Global Information Assurance Certification Paper

Steve Wescoat

December 2, 2003

Different Layers in Defense in Depth

Abstract

This paper explains how to setup Defense in Depth in the perimeter network. In today's world, a company cannot have a firewall as your only defense. Most companies are connected to the Internet and have business partner's virtual private networks (VPN) or intranet sites that need to be protected. You need to have a layered approach to network security. If a hacker gets thru your firewall then they are in your network and can have free range to do whatever they would like to do. If you use Defense in Depth strategy then your chances of a break-in is reduced because of the layers you add. You need have a security policy that defines the blueprint for you network security. Then you need to harden your perimeter router and firewall. If you are going to host any type of Internet service then you must have a DMZ or screen subnet. Virus scanning on your servers and desktops is a requirement. Next, you need to have some type of Intrusion detection system on your network to monitor your traffic. Patch management is another layer that needs to be address in a company. The last item you need to have is a well-informed user base. If you use each layer of defense in you network then you reduce the risk of one failing and if one does fail then you have the added protection of the others. This will give you more time to detect an intruder and then minimizes the risk. This paper will show the different areas of the triage of network security that is used. The triage is confidentiality, integrity, and, Availability. If one of triage fails then your security is comprised.

What to include in Defense in Depth setup in the perimeter network.

In today's world, most companies are connected to the Internet. Companies have sensitive and propriety information that they need to protect. Networked computers play a big role in their organization. Users have come to depend on computers for everything from email, Internet browsing, data storage, chat, and other activities that they could not do their job without their computers. As a Security Manager, you need to protect and educate all employees in the company on network security.

When a company is going to connect their data networks to the public Internet they cannot just throw in a firewall and say they are secure. Because the user communities are, getting smarter and more hackers and crackers are trying to break into your network. If you look at your firewall logs, you will see that you are being port scan everyday by script kiddies or some form of Internet attacker. Companies need to use a layered approach or Defense in Depth (DID) setup. Defense in Depth is taken from the military practices. Defense in Depth

has been labeled for a multi-layered security architecture that involves the deployment of the following firewalls, anti-virus software, intrusion-detection systems (IDS) and so on. The idea is to combine technology components with good security management practices to form layers of protection that will reduce the risk of attacks or intrusions. You cannot depend on only one layer of protection. You need to make it harder for an attacker to break into your network. With a layered approach to network security this can be achieved with Defense in Depth.

This paper will discuss the following items to use in a Defense in Depth layered approach setup; security policy, perimeter router hardening, firewall, anti-virus software, network switches, IDS, employees training, physical security and patch management.

Security Policy

One of the first layers in Defense in Depth that a company needs to create is a security policy. A security policy is the blueprint of the company's security practices. This document needs to be defined by what the company is trying to protect. How are they going to do it? It not only helps a system administrator but also the end users if you have a security breach. Writing a security policy is not an easy task. You need to decide if you are going to write one policy or break into smaller parts. Every company should have the following policies in place: Internet use Policy, Password Policy, Remote Access Policy, and Configuration Policy. When writing the policy you need to remember your audience. If you are writing a policy for your user community you need to use laymen terms and explain it in to them in words they can understand. If you make it too technical then the user will not adhere to it or even read it. Most companies give these polices to new hire during the employee orientation. The make them sign it and then keep it on file if they need to use the policy for complicacy. You need to test your policy by giving it to someone and have him or her read it. If they do not understand the policy then it must be rewritten so that the end user can make sense of it. If you are writing it to upper management you need to make it short and very concise report because they will not read a 20 page document. You need to have management "buy-in" for each policy. If management does not give their approval, then when it is time you need to enforce the policy it will be extremely tough. The policy cannot be written and then filed away. The policy must be kept current. You need to review your policy at least twice a year.

Perimeter Router access

Every company that connects to the Internet uses some sort of router to route traffic out to the Internet. I will discuss Cisco products because they are the most popular routers in the world. You cannot install a router and use only the default settings. There are websites that list the default user id and

passwords for every vendor's products on the Internet. A router provides access out of your network and it is your first layer of defense. You need keep your router IOS software up to date and use the following tips. This will stop many attacks against your perimeter network.

