The Design and Implementation of On-Line Examination Using Firewall security

V.Selvi[1], R.Sankar[2], R.Umarani[3]

[1]*Master of Computer Applications, M.A.M College of Engineering, Siruganur, Tamil Nadu.India*
[2]*Computer science and Engineering, M.A.M College of Engineering, Siruganur, Tamil Nadu.India.*
[3]*Department of Computer Science, Sri Saradha College for Women, Salem, Tamil Nadu.India.*

Abstract: *Online Examination System is a software solution, which allows a company or institute to arrange, conduct and manage examinations via an online environment. This can be done through the Internet, Intranet and/or Local Area Network environments. In this paper propose a system that provides security to improve on-line Examination by utilizing DMZ Concept in firewall technology. This research paper, discuss the performance of online exam with respect to the security provided by the firewall technology. This paper concludes that by improving the security system using a firewall that can be incorporated into the proposed system to fulfil the challenge of online examination system. We proposed a system using firewall technology to monitor candidates and control network packets of all machines incorporating the username and password for authentication. This paper provides an overview of online Examination System using firewall technologies.*

Keywords: *Firewall, Network security, Online examination system, Firewall security.*

I. Introduction

Online Examinations, sometimes referred as e-examinations, are the examinations conducted through the internet or in an intranet (if within the Organization) for a remote candidate (s) [1].Online examination system is designed for universities, schools, colleges and even Banking, Government for recruitment purposes. Today many organizations are conducting online examinations worldwide successfully and produce the results in online [2].

Online Examination System is used for conducting online objective test; the test will be customized such that system will have automated checking of answers based on the user interaction [3]. Exam System is very useful for Educational Institute to prepare an exam, safe the time that will take to check the paper and prepare mark sheets [4]. Online Examination System (OES) is a Multiple Choice Questions (MCQ) based on examination system that provides an easy to use environment for both Test Conductors and Students appearing for Examination. This system is secure information is provided to user [5].

Most of the examinations issue results as the candidate finish the examination, when there is an answer processing module also included with the system. Candidate is given a limited time to answer the questions and after the time expiry the answer paper is disabled automatically and answers sent to the examiner. The examiner will evaluate answers, through automated process and the results will be sent to the candidate through email or made available in the web site [6].

The system is consisting of a web based server with a database facility. Database it contains User information and authentication for the Examination. This server is configured with proper security measures. Clients (candidates) can connect through the internet with a web browser (Eg: Internet Explorer, Mozilla Firefox etc) or Intranet or using a small application in client system to connect the server and take the examination. Examiners too can connect to the server through the internet or through the intranet for setting up papers and to do other related tasks. The system should be designed in as a secured system applying safety measures. Special exception handling mechanism should be in place to avoid system errors. In case of scenarios where data integrity can be compromised, measures should be taken to ensure that all changes are made before system is shut down.

One of the protective mechanisms under serious consideration is the Firewall. A firewall is one of the protective mechanisms to protect a network which is used for conducting the secure online examination using internet and intranet. It is mainly used for to avoid the internal and external network traffic and to avoid the External Ethical hackers for attack the network [7]. Firewalls are becoming more sophisticated by the day, and new features are constantly being added, so that, in spite of the criticisms made of them and Developmental trends threatening them, they are still a powerful protective mechanism.

II. Need of Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

If your PC is connected to the Internet, you are a potential target to an array of cyber threats, such as hackers, key loggers, and Trojans that attack through unmatched security holes. This means that if you, like most people shop and bank online, are vulnerable to identity theft and other malicious attacks.

A firewall works as a barrier, or a shield, between your PC and cyber space. When you are connected to the Internet, you are constantly sending and receiving information in small units called packets. The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data. This way, hackers cannot get inside and steal information such as bank account numbers and passwords from you.

