Global Information Assurance Certification Paper

Design Secure Network Segmentation Approach

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version.1.4c

Option 1 - Research on Topics in Information Security

Submitted by: Ibrahim N.Alateeq
Submitted Date: Saturday, January 08, 2005
Location: SANS Down Under 2004, Melbourne
Paper Abstract: This paper written to obtain GSEC certification and its will be guidance for Network Administrator in Small Office Home Office (SOHO) networks to implement a secure network.

Table of Contents

List of Figures

Abstract/Summary

In this document I will discus some issues related to security on network and how design a secure network. We will look to network segmentations and how it will help us to identify the network topology. Our segment will be defined based on security level for each segment. The segments will be outside, internal, services and remote users. I will discus each segment in details and guide the NetAdms to steps that will help them to secure each segment.

Introduction

This paper written to obtain GSEC certification and its will be a small guide for Network Administrator in small Office Home Office (SOHO) networks.

SOHO networks usually have a small number of users. In this situation usually you do not have a security specialist but you still need a good level of security in your network. I concentrate in this paper to help and guide NetAdm people to design a secure network.

I build these guidelines and checklists based on some assumptions to simplify this task for the Network Administrator to achieve his goal by designing his network to meet his requirements with good level of security. These assumptions are:

- It is designed for SOHO networks and it may be not suitable for big networks, which they are; need procedures that are more complex.
- I consider in this paper that a network will be implemented from scratch. These guides will work very well for existing network but you must consider some factors when you want to apply these procedures on existing network. These factors like downtime planning, define specific services that you provide it in your network and any specific issue or concerns in your network.
- I prefer to use “Good Level of Security” term to describe high level of security. As security specialists, we know there is no 100% secure network. When I say “Good Level of Security”, I mean 90% - 95% of security.
- Also, I will consider this network contains the following Product and services. Edge Router, Firewall, Mail Server, Web Server, Applications Server, DNS, PCs, and Remote Access users. Whatever the vendors, these guide based on standard options on each products.

In this guide I will discuss the technical issues and define policies you will need it to secure the network. So, we will find in each chapter the security techniques and polices.

Chapter 1: Network Topology

Typically, SOHO network is simple one and you do not need to divide it to many segments. However, because this network contains different level of security, you need to know some weakness pointes in your network to protect it very well. The simplest way to define that is segmentation your network based on security level needed by each segment. This procedure called network segmentation and it will help us very much when we get later to firewall configuration. As you Shown in the figure (Figure 1), you will see all main devices and different segments.

The optimal segmentation for SOHO is dividing it to four segments. Here are the specifications for each segment (Figure 1).

1. Outside Segment

In this segment, you have only the edge router and in our case, it is the internet. In this segment, you have no control on traffic coming to you, But you have a full control (by Access-lists) to decide which traffic can get in your network and which traffic can travel to outside.

2. Services Segment

This segment contains the main services you are looking to provide them to the public. In some paper they are called DMZ zone. In this segment, you need to allow any request coming from outside to your network services. We will define it very well in next section.

3. Internal Segment

This is the highest security level in your network. It is containing the internal stations and internal servers that contain all your business plan, marketing plan and financials details.

4. Remote User Segment

This segment is the most critical one and you must concern about it. A first time you must ask your self in advance, “Do we need our staff to access our internal network from outside or not?” If **NO,** just remove this segment and don’t care about it. Otherwise you must define your polices and techniques to secure this segment.

We will look in more details how to secure each segment. In the following chapters we will discuss each segment in details and we will define polices needed and techniques to secure SOHO network.

In the Following Figure (Figure 1), we illustrate the topology of the

network that we will discuss it.