- Limit Telnet access to router
- Use SSH to manage router
- Lockdown Simple Network Management Protocol (SNMP)
- Use Terminal Access Controller TACACS+) to connect to router
- Turn off unneeded services
- Syslog to a different box
- Use strong Passwords
- Access Control List
- Post warning banners

The main way to configure your router is thru telnet. Telnet is not secure do to the fact that sends date in clear text. If you use SSH the telnet session will be encrypted. The primary reason you should harden your router is that it is the first line of defense of your layered network design. Some Internet Service Providers (ISP) maintains your Internet router. You need to make sure they are keeping it up to date and can respond to your requests to put in an access list to stop certain attacks you do not want to have to wait 24 hours for them to get back to you. Some of the latest virus attacks have been stop at the perimeter routers by using Access control lists to block the port that attackers have been using.

Firewalls

The next layer of Defense in Depth is your firewall. Anybody that is connected to Internet needs some type of firewall. There are a variety of systems that can be used such as, a packet filtering, a stateful, and proxy firewalls. When determining which firewall type to use in a company is speed. The fastest type is packet filtering but it does not offer a lot of security. The most secure Firewall is Proxy firewall be it is the slowest because it has to dig deeper into the IP packet to determine how to handle it. A firewall's job is to let traffic in that you have defined to come into your network. It also lets you connect your company to the Internet with only one IP address. The Internet is running out of IP addresses and the solution for the time being is RFC1918 Network Address Translation (NAT). Most ISP gives a company a certain number of IP addressee's when they sign up for Internet service. To overcome this limitation firewalls and routers can use NAT. You can setup up NAT with the following private address range

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

This networks IP ranges should not be routed across the Internet. All ISP are supposed to block these ranges on their routers. A company will pick an address range that fits their current demand and allows for future growth. The firewall's main purpose is to let traffic in only if it meets a rule that is defined in it rules set. You should use the default-deny philosophy that dictates configuring routers and firewalls to block protocols that are not expressly permitted. Experts say that most network segments only need basic services such as SMTP for email (port 25) DNS (port 53), HTTP for web (port 80) and SSL (port 443). All other ports can be closed unless required by some application or business need. The deny policy is harder to administrate but will keep out unwanted traffic. You have to do a lot of planning to know which ports are already in place and what needs to be open.

If a company is going to host a web server or email server they need to setup a DMZ or screened subnet. The screened subnet is a separate network where you put your front end server's that will tie into your sever on the production network. This network segment is protected by the firewall and is separate from your internal network segment. If an attacker breaks into your screen subnet your internal network is still safe and this adds another level of protection. You can also setup a DMZ for your partner's to connect to your network. If you are going to let a partner connect to your network you are giving explicit trust to them. This means are you going to trust that their network is secure on their side of the firewall. You should not trust them because an attacker can break into their network and then they would have a clean path into yours. You need to setup a screened subnet and only give access and open ports that are necessary to conduct business.

Some firewalls have Virtual Private Networks (VPN) built into them. This gives you a secure connection into your network. Companies are doing away with remote dial-in access servers and are using VPN for remote uses instead. Most remote users have high-speed Internet access, which allows them to connecting from home as if they were using their computers at the office. It also gives them a secure encrypted connection into your network. You need to make sure that each user has a personal firewall or they could let an attacker using their connection into the network. You can setup a site-to-site VPN between your remote offices and it usually is cheaper and faster then frame-relay or service provider network.

With any firewall you need to monitor your system logs. You should setup your Syslog's to a separate server and monitor it daily. Why do you need to use a separate logging server? If your firewall is down you will not be able to view the logs to troubleshoot it if there was an attack. You want the firewall to only block traffic or permit traffic. By using a syslog server you offload the processor and storage so the firewall can run faster and cleaner.

As you can see this is the second layer of Defense in Depth in your network. You need to protect this piece of hardware with the latest service patches and updates. If you do not then your firewall is your single point of failure. Some companies are install 2 firewall for failover capabilities or high availability solutions.

