

## Managing Bandwidth - The User based approach

### Are you facing problems in handling any of the following situations?

- Unable to deliver/allocate bandwidth to the needy Users
- Unable to deliver/allocate bandwidth to each user according to their needs
- Unable to control the heavy downloads of Music & Video files
- Facing reduced employee productivity problem due to chatting and mailing activity not related to work

- Small number of users consuming the majority of Bandwidth & robbing others
- Unable to put a check on non-work related traffic

If Yes, then you are not the only one, but sailing in the same boat of Network Managers across the world.

Above mentioned are a few examples of the huge potential time waster for Employees and bandwidth issues for the Network manager.

### Cyberoam and Bandwidth

In the battle for Bandwidth on Internet access links, Users consuming huge bandwidth for non-business related work can so flood the capacity that the Business-Critical Users are completely undermined. Abundant data that swell to use any available bandwidth, network bottlenecks, and bandwidth hungry applications.... all seem to conspire against network performance.

This whitepaper discusses how Cyberoam delivers centralized bandwidth control, optimized Network performance and increased productivity to IT Organizations.

### Addressing the Problem

The very first solution for bandwidth unavailability is to “add more bandwidth”. However, simply adding bandwidth does not solve the problem. Bandwidth Abusers will consume more if you add more and the problem remains. This leads to another solution “add more management”. “Add more management” is a better long-term strategy than simply “add more bandwidth”.

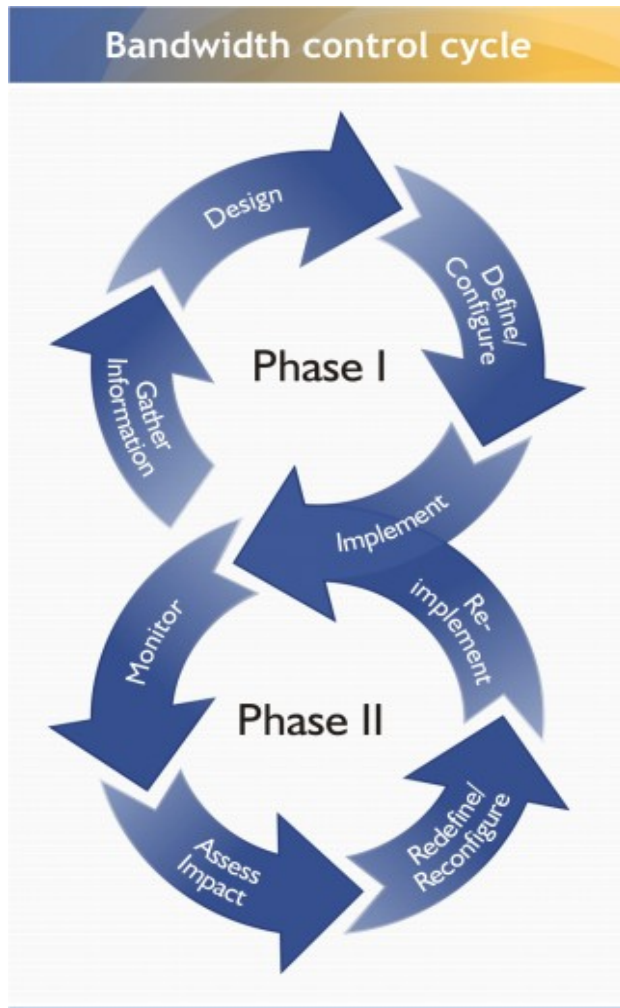
Identifying the problem is the first step and finding the solution is another, but finding the solution is not enough. Cyberoam gives you the ability to implement “add more management” and helps solve the problem.

Cyberoam helps to evaluate the traffic and regulate its flow through the Network in accordance with pre-established management policies. The objective is to maximize the throughput and minimize the bandwidth wastage & unutilization.

Various approaches to this type of Bandwidth management are articulated below that can be attained with the help of Cyberoam.

#### Cyberoam Solution Components

- Allocate committed bandwidth on per-user basis
- Automatically allocate unutilized bandwidth (Burstable policy)
- Schedule Internet access based on time and day and control bandwidth
- Block Streaming media files and recreational web surfing
- Limit uploads and downloads
- Block Virus Signatures & pattern
- Optimize Network performance by Caching



Cyberoam Bandwidth management provides the method for observing data traffic flowing through the network, evaluating that data for potential network capacity concerns, and then making bandwidth throttling, priority, and traffic-filtering decisions based on a set of usage policies.

Cyberoam controls bandwidth allocation with a tremendous amount of flexibility and power and helps Network managers effectively manage, monitor and control the available bandwidth. It can provision bandwidth on per-user basis.

Each user maps to a bandwidth allocation policy which ensures an appropriate bandwidth slice and allows Business-Critical Users higher priority and more bandwidth than the typical User.

## Cyberoam Approach

### User-based Bandwidth Management

Corporate Networks must support myriad applications, but not all the applications have a direct relation with the business activities like:

Business applications can also have non-critical aspects - Email, File transfers

Frivolous applications can also have a business aspect Chatting & Audio-visual presentations

In view of the above scenario, controlling only the Application access will not be sufficient; you need to control individual User's access to the Internet i.e. you need to place bandwidth limits as well as deny access based on content type.