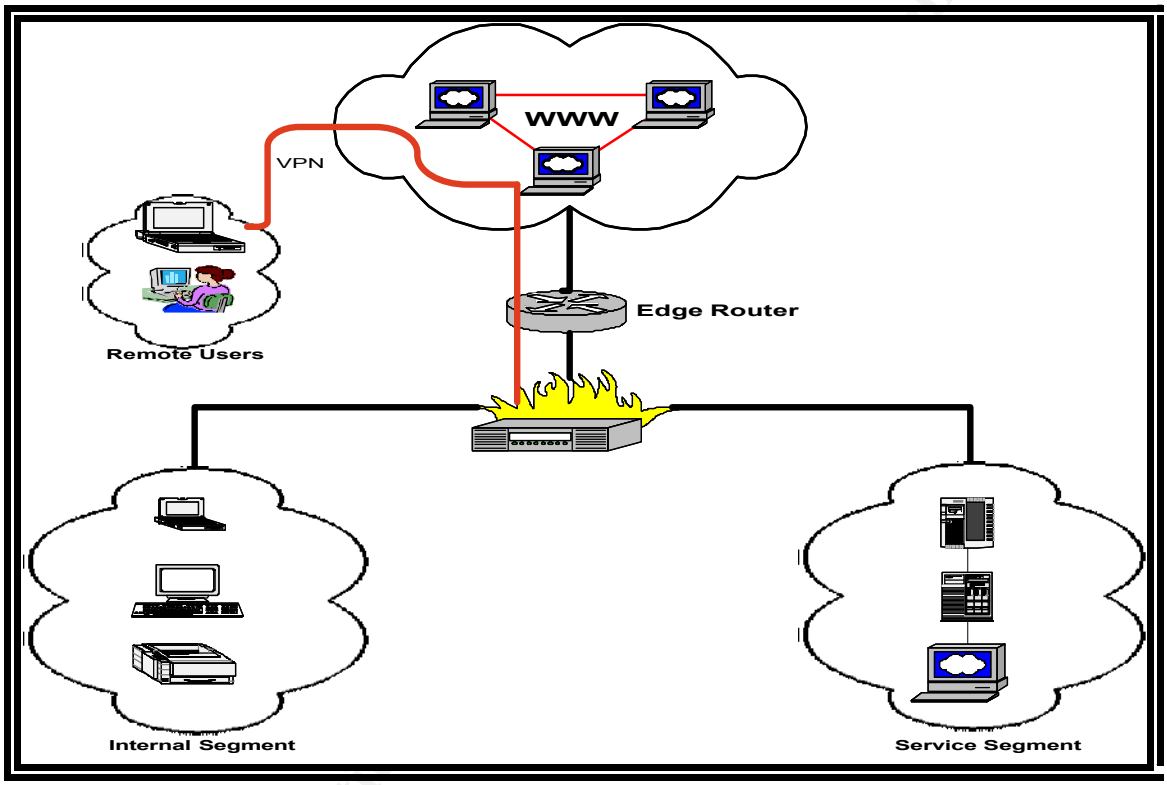

Figure 1: General Network Topology

Chapter 2: Securing Edge Router

1. Technical Considerations:

In general and regardless of vendors, the router technology provides basic services and they must be available in each router. These services are:

1. WAN Connectivity that will be provided by your ISP. This connectivity its may be varying based on your requirements and what your ISP can provide. Whatever the connectivity type – ADSL, ISDN, Frame Relay or ATM, the router capabilities and functionalities still the same.
2. Routing capability based on destination address whatever protocols are used.
3. Traffic filtering based on source address, destination address or Services port.

Nowadays, most routers existed in internet are “Cisco Router”. Therefore, in this paper you will find me use Cisco syntax.

2. IP Spoofing

The first issue in Edge router you must concern about it is IP spoofing. IP spoofing is denied by ensuring following rules applied: from any interface, access-lists accept only packets with legit source address. This means that only packets with source address from connected network's IP address space are allowed. If this rule cannot be fully enforced, we deny packets with source-address that cannot be right. For example, no packet with source address of your network can come in from external interface (Outer-If) (Figure 2). In Summary, inbound & outbound access-lists on every interface filter out spoofed packet.

