Best practices for firewall configuration and maintenance in higher education

Graduate Student in the College of

Engineering and Technology

Wendell Collie Jr.

Department of Technology Systems

East Carolina University

Fundamentals of Network Security

Phil Lunsford, Advisor

November 16th, 2016

Abstract

This paper's purpose is to investigate best practices for firewall configuration and maintenance in higher education. It seeks to aid these learning institutions by providing an in-depth analysis of firewalls. In particular, this study will have compared various types of firewall technologies along with its features.

The information presented is obtained from interviews, surveys, and analysis of available reports. That data and the information are then analyzed and summarized to be graded against various evaluation criteria to determine which methods are best suited for a higher education environment.

Afterward, a detail pros and cons model will provide in-depth knowledge of each feature which transitions to a list of common bad practices, its associated risk and how to avoid/fix them. Lastly, we will explore numerous policies that will provide network administrators with strategies and guidelines to make decisions more efficiently.

I. Introduction

In today's society, cyber security attacks have increased exponentially. The Educational sector is seeing an increase in security breaches. It has been a challenge for these institutions because of the fundamental design of their business. Universities are structured to be open and inviting for its students. However, attackers take advantage of this with malicious intent. According to Symantec's Internet Security Threat Report (2015), "6.6% of reported sub-sectors breached in 2015 involved educational services. This trails only the health services (39.3%) and business services (6.6%)".

According to Cisco.com (2016), "a firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of safety rules." Firewall are mainly designed to regulate the flow of IP traffic coming to and from a network. A firewall serves primarily as a defense mechanism against external threats to an institution's computer network. With cyber crimes increasing every year, firewall networks are more important than ever.

Networks without a firewall will not be able to prevent much-unauthorized access to their computer systems and resources. These unauthorized accesses can result in loss of confidential information, the loss of services that can result in hefty financial loss or the unauthorized changes or deletion of data. Hence, the firewall provides a university with security appliances that can regulate access to its computer network. In this paper, the focus is on best practices for firewall configuration and maintenance in higher education.

Firewalls are usually considered to be network or host based. A Network firewall is often an instrument that is attached to a network for the sole purpose of regulating traffic to a single or multiple devices on a network.
A host firewall is usually an application with a Graphical User Interface (GUI) that addresses access to a single host. Additionally, an administrator can manage the firewall and can create custom rules from the host.

Firewall precisely checks all of
the packets that flow through its input-output interfaces by strictly following the predefined rules (Atipong et al. 2013). These rulesets specify which services are allowed to pass through the firewall. The rule-set has three categories. They are:
The basic rule set - These usually blocks all traffic except for a list of exceptions for commonly used services.
The custom rule set – These rules overrides but compliments the base rule set.
The signature rule set – These are designed to prevent known exploits.
They typically override all rules and must be updated regularly.

Creating a firewall policy that includes each type of ruleset, can help enhance the security of a network. However, A poorly configured firewall will create holes in an organization's security and leave it vulnerable to attacks. This section will focus on the various types of firewalls and the pros and cons for each.

Firewalls are used to protect both home, corporate and campus networks. There are several types of firewall used to prevent malicious information from entering these network: Packet Filtering, Stateful Inspection, Application Level Gateway, and Circuit Gateway.

II. Types of Firewalls

A. Packet Filtering Firewall

Packet Filtering Firewall analyzes traffic at the transport protocol layer. Each packet that passes through a firewall is examined and compared to a predefined set of rules before it is allowed to go through. The control determines whether a communication is allowed and respond by either denying or permitting the packet. Packet filtering allows the administrator to allow or deny traffic based on the source and destination IP address, the sources and destination port or the protocol used in for the packet as shown in Table 1.

