Global Information Assurance Certification Paper

If a network is secure, then it has more than a firewall

Josh A. Karl

GIAC Security Essentials Certification Practical (GSEC)

January 2005

Practical Assignment Version 1.4c Option 1

Table of Contents

1.0 Abstract

It seems that there is a common misconception in the world today when it comes to Network Security. Whether the organization is large or small there is a common notion that firewalls are the heart and core of securing a network. There is no doubt that firewalls play a vital role in any network security model but in today's world it takes more than just a firewall to protect an organization's resources and assets. With technology improving and new exploits emerging at a rapid rate there are several ways to get around an organizations firewall. When emerging technologies and exploits get in the wrong hands it could spell disaster for and organization that is not adequately protected.

Network Security needs to include more than just a firewall to protect the confidentiality, integrity and availability of an organization. Network Security in today's world is built upon a layered approach; which should include first and for most, an up-to-date security policy, firewalls, intrusion detection system, perform threat and vulnerability assessments, and patch management. This paper intends to introduce network security concepts and terminology to an audience of network analysts and network administrators that are entering the network security arena.

2.0 Security Policies

"Without a security policy, any organization can be left exposed to the world," [10]. Most organizations know the importance and necessity of having a precise and up to date security policy, but implementing and monitoring the security policy is no easy task. Organizations often have an unwritten security policy which makes the security policy very difficult to enforce. Once an organization has a security policy in writing it makes the policy enforceable and it can also reduce the legal liability to the organization. With no security policy in place, an organization's confidentiality, integrity, availability, and critical assets are at risk.

2.1 What is a security policy?

Security policies provide the foundation for an organization's security infrastructure. "A security policy is a document or set of documents that conveys the management's intentions and decision on how security will play a role within the organizations," [7]. In most cases security policies are high level and are not technical in nature. Security policies are intended to be an overview to educate end users of the acceptable use of information assets, as well as explain what is classified as appropriate or allowable use of an organization's information assets. A security policy should also describe in detail prohibited activities of information assets.

A complete and well developed security policy should address some of these

following issues:

- How sensitive information must be handled.
- How to properly maintain user ID(s) and password(s), as well as any other accounting data.
- How to respond to a potential security incident, intrusion attempt, etc.
- How to use workstations and Internet connectivity in a secure manner.
- How to properly use the corporate e-mail system. [4]

2.2 Who's involved with a security policy?

One of the first steps in creating a security policy is to determine who is going to sign off and own the security policy. This role and responsibility is held by the Chief Security Officer (CSO) of the organization. The CSO brings a large amount of knowledge and expertise to a security team, but they alone can not solely create a security policy. Successful and well developed security polices are not written by one individual but rather by a team of individuals.

"The next key step in creating a security policy is to establish a security team structure. Create a cross-functional security team led by a Security Manager with participants from each of your company's operational areas," [3]. This only makes sense. Individuals from each operational area know their areas better than anyone else because they are involved in the day to day operations. Where as, if the CSO were to write the security policy they might not know exactly what goes on in a specific operational area and may not realize that there is a need for a specific practice or procedure. Using a security team structure allows individuals from various operational areas to educate the Chief Security Officer on key business practices and procedures that they may not be familiar with. "The goal of the security team will be to make sure that the security policy meets the needs of the organization," [9].

2.3 Conducting a risk analysis

When an organization decides to draft and create a security policy it must first conduct a risk analysis in order to determine their policy needs. Although a workstation within an organization may cost two to three thousand dollars, the data on that workstation maybe worth upwards of one-hundred thousand dollars if it gets into the wrong hands. This is where it is vital that an organization identify and locate all of its network assets and perform a risk analysis on those assets.

"Risk Analysis is the process of identifying the critical information assets of the company and their use and functionality – an important (key) process that needs to be taken seriously," [4]. "The purpose of a risk analysis is to identify portions of the network, assign a threat rating to each portion, and apply an appropriate

level of security," [3]. These portions of the network may include key applications and systems, application servers, web servers, switches, routers, firewalls, etc. One approach is to assign each network resource one of following three risk levels:

> ***Low Risk***: Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access or other systems.
>
> ***Medium Risk***: Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process in disruptive to the system.
>
> ***High Risk***: Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems. [3]

Once the network resources have been assigned a risk level it is important to identify the types of users that will be using these network resources as well. The users can include, but not limited to, administrators, power users, users, partners, external vendors, and others.