In practically, this technique can be done by deny any packet with source address of your network and any packet has a privet address as mention on RFC 1918. Also deny any packet with broadcast or multicast source addresses, and packet with the reserved loop back address as a source address. It's usually also appropriate for an anti-spoofing to filter out all ICMP redirects, regardless of source or destination address. “**Step by Step - Cisco 827 ADSL Router Configuration**” http://www.secwiz.com/Default.aspx?tabid=49 . All these applied at outer interface as inbound access list. And to protect outside from your spoofing, you must deny any packet going to internet with IP not belong to you. You can apply this as outbound access list at inner interface.

```
! Anti-Spoofing
!inbound Access list@ outer interface
access-list 100 deny ip 0.0.0.0 0.255.255.255 any
! RFC 1918 Private Network
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
! Loopback Address
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
! Link Local Networks
access-list 100 deny ip 169.254.0.0 0.0.255.255 any
! TEST-NET
access-list 100 deny ip 192.0.2.0 0.0.0.255 any
! Class D Multicast & Class E Reserved & Unlocated Address
access-list 100 deny ip 224.0.0.0 31.255.255.255 any
access-list 100 deny ip 240.0.0.0 15.255.255.255 any
access-list 100 deny ip 248.0.0.0 15.255.255.255 any
! ICMP Redirect
access-list 100 deny icmp any any redirect
! Yor Network
access-list 100 deny ip Your Network IP Space any
!
! Outbound Access list@ inner interface
access-list 102 permit ip Your Network IP Space any
```

3. Protect Your Network

Access to your network is limited to certain hosts offering public services like WWW, DNS and Mail. This done by using inbound access-lists on interfaces directly connected to your network (Inner-If) (Figure 2) to filter traffic entering your network. Some one may be ask, “Why we do that in Router?” The answer will be to implement (Defense-in-Depth) concept. In this stage, the router filtering will be act as first level of defense to your network. You will see in the next section that we will do the same protection in firewall to be a second layer of Protection.

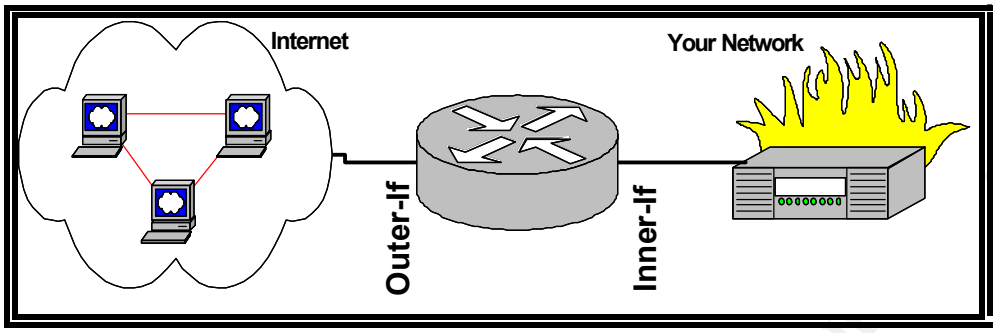

Figure 2: Inner and Outer Interface

In practically, this restriction technique can be done by applying this access list:

```
! Allow FTP services (ftp.yourcompany.com)
access-list 101 permit tcp any host ftp.yourcompany.com eq ftp
access-list 101 permit tcp any host ftp.yourcompany.com ftp-data
access-list 101 permit tcp any host ftp.yourcompany.com gt 1023
!
! Allow SMTP services (smtp.yourcompany.com)
access-list 101 permit tcp any host smtp.yourcompany.com eq smtp
!
! Allow DNS query ONLY (ns.yourcompany.com)
access-list 101 permit udp any host ns.yourcompany.com eq domain
!
! Allow DNS replaies to anywhere including Your network
access-list 101 permit udp any eq domain any
!
! Allow Zone Transfer from your slaves servers
access-list 101 permit tcp host A-Root host ns1.yourcompany.com eq
domain
access-list 101 permit tcp host A-Root host ns2.yourcompany.com eq
domain
!
! Allow WWW services to www.yourcompany.com
access-list 101 permit tcp any host www.yourcompany.com eq www
```

