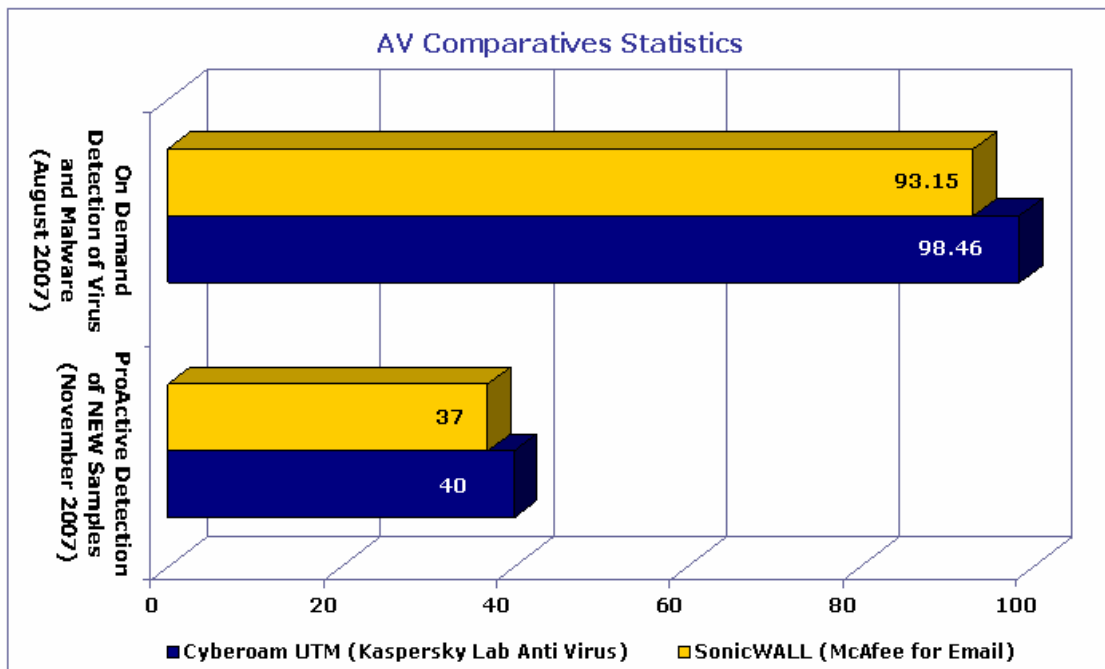
While Kaspersky topped with 97%, SonicWALL was dragging its feet with 54% detection rate.



SonicWALL has an OEM with McAfee VirusScan for its mail-based anti virus.

Both the Anti Virus solutions have been tested in August and November 2007, by AV-Comparatives.org, an independent organization based in Austria providing comparative reviews on Antivirus software.

The comparative results are as below.



Cyberoam's Real-Time RPD™ Anti Spam Technology

Cyberoam's RPD™ technology focuses on detecting recurrent message patterns in outbreaks. Message patterns are extracted from the message envelope, headers, and body. Patterns are extracted in real time from the message hashes being continuously sent to the detection centers. Cyberoam has a User based Self Service Quarantine area, so that no business mails are lost to security.

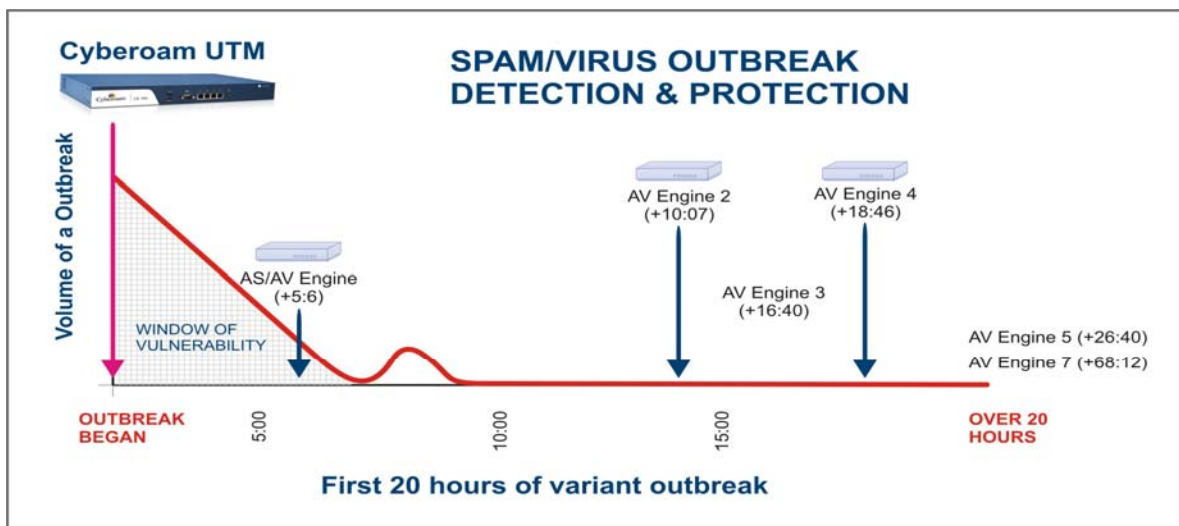
Anti Spam Statistics:

