GIAC CERTIFIED FIREWALL ANALYST

PRACTICAL ASSIGNMENT

VERSION 1.9

by

Kenneth Baldridge

Date Submitted

April 15, 2003

TABLE OF CONTENTS

Abstract

This paper is an attempt to fulfill the written requirements portion of the GIAC Certified Firewall Analyst (GCFW) certification (the practical assignment).

The paper consists of six parts. Parts one to four correspond to the assignments one to four of the GCFW practical version 1.9 revised January 20, 2003. Part five contains further information relevant to the first four sections. Part 6 contains references to information and tools either used by the author in preparation of the assignment or containing information regularly used by the author in day to day business.

ACKNOWLEDGMENTS

I would like to thank my wife for putting up with me while I worked very odd hours on this paper and taking a week off to attend the December 2002 San Francisco conference.

Part 1

BUSINESS STRUCTURE OVERVIEW

GIAC Enterprises is an e-business dealing in the online sales of fortune cookie sayings. The business has done well over the last two years and is moving to a new location. We have been hired to define the network security architecture at the new facility. In performing preparatory review of the business structure we have found the following major points:

Business Dynamics:

1. Medium-sized business with 200-300 employees.
2. Currently doing well having met its budget guidelines for the last two years.
3. Has experienced a 28% annual growth rate for the last two years and this trend is expected to continue for at least two more years.
4. Average annual profits of 2-5 million dollars.
5. Looking to continue to expand its market share.
6. Looking at branching into other areas of e-business.
7. Has a 7X24 operations staff for technical as well as application based emergencies.
8. The data center relocation effort is fully funded with some budget available for new purchases.
9. The capital expenditure budget for the next two years is significant and can be counted upon for future requirements.

Business Operations:

1. The business applications are structured in a tiered approach utilizing web servers located on a screened network for interaction with the customers and suppliers. The applications located on the web servers interact with a data-access layer housed on another set of servers located on a different screened network. The data-access layer of the application then communicates with the information stores located on backend database servers in the production network.
2. All web server access other than the public company website utilizes SSL over port 443.
3. Employee access (both VPN and Web) requires secondary (two factor) authentication utilizing certificates issued by the internal certificate authority.
4. Operational Access:

a. **Customers** (companies or individuals that purchase bulk online fortunes) access the product via web farm 1 at the following URL. https://customer.gaiccookies.com/

b. **Suppliers** (companies that supply GIAC Enterprises with their fortune cookie sayings) access the product via web farm 2 at the following URL. https://supplier.gaiccookies.com/

c. **Partners** (International companies that translate and resell fortunes) access the product via web farm 3 at the following URL. https://partner.gaiccookies.com/

d. **Bulk Data file delivery** is available via HTTPS or Secure FTP utilizing Valicert Secure Transport software. URL's are documented in the IP scheme.

e. **GIAC Enterprises employees (Intranet)** located on GIAC Enterprises internal network access the product based on job role and function.

   i. IT employees access the servers directly via console.

   ii. DBA's access the databases directly via database tools.

   iii. Sales and Product support access the application via an intranet web site. https://intranet/cookies

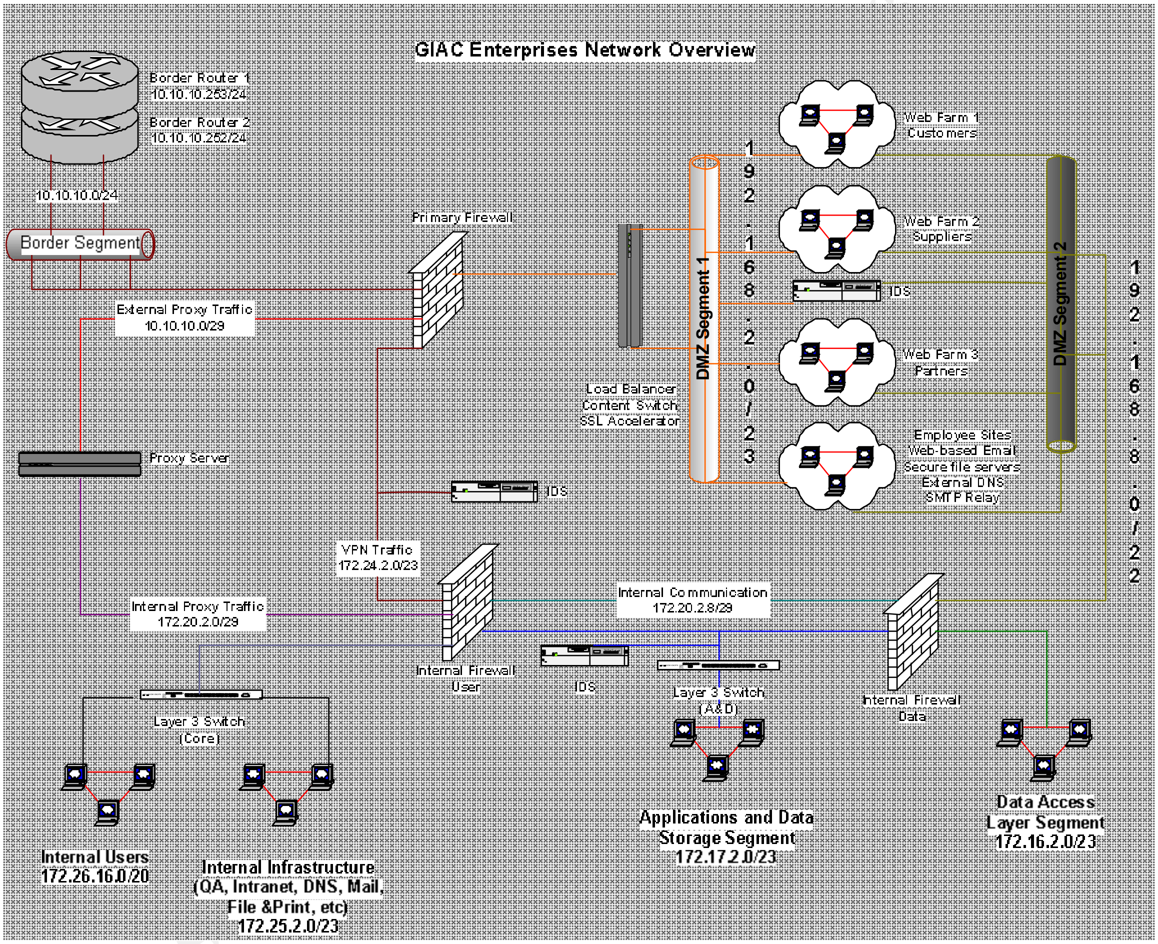
   iv. There are Staging and QA environments containing non-production data for use by the Quality Assurance and Product Development departments.

5. **GIAC Enterprises employees (extranet)** working from outside of the building connect to the employee web site for employee-level applications access at the following URL, https://employee.giaccokies.com .
6. Web-based email retrieval is available to all employees at the following URL. https://employee-mail.gaiccookies.com/
7. Internal Internet out-going access for non- IT staff is limited to FTP, HTTP and HTTPS via a Proxy server.
8. There needs to be limited Internet access available on an occasional basis to members of the IT staff that bypasses the Proxy Server but which is still fully logged.
9. VPN access is restricted but available to Employees on a case-by-case basis according to job function and need.
10. Centralized Application, Server, Anti-viral and IDS monitoring/alerting information is available to the 7X24 Operations staff.

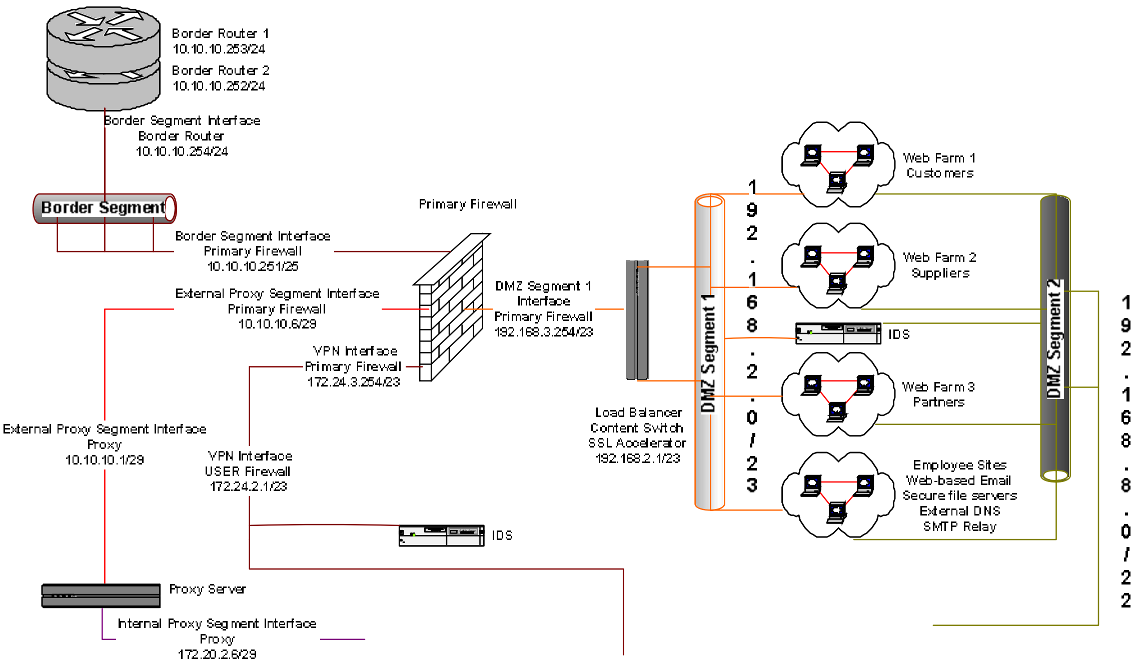
Based on this review the following design has been developed.
General IP addressing information is present in the designs.

For specific brand and version information on equipment please see <u>Business Equipment Overview</u> on page 42.

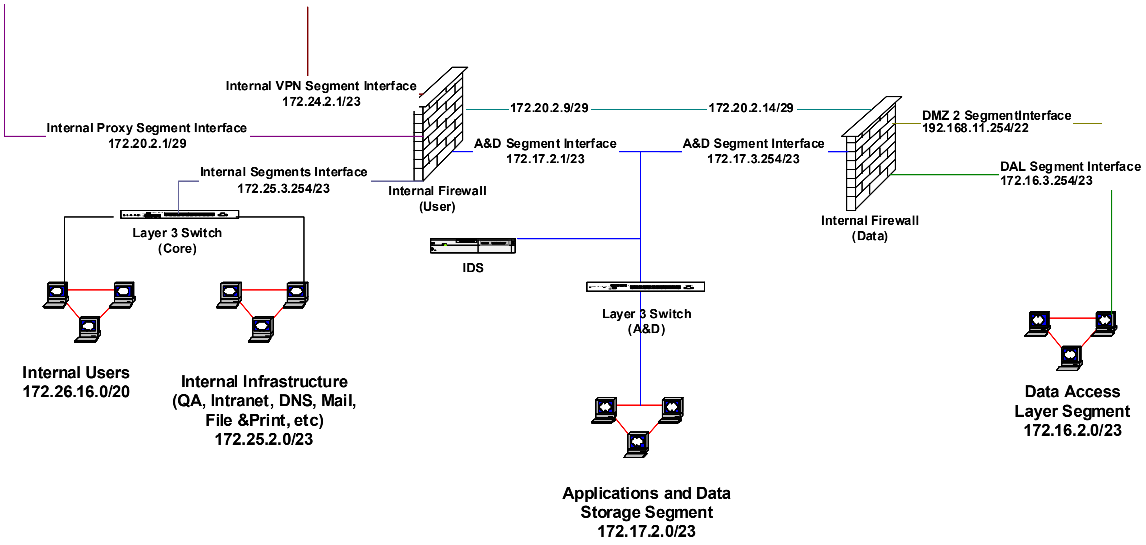
For the complete IP addressing scheme please see <u>IP Address Scheme</u> on page 44.



GIAC Enterprises Network Close-up
Section One



GIAC Enterprises Network Close-up
Section Two



Component Design & Placement Overview

This network is structured in a multi-layer design with two focal points, the border routers and the primary firewall. After passing these two areas traffic (depending on destination) is funneled through one of three secondary devices before reaching the computer systems themselves.

1. The border router is the primary gateway into the network and serves as our first line of defense. Since all traffic entering and leaving the network passes this point this device is used to restrict traffic based on both incoming and outgoing parameters.
2. The primary firewall is used for inspection of the traffic that has been permitted onto the reserved external segment of the network by the border router or that is attempting to reach that segment by leaving the internal network areas.
3. Incoming traffic that passes the rule sets of the Primary firewall continues on to one of three destinations:
    a. The Proxy server. In this design this device has multiple roles.
        i. It is used to conserve bandwidth for the production / application area.
        ii. Traffic screening; through the use of content management tools (Website, antivirus and code screening) along with the inherent functions of the proxy itself.
        iii. The company also achieves a measure of protection by blocking/removing websites, materials and traffic that would pose both a network and/or a business risk due to malicious and/or inappropriate content.
    b. The internal (user) firewall on the VPN segment.
    c. The secure application switch / DMZ segment 1. The secure application switch bridges the network at this point and among other features provides SSL acceleration / termination and load balancing across the web services / applications located in the screened network.
4. Both internal Proxy and VPN traffic terminates at the Internal (User) Firewall which provides traffic, access and logging for all traffic entering and leaving the Internal User areas as well as controlling the access from this side of the network into the Applications and Data Storage segment and the Authentication Segment.
5. An IDS box is located in the VPN section between the Primary and Internal (USER) firewalls to examine traffic in this area for known signatures or anomalous activity.
6. All machines located in the screened network area are multi-homed and have a presence in both DMZ segment 1 and DMZ segment 2. Traffic continuing into the network from DMZ segment 1 will do so via segment 2 and the connection to the Internal (Data) Firewall. An IDS box is located in

the screened networks to examine traffic in either area for known signatures or anomalous activity.

7. Applications/machines located in the DMZ segments are not allowed to access the Applications & Data storage area directly. Access to information is granted via the data access layer machines. This design is multi-purpose. It protects data from direct manipulation by exposed machines, establishes set traffic patterns that we can look for at our IDS boxes (either present, or deviated from) and reduces licensing fees associated with SQL server. (These would be lower powered machines with fewer processors than our data farms)
8. The Internal (Data) Firewall is responsible for traffic, access and logging for all traffic entering and leaving the Data Access Layer segment as well as this side of the Applications and Data Storage segment and the internal communications segment.
9. The Applications and Data Storage segment is used for all production related systems and information storage so an IDS box is also located in this area to examine traffic for known signatures or anomalous activity.
10. The layer 3 switches located in both the Internal and A & D area segments are used to provide routing along with some traffic control via VLANS and access control lists.

