GIAC Enterprises Goes Cyber!

Firewalls, Perimeter Protection and VPN's

GCFW Practical Assignment Version 1.6a (revised October 26, 2001)

by Michael Desrosiers
March 21, 2002

Assignment 1 – Security Architecture

Preamble

I have always admired my uncle. Back in the 1960's he decided that there was a great big world just waiting to be explored. He had always wanted to start his own business, so he and his wife left the East Coast and relocated in California looking to fulfill the American dream. He leveraged himself to the hilt, and along with my anxious aunt, started GIAC (Good Intelligent Answer Cookies) Enterprises. They became the first company on the West Coast that dealt with the writing, packing and distribution of fortune cookie sayings. They have steadily grown the company over the years to the point where they now need an e-business strategy to meet there customers and distributors needs. The have enlisted the assistance of there loving nephew, myself, to help them develop a secure policy and implementation to protect there key assets. This section deals with the overall general network infrastructure and the access requirements and restrictions that all participants, including internal GIAC Enterprises employees, must abide by.

After talking to my uncle, I was able to grasp exactly what business needs that his company should consider. We discussed the issues in regards to at what cost do we protect the crown jewels of GIAC Enterprises, the customer database. The main concern with an e-business plan in regards to security is always the question, "Is the data that you are protecting worth the money that you are using to protect it." With this in mind, GIAC Enterprises will make every concerted effort to follow a best practices policy, in regards to its network topology. Because we have a tight budget to work with, we will have to become very creative in our schemes, but not our methods.

We are going to follow the guidelines of the 3 fundamental rules of security that conform to the **C**onfidentiality, **I**ntegrity and **A**vailability model.

A. That the network attempts to ensure that the material that customers, vendors and employees obtain is viewed only by the parties that are authorized too.

B. That the data itself has not been altered or replaced

C. That the business critical information is accessible 24 hours a day/ 7 days a week.

The decision has also been made to follow a layered security model, that is based on a best practices scenario, which organizations such as the SANS Institute promote. They are as follows:

Defense-in-depth

Where feasible, multiple layers of defense against unauthorized entry will be used. We will use the same filtering rules on the border router and external firewall, so that the illegal network traffic will be blocked in case the device fails or it becomes compromised.

Principle of Least Privilege

All groups will be allowed to access only the services and systems that are deemed necessary to successfully perform the work responsibilities required of them and restricted from accessing any other services

Isolate systems providing network services

Systems offering services to external or internal users will be on dedicated service networks and will not be dual-use. The system hosting the publicly available web server will be on a screened subnet and will only host the web server. It will not host multiple instances of services. One host=One service.

Our plan is to design, configure and audit the architecture. Obviously there is a risk of not catching all the "gotcha's." To avoid this we will plan to have an outside agency that has been involved with security audits for years, conduct a full audit of the architecture to ensure there are no issues before we roll out the production environment. What we hopefully will gain by this is that if we find problems, we are willing to not only assume or assign the risk, but to plan ways to rectify them. The design will be geared towards the future implementation of http proxies and mail relays to help address some of our current shortcomings. We also are allowing for the deployment of and IDS server (ozzy) in our internal network. The IDS server will utilize snort, but as of this time, will not be deployed. Also we can budget for the following fiscal year to help alleviate some of the weaknesses that we will uncover in our assessments.

Objective

To devise a network topology that will provide layers of security without limiting the functionality of the business. Sounds pretty straight forward huh! We will try and establish some ground rules that the company must embrace to make this project work. So as Cipher in the movie, "The Matrix" once said, "Buckle up your seatbelt Dorothy, cause Kansas is going bye, bye!"

- Breaches of network security are not to be tolerated**,** but will most likely be an occurrence. We cannot eliminate the risk entirely, only identify and manage it. GIAC Enterprises needs to understand this and ensure that it has procedures in place to prevent, detect and react to problems as they arise.
- Defense in depth, layered security does not mean have a firewall in place and all your problems seem to disappear. GIAC will need to understand this, map the environment using a documented process and ensure that all devices under our control apply adequate security controls. This applies to the **whole** infrastructure.
- Customers, partners and developers will be granted **minimum** access to the number of services required to carry out the business. This falls in line with the Principle of Least Privilege security model.
- We **must** be a good internet neighbor. Our systems will employ appropriate measures, in regards to staying current with patches and vulnerabilities that pertain to our

environment. A good example of this is monitoring bugtraq's web site at http://online.securityfocus.com/archive/1, Carnage Mellon's web site at http://www.cert.org and the SANS top 10 vulnerability assessment list at http://www.sans.org/topten.html.

- The security architecture must not impede the growth of the business. The business provides our environment. We need to concentrate on the notion e-business is an investment in the future, not a drain on the bottom line.

Network Architecture

We will define an e-business security architecture for GIAC Enterprises which deals in the online sale of fortune cookie sayings. Our architecture must include the following components:

- filtering routers
- firewalls
- VPN to business partners
- secure remote access
- internal firewalls

GIAC Enterprises architecture must consider access requirements (and restrictions) for:

1. Customers (the companies and consumers that purchase bulk online fortunes);
2. Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
3. Partners (the international partners that translate and resell fortunes).

The network architecture for GIAC Enterprises is shown in **Figure 1**, on the next page. To help defray some of the cost, we have leased a small sixteen address subnet with publicly routable ip addresses from an ISP, for our service network servers. These addresses (208.200.171.0/28) have been sub netted to allow for greater flexibility and administration. The GIAC Enterprises services network will reside on the (208.200.171.16/29) subnet which is used for servers that will be accessible from the internet. The VPN gateway network has been assigned the (208.200.171.8/29) subnet for authorized remote access. Eight additional ip addresses are masked into two small subnets for the connections between the border router and ISP (208.200.171.0/30) and the border router and our firewall (208.200.171.4/30).

We will start on the border between GIAC Enterprises and the ISP. We are passing all network traffic from the ISP router to the border router using a Cisco 2514 router with a T1 CSU/DSU module for the PPP connection. From the ethernet interface of the router, we then will connect to our network. Next on the wire is a firewall running netfilter iptables v1.2.4 installed via a base install of Red Hat 7.2 (giac_zion). We also have installed and run Bastille Linux 1.3.pre10 on the firewall server to further secure and harden the operating system. For a more detailed view of Bastille, please visit Jay Beale's web site at http://www.bastille-linux.org. The firewall has four network interfaces: one connected to the border router (208.200.171.6), one connected to the service network (208.200.171.17), one connected to an isolated VPN service gateway subnet (208.200.171.9) and the last one connected to an internal service and internal employee's subnet (192.168.1.1). The firewall performs network address translation (NAT) so that the internal systems with private ip addresses can have access to the internet, yet not be routable on the internet.

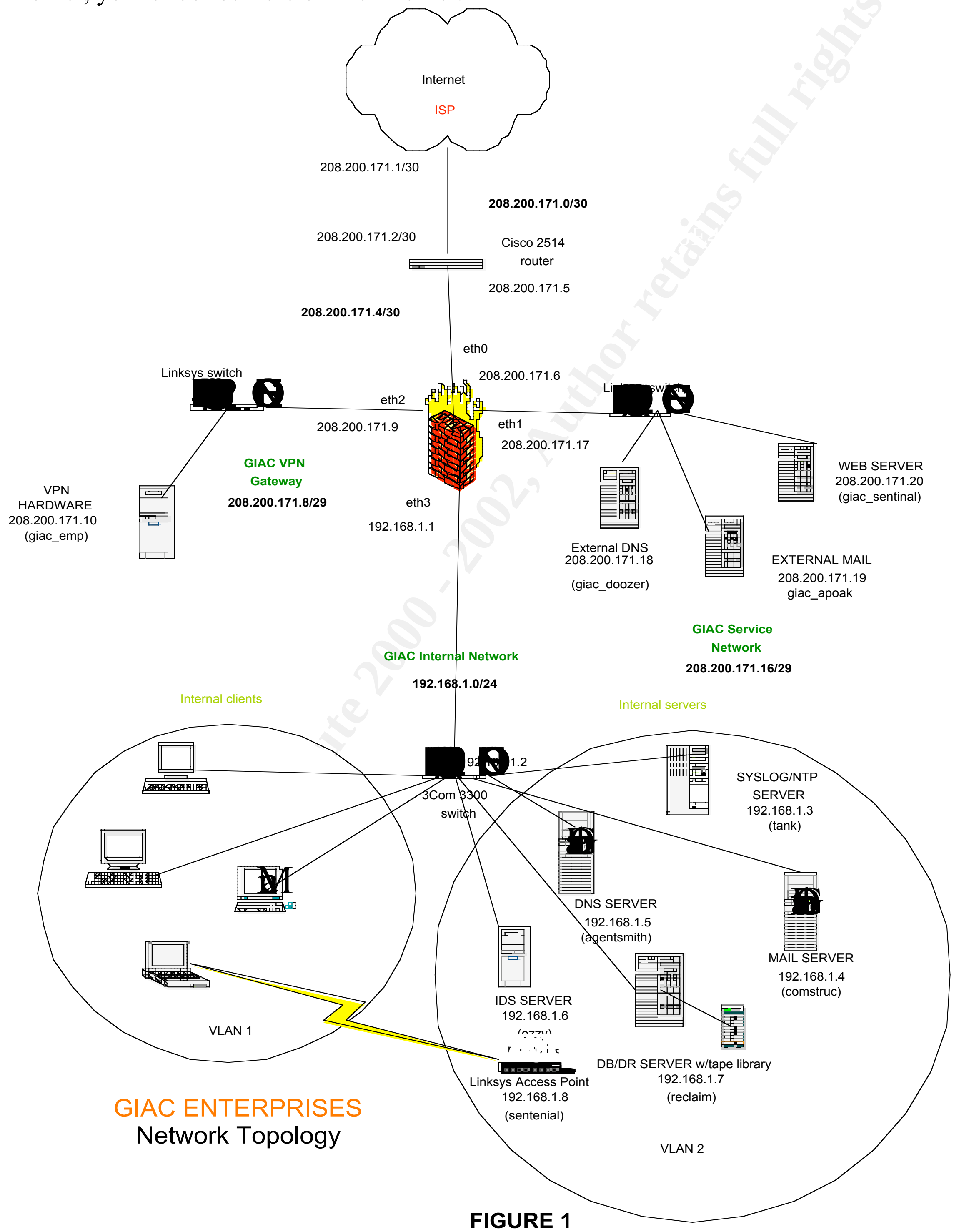


FIGURE 1

.

Service Network (208.200.171.16/29)

The service network subnet hosts all the systems that will be accessible to the outside world through the internet. They include the company's web server (giac_zion), the external mail server (giac_apoak), and external dns server (giac_doozer). All systems are IBM pseries R/S 6000 servers running AIX 5100-01 with the latest firmware microcode and at the latest patch levels. We also will be using openssh 2.9p2-12 client and server for remote administration. They have been hardened using procedures such as password aging, restricting setuid programs and eliminating unused services and daemons. For a more detailed description of this process, I have included them in *Appendix A* of this document. All are configured to send log data to the GIAC syslog server (see tank below) and none are allowed network services that are not essential to our business objectives or to there job responsibilities.

giac_apoak has postfix 20010228 installed, and accepts smtp connections from anywhere, and acts solely as a mail relay. Email from the internet destined for any employee mailbox is relayed to the internal mail server. Email from the internal mail server is relayed to the internet. Relaying of all other email is denied.

giac_doozer accepts udp and tcp connections to port 53 from anywhere. GIAC Enterprises employs a split-horizon dns; therefore giac_doozer hosts dns records only for systems directly accessible from the internet. Any ip resolution requests for systems with private addresses are forwarded to the internal dns server. SPLIT DNS: The internal dns is placed on this subnet and is protected by restricting traffic to udp 53. No zone transfers will be permitted from this machine and it will only allow dns queries to and from the internal networks using udp port 53. This may cause some queries to be truncated but this can be verified through the audit and the logs. That is why logging is a critical piece of this puzzle! Script and parse……….

giac_sentinal has apache 1.3.22-2 and mod_ssl 2.8.5-1 installed and accepts http and https connections. For proper business operations, the server occasionally needs to complete connections to the fortune cookie saying database (mysql) on the internal service network. Different areas of the company's website are made available to the different groups of users depending on their business needs. For an example, the pages with general company information and marketing material are made available via unauthenticated, unencrypted http to anyone on the internet while the pages used by the business partners to deliver translations of sayings are only available via authenticated, encrypted https. If orders are to be placed by credit card, GIAC Enterprises has contracted with an online credit card processing company to provide this service. To complete the processing, giac_sentinal initiates https connections to the credit card processing server. This allows for a secure tunnel to encrypt and secure communications.

VPN Gateway (208.200.171.8/29)

giac_emp server resides on its own subnet. It is isolated from the systems on the service network. The main reason behind this topology, is to reduce the risk of exposing encrypted data to the internet, should one of the other systems in the service network be compromised. If there is a Man in the Middle attack we can somewhat guard against it with this configuration, limiting the damage.

GIAC Internal Network (192.168.1.0/24)

The internal network is comprised of the the log server (tank), the database server (reclaim), the mail server (comstruc) and the dns server (agentsmith). All are configured to send remote log data to the syslog server (with the exception of tank, which logs to itself) and none offer any network services that are not required by its primary business function. This network also entails the internal employee's workstations. We have provided an additional layer by creating 2 VLAN's off of a 3Com 3300 switch. The workstations (clients) are on VLAN1 and the servers are on VLAN2

tank has sysklogd 1.4-7 installed and configured to accept remote log messages on udp port 514. It serves as the central collection point for log data generated by all systems on the internal and external service networks. To automate log event monitoring, logcheck is installed and configured to review logs hourly for suspicious events. Tank also has ntp 4.0.1-4 installed and is the time ntp server used to synchronize system clocks at GIAC Enterprises so log data from different machines can be correlated and authenticated.

reclaim has a mysql server 3.23.41-1 installed and hosts the GIAC Enterprises fortune cookie sayings database as well as databases with information on customers, partners and suppliers. The db server accepts connections on port 3306 that originate from the internal network only. Since mysql sends authentication information clear text over the network, connection requests from the web server on the service network is tunneled through the external firewall using an ssh connection that forwards port 3306 on giac_sentinal to port 3306 on reclaim. This sever also doubles as our disaster recovery server also. It is running Tivoli Storage Management version 4.2 software with a IBM 7133 tape library.

comstruc has qmail 1.03 installed, accepts smtp connections from internal users and giac_comstruc, and supports pop3 and imap so internal users can use popular email clients to retrieve their mail.

agentsmith accepts udp and tcp connections to port 53 from giac_doozer as well as performs lookup requests for users on the internal network.

Because of issues with wiring in the warehouse, we have installed a wireless access point to allow their workstations access to the internal network. We are using the Linksys WAP11 2.4 GigHz wireless access point with version 1.72 firmware. The tftp server allows easy updating of the firmware. We are well aware of the vulnerabilities that this presents, but have taken steps to secure the connection. For a more detailed look at how to harden the access point, we have included some steps that can be found in *Appendix B*.

The GIAC internal network also includes the corporate workstations of all employees. The workstations have a Windows 2000 image that has been scrubbed and sanitized. All workstations are loaded from a secure standardized "golden" image. To allow for updates and patches to stay updated, we are loading HFNETCHK version 3.3 on all desktops. The policy of GIAC Enterprises is to disallow all connection attempts originating from outside the internal network destined for inside the internal network. In order to be connected to the GIAC internal network, workstations **must** have personal firewalls operational on them. We use TPF (tiny personal firewall) version 2.0.15A and ZoneAlarm Pro version 3.0.091. Also Norton Anti-Virus v7.51 is **mandatory** on all clients. To allow for better administration in the future, we will centralize both of these products, to provide server (push) functionality to our environment. This will allow us to automate this process. We also highly recommend to our employees to use PGP (windows) or GNUPG (linux,*nix) for both encrypting email and protecting sensitive data residing on the workstations hard drive. This adds another layer of security to our environment. We are for full access to the internet at GIAC, so we must protect all desktop data and outbound connections to the internet.

Business Objectives Overview

Each of the following groups require access to GIAC Enterprises environment, during the business day: the business partners and suppliers, the internet, customers and of GIAC employees. To comply our stated goal of the principle of least privilege with regards to accessing network resources, users within each group are allowed access to only the systems and services they will need to complete there job responsibilities and nothing more. Later, we will explain what these definitions shall be.

Business Partners & Suppliers

Besides access to the internet, GIAC suppliers and partners that sell fortunes require direct connection to giac_sentinal via https protocol (port 443). As with customers, GIAC proprietary cgi- bin applications accept a supplier's or business partner's account ID and password, validate the information against account data stored on the internal database server (reclaim), and generate a time-sensitive session ID that is passed back to the supplier's browser and used for the remainder of the session. Because both of these groups need and require permission to upload sensitive data into the cookie sayings database, GIAC Enterprises has implemented additional security to access their area of the web site. Authentication via client certificate is enforced by the apache configuration file for these web pages. Since no other direct connections are necessary for providing fortunes, none will be granted.

Internet

We will restrict access to GIAC Enterprises from the internet. They can initiate http connections to giac_sentinal to view selected pages with non-specific company information and sales/marketing company material. They can generate smtp connections to giac_apoak to send mail to employees in the giac.com domain. They can process dns queries to giac_doozer to resolve the ip addresses for GIAC systems with routable addresses. Since no other direct connections originating from the internet are necessary for normal business operations, none are allowed. That is the **RULE**!

Customers

In addition to internet access, customers purchasing substantial orders of cookies online require direct a connection to giac_sentinal via https protocol (port 443). GIAC proprietary cgi-bin applications accept a customer's account name and password, confirm the information against account data stored on reclaim, and generate a time-sensitive session ID that is passed back to the customer's browser and used for the remainder of the session. During the session, giac_sentinal initiates connections with data provided by the customer. Database queries are tunneled through a ssh connection to reclaim to validate authentication credentials and display fortune cookie sayings options and prices, then https connections to the credit card processing server for obtaining payment approval. Since no other direct connections originating from customers' systems are necessary for online purchasing, none are allowed.

GIAC Enterprise employees

GIAC employees on the internal network use the services on the systems for day-to-day business operations. They require access of the imap, pop3 and smtp protocols to comstruc to retrieve and send email. They require access via dns protocol to agentsmith to resolve ip addresses for any hostname they wish to contact. Certain employees require access to the database on reclaim to review and make updates to customer, supplier and business partner account records. Also limited access to the internet is granted. GIAC understands how valuable the internet is as a tool. They are allowed access to the internet from the internal network, are allowed to initiate anonymous ftp sessions for downloading of software updates and patches and can initiate ssh sessions to other remote systems. Secure shell access using ssh2 only, from the internal network is required by administrators to all the systems on the internal network, the service network and the vpn subnet. For remote employee access, a few employees are granted enough access to the internal network to enable sending and receiving of email. This is done by creation of an IPSec connection using tunnel mode ESP to the vpn server. The firewall allows smtp (port 25), pop3 (port 110) and imap (port 143) to comstruc from the vpn gateway network.

