GCFW (GIAC Firewall Analyst) Practical Version 3.0

Perimeter Security Design For GIAC Enterprises

Jimmy S. Lister

GCFW Practical, Version 3.0

June 27, 2004

Table of Contents

Absstract

This paper disuses the use of a Cisco Pix 515E firewall and Watch Guard X1000 firewall to secure the computer network of GIAC Enterprises. GIAC Enterprises is a small company which specializes in selling fortune cookie sayings online. All aspects of the design, installation and testing will be covered. Like many companies in today's tight business market GIAC Enterprises does not have unlimited finical resources; therefore their design will be secure but economical. This paper will also outline a simulated attack on another network and ways to prevent such attacks. Lastly this paper will present a detailed work procedure for installing and configuring a partner with VPN access to GIAC Enterprises network

Assignment 1 – Security Architecture

GIAC Customers

GIAC's customers are a diverse group spread across the globe. They are made up mostly of small family run businesses that produce and sell fortune cookies. GIAC's customers must be able to easily and securely purchase fortune cookies sayings over the Internet. Most of GIAC's customers lack any in-house technical staff and many are still using 56k dial-up accounts for their Internet connection. The large number of clients, lack of technical know-how, and the use of slow Internet connections rules out the use of VPN connections. The cost of installation and technical support would be too high. Also, the added complexity would not meet our requirement of ease of use for the customers. In order to allow our customers to easily and securely purchase sayings online they will connect to us over the Internet via our website using SSL. SSL meets our first requirement in that it is easy to use. All of the major browsers in use today support SSL; therefore there is no need for any type of client side setup. SSL also meets our second requirement of security. The SSL protocol has been used for online purchases and online banking for many years and should provide more than an adequate level of security for our online transactions.

One of our major concerns in using SSL is single factor authentication. Single factor authentication is susceptible to brute force and social engineering attacks. To help reduce the risk of unauthorized users accessing our online database we will encourage our customers to change their passwords on a regular basis. They will be required to use passwords that are at least 7 charters and we will encourage them to use hard to guess passwords. Although we would like to require our users to change their passwords on a regular basis and also to require them to use complex passwords, we chose to go with a less restrictive password policy of encouragement and education, to insure that we do not upset our paying customers. Since they only have read access to our fortune cookie sayings database, if a customer's login were to become compromised by a hacker there is very little damage that could be done. On the other hand if we made our password policy for our clients so strict that they were constantly getting locked out of the website we could lose them to a company with a website that is more user-friendly.

GIAC Suppliers

GIAC Enterprises suppliers consist of a diverse group of 15 individuals and 4 small companies that are spread out across the world. These suppliers are retained fulltime to provide creative and up-to-date sayings for GIAC Enterprises. GIAC's suppliers need to securely and easily transmit their work to corporate headquarters from anywhere in the world. They also need a way to securely communicate with GIAC Enterprise's creative director, the sales department, and also amongst themselves. In order to meet the supplier's requirements we will provide them with a user account and mailbox on our Exchange server. They will access the mailbox via Outlook Web Access (OWA). Each user will be able to send and receive e-mail both internally and externally. They will also have access to Exchange's Public Folders to store and share files. To upload their work they are required to post their assignments in text format, to their assigned Public Folder. From there it can be reviewed by our creative director and if approved, uploaded to our database server.

One advantage of using OWA is that there is no client side setup. To access OWA our suppliers only need access to a computer with Internet access and an up-to-data Web browser. Another advantage is that all communications between the internal staff and our suppliers will stay within our trusted internal network. Although we warn our users about sending sensitive information via email many still do, especially when communicating with other employees. Also all of their email and work related data will be stored on the Exchange server and not on a remote workstation, adding an extra level of security. Suppliers will be required to connect to OWA using Secured Sockets Layer (SSL) with 128 bit encryption. 128 bit SSL is supported by all major Web Browsers in use today. SSL is the prominent protocol for securing online transactions and is used in banking and online sales. SSL will provide an adequate level of protection for our supplier's connection into our network.

Like with any security designs this one is not 100% full proof. OWA only uses a username and password for authentication. This type of authentication is venerable to brute force guessing attacks and also social engineering attacks. Also, OWA runs on Microsoft's Internet Information Server, a web server that in the past has suffered some major vulnerabilities. To overcome these security flaws we plan to adhere to a Defense-in-Depth design and use layered security to overcome the weaknesses within OWA. To overcome OWA single factor authentication we will require our OWA users to use passwords that are at least 7 charters. We will require that their passwords be complex using uppercase, lowercase, numbers and special charters. All OWA users will be required to change their passwords every 60 days. We will enforce a 5 attempt lockout policy that will require the user to call tech support to get the account reset if they become locked out. These steps will help protect against brute force guessing attacks. To help protect against social engineering attacks, all OWA users will be instructed that at no time should they give out their password. They will also be informed that GIAC's technical support staff will never contact them via phone or email requesting their password. If they receive such a request they should not respond to it and should report it to our security staff. GIAC's technical support staff will not have the ability to view user passwords. If a user forgets his/her password our technical support staff can reset the password but the user must be able to answer two predefined questions such as mother's maiden name and date of birth. To help protect against flaws in IIS and the Windows operating system that OWA runs on we will harden the OS, install the latest patches and close all non-essential ports.

GIAC Partners

GIAC Enterprises has two partners that translate and resell fortunes. These partners need to be able to connect to GIAC Enterprises securely over the Internet to download large amounts of data. To achieve this goal our two partners will connect to our internal network via a VPN connection. We will utilize the Mobile User VPN (MUVPN) software bundled in with our Watch Guard firewall. Watch Guard's MUVPN software uses128 bit 3Des encryption and two factor authentication. Although the MUVPN software we plan to use provides a high level of security for our connection with our partners, it does have some security holes that need to be addressed.

One of our major concerns about the use of VPNs is the possibility of opening a backdoor for an attacker to use. VPNs were designed to allow remote users and networks to connect to local recourses just as if they were on the local network themselves. From a user's stand point this is great because it allows them to work just as if they were plugged directly into the local network. From a security stand point it can be a nightmare because it creates another network that must be secured. In our case we have an added level of complexity in that we have no control over our partner's network. A security breech in their network could lead to a security breech in our network.

To overcome this vulnerability we will again rely on a defense-in-depth design using layered security. Since these remote hosts only need access to our database server all other access will be denied and logged. Remote hosts will only be allowed to connect to the database server via SQL port 1433 to export fortune cookie sayings. All other access will be denied and logged.

GIAC Internal Enterprise Employees

GIAC internal employees will be located behind the trusted port of the Watch Guard firewall. All internal employees will have standard Internet access which will include HTTP, HTTPS, and FTP. To reduce our exposure to Worms, Back Doors, and P2P file sharing programs all other access to the Internet via client workstations will be denied. All browsing by our internal users will be controlled via the X1000's HTTP proxy service. We will utilize this service to remove client connection information, deny Java and ActiveX applets, and to remove unknown headers. Enabling these controls can cause some business related web browsing to function improperly, especially denying Java and ActiveX applets. These sites will be handled on a case by case basis. Internal workstations will have limited access to the Service network; this will include HTTP and HTTPS. This will allow our internal users to access both our company's website and OWA. Restricting internal user's access to our service network helps us adhere to a Defense-in-Depth design by only allowing what is needed and denying the rest.

Internal and external DNS requests will be handled by our Windows 2003 domain controller. It will house our internal domain name GIAC.int. Resolution requests for all other domain names will be forwarded to our ISP's DNS servers. Allowing our domain controller to run a service that needs to connect to hosts on the Internet is a security risk. Although it is a good idea to run our internal DNS services on a stand alone server, budgetary reasons will not permit us to add any new servers at this time. So to reduce our risk we will unitize the X1000's DNS proxy service. We will also restrict DNS traffic to only be allowed from our DNS server to our ISP's DNS servers.

In order for our Exchange Front-end server and our cookie database server to function properly they will need to be able to communicate with the servers on our internal network. The Exchange Front-end server will need two-way communication to both the Exchange Back-end server and the Windows 2003 Domain controller. Only the ports required will be opened and access will be controlled via IP address of the servers. Our internal accounting server will need to be able to import data form the cookie database server on the service network. Only the accounting server will be able to make the connection and only on SQL port 1433.

GIAC Mobile and Teleworkers Employees

GIAC Enterprises has a mobile work force which is made up of 5 sales people that travel the world finding new clients. These 5 employees need secure access to both their email and to their files stored on GIAC Enterprises internal network. Some of the problems presented by these users include the fact they are on the road 95% of the time, many lack any technical know-how and the majority of the time they have to use dial-up connections for Internet access. Using Watch Guard's MUVPN software would allow these users to connect to our network securely, but would also introduce some significant problems. Since the sales force spends over 95% of their time out of the office we would have very little control over their laptops. That combined with the users lack to technical skill would make these laptops a high risk to our network. Also, running MUVPN over dialup connections can be painfully slow if not impossible at times.

To overcome these problems and still meet the needs of our mobile sales force we will utilize a new feature built into Outlook 2003 and Exchange 2003, RPC over HTTP. For security the traffic will be secured using 128 bit SSL encryption. Our sales force will have access to both internal and external email and also shared resources through Public Folders. Some advantages of using this type of connection include ease of use, a limited attack window for our internal network and better performance over dialup. Most office workers are familiar with Outlook or other groupware products like it. The only port the sales force will require access to is SSL (443), which means that if one of the sales person's laptops were to become compromised an attacker would only have a limited window within to attack our internal network.

General Public

GIAC Enterprises hosts a website that the general public will need access to. To achieve this goal we will allow any host to access our web server via port 80 (HTTP). All other access will be denied and logged. Although external hosts will have limited access to this server there are still some vulnerabilities that need to be addressed. The website is hosted on Microsoft's Internet Information Server 6 (IIS6), a web server with a history of known exploits. Although Microsoft has made a lot of effort to make IIS more secure, new vulnerabilities are found every month. To reduce our risk to possible compromise via vulnerabilities in IIS we will adhere to a patch management system that keeps our server up-to-date with the latest Service Packs and Hotfixes. The server that IIS runs on will be hardened. All nonsensical services will be removed or disabled. The local administrator account will be renamed and the password will be changed every thirty days.

Network Architecture

External DNS

Our External DNS name is a critical part of our business and if our clients are unable to resolve our DNS name they will be unable to make purchases from us. Since this service is a critical part of our business and we lack any in-house expertise on securely hosting a public DNS server, we have decided to outsource this service to a company that specializes in this type of service. One of our major requirements is that the company hosting our DNS does not allow zone transfers.

Internet Connection

Our Internet connection is a T1 line provided by a local ISP. The T1 line terminates in a locked equipment room, that only the IT staff and a few managers have access too.

Filtering Router

Our external router is a Cisco 1720 router. We chose the Cisco 1720 for its reliability, speed, and price. Since we have decided to implement a two firewall network design we will allow our external Pix firewall to filter most unwanted incoming connections. This will reduce the load on our external router and allow it to do what it does best, which is to forward packets. We will however filter out some absolutes with the router. Our external router will be configured to block private addresses, ICMP redirects, broadcasts, BOOTP/DHCP, and our own IP addresses from entering the external interface of the router. Although both internal firewalls will be configured to block outgoing spoofed IP address, our external router will also block any outgoing connection that does not have a source address of our internal network. Modification of our router will be done through the use of a console cable. Access via Telnet will be disabled. All nonessential services will be disabled. The latest IOS version, 12.2, will be installed on the router and be kept up-to-date as new versions are released.

Pix Firewall

The first firewall in our network design is a Cisco PIX 515E, running IOS 6.23. The PIX 515 is a stateful inspection firewall. One of the main reasons we chose the PIX as our external firewall is speed. It can deliver up to 188Mbps of firewall throughput.[1] Another reason we chose the PIX as our external firewall is reliability. Our external firewall will be our first major line of defense from the bad guys. Our external firewall will be expected to withstand and block most of the attacks launched against our network. Cisco's IOS and Adaptive Security Algorithm (ASA) have a proven track record when it comes to protecting networks.

