Cyberoam

Unified Threat Management

Product Comparison

Cyberoam Unified Threat Management Appliance

vs.

Astaro Security Gateway

Cyberoam is Recession Proof Investment

Many Astaro Customers often complain on two major things. Stability of ASG, and its post-sales support.

www.cyberoam.com

Cyberoam, a Recession Proof Investment – Superior RoI

Cyberoam Certifications

Westcoast Labs Checkmark Certification:
UTM Level 5
Categories:

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

ICSA Certification Category:
Corporate Firewall

Awards

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

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

Winner of 2008/2009 ZDNet Award Category:

- IT Leader
- Asia's Most Promising Asian TechnoVisionaries

Product Review

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

Cyberoam UTM is a member of:

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

Cyberoam: Superior RoI & Recession Proof Investment

Cyberoam gives much higher Return over Investment, as compared to Astaro.

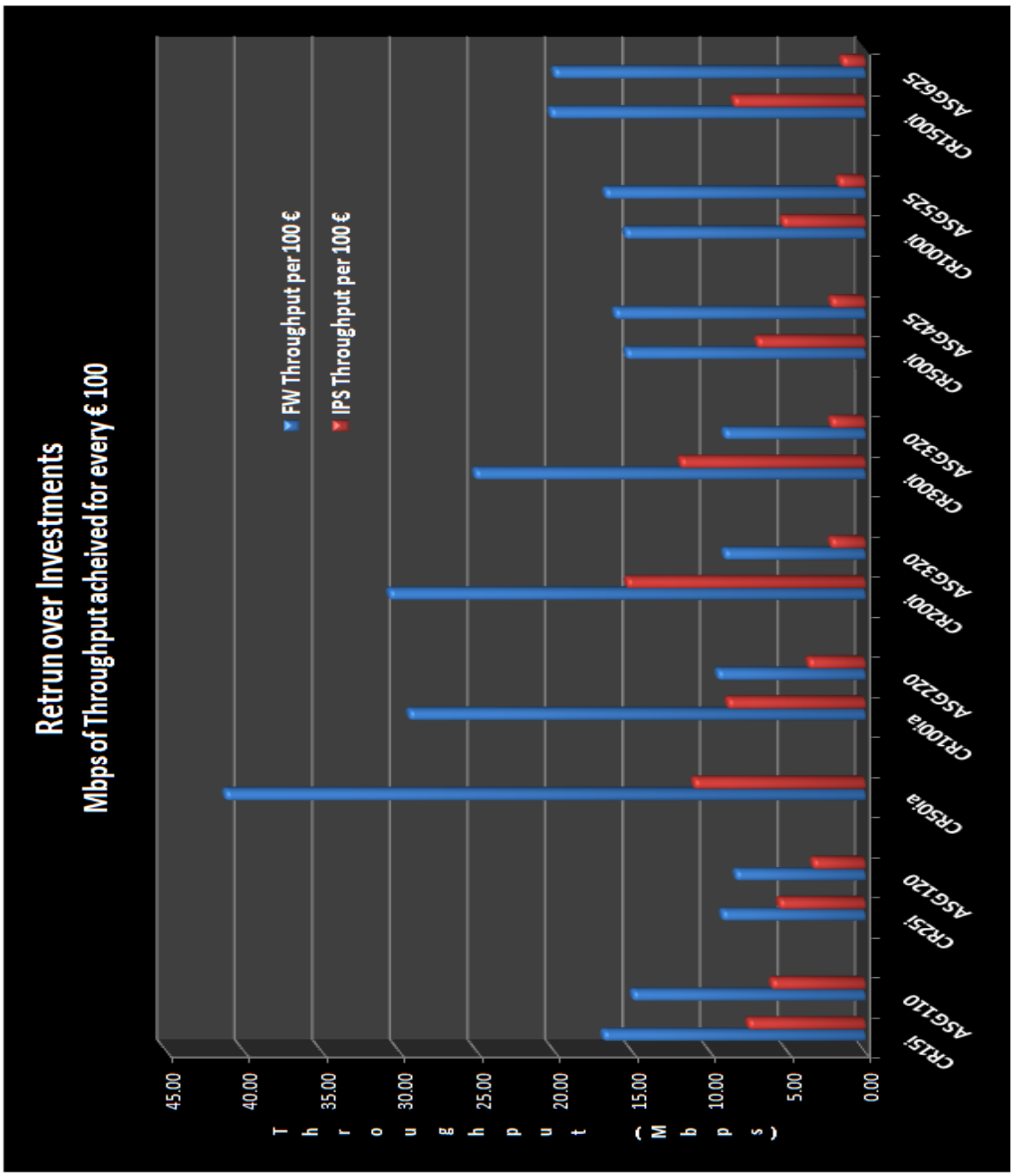
Below given are two graphical comparison of Firewall and IPS throughput in both the solutions per Euro.