Assignment 2 – Security Policy

Border Router (giac_matrix)

The border router (giac_matrix) is a Cisco 2514 router. GIAC will use extended access control lists (ACL) on the border router to implement the use of filtering on port numbers. The border router is used exclusively for static packet filtering. ACL 100 is applied inbound to the ethernet interface coming from giac_zion and ACL 101 is applied inbound to the internet facing interface going to the ISP. Each rule has a brief explanation preceded by an !, the comment character used by the Cisco IOS.

```
! Access Control List 100 (coming in from internal network)
!
no access-list 100
access-list 100 deny ip 208.200.171.0 0.0.0.3 any log
```

```
! deny and log traffic with source ip of network connecting to ISP
access-list 100 permit icmp host 208.200.171.6 any
! allow icmp from source ip of eth0 on the firewall
access-list 100 permit tcp host 208.200.171.19 any 25
! allow smtp(mail) from source ip of giac_apoak
access-list 100 permit tcp host 208.200.171.18 any 53
! allow dns(tcp) from source ip of giac_doozer
access-list 100 permit udp host 208.200.171.18 any 53
! allow dns(udp) from source ip of giac_doozer
access-list 100 permit tcp host 208.200.171.6 any 80
! allow http from source ip of eth0 to the firewall
access-list 100 permit tcp host 208.200.171.6 any 443
! allow https from source ip of eth0 on the firewall
access-list 100 permit icmp host 208.200.171.0 0.0.0.15 any
! allow icmp from source ip of service network or vpn
access-list 100 permit tcp host 208.200.171.6 any range 20 22
! allow ftp and/or ftp data and/or ssh from source ip of eth0 on the
firewall
access-list 100 permit tcp host 208.200.171.20 host 206.36.14.60 443
access-list 100 permit tcp host 208.200.171.20 host 206.36.14.61 443
! allow https from source ip of giac_sentinal to the credit card
servers
access-list 100 permit tcp host 208.200.171.6 any 80
! allow http from source ip of eth0 on the firewall
access-list 100 permit tcp any any established
! allow existing connections (with ACK and/or RST set)
access-list 100 deny ip any any log
! deny and log anything else
!
! Access Control List 101 (coming into giac.com from ISP)
!
no access-list 101
access-list 101 deny ip 208.200.171.0 0.0.0.15 any log
access-list 101 deny ip 208.200.171.4 0.0.0.3 any log
! deny and log anything with source ip inside border router
access-list 101 permit icmp any host 208.200.171.6
! allow icmp with destination ip of eth0 on the firewall
access-list 101 permit icmp any 208.200.171.0 0.0.0.15
! allow icmp with destination ip of service network or vpn
access-list 101 permit tcp any host 208.200.171.20 eq 80
! allow http to destination ip of giac_sentinal
access-list 101 permit tcp any host 208.200.171.20 eq 443
! allow https to destination ip of giac_sentinal
access-list 101 permit udp any host 208.200.171.18 eq 53
! allow dns (udp) to destination ip of giac_doozer
access-list 101 permit tcp any host 208.200.171.19 eq 25
! allow smtp(mail) to destination ip of giac_apoak
access-list 101 permit tcp any host 208.200.171.19 eq 113
! allow ident to destination ip of giac_apoak
access-list 101 permit tcp any host 208.200.171.18 eq 53
! allow dns (tcp) to destination ip of giac_doozer
access-list 101 permit 50 any host 208.200.171.10
! allow ipsec esp protocol to destination ip of giac_emp
access-list 101 permit udp any host 208.200.171.11 eq 500
! allow ike to destination ip of giac_emp
access-list 101 permit tcp any any established
! allow existing connections (with ACK and/or RST set)
```

There are some rules I want to point out that we are also using on the border router. The routers ACLs have an implicit deny as the last rule, so we do not need one at the end of the 101 ACL to deny traffic we do not want to allow in. The explicit deny at the end of the 100 list will log all unexpected traffic that comes into the GIAC Enterprise network. We are allowing ftp, http and https traffic to the eth0 interface on the firewall to enable internally connected employees to access the internet because the ip address of that interface is the source IP used by the hiding NAT. IDENT traffic is allowed through so the firewall can send back an immediate reset and avoid a possible email delivery delay for smtp connections. In addition to the ACL's filtering inbound and outbound traffic, several other configuration options are present in the config file to harden the router and avoid GIAC from becoming an unwilling DDOS network or internet zombie.

These recommendations are in the SANS Track 2 courseware.

```
enable secret
service password encryption
! store password as md5 has in configuration file (default is plain text)
no snmp
! disable snmp
no ip source-route
! disallow source routed packets
no service tcp-small-servers
no service udp-small-servers
! disable small services (echo, discard, chargen, and daytime)
no service finger
! disable finger service
no ip http
no ip bootp
! do not start http or bootp servers on the router
no cdp
! disable cisco discovery protocol
no ip direct-broadcast
! help prevent smurf attacks by disabling broadcast packets to remote networks
no ip unreachables
banner / Secure site. No unauthorized access /
! add a warning banner
logging 192.168.1.3
! Log messages to tank (As discussed later, the firewall will nat these)
```

The syslog server does not reside on the firewall itself. Instead, traffic to udp port 514 destined for the IP address of the firewall interface is statically NAT'ed by the firewall to have the private destination IP address of tank (see end of script in Appendix D)

Firewall (giac_zion)

The firewall that we have chosen, is a red hat 7.2 linux system running iptables. We have hardened the operating system using Bastille-Linux. We also are security checklist that I found on the internet, for linux installations. It can be found at the following web site:

http://isc.gsfc.nasa.gov/IT_Security/linux-checklist.htm.

Iptables is capable of performing stateful inspection of packets and network address translation. While iptables does not provide a fancy graphical user interface, it does include more than enough capability to enable us to enforce the access policies outlined for each of the various groups discussed in the previous section. In addition, the functionality is built into the linux kernel, so it gives us better performance.

An excellent resource for netfilter and iptables can be found at the following web site:

http://netfilter.samba.org/

In order to better understand the implementation of security policies using iptables is the concept of a rule chain, usually referred to simply as a chain. A rule chain is simply an access control list (ACL) containing rules to which a packet is matched with. Upon matching a rule, a defined action is taken. If the packet reaches the end of the chain and no rules have been matched, the default action or policy is performed for the chain. As described in the figure and text below, taken from the *netfilter.samba.org* web site, there are three built-in chains: INPUT, FORWARD, and OUTPUT.

```
Incoming                 /     \         Outgoing
       -->[Routing ]--->|FORWARD|------->
          [Decision]     \_____/        ^
               |                        |
               v                       ____
              ___                     /    \
             /   \                  |OUTPUT|
            |INPUT|                  \____/
             \___/                      ^
               |                        |
                ----> Local Process ----
```

1. When a packet comes in (say, through the Ethernet card) the kernel first looks at the destination of the packet: this is called `routing'.
2. If it's destined for this box, the packet passes downwards in the diagram, to the INPUT chain. If it passes this, any processes waiting for that packet will receive it.
3. Otherwise, if the kernel does not have forwarding enabled, or it doesn't know how to forward the packet, the packet is dropped. If forwarding is enabled, and the packet is destined for another network interface (if you have another one), then the packet goes rightwards on our diagram to the FORWARD chain. If it is accepted, it will be sent out.
4. Finally, a program running on the box can send network packets. These packets pass through the OUTPUT chain immediately: if it says ACCEPT, then the packet continues out to whatever interfaces it is destined for.

The user is free to create additional user-defined chains, which are primarily used to make the overall rule-set compartmentalized and more readable. Also, there are two special chains for implementing Network Address Translation named PREROUTING and POSTROUTING. PREROUTING rules are processed before the routing decision is made and POSTROUTING rules are processed just before the outgoing packets leave the interface. Finally, a brief description of the syntax used for iptables is included. For a detailed explanation of the syntax of the iptables command refer to its man page. The majority of the time, a command is written to append a rule to the end of the rule-set and it follows the format:

```
iptables -A CHAIN -i IF -p PROTO --sport PORT1 --dport PORT2 -s SOURCE -d DEST
                    -j ACTION -m state --state LIST
```

where

-A *CHAIN*	Add the rule to the end of the built-in or user-defined *CHAIN*
- *IF*	arriving interface of the packet is *IF*
-p *PROTO*	packet protocol is PROTO
--sport *PORT1*	(valid for tcp & udp) packet source port is *PORT1*
--dport *PORT2*	(valid for tcp & udp) packet destination port is *PORT2*
-s *SOURCE*	host or network where packet originated is *SOURCE*
-d *DEST*	host or network for packets final destination is *DEST*
-m state	keep track of this connection in the state table
--state *LIST*	types of connection states that should match
-j *ACTION*	what should be done with packets that match If *CHAIN* is specified, packet jumps to beginning of *CHAIN* for further processing.

If any option is omitted from the command line, then all valid values are matched. For example, if "-d *DEST*" is left out of a rule, then packets to any destination will match the rule. There are of course other flags to insert (-I), delete (-D), and replace (-R) rules in a chain, but due to the implementation procedure described in the next section, they seldom need to be used.

Rule-set Policy

Since GIAC Enterprises only allows shell access to the firewall from the system's console, the INPUT and OUTPUT chains are somewhat irrelevant. The first rule in both chains allows traffic where the source and destination are both the internal loopback interface. The INPUT chain includes a rule allowing ntp traffic in to the firewall from the log server (tank). The OUTPUT chain includes a rule allowing syslog traffic out to (tank). Finally, both chains then have the same rules to allow icmp traffic so the firewall can ping other systems (see ACT_ON_ICMP chain), eliminate traffic GIAC is not interested in logging (see KILL_TRASH chain), log then reject everything else. Note that a catch-all REJECT rule is included for fallback protection, even though the policy for both chains is to DROP packets that reach their ends without matching any rule. Of course, order is important, since all packets will match the REJECT rule, any rules that ACCEPT packets after it will never be matched. The complete policy rule-set for the firewall can be found in *Appendix C*.

The firewall mainly uses the built-in FORWARD chain and its user-defined chains to perform its role as the network enforcer. The logic goes as follows, after handling icmp packets, rules in the FORWARD chain determine which user-defined chain to use to further process the packet based on its arriving interface, source ip address and destination ip address. As with the other pre-defined chains, the FORWARD chain ends with rules to toss out, log or reject any packet that has not matched a previous defined rule.

We have defined and implemented the following chains to enforce our rules that have been discussed in the previous sections security policy.

eth0 - **TO_ZION** – traffic to the border router (internet)
eth1 - **TO_MORPHEUS** - traffic to the service network
eth2 - **TO_ORACLE** - traffic to the vpn gateway
eth3 – TO_NEBUCHADNEZZAR – traffic to the internal network

For further explanation of any rules in the FORWARD chain or any of the pre-defined chains, please see the comments in the script implementing the policy in *Appendix D*.

Rollout

Since the rule-set kernel based, the firewall server must be configured so that they are loaded automatically during the boot process. Also, to ensure there is no period of time in which network connectivity is enabled without filtering rules in place, loading of the rule-set occurs prior to bringing up any of the interfaces. The Red Hat iptables start-up script (*/etc/rc.d/init.d/iptables*) runs just before the network start-up script (*/etc/rc.d/init.d/network*) and attempts to load rule-sets found in a file named */etc/sysconfig/iptables*, if it exists. What we have decided to do is to create a script to implement the rule-set, load it into the kernel, and then generate the */etc/sysconfig/iptables* file automatically with the "*/etc/rc.s/init.d/iptables save*" command. Additional modifications to the firewall policy can then be made to the script. To install the new rules in memory, simply run the script again. Now we want to save them using the *save* command above which we will overwrite the old rule-set in the */etc/sysconfig/iptables* file. You can find the rc.firewall script in Appendix D.

The following is a step by step implementation of the policy:

1. Verify that the kernel is compiled with support for iptables
   Modular support for iptables is compiled into the kernel rpm installed by the red hat distribution. To ensure that a custom built kernel contains the correct config options read the man page and run make xconfig to see the options.
2. Ensure that iptables is installed and configured to start
   The iptables rpm installed by the red hat distribution should take care of the details of putting the necessary files in the right places. Make sure iptables is configured to start by issuing the command:

```
[root@giac_zion]# /sbin/chkconfig iptables on
```

3. Ensure that the firewall is configured to send kernel log messages from iptables to tank by including the following line in the */etc/syslog.conf* file
   kern.*   @192.168.1.3
4. Copy the script in *Appendix D* to the firewall server and execute it to load the rule-set
5. Review the rule-set for errors/omissions with the command

```
[root@giac_zion]# /sbin/iptables -L -n -v
```

6. Test that the rules are working properly. Examples:

   A. Rule description:
   FTP traffic from internal network is allowed to the internet.
   iptables command syntax:

```
iptables -A TO_ZION -p tcp --dport 21 -s 192.168.1.0/24 -m state \
              --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

   Test procedure:
   From a system on the GIAC internal network, ftp to an internet server (like ftp.redhat.com), connect and download a file.

   Expected result:
   FTP connection should be allowed and file download should succeed since the ftp data connection is related to the initial port 21 connection.

   B. Rule description:
   Attempt to open a connection to ident (port 113) on giac_apoak from the internet.
   iptables command syntax (matches the end of the TO_MORPHEUS chain):

```
$IPTABLES -A TO_MORPHEUS -p tcp --dport 113 -j REJECT --reject-
with tcp-reset
```

   Test:
   From a system with a internet based ip address on the internet, use telnet command to attempt to connect to port 113 on giac_apoak.

   Expected result:
   Connection should be blocked (i.e. no packet arrives at giac_apoak interface). Originating system should receive a TCP reset, immediately breaking down the connection.

   C. Rule description:
   The smtp traffic from the internal network is not allowed to the service network mail server giac_apoak (matches end of TO_MORPHEUS chain).
   iptables command syntax:

```
$IPTABLES -A TO_MORPHEUS -j $LOGFLAG --log-prefix "END
TO_MORPHEUS CHAIN:"
$IPTABLES -A TO_MORPHEUS -j REJECT
```

Test procedure:
From an internal system, attempt to telnet to port 25 on giac_apoak.

Expected result:
Should receive an icmp port unreachable message. Log message prefixed by 'END TO_MORPHEUS CHAIN' should be sent to the log file on tank designated for kernel facility messages.

7. Store the rule-set with the command

```
[root@giac_zion]#/etc/rc.d/int.d/iptables -save
```

8. Reboot the server and verify that rules get loaded automatically when system boots by listing them again.

```
/sbin/iptables -L -n -v
```

VPN Gateway (giac_emp)

The VPN Gateway Server is a Red Hat 7.2 linux system running Free/SWAN. The packages contain all the necessary kernel modifications and user utilities which can be downloaded from http://rpms.steamballoon.com/freeswan. This server also has been hardened with Bastille Linux 1.3.pre10. Client systems are mobile users' laptops running primarily Windows 2000. They have Sentinel Internet Pilot v1.2.3 software from SSH Communications Security (http://www.ipsec.com) installed to enable creating of the tunnel.

Secure remote access for GIAC Enterprises employees connecting from the internet is essential. After getting appropriate managerial level approval, a shared secret is generated for the employee. The following line is added to the */etc/ipsec.secrets* file on the vpn gateway server to allow the connections from any ip address on the internet:

```
208.200.171.10 0.0.0.0: PSK "really random shared-secret string"
```

The shared secret is loaded onto the employee's laptop, along with a corporate banner warning message stating the importance of keeping it secure. The process of loading and configuring the secret onto the laptop is covered in great detail in both Sentinel documentation and the articles written by Duncan Napier.

The vpn connection description for remote users is located in /etc/ipsec.conf and reads:

```
conn giac_remote
        type=tunnel
        left=208.200.171.10
        leftnexthop=208.200.171.9
        leftsubnet=192.168.1.0/24
        right=0.0.0.0
        keylife=30m
        authby=secret
        auto=add
```

The configuration defines the ip address, the next hop and protected subnet for the left participant (giac_emp). The right participant (the remote employee) can come from any network. The only method of key exchange supported by Free/SWAN is IKE and the key life is set to 30 minutes. Renegotiation of the connection keys will occur every 30 minutes with perfect forward secrecy enabled (the Free/SWAN default). Therefore, compromise of any given connection key will only compromise the data protected by that key, not future connections. Tunnel mode must be used because the vpn server acts as a gateway to the internal network and, therefore the ultimate destination of a packet to comstruc has a different destination ip address than the IPsec gateway itself. Finally, in order to avoid having the remote user's email account password and username, as well as, the contents of his email traveling across the internet in clear text for anyone to see, encapsulating security payload (ESP) is used. Packet sniffing would now be a more cumbersome and harder proposition for a cracker. ESP provides encryption of the entire packet payload.

The firewall and vpn server are can accept packets with any source ip address using IKE (udp port 500) and ESP (ip protocol 50). However, the vpn server will create connections only for packets from systems with a pre-shared secret listed in the */etc/ipsec.secrets* file. These packets will be decrypted and sent back through the firewall on their way to their final destination. To strictly comply with our firewall policy, only the packets destined for the internal mail servers smtp (port 25), pop3 (port 110) and imap (port 143) will be allowed out of the vpn subnet. Remote users attempting to use other services on other systems or subnets will be denied access.

Assignment 3 - Audit the Security Architecture

GIAC Enterprises requires an audit of their primary firewall. This audit was part of our original scope of work, and is essential before we go live with this environment. A detailed description of the audit process follows.

Plan the audit

The audit to verify that the primary firewall is properly enforcing GIAC Enterprises' security policy must include steps to test the following:

1. Packets that should get dropped are dropped
2. Any activity that should get logged does get logged

We will be performing the audit in two stages. First passive network observation and then real time scanning. In the passive observation phase, samples of our network traffic will be collected from each subnet. The captured packets will be reviewed that should have been dropped by the firewall, but were not, indicating that the firewall is not enforcing correct policy guidelines. In the scanning phase, each service system will be scanned from the internet, service network, vpn and internal subnets. During the scanning, packets on the destination subnet with a source ip address of the scanning system will be captured. Output from the scans, log entries recorded during scanning, and packets capture during scanning will be reviewed to determine if the firewall is enforcing policy and logging properly. The passive observation phase should be during normal business hours when network traffic is usually at its highest point. This part of our audit generates no packets, so it will not affect the networks performance. At least three, one-hour snapshots, taken at different intervals during the day over the span of a week, should benchmark for the individual subnets.

The active scanning will not disrupt GIAC Enterprises normal business operations either since unusual or unexpected packets should be dropped by the firewall before affecting any of its systems. However, it should be carried out at a time when it will cause minimal disruption should any problems occur. The best times are third shift or pre-arranged hours on a weekend or vacation day. System and Network administrator should be notified in advance and necessary personnel should be present to recover from any unexpected down-time event. Back out procedures should also be in place

The total time required by the audit is 40 hours (@ 250$/hour the cost will be $10,000). The effort breaks down as follows:

TCPDUMP filter rule creation	-	3 hours
Scanning script planning and creation	-	2 hours
Equipment setup	-	5 hours
Running tests and collecting data	-	20 hours
Post processing and evaluating results	-	10 hours

The equipment used for the audit are a pair of 4 port hubs and two laptops. The laptops should have network scanning tools (nessus, nmap, sara) and packet capturing (ethereal, tcpdump,ettercap and dsniff) software.

Conduct the audit - Passive Phase

Start by connecting a laptop to a hub placed on the service network between the firewall interface and the switch. Use the following list as a guide to develop the tcpdump filter file that screens out packets known to be allowed on this subnet by the firewall policy (named *servicenetwork.filter*).

