Firewall Content Filtering

Ashish Khandelwal, Dr Swapnesh Taterh
Amity University, Jaipur, Rajasthan, India

Abstract**—***A firewall is a set of related program's that protects resources of a private network and also protects the entire network against all external or internal attacks or threats. Firewall apply on both software and hardware or someplace it's combination of both. All messages entering or leaving the internet pass through the firewall.*

A recent survey reported the average age when a child first sees porn online is 11 years. This comes as both a surprise and a concern to parents, especially those who believe they have done all they can to monitor and protect their child's online viewing.

In this scenario we provide technical solution of this kind of problem is "content filtering". Content filtering works by matching strings of characters. When the strings match, the content is not allowed through. Content filters are often part of Internet firewall.

Thus we are providing power to control the information filtering (pornographic materials or social-networking sites unrelated to work) by content filtering to organization, universities, schools and parents also.

Keywords**—***firewall, pornographic, social-networking, filtering, internet and content filtering.*

I. INTRODUCTION

1.1 What is Firewall ?

firewall are mostly used in current internet, this are provide security in cooperative and integrated network. A firewall is a System or group of systems to manage Access control between two network entities. Firewall rules are used to block or allow specific traffic passing through from one side to other. In other words we can say that firewall is a mediator between client or server and vice-versa.

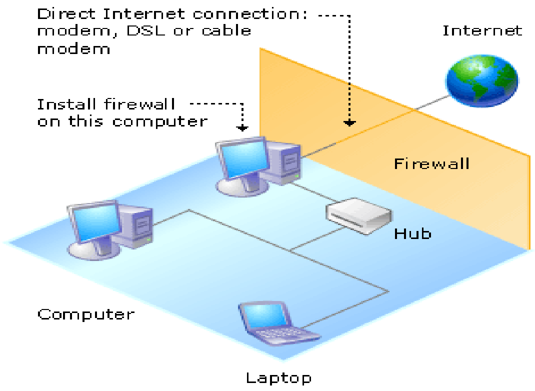

Direct Internet connection: modem, DSL or cable modem
Internet
Install firewall on this computer
Firewall
Hub
Computer
Laptop

Fig. 1 Working of Firewall

1.2 What is the content filtering?

Content filtering is the program to prevent access to certain items, which may be harmful if opened or accessed. The mostly filter items are executables, emails or websites. This is apply by software or via hardware based techniques. Content filtering is based on character or strings matching process. In this process admin are set some character or some string in a list and this list is match by content which are client search. If the content are match from this list then that type of content are not show or not pass through the firewall. This type of process is called content filtering.

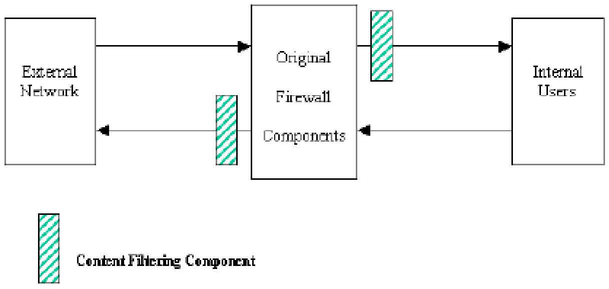


Fig. 2 Block diagram of Content Filtering.

In this fig: 2 we are show the internal user are send request to external network through the firewall. The firewall passes this request to content filtering concepts or process. This process are match the content through the list of character or string which is blocked if the user content are found in the list then request are not send to external network and user see this type of message "the content are blocked". Or the external network is send the blocked content to internal user through the firewall, firewall are send this content to content filtering process. The complete process is same as internal user send request to external network.

II. USE OF CONTENT FILTERING

The problem is providing information on internet about social-networking and pornographic.I Explain first mean of social-networking is "The use of dedicated websites and applications to communicate with other users, or to find people with similar interests to one's own." The social networking sites are best way to interact or connect with those people which have same kind of interest. But the questions are on age limits on social sites. Many Childs are creating their own account or profile on these sites with fake D.O.B. Also organizations are warred for their employees because employees are using social sites in there working hours. We have some statics data on this topic.

