Detection of Proxy Misconfigurations via Log Alarms

Samet GANAL
Department of Computer Engineering
Süleyman Demirel University
Isparta, Turkey
samet.ganal@kuveytturk.com.tr

Mehmet Ali YALÇINKAYA*
Department of Computer Engineering
Ahi Evran University
Kırşehir, Turkey
mehmetyalcinkaya@ahievran.edu.tr

Ecir Uğur KÜÇÜKSILLE
Department of Computer Engineering
Süleyman Demirel University
Isparta, Turkey
ecirkucuksille@sdu.edu.tr

***Abstract*— Today, institutions use proxy products for the internet access of their users and arrange the internet access policies of their users by way of this device. Even though proxy takes on the internet access load of the institution by itself, it enables many changes during the day. Human based errors may occur during operations carried out in the day and these errors may cause difficulties for the institution with regard to information security. The objective of this study was to enable automatic detection of erroneous structuring on the proxy without any user feedback before the problem gets out of hand and to initiate the solution process starting from the time that the problem occurs.**

Keywords— proxy server, misconfiguration, log alarm

I. INTRODUCTION

Today, institutions use many different security products for protection against cyber attacks and to prevent user abuse. Proxy, which is one of these security applications enables the users to access internet from a single point, increases line efficiency and records the access requests. In addition, the requests made by the users do not go outside, the recalled site is brought into the proxy and presented to the user from there [1].

Internet traffic access is handled by proxy in large scale institutions. Middle and small scale institutions may use firewall instead of proxy to cut down on costs. Even though proxy and the firewall used for proxy purposes are critical systems with significant amount of traffic, many of their configuration settings are changed during both work hours and off-work hours. Proxy administrator may carry out many actions during the day such as banning harmful domains, providing website access to users, temporarily increasing internet access authorization and arranging the internet policy categories. Every configuration that is changed increases the margin for error thereby opening new windows to a possible access problem.

Of the surveys conducted with proxy titles in literature, Schreiber et al. [2] explains working method of internet and proxy sites. In addition, during the call of the user's internet page, they show all the processes that happen in the background. Winston mentions cache and proxy, and explains these two different concepts in detail, and specifies their types in the chapter "Cache and Proxy" in his book [3]. Sha et al. in their studies [4] focuses on development of web usage data by developing proxy logs. In this study, the focus was on human caused errors during daily work activities instead of basic problems that may occur in the proxy application. No similar study was determined as a result of the literature survey carried out.

The second section of this study includes proxy use and logging logic, the third section includes ratings of proxy misconfigurations, the fourth section includes issues that may result from proxy misconfigurations, the fifth section includes log alarm generation for detecting proxy misconfigurations and the sixth section includes the results.

II. PROXY USE AND LOGGING METHOD IN INSTUTITIONS

There are different approaches for where the proxy is positioned in the technology world of our day. The most preferred technique is placing it between the firewall and the user computers [5].

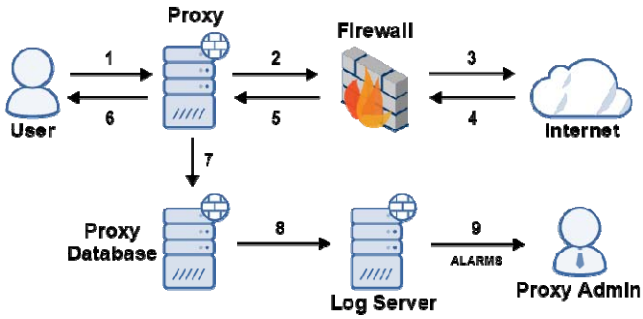

Fig. 1. Internet access stages for an institution user

Figure 1 shows the internet access of a user, placement of the generated logs inside the log server and the misconfiguration notifications to the proxy manager. When a user wants to access an internet website, the access request reaches the proxy. Here, the internet policy assigned to the user and the address of the the request are compared. If the user has access authorization for this address, the website is displayed; if not, the website is not recalled and an access denied page is displayed.

Regardless of whether the user request is allowed or denied, both cases are recorded. Proxy application records these instances in its own database. Whereas the log record product used in the institution records this entry in its own

*Corresponding Author.