E.g., you want to allow marketing group to view high bandwidth streaming media, but allow the Accounting group to view up to only 64k OR block MP3 files for everyone except Webmaster OR block MP3 files from being downloaded.

### How?

- Identify User
- Identify traffic that will be generated
- Identify Content type
- Allocate/reserve bandwidth
- Deny/Allow access to Content type

If employees are waiting to download Excel or Visio files while the Webmaster tests his/her development Web content, frustration will be felt by all due to the slow-down in performance. Isolating the Webmaster from the rest of the staff can help better bandwidth utilization.

Because the control is placed on per-user basis, whenever the User requirement changes, only the User's policy needs to be changed. This also ensures consistent control on the User's access i.e. the access control is applied irrespective of the time and place from where User logs in.

## Cyberoam User Definition

Different Users have different needs for Internet access. You cannot control User access without knowing User's need and for this; you need to identify which User needs to access for what purpose and during which time slot of the day. Once you identify such Users, you can block access for the remaining Users.

For any Organization, one can divide Users into three types:

- Business-Critical users
- Business-Non-Critical Users
- Bandwidth Abusers and they need to be prioritized and provisioned differently.

Cyberoam peeps into all the Web requests & responses, gathers the complete details on the transaction between User and Server, and produces report on Users and their bandwidth usage. These details can be utilized to identify Users and traffic generated by them.

## How do you differentiate between Users?




Cyberoam helps Network managers recognize and differentiate between the Users by

- Monitoring the traffic on your Network
- Reporting traffic trends
- Keeping track of the Users who generate the most traffic
- Keeping track of Bandwidth consumption

The User information gathered by Cyberoam includes:

1. IP address, Time & day of the request & response
2. Web page category
3. File type
4. Content type
5. Complete URL
6. Bandwidth utilized
7. History of all the requests

Based on the information gathered, various policies can be defined.

User	
	<p><b>Business-Critical Users</b></p> <p>Generate highest level of business-critical traffic Need consistent and predictable bandwidth performance</p> <p>They are the users who need bandwidth performance to do their job. Their work should not suffer because of unavailability of Bandwidth or the speed of Network.</p>
	<p><b>Business-Non-Critical Users</b></p> <p>Generate business related traffic Need less consistent and predictable Bandwidth performance than Business-Critical Users</p> <p>Their work will not suffer because of unavailability of Bandwidth or the speed of Network but need bandwidth.</p>
	<p><b>Bandwidth Abusers</b></p> <p>Generate more non-business related traffic Need minimum bandwidth Actually, consume maximum bandwidth</p> <p>Because of them, Business-Critical Users suffer as their applications take more time to process and have to wait, which leads to productivity loss, and finally the organization suffers.</p>
<p>Business-Critical Users should get the highest priority while Bandwidth Abusers should get the lowest priority for bandwidth and Internet access.</p>	

## Bandwidth Management

## Challenges & Cyberoam Solutions

### Challenge 1

Allocate required bandwidth to the Business-Critical Users every time

- Identify Business-Critical Users
- Make a Group of Business-Critical Users (If more than one)
- Define Committed Bandwidth Policy

This is the way you can ensure constant and required bandwidth to the Business-Critical Users and automatically allocate unutilized bandwidth

- Identify Bandwidth Abusers
- Make a Group
- Define Bandwidth Policy and allocate minimum bandwidth

### How it works:

One, it guards the Bandwidth need of Business-Critical Users by guaranteeing certain amount of bandwidth every time and two, it ensures Bandwidth Abusers get minimum bandwidth and cannot play with the bandwidth at the cost of work.

Committed bandwidth is the bandwidth that User will get every time i.e. guaranteed bandwidth

Burstable bandwidth is the maximum bandwidth that the user can draw, if available.

### Challenge2

Restrict Internet access and control bandwidth of the Users other than Business-Critical Users specifically during the Peak hours

- Check Data transfer trend
- Identify Peak hours for the Organization workload
- Determine maximum data transfer
- Identify Users other than Business-Critical users performing maximum data transfer at peak hours
- Define Schedule of Bandwidth policy for the identified Users that restricts:

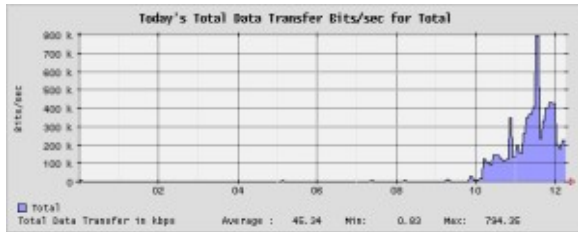
1. Access within certain defined period only e.g. can access between 12 AM to 2 PM only and not throughout the day
2. Bandwidth usage during that defined period



### How it works:

One, it restricts other than Business-Critical Users from using maximum bandwidth during the peak hours and two,

Handles peak hour traffic load with improved response time



### Above solution can also be used to:

- Schedule the bandwidth usage of Business-Non-Critical Users during any time of the day
- Restrict the bandwidth usage of Bandwidth Abusers

### Challenge 3

#### Block non-business related traffic

- Non-business related traffic can be defined as
- Non-business related contents like advertisements, unwanted information
- Sites like Music, Chatting, Online Shopping & Gambling
- Any site or content, which consumes too much bandwidth
- Check the surfing trend like maximum non-business related sites surfed and data transfer
- Identify sites
- Identify Content types
- Identify file types
- Define Web category with site names, file types, keywords
- Define Security policy and attach Web category

### How it works:

Blocks non-work related contents that could reduce Employees productivity, network speed and consume unnecessary bandwidth.



