Managing Corporate Internet Access

Why Internet Access Management ?
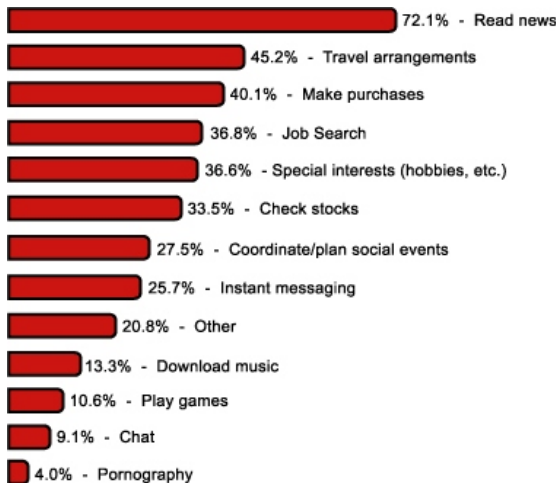
Not so surprising statistics

- 70% of porn is downloaded between 9am and 5pm SexTracker
- The number of hacking sites grew 45% in the past year Websense Survey
- 1 in 3 companies have detected spyware on their network UK Survey
- 80% of network security managers claim their biggest security threat comes from their own employees Gartner
- 5 billion music files were downloaded from P2P networks - Yankee group

17th August 2001, Perth, Western Australia:

Figures recently released by The Computer Security Institute (CSI) in their sixth annual "Computer Crime and Security Survey." again show a trend of increased abuse of employee Internet Access privileges.

Use

What non-work related functions do you use your Internet access at the office for? Source: Vault.com Internet Use Survey of 451 Employees, Fall 2000

- 72.1% - Read news
- 45.2% - Travel arrangements
- 40.1% - Make purchases
- 36.8% - Job Search
- 36.6% - Special interests (hobbies, etc.)
- 33.5% - Check stocks
- 27.5% - Coordinate/plan social events
- 25.7% - Instant messaging
- 20.8% - Other
- 13.3% - Download music
- 10.6% - Play games
- 9.1% - Chat
- 4.0% - Pornography

Internet has become extremely widespread over the several past years. With all its advantages, it may become pure loss for a company unless controlled and managed properly.

Organizations using Internet as a business tool need to address certain issues like:

Productivity lost
- Gaming, Shopping, Gambling
- News reading, Chat rooms, Emails
- Pornography

Bandwidth Abuse
- Music, Movie heavy downloads

Increased Employees dissatisfaction

Productivity

Internet access is available to employees in the majority of companies however controlling their access can be difficult.

- Employees everywhere are wasting time by using Internet for
- Personal non-work related surfing
- Chatting
- Online shopping and gaming
- Stock trading
- Swapping music files
- Accessing pornography

This has become an increasing problem in offices and effect employee productivity, thus affects the corporate performance.

Data security

Using Internet for communication and client interaction exposes corporate resources to security vulnerabilities. Question of data integrity arises whenever the business sensitive data transfer, outside the corporate network is involved.

Apart from the official data transfer, sharing of organization's data & information through emails & chats have made Organizations re-think on controlling the access to email & to chatting application.
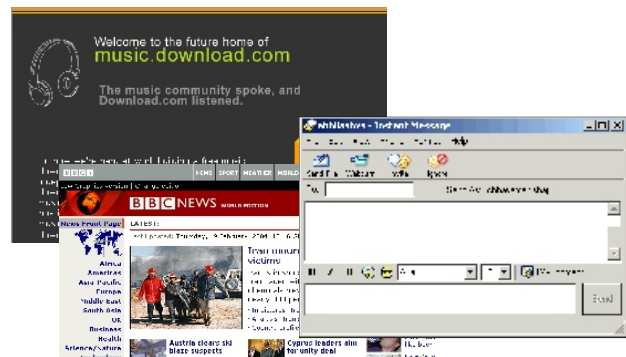
Why Internet Access Management ?