Note:

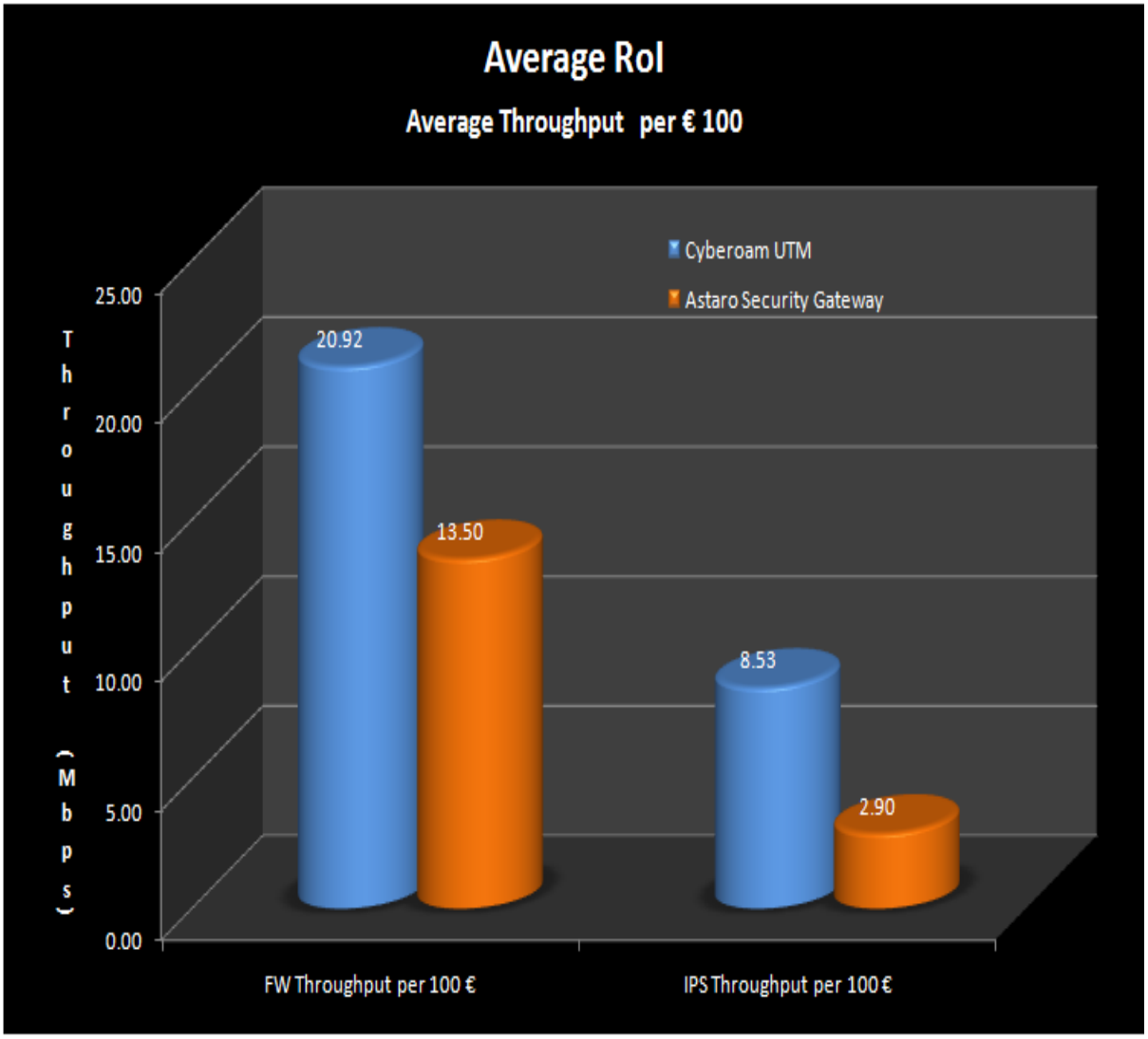
1. While Cyberoam price is **inclusive** of 8x5 support, Astaro's prices **do not** include any kind of support. It costs extra to buy support.
2. Cyberoam give its UTM throughput. UTM throughput is the throughput achieved when all the security features are enabled. Astaro only gives Intrusion Prevention System (IPS) throughput. Hence we have used Firewall and IPS Throughput of both the products for the comparison.