Traffic exiting the internal network follows the reverse of the above paths with appropriate screening. End user traffic exiting the network is required to follow either the Proxy or VPN path while production / application traffic follows the DMZ segment path. The internal communication path between the Internal (User) firewall and the Internal Data firewall is used for required traffic between DMZ Segment 2 and the Internal Infrastructure/User areas. This method bypasses the sensitive data storage areas and simplifies auditing.

In this business scenario Service Level Agreements are very loose while audit requirements have significantly tightened. In a business decision the company has decided that it wants to invest resources this year in multiple layers of protection with product performance enhancements and understands that there are currently single points of failure in the design. To mitigate this issue there are 4 hour support contracts on all of the equipment and spare parts / equipment is on-site. In addition to this a comprehensive Disaster Recovery plan is in place that includes the firewalls.

The company currently projects both profits and expansion for the next two years. Based on this fact along with the warnings that we have given them about the single points of failure at the Firewalls, the secure application switch and the internal routers they have added an additional requirement.

This requirement is that the design allow for expansion in the future in a manner that will eliminate the failure points. These requests are allowed for in the following ways.

1. Routers and switches are modular and /or support some type of aggregation and standby mechanism for increased bandwidth, capability and availability enhancements.
2. All firewalls support high-throughput and high-availability cluster types.
3. The Authentication System supports multiple servers with replication.
4. The Proxy server is less than 25% utilized but supports expansion and / or clustering if needed.
5. All IP address ranges are less than 25-50% utilized and adjacent ranges are available if needed.

VPN usage is currently very restricted and reflects the fact that there is staff on hand 24x7. Recognizing this fact the load placed on the primary firewall by the VPN traffic is minimal. If demand for this option increases in the future the design allows for the following modifications with minimal downtime.

a. Installation of a VPN accelerator card into the primary firewall.
b. Placement of a dedicated VPN device into the area between the Primary and User firewalls. (Similar to the placement of the proxy server)
c. Moving VPN services to the internal (User) firewall.

This design is the most cost-effective means of achieving the business goals this year since it utilizes existing equipment almost entirely throughout. The only additional equipment being purchased is the hardware and software for the internal firewalls required by the new audit structure.

Part 2

SECURITY POLICY AND TUTORIAL

Border Router ACL's

Please note, for a more complete print out of the border router configuration please refer to Border Router Configuration on page 49 .

On our border router we have three access control lists, 182, 2000 and 2200.

Rules (ACL's, Security, Desktop, etc) for the perimeter equipment used in this paper are read by the software from first to last (top to bottom). This means that the first rule which matches the condition being examined will determine the action taken by the equipment software. This makes the order of the rules very important in achieving the desired result.

Though short, a good example of this can be found in our first Access list, number 182. The intent of this control list is to allow a connection coming from a specific address while denying access from all other addresses. Since the specific address is a subset of all addresses we have to get the machine to "see" a rule that matches our "specific address" before it "sees" a rule that matches "all other addresses"

Using the "top to bottom" ordering scheme, the first rule is a specific permit and the second is a flat deny. When the router receives a terminal communication attempt it will read this list. If the conditions match the first statement it comes to, meaning that the communication is from our "specific address", the machine stops reading the list and the session is allowed. If the conditions do not match the machine continues to the next statement, and the next, and so on until the list runs out or it finds a match.

Since our next statement in the list will match all other addresses attempting to connect to the machine, no other connections will be allowed.
It is easy to see from this example that if the rule order were reversed, then it would not matter that you had a permit statement in the list since the first statement that would match would always be a "deny".

All Incoming traffic to our Border Routers and Firewalls is subject to the "Default Deny" rule. If we haven't set up a rule accepting the traffic we want the traffic to be dropped. We drop rather than reject the traffic in order to avoid providing information in response to probes as well as minimizing unnecessary and possibly harmful excess traffic being generated by our devices.

Access list 182 is used to control administrative access to the border router and is applied to the VTY configuration.

```
access-list 182 remarkaccess list for administrative access
```

(The first line is a remark identifying the list.)

```
access-list 182 permit tcp host 10.10.10.2 any
```

(permits tcp traffic coming from 10.10.10.2, our administrative address.)

```
access-list 182 deny   ip any any log
```

(denies all ip traffic.)

Access list 2000 is applied to inbound (Internet to our network) traffic on the serial interfaces of the routers.

```
access-list 2000 remark  Incoming Serial ACL
```

(The first line is a remark identifying the list.)

```
access-list 2000 deny   ip 10.10.10.0 0.0.0.255 any log-input
access-list 2000 deny   ip host 0.0.0.0 any log-input
access-list 2000 deny   ip 127.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 224.0.0.0 15.255.255.255 any log-input
access-list 2000 deny   ip 240.0.0.0 15.255.255.255 any log-input
access-list 2000 deny   ip 10.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 172.16.0.0 0.15.255.255 any log-input
access-list 2000 deny   ip 192.168.0.0 0.0.255.255 any log-input
access-list 2000 deny   ip 169.254.0.0 0.0.255.255 any log-input
access-list 2000 deny   ip 1.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 2.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 5.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 7.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 23.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 27.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 31.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 36.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 37.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 39.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 41.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 42.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 58.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 59.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 60.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 70.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 71.0.0.0 0.255.255.255 any log-input
```

```
access-list 2000 deny   ip 72.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 73.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 74.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 75.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 76.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 77.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 78.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 79.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 83.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 84.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 85.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 86.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 87.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 88.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 89.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 90.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 91.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 92.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 93.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 94.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 95.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 96.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 97.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 98.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 99.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 100.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 101.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 102.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 103.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 104.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 105.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 106.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 107.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 108.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 109.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 110.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 111.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 112.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 113.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 114.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 115.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 116.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 117.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 118.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 119.0.0.0 0.255.255.255 any log-input
```

```
access-list 2000 deny   ip 120.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 121.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 122.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 123.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 124.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 125.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 126.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 197.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 240.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 241.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 242.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 243.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 244.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 245.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 246.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 247.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 248.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 249.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 250.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 251.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 252.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 253.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 254.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 255.0.0.0 0.255.255.255 any log-input
```

(These lines deny incoming internet traffic from our own subnet, the reserved (private) subnets and the non-assigned subnets. This helps to prevent non-legitimate traffic from ever entering our network area. The information from the logs can help us to identify potential attacks.)

```
access-list 2000 permit tcp any any established
```

(permits established traffic, allowing replies to outgoing network requests)

```
access-list 2000 permit tcp host 10.10.102.25 host 10.10.103.10 eq bgp
```

(permits bgp traffic from our peer for routing purposes)

```
access-list 2000 permit tcp any host 10.10.10.130 eq 443
access-list 2000 permit tcp any host 10.10.10.131 eq 443
access-list 2000 permit tcp any host 10.10.10.132 eq ftp
access-list 2000 permit tcp any host 10.10.10.140 eq 443
access-list 2000 permit tcp any host 10.10.10.141 eq 443
access-list 2000 permit tcp any host 10.10.10.142 eq ftp
access-list 2000 permit tcp any host 10.10.10.150 eq 443
access-list 2000 permit tcp any host 10.10.10.152 eq ftp
access-list 2000 permit tcp any host 10.10.10.160 eq 443
access-list 2000 permit tcp any host 10.10.10.161 eq 443
access-list 2000 permit tcp any host 10.10.10.162 eq ftp
access-list 2000 permit tcp any host 10.10.10.163 eq 443
access-list 2000 permit tcp any host 10.10.10.164 eq smtp
```

```
access-list 2000 permit tcp any host 10.10.10.175 eq domain
access-list 2000 permit udp any host 10.10.10.175 eq domain
access-list 2000 permit tcp any eq domain host 10.10.10.175
access-list 2000 permit udp any eq domain host 10.10.10.175
access-list 2000 permit tcp any host 10.10.10.180 eq www
access-list 2000 permit tcp any host 10.10.10.181 eq 443
access-list 2000 permit tcp any host 10.10.10.251 eq 264
access-list 2000 permit tcp any host 10.10.10.251 eq 500
access-list 2000 permit udp any host 10.10.10.251 eq 500
access-list 2000 permit udp any host 10.10.10.251 eq 1548
access-list 2000 permit udp any host 10.10.10.251 eq 1549
access-list 2000 permit udp any host 10.10.10.251 eq 2746
access-list 2000 permit tcp any host 10.10.10.251 eq 18231
access-list 2000 permit tcp any host 10.10.10.251 eq 18232
access-list 2000 permit udp any host 10.10.10.251 eq 18233
access-list 2000 permit udp any host 10.10.10.251 eq 18234
```

(This section permits specific inbound traffic to our defined internet facing hosts, allowing external parties to reach us to conduct business and the VPN)

```
access-list 2000 permit gre any any
access-list 2000 permit udp host 10.10.105.20 any eq ntp
access-list 2000 permit udp host 10.10.105.21 any eq ntp
access-list 2000 permit udp host 10.10.105.22 any eq ntp
```

(This section permits gre and ntp traffic for routing and time updates.)

```
access-list 2000 deny   ip any any log-input
```

(This section denies any inbound traffic not previously permitted, the "default deny all" that keeps out traffic that we haven't expressly allowed)

Access list 2200 is applied to outbound (our network to the Internet) traffic on the serial interfaces of the routers.

```
access-list 2200 remark  Outbound serial ACL
```

(The first line is a remark identifying the list.)

```
access-list 2200 deny   tcp any any eq telnet
access-list 2200 deny   tcp any any eq 135
access-list 2200 deny   udp any any eq 135
access-list 2200 deny   tcp any any eq 137
access-list 2200 deny   udp any any eq netbios-ns
access-list 2200 deny   tcp any any eq 138
access-list 2200 deny   udp any any eq netbios-dgm
access-list 2200 deny   tcp any any eq 139
access-list 2200 deny   tcp any any eq irc
access-list 2200 deny   udp any any eq netbios-ss
access-list 2200 deny   tcp any any eq 514
access-list 2200 deny   tcp any any eq 1214
```

```
access-list 2200 deny   tcp any eq 1214 any
access-list 2200 deny   tcp any any eq 1333
access-list 2200 deny   tcp any any eq 1334
access-list 2200 deny   tcp any any eq 1503
access-list 2200 deny   tcp any any eq 1863
access-list 2200 deny   tcp any any eq 3389
access-list 2200 deny   tcp any any eq 3570
access-list 2200 deny   tcp any any eq 3574
access-list 2200 deny   udp any any eq 4000
access-list 2200 deny   udp any any eq 4001
access-list 2200 deny   tcp any any eq 4443
access-list 2200 deny   tcp any any eq 5010
access-list 2200 deny   tcp any any eq 5050
access-list 2200 deny   tcp any any eq 5190
access-list 2200 deny   tcp any any eq 6346
access-list 2200 deny   tcp any eq 6346 any
access-list 2200 deny   tcp any any eq 6701
access-list 2200 deny   tcp any any eq 6891
access-list 2200 deny   tcp any any eq 7320
access-list 2200 deny   udp any any eq 13324
access-list 2200 deny   udp any any eq 13325
```

(This section specifically blocks ports normally used for carrying traffic that we don't want going out of our network for both security and business reasons. Netbios, telnet, irc, Kazaa, AOL, MSN,ICQ,Yahoo,syslog, ms-sql)

```
access-list 2200 deny   ip host 0.0.0.0 any log-input
access-list 2200 deny   ip 127.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 224.0.0.0 15.255.255.255 any log-input
access-list 2200 deny   ip 240.0.0.0 15.255.255.255 any log-input
access-list 2200 deny   ip 10.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 172.16.0.0 0.15.255.255 any log-input
access-list 2200 deny   ip 192.168.0.0 0.0.255.255 any log-input
access-list 2200 deny   ip 169.254.0.0 0.0.255.255 any log-input
access-list 2200 deny   ip 1.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 2.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 5.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 7.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 23.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 27.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 31.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 36.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 37.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 39.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 41.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 42.0.0.0 0.255.255.255 any log-input
```

```
access-list 2200 deny   ip 58.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 59.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 60.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 70.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 71.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 72.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 73.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 74.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 75.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 76.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 77.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 78.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 79.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 83.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 84.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 85.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 86.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 87.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 88.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 89.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 90.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 91.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 92.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 93.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 94.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 95.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 96.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 97.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 98.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 99.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 100.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 101.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 102.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 103.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 104.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 105.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 106.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 107.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 108.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 109.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 110.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 111.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 112.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 113.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 114.0.0.0 0.255.255.255 any log-input
```

```
access-list 2200 deny   ip 115.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 116.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 117.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 118.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 119.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 120.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 121.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 122.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 123.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 124.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 125.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 126.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 197.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 240.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 241.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 242.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 243.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 244.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 245.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 246.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 247.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 248.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 249.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 250.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 251.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 252.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 253.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 254.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 255.0.0.0 0.255.255.255 any log-input
```

(Deny outgoing internet traffic from the reserved (private) subnets and the non-assigned subnets. Our legitimate internally generated outbound traffic will always be translated to an external address before leaving the network. Traffic leaving our network from unused addresses is a good sign that we have an unapproved program or some other problem so we don't allow it and we keep a record of the event)

```
access-list 2200 permit ip any any
```

(Permits all outgoing traffic not earlier denied. Since this is the outbound side we permit all traffic that we have not specifically denied to allow internal traffic out.)

Firewall Access Rules

Please see "Primary Firewall and VPN Configuration" on page 60 for expanded configuration information

Community Rule

Source:	MemberGWs.EncDomain@MyIntranet
Destination:	MemberGWs.EncDomain@MyIntranet
If Via:	Any
Service:	EncryptedServices@MyIntranet
Action:	Encrypt&Continue
Track:	-----
Time:	Any
Install on:	Any
Comment:	Automatic Encryption Rule for community:MyIntranet

Since we are using Simplified Mode this rule has been automatically installed by the Firewall system to handle VPN traffic encryption.

Rule 1

Source:	Remote_Access@Any
Destination:	VPN
If Via:	Remote Access
Service:	Any
Action:	clientencrypt
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows users in the RemoteAccess Group to reach the VPN network via remote access.

Rule 1 is used in conjunction with VPN access to permit users in the Remote_Access user group to make connections to the VPN network.

Rule 2

Source:	Administrative_FW
Destination:	box1
If Via:	Any
Service:	Any
Action:	accept
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows access from the translated administrator's address to the firewall.

