Global Information Assurance Certification Paper

Controlling Firewall Port Openings

GSEC Practical Assignment v1.4b (Option 1)

By David Fore

July 11, 2003

Abstract

The following paper discusses the decision making process that can be used when deciding which ports to open on a corporate firewall. An analyst with the responsibility of securing the corporate network must weigh the risk to their network with Internet functionality. This applies when deciding which ports can safely and effectively be opened. Some of the processes, points for thought, as well as some of the tools needed to assist an analyst with these decisions will be discussed. The goal is to put forth logical order and standard questions that will help maintain consistency with opening ports and ensuring accountability during a review or audit.

I - Introduction

My SANS Track 1 instructor told our class that if you have more than 10-30 rules on your firewall, then you probably have too many. Great, I have might have 10 times that number! Does that mean I am vulnerable? Will my internal network be compromised? Is my DMZ at risk? Not necessarily. If an organization has written procedures based on set criterion, management approval of the procedure, port openings that follow the procedure, and the open firewall ports are audited on a set schedule, then some firewall ports can be opened. This will provide users with their required business functionality, while continuing to protect the company's network from malicious attacks.

II - Why do we need procedures?

Deciding which ports to allow through a corporate firewall is a daunting task. There is a constant battle between the business unit and the IT security department over functionality verses security. One usually rules over the other depending on the organization. There is even a battle among IT security professionals when deciding security related issues. For example, there are security analysts that tell you not to open any ports, except port 80 into your network, and there are some analysts that only allow users to access the Internet via port 80. There are also analysts that tell you that certain ports are absolutely taboo. A network analyst must know what ports are open through the corporate network. In fact, the Internet Security Task Force (ISTF) listed “unnecessary open ports in firewalls" as one of the most commonly overlooked areas in e-Business (ISTF p.1). So what is a security analyst to do? The short answer is that it depends on your organization and its needs.

It is important for a company to make its own decisions on opening ports. An open port is an avenue for an attacker to gain access to an internal server or network, which enables the attacker to launch other attacks. However, the Internet is filled with valuable information and resources that a company can use

to maximize their effectiveness. In addition, by allowing customers access to their e-Business web site, a business can gain valuable exposure. Therefore, a company must decide what risk level it is willing to accept on their network, in exchange for their business functionality.

An increasing number of companies have implemented e-Business solutions, which require users to access the sites on ports other than standard HTTP or HTTP-s. Web masters have various reasons for designing their web sites with other access requirements. These reasons may include increased security for the application or an application may require the use of a "well-known" port below 1024.

In addition to web site access, companies may require access to servers or network management components from the internal network that require special communication ports. For instance, a network analyst has to decide how updates will be made to the routers in a DMZ environment. This could require an open port for a service such as TFTP. Additionally, NTP may be required in order to synchronize the time on servers. Also, many companies have deployed VPNs throughout their network to allow controlled access from the outside. These also need open ports to work properly.

There can also be multiple network zones deployed across a company network that can consist of an untrusted public DMZ, an isolated DMZ, a management DMZ, and the internal network. Ports opened between each of these zones and the Internet will be different based on the associated risk-reward analysis. Each zone represents its own risk to the internal network and components. It is important that each of these zones is evaluated separately.

Companies must also differentiate between internal users and external users. External users present a potential security problem to the internal corporate networks. Hackers, crackers, and script kiddies are well documented in mainstream media. However, security policies must not overlook the internal users and the dangers they pose. According to ISTF, "up to 70% of security breaches are internal" (ISTF p.1). It may be up for debate whether or not internal users pose as much of a risk to the internal network as external users do. A well-informed security analyst must account for both types of exposures and act accordingly.

Also, with the myriad of application that exist today, it impossible to know exactly how an application interacts with a network or user. It is necessary for the security analyst to understand the interaction and how that can effect their decision to open a firewall port. An analyst can not assume anything about an application because of similarities between other applications.

Finally, it is absolutely imperative that network analysts know what ports are open and in which direction. There are new worms and viruses that propagate at

such an alarming rate, incident response teams do not have enough time to protect their systems before they are infected. Consider the example of the SQL Slammer worm. “The propagation of this malicious code has caused varied levels of network degradation across the Internet and the compromise of vulnerable machines" (CERT p.1). Not only did this worm cause unprecedented disruption across the Internet, it did so with an amazing speed. In fact, CNET reported " last week's SQL Slammer worm infected more than 90 percent of vulnerable computers within 10 minutes, opening a new era of fast-spreading viruses on the Internet, according to a news report" (Broersma p.1). Can your Incident Response team protect your company in less than 10 minutes?

These points must all be taken into account when opening firewall ports. Firewalls and port openings are only a small part of the concept of "defense in depth" for the modern corporate environment. Firewall port openings are only one layer and the only aspect of defense in depth that will be covered in this paper.

III - Start Here - Policies and Initial Rule Sets

A policy is used to set forth guiding principles that will address certain aspects of a company. From a well-worded, approved Perimeter Security Policy (a.k.a. firewall policy) and Internet Acceptable Use Policy, network managers can develop solid procedures that facilitate proper port opening decision-making. SANS identifies perimeter security management policy and an acceptable use policy as key policies for an organization (Guel p.1).

Each policy is a separate entity; however, the Perimeter Security Policy should get drafted first. The Internet Acceptable Use Policy should be an extension to the Perimeter Security Policy.

A Perimeter Security Policy should include information such as:

- How access is authorized and what groups need access (includes access to and from the Internet)
- How and when access is reviewed
- How and where the firewall configuration is stored and accessed
- How and when the firewall configuration is backed up
- When the firewall configuration is reviewed or audited
- Problem and change management procedures

The above bullets point out some elements that need to be in a Perimeter Security Policy. The key objective is to "set appropriate behavior and set the stage for what tools and procedures are needed” (Guel p.1).

The Internet Acceptable Use Policy is more detailed than a general Acceptable Use Policy. The Acceptable Use Policy would cover all aspects of a company's

computing resources. Some companies opt to create a separate Internet Acceptable Use Policy so they can address key differences with the resources and to remain evergreen with the rapid changes in Internet technology.

Some points that an Internet Acceptable Use Policy may contain are as follows:

- Who, internally may access resources on the Internet
- Who, externally, may access what resources on your network
- Any authentication requirements for access to/from the Internet
- What business justification must exist to use the Internet
- Any restrictions for web browsing
- Ramifications if the policy is not followed.

The above points set the outline for who can access resources as they pertain to the Internet. The key objective is to set expectations as to how the Internet is used as a company resource.

The above references to policy are by no means an exhaustive conversation to network security, but instead a quick introduction to a step necessary before opening ports on a firewall. It is important that the policy is inline with existing business plans. Allen states " Your organization's networked systems security policy should ensure that the firewall system installation/deployment plan and schedule are consistent with your site infrastructure business plan and schedule of infrastructure upgrades" (Allen p.172). These policies are part of a comprehensive set of policies that address all aspects of computing resources within a company. They are also the starting point to start a discussion on procedures. Management approval is perhaps the most important aspect of a company policy, because without approval, the policy can not be enforced. There are multiple resources on the Internet to help an analyst develop policies. Web sites such as: sans.org and nist.gov are excellent resources for policies.

Once the company's network policy is set, then a firewall ruleset must be implemented based on the policy. The policy may state that everything is denied, except that which is explicitly allowed. Alternatively some traffic may be allowed globally (e.g., DNS access or external Internet access), but everything else is denied, unless explicitly allowed. The policy may allow even more access to the Internet. However, my opinion is that a policy should be very restrictive, but flexible enough to allow business justified access.

> " As a general rule, any protocol and traffic that is not necessary, i.e., not used or needed by the organization and/or denied by policy, should be blocked via use of a boundary router and packet filtering technology. This will result in reduced risk of attack and will create a network environment that has less traffic and is thus easier to monitor" (Wack, et all, p.69).

The above quote from NIST (Computer Security Resource Center) allows for the flexibility necessary to restrict access and protect Internet networks while allowing for increased accessibility if necessary.

In addition to a general access statement, such as deny all unless explicitly allowed, a perimeter policy may include ports which should never be opened. Sometimes there is no way to mitigate the risk associated with a port. Also, there are some ports that require additional consideration before they are opened. Again, the NIST (CSRC) has a great resource that outlines not only firewall policy, but also some familiar ports and their recommended action against these ports. The actions could be restricted with strong authentication or block entirely. (Wack, et all, p.70-71) .

Other considerations with the firewall ruleset include inbound and outbound rules as well as established vs. initiated traffic. These should also be addressed within the firewall policy too.

Finally, there are several web sites available that will provide a network security analyst with services and the ports they use (Ports Database p.1). In addition, there are sites that have a list of ports that well-known malicious code uses(von Braun p.1). These sites are valuable in configuring an initial rule set as well as a valuable tool in determining ports to open in the future.

Once the initial ruleset is established, there must be controls in place to ensure the ruleset does not change without authorization. The firewall policy addresses this with specific information on who is responsible for the firewall and who can access the configuration, as well as who is responsible for configuration review. In addition, to ensure integrity of rules firewall configuration settings should be version controlled and reviewed against a “known good” configuration

All these steps are essential to opening additional ports on a firewall. Without the initial steps, then the procedures to open a firewall port are on an unstable base and leave your network vulnerable to intrusion. If the firewall is compromised, then all other network attached devices are at risk for attack.

IV - Procedure

Now that the company has a firewall and Internet acceptable use policy, as well as the initial firewall rule set, the procedure that allows extra ports to be open can now be written. The goal of the procedure is to protect the internal network based on the guidelines set by these policies. The procedure provides the mechanism an organization needs to make consistent and uniform decisions. These decisions are based on approved criterion as well as providing the user with the information that is expected of them in this process. The procedure must be approved by appropriate management levels as well as communicated to the user and made readily available to both users and the network analysts.

User worksheet

A standard request form is essential for both the user and the group that will process requests to open firewall ports. The form must be easily assessable to the user with a set of directions on how to fill out the necessary information. Many times a DMZ project will need ports open between the DMZ and the backend network. The project analyst will most often need to work with the firewall group to understand the requirements of the DMZ software and ports that will need to be opened.

This standard document should be tailored to an individual organization's needs, but some basic information should be included. Such as:

- Submitter Name
- Phone Number
- Organization / Department
- Project Management Approval
- Contact Information (if different from submitter)
- Date Submitted
- Date Needed
- Description of project or access needed
- Details of port opening
    - Application name (i.e., Internet Explorer, Citrix, etc)
    - Service (i.e., TCP, UDP, Echo, etc)
    - Source IP addresses and port(s)
    - Destination IP addresses and port(s)

The use of a standard request form ensures that all necessary information is included and starts the trail that will be used for audit or review purposes. The worksheet is labeled as 'user', but an organization must also determine who can submit these requests.

Single Point of Entry

A single point of entry must be defined for this process. In other words, there is one database where users can send their request for processing. One database provides a central repository that benefits both the user and the implementing organization. The user has a single point of contact for their request. In addition, the organization has a single repository that is used to store the request for further processing as well safe storage when reviews and audits are conducted, or a management report needs to be produced.

Risk Analysis

The most difficult aspect of opening ports is deciding if the risk of opening a port is worth the exposure it might create to the internal network. Representatives from several different departments should make these decisions. A network analyst weighs the benefit as it pertains to the internal network and how the port opening and application interact with the existing infrastructure. A security analyst weighs the risk to existing systems and applications. In addition, the request must comply with existing usage policies. The request must be in compliance with the existing infrastructure. Finally, a single point of contact must be designated for the customer and can be one of the aforementioned analysts or other designated contact within the organization.

It is imperative that the people deciding to open ports has a clear understanding of the system or application and how it relates and interacts with the existing infrastructure. For example, a DMZ application may need to interact with a backend system. However, the DMZ application may be too permissive with requests it receives from the Internet. A good example of this would be an application that is a "pass-through" proxy. In this example, the application receives a request from an outside user. The application would simply pass the request to the backend application. This may be a problem because the application did not check the command string passed by the user. If the command string contained an exploit for the backend system, the backend system may become compromised. Greater controls may be required, such as an "isolation" zone between the DMZ and internal network before allowing the port to be opened. An isolation zone would move some of the processing into the protected zone, while the business logic remains inside the corporate network.

Also, a user may require access to a web site that uses a large amount of bandwidth. The existing network may not be able to accommodate the additional bandwidth unless restricted by source IP address. Both scenarios illustrate the need to understand how the port is going to be used.

Other risk factors must be examined if a user needs access to a web site that requires non-standard ports. The network and security analysts need to understand how the application interacts with the network. There are applications that you may not want to allow in your company's environment. For example, a connection to a Citrix server can allow a 3rd party to gain control over the workstation that is connected to it. In these cases, you can require the 3rd party to control their Citrix server before you allow the port to be opened. In addition, destination IP controls are appropriate to ensure that Citrix ports are only used to access approved sites. Source IP rules can also be used to further control access.

Some other application questions that should be answered include:

1. Is the application a well known and is the protocol published? Citrix is a good example. It is a well known application and the protocol is

understood. This allows analysts to make the port opening decision with confidence.

2. Does the application use a well-known port and is that port assigned to that application by IANA? Applications should not use well-known ports unless the ports have been assigned to the application by IANA. There have been cases were a web site decided to use port 444 for standard SSL communication. Port 443 is used for SSL, not 444. In this case, the 3rd party was trying to the security through obscurity route.
3. Do you have access to the application source code? Many application writers are not known for their security prowess. They seem more interested in functionality. If code is not available, or the 3rd party is unwilling to give great detail about the application, then that should raise a red flag.

Outbound access to web sites can further be controlled by using a proxy server. The proxy server performs several functions. It can control who can access the Internet. Circuit-level proxy servers can control the ports allowed. Also, if all access requests come from the proxy, then the internal network address range can be hidden. The only address seen on the Internet is either the proxy server's network address, or its NAT'ed address.

Not only does the analyst have to understand how the port will be used, but the analyst also has to understand the different protection zones a request will travel. It should be unacceptable to allow externally-initiated sessions into the network unless the request is proxied in some manner. In this case, rules to allow an inbound connection directly to an internal IP address would deny access. However, if an external user has a need for data hosted internally, then a port can be opened from the Internet to the appropriate DMZ application. The DMZ application would then proxy the request to a backend business process. This ensures that the backend is protected because the request is coming from a trusted source, your DMZ application. This of course assumes the DMZ application is sufficiently protected from exploits or compromises.

Externally-initiated sessions that are destined for you internal network, bypassing the DMZ, should never be allowed. Even the ports above 1023 should not allow externally-initiated sessions. A better practice would be to examine the ACK bit and limiting the types of incoming data to only response packets.

The examples demonstrate that applications can affect protection zones in different manners. There are differences between protection zones within a corporate network. In order to make a sound decision, the characteristics of the application and protection zone must be understood and accounted for when reviewing a request.

The risk analysis must also examine the impact to the network. Some impacts are obvious, such as bandwidth requirements. However, the risk analysis must

also ensure that any port opening requests are not going to compromise the network or exploit a gap in rules. For example, NIST has a web site that specifically details what type of network and port traffic should never be allowed (Wack, et all, p. 61).

It is important to understand that once a server is on the network in a DMZ and a port is opened for that server, that server is now fair game on the Internet. Within 24 hours, a new server can be scanned for vulnerabilities and attacked many times! For this reason, there should be no distinction between development / acceptance servers and production servers. They should all have the same risk analysis and controls requirements. Otherwise, the internal network can be compromised.

V - Decision points

Decisions can now be made because the application is understood. The application's interaction with the network is understood. This risk analysis has been completed and appropriate levels of control are in place.

Each organization is different and port opening decisions will differ from company to company. However, there are several generic decision points that are relevant to most organizations.

- Business justified - Has the application and the project been justified by the business unit? This is not a function of the IT department, but rather the business unit. The business unit must ensure that the application or project is consistent with their objectives.
- Risk understood - Is the risk understood by the analysts recommending the port opening? As discussed previously, the application risks and the network risks must be fully understood in order to make a sound decision. In addition, the business unit must understand any residual risks associated with doing business on the Internet.
- Consistent with policies - Is the port opening and the usage consistent with existing policies? If the not, then the decision must be made whether to amend the policy or not recommend the port opening.
- Controls in place - Are all the necessary and pre-set controls in place? Each company should have their own set of standard controls. Production servers and acceptance/development servers are treating the same when they are in a DMZ.
- Any extra controls or requirements - Did the review of the port opening request reveal a need for additional controls or special requirements? If so, are they in place?
- Project is ready - This is a joint decision between the business unit and the IT department. Stakeholders from each department should review the project and decide if the project is at a point that ports can be opened safely.

- Penetration test - Has a penetration test been performed against the application and have the results been reviewed.

These decision points assist an organization in the decision-making process. Each organization should tailor these to fit their environment and culture. A consistent approach to decision making is a valuable tool to a stable computing environment.

VI - Approvals

A clear approval chain needs to be established for the port opening procedure. Again, organizational needs are different, but approvals are always necessary. Some organizations are comfortable with allowing the technical reviewers (network analyst and security analyst) to review and approve a port opening request. Other organizations may require a higher level of approval. The approval process must be specified before the port opening procedure is put into effect.

The approval trail is important to ensure accountability and improve documentation for an audit or review. During a review of open ports or an audit, the approval trail documents that the appropriate personnel have review and approved a security request.

VII - Stewardship

Stewardship is an important aspect to this procedure. It not only allows an organization to ensure they are in compliance with policies, it also ensures that procedures are followed. Both are import in an organization to ensure its business viability.

Audits

Open ports must be reviewed. As stated earlier, open ports are a gateway for attackers into a corporate network. Open ports should be reviewed on a set, periodic basis to ensure there are no unnecessary ports open. In addition, an audit ensures that procedures are being followed and decisions are made in a consistent manner.

A copy of the current firewall ruleset is a valuable tool in this process. Each rule must be reviewed and judged to ensure it is still necessary. In many cases the analyst will have to verify with the original requestor if an open port is still necessary. Once the firewall ruleset is reviewed and verified, all unnecessary ports should be closed as soon as possible.

The frequency of a review will depend on organizational needs. I recommend a full review of firewall ports once a year. This may be in addition to any other

periodic automated review done for the firewall ruleset. A yearly review is sufficient because it does not keep analysts busy with security reviews all the time. However, a yearly review still ensures appropriate accountability.

Penetration tests

Employees are fallible and hackers are malicious. A yearly penetration test is a good way to ensure you are as secure as you think you are. A third party penetration testing company is a good neutral source for a penetration test. Not only can you ensure your border security is adequate, you can also ensure your DMZ services are protected.

Typically, a third party does not know which ports a company has decided to open. They will run a port scan against the border security and provide a report of their findings to management. There are many other vulnerability tests that a third party vendor can run, but the port scanner gives an "Internet view" of the open ports on your firewall. All that has to be done now is to reconcile it with the yearly audit that was already performed, and you have a good handle on what ports are open.

Stewardship must be done to ensure there are no security holes in your border security. Audits and penetration tests are invaluable to completing this stewardship. Audit and penetration tests should be done in conjunction with each other in order to gain the maximum benefit. Each should be done on a yearly basis.

VIII - Conclusion

The port opening procedure at first appears to be very in-depth and time consuming. Of course, a security analyst's job is to protect the company's network, and that may involve time consuming duties. Experience has taught me that once the procedure is established and approved, the mechanics of deciding port openings is not time consuming. However, I found that port opening reviews were much more consistent and objective.

In order to achieve a secure environment and objective results, the following must be in place: The procedure must be approved by management and based on access policies already in place. The procedure must be available to both the users and the analyst. There must be a single entry point for submitting port opening requests. Organizations must assign the appropriate resources to review requests. Risk analysis must be done on the application as well as the assessing the impact to the network. Each DMZ network zone must be accounted for and examined in the decision process. Set decision points must be established to ensure consistent results and reviews. Approvals are critical to ensure appropriate review and accountability. Audits and penetration test must be

conducted yearly to ensure procedures are followed and only necessary ports are open.

It is clear to see that open ports on a firewall are a great risk to a company if they are not managed properly. Unfortunately, businesses need Internet functionality in order to take advantage of the vast marketing potential on the Internet. Business needs often trump security practices. However, a company can achieve a much higher level of confidence in their security if they follow a set procedure when making a decision to open firewall ports.

Reference Page

(1) Internet Security Task Force. "Initial Recommendations For Conducting Secure eBusiness". March 1, 2000. URL: http://www.ca.com/ISTF/recommendations.htm (May 5, 2003).

(2) Internet Security Task Force. "Initial Recommendations For Conducting Secure eBusiness". March 1, 2000. URL: http://www.ca.com/ISTF/recommendations.htm (May 5, 2003).

(3) CERT® Advisory CA-2003-04 MS-SQL Server Worm. January 27, 2003. URL: http://www.cert.org/advisories/CA-2003-04.html (May 4, 2003).

(4) Broersma, Matthew Slammer -- "The First 'Worhol' Worm?". February 3, 2003. URL: http://news.com.com/2100-1001-983197.html (May 5, 2003).

(5) Guel, Michael. The SANS Institute. "A Short Primer for Developing Security Policies". 2001. URL: http://www.sans.org/resources/policies/Policy_Primer.pdf (May 4, 2003).

(6) Guel, Michael. The SANS Institute. "A Short Primer for Developing Security Policies". 2001. URL: http://www.sans.org/resources/policies/Policy_Primer.pdf (May 4, 2003).

(7) Allen, Julia, H. The CERT® Guide to System and Network Security Practices. Boston. Addison-Wesley. May 2001.

(8) Wack, John, et all. "Guidelines on Firewalls and Firewall Policy". January, 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (May 6, 2003).

(9) Wack, John, et all. "Guidelines on Firewalls and Firewall Policy". January, 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (May 6, 2003).

(10) The Internet Ports Database. January 17, 2002. URL: http://www.portsdb.org/ (May 4, 2003).

(11) von Braun, Joakim. October 15, 2002. URL: http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html (May 4, 2003).

(12) Wack, John, et all. "Guidelines on Firewalls and Firewall Policy". January, 2002. http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (May 6, 2003).