- According to a surrey employee are wasting 2.09 hours per 8 hours working day and that doesn’t include lunch or scheduled break time.
- Top time wasting Industries.
  Insurance-2.5 hours per day
  Public sector-2.4 hours per day
  Research & devolvement- 2.3 hours per day
  Education -2.2 hours per day.
  Software industry-2.1 hours per day.
- In education sector 44.7% employees are surfing internet for personal use or social networking sites in these 2.2. Hours.
- If a organization 1000 Rs are paid for 8 hours per day, and
- Employee waste 2.09 hours per day so that organization is paid 261.25 Rs per day for his wasting hours by employee.

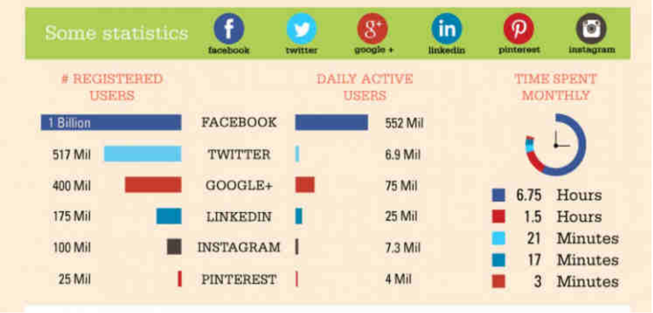
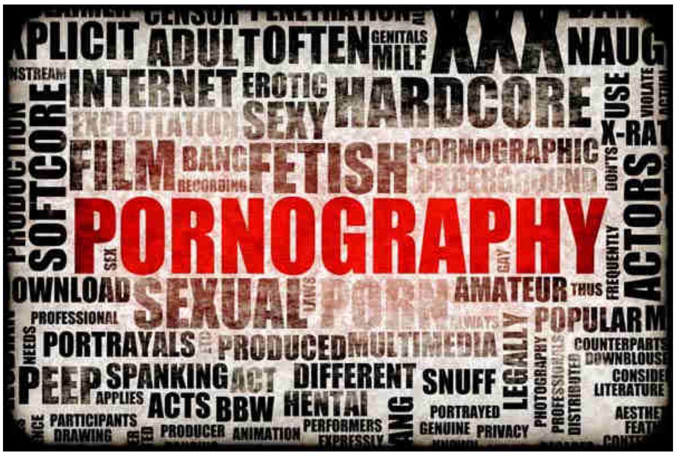


Fig. 3 show the no of profiles or a/c on social sites in current.

- 95% teens (12-17 ages) are use internet and 81% of that are used social networking (2013) and this teens have online a/c on Facebook-94%, Tweeter-26% and Google+ 3%.
- 69% of those teens regularly receive personal messages online form they do not know.
- 58% of teens don’t think posting photos or other personal info on social networking sites.
- 1 in 3 teens (aged 12-17) have experienced online harassment. Girls are more likely to be victims of cyber bullying (38% girls and 26% boys).
- 70% girls are text daily vs. boys 60% are text daily(on online social sites).
- 45 million kids under 18 are have social site a/c and 1 in 5 has revised an online sexual offer.

After social networking we are talk on pornography. The depiction of erotic behaviour intended to cause sexual excitement. Pornography is the explicit portrayal of sexual subject matter for the purpose of sexual arousal. Pornography may use a variety of media, including books, magazines, postcards, photos, sculpture, drawing, painting, animation, sound recording, film, video, and video games.

- The UNH centre, found that 42 percent of a nationally representative sample of 1,500 Internet users ages 10 to 17 had been exposed to online porn in the last year, with two-thirds reporting only unwanted exposure.



- The incidence of unwanted exposure has risen for this age group, from about 26 percent between 1999 and 2000, to 34 percent in 2005, the team has found.
- A recent survey reported the average age when a child first sees porn online is 11 years.
- 48% teens have received a sexually suggestive message.
- Data is related to pornography or sexual content on the internet are 15% of total web pages.
- 36% teens have access sexual topics online.
- 32% teens accesses nude content or porn online.

This comes as both a surprise and a concern to parents, especially those who believe they have done all they can to monitor and protect their child's online viewing. There are some ways teens are fooling their parents.

