Full Lifecycle Security Assessment - A Case Study

Gregory Golightly

Full Lifecycle Security Assessment – A Case Study

GSEC Practical Assignment 1.4
By Gregory J Golightly
August 2002

Summary

I had the opportunity to work with an organization and perform a security assessment that led to follow up work securing their environment based on the recommendations I put forth.

The project was a success, based on a number of criteria. The following goals were met at the end of the project:

- their environment saw a significant increase in the level of security;
- security awareness increased as a result of documentation;
- the organization gained a clear understanding of their vulnerabilities and how to address them;
- the organization had a clear roadmap of vulnerabilities to address and in what order; and
- the project was completed on time and on budget.

In addition to meeting the basic criteria above, the organization was presented with information and policy templates that could help them evolve from a reactionary based technology department to one that thinks and acts in a proactive manner.

I was able to help a non-profit organization with assets of over a billion dollars secure their infrastructure using a best practice approach, expert knowledge, along with vulnerability assessment tools by ISS. The organization has migrated from a totally open environment to an above average secure environment, by utilizing private IP addresses, NAT, DMZs, and redundant firewalls with the appropriate rule set.

Before

Since the basis of this project was security, the confidentiality of the client is required. The client will be called ABC Foundation (ABC).

ABC is the not for profit fund-raising entity for a large company. ABC has assets of over $1 billion in cash, stock, and property. Although they raise money for a public entity, they are a private entity and are not required to publish financial information or donor records.

The release of any donor information could be very damaging to the reputation of ABC and could have a critical effect on future donations. In addition, their books are private and information of what they own could be detrimental as well. Based on this, ABC requested that I perform a security assessment. They were concerned that they were vulnerable to attacks that could compromise the confidential data. After the results of the assessment were presented, they wanted to work with me to implement solutions that would provide them with the security that they desired without sacrificing functionality.

To complete this project, I followed the following lifecycle model:

Assess (part of the Before stage)
Design (part of the During stage)
Deploy (part of the During stage)
Optimize (part of the After stage)

Assess

The first step in the project lifecycle was to look at all areas of security of ABC. Once that information was gathered, I needed to assess all of the vulnerabilities. During the Assess stage, I utilized a number of tools along with my expertise and knowledge. Automated tools, such as network and database scanners from ISS were used. One of the tools, Internet Scanner, tests for potential network based vulnerabilities.

> *Internet Scanner is a network security solution that provides automated security vulnerability detection and analysis for devices on a network. From a single, easy to use interface, Internet Scanner automatically scans a network for vulnerabilities, and displays scan results and fix information in clear reports that allow users to respond quickly to critical vulnerabilities*[1].

I ran the Internet Scanner tool against all their IP addresses. Due to the wide-open nature of the network, I was able to scan their addresses and receive identical results from locations inside their network as well as from points on the Internet.

Utilizing ISS's Internet Scanner, I ran all levels of network and machine scans. All of the ISS scans were run during the off hours of 9 pm – 7 am so as not to negatively impact network traffic during business hours. The scans yielded a great number of violations that ranged in severity from very critical to ones of

[1] ISS Internet Scanner Whitepaper, p.2

much lower importance. Most of the violations could have been avoided with strict policies on machine configuration and software updating.

I scanned the database servers with ISS's Database scanner. I first scanned the database from the outside in a blind manner (with no knowledge of credentials). I then scanned the database from the inside with an administrator level account. Most database violations were weak passwords and poor account management.

The following are the main issues found through network scans, observations, and interviews:

1. No Firewall or Utilization of Public IP Addressing scheme
2. LAN/WAN issues
3. No DMZ
4. No IDS
5. No documented Policies and Procedures

No Firewall and Utilization of Public IP Addresses Scheme

The firewall, while not being a one-stop fix for everything security related, is the most basic step that should be employed by any entity connected to the Internet. Firewalls provide a barrier to the Internet and security through properly configured rules that hide the internal network and control access to resources. A firewall is a first step to secure an open network from the outside world, but they provide little to no protection from threats inside a network, where a great number of attacks generally originate. ABC wanted to secure themselves from the outside first, so a firewall was critical to this initiative.

A properly designed firewall is a key point of failure to a network, as it provides access to and from the Internet and often controls VPN access and content filtering. These roles make the firewall an area that requires redundancy. Even in the assessment phase, I made sure to explain that any firewall solution they implement should have some level of redundancy.

