# Effective Multi-Layer Security for Campus Network

*Isiaka A. Alimi*
*Department of Electrical and Electronics Engineering, School of Engineering and Engineering Technology,*
Federal University of Technology,
Akure, Nigeria.
compeasywalus2@yahoo.com

***Abstract*— The development in different communication systems as well as multimedia applications and services leads to high rate of Internet usage. However, transmission of information over such networks can be compromised and security breaches such as virus, denial of service, unauthorized access, and theft of proprietary information which may have devastating impact on the system may occur if adequate security measures are not employed. Consequently, building viable, effective, and safe network is one of the main technical challenges of information transmission in campus networks. Furthermore, it has been observed that, network threats and attacks exist from the lower layers of network traffic to the application layer; therefore, this paper proposes an effective multi-layer firewall system for augmenting the functionalities of other network security technologies due to the fact that, irrespective of the type of access control being employed, attacks are still bound to occur. The effectiveness of the proposed network architecture is demonstrated using Cisco Packet Tracer. The simulation results show that, implementation of the proposed topology is viable and offers reasonable degree of security at different network layers.**

***Keywords*—** *campus network; firewall; network security; intrusion detection systems; demilitarized zone.*

## I. INTRODUCTION

Local area network (LAN) provides network services and applications to people within a common managerial structure such as home, office building, campus or region [1]. However, this network has reach limitation which is addressed by the introduction of wide area network (WAN) that spans a relatively large geographic area, such as a state, province or country. A WAN consists of two or more LANs and it enables them to communicate by serving as the information channel between them. The internet, the most popular WAN, is the main channel for information transmission for various applications and services. Therefore, there is need for an effective security scheme to prevent vulnerability of information to unauthorized users that can compromise it at various levels of transmission as well as while in storage [2], [3]. To this end, one of the major functions of campus network management is based on network security.

There are various advanced network security technologies such as virtual local area network (VLAN), firewall, encryption, virtual private network (VPN), and public key infrastructure (PKI), which have been reported in the literature for securing campus network [4]. Some threatens to campus network security are analyzed in [4] and certain solutions are presented in order to achieve a secure network. Also, [5] examines a set of security models for preventing external invasion and internal data theft. It also presents a theoretical intelligent network security model and suggests the need for further study on its practical implementation. Similarly, [1] presents practical application of network virtualization by the implementation of VLAN as well as ways by which it addresses scalability, flexibility, security, and network management issues which are associated with the traditional LAN in an enterprises network. An encryption algorithm with improved precision, confidentiality and security is reported in [3] for preventing technical challenges in transmission and storage of digital data. Moreover, [6] proposes a distributed snort intrusion detection system model to improve the speed and accuracy of the intrusion detection system. A cost-effective and resilient large-sized campus model that ease the required security measures for the network administrators so that they can easily shape the traffic, adjust the access control lists and block unwanted traffic is proposed in [7]. Furthermore, [8] proposes radius authentication login to improve the safety of network device in the campus network environments. A data mining approach for enhancing the performance of firewall system is presented in [9]. The work reports that the processing time of the firewall is reduced by predictive approach instead of standard firewall linear method of packet filtering. Likewise, [10] proposes a method for designing modular firewalls with small inversion metrics for design understanding. Furthermore, a firewall rule management policy without conflict and an algorithm to fast-check the firewall rules is demonstrated in [11].

This paper focusses on securing campus network with firewalls and proposes an effective multi-layer firewall system for augmenting the functionalities of other network security technologies. This is due to the fact that network threats and attacks exist from the lower layers of network traffic to the application layer. Also, it has been observed that, irrespective of the type of access control being employed, attacks are bound to occur. Consequently, an intrusion detection system (IDS) is recommended for detecting network attacks. The subsequent section gives an overview of network firewall systems and IDS which can be employed to control the network traffic and to detect attacks. Section III, presents the proposed security architecture for campus network. Furthermore, in Section IV, to demonstrate the viability and effectiveness of the proposed

topology in securing the network against threats and attacks, experimental results and analysis which are based on Cisco Packet Tracer network simulator are discussed and cconclusions are drawn in Section V.