Increased Employees dissatisfaction
Different employees have different needs for Internet access. When the Business-critical Users do not get the required bandwidth or network performance, dissatisfaction level increases.

Bandwidth management

Bandwidth continues to be a costly resource that must be used as aggressively as possible to boost network efficiency and reduce network-operating costs.

Heavy downloading, online gaming can take its toll on network performance, as they are the bandwidth eater applications. Lack of responsiveness often results in large amounts of traffic used by a small number of Users. Sometimes even a single user can bring an entire Network to a crawl, as it gets flooded with traffic.

However, it is not always because of a malicious user trying to bring the network down. It can also happen if the user and network administrator have no way of controlling the bandwidth used.

This white paper provides useful background information on Internet access issues and discusses how Cyberoam delivers centralized control, unprecedented visibility, greater coordination and increased productivity to IT organizations.

What are the common ways to turn Internet access from loss to profit?

Clear definition of who may access Internet, at what time and day of week, reasonable limitations of time and types of Internet services used.

In general, some basic questions need to be answered before defining the Internet access policy:

1. Who in the organization needs the Internet access? Which employees ?

2. What Internet services do the employees need?
    - Browsing/surfing ?
    - Email?
    - Chat?
    - Research activities?
    - Access to organization's data

3. What type of access do the employees need?
    - Full-time, periodic or casual?

Manage internal demands and resources according to the policies created i.e. who can do what, where and when

Cyberoam and Internet Access

Cyberoam helps in Internet access management. It monitors Internet traffic generated by each user, the time one spends on Internet resources and allows setting access limitations based on time and day of the week.

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

The User information gathered by Cyberoam includes:

1. Time & day of the request & response
2. Web page category
3. File type, Content type accessed
4. Complete URL
5. Total Data uploaded/downloaded
6. Bandwidth utilized
7. History of all the requests

Based on the information gathered, Network manager will be able to check the Internet access and data transfer trends and define various policies.

Cyberoam
- Monitors incoming and outgoing traffic
- Manages real Internet time
- Monitors Web access
- Manages User access
- Restricts access
- Generates reports

Cyberoam achieves above goals of

Productivity management
By blocking

1. Chat
2. Online Stock trading
3. Downloads Music & Entertainment
4. Advertisements
5. Online Games & Shopping

Bandwidth management
By blocking

1. Streaming media - Music
2. File sharing

Security management
By blocking

3. Malicious web sites

Cyberoam Solutions

Cyberoam Policies allows Administrator to define powerful policies based on almost limitless combinations of factors like:

- Individual users
- Groups of users
- Time of day
- Total surfing hours
- Protocol type
- Content type
- Bandwidth usage (for streaming content)

Challenge 1
Restrict Internet access

Cyberoam not only tracks and logs Internet activity, but proactively manage the access to the Internet. Usual way to control users is blocking Internet access after time quotas are exhausted. Besides this, Cyberoam also restricts Internet access based on the time or day of the week. In case the access is blocked, the user gets the page explaining why he was blocked.

1. Check Internet access trend
2. Identify User
3. Identify access time needs
4. Set schedule based on day of the week and/or time of day
5. Define Internet Access policy for the identified Users that retricts: Allow/Diallaow Internet access within certain defined period
E.g. can access between 12 AM to 2 PM only

How it works:
Restricts Internet access based on the time or day of the week
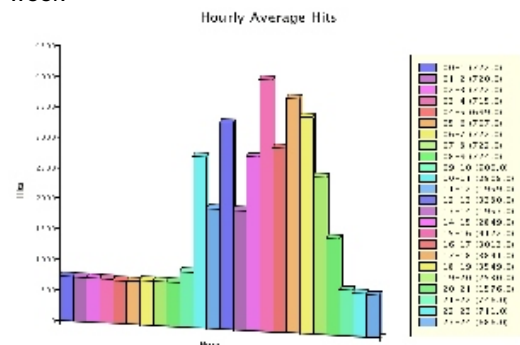
Challenge 2
Limit hours of Internet time

