Distribution of web traffic toward the centralized cloud firewall system

Ivan Ivanovic
Belgrade University Computer Centre
University of Belgrade
Belgrade, Serbia
Email: ivan.ivanovic@rcub.bg.ac.rs

***Abstract*—This paper presents methods that are used in AMRES (Academic Network of Serbia) network in order to equally distribute a large amount of web traffic toward the centralized cloud firewall system. Although some of the methods can be only used with the Cisco equipment, other methods can be used with equipment of any manufacturer or open-source solutions that are relaying on proxy functionality in order to forward the web traffic. The Idea for the paper was born during the work on the Géant3 plus project on the NA3T2 (Network Activity 3/Task 2) task.**

Keywords—Load balancing; DNS; round-robin; cloud; firewall

I. INTRODUCTION

During the development of AMRES most of the budget funding was used for the deployment of the backbone infrastructure and datacenter servers that were used in order to provide services for the AMRES users. Due the lack of the funding and different budget positions of AMRES institutions digital divide was the common issue that left some of the institutions unprotected from the malicious web threats that came from the Internet. For a long time simple access lists were used on the backbone of the network to provide basic level of security for the end users. In a situation were Squid proxy server was used, blocking of access to malicious web sites was also possible. As the network expanded number of internet users also increased. At some point it became very hard to maintain a large amount of details in access lists and protection relaying on access lists became insufficient. The reason was the increased development of malicious software and threat techniques. Since the malicious type of traffic can be hidden at the upper layers of OSI model, it can easily pass access lists inspection. Although the access lists are still used for the protection of undesired access to the network, it was required to provide protection that is aware of the traffic content. During the national “Connecting School” project the government decided to provide protection for youngest and most vulnerable users of AMRES Internet services: high school children.

II. CENTRALIZED CLOUD FIREWALL SYSTEM

The most used service in AMRES is the Internet connectivity. A lot of malicious threats and bad aspects of the Internet is coming from different web sites. Because of that the government had mandatory demand that new firewall devices must have a filtering function based on a web site categorization. After the testing of different firewall equipment, Cisco Ironport S670 Web security appliances were chosen. Beside the Ironport S670 firewall devices one centralized Ironport management device M160 was also bought. This way a configuration of all Ironport firewall devices could be done at one centralized place. Feature of Ironport management device that provides integration with LDAP directory enabled AMRES institution administrator’s centralized access to the first AMRES cloud service.

III. FIREWALL CLOUD SERVICE LOCATION AND USAGE

The Ironport management device coupled with LDAP provided AMRES institution administrators access to the specific filtering policy that can only process web traffic originating from administrator’s home institution.

AMRES backbone network has a star topology design with its center in BUCC (Belgrade University Computing Centre) and primary internet links are also located there. BUCC presents an optimal place for the deployment of a centralized firewall system since all Internet traffic must pass through the BUCC. Figure 1 presents the position of the Ironport cloud firewall system in AMRES network.

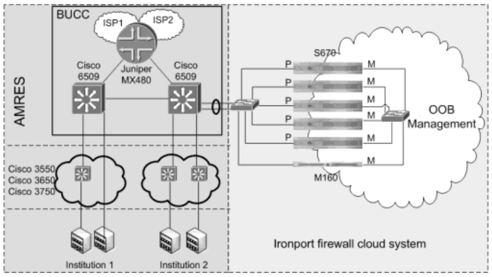


Figure 1 – Position of the cloud firewall system

The administrators from AMRES institution can access to the Ironport management device and configure the filtering policy using any web browser. After a successful authentication in LDAP database, the access to the specific policy is granted to the administrators. The administrators can now make changes to the specific policy configuration and they can also publish changes to all firewall devices in the cloud. The filtering policy is tied to the IP address range of AMRES institution so policy can only block/filter the specified web traffic. Figure 2 presents the example of the deployment of filtering policy to the Ironport firewall cloud system.