4. Protect Your Router

Router can be, by default, accessed physically by console port or remotely by TELNET or SSH. In this case, you must follow this policy to protect router itself from unauthorized access:

1. Set a good password by using Alphanumeric and special characters. And you must change it periodically – each Tow or three months -
2. Use SSH whenever you can.
3. Permit only your teams' workstation (NetAdm PC) to access router by telnet. In Cisco Router you can do that be this commands:

```
! Configure Access list To Permit TELNET
from SysAdm PC
!
RouterA(config)#access-list 50 permit
NetAdm-WorkStation-IP
RouterA(config)#line vty 0 4
!
! Apply access list to TELNET Virtual
```

Note: In some Cisco IOS, there is no supporting for Secure Remote Access like SSH. If it supported in your router it is prefer to use it and disable TELNET access.

Chapter 3: Firewall Traffic Map

In this section we will configure the main device in your network to protect you from outside attacker. The firewall in our network will be the contact point with outside world (Internet). Therefore, we need to identify each service that will allow going outside and each service, which will allow reaching our network. This procedure called “Traffic Map”.

Firewall traffic map is a procedure that will define based on your network segmentations and which traffic can be going from any segment to another. This procedure is most useful one to identify your services in each segment and from where you can reach these services. Again, regardless of vendors you can use this traffic map to implement your policy in your firewall.

Based on our network segmentations in chapter 1 and based on the services (WWW, DNS, and Mail) we mentioned about it in our assumptions, we can write the traffic map as following:

Service	protocol	Src. Segment	Src. Server	Dst. Segment	Dst. Server	Action	Comments
SSH	TCP	Internal	Any	Services	Any	Permit	
HTTP	TCP	Internal	Any	Services	WWW	Permit	
HTTPS	TCP	Internal	Any	Services	WWW	Permit	
FTP	TCP	Internal	Any	Services	FTP	Permit	
DNS	UDP	Internal	Any	Services	DNS	Permit	
SMTP	TCP	Internal	Any	Services	Mail	Permit	
POP3	TCP	Internal	Any	Services	Mail	Permit	
Any	Any	Internal	NetAdm PC	Services	Any	Permit	
Any	**Any**	**Internal**	**Any**	**Services**	**Any**	**Deny**	**Implicit Deny***
Any	Any	Internal	Any	Outside	Any	Permit	
Any	**Any**	**Internal**	**Any**	**Outside**	**Any**	**Deny**	**Implicit Deny***
HTTP	TCP	Outside	Any	Services	WWW	Permit	
HTTPS	TCP	Outside	Any	Services	WWW	Permit	
FTP	TCP	Outside	Any	Services	FTP	Permit	
Any	**Any**	**Outside**	**Any**	**Services**	**Any**	**Deny**	**Implicit Deny***
Any	Any	Outside	Any	Internal	Any	Deny	
Any	Any	Services	Any	Internal	Any	Deny	
Any	Any	Services	Any	Outside	Any	Permit	

VPN	TCP	Remote User	Any	Internal	Any	Permit	
Any	**Any**	**Remote User**	**Any**	**Internal**	**Any**	**Deny**	**Implicit Deny***
Any	**Any**	**Remote User**	**Any**	**Services**	**Any**	**Deny**	**Implicit Deny***

Table 1: Firewall Traffic Map

*implicit Deny: in most Firewall also in ACL configuration in Cisco Router, you just need to tell the firewall which traffic can be pass the firewall and by default the firewall will deny all another traffic.

Chapter 4: Securing Services Segment

In this section, we will discuss the services you want to provide it to public and how you will secure it.

1. *One service per server*

You need to consider this technique. One service per server is a good policy to your network security. Dividing various services between different servers has the following advantages:

- "This minimizes the complexity for any server, and helps to slow down an attacker from spreading their control throughout your servers if one server is compromise.
- It also greatly simplifies recovery in case of a successful attack". **Ray Ingles. *"Securing Server Hosts"*.**

http://ingles.homeunix.org/presos/websec/.