Rule 2 is used to allow the VPN network address designated for administrative use access to the firewall for management purposes.

Rule 3

Source: Any
Destination: box1
If Via: Any
Service: Any
Action: drop
Track: Log
Time: Any
Install on: Any
Comment: Deny all other attempts to reach the firewall

Rule 3 is placed here to prohibit all other traffic (not matching rules 1 or 2) from being accepted by the firewall.

Rule 4

Source: BorderRouter_1
BorderRouter_2
BorderRouter_HSRP
Destination: syslog.giaccookies.com
If Via: Any
Service: syslog
Action: accept
Track: Log
Time: Any
Install on: Any
Comment: Accept syslog traffic from the border routers to the syslog server.

Rule 4 allows syslog traffic originating with the border routers to pass the firewall going to the address designated for the syslog server.

Rule 5

Source: Any
Destination: https.customer
https.customer-file
https.employee
https.employee-file
https.employee-mail
https.partner
https.partner-file
https.supplier
https.supplier-file
https.www.giaccookies
If Via: Any

Service: https
Action: accept
Track: Log
Time: Any
Install on: Any
Comment: Allows https traffic to the various company web servers.

Rule 5 is designed to permit HTTPS traffic from all users to reach our web based applications servers.

Rule 6

Source: Any
Destination: http.www.giaccookies
If Via: Any
Service: http
Action: accept
Track: Log
Time: Any
Install on: Any
Comment: Allows http traffic to the public company web site.

Rule 6 is designed to permit HTTP traffic from all users to reach our open (company web site) servers.

Rule 7

Source: Any
Destination: ftp.customer-file
ftp.employee-file
ftp.partner-file
ftp.supplier-file
If Via: Any
Service: ftp
Action: accept
Track: Log
Time: Any
Install on: Any
Comment: Allows FTP traffic to the company FTP servers.

Rule 7 is designed to permit FTP traffic from all users to reach our web based file servers.

Rule 8

Source: Any
Destination: dns.giaccookies.com
If Via: Any
Service: dns
Action: accept
Track: Log

Time:	Any
Install on:	Any
Comment:	Allows DNS traffic to the company DNS server.

Rule 8 is designed to permit DNS traffic from all users to reach our DNS servers.

Rule 9

Source:	dns.giaccookies.com
Destination:	Any
If Via:	Any
Service:	dns
Action:	accept
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows DNS traffic from the company DNS server.

Rule 9 is designed to permit outbound DNS traffic from our DNS servers.

Rule 10

Source:	Any
Destination:	smtp.giaccookies.com
If Via:	Any
Service:	smtp
Action:	accept
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows SMTP traffic to the company mail gateway.

Rule 10 is designed to permit SMTP traffic from all users to reach our SMTP servers.

Rule 11

Source:	smtp.giaccookies.com
Destination:	Any
If Via:	Any
Service:	smtp
Action:	accept
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows SMTP traffic from the company mail gateway.

Rule 11 is designed to permit outbound SMTP traffic from our SMTP servers.

Rule 12

Source:	Administrative_Outgoing
Destination:	Any
If Via:	Any
Service:	Any
Action:	accept
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows Administrative traffic bypassing the Proxy server. *Note that rule 3 will block traffic to the firewall itself*

Rule 12 is designed to permit all outbound traffic from our designated administrative address that bypasses the Proxy Server.

Rule 13

Source:	Proxy_Server
Destination:	Any
If Via:	Any
Service:	ftp http https dns
Action:	accept
Track:	Log
Time:	Any
Install on:	Any
Comment:	Allows outgoing Proxy traffic for FTP, HTTP, HTTPS, and DNS. *Note that rule 3 will block traffic to the firewall itself*

Rule 13 is designed to permit outbound FTP, HTTP, HTTPS and DNS traffic from our designated Proxy server address.

Implicit Rule

Source:	FireWall (Box1)
Destination:	Any
If Via:	Any
Service:	Any
Action:	accept
Track:	-----
Time:	Any
Install on:	Any
Comment:	Implicit rule: Enable Outgoing Connections

This rule is automatically installed by the Firewall system to permit traffic originating from the firewall.

Rule 14

Source:	Any
Destination:	Any
If Via:	Any
Service:	Any
Action:	drop
Track:	Log
Time:	Any
Install on:	Any
Comment:	Deny all traffic not previously permitted.

Rule 14, the last in our series, is set to deny all traffic that doesn't match any earlier rules.

While these 14 numbered rules are the complete explicit ruleset on our primary firewall the reader should note the community and implied rules. There are a number of settings within the software that also play a part in how the firewall will handle a given traffic pattern or request.

Antispoofing:

The topology of the Firewall interfaces is defined by the address and network mask of the interface and antispoofing is enabled. This means that traffic from an address that would normally be allowed by the explicit ruleset will be denied if it tries to enter the firewall by the wrong network adapter. All traffic will be blocked at the interface if it is marked as originating from an undefined network address.

SmartDefense:

The CheckPoint SmartDefense module is enabled with its default settings. This means that traffic will be inspected against a number of known scenarios (for instance non-DNS traffic over port 53) and possibly denied. An administrative user has to be aware of this since these items may cause otherwise legitimate traffic to be denied. An example of this is the "Max Ping Size" setting. At its default this will deny ping traffic from Cisco Equipment since their default size of 100 bytes is larger than SmartDefense's default size of 64 bytes.

Community and Implied Rules:

Community and Implied rules are not shown in the GUI by default but can be shown by checking, VIEW – Implied rules and VIEW – Community Rules. There are a number of rules here based on Global Properties and settings within the various optional components like FloodGate-1 and VPN-1 Pro. These rules, their position in the rule sets and their settings should be reviewed to determine if you are allowing only the traffic you want to allow. Examples of these automatically created rules can be found before rule numbers 1 and 14 in the rule list above.

VPN Policy

There are very few explicit rules in our VPN configuration.

Rule 1 of our Firewall allows only users in the Remote_Access group to access our VPN network by connecting via the VPN. We have this rule to control what users can use the VPN to access our network.

The other explicit rule set that is used in our VPN configuration is the client desktop rules.

Rules for the SecureClient Desktop are:

Inbound (Traffic going to the Desktop)
Rule 1

Source:	VPN
Desktop:	Remote_Access@Any
Service:	Any
Action:	encrypt
Track:	Log
Comment:	Allows our VPN network to reach the desktop with encrypted traffic.

Rule 1 makes sure that all traffic coming into our desktop from the VPN is encrypted.

Rule 2

Source:	Any
Desktop:	All Users@Any
Service:	Any
Action:	block
Track:	Log
Comment:	Blocks all other traffic coming into the Desktop.

Rule 2 keeps the desktop from communicating with other areas while using our VPN (split tunneling, etc).

Outbound (Traffic leaving the Desktop)

Rule 3

Desktop:	Remote_Access@Any
Destination:	VPN

Service: Any
Action: encrypt
Track: Log
Comment: Encrypts our traffic to the VPN network.

Rule 3 prohibits the desktop from sending information across the wire to our network without encryption.

Rule 4

Desktop: All Users@Any
Destination: Any
Service: Any
Action: Accept
Track: Log
Comment: Allows our desktop anywhere else with unencrypted traffic.

Rule 4 allows our desktop to communicate with areas other than our internal network without encryption.

As explained with the Firewall rule sets earlier there are a number of settings within the Global Properties (Policy ----Global Properties) and the Gateway object (double-click the object or select the object and chose edit to view the gateway properties) pages that directly affect VPN action and performance. Administrators should make sure that they are aware of these settings. On our Firewall the following are our settings, most of these are self-explanatory, for the others I have included brief notes.

1. VPN-1 Pro
    a. VPN configuration Simplified Mode.
    b. Renegotiate IKE phase 1 every 1440 minutes and phase 2 every 3600 minutes.
    c. CRL Grace periods
        i. Before valid: 1800 seconds.
        ii. After no longer valid: 1800 seconds.
        iii. Extension for SecureRemote/SecureClient: 3600

Controls VPN-1 Pro gateway connections. Defines the configuration mode as Simplified, (we don't have to create encryption rules ourselves) and the time frames for IKE renegotiation and Certificate revocation list grace periods.

2. VPN 1-Net
    a. Accept encrypted connections.
    b. Hide all connections.
    c. Log all traffic.

Controls VPN 1-Net gateway connections. Requires connections to be encrypted, hides all VPN connections with NAT and logs all accepted and blocked VPN traffic.

3. Remote Access
    a. Topology Update
        i. Every 24 hours
        ii. Automatic
    b. Authentication Timeout
        i. Validation timeout 60 minutes.
    c. Encrypt DNS Traffic
    d. SecureClient Desktop security policy expiration time 60 minutes

Topology is automatically updated every 24 hours after key exchange, authentication times out every 60 minutes, DNS traffic is encrypted and the SecureClient Desktop reverts to the default policy after 60 minutes not logged into the policy server.

4. VPN – Basic
    a. Supported authentication methods
        i. Public Key Signatures
        ii. Hybrid Mode
    b. IKE over TCP is supported
    c. IP compression is supported for SecureClient
5. VPN – Advanced
    a. Encryption Algorithm is 3DES
    b. Data Integrity is SHA1
    c. These settings are enforced on all users
6. IKE Security associations
    a. Supports and Uses Diffie-Hellman group 2 (1024 bit)
7. Certificates
    a. Client verifies gateway's certificate against the revocation list.
    b. Automatically attempt to update user's certificate beginning 60 days before the expiration date.
8. Secure Configuration Verification
    a. Apply SCV on Simplified Mode Security Policies.
    b. Policy is installed on all interfaces
    c. Only TCP/IP protocols are used.
9. Configuration Violation Notifications
    a. Generate a log on the client
    b. Notify the user.
10. Early Versions compatibility
    a. The required policy for all desktops is "allow outgoing only".
    b. Client is enforcing required policy.

Earlier versions (non-NG) of the Checkpoint Secure Client will receive their configuration information from these settings rather than the Desktop Client rules outlined above.

Users must be defined with a Certificate for authentication. This is set when creating the user.

Users are required to have the Checkpoint SecureClient software.

OfficeMode is configured for the Remote_Access user group using the "VPN_Office_Mode" network for the assignment of IP addresses.

The following IP Pool Optional parameters are set:

a. DNS Server = VPN_Services
b. WINS Server = VPN_Services
c. Domain Name = vpn.giaccookies.com

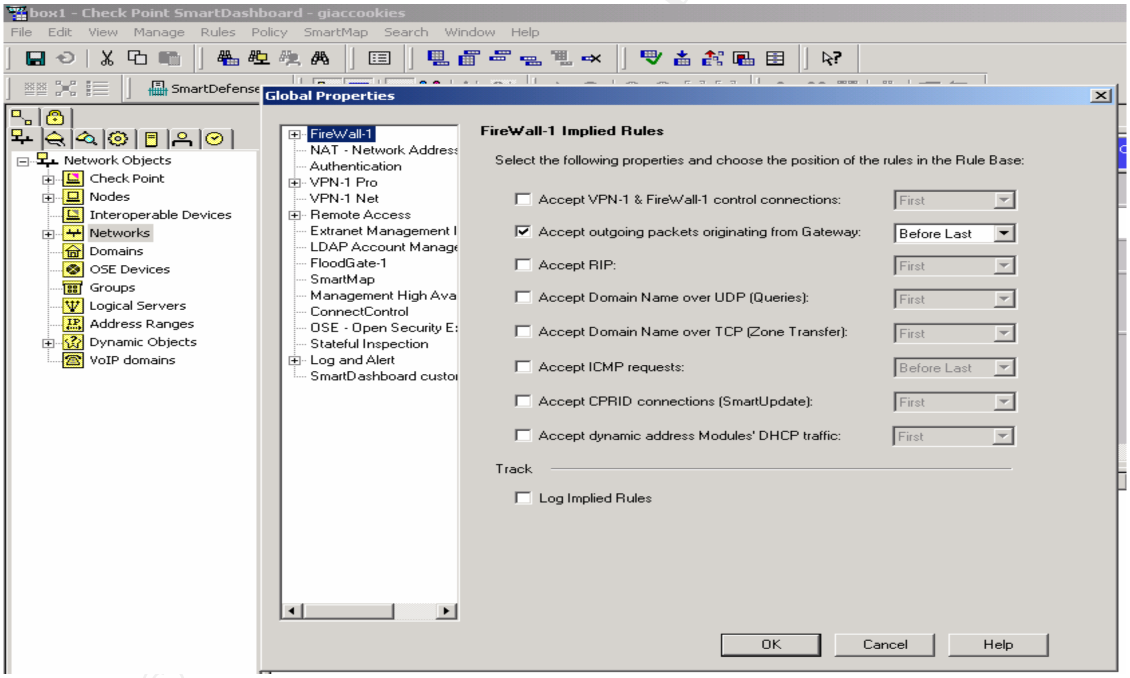
IP lease duration is 30 minutes.

VPN Setup Tutorial

In our scenario the VPN is setup with the user base utilizing the SecureClient software with Certificates for authentication and Office Mode for IP address and associated information assignment.

We begin with the Firewall set up and operational. The optional Policy Server component was included at the initial installation. We have connected to the management server with the Check Point SmartDashboard client and will be working from that interface. Under the "View" menu the status bar, objects tree, rule base and objects list are checked.

First we will check the configuration of the Global properties to ensure that they match our requirements. Open the Global properties page by choosing the "Policy" menu item and selecting "Global Properties" review the settings listed, making sure that they meet your requirements. The global settings used in our VPN configuration can be found in the previous chapter, VPN Policy.