## II. Network firewall Systems

Firewall is the most widely adopted technology for controlling the flow of network traffic between an organization's internal network and the Internet [12], [13]. It maintains security measures by preventing intrusion from hackers, viruses, and worms into a private network [14]. Also, firewalls prevents unauthorized access into an enterprise systems and resources from the Internet as well as restricting connectivity to and from part of internal networks that is used for sensitive functions. Network firewalls are often placed at the perimeter of a network, that is, between the internal network and the external network so as to monitor all incoming and outgoing packets and decide whether to accept or discard them based on the specified policy [12], [14]. Besides the high-level security policy mechanisms through the blacklists and the whitelists, there are low-level access control lists (ACL) that firewall employs to define filtering patterns for authorized and illegitimate traffic flows [15]. There are three major types of firewalls, each with different proficiencies for scrutinizing network traffic up to a particular layer of the protocol stack and then allow or block specific instances by comparing traffic characteristics to existing policies. Such firewalls are packet filter, stateful packet filter, and application proxy [12], [14]. A typical firewall system is depicted in Fig. 1.

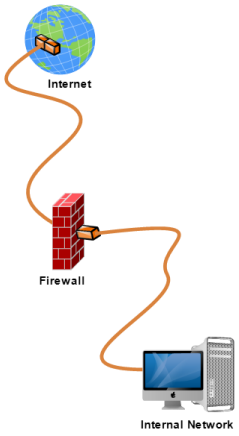


Fig. 1. Typical Firewall system.

### A. Packet Filter

In a packet filtering firewall, packets are examined up to the network layer and are filtered based on the available information at the layer. Such information regarding the source and the destination includes IP addresses, ports and the Transmission Control Protocol (TCP) flag bits [14]. The potentials for packet filtering are integrated into most operating systems and devices such as routers which are capable of routing using the access control lists [12]. Furthermore, the simplicity of this approach is due to the fact that packets are filtered based on ingress or egress filtering ruleset that requires just the header information for packet processing which results in implementation efficiency. Nevertheless, this approach has certain weaknesses such as inability to keep track of the state of each flow of traffic which results in not being able to associate multiple requests within a single session to each other. This is the reason why a packet filtering firewall is also called stateless inspection firewall [14], [16]. Furthermore, packet filter has no concerned about the content of the packets, thereby, it is blind to application data in which viruses reside. Moreover, packet filters are prone to the TCP Acknowledgment scan (TCP ACK scan) attack which is a technique that unauthorized users employ to scan for open ports through the firewall. Therefore, in order to prevent this attack, the firewall has to remember existing TCP connections to be able to realize that the ACK scan packets are not part of legitimate connection [12], [14].

### B. Stateful Packet Filter

A stateful packet filter is an advanced type packet filter with enhanced functionalities for tracking the state of connections and blocking packets that deviate from the expected state [16]. This type of firewall operates at the transport layer in which greater awareness is incorporated for system improvement. In relation to packet filtering, stateful filter inspects intercepted packets at the network layer for conformity with an existing ruleset, on the other hand, unlike packet filtering, stateful filter keeps track of each connection in a state table that has typical contents such as source and destination IP addresses, port numbers, and connection state information [12]. This is the main benefit of a stateful filter which prevents the TCP ACK scan attack. However, besides the fact that a stateful packet filter cannot examine application data, it requires more processing time which makes it to be comparatively slow [14].