- It is easier to configuration of the individual servers with Simple and more secure configuration.
- It is most reliability. When one service is down it will not affect another services.

"It should be possible to compensate for any negative consequences that may a rise, such as higher hardware costs for purchasing several servers with fact that the individual server do not have the same performance, do not have to be more expensive than one particularly powerful server. Also Administration costs do not necessarily have to rise with the number of server, either, because simpler configuration of the individual server saves time". **Dr. Udo Helmbrecht**. ***IT Baseline Protection Manual.*** (BSI, German Information Security Agency) http://www.bsi.bund.de/gshb/english/s/s04097.html

2. *One Platform for All Server*

As a part of simplifying your network setup, which will help you very well to secure it, you need to use one platform in yours servers. By using a unique platform (Windows, Linux, and UNIX), it will be a simple to you to achieve the following security technique:

- Updating or Patching Operating System is an important procedure to fix many holes in your OS. By using one OS in your environment, this task will be simpler.
- In case of your system is crashed or Compromise and you want to recover it this will be easy with one OS. In RedHat Linux there is a technology called "kickstart". KickStart is a procedure to automate installation. "Using kickstart, a Network Administrator can create a single file containing the answers to all the questions that would normally be asked during a typical Red Hat Linux installation. This installation method can support the use of a single kickstart file to install Red Hat Linux on multiple machines, making it ideal for network and system administrators. Kickstart lets you automate most of a Red Hat Linux installation, including: Language selection - Network configuration - Keyboard selection - Boot loader installation (LILO) - Disk partitioning - Mouse selection - X Window System configuration " **Red Hat Linux 7.1 Manuals *"What are Kickstart Installations?"***
http://www.redhat.com/docs/manuals/linux/RHL-7.1-Manual/custom-guide/ch-kickstart2.html
Like Kickstart, there is a Jumpstart in Solaris environment.
- As Administration wise, it is simpler to NetAdm to dealing with one OS than different OS and it help them to take a quick action if needed. The quick action is very important especially when server is down.

3. Secure Your Servers – Operating System Side

Based on you decision on previous section about your platform, we need some issues you must consider it to protect the server it self. Regardless OS you are use and the methods to secure server, you must do the following to protect server OS:

- **Securing File System:**
  The core of your server is the OS files system. In this part, you must concern about some issue in OS Files system and you must consider it during setup the server because you need to do these steps in installation phase. To do that follows these steps:
  - Configure OS and data partitions with files system that support security features. (e.g., NTFS)
  - Configure file system with proper access permissions specifically you need to restrict access to files system and executables.
- **Securing Log On**
  The most weakness ring in security chain is people. Therefore, you must write and apply some policies to minimize this risk. The following policies and technique you as NetAdm take care to apply it and monitoring its operation.
  - Disable any access to server by TELNET (if possible) because

it uses a clear text to send data and replace it by encrypted method like Secure Shell (**SSH**).

- Set a strong password for administrator/root and users account. All Passwords must have the following conditions: At least (8) characters contain Upper/Lower Characters, numeric values and 2 Special Characters. No dictionary word is allowed
- Each user has own user account.
- Disable Guest account if enabled.
- Logging all accessing to your servers and create warning message against unauthorized access or use of restricted resources.
- Disable anonymous user logons.
- Disable caching of user logons
- Create a group for each department that shares information and assign each user to his group.

Some of these policies (in above) you can find it in this link. I use some of them in this section and if you have more complex environment it will help you to write your policies. ***Robert L. Williams. "Computers and Network Security in small Libraries".*** http://www.tsl.state.tx.us/ld/pubs/compsecurity/index.html

- **Securing Files and Folders**
  Your data in your system and your configuration files have the most values you in your network. You must care if any body modify or change these files. The good tool to do that is Tripwire. "Tripwire is a tool that checks to see what has changed on your system. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc". Various free of charge versions of tripwire an available for Linux in this link." **From** http://www.tripwire.org