1. Cyberoam's Spam Detection Rate is industry's best: **98%**
2. Cyberoam's False Positive Rate is **0.000006%**

SonicWALL: NO ANTI SPAM, Only RBL Support

SonicWALL only supports RBL Filter for its UTM appliances. There are no relevant statistics are available for SonicWALL UTM's anti spam performance. (For more details please refer to the Excel Sheet Comparison)

Cyberoam Minimizes the Window of Vulnerability



Cyberoam provides proactive protection against new email-borne virus outbreaks, hours before the signatures are released. It has empowered with the proactive virus detection technology which detects and blocks the new outbreaks immediately and accurately.

It provides a critical first layer of defense by intelligently blocking suspicious mails during the earliest stage of a virus outbreak.

Bandwidth Management vs. Bandwidth Control

Cyberoam gives Bandwidth Management which is a full fledged user-based policy level management designed to provide:

1. Guaranteed or burst-able bandwidth
2. Flexible, prioritized, bidirectional rules
3. Rules for Users, Groups, IP addresses
4. Transparency for end users
5. Detailed and comprehensive bandwidth reports

SonicWALL UTM on the other had provided preconfigured options from **Firewall > QoS Mapping** option. The options are not self explanatory.

Cyberoam's User-based Multiple IPS Policies

User-based flexible multiple policies are supported by Cyberoam UTM only and not by SonicWALL. SonicWALL does not support Custom IPS signatures. (For more details please refer to the Excel Sheet Comparison)

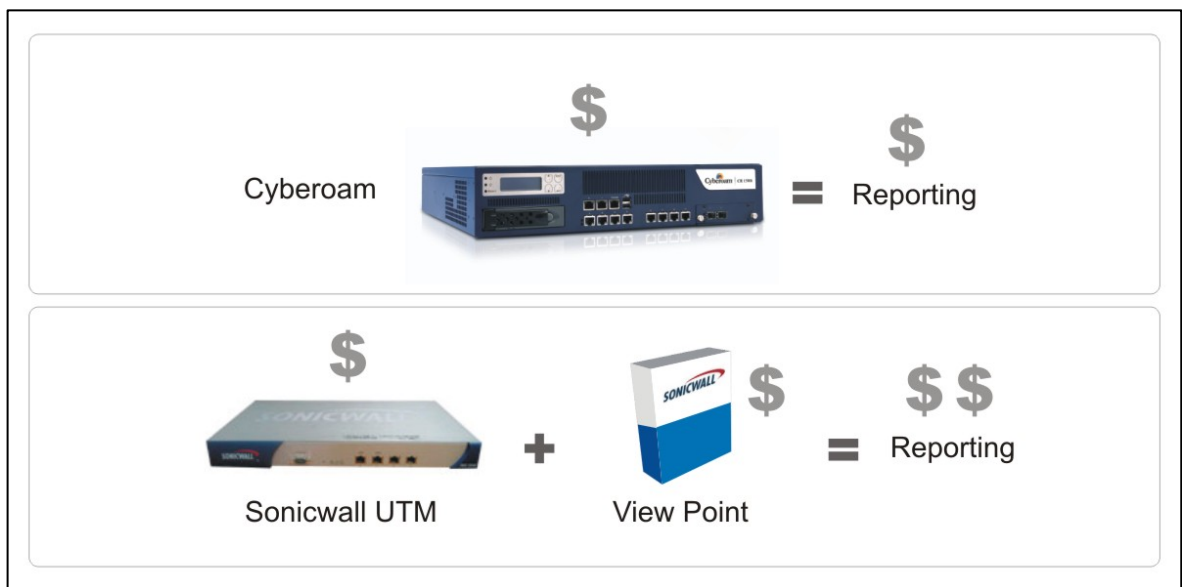
Cyberoam Reporting – Free + User Friendly

In SonicWALL, the customer needs to purchase and deploy ViewPoint software to get detailed reporting. This is a steep escalation in terms of Capital Expenditure and Operational Expenditure.