Switches

One of the simplest fixes a security manager can recommend to a company is to replace all shared hubs with network switches. When using a Hub everyone is sharing the same media. This means everyone on the network is on the same broadcast domain that means they can listen to all traffic on that network. When a company is using shared media it is really easy to plug into a network jack in a conference room and load a network sniffer and start to listen for user ID and passwords. You can replace your hubs with a switch and this will make it more difficult. A switch will learn who is on the network by remembering your MAC address. Each Network interface card has a unique MAC address. It makes a one to one connection from the server to the client or other clients. You only see the traffic on that connection. It cuts down on broadcast traffic and makes sniffing a network much harder. To be able to sniff the network with a switch you will need to create a special port that will listen to all other ports. You have to physically create this port on the switch. Then you connect your computer to this spanning port you will be able to listen all traffic that crosses that switch. You can create a Virtual Local Area Network (VLAN) and group computers together that need to communicate with each other. When grouping the computers together on the same VLAN they can only talk to those computers on that VLAN. You will need a router to communicate if you have more then one VLAN. Make sure you turn off all network jacks that do not need to be live. This will cut down on people walking into a conference room or hiding a laptop to detect user id and passwords on the network.

Anti-Virus

One of the most used defenses in depth layers is your Anti-virus software. Anti-virus software should be installed on all your servers and desktops computers. All an attacker has to do is get thru your firewall by using a common port that you have open and they can create havoc on the network. If you have anti-virus software on your servers and desktops this will help stop some attacks. Anti-virus software establishes a significant layer in a reinforced security perimeter. Anti-virus has several strengths:

1. Anti-Virus software is effective at numerous popular Male ware specimens

2. Anti-virus software is unobtrusive because it has a relatively low rate of false positive. You can install the product and then configure it to receive update and the client will not see it running in the background
3. Anti-virus software is affordable and is a must have!

All anti-virus companies have updates that need to be applied to your servers and desktop. Most enterprise anti-virus Company has a central console that can you schedule your updates that need to be pushed out to the clients on a weekly basis. If a zero-day virus is released in the wild then you will need to apply a hotfix to your virus software and push it out immediately. The console will help you keep track of which user who has a virus and then you can run a report and have your Desktop support team try to clean the virus for off the computer. Anti-virus is a must have for a network.

Encryption

Why should we be concerned with encryption in Defense in Depth strategy? It really depends on what you are trying to protect. If your users are using the internet to do research then it really does not matter, but if your are a bank and need to make sure your client bank records are encrypted while traveling across the internet. All traffic that crosses the Internet by default is not secure. It is sent in clear text. When you use encryption with the Internet or data networks you usually will use port 443 or secure socket layer (SSL). When using data encryption you take a performance hit because of the added layers to your IP packets. The performance hit depends on your connection speed if you will notice a difference. Some other examples when to use encryption is VPN, PGP, PKI, Email, Passwords and secure logins. Encryption makes sure that confidentially and integrity is indeed being used. You can tell if a message or packet has been tampered. Encryption adds another layer that attacker would need to break thru.

Intrusion Detection Systems

The next layer of defense in depth that needs to be address is intrusion detection systems. As a security professional you are not going to be able to monitor your network 24 hours a day 7 days a week. The intrusion detection systems will help your overcome that. The IDS will monitor your network for signatures of attacks and can then report this information to the system administrator via email or pager. You have many different vendors to choose. You need to decide if you want network based intrusion detection or host based intrusion detection system.