During the assessment, I found that all of their network devices had public registered IP addresses. Today IP is the protocol of choice for nearly all networks and is based on a number of standards, including class addressing. As part of class addressing, a number of IP addresses are set aside as private. These private addresses are not owned by any company, and they are not for use on the Internet. Their purpose is to be used by organizations internally. The reasons for this are several:

- It allows a company to provide Internet access to all of their devices while only having one public/registered address. This saves companies money while at the same time it preserves the number of addresses available, which are in short order.

- It allows a company to hide their internal network behind a limited number of real IP addresses, which increases security.

Microsoft recommends the use of private IP addresses:

> *For private TCP/IP networks that are not directly or indirectly connected to the Internet, you can use any range of valid IP addresses from Class A, B, or C.*
> *For private TCP/IP networks that are indirectly connected to the Internet by using a network address translator (NAT) or an application layer gateway such as a proxy server, the Internet Assigned Numbers Authority (IANA) recommends that you use the private IP addresses shown in the following table.*

Private network ID	***Subnet mask***	***Range of IP addresses***
10.0.0.0	*255.0.0.0*	*10.0.0.1 - 10.255.255.254*
172.16.0.0	*255.240.0.0*	*172.16.0.1 - 172.31.255.254*
192.168.0.0	*255.255.0.0*	*192.168.0.1 - 192.168.255.254*

> *Numbers in these ranges are reserved by IANA for private use on TCP/IP networks and are not used on the Internet.*
> *Usually, for security reasons, you should not connect more than a few TCP/IP systems within your network directly to the Internet. For any host systems on your network that connect to the Internet, you must obtain the use of registered IP addresses from your Internet service provider (ISP).*[2]

The use of public IP addresses with no firewall allows all of ABC's devices to be seen from anywhere on the Internet. Every device can be pinged and scanned with ease. The consequences of this are significant, as these devices have no protection from Internet borne threats. Anyone and everyone can see everything ABC has, even with limited hacking knowledge and tools. In addition, ABC had no ability to know when they are being scanned; so would-be hackers could poke around with no chance of being caught.

LAN/WAN Issues

ABC has two locations that are both connected to the Internet. All communications between the sites happens over the Internet. In this case the WAN is based on public networks. This is common with smaller companies, as it keeps the cost of interconnection down. There are special security concerns that must be addressed when using public networks for a WAN. ABC had not addresses these concerns. They connected the two offices with no extra security measures like VPNs.

[2] Numbering your network, Microsoft

The head office has a single LAN environment that contains all servers, workstations, printers, and networking equipment. This LAN is a single logical subnet with one range of IP addresses. All equipment is on the same core switch. A single router is used to connect the LAN to the Internet, as well as the remote office.

A flat switched network is not the most secure configuration. The best configuration follows Cisco's network hierarchy: Core, Distribution, and Access. This allows for better management of the network. In addition, security can be greatly tightened through the use of VLANs and access lists.

The remote office has a single LAN that is hub based. A single hub serves all the equipment in the office. A single router is connected to the hub and used to connect the office to the Internet as well as the head office.