Our External firewall will be configured to only allow traffic in and out that is required to do business. All allowed and blocked traffic will be logged to a syslog server. Logs will be viewed on a regular basis. The latest IOS version will be installed and new versions will be applied as they are released. Modifications to the PIX will be done through the console port.

Watch Guard Firewall

The seconded firewall in network design is a Watch Guard X1000, running WatchGuard System Manager 7.2 Strong Encryption. The X1000 provides both statefull inspection and proxy services. It can provide proxy services for applications such as HTTP, SMTP, FTP, and many more. The X1000 runs on a 1.26 GHz Intel-Based Processor and has 256mb of ram. It can support transfers speeds upto 225 Mbps.

Like many companies cost was a major factor in our decision making process. The Watch Guard X1000 was designed as an all-in-one security appliance. It includes features such as user authentication, application proxies, Intrusion Prevention, Intrusion Detection, secure logging, content filtering, and reporting features. The vantage to this type of firewall is that we are able to utilize security features that we could not otherwise afford to deploy. Although these added features increase the overall security of our network, there is a disadvantage in putting all of our eggs in one basket. For example a failure in

[1] http://cisco.com/en/US/products/hw/vpndevc/ps2030/ps4094/index.html

one service could disrupt our entire network. When the budget and time permit we will offload content filtering, user authentication, and application proxies to standalone devices. Another reason we chose the X1000 is its bundled support for both Branch Office VPN and Remote user VPN. VPNs are a critical part of our network design. The X1000 supports 500 Branch Office VPNs and 50 remote user VPNs, at no added cost.

External Interface – Port 1 (X1000)

The External Interface is one of the ethernet ports on the X1000 that will connect to the Inside Ethernet port on the Pix. The only host that will reside in this security zone is a workstation station running Linux RedHat 9.0 and Snort v2.1.2.

Internal Network – Port 2 (X1000)

Port 2 on the X1000 will connect to our internal network. It will house all internal users, our logging servers, Domain Controllers, the Exchange Back-end server, and our accounting server.

Service Network – Port 3 (X1000)

Port 3 on the X1000 will connect to our service network. It will house our Exchange Front-end server and cookie saying database server.

Intrusion Detection

For intrusion detection GIAC Enterprises will deploy a layered approach; utilizing both network and host monitoring. Snort V2.1.2[2] will be deployed between our external firewall and our internal firewall. We chose to deploy our sensor in this location to reduce the number of false positives our IT staff would have to wade through. Traffic passing between the two firewalls is very limited; therefore tuning the sensor to reduce false positives should not be too intensive. Also, placing the sensor in this location will help with auditing our internal and external firewalls to insure that no unwanted traffic is being allowed out by the internal firewall or allowed in by the external firewall. Snort will be loaded on a small server running Redhat 9.0. Only the required services will be loaded on the server. Software updates will be applied to this server as soon as they are released and tested. Swatch[3] will be used for real-time alerting. Since the location of our IDS allows for a low level of false positives all alerts will be

[2] http://www.snort.org/dl/binaries/linux/
[3] http://swatch.sourceforge.net/

emailed to the three IT staff members responsible for incident response. For an added layer of security GIAC Enterprises will deploy GFI's LANguard Security Event Log Monitor[4] on all servers. LANguard S.E.L.M. provides host based intrusion detection by monitoring Windows event logs and alerting suspicious activity. The program can also be used to pull all of the event logs to one location for review. Being able to view and compare all of our server's security logs enables us to better identify a possible security breech.

Logging servers

We plan to use two old servers for logging purposes. One server will house our syslog server and the other server will house our WatchGuard management and logging server. Both servers have been equipped with CDRW drives. Both servers will have their logs backed up to a CD on a weekly basis. Once a hacker gains access to a network the first thing he/she will want to do is try to cover their tracks. Our logging servers will be a prime target. Backing up our logs to CD will allow us to have a temper proof record of the traffic entering and exiting our network. If a hacker were to compromise our network we could rely on these logs to trace his/her actions, provide evidence in a criminal case or provide a state of last known good.

Virus Protection

Virus prevention and protection is a major concern in GIAC Enterprises network design. Our firewall policies will block most worms from entering our network form the Internet. Our firewall policies also help ensure that if a host or hosts on our network were to become infected their ability to attack other networks is very limited, since we are only allowing limited out going traffic. To prevent internal host from becoming infected we will run Norton Enterprise Edition 9.0[5] on all workstations and servers.

SMTP Proxy

Many of today's exploits enter closed networks through email. It is much harder to find and exploit holes in a firewall than it is to trick a user into running a virus or trojan laden attachment. To help reduce our exposure to email born attacks we will utilize the Watch Guard firewall SMTP proxy service to block possible harmful file attachments. Attackers may also try to use brute force password guessing programs against our mail server to gain access to our network or to relay off our mail server. Since we have no requirement for external users to relay mail off our mail server we will block the ESMTP AUTH command. Also, all unknown headers will be blocked.

[4] http://gfi.com/lanselm/

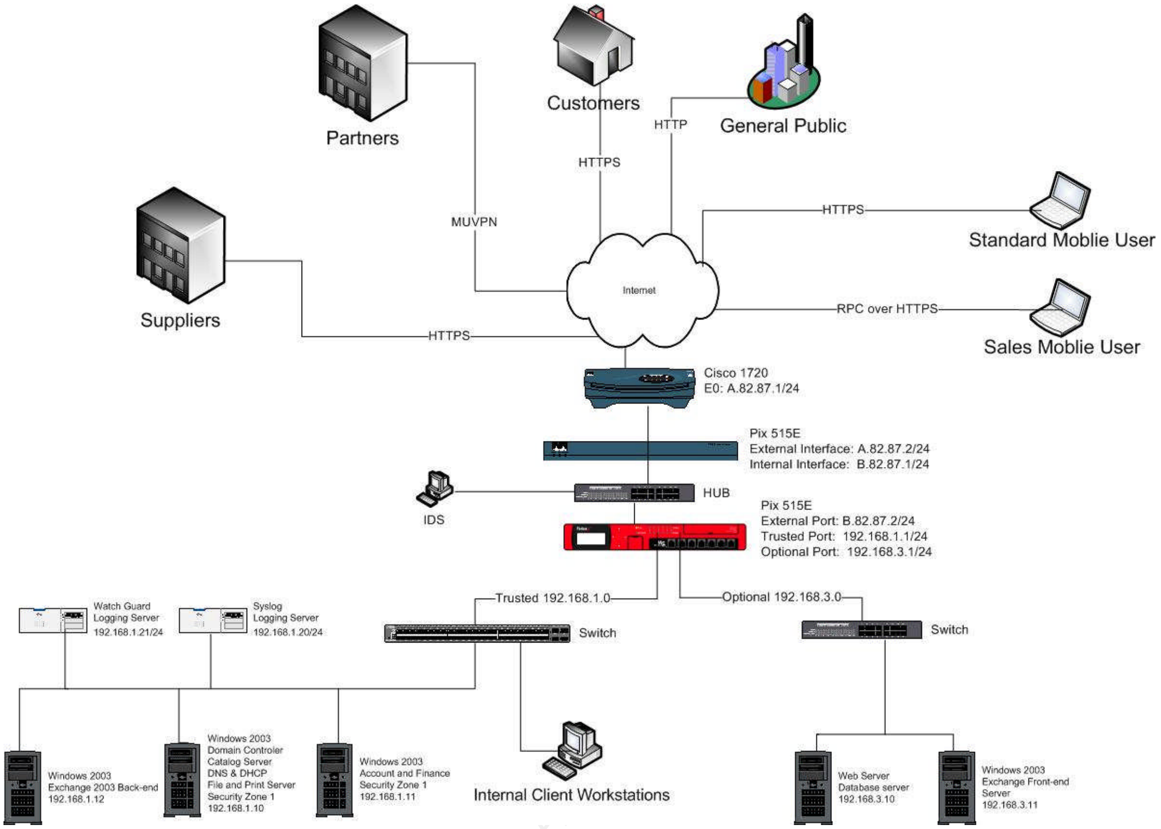
[5] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=64&EID=0

Defense-in-Depth Discussion

Defense-in-Depth adheres to the fact that nothing in network security is 100% effective. As fast as we come up with ways to protect our networks the bad guys come up with ways to get around our defenses. Since there is no single magical device that can be used to protect a network, Defense-in-Depth prescribes a layered approach that utilizes different types of hardware, software and procedures to provide protection. In an ideal design the layers should complement each other, providing protection for another layer's weakness. Another major principle in Defense-in-Depth is that things change fast. The bad guys are always updating and adding new tools to their arsenal, internal and external users require new services, new software is added to the network and old programs are updated. A network that was secure a year may no longer provide the protection it once did. Defense-in-Depth prescribes that a network must continuously be monitored, tested, updated and modified to maintain a high level of security.

GIAC Enterprises adheres to Defense-in-Depth principles by using layered security to avoid a single point of failure. A filtering router will be deployed to help filter out traffic that should never be allowed into a closed network. Two different types of firewalls will be deployed to provide stateful packet inspection and proxy services. Our two firewall design gives a higher level of protection in that a security vulnerability in one device does not leave our entire network exposed. We will log incoming and outgoing traffic. We will also run periodic tests against our network to insure that there are no holes or mistakes in our configuration. GIAC Enterprises network security will modified as new treats emerge.

Network Diagram



Assignment 2 – Security Policy and Component Configuration

Note: I did not have access to a Cisco router or a Cisco Pix firewall during the writing of this practical. I did have limited access to a WatchGuard X1000 firewall, but could not save any changes to the X1000.

IP Address Assignment

Filtering Router	E0 Interface	A.82.87.1/24
Pix External Firewall	Outside Interface	A.82.87.2/24
Pix External Firewall	Inside Interface	B.82.87.1/24
X1000 Internal Firewall	External Interface	B.82.87.2/14
X1000 Internal Firewall	Trusted Interface	192.168.1.1/24
X1000 Internal Firewall	Optional Interface	192.158.3.1/24

Filtering Router

For our filtering router we are using a Cisco 1720 running IOS 12.2(24). We will start by setting the host name, enabling logging, and setting access passwords, followed by disabling unneeded services and configuring access-lists.

Following the Defense-in-Depth principles we will not give away any clues as to the use of a device by its host name.

```
cisco(config)#hostname sam1
```

Enable logging

```
sam1(config)#logging 192.168.1.20
```

The console password controls unprivileged access to the router via the console port on the back of the router. In order to connect by this method a user must have access to a computer that is physically connected to the router’s console port. Since a user must have access to a computer that is physically connected to the router, the console password may not seem like an important password to set. But a remote user may be able to again access via a computer running remote control software such as PCAnyWhere, Terminal Services or Remote Desk.

```
sam1> enable

sam1# config t

sam1(config)# line console 0

sam1((config-line)#password Run Jack run!

sam1(config-line)#login
```

Instead of using hard to remember passwords such as ty11@Tyu5Tjks, I have chosen to use a simple phrase. A phrase such as “Run Jack run!” has 13 characters including two uppercase, one special character and two open spaces. It may seem like a password like this would be easy to crack since it is made up of three words found in the dictionary, but to a password cracking program the phrase is seen as one word. It is as though to crack as the first password, but much easier to remember.

The next password we will set is the Enable password. The Enable password controls privileged access to the router.

```
sam1> enable

sam1# config t
```

```
sam1(config)#enable secret We will meet@9
```

Our next step will be to insure that telnet connections are disabled. Telnet connections transmit usernames and passwords in clear text. Since our policy states that all configuration of the router will be done via console access this service is not required.

```
sam1(config)#line vty 0 4

sam1(config-line)#login
% Login disabled on line 6, until 'password' is set
% Login disabled on line 7, until 'password' is set
% Login disabled on line 8, until 'password' is set
% Login disabled on line 9, until 'password' is set
% Login disabled on line 10, until 'password' is set
```

By default this service should be disabled but it is a good idea to check. If you need to disable this service use the following commands.

```
sam1(config)#line vty 0 4

sam1(config-line)#login
sam1(config-line)#no password
```

The next step in the process will be to disable any unneeded services. Although many of these services present no security risk at this time, they may become venerable to attack sometime in the future. Rather then run the risk of getting caught off guard it is better to disable these services until they are required.

```
sam1(config)#no service finger
sam1(config)#no cdp run
sam1(config)#no ip source-route
sam1(config)#interf s0
sam1(config-if)#no ip http server
```

Now we will create and apply both the incoming and outing access lists.