2.4 Implementation of the security policy

When the security policy has been drafted, reviewed, revised, and agreed upon by the Chief Security Officer and the members of the security team, it is time to move forward with the implementation. "This is usually harder than the creation of the policy itself, due the fact that at this stage you also need to coach and educate your staff to behave in a "secure" manner, following each of the core elements pointed out in the formal security policy," [4].

The security policy must be readily available at all times to all employees within the organization. A copy of the security policy may be published on the organizations internal network or on the Intranet.

The security policy is a living document and should adapt to the ever changing IT world. To have a successful security policy the employees will have to continually be educated on the importance of the topics detailed in the policy.

The security team should be constantly reviewing the policy and employees should be required to review and sign the security policy on an annual basis.

2.5 Monitoring and auditing the security policy

"Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation," [3]. After a risk analysis is conducted, an organization has assigned each network resource with a risk level, low, medium, or high.

In most cases an organization would assign a high risk level to a firewall. This means that a firewall should be monitored heavily for any changes due to the function of the firewall. In order to set up monitoring, a SNMP polling agent needs to be installed to start monitoring for things such as failed login attempts, configuration changes to the firewall, services started or stopped, unusual traffic, and access that has been granted to the firewall. The monitoring software will detect the violation and then trigger an alert to the organizations operations center and security team via pager or cell phone.

Cisco recommends creating a monitoring policy for each area identified in the risk analysis. They recommend monitoring low-risk equipment weekly, medium-risk equipment daily and high-risk equipment hourly [3].

Security policies are difficult to manage and difficult to ensure that employees are obeying by the policy. For that reason periodical audits by internal auditors (if the organization is large enough to have their own) or an outside auditing firm is necessary. "Any deviation from the policy should be reviewed, a reason for the deviation determined and, assuming there's no reason for the deviation, the individual(s) should be disciplined," [5]. Security policies need to be enforced. All creditability of the policy is gone if the policy is not enforced.

3.0 Firewalls

Everybody is concerned about connecting their organizations to the Internet these days. It used to be that you rarely heard that an organization had been hacked and millions of dollars of data had been stolen. Times have changed and it's occurring more than we hear. In today's IT world it is in the best interest of an organization to install a firewall before connecting to the World Wide Web.

3.1 What is a firewall?

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 and leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified criteria [13].

3.2 How does a firewall work?

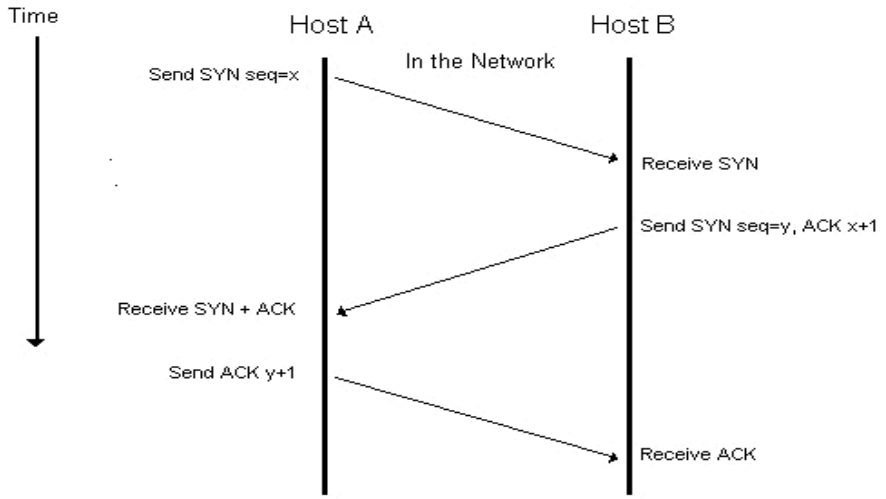
Since a firewall examines every packet entering and leaving an internal network, the firewall is able to make a decision on whether to "allow" or "deny" the packet. A firewall is able to make this decision based on rules that have been added to the software.

