

**Firewalls**

**Justin Falk**

**MIS542**

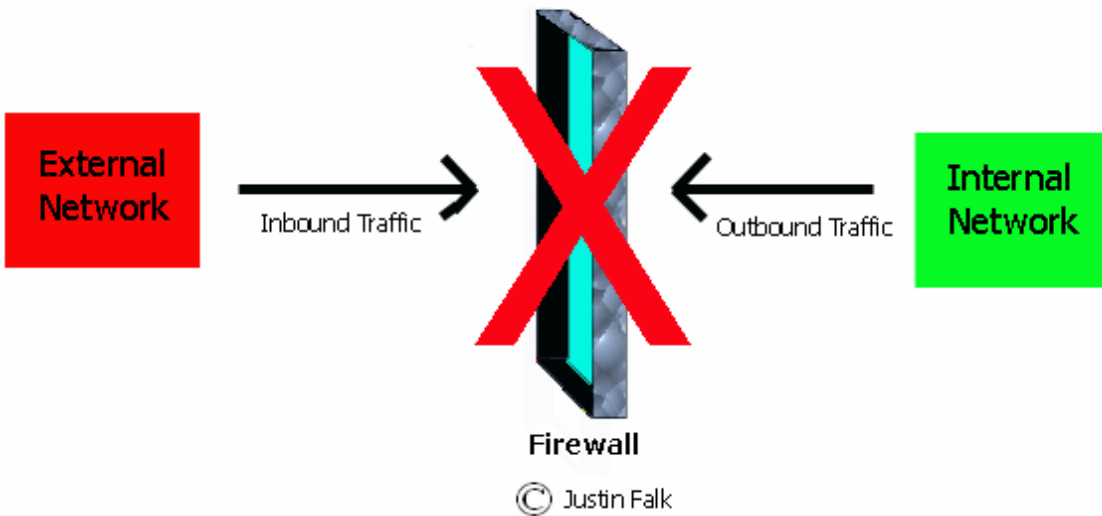
**Robert Morris College**

## Introduction

Concern for security is significantly increasing in today's technical world. Individual and business operations are commonly performed via insecure computer networks. Because of this constant exposure there is also an ever increasing need to protect a computer or internal network from attackers. The internal network and its assets are too valuable to jeopardize. The solution for this problem is called a firewall.

## Definition

A firewall is a leverage-increasing device from a network management point of view (Ranum 9). In comparison, it is similar to a barricade put up by law enforcement. The policing authority (network management) will limit vehicles (network traffic) through the barricade based on certain criteria (policy.) Another comparison is a screen containing multiple holes for many different shapes. Only if the shapes match certain holes in the screen will they be able to pass through it. The shapes are information in the form of network traffic passing through the firewall from one network to another. Sheldon defined a firewall as "a barrier that controls the flow of traffic between networks" (1). Vicomsoft describes a firewall as protecting "networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service" (2). Regardless of the definition or purpose of a firewall, it can be considered a great tool for securing an information system.



**Figure 1** – A firewall preventing all traffic

### **The Need for a Firewall**

With communications, access to the internet, and networking amongst organizations now at an all time high, securing the sensitive data inside a network has become undoubtedly imperative. Times now call for immediate access to extranets and the internet for necessary business operations. Even individuals can be exposed when configuring a private system to connect to an outside environment. If sensitive information is exposed or systems vandalized, losses can be devastating both fiscally and physically. Protecting a secure connection route for necessary business functions for both employees and users is critical. Denial of service attacks will cause loss of these critical functions. Prevention of such damages can easily be stopped or at least mitigated by the implementation of a firewall. Management within organizations or business should easily understand its importance and justify costs or time involved. As

the world continues its upward trend of internet connectivity firewalls will continue to be a key point in securing one's assets.

### **Firewall Functionality**

A firewall is placed between two or more networks to allow or disallow information to pass through. It can be thought of as a gatekeeper not only protecting what can come in, but also what can be sent out. The firewall can prohibit the information from passing through the network in forms of filters. It can also manage access control to networked resources, log traffic or unauthorized log in attempts, and set off alarms. Some types of firewalls can reroute traffic through a proxy gateway. This would be like a traffic cop rerouting automotive traffic on a different route to arrive at its destination. In summary it protects the trusted networks located behind the firewall from the untrusted networks on the other side of the firewall.

### **Who Should have a Firewall?**

A firewall is needed by any person that is connected to an untrusted network. Even an individual should strongly consider using a firewall. Identity theft or passive attacks such as eavesdropping may warrant individual implementation. Also vandalism may occur in which software is destroyed or sabotaged. Any person in charge of managing security, such as an IT officer or network administrator, is responsible for protecting internal systems and networks. Today a firewall is considered almost essential, and even a basic one is built in to the Windows XP operating system.