```
Allowed packets on service network:
  tcp from NET_SVCNET to anywhere with SYN bit set
  any protocol from NET_SVCNET to NET_SVCNET
  udp from NET_SVCNET to anywhere
  icmp from NET_SVCNET to anywhere
  tcp from GIAC Internal ports 1024:65535 to NET_SVCNET port 22 (and returning)
  tcp from GIAC Internal ports 1024:65535 to giac_sentinal port 80, 443 (and returning)
  tcp from tank ports 1024:65535 to giac_apoak port 25 (and returning)
  tcp from agentsmith ports 1024:65535 to giac_doozer port 53 (and returning)
  udp from agentsmith ports 1024:65535 to giac_doozer port 53 (and returning)
  tcp from any external ports 1024:65535 to giac_apoak port 25 (and returning)
  tcp from any external ports 1024:65535 to giac_doozer port 53 (and returning)
  udp from any external ports 1024:65535 to giac_doozer port 53 (and returning)
  tcp from any external ports 1024:65535 to giac_sentinal port 80, 443 (and returning)
```

Capture packets using the following tcpdump command:

```
tcpdump -n -i eth0 -F servicenetwork.filter -w
servicenetwork.capture

      -i    laptop interface connected to target subnet
```

```
-n    do not resolve IP addresses
-F    use named file to filter capture
-w    write packets to file (not stdout)
```

Next move the laptop to a hub placed on the vpn subnet between the firewall interface and the switch. Use the following list as a guide to develop the tcpdump filter file that screens out packets know to be allowed on this subnet by the firewall policy (named *vpn.filter*).

```
Allowed packets on VPN subnet:
  tcp from giac_emp to anywhere with SYN bit set
  udp from giac_emp to anywhere
  icmp from giac_emp to anywhere
  tcp from GIAC internal ports 1024:65535 to giac_emp port 22 (and returning)
  ip protocol 50 from any external to giac_emp (and returning)
  udp from any external port 500 to giac_emp port 500 (and returning)
```

Capture packets using the tcpdump command given for the service network, substituting vpn subnet filenames, as appropriate.

Now connect the laptop to a hub placed on the internal service subnet between the firewall interface and the switch. Use the following list as a guide to develop the tcpdump filter file that screens out packets know to be allowed on this subnet by the GIAC firewall policy (named *internal.filter*).

```
Allowed packets on internal service network:
  tcp from NET_INTERNAL to anywhere with SYN bit set
  any from NET_INTERNAL to NET_INTERNAL
  udp from NET_INTERNAL to anywhere
  icmp from NET_INTERNAL to anywhere
  tcp from GIAC Internal ports 1024:65535 to NET_INTERNAL port 22 (and returning)
  tcp from GIAC Internal ports 1024:65535 to comstruc port 25 (and returning)
  tcp from GIAC Internal ports 1024:65535 to agentsmith 53 (and returning)
  udp from GIAC Internal ports 1024:65535 to agentsmith 53 (and returning)
  tcp from GIAC Internal ports 1024:65535 to reclaim port 3306 (and returning)
  tcp from giac_emp ports 1024:65535 to comstruc port 25 (and returning)
  tcp from giac_emp ports 1024:65535 to comstruc port 110,143 (and returning)
  udp from giac_emp ports 1024:65535 to tank port 123,514 (and returning)
  tcp from giac_sentinal ports 1024:65535 to reclaim port 22 (and returning)
  tcp from giac_apoak ports 1024:65535 to comstruc port 25 (and returning)
  tcp from giac_doozer ports 1024:65535 to agentsmith port 53 (and returning)
  udp from giac_doozer ports 1024:65535 to agentsmith port 53 (and returning)
  udp from NET_SVCNET ports 1024:65535 to tank port 123,514 (and returning)
  udp from giac_matrix ports 1024:65535 to tank port 514 (and returning)
  udp from giac_zion ports 1024:65535 to tank port 123 (and returning)
```

Finally move the laptop to a hub placed on the subnet between the firewall interface and the border router. Use the following list as a guide to develop the tcpdump filter file that screens out packets know to be allowed on this subnet by the GIAC firewall and border router policy (named *giac_zion.filter*).

```
Allowed packets on the GIAC border router subnet:
  icmp from anywhere to 208.200.171.6 (SNAT firewall interface IP)
  icmp from anywhere to 208.200.171.0/28 (service network and vpn subnets)
  tcp from anywhere ports 1024:65535 to giac_apoak port 25,113 (and returning)
  tcp from anywhere ports 1024:65535 to giac_sentinal port 80,443 (and returning)
  tcp from anywhere ports 1024:65535 to giac_doozer port 53 (and returning)
  udp from anywhere ports 1024:65535 to giac_doozer port 53 (and returning)
  udp from anywhere ports 1024:65535 to giac_emp port 500 (and returning)
  protocol 50 from anywhere to giac_emp (and returning)
```

```
tcp from 208.200.171.6 ports 1024:65535 to anywhere port 20, 21, 22, 80, 443 (and
returning)
tcp from giac_sentinal ports 1024:65535 to credit server port 443 (and returning)
tcp from giac_apoak ports 1024:65535 to anywhere port 25 (and returning)
tcp from giac_doozer ports 1024:65535 to anywhere port 53 (and returning)
udp from giac_doozer ports 1024:65535 to anywhere port 53 (and returning)
```

Capture packets using the tcpdump command given for the service network, substituting the border router subnet filenames, as appropriate. Any packets that are captured by any of the above tests indicate potential problems with the firewall enforcement security policy. If a packet is captured does conform to policy, review the tcpdump filter files for errors or omissions.

Conduct the audit - Scanning Phase

The scanning phase is broken down into internal and external portions. The goal of the internal portion is to verify that the firewall is segmenting internal traffic correctly. The goal of the external portion is to verify that the firewall handles traffic inbound from an ip address outside of the our network correctly. The internal portion utilizes two laptops during each scan, one performing the scans and one listening on the target host's subnet for any packets that are passed by the firewall. Four scans (two tcp, one udp, and one protocol 50) should be run against each target service host using the following *nmap* commands:

```
nmap -sT -p 1-65335 -oN test030102.out -iL SVCNEThosts.list
nmap -sA -p 1-65335 -oN test030102.out -iL SVCNEThosts.list
nmap -sU -p 1-65335 -oN test030102.out -iL SVCNEThosts.list
nmap -sO -p 50 -oN test030102.out -iL SVCNEThosts.list

Flags:  -sT     generic TCP scan
        -sA     TCP ACK scan
        -sU     UDP scan
        -sO     protocol scan
        -p      port or range of ports. exception: Protocol # when sO is used
        -oN     send human readable output to named file
        -iL     read targets from named file
```

To reduce the time required for the audit and insure repeatability of results, scripts containing the appropriate set of nmap commands should be created in advance. Scripts with the appropriate tcpdump command to capture packets generated by each scan should also be developed in advance. In addition, three files to be used as input should be created, each containing a space-separated list of ip addresses for a subnet with service hosts (service network, vpn and internal network). All scripts and input files should be placed on both laptops. The auditing company will be helping us with both the scripts and input files. To insure that all combinations are tested, place laptops according to the following table:

Test #	Scanning Laptop (Source Subnet)	Listening Laptop (Dest. Subnet)
1	Internal Network	VPN Network
2	Internal Network	Service Network
3	Service Network	VPN Network
4	Service Network	Internal Network
5	VPN Network	Service Network
6	VPN Network	Internal Network

The external audit includes a scan generated from an ip address outside the our network against each of the four systems with a publicly routable ip address, giac_sentinal, giac_apoak, giac_doozer and giac_emp. A laptop is placed on the target subnet to capture any traffic that is passed by the firewall. Connect the laptop to the GIAC subnet between the border router and firewall (208.200.171.4/30) and assign it a non-GIAC ip address. Run the same set of four nmap scans against each server, with two modifications. Add the -P0 flag so the scan will run without sending a ping to the host first and change -sT to -sS to run a SYN scan. Note that to avoid return packets being sent back out to the Internet, temporarily add a deny statement for the scanning laptop ip address to ACL 100 for the router (the one applied inbound to ethernet interface looking towards the internal network). Use a tcpdump filter file on the listening laptop design to only capture packets with source host matching the ip address of the scanning laptop. Reviewing the nmap output, the syslog files during the time of the scans and the packet captures will assist us in assessing firewall policy performance.

Evaluate the audit

Recommendations for improvements or alternate architecture

1. Add a reverse-web proxy to allow for a more thorough content based filtering of traffic to giac_sentinal. This would add an additional layer of protection against web based attacks targeting the http server. This step is strongly recommended since GIAC Enterprises uses the web server as the access point for suppliers and partners, so downtime or a compromise of the system would be costly.
2. Consider using RSA public/private key pairs for the vpn authentication instead of a simple pre-shared secret. If a laptop configured for vpn access is stolen, the thief will not be able to access network resources without also having the pass phrase that is protecting the RSA private key on it.
3. Security of the GIAC network could be greatly enhanced by the implementation of an intrusion detection system (IDS). Though we have and idea and server in place (ozzy), we do not have the budget for the dasd needed to log the traffic as of this time. Such a system could alert administrators of pre-attack activities originating from source ip addresses or networks that could then be blocked from accessing the GIAC network. We have discussed the possibility of using snort (http://snort.sourcefire.com/downloads.html) on the firewall or implement a network-based system like shadow (http://www.nswc.navy.mil/ISSEC/CID/) with sensors placed in service network and VPN network reporting to an analyst console in the internal service network (ozzy)

Assignment 4 – Design Under Fire

For the final part of this practical, we will need to choose a previously completed and posted GCFW practical to try to exploit. We will need to find several methods that we can use to attack the architecture presented by the practical. I have chosen the following practical by Daniel Bachrach.

www.giac.org/practical/Daniel_Bachrach_GCFW.doc

In (Figure 2), you will see the design of his network architecture. We will use the following types of attacks against his infrastructure. The first attack will be against the border router. We have identified several possible vulnerabilities in the border router. Some of these are Denial of Service (DoS) attacks, and others will be used to gain access to the router and its protected network. The following is a list of the attacks we will attempt. We will look at the PIX 520 firewall first; it is running version 5.1(1) PIX code.

Cisco Secure PIX Firewall Mailguard Vulnerability
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml
Cisco bug ID CSCdr91002, CSCds30699 and CSCds38708

The PIX firewall has a feature known as "`mailguard`". This function limits the types of smtp commands an attacker can send through the firewall. It will only permit valid smtp application layer commands. The vulnerability can be used to bypass this function. PIX firewalls with software versions up to and including 4.4(6), 5.0(3), 5.1(3) and 5.2(2) are at risk. The problem is with the "`fixup protocol`" command. If you have configurations on the PIX as follows to protect a mail server, your firewall may be vulnerable.

```
fixup protocol smtp 25
```

and either

```
conduit permit tcp host 10.10.10.1 eq 25 any
conduit permit tcp 10.10.10.1 255.255.255.0 eq 25 any
```

or

```
access-list 100 permit tcp any host 10.10.10.1 eq 25
access-group 100 in interface outside
```

This intent of the command and feature is to protect vulnerable mail server software. If the mail servers software is not patched to the fixed version that is vulnerable to this kind of attack, an attack could gain access to it.

Cisco Secure PIX Firewall FTP Vulnerability
http://www.cisco.com/warp/public/707/pixftp-pub.shtml
Cisco Bug ID CSCdr09226

A PIX firewall will interpret ftp commands out of context and open temporary access through the firewall inappropriately. When an internal host clicks on a link for a file transfer, the command is interpreted by the firewall as two separate ftp commands. The host will surprisingly open two connections through the firewall, one with intent and one that it did not intend to. This channel can then be used to send data through the firewall without proper access control. PIX firewalls with software versions up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1) are affected. As before, any PIX with the following commands are at risk: `fixup protocol ftp`

Cisco PIX Firewall Authentication Denial of Service Vulnerability
http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml

Cisco bug ID CSCdt92339

A PIX firewall configured with AAA authentication can be vulnerable to a DoS attack. PIX firewalls with software versions 4.0 up to and including 4.4(8), 5.0(3), 5.1(3), 5.2(2), and 5.3(1) that have AAA configured are vulnerable. An attacking host could utilize all the authentication resources thus preventing valid users from authenticating. This does not affect traffic passing through the PIX, but will prevent others from being authenticated. It could be used with other attacks to gain and keep control of your network resources. An attacking host can exploit the vulnerability as follows. We would use a traceroute to determine if either telnet or ssh is open on the firewall. If either were, we would open multiple sessions of each from a single host. This would lock out any administrator from logging in to the firewall for management purposes. This would be followed with an attack on the internal systems. It would cause confusion and would grant the attacker more time to perform whatever attack they may want to carry out.

The next step of our attack will be compromise a host on the network. We have chosen the Cisco 3524 switch that is located just behind the border router. There are many things that have not been addressed in the router configuration, so we will assume that the same shortcomings have been made in the switch configuration. For example, no effort is made to secure the VTY, CON, or AUX ports of the router. Any host could attempt to make connections to the router at its external interface. Source routing is also allowed. There are several commands that are not used correctly or that just do not exist. The following vulnerability will be used for accessing the switch.

Cisco Secure PIX Firewall TCP Reset Vulnerability
http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml
Cisco bug ID CSCdr11711

The PIX firewall is unable to tell apart a crafted tcp reset packet and a legitimate one. The result is that an attacker can terminate any tcp connection if the connection can be uniquely determined. The problem is independent of firewall configuration. This vulnerability exists in all PIX firewall software releases up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1). The problem with the above versions of software is that they evaluate the validity of the tcp reset based on the source ip of the port and destination ip of the port. If these values are matched in the reset packet, the connection will be torn down. The fix for this will is allowing the firewall to check sequence numbers before it tears down the connection. We have chosen a DOS attack against the PIX firewall.

Cisco Security Advisory: IOS HTTP Authorization Vulnerability
http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html
Cisco Bug ID CSCdt93862

The HTTP server on 3500XL series switches is enabled by default. If it is enabled with local authorization (no TACACS/RADIUS), authentication can be bypassed to allow command execution no matter what the privilege level (1-15 where 15 is highest). All releases of Cisco IOS starting with release 11.3, are vulnerable. Any device running IOS is vulnerable. We need to determine the ip address of the switch. We can use several methods. We can use the dns server, or we could use a tool like nmap or solarwinds to map the network. Another utility that we could use would be Retina. Both of these tools have the ability to identify a Cisco device by certain traits and characteristics that they show. Once we gain the address of the switch, we send a crafted URL request to it. The URL is not the same for all Cisco devices, but there are only 84 possibilities for the URL. It will not be hard finding the right combination. The following is the format of the URL:

```
http://<switch_ip_addres>/level/XX/exec/....

NOTE:  XX is a number between 16 and 99
```

We can gain complete control over the switch with the insertion of one command.

```
snmp-server community AttackerCommunity RW
```

This command will enable us to manage the switch remotely using snmp. The simplicity of the static filters on his border firewall is one of the main reasons for choosing this device. We will follow that command with an "snmp put" to enter this into the configuration.

```
access-list 8 permit imgonnagetya.com
access-list 8 deny any
no snmp-server community AttackerCommunity RW
snmp-server community AttackerCommunity RW 8
```

The above configuration will create an access list that will only allow my attacking network access via snmp for that particular read/write community string. It will remove the initial line we had inserted and replace it with the same line of configuration plus the access list. Once we gain control over this switch, we will then be able to use it to gain access to other network resources, but first we want to cover our tracks. Instead of disabling logging, we will change the logging level to only log critical events. This will stop the switch from logging any configuration changes. Even without logging, we could still be found if the administrators utilize a tool like RANCID (Really Awesome New Cisco Config Differ) found at http://www.shrubbery.net/rancid. RANCID can be set up to notify a set of administrator if any changes occur in the router configurations. We could use the configuration on the switch to give us a tremendous amount of information regarding passwords, snmp community strings, etc. Chances are good that we will be able to use the switch's configuration to gain access to routers and possibly even firewalls. To automate our efforts, we can use a utility that can be found at:

http://packetstorm.widexs.nl/cisco

ios-w3-vul.c is the name of the tool that will scan a Cisco IOS device for the above vulnerability and if the vulnerability exists, it has the ability to fetch the configuration. The above site contains many utilities and scripts that enable an attacker to gain access to poorly configured devices. We also want to look at a possible DoS attack at the border router. The following is a possibility for that type of attack.

IOS Reload after Scanning Vulnerability

http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml
Cisco Bug ID CSCds07326

A security/port scan can cause a memory error in IOS and cause the device to reload. IOS versions 12.1(2)T and 12.1(3)T are affected. When a port scanner attempts to make connections to TCP ports 3100-3999, 5100-5999, 7100-7999, and 10100-10999 the device will unexpectedly reload the next time a command is run that will access the configuration file. The connection attempts will cause memory corruption and the later router reloads. If the router has never had a copy of running-config to startup-config, you can see where this exploit could cause headaches.

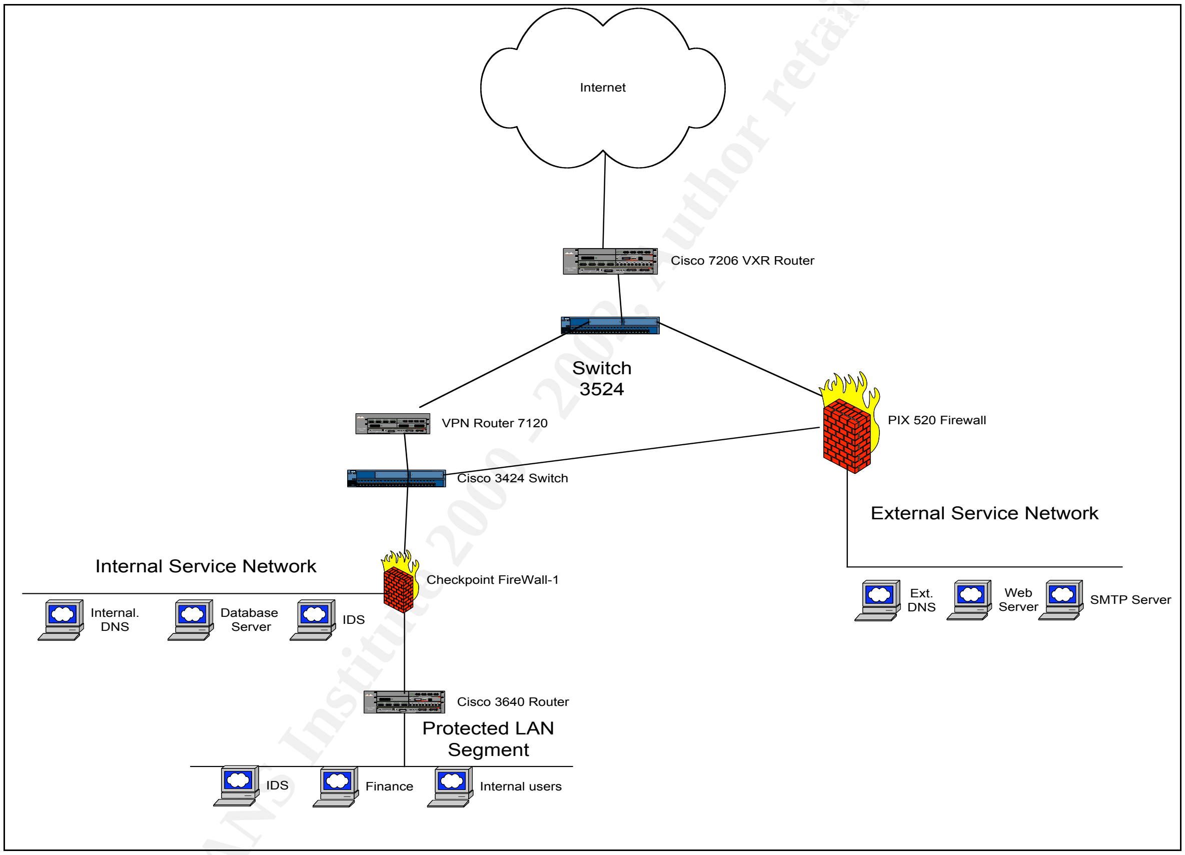


FIGURE 2

Appendix A – AIX Default Secure Installation

Securing AIX Server Installations

IMPORTANT NOTE: SERVER IS TO BE DETACHED FROM NETWORK UNTIL HARDENING IS COMPLETE & SERVER IS CERTIFIED.

You will have to access the SMS (System Management Services) menu to set the install device. To do this at the R/S6000 logo screen hit the F1 (GUI) or 1(ASCII terminal) key before the speaker icon or name appears. At the multiboot icon or line , press enter. Now access the boot sequence icon. Select Install and proceed through the prompts until the default install screen appears.

Here in example 1.1, is the ASCII screen of a default installation screen looks like. The only settings that should have to be changed are the default System Settings in line 1. You will want to set this to New and Complete Overwrite and also just install filesets to one drive for now. You can mirror rootvg later. The loading of filesets could take up to 20 minutes depending on system clock speed.