What is a packet? A packet is data packaged in a predefined size, and kept small for easy transmission [5]. When large amounts of data are sent across a network the data is broken up in numbered packets and then reassembled based on its number when it arrives at its destination. A packet consists of the source IP and port number, destination IP and port number, data, protocol, and error checking.

All communication via the internet takes place by the exchange of individual "packets" of data between two machines. A packet originates from a source machine and is sent to a destination machine. Once two machines exchange packets we often refer to this as a "connection" although in fact the connection consists of individual packets traveling between the two machines. This connection is set up by the "three-way handshake".

The three-way handshake is explained in the following paragraph:

> The source machine sends an initial packet that is referred to as a "SYN" to establish communication and "synchronize" sequence numbers in counting bytes of data which will be exchanged. The destination then sends a "SYN/ACK" back to the source which again "synchronizes" its byte count with the source and acknowledges the initial packet. The source then returns an "ACK" which acknowledges the packet the destination just sent. The connection is now "OPEN" and ongoing communication can take place until either the source or destination issues a "FIN" or a "RST" packet or the connection times out [8].



Every packet that is sent across the internet must include the destination IP address and a port number. The destination machine also needs to know the originating machines IP address and port number to validate that the originating machine is indeed who it claims to be. In other words, every packet contains the source IP address, source port number, destination IP address, and destination port number. The basic form of a firewall is able to examine the packet header, compare the source and destination IP's/ports to the rule base, and make a decision to "allow" or "deny" the packet.

3.3 Types of firewalls

There are a variety of different types of firewalls and they all work in different ways. The most common terminology you will hear firewalls referred to as are:

- Packet Filter
- Application / Proxy Gateway
- Circuit-level Gateway
- State-full inspection

Packet Filter

This type of filtering is the most basic of all and almost all firewalls support packer filtering. A packet filter looks at the header of each IP packet entering and leaving an internal network and "allows" or "denies" the packet based on the source IP address, source port, destination IP, and destination port.

In packet filtering, all decisions to "allow" or "deny" are based on the information contained in the packet header. No application level information is analyzed [6]. Due to the simplicity of packet filtering they tend to perform at high levels than proxy-based firewalls and they are more transparent to the end user and applications because they monitor at the network and transport layers.

Packet filtering works well controlling where users can and cannot go and helps manage traffic entering and leaving a network. However, it is susceptible to IP spoofing. IP spoofing is a common method used by intruders to bypass a packet filter by changing their IP address to look as though it is an internal IP address and therefore looks like legitimate traffic to the firewall. Packet filtering alone will not prevent an intruder from gaining access to a network.

Application / Proxy Gateways

Application gateways are often referred to as a Proxy Gateway. Proxy Gateways are able to add a security mechanism to specific applications such as Telnet and FTP. As discussed before packet filters monitor network traffic at the network and transport layers while Proxy filters monitor the network traffic at the application layer, which allows control over the interaction between client and server.

"In this environment, a client machine establishes a connection to a process on the firewall that listens for client connections. This process is known as an "application proxy," a "proxy server "or a "proxy"," [6]. By connecting to the proxy, the user has authenticated to the firewall. The user or the user's client software then indicates which server they want to access. Once the information about the requested server is received, the proxy connects to the remote host and from that point on the proxy relays the information being sent from the server to the client and vise versa.

The client thinks that the proxy server is the actual server and the actual server thinks that the proxy is the actual client. All traffic appears to come from the "actual client" or the "actual server" but its actually being relayed from the proxy. "By operating in this manner, the proxy can protect both the client and server by authenticating the client, determining if the client can use the requested service, preventing attacks and prohibiting certain application-level events (such as FTP PUT and FTP GET)," [6].