Cyberoam's On-Appliance **Plug-and-Play** reporting provides detailed reports.

Some unique Cyberoam Reports include:

1. User-wise reports of all types (Web Filtering, Internet Surfing, IPS)
2. User-wise Data Transfer
3. User-wise Search Keywords (reports of web searches)
4. Web Surfing Trends reports as per: User, Organization, Site, Category (graphical reports)
5. Compliance reporting comprising of: HIPAA, GLBA, SOX, PCI, FISMA



Broad Feature Comparison:

Points to Ponder	SonicWALL UTM	Cyberoam UTM
<p>Enhanced Firewall Decision Matrix:</p> <p>Firewall is a primary security component in network security.</p> <p>A normal decision matrix in a firewall stops at the IP address of a machine.</p> <p>In the blended threat scenario, social engineering is used to target the weakest link – end user. So a user's identity becomes an important decision and control parameter in the firewall matrix.</p>	<p>SonicWALL UTM does not use identity as a parameter in the decision matrix.</p>	<p>Cyberoam extends the firewall's rule matching criteria to include schedule and the user's identity.</p> <p>Similarly, the firewall actions are extended to include complete policy based control over all the security solutions like, content filtering, IPS, Internet access management, bandwidth management and anti-virus and anti-spam scans.</p>
<p>State-of-Art Identity-based Access Management:</p> <p>IAM is a combination of Identity, time scheduling and access management. This is a powerful control mechanism which reaches down to all the security solution in a UTM. Identity and time schedule are the two dimensions used to define a user's real time identity in a security solution.</p>	<p>SonicWALL UTM does not use identity as a parameter in the decision matrix.</p>	<p>Cyberoam's identity-based access management feature provides unparalleled flexibility, security and control to the network administrator over the end user.</p>
<p>Centralized point of UTM Management:</p> <p>Aggregation of security solutions is not enough. A UTM should be easily manageable. This makes it user friendly and the learning curve of the end user remains low.</p>	<p>SonicWALL UTM does not have this flexibility and ease of use.</p>	<p>Cyberoam is manageable through its single firewall page. It is designed to provide a central management of all member security packages of the UTM. In a few clicks, you can have custom policy to meet any security demand.</p>

Points to Ponder	SonicWALL UTM	Cyberoam UTM
<p>Business Friendly Anti Virus /Anti Spam Scans:</p> <p>For most users, missing a legitimate email is an order of magnitude worse than receiving spam or virus.</p> <p>To avoid such an unpleasant situation you need to control the parameters used to classify a mail as spam or virus infected and the necessary action.</p> <p>User-based customized scans can ensure that not a single mailed business opportunity is lost to security.</p>	<p>SonicWALL UTM does not provide any such control over its AV and AS scans.</p>	<p>Cyberoam UTM has an OEM license from Kaspersky's Gateway AV. Similarly, Commtouch RPD Anti-spam technology (OEM) is used in Cyberoam.</p> <p>No separate AMCs are levied.</p> <p>Using Cyberoam UTM you can define custom scan rules based on sender or recipient, IP address, mime header and message size.</p> <p>You have the flexibility to configure a scan as per your needs, rather than adjusting yourself to the way a security solution operates.</p>
<p>Self-service Anti Virus /Anti Spam Quarantine Area:</p> <p>Quarantine area is a safe holding area for all suspicious/infected files. This allows organizations to remove infected files from general circulation without deleting them.</p> <p>A gateway quarantine area should be self-service as there are a large number of users involved. So the users ought to get notified that a mail has been quarantined and he can access and deal with it without depending on the administrator.</p>	<p>SonicWALL UTM does not have this feature.</p>	<p>The Self-service quarantine area from Cyberoam UTM enables individual mail recipients to view and manage their infected / Spam messages.</p> <p>The self-service feature removes user's dependency on administrator to manage quarantine mails.</p>
<p>Superior Spam Filtering:</p> <p>In 2007, the spam proliferation has increased by 35% per year and 99% of all emails was spam. Image and Instant Messaging-based spam (spim) can prove to be a major drain on mail storage and employee productivity. Spim blockage requires specialized anti-spam filters.</p>	<p>SonicWALL UTM solely relies on RBL based spam blocking and customizes the AS policies as per your needs.</p> <p>SonicWALL only scans SMTP protocol for Spam.</p>	<p>Cyberoam has an OEM with Commtouch Software Ltd. Recurrent Patterns Detection (RPD) technology, based on the identification and classification of message patterns delivers the industry's best and highest spam and threat detection capabilities providing protection from all types of email-borne threats.</p> <p>Cyberoam watches over SMTP, POP3 and IMAP protocols for Spam. This provides comprehensive anti-spam cover.</p>