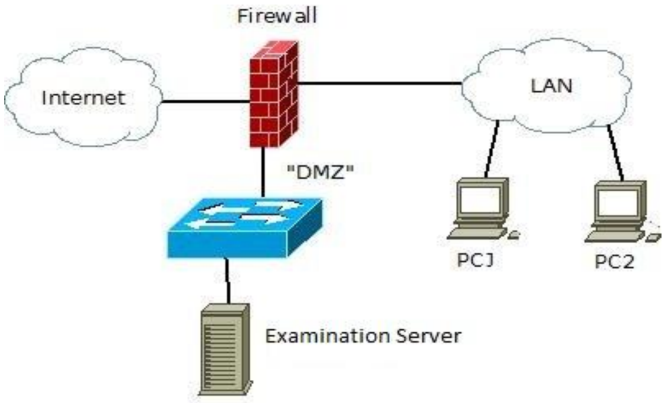

Fig 1 Firewall with network security

III. Characteristics of Firewall:

3.1 Firewall Capabilities

- A firewall defines a single choke point that keeps unauthorized users out the protected network.
- A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
- A firewall is a convenient platform for several Internet functions that are not security related.
- A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private network.

3.2 Design Goals

- All traffic from inside to outside, and vice verse, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration. This implies the use of a trusted system with a secure operating system.

3.3 Methods Of Control In Firewall

- User control: Only authorized users are having access to the other side of the firewall.
- Access control: The access over the firewall is restricted to certain services. A service is characterized e.g. by IP address and port number.
- Behaviour control: For an application, the allowed usage scenarios are known. E.g. filters for e-mail attachments (virus removing).
- Direction control: Different rules for traffic into the Intranet and outgoing traffic to the Internet can be defined.

IV. Types of Firewall

For the general user, you can place firewalls into two simple categories: hardware and software. Hardware firewall can be purchased as a stand-alone product but are also typically found in router, and should be considered an important part of your system and network set-up. You can plug more computers into the router, and each will be protected by the firewall that's part of the router.

A software firewall is one like Zone Alarm. You install it on your PC, and it will hide open ports, deflect incoming attacks, and warn you about suspicious outgoing traffic. For added protection, you can have a software firewall on each computer that sits behind the router. An attacker would have to be very determined to get through your router's firewall and your software firewall!

4.1 Common Firewall Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through.

4.2 Packet Filter

A basic firewall uses packet-filtering routers. The router applies a set of rules to each incoming IP packet and then forwards or discards the packet. It is usually designed to filter packets going in both directions. Filtering rules are based on fields in the IP or transport header, including source and destination IP addresses and TCP or UDP port numbers. The filter is set up as a list of rules to determine whether to permit or block a packet. When a packet comes, the router checks whether it matches one of the rules. The rules are checked from top to bottom on the list. If a rule is matched, then the rule is invoked. Otherwise, a default action is called.

4.3 Application Gateway

An application-level gateway is also called a proxy server. The user contacts the gateway using a TCP/IP application and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the remote host and relays the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. The gateway can be configured to support only specific features of applications.

4.4 Circuit-level Gateway

A circuit-level gateway does not permit an end-to-end TCP connection. The gateway sets two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. The firewall intercepts TCP connections being made to a host behind it and completes the handshake on behalf of this host. The security function consists of determining which connection will be allowed. Once the two connections are established, the gateway usually will not exam the TCP segment.

A typical use of circuit-level gateway is in a situation in which the internal users are trusted. Then the gateway can be configured to support circuit-level functions for outbound connections and proxy service on inbound connections (i.e., check incoming data but not outgoings data).

4.5 Proxy Server

A Proxy is a central machine on the network that allows other machines in that network to use a shared Internet connection. Proxy servers are intermediate servers which accept requests from clients and forward them to other proxy servers, a source server, or service the request from their own cache. The proxy is also called 'server' or 'gateway'. Proxy allows users on a network to browse the Web, send files over FTP, and work with E-mail and other Internet services.

A Firewall Proxy provides Internet access to other computers on the network but is mostly deployed to provide safety or security. It controls the information going in and out the network. Firewalls are often used to keep the network safe and free of intruders and viruses. Firewall proxy servers filter, cache, log, and control requests coming from a client. A firewall proxy is one that is used for restricting connections from a proxy to the outside world or to the source server inside of the LAN. This is different from a conventional firewall, in that a conventional firewall restricts connections coming from the outside world.