4. Secure Your Servers – Services Side

The services available in your server are the interface with others and any communication between your servers and any body it come through the services available in your server. Therefore, you need to consider the following technique to minimize accessing to server just for services you are want to provide it. You must remove unnecessary services in the system. You need to back to your system manuals to know how to do that. To simplify your task I collect here some nice guides for example if you are using IIS Server See this line http://support.microsoft.com/default.aspx?scid=kb;en-us;321141. If you are using Linux see these links to guide you how remove unwanted services.
http://www.talug.org/events/20031206/basic_linux_security.html
http://www.linux.com/howtos/Security-Quickstart-HOWTO/services.shtml
As A part of this, also you need to remove unnecessary files/programs.

Second, each services has its own procedures to secure it and it is based on software you use it to provide this service. For example, if you use Apache on your WWW server it is good to look to these guides:

1. **"Securing Apache HTTP Server"**
http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-http.html.

2. "**Securing Apache 2: Step-by-Step"**
http://www.securityfocus.com/infocus/1786

3. If you are use IIS Server See "**A Guide to Securing IIS 5.0**"
http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/deploy/depovg/securiis.mspx.

4. For DNS, it is very good to refer to "**The SANS Top 20 Internet Security Vulnerabilities**". http://www.sans.org/top20/. There is a very nice reference to this issue in DNS part.

5. For Mail see "**Securing Sendmail"**.
http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-mail.html

Any why, to simplify your job, you must diced which software you will use it to the specific service and go back to product's homepage on internet. I sure you will find a good guide to secure this service.

Chapter 5: Securing Internal Segment

This is your highest security level on your network. This segment contains your staff PCs, Printers and internal servers that may be contain your confidential information. Not like server segment, in this segment you cannot force your staff to use specific OS because every body wants to use his favorite OS (Windows, Linux, and Mac OS). Because that you need policies more than techniques and you must be serious when you apply it to secure this important segment in your network.

Your policies in this segment will be covering your staff from variant vulnerability. Some of these vulnerabilities related to OS it self and some of them related to your staff behavior. Many employees let his PC working all the time without Lockout Timer or they like to try many software from internet. This is an example about employees' behavior and you as a NetAdm, must put your policies to avoid any irresponsible behavior.

There is a lot of paper in internet describing how to protect PC and a lot of tools and software that may be help you in this task. To help you, you can follow these policies to achieve this task. Some of these policies from this document in this link which it has a lot of policies and very nice ideas. ***Robert L. Williams. "Computers and Network Security in small Libraries".***
http://www.tsl.state.tx.us/ld/pubs/compsecurity/ptthreecheck.html

- Set a strong password for users account. All Passwords must have the following conditions: At least (8) characters contain Upper/Lower Characters, numeric values and two Special Characters. No dictionary words are allowed.
- Disable Guest account if enabled.
- Set Logout Timer to logout when no body works on PC.
- Disable Guest user logons.
- Disable caching of user logons and passwords.
- Install Antivirus Software and update it regularly (at least once every two weeks).

- Install a personal Firewall in each PC.
- Restrict access to hard drive. By another word, don't allow your staff to install any software. Any software needed must install under your permission. This to avoid install software has backdoors.
- Configure web browser to enhance privacy, and restrict access to web browser settings.
- Install software to restrict access to system functions within Windows applications.
- Remove unnecessary/unused files/programs from hard drive
- Schedule a periodic download for service pack and patches.

Whatever policies you have, it has no value if your staff does not care about security. Awareness training must be providing to your staff to let them realize the risk and help you to secure this segments.

Chapter 6: Securing Remote Access Segment

As we discuss in First chapter, you may be do not need this segment. However, in case you want your staff to reach your internal network from internet you must consider some issues to be sure about your network security.

First of all, do not allow any communication between internal segment and outside world unless you use encrypted method, regardless the services you will offer it. By this policy, you will be sure about traffic communication to your internal network will be encrypted. The VPN is the technique will help you to doing that.