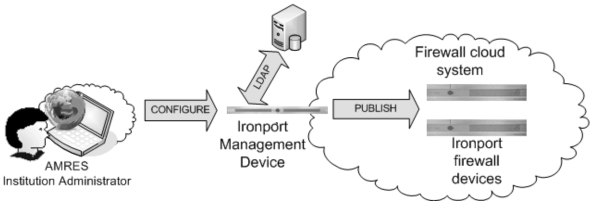

Firewall cloud system
CONFIGURE
LDAP
PUBLISH
Ironport Management Device
Ironport firewall devices
AMRES Institution Administrator

Figure 2 – Configuration of firewall cloud service

Ironport firewall devices are providing a set of filtering features. But the two most important that are used in AMRES are:

- Filtering based on web categories
- Antimalware filtering using Webroot scanner

Mandatory blocked web categories are:

- Child Abuse Content
- Filter Avoidance
- Gambling
- Hate Speech
- Illegal Drugs
- Pornography

Antimalware filtering provides a protection from web sites that contain malware like viruses, adware, Trojans, etc. Anti-malware feature uses a Webroot scanner in combination with WBRS (Web Reputation Score) in order to provide a final decision about web site trustiness.

IV. WEB TRAFFIC LOAD BALANCING METHODS USED IN AMRES

AMRES is providing Internet connectivity to more than 150 institutions. It is hard to determine a number of active users since a lot of institutions are still using NAT (Network Address Translation) and large number of users are hiding behind one IP address. It has been measured that web traffic is reaching a speed of 1Gbps with increasing trends. Since AMRES administrators have different filtering and scanning demands, processing burden on the firewall system can be heavy. To provide an optimal performance for the users, the Ironport firewall cloud filtering system contains five firewall devices.

Five firewall devices can easily process a large amount of web traffic without impact to the performance of the system. The problem that arises is how to equally distribute web traffic to the five firewall devices without additional load balancing equipment.

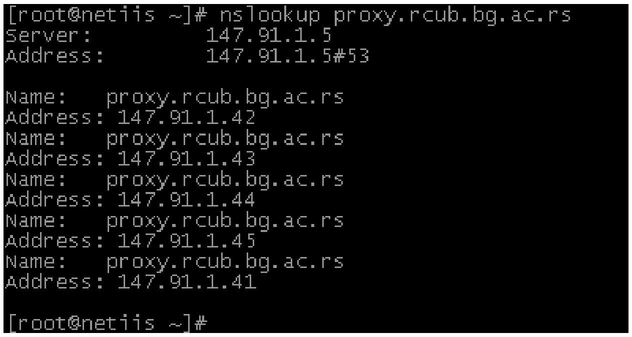
The web traffic load balancing can be achieved using two different methodologies. The first methodology implies a configuration at the AMRES institution workstations or local proxy servers of institution and in this situation end users can choose if they want to use centralized firewall system. The second method implies redirection of the web traffic to the centralized firewall system without the influence of end users.

A. *Web browser proxy configuration*

- Manual configuration

In this method end user must configure his own web browser in order to redirect web traffic to the Ironport firewall cloud system. Configuration can be done in a couple of ways.

The easiest one is a direct configuration of DNS (Domain Name System) name of the Ironport firewall cloud system in the proxy configuration of the web browser. It is very important to use the DNS name instead of the IP address since DNS service is configured to resolve the Ironport filtering system DNS name in a round-robin fashion to multiple IP addresses. Relaying on DNS end users will equally use all five Ironport devices during the Internet browsing. Figure 3 presents the example of DNS round-robin resolving.



```
[root@netiis ~]# nslookup proxy.rcub.bg.ac.rs
Server:         147.91.1.5
Address:        147.91.1.5#53

Name:   proxy.rcub.bg.ac.rs
Address: 147.91.1.42
Name:   proxy.rcub.bg.ac.rs
Address: 147.91.1.43
Name:   proxy.rcub.bg.ac.rs
Address: 147.91.1.44
Name:   proxy.rcub.bg.ac.rs
Address: 147.91.1.45
Name:   proxy.rcub.bg.ac.rs
Address: 147.91.1.41

[root@netiis ~]#
```