## **Benefits of a Firewall**

Using a firewall can yield many benefits. Connecting to the internet is essential for today's level of worldly interaction. The connection is an incredibly valuable resource that gives more advantages than disadvantages. A firewall eliminates and reduces the risks and disadvantages of operating at such a level. In some cases such exposure of dealing with untrusted networks may not be worth the potential negative outcomes. In these situations a firewall may be the only way to allow such connectivity. Aggressive attacks called hostile intrusions may be prevented. Firewalls allow for a selectivity of information, an essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what (Vicomsoft 11). Also firewalls can ensure that sensitive data is not exposed or exported to those beyond the trusted network which may use it for detrimental purposes. The cost of using a firewall should far outweigh the negatives. Just having peace of mind that one is relatively secure may be benefit enough.

## **How Does a Firewall Work?**

Ideally a firewall would block out 100% of all traffic passing through which could potentially cause harm. However, this is not capable as it would severely hinder the operation of the network connection. Firewalls work by determining whether to permit or deny the traffic passing it into the network or next level of security protocol. Outbound traffic may be denied trying to leave the network also. Firewalls work by determining which traffic to permit and which to deny. Certain firewalls use simple

methods such as an access list of permissible sources. Others may closely examine destination addresses or type of information being sent.

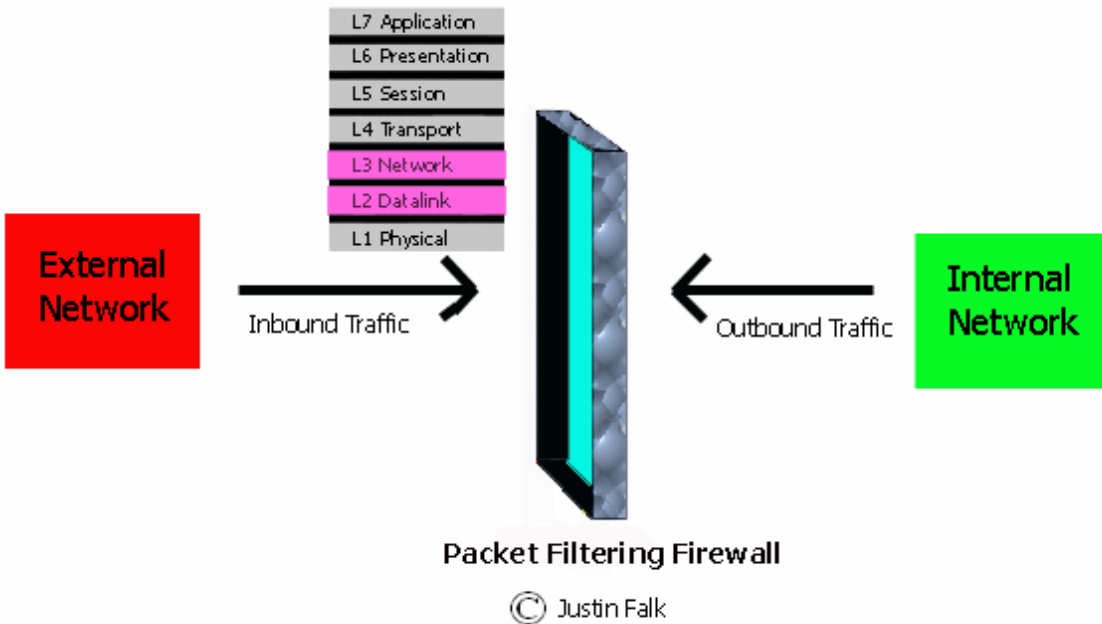
### **Which Type of Firewall to use?**

Determination of firewalls can be based on a multitude of factors. Size of the network, physical layout of the network, type of network traffic, amount of network traffic, needed level of security, access to network resources and applications, and ease of use by users must all be considered. Firewalls should be implemented based on the details of these factors and not based on the way a firewall internally operates. A policy should be implemented to best cover all the factors. Below is a basic summary of the many different types of firewalls available.

