Cyberoam

Unified Threat Management

Product Comparison

Cyberoam

vs.

FortiGate

The design philosophy behind Cyberoam UTM is to balance between One Box Total Solution and Optimum Performance to provide superior value for money.

Fortinet lacks the One Box Solution philosophy

www.cyberoam.com

Cyberoam Certifications

Westcoast Labs Checkmark Certification: UTM Level 5

Categories:

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

ICSA Certification

Category:

- Corporate Firewall
- High Availability

Awards

Winner of 2008/2009 ZDNet Award

Category:

- IT Leader
- Asia's Most Promising Asian TechnoVisionaries

Winner of 2007 Global Product Excellence Awards - Customer Trust Category:

- For Integrated Security Appliance
- For Security Solution for Education
- For Unified Security

Product Review

- **SC Magazine** : Cyberoam UTM Overall Rating: ★★★★★ **- 5 Stars**

Cyberoam UTM is Certified by Virtual Private Network Consortium (VPNC) :

- Basic Interop
- AES Interop
- SSL Portal
- SSL Firefox
- SSL Java Script
- SSL Basic Network Extension
- SSL Advanced Network Extension

SC Magazine's Comparative Review:

Cyberoam – CR200i: 5 Stars Rating	FortiGate-110C: 4 Stars Rating

Product Rating	
Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★☆
Overall Rating	★★★★★

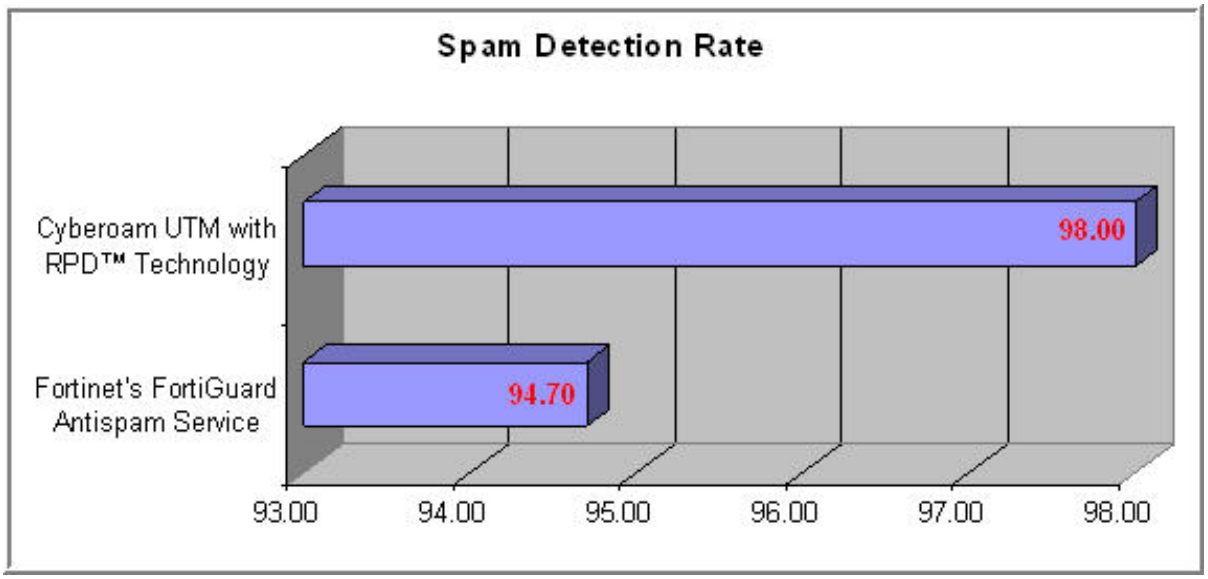
Product Rating	
Features	★★★★★
Ease of Use	★★★★☆
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★☆☆
Overall Rating	★★★★☆

