Determine the operation of a firewall to block avoidance internet censorship systems based on proxy

Diseño de un cortafuegos para bloquear sistemas de evasión de censura de internet basados en proxy

**Christian Augusto Romero Goyzueta, Ferdinand Edgardo Pineda Ancco, Jesús Vidal Lopez Flores**

Profesional de Ingeniería Electrónica de la Universidad Nacional del Altiplano, Puno - Perú

Correspondencia: ¡romeroc24@gmail.com, ¡ferpineda@gmail.com, ¡jlovidal@gmail.com

Within the policies of an organization it is possible to find not to allow users to access sites on the Internet for entertainment or social networks, as in the case of production organizations and educational therefore a firewall that is used implemented certain rules based on the policies of the organization, blocks access to certain defined sites while you let others free. However there is no implemented rules to block proxies of Avoidance Internet Censorship Systems, the user can access easily to those proxies. The addresses of these proxies change very frequently, so it is almost impossible to block them all, and eventually they appear more. The proposed solution is to create a firewall that uses dynamic rules, these rules are created for the dynamic firewall. A test of each address to a destination is made and if it finds that the destination is a proxy of one of these evasion systems; the firewall creates a new rule and automatically implemented. In this way the user will lose access to the proxy.

**KEY WORDS:**
ultrasurf, torbrowser, security policies, network security.

**INFORMACIÓN DEL ARTÍCULO**

Artículo recibido 30-09-2016
Artículo aceptado 12-12-2016
On line: 20-12-2016

**PALABRAS CLAVES:**
ultrasurf, torbrowser, security policies, network security.

**ABSTRACT**

Within the policies of an organization it is possible to find not to allow users to access sites on the Internet for entertainment or social networks, as in the case of production organizations and educational therefore a firewall that is used implemented certain rules based on the policies of the organization, blocks access to certain defined sites while you let others free. However there is no implemented rules to block proxies of Avoidance Internet Censorship Systems, the user can access easily to those proxies. The addresses of these proxies change very frequently, so it is almost impossible to block them all, and eventually they appear more. The proposed solution is to create a firewall that uses dynamic rules, these rules are created for the dynamic firewall. A test of each address to a destination is made and if it finds that the destination is a proxy of one of these evasion systems; the firewall creates a new rule and automatically implemented. In this way the user will lose access to the proxy.

**RESUMEN**

Dentro de las políticas de una organización podría encontrar el no permitir que los usuarios accedan a sitios en Internet para el entretenimiento o las redes sociales, como en el caso de las organizaciones de producción y educativas, por tanto, un firewall o cortafuegos utiliza ciertas reglas en base a las políticas de la organización, bloquea el acceso a ciertos sitios definidos, mientras deja los demás libres. Sin embargo, como no se ha implementado reglas para bloquear proxies de Sistemas de Evasión de Censura de Internet, el usuario puede acceder a los proxies fácilmente. Las direcciones de estos servidores proxy cambian con mucha frecuencia, por lo que es casi imposible de bloquear a todos ellos, y con el tiempo aparecen más. La solución propuesta es la creación de un cortafuegos que utiliza reglas dinámicas, estas reglas las crea el firewall. Una prueba de cada dirección a un destino se hace, y si comprueba que el destino es un proxy de uno de estos sistemas de evasión; el cortafuegos crea una nueva regla y se aplica de forma automática. De esta manera el usuario perderá el acceso al proxy.
INTRODUCTION

The rules implemented in a firewall in order to block access to certain sites on the Internet, are entered by the administrator and remain until the administrator decides to make updates or changes (Smith, 2011). Users have found a way to prevent the firewall blocks access to sites not permitted by the organization, making the use of avoidance Internet censorship systems, as the case of Ultrasurf, Tor Browser or Proxy for Chrome (Adelstein, 2007). This avoidance system works by running software on the client that allows the user to connect to a proxy, usually a HTTP Proxy, and not connecting the user directly to the desired website. The proxy located somewhere in the world receives user requests and redirects data from there to the desired user sites (Bhargava, 2016).