Table 1. An example of a packet filtering firewall rule set

	Type	Source Address	Destination Address	Source Port	Destination Port	Action
1	TCP	any	172.16.1.1	>1023	25	Permit
2	TCP	any	192.168.1.3	>1023	25	Permit
3	TCP	any	192.168.1.4	25	>1023	Permit
4	TCP	192.168.1.2	any	>1023	25	Deny
5	any	any	any	any	any	Deny

Pros

Packet filtering is the fastest firewall technology as it uses fewer evaluations and uses less processing than the others. It only processes information up to layer 4 of the OSI model and is easily implemented.

Cons

Packet filtering firewalls cannot block specific application commands due to its limitation of upper-level OSI functionality. It also do not support advanced user authentication patterns and is unable to filter by a trusted host. Attacks or exploits that use the TC/IP structure and protocol stack exposes this flaws of this firewall. Many packet filtering firewalls cannot detect an altered network packet. Therefore, an easy way for intruders to bypass this type of firewall is by using spoofing attacks. Packet Filtering Firewalls are predisposed to security breaches caused by accidental configuration due to the limitation employed in its ACL decisions. Subsequently, little to no audit generation and alerting mechanism are available with this firewall.

Countermeasures to common packet filtering attacks

IP addressing spoof – Discard all packets that arrived on an external interface but has an inside source address.

Source routing attacks – Discard all packets that specifies the route a packet will take while traversing the internet.
Tiny Fragment attacks – Apply rules that determine a predefined minimum amount for the transport header of the first fragment of a packet.

B. Stateful Inspection Firewall

The stateful inspection firewall keeps track of the state of network connections such as TCP and UDP traveling through it and stores it in a dynamic table. Only packets matching known connections are allowed to pass through the firewall; all others are discarded. The data stored in this table is evaluated so that future filtering decisions will not be based solely on the administrator's firewall rules but also in the context of previously opened network connections. The firewall prevents the table from overloading with connections by dropping it after a period of no activity. Applications use Keep Alive messages that are periodically sent to the firewall to prevent active connections from dropping.

Pros
Stateful Inspection firewalls keep track of connection by storing it in a table. It is easy to log and audit all traffic to the application level of the TCP model. For instance, the table would include the source and destination port, the source and destination IP address and the status of the connection as shown in Table 2.

	Source Address	Source Port	Destination Address	Destination Port	Connection State
1	192.168.1.100	1023	172.16.1.1	25	Established
2	172.16.32.12	1024	192.168.1.3	25	Established
3	10.1.0.1	1025	192.168.1.4	80	Established
4	192.168.1.2	1026	10.2.3.4	25	Established

Cons
The primary disadvantage of using stateful inspection firewall is its additional overhead on each connection. When a connection has initiated, the gateway must examine incoming and outgoing traffic from both ends of the connection. Unwanted overhead processing occurs when many packets are entering the firewall.

C. Application Level Gateway

An Application Level Gateway acts as a relay for the OSI's application level traffic. It intercepts incoming and outgoing packets and decides whether to drop the packet or allow them through based on the application information within the packet. This process is initiated by setting up different proxies on a single firewall for various applications. The client and server both set up a connection to the proxies instead or directly connecting to each other. Once the connection has started, the firewall can discard any suspicious data or links. Application level firewalls inspect individual sessions and drop them based on the information in the application

protocol header or the payload. Most application firewalls include specialized application software along with proxy services.

These proxy services can provide increased access control, detail checks for valid data and generate audit reports about the traffic they transfer. The application firewall analyzes the complete command for a single protocol. When an incoming packet is received, it is moved through the OSI model until it reaches the highest protocol layer in the packet. After the packet has processed, the data is transferred to the proxy server which is listening on a TCP or UDP port. The proxy services then process that information and compare it to the set of rules designed by the administrator. The proxy then decides whether to accept or deny the packet based on the results of the comparison.

Pros

Application gateways have the capability to authenticate users directly. They can permit or deny specific incoming protocol commands from a particular user, while other firewalls can only regulate general incoming request. Application level gateway provides great content filtering because of its ability to examine a packet's payload and the capacity to make decisions on its content.

