Overview

Introduction : In today's organization, application, employees, vendors, clients, and security threats fight for the same network resources. It has become difficult for small to medium enterprises to manage their infrastructure as they are unable to distinguish between good traffic v/s bad traffic. Threats or various productive applications have become smarter as they camouflage data transfer using standard internet ports. GajShield's Unified Performance and Threat Management devices give the power to organizations to improve the end-user experience in accessing information. Its patent pending technology provides an insight into the network infrastructure and helps them to make intelligent decisions. It is the only security solution which gives an administrator the power to load-balance, wan auto-failover on a per service. The smart engine correlates the information provided by security engine, network monitoring engine, deep inspection stream analyzer, wan availability, behavior analysis engine to provide real-time knowledge into the network.

There is a big challenge for any network administrator to detect threats quickly and to contain them proactively. Current day security devices lack the intelligence to pinpoint the attacked resource. Loads of logs are dished out giving no indication of the problem. Threats can cause direct and indirect productivity loss. For example, systems which are infected by spyware or viruses load the network causing choking and loss of productivity for others in the network too.

Productivity loss is not always because of external threats. Many organizations lose valuable business time when network connectivity becomes slow due to employees visiting not relevant internet sites. One employee can affect others in the network. To quickly detect and take proactive action is the need of the hour. This is what most security devices lack today.

GajShield is the only security device which quickly identifies threat, and gives you the tool to curb or block it. With its unique technology which detects Threat using Distributed Network Behavioral Analysis (DNA), all organization under the GajShield security umbrella are provided quick threat identifiers and provided a mechanism to block them and improve the performance of your network, applications and users.

How does GajShield help in improving performance in an organization

Growth in the available WAN & Internet pipes capacities and speeds though have not been able to keep up with business usage.

This has created a very big GAP between business demand & the network's ability to supply. The loss of users productivity because of the "wait for Application" due to the bandwidth not being available for business critical application completely erodes the savings generated by lower bandwidth costs.

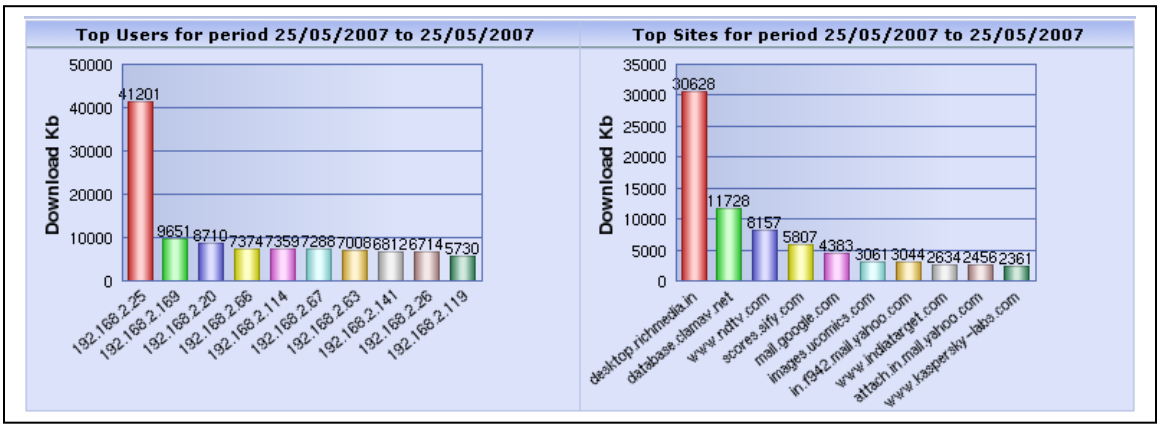
The "wait for application" is calculated based on how much time is spent by users waiting for an application to respond. Crores for rupees are lost in employee productivity per annum for an organization of 200 users with a mere 10 minute delay daily.

GajShield deep inspection engine inspects all the packets passing through the UTPM and classifies the various packets based on categories and not just based on the ports. For example : GajShield would identify from the port 80 traffic (Browsing port) that the packet was of Skype or Spyware or it was a web site. It would classify and segregate the above traffic based on the applications, websites and users. This give a comprehensive view of what network resources are being used by which applications or users. Further classification of the network resource is done

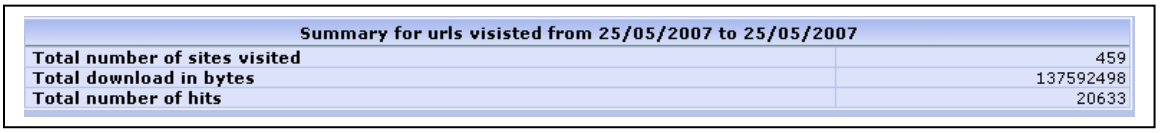
based on available ISP's (Internet Service providers), Applications, Users and the Top ten usage.