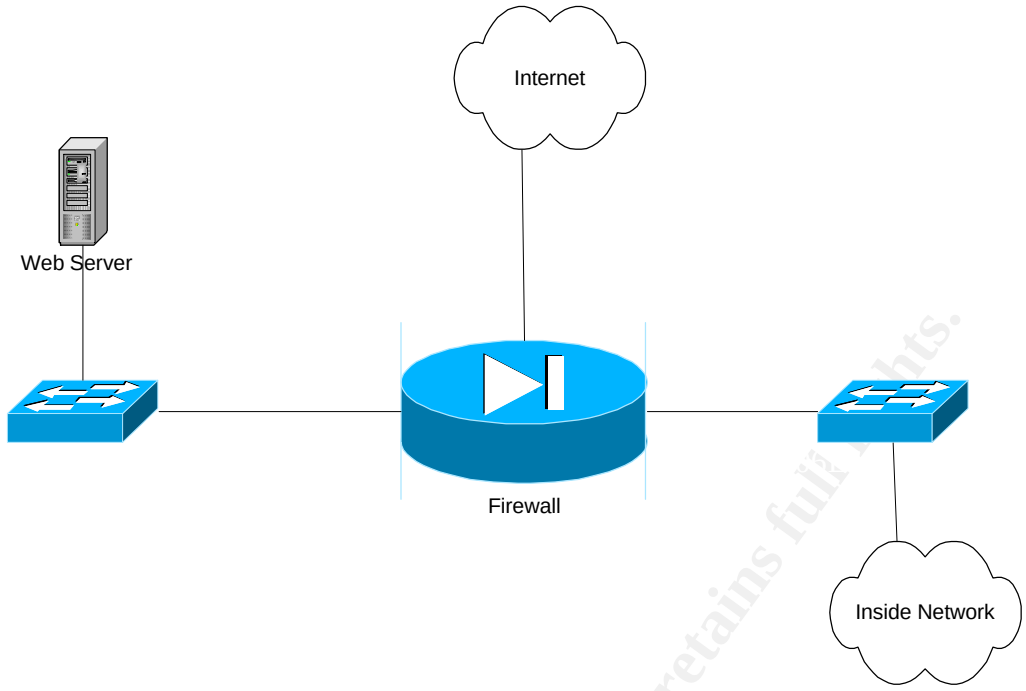
A hub based network is the most insecure network configuration. In a hub based environment, every device on the network can see all communication sent between any and all devices on the network. A hacker, or mischievous employee, only needs to get on the network with a sniffer to see all data that is sent and received by all servers and workstations. Critical information like passwords can be easily sniffed with freeware that requires very little expertise to operate.

No DMZ

ABC had a web server that needed to be available from the Internet. This server needed to be able to respond to web requests from users on the Internet, but also need to be as secure as possible.

Web servers, by their very nature, are the most likely to be compromised by a hacker. Mitigating this risk is key to a secure environment. Moving the web servers into a DMZ that is created by one or more firewalls is the optimal way to minimize this risk. By isolating the web servers from the network, the inside network is protected from the company's own computers (web servers) if they were used to attack the company.

The term DMZ is a military term that stands for De-Militarized Zone. In the computer world, a DMZ is separate network created by one or more firewalls. The following depicts a simple DMZ.



In the current configuration, ABC's web servers reside on the same segment as all of their equipment. If one of these servers were compromised, there would be nothing to stop them from jumping to other company servers. Firewalls.com explains the need for a DMZ as such:

> *The main advantage of using a DMZ port is to keep yoru private network protected from internet users. If a publicly accessed server becomes compromised by a malicious user then that user may be able to access resources on that network LAN segment. By keeping your private LAN on a separate network segment you do not run the risk of the malicious user accessing your corporate network.*[3]

No IDS

The ability to detect unauthorized activity is essential to a complete security plan. Sometimes new vulnerabilities are found and exploited before they can be fixed. In this case, even up-to-date security measures will not protect a company from being attacked. Intrusion Detection Systems (IDS) watch a network and all machines to look for things that should not be happening. They use a combination of signature files (much like an anti-virus program) to look for known attacks and they look for changes to files (adds, deletes, changes) that should not happen.

IDS allow a company to know that they are being attacked. In addition, they can tell who is attacking them, how they are doing it, and what they might be looking

[3] The DMZ Zone Explained

for. IDS can alert an administrator that the network was just port scanned. Using this information, the administrator can contact the service provider of the potential hacker and have their account shut down. If this were done enough on a global scale, there would be few places for the hackers to reside on the Internet.

There are two types of IDS, host based and network based along with a hybrid that is based on both types. Host based watches a host for any potential hacking activity by looking at how, when and by who all files are accessed. Network based watches for network activity that might indicate a hacker. Hybrid systems provide both. Neither host based nor network based can provide total monitoring, but by using both, or using a hybrid increased monitoring can take place.

No documented Policies and Procedures

ABC had little to no documented IT procedures. As such, everything was done 'ad hoc', which leads to systems that are hard to administer effectively. A complete IT handbook with policies and procedures is the foundation that a security plan is built upon. Everything within IT should be covered in a policy. Only after everything is done in a documented manner, time after time, does a network become standard enough to secure.

An example of how ABC could reduce vulnerability through the use of policies is a Server Setup Policy. On ABC servers, there was no consistency on how they were setup. A policy would have step-by-step procedures detailing how to disable guest accounts and enforce password standards. No such document existed and some servers had guest accounts and weak passwords.

The databases utilized by ABC, which hold their critical information, have poor password and account management. Many passwords were either 'password' or the same as the account name. This is a recipe for disaster. To aggravate issues, several default and guest accounts were active, some with extended privileges. A simple but well defined password policy could help eliminate this problem.