### C. Application Proxy

This is an advanced firewalls that combines lower-layer access control with upper-layer functionality in order to process an incoming packets all the way up to the application layer. This type of firewall has the ability to verify legitimacy of the packet as well as inspecting the actual content of the traffic [12], [14]. In addition to being able to perform TCP handshake with the source system, it also protects the system against exploitations at each stage of communication [12]. The main benefit of the application proxy is that, it has a comprehensive view of connections and the application data. Consequently, apart from being capable of filtering bad packets at the transport layer, the application proxy is also able to filter bad data such as viruses at the application layer. However, because the packet has to be processed up to the application layer and the resulting data has to be interpreted, an application proxy relatively requires much more time [14]. It has been observed that irrespective of the strength of the firewalls, there is still high tendency of network intrusion, so, there is need for intrusion detection [12].

### D. Intrusion Detection

It has been observed in [12] and [14] that, system authentications, firewalls, and virus protections are means of preventing intrusions in a network. However, regardless of

measures taken for intrusion prevention, occasionally, there may be security breach which results in unauthorized access into the enterprises systems and resources. To address this issue, intrusion detection system (IDS) may be employed to detect attacks before, during, and after they might have occurred by looking for unusual activities in the network [12]. Basically, there are two IDS architectures; the first architecture is a host-based IDS that focusses its detection scheme on activities that occurs on the hosts and aimed at detecting attacks such as buffer overflows and escalation of privilege [12]. Moreover, the second architecture is network-based that applies detection methods to network traffic and aimed at detecting attacks such as network probes, denial of service, and malformed packets. Furthermore, there are two intrusion detection methods which are signature-based and anomaly-based IDSs. The former detects attacks based on known *signatures* or *patterns* while the latter defines a standard behavior of the system and then provides a notification any time the system strays too far from the set standard [12].

## III. Proposed Network Security Architecture

This study proposes a multi-layer firewall system for augmenting the functionalities of other network security technologies. This gives multiple security measures to protect network integrity because, it will be more difficult to breach a complex and multi-layer system by intruders. To achieve a layered protection, a packet filtering firewall, application proxy firewalls, and intrusion detection systems (IDSs) are proposed to be implemented at different levels in a campus network. To start with, the campus network is divided into two main parts which are, the demilitarized zone (DMZ) and the internal network that is further divided into virtual local area networks (VLANs) in order to ease the required security measures so that network traffic and access control lists can be easily administered. The DMZ is the network part that receives most of the outside traffic and needs to be exposed to the outside world. It contains the campus network public servers such as web and mail servers. Therefore, to prevent any devastating attacks on this part and to enable external access, a packet filter is employed at the perimeter of the network to prevent low-level attacks on the systems in the DMZ.

Furthermore, an application proxy firewall and IDS are positioned between the internal network and the DMZ to give better protection for the internal network against attack. It should be noted that network virtualization addresses scalability and flexibility issues as well as providing certain degree of security in the network. Moreover, for each VLAN, another application proxy firewall is employed and IDS may also be employed to detect attacks. It is also suggested that internet security software such as anti-malware should be installed in order to detect and remove hostile or intrusive software such as worms, Trojans, rootkits, rogues, spyware, and other malicious programs from the systems in the network. Furthermore, hierarchical passwords and biometric verification should also be implemented in certain part of the network. All these measures create defense-in-depth security policy that addresses both internal and external security threats. The proposed security architecture is shown in Fig. 2.