978-1-5386-3449-3/18/$31.00 ©2018 IEEE

database. The records are properly separated and categorized in the log record product and alarms may be generated based on demand [4]. The generated alarms can be sent to the desired individuals and in this study it is the security engineer who is the proxy/firewall administrator.

III. Misconfiguration Ratings

Proxy applications are not preferred by small scale institutions and they are generally used by middle and large scale institutions. A problem that may arise in small scale institutions which do not use proxy will be realized in a much shorter period of time in comparison with large and middle scale institutions according to the structure of the institution and its number of employees. In addition, generating log alarms can be an unnecessary and burdensome task for small scale institutions since they will not have a complex log processing product. Hence, middle and large scale institutions are at the focus of this study.

The population that is affected from misconfigurations increases as the number of proxy users in the instiutiton increases. In this section, potential misconfiguration settings were evaluated with regard to the population they address and a hazard classification has been made.

Accordingly, proxy misconfigurations have been classified into 3 main categories according to the population they address: Kurum kullanıcılarının %1 ve altını etkileyebilecek küçük ölçekli yanlış yapılandırmalar,

- middle scale misconfigurations that may affect 1-10% of the users in the institution,
- large scale misconfigurations that may affect 10% and above of the users in the institution.

Proxy xisconfigurations that may affect 1% and lower users in the institution shall affect a small group of people regardless of how large the institution is. Such that, there is even a chance that none of the users subject to this misconfiguration shall realize it. The probability of such misconfigurations to cause large problems is very small since they address a very small population.

Whereas proxy misconfigurations that affect 1-10% of an institution may result in significant issues and should be evaluated as high level of criticality. Since the number of affected users is high in such cases, it should be expected that the misconfiguration will be realized at least by a portion of the users. The users may realize this error and use it, abuse it and even cause problems because of it. On the other hand, a user who realizes and makes use of this change in access may think that the information technologies department is aware of the issue, or may continue benefiting from it even though he/she is fully aware of everything. It may take a long time to realize the error made by the proxy administrator when there are no feedbacks or it may not be realized at all. This is what makes a misconfiguration hazardous.

Whereas misconfigurations that affect 10% or more users in an institution are also of significant importance. A misconfiguration that affects 10% or more of the users in an institution may result in significant issues since they address a large population. On the other hand, since there will be lots of feedback in misconfigurations that address a large population, the problem will be realized faster and steps to solve this issue will be taken at a shorter notice.

Even though large scale misconfigurations seem as the most important when classified according to the level of importance, it can be observed that such cases will not cause significant problems since they will be detected and solved rapidly. A short term misconfiguration setting is an acceptable situation. Short scale misconfigurations do not cause significant problems due to the number of people that are affected. Middle scale misconfigurations may be overlooked since there are no user feedbacks or due to the fact that the number of feedbacks is small and this may result in significant problems especially over a long period of time.

IV. Possible Results Of Proxy Misconfigurations

Complex devices such as proxy and firewall are prone to errors since they have many configuration settings. Especially settings that are used in daily tasks which need to be changed frequently are open to errors. The internet policies of users, the exceptions assigned to them and in short all access settings may be changed on a normal day.

Proxy misconfigurations may result in two situations. These are;

- Users Having Access to Blocked Sites
- Users Failing to Access Required Web Sites

A. Users Having Access to Blocked Sites

Users are placed in an internet policy in accordance with their positions in their institutions and they access the internet as allowed by the related policy. Misconfigurations made by the proxy administrator may result in users having access to they should not. The errors made at this point may cause malwares to enter the system of the institution, important data to leak out or behaviors that violate the institute culture. Primary errors that may cause such results during configuration have been listed below.

1) Using a Common and Mischaracterized Keyword When Defining an Exception for the Website that the Users Should Have Access to: Defining exceptions is one of the tasks that the proxy administrator does almost every day. Utmost attention should be given to keywords when defining an exception. For instance, when access to a user will be granted for https://dl.google.com libraries, the “dl.google” form should be used. If the user is accidentally allowed to use the “google” word, that user may easily access https://drive.google.com website and share folders or access the https://chrome.google.com website and install the add-ons of his/her choice. The user may intentionally or unintentionally leak data outside of the institution by benefiting from this error made by the proxy administrator or he/she may download malware. Similarly, the security of the institution may be at risk due to the add-ons installed by the user.