The existing problem is that the policies of the organization are broken and the low productivity of the working groups which have free access to the Internet, despite implementing a corporate firewall that denies access to certain sites on the Internet.

We are using iptables is a user program that allows a system administrator to configure the tables provided by the Linux kernel firewall implemented by different Netfilter modules. Different kernel modules and programs are currently used for different protocols such as IPv4, IPv6, ARP and Ethernet frames (Van Vugt, 2013). This way you can manage the tables for certain protocol and allow, reject or ignore packets entering, pass or leave the system (Firewall). For example, you can configure an IPv4 packet is rejected as it leaves the Firewall. This way you can describe the actions that are governed by rules in the Firewall as follows (Lammle, 2013).

- (Permit), this rule allows a packet is processed without restrictions.
- (Reject), this rule makes a package is rejected and an error notification is displayed to the user.
- (Drop), this rule rejects the package silently, i.e. not notify the user in any way about the action taken.
- (Input) is an action taken when the packet enters a network interface.
- (Output), the action is taken when the packet exits through a network interface system.

Another tool is bash and is a command processor that typically runs in a text window, where the user types commands that cause actions. Bash can also read commands from a file, called a script (Van Vugt, 2008). Like all Unix shells, it supports filename globbing (wildcard matching), piping, here documents, command substitution, variables and control structures for condition-testing and iteration. The keywords, syntax and other basic features of the language were all copied from sh. Other features, e.g., history, were copied from csh and ksh. Bash is a POSIX shell, but with a number of extensions (Lammle, 2014).

Expect, will help us like an extension to the Tcl scripting language written by Don Libes, is a program to automate interactions with programs that expose a text terminal interface. Expect was originally written in 1990 for Unix systems, but is now also available for Microsoft Windows and other systems. It is used to automate control of interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, ssh, and others. Expect uses pseudo terminals (Unix) or emulates a console (Windows), starts the target program, and then communicates with it, just as a human would, via the terminal or console interface. Tk, another Tcl extension, can be used to provide a GUI (Madummal, 2016).

MATERIALS AND METHODOLOGY

2.1. Objectives
Determine the operation of a firewall with dynamic rules to block avoidance Internet censorship systems based on proxy.

2.2. Hypothesis
A firewall with dynamic rules will permit to block avoidance Internet censorship systems based on proxy.
2.3. Research Design

Experiments are most effective for explanatory research and are often limited to topics in which you can manipulate the situation where people are. In such experiments, it divides people under investigation in two. This research is experimental because it is a type of research that uses logic and principles found in the natural sciences. Experiments can be performed in the laboratory or in real life. Here a relatively small number of individuals or teams involved and address a very focused question.

2.4. Level Research

It is explanatory, by manipulating the independent variable, to see the effect that has on the dependent variable.

2.5. Type Of Investigation

The type is descriptive because is necessary the description of practical use of knowledge and theories networks of firewalls in order to improve and solve the specific problem called avoidance Internet censorship systems based on proxy.

2.6. Space and Time

The research was made from June 2nd to September 13th 2016 on the Cisco Academy Laboratory, of the Electronics Engineering Department of the Universidad Nacional del Altiplano; on Puno, Perú.

2.7. Techniques and Tools

- Techniques

The technique used was the playtesting, that is a technique of improve the software with the progress of the research and each iteration. This technique is so simple like a while operation, every iteration evaluate the condition, if the condition is true, the system can be improved but if is false the stop is used to start again from the initial reference.

- Instruments

The instrument is the test, the researcher takes steps to evaluate the behavior of the system.

- Data Collection Plan

The following steps for data collection followed:

- Scan datagrams on Wireshark.
- Scan datagrams on tcpdump.

2.7.1. Plan Data Processing

The main purpose of the research is test the proxy base on the web contents.

- Hardware:

  ✓ Desktop PC (Laptop S55-B).
  ✓ Server Power Edge R620.