### Challenge 4

Increase Network speed using Cache and gain bandwidth, Accelerate web content & save cost

Web servers are responsible for delivering web content to the Users. However, under the pressures of rising traffic volumes, richer content types and increasing user expectations, these server-dependent infrastructures experience significant strain.

### Benefits

#### Optimized Network performance

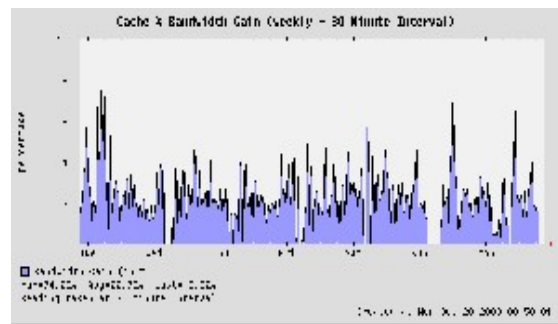
Speeds end-user response time by decreasing bandwidth consumption

#### Policy based Caching

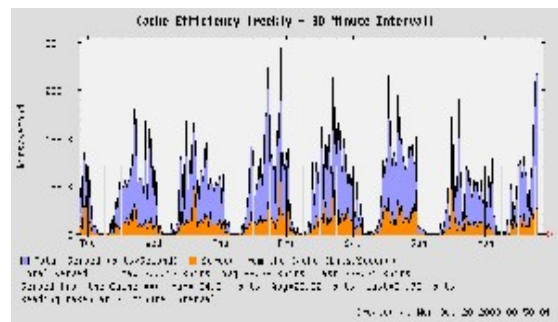
Cache is controlled by Category based lists. Each Category can contain one of many matching patterns/URL, followed by an action. This makes configuration of the Cache Server extremely flexible

Cyberoam Cache server reduces the strain on Network and significantly improves the end-user response time.

A HTTP Cache helps in improving the performance of network by reducing web access time and web traffic. All visited static websites are cached on the Cyberoam server hard drive or in the memory.



Advantage: It will cache the static Web pages once requested and serve them locally when they are requested the next time. Web caching enables up to 35% bandwidth gain and faster response time.



## Challenge 5

### Block Virus signatures and save Network from Virus attacks

Attacks to the Servers and Networks have occurred almost since the origin of the Internet. As Networks and Servers become more sophisticated, the types and sophistication of attacks grow. Exposure to the Internet means exposure to Internet viruses like Nimda, Fun love and Code Red. But, no longer do hackers just attack Web sites and servers directly. Today, viruses, worms, and other forms of attack enter through E-mail attachments, downloadable files, and embedded objects. The list grows constantly. If viruses enter the network, it can be down for hours or days.

Whenever a new Virus attacks, Cyberoam updates firewall and reconfigures the content filtering by adding the signature of the Virus in the block list. With the help of 'Cyberoam Auto Upgrade' feature, install the new version, which helps to minimize the impact of the Virus attack.

This not only stops the propagation but also guards against future attacks of the same virus.

## Impact of the Policies

How would you check whether the policy implemented is right and in tune with your requirements?

- Check Bandwidth utilization graph before & after the implementation of the Bandwidth policy
- Check User wise and Content wise
- Data transfer graphs
- Check User wise and Content wise Internet Usage graphs
- Check Web surfing graphs

Bandwidth utilization is directly related to the Network efficiency. Cyberoam provides the easy-to-understand & interpret graphs to check the bandwidth utilization.

It shows the history of bandwidth consumption in bits-per-second. This answers the question "How much bandwidth does my traffic typically take?"

It also displays average & peak bandwidth consumption over a time. It also shows the amount of bandwidth not utilized or wasted. By checking the peaks, you can see if the traffic is frequently hitting a capacity limit and get an answer for the questions like:

- "Does the usage vary a lot?"
- "What are my average bandwidth needs?"
- "I have xxxx kbps bandwidth is all that bandwidth really needed?"
- "How frequently is my bandwidth insufficient?"
- "How much bandwidth remains unutilized most of the times?"

## Conclusion

With the right policies in place, Organization saves cost by reducing bandwidth unutilized, increases Network efficiency and improves productivity.

An effective policy is the one that balances the need for information access, respect for privacy, and the mission requirements of the organization.

Reducing or eliminating non-business-related network traffic will mitigate the need to add network resources so that the Business-Critical Users are not impacted.

In addition, allowing only the content that cannot be considered threatening will reduce an organization's exposure to the growing attacks of Viruses. Lastly, an appropriate policy ensures that the internal network remains secure.