2) Giving Access to a Different User or User Group when Granting Access to a User: In this error, access right is granted to a different user or user group by the administrator. Such problems may take place frequently especially in large instiutions due to similarities in the names of employees. The access granted to the wrong user may result in the correct user to get in a difficult situation because he/she does not have access or the wrong user to abuse institution security. Access right may also be accidentally granted to a group that the user is in or not. In this case, users who should not have this access right may have access to these locations thereby risking institution security.

3) Assigning Wrong or Unlimited Internet Policy to the User or the User IP: Proxy administrator may face many different access problems during the day and he/she may need to provide temporary authorizations to detect the root cause of these issues. This is performed by temporarily granting a higher level or unlimited internet access to the user or the user IP. At this point, the proxy administrator should refrain from giving unlimited internet access to a user. Because once the user realizes the authorization provided, he/she will start to carry out an action that was previously not possible. Accessing a previously blocked website may be given as an example to this case. This may put the institution security at risk. Therefore, a policy that prohibits access to harmful web sites should be preferred even when authorization is increased for testing purposes.

4) Giving Access to a Wrong Category when Regulating the User Internet Policy: Regulation of user internet policies is not a frequent procedure, however there is always an update or the addition of a new category at the producer side. At this point, users may have access to websites which should be prohibited if the proxy administrator does not regulate the access to this new category. Another situation arises when the proxy administrator mistakenly allows access to the main category and applies it to all the sub-categories while regulating category accesses. This will also increase the access of users thereby resulting in undesired instances.

5) Neglecting the Possibility that the Address is Tunnelled on the Content Gateways After Shutting Down Access to a Category: After shutting down category or url based access to a certain website, the administrator naturally thinks that no one will be able to access them. However, there is one more point that he/she should check. Some websites may be tunneled at content gateways for some purpose. The tunneling of a website means that the correct requests made to that address are carried out directly without consulting the policy server. Contrary to the opinions of the administrator, this may result in the access of the user to that website even when category based access is disabled.

6) Giving Access to an Unfixed IP Adress: Access authorization may be provided over an IP when the user name to be granted access is not known or when access authorization is required for all users of the related computer. In this case, the IP address granted access should be fixed over DHCP. If the IP is not fixed, the IP will be reassigned to another computer when the DHCP lease time is over and thus the access authorizations defined for the related IP will be assigned to the new device. The owner of a device with special authorizations may suddenly find himself/herself with an upper policy and abuse the new authority. Therefore, care should be given whether the IP is fixed or not when assigning authorization to an IP.

7) Opened Access Due to Miscategorization by the Owner: The proxy or firewall device used takes the website category information from a master database prepared by the owner which is updated continuously. There are more than one billion websites in the technological world of our day. Hence, the owners do not always carry out website categorization attentively which results in having access to websites which should be blocked. It is very difficult to detect such errors. However, controlling the accessed websites by way of regular reports and giving feedback to the proxy product institution for changing the master database category of related websites may be a solution. According to the aforementioned scenarios, the proxy administrator has unknowingly given access to the users for websites that they should not have access to. It is difficult to perceive the problem in such cases since the number of feedbacks is low. Regular reports make it easier to detect such problems. Success is possible through the effort and attention of the proxy administrator.

B. Users Failing to Access Websites They Should Have Access to

Internet policies are assigned to users according to their tasks and their internet access is controlled in accordance with these policies. Proxy administrator may sometimes mistakenly prevent access to a website that is required for the users. In this case, the users may not carry out their jobs thereby resulting in significant reactions. Examples of misconfigurations by the proxy administrator have been given under the below headings.

1) Using a Popular Keyword When Preventing Access to a Website that the Users Should Not Access: In today's cyber world, a new malware content website is published at every single moment. Therefore, the proxy administrators carry out operations for blocking off access to certain malware content websites several times per day. Keywords may be used especially in cases when there are many websites using the same words. However, care should be given to use a unique word when writing down the keyword. Because if the keyword used by the proxy administrator is used in the names and extensions of other websites, the sites that should be accessed may also become blocked.

2) Blocking Off a Wrong Category While Regulating User Internet Policy: It may be logical to block access based on URL' s instead of on categories. Other websites may also be affected when access is blocked based on category resulting in more access limitation that was intended. In another case, blocking a main category that the users should not have access to also results in blocking access to its sub-categories. This may also result in more access limitation that was intended.