Throughput to Price Ratio

Below given is the Firewall and IPS Throughput per every EURO that you spend. This is a per model breakup. Based on this graph, it is amply clear that Cyberoam gives a huge advantage.



In a consolidated format – Average Return over investment, the result is given below.
This is the average RoI over full appliance range of both the UTMs.



Note: Both the graphs have been placed separately in KB for your convenience.

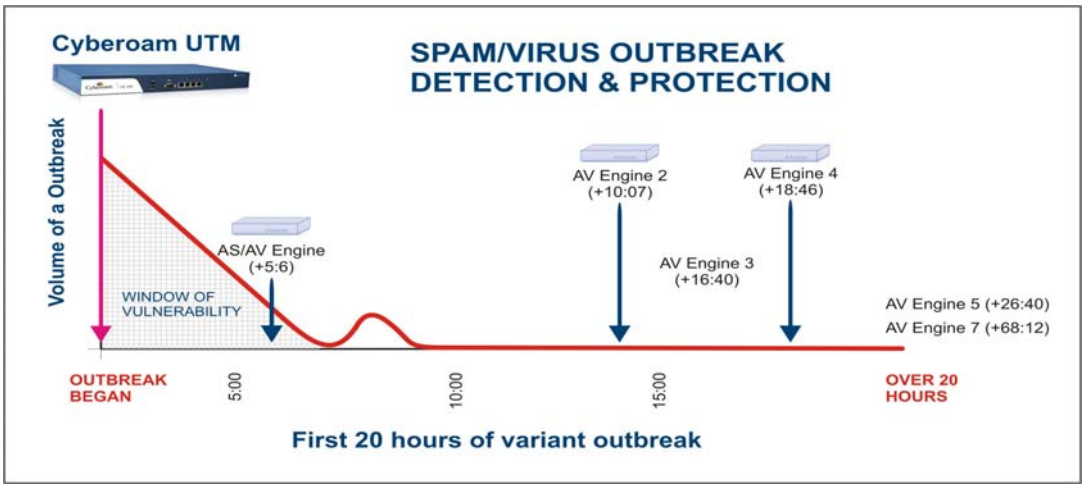
Astaro's Shifting Anti Virus Alliance

From Version 7.400 Beta, Astaro introduced Avira with Clam.
Before this, it used Authentium and Clam AV. This combination was a huge failure.
Cyberoam has Kaspersky since its inception.

Identity and Quarantine

Cyberoam	ASG
Identity based Anti Virus policies of Cyberoam enables the administrator to formulate custom policies.	No Identity-based Anti-Virus policies
Cyberoam can quarantine spam email and malware infected mails and files.	Does not quarantine infected files. Only mails are quarantined.

Cyberoam's Virus Outbreak Detection: 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.

In spite of having dual Anti Virus engines, Astaro does not have this feature.

Anti Spam Comparison

Cyberoam and ASG both use Recurrent Pattern Detection™ technology. Astaro has introduced RPD much after Cyberoam. In spite of using similar technologies, there are a few distinct Cyberoam advantages listed below

Cyberoam	ASG
Scans SMTP, POP3 and IMAP	Does **not** supports IMAP
Cyberoam's Identity based Anti Spam policies enable the administrator to formulate granular controls.	No Identity-based Anti Spam policies
Provides Mail Management features like Transparent Mail Copy and Mail Redirection.	No such features are supported.