Block broadcasts, multicasts, loopback addresses, and ICMP redirects. Since this type of traffic is so common on the Internet it will not be logged.

```
sam1(config)#access-list 101 deny ip 224.0.0.0 31.255.255.255 any
sam1(config)#access-list 101 deny ip host 0.0.0.0 any
sam1(config)#access-list 101 deny icmp any any redirect
sam1(config)#access-list 101 deny ip 127.0.0.0 0.255.255.255 any
```

Block internal IP addresses commonly used to by attackers. Again this type of traffic is so common on the Internet it will not be logged.

```
sam1(config)#access-list 101 deny ip 192.168.0.0 255.255.0.0 any
sam1(config)#access-list 101 deny ip 172.16.0.0 255.255.0.0 any
sam1(config)#access-list 101 deny ip 10.0.0.0 255.255.255.0 any
```

Block hosts spoofing our IP address range. This type of traffic could alert us to a targeted recon or possible attack on our network. Therfore denied packets will be logged.

```
sam1(config)#access-list 101 deny ip A.82.87.0 255.255.255.0 any log
sam1(config)#access-list 101 deny ip B.82.87.0 255.255.255.0 any log
```

Block and log unknown hosts from connecting to the IDS server.

```
sam1(config)#access-list 101 deny ip any host B.82.87.2 log
```

Allow in all other traffic.

```
sam1(config)#access-list 101 permit ip  any any
```

Apply access-list to serial interface 0

```
sam1(config-if)#ip access-group 101 in
```

Configure and apply outgoing access-list. Only the three IP addresses assigned to the WatchGuard firewall will be allowed to make outgoing connections. All other connections will be denied and logged.

```
sam1(config)#access-list 102 permit ip host B.82.87.2 any log
sam1(config)#access-list 102 permit ip host B.82.87.3 any log
san1(config)#access-list 102 permit ip host B.82.87.4 any log
sam1(config)#access-list 102 deny ip any any log
```

The last step will be to save our changes to the router.

```
sam1# copy run start
```

External Pix Firewall

As an external firewall we will use a PIX 515E running Cisco IOS 6.2. The primary purpose of this firewall is to block all incoming and outgoing traffic unless specifically defined.

The first step will be to change the hostname of the firewall. Again following the Defense-in-Depth principles the host name will not give any clause as to the purpose of the device.

```
Pix> enable
Pix# config t
Pix(config)# hostname mac1
```

The second step will be to configure the enable passoword.

```
mac1> en
mac1# config t
mac1(config) enable password Jump Jim Jump!
```

The next step will be to disable NAT. NAT will be handled by the WatchGuard X1000 firewall.

```
mac1(config)# access-list no-nat permit ip any any
mac1(config)# (inside) 0 access-list no-nat
mac1(config)# (outside) 0 access-list no-nat
```

Next we will enable and configure logging. Our syslog server is behind the internal X1000 firewall. Syslog messages will be sent to the external interface of the X1000 and then NATed into the syslog server. Since we have a mordorate traffic load on the pix and syslog server with a large hard drive we will set the logging to the highest level so that we can record all incoming and outgoing traffic.

```
mac1(config)# logging on
mac1(config)# logging host B.82.87.2
mac1(config)# logging trap 7
```

Now we will disable unneeded fixup protocol handling features. These protocols will be secured by the X1000's proxy services. Leaving these fixup protocols enabled could make trouble shooting proxy problems difficult; it could also cause conflits.

```
mac1(config)# no fixup protocol ftp 21
mac1(config)# no fixup protocol http 80
mac1(config)# no fixup protocol smtp 25
```

Now it is time to configure and apply incoming and outgoing access lists.

Incoming access-list:

The first rule in our incoming access-list will permit our clients to access the fortune cookie sayings database. Since this rule will receive the most hits it will be the first rule in our incoming access-list.

```
mac1(config)# access-list incoming permit tcp any host B.82.87.3 eq https
```

The second rule in our incoming access-list will allow the general public access to our website.

```
mac1(config)# access-list incoming permit tcp any host B.82.87.3 eq www
```

Next we will allow incoming e-mail and incoming Outlook RPC over HTTPS traffic.

```
mac1(config)# access-list incoming permit tcp any host B.82.87.4 eq smtp
mac1(config)# access-list incoming permit tcp any host B.82.87.4 eq https
```

Now we need to allow in VPN traffic to the WatchGuard X1000 firewall.

```
mac1(config)# access-list incoming permit udp any host B.82.87.2 eq 500
mac1(config)# access-list incoming permit tcp any host B.82.87.2 eq 50
mac1(config)# access-list incoming permit tcp any host B.82.87.2 eq 51
```

Outgoing access-list:

Allow traffic from incoming access-list back out.

```
mac1(config)# access-list outgoing permit tcp host B.82.87.3 any eq https
mac1(config)# access-list outgoing permit tcp host B.82.87.3 any eq www
mac1(config)# access-list outgoing permit tcp host B.82.87.4 any eq smtp
mac1(config)# access-list outgoing permit tcp host B.82.87.4 any eq https
mac1(config)# access-list outgoing permit udp host B.82.87.2 any eq 500
mac1(config)# access-list outgoing permit tcp host B.82.87.2 any eq 50
mac1(config)# access-list outgoing permit tcp host B.82.87.2 any eq 51
```

Allow outgoing traffic from internal network.

```
mac1(config)# access-list outgoing permit tcp host B.82.87.2 any eq 53
mac1(config)# access-list outgoing permit tcp host B.82.87.2 any eq www
mac1(config)# access-list outgoing permit tcp host B.82.87.2 any eq ftp
mac1(config)# access-list outgoing permit tcp host B.82.87.2 any eq https
```

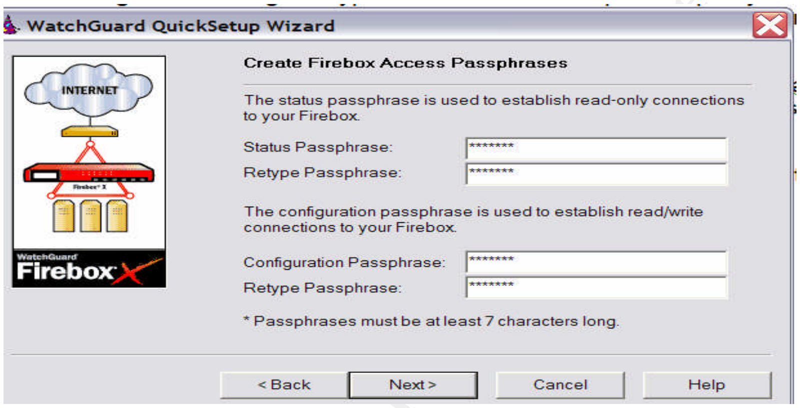
Now we need to save our changes to the pix firewall.

```
mac1(config)# write memory
```

Internal WatchGuard Firewall
For our internal firewall we will use a WatchGuard X1000 running WatchGuard System Manager 7.2 Strong Encryption. The X1000 will provide proxy services for HTTP, SMTP, and FTP. It will also be used to segment our network and terminate VPN connections.

The X1000 is managed by WatchGuard's Firebox System Manager software. The Firebox System Manager software must be loaded on a server or workstation running Windows NT, XP, 2000 or 2003.

During the installation of the System Manager software we will be asked to enter a Status Passphrase and a Configuration Passphrase. We will also need to set our internal and external IP addresses. The status phrase allows you to access the System and Policy manager to view settings and make changes. In order for the changes to take affect you must use the Configuration phrase to save the settings to the X1000


WatchGuard QuickSetup Wizard

Create Firebox Access Passphrases

The status passphrase is used to establish read-only connections to your Firebox.

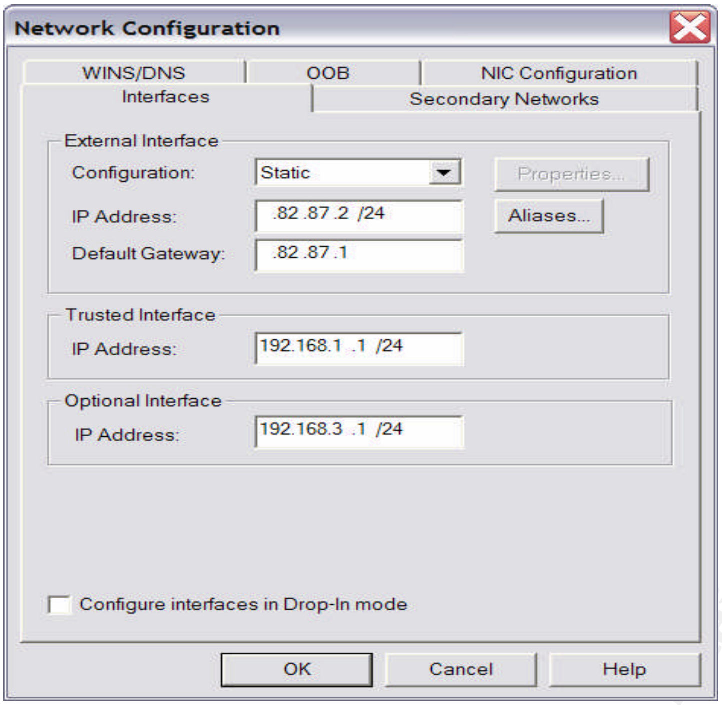
Status Passphrase: *******
Retype Passphrase: *******

The configuration passphrase is used to establish read/write connections to your Firebox.

Configuration Passphrase: *******
Retype Passphrase: *******

* Passphrases must be at least 7 characters long.

Set the internal and external IP addresses.



External Interface

Configuration: Static

IP Address: .82 .87 .2 /24

Default Gateway: .82 .87 .1

Trusted Interface

IP Address: 192.168.1 .1 /24

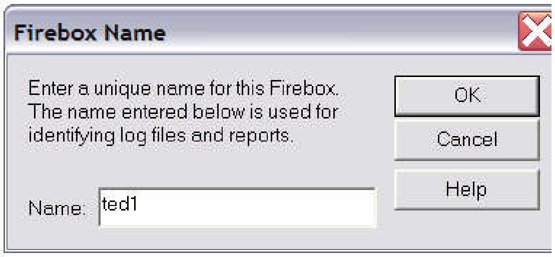
Optional Interface

IP Address: 192.168.3 .1 /24

□ Configure interfaces in Drop-In mode

Now that we have a basic configuration saved to the X1000 we can use the Policy Manager to modify the firewall to match our security policy.

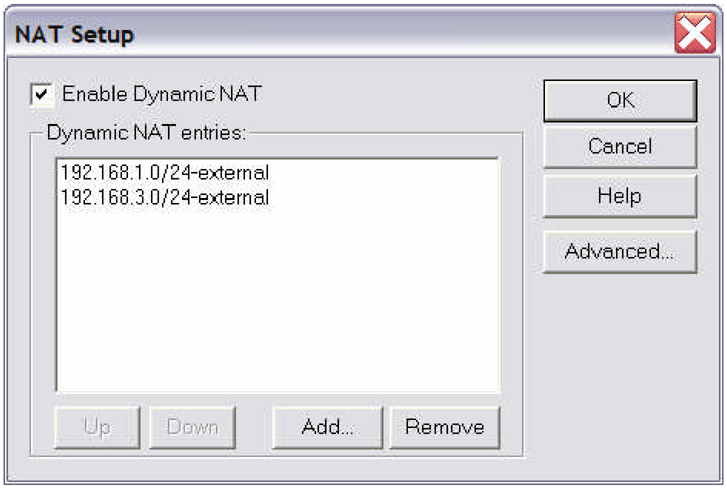
The first thing we need to do is to name the firewall. Again to adhere to our security policy the name of the firewall will not give away any information as to its role in our network.