FireWall-1 Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

- □ Accept VPN-1 & FireWall-1 control connections: First
- ☑ Accept outgoing packets originating from Gateway: Before Last
- □ Accept RIP: First
- □ Accept Domain Name over UDP (Queries): First
- □ Accept Domain Name over TCP (Zone Transfer): First
- □ Accept ICMP requests: Before Last
- □ Accept CPRID connections (SmartUpdate): First
- □ Accept dynamic address Modules' DHCP traffic: First

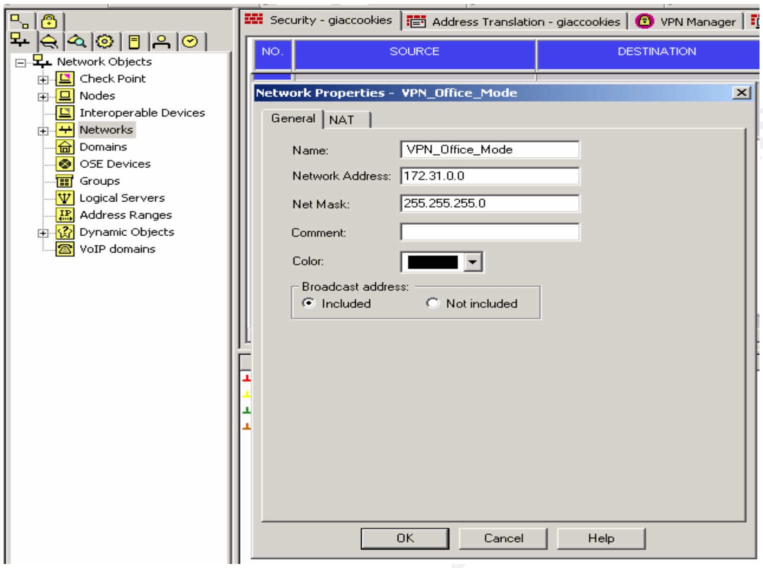
Track

- □ Log Implied Rules

Next we will define the network object that will be used to assign IP address information to the clients. In Office Mode the Gateway will assign IP addresses from the range that is defined by this object. We have chosen the network segment 172.31.0.0/24 for this purpose. Note that this segment is not used anywhere else in our network and is not part of our encryption domain. We expect to use only a very small portion of the available addresses in this range but having them available will allow us plenty of room for expansion should needs change.

To create our network object we right-mouse click on the “Networks” object in the objects tree and select “New Network”. Fill in the blanks (note that the name cannot contain spaces) with the required information. In our case this information is as follows:

Name: VPN_Office_Mode
Network Address: 172.31.0.0
Net Mask: 255.255.255.0
Comment: none

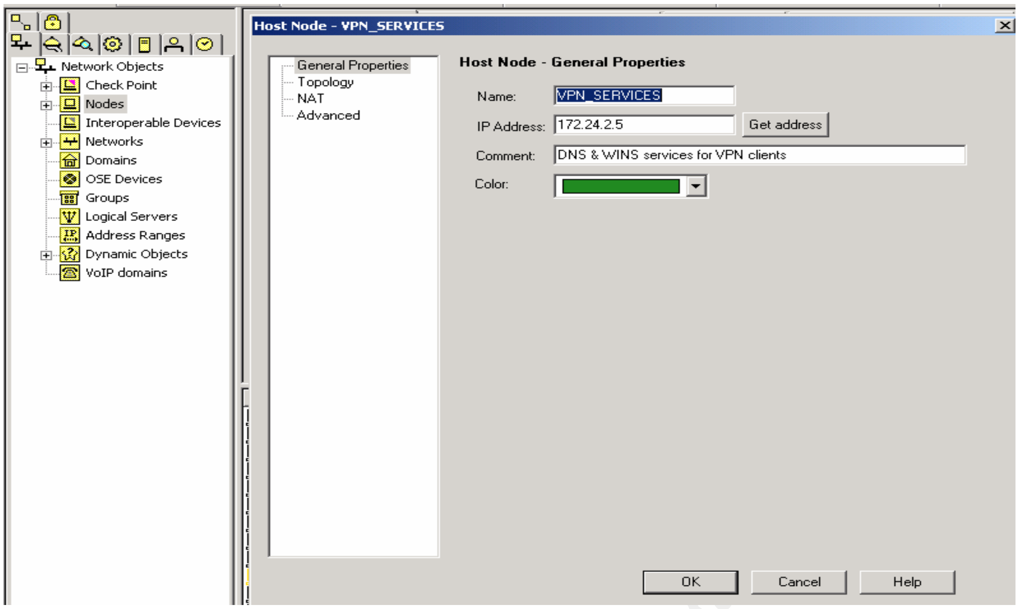


Network Properties - VPN_Office_Mode

Name: VPN_Office_Mode
Network Address: 172.31.0.0
Net Mask: 255.255.255.0
Comment:
Color:
Broadcast address: ● Included ○ Not included

Now we will define the Node that will be used to offer DNS & WINS services to the VPN users. Right-mouse click on the “Nodes” object in the objects tree, select “New Node” and “Host”. Fill in the blanks (note that the name cannot contain spaces) with the required information. In our case this information is as follows:

Name: VPN_Services
Network Address: 172.24.2.5
Comment: DNS & WINS services for VPN Clients


Host Node - VPN_SERVICES

Host Node - General Properties

Name: VPN_SERVICES

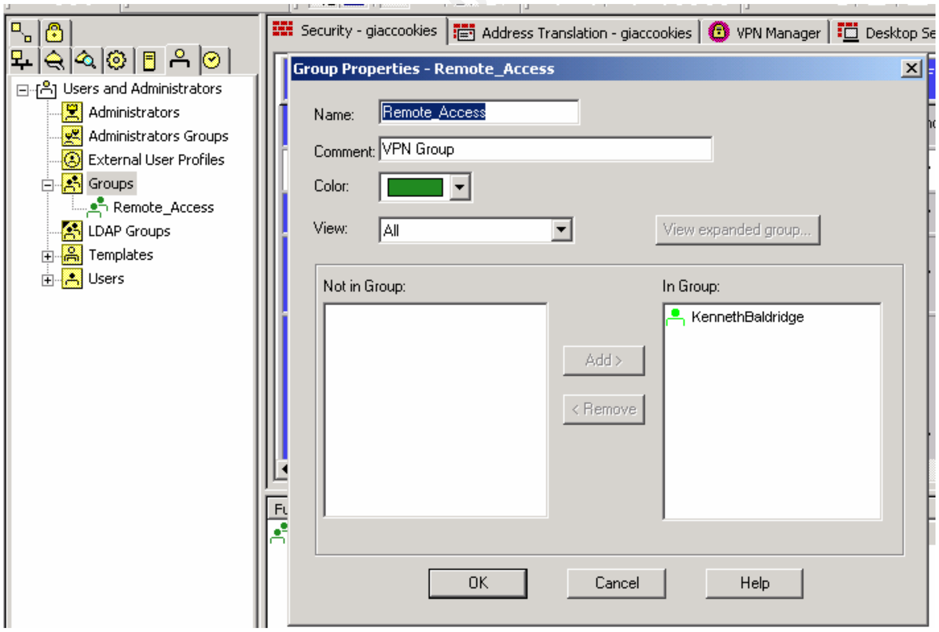
IP Address: 172.24.2.5

Comment: DNS & WINS services for VPN clients

Color: 🟩

Next we will set up a group to use for remote access. All members of this group will be able to use the Office Mode VPN. To create this group select the "Users and Administrators" section in the objects tree, right-mouse click "Groups" and select "New Group". Fill in the blanks with the required information. In our case this information is as follows:

Name:	Remote_Access
Comment:	VPN Group


Group Properties - Remote_Access

Name: Remote_Access

Comment: VPN Group

Color: 🟩

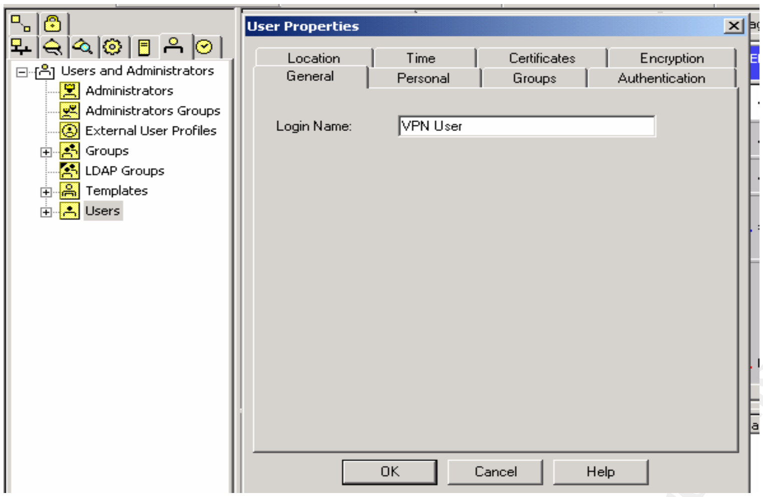
View: All

Not in Group:

In Group: KennethBaldridge

Users that you want to have VPN access can be added to this group at any time.

New Users are created by selecting the “Users” object, right-mouse click “new user” – “Default”.

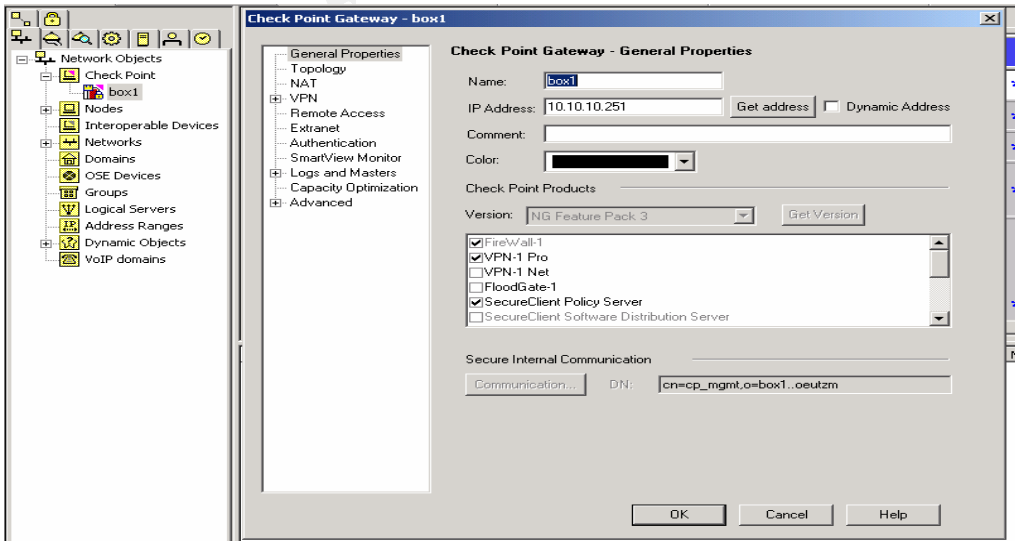


Login Name: VPN User

Be sure to go through all of the tabs and check the information. For our purposes the default information is fine in most cases. The exceptions are:

1. Groups: Add the user to the appropriate group, for us this is the Remote_Access group we just created.
2. Encryption: Check the IKE object
3. Certificates: Generate and save a certificate for the user. (You should keep track of these in a secure location)

Now we are ready to set the VPN properties on the Firewall object itself. Expand the Check Point object in the objects tree, right-mouse click the firewall object and choose “edit”.



Name: box1

IP Address: 10.10.10.251

□ Dynamic Address

Comment:

Color:

Version: NG Feature Pack 3

☑ FireWall-1
☑ VPN-1 Pro
□ VPN-1 Net
□ FloodGate-1
☑ SecureClient Policy Server
□ SecureClient Software Distribution Server

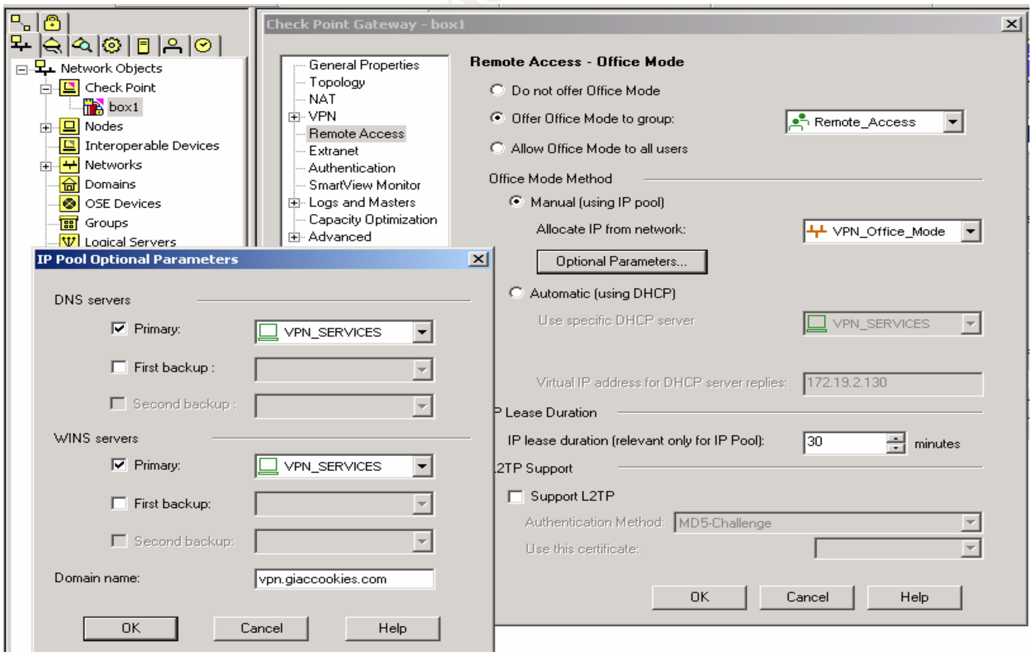
DN: cn=cp_mgmt,o=box1..oeutzm

On the “General Properties” page make sure that “VPN-1 Pro” and “SecureClient Policy Server” are checked. The IP address listed should also be the same as the external address of the gateway. Be careful with this, it could affect your license depending on the type you are using (local or central).

Now on the “Authentication” page add the “Remote_Access” group to the Policy Server section and select the authentication types that you will be using. Now close and reopen the object, this will cause the IKE default certificate to be generated.

Next go to the “VPN” page and add the “RemoteAccess” community to the VPN communities that this module participates in. Expand the VPN section and on the “VPN Advanced” page ensure that the “Support Nat…” “Support Key…” and “Perform and organized……” options are checked and “Support clientless VPN” is not checked.

On the “Remote Access” page check “Offer Office Mode to group” and use the drop down list to select “Remote_Access”
Under Office Mode Method select “Manual” and use the drop down list to select the “VPN_Office_Mode” network.
Now after selecting the “Optional Parameters” button check the DNS & WINS server boxes and use the drop down list to select the VPN_Services object. Last on this page fill in the Domain name with the desired suffix.