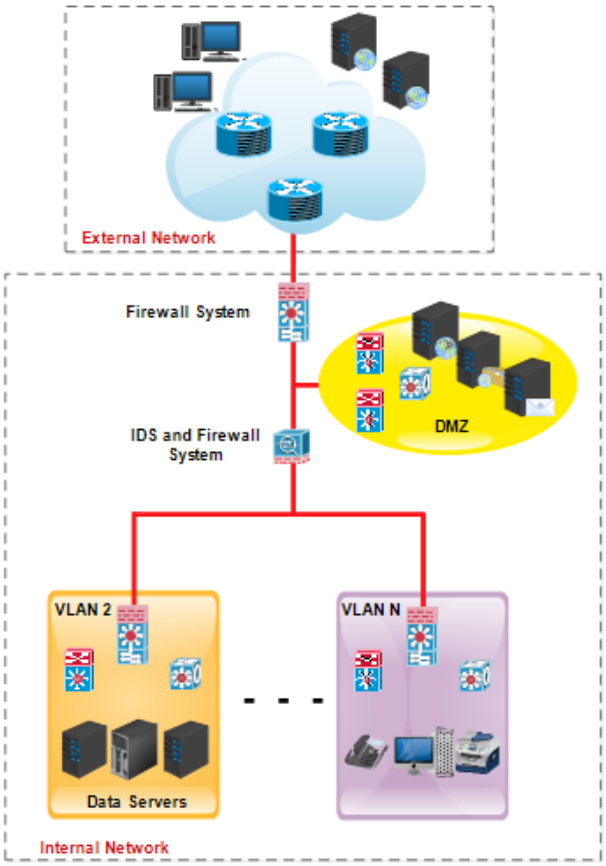


Fig. 2. Proposed security architecture.

## IV. Experimental Results and Analysis

This paper presents comprehensive practical application of access control list in managing network security by defining ruleset on a router that serves as the firewall. The security analysis in this work is divided into two main sections. The first part demonstrates how to use the firewall to prevent unauthorized access to the internal network from the internet while still permitting necessary access to the campus web servers. Also, the second part deals with how the firewall enables access to the internal network from the internet when the action is established from within. The experimental network security architecture shown in Fig. 3 consists of external (internet) and internal networks which are connected through the serial interface. The latter consists of two routers in which one serves as the firewall while the other functions as integrated firewall and intrusion detection system (IDS). Also, it has three multi-layer switches each of which supports different VLANs. The first switch in the DMZ connects the Web and Simple Mail Transfer Protocol (SMTP) servers to the network. The second switch supports the internal data server and host while the last one connects host and other network devices. Furthermore, the external network consists of a router and two multi-layer switches in which one connects the servers and the other connects the hosts to the network.

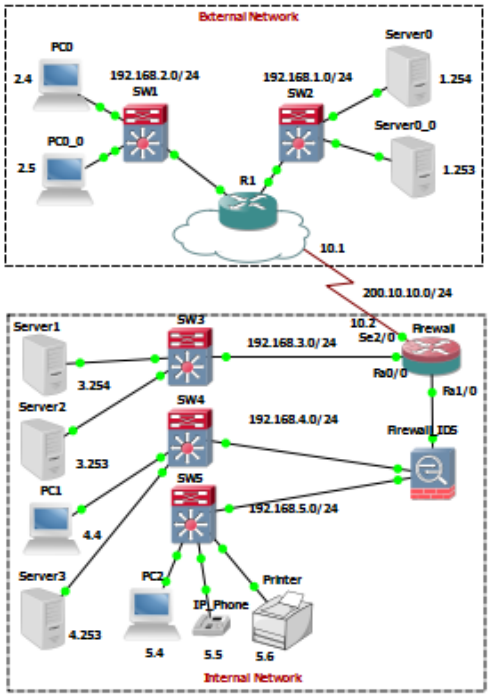


Fig. 3. Experimental network security architecture.

For simplicity, only the analyses for the PC0 and Server0 in the external network as well as the PC1, Server1, and Server2 in the internal network are presented. The network architecture employed is simulated using Cisco Packet Tracer, a graphical network simulator. The system topology is first tested to be functioning well by pinging each of the considered network components. The results presented in Fig 4-10 show that there is duplex communication between the network components of the external and internal networks.

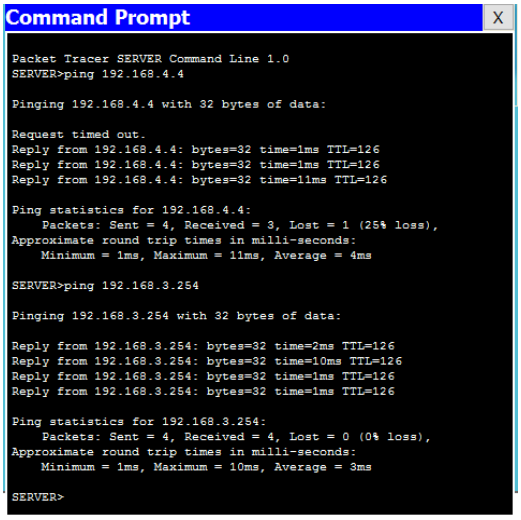


Fig. 4. *Ping results from Server0 to PC1 and Server1*.