Cyberoam tracks and limit overall time, used on surfing the Internet resources

- Check Web surfing trends
- Identify User
- Identify surfing needs
- Set User surfing quota according to the needs Identified

1. Daily Quota restricts surfing hours per day
2. Weekly Quota restricts surfing hours per week
3. Monthly Quota restricts surfing hours per month
4. Yearly Quota restricts surfing hours per year

At the end of each Cycle, cycle hours are reset to zero i.e. for 'Weekly' Cycle type, cycle hours will to reset to zero every week even if cycle hours are unused/ not exhausted

- Define Surfing Quota policy for the identified Users that retricts the total surfing time
  E.g. can access for 2 hours daily throughout a month

How it works:
Allows Users to access Internet access only for the allocated time and blocks access after time quotas are exhausted.

Challenge 3
Block non-business related traffic i.e. deny or allow the access based on web categories

Cyberoam tracks Users requests to websites. Later on you may easily get the information where and when this particular user has been in the Internet by generating a report.

Non-business related traffic can be defined as

- Non-business related contents Like advertisements, unwanted information
- Sites like Music, Chatting, Online Shopping & Gambling
- 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

It also provides an added level of protection against malicious virus attacks by blocking the Virus signatures.

How it works:
Blocks non-work related contents that could reduce Employees productivity

Web category is the grouping of URL keywords for Internet site filtering

Cyberoam allows to categorize Web sites such as Games, Music, Chat etc.. Once the web sites and contents are categorized, access to those sites and contents can be controlled through policies.

Depending on the organization requirement, allow or deny the access to the categories with the help of policies by groups, individual user, and time of day.

Impact of Policies

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

1. Check Web surfing and Internet access trends before & after the implementation of the Internet access, Surfing quota policy.
2. Check User wise Internet surfing trend
3. Check Site wise Internet surfing trend
4. Check User wise and Content wise Data transfer graphs
5. Check Web surfing graphs

Internet access and surfing is directly related to the Employees productivity. Cyberoam provides the easy-to-understand & interpret graphs to monitor and control Internet access:

- Top Web Users
- Top Sites accessed
- Top Contents accessed and data transferred
- Trends

It shows the history of Internet access - user wise and site wise.

By checking the various reports and graphical trends, you will get an answer for the questions like:

"Does the usage vary a lot?"

"Who is accessing at what time?

"What is being accessed by whom?"
"How frequently is the non-work related traffic generated?"
"Who is generating the most of the non-work related traffic and when?"

"What web categories/sites need to be blocked during the work hours?"

"How frequently is the non-work related traffic generated?"

Conclusion

Each day, companies strive to correlate business decisions to things that actually happen on their network.

- Selecting which Users have access to which network resources
- Prioritizing, which User's Internet access is critical to the company operations
- Delivering differentiated services to each User according to their needs
- Managing the video and other data transfer demands
- Managing the overall flow of traffic through Networks

All of the above actions share a common requirement of applying business policies to Internet access management and security. Today, the Network manager must manage policies for all of these activities by managing a wide array of users and resources to determine policies and then configuring for each.

What is needed is a comprehensive, policy-based system that will allow the Network manager to define, in a concise and organized fashion, corporate policies that automatically effect change in the employee's productivity. And Cyberoam delivers that.

Cyberoam is designed to help you manage how your employees use the Internet through monitoring and reporting. It will help you in dealing with the lost productivity in a responsible manner that helps your organization to maximize the benefits of the Internet as a valuable business resource. Elitecore advocates a philosophy of responsible approach to Employee Internet Access Management that involves both monitoring and giving limitless/full/ access using an Internet Usage Policy.

Elitecore Product

Cyberoam
Unified Threat Management

Visit: www.cyberoam.com
Contact: info@cyberoam.com

USA - Tel: +1-978-465-8400, Fax: +1-978-293-0200
India - Tel: +91-79-66065606 / 26405600, Fax: +91-79-26407640

www.cyberoam.com