This firewall type has the power to review the entire packet rather than some network information such as source and destination ports. Furthermore, the firewall has more extensive logging capabilities, which provide vital information for handling security incidents and policy implementation. Application firewall by default shields internal IP addresses from the external world with the use of Network Address Translation (NAT). NAT makes network discovery substantially more challenging because attackers do not receive packets created directly by their target.

Cons

This firewall has numerous useful features; however, it does have a few disadvantages. Two of them are cost and performance. Because all traffic is inspected at the application level, it must pass through all seven layers of the OSI model before being inspected. As a result of this, the inspection process requires more processing power and has the potential to become a bottleneck for the extremely high-bandwidth network. Furthermore, Application firewalls are more susceptible to distributed denial of service attacks. The configuration of firewall proxies can be more arduous than other firewall technologies. Finally, an application layer firewall main focus is layer 7 of the OSI model and does not protect against lower layer attacks.

D. Circuit Level Firewalls

The Circuit level firewall looks at the Session layer of the OSI model. They continuously monitor TCP authentication between packets to determine if the requested session is legitimate. A circuit-level firewall establishes a connection between two authenticated trusted hosts. Once the session is connected, the gateway relays TCP segments from one connection to the other without examining the content. "The gateway maintains a table of established connections, allowing data to pass when session information matches an entry in the table (Midwest, 2008)". Once the section has ended, the gateway removes the connection from its table.

Pros
Like the Packet Filtering Firewall, Circuit level firewall has little impact on the network's performance. This firewall can conceal network from the sources. The information passed through a circuit-level firewall appears to be from the gateway and not the actual host. This is extremely useful when trying to hide information about a network.

Cons
Although Circuit firewall examines each session, it does not filter individual packets nor does it examine the contents of each packet. Once a connection between two authenticated trusted host begins, it just forwards packets in both directions.

The four types of firewalls are designed to control traffic flow. Each type has its advantages and disadvantages. Deciding which technique(s) is best depends on the institution's security policy.

III. Review of University firewall policies.

It is important that universities have firewall policies that correlate with its security policy. This section is going to review a few universities' firewall policy and look at some instances of attacks against their networks.

A. University of Cincinnati

The University of Cincinnati firewall policy procedures consists of a multi-layer approach to network security. It contains three different security layers: Tier 1, 2 and 3.

Tier 1 – Internet boundary connection of the University of Cincinnati.
This layer consists of a perimeter firewall, Intrusion Detection System (IDS), and VPN concentrator. The University uses these technologies for detecting and preventing any security breaches/intrusions.
Tier 2 – Subnet/router layer
This layer provides a firewall software and IDS. It is for the internal colleges, units, and the university's infrastructure servers.
Tier 3 – Desktop Machine, file servers or a UCit customer
A Personal Firewall and Anti-Virus software are provided to protect individual machines by installing updates, patches and performing backups regularly.

The University of Cincinnati logs all changes to the firewall using a Security Policy Modification Form. This form is used to keep track changes such as adding a new rule, modifying an existing rule or deleting a rule. The form requires the source or destination IP addresses along with the port numbers that are going to be affected by the change.

B. Brown University

In December 2003, Brown University created a firewall policy. At the time, there were over 15,000 hosts with 300 protected by a central firewall and 500 by a departmental firewall. Many at the university agreed that a firewall should protect the system, but some were adamant about it. They ensure that the firewall administrators were sufficiently trained to manage and monitor their logs to detect problems such as malicious activities or legitimate traffic blocking. They believe that the best option was to redesign the network infrastructure, but it was not feasible.

Subsequently, they decided to protect critical systems such as email, the web, and financial servers, with a firewall with hopes to gradually secure more systems and devices behind a firewall. The University recommended that the security administrators put central systems that provide critical services to the campus behind a large firewall and set up rules that allow authorized users to get data in and out of that secured environment. They went on to say that campuses with a distributed IT team, should implement smaller firewalls for a few machines and have the logs sent to a centralized logging server for future analysis.