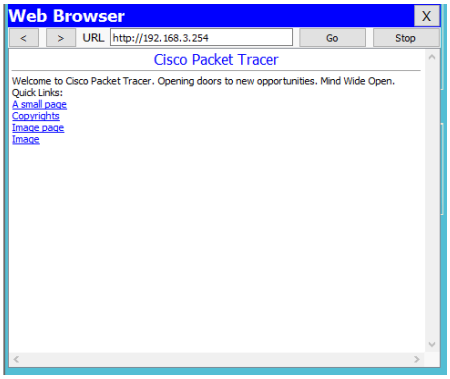


Fig. 5. Browser result from PC0 to Server1.

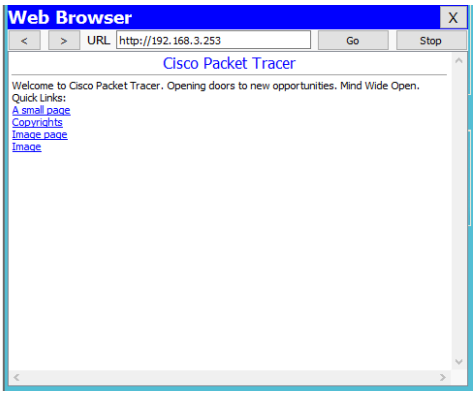


Fig. 6. Browser result from PC0 to Server2.

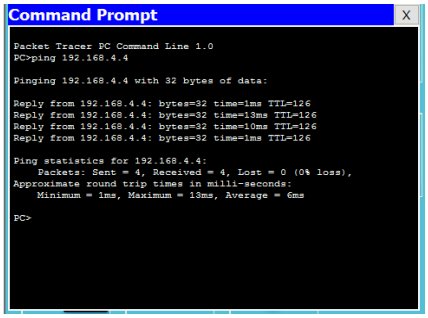


Fig. 7. Ping result from PC0 to PC1.

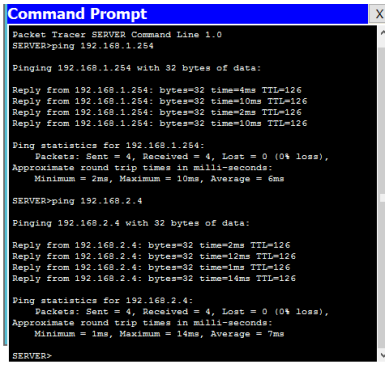


Fig. 8. Ping results from Server1 to PC0 and Server0.


Fig. 9. Browser result from PC1 to Server0.

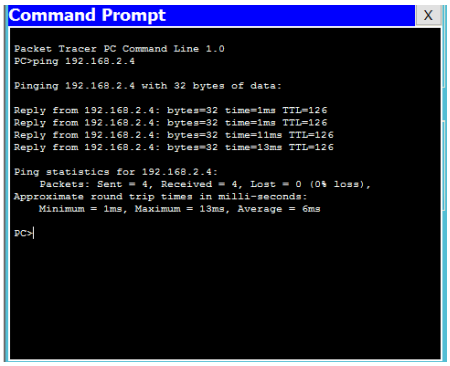


Fig. 10. *Ping result from PC1 to PC0*.