As an organization which allows internet access to it's employees it is important to look at the various behavior analysis to provide proactive performance management to organizations. Let us look at the various behavior analysis done by GajShield Unified Performance and Threat Management Appliances.

Organization behavior (Categories visited)
GajShield UPTM inspects and provides find out whether the utilization is for business or for non-business usage. The analysis would should the Top ten users who are doing the maximum downloads for a specified time-frame and the Top ten website from where the maximum download has been done. This enables the administrator to find out if the bandwidth is being abused because of any website or any users.

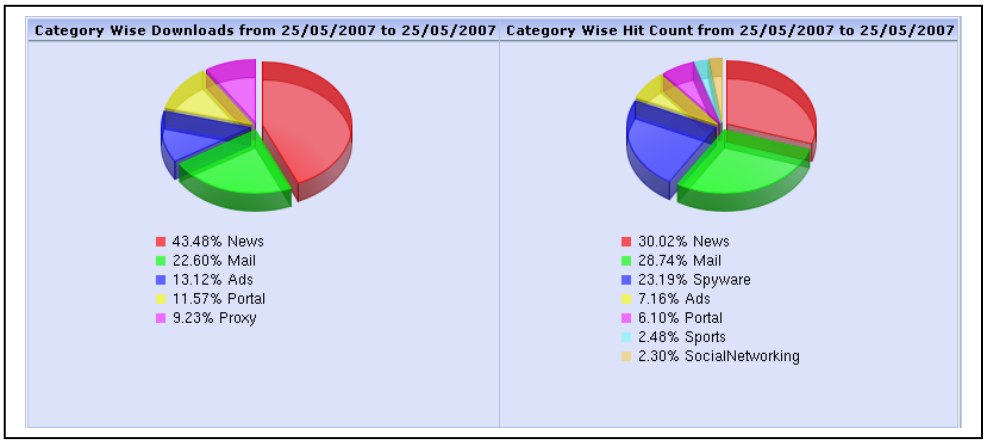


Shows the summary of the number of websites visited, total size of downloads through web browsing which help in administrators in zero down whether browsing is creating a bandwidth choke.



Summary for urls visisted from 25/05/2007 to 25/05/2007	
Total number of sites visited	459
Total download in bytes	137592498
Total number of hits	20633

GajShield UPTM would analyse top categories from the bandwidth utilization point of view and Website hit count of view. This will help in analyzing whether the bandwidth utilization is for business or non-business purpose. Also helps in finding out if there are any rouge applications being used in the network.

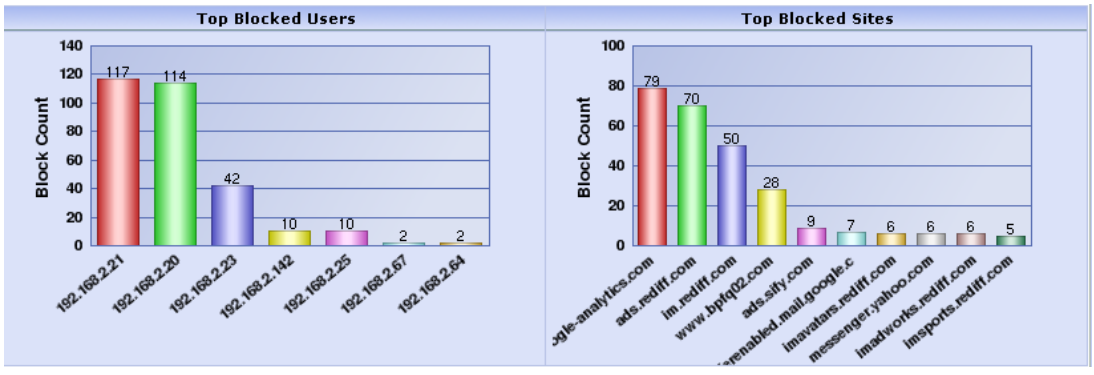


Increased User Productivity - User behavior (Top users)
Once this is known then the administrator can shape, regulate of stop the misuse by the users or block the non work related websites or increase the bandwidth if the usage has increased genuinely.