C. Ulster University

At Ulster, the IT department deployed corporate firewall services for its network. The installation of the firewall moved the university from the default permit all traffic to the default deny inbound network. The tighten of security did not prohibit official University services but had further secured the existing services and network infrastructure. Ulster University realizes that having a firewall without a security policy is inexplicable. The university created a server connection policy and built its firewall rule-set around it. Any network traffic that does not comply with it was not allowed access through the firewall. Additionally, for a department to apply for access to the firewall for a particular application, a Server Connection Application Form was needed.

The process to make changes to the firewall: A user logs onto the shared application and completes the form. After the form is completed and submitted, the Approver will receive an email. Once approved then form will be directed to the Network team. The team will perform a risk analysis and scan the server for any vulnerabilities. If the risks are small or, there are no vulnerabilities detected, the firewall will be updated with the new rule, and the user will be made aware by an email.

To further bolster the security, all system administrators supporting services visible through the firewall were required to implement the following practices:
Install antivirus software and keep the definitions up to date.
Turn off or remove all unused network services.
Change all default passwords having them comply with the password policy.
Change all administrator or privileged account password regularly.
Keep the operating system and its applications patched to the latest version.
Ensure that critical data is backed up regularly.

D. Maryland University

On February 18th, 2014, a data breach occurred at the University of Maryland College Park (UMCP) which resulted in the loss of confidential information. The breach involved data such as social security number, names, date of birth and UMCP identification number. The breach happened through a vulnerable public accessible web server and application. Although the firewall had not been the focal point of the attack, an audit done by the Office of Legislative Audits viewed the firewall as a vulnerability. The results of their finding indicated 1) UMCP did not ensure that the firewall had properly secured all of the campus networks and 2) the firewall and intrusion presentation system were not configured to make sure that the network was secured.

The university's firewalls were not used at points were UMCP network connected to the public network and had limited packet filtering rules to protect access to the network. UMCP also did not have campus-wide policies mandating the use of firewalls to secure the local networks for departments. While the staff periodically examined the firewall security logs, it was not reviewed properly. They did not address specific events such as failed login attempts nor were they documented.

An additional audit was completed in December 2014, and University of Maryland's campus network was vulnerable to hackers. There still existed security gaps identified during a previous inspection in 2009. Some of the universities networks lack proper firewalls or systems that can detect intruders or malware. The audit further revealed that the firewalls did not protect all of the computers and no university policy for protecting the departmental networks existed. Auditors discovered that only 15 of the 500 plus campus departments laid behind a campus-wide firewall and many agencies were vulnerable to unauthorized access through computer labs or the Internet. Furthermore, auditors found that the university's firewall was operating on weak or outdated rules and there were no proper reviewing the security incidents logs. The school is aware of the issues and are strengthening its security by making improvements to the network and firewalls.

IV. Bad Practices

According to Chen et al. (2012), a fault model of firewall policies is an explicit hypothesis about potential faults in firewall policies. Their proposed model include five types of faults (pp 4):

Missing rules: When creating a firewall policy, it is easy not to add rules especially if there is not policy or it is not updated.
Wrong order of rules: The order of the rule is incorrect, and the firewall is permitting or deny the network traffic.
Wrong predicates: This indicates that the field of some rules is incorrect. The fields should be based on the security requirements.
Bad decisions: The decisions for some rules are wrong and are adversely affecting the network security.

Unintended extra rules: Security policies are always changing, and when an administrator make changes to a firewall policy, sometimes they forget to delete old rules that filter unintended traffic.

According to Chen et al. (2012) when trying to correct inconsistent firewall rules, there are five correction techniques to resolve the issues (pp 5):
Order fixing - Order fixing is changing the order of the rules and testing them to determine if the appropriate packets are permitted or denied.

Rule deletion - Deleting unnecessary or unwanted rules to will permit or deny traffic and checking it against the network security policy.
Predicate fixing - This is similar to adding a new rule. Find all the failed field and change them to the correct predicate.
Rule Addition - Adding a rule to the firewall policy that is going to strengthen the security of the network. The challenge with this is determining which position best suits the new rule.