Enter a unique name for this Firebox. The name entered below is used for identifying log files and reports.

Name: ted1

By default the X1000 will perform NAT for the internal IP addresses 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8. Since our security policy states that the X1000 should prevent internal hosts with spoofed IP addresses from making connections to the outside world, the X1000's default NAT policy will need to be changed.



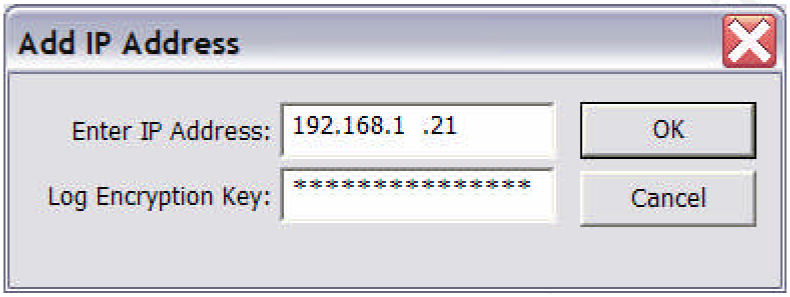
NAT Setup

☑ Enable Dynamic NAT

Dynamic NAT entries:

192.168.1.0/24-external
192.168.3.0/24-external

Now we need to set the logging server and the encryption key.

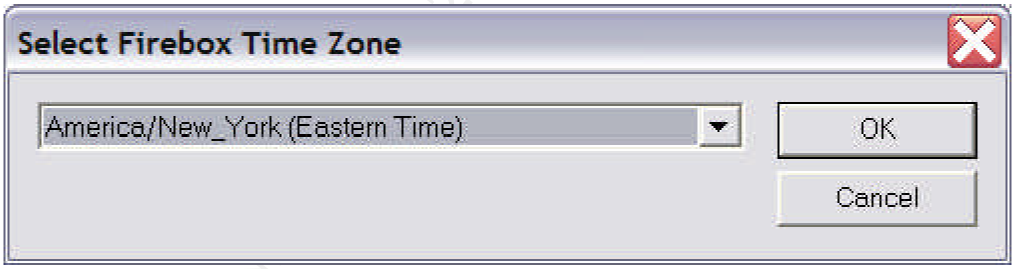


Add IP Address

Enter IP Address: 192.168.1 .21

Log Encryption Key: ***************

To ensure that our logs have the correct time we must set the correct time zone.



Select Firebox Time Zone

America/New_York (Eastern Time)

Now that we have the basics setup it is time to configure the rules to allow traffic in and out of our network. By default the X1000 blocks incoming and outgoing traffic unless there is a rule defined to allow it. A rule has three settings; enabled and allowed, enabled and denied, and disabled. On rules that we plan to use for outgoing traffic only we will set the incoming portion of the rule to disabled. We could set the rule to enable and denied, but this could cause a conflict later down the road if another rule is added to allow in traffic that the first rule is blocking.

The first rule will allow HTTPS incoming to our fortune cookie sayings database server and to our Exchange front-end server. It will also allow internal clients to make outgoing HTTPS connections.

Rule Name: HTTPS
Port: 443

__**Incoming**__
From: Any

To:
NAT B.82.87.3 → 192.168.3.10
NAT B.82.87.4 → 192.168.3.11

__**Outgoing**__
From: Any

To: Any

__**Logging**__
Incoming:
Allowed
Denied

Outgoing:
Allowed
Denied

The default log setting for the X1000's rules is to only log denied connections. To ensure that we get a clear picture of the traffic entering and leaving our network we will log both allowed and denied connections.

The next rule will allow external hosts to connect to our web server via HTTP. It will also allow our internal clients to make outgoing HTTP connections.

Rule Name: HTTP
Port: 80

__**Incoming**__
From: Any

To:
NAT B.82.87.3 → 192.168.3.10

__**Outgoing**__
From: Any

To: Any

Logging
Incoming:
Allowed
Denied

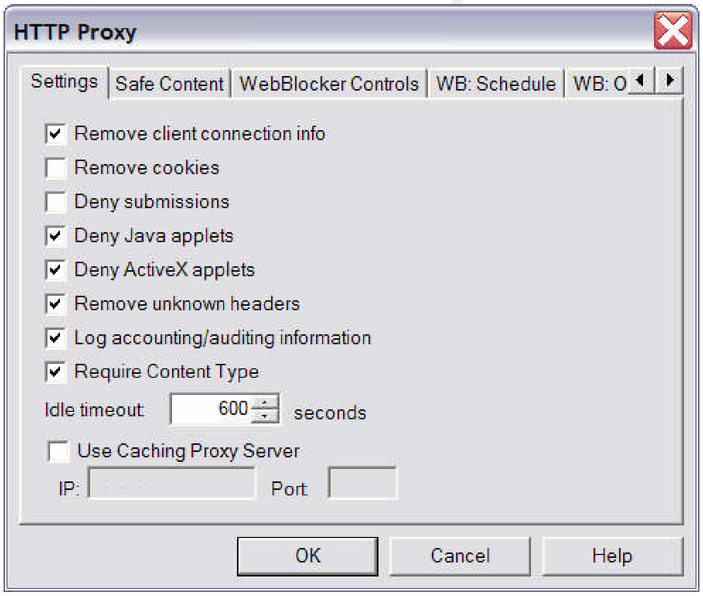
Outgoing:
Allowed
Denied

Since most networks allow their internal clients to have access to the Internet via HTTP/80, the bad guys have come up with ways to exploit flaws in common Web Browsers to load spyware, viruses and even backdoor programs. To reduce the added security risks of allowing our clients to have Internet access we will utilize the X1000's HTTP proxy service to protect our client connections.

Proxy Setttings

The settings we will change to enhance our security include

- **Removing client connection information to help reduce the amount of information about our network that passes to external hosts.**
- **Deny Java and ActiveX applets, both programs capable of loading spyware and Trojan programs.**
- **Remove unknown headers to help protect against IE exploits.**
- **Log accounting/auditing information**
- **Set the idle timeout to reduce the risk of DOS attacks.**



☑ Remove client connection info
□ Remove cookies
□ Deny submissions
☑ Deny Java applets
☑ Deny ActiveX applets
☑ Remove unknown headers
☑ Log accounting/auditing information
☑ Require Content Type
Idle timeout: 600 seconds
□ Use Caching Proxy Server
IP: . . . Port:

The next two rules will allow email in and out of our network. All incoming and outgoing email will be handled by our Exchange Front-End server. Incoming email will be processed by the X1000's SMTP proxy service. Outgoing email will be handled by the X1000's SMTP packet filter. The reason for using the packet filter on outgoing email is that the X1000's SMTP proxy service has problems communicating with some email servers. Since our major security concerns come from outside email entering our trusted network and it is critical that outgoing email reaches our clients without any disruptions we will not use the SMTP proxy services for outgoing email.

Rule Name: Incoming_SMTP
Port: 25

<u>Incoming</u>
From: Any

To:
NAT B.82.87.4 → 192.168.3.11

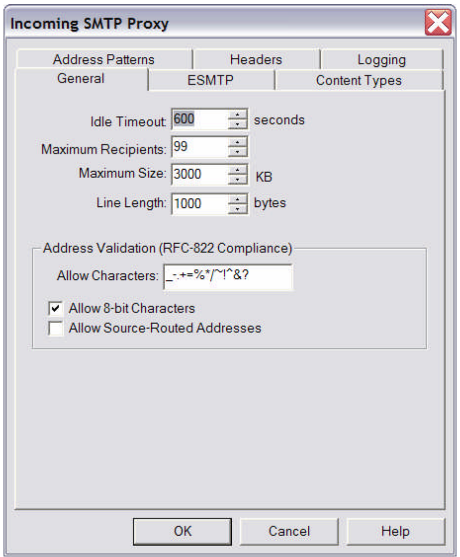
<u>Outgoing</u>
Disabled

<u>Logging</u>
Incoming:
Allowed
Denied

<u>Proxy Settings</u>

The settings we will change to enhance our security include.

- Setting the idle timeout to help protect against DOS attacks.
- Setting the maximum number of recipients which will help reduce incoming spam and some worms.
- Block unused ESTMP commands which could be used to relay off our mail server.
- Deny unsafe file attachments which could carry viruses, worms or trojans.
- Deny unknown headers that could help protect against application exploits.



Idle Timeout: 600 seconds

Maximum Recipients: 99

Maximum Size: 3000 KB

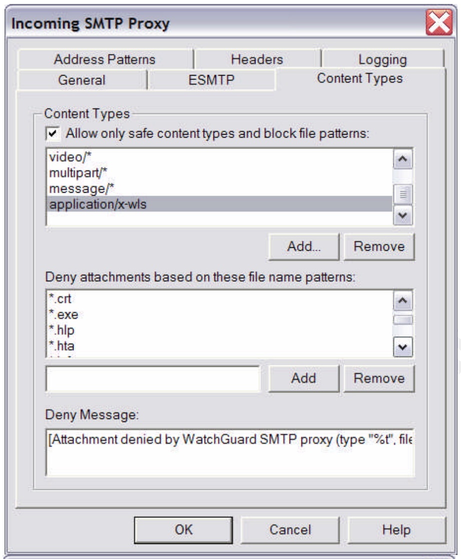
Line Length: 1000 bytes

Address Validation (RFC-822 Compliance)

Allow Characters: _-.+=%*/~!^&?

☑ Allow 8-bit Characters

□ Allow Source-Routed Addresses



Content Types

☑ Allow only safe content types and block file patterns:

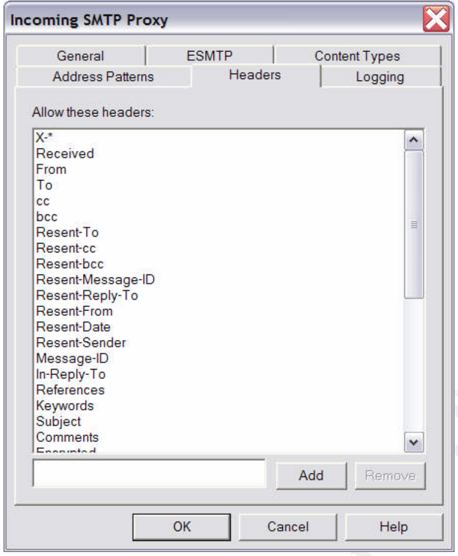
video/*
multipart/*
message/*
application/x-wls

Deny attachments based on these file name patterns:

*.crt
*.exe
*.hlp
*.hta

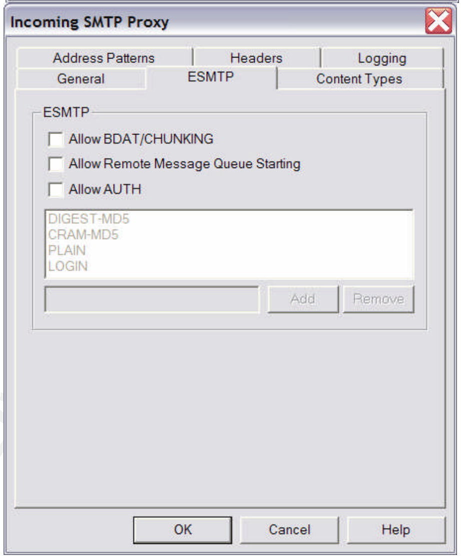
Deny Message:

[Attachment denied by WatchGuard SMTP proxy (type "%t", file



Allow these headers:

X-*
Received
From
To
cc
bcc
Resent-To
Resent-cc
Resent-bcc
Resent-Message-ID
Resent-Reply-To
Resent-From
Resent-Date
Resent-Sender
Message-ID
In-Reply-To
References
Keywords
Subject
Comments



ESMTP

□ Allow BDAT/CHUNKING

□ Allow Remote Message Queue Starting

□ Allow AUTH

DIGEST-MD5
CRAM-MD5
PLAIN
LOGIN

Rule Name: Outgoing_SMTP
Port: 25

Incoming
Disabled

Outgoing
From: 192.168.3.11

To: Any

Logging
Outgoing:
Allowed
Denied

The next rule will allow our internal DNS server to forward name resolution requests to our ISP's DNS servers. It will also allow the Exchange Front-End server and the Database server to query our internal DNS server for name resolution.