#### ***Packet Filtering***

Packet filtering firewalls operate at level 2 and level 3 in the Open Systems Interconnection (OSI) Reference Model, meaning it is mainly concerned with the inspection of packets in the Datalink and Network layer rather than other layers. Packet firewalls are one of the most basic types and are usually found in conjunction with routing devices. The source address, destination address, and the type of traffic are examined. Packet filtering ability is often a basic feature of a router. They sometimes can be referred to as a screening router. If packet filtering is not part of a router it is usually on a computer which uses two network interface cards called a dual-home gateway. In this instance all direct forwarding is turned off. The gateway must relay the data to the other network card for it to arrive at its destination. Packet filters can also be

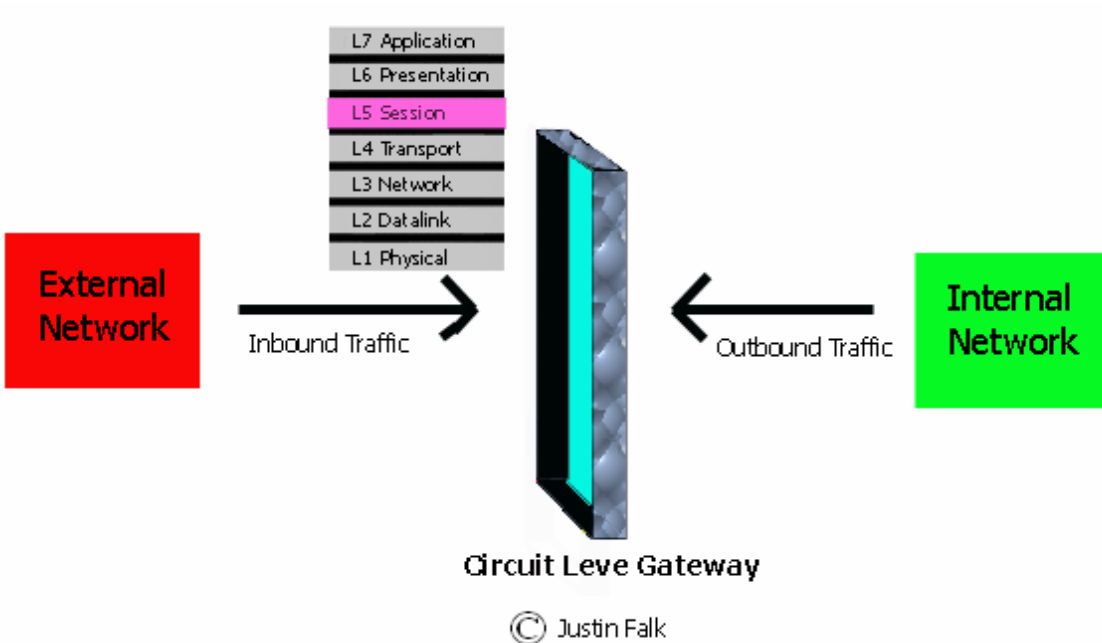
used to block traffic by turning off ports. The advantage of this simple type of firewall is its low cost and insignificant influence on network performance.



**Figure 2** – A firewall filtering packets

### ***Circuit Level Gateway***

Circuit level gateways perform their inspection at level 5 of the OSI model (Session layer). They check to see if session levels are indeed genuine (coming from its original source) during a connection. They are a low level form of a true proxy. Any packets permitted to be exported through the through the gateway will be rebuilt with new source information in its header causing its appearance to seem like it was the original source. This is very useful in hiding IP addresses and information about the internal network to outsiders, however it may cause the network to run slow. This greatly reduces crackers or eavesdroppers from targeting the network. Circuit level gateways are also rather inexpensive.