- Software:

  ✓ 64-bit Operating System Windows 8.1 Professional.
  ✓ Linux Operating System: Ubuntu Server 14.04.1 LTS.
There are many features and functions that a firewall can assume. A method to block access to certain IP addresses and allow access to any other IP addresses can be used. For example, another method that is opposite to the above, what it does, is allow access to certain IP addresses while blocking access to the rest or any other IP addresses, the latter method can even block avoidance Internet censorship systems, but has a very big disadvantage; both methods are described below.

### 3.1. Block access to certain IP addresses and allow access to the rest

This method is quite to use, because it is very useful for organizations that want access to all Internet sites except some sites, such as whether you want users should not access social networks as facebook.com, but if they can access pages from around the world to do research.

To achieve this configuration on firewall, add rules to block sites and allow access to any other site (Mauerer, 2008).

**Fig. 3. A client is trying to access a prohibited site and is blocked by the firewall.**

The problem with this method is that the avoidance Internet censorship systems based on proxy based on proxy can easily hack it.

This happens in the following way, the user does not directly access a site blocked by the firewall, the user accesses a proxy that has an address that the firewall is not blocking, then this proxy redirects the connection to the real destination. In this way the user avoid the firewall without problems (Negus, 2009).

**Fig. 4. A client can use a proxy to avoid the firewall.**

### 3.2. Allow access to certain sites and block access to all other Internet

This method is very useful especially to block the Avoidance Internet censorship systems based on proxy based on proxy, because a user is able to access certain sites allowed by the firewall and all the rest of the Internet, including proxy, are blocked (Negus, 2013).

**Fig. 5. A client can only Access to one or a few sites and any other Access is blocked.**
The problem with this method is that users cannot access more than a few sites on the Internet, and would not have the flexibility to explore or investigate on Internet (Saini, 2011).

The firewall with dynamic rules, in this research, is characterized by the ability to test a website and if this site is a proxy, then it is blocked, if it is a common web site, it is allowed.

Fig. 6. Firewall can test a site and block it if it is a proxy.

3.3. Implementing Dynamics Rules
Dynamic rules are not implemented by the user, who implements is the firewall. Is based on a test that is done to the destination. The firewall can have static rules previously entered by the user and the firewall will add more rules later.

This is where the use of bash scripting and expect is done, because they automate process methods and commands on GNU/Linux. Bash allows you to enter commands into the operating system, and expect allows you to enter commands in response to certain outputs returned by the operating system.

This is the web output of a proxy server for Internet censorship avoidance systems.

Fig. 7. The web output of a proxy server for avoidance Internet censorship systems based on proxy.

ERROR
The request could not be satisfied.

Bad request.

Source: Authors.

The firewall will compare this web output with a common web and determine if it is a proxy server for Avoidance Internet censorship systems based on proxy. The firewall can use the html code and other methods to search proxy servers.

Fig. 8. The html web output of a proxy server for avoidance Internet censorship systems based on proxy.

The nmap scan of a proxy server can show us the ports available and other data that can be tested. For example the next output show us that this proxy server is a linux server with open ports 80 (http) and 443 (https) to make the test operations. The firewall can test both ports and determine if is a common web page or if is a proxy.
Fig. 9. The nmap scan of a proxy server for avoidance Internet censorship systems based on proxy.

```
Fig. 9. The nmap scan of a proxy server for avoidance Internet censorship systems based on proxy.
```
denied to the site immediately. Bash and expect automate all processes to implement dynamic rules in the firewall. GNU/Linux is a great choice for its flexibility, performance and low cost of implementation. The difference against a common firewall is the dynamic creation of the policies and rules by the firewall and not by the human administrator. To achieve this, the firewall needs high processing capacity, which is get it with a very affordable processor on the market, it then proceeds to perform the test and finally automation allows it to add firewall rules by itself.

ACKNOWLEDGEMENTS

We thank our good friends, families and our university who help us at all times.

BIBLIOGRAPHIC REFERENCES


Determine the operation of a firewall to block avoidance internet censorship systems based on proxy.