Cyberoam's Real-Time RPD™ Anti Spam Technology

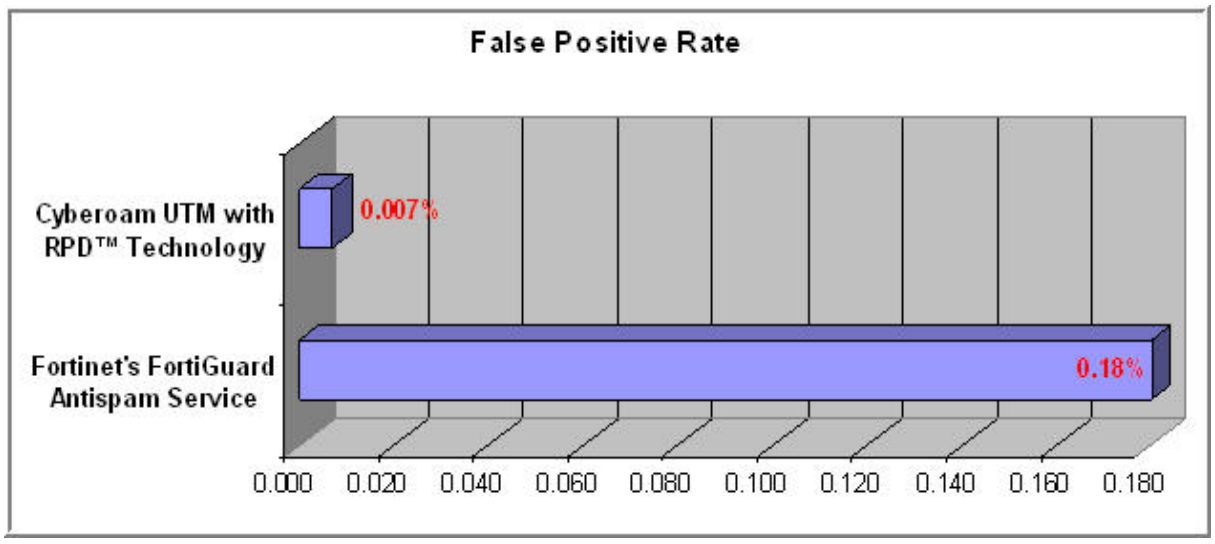
Cyberoam's RPD™ technology focuses on detecting recurrent message patterns in outbreaks. Message patterns are extracted from the message envelope, headers, and body. Patterns are extracted in real time from the message hashes being continuously sent to the detection centers.

A Graphical comparison of Anti Spam Spastics:

1. Cyberoam's Better Spam Detection Rate:



2. Cyberoam UTM's Minimal False Positive Rate:



If the user wants, Cyberoam also provides a Self Service Spam Quarantine area.

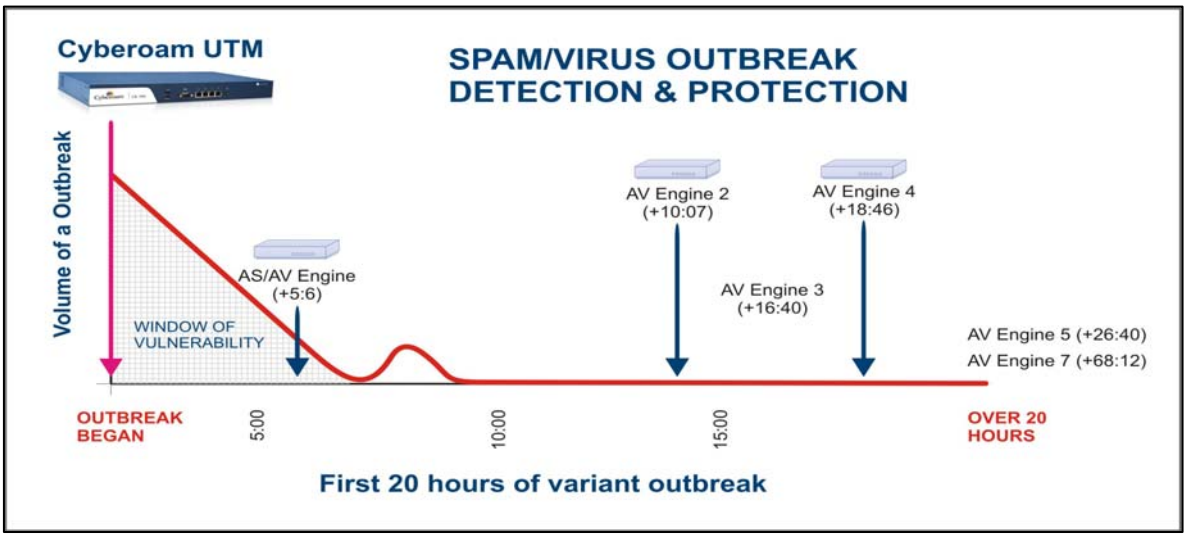
Note:

- The Fortigate numbers were taken from the Fortigate Knowledge Base. The link has now been disabled.
- Fortigate publishes number of Fortimail. It is a secure email appliance and entails extra capital and operational overheads.