"A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses" "**From**: www.whatis.com "

Many Firewall now coming with VPN capability. Therefore, to implement VPN you need to install client in Remote PCs and the server will be your firewall. VPN used port TCP 50 or TCP 51 as mention in RFC 1700. The Port 50 for Encapsulation Security Payload (ESP) and 51 for Authentication Header (AH). The ESP and AH are security services providing by IPsec which the VPN is implementation method of it. In windows XP there is a nice guide in How to "Use VPN for Secure Data Transfer" in this link

http://www.microsoft.com/windowsxp/using/mobility/expert/vpns.mspx

VPN policy and remote access policy are very important to you in this segment. There is a very nice sample policy in SANS site you can use it and add what you think is important to you. See this http://www.sans.org/resources/policies/

Chapter 7: Securing NetAdm Mentality

Do not be strange from this title. Because, whatever techniques you are use and policies you are write they have nothing without your actions. As we know in security world the most weakness coming from peoples not from products. So, you must concern about your security and be sure to use the products in optimal way and apply your policies without exceptions.

The security in IT environments it is not a product it is a process. Therefore, when you apply every thing, we are talking about it in this paper; do not think you are in safe now. No, you need to monitor your network in daily bases to be sure there is no new threats are coming. For example, every day there is a new viruses coming in the internet and if you do not update antivirus software, you will be in risk. In this paper I will list some policies and procedure that may be help you and put you updated about any new risks are coming. These policies and procedures are following:

1. Subscribe in security Mailing List like CERT Mailing List (http://www.us-cert.gov/cas/) or (http://www.microsoft.com/security/bulletins/alerts.mspx).
2. Read any alert carefully and be sure it is not effect you. If it is effect your network you must quickly fix that.
3. Subscribe in vendors mailing list related to your products to be updated about any alerts or vulnerabilities.
4. See your systems log in daily bases. It is a very nice task at starting your day with a cup of coffee☺.
5. You must care about Applying Policies and do not allow to break it.

Conclusion

By applying these techniques and policies discussed in this paper, you will reach to simple network with good level of security. As I said before, the security is not a product it is a process. So, you need to keep in your mind this issue. When you do that you can decide what is a new risks coming to your network and how you can avoid this risk to affect you or at least how minimize this risk. I hope this guide will be your first step in Security implementation with my best wishes.

References

1. Val Thiagarajan B.E., "Information Security Management Audit Check List"
http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

2. Article: "Network Infrastructure Security Checklist"
http://www.redsiren.com/pdf/advisory_virus/NetworkInfrastructureSecurityChecklistnew.pdf

3. Article: "District Security Self-Assessment Checklist"
http://securedistrict.cosn.org/Downloads/DistrictSelfAssessmentChecklist.pdf

4. Robert Boyce, "Vulnerability Assessments: The Pro-active Steps to Secure Your Organization"
http://www.sans.org/rr/papers/60/453.pdf

5. Robert L. Williams. "Computers and Network Security in small Libraries"
http://www.tsl.state.tx.us/ld/pubs/compsecurity/index.html

6. Article: "Step by Step - Cisco 827 ADSL Router Configuration"
http://www.secwiz.com/Default.aspx?tabid=49

7. Victor Hazlewood, Defense-In-Depth Information Assurance for 2003
http://www.sdsc.edu/~victor/DefenseInDepthWhitePaper.pdf

8. Article: "Help Defeat Denial of Service Attacks: Step-by-Step "
http://www.sans.org/dosstep/index.php

9. Germany. German Information Security Agency, Dr. Udo Helmbrecht. IT

© SANS Institute 2000 - 2005 Author retains full rights.