Proxy firewalls get more involved with the connection and have a lower performance that packet filtering. They also provide greater ability for audit logging but may require more managing and configuration than packet filters.

Circuit-level Gateways

A Circuit-level Gateway is a type of a proxy firewall but this proxy goes a little further than packet filtering. Instead of just filtering on information in a packet header, circuit-level gateways validate and monitor each session that is established in the communication [9]. A session has to be open and if it is not then traffic is blocked. A circuit-level gateway can determine if a connection is valid by the following:

- Source and destination IP's/ports
- Protocol
- User ID
- Password
- Time of day

Circuit-level gateways have an advantage over packet filter firewalls because they go beyond just checking the source and destination IP's/ports. By being able to validate by the above criteria lets a network administrator lock down access in a granular fashion. Another advantage of a circuit-level gateway is that it can handle UDP (user datagram protocol) traffic because it is able to validate the session by verifying the source IP. This is not always possible when it comes to UDP because there normally isn't any validation with UDP traffic. An attempt to bypass the firewall by IP spoofing becomes much more difficult.

Stateful Inspection

Stateful Inspection, also referred to as dynamic packet filtering, was invented by Check Point Software Technology's in the early 1990's. "Unlike packet filtering based firewalls, stateful inspection firewalls look at the data and track each connection traversing all interfaces of the firewall and make sure they are valid," [15].

Instead of letting packets through the firewall just because they have the right IP addresses and ports, stateful inspection puts the packets into the "context" of what's happening on the network. For example, a firewall sits, waiting to receive packets, and it sees a DNS (Domain Name System) request originating from a system on the internal network and destined for an external DNS. The firewall records this in its state table. When the firewall later receives an incoming DNS response, it checks it against the outgoing ones it's recorded in the state table. The firewall then permits it through only if the response matches a known request. "What it's effectively doing is putting the packets in "context", or monitoring the "state" of each interaction," [1].

What this means is stateful inspection firewalls have the ability to base control decisions (i.e. accept, deny, authenticate, log attempts) based on previous communications with external hosts. Stateful inspection firewalls are more intelligent in decision making than a packet filtering firewall.

4. Intrusion Detection Systems

4.1 What is Intrusion Detection?

An IDS (intrusion detection system) uses sensors placed within an infrastructure

to examine network activity and identifies suspicious patterns that may indicate that someone could be attempting to break in or compromise a network or computer [14]. An IDS examines the network traffic and then compares the traffic to signatures that are kept in a large database. An IDS can only check for known attacks or vulnerabilities. The best way to describe an intrusion detection system is that it's similar to a burglar alarm. In the case of a possible intrusion it will send some type of warning or alert to an organization's incident response team.

4.2 Types of Intrusion Detection Systems

There are several ways to categorize intrusion detection systems:

- *Host Based Intrusion Detections Systems (HIDS)* – IDS systems that operate on a host to detect malicious activity on that host.

- *Network Based Intrusion Detections Systems (NIDS)* – IDS systems that operate on network data flaws.

- *Misuse Detection* – IDS analyzes the information it gathers and correlates it to signatures that are kept in a database. If the signatures are not in the database then the IDS is unable to trigger an alert. In this method the IDS is only as good as the database.

- *Anomaly Detection* – A system administrator defines a baseline of the "typical" network traffic load. Then an anomaly detector monitors the network to compare its current state to the baseline and it looks for any anomalies, [14].

4.3 IDS Sensor placement

A large organization with multiple network segments and that use a large amount of internet based services should deploy multiple network sensors throughout its infrastructure. For a small shop with a basic network design one or two network sensors could be sufficient. Deploying more sensors within an organization produces better results.

"Typically, IDS sensors are often paired with firewalls, near internet access points," [9]. Ideally you would want to have a sensor on the internal and external side of the filtering device. This way the traffic on the external side of the firewall can be monitoring for suspicious activity trying to come through an organizations firewall. The purpose of the sensor on the internal side of the firewall is to identify suspicious activity that actually made it through the firewall.