Cyberoam's Cynosure - Identity:

Cyberoam	ASG
• Firewall	• Web Filtering
• Gateway Anti-Spam	
• Intrusion Detection and Prevention	
• Gateway Anti-Virus	
• Web Filtering	
• Bandwidth Management	

Identity as a security parameter means using an end user's identity, the administrator can create a granular security policy.

Cyberoam also uses IP Address, Service, MAC address and Time Schedule as security parameters. This lends unparallel flexibility to configure business friendly security policies.

Identity-based security and network access management deals with identifying and securing individuals in a system (such as a network, or an enterprise) by controlling their access to resources within the system by associating user rights and restrictions with their established identity.

Cyberoam UTM's identity-based security and network access management paradigm offers extensive visibility and perfect controls over the network traffic even in DHCP and Wireless environments through its granular policies.

Cyberoam's Automated SSO

Cyberoam's Automated Single Sign On ensures that the end user logs on to the UTM appliance transparently when he logs into his computer. Once logged-in, the user can safely use all the permitted protocols while the usage are monitored and logged. There are no exceptions and hidden limitations.

ASG's Browser Dependent Limited SSO

ASG's SSO is "only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the HTTP proxy in their browser configuration." (Quoted from ASG's Online Help)

Further the online help states: "the proxy cannot handle FTP and HTTPS requests in this mode." So the SSO is only applicable for HTTP over IE browser. For all other protocols, specific firewall rules have to be created to accommodate them.

"To support such traffic, you must either use a different mode or enter an explicit packet filter rule allowing them." ASG's Online Help states

No Pharming Protection in Astaro

Pharming leads unsuspecting users to look alike malicious sites which foxes the user to unknowingly divulge personal information which is later used to financial gains.

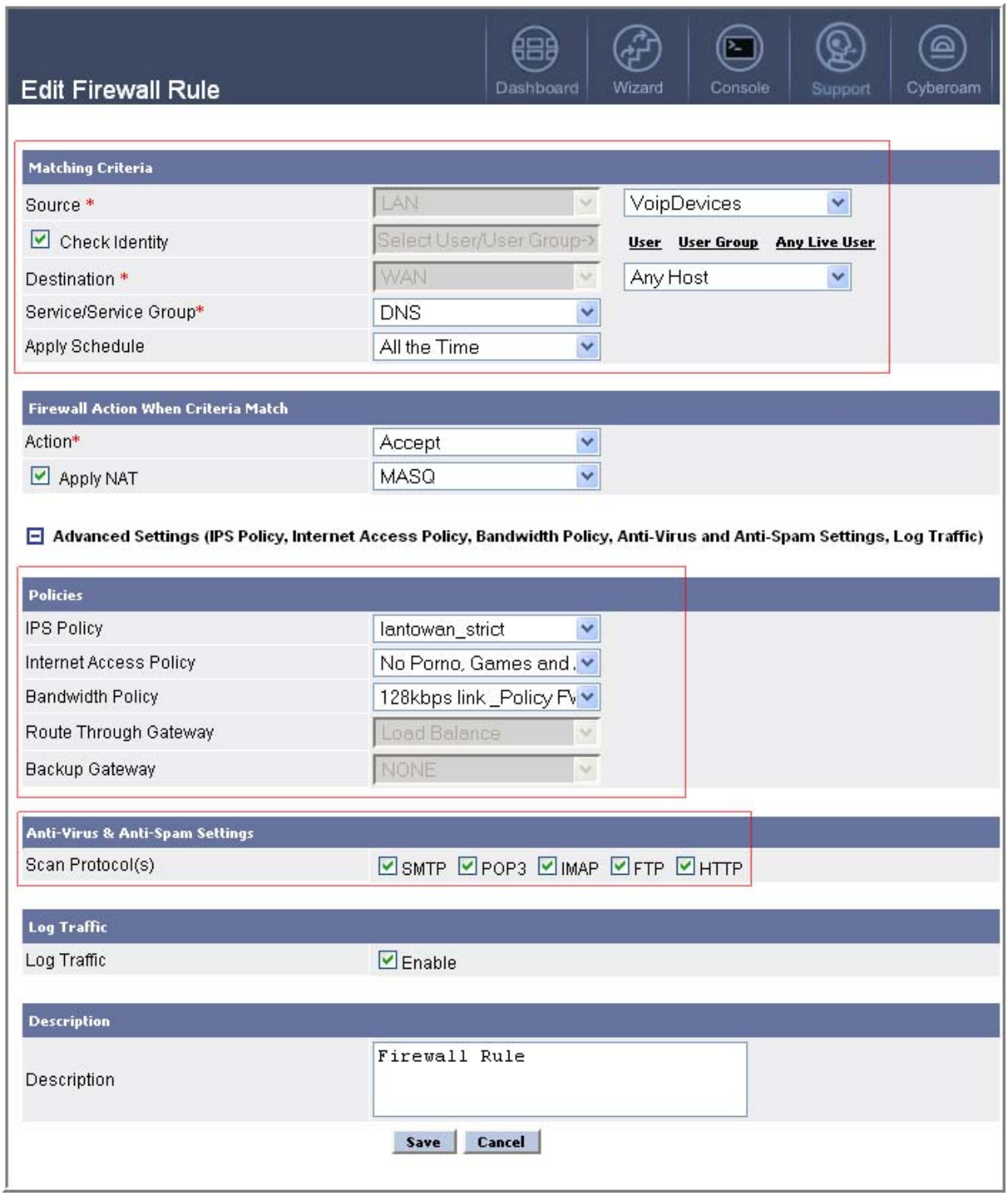
Cyberoam	ASG
Cyberoam verifies every surfing request with a preconfigured DNS server, to ensure that an end user's sabotaged host file does not redirect him to a Pharming site.	No Pharming Protection