Remote Access - Office Mode

○ Do not offer Office Mode
● Offer Office Mode to group: Remote_Access
○ Allow Office Mode to all users

Office Mode Method
● Manual (using IP pool)
Allocate IP from network: VPN_Office_Mode
Optional Parameters...
○ Automatic (using DHCP)
Use specific DHCP server: VPN_SERVICES
Virtual IP address for DHCP server replies: 172.19.2.130

P Lease Duration
IP lease duration (relevant only for IP Pool): 30 minutes

2TP Support
□ Support L2TP
Authentication Method: MD5-Challenge
Use this certificate:

OK Cancel Help

IP Pool Optional Parameters

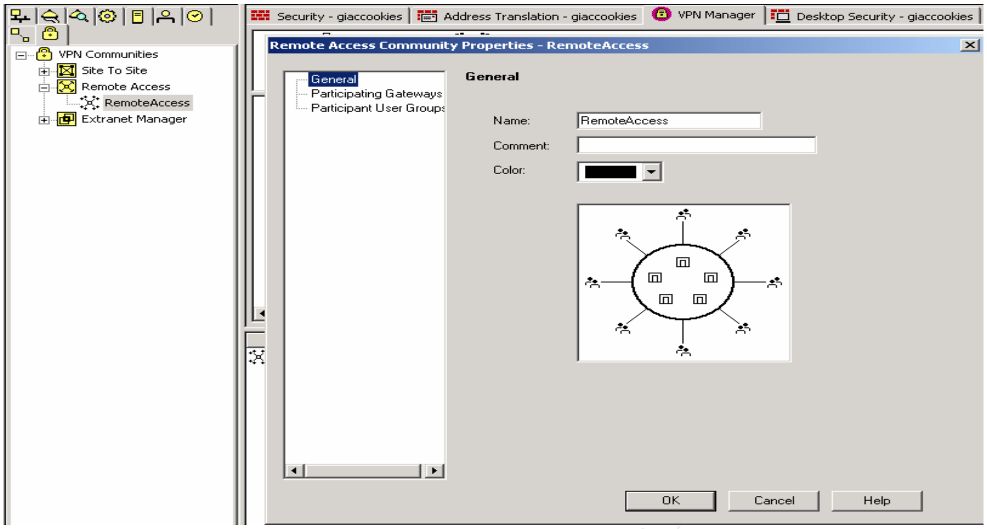
DNS servers
☑ Primary: VPN_SERVICES
□ First backup :
□ Second backup :

WINS servers
☑ Primary: VPN_SERVICES
□ First backup:
□ Second backup:

Domain name: vpn.giaccookies.com

OK Cancel Help

Next we need to verify the settings of our remote access community. Select the VPN object in the objects tree, expand the Remote Access object, right-mouse click the sub Remote Access object and choose “edit”.



General

Name: RemoteAccess

Comment:

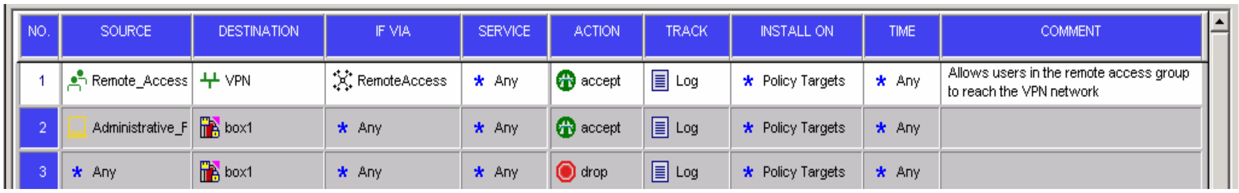
Color:

Make sure that your Firewall is in the “Participating Gateways” group and that your VPN users group (in our case Remote_Access”) is in the “Participant User Groups” section.

This completes the setup of the VPN itself, now we need to create some rules for use with the VPN. First we will add a rule to our Firewall rulebase to allow the VPN traffic to pass.

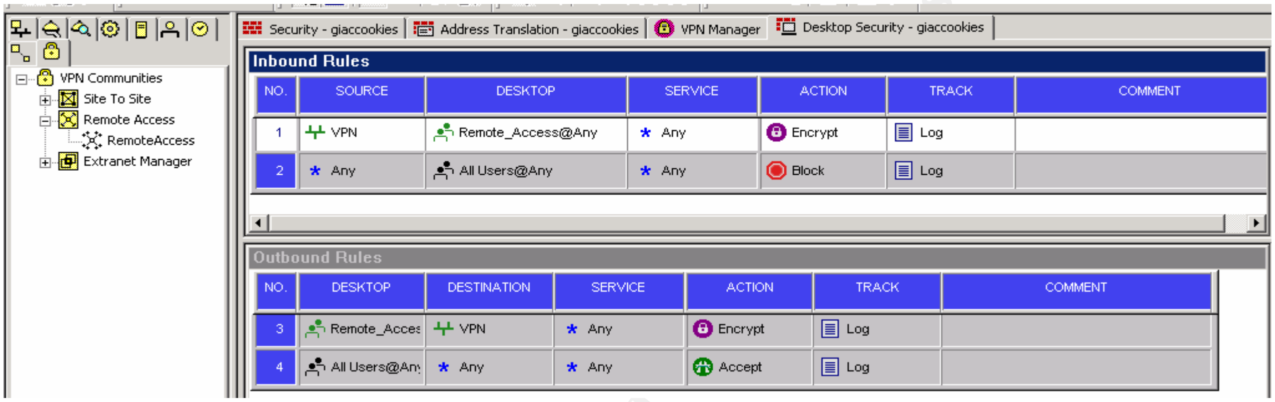
Mouse click on the Security tab in the GUI to display the rule set. Then select the “Rules” menu item, “Add rule”--- “top” we want this to be the first rule in our list so that the VPN traffic will not be blocked by the rule that we created earlier blocking all connections to the firewall itself.

We now need to set the appropriate Source, Destination, etc items for the rule that we just created. To do this we simply need to right-mouse click the item in each column that we want to change and add in the item that we want. We want to set this rule so that our designated user group “Remote_Access” (source) can get to the “VPN” network (destination) if they are using the VPN “RemoteAccess” (if via) for any traffic (service) “accept” (action) and “log” (track) so that we have a record.



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Remote_Access	VPN	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any	Allows users in the remote access group to reach the VPN network
2	Administrative_F	box1	* Any	* Any	accept	Log	* Policy Targets	* Any	
3	* Any	box1	* Any	* Any	drop	Log	* Policy Targets	* Any	

It isn’t required but if you like you can now set any rules that you want your SecureClient desktops to follow by going to the Desktop Security tab. Rules are added here the same way they are for the firewall. You should be sure to remember that “Inbound” means that the rule will affect traffic coming into the desktop while “outbound” means that the rule will affect traffic leaving the desktop. I have seen a number of administrators that set these rules as if they related to traffic arriving and leaving the firewall.   We set our rules as follows.



Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENT
1	VPN	Remote_Access@Any	* Any	Encrypt	Log	
2	* Any	All Users@Any	* Any	Block	Log	

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
3	Remote_Acces	VPN	* Any	Encrypt	Log	
4	All Users@Any	* Any	* Any	Accept	Log	

Before we can use the VPN gateway we need to install the SecureClient software. This can be done manually but to ease the administration burden we will create an installation package that can be used by the desktop administrators when setting up a box for the end user. To do this we start the SecureClient Packaging tool and (after logging in) choose new profile. Enter a name for the profile and select next.

Most of the defaults will work fine for us with a few exceptions that I’ve noted below:

1. Client mode must be set to “connect mode” to enable support for Office Mode on the firewall.
2. We don’t want our clients changing modes so we will clear the “enable mode transition” check box.
3. Under “Advanced Encryption options” we will select “IKE over TCP” and “Force UDP encapsulation for IPsec connections”
4. Check the box for “partial topology” and enter the Firewall/VPN information in the drop down boxes.

Once you have finished the new profile wizard you can choose to generate a package now or later. After you have generated an install package it is a simple matter of running the package to install SecureClient with the appropriate settings.

Part 3

Verify the Firewall Policy

Plan the Audit.

We have been asked to verify that the Primary GIAC firewall correctly enforces the policies described earlier. Since this is an internal audit at the request of Management we have direct access to the Firewall itself as well as the subnets surrounding it.

To determine if the firewall is performing as expected we will:

1. Capture and print out the current firewall configuration.
2. Compare the configuration to the design policies.
3. Identify what traffic should and should not be passing the firewall.
4. Ask the IT staff to provide us with the past weeks logs for the:
    a. Firewall
    b. Border Router
    c. Proxy Server
    d. Internal Firewall (USER)
    e. Secure Application Switch
    f. IDS located in the DMZ-1 and VPN Segments
5. Place a computer with scanning software on the External Subnet in front of the firewall but behind the Border Router.
    a. Place computers with packet-sniffing software on the subnets behind the firewall:
        i. Proxy network
        ii. VPN network
        iii. DMZ network
6. The scanning computer will then be swapped with capturing computers on the other subnets and the tests repeated.
7. We will also attempt management station connections to the firewall from each of the computer systems located on the various subnets.
8. After completion of all scans firewall logs for the scanning period as well as logs from our scanning and capture machines will be analyzed.

The Company has scheduled a maintenance weekend for testing. We will be taking advantage of this time period to avoid impacting either customers or business operations. We will be conducting address/port/service scans beginning at 7am local time on Saturday. This will allow a buffer zone of time on Sunday to correct any unexpected complications, errors or issues that may arise from the scans prior to the next business week.

We currently estimate 16 to 20 man hours to conduct the examination and produce reports. The estimates are based on internal staff providing us with:

1. The logs outlined in item 4 in standard format for import into our database for analysis.
2. Availability of working space upon arrival including ports and IP addresses for our equipment. Hubs will be placed between the firewall network interfaces and the attached networks to facilitate the placement of our equipment and the capture of traffic. We have found this method to be faster and more reliable than configuring and reconfiguring switch ports as we move our equipment between sessions on each segment.

Extra time required to meet these conditions outside of the schedule will be billed accordingly. The estimated costs were included in our bill for creating the design but it would not be uncommon for these services to cost in the area of $150 to $200 per hour.

Any use of scanning and vulnerability assessment tools carries the risk of creating a Denial of Service condition by blocking access to, stopping services on, or crashing/locking equipment. We have mitigated these risks by arranging for downtime, performing the work during off hours and making sure that adequate staff is on hand to perform any work that needs to be done.

These plans and the potential risks of using scanning tools have been explained to company management and the times and procedures have been signed off on in a statement of work.

Conduct the Audit.

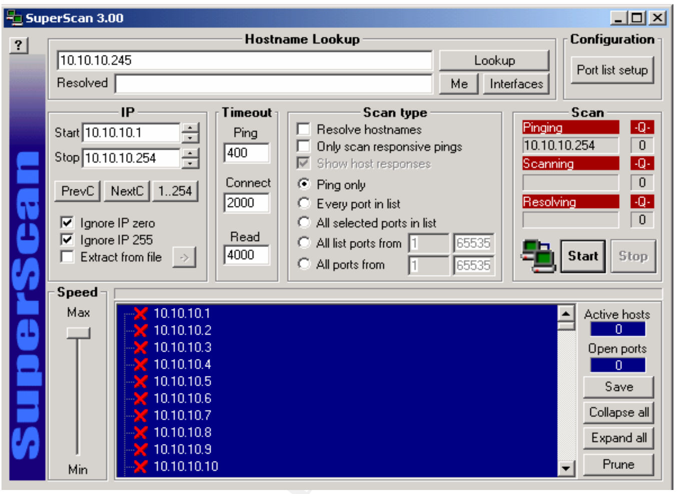
In conducting this audit the following steps have been followed.

1. Examine and verify the firewall configuration and rule sets.
    a. The firewall configuration was examined and found to be consistent with policy.
    b. The firewall configuration is the same as that identified in the section titled: Primary Firewall and VPN Configuration
2. The logs from each device have been imported into separate databases and queries run to determine if any traffic is reported as present on that subnet inconsistent with the network security policy. Example queries are:
    a. Traffic with an origin other than local.
    b. Traffic for unused services.
    c. Outbound traffic denied at the border router.
3. The logs from the Firewall were also examined for control connections and changes.

4. The two scanning computers have been configured with the following scanning/assessment tools.
    a. System one is a FreeBSD box with NMAP 3.20 from www.nmap.org.
    b. System two is a Windows 2000 box with:
        I. SuperScan 3 from www.foundstone.com/knowledge/free_tools.html
        II. Retina Network Scanner 4.9.66 from http://www.eeye.com/html/Products/Retina/index.html.
5. The capturing computers have been configured with Iris Network Traffic Analyzer from http://www.eeye.com/html/Products/Iris/index.html.

In preparation for the tests we have examined the system logs that were provided to us and found no indication of unacceptable traffic.

We will begin our on-site test using scanning system two running SuperScan, scanning with the "ping only" setting against each of the IP ranges present in our network segments.


SuperScan 3.00

Hostname Lookup: 10.10.10.245
Resolved:

IP
Start 10.10.10.1
Stop 10.10.10.254
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
● Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Scan
Pinging -0-
10.10.10.254 0
Scanning -0-
0
Resolving -0-
0

10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
10.10.10.5
10.10.10.6
10.10.10.7
10.10.10.8
10.10.10.9
10.10.10.10

Active hosts 0
Open ports 0

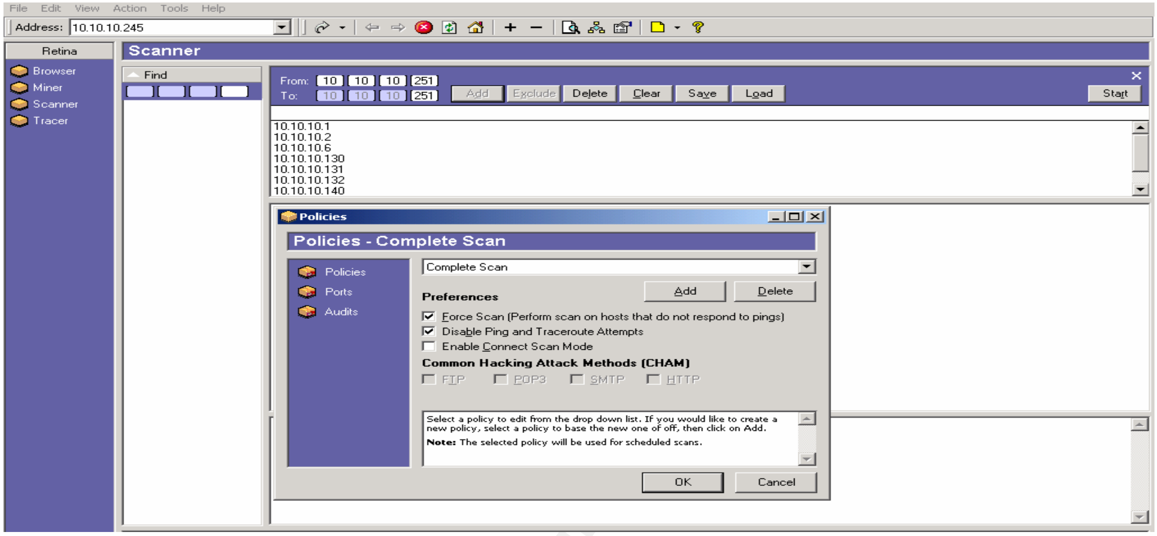
We then begin NMAP scans from scanning system one. We will run NMAP with the following command line for each of our networks:

```
nmap –P0 –oX loggiac10 –n –r –T Insane  10.10.10.1-255
nmap –P0 –oX loggiac192 –n –r –T Insane  192.168.2-3.1-255
nmap –P0 –oX loggiac172 –n –r –T Insane  172.17.2-3.1-255
```

While the NMAP scans are running on the external segment we will rotate our SuperScan box around the other segments for more ping sweeps.
a. DMZ-1 network – sweep 10.10.10.0/24 and 172.17.2.0/23
b. VPN network – sweep 10.10.10.0/24 and 192.168.2.0/23
c. Proxy network – sweep of all segments.