Figure 3 –DNS round-robin resolving method

- Configuration of PAC file location

The redistribution of the web traffic could be done using PAC (Proxy Auto Configuration) file. The user must configure a location of pac.dat file in the web browser proxy settings in order to redirect the web traffic to the Ironport firewall cloud system. PAC file presents a simple java script that contains rules about redirection of web traffic. PAC file also contains the DNS name of the Ironport firewall cloud system instead of IP address. Equal load balancing of web traffic using PAC file is also achieved relaying on DNS round-robin resolving.

- Dynamic auto configuration using WPAD (Web Proxy Autodiscovery Protocol)

Enabling the WPAD option in the web browser users can also redirect the web traffic toward the Ironport firewall cloud system. Unlike the previous case, WPAD is using DNS hierarchy in order to find the wpad.dat file automatically. WPAD file contains same information like java script pac.dat file mentioned earlier. In this case DNS name of Ironport firewall cloud system is also used instead of the specific firewall IP addresses.

In all three examples of the web browser configuration, the DNS name of the Ironport firewall cloud system is used. The DNS service is indirectly responsible for an equal load balancing of web traffic and in the figure 4 we can see the results this methodology.

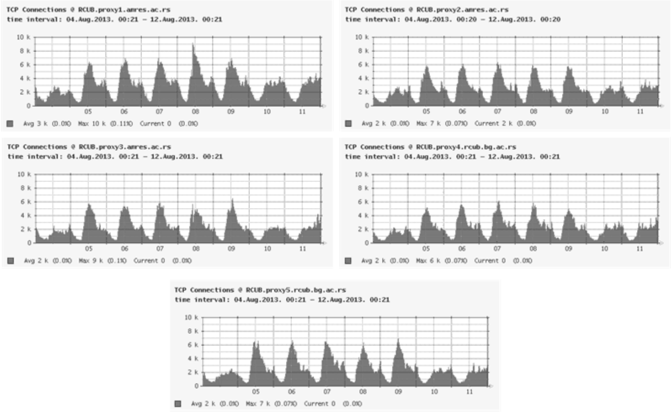


Figure 4 – Number of established TCP connection on five Ironport firewall devices

Figure 4 present's statistics of established TCP connection during the time measured using SNMP (Simple Network Management Protocol) protocol on all five Ironport firewall devices. The number of the established TCP sessions is not the same on all devices because some of AMRES institutions and users are still using IP address of the specific Ironport firewall device and not the DNS name of the whole Ironport firewall cloud system. Some of AMRES institutions are using Ironport firewall cloud system as the parent proxy and they also still use IP address instead of the DNS name. This inconsistency in configuration of equipment/browsers is causing small differences in web traffic redistribution that could be noticed on Figure 4. From the figure 4 we can conclude that the web traffic load-balancing is achieved and the filtering and scanning of the web traffic is distributed to all five Ironport firewall devices almost equally.

B. *Policy based web traffic redirection*

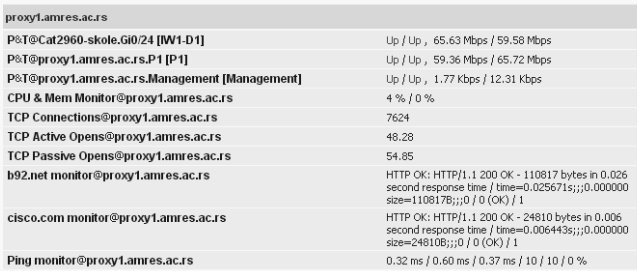
The web traffic redirection could be also achieved using PBR (Policy Based Routing). PBR should be configured at the core of the network in order to match all web traffic packets and send them to the firewall device. The problem with PBR is that it could only redirect traffic to the one firewall appliance. PBR will not provide good results when more than one firewall device is needed. In the case of AMRES PBR could not provide good results since all web traffic could not be processed by only one firewall appliance.