```
                Installation and Settings

                 Either type 0 and press Enter to install with current settings, or type the
                 number of the setting you want to change and press Enter.

                1  System Settings:
                    Method of Installation.............New and Complete Overwrite
                    Disk Where You Want to Install.....hdisk0

               2  Primary Language Environment Settings (AFTER Install):
                    Cultural Convention................English (United States)
                    Language ..........................English (United States)
                   Keyboard ..........................English (United States)
                   Keyboard Type......................Default

               3  Advanced Options

    >>> 0  Install with the current settings listed above.

                                                   +----------------------------------------------------
    88  Help ?                                      |   WARNING: Base Operating System Installation will
    99  Previous Menu                               |   destroy or impair recovery of ALL data on the
                                                    |    destination disk hdisk0.

>>> Choice [0]:
```

Example 1.1

After the filesets have been loaded onto the server, you will be asked several configuration questions. Once again in figure 1.2, the snapshot is taken from an ASCII screen. You can see what the configurable options will be. For the purpose of the base install, we only need to concern ourselves with the selections that have been highlighted. The options are self-explanatory except for the option to install software applications. Once again we need to implore you to establish a policy of least access.

Installation Assistant

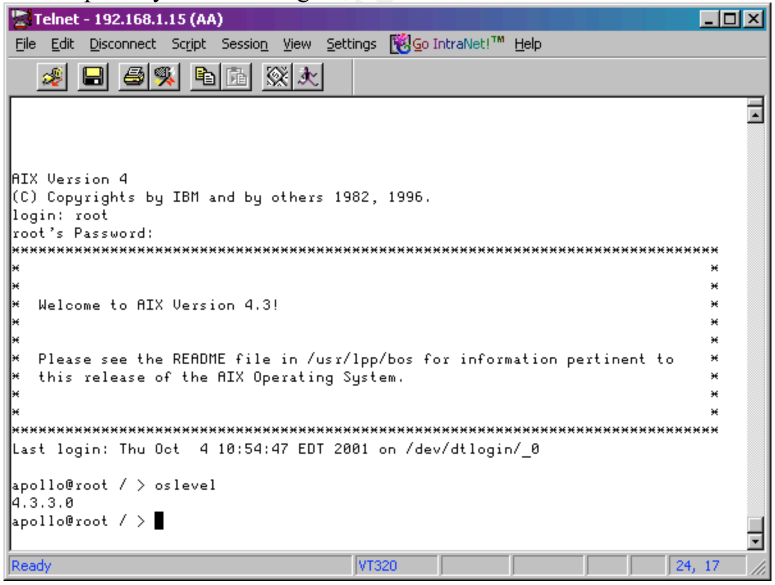
Move cursor to desired item and press Enter.

```
➡ Set Date and Time
➡ Set root Password
  Set Installation Device
  Configure Network Communications
➡ Manage System Storage and Paging Space (rootvg)
  Manage Language Environment
  Create Users
  Define Printers
  Import Existing Volume Groups
➡ Install Software Applications
  Back Up the System
  Using SMIT (information only)
  Tasks Completed - Exit to Login


F1=Help         F2=Refresh       F3=Cancel        F8=Image
F9=Shell        F10=Exit         Enter=Do
```

Example 1.2

This is a **BOS** or **b**ase **o**perating **s**ystem installation of IBM's AIX software. As far as what filesets have been loaded by default, you can see them in Appendix A.
Upon rebooting the server when the R/S 6000 logo screen appears hit the F1 (Function one key) before the last speaker icon is shown on the screen. You need to go into the System Management Services menu to do 3 things. First you need to go and set your bootable device table. At the main 3 panel screen, click on multiboot and then Boot Sequence. Just choose the hdisk that the OS resides on. This is to prevent a floppy, tape or cd to be booted to to cause a compromise. Second you need to setup a power up password and a privileged password to protect hardware and assembly/machine code language. At the 3 panel screen select Utilities, then Password. Chose an 8 character power on & an 8 character privileged password to prevent access to both the system OS and the SMS configuration menus.

The output of your new image is shown below:


Telnet - 192.168.1.15 (AA)
File Edit Disconnect Script Session View Settings Go IntraNet!™ Help
Ready
VT320
24, 17

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password:
********************************************************************************
*                                                                              *
*                                                                              *
*  Welcome to AIX Version 4.3!                                                 *
*                                                                              *
*                                                                              *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                   *
*                                                                              *
*                                                                              *
********************************************************************************
Last login: Thu Oct  4 10:54:47 EDT 2001 on /dev/dtlogin/_0

apollo@root / > oslevel
4.3.3.0
apollo@root / > 
```

Example 1.3

Now you want to load the latest microcode and ptf's for AIX 4.3.3.x. First lets look at how to do the latest maintenance level of AIX. You can obtain the latest maintenance level at:

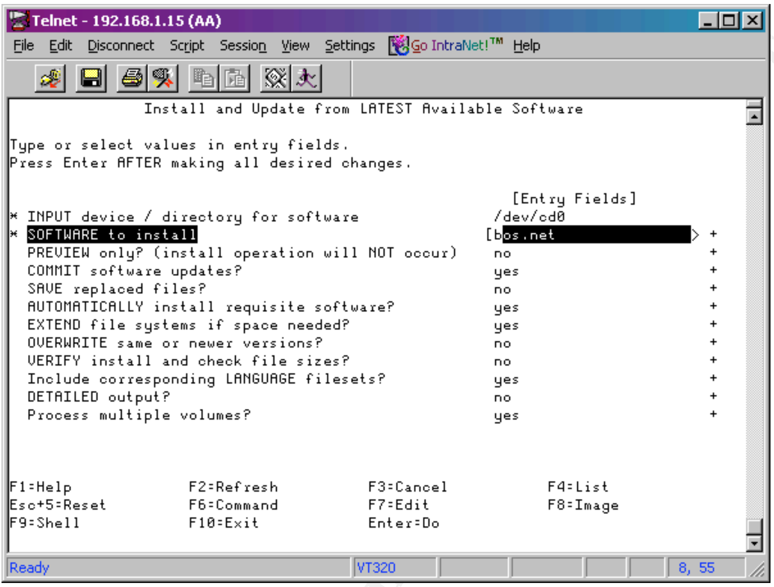
http://techsupport.services.ibm.com/support/rs6k/ml.fixes.html

As a matter of convenience, setup a separate jfs of /usr/local/bin/aix_ptfs/AIX4.3.3.09 or something along those lines. Put all the gzip files in here.

After obtaining the fixes, we will now install them. For easier distribution you will want to install them into a central repository, from which we can use an nfs mount point to distribute them.

You will now want to load out some additional filesets that are needed for this installation, including bos.net and bos.perf filesets.

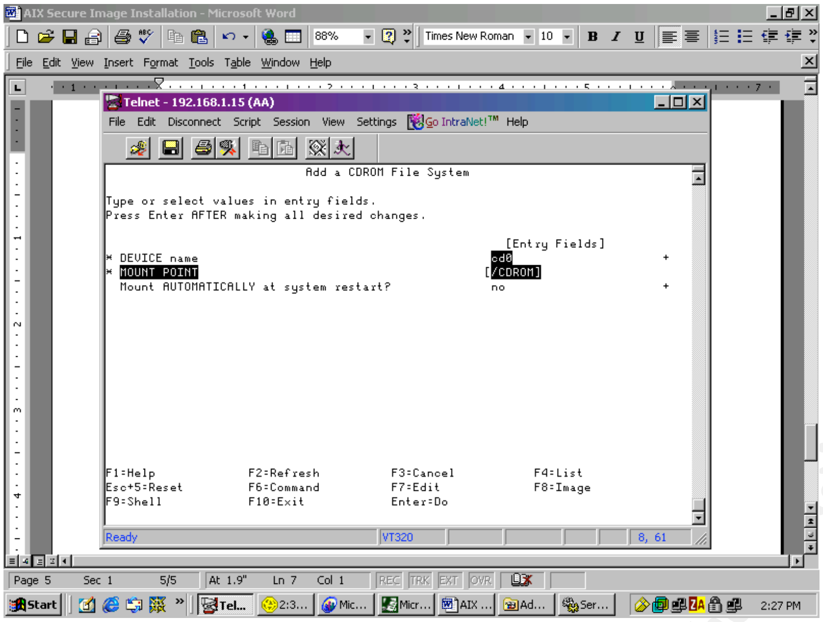
If you notice in example 1.4, these filesets will be committed to the kernel


Telnet - 192.168.1.15 (AA)
File Edit Disconnect Script Session View Settings Go IntraNet!™ Help
Ready
VT320
8, 55

```
                    Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* INPUT device / directory for software               /dev/cd0
* SOFTWARE to install                                [bos.net           >  +
  PREVIEW only? (install operation will NOT occur)    no                   +
  COMMIT software updates?                            yes                  +
  SAVE replaced files?                                no                   +
  AUTOMATICALLY install requisite software?           yes                  +
  EXTEND file systems if space needed?                yes                  +
  OVERWRITE same or newer versions?                   no                   +
  VERIFY install and check file sizes?                no                   +
  Include corresponding LANGUAGE filesets?            yes                  +
  DETAILED output?                                    no                   +
  Process multiple volumes?                           yes                  +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Example 1.4

At this time, we will be setting up a cdrom mount point on the system. The issues from a security standpoint are to make the directory privileged and also not to let it mount automatically. Type in smitty cdrfs from the command line. Here in example 1.5, you can see the settings of the cdrfs:



AIX Secure Image Installation - Microsoft Word
Telnet - 192.168.1.15 (AA)
File Edit Disconnect Script Session View Settings Go IntraNet!™ Help
Ready
VT320
8, 61

```
                         Add a CDROM File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* DEVICE name                                           cd0                   +
* MOUNT POINT                                          [/CDROM]
  Mount AUTOMATICALLY at system restart?                no                    +

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Example 1.5

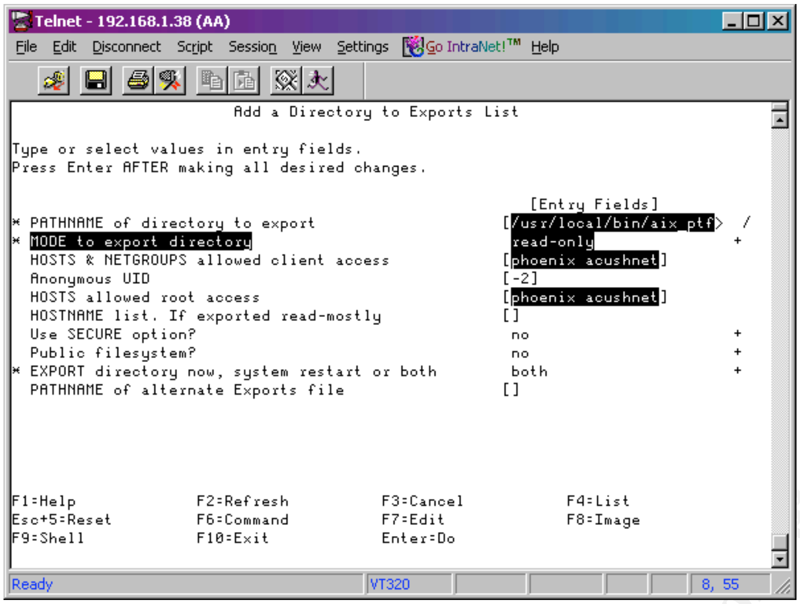
The reason why you do not want the filesystem to mount automatically is access to the /CDROM mount point. Also allowing this mount to be exported with NFS opens up this vulnerability to the entire realm. Also if a person has written some exploit Trojan code to a cd, they (if the have physical access to the server) can put the cd in the drive and move the code to the server by this mount point. Which if they have physical access to the console the game would be over. So once again follow this rule of thumb, "Only allow as little functionality to allow for people to do their jobs. "

Now since the downloads are of the gzip variety, you must obtain gunzip. And the best place to obtain them for the AIX operating system is at the following web site:

http://freeware.bull.net/

At this time all we need is gnu.gzip-1.2.4.1, but we will be returning for other tools later. To keep oneself organized better create a freeware directory like /usr/local/bin/freeware to house these files. After obtaining the binary run ./gnu.gzip-1.2.4.1 to uncompress it. It automatically builds the .toc file for you. Now you can go into the smitty installp screen and install the .bff's. After the binary has been installed you can know gunzip the maintenance level download bundles. After un-bundling , you can un-tar them. Now you can go ahead and run smitty update_all to update the filesets that are loaded as part of the BOS install. The key is to make sure that the filesets are **not** committed, that way they can be backed off more easily, as we show in example 1.7: Also note **ONLY** export to the servers in your environment by name. Using the export to everyone is the default setting and it is both very insecure.

To make this update accessible through the AIX realm, the nfs directory must know be created. Using the smitty compat as you can see in example 1.9, the secure method is used:


Telnet - 192.168.1.38 (AA)
File Edit Disconnect Script Session View Settings Go IntraNet!™ Help

```
                        Add a Directory to Exports List

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* PATHNAME of directory to export                      [/usr/local/bin/aix_ptf>  /
* MODE to export directory                              read-only               +
  HOSTS & NETGROUPS allowed client access              [phoenix acushnet]
  Anonymous UID                                        [-2]
  HOSTS allowed root access                            [phoenix acushnet]
  HOSTNAME list. If exported read-mostly               []
  Use SECURE option?                                    no                      +
  Public filesystem?                                    no                      +
* EXPORT directory now, system restart or both          both                    +
  PATHNAME of alternate Exports file                   []




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Example 1.6

USER ACCOUNTS AND PASSWORD PREPARATION

root accessibility has to be locked down, and user access has to be limited. The best way to accomplish this is to change root's password on ALL SYSTEMS and to make it UNIQUE on each system. This way the IT Administration department will have control over the environment and know of all changes in it. Also remote access to a direct root shell must be changed. All this takes is a change in smitty to root's remote login field... (remote login = false). This will force all root activity to be done thru a /home/$USER environment shell using the $PATH configuration that sys admin has set up. Also su capability for the everyday user must be changed. This can be done in the /etc/security/user file.

Default	Recommended
default:	default:
admin = false	admin = false
login = true	login = true
su = true	su = false
daemon = true	daemon = true
rlogin = true	rlogin = true
subgroups = ALL	sugroups = ALL
admgroups =	admgroups =
ttys = ALL	ttys = ALL
auth1 = SYSTEM	auth1 = SYSTEM
auth2 = NONE	auth2 = NONE
tpath = nosak	tpath = nosak
umask = 022	umask = 077
expires = 0	expires = 0
SYSTEM = "compat"	SYSTEM = "compat"
logintimes =	logintimes =
pwdwarntime = 0	pwdwarntime = 14
account_locked = false	account_locked = false
loginretries = 0	loginretries = 3

histexpire = 0	histexpire = 26
histsize = 0	histsize = 6
minage = 0	minage =2
maxage = 0	maxage = 4
maxexpired = -1	maxexpired = 4
minalpha = 0	minalpha = 2
minother = 0	minother = 1
minlen = 0	minlen = 8
mindiff = 0	mindiff = 3
maxrepeats = 8	maxrepeats = 2
dictionlist =	dictionlist =/usr/share/words
pwdchecks =	pwdchecks =

These recommended parameters should be used for all new users. The definitions are given in the previous sections in regards to AIX General Security on pages 6 thru 8. But some of the differences are in regards to default world-readability for users umask = 022, to more refined password qualifications maxage =4 (weeks).

Another issue is unattended sessions. A variable TMOUT=xx variable should be part of the users .profile. This can easily be done by modifying the /etc/security/.profile file to give all new users the same .profile to protect both the $PATH and other issues with the default shell. Also another useful change should be to add the $PWD to the default .profile which would allow them to see their current $PATH without having to type in present working directory. This would help in allowing users who work in multiple directories to know at all times where they are.

Also a good security maintenance plan would include overall group, userid and user account configuration. A good first step is to routinely run these commands:

1. grpck - which examines all users listed as group members are indeed defined as users. Example: grpck -t ALL
2. usrck - verifies parameters of a userid definition. Example: usrck -t ALL
3. pwdck - checks users authentication stanzas. Example: pwdck -t ALL

NOTE: The -t flag allows for prompting for corrective action,
Get a report please use the -n flag. Also the lsgroup and the lsuser commands can be helpful.

Some other things to consider are editing the /etc/motd to provide a detailed business objective and warning to all users.

And to edit the /etc/security/login.cfg to add specific verbiage (herald) warning that this system is secure and that auditing is taking place.

Also the extended access control lists or acl could be used along with numerous other features of AIX. A great tool to get is tcpwrappers which you can obtain from the bull site. It provides further ACL functionality, while also establishing a level of HIDS (Host Intrusion Detection System).

FILE SYSTEM SECURITY

In AIX the journaled file system (jfs) does not require user or administrative intervention. Logging of the file system and fsck are done automatically. Issues that should be looked into are the availability of common users to mount filesystems and remove the filesystems. So called "world" access should be changed to prevent this. Though this is more of a usability issue then security, it should be looked into. Also CD-ROM's can be executed using suid root file privileges. Someone could create an extremely dangerous suid root program on another system and create a CD-ROM containing this file. They then could mount it on your system an execute it with suid root authority. To prevent this, use the -o flag when mounting a /CDROM and also include it in all batches or scripts using this filesystem.

Now the reason gid and uid are important is it allows access to the different files and directories on these systems. That is why a comprehensive structure should be in place to limit user's access to these files using group, user and permissions security concepts.

