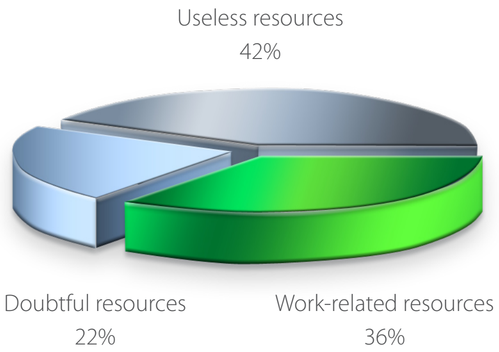
Traffic Filtering – First Step to Network Security



Most companies that extensively use the Internet in their day-to-day activities are now facing the issues of corporate local area network (LAN) protection, virus attacks from untrustworthy web sites, Internet channel traffic overload due to employees using the Internet for personal reasons, and optimization of Internet-related costs. Integrated control of Internet resources access can help manage and maintain Internet usage and guarantee the continuity and integrity of the business process.

Internet Abuse

According to statistics, employees of companies without flexible Internet access control daily use around 42% of overall Internet traffic to access useless and dangerous Internet resources, another 22% for web sites of doubtful quality; only 36% of traffic is used to access work-related Internet resources[1].

The leaders on the list of undesirable web resources are social networks, portals with obscene and adult content, online game servers, as well as web sites that generate so-called "heavy" traffic by prompting one to download and browse videos and flash-banners.

Along with the work time abuse, potential threats that result from the browsing of non-work-related web sites include:

- Excessive network load caused by the uncontrolled downloading of large-size files from the Internet. If a company uses a permanent or dedicated channel with a fixed data transfer rate, the browsing or downloading of video files from services like YouTube or file exchange networks can degrade the distribution of network resources and increase channel load as well as the cost of inappropriate traffic.
- Abuse of network resources and working hours by office employees involved in on-line gaming with video or voice chats.
- Uncontrolled remote connections established with corporate network servers via VPN or Hamachi-type utilities may infect a LAN with viruses from a remote PC.
- If no web site access control (including subject matter control) is established, it can downgrade corporate LAN security as internal resources and information are the most frequent subjects of threats and risks. Computer Economics reports that annual amounts of fiscal losses caused by different viruses are estimated in dozen billions of US dollars. For example, the annual losses caused by the Melissa virus attacks equals $1.10 Bln[2].

[1] BrightCloud, 2008, http://www.brightcloud.com/longtail.asp
[2] Computer Economics, 2000

Risk Zones

Potential risk zones for the spread of viruses, phishing attacks, information leaks, password theft and other spyware tricks have always included porn sites, regular social networks and blogs, entertainment portals and other adult web sites where thousands of new web pages get infected daily and new modifications of long-known threats appear.

For example, users of the social network VKontakte ("In Touch") were attacked by a "worm" in 2008 that forwarded a contaminated web site link from infected computers to the other users of this network.

In addition, WatchGuard Technologies[3] specialists believe "Users will be attacked from regular, unsuspicious, web sites that are unobtrusively infected through SQL-shots."

Viruses may infect a wide range of web sites with different categories of content, from cars, tourism, dating, movies and music to job search, real estate and other seemingly harmless sites on the world-wide web. Viruses from the infected web sites get into the computer of a single careless employee and can immediately spread over the LAN, sometimes causing a company irreparable damage.

According to statistics, most information leaks occur through employee negligence, while dedicated attacks make up only a small portion of such cases.

These are well-known facts, but Vault research indicates that around 87% of employees visit social networks and entertainment sites at work through official computers connected to a corporate LAN. More than that, over 50% of them does it at least once a day regardless of all the security consideration and place the entire LAN under threat[4].

From the work efficiency point of view, every 5-10 minutes of an hour employees spend on reading useless resources, browsing pictures and visiting forums add up by the end of each month to many lost hours of work for the company and a useless expense.

Traffic Filtering Processes

A company needs tools to control Internet traffic to maintain business security and integrity, eliminate potential information leaks and increase work effectiveness. The only proper solution in a struggle against chaotic and uncontrolled web traffic for any company is the filtration of web requests. By setting up network filters to deny access to certain web resources, a company will optimize work hours, reduce costs for the use of non-work-related Internet resources, and significantly minimize the risk of infecting the corporate local area network resources.

Most companies have long been trying to find and implement appropriate solutions that would help minimize external threats and control Internet access.

Founded in 2001, Entensys Corporation has been intensively working in the fields of Internet security solutions and web filters. The company is working in close cooperation with vendors of filtering systems and anti-virus software, and offers users up-to-date integrated solutions. As a result of this work, UserGate Proxy & Firewall[5] is being successfully used by thousands of large and medium commercial corporations, a wide range of governmental organizations and affiliated entities, as well as non-profit and educational organizations.

[3] WatchGuard Technologies, 2009, https://www.watchguard.com/latest/security-predictions.asp

[4] Research by Vault.com, 2005

[5] UserGate Proxy & Firewall is a complex software solution dedicated to the management of Internet access and network security. Read more details at the vendor's web site http://www.entensys.com

Flexible filtering tools developed by BrightCloud[6], the leading expert in category-based web content filtering are integrated into UserGate to allow the software to manage access permissions for different categories of web sites. BrightCloud's main database contains over 450 million continuously-updated web sites sorted by 70 basic categories[7], such as Online Dating, Games, Social Resources, Shopping, Traveling, Education, Business and Finance, Internet and others, including a trust rating for each category as well as multiple Internet resources in all major languages. Advanced support for Russian-language web sites is an important factor.

UserGate traffic filtering system is especially convenient due to the topical classification of undesirable web resources: there is no need to manually list and restrict access to each undesirable web site – by denying a certain category you can deny access to all the web sites that fall into this category. Besides, this solution helps to avoid the common practice of inefficiently separating a large numbers of sites into "black lists" and "white lists," giving more flexibility to corporate security policies.

By using the miscellaneous filtration rules integrated into UserGate and analyzing the content downloaded from the Internet by its employees, a company can significantly reduce Internet abuse and minimize lost work time.

In addition, UserGate establishes quotas for downloading "heavy" files, such as video files or files larger than the defined size. Together with the restriction of access to certain categories of web sites, this approach optimizes the use of network capabilities and reduces the loading of external Internet access channels, saves a company from unwanted traffic costs and provides extra security of office computers connected to the LAN.

Integrated anti-virus modules scan the incoming traffic searching for viruses, allow only safe traffic flow and ensure the comprehensive protection of local area networks.

Conclusion

The volume of web traffic is increasing every day, which shows how important it is to protect computer systems from network intrusions, control spreading of viruses and users' unauthorized network activities, as well as reduce the unreasonable use of network resources. The demand to analyze web traffic has grown to the extent that a software solution with a flexible filtering process has become of vital importance to many companies that use the Internet in their work. Entensys' solution represents a reliable office security strategy based on the flexible filtering of Internet resources achieved through the denial of access to potential risk zones, which also provides Internet access control capabilities.

[6] American company BrightCloud Inc. is the leading developer of category-based URL-filtering algorithms. More details at http://brightcloud.com

[7] See a full list of web site categories at http://www.brightcloud.com/masterdburllist.asp