C. *Web traffic redirection using WCCP (Web Cache Communication Protocol) protocol*

WCCP (Web Cache Communication Protocol) is Cisco proprietary protocol that can group core network devices and Ironport firewall devices in a WCCP cluster. Core devices communicate with all firewall devices in a cluster and equally redistribute the web traffic toward them. End users don't need to configure their web browsers and they are not aware of the web traffic redirection. The configuration of WCCP on core devices could be sensitive since it could add additional processing burden on core devices. AMRES is using WCCP only for eduroam® service.

V. MONITORING OF FIREWALL CLOUD SERVICE

In order to achieve optimal usage of the Ironport cloud firewall system, it is very important to conduct monitoring of important device parameters. Centralized Ironport M160 device have a capability to perform monitoring of all other Ironport firewall devices but additional license for the monitoring is required. Since AMRES already has developed a monitoring system that is modular and adjustable, a monitoring of Ironport firewall cloud system is integrated in it. Parameters that are monitored are displayed on the Figure 5.



proxy1.amres.ac.rs	
P&T@Cat2960-skole.Gi0/24 [IW1-D1]	Up / Up , 65.63 Mbps / 59.58 Mbps
P&T@proxy1.amres.ac.rs.P1 [P1]	Up / Up , 59.36 Mbps / 65.72 Mbps
P&T@proxy1.amres.ac.rs.Management [Management]	Up / Up , 1.77 Kbps / 12.31 Kbps
CPU & Mem Monitor@proxy1.amres.ac.rs	4 % / 0 %
TCP Connections@proxy1.amres.ac.rs	7624
TCP Active Opens@proxy1.amres.ac.rs	48.28
TCP Passive Opens@proxy1.amres.ac.rs	54.85
b92.net monitor@proxy1.amres.ac.rs	HTTP OK: HTTP/1.1 200 OK - 110817 bytes in 0.026 second response time / time=0.025671s;;;0.000000 size=110817B;;;0 / 0 (OK) / 1
cisco.com monitor@proxy1.amres.ac.rs	HTTP OK: HTTP/1.1 200 OK - 24810 bytes in 0.006 second response time / time=0.006443s;;;0.000000 size=24810B;;;0 / 0 (OK) / 1
Ping monitor@proxy1.amres.ac.rs	0.32 ms / 0.60 ms / 0.37 ms / 10 / 10 / 0 %

Figure 5 – Monitoring of centralized Ironport cloud system

Important parameters for monitoring during the web traffic redistribution toward Ironport firewall devices are number of established TCP connections, CPU and memory state and amount of traffic on Ironport firewall production interfaces. Other parameters on Figure 5 are used in order to monitor firewall devices availability and functionality. Monitoring of Ironport firewall cloud system is mandatory since it is the only way to know if the web traffic is distributing equally to all devices. All monitored values have predefined alarms with thresholds that are used to alert administrator of Ironport firewall cloud system.

VI. CONCLUSION

Although the Ironport firewall system is designed in order to satisfy most of the enterprise demands, some of the Ironport features can be used in the environment where security policy is not so strict. AMRES presents this environment where institutions like libraries, middle schools, institutes and faculties have not so strict security policies. AMRES institutions only need tools to protect their employees and students, especially younger population of students from the bad aspects of the Internet.

Ironport cloud firewall system is highly scalable. In the case of increased web traffic additional Ironport device can be easily added to the system. In order to continue to provide equal distribution of web traffic to all devices in the system, IP address of newly introduced Ironport device must be added to the Ironport cloud firewall system DNS A record. After the update of the DNS record all web traffic will start to flow equally to the all firewall devices in the system.

The cloud approach provided a great result because AMRES institutions with low budgets now have a simple but powerful tool to protect themselves from the malicious software and undesired web sites on the Internet.

REFERENCES

[1] *http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-629052.html*

[2] *http://www.senderbase.org*