```
sp2-node81# find / -perm -0007 -type d -print

/var/adm/ras
/var/locks
/var/msgs
/var/news
/var/preserve
/var/spool/secretmail
/var/spool/uucppublic
/tmp
/usr/lpp/servdir
/usr/lpp/servdir/sd_calls
/usr/lpp/bos.net/inst_root/var/spool/secretmail
/usr/lpp/bos.net/inst_root/var/spool/uucppublic
/usr/lib/cns
/usr/lib/cns/tools
/usr/system/tools/platinum/autouser
/usr/system/tools/platinum/autouser/out
/usr/system/tools/platinum/autouser/sounds
/usr/system/tools/platinum/autouser/archive
/usr/system/prism/prod/logs/PRIMLOC
/usr/system/prism/prod/working/provinterf/bcp
/usr/system/prism/prod/working/ENA/Unprocessed/original
/usr/system/prism/prod/working/nov
/usr/system/prism/prod/working/nov/provinterf/bcp
/usr/system/prism/prod/working/oct
/usr/system/prism/prod/working/oct/provinterf
/usr/system/prism/prod/working/oct/provinterf/bcp
/usr/system/prism/prod/working/sept
/usr/system/prism/prod/working/sept/provinterf
/usr/system/prism/prod/working/sept/provinterf/bcp
/usr/system/provconv
/usr/system/provconv/lost+found
/usr/system/provconv/data1
/usr/system/provconv/data1/pta
/usr/system/provconv/data2
/usr/devel/src/caraccess
/usr/devel/src/custserv
/usr/devel/src/custserv/src
/usr/devel/src/custserv/t
/usr/devel/src/edms
/usr/devel/src/edms/handling
/usr/devel/src/edms/src
/usr/devel/src/ena
/usr/devel/src/ena/procs
/usr/devel/src/ena/sqlscripts
```

```
/usr/devel/src/ena/unixscripts
/usr/devel/src/letters
/usr/devel/src/letters/maint
/usr/devel/src/letters/newlet
/usr/devel/src/letters/nroff
/usr/devel/src/opti
/usr/devel/src/phone
/usr/devel/src/util
/usr/stk/reel
/usr/stk/reel/lib/REEL/TMP
/usr/stk/reel/lib/REEL/TMP/Dlocks
/usr/legato/tmp
/usr/legato/applogs
/u/jmf2
/u/jmf2/bin
/u/jmf2/bin/util
/u/jmf2/bin/install
/u/jmf2/bin/logs
/a/hps1-5/usr/users/DBA
/a/hps1-5/usr/users/DVL
```

Without knowing what these files do, I don't believe world writable functionality of the /usr/devel and /usr/system/prism directory tree is appropriate. Things like this should be addressed. The /tmp and lost + found directories are special cases, but the other files should be looked into. This is another reason to look into the trusted computing base or tcb.

Network Security

TCP/IP by default provides adequate secure authentication in its operational environment. Commands such as ftp, rexec and telnet provide this, although once the person is into the environment all bets are off. For this reason, a look at the script /etc/securetcpip should be considered. This will disable the daemons: rshd, rlogind and tftpd. Also the commands: rlogin, rcp, rsh, and tftp. Basically, this script disables these processes in the /etc/inetd.conf file, and can be reversed. It creates a /etc/security/config file that restricts .netrc usage by ftp and rexec also. This will provide better administrative control and network security by preventing unauthorized users from having access to your systems. It will force telnet to be used. The only issue we see is to plan on modifying the tftpd to allow NIM installs for the SP's.

Another way you could secure the infrastructure is to make better use of the /etc/hosts.equiv function in AIX, if securetcpip is not used. By setting up hosts and user parameters this will allow entry to this particular system, for each user that needs access. The .rhosts files that are liberally used are not in itself, a problem. But since root is exposed their use should be eliminated by removing them or disabling rlogin by running securetcpip. The .netrc files are a security risk because they contain unencrypted password information that control outgoing user traffic and not incoming as .rhost and hosts.equiv do.

NFS mounted filesystems should always be read-only. The reason why this is important is that access to this directory must be restricted in some why, unless every user involved is trustworthy. Two things must be done. First by default option for NFS file system is read-write, so changing this to read-only is necessary. Become as detailed as possible with the pathname, no allowing full directory use.

Example: /usr/local/bin/stuff not /usr/local/bin.

As was mentioned before, using /etc/ftpusers is recommended to eliminate ftp as a security risk on your systems.

Logging and Auditing

Though AIX has a standard accounting subsystem, other more system intensive auditing can be enabled. If you suspect a problem, enable auditing at that point, otherwise the overhead is not needed. Though these system logs are not very useful against root, by restricting access to root, you will have better control of the environment.

/var/adm/wtmp - contains user log info for every entrance and exit from the system. Syntax: last $usrname or who -a for the whole file.

/etc/utmp - contains info in regards ro current active users and subsystems. Syntax last $username or who -a for whole file.

/var/adm/sulog - contains su command usage. Syntax: pg or cat.

/etc/security/failedlogin - contains failed logins. Syntax is who -a.

/etc/security/lastlogin - This is used by the system as a overall logging file. It is not useful since it contains seconds since January 1, 1970. But a script can be used against this file to provide a better logging record.

If auditing is deemed necessary using a basic audit stream and object profile mode would be the best method. It is highly recommended that a plan be formulated to enable this when necessary. We do not believe there is one in place at the present time. Also a rather sophisticated product called Stalker for AIX/6000 is available from Haystack Labs, Inc. in Austin, Tx. This allows centralized monitoring of multiple R/S 6000 systems.

Auditing events and objects

A list of audit events built into AIX, along with a list of predefined audit objects, can be found in the file /etc/security/audit/events.

In general, auditing events are defined at the system call level. A single operation at the command line would result in records of several events in the audit trail. For example, when viewing a file using the cat or more command, you would see the following records logged into the audit trail:

FILE_Open (file is opened)
FILE_Read (file is read)
FILE_Write (file is written to standard output)
PROC_Create (process creation for more OR cat)
PROC_Execute (command execution)
PROC_Delete (process completion)

Auditing all possible events can produce a huge amount of data. Through audit controls (that is, modifying the configuration files), you can select events to be recorded.

Audit events are grouped into classes. The events can be defined by which events are in a class. While the class names are arbitrary, they, rather than individual event names, are associated with user IDs when the audit subsystem is active.

Auditing objects are just individual files that will be monitored. Three operations can be audited: read, write, and execute.
Objects are not associated with user IDs. Audit records are generated whenever an audited object is referenced by any user (including root).

To add further audit objects, extend the /etc/security/audit/objects file.

Auditing mode: BIN and STREAM

There are two modes of operation for auditing: BIN and STREAM. BIN mode writes the audit trail to alternating temporary files (bins), then to a single trail file. STREAM mode writes to a circular buffer that is read synchronously through an audit pseudo-device (/dev/audit).

An audit can be started in one OR both of these modes.

Using the audit configuration setup shipped with AIX, /etc/security/audit/config, the BIN mode alternates between /audit/bin1 and /audit/bin2. When one BIN is full (the binsize parameter determines the size of the bin), the audit switches to the other BIN file while adding the accumulated data in the first file to the audit trail (defined in /etc/security/audit/bincmds), /audit/trail. Use audit shutdown to be certain that all audit records have been added to /audit/trail. The BIN mode audit record is in binary format. You can read it with audit commands such as auditpr.

In STREAM mode, the default AIX configuration provides a program to read the STREAM buffer and processes each record with the commands found in /etc/security/audit/streamcmds. These commands format the output into human-readable form and write it in /audit/stream.out. This file is NOT cumulative; it is restarted every time the audit is restarted. The STREAM audit trail can be read in real time by reading /audit/stream.out, or by sending output directly to a terminal or printer.

Starting and stopping audit

There are five audit subcommands for invoking auditing. They are as follows:

audit start
  to activate the audit subsystem (This is the only correct way to start audit.)

audit shutdown
  to stop auditing subsystem, processing final BIN records and removing the /audit/auditb file that is used as an "active" indicator by the audit modules
audit off
  to suspend auditing temporarily
audit on
  to resume audit after audit off
audit query
  to display the status of auditing

NOTE: Using audit commands in the wrong order can confuse the auditing subsystem. If the auditing subsystem gets confused, reset everything by deleting all files in the /audit directory (except trail, stream.out and bin files).

Auditing can be run at the discretion of the system administrator. Depending on the environment, it is usually not necessary to have auditing running at all times. If it is configured to monitor a large number of events or objects at all times, the amount of data generated would be so substantial that its overhead would outweigh its benefit. It is worthwhile to take time to configure auditing to collect selected information.
To start auditing at system startup, add the following line to the /etc/rc file, just prior to the line reading dspmsg rc.cat 5.

'Multi-user initialization completed':

```
    /usr/sbin/audit start
```

If auditing is running at all times, make sure to run or to add the following in the /usr/sbin/shutdown script to properly shut down:

```
/usr/sbin/audit shutdown
```

Auditing configuration

All auditing related configuration files reside in /etc/security/audit. The /etc/security/audit/config file contains the key audit controls. It has the following stanzas:

start - specifies whether BIN or STREAM (or both) should be used for auditing
bin and stream contain controls for each mode; the names of the BIN files are specified here
classes defines several groups (classes) of auditing events

The predefined classes are: general, objects, SRC, kernel, files, SVIPC, mail, cron, and TCP/IP. New classes can be defined using the auditing events in the /etc/security/audit/events file. All audit classes except the objects class are associated with user IDs. For example, audit the events defined as general and TCP/IP for user root.

user stanza lists specified users and the audit classes assigned to them; each user name must be the login name of a system user or the string 'default'.

An example of this stanza is as follows:

```
users:
           root = general
           joe = general, files, TCPIP
          default = general
```

When auditing starts, it ALWAYS audits the events specified for every user ID defined in the config file and ALL the objects defined in /etc/security/audit/objects. If the objects' audit records are not wanted, remove or comment out (using an *) the objects defined in the objects file.

If there are specific classes of events that are not wanted as audit records, specify No_Events for that specific class in the config file.

For example:

```
files = No_Events
     or
tcpip = No_Events
```

The objects file contains all objects to be audited when auditing is active. A user defined object is displayed as:

```
/home/joe/my.stuff:
                r = "JOE_READ"
                w = "JOE_WRITE"
```

The names JOE_READ and JOE_WRITE are referenced in the /etc/security/events file to define the format of the auditpr output:

```
JOE_READ = printf "%s"
JOE_WRITE = printf "%s"
```

NOTE: There is no need to add the newly added objects to the objects stanza in the /etc/security/audit/config file, since the objects line is not referenced. Only the objects file is referenced.

The streamcmds file has commands that are entered for STREAM audit records. The default file contains one command.

Enter:

```
   /usr/sbin/auditstream | auditpr > /audit/stream.out &
```

Adding the -v flag for the auditpr command improves this command at the expense of having more information. Without -v, full path names for files are not shown in the audit output; only file descriptors are recorded.

To limit the amount of data collected during the auditing operation, use the -c option on the auditstream command to select a specific class of events as defined in the config file, or use the auditselect command to select specific events.

For example:

NOTE: This command must be all on one line in the streamcmds file. This command will collect only FILE_Open event records.

```
 /usr/sbin/auditstream | /usr/sbin/auditselect -e "event == FILE_Open"
 | auditpr -v > /audit/stream.out &
```

NOTE: The following command will limit data collection to only the TCP/IP class of events as defined in the config file.

```
   /usr/sbin/auditstream -c tcpip | auditpr -v > /audit/stream.out &
```

The bincmds file contains commands that are entered whenever a BIN file fills or when auditing is shut down. The file distributed reads like the following:

```
   /usr/sbin/auditcat -p -o $trail $bin
```

The environment variables in the preceding command are defined while auditing is active. The auditselect command can be added to select specific events, reducing the amount of audit records.

The bincmds file will only collect audit records that match USER_SU or USER_Login audit events. Enter:

```
   /usr/sbin/auditselect -e "event== USER_SU || event== \
     USER_Login" $bin > /audit/trail.login
```

Auditing a user

For example:

1.To audit classes, use the fastpath command smit chuser.

```
    *User NAME            [joe]
    AUDIT classes         [general, files]
```

A user stanza should be displayed for joe in /etc/security/audit/config file.

2.At the command line, edit the /etc/security/config file. In the classes stanza, add the following new class:

```
    procmon = PROC_Create, PROC_Delete, PROC_Execute
```

In the users stanza, the following could exist:

```
    joe = procmon
```

The newly assigned audit classes will take effect at the next login for user joe.

3.The BIN mode audit trail can be read with the following:

```
    auditpr -v < /audit/trail | more
```

The STREAM mode audit file /audit/stream.out can be viewed directly. Remember that the /audit/stream.out file is rewritten each time the auditing subsystem is started. Save the old stream.out before starting auditing.

If you do not want the objects audit records when auditing a user ID, comment out the objects defined in the /etc/security/audit/objects file or rename this file.

Auditing an object

In the following example, all processes writing to the /etc/utmp file will be audited.

1.Edit the /etc/security/audit/objects file to add the following:

```
/etc/utmp:
w = "UTMP_WRITE"
```

2.Edit the /etc/security/audit/events file to include the following:

```
* /etc/utmp
UTMP_WRITE = printf " %s "
```

The audit record is displayed as follows:

```
UTMP_WRITE      root    OK      Wed Jul 12 12:12:25 1995  init
```

In this case, the init process owned by root wrote to the file.

NOTE: The length of an audit event or object name cannot exceed 15 characters. This limit is defined in the header file /usr/include/sys/audit.h, ah_event [16]. The following error message usually indicates an invalid event or object name.

```
"auditevents (): Invalid argument"
```

Disk space consideration

Each record in the audit trail takes about 50 to 150 bytes depending on what mode is used and whether the verbose mode flag is specified. This means that 1MB of data could contain about 6800 entries.

Understanding the output

It is important to specify what information should be reviewed while auditing. Although you can configure auditing to record events of interest, there may still be too much data to be useful when viewed all at once.

The auditselect command can be used with auditpr to sort through volumes of information and pull out only that which is needed for a specific report. It can be used to pull all data from a specific time period, for a specific user, or for a specific event, or any combination of these three.

For example:

```
/usr/sbin/auditselect -f /audit/pick \
/audit/trail | /usr/sbin/auditpr -v
```

The /audit/pick file reads as follows:

```
command == rlogin && \
time >= 08:00:00 && time <= 17:00:00 && \
data >= 04/01/96 && date <= 04/12/96
```

This command reports the use of the rlogin command within the specific time interval (8AM-5PM between April 1 and April12).

The compressed trail data from the binmode auditing is not in the same format at AIX version 3.2 as it is in 4.1 or later. There is a utility to convert the data from a pre-AIX Version 4 format to the Version 4 format. It is a command called auditconv.

Common problems with auditing
Errors when starting audit
There are certain errors that appear when running audit start.

Error message:

```
** failed setting kernel audit objects
```

This occurs when there is a syntax error in the /etc/security/audit/objects file.
Error message:

```
auditbin: ** failed backend command
/etc/auditcat -p -o /audit/trail -r /audit/bin1
```

This error can be corrected by removing or renaming the BIN files. It is sometimes helpful to run audit shutdown again
and then to retry audit start.

Error in config file:

It is necessary to have the user stanza in the /etc/security/audit/ configuration file or the following error will display when
you start auditing:

```
Unable to find the user stanza in /etc/security/audit/config
```

If it is not obvious that the user stanza is missing, verify that each of the classes are defined on a single continuous line.

Data overload

Given the way that cron and the TCPIP code is written, each sets up its own set of audit events. These events will get written into the audit trail regardless of how the config files are set up. The workaround is to use auditselect to exclude these events when generating the audit report. TCPIP sessions, ftpd, rexecd, and telnetd all call auditproc() to set up process auditing using the class tcpip in /etc/security/audit/config. The same thing is done in the cron code (at, cron, and cronadm) for the cron class in /etc/security/audit/config. These events will be written into the audit trail. The best thing to do is to filter them using auditselect.

For example:

```
   auditselect -e"event!=AT_JobAdd && event!=AT_JobRemove && ..."
```

This will exclude events AT_JobAdd and At_JobRemove and so on.

Or select on the command name:

```
    auditselect -e"command!=cron && command!=at && ..."
```

Base AIX 5.1 install filesets:

```
 Fileset                      Level  State  Description
 ----------------------------------------------------------------------------
 IMNSearch.bld.DBCS         2.3.1.0    C    NetQuestion DBCS Buildtime Modules
 IMNSearch.bld.SBCS         2.3.1.0    C    NetQuestion SBCS Buildtime Modules
 IMNSearch.msg.en_US.rte.com  2.3.1.0    C    Text Search Messages - U.S. English
 IMNSearch.rte.DBCS         2.3.1.0    C    NetQuestion DBCS Search Engine
 IMNSearch.rte.SBCS         2.3.1.0    C    NetQuestion SBCS Search Engine
 IMNSearch.rte.client       2.3.1.0    C    Text Search Client
 IMNSearch.rte.com          2.3.1.0    C    Text Search Client/Server Shared Files
 IMNSearch.rte.httpdlite    2.0.0.2    C    Lite NetQuestion Local Web Server
 IMNSearch.rte.server       2.3.1.0    C    Text Search Server
 Java130.rte.bin            1.3.0.0    C    Java Runtime Environment Executables
 Java130.rte.lib            1.3.0.0    C    Java Runtime Environment Libraries
 Netscape.communicator.com  4.7.5.0    C    Netscape Communicator Common Files
 Netscape.communicator.us   4.7.5.0    C    Netscape Communicator U.S.Version
 Tivoli_Management_Agent.client.rte  3.2.0.0    C    Management Agent runtime"
 X11.Dt.ToolTalk            5.1.0.0    C    AIX CDE ToolTalk Support
 X11.Dt.bitmaps             5.1.0.0    C    AIX CDE Bitmaps
 X11.Dt.helpmin             5.1.0.0    C    AIX CDE Minimum Help Files
 X11.Dt.helprun             5.1.0.0    C    AIX CDE Runtime Help
 X11.Dt.lib                 5.1.0.0    C    AIX CDE Runtime Libraries
 X11.Dt.rte                 5.1.0.0    C    AIX Common Desktop Environment (CDE) 1.0
 X11.apps.aixterm           5.1.0.0    C    AIXwindows aixterm Application
 X11.apps.clients           5.1.0.0    C    AIXwindows Client Applications
 X11.apps.config            5.1.0.0    C    AIXwindows Configuration  Applications
 X11.apps.custom            5.1.0.0    C    AIXwindows Customizing Tool
 X11.apps.msmit             5.1.0.0    C    AIXwindows msmit Application
 X11.apps.pm                5.1.0.0    C    AIXwindows Power Management GUI  Utility
 X11.apps.rte               5.1.0.0    C    AIXwindows Runtime Configuration Applications
 X11.apps.util              5.1.0.0    C    AIXwindows Utility Applications
 X11.apps.xterm             5.1.0.0    C    AIXwindows xterm Application
 X11.base.common            5.1.0.0    C    AIXwindows Runtime Common Directories
 X11.base.lib               5.1.0.0    C    AIXwindows Runtime Libraries
 X11.base.rte               5.1.0.0    C    AIXwindows Runtime Environment
 X11.base.smt               5.1.0.0    C    AIXwindows Runtime Shared Memory Transport
 X11.fnt.coreX              5.1.0.0    C    AIXwindows X Consortium Fonts
 X11.fnt.defaultFonts       5.1.0.0    C    AIXwindows Default Fonts
 X11.fnt.iso1               5.1.0.0    C    AIXwindows Latin 1 Fonts
 X11.loc.en_US.Dt.rte       5.1.0.0    C    AIX CDE Locale Configuration - U.S. English
 X11.loc.en_US.base.lib     5.1.0.0    C    AIXwindows Client Locale Config - U.S. English
 X11.loc.en_US.base.rte     5.1.0.0    C    AIXwindows Locale Configuration - U.S. English
 X11.motif.lib              5.1.0.0    C    AIXwindows Motif Libraries
 X11.motif.mwm              5.1.0.0    C    AIXwindows Motif Window Manager
 X11.msg.en_US.Dt.helpmin   5.1.0.0    C    AIX CDE Minimum Help Files - U.S. English
 X11.msg.en_US.Dt.rte       5.1.0.0    C    AIX CDE Messages - U.S. English
 X11.msg.en_US.apps.aixterm 5.1.0.0    C    AIXwindows aixterm Messages - U.S. English
 X11.msg.en_US.apps.clients   5.1.0.0    C    AIXwindows Client Application Msgs - U.S. English
```

```
X11.msg.en_US.apps.config  5.1.0.0    C    AIXwindows Config Application Msgs - U.S. English
X11.msg.en_US.apps.custom  5.1.0.0    C    AIXwindows Customizing Tool Msgs - U.S. English
X11.msg.en_US.apps.pm      5.1.0.0    C    AIXwindows Power Mgmt GUI Msgs - U.S. English
X11.msg.en_US.apps.rte     5.1.0.0    C    AIXwindows Runtime Config Messages - U.S. English
X11.msg.en_US.base.common  5.1.0.0    C    AIXwindows Common Messages - U.S. English
X11.msg.en_US.base.rte     5.1.0.0    C    AIXwindows Runtime Env. Messages - U.S. English
X11.msg.en_US.motif.lib    5.1.0.0    C    AIXwindows Motif Libraries Messages - U.S. English
X11.msg.en_US.motif.mwm    5.1.0.0    C    AIXwindows Motif Window Mgr Msgs - U.S. English
X11.msg.en_US.vsm.rte      5.1.0.0    C    Visual System Mgmt. Helps & Msgs  - U.S. English
X11.vsm.lib                5.1.0.0    C    Visual System Managment Library
bos.adt.lib               5.1.0.0    C    Base Application Development Libraries
bos.diag.com               5.1.0.0    C    Common Hardware Diagnostics
bos.diag.rte              5.1.0.0    C    Hardware Diagnostics
bos.diag.util             5.1.0.0    C    Hardware Diagnostics Utilities
bos.docregister.com        5.1.0.0    C    Docregister Common
bos.docsearch.client.Dt    5.1.0.0    C    DocSearch Client CDE Application Integration
bos.docsearch.client.com   5.1.0.0    C    DocSearch Client Common Files
bos.docsearch.rte          5.1.0.0    C    DocSearch Runtime
bos.help.msg.en_US.com     5.1.0.0    C    WebSM/SMIT Context Helps - U.S. English
bos.help.msg.en_US.smit    5.1.0.0    C    SMIT Context Helps - U.S. English
bos.html.en_US.topnav.navigate   5.1.0.0    C    Top Level Navigation - U. S. English
bos.iconv.com              5.1.0.0    C    Common Language to Language Converters
bos.iconv.ucs.com          5.1.0.0    C    Unicode Base Converters for AIX Code Sets/Fonts
bos.loc.iso.en_US          5.1.0.0    C    Base System Locale ISO Code Set- U.S. English
bos.man.en_US.cmds         5.1.0.0    C    AIX Man Commands  - U.S. English
bos.mp                    5.1.0.0    C    Base Operating System Multiprocessor Runtime
bos.msg.en_US.diag.rte     5.1.0.0    C    Hardware Diagnostics Messages - U.S. English
bos.msg.en_US.docregister.com    5.1.0.0    C    Docregister Common Messages - U.S. English
bos.msg.en_US.docsearch.client.Dt   5.1.0.0    C    DocSearch CDE Action - U.S. English
bos.msg.en_US.docsearch.client.com  5.1.0.0    C    DocSearch Common Messages - U.S  English
bos.msg.en_US.mp           5.1.0.0    C    Base Operating System MP  Messages - U.S. English
bos.msg.en_US.net.tcp.client    5.1.0.0    C    TCP/IP Messages - U.S. English
bos.msg.en_US.rte          5.1.0.0    C    Base Operating System Runtime Msgs - U.S. English
bos.msg.en_US.svprint      5.1.0.0    C    System V Print Subsystem Messages - U.S. English
bos.msg.en_US.txt.tfs      5.1.0.0    C    Text Formatting Services  Messages - U.S. English
bos.net.ncs               5.1.0.0    C    Network Computing System 1.5.1
bos.net.nfs.client         5.1.0.0    C    Network File System Client
bos.net.snapp              5.1.0.0    C    System Networking Analysis and  Performance Pilot
bos.net.tcp.client         5.1.0.0    C    TCP/IP Client Support
bos.net.tcp.smit           5.1.0.0    C    TCP/IP SMIT Support
bos.perf.perfstat          5.1.0.0    C    Performance Statistics Interface
bos.powermgt.rte           5.1.0.0    C    Power Management Runtime Software
bos.rte                   5.1.0.0    C    Base Operating System Runtime
bos.rte.Dt                5.1.0.0    C    Desktop Integrator
bos.rte.ILS               5.1.0.0    C    International Language Support
bos.rte.SRC                5.1.0.0    C    System Resource Controller
bos.rte.X11               5.1.0.0    C    AIXwindows Device Support
bos.rte.aio               5.1.0.0    C    Asynchronous I/O Extension
bos.rte.archive            5.1.0.0    C    Archive Commands
bos.rte.bind_cmds          5.1.0.0    C    Binder and Loader Commands
bos.rte.boot              5.1.0.0    C    Boot Commands
bos.rte.bosinst            5.1.0.0    C    Base OS Install Commands
bos.rte.commands           5.1.0.0    C    Commands
bos.rte.compare            5.1.0.0    C    File Compare Commands
bos.rte.console            5.1.0.0    C    Console
bos.rte.control            5.1.0.0    C    System Control Commands
bos.rte.cron              5.1.0.0    C    Batch Operations
bos.rte.date              5.1.0.0    C    Date Control Commands
bos.rte.devices            5.1.0.0    C    Base Device Drivers
bos.rte.devices_msg        5.1.0.0    C    Device Driver Messages
bos.rte.diag              5.1.0.0    C    Diagnostics
bos.rte.edit              5.1.0.0    C    Editors
bos.rte.filesystem         5.1.0.0    C    Filesystem Administration
bos.rte.iconv              5.1.0.0    C    Language Converters
bos.rte.ifor_ls            5.1.0.0    C    iFOR/LS Libraries
bos.rte.im                5.1.0.0    C    Input Methods
bos.rte.install           5.1.0.0    C    LPP Install Commands
bos.rte.jfscomp            5.1.0.0    C    JFS Compression
bos.rte.libc              5.1.0.0    C    libc Library
bos.rte.libcfg             5.1.0.0    C    libcfg Library
```

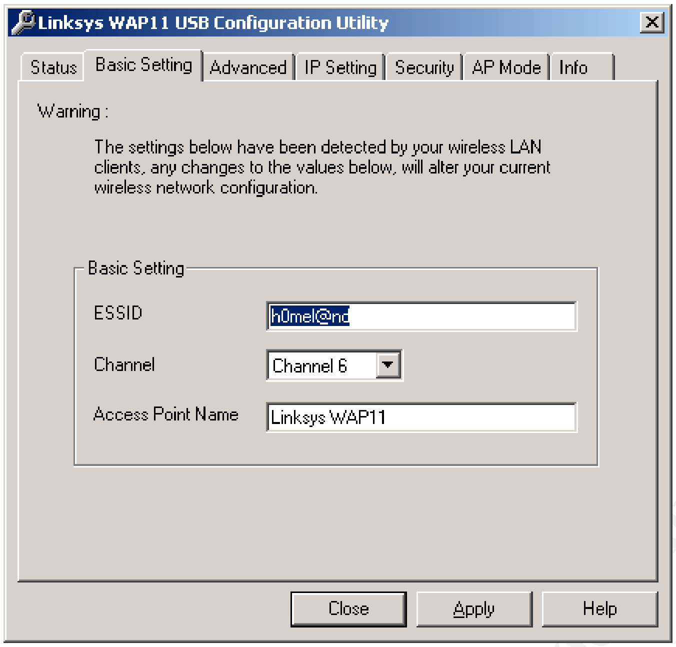
```
  bos.rte.libcur           5.1.0.0    C    libcurses Library
  bos.rte.libdbm            5.1.0.0    C    libdbm Library
  bos.rte.libnetsvc         5.1.0.0    C    Network Services Libraries
  bos.rte.libpthreads       5.1.0.0    C    pthreads Library
  bos.rte.libqb            5.1.0.0    C    libqb Library
  bos.rte.libs            5.1.0.0    C    libs Library
  bos.rte.loc             5.1.0.0    C    Base Locale Support
  bos.rte.lvm             5.1.0.0    C    Logical Volume Manager
  bos.rte.man             5.1.0.0    C    Man Commands
  bos.rte.methods          5.1.0.0    C    Device Config Methods
  bos.rte.misc_cmds        5.1.0.0    C    Miscellaneous Commands
  bos.rte.net             5.1.0.0    C    Network
  bos.rte.odm             5.1.0.0    C    Object Data Manager
  bos.rte.printers         5.1.0.0    C    Front End Printer Support
  bos.rte.security         5.1.0.0    C    Base Security Function
  bos.rte.serv_aid          5.1.0.0    C    Error Log Service Aids
  bos.rte.shell           5.1.0.0    C    Shells (bsh, ksh, csh)
  bos.rte.streams          5.1.0.0    C    Streams Libraries
  bos.rte.tty             5.1.0.0    C    Base TTY Support and Commands
  bos.svprint.fonts         5.1.0.0    C    System V Print Fonts
  bos.svprint.hpnp          5.1.0.0    C    System V Hewlett-Packard JetDirect
  bos.svprint.ps           5.1.0.0    C    System V Print Postscript
  bos.svprint.rte          5.1.0.0    C    System V Print Subsystem
  bos.sysmgt.loginlic       5.1.0.0    C    License Management
  bos.sysmgt.nim.client      5.1.0.0    C    Network Install Manager - Client Tools
  bos.sysmgt.serv_aid       5.1.0.0    C    Software Error Logging and Dump Service Aids
  bos.sysmgt.smit          5.1.0.0    C    System Management Interface Tool (SMIT)
  bos.sysmgt.sysbr          5.1.0.0    C    System Backup and BOS Install Utilities
  bos.sysmgt.trace          5.1.0.0    C    Software Trace Service Aids
  bos.terminfo.com.data      5.1.0.0    C    Common Terminal Definitions
  bos.terminfo.dec.data      5.1.0.0    C    Digital Equipment Corp. Terminal Definitions
  bos.terminfo.ibm.data      5.1.0.0    C    IBM Terminal Definitions
  bos.terminfo.pc.data       5.1.0.0    C    Personal Computer Terminal Definitions
  bos.terminfo.rte          5.1.0.0    C    Run-time Environment for AIX Terminals
  bos.terminfo.svprint.data  5.1.0.0    C    System V Printer Terminal Definitions
  bos.txt.spell           5.1.0.0    C    Writer's Tools Commands
  bos.txt.spell.data        5.1.0.0    C    Writer's Tools Data
  bos.txt.tfs             5.1.0.0    C    Text Formatting Services Commands
  bos.txt.tfs.data          5.1.0.0    C    Text Formatting Services Data
  devices.chrp.base.diag     5.1.0.0    C    RISC CHRP Base System Device Diagnostics
  devices.chrp.base.rte      5.1.0.0    C    RISC PC Base System Device Software (CHRP)
  devices.chrp.pci.rte       5.1.0.0    C    PCI Bus Software (CHRP)
  devices.common.IBM.async.diag  5.1.0.0    C    Common Serial Adapter Diagnostics
  devices.common.IBM.disk.rte   5.1.0.0    C    Common IBM Disk Software
  devices.common.IBM.ethernet.rte   5.1.0.0    C    Common Ethernet Software
  devices.common.IBM.fda.diag   5.1.0.0    C    Common Diskette Adapter and Device Diagnostics
  devices.common.IBM.fda.rte   5.1.0.0    C    Common Diskette Device Software
  devices.common.IBM.ktm_std.diag  5.1.0.0    C    Common Keyboard, Mouse, and Tablet Device
  Diagnostics
  devices.common.IBM.ktm_std.rte  5.1.0.0    C    Common Keyboard, Tablet, and  Mouse Software
 devices.common.IBM.modemcfg.data   5.1.0.0    C    Sample Service Processor Modem Configuration Files
 devices.common.IBM.pmmd_chrp.rte   5.1.0.0    C    CHRP Power Management Software
 devices.common.IBM.ppa.diag    5.1.0.0    C    Common Parallel Printer Adapter Diagnostics
 devices.common.IBM.ppa.rte    5.1.0.0    C    Common Parallel Printer Adapter Software
 devices.common.IBM.scsi.rte   5.1.0.0    C    Common SCSI I/O Controller Software
 devices.common.IBM.ssa.diag   5.1.0.0    C    SSA Common Adapter Diagnostics
 devices.common.IBM.ssa.rte   5.1.0.0    C      Common SSA Adapter Software
 devices.common.base.diag   5.1.0.0    C    Common Base System Diagnostics
devices.common.rspcbase.rte    5.1.0.0    C    RISC PC  Common Base System Device Software
devices.graphics.com       5.1.0.0    C    Graphics Adapter Common Software
devices.isa_sio.PNP0303.diag    5.1.0.0    C    ISA Keyboard Diagnostics (PNP0303)
devices.isa_sio.PNP0400.rte  5.1.0.0    C    RISC PC Standard Parallel Port Adapter Software (PNP0400)
devices.isa_sio.PNP0501.rte  5.1.0.0    C    RISC PC Standard Serial Adapter Software (PNP0501)
devices.isa_sio.PNP0700.rte  5.1.0.0    C    RISC PC Diskette Adapter Software (PNP0700)
devices.isa_sio.PNP0F03.diag   5.1.0.0    C    ISA Mouse Diagnostics (PNP0F03)
devices.isa_sio.chrp.8042.diag   5.1.0.0    C    ISA Keyboard & Mouse Diagnostics (CHRP)
devices.isa_sio.chrp.8042.rte  5.1.0.0    C    ISA Keyboard & Mouse Software (CHRP)
devices.isa_sio.km.diag    5.1.0.0    C    ISA Keyboard & Mouse Diagnostics
devices.isa_sio.pnpPNP.400.diag  5.1.0.0    C    Standard Parallel Adapter Diagnostic (pnpPNP,400) Software
devices.isa_sio.pnpPNP.400.rte   5.1.0.0    C    RISC PC Standard Parallel Port Adapter Software (pnpPNP,400)
devices.isa_sio.pnpPNP.501.diag  5.1.0.0    C    CHRP Serial Adapter Diagnostics (pnpPNP.501)
devices.isa_sio.pnpPNP.501.rte   5.1.0.0    C    CHRP Serial Adapter Software (pnpPNP.501)
devices.isa_sio.pnpPNP.700.diag   5.1.0.0    C    CHRP Diskette Adapter Diagnostic Software (pnpPNP.700)
devices.isa_sio.pnpPNP.700.rte   5.1.0.0    C    CHRP Diskette Adapter Software  (pnpPNP.700)
devices.msg.en_US.base.com   5.1.0.0    C    Base System Device Software Msgs - U.S. English
devices.msg.en_US.diag.rte   5.1.0.0    C    Device Diagnostics Messages -  U.S. English
devices.msg.en_US.rspc.base.com  5.1.0.0    C    RISC PC Software Messages - U.S. English
devices.msg.en_US.sys.mca.rte   5.1.0.0    C    Micro Channel Bus Software Messages - U.S. English
devices.pci.00100100.com   5.1.0.0    C    Common Symbios PCI SCSI I/O  Controller Software
devices.pci.00100100.rte   5.1.0.0    C    Standard NCR53C810 SCSI Software
devices.pci.00100300.diag  5.1.0.0    C    PCI 16-bit SCSI I/O Controller Diagnostics
devices.pci.00100300.rte   5.1.0.0    C    PCI 16-bit SCSI I/O Controller Software
devices.pci.00100f00.rte   5.1.0.0    C    SYM53C8xxA PCI SCSI I/O Controller Software
devices.pci.14104500.diag  5.1.0.0    C    SSA Adapter (14104500)Diagnostics
devices.pci.14104500.rte   5.1.0.0    C    SSA Adapter (14104500) Software
devices.pci.22100020.diag  5.1.0.0    C    PCI Ethernet Adapter Diagnostics
devices.pci.22100020.rte   5.1.0.0    C    IBM PCI Ethernet Adapter Software
devices.pci.23100020.diag  5.1.0.0    C    IBM PCI 10/100 Mb Ethernet Adapter (23100020) Diagnostics
devices.pci.23100020.rte   5.1.0.0    C    IBM PCI 10/100 Ethernet Adapter Software
devices.pci.2b101a05.X11   5.1.0.0    C    AIXwindows GXT120P Graphics Adapter Software
devices.pci.2b101a05.rte   5.1.0.0    C    GXT120P Graphics Adapter Software
devices.pci.2b102005.X11   5.1.0.0    C    AIXwindows GXT130P Graphics Adapter Software
devices.pci.2b102005.diag  5.1.0.0    C    GXT130P Graphics Adapter Diagnostics
devices.pci.2b102005.rte   5.1.0.0    C    GXT130P Graphics Adapter
devices.pci.86808404.com   5.1.0.0    C    Common ISA Bus Software
devices.pci.86808404.rte   5.1.0.0    C    ISA Bus Software
devices.pci.PNP0A03.rte    5.1.0.0    C    PCI Bus Bridge Software
devices.pci.isa.rte        5.1.0.0    C    ISA Bus Bridge Software (CHRP)
devices.pci.pci.rte        5.1.0.0    C    PCI Bus Bridge Software (CHRP)
devices.scsi.disk.diag.com    5.1.0.0    C    Common Disk Diagnostic Service Aid
devices.scsi.disk.diag.rte   5.1.0.0    C    SCSI CD_ROM, Disk Device Diagnostics
devices.scsi.disk.rspc     5.1.0.0    C    RISC PC SCSI CD-ROM, Disk, Read/Write Optical Software
devices.scsi.disk.rte      5.1.0.0    C    SCSI CD-ROM, Disk, Read/Write Optical Device Software
devices.scsi.tape.diag     5.1.0.0    C    SCSI Tape Device Diagnostics
devices.scsi.tape.rspc     5.1.0.0    C    RISC PC SCSI Tape Device Software
devices.scsi.tape.rte      5.1.0.0    C    SCSI Tape Device Software
devices.ssa.IBM_raid.rte   5.1.0.0    C    SSA Raid Manager Software
devices.ssa.disk.rte       5.1.0.0    C    SSA DASD Software
devices.sys.pci.rte        5.1.0.0    C    PCI Bus Software
devices.tty.rte           5.1.0.0.0    C    License Use Management Runtime Code
ifor_ls.msg.en_US.base.cli    5.1.0.0    C    LUM Runtime Code Messages - U.S. English
invscout.ldb              1.1.0.1    C    Inventory Scout Logic Database
invscout.rte              1.1.0.1    C    Inventory Scout Runtime
perl.rte                 5.5.3.0    C    Perl Version 5 Runtime Environment
printers.msg.en_US.rte     5.1.0.0    C    Printer Backend Messages - U.S. English
printers.rte              5.1.0.0    C    Printer Backend
rsct.core.auditrm         2.1.0.0    C    RSCT Audit Log Resource Manager
rsct.core.errm            2.1.0.0    C    RSCT Event Response Resource Manager
rsct.core.fsrm            2.1.0.0    C    RSCT File System Resource Manager
rsct.core.gui             2.1.0.0    C    RSCT Graphical User Interface
rsct.core.hostrm          2.1.0.0    C    RSCT Host Resource Manager
rsct.core.rmc             2.1.0.0    C    RSCT Resource Monitoring and Control
rsct.core.sec             2.1.0.0    C    RSCT Security
rsct.core.sr              2.1.0.0    C    RSCT Registry
rsct.core.utils           2.1.0.0    C    RSCT Utilities
sysmgt.help.msg.en_US.websm  5.1.0.0    C
WebSM Context Helps - U.S. English
sysmgt.msg.en_US.websm.apps    5.1.0.0    C
WebSM Client Apps. Messages - U.S. English
sysmgt.sguide.rte         5.1.0.0    C    TaskGuide Runtime Environment
sysmgt.websm.apps         5.1.0.0    C    Web-based System Manager Applications
sysmgt.websm.diag         5.1.0.0    C    Web-based System Manager Diagnostic Applications
sysmgt.websm.framework    5.1.0.0    C    Web-based System Manager Client/Server Support
sysmgt.websm.icons        5.1.0.0    C    Web-based System Manager Icons
sysmgt.websm.rte          5.1.0.0    C    Web-based System Manager Runtime Environment
sysmgt.websm.webaccess    5.1.0.0    C    WebSM Web Access Enablement
xlC.aix50.rte             5.1.0.0    C    C Set ++ Runtime for AIX 5.0
xlC.cpp                   5.1.1.0    C    C for AIX Preprocessor
xlC.msg.en_US.cpp         5.1.1.0    C    C for AIX Preprocessor Messages
xlC.msg.en_US.cpp         5.1.1.0    C    C for AIX Preprocessor Messages en_US
xlC.msg.en_US.rte          5.1.0.0    C    C Set ++ Runtime Messages--U.S. English
xlC.rte                    5.1.0.0    C    C Set ++ Runtime