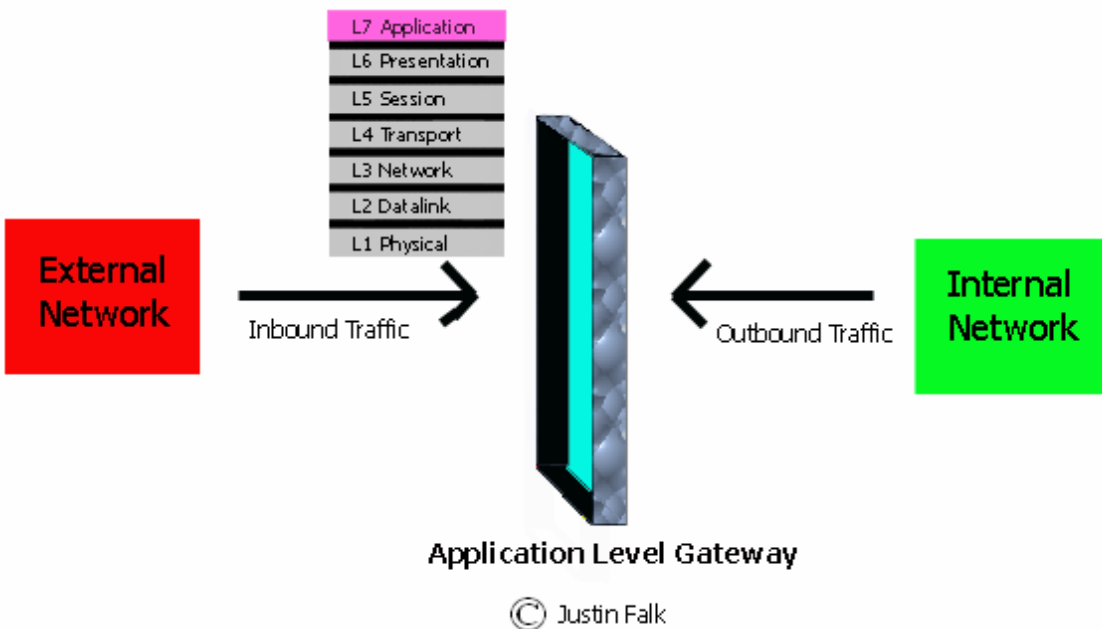


**Figure 3** - A firewall filtering TCP/IP sessions

### ***Application Level Gateway***

Application level gateways perform their inspection at level 7 of the OSI model (Application layer). They are slightly more sophisticated than lower level filters to allow for further determination of traffic. They are most often referred to as proxies. Proxies serve as an in between inspection point. This would be similar to adding a distributor in the chain of logistics (middleman) from a manufacturer to end consumer perspective. Traffic going through the gateway is only permitted if the proxy allows that category of service. Because of this, internal network information is hidden just like circuit level gateways. An FTP gateway, for example, will only allow FTP commands to pass through. An HTTP command would be denied in this scenario. Furthermore, application gateways often have the ability to filter specific requests within the

application and log user activity. A specific gateway computer can be used as a proxy, or inexpensive software may be configured. An unfortunate disadvantage of a proxy configuration is that each client must be individually configured with the proxy information. This can be cumbersome and requires more knowledge than previous types of firewalls. Users can tell they are accessing information through a proxy, and network performance is often slowed.

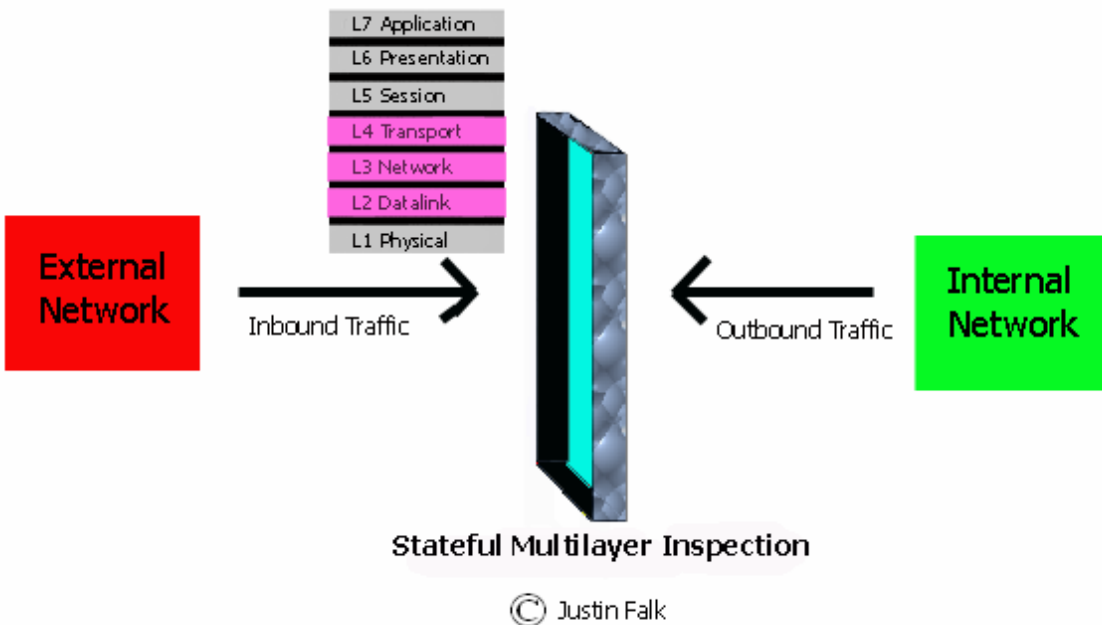


**Figure 4** – A firewall filtering by application

### ***Stateful Multilayer Inspection***

For higher security purposes stateful multilayer inspection firewalls are a good choice. They are called this because they have the ability to filter traffic amongst many layers in the OSI model. This reduces having to create multiple proxies; one proxy for each of the many functions needed for the network. Besides having this ability, SMLIs do not show the changing in the flow of traffic like a proxy does. This is referred to as

transparency (Vicomsoft 8). Unfortunately, this does expose the valuable network information that a true proxy would hide. SMLIs can be rather costly, and so can the cost be to employ someone with the knowledge to configure and maintain one. If configured properly this is a well rounded system that can be tuned to have little impact on network performance. This is done by keeping all ports closed and only opening them when requested. Unfortunately because the SMLI operates at so many levels it often contains many security vulnerabilities to the network.