Anything that requires user interaction, like a password policy or Internet usage policy, should have user signoff to ensure that they policy is understood and followed.

Cisco provides similar recommendations:

> *We recommend creating usage policy statements that outline users' roles and responsibilities with regard to security. You can start with a general policy that covers all network systems and data within your company. This document should provide the general user community with an*

understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If your company has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.[4]

During

Design

Here are the items that needed to be addressed:

1. Firewall
2. DMZ
3. IP Addressing
4. Network re-design
5. IDS
6. IT Policies

Firewall
ABC was in desperate need of a firewall solution. The firewall would provide the foundation of several security initiatives such as: protection from the Internet, creation of a DMZ, Network Address Translation (NAT), as well as for some potential future initiatives like content filtering.

The proposed firewall solution had to meet their needs while staying within a budget. The following is a list of requirements that had to be met:

- Redundancy capability
- Multiple interfaces available / DMZ capability
- NAT capable
- VPN capable

Since the firewall would now be a single point of failure for the entire network, redundancy is key. If the firewall went down, inbound and outbound Internet connectivity would be lost. The minimum recommended configuration would be two firewalls in a failover system. A fully enabled failover setup allows for zero downtime in the event of a firewall failure. The pair are essentially mirrors of each other, with one acting as the primary. The secondary spends all its time making sure that the primary is up and functioning. If the primary fails, the secondary unit takes over almost instantly.

[4] Network Security Policy: Best Practices White Paper, Cisco

Verisign's thoughts on redundancy:

> *The definition of high availability is a hardware and software configuration in which a device takes over the tasks of another device that has gone down. In other words, communications are maintained in the event of a failure. No more valuable time lost due to down time and no more lost customers.*[5]

The key to setting up any firewall is to have a qualified individual work with the organization in order to create the simplest set of rules that accomplish the required filtering. Many organizations have firewalls with rules that they cannot explain enacted on them. There should be a process for adding or subtracting any rules on a firewall. I recommend a complete firewall log that covers every change ever made. This log has a printout or electronic copy of every configuration file before and after it is created, and should have a system for commenting on every rule to explain:

- Why the rule was created;
- Who created the rule;
- When the rule was enabled; and
- When the rule should be disabled, if applicable.

DMZ

With the addition of a firewall, ABC needs to implement a DMZ. This can be done with an additional Ethernet interface on the firewall (one on each if there is a redundant pair). The DMZ is just another network on the firewall. As such, it needs to have a complete rule set that governs the traffic in and out.

IDS

ABC should implement IDS as part of their security plan. IDS is the watchdog that adds a layer of comfort over all security systems and policies. IDS watches the entire system, from the DMZ to the entire inside network. This would typically involve one network sensor for each network segment and host based sensors for critical servers.

Policies

Every business process should be documented. A business has a much greater ability to continue through disasters and employee loss if every process is documented. Nowhere is this more apparent than in the IT department. IT

[5] High Availability FireWall-1 on Nokia

traditionally has high turnover, and solid documentation is the only defense against the losses that turnover can cause.

ABC had neither an IT handbook, nor any IT policies in place. Everything was done the way that the particular employee wanted to do it when it was done. Servers with the same OS had very dissimilar settings, and workstations were not all alike. Some network devices have SNMP enabled but not configured (a significant security risk) while others had it disabled.

Deploy

I assisted ABC with the deployment of a number of technologies and practices that greatly improved their overall security. They decided not to deploy several of the things I recommended due to budgetary constraints. I assisted them with implementing a firewall, DMZ, redoing the IP address range while utilizing NAT, and the creation of IT policies. They decided not to move forward with redesigning their LAN/WAN or implementing an IDS solution.

Firewall

The firewall solution had to be an industry standard solution that could support a DMZ and failover capability. Another requirement of the client is the ability to find external resources that could administer and troubleshoot the firewall as needed, as ABC had limited skills in-house. Cisco's line of PIX firewalls met ABC's firewall requirements.

I assisted them in implementing a redundant pair of Cisco PIX 525 firewalls. The PIX 525 is an industry standard firewall appliance that has a large market share. This fact ensures that there is a wealth of talent available to work on them if needed. It also ensures that this solution is a trusted technology that will be around for the coming years. In addition, the 525 is powerful enough to handle growth and expansion. Down the road, this solution could handle multiple DMZ's and could provide a VPN solution for remote access.