User	Hit Count	No. of Urls	Download (Bytes)
192.168.2.25	5771	120	44588882
192.168.2.111	3432	64	5631854
192.168.2.63	2072	65	7217203
192.168.2.67	1934	73	7463820
192.168.2.66	1792	57	9454030

URL	Hit Count	No. of Users	Download (Bytes)
www.ndtv.com	3494	2	8936317
mail.google.com	3345	11	4644658
www.mvpsf.com	2502	1	912834
scores.sify.com	909	1	6904257
images3.orkut.com	749	7	1777819
us.i1.yimg.com	648	13	1275632
ads.rediff.com	638	9	1232681

Enhanced Security - Block Categories (Infected sites)
User productivity is important to organization and along with it is important that security problems are identified quickly so that the administrator can take pro-active security measure. Using the indepth information available in the GajShield UPTM the administrator can quickly find which systems are infected by spywares, adwares, etc. and also if any users are persistently trying to access the unacceptable sites as per company internet policy.

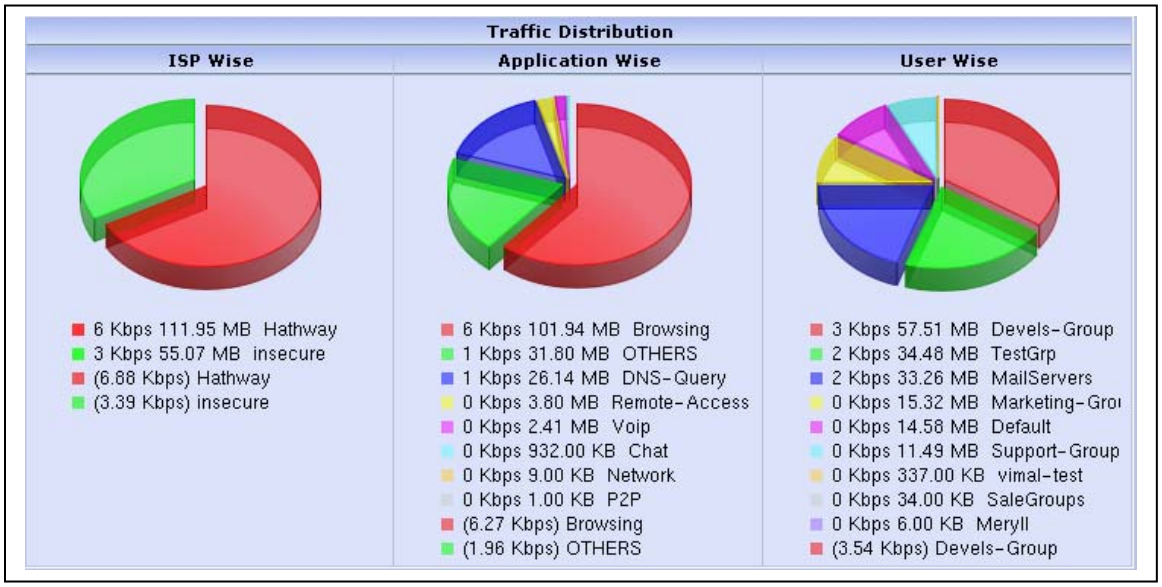


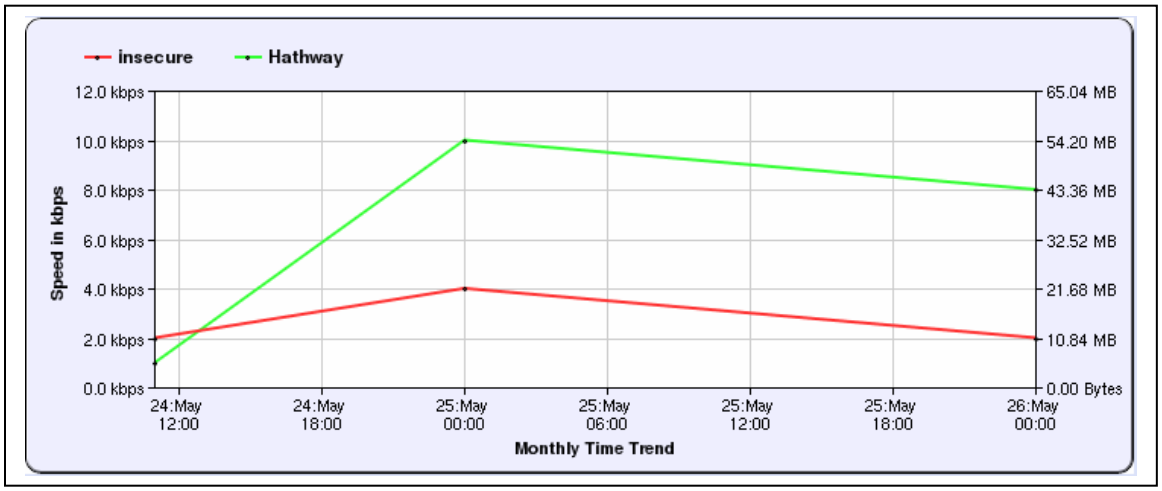
Date	Block Count
26/05/2007	297

Category	Block Count	User Count
Ads	165	3
Chat	5	3
Ecommerce	5	1
InstantMessaging	8	2
MobilePhone	5	1
Sports	7	3
Spyware	28	1

Date	Time	User	IP	URL	Status	Comment
20070526	17:50:41	-	192.168.2.23	http://www.google-analytics.com/urchin.j	Blocked	Site in Blocked Category Ads for group Support-Group
20070526	17:25:41	-	192.168.2.23	http://www.google-analytics.com/urchin.j	Blocked	Site in Blocked Category Ads for group Support-Group
20070526	17:18:21	-	192.168.2.23	http://ads.yimg.com/us.yimg.com/i/us/sea	Blocked	Site in Blocked Category Ads for group Support-Group
20070526	16:52:16	-	192.168.2.23	http://www.google-analytics.com/urchin.j	Blocked	Site in Blocked Category Ads for group Support-Group
20070526	16:51:01	-	192.168.2.23	http://www.google-analytics.com/urchin.j	Blocked	Site in Blocked Category Ads for group Support-Group

Many factors affect the continued growth of network traffic – corporate initiatives like VoIP, new application implementations such as an ERP, and even recreational usage like streaming radio or video. These business changes, along with technology innovation, have led to an explosion of new, bandwidth-intensive applications and an increased probability of network congestion – a significant risk to business processes. Without information on what applications are consuming bandwidth corporations are forced to upgrade to higher and higher speed networks. With the GajShield you can report on and analyze growth trends and usage patterns in order to make decisions about optimizing bandwidth, rescheduling activities, reallocating traffic, or even creating usage policies. This provides the justification for capacity planning and allows you to keep your budget in check.





The benefits of Capacity Planning