Baseline Protection Manual
http://www.bsi.bund.de/gshb/english/s/s04097.html

10. Sheldon, Tom. The Encyclopedia of Networking Electronic Edition (CD-ROM). Modern Age Books Inc, 1997 (I use it for terminology and Definitions)

11. www.whatis.com (I use it for terminology and Definitions)
12. http://business.cisco.com/glossary (I use it for terminology and Definitions)
13. http://www.webopedia.com (I use it for terminology and Definitions)
14. http://www.cyber.ust.hk/handbook4/03_hb4.html#ChapTocTop
15. http://www.information-security-policies.com/
16. http://www.sans.org/resources/policies/
17. http://www.faqs.org/rfcs/rfc1918.html
18. http://www.faqs.org/rfcs/rfc1700.html
19. http://rusecure.rutgers.edu/sec_plan/checklist.php

Terminology

Access Control	A process that determines who is given access to a local or remote computer system or network, as well as what and how much information someone can receive.
ADSL	An asynchronous digital subscriber line, which is a DSL variant in which traffic is transmitted at different rates in different directions. Suitable for Home Users or remote LAN access.
Asynchronous Transfer Mode	ATM is a dedicated-connection switching technology that organizes digital data into 53 cell units and transmits them over a physical medium using digital signal technology.
Authentication Header	AH allows authentication of the sender of data.
Defense in Depth	The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.
DMZ	It is a sub network that sits between internal network (LAN), and external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web, FTP, Email and DNS servers.

Domain Name Service	DNS an Internet translation service that resolves domain names to IP addresses and vice versa.
Encapsulation Security Payload	ESP supports authentication of the sender and encryption of data as well
Encryption	The manipulation, or encoding, of information to prevent anyone other than the intended recipient from reading the information. There are many types of encryption, and they are the basis of network security. Encryption is only a part of the basis of Network Security. There are other elements.
Firewall	A server or collection of components that control all traffic in and out of a network permitting only traffic that is authorized by local security policy to pass.
Firewall Traffic Map	A collection of network traffic filters and actions that can be applied to your firewall
Frame Relay	It is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between LANs and between end-points in a WAN. Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission.
ICMP redirects	ICMP redirect packets are used by routers to inform the hosts of correct routes to a particular destination. If an attacker is able to forge ICMP redirect packets, he or she can alter the routing tables on the host and possibly subvert the security of the host by causing traffic to flow via an unintended path
Inner-Interface	This is the interface that will accept connections from internal Network.
Integrated Services Digital Network	ISDN is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media

IP Spoofed	A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
IPsec	IPsec is a framework for a set of protocols for security at the network or packet processing layer of network communication provides two choices of security service: Authentication Header (AH) and Encapsulating Security Payload (ESP). The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.
Jumpstart	A type of installation in which the Solaris software is automatically installed on a system by using the factory-installed JumpStart software
Kickstart	is a procedure to automate installation in RedHat environment.
Layer 2 Tunneling Protocol	L2TP An IETF protocol for creating VPN using Internet. It supports non-IP protocols such as Apple Talk and IPX as well as the IPSec security protocol. It is a combination of Microsoft's Point-to-Point Tunneling Protocol and Cisco's Layer 2 Forwarding technology.
Logging	The process of storing information about events that occurred on the firewall or any network devices.
Network Topology	A topology (from Greek *topos* meaning place) is a description of any kind of locality in terms of its layout. In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines.
NTFS	NTFS (NT file system; sometimes New Technology File System) is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk. NTFS is the Windows NT equivalent of the Windows 95 file allocation table (FAT) and the OS/2 High Performance File System (HPFS). However, NTFS offers a number of improvements over FAT and HPFS in terms of performance, extendibility, and security.

Outer-Interface	This is the interface that will accept connections from internet.
Policy	Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.
Secure Shell Protocol	SSH protocol is communication protocol that is written with security in mind. It relays on strong encryption to secure the communication between the SSH server and client. If you want to allow others to connect remotely to their accounts, you better use SSH.
Secure Sockets Layer	SSL A security protocol developed by the Netscape Communications Corp. to encrypt sensitive data and to verify server authenticity.
Security Awareness Course	It is a course provides the attendees a basic skills and information needed to focus attention on securityand risks in IT environments.
Simple Network Management Protocol	SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.
Small Office Home Office networks	SOHO In information technology, SOHO is a term for the small office or home office environment and business culture. A number of organizations, businesses, and publications now exist to support people who work or have businesses in this environment.
VPN	is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.