As we complete each segment we will utilize NMAP with the above command lines to complete the same sweeps.

Any addresses that show up on the sweeps are examined using the Retina software set on complete scan to help further identify what traffic is being allowed to pass.



Address: 10.10.10.245

From: 10 10 10 251
To: 10 10 10 251

```
10.10.10.1
10.10.10.2
10.10.10.6
10.10.10.130
10.10.10.131
10.10.10.132
10.10.10.140
```

Policies - Complete Scan

Complete Scan

Preferences

☑ Force Scan (Perform scan on hosts that do not respond to pings)
☑ Disable Ping and Traceroute Attempts
☐ Enable Connect Scan Mode

Common Hacking Attack Methods (CHAM)

☐ FTP ☐ POP3 ☐ SMTP ☐ HTTP

Select a policy to edit from the drop down list. If you would like to create a new policy, select a policy to base the new one of off, then click on Add.
Note: The selected policy will be used for scheduled scans.

Evaluate the Audit.

Our audit shows the Primary Giaccookies firewall to be functioning as required. This statement is based on the following results of our testing:

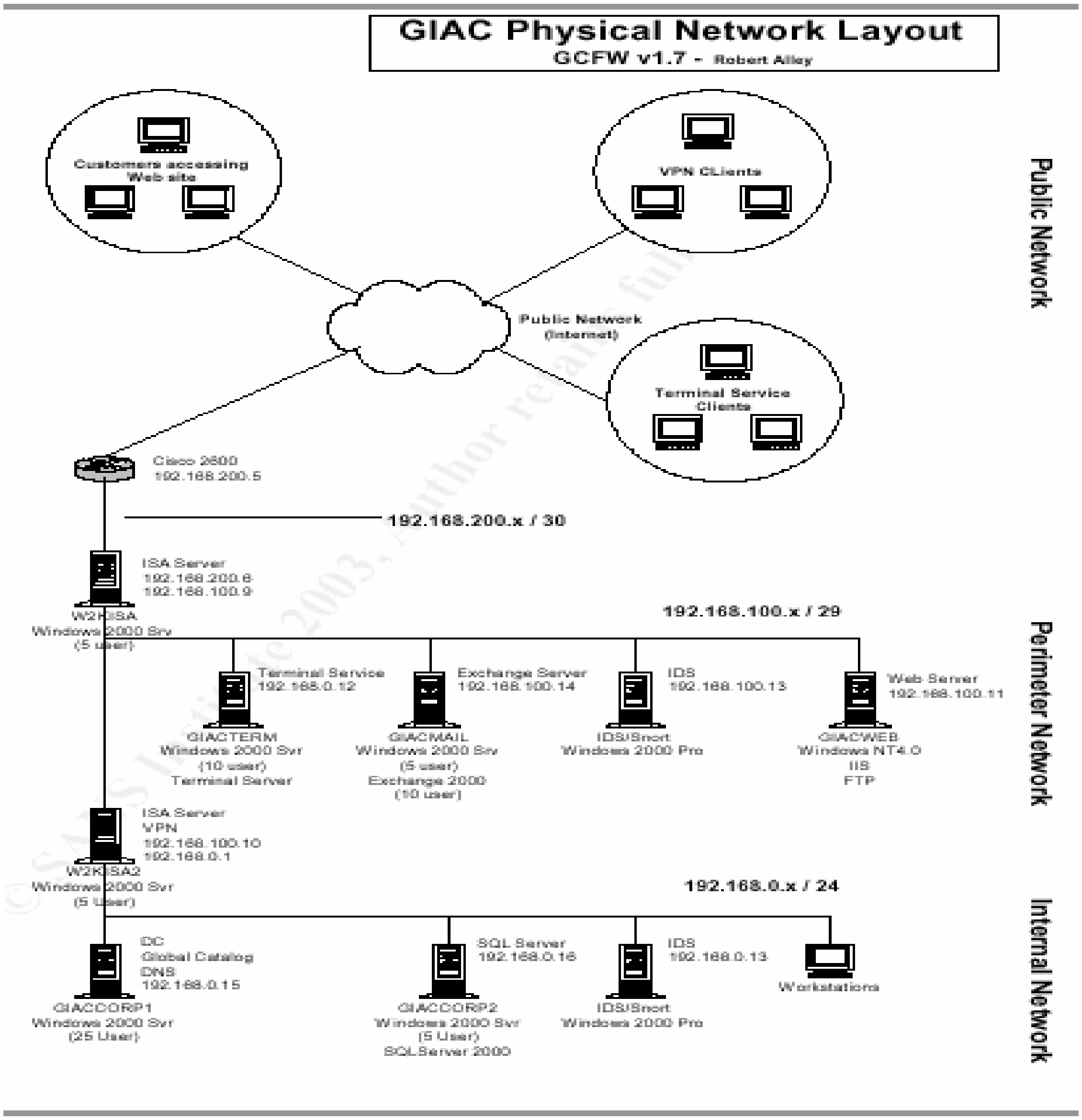
1. A review of the firewall settings and rule sets shows the firewall to be configured as recommended with no recent configuration changes.
2. Reviews of the log files provided to us prior to our on-site visit do not show any traffic that is inconsistent with firewall policy.
3. Reviews of the logs created during the on-site visit do not show any traffic that is inconsistent with policy.
4. All scans and operations checks show that the firewall is allowing the approved required communications.
5. All ping sweeps returned a negative result.
6. All NMAP scans returned either a negative result or results consistent with expected communications paths/ports.
7. Retina based scans did show some issues with two of the internal hosts but the firewall handled all traffic consistent with policy.

Based on these results we do not recommend any changes to the current architecture.

Part 4

Design Under Fire

For this section I have selected the paper posted in December 2002 by analyst number 360 Robert Alley. The paper may be reviewed at http://www.giac.org/practical/GCFW/Robert_Alley_GCFW.pdf



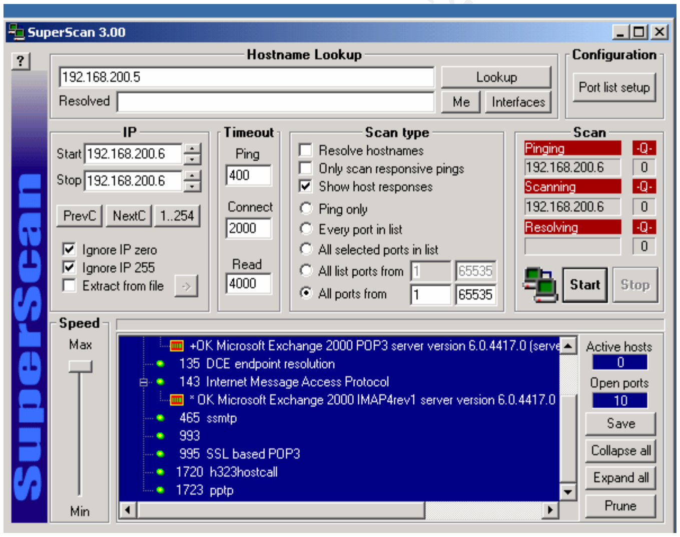
Preparation

In preparation we have queried the DNS servers and found that the GIAC Enterprises Email and Web servers are located at 192.168.200.6. Further inquiry shows that numbers in this range are owned by an ISP that provides small business hookups. A query run on the whois engine on the ISP's home page shows only the one address assigned to GIAC Enterprises.

Trace routes and a quick scan of the numbers surrounding this address have shown that the mask in use by GIAC Enterprises is likely to be 255.255.255.252. The reasoning behind this supposition is:

1. Trace routes show that the GIAC machine is using a router at 192.168.200.5
2. Scans show that there are machines belonging to other companies at addresses to either side of the subnet that GIAC is using.
3. Trace routes to the machines in use by the other companies show them to be using routers at different addresses.
4. All of the companies leave their respective networks and hop to the same ISP router.

A scan of the addresses in use by GIAC 192.168.200. 5-6 indicates again that 5 is a router and 6 is the edge of the GIAC network. A port scan of 192.168.200.6 yielded the following results.



SuperScan 3.00

Hostname Lookup: 192.168.200.5
Resolved:

IP
Start 192.168.200.6
Stop 192.168.200.6
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
● All ports from 1 65535

Scan
Pinging -Q-
192.168.200.6 0
Scanning -Q-
192.168.200.6 0
Resolving -Q-
0

```
    +OK Microsoft Exchange 2000 POP3 server version 6.0.4417.0 (serve
  135  DCE endpoint resolution
  143  Internet Message Access Protocol
    * OK Microsoft Exchange 2000 IMAP4rev1 server version 6.0.4417.0
  465  ssmtp
  993
  995  SSL based POP3
  1720  h323hostcall
  1723  pptp
```

Active hosts 0
Open ports 10

Open Ports:

1.	21	FTP
2.	25	SMTP
3.	80	HTTP
4.	110	POP3
5.	135	RPC Locator
6.	143	IMAP
7.	465	SMTPS
8.	993	IMAPS
9.	995	POP3S
10.	1720	h323 hostcall
11.	1723	PPTP

note: there is a very minor discrepancy here. The ISA setup specifies that RPC be opened but includes a cautionary note. The audit scan conducted by the analyst in his paper does not show this port as open but does show port 389 as open. For the purposes of this paper we will assume that both port 389 and port 135 have been closed at the firewall as a result of the earlier audit.

Having found the ports in use a scan utilizing LANguard network security scanner was conducted. The banners (along with other information) presented by the open ports indicates that Windows 2000 and Exchange 2000 are being used for SMTP and POP3 services. The version numbers returned from Exchange banners indicate Exchange service pack 2 is in use. This setup also tells us that at least SP2 is in use on the Windows 2000 boxes. We can also tell that IIS 4 server (Windows NT4) is in use for HTTP and FTP services. A connection can be made to the PPTP server using a standard Windows client. The presence of such disparate services at the same address tells us that there is some sort of pass-through or proxy situation going on with the machine at this location. Given the equipment in use along with the returns received in scanning and tracing the likely scenario is that the machine at this location is a Windows 2000 box running Remote Access and ISA.

An Attack against the Firewall Itself

Research was conducted by querying several search engines for information related to Windows 2000, Remote Access and ISA vulnerabilities.
For a listing of research URL's please see the references section

A quick search of vulnerabilities returned a likely candidate for our test, Microsoft Security Bulletin MS02-063.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-063.asp

This bulletin outlines an issue with an unchecked buffer in Microsoft's PPTP implementation possibly resulting in a denial of service attack. Further investigation yielded a very good explanation of the issue on the NewOrder site at:

http://neworder.box.sk/explread.php?newsid=7575

And at SecuriTeam.com at:

http://www.securiteam.com/windowsntfocus/5GP11008AE.html

The SecuriTeam article includes exploit code for use with the Spike tool (an excellent tool) available from: http://www.immunitysec.com/spike.html. Since I already have a box set up with spike I executed the SecuriTeam supplied code against the ISA server address (192.168.200.6).

The result was a lock-up of the machine creating a denial of service. The result would have been noticed very quickly since internet connectivity was suspended. As there was no logging at the edge router however, the cause of the condition would not be readily apparent and the attack could probably be duplicated a number of times. Timing would be important if the intent were an extended outage. For example the problem would likely not be noticed as quickly on the weekend or beginning early in the evening. For a workday outage the attacks would start early in the morning and come at irregular intervals throughout the day.

Countermeasures for this exploit: Patch updates are available from Microsoft but I would recommend discontinuing the use of PPTP and blocking the port in addition to the patch. For tracking purposes logging at the router sent to a central server for review would be valuable.

Denial of service attack utilizing 50 compromised systems

For this attack we have compromised 50 dsl/cable modem systems installing the WebLoad tool from Radview systems at: http://www.radview.com/products/WebLOAD.asp we have configured a script which calls for the product to initiate calls to the GIAC enterprises web site simulating 1000 users (per compromised system) accessing the site. This results in a seeming load of approximately 50,000 users attempting to view the web pages. Traffic demand will continue even if the web server itself fails, affecting the ISA server and the router. Since the traffic mimics that of a normal user it will not be instantly noticeable to administrators that this is an attack, although it wouldn't take long to come to that conclusion with that much new traffic. Since we know the account to be a business DSL connection we can reasonably expect this much traffic to fill the pipeline even if the edge router is configured to drop the packets after they are identified. This means that the business will likely be offline until the attacks stop or the ISP is contacted to block the traffic.

Countermeasures for this exploit: Since this is basically a saturation attempt of a small router and DSL pipeline there is little that can be done to prevent it other than some type of early notification with contingency plans in place with the ISP.

Exploit an Internal System

In our earlier examination of the open ports on the primary firewall we found that ports were open for SMTP, IMAP and POP3 traffic. Banner information from these services allows us to identify the system in use as a Microsoft Exchange 2000 SP2 system. Exchange servers that are used for multiple traffic like this are often not configured to block all mail relay. Since our address has been blocked from sending email to a number of addresses we are very interested in this setup. To test the relaying capability of this system we configure our email software to use this system for our outgoing mail and attempt to send a message to some generic accounts that we have set up on a public server. Our tests confirm that this system will accept mail for delivery to other systems using both POP3 and SMTP. This means that we now have another address to send mail from that is not blocked and that GIAC will be blamed for sending our email if someone complains.

Countermeasures for this exploit are careful configuration of the email system to prevent mail relay.