- **Proactively combat network congestion** by reporting on bandwidth growth and forecasting capacity shortfalls
- **Provide quantifiable business justification** by understanding and reporting on which applications consume your network resources in order to postpone upgrades and justify growth & upgrade decisions

- **Tune traffic to optimize resources** by identifying over- and under-utilized WAN links so you can redistribute load and reduce costs
- **Curtail network misuse** for better network utilization by identifying and reporting on non-business uses of the network

Pro-active Security - Trend analysis of ISP, Users, Applications
Various applications such as MP3s, streaming video, and online chats require a great deal of bandwidth and can seriously affect the network's speed and performance. Spyware, Adware & P2P increases the bandwidth cost as well as making systems and applications slow. This typically calls for the administrator to either increase the bandwidth or regulate the users. Hence it requires an organization to identify the bandwidth consumption user wise and identlfy the bandwidth hungry users and applications. Drill down to find out the abusive users based on the downloads and the websites . Once this is known then the administrator can shape, regulate of stop the misuse by the users or block the non work related websites or increase the bandwidth if the usage has increased genuinely.

Auto-failover/Load balancing

Networks and application delivery mechanisms are extremely sophisticated, with an intricate interdependence of diverse, multi-vendor infrastructure components and technologies. Similarly in an organization not all the services are equal, some would be business critical, some non-business critical and hence blanket policies in terms of WAN link failover and load balancing loses it's value because if even the non business critical applications are in failover that would affect the performance of the business critical applications. GajShield UPTM empowers the administrator to define WAN Failover & Load Balancing on per service hence enhancing the performance of business critical applications. The administrator may want to load balance the business-critical applications between those WAN link which have higher bandwidth and non-business critical applications via lost cost Broadband connections.

The benefits of Policy based WAN fail-over & load balancing are as follows :

- Improve performance of business critical applications through Service based Load Balancing or failover
- Reduce expensive cost of upgrade by load balancing non-time critical services like FTP, Email through broadband connections
- Achieve 100% application uptime for business-critical services.
- Increased User productivity because of enhanced application response.