Points to Ponder	SonicWALL UTM	Cyberoam UTM
<p>Protection Against Phishing and Pharming:</p> <p>Phishing and Pharming are the next generation threats instigating the end users to breach the network security from within. Phishing is a passive baiting through mail and Pharming is an active process of host file corruption which leads the user unknowingly to a malicious site.</p>	<p>SonicWALL sole reliance on RBL leaves security loophole for Phishing mails.</p> <p>It has no Pharming protection.</p>	<p>Cyberoam UTM protects against Phishing and Pharming, both. Its Anti Spam technology and WEBCat database effectively mitigate Phishing threats.</p> <p>In case of a host file corruption due to a Pharming attack, the DNS configured in Cyberoam UTM makes sure that the user is not directed to a malicious site.</p>
<p>Define Multiple IPS Policies and Custom IPS Signatures:</p> <p>Blanket policies, over time force the administrator to open security loop holes.</p> <p>Customized policies provide you the comfort to deploy customized IPS policies as per your needs.</p> <p>Custom IPS signatures reach deeper than a firewall and antivirus to protect the network from blended threats.</p>	<p>SonicWALL UTM does not have Custom IDP Policies. In the latest versions Custom IDP Signatures have made a brief appearance.</p>	<p>Cyberoam UTM provides the administrator with the ability to attach an individual IPS policy to a combination of source, destination, application, identity and schedule.</p> <p>This ensures customized IPS policy as per your needs.</p> <p>Cyberoam UTM also provides you the facility to use custom IPS signatures.</p> <p>These features ensure that your network security is geared up meet any exceptions as well as general threat conditions.</p>
<p>Identity-based IPS Policies and Reporting Ensures Transparency:</p> <p>To deploy security policies the administrator has to know his target. IP addresses are not target enough.</p> <p>The most harmful intrusion attempts are attempted from inside a network. In IP address based IPS policies and reporting the identity gets lost.</p> <p>To ensure complete transparency in a network, the IPS policies and reporting should also take the user's identity into its ambit.</p>	<p>SonicWALL UTM does not have identity based IDP reporting.</p>	<p>Cyberoam UTM provides IP address and User-based reports. Providing complete visibility, it thwarts anonymity in DHCP, Wireless and Computer sharing environments.</p> <p>In case of threat detection; it reduces the administrator's reaction time. The administrator can personally contact the erring user.</p> <p>Identity based policies also lends unprecedented granularity to the IPS policies.</p> <p>Cyberoam's IPS module also provides mail alerts.</p>