**Figure 5** - A firewall filtering across many layers

### ***Bastion Host***

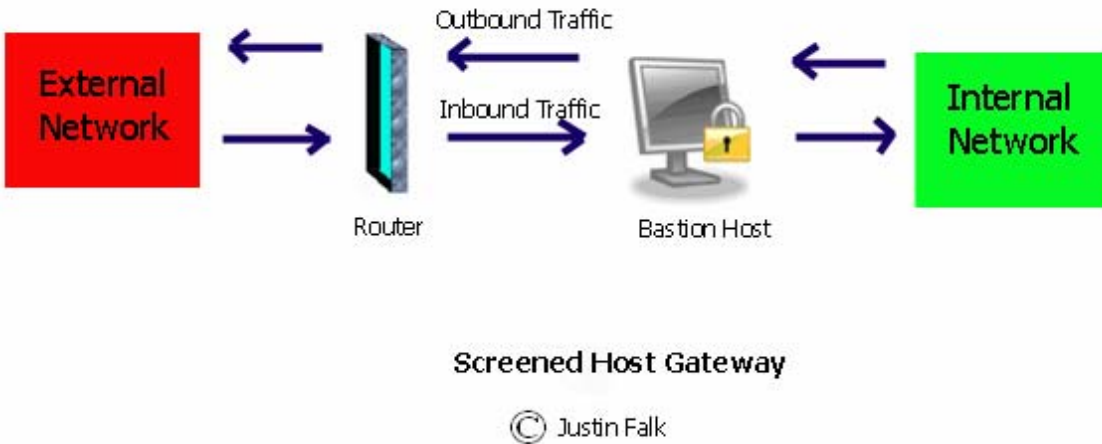
Bastion Hosts are any key critical security points in the network. They are not a specific type of firewall. They are points or computers that frequently have security measures on them to protect the integrity of the network. They can have one or numerous types of firewalls. They are called bastion hosts because they are the

stronghold for protecting the network. They are frequently monitored and used by security administrators within the system. A router that is left virtually unmonitored with packet filtering firewall would not be an example of a bastion host. However, a dual homed gateway in which a network administrator frequently checks logs at is a prime example of a bastion host.

## **Configurations**

### ***Screened Host Gateway***

A screened host gateway configuration uses both a screening router and a bastion host. Internet traffic is first filtered through the screening router, which is placed in front of the bastion host, preventing all outside access from directly interacting with the bastion host. The internal networks only interaction to the external world is through the bastion host. This is seen as an additional level of security by preventing most traffic from direct interaction with the key strong point (bastion host) protecting the network. This is rather easy to setup and provides an easy way to step up security.