Cyberoam Minimizes the Window of Vulnerability

Cyberoam provides proactive protection against new email-borne virus outbreaks, hours before the signatures are released. It has introduced 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 mail during the earliest stage of a virus outbreak.



Gateway Load Balancing vs. Load Sharing: Automated vs. Manual

Cyberoam UTM provides Load Balancing. FortiGate provides Load Sharing.

Load sharing means one can split the traffic from a network to be transported by different routers (paths). So it requires a pre-specified manual route configuration and there is no balancing.

Load balancing means distributing the traffic as per defined weights dynamically among different paths to avoid link congestion and saturation. This can be done per destination in a round-robin fashion. The packets sent by a host follow different paths to the same destination. All paths belong to all hosts. So, as per the pre defined weights, the links are used. In case a specific user needs to use a particular gateway; that can also be configured.

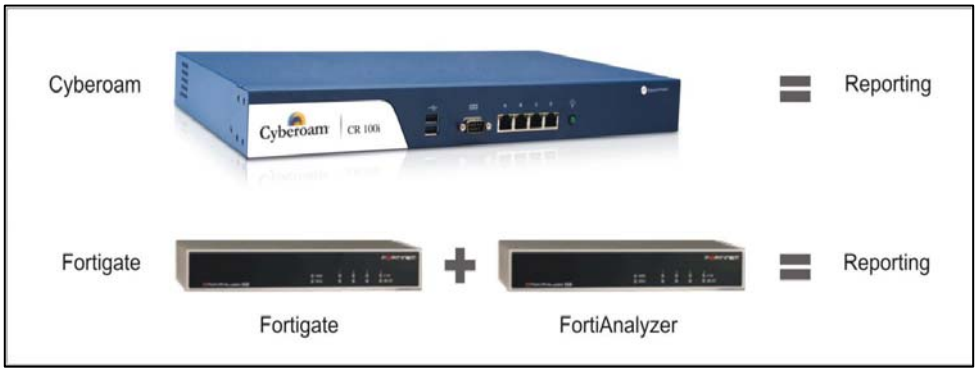
Multiple Gateway Support: Cyberoam Checks the Link for its Functional Requirement

FortiGate supports a Single Ping Rule to query the status of multiple gateways. If the ISP or the external site has blocked the ICMP Ping, this rule can fail.

Cyberoam supports Multiple Failover Conditions using which a link status can be queried for the specific functional purpose. Apart from the ICMP ping, Cyberoam also supports UDP and TCP protocols to query the link status.

This implies that in case a specific link is used for a database server for UDP traffic and the ping does not reply, FortiGate will consider it non-functional. While Cyberoam UTM will send an UDP Echo to check the link status, and in case it received a reply, the link is functional.

Reporting



To get reporting in FortiGate the customer need to purchase and deploy FortiAnalyzer with a Fortigate appliance. This is a steep escalation in terms of Capital Expenditure and Operational Expenditure.

In spite of this extra Capex and Opex there are a few reporting features that Fortinet still lacks:

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 per: User, Organization, Site, Category(graphical reports)
5. Compliance reporting comprising of: HIPAA, GLBA, SOX, PCI, FISMA

Cyberoam also supports external reporting – iView.

Overview of Cyberoam's Security Approach:

- Who 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 (IPS) and Bandwidth Management solutions.