Part 5

Business Equipment Overview

1. Border Routers = Cisco 3660
    a. Version 12.2 (13)
2. Primary Firewall = Checkpoint NG FP3 HF2
    a. Windows 2000 SP3.
3. Proxy Server = Microsoft ISA server SP1
    a. Feature Pack 1
    b. Traffic monitoring/logging
    c. Content and A/V screening
4. Internal Firewall (user) = Checkpoint NG FP3 HF2
    a. Windows 2000 SP3
5. Load Balancer / Content Switch = Netscaler RS9800
    a. SSL accelerator
    b. Secure Application Switch code
6. Web Servers = Microsoft Internet Information Server 5
    a. Custom web based product application
    b. Custom C++ application
7. External DNS = Windows 2000
8. Secure File Delivery = Valicert Secure Transport
9. Web Based email = Outlook Web Access
    a. Exchange 2000 SP3
10. SMTP Relay = Symantec Enterprise (SMTP Gateway)
    a. Definitions updated daily
11. IDS = SNORT
    a. Definitions current to April 15, 2003.
    b. Definitions updated weekly.
    c. FreeBSD 4.7
12. Internal Firewall (data) = Checkpoint NG FP3 HF2
    a. Windows 2000 SP3.
13. Data Access Layer = Microsoft SQL 2000 SP3
    a. Custom C++ application
14. Layer 3 Switch (A & D) = Cisco 3550
    a. Version 12.1 (11)
15. Database Layer = Microsoft SQL 2000 SP3
    a. Custom C++ application
16. Layer 3 Switch (core) = Cisco 6509
    a. Switch = 7.4(3)
    b. MSFC = 12.1 (13)

17. Anti-Viral Solutions =
    a. Symantec Antivirus Enterprise Version 8
        i. Servers
        ii. Desktops
    b. Sybari Antigen for Exchange
18. Centralized Monitoring / logging = HP Open View
    a. Windows 2000 SP3

All servers other than the IDS boxes are Windows 2000 SP3 and are patched current to April 15, 2003. Patches are regularly reviewed and installed after testing if applicable.

The business has settled on the Dell server line as a standard.

A. Web class boxes are dual processor1650 machines.
B. IDS boxes are single processor 1650 machines.
C. Data Access Layer boxes are dual processor 2650 machines.
D. Checkpoint firewall boxes are dual processor 2650 machines.
E. SQL server boxes are 4-6 processor 8450 machines.
F. Hardware RAID, hot swappable drives.
G. Infrastructure boxes are a mix depending on purpose but are primarily in the 1650 and 2650 classes.

IP Address Scheme Information:

External (Internet) address range:

1. External Range 10.10.10.0/24
    a. Mask = 255.255.255.0
    b. Broadcast = 10.10.10.255
    c. Host Range = 10.10.10.1 to 10.10.10.254

This range is further subdivided by sections:

1. External Web-Based Services Range 10.10.10.128/25
    a. Mask = 255.255.255.128
    b. Broadcast = 10.10.10.255
    c. Host Range = 10.10.10.129 to 10.10.10.254

2. External Proxy Range 10.10.10.0/29
    a. Mask = 255.255.255.248
    b. Broadcast = 10.10.10.7
    c. Host Range = 10.10.10.1 to 10.10.10.6

Note: The ranges above will be substituted for actual publicly routable addresses in this paper.

Internal (non-public) address ranges:

All segments are currently less than 25-50% utilized. All segments are designed to allow for future expansion with the addition of adjacent classes and routing or a change to the appropriate subnet mask.

1. DMZ Segment 1 192.168.2.0/23
    a. Mask = 255.255.254.0
    b. Broadcast = 192.168.3.255
    c. Host Range = 192.168.2.1 to 192.168.3.254

2. DMZ Segment 2 192.168.8.0/22
    a. Mask = 255.255.252.0
    b. Broadcast = 192.168.11.255
    c. Host Range = 192.168.8.1 to 192.168.11.254

This segment is designed to allow for a NAT address range hiding internal addresses. The first half (two class C ranges) of the available pool will be primarily used for providing addresses to the network interfaces of the machines located in the screened network with active addresses on DMZ segment 2. The second half (two class C ranges) of the available pool will be primarily used to provide DMZ 2 statically translated addresses to the computers located on the Data Access Layer Segment.

3. Data Access Layer Segment 172.16.2.0/23
   a. Mask = 255.255.254.0
   b. Broadcast = 172.16.3.255
   c. Host Range = 172.16.2.1 to 172.16.3.254

4. Applications and Data Storage Segment = 172.17.2.0/23
   a. Mask = 255.255.254.0
   b. Broadcast = 172.17.3.255
   c. Host Range = 172.17.2.1 to 172.17.3.254

5. Internal / backend communications = 172.20.2.0/24
   a. Mask = 255.255.255.0
   b. Broadcast = 172.20.2.255
   c. Host Range = 172.20.2.1 to 172.19.2.254

This range is currently further subdivided by these sections:

   A. Internal Communication 172.20.2.8/29
      a. Mask = 255.255.255.248
      b. Broadcast = 172.20.2.15
      c. Host Range = 172.20.2.9 to 172.20.2.14

   B. Internal Proxy Range 172.20.2.0/29
      a. Mask = 255.255.255.248
      b. Broadcast = 172.20.2.7
      c. Host Range = 172.20.2.1 to 172.20.2.6

6. Internal VPN Range 172.24.2.0/23
   a. Mask = 255.255.254.0
   b. Broadcast = 172.24.3.255
   c. Host Range = 172.24.2.1 to 172.24.3.254

7. Internal Infrastructure 172.25.2.0/23
   a. Mask = 255.255.254.0
   b. Broadcast = 172.24.3.255
   c. Host Range = 172.24.2.1 to 172.24.3.254

8. Internal Users 172.26.16.0/20
   a. Mask = 255.255.240.0

    b. Broadcast = 172.26.31.255
    c. Host Range = 172.26.16.1 to 172.26.31.254

The internal users segment is designed to allow for multiple subnets and vlans based on purpose and/or job category. Each designated subnet would be placed in a VLAN assignment and pointed to the Layer 3 switch as its gateway. Additional internal security could be achieved with the appropriate switch configuration and assignment of access control lists. Examples of this would be segmentation into Finance, Human Resources, Network and System administration areas. However this is beyond the scope of this paper.

9. VPN-Office Mode Range 172.31.0.0/24
    a. Mask = 255.255.255.0
    b. Broadcast = 172.31.0.255
    c. Host Range = 172.31.0.1 to 172.31.0.254

IP Address Assignments of interest by section.

External:

Proxy External Interface	10.10.10.1/29
Administrative_Connection (Translated-Hide)	10.10.10.2/29
Primary Firewall Proxy Interface	10.10.10.6/29
https://customer.gaiccookies.com/	10.10.10.130/25
https://customer-file.gaiccookies.com/	10.10.10.131/25
ftp://customer-file.gaiccookies.com/	10.10.10.132/25
https://supplier.gaiccookies.com/	10.10.10.140/25
https://supplier-file.gaiccookies.com/	10.10.10.141/25
ftp://supplier-file.gaiccookies.com/	10.10.10.142/25
https://partner.gaiccookies.com/	10.10.10.150/25
https://partner-file.gaiccookies.com/	10.10.10.151/25
ftp://partner-file.gaiccookies.com/	10.10.10.152/25
https://employee.gaiccookies.com/	10.10.10.160/25
https://employee-file.gaiccookies.com/	10.10.10.161/25
ftp://employee-file.gaiccookies.com/	10.10.10.162/25
https://employee-mail.gaiccookies.com/	10.10.10.163/25
smtp.gaiccookies.com	10.10.10.164/25
dns.gaiccookies.com	10.10.10.170/25
syslog.gaiccookies.com	10.10.10.175/25
http://www.gaiccookies.com	10.10.10.180/25
https://www.gaiccookies.com	10.10.10.181/25
vpn connection address	10.10.10.250/25
Primary Firewall External Interface	10.10.10.251/25
Border Router 2	10.10.10.252/24
Border Router 1	10.10.10.253/24

Border Router (HSRP)	10.10.10.254/24

DMZ Segment 1:

Primary Firewall Interface	192.168.3.254/23
Application Switch	192.168.2.1/23
https://customer.gaiccookies.com/	192.168.2.130/23
https://customer-file.gaiccookies.com/	192.168.2.131/23
ftp://customer-file.gaiccookies.com/	192.168.2.132/23
https://supplier.gaiccookies.com/	192.168.2.140/23
https://supplier-file.gaiccookies.com/	192.168.2.141/23
ftp://supplier-file.gaiccookies.com/	192.168.2.142/23
https://partner.gaiccookies.com/	192.168.2.150/23
https://partner-file.gaiccookies.com/	192.168.2.151/23
ftp://partner-file.gaiccookies.com/	192.168.2.152/23
https://employee.gaiccookies.com/	192.168.2.160/23
https://employee-file.gaiccookies.com/	192.168.2.161/23
ftp://employee-file.gaiccookies.com/	192.168.2.162/23
https://employee-mail.gaiccookies.com/	192.168.2.163/23
smtp.gaiccookies.com	192.168.2.164/23
dns.gaiccookies.com	192.168.2.170/23
syslog.gaiccookies.com	192.168.2.175/23
http://www.gaiccookies.com	192.168.2.180/23
https://www.gaiccookies.com	192.168.2.181/23

DMZ Segment 2:

Internal Firewall (Data) Interface	192.168.11.254/22

Data Access Layer Segment:

Internal Firewall (Data) Interface	172.16.3.254/23

Applications and Data Storage Segment:

Internal Firewall (Data) Interface	172.17.3.254/23
Internal Firewall (User) Interface	172.17.2.1/23

Internal Communication:

Internal Firewall (Data) Interface	172.20.2.14/29
Internal Firewall (User) Interface	172.20.2.7/29

Internal Proxy Range:

Internal Firewall (User) Interface	172.20.2.6/29
Proxy Internal Interface	172.20.2.1/29

Internal VPN Range:

Primary Firewall Interface	172.24.3.254/23
Internal Firewall (User) Interface	172.24.2.1/23
VPN-DNS&WINS (Translated-Static)	172.24.2.5/23
Administrative_FW(Translated-Hide)	172.24.2.10/23

Internal Infrastructure:

Internal Firewall (User) Interface	172.25.3.254/23
https://intranet/cookies	172.25.2.25/23
VPN-DNS&WINS	172.25.2.20/23

Border Router Configuration

```
Border_Router_1#show conf
Using 22315 out of 129016 bytes
!
! Last configuration change at 10:22:10 Central Tue Mar 25 2003
! NVRAM config last updated at 10:23:50 Central Tue Mar 25 2003
!
version 12.2
no service pad
(Disables packet assembler/disassembler commands/connections)
service tcp-keepalives-in
(generates keepalive packets on idle incoming connections)
service timestamps debug datetime msec localtime show-timezone
(generates timestamps with date/time including the second in local time with
timezone information for debug messages)
service timestamps log datetime show-timezone msec
(generates timestamps with date/time including the second for log messages)
service password-encryption
(provides for password encryption)
no service dhcp
(disables dhcp server and relay)
!
hostname "Border_Router_1"
(Specifies the name of the router)
!
logging buffered 16000 debugging
(limits logging to the internal buffer to debug level messages with a buffer size of
16000)
!
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
(defines authentication for connections to the router)
!
username giacuser password A123456789
(defines a local user name and password)
!
clock timezone GMT 0
(sets the timezone and UTC offset to GMT)
no clock summer-time
(sets the clock to ignore daylight savings time change)
ip subnet-zero
(allows the use of subnet 0 for interfaces and routing updates)
no ip source-route
```

(disables the use of packets with source routing options set)

```
ip cef
```

(enables Cisco express forwarding)

```
!
no ip domain-lookup
```

(disables DNS)

```
!
no ip bootp server
```

(disables access to a bootp server)

```
ip inspect audit-trail
```

(enables context-based access control audit messages)

```
ip inspect name inspect_prot ftp
ip inspect name inspect_prot http
ip inspect name inspect_prot smtp
ip inspect name inspect_prot udp
ip inspect name inspect_prot tcp
ip inspect name inspect_prot fragment maximum 256 timeout 1
```

(these commands set up an inspection list named inspect_prot for the named protocols)

```
ip audit notify log
```

(specifies that notifications will go to the log)

```
ip audit po max-events 100
```

(limits the number of events in the cue to 100)

```
!
call rsvp-sync
```

(default setting enabling synchronization between RSVP and H.323)

```
!
controller T1 0/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
 no yellow generation
 no yellow detection
!
controller T1 0/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
 no yellow generation
 no yellow detection
```

(T1 controller configurations with no yellow alarm detection or generation)

```
!
interface Loopback0
 ip address 10.10.100.20 255.255.255.248
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 no ip mroute-cache
```

(Interface Loopback0 configuration)

(disables ICMP redirects and unreachable messages, proxy-arp and multi-cast switching)

(enables ip accounting)

```
!
interface FastEthernet0/0
 ip address 10.10.10.253 255.255.255.0
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 no ip mroute-cache
 duplex full
 speed 100
 standby 1 ip 10.10.10.254
 standby 1 preempt
 standby 1 track Serial0/0
 standby 1 track Serial0/1
```

(Interface FE0/0 configuration)

(disables ICMP redirects and unreachable messages, proxy-arp and multi-cast switching)

(enables ip accounting)

(sets interface to full duplex 100)

(activates HSRP with a group number of 1 leaving the priority value at the default of 100 and setting the preempt flag.)