Cyberoam's Tunable IPS Policies

Cyberoam	ASG
Cyberoam supports identity based IPS policies.	No customization possible.
Cyberoam supports multiple IPS policies, i.e. different IPS policies for users and different for servers.	ASG offers only inflexible blanket policies
Cyberoam supports custom signatures.	No support for custom signatures

Cyberoam's Fusion Technology Driven UTM

How would you configure a custom anti-spam and anti-virus policy applicable through firewall for a particular user? In Fusion technology driven Cyberoam, go to the firewall. It has a central control over all the member security solutions.



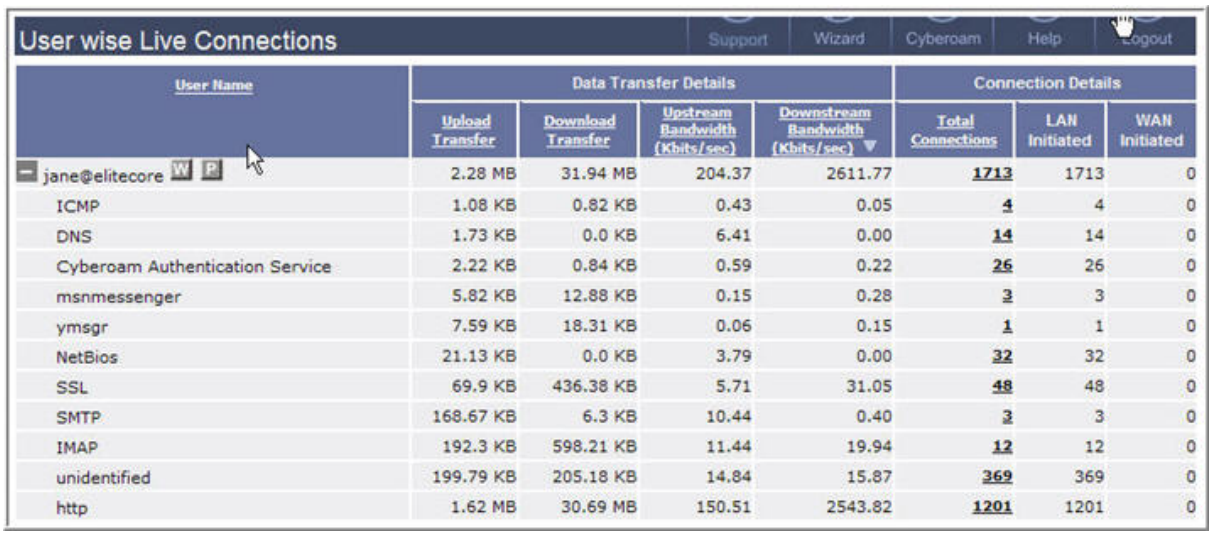
ASG has no such central point of integration and no user-based custom policies are possible in ASG.