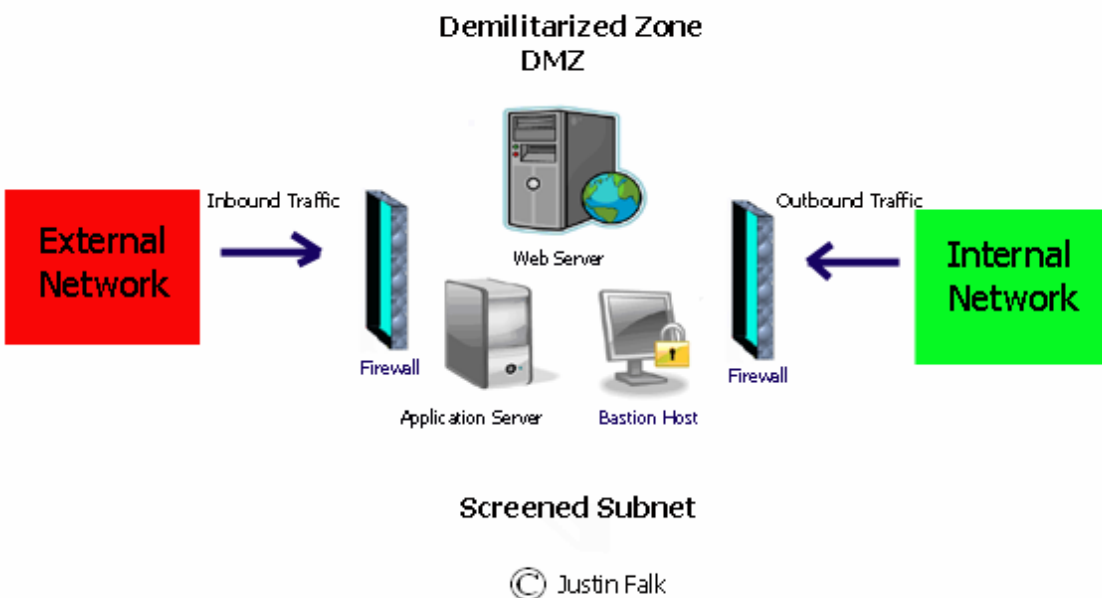


**Figure 6** – Configuration for screened host gateway

### ***Screened Subnet***

A screened subnet configuration consists of security devices to protect it from the internet, hence the name screened, and a subnet which contains multiple gateways or filtering devices. An additional firewall is behind the subnet to further protect the internal network. External networks such as the internet can interact with the subnet. The private internal network can also interact with the subnet, however there is no direct traffic allowed to pass across the subnet from the internal network to an external network, and vice versa. The subnet can consist of multiple screening routers and bastion hosts. This subnet can consist of web servers, database servers, etc., and can often be referred to as a Demilitarized Zone (DMZ). This is the defined space between the firewalls. It can be a complicated setup but if implemented will be very difficult for any attacker to gain access, and especially difficult to do it without being detected. The

attacker would have to gain access to the devices protecting the subnet, the internal network, and then the subnet. All three areas would then have to be reconfigured to route traffic directly across the subnet which would probably set off warnings, and any administrator would also notice the configuration changes very quickly.



**Figure 7** – Configuration for a screened subnet

### ***Hybrid Gateways***

Hybrid gateways are recently becoming more popular. With recent advances in technology many forms of firewalls are often combined into one gateway or router system. These gateways can monitor many protocols and have all the advantages of SMLIs. Packet filtering software is usually combined with proxy abilities and vice versa. There is no standard in a hybrid gateway. A very good advantage of this proprietary

configuration is it often makes it very difficult for attackers to exploit the network because they are not quite sure how it is configured.

### **Implementation & Policy**

Creating a firewall policy is a key component to management security. Many decisions need to be made for the firewall to be most successful in performing its desired job. Although there is no best implementation strategy, many questions should be answered to best suit an individual's or organization's needs. No particular approach is always better due to differing requirements requiring different operations of the firewall to protect the network.

A good starting approach is to block absolutely everything. Nothing is allowed through the firewall both out and in the network. Assuming no clients have an individual dial-up connection, by using this approach only the necessary vulnerabilities will be created to permit traffic through the security firewall. Access will only be given to non-trivial services. The following set of five decisions should definitely be considered in regards to implementation.

The first decision should be to determine which and what is permitted into the network, called an inbound access policy. Will traffic be allowed from which the source is not an internal IP? What external network traffic packets should be allowed through? What sites or addresses are trusted and can be added to a list of trusted sources? What services or resources will be allowed to be accessed from external sources?

What protocols will be needed? These are a few example questions in determining rulesets to design an inbound access policy.

The second decision should be to determine which and what is permitted out of the network, called an outbound access policy. Which destinations are needed? Which services and users will be allowed to distribute information out of the network? Which sites are needed for key operations? These are a few example questions in determining rulesets to design an external outbound access policy.

The third decision should be to determine the sensitivity of the organization. How important is the data contained on the network? Is this information classified? How much knowledge should outsiders be able to see about the network? What are the primary threats to the organization? The more sensitive or classified an organization or its operations the further sophisticated its firewall implementation should become to ensure proper security.

Along with the sensitivity of an organization a proper risk analysis should be performed. If key services or components are exposed what will be the consequences? What would be the repercussions of outsiders finding data or valuable knowledge of operations? How difficult will it be to detect both successful and unsuccessful intrusion attempts? What will happen and should be done upon discovery of the attempts? These are a few examples of questions corresponding risk analysis to sensitivity.

The fourth set of decisions should be in regards real world constraints. How large is the network? How many physical sites does it encompass? How many gateways, hosts, routers, (often referred to as zones of risk) will be exposed? How much financial resources are available to the security department? Is this worth the time or money spent to implement such a system? And lastly, but not least important, how will this effect network performance and ease of use?