The addition of the firewall had to coincide with the all the addressing changes, or at least it needed to so as to avoid any extra steps. To ensure that the firewall was ready, I had setup the failover pair in a lab environment setup. The lab was an isolated network in which I recreated the 'outside', the firewalls, and the 'inside'. This allowed me to test all the firewall rules without risking production downtime. After the system tested out, and all bugs were fixed, I made the production switchover with total confidence.

DMZ

The firewall was ordered with enough interfaces to implement a DMZ. Making a DMZ is rather simple once the firewall is setup and configured. I enabled the interface used for the DMZ, added some basic rules, and plugged in a switch to the DMZ interface to create a fully functional DMZ.

ABC placed their web server in the DMZ. At this time, ABC only had one web server. In addition, they did not have any other servers that needed to reside on the DMZ. Down the road, I recommended that they move their email server to the DMZ, or create a mail relay server to place in the DMZ to better control the security of mail flow.

In order for the web server to be moved into the DMZ while keeping downtime to a minimum, I kept the external IP address of the server the same. I created the DMZ on the firewall and had the rule to forward port 80 and 443 requests to the web server's DMZ address. I moved everything at one time in the middle of the night to reduce impact. I had a full back out plan ready to use in case of a problem. As soon as the switch was made, I verified that the web server could be hit from a number of external locations.

IP Addressing

ABC had access to a full class C address range, which was currently being used on all machines in the network. I moved them to a configuration in which only 2 real IP addresses were in use, one for their website and one for their email. We kept the two addresses that were being used for this purpose previously, so as not to have to make any DNS changes. This kept downtime of the web site and email to a minimum.

The rest of the equipment on the network moved to a private class A addressing scheme, 192.168.1.x (for inside) and 192.168.5.x (DMZ). In order to keep the two real IP addresses functioning, I configured the firewall to direct all traffic to the correct machine. The firewall would forward any port 80 or 443 requests directed for the real IP address of the website to the DMZ address of 192.168.5.10, the DMZ address of the web server. Any mail traffic headed for the mail server real IP address would be forwarded to the internal address of 192.168.1.10, the inside address of the mail server.

I assisted ABC in changing all server IP addresses (except the web server, which is in the DMZ) to addresses from 192.168.1.10 to 192.168.1.49. I changed all network-based printers to addresses from 192.168.50 to 192.168.1.79. The employee machines are now on a DHCP scope from 192.168.1.100 to 192.168.1.200.

Changing all IP addresses, even in a small network, is not a quick and simple task. The first task required is to look into the use of all IP addresses in drive mapping, printer mapping, and in software code. This needs to be done well

ahead of the switchover date. The most problematic issue is the hard coding of IP addresses in code. Developers should know better than to do this, but it often happens in order to make something work when a deadline is near. Fortunately, ABC did not have any IP addresses coded into any software. In fact, all mappings and connections were made by server name, which made the switch much easier. In addition, I checked for the use of host and lmhost files on any machines, of which there were none.

The first thing I did was to create a DHCP server that had the new range of addresses. I put it on a separate subnet to test it without disrupting the real systems. I created a complete spreadsheet of before and after addresses for all the static items such as the servers and printers.

On the night of the switch over, we put the firewall into place (which had been tested in a lab) and started the process of the switching all IP addresses over. We started with the servers, and then the printers. Using a statically addressed machine, I tested connectivity to the servers by name and IP address. I then printed to all the printers by their server share and their new IP address. Once that tested out successfully, I checked access out to the Internet, which passed as well. I then switched my machine to DHCP, and it received an address with no problem. We then started powering on all the workstations. Most of all them grabbed a new address with no problem. A few Windows 9x boxes held on to their old addresses, and I manually ran a renew on them.

The next working day there were less then five issues; most of them were IP addresses that needed to be refreshed. Nothing took over 10 minutes to fix.

Policies

ABC could address many of its security flaws simply through the use of well-written policies and procedures. Here is a list of policies I have started for ABC:

- General IT Policy
- Security Policy
- Password Policy
- Server Configuration Policy
- Workstation Configuration Policy
- Disaster Recovery Plan
- Disaster Recovery Testing Plan
- Security Awareness Program
- Multi-Tier Termination Policy
- Public Internet Usage Policy
- Electronic Mail Policy
- Internal Employee Privacy Policy
- Public Web Site Privacy Policy
- PDA Usage Policy

- Data Ownership Contract / Policy

I gave ABC these templates and helped them put together an internal committee to agree on standards for all the policies.