(sets interfaces to track for HSRP availability dependency)

```
!
interface Serial0/0
bandwidth 1536
ip address 10.10.101.20 255.255.255.252
ip access-group 2000 in
ip access-group 2200 out
no ip redirects
no ip unreachables
no ip proxy-arp
ip accounting access-violations
ip load-sharing per-packet
ip inspect inspect_prot in
encapsulation ppp
!
interface Serial0/1
bandwidth 1536
```

```
ip address 10.10.100.21 255.255.255.252
ip access-group 2000 in
ip access-group 2200 out
no ip redirects
no ip unreachables
no ip proxy-arp
ip accounting access-violations
ip load-sharing per-packet
ip inspect inspect_prot in
encapsulation ppp
```

(Interface Serial 0 & 1 configurations)

(Attaches access lists 2000 incoming and 2200 outgoing)

(disables ICMP redirects and unreachable messages, proxy-arp)

(enables ip accounting)

(enables per packet load sharing)

(attaches the inspect_prot inspection list incoming)

(sets the encapsulation to ppp)

```
!
router bgp 14000
 bgp log-neighbor-changes
 network 10.10.10.0 mask 255.255.255.0
 neighbor 10.10.10.252 remote-as 14000
 neighbor 10.10.10.252 next-hop-self
 neighbor 10.10.102.25 remote-as 4000
 neighbor 10.10.102.25 ebgp-multihop 3
 neighbor 10.10.102.25 update-source Loopback0
 neighbor 10.10.102.25 send-community
```

(sets bgp system ID, logs bgp neighbor changes,specifies the network to be advertised, adds entry to BGP table, allows connections to peers not directly connected, allows iBGP to use the loopback, send communities attribute)

```
!
ip classless
```

(allows routing to the best possible net for packets with no network default route)

```
ip route 10.10.10.0 255.255.255.248 10.10.10.251 permanent
```

(sets static route to proxy subnet via firewall)

```
no ip http server
```

(disables the web server)

```
ip bgp-community new-format
```

(sets the bgp display format to AA:NN)

```
ip pim bidir-enable
```

(sets Protocol Independent Multicast to bi-directional)

```
!
logging history size 16
logging trap debugging
logging facility local5
logging 10.10.10.175
```

(sets logging to a maximum of 16 messages stored in the table, trap level is debugging, local level 5, defines syslog servers/receivers)

```
access-list compiled
```

(turbo ACL enabled)

```
access-list 182 remarkaccess list for administrative access
access-list 182 permit tcp host 10.10.10.2 any
access-list 182 deny   ip any any log
access-list 2000 remark  Incoming Serial ACL
access-list 2000 deny   ip 10.10.10.0 0.0.0.255 any log-input
access-list 2000 deny   ip host 0.0.0.0 any log-input
access-list 2000 deny   ip 127.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 224.0.0.0 15.255.255.255 any log-input
access-list 2000 deny   ip 240.0.0.0 15.255.255.255 any log-input
access-list 2000 deny   ip 10.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 172.16.0.0 0.15.255.255 any log-input
access-list 2000 deny   ip 192.168.0.0 0.0.255.255 any log-input
access-list 2000 deny   ip 169.254.0.0 0.0.255.255 any log-input
access-list 2000 deny   ip 1.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 2.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 5.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 7.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 23.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 27.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 31.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 36.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 37.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 39.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 41.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 42.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 58.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 59.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 60.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 70.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 71.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 72.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 73.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 74.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 75.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 76.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 77.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 78.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 79.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 83.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 84.0.0.0 0.255.255.255 any log-input
```

```
access-list 2000 deny   ip 85.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 86.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 87.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 88.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 89.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 90.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 91.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 92.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 93.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 94.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 95.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 96.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 97.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 98.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 99.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 100.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 101.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 102.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 103.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 104.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 105.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 106.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 107.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 108.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 109.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 110.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 111.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 112.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 113.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 114.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 115.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 116.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 117.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 118.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 119.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 120.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 121.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 122.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 123.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 124.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 125.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 126.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 197.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 240.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 241.0.0.0 0.255.255.255 any log-input
```

```
access-list 2000 deny   ip 242.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 243.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 244.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 245.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 246.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 247.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 248.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 249.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 250.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 251.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 252.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 253.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 254.0.0.0 0.255.255.255 any log-input
access-list 2000 deny   ip 255.0.0.0 0.255.255.255 any log-input
```

(Deny incoming internet traffic from our own subnet, the reserved (private) subnets and the non-assigned subnets)

```
access-list 2000 permit tcp any any established
```

(permits established traffic)

```
access-list 2000 permit tcp host 10.10.102.25 host 10.10.103.10 eq bgp
```

(permits bgp traffic from our peer for routing)

```
access-list 2000 permit tcp any host 10.10.10.130 eq 443
access-list 2000 permit tcp any host 10.10.10.131 eq 443
access-list 2000 permit tcp any host 10.10.10.132 eq ftp
access-list 2000 permit tcp any host 10.10.10.140 eq 443
access-list 2000 permit tcp any host 10.10.10.141 eq 443
access-list 2000 permit tcp any host 10.10.10.142 eq ftp
access-list 2000 permit tcp any host 10.10.10.150 eq 443
access-list 2000 permit tcp any host 10.10.10.152 eq ftp
access-list 2000 permit tcp any host 10.10.10.160 eq 443
access-list 2000 permit tcp any host 10.10.10.161 eq 443
access-list 2000 permit tcp any host 10.10.10.162 eq ftp
access-list 2000 permit tcp any host 10.10.10.163 eq 443
access-list 2000 permit tcp any host 10.10.10.164 eq smtp
access-list 2000 permit tcp any host 10.10.10.175 eq domain
access-list 2000 permit udp any host 10.10.10.175 eq domain
access-list 2000 permit tcp any eq domain host 10.10.10.175
access-list 2000 permit udp any eq domain host 10.10.10.175
access-list 2000 permit tcp any host 10.10.10.180 eq www
access-list 2000 permit tcp any host 10.10.10.181 eq 443
access-list 2000 permit tcp any host 10.10.10.251 eq 264
access-list 2000 permit tcp any host 10.10.10.251 eq 500
access-list 2000 permit udp any host 10.10.10.251 eq 500
access-list 2000 permit udp any host 10.10.10.251 eq 1548
access-list 2000 permit udp any host 10.10.10.251 eq 1549
access-list 2000 permit udp any host 10.10.10.251 eq 2746
```

```
access-list 2000 permit tcp any host 10.10.10.251 eq 18231
access-list 2000 permit tcp any host 10.10.10.251 eq 18232
access-list 2000 permit udp any host 10.10.10.251 eq 18233
access-list 2000 permit udp any host 10.10.10.251 eq 18234
access-list 2000 permit gre any any
access-list 2000 permit udp host 10.10.105.20 any eq ntp
```

(This section permits specific inbound traffic to our defined internet facing hosts)

```
access-list 2000 deny   ip any any log-input
```

(This section denies any inbound traffic not previously permitted)

```
!
access-list 2200 remark Outbound serial ACL
access-list 2200 deny   tcp any any eq telnet
access-list 2200 deny   tcp any any eq 135
access-list 2200 deny   udp any any eq 135
access-list 2200 deny   tcp any any eq 137
access-list 2200 deny   udp any any eq netbios-ns
access-list 2200 deny   tcp any any eq 138
access-list 2200 deny   udp any any eq netbios-dgm
access-list 2200 deny   tcp any any eq 139
access-list 2200 deny   tcp any any eq irc
access-list 2200 deny   udp any any eq netbios-ss
access-list 2200 deny   tcp any any eq 514
access-list 2200 deny   tcp any any eq 1214
access-list 2200 deny   tcp any eq 1214 any
access-list 2200 deny   tcp any any eq 1333
access-list 2200 deny   tcp any any eq 1334
access-list 2200 deny   tcp any any eq 1503
access-list 2200 deny   tcp any any eq 1863
access-list 2200 deny   tcp any any eq 3389
access-list 2200 deny   tcp any any eq 3570
access-list 2200 deny   tcp any any eq 3574
access-list 2200 deny   udp any any eq 4000
access-list 2200 deny   udp any any eq 4001
access-list 2200 deny   tcp any any eq 4443
access-list 2200 deny   tcp any any eq 5010
access-list 2200 deny   tcp any any eq 5050
access-list 2200 deny   tcp any any eq 5190
access-list 2200 deny   tcp any any eq 6346
access-list 2200 deny   tcp any eq 6346 any
access-list 2200 deny   tcp any any eq 6701
access-list 2200 deny   tcp any any eq 6891
access-list 2200 deny   tcp any any eq 7320
access-list 2200 deny   udp any any eq 13324
access-list 2200 deny   udp any any eq 13325
```

(this list section specifically blocks information that we don’t want going out of our network. Netbios information, telnet, irc, Kazaa, AOL, MSN,ICQ,Yahoo,syslog, ms-sql)

```
access-list 2200 deny   ip host 0.0.0.0 any log-input
access-list 2200 deny   ip 127.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 224.0.0.0 15.255.255.255 any log-input
access-list 2200 deny   ip 240.0.0.0 15.255.255.255 any log-input
access-list 2200 deny   ip 10.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 172.16.0.0 0.15.255.255 any log-input
access-list 2200 deny   ip 192.168.0.0 0.0.255.255 any log-input
access-list 2200 deny   ip 169.254.0.0 0.0.255.255 any log-input
access-list 2200 deny   ip 1.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 2.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 5.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 7.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 23.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 27.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 31.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 36.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 37.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 39.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 41.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 42.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 58.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 59.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 60.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 70.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 71.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 72.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 73.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 74.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 75.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 76.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 77.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 78.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 79.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 83.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 84.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 85.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 86.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 87.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 88.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 89.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 90.0.0.0 0.255.255.255 any log-input
```

```
access-list 2200 deny   ip 91.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 92.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 93.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 94.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 95.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 96.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 97.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 98.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 99.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 100.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 101.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 102.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 103.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 104.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 105.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 106.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 107.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 108.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 109.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 110.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 111.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 112.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 113.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 114.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 115.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 116.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 117.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 118.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 119.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 120.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 121.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 122.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 123.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 124.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 125.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 126.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 197.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 240.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 241.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 242.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 243.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 244.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 245.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 246.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 247.0.0.0 0.255.255.255 any log-input
```

```
access-list 2200 deny   ip 248.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 249.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 250.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 251.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 252.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 253.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 254.0.0.0 0.255.255.255 any log-input
access-list 2200 deny   ip 255.0.0.0 0.255.255.255 any log-input
```

(Deny outgoing internet traffic from the reserved (private) subnets and the non-assigned subnets)

```
access-list 2200 permit ip any any
```

(permits all outgoing traffic not earlier denied)

```
no cdp run
```

(disables cisco discovery protocol)

```
!
line con 0
exec-timeout 5 0
login authentication default
password B234567891
line aux 0
exec-timeout 5 0
no exec
transport input none
login authentication default
password C345678912
line vty 0 4
 access-class 182 in
 exec-timeout 5 0
 logging synchronous
 login authentication default
 password D456789123
 transport input telnet ssh
```

(defines access types/restrictions for connections to the router)

```
!
ntp master 3
ntp server 10.10.105.20 prefer
ntp server 10.10.105.21
ntp server 10.10.105.22
```

(defines network time protocol servers)

```
end

Border_Router_1#
```

Primary Firewall & VPN Configuration

RULE	SOURCE	DESTINATION	If Via	SERVICES	ACTION	TRACK	TIME	INSTALL ON	COMMENTS
1	Remote_Access@Any	VPN	Remote Access	Any	accept	Log	Any	Any	Allows users in the RemoteAccess Group to reach the VPN network via remote access.
2	Administrative_FW	box1	Any	Any	accept	Log	Any	Any	Allows access from the translated administrator's address to the firewall.
3	Any	box1	Any	Any	drop	Log	Any	Any	Deny all other attempts to reach the firewall
4	BorderRouter_1 BorderRouter_2 BorderRouter_HSRP	syslog.giaccookies.com	Any	syslog	accept	Log	Any	Any	Accept syslog traffic from the border routers to the syslog server.
5	Any	https.customer https.customer-file https.employee https.employee-file https.employee-mail https.partner https.partner-file https.supplier https.supplier-file https.www.giaccookies	Any	https	accept	Log	Any	Any	Allows https traffic to the various company web servers.
6	Any	http.www.giaccookies	Any	http	accept	Log	Any	Any	Allows http traffic to the public company web site.
7	Any	ftp.customer-file	Any	ftp	accept	Log	Any	Any	Allows FTP traffic to the

		ftp.employee-file ftp.partner-file ftp.supplier-file							company FTP servers.
8	Any	dns.giaccookies.com	Any	dns	accept	Log	Any	Any	Allows DNS traffic to the company DNS server.
9	dns.giaccookies.com	Any	Any	dns	accept	Log	Any	Any	Allows DNS traffic from the company DNS server.
10	Any	smtp.giaccookies.com	Any	smtp	accept	Log	Any	Any	Allows SMTP traffic to the company mail gateway.
11	smtp.giaccookies.com	Any	Any	smtp	accept	Log	Any	Any	Allows SMTP traffic from the company mail gateway.
12	Administrative_Outgoing	Any	Any	Any	accept	Log	Any	Any	Allows Administrative traffic bypassing the Proxy server. *Note that rule 3 will block traffic to the firewall itself*
13	Proxy_Server	Any	Any	ftp http https dns	accept	Log	Any	Any	Allows outgoing Proxy traffic for FTP, HTTP, HTTPS, and DNS. *Note that rule 3 will block traffic to the firewall itself*
	box1	Any	Any	Any	accept	-----	any	gateways	Implicit rule: Enable Outgoing Connections
14	Any	Any	Any	Any	drop	Log	Any	Any	Deny all traffic not previously permitted.

Address Translation Rules

RULE	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1 (implicit)	dns.giaccookies.com	Any	Any	10.10.10.170 (static)	Original	Original	Gateways	implicit NAT set in object definition
2 (implicit)	Any	10.10.10.170	Any	Original	dns.giaccookies.com (static)	Original	Gateways	implicit NAT set in object definition
3 (implicit)	ftp.customer-file	Any	Any	10.10.10.132 (static)	Original	Original	Gateways	implicit NAT set in object definition
4 (implicit)	Any	10.10.10.132	Any	Original	ftp.customer-file (static)	Original	Gateways	implicit NAT set in object definition
5 (implicit)	ftp.employee-file	Any	Any	10.10.10.162 (static)	Original	Original	Gateways	implicit NAT set in object definition
6 (implicit)	Any	10.10.10.162	Any	Original	ftp.employee-file (static)	Original	Gateways	implicit NAT set in object definition
7 (implicit)	ftp.partner-file	Any	Any	10.10.10.152 (static)	Original	Original	Gateways	implicit NAT set in object definition
8 (implicit)	Any	10.10.10.152	Any	Original	ftp.partner-file (static)	Original	Gateways	implicit NAT set in object definition

9 (implicit)	ftp.supplier-file	Any	Any	10.10.10.142 (static)	Original	Original	Gateways	implicit NAT set in object definition
10 (implicit)	Any	10.10.10.142	Any	Original	ftp.supplier-file (static)	Original	Gateways	implicit NAT set in object definition
11 (implicit)	http.www.giaccookies	Any	Any	10.10.10.180 (static)	Original	Original	Gateways	implicit NAT set in object definition
12 (implicit)	Any	10.10.10.180	Any	Original	http.www.giaccookies (static)	Original	Gateways	implicit NAT set in object definition
13 (implicit)	https.customer	Any	Any	10.10.10.130 (static)	Original	Original	Gateways	implicit NAT set in object definition
14 (implicit)	Any	10.10.10.130	Any	Original	https.customer (static)	Original	Gateways	implicit NAT set in object definition
15 (implicit)	https.customer-file	Any	Any	10.10.10.131 (static)	Original	Original	Gateways	implicit NAT set in object definition
16 (implicit)	Any	10.10.10.131	Any	Original	https.customer-file (static)	Original	Gateways	implicit NAT set in object definition
17 (implicit)	https.employee	Any	Any	10.10.10.160 (static)	Original	Original	Gateways	implicit NAT set in object definition
18 (implicit)	Any	10.10.10.160	Any	Original	https.employee