Head to Head:

Points to Ponder	Fortigate	Cyberoam UTM
Identity based security – Cyberoam's First Movers Advantage: UTM's Single platform demands an approach that holds the diverse solutions together to strengthen and provide a simplistic operational synergy. The best security system is vulnerable to human error. If the end user is contained in a decision matrix, it lends completeness.	Fortigate lacked a user-centric approach till Forti OS 4.0. It has recently added this feature, which is still a catch-up feature and lacks the level of maturity.	Cyberoam was one of the first UTM solutions that embedded user identity in the firewall rule matching criteria apart from MAC address, IP address, protocol and time schedule. Similarly, the firewall actions are extended to include policy based control over all the member security features like Filtering, Anti Virus, Anti Spam, IPS and Bandwidth Management. User's identity binds Cyberoam UTM's security features together to create a single consolidated security unit.
Total VPN Solution: With mobile workforce on the rise, VPN has become a mainstay to promote secure connectivity to remote users. VPN ensures that the organizational resources are utilized securely over public networks.	Fortigate has PPTP, L2TP, IPSec and SSL VPN, on appliance.	Cyberoam has PPTP, L2TP, IPSec and SSL VPN, on appliance.

Points to Ponder	Fortigate	Cyberoam UTM
Comprehensive Anti Virus and Anti Spam Protection: Viruses, Trojans, Spyware and other Malware infiltrate an organization through internet using various vectors. From mail to Web surfing to Instant Messaging all are the most common mediums of infection. Zero day attacks are a very potent weapon which is wielded to achieve maximum penetration as the traditional security systems are reactive in natures and rely heavily on signatures.	Fortigate does not have a Zero Day Protection. As they have a proprietary anti virus feature which is signature driven and reactive in nature, the security gap is glaring. Fortigate has a response time of three (3) hours to release an anti-malware signature. Reference: www.fortinet.com/doc/solution brief/antivirus_sol_brief.pdf	Cyberoam has the industry's best gateway anti virus solution – Kaspersky. It has one of the best response-time as compared to Fortinet AV. Cyberoam's Virus Outbreak Detection technology is a proactive, signature-less proactive security technology, which primarily defends the organization against Zero Day Attacks. Cyberoam detects all malware on all Web, Mail and IM protocols. It also scans forty (40) different types of compressed files. Kaspersky has a response time that is less than 2 hours. References: http://forum.kaspersky.com/index.php?showtopic=7735 http://usa.kaspersky.com/about-us/comparative_test.php?test=Response
Adaptable AV/AS Scans: For most users, missing a legitimate email is an order of magnitude worse than receiving spam or virus. When a critical mail gets classified as a virus or a spam you should have the right to choose; what to allow and block	Fortigate provides limited control over its AV and AS scans. To get granular controls over the mail traffic, the users are urged to buy, FortiMail. This is a separate mail security device.	Using Cyberoam UTM you can define custom spam filtering rules based on sender or recipient, IP address, mime header and message size. You have the flexibility to tweak a spam scan as per your needs, rather than adjusting yourself to the way a security solution operates. All these are features are given in One Box – Cyberoam.

Points to Ponder	Fortigate	Cyberoam UTM
Self-service AV Quarantine Area: The user first has to know that a mail has been quarantined and then get access, to deal with it. So a Gateway AV quarantine area proves to be a bottle-neck for users and administrator, alike. Self-Service quarantine area is the solution.	Fortigate does not have self-service quarantine facility.	The Self-service quarantine area from Cyberoam UTM enables individual mail recipients to view and manage their infected messages. The self-service feature removes user's dependency on administrator to manage user's quarantine mails.
Superior Spam Filtering: Spammers use various techniques to circumvent the gateway anti spam solutions. Minor changes in the content and language can easily for the traditional anti spam solutions.	Fortigate is not effectively equipped spam. The users are urged to buy, FortiMail.	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 all types of email-borne threats. The spam detection is not based on the language or the content of the mail.
Category Based Bandwidth Management: Enterprises often need to provide category based bandwidth management. Productive and business related categories need to be given a priority over other categories.	Fortigate does not have this feature.	Cyberoam UTM provides a comprehensive category based bandwidth management. This ensures productivity.

Document Version: 5.0 – 96016 – 14052009

Cyberoam
Visit: www.cyberoam.com
Contact: info@cyberoam.com
USA - Tel: 201-484-7581, Fax: 201-777-2113
India - Tel: +91-79-26405600, Fax: +91-79-26407640