Rule Name: Outgoing_DNS
Port: 53

Incoming
From:
192.168.3.10
192.168.3.11

To: 192.168.1.10

Outgoing
From: 192.168.1.10

To:
C.152.0.8
C.152.16.8

Logging
Incoming:
Allowed
Denied

Outgoing:
Allowed
Denied

Our next rule will allow internal clients to make outgoing FTP connections.

Rule Name: Outgoing_FTP
Port: 21

Incoming
Disabled

Outgoing
From: Any

To: Any

Logging

Outgoing:
Allowed
Denied

Set the default WatchGuard rule to only allow the WatchGuard logging server to access the firewall from our internal network. Also set the rule to deny connections from the outside world. In our other rules the incoming settings were changed to disable for fear of conflicts later down the road. We never want external hosts to be able to make a connection to our firewall; therefore the incoming settings will be set to enabled and denied.

Rule Name: WatchGuard
Port: 4105, 4103

Incoming
Enabled and denied

Outgoing
From: 192.168.1.21

To: Any

Logging
Outgoing:
Allowed
Denied

Incoming:
Allowed
Denied

Our internal Accounting server needs to be able to import data to and from our fortune cookie database server. Only the Accounting server will be able to initiate the connection.

Rule Name: Acctsvr_Databasesvr
Port: 1433

Incoming
Disabled

Outgoing
From: 192.168.1.11

To: 192.168.3.10

Logging
Outgoing:
Allowed
Denied

Next is a custom rule created to allow communication between the Exchange Front-End, Back-End, Domain Controller servers.

Rule Name: Exchange_Frontend
Ports:
80/TCP
25/TCP
389/TCP
389/UDP
3268/TCP
88/TCP
88/UDP
135/TCP
1600/TCP

Incoming
From: 192.168.3.11

To: 192.168.1.10

Outgoing
From: 192.168.1.10

To: 192.168.3.11

Logging
Outgoing:
Allowed
Denied

Incoming:
Allowed
Denied

In order for our router and Pix firewall to be able to log to the internal syslog sever the traffic must be allowed and NATed into our internal network.

Rule Name: Syslog
Port: 514/UDP

Incoming

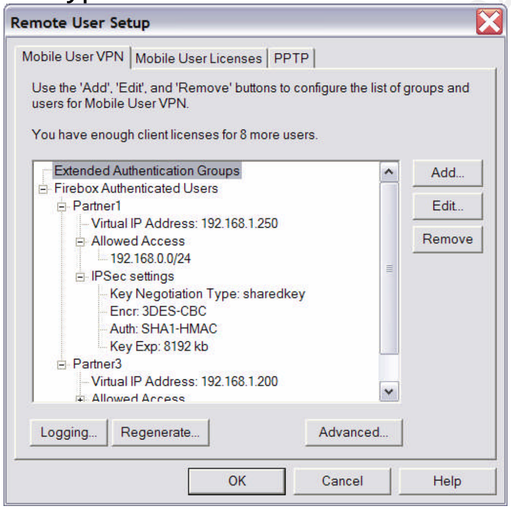
From:
A.82.87.1
B.82.87.1

To: NAT B.82.87.2 → 192.168.1.20

<u>Outgoing</u>
Disabled

<u>Logging</u>
Incoming:
Allowed
Denied

GIAC Enterprises has two partners that will need to connect via MUVPN to import large amounts of data. Two user accounts will be added to the firewall and both users added to a single group called Partners. This group will only have access to the fortune cookie database server via port 1433. Our partners will connect to our network via WatchGuard's MUVPN software. They will use a shared key for key negotiation, 3DES-CBC for encryption, and SHA1-HMAC for authentication. The type of data our partners are importing from our database server could be secured with a faster encryption method such single DES, but since speed is not an issue at this time we will utilize the more secure 3DES encryption method.



Use the 'Add', 'Edit', and 'Remove' buttons to configure the list of groups and users for Mobile User VPN.

You have enough client licenses for 8 more users.

```
Extended Authentication Groups
Firebox Authenticated Users
  Partner1
    Virtual IP Address: 192.168.1.250
    Allowed Access
      192.168.0.0/24
    IPSec settings
      Key Negotiation Type: sharedkey
      Encr: 3DES-CBC
      Auth: SHA1-HMAC
      Key Exp: 8192 kb
  Partner3
    Virtual IP Address: 192.168.1.200
    Allowed Access
```

Rule Name: Partners_DatabaseSRV
Port: 1433

<u>Incoming</u>
From: Partners

To: 192.168.3.10

Outgoing
From: 192.168.3.10

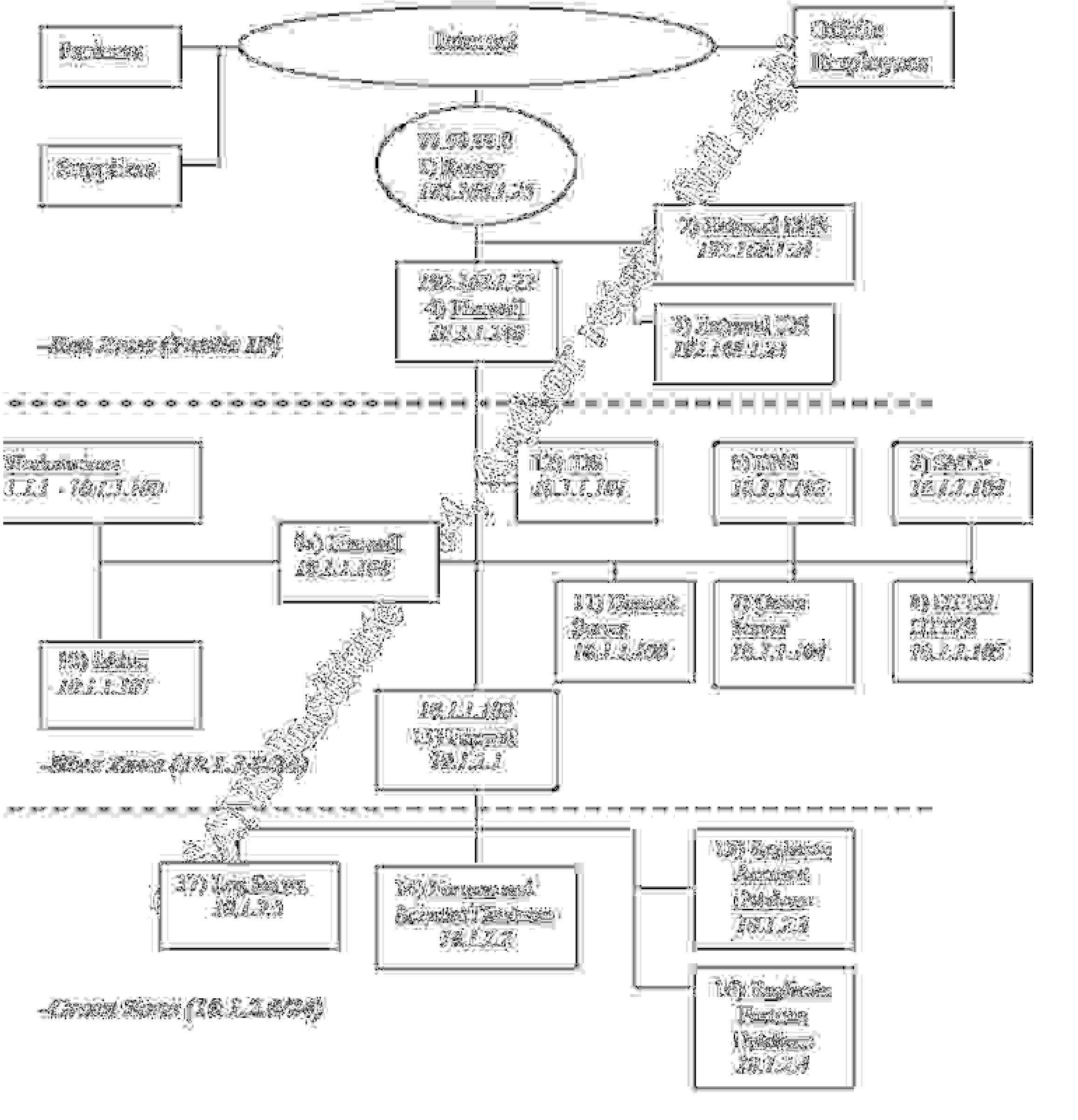
To: Partners

Logging
Outgoing:
Allowed
Denied

Incoming:
Allowed
Denied

Assignment 3 – Design Under Fire

In this portion of the practical I will assume the role of a hacker and try to penetrate another company's network. My goal will be to gain access to a system that is not accessible from the Internet. This attack will be entirely simulated and be will lunched against the practical. http://www.giac.org/practical/GCFW/Andy_Millican_GCFW.pdf.



I will follow the following rules during the simulated attack.

1. The attack must be realistic.

2. Any actions, procedures or technology not stated in the practical will be assumed to be nonexistent.

My attack will consist of the following three phases.

1. Reconnaissance: During this phase I will try to learn as much about the network as I can without drawing attention to my activities.

2. Planning: During this phase I will use the information I learned during my reconnaissance to find weaknesses within the target's network design that can be exploited.

3. Attack: The third and final phase will be to launch a simulated attack against the targeted network.

Recon

I will start my reconnaissance by checking Network Solutions Whois[6] database. The first thing that I will be looking for is that the domain name that I have for the company is actually their domain and not someone else's. Many companies have domain names that are similar and I would not want to attack the wrong site. The second useful piece of information that I can pull off the site is the technical contact's email address. Many companies will list an IT director or network administrator as their technical contact. Since many companies also use an employees first and last names in their email address it could be possible to find the name of someone within their IT staff.

One way to stop a hacker from gaining this type of information is to use a generic email account for this contact such as info@company.com or dnsadmin@company.com.

Now that I have verified that I have the correct domain name for my target, it is time to find some hosts belonging to their network. To do this I will use the DNSStuff.com website. The site has a whole list of tools that will allow me to probe my targets network without leaving any traces of my computer's IP address in their logs. From this site I will ping some common host names such as mail, FTP, POP, SMTP, and WWW to see which names get resolved and if any respond to my ping requests. I can also check the MX record to get the IP address of their mail server. I can also run a trace route to try a find the IP address of their Internet router or firewall.

Stopping hackers from gaining this type of information is very hard. You must have an MX record if you wish to receive email. You will also need to have valid host records if you plan to give Internet users access to services like FTP, POP3 and HTTP. In many cases it does not make sense to change a host's name from FTP too SVR1 in order to hide its role, but if it is a sensitive server and only a few users need access to it, it may make sense.

The next stage of my reconnaissance will require me to directly communicate with the target's hosts. To try to cover my tracks I will need a way to scan their network from a host or network other than my own. One method would be to use my local library. On a recent trip to the library I discovered that they had

[6] http://www.networksolutions.com/en_US/whois/index.jhtml

computers with Internet access for use by the general public. For security the computers were locked down so that no one could load any software on these machines. But the computers did still have both the CDROM and floppy disk installed and working. To use one of these computers to scan my targets network, I would just pop in a CDROM containing PHLAK[7] and power cycle the computer. If the computers were left with a default setting to boot off of the CDROM first, I would have a computer running Linux with Internet access. Since the workstations were somewhat locked down, we could assume that the admin took the extra step and set the computers to only boot from the hard drive and password protect the system BIOS. My next option would be to check into a hotel that has free high speed Internet access. Many small hotels provide high speed internet to guest rooms via a DSL or cable modem connection using a SOHO firewall to perform NAT and allow outgoing access. Many if not all of these types of connections allow all outgoing traffic and perform no logging. During my scans of the target's network the only IP address that would show up in their logs would be the hotels Internet connection's IP address. Since this address is on a residential type connection it is hard to trace. The only action the target's network admin would probably take if they were to become aware of my scanning activities would be to block the IP address of the hotel.