5.0 Threat and Vulnerability Assessment

Every network is vulnerable. The real question is where. In today's world, new threats and vulnerabilities are discovered at a rapid rate and they are being exploited in new ways. It is very difficult to stay on top of security threats to a network when technology is continually changing. This is where a threat and vulnerability assessment can be very beneficial to an organization.

5.1 What is Threat and Vulnerability?

- *Threat* – *A*ny activity that represents possible danger to an organization's information. An example would be attackers routinely on the internet looking for open ports.

- *Vulnerability* – A weakness in an organizations security that could be exploited by a threat. For example, a network administrator misconfigured a firewall and left a port open.

5.2 What is a Threat and Vulnerability Assessment?

A threat and vulnerability assessment (TVA) is when an organization scans its firewalls, web servers, mail servers, and all other internet-facing devices [12]. A threat and vulnerability assessment paints a picture for an organization as to where security breaches are located within their enterprise. This is a very powerful tool and most threat and vulnerability utilities will show open ports, number of security weaknesses, suggested fixes, patch links, and workaround tips.

The primary goal of a TVA is to provide information necessary for an organizations management to understand levels of risk associated with various activities. In other words, TVA's are audits performed to ensure security controls are operative and adequate.

5.3 Why perform a Threat and Vulnerability Assessment?

Today's threats can prevent an organization from doing business with it's customers by causing a significant amount of downtime. According to the CSI/FBI 2003 Computer Crime and Security Survey, "the total amount of annual losses caused by computer crime for the 251 organizations that responded was $201, 797,340. According to the same survey, the largest loss came from theft of proprietary information," [11].

An organization does not want to wait to find that a hacker has been walking through their enterprise at free will. At the point it is too late. Who knows how long the hacker has had access to the network and what data was compromised? It is critical for an organization to be proactive and finds it's vulnerabilities before a hacker discovers the vulnerabilities and exploits them. It

is beneficial for an organization to scan its own network from the outside to see the same vulnerabilities a hacker sees.

5.4 Threat and Vulnerability Assessment Tools

Online network scanners are current and up to date because they are updated on the backend. There are several scanning tools available on the internet.

Vender Name	Product Name	Vendor Web Site
eEye	Retina	http://www.eeye.com/
Foundstone	FS1000	http://www.foundstone.com/
Harris	STAT	http://www.harris.com/
Nessus	Nessus	http://www.nessus.com/
nCircle	IP360	http://www.ncircle.com/
ISS	Internet Scanner	http://www.iss.net/
Qualys	QualysGuard	http://www.qualys.com/

[11]

6.0 Patch Management

The downtime and expense that an exploited vulnerability can cause is un-measurable. Over the past few years it is obvious that patch management is a growing concern in network security. It used to be that once you installed an operating system or software it rarely needed updated. Those days are long gone. With the increase of worms and malicious code targeting known vulnerabilities and un-patched systems, patch management has become a high priority in organizations.

6.1 What is Patch Management?

"A patch is a bug fix, security fix, or an upgrade to an operating system," [5]. Patch management is the process of identifying and deploying patches throughout an organization in order to eliminate security vulnerabilities. Once a vulnerability is identified, a fix or patch is developed to fix the vulnerability.

Patch management is a difficult process to manage no matter the size of the organization. One of the biggest obstacles is managing updates for all the different kinds of applications and operating systems, and it gets more complex when telecommuters and remote offices are involved.

6.2 The Patch Management Process

"An organization needs to apoint a person or team that is responsible for

keeping up to date on newly released patches and security issues that affect systems and applications deployed in its environment," [2].

An up-to-date asset management system is extremely beneficial when it comes to patch management. The asset management system will help the patch management team identify systems that are vulnerable and require remediation. Furthermore, if there is not a centralized asset management system how can an organization truly determine if they are vulnerable?

Typically, organizations have relationships with vendors of their operating systems, applications, and network devices. These relationships help with the fast delivery of security patches and other security issues. Many organizations choose to have monthly or bi-weekly meetings with the vendors or sign up for mailing lists to keep them updated on patches and other security issues.