3) Assigning a Wrong and More Secure Internet Policy to a User: An internet policy is assigned to each individual working at an institution. Users with no internet policy go online with the default internet policy. At this point, the internet policy of a user should be in accordance with his/her responsibilities. Erasing the policies assigned to a user by mistake may result in the user going online with the default policy thereby limiting the user more than necessary. It is more logical to assign a policy to the unit of the user instead of writing user based internet policies.

4) Blocking Access to an Unblocked Website Without Evaluating the Internet Website Blocking Suggestions: The proxy administrator blocks off access to many malware/phishing websites during the day based on information acquired from many different sources. Accepting website blocking requests without any evaluations may sometimes resultin blocking a website that should not be blocked. For instance, it cannot be accepted to block access to facebook completely just because a facebook group is subject to a phishing attack. Hence, the proxy administrator should check the access requests for the related websites before blocking access and should strive to ensure that the users do not experience any problems. The proxy administrator receives feedback rapidly when users cannot access websites that they should have access to. Therefore, the proxy administrator would understand this issue right away and solve it immediately.

V. Possible Results Of Proxy Misconfigurations

A log record is generated for every change made on the proxy application and every request via the proxy. If a log processing product is present in the institution and if the proxy logs are made in this product, it is one step easier to prevent errors. These generated logs may easily be identified in the log processing product and alarms may be set for spotting undesired instances.

At this point, it is required to set up an alarm that serves two main purposes which are detecting when users have access to websites that are not allowed when users cannot access the allowed websites. Many different parameters may be used when setting up these alarms.

A. Setting Up an Alarm for Cases when High Level Users May Not Access Allowed Websites

An error made by the proxy administrator may have impact on almost all users. Special attention is given in large institutions to make any mistakes regarding the access rights of high level executives.

Fig. 2. Setting up alarm for high level users

Figure 2 shows an alarm generated for when the access of high level users is blocked for an "uncategorized" website and the matching of the below parameters has been required for triggering this alarm. The first parameter is the proxy institution information used for distinguishing the proxy logs from all logs which is the "Websense Security" filtering in this example. Filtering has been made in the second line for the KT_WSN_VIP internet policy which is the internet group of high level users in the institution.

Every internet category has a unique id number. The category numbered 29 has been given as an example here and the proxy access requests of important users in the institution have been recalled. Finally, the "blocked" logs from this access request have been separated. According to the final state of the alarm, the alarm will trigger when one of the users in the KT_WSN_VIP category is blocked in the category numbered 29.

In conclusion, the alarm will trigger if a user who should have access to this category under normal circumstances fails to do so; the situation will be realized without the need for any user feedback and a solution will be seeked.

B. Setting Up an Alarm for Detecting Users Failing to Access Websites Allowed to All Users

Some websites that all users in the institution should have access to need to be allowed to everyone at all times. If a user fails to access a website that should be allowed to all users, it means there is a problem and a flaw in service.

- Proxy log
- Target Host Name Contains google.com
- Device Action = blocked

The alarm given above triggers when any user is blocked while trying to access the Google.com website. If the Google.com website is allowed for all users for which no blocking is required and if an alarm is still triggered, it means there is a problem somewhere.

- Proxy log
- Target Host Name Contains google.com
- Device Action = blocked
- 5 times in a 1 minute

The same alarm can be improved by adding the "time – number of blocks" as shown above. An alarm will not be triggered when access is blocked to google.com website until the same instant occurs 4 times in one minute. Blockings experienced by different users will all be included in this alarm since there is no specific user restriction. Thus, the false positive value of the alarm can be decreased.

C. *Setting Up an Alarm for Controlling the Increase in the Number of Blocks to Access Request*

Setting up an alarm one by one for every website that the users should have access to is an impossible task. Therefore, setting up a more general alarm may make things easier. For this purpose, the number of blocks in an average period of time should be determined and the alarm should be set up accordingly.

- Proxy log
- Device Action = blocked
- 500 times in a 5 minute

On average, 250 website blocks take place in an average of 5 minutes at the institution for which the above alarm has been set up. In this case, if the number of blocks is greater than twice the average value, it is probable that there is something wrong which is due most likely to a proxy misconfiguration.