ASG does not have Traffic Discovery feature

Cyberoam's Traffic Discovery feature enables real time visibility of bandwidth consumption and data transfer for every:

- User
- IP Address
- Application

Check a sample screen shot given below.



User wise Live Connections

Support Wizard Cyberoam Help Logout

User Name	Data Transfer Details				Connection Details		
	Upload Transfer	Download Transfer	Upstream Bandwidth (Kbits/sec)	Downstream Bandwidth (Kbits/sec)	Total Connections	LAN Initiated	WAN Initiated
jane@elitecore	2.28 MB	31.94 MB	204.37	2611.77	1713	1713	0
ICMP	1.08 KB	0.82 KB	0.43	0.05	4	4	0
DNS	1.73 KB	0.0 KB	6.41	0.00	14	14	0
Cyberoam Authentication Service	2.22 KB	0.84 KB	0.59	0.22	26	26	0
msnmessenger	5.82 KB	12.88 KB	0.15	0.28	3	3	0
ymsgr	7.59 KB	18.31 KB	0.06	0.15	1	1	0
NetBios	21.13 KB	0.0 KB	3.79	0.00	32	32	0
SSL	69.9 KB	436.38 KB	5.71	31.05	48	48	0
SMTP	168.67 KB	6.3 KB	10.44	0.40	3	3	0
IMAP	192.3 KB	598.21 KB	11.44	19.94	12	12	0
unidentified	199.79 KB	205.18 KB	14.84	15.87	369	369	0
http	1.62 MB	30.69 MB	150.51	2543.82	1201	1201	0

Bandwidth Management Comparison

Cyberoam	ASG
Cyberoam supports identity based Bandwidth Management Policies.	ASG does not support this feature.
Cyberoam supports eight (8) levels of priorities in Bandwidth Management.	ASG offers only offers two (2) levels of priority.
Cyberoam supports application based bandwidth management.	ASG does not support this feature

Complimentary to Compliance

Cyberoam's Web Filtering and On-Appliance Reporting are directly complimentary to compliance. It supports CIPAA, HIPAA, GLBA, SOX, PCI, and FISMA. All these facilities are provided at no extra cost. Apart from that if required, Cyberoam also supports its proprietary external reporting module.

Astaro does not provide any of these facilities.

Head to Head Comparison:

Points to Ponder	ASG	Cyberoam UTM
Enhanced Firewall decision Matrix: Firewall is a primary security component in network security. If the decision matrix is expanded to take more parameters into account, the network control gets augmented. In the blended threat scenario where a user is targeted; identity is an important decision and control parameter.	ASG has an IP address based firewall. Policy based decision matrix is partially available, but is quite inflexible and the GUI, once more, makes it unwieldy.	Cyberoam, in a paradigm shift, extends the firewall's rule matching criteria to include schedule and the user's identity. 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.
Identity-based Access Management - The Best ROI for Internet Resources: IAM is a combination of Identity, time scheduling and access management. This is a very potent combination when all the UTM constituent solutions use it. This feature provides unparalleled flexibility and security.	ASG has an option of Time Events under Definition section. However it is only applicable to the firewall policy. It is not used at a granular level to control the other security features of the UTM.	Cyberoam's identity-based access management feature is one of its strongest features as it is a control mechanism running common in all its member security solutions. Schedule based access reaches down to the policies in all the solutions providing seamless flexibility. The cyclic access feature ensures that a single student does not corner the Internet resources in an educational institute.
Adaptable AV/AS Scans: For most users, missing a legitimate email is an order of magnitude worse than receiving spam or virus. There are times, you need a mail and it gets classified as a virus or a spam. This is detrimental and you should have the right to choose, what to allow and block. The gateway AV/AS should also watch over the full mail protocol spectrum which includes SMTP, IMAP and POP3 to guarantee complete mail security.	ASG has two independent anti virus engines: one for email and virus protection and second for Web security subscriptions. 1. AVIRA 2. Clam Anti Virus (Email Virus Scanner) In this maze of AV engines, the integration and granular control over them is lost. ASG does not support IMAP protocol.	Cyberoam UTM has an OEM with Kaspersky Labs and it uses Kaspersky's Gateway AV. It is one of industry's best gateway antivirus solutions. Using Cyberoam UTM you can define custom spam filtering rules based on sender or recipient, IP address, mime header and message size. Cyberoam UTM also utilizes configurable RBLs for complete anti-spam coverage. You have the flexibility to configure a spam scan as per your needs, rather than adjusting yourself to the way a security solution operates. Cyberoam UTM watches over the complete protocol spectrum.