A key step in the patch management process is to test the patch in a test environment that mirrors the production environment as closely as possible. If an organization rolls out a patch without prior testing of it, it can create a disaster enterprise wide. The patch should be tested on all platforms and on critical applications. The closer the test environment is to production-like systems, the smoother the patch rollout process should be.

Once the patch has been thoroughly tested it is ready for deployment. Organizations can deploy patches manually or by using an automated tool. One of the main questions organizations ask is whether they should buy or build tools to implement a patch. This depends on the complexity of the organization's infrastructure. "Historically, many organizations have created custom solutions using scripting languages combined with available platform tools to distribute and apply patches," [2].

Patch management is a never ending process. At the rate in which vulnerabilities are being identified, it is crucial for an organization to continue monitoring networks for vulnerabilities.

7.0 Conclusion

As computer crimes are more evident in our society there is no doubt that companies are having a tougher time keeping their networks secure. No network is 100% secure from being attacked or exploited. But, there are proactive measures an organization can put in place to mitigate the risk of being compromised.

Any one of the security topics I have discussed could have very well been a security research topic by itself. However, it takes more than any ONE technology to secure an enterprise's infrastructure. This paper gave an overview of technologies that can be used to "layer" security technology within

and organization. A layered approach is also known as "Defense in Depth". In essence, Defense in Depth is a security practice in which there are layers of defense and if the first layer is penetrated by an attacker then the attacker has to then make it through multiple layers of security before actually getting into an enterprise.

This paper is to introduce network security concepts and terminology to an audience of network analysts and network administrators that are entering the network security arena.

References

[1] Cartwright, David. "Statful vs deep inspection firewalls". 2004. URL: http://www.techworld.com/security/features/index.cfm?featureid=268&Page=1&pagePos=9 (January 2, 2005)

[2] Chan, Jason. "Essentials to Patch Management Policy and Practice". 2004. URL: http://www.patchmanagement.org/pmessentials.asp (December 27, 2004)

[3] Cisco Corp. "Network Security Policy: Best Practices White Paper". URL: http://www.cisco.com/warp/public/126/secpol.html (January 2, 2005)

[4] Danchev, Dancho. "Building and Implementing a Successful Information Security Policy". 2003. URL:http://secinf.net/policy_and_standards/Building_Implementing_Security_Policy1228.html (January 2, 2005)

[5] Guinan, Derran. "But I have a firewall, my network's secure!" SANS Institute, 2004. URL:http://www.giac.org/practical/GSEC/Derran_Guinan_GSEC.pdf

[6] Hall, Eric. "Internet Firewall Essentials". October 2002. URL: http://secinf.net/firewalls_and_VPN/Internet_Firewall_Essentials.html (December 24, 2004)

[7] Harris, Shon. All In One CISSP Certification. California: The McGraw-Hill Companies, 2003.

[8] Loop, John D. "Why you should always wash your hands after leaving the restroom". April 2004. URL: http://www.pccitizen.com/threewayhadnshake.htm (January 2, 2005)

[9] Northcutt, Stephen, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey. Inside Network Perimeter Security. Indiana: New Riders Publishing, 2003.

[10] SANS Institute. Track 1 – Defense in Depth. Volume 1.2. SANS Press, January 2004.

[11] Taylor, Laura. "Vulnerabilities and Threats 101". 2004. URL: http://www.intranetjournal.com/articles/200404/ij_04_21_04a.html (December 27, 2004)

[12] Threat Focus Corp. "Vulnerability Audits". URL: http://www.threatfocus.com/vulnerability_audits.php (December 27, 2004)

[13] Webpedia. "What is a firewall? A word definition from the Webpedia Dictionary". URL: http://www.webpedia.com/TERM/f/firewall.html (December 27, 2004)

[14] Webpedia. "What is Intrusion Detection System? A word definition from the Webpedia Dictionary". URL: http://www.webpedia.com/TERM/i/intrusion_detection_system.html (December 27, 2004)

[15] Webpedia. "What is Stateful Inspection? A word definition from Webpedia Dictionary". URL: http://www.webpedia.com/TERM/S/stateful_inspection.html (December 27, 2004)