To scan the targets network I will use two programs, Nmap 3.5[8] and Superscan V4.0[9]. The reason for using two scanning engines is that one might find protocols or be able to finger print an OS that the other misses.

I will use the Windows version of Nmap to scan the target network.

c:\nmap –sS –vv –P0 –O 192.168.1.25 (note: In Andy's paper this internal address is considered a live public address.)

The –sS option sends a SYN packet to the target and then waits for either a ACK or RST. The primary advantage to this scanning technique is that fewer sites will log it[10].

The –P0 option tells Nmap not to ping the targeted host first. The reason I set this option is that some firewalls can and are set to auto block any host that tries to ping a host protected by the firewall. For example, the WatchGuard X1000 can be set automatically block an Internet host form communicating with an internal host for a set time period if the external host first tries to ping the internal host.

[7] http://www.phlak.org

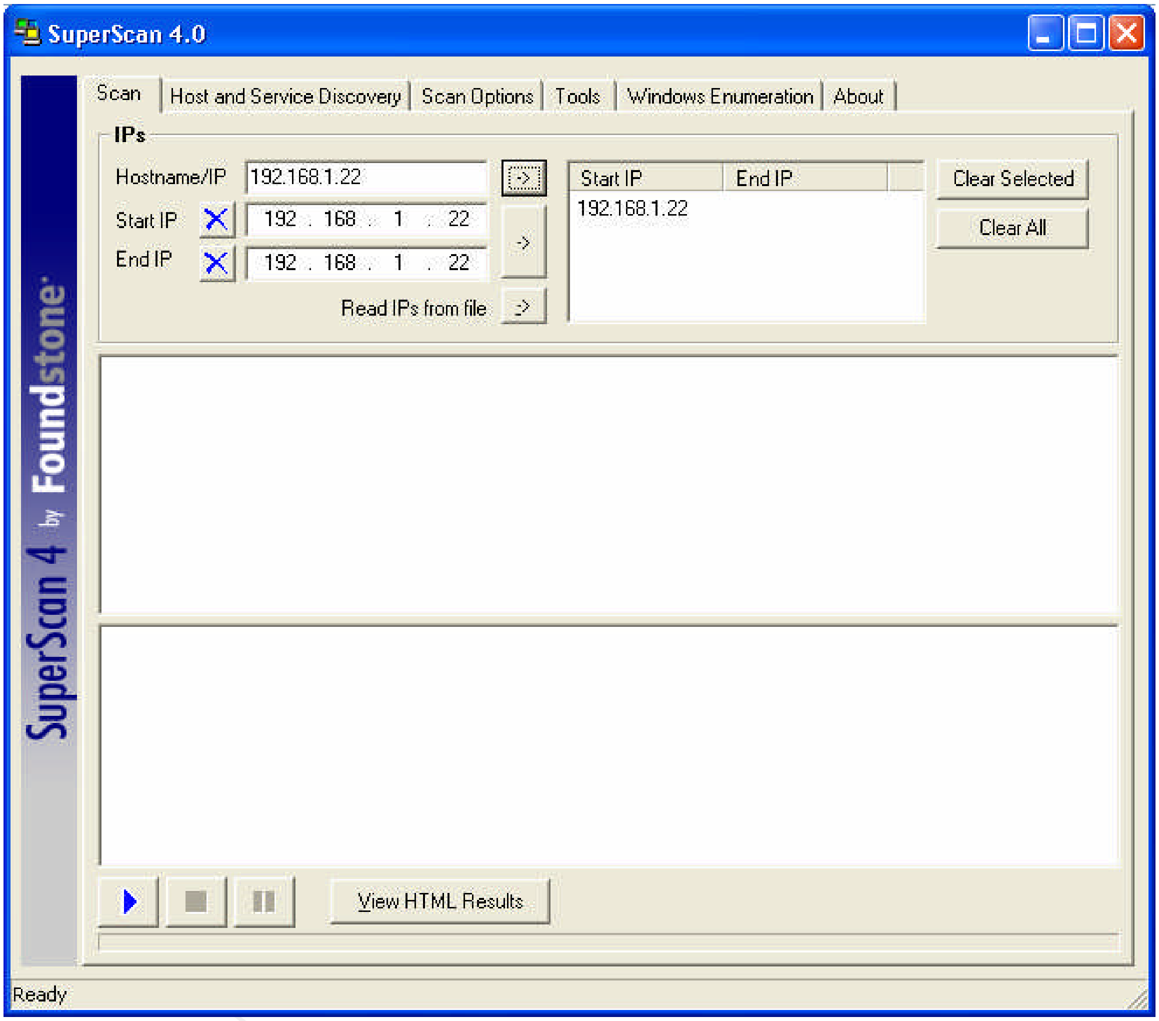
[8] http://www.insecure.org/nmap/

[9] http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm

[10] Fyodor. "The Art of Port Scanning". 6 Sep 1997. URL: http://www.insecure.org/nmap/nmap_doc.html#syn

The –O options tells Nmap to try and fingerprint the operating system of the targeted host. If Nmap is able to fingerprint the OS it will help me find possible ways to exploit the host.

The second tool I will use to recon the target's network is SuperScan. SuperScan runs on Windows and has a nice graphical user interface.



SuperScan 4.0

Hostname/IP: 192.168.1.22

Start IP: 192 . 168 . 1 . 22

End IP: 192 . 168 . 1 . 22

Start IP	End IP
192.168.1.22	

Ready

Using these two tools would hopefully give me an idea of the types of services running on the targets network. Based on Andy's practical I should find hosts listening and providing services for HTTP, HTTPS, SMTP, and SSH.

Although Nmap and Superscan both have ways to try and fingerprint the OS on a scanned host, neither is perfect. To try and find out what operation system or program a host is running and find vulnerabilities, I will use Nessus 2.0.10[11]. Nessus is a security scanner that has a server portion that runs on Linux and a client portion that runs on either Linux or Windows.

[11] http://www.nessus.org/

Attack Planning

The goal of my attack is to gain access to a system that is not accessible from the Internet. To achieve this goal I will need to find a way past the target's external firewall and any internal firewalls while avoiding any logging servers and IDS systems along the way.

During my recon I tried to locate the name of an internal IT staff member. When attacking a network the best approach is to attack the weakest point. Many IT staff members have remote access to the internal network. Unlike standard remote user accounts which have limited access, IT members with remote access tend to have full access of the network. One of the hard parts about attacking a remote user to gain access is that they tend to be mobile and hard to find. This is not the case most of the time when it comes to IT members since the majority of their access is done from their home. A static remote connection can still be hard to locate; this is where knowing an IT staff members name can come in handy.

I have known many Network Adims that run workstations and servers at their home that are directly accessible form the Internet. Some do it for personal reasons and some run a side business such as Web Hosting. A lot of the time these servers tend to be less protected then production servers in a business environment. It may be easier to attack one of these servers in order to find a backdoor into the targets network.

In Andy's practical he states "An admin can access many critical servers from home via this server", meaning a admin can connect to the (11) Deposit server from home over SSH and then control other servers within the network. Gaining control over a remote administrator's home computer would give me almost full access to the target's network, but there are some problems with this attack. Many of the requirements for this attack to succeed rely on what-ifs.

- I would need an administrators name
- I would need to be able to locate him on the Internet
- He would need to be running a server I could compromise

I believe there are too many what-ifs for this attack to work.

Although this attack is hard to pull off, there are some steps that should be taken in order to prevent such an attack.

- Try to limit the amount of information freely available about your network and internal staff.

- Try to limit the number of IT staff members that have remote access to the network. How many of them really work form home?
- Also try to limit the amount of access they have. Do they really need access to every sever in the network?

My next option would be to find a host running a service with a flaw that I could exploit to gain control of the server and then launch attacks against other internal hosts. By using Nnap, Superscan, and Nessus I have pretty good idea of the types of services that are running on the target's network. My attack window for this type of attack is very limited, but other attacks of this nature have been very successful for other hackers. Since this is a simulated attack I do have access to more information than an attacker would. From Andy's practical I know that the servers are running FreeBSD 5.1, but the type of web server or mail server is not listed. Since these programs are unlisted I will assume that the default programs that normally ship with Linux are being used.

The Attack

There are three hosts accessible from the Internet. All three hosts seem to be running FreeBSD 5.1. One server is accessible via SSH, one is accessible via SMTP and the last server is accessible via both HTTP and HTTPS. No other information is known about the servers. In order to compromise one of these servers I must find a exploit in one of the accessible services.

I know from FreeBSD's website that the latest version is 5.2.1. Since I did not see any information of when updates would be applied to the servers I will assume that they are still running 5.1.

My next step would be to check the CERT[12] website for any possible vulnerability in FreeBSD 5.1.

While searching the CERT website I came across a flaw in the version of SendMail that ships with FreeeBSD 5.1.

CERT® Advisory CA-2003-25 Buffer Overflow in Sendmail

I. Description

Sendmail is a widely deployed mail transfer agent (MTA). Many UNIX and Linux systems provide a sendmail implementation that is enabled and running by default. Sendmail contains a vulnerability in its address parsing code. An error in the `prescan()` function could allow an attacker to write past the end of a buffer, corrupting memory structures. Depending on platform and operating system architecture, the attacker may be able to execute arbitrary code with a specially crafted email message.

[12] http://www.cert.org

This vulnerability is different than the one described in CA-2003-12.

The email attack vector is message-oriented as opposed to connection-oriented. This means that the vulnerability is triggered by the contents of a specially crafted email message rather than by lower-level network traffic. This is important because an MTA that does not contain the vulnerability may pass the malicious message along to other MTAs that may be protected at the network level. In other words, vulnerable sendmail servers on the interior of a network are still at risk, even if the site's border MTA uses software other than sendmail. Also, messages capable of exploiting this vulnerability may pass undetected through packet filters or firewalls.

Further information is available in VU#784980. Common Vulnerabilities and Exposures (CVE) refers to this issue as CAN-2003-0694. [13]

I will now try to exploit this flaw in order to take control over the targets mail server. Since the goal of my attack is to gain access to a server or workstation that is not accessible from the Internet, once in control of the mail server I would begin probing and scanning the internal network for other hosts to attack.

If I were a skilled hacker I could craft an email that could take advantage of this flaw and take over the email server. Since like most hackers I lack the skills to do it myself I will rely on others to do it for me. I don't know of any hacker sites to search so I will begin with ww.google.com. After a few hours of searching and a many unanswered posts in chats rooms devoted to hacking, I would have to say that my attack is a failure. Although I was able to find a flaw to exploit I was unable to find a program or a how-to paper to use against the target.

Countermeasures

Although my attack was a failure someone with more skill could have been able to gain control of the mail server and launch attacks against internal hosts.

Andy's network design did provide for internal firewalls to protect his users and critical servers from a possible security breech of this nature. He also put his central logging server in the "Red Zone" which means the hacker would have to crack another firewall in order to cover his/her tracks. Andy's use of internal IDS could alert the internal staff to the security breech and possibly stop the attacker before he/she is able to attack another host.

There were rules in the firewall to allow for updates but there was no mention of when if ever these updates would be applied. Since most security breeches happen because of known vulnerabilities, it is critical that internal hosts that communicate with a host on the Internet be kept up-to-date.