D. *Setting Up an Alarm for Controlling Whether Users Access a Blocked Internet Category*

There is a category above all proxy applications the access to which should be blocked for all users. Websites containing malware are especially blocked to access. An alarm can be set up as below for determining the users who accidentally access a blocked website.

- Proxy log
- Category Name Contains Malware_Websites
- Device Action = permitted

Thanks to the parameters used, an alarm will be triggered if the access request of a user to a website in the malware_websites is permitted. If this scenario takes place, it means that there is a serious issue regarding institution sescurity and immediate action is required.

E. *Setting Up an Alarm for Controlling the Access of Users to Blocked Sites*

Institutions may limit access to certain websites based on their own policies.

- Proxy log
- Target Host Name Contains drive.google.com
- Device Action = permitted

The above alarm has been set up for cases when the access requests are permitted to the drive.google.com website which is actually blocked in accordance with instiutiton policy. This may take place due to many reasons such as a temporary increase in the internet policy of a personnel, mistakenly opening the related website to access or permitting a general keyword.

On the other hand, some users may need access this blocked website due to their jobs. In this case, the above alarm will be triggered as false positive thus resulting in an unnecessary triggering of the alarm. The following additional arrangements can be made to the alarm for decreasing the number of false positive cases.

- Proxy log
- Target Host Name Contains drive.google.com
- Device Action = permitted
- Device Custom String1 Not contains Human_Resources
- Device Custom String1 Not contains KT_WSN_VIP

According to the alarm given above, an alarm will not be triggered even when a user in the human resources or the vip group accesses the drive.google.com website which is actually blocked for access in accordance with institution policies.

Fraud detection is also possible thanks to the above filter. The users may request temporary higher authorization levels from the proxy administrator for various reasons. The proxy administrator may temporarily increase the authorization level of the user for eliminating his/her access problem and enable the user to test it. An alarm shall be triggered if the user uses his/her excuse as a front to visit the blocked drive.google.com website and the proxy administrator shall realize that there is something wrong. In conclusion, fraud detection is also possible thanks to these alarms.

VI. Conclusions

In this study, the use of proxy, its positioning and means of operation have been explained in detail. Misconfigurations have been classified into three groups according to the percentage of users they affect, the most dangerous misconfiguration type was put forth as middle scale misconfiguration targeting 1-10 % of the users.

Proxy configurations have been examined under two main headings of failure to access unblocked websites and accessing blocked websites. Scenarios that might cause these cases were handled in detail under each heading and proxy misconfigurations were tried to be explained in a clear and understandable manner.

The final section focuses on the kinds of alarms that may be set up for detecting misconfigurations and examples were given under five main headings. Accordinglt, the proxy administrator will realize that there is a misconfiguration without any feedback in cases when such alarms have been set up in an institution.

Whereas it is fairly easy to set up the alarms described within the scope of this study, it was observed that they result in many significant advantages for the institution. There is a great difference between when the proxy administrator realizes

the mistake he/she has made as a result of a triggered alarm or as a result of user feedbacks. When the alarm notifies a misconfiguration, the proxy administrator also learns of this situation together with the user and starts working to find a solution immediately. In cases when no alarm is triggered, user feedback is expected and solving the problem takes much longer. Institutions may evaluate misconfiguration alarms in accordance with their own policies and set them up accordingly. The alarm types included in this study are not limited only with proxy and may easily be used for other applications as well.

REFERENCES

[1] S.,B.,Blum; J.,Lueker. "Transparent proxy server." U.S. Patent No. 6,182,141. 30 Jan. 2001.

[2] Z., Schreiber et al. "System and Method for Browser within a Web Site and Proxy Server." U.S. Patent Application No. 12/530,461. 2010.

[3] A., Winston, OpenVMS with Apache, WASD, and OSU: The Nonstop Webserver. Digital Press, 2002.

[4] H., Sha et al. EPLogCleaner: improving data quality of enterprise proxy logs for efficient web usage mining. Procedia Computer Science, 2013, 17: 812-818.

[5] M.,Sysel; O., DOLEŽAL. An educational HTTP proxy server. Procedia Engineering, 2014, 69: 128-132.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.