Points to Ponder	SonicWALL UTM	Cyberoam UTM
<p>Practical Approach to Bandwidth Management:</p> <p>Percentile based bandwidth management is not practical as, if a VoIP application needs 128Kbps; you cannot assign 10% of the bandwidth.</p> <p>Moreover back calculating bandwidth on percentage basis is cumbersome.</p>	<p>SonicWALL UTM's bandwidth management policy is not very effective in the practical implementation because it allocates bandwidth on percentile basis.</p> <p>It lacks user specific bandwidth allocation and does not have the Priority feature.</p>	<p>Using Cyberoam you can provide QoS to a combination of source, destination and service/service group by committing bandwidth to users, applications and servers based on time schedules.</p> <p>You can manage interactive applications like VoIP, Video Conferencing, SSH, telnet etc. better by assigning higher priority to get better and instant results</p>
<p>Secure Vital Information by Rule based Application and IM Controls:</p> <p>Unmonitored content leaving an organization through an IM application introduces security, legal and competitive risk. It is difficult for the IT department to discover potential breaches of policy or to hold individuals accountable.</p>	<p>SonicWALL UTM does not support granular control over IM.</p> <p>They are either fully allow or are deny an application, there is no granular control over it.</p>	<p>Cyberoam UTM's application filtering solutions is powerful enough to control file transfer over any IM application. Identity can be used as a control parameter in these control policies.</p>
<p>User Identity Based Comprehensive Reporting:</p> <p>Reports are an integral part of any security solution as they are the tools to provide visibility.</p> <p>Clear and precise reports are the most valuable tools that makes sure that organization's resources are focused on maximum productivity</p>	<p>SonicWALL UTM comes with limited reporting facilities. However, if the organization needs extensive reporting, it has to buy and install a separate proprietary application SonicWALL Viewpoint.</p> <p>The applications needs separate hardware platform.</p>	<p>Cyberoam has an integrated plug-and-play reporting module which provides IP address and user identity based in-depth reports.</p> <p>All reports are HTTP/HTTPS based, and so are platform, location and client independent.</p> <p>As a value aided feature Cyberoam reports are complimentary to CIPA, HIPAA, GLBA, SOX, PCI, FISMA compliances.</p> <p>Cyberoam also provides external reporting with the help of Cyberoam Aggregated Reporting and Logging Solution.</p>

<p>Automated Single Sign On Ensures hassle free Transparent Authentication :</p> <p>Authentication often gives administrators nightmares as they involve a lot of hassles and changes in the existing setup. SSO ensures that the user's authentication is seamless and transparent. It also ensures that the user has his well-defined secure microcosm.</p>	<p>SonicWALL UTM does not have automated SSO.</p>	<p>Cyberoam SSO ensures that the UTM remains transparent and it seamlessly blends into the network. The user is never explicitly aware of its existence. Only in case of treading on forbidden paths, he is reminded of the UTM's presence. The SSO promotes a one stop, transparent entry into the network, reducing administrative maintenance.</p>
<p>Data Transfer Accounting and Control:</p> <p>Data transfer accounting and control helps you to see the actual internet consumption by an individual user or an application. This feature also helps when you want to find the exact costing of Internet usage in case if an ISP is charging for the amount of data transferred.</p>	<p>SonicWALL does not have this feature.</p>	<p>Cyberoam provides a comprehensive, application and user based data transfer accounting and control. This feature comes in handy in educational institutions where Internet consumption per individual is important.</p>
<p>Multiple WAN Interface Support:</p> <p>A UTM appliance deployed at the gateway should support more than 2 WAN interfaces for the continuous business connectivity. The failover conditions should support the business need of the organization.</p>	<p>SonicWALL supports only 2 WAN links. It does not have Multiple Failover Rule support.</p>	<p>Cyberoam supports multiple WAN links (More than 2). The Multiple Failover rules in Cyberoam ensure that the link status is checked for its true business needs. Hence it leads the organization to an uninterrupted Internet availability.</p>



USA - Sales Toll Free: +1- 866-663-2927 | Support Toll Free: +1-877-380-8531

India - Sales: +91-79-66065606 | Support Toll Free: 1-800-301-00013

EMEA/APAC - Sales: +91-79-66065787 | Support: +91-79-66065777

Copyright © 1999 - 2008 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.



Overview of Cyberoam's Security Approach:

- Whom do you give access to: An IP Address or a User?
- Whom do you wish to assign security policies: User Name or IP Addresses?
- In case of an insider attempted breach, whom do you wish to see: User Name or IP Address?
- How do you create network address based policies in a DHCP and a Wi-Fi network?
- How do you create network address based policies for shared desktops?

Cyberoam UTM approaches the Security paradigm from the *identity* perspective. The blended threats circumvent the perimeter defense and launch an attack from within. The network's own resources are used to subvert it. The main target is thus the end user who knowingly or unknowingly breaches the perimeter defense.

While providing a robust perimeter defense, Cyberoam UTM's Identity-based access control technology ensures that every user is encapsulated in a tight, yet granular security policy that spans across Cyberoam UTM's Firewall/VPN, Gateway Anti Virus, Anti-Spam, Web Filtering, Intrusion Prevention System (IPS) and Bandwidth Management solutions.

Disclaimer:

The comparison is based on our interpretation of the publicly available information of the compared product.

Either of the product features is likely to change without prior notice.

This document is strictly confidential and intended for private circulation only.

Document Version: 5.1 – 95322 – 23/06/2008