 State Codes:
 A -- Applied.
 B -- Broken.
 C -- Committed.
 O -- Obsolete.  (partially migrated to newer version)
 ? -- Inconsistent State...Run lppchk -v.
```

Current R/S 6000 microcode levels can be found on :

URL: http:// techsupport.services.ibm.com/server/mdownload2/download.html

Appendix B – Linksys WAP11 Wireless Access Point

Step 1 – Out of the box ESSID of linksys should be changed immediately. Also channel should be noted also for client station WEP access.



Warning :

The settings below have been detected by your wireless LAN clients, any changes to the values below, will alter your current wireless network configuration.

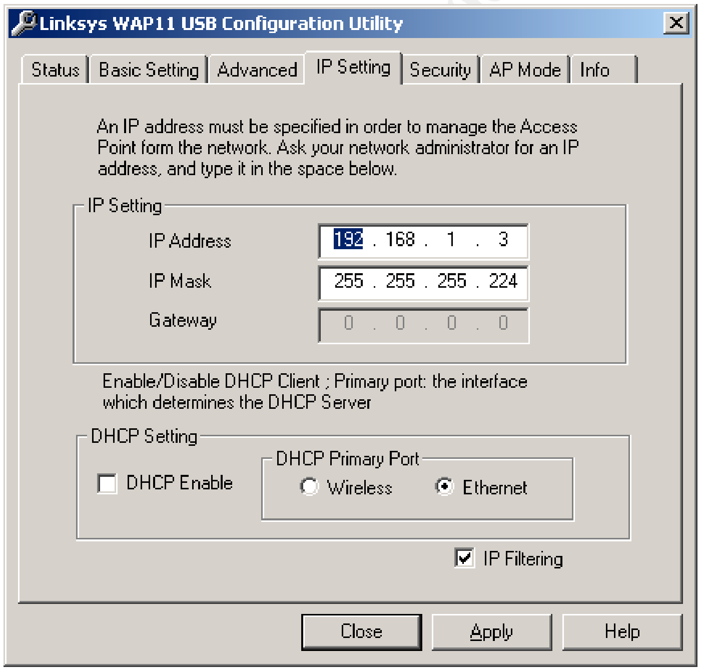
Basic Setting

ESSID: h0mel@nd

Channel: Channel 6

Access Point Name: Linksys WAP11

Step 2 – In this slide the ip address must be set and another nice feature to make use of is check the IP Filtering box for added security.



An IP address must be specified in order to manage the Access Point form the network. Ask your network administrator for an IP address, and type it in the space below.

IP Setting

IP Address: 192 . 168 . 1 . 3

IP Mask: 255 . 255 . 255 . 224

Gateway: 0 . 0 . 0 . 0

Enable/Disable DHCP Client ; Primary port: the interface which determines the DHCP Server

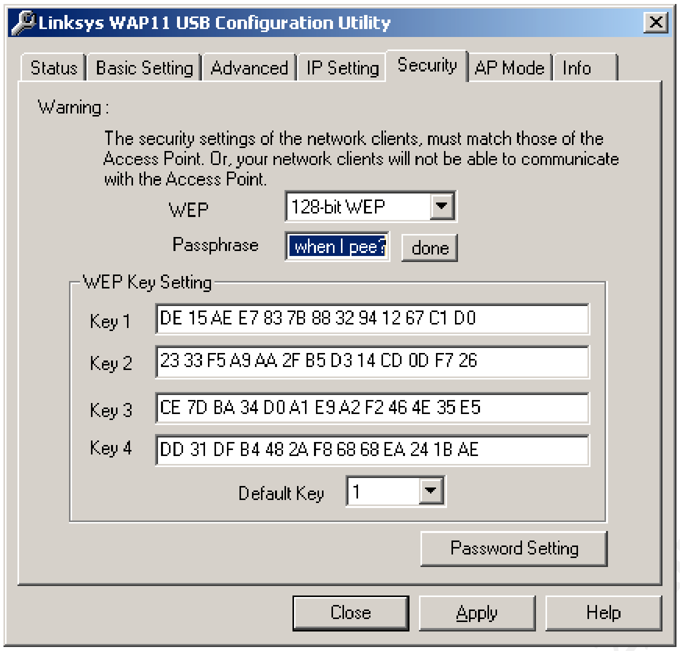
DHCP Setting

☐ DHCP Enable

DHCP Primary Port: ○ Wireless ● Ethernet

☑ IP Filtering

Step 3 – And last but not least, enable 128-bit WEP key encryption. When a strong passphrase has been entered and the done key is engaged, the 4 WEP keys will be generated. You now can use any of the 4 keys.



Warning :

The security settings of the network clients, must match those of the Access Point. Or, your network clients will not be able to communicate with the Access Point.

WEP: 128-bit WEP

Passphrase: when I pee?

WEP Key Setting

Key 1: DE 15 AE E7 83 7B 88 32 94 12 67 C1 D0

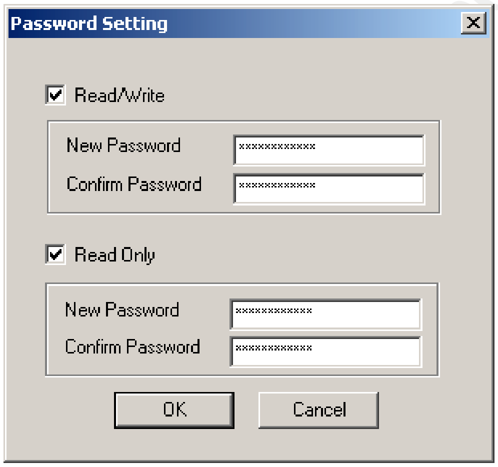
Key 2: 23 33 F5 A9 AA 2F B5 D3 14 CD 0D F7 26

Key 3: CE 7D BA 34 D0 A1 E9 A2 F2 46 4E 35 E5

Key 4: DD 31 DF B4 48 2A F8 68 68 EA 24 1B AE

Default Key: 1

Note: The key used on the access point is the key you must enter on your wireless clients in order to establish and communication link. Also do yourself a favor, and set both the read/read-write passwords on the access point also. Remember, "Layers Rule!"



☑ Read/Write

New Password: ************

Confirm Password: ************

☑ Read Only

New Password: ************

Confirm Password: ************

Appendix C - Complete rule-set for external firewall

```
[root@giac_zion/] /sbin/iptables -L -n -v -t nat

Chain PREROUTING (policy ACCEPT 16591 packets, 2993K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       udp  --  eth0   *       0.0.0.0/0            208.200.171.6  udp dpt:514
to:192.168.1.3:514

Chain POSTROUTING (policy ACCEPT 3306 packets, 246K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 SNAT       all  --  *      eth0    192.168.1.0/24       0.0.0.0/0      to:208.200.171.6

[root@giac_zion] /sbin/iptables -L -n –v


Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     *       127.0.0.1            127.0.0.1
    0     0 ACCEPT     udp  --  eth3   *       192.168.1.3          192.168.1.1          udp dpt:123
    0     0 ACT_ON_ICMP icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 KILL_TRASH all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0      LOG flags 0 level 5 prefix `END INPUT
CHAIN:'
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0      reject-with icmp-port-unreachable

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     sourcedestination
    0     0 ACT_ON_ICMP icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 TO_MORPHEUS all --  eth0   *       !192.168.1.0.0/24    208.200.171.16/29
    0     0 TO_MORPHEUS all --  eth3   *       192.168.1.0/24       208.200.171.16/29
    0     0 TO_MORPHEUS all --  eth2   *       208.200.171.8/29     208.200.171.16/29
    0     0 TO_ORACLE  all  --  eth0   *       !192.168.1.0/24      208.200.171.8/29
    0     0TO_NEBUCHADNEZZAR all --  eth0      *       !192.168.1.0.0/24
    0     0TO_NEBUCHADNEZZAR all --  eth1      *       208.200.171.16/29  192.168.1.0/24
    0     0TO_NEBUCHADNEZZAR all --  eth2      *       0.0.0.0/0          192.168.1.0/24
    0     0 TO_ZION    all  --  eth1   eth0    208.200.171.16/29    0.0.0.0/0
    0     0 TO_ZION    all  --  eth2   eth0    208.200.171.8/29     0.0.0.0/0
    0     0 KILL_TRASH all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0      LOG flags 0 level 5 prefix `END FORWA
CHAIN:'
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0      reject-with icmp-port-unreachable

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       127.0.0.1            127.0.0.1
    0     0 ACCEPT     udp  --  *      eth3    127.0.0.1            192.168.1.3    udp dpt:514
    0     0 ACT_ON_ICMP icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 KILL_TRASH all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0      LOG flags 0 level 5 prefix `END OUTPU
CHAIN:'
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0      reject-with icmp-port-unreachable

Chain ACT_ON_ICMP (3 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       127.0.0.1            0.0.0.0/0      icmp type 8 state
NEW,RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       192.168.1.0/24       0.0.0.0/0      icmp type 8 state
NEW,RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       208.200.171.16/29    0.0.0.0/0      icmp type 8 state
NEW,RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       208.200.171.8/29     0.0.0.0/0      icmp type 8 state
NEW,RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      !eth0   192.168.1.0/24       0.0.0.0/0      icmp type 8 state
NEW,RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0            208.200.171.16/29      icmp type 8 state
NEW,RELATED,ESTABLISHED
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0      LOG flags 0 level 5 prefix `END
HANDLE_ICMP:'
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0      reject-with icmp-port-unreachable
```

```
Chain

TO_ZION (3 references)
    pkts    bytes        target            prot      opt       in        out              source                    destination
      0        0        ACCEPT           tcp        --         *          *            208.200.171.20              206.36.14.60     tcp dpt:443 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *            208.200.171.20              206.36.14.61     tcp dpt:443 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *            208.200.171.19                0.0.0.0/0         tcp dpt:25 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           udp        --         *          *            208.200.171.18                0.0.0.0/0         udp dpt:53 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *            208.200.171.18                0.0.0.0/0      tcp dpt:53 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24               0.0.0.0/0      tcp dpt:22 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24               0.0.0.0/0      tcp dpt:80 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24               0.0.0.0/0      tcp dpt:443 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24               0.0.0.0/0      tcp dpt:21 state
NEW,RELATED,ESTABLISHED
      0        0      KILL_TRASH         all        --         *          *               0.0.0.0/0                  0.0.0.0/0
      0        0          LOG            all        --         *          *               0.0.0.0/0                  0.0.0.0/0      LOG flags 0 level 5                prefix
`END TO_ZION CHAIN:'
      0        0        REJECT           all        --         *          *               0.0.0.0/0                  0.0.0.0/0      reject-with icmp-port-unreachable
Chain

TO_MORPHEUS (4 references)
    pkts    bytes        target            prot      opt       in        out              source                    destination
      0        0        ACCEPT           tcp        --         *          *               0.0.0.0/0               208.200.171.20        tcp dpt:80      state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *               0.0.0.0/0               208.200.171.20        tcp dpt:443     state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *               0.0.0.0/0               208.200.171.19        tcp dpt:25      state
NEW,RELATED,ESTABLISHED
      0        0        REJECT           tcp        --         *          *               0.0.0.0/0                  0.0.0.0/0          tcp dpt:113     reject-with tcp-reset
      0        0        ACCEPT           udp        --         *          *               0.0.0.0/0               208.200.171.18        udp dpt:53      state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *               0.0.0.0/0               208.200.171.18        tcp dpt:53      state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           udp        --         *          *              192.168.1.12                0.0.0.0/0          udp dpt:123     state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24               0.0.0.0/0          tcp dpt:22      state
NEW,RELATED,ESTABLISHED
      0        0      KILL_TRASH         all        --         *          *               0.0.0.0/0                  0.0.0.0/0
      0        0          LOG            all        --         *          *               0.0.0.0/0                  0.0.0.0/0          LOG flags       0 level 5    prefix `ENI
TO_MORPHEUS                                                                                                                         CHAIN:'
      0        0        REJECT           all        --         *          *               0.0.0.0/0                  0.0.0.0/0          reject-with icmp-port-unreachable
Chain

TO_NEBUCHADNEZZAR (4 references)
    pkts    bytes        target            prot      opt       in        out              source                    destination
      0        0        ACCEPT           tcp        --         *          *            208.200.171.19               192.168.1.4     tcp dpt:25 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24              192.168.1.4     tcp dpt:25 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24              192.168.1.4     tcp dpt:110 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24              192.168.1.4     tcp dpt:143 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --        eth1        *               0.0.0.0/0                 192.168.1.4     tcp dpt:25 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *               0.0.0.0/0                 192.168.1.4     tcp dpt:110 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --        eth1        *               0.0.0.0/0                 192.168.1.4     tcp dpt:143 state
NEW,RELATED,ESTABLISHED
      0        0        ACCEPT           tcp        --         *          *             192.168.1.0/24              192.168.1.7     tcp dpt:3306 state
NEW,RELATED,ESTABLISHED
```

```
    0      0     ACCEPT      udp    --     *     *       0.0.0.0/0           192.168.1.3    udp dpt:514 state
NEW,RELATED,ESTABLISHED
    0      0     ACCEPT      tcp    --     *     *      192.168.1.0/24        0.0.0.0/0     tcp dpt:22 state
NEW,RELATED,ESTABLISHED
    0      0     ACCEPT      tcp    --     *     *      208.200.17120        192.168.1.7    tcp dpt:22 state
NEW,RELATED,ESTABLISHED
    0      0   KILL_TRASH    all    --     *     *       0.0.0.0/0            0.0.0.0/0
    0      0      LOG        all    --     *     *       0.0.0.0/0            0.0.0.0/0     LOG flags 0 level   5        prefix
   `END TO_NEBUCHADNEZZAR CHAIN:'
    0      0     REJECT      all    --     *     *       0.0.0.0/0            0.0.0.0/0     reject-with icmp-port-unreachable
Chain

TO_ORACLE (2 references)
  pkts   bytes    target     prot   opt    in    out       source              destination
    0      0     ACCEPT   ipv6-crypt   --   *     *       0.0.0.0/0            0.0.0.0/0     state    NEW,RELATED,ESTABLISHEI
    0      0     ACCEPT      udp    --     *     *       0.0.0.0/0            0.0.0.0/0     udp dpt:500 state
NEW,RELATED,ESTABLISHED
    0      0     ACCEPT      udp    --     *     *      192.168.1.12          0.0.0.0/0     udp dpt:123        state
NEW,RELATED,ESTABLISHED
    0      0     ACCEPT      tcp    --     *     *      192.168.1.0/24        0.0.0.0/0     tcp dpt:22 state
NEW,RELATED,ESTABLISHED
    0      0   KILL_TRASH    all    --     *     *       0.0.0.0/0            0.0.0.0/0
    0      0      LOG        all    --     *     *       0.0.0.0/0            0.0.0.0/0     LOG flags 0 level   5        prefix
   `END TO_ORACLE CHAIN:'
    0      0     REJECT      all    --     *     *       0.0.0.0/0            0.0.0.0/0     reject-with icmp-port-unreachable
Chain
KILL_TRASH(7 references)
  pkts   bytes    target     prot   opt    in    out       source              destination
    0      0      DROP       tcp    --    eth0   *       0.0.0.0/0            0.0.0.0/0          tcp dpts:137:139
    0      0      DROP       tcp    --    eth0   *       0.0.0.0/0          !208.200.171.20      tcp dpt:80
    0      0     RETURN      all    --     *     *       0.0.0.0/0            0.0.0.0/0
```

Appendix D - IPTABLES rc.firewall script

```
#! /bin/bash
#
# Description: Loads iptables firewall rule-set
#
# Next line used for debugging
# set -x
#
# Variable definitions

# The full path to the iptables executable.
IPTABLES="/sbin/iptables"

# INTERFACES

# The loopback interface and address
IF_LO="lo"
IP_LO="127.0.0.1"
# The interface and ip between the firewall and border router
IF_ZION="eth0"
IP_ZION="208.200.171.6"
# The interface and ip between the firewall and the service network
IF_MORPHEUS="eth1"
IP_MORPHEUS="208.200.171.16"
# The interface and ip between the firewall and vpn gateway
IF_ORACLE="eth2"
IP_ORACLE="208.200.171.8"
# The interface and ip between the firewall and internal network
IF_NEBUCHADNEZZAR="eth3"
IP_NEBUCHADNEZZAR="192.168.1.1"

# NETWORKS

# service network
NET_SVCNET="208.200.171.16/29"
# VPN network
NET_VPN="208.200.171.8/29"
# Internal Network
NET_INTERNAL="192.168.1.1/24"
NET_GIAC="192.168.1.0/24"

# GIAC SYSTEMS
giac_sentinal="208.200.171.20/32"
giac_apoak="208.200.171.19/32"
giac_doozer="208.200.171.18/32"
giac_emp="208.200.171.10/32"
reclaim="192.168.1.7/32"
comstruc="192.168.1.4/32"
agentsmith="192.168.1.5/32"
tank="192.168.1.3/32"
IP_INTERNAL_LOG="192.168.1.3"

# NON-GIAC SERVERS
creditcardA="206.36.14.60"
creditcardB="206.36.14.61"

# Variables end here.

# Get the environment ready. No rules defined, no user-defined chains, and default
# policies that DENY everything. First flush all the rules.  This should be done prior to
# attempting to delete user-defined chains because a user-defined chain will not be
# deleted if a rule exists that references it.