### A. *Experiment 1: Unauthorized Access Prevention by the Firewall*

This part presents how unauthorized access can be prevented. To achieve this, the firewall is configured to intercept and inspect each incoming packet and take a decision on whether to accept the packet for onward transmission or to discard it based on ingress or egress filtering ruleset. A firewall system operation is based on first-match criterion to determine which rule should be applied to which packet. The filtering ruleset is sequential and divided into two parts, namely predicate and decision and is of the form [11], [10].

$$< predicate > \rightarrow < decision >$$

where <*predicate*> is a function that assigns a Boolean value true or false to each packet fields, such as the protocol type, source and destination IP addresses and port numbers while <*decision*> is either "accept" or "discard". A firewall *F* executes two steps when an incoming packet *p* reaches it. In the first step, it identifies the first rule *r* in the sequential ruleset whose <*predicate*> allots the value true to packet *p* due to the matches in the fields while in the second step, if the <*decision*> of rule *r* is to accept or to discard packet *p*, then, the firewall accepts or discards the packet as the case may be [11], [10].

The firewall is configured with access control lists (ACLs) to permit access to server1 and serve2 in the DMZ of the internal network. Furthermore, there is implicit deny all that prevent unauthorized access in the ACL. The ACL configuration on the firewall in the running configuration which indicates that the ACL is applied on interface serial2/0 of the router in the inbound direction is depicted in Fig. 11. Moreover, Fig. 12 and Fig. 13 show that PC0 can access the web server and SMTP server respectively. However, the ACL prevents access from PC0 to PC1, so, the result in Fig. 14 shows that the destination host is unreachable.

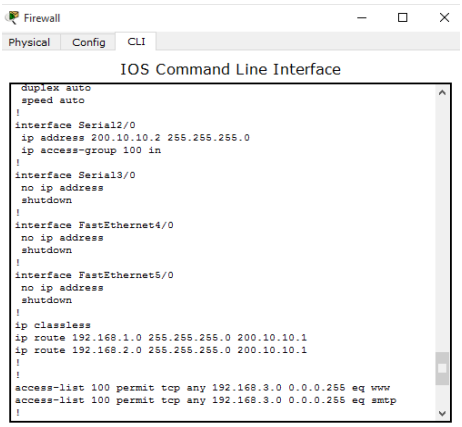


Fig. 11. Firewall configuration.

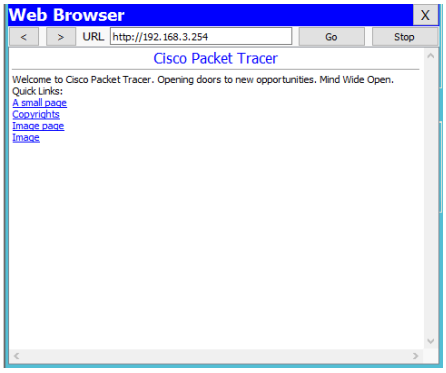


Fig. 12. Browser result from PC0 to Server1.

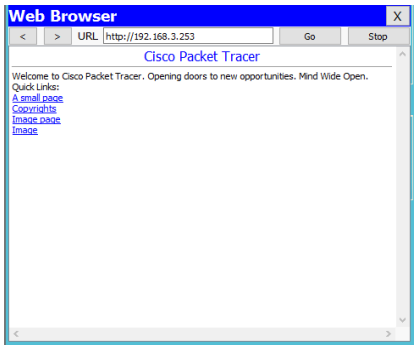


Fig. 13. Browser result from PC0 to Server2.

The configuration shown in Fig. 11 is efficient in preventing an unauthorized access, however, when the PC1's web browser tries to communicate with the internet web server0, Hypertext Transfer Protocol (HTTP) request timed out responses in Fig. 15 and Fig. 16 are obtained despite the fact

that HTTP and HTTP Secure (HTTPS) are enabled on server0 as shown in Fig. 17.

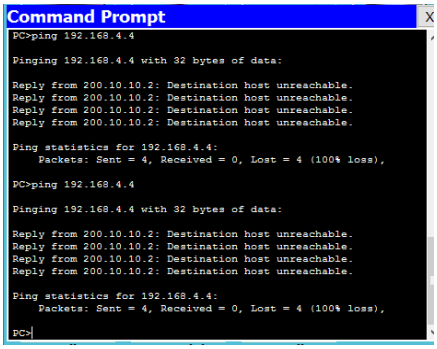


Fig. 14. Ping result from PC0 to PC1.