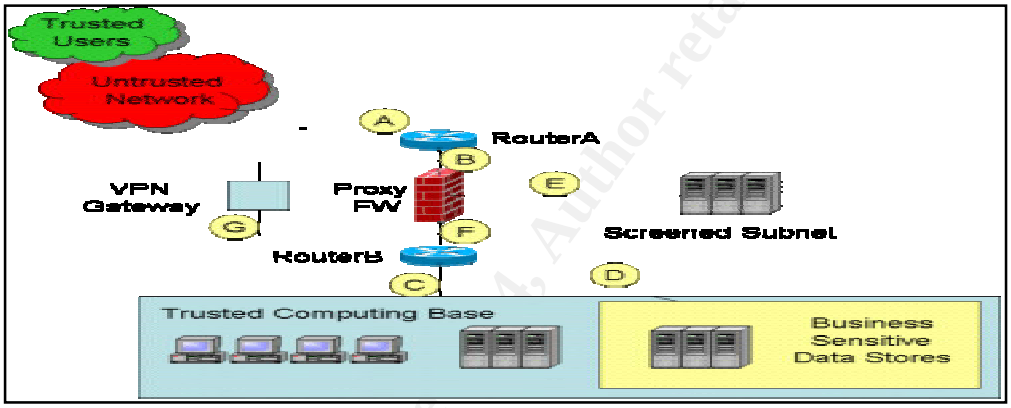
Network Intrusion Detection Systems monitors network segments. You will need a network IDS system for each subnet on your network that you would like to monitor. It also examines network traffic and detects scans, probes and attacks. Without intrusion detection most attacks would go unnoticed. Network based IDS uses two type of scanning techniques Signature-based ID and

Statistical anomaly-based ID. Signature-based IDS systems use a pattern when looking at data on your network. When it finds a match it will generate an alert.

Host-based intrusion detection involves monitoring the systems network activity, file systems; log files, and user actions on that server. It will generate an alert when it finds a match. Host-based IDS have the following benefits over network based.

1. Host-based IDS sensors can monitor user-specific activity on the systems. It can monitor the user's local activity of the system
2. Host-based IDS sensors can monitor data exchange of encrypted network streams by tapping in at the connection endpoint.
3. Host-based IDS sensors can help detect attacks that utilize network IDS evasions techniques

You also need to decide where you need to load the IDS sensors. The following diagram shows the recommended places to place your IDS sensors.



You need to have one IDS system monitor for your screened subnet, one for your internal network and last you need one between your firewall and perimeter router. IDS systems are a layer of defense that helps the systems administrators monitor and then alert them of attack that might go unnoticed. You should consider using both type IDS systems on your network. The NIDS will help you get an overall look at your network. The HIDS should be put on your high availability servers so you when an alert is triggered you know you must take action immediately.

Physical Security

Physical security is one layer that is most often overlooked. You need to have a secure location that you can store your networking and server equipment. It needs to be in a location that is secured by lock and key or badge access. The doors need to be labeled for IT personnel only to warn people about the area. Administrators are the only ones that need access to this room. The doors should automatically lock themselves after they have been closed. You should

have a login/logout book that list what changes have been made to the system and who did them. All server consoles should be logout and a password protected screen saver that actives after 10 minutes to reduce the risk of someone walking up to the console. You a can disable the floppy and CD-ROM drive in the bois and then password protect it. This would stop someone from copy configuration files or sensitive information to a Floppy or CD-ROM. Tapes need to be stored in a fireproof safe and at least monthly backups kept off site. If your site can afford closed circuit televisions then they need to be placed at the entrance of the data center doors. All visitors should be escorted in and out of the data center and never be left alone. They could put in a Linux boot disk and reboot the server then change the administrator password on you Windows or Linux box and have full access to your network. Physical security is very important to keep people out of areas they do not need to be in.

Employee Training

Another layer in you Defense in-Depth is to train the employees. Most of your security breaches come from inside your network. You need to update your user community on why it is important to change their password every 45 days or whatever you password policy states. By changing their passwords it protest the users from having their passwords used in attacks. You need to inform the users not to write down their passwords down and keep them under their keyboards or any other easily accessible place. This one of the first places an intruder will look for the user id and their passwords. You can put of posters to inform your users on new security measure or create a monthly newsletter that explains a new security topic for the month. If you keep your employee informed they can be your extra set of eyes and ears. An attacker will use social engineering to gain access. They will call the end users to try and get information that they can use to attack your network. If you users do not recognize the person calling you should tell your users to either look them up in the company directory or get a number to call them back. The user should never give out their username and password to a person that calls them. If this happens then the users need to inform the security personnel so that they can write up an incident form to try to catch this attack. They can also inform other users that someone is trying to get information from the user community.