V. Intrusion Detection System

An intrusion detection system (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place − not prevent them. An IDS essentially reviews your network traffic and data and will identify probes, attacks, exploits and other vulnerabilities. IDSs can respond to the suspicious event in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. In some cases the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion.

5.1 Intrusion detection functions include

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

5.2 Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network. A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN). VPNs are often used to extend intranets worldwide to disseminate information and news to a wide user base. Educational institutions use VPNs to connect campuses that can be distributed across the country or around the world.

In order to gain access to the private network, a user must be authenticated using a unique identification and a password. An authentication token is often used to gain access to a private network through a personal identification number (PIN) that a user must enter. The PIN is a unique authentication code that changes according to a specific frequency, usually every 30 seconds or so.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunnelling protocols such as the Layer Two Tunnelling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

5.3 NAT (Network Address Translation)

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

5.4 DMZ (demilitarized Zone)

A DMZ (demilitarized Zone) is a conceptual network design where publicly accessible servers are placed on a separate, isolated network segment. The intention of a DMZ is to ensure that publicly accessible servers cannot contact other internal network segments, in the event that a server is compromised. A Firewall is particularly relevant in DMZ implementation, since it is responsible for ensuring that proper policies are in place to protect local networks from the DMZ, while maintaining accessibility to the DMZ. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ. Those computers on the outside intercept traffic and broker requests for the rest of the LAN, adding an extra layer of protection for computers behind the firewall.

VI. Conclusion

In this paper mainly focused on to Conduct an Online Examination System in more secure way using a Hardware firewall. The DMZ is a one of the main concept in a Hardware Firewall and their usage in enhancing security in online Examination system. The demilitarized Zone is a restricted Zone in network. It is mainly used for to keep the Online Examination System servers in this Zone for network protection and to avoid the Internal and External network traffic and to avoid the Internal and External Hackers and to provide more secured authenticated system to the examination users.

References

[1] http://www.esigmatechnologies.com/etest-online.html.

[2] Chi-Chien Pan et al, Secure online examination architecture based on distributed firewall , e-Technology, e-Commerce and e-Service, 2004 IEEE International Conference on , 28-31 March 2004 ,533 - 536 .

[3] http://eduexamsoftware.weebly.com.

[4] www.projectcorner.in/online-examination-system-college-project-asp-net.

[5] Bhagyashri Kaiche et al , Online Descriptive Examination and Assessment System, International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014.

[6] http://oes.sourceforge.net.

[7] http://www.esigmatechnologies.com/etest-online.html.

[8] Borromeo, R.M.H. , Online exam for distance educators using moodle, Educational Media (ICEM), 2013 IEEE 63rd Annual Conference International Council for DOI: 10.1109/CICEM.2013.6820155 Publication Year: 2013 , Page(s): 1 – 4.

[9] Gupta, P.K., Mobile examination system, Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on DOI: 10.1109/PDGC.2012.6449836 ,Publication Year: 2012 , Page(s): 302 – 306.

[10] Ullah, A. ; Hannan Xiao ; Lilley, M. ; Barker, T. , Usability of profile based student authentication and traffic light system in online examinations, Internet Technology And Secured Transactions, 2012 International Conference for Publication Year: 2012 , Page(s): 220 - 225 .

[11] Ruhnow, M. ; Kohser, J. ; Bley, T. ; Boschke, E. ; Bulst, M. ;Wegner, S. , Robust multi-parametric sensor system for the online detection of microbial bio films in industrial applications — Preliminary examinations, Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on , Publication Year: 2014 , Page(s): 1 - 4

[12] Jani, H.M. , Benefiting from online mental status examination system and mental health diagnostic system, Information Sciences and Interaction Sciences (ICIS), 2010 3rd International Conference on ,Publication Year: 2010 , Page(s): 66 – 70.

[13] Swe Zin Hlaing , An Authenticated Paradigm for Mobile Agent System in Online Examination, Computer Engineering and Technology, 2009. ICCET '09. International Conference on ,Volume: 2 , 2009 , 420 – 424.