[13] CERT/CC. CERT® Advisory CA-2003-25 Buffer Overflow in Sendmail. 29 Sep 2003. URL: http://www.cert.org/advisories/CA-2003-25.html

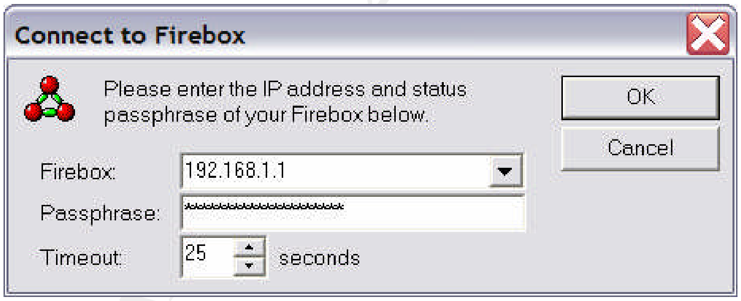
Assignment 4 – Remote User VPN Work Procedure

As GIAC Enterprises grows new partners will need to be given access to our network to import fortune cookie sayings from our database server. To insure that this in done securely and properly the following steps must be taken.

The first step in the process is to gain access to the WatchGuard X1000 firewall. This can only be done via the WatchGuard logging and management server. Attempted access via any other host will be denied.

To start the management software:

1. Left click on "start"
2. Go to programs\WatchGuard
3. Left click on "Firebox system manager"
4. Insure that the IP address for the internal interface is correct and then enter in the read Passphrase. The read Passphrase is case sensitive. A common mistake made here is to enter in the wrong Passphrase. The Firebox has two passwords or "Passphrases". The first password allows you to gain access to the Firebox; it saves an updated config file to the management station. When you make changes to the config file you are actucely changing the local config file and not the firewall. No changes are made to the firewall until you save the updated config file to the firewall. To do this you must enter in the write Passphrase. If the wrong Passphrase is entered the management software will prompt you to enter in the correct one.



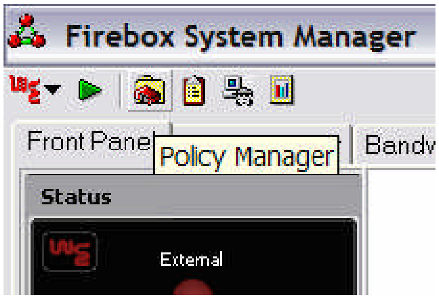
Please enter the IP address and status passphrase of your Firebox below.

Firebox: 192.168.1.1

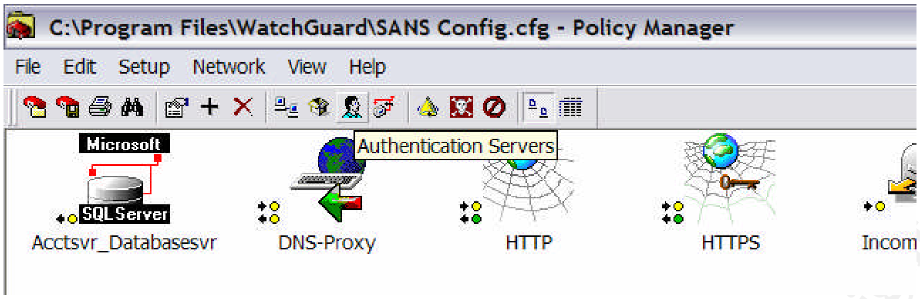
Passphrase: ********************

Timeout: 25 seconds

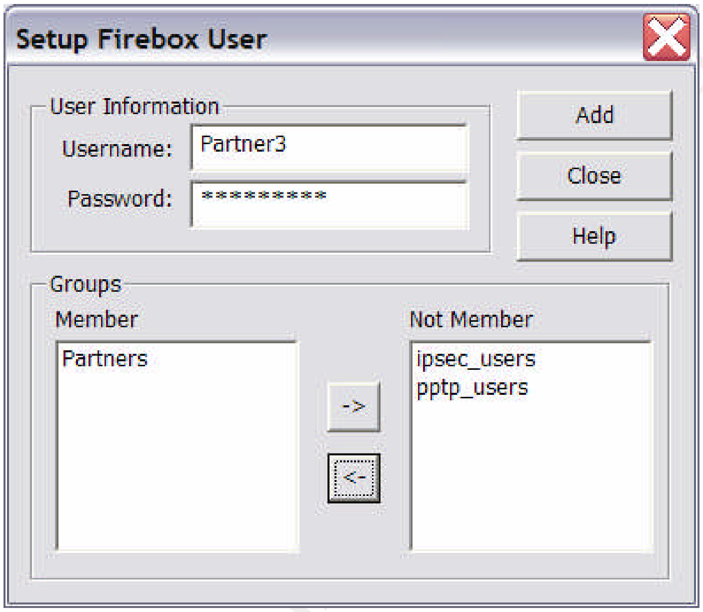
After gaining access to the Firebox System Manager you must open the policy manager.



Once inside the Policy Manager you must select the Authentication Servers Icon.


C:\Program Files\WatchGuard\SANS Config.cfg - Policy Manager
File Edit Setup Network View Help
Authentication Servers
Microsoft
SQL Server
Acctsvr_Databasesvr
DNS-Proxy
HTTP
HTTPS
Incom

The next step will be to add a new user and add them to the partners group. Be sure that password is eight characters long and meets our complexity requirements and that you only add them to the Partners group.



User Information

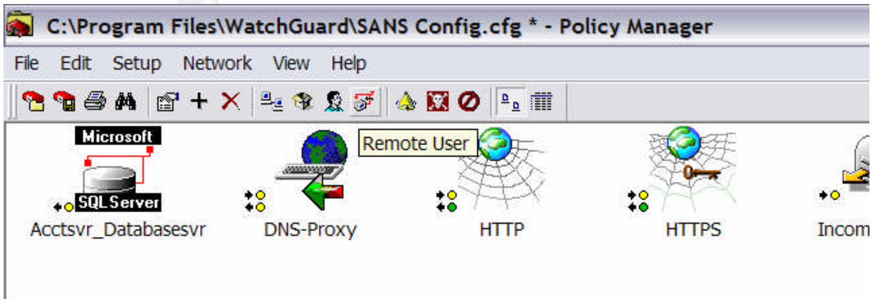
Username: Partner3

Password: *********

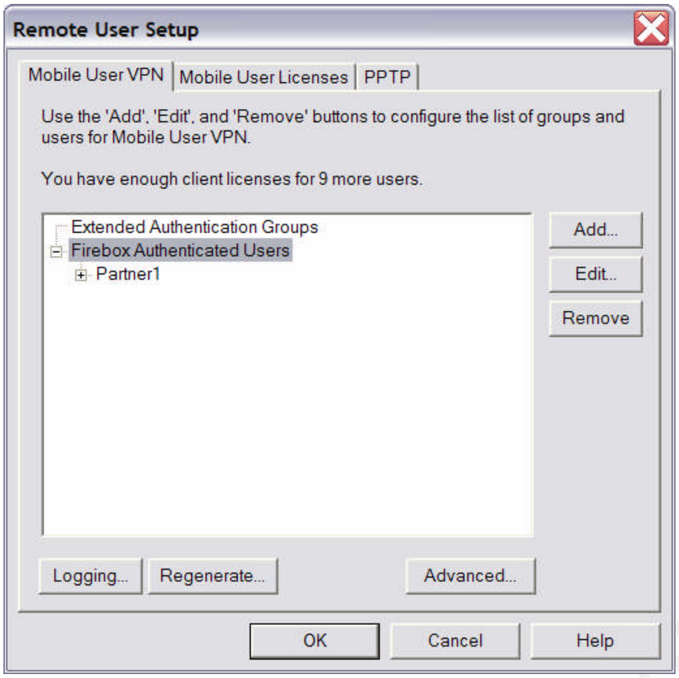
Groups

Member	Not Member
Partners	ipsec_users pptp_users

Now that the new partner has a user account it is time to configure their remote access. Left click on the Remote Users icon.


C:\Program Files\WatchGuard\SANS Config.cfg * - Policy Manager
File Edit Setup Network View Help
Remote User
Microsoft
SQL Server
Acctsvr_Databasesvr
DNS-Proxy
HTTP
HTTPS
Incom

Now make sure “Firebox Authenticated Users” is selected and left click on “Add”.

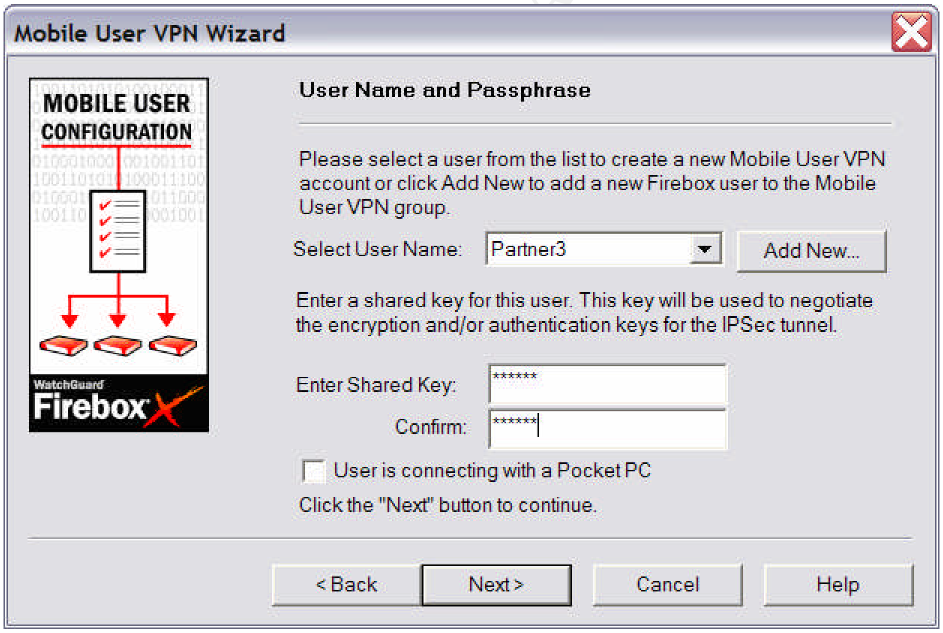


Use the 'Add', 'Edit', and 'Remove' buttons to configure the list of groups and users for Mobile User VPN.

You have enough client licenses for 9 more users.

- Extended Authentication Groups
- Firebox Authenticated Users
  - Partner1

Left click on "Next".
Left click on the down arrow and select the new user account you just added.



User Name and Passphrase

Please select a user from the list to create a new Mobile User VPN account or click Add New to add a new Firebox user to the Mobile User VPN group.

Select User Name: Partner3

Enter a shared key for this user. This key will be used to negotiate the encryption and/or authentication keys for the IPSec tunnel.

Enter Shared Key: ******

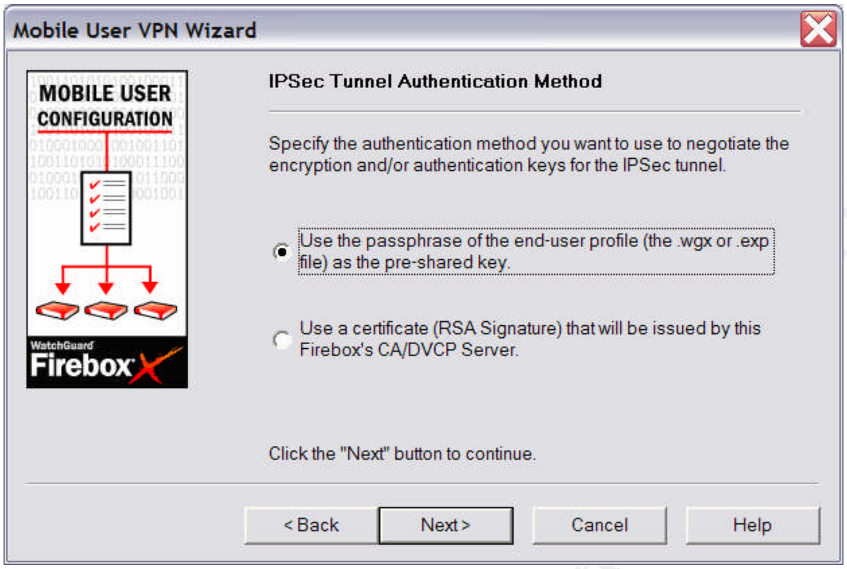
Confirm: ******

□ User is connecting with a Pocket PC

Click the "Next" button to continue.