$IPTABLES -F
$IPTABLES -F -t nat

# Delete all user-defined chains
$IPTABLES -X
```

```
# Set default policy for built-in chains
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Create user-defined chains
$IPTABLES -N TO_ZION
$IPTABLES -N TO_MORPHEUS
$IPTABLES -N TO_ORACLE
$IPTABLES -N TO_NEBUCHADNEZZAR
$IPTABLES -N ACT_ON_ICMP
$IPTABLES -N KILL_TRASH

# Set log level
LOGFLAG="LOG --log-level notice"

# End environment set-up

# THE KILL_TRASH CHAIN
# Packets entering this chain have not matched
# any rule yet and would get logged if not dropped.
# This is used to get rid of messages that fill the logs.

# netbios traffic from the internet
$IPTABLES -A KILL_TRASH -i $IF_ZION -p tcp --dport 137:139 -j DROP

# http requests from border router not destined for giac_sentinal
$IPTABLES -A KILL_TRASH -i $IF_ZION -p tcp --dport 80 -d ! $giac_sentinal -j DROP

# RETURN to the chain that sent the packet here
$IPTABLES -A KILL_TRASH -j RETURN

# THE ACT_ON_ICMP CHAIN
# Packets entering this chain match icmp protocol

# ping allowed from loopback to anywhere
$IPTABLES -A ACT_ON_ICMP -p icmp --icmp-type echo-request -s $IP_LO -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ping allowed from internal systems to anywhere
$IPTABLES -A ACT_ON_ICMP -p icmp --icmp-type echo-request -s $NET_INTERNAL -m state --
state NEW,ESTABLISHED,RELATED -j ACCEPT

# ping allowed from service network to anywhere
$IPTABLES -A ACT_ON_ICMP -p icmp --icmp-type echo-request -s $NET_SVCNET -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ping allowed from VPN gateway to anywhere
$IPTABLES -A ACT_ON_ICMP -p icmp --icmp-type echo-request -s $NET_VPN -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ping allowed from internal network to anywhere except border router interface
$IPTABLES -A ACT_ON_ICMP -o ! $IF_ZION -p icmp --icmp-type echo-request -s $NET_INTERNAL
-m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# ping allowed from border router interface to service network servers so people on
# the internet can check if our service network servers are alive
$IPTABLES -A ACT_ON_ICMP -i $IF_ZION -p icmp --icmp-type echo-request -d $NET_SVCNET -m
state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# LOG and REJECT everything else
$IPTABLES -A ACT_ON_ICMP -j $LOGFLAG --log-prefix "END ACT_ON_ICMP:"
$IPTABLES -A ACT_ON_ICMP -j REJECT

# THE TO_MORPHEUS CHAIN
# Packets entering this chain have destination ip
# of $NET_SVCNET and could come from anywhere.

# HTTP/HTTPS traffic is allowed to our web server
$IPTABLES -A TO_MORPHEUS -p tcp --dport 80 -d $giac_sentinal -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
$IPTABLES -A TO_MORPHEUS -p tcp --dport 443 -d $giac_sentinal -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# smtp traffic is allowed to our mail server
$IPTABLES -A TO_MORPHEUS -p tcp --dport 25 -d $giac_apoak -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# send connection resets to ident requests to avoid delays
$IPTABLES -A TO_MORPHEUS -p tcp --dport 113 -j REJECT --reject-with tcp-reset

# dns traffic is allowed to dns server (both UDP and TCP inbound traffic)
$IPTABLES -A TO_MORPHEUS -p udp --dport 53 -d $giac_doozer -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_MORPHEUS -p tcp --dport 53 -d $giac_doozer -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ntp from tank
$IPTABLES -A TO_MORPHEUS -p udp --dport 123 -s $tank -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ssh from internal network to all systems
$IPTABLES -A TO_MORPHEUS -p tcp --dport 22 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# KILL_TRASH, LOG and REJECT everything else
$IPTABLES -A TO_MORPHEUS -j KILL_TRASH
$IPTABLES -A TO_MORPHEUS -j $LOGFLAG --log-prefix "END TO_MORPHEUS CHAIN:"
$IPTABLES -A TO_MORPHEUS -j REJECT

# THE TO_ORACLE CHAIN
# Packets entering this chain have destination ip
# of $giac_emp and could come from anywhere.

# ipsec traffic
$IPTABLES -A TO_ORACLE -p 50 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_ORACLE -p udp --dport 500 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT

# ntp from tank
$IPTABLES -A TO_ORACLE -p udp --dport 123 -s $tank -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ssh from internal network for administration
$IPTABLES -A TO_ORACLE -p tcp --dport 22 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# KILL_TRASH, LOG and REJECT everything else
$IPTABLES -A TO_ORACLE -j KILL_TRASH
$IPTABLES -A TO_ORACLE -j $LOGFLAG --log-prefix "END TO_ORACLE CHAIN:"
$IPTABLES -A TO_ORACLE -j REJECT

# THE TO_INTERNAL CHAIN
# Packets entering this chain have destination ip of
# $NET_INTERNAL and could be from anywhere except $IF_ZION

# smtp traffic to comstruc from giac_apoak
$IPTABLES -A TO_INTERNAL -p tcp --dport 25 -s $giac_apoak -d $agentsmith -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# smtp, pop3 and imap traffic to comstruc from internal network
$IPTABLES -A TO_INTERNAL -p tcp --dport 25 -s $NET_INTERNAL -d $comstruc -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

$IPTABLES -A TO_INTERNAL -p tcp --dport 110 -s $NET_INTERNAL -d $comstruc -m state --
state NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_INTERNAL -p tcp --dport 143 -s $NET_INTERNAL -d $comstruc -m state --
state NEW,ESTABLISHED,RELATED -j ACCEPT

# smtp, pop3 and imap traffic to comstruc from the vpn gateway interface
$IPTABLES -A TO_INTERNAL -i $IF_ORACLE -p tcp --dport 25 -d $comstruc -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
$IPTABLES -A TO_INTERNAL -p tcp --dport 110 -d $comstruc -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_INTERNAL -i $IF_ORACLE -p tcp --dport 143 -d $comstruc -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# mysql traffic to reclaim from internal network
$IPTABLES -A TO_INTERNAL -p tcp --dport 3306 -s $NET_INTERNAL -d $reclaim -m state --
state NEW,ESTABLISHED,RELATED -j ACCEPT

# syslog traffic from anywhere to tank
$IPTABLES -A TO_INTERNAL -p udp --dport 514 -d $tank -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ssh from internal network for administration
$IPTABLES -A TO_INTERNAL -p tcp --dport 22 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ssh initiated from giac_sentinal to reclaim for port forwarding
$IPTABLES -A TO_INTERNAL -p tcp --dport 22 -s $giac_sentinal -d $reclaim -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# KILL_TRASH, LOG and REJECT everything else
$IPTABLES -A TO_INTERNAL -j KILL_TRASH
$IPTABLES -A TO_INTERNAL -j $LOGFLAG --log-prefix "END TO_INTERNAL CHAIN:"
$IPTABLES -A TO_INTERNAL -j REJECT

# THE TO_ZION CHAIN
# Packets entering this chain have destination outside
# of the GIAC ENTERPRISE and could be from service network, vpn or internet

# https traffic can be initiated from web server to credit servers
$IPTABLES -A TO_ZION -p tcp --dport 443 -s $giac_sentinal -d $creditcardA -m state --
state NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_ZION -p tcp --dport 443 -s $giac_sentinal -d $creditcardB -m state --
state NEW,ESTABLISHED,RELATED -j ACCEPT

# smtp traffic to other mail servers from giac_apoak
$IPTABLES -A TO_ZION -p tcp --dport 25 -s $giac_apoak -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# dns traffic to other dns servers (both udp and tcp traffic)
$IPTABLES -A TO_ZION -p udp --dport 53 -s $giac_doozer -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_ZION -p tcp --dport 53 -s $giac_doozer -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ssh from the internal network
$IPTABLES -A TO_ZION -p tcp --dport 22 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# http or https from the internal network
$IPTABLES -A TO_ZION -p tcp --dport 80 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A TO_ZION -p tcp --dport 443 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# ftp from the internal network
$IPTABLES -A TO_ZION -p tcp --dport 21 -s $NET_INTERNAL -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# KILL_TRASH, LOG and REJECT everything else
$IPTABLES -A TO_ZION -j KILL_TRASH
$IPTABLES -A TO_ZION -j $LOGFLAG --log-prefix "END TO_ZION CHAIN:"
$IPTABLES -A TO_ZION -j REJECT

# THE INPUT CHAIN
# Only packets destined for the firewall box
# itself should enter this chain.

# Allow traffic to self
$IPTABLES -A INPUT -i $IF_LO -s $IP_LO -d $IP_LO -j ACCEPT
```

```
# Allow ntp traffic from tank
$IPTABLES -A INPUT -i $IF_INTERNAL -p udp --dport 123 -s $tank -d $IP_INTERNAL_LOG -j
ACCEPT

# icmp traffic
$IPTABLES -A INPUT -p icmp -j ACT_ON_ICMP

# Before logging, weed out packets we know we can drop
# and don't care to log.  Log and reject everything else
$IPTABLES -A INPUT -j KILL_TRASH
$IPTABLES -A INPUT -j $LOGFLAG --log-prefix "END INPUT CHAIN:"
$IPTABLES -A INPUT -j REJECT

# THE OUTPUT CHAIN
# Only packets originating on the firewall box
# itself should enter this chain.

# Allow traffic to self
$IPTABLES -A OUTPUT -s $IP_LO -d $IP_LO -j ACCEPT

# Allow syslog messages to tank
$IPTABLES -A OUTPUT -o $IF_INTERNAL -p udp --dport 514 -s $IP_LO -d $tank -j ACCEPT

# icmp traffic
$IPTABLES -A OUTPUT -p icmp -j ACT_ON_ICMP

# KILL_TRASH, log, and reject everything else
$IPTABLES -A OUTPUT -j KILL_TRASH
$IPTABLES -A OUTPUT -j $LOGFLAG --log-prefix "END OUTPUT CHAIN:"
$IPTABLES -A OUTPUT -j REJECT

# THE FORWARD CHAIN
# This is where the traffic is passing through the firewall.
# To make management of rules simpler, we send packets to
# user-defined chains for further processing.

# REJECT non-routable IP addresses from the border router
for NET in $IP_PRIVATE; do
   $IPTABLES -A FORWARD -i $IF_ZION -s $NET -j DROP
done

# Act on icmp traffic (since we allow most related icmp
# that is appropriate to be handled by state table)
$IPTABLES -A FORWARD -p icmp -j ACT_ON_ICMP

# Traffic to service network goes to the TO_MORPHEUS chain
# coming from border router accept any source ip (non-internal network)
$IPTABLES -A FORWARD -I $IF_ZION -s ! $NET_GIAC -d $NET_SVCNET -j TO_MORPHEUS
# Coming from internal network with source ip internal network
$IPTABLES -A FORWARD -I $IF_INTERNAL -s $NET_INTERNAL -d $NET_SVCNET -j TO_MORPHEUS
# Coming from vpn with source ip of vpn network
$IPTABLES -A FORWARD -i $IF_ORACLE -s $NET_VPN -d $NET_SVCNET -j TO_MORPHEUS

# Traffic to vpn goes to the TO_ORACLE chain
# Coming from border router accept any source ip if not GIAC internal network
$IPTABLES -A FORWARD -i $IF_ZION -s ! $NET_GIAC -d $NET_VPN -j TO_ORACLE
# Coming from internal network with source ip of the internal network
$IPTABLES -A FORWARD -i $IF_INTERNAL -s $NET_INTERNAL -d $NET_VPN -j TO_ORACLE

# Traffic to internal network goes to the TO_INTERNAL chain
# Coming from border router accept any source ip if not GIAC internal network
$IPTABLES -A FORWARD -i $IF_ZION -s ! $NET_GIAC -d $NET_INTERNAL -j TO_INTERNAL
# Coming from service network accept service network source ip
$IPTABLES -A FORWARD -i $IF_MORPHEUS -s $NET_SVCNET -d $NET_INTERNAL -j TO_INTERNAL
# Coming from internal network with source ip internal network
$IPTABLES -A FORWARD -i $IF_INTERNAL -s $NET_INTERNAL -d $NET_INTERNAL -j TO_INTERNAL
# Coming from vpn with any source ip
$IPTABLES -A FORWARD -i $IF_ORACLE -d $NET_INTERNAL -j TO_INTERNAL

# Traffic to border router goes to the TO_ZION chain
# Coming from service network interface with source ip of service network
```

```
$IPTABLES -A FORWARD -i $IF_MORPHEUS -o $IF_ZION -s $NET_SVCNET -j TO_ZION
# Coming from service network interface with source ip of vpn
$IPTABLES -A FORWARD -i $IF_ORACLE -o $IF_ZION -s $NET_VPN -j TO_ZION
# Coming from internal network interface, source ip of internal network
$IPTABLES -A FORWARD -i $IF_INTERNAL -o $IF_ZION -s $NET_INTERNAL -j TO_ZION

# KILL_TRASH, log, and reject everything else
$IPTABLES -A FORWARD -j KILL_TRASH
$IPTABLES -A FORWARD -j $LOGFLAG --log-prefix "END FORWARD CHAIN:"
$IPTABLES -A FORWARD -j REJECT

# NETWORK ADDRESS TRANSLATION
# Use NAT for hiding packets connecting to the
# internet from the GIAC internal network

# Flush the NAT table
$IPTABLES -F -t nat

# Use hiding NAT for traffic from internal to outside world
$IPTABLES -t nat -A POSTROUTING -o $IF_ZION -s $NET_INTERNAL -j SNAT --to-source $IP_ZION

# Use static NAT so router can log to syslog
$IPTABLES -t nat -A PREROUTING -i $IF_ZION -p udp --dport 514 -d $IP_ZION -j DNAT --to-
destination $IP_INT_LOG:514
```

References

1. "VPNs and Remote Access.", SANS GCFW Course Book 2.*4*, p. 6 - 30, December 2001.

2. "Firewalls 101: Perimeter Protection with Firewalls.", SANS GCFW Course Book 2.2, p. 207, December 2001.

3. "Firewalls 102: Perimeter Protection and Defense In-Depth.", SANS GCFW Course Book 2.3, p. 57, December 2001.

4. Rusty Russell, "Linux 2.4 Packet Filtering HOWTO". Revsion 1.1, 07-JAN-2002.
URL: http://netfilter.samba.org/documentation/HOWTO/packet-filtering-HOWTO.txt

5. Linux Free S/WAN Project, FreeS/WAN documentation,
URL: http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/index.html

6. Duncan Napier, "Setting up a VPN Gateway.", Linux Journal, Issue 93, January 2002.
URL: http://www.linuxjournal.com/article.php?sid=4772

7. Duncan Napier, "Administering Linux IPSec Virtual Private Networks.", Sys Admin Volume 11, Number 3, March 2002.
URL: http://www.samag.com/documents/s=4072/sam0203c/sam0203c.html

8. Lee Barken, "Wireless Security Step by Step." Business Security Advisor Magazine Volume 20, Number 2 April 2002.
URL: http://www.Advisor.com/Article/BARKL01

9. Chris Brenton, "Mastering Cisco Routers.", Sybex Inc. Copyright 2000

10. AIX 4.3 Elements of Security Effective and Efficient Implementation
URL: http://www.redbooks.ibm.com/redbooks/SG245962.html

11. David B. Koconis, "GCFW Practical Assignment", February 2001
URL:// www.giac.org/practical/David_Koconis_GCFW.doc

12. Richard W. Stevens, "TCP/IP Illustrated, Volume 1." USA: Addison Wesley February 2000.

13. Robert L Ziegler, "Linux Firewalls, 2nd Edition." New Riders November 2001

14. SSH Communications Security Corporation, "SSH Sentinel 1.2 User Manual", October 2001
URL:http://www.ipsec.com

Other URL’s researched:

http://me.mit.edu/computing/security-guidelines.html
http://www.sans.org/infosecFAQ/firewall/router2.htm
http://www.nrc.ca/inms/time/ntpnrc.html
http://www.unixtools.com/security.html
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix2_ds.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt5/scpasswd.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/112cg_cr/1rbook/1rsysmgt.htm#xtocid1962109
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fctroubl.htm#xtocid1767115
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fctroubl.htm#xtocid1767115
http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/cef_wp.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm#xtocid2056541
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/SSHv1.htm#xtocid25517
http://www.iana.org/assignments/ipv4-address-space
http://www.cert.org/advisories/CA-1998-01.html - CERT Advisory CA-1998 Smurf IP Denial-of-Service Attacks
http://www.isi.edu/in-notes/rfc1918.txt
http://www.arin.net/templates/asntemplate.txt
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm#xtocid6
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/icsbgp4.htm
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42cmd.htm#xtocid2394415
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0116
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm
http://www.enteract.com/~lspitz/armoring.html Lance Spitzners white papers
http://www.linuxguruz.org/iptables/howto/iptables-HOWTO.html
http://monmotha.mplug.org/firewall/index.php