VI. Best Practices

The following is a list of best practices that should be considered when configuring and maintaining a firewall in a higher education environment:

Ensure that the firewall rules are in the correct order. Misordering the firewall rules can misconfigure a firewall and allow unwanted traffic to the network.

It is best to deny all network traffic by default and only enable services that are needed. By doing this, it limits the opportunity for attackers.

All unnecessary services and software on the firewall should be disabled or uninstalled if the institution does not require it. Not doing so, can create a vulnerability in the system.

If it is possible, run the firewall services as a unique ID other that the administrator or root account so that an attacker will not be able to use that id for any other unauthorized access.

The default firewall administrator password should alway change after the initial login. Furthermore, there should be a password policy that should define the requirements for a network password.

Relying solely on a type of firewall is not recommended. Using a combination of firewall types can significantly decrease the chances of unauthorized access to a network.

Ensure that the system is filtering or disabling unused, unnecessary or vulnerable ports. Doing this will limit the opportunities for an attack on the network.

A university has an enormous amount of students and staff access its assets regularly. Ensuring that physical access to the firewall is secure/controlled is necessary.

Every institution should have a security policy. It is the responsibility of the administrator to ensure that the rules on the firewall are consistent with the organization's security policy.

An insecure operating system can make a firewall useless. Ensure that the operating systems have the latest patches and are regularly monitored for any new release patches for system vulnerabilities.

It is best to use a firewall conjunction with a router when connecting to the Internet to help prevent DDoS attacks.

Ensuring enable firewall logging and alerting if possible. Also regularly monitor these logs and investigate immediately if the entries look abnormal.

As discuss early in the Review of Educational policies, an institution should use change management forms to approved and monitor changes to the firewall. This form should contain the reason(s) for a change, the ports, and rule being added or removed and the affected services, IP addresses, and protocols.

Quarterly audits should be performed on the firewall to ensure that the firewall is adhering the security policy.

VII. Conclusion

In this paper, investigated best practices for firewalls and maintenance in higher education. An in-depth analysis of the four type of firewalls: Packet Filtering, Stateful Inspection, Application Level Gateway and Circuit Level Gateway were discussed. A list of best practices for firewall was provided to assist network administrators with strategies and guidelines to make decisions more efficiently.

Reference:

Beaver, K (). Firewall Best Practices. TechTarget. Retrieved from http://searchsecurity.techtarget.com/tip/Firewall-best-practices

Brown University (2003). Brown University Effective Practice: Firewall Strategy. Retrieved from https://net.educause.edu/ir/library/pdf/EPS172.pdf

Cisco.com (2016). What is a firewall? Retrieved from http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-fire wall.html

* Chen, F., Liu, A. X., Hwang, J., & Xie, T. (2012). First Step Towards Automatic Correction of Firewall Policy Faults. https://www.cse.msu.edu/~alexliu/publications/FirewallFixingMSU/FirewallFixing_Lisa.pdf

Dance, S (2014). Audit finds flaws remain in UM network security, even after data breach. The Ba ltimore Sun. Retrieved from http://www.baltimoresun.com/news/maryland/education/bs-md-umd-data-breach-audit-20141210-story.html

*Khummanee, S., Khumseela, A., Puangpronpitag, S. (2013) Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules. Retrieved from http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/xpls/icp.jsp?arnumber=6567326

Midwest Data Recovery Inc. (2008). Firewalls Explained: A Technical Overview. Retrieved from http://www.midwestdatarecovery.com/firewalls-explained.html

Symantec (2016). Internet Security Threat Report Vol 21, April 2016. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Ulster University (2000). Firewall. Retrieved from http://www.ulster.ac.uk/isd/services/networking/firewall

University of Cincinnati (2002). University of Cincinnati Perimeter Firewall Policy. Retrieved from https://www.uc.edu/content/dam/uc/ucit/docs/itpolicies/perimeter_firewall_policy.pdf

University of Maryland College Park (2000). University System of Maryland University of Maryland, College Park Division of Information Technology. Retrieved from