Enter in the shared key. Make it the same as the user password you entered in when creating the account. The password and shared key do not tie in together but making them the same makes record keeping easier. A common mistake here is to mistype the shared key and make sure caps lock is not on. Also remember that the shared key and password should be eight charters long and meet our complexity requirements.

Select "Use the passphrase of the end-user profile (the .wgx or .exp file) as the pre-shared key".


Mobile User VPN Wizard

IPSec Tunnel Authentication Method

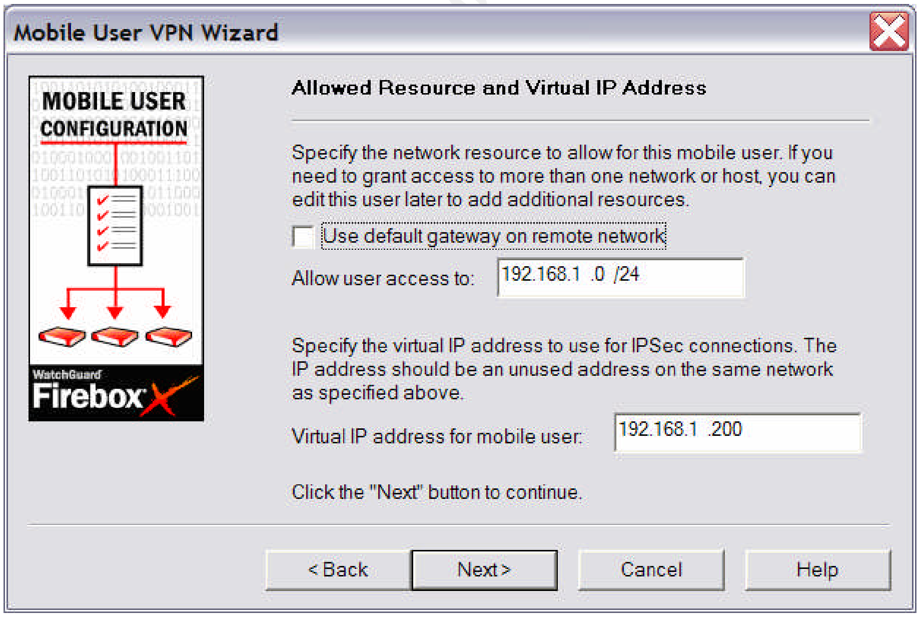
Specify the authentication method you want to use to negotiate the encryption and/or authentication keys for the IPSec tunnel.

● Use the passphrase of the end-user profile (the .wgx or .exp file) as the pre-shared key.

○ Use a certificate (RSA Signature) that will be issued by this Firebox's CA/DVCP Server.

Click the "Next" button to continue.

Ensure that "Use default gateway on remote network" is unchecked and that our local internal IP address range is correct. Also assign a unused IP address from our local network.


Mobile User VPN Wizard

Allowed Resource and Virtual IP Address

Specify the network resource to allow for this mobile user. If you need to grant access to more than one network or host, you can edit this user later to add additional resources.

□ Use default gateway on remote network

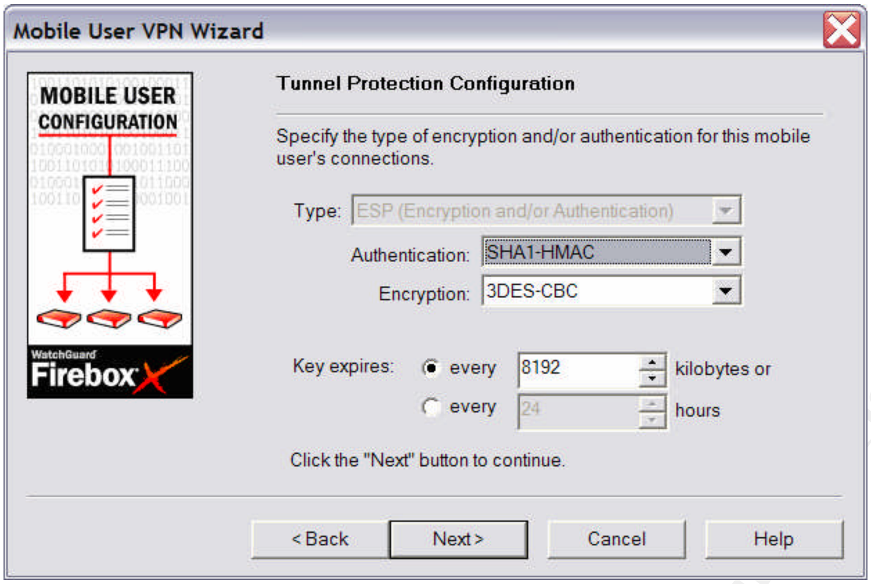
Allow user access to: 192.168.1 .0 /24

Specify the virtual IP address to use for IPSec connections. The IP address should be an unused address on the same network as specified above.

Virtual IP address for mobile user: 192.168.1 .200

Click the "Next" button to continue.

Set the Authentication to SHA1-HMAC and set the encryptions to 3DES-CBC. Leave the key expiration set to it's default of 8192 kilobytes.



Tunnel Protection Configuration

Specify the type of encryption and/or authentication for this mobile user's connections.

Type: ESP (Encryption and/or Authentication)

Authentication: SHA1-HMAC

Encryption: 3DES-CBC

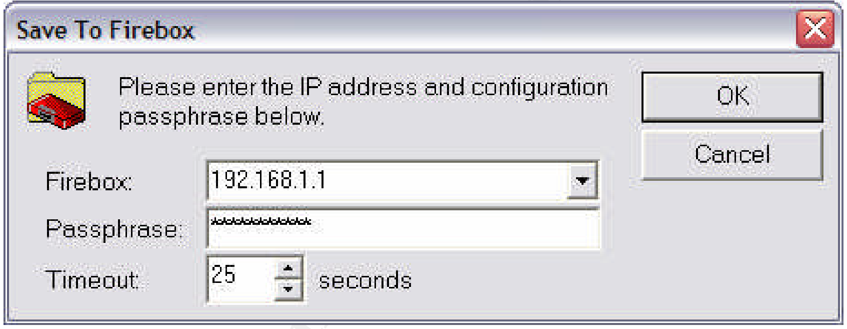
Key expires: ● every 8192 kilobytes or

○ every 24 hours

Click the "Next" button to continue.

Now you must save the changes to the Firebox.

1. Go to File\Save\To Firebox
2. You will be prompted to save a new local config file
3. When prompted to replace the old file select yes
4. You will then be asked for the write Passphrase.



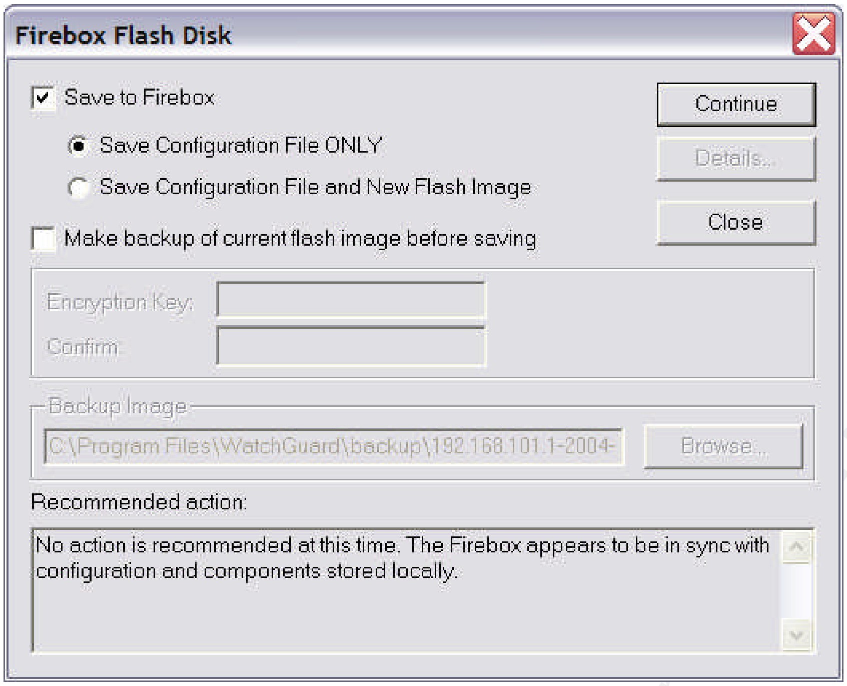
Please enter the IP address and configuration passphrase below.

Firebox: 192.168.1.1

Passphrase: ************

Timeout: 25 seconds

5. Once the correct Passphrase is enter the Firebox Flash Disk box will appear.
6. Select “Save Configuration File ONLY” and then left click on “Continue”. This will save the configuration to the Firebox without a reboot. If you select “Save Configuration File and New Flash Image” a new image will be flashed to the Firebox requiring you to reenter the log encryption key, the read passphrase and the write passphrase. It will also require the Firebox to reboot. A common mistake made here is to flash a new image to the Firebox thinking that the first selection only updates the local config file on the management station and not the Firebox.



Firebox Flash Disk

☑ Save to Firebox

● Save Configuration File ONLY

○ Save Configuration File and New Flash Image

□ Make backup of current flash image before saving

Encryption Key:

Confirm:

Backup Image: C:\Program Files\WatchGuard\backup\192.168.101.1-2004-

Recommended action:

No action is recommended at this time. The Firebox appears to be in sync with configuration and components stored locally.

Now that the Firebox is prepared for a new partner connection it is time to prep a CD with the MUVPN software and the username.wgx file. When we created a new Mobile user and saved the configuration to the Firebox a username.wgx file was created. This file contains all the settings the mobile user will need in order to make a VPN connection to our network. The file is secured via the shared key we entered when creating the new user. The file will be located on the management station under d:\programfiles\WatchGuard\RUVPN\B.82.87.2\wgx\username.

Copy the file to a CD along with the MUVPN software. Then ship the CD with the MUVPN software and the username.wgx file and the shared key to the partner via UPS. Once the partner receives the shipment they should load the MUVP software on the station or server they plan to use to import data. At the end of the software installation it will ask them for the username.wgx file. The partner will need to browse to the username.wgx file location. Once the file is located the computer will need to reboot. Once the computer reboots it will ask the partner for the shared key. If the partner enters in the correct shared key the MUVPN software will import the correct connection information form the username.wgx file. A common mistake many users make when installing the MUVPN software is not being able to locate the username.wgx and rebooting without locating it first. If this happens the partner merely needs to locate the username.wgx file on the CD and double click on the file. They will be prompted for the shared key and again if entered correctly the connection information will be imported from the username.wgx file.

Partners will only be able to connect to our fortune cookie sayings database via SQL port 1433, therefore stand trouble shooting procedures such as pinging the remote host will not work. The two best options for trouble shooting a failed MUVPN connection will be the Firebox logs and the MUVPN logs. One way to access the Firebox logs is to open the Firebox System Manager and click on the Traffic Monitor tab. This tool will show you reel time logs as they happen. The best way to use this feature is to have partner on the phone and have them try to connect as you watch the logs. One common problem that doing this type of testing can help you resolve is a partner unable to make a IPSec connection from behind their firewall. If you see no "iked[181]" logs at the time the partner is trying to connect no IPSec packets are reaching our firewall.

At this point you will need to trouble shoot the partner MUVPN installation to ensure that it is working. This is where the MUVPN logs will come into play. To view the MUVPN logs right click on the MUVPN icon running in the system tray and then left click on "Log View". This tool will allow you to verify the partners MUVPN software is working properly. Some common problems the logs can help you resolve is the SafeNet Adapter not getting bound to a live NIC or the MUVPN not being able to connect to our firewall. Trouble shooting a MUVPN can be very difficult and some simple steps to take to resolve this common problem is to insure that the partners firewall supports IPSec pass-through and that IPSec traffic is allowed out of their network. Also, having the partner remove and reload the software can fix some minor problems. Any trouble shooting steps outside these small issues should be passed off to a higher level engineer.