Points to Ponder	ASG	Cyberoam UTM
Identity-based IPS Policies and Reporting: To deploy security rules and policies the administrator has to know his target. IP addresses are not target enough. Most potent intrusion attempts are attempted from inside a network. In IP address based IPS reporting the identity gets lost.	ASG does not have identity based IPS reporting and control.	Cyberoam UTM provides IP address and User based reports. Providing complete visibility, it thwarts anonymity in DHCP, Wireless and Computer sharing environments, and in case of threat detection; it reduces the administrator's reaction time. You can contact the erring user and educate him too.
Tunable IPS Policies and Custom IPS Signatures: Blanket policies, over time force you to open security loop holes. Customized policies provide you the comfort to deploy customized IPS policies as per your needs. Custom IPS signatures reach deeper than a firewall and antivirus to protect the network.	ASG has blanket IPS policies which do not provide any leeway to the administrator. It does not have the facility to import and use custom IPS signatures.	IPS can be plagued by false alarms. Cyberoam UTM provides you the ability to attach an individual IPS policy to a combination of source, destination, application, identity and schedule. This leads to customization of each IPS policy as per your needs and better security. Cyberoam UTM can also use custom IPS signatures.
User and Policy based Bandwidth Management: A Bandwidth management solution should provide the flexibility and power for policy based bandwidth management. Bandwidth management is not mere traffic control. It is a well known fact that unplanned bandwidth addition without intelligent management, does not help.	ASG has no granular bandwidth management.	Cyberoam UTM provides user and policy based bandwidth management. It also provides individual upstream and downstream bandwidth control. Using Cyberoam UTM 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. Cyberoam UTM has user-wise bandwidth distribution and control over bandwidth usage individually both: Upstream and Downstream
Data Transfer Accounting and Control: Data transfer accounting and control helps you see the actual bandwidth consumption by an individual or an application. This feature also helps find the exact Internet usage costing in case of fixed data transfer quotas.	ASG does not have this feature.	Cyberoam UTM 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.
Gateway Failover and Load Balancing: In case of multiple ISP links, a failover solution is indispensable. However the criteria for classifying an ISP link as "non-working" are critical. There are times that a mission critical application is unreachable through a specific ISP link, while the same is reachable through the other one. In this case the failover solution should take over. In case of multiple gateway support, load balancing is indispensable.	ASG does not support multiple gateways. It can only support two (2) WAN links.	Cyberoam UTM supports complex rules to check the network status of a particular application. Cyberoam UTM can detect and mange a link failure for the true use of Internet.

Points to Ponder	ASG	Cyberoam UTM
Single Sign-On Support: Single sign-on is the tool to identify a user in a security system. It not only authenticates a user, but also creates a security bubble which can be audited and secured.	ASG has browser dependent limited SSO	Cyberoam UTM supports external ADS, PDC, LDAP and Radius and Local. Cyberoam supports Client-based and Clientless Automated Single Sign-On.
File Transfer Control over IM: 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.	ASG has blanket policies and lacks granular control.	Cyberoam UTM's application filtering solution is powerful enough to control file transfer over any IM application. In the recent version, it can log and control total user behavior over Yahoo IM.

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 products.

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: 9.0 – 95838 – 03/02/2009