This issue is caused by the firewall that allows the echo-request that is outbound from PC1 but prevents the echo-reply that is inbound. The next subsection presents how to address the issue.

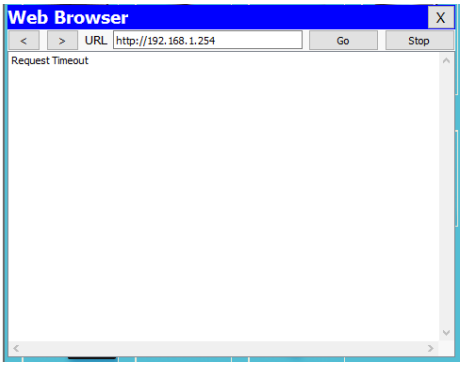


Fig. 15. Browser result from PC1 to Server0.

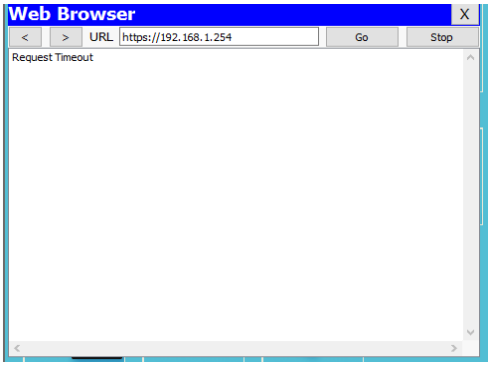


Fig. 16. Browser result from PC1 to Server0.

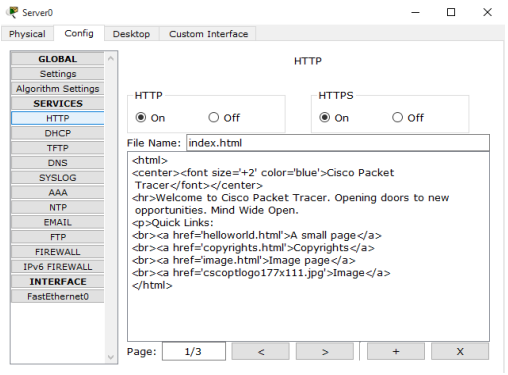


Fig. 17. Server0 HTTP configuration.

## B. *Experiment 2: Established Traffic Permission by the Firewall*

The part addresses the issue in the previous experiment by making the firewall to be more intelligent in recognizing that, whenever the request is made from the inside, it should allow the reply to enter the internal network. To achieve this, another ACL is configured on the firewall to allow any Transmission Control Protocol (TCP) session that is established from the network. The ACL configuration on the firewall in the running configuration which indicates that the ruleset is applied on interface serial2/0 in the inbound is depicted in Fig. 18. Moreover, Fig. 19 and Fig. 20 show that PC1 web browser can now access the web server0 because the echo-request and echo-reply are allowed by the firewall.

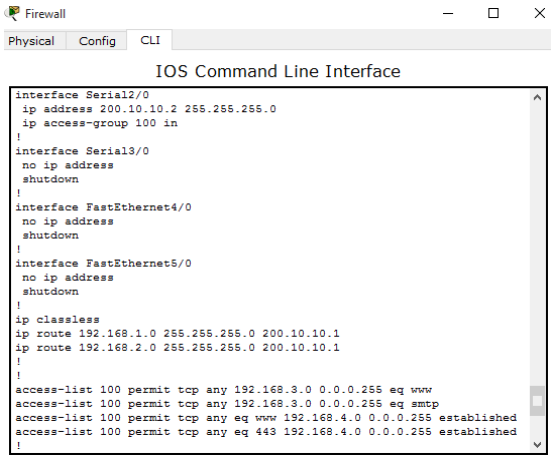


Fig. 18. Firewall configuration.