1. 53% of teens clearing the browser history.
2. 46% of teens close /minimize browser parent walked in.
3. 34% of teens hide or delete IMs or videos.
4. 23% of teens lie or omit details online activities.
5. 21% of teens use an internet-enabled mobile device.
6. 20% of teens Use private browsing modes.
7. 9% of teens Create duplicate /fake social network profile.

This are the only 2 topic which we are explain and show the need of content filtering and impotents of content filtering. Because internet is provide sexual content very easily.

Techniques of content filtering

We have two major techniques which help we are apply content filtering on firewall.

1- **content filtering for same group.**
   a. **content filtering for plaintext file.**
   b. **Content filtering for non- plaintext files.**

2- **Content filtering for Different groups.**

a. Content filtering for plain text file: content filtering for these files is based on exact string matching. Like the pornographic web pages containing a particular word may be detected by the firewall. We are providing some steps to implement content filtering for plain text file.

i. Locate the corresponding source files for various network services, such as HTTP, FTP and TELNET.
ii. Modify these codes to add content filtering functionality.
iii. Reconfigure and restart the firewall.

b.Content filtering for non-plaintext files: Some files may in non-text formats, such as portable Document formats(pdf) or doc and some may be in compressed formats, such as zip and winrar. steps are here to apply content filtering on this type of files.

i. When a file passes through the firewall, the firewall will try to determine whether it is a non-plaintext file. This can be done by analysing the header of the file or by calling external programs such as zip. The firewall does not use the suffix of the file but look into the real content. In this way, the firewall can detect zip files that are renamed.
ii. If the file is a non-plaintext, then an appropriate program known to the firewall extracts the text. Otherwise, the firewall will do content filtering directly for this file and transfer it to the destination.
iii. The firewall does content filtering on the extended text files.
iv. The firewall re-packs the checked files into their received format.
v. The firewall transfers the non-plaintext file to the destination.

2. Content filtering for different groups: the need of this content filtering is the set of rules that tell who can use what service or resource and what privileges users have.

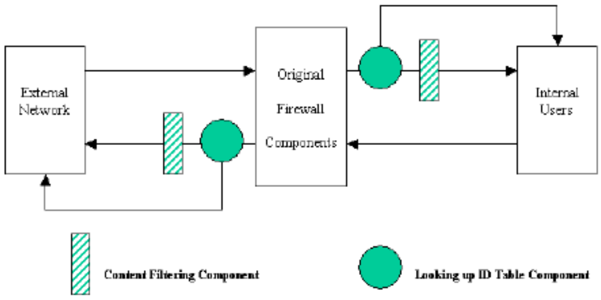

External Network
Original Firewall Components
Internal Users
Content Filtering Component
Looking up ID Table Component

Fig. 4 Working of different groups content filtering.

In this fig. We show the login id table concepts. In this table we are save the IP's of user which have permission to access direct external network without checking of content filter or vice-versa. All other user which IP's are not in this list who's pass through the content filter and after it access the internet. This is the different group content filtering concepts.

III. CONCLUSION

Content filtering must be needed in all type of networks. But the major problem or limitation of it is this process are pure technical and every one can't add character, blocked data or string in content filtering list after it replacing of this file with filtering file.

In future work we are creating that GUI program which provide easily add data, character or strings of blocked content to content filter list by administrator.

REFERENCES

[1] Rongbo Du, Rei Safavi-Naini and Willy Susilo(2002/8) ,"Design and Implementation of A Content Filtering Firewall", Journal of DePaul University, CTI, Tech. Rep.

[2] Chi-Shih Chao, An-Chi Liu (2006)," An internet firewall policy verification system", Journal of Proceedings of the 9th Asia-Pacific network operations and management symposium, Poster session, volume 1.

[3] www.wikipedia.com

[4] www.davidsonstaffing.com

[5] www.1247wallst.com

[6] www.onlinecollegecourses.com

[7] www.nersmartz.org/safety/statistics.com

[8] www.pewinternet.org/reports/2013/teens-social-media-and-privacy/main-report/port-1.apx

[9] dailytech.com/surey+94+percent+of+teens+use+facebook/articles/1611.htm