The fifth set of decisions should be in regards to performing the task in house or outsourcing it? Is it too complex of an operation to handle? Is there an existing software suite or hardware equipment available? Should it be created in-house or simply purchased outright? These are the imperative decisions in the last step before full implementation.

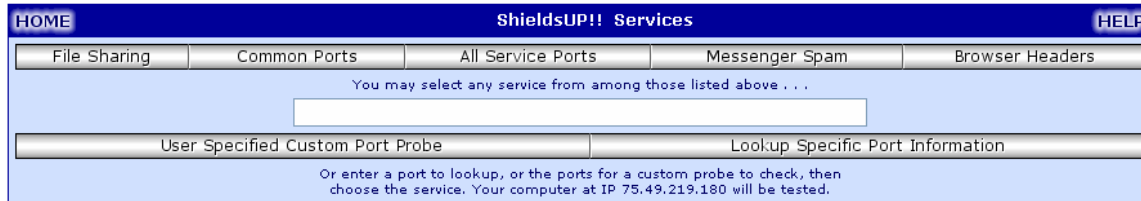
### **Placement**

The environment should determine how many firewalls are needed and where to place them. There are a few key things to keep in mind to best secure the network regarding firewall and server placement. Any external server should obviously be protected at minimum with a router or packet filter. If possible, servers that need external access to vendors or others should not be placed within the internally protected network. Just the opposite of the previous rule is any server only being accessed internally should be placed behind internal firewalls. There is no reason to expose them in a DMZ or subnet environment. If possible, do not allow servers to interact with anything more on the network than what is necessary. For example, the web server

does not need to interact with the email server. In some cases the web server may need to interact with the database server for web applications. But if not, any interaction between the two should be disabled. This will limit exposure to a potential attacker as not to jeopardize the rest of the network if the attacker is successful in gaining access to one entity within the system.

### **Testing & Review**

An established procedure should be created for testing the firewall policy. A designated time period should be given to routinely test the effectiveness of the firewall configuration. Firewalls may also be frequently monitored and logs verified to ensure all behavior is only the intended kind. Diagrams or configuration schemes may be reviewed to check the physical placement and layout of the network. Any written documents will help with current and future testing procedures. Approved activities may be checked to ensure they are still permitted, and prohibited activities still remain denied. Some testing can individually be tested in regards to simple tasks. Also there are software tools that can either probe or detect areas that can expose the network to potential threats. A free tool can be used by Gibson Research Corporation available at <http://www.grc.com> called Shields Up. Many other tools exist like this. Here are a few screenshots to give an example of how these tools can easily look at a lot of information about the network to help you identify weaknesses very quickly.



**Figure 8** – GRC ShieldsUp screenshot (GRC)

Shields UP! is checking **YOUR** computer's Internet connection security . . . currently located at IP:

**75.49.219.180**

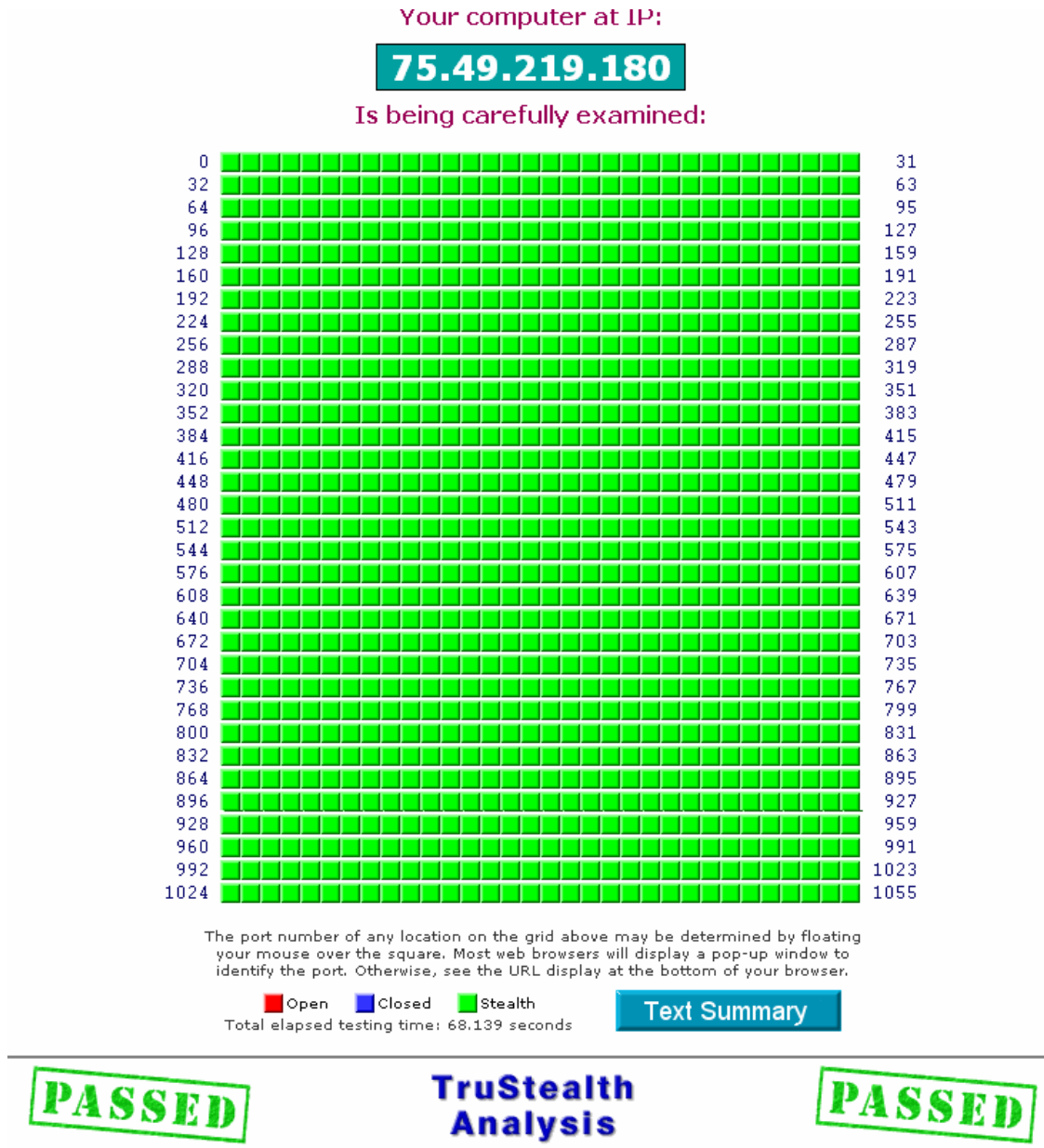
Please Stand By. . .

- 1** **Attempting connection to your computer. . .**  
**Shields UP!** is now attempting to contact the **Hidden Internet Server** within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an **Internet Server** with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!
- **Your Internet port 139 does not appear to exist!**  
**One or more ports on this system are operating in FULL STEALTH MODE!** Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. **But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND** (that's very cool!) which represents advanced computer and port stealthing capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attack and intrusion.
- **Unable to connect with NetBIOS to your computer.**  
All attempts to get **any** information from your computer have **FAILED**. (This is **very** uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be **VERY SECURE** since it is **NOT exposing ANY** of its internal NetBIOS networking protocol over the Internet.

**Figure 9** – GRC Internet connection check screenshot (GRC)



**Figure 10** – GRC TruStealth common open port analysis screenshot (GRC)



**Figure 11** – GRC All Port open/closed/stealth screenshot (GRC)

### Summary

In conclusion, firewalls are devices that help protect an internal network from intruders and attackers. The need for a firewall will continue to grow as demand for extra security increases. There are many security benefits to a firewall depending

on the functionality needed. Many different types of firewalls are available, and many are being combined together to provide extra capabilities to meet the multiple demands of a security administrator. Implementing a firewall is determined by a multitude of decisions that need to be made by security authorities. Configuration of the firewall both physically and through the software is very critical to its security effectiveness and should match implementation policy. After a firewall has been placed it is important to test its effectiveness routinely to be sure it is operating effectively.

## Works Cited

GRC | Gibson Research Corporation Homepage. January 21, 2007. Spinrite 6.

<<http://www.grc.com>>

Intoto Inc. Firewall Whitepaper - Enabling Security Infrastructure. 2002. Santa Clara  
California

Ranum, J. M. Thinking About Firewalls, Trusted Information Systems, Inc., Glenwood  
Maryland

Sheldon, T. WindowsSecurity. General Firewall White Paper. 2002. January 11, 2007.

<[http://www.windowsecurity.com/whitepapers/General\\_Firewall\\_White\\_Paper.html](http://www.windowsecurity.com/whitepapers/General_Firewall_White_Paper.html)>

Vicomsoft. KnowledgeShare – Producing for Productivity Firewall Q&A. 2006. January

11, 2007. <<http://www.vicomsoft.com/knowledge/reference/firewalls1.html>>

Wack J., Cutler, K., Pole J. National Institute of Standards and Technology –

Technology Administration U.S. Department of Commerce. 2006. Firewall

Whitepaper – Enabling Security Infrastructure. Gaithersburg, Maryland