Fig. 19. Browser (http) result from PC1 to Server0.


Fig. 20. Browser (https) result from PC1 to Server0.

## V. Conclusion

The development in communication systems as well as high rate of Internet usage require adequate security for effective transmission of information over such media in order to prevent some security breaches. This paper presents an effective multi-layer firewall system for augmenting the functionalities of other network security technologies. The effectiveness of the proposed network architecture is demonstrated using Cisco Packet Tracer. The simulation results show that, implementation of the proposed topology is viable and offers a reasonable degree of security at different network layers.

## References

[1] I. A. Alimi, A. O. Mufutau, "Enhancement of network performance of an enterprises network with VLAN," American Journal of Mobile Systems, Applications and Services, vol. 1, no. 2, pp. 82-93, July 2015.

[2] M.P. Leong, S.Z.M. Naziri and S.Y. Perng, "Image encryption design using FPGA," 2013 International Conference on Electrical, Electronics and System Engineering, Kuala Lumpur, pp. 27-32.

[3] I. A. Alimi and O. Aboderin, "Enhanced encryption algorithm based on a modified confusion and diffusion scheme," American Journal of Mobile Systems, Applications and Services, vol. 1, no. 1, pp. 20-29, July 2015.

[4] W. Cuihong, "The problems in campus network information security and its solutions," 2nd International Conference on Industrial and Information Systems, Dalian, vol.1, pp.261-264, July 2010.

[5] Z. Wang, "A new type of intelligent network security model of the campus study," 3rd International Conference on Computer Research and Development, Shanghai, vol.2, pp.325-329, March 2011.

[6] H. Changwei, X. Jinquan, and P. Zhengwen, "Applied research on snort intrusion detection model in the campus network," IEEE Symposium on Robotics and Applications, Kuala Lumpur, pp.596-599, 3-5 June 2012.

[7] I. A. Alimi, A. O. Mufutau and T. D. Ebinowen, "Cost-effective and resilient large-sized campus network design," American Journal of Information Science and Computer Engineering, vol. 1, no. 1, pp. 21-32, June 2015.

[8] K. Han, "The study of cryptography in the application of the land management of campus network," 3rd International Conference on Intelligent System Design and Engineering Applications, Hong Kong, pp.1554-1556, Jan. 2013.

[9] U. Mustafa, M.M. Masud, Z. Trabelsi, T. Wood, and Z. Al Harthi, "Firewall performance optimization using data mining techniques," 9th International Wireless Communications and Mobile Computing Conference, Sardinia, pp.934-940, July 2013.

[10] H.B. Acharya, A. Joshi, and M.G. Gouda, "Firewall modules and modular firewalls," 18th IEEE International Conference on Network Protocols, Kyoto, pp.174-182, Oct. 2010.

[11] S. Khummanee, A. Khumseela, and S. Puangpronpitag, "Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules," 10th International Joint Conference on Computer Science and Software Engineering, Maha Sarakham, pp.93-98, May 2013.

[12] M. Stamp, Information Security Principles and Practice, Canada, John Wiley & Sons, 2006, pp. 191-198.

[13] C. Fei, B. Bruhadeshwar, and A.X. Liu, "Cross-domain privacy-preserving cooperative firewall optimization," IEEE/ACM Transactions on Networking, vol.21, no.3, pp.857-868, June 2013.

[14] K. Scarfone and P. Hoffman, Guidelines on Firewalls and Firewall Policy, Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev.1, pp. (2-2)-(2-6), Sep. 2009.

[15] Z. Du, L. Jujjavarapu, and L. Meiliu, "Detecting and resolving inconsistencies in firewalls," IEEE 15th International Conference on Information Reuse and Integration, CA, pp.1-7, Aug. 2014.

[16] M.G. Gouda and A.X. Liu, "A model of stateful firewalls and its properties," Proceedings. International Conference on Dependable Systems and Networks, pp.128-137, June 2005.