Patch Management

System administrators love to patch their systems. Microsoft is one of the hardest systems to keep updated. It seems that Microsoft comes out with a new security fix every week. Other Companies are just as worse as Microsoft but you hear more about them. How can a Sysadmin keep up with all the updates and which ones do they need to apply? The best way to know is to subscribe to a

vulnerabilities list or newsgroup. You can use CERT or SANS websites to get the latest news on which patches to watch for. How do you know if your company needs the update or can they wait for the next service patch? Fred Avolid has a six-step process to practical patching.

1. Develop an update inventory of all production systems. You can make a database that has the following in it OS type, Support pack levels, application, type of hardware
2. Devise a plan for standardizing production systems to the same version of OS or application software. If you have windows 2000 server then make everyone have the same support pack. When a hot fix comes it depends on a certain support pack level. If you have different levels of support packs then you would have to waste time finding out who has what. You can us your inventory list and know exactly which ones need updating.
3. Make a list of all security controls you have in place like routers, firewalls, IDS'S, AV as well as their configuration.
4. Compare reported vulnerabilities against your inventory/control list. Subscribe to at least one mail list that warns you of new vulnerabilities and the updates give you background on the vulnerability and will tell you if you need to be use it or not.
5. Classify the risk assesses the vulnerability and if you are at risk.
6. Apply the Patch.

If you follow his advice you have an updated list of all your servers and if a new patch comes out you can decide if you need to apply it or not. If you keep your servers patched you will keep of the many known vulnerabilities from comprising your systems. Patch management is one area the people do not spend enough time on. This is the easiest area to concentration on because it is something that we should already be doing. This area also is where we should spend our time and effort if you cannot get funding for new firewalls or IDS systems. If your servers and workstations are patched then this will prevent more attacks then a high-powered firewall. We have seen were the firewalls are blocking the correct ports but then you have a laptop that is taken home and gets infected then the user put it back on the network and it infects all you un-patched Desktops. We show this happened with the SQL slammer worm. Microsoft has come out with a tool called Software Update Services (SUS). You configure all your desktop or servers to connect to this server to get all of it windows update. You can approve the patches that you would like to pushes out to the client machines. This cuts down your Internet bandwidth and users install updates that might break your software builds. The hardest part of patch management is the desktop because of the time required to touch each one. Now with Microsoft SUS at least you can push out the patches to the desktops with have to touch each one.

Conclusion

Setting up a secure network is not just putting up a firewall and you are done. You need to have a defense in depth frame of mind. You need to create a security policy that defines what you are trying to protect and how you are going

to do it. Next, you need to Setup your firewall to protect your internal network and your screen subnet. Then you need to decide on which anti-virus product you will use. You will need to install it on your servers and desktops to get the maximum coverage. IDS systems help you monitor your network 24/7 and help find attacks that the naked eye would miss. Keeping employees out of the data center this will prevent accidents from happing. Then you need to train your employees on security issues. The last layer is to keep your systems patched. This is a blueprint to start your defense in depth project. This paper gives a little insight on the different layers that you can use to make your network more secure. The more layers you have on a network the harder it is to get in. If you have an inexperience attacker then he will by pass your network for a less secure one. We know there is a ton out there.

References

Avolio, Fred. “Practical Patching” March 2003
URL: http://infosecuritymag.techtarget.com/2003/mar/justthebasics.shtml

Nelson, Brain. “Defense-in-Depth: An introduction” June 30, 2001
URL: http://www.sans.org/rr/policy/defense.php

Northcutt, Stephen. “Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPN), Routers, and Intrusion Detection Systems”

Hickey, Dan Capital College “ Network Security 680 classroom notes”

RFC 1918
http://www.faqs.org/rfcs/rfc1918.html

Van Meter, Charlene. “Defense In Depth: A Primer” February 19, 2001
URL: http://www.sans.org/rr/start/primer.php

Walsh, Lawrence M. “Stop: Deny Everything” March 2003
URL: http://infosecuritymag.techtarget.com/2003/mar/news.shtml

“Network Security Best practices” September 12, 2002
URL:

http://asia.cnet.com/itmanager/specialreports/0,39006603,39100220,00.htm

http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event