After

Optimize

Optimization is an often overlooked aspect of a project lifecycle. Once a technology, procedure, or policy is in place, it needs to be adjusted and modified to best suit a company. Even if a solution is perfectly matched to a company at the beginning of a project, the natural changes and modifications that occur during the project will require some adjustments to the solution.

In the case of ABC and their security assessment, the number one thing I tried to impress on them was that all of their policies, along with all of the technology we put into place, must be kept up-to-date. If not, then they will not maintain the level of security they have now. The worst case scenario can be to believe you are secure while you are not. At least in the previous state of affairs, they were not secure, but they knew they were not secure. While they are somewhat secure now, if they do not keep everything up-to-date, they will not stay that way.

Resolution

After the completion of the security assessment and the changes that were driven out of that, ABC is clearly more secure for the following reasons:

- Firewall
  - They now have a redundant pair of industry standard firewalls that protect them from the Internet. No longer are all machines totally open from the Internet. All traffic inbound is blocked by default, unless specified in a rule.
- DMZ
  - The web server is in a protected DMZ. The DMZ provides protection from the outside world, while still allowing access to port 80 and 443 as needed. In addition, the firewall protects the inside network from the web server, while allowing the inside to still update the web server.
- IP Addressing

    - ABC now uses private IP addresses inside their network. In addition to reduced cost, using private IP addresses is preferable to keep better tabs on data traffic in and out of a network
- Policies
    - ABC now has the basic groundwork for an IT handbook in place. Many security issues are addressed in the handbook.

ABC is not totally secure. No company is totally secure. They have a weakness without implementing an IDS solution, but that is a choice that they have to weigh against the funds they have available. IDS is one of the final steps that can help watch a network for any questionable activity. As their network stands now, they are still very vulnerable from the inside of the network. Even though ABC was told that internal threats are very significant, the purpose of this security assessment and follow up work was to tighten security from the outside world. Overall, I believe that this project was a success based on those criteria.

Many of the things I have learned while studying for the GSEC certification have helped me. I used several tools that they mention to assess ABC's current state of security. In addition, the overall security concepts have allowed me to better understand the ways hackers work, which allows me to recommend ways to defend against their tactics.

For the after section, you must be able to clearly outline a state of enhanced security in the system or subject that you are writing about. Was the problem resolved? Did the fix cause additional complications? Is there still vulnerability? What is the risk now? How did your existing knowledge and/or the topics covered in the SANS Security Essentials course aid you in the overall process of outlining risk and vulnerability, and identifying and applying the right solution?

Impact

Firewall/NAT
Now only two IP addresses show up when scanned from the outside, and those only have limited ports listening. The IP address listed for the web server is listening on Port 80 and 443 and the IP address for the mail server is listening on port 25. No other machines can be pinged. Nothing else is listening or responding. This is a critical step to stopping hackers.

DMZ
The addition of a DMZ allows ABC to host web content without opening their inside network to attacks. ABC can update its web site as needed without being hindered by security, while at the same time their web server is not a threat to them.

Policies

ABC now has the foundation of a IT manual that sets forth standards for everything. Immediate impacts of this documentation can be seen from password policies to server setup, which is no longer done on the fly but is set forth in a complete set of instructions.

Summary

A security assessment is the first step to security awareness. Often a company knows that they are not secure simply because they have not taken proactive steps to address it. However, they have no idea what makes them insecure. Having a qualified security consultant or firm come in to perform a complete security assessment (which is more than is addressed in this paper, with topics such as physical security, mobile security, and much more) should be done before any money is spent on hardware or software. This assessment should give you the roadmap for where and what to spend money on, and in what order.

References

Internet Scanner Technical Overview
http://documents.iss.net/whitepapers/IS_TechOverview.pdf

Network Security Policy: Best Practices White Paper
Cisco
http://www.cisco.com/warp/public/126/secpol.html

Numbering your network
Microsoft
http://www.microsoft.com/windows2000/en/server/help/sag_TCPIP_imp_config_num.htm

The DMZ Zone Explained
Firewalls.com
http://www.firewalls.com/document-dmz.asp

High Availability FireWall-1 on Nokia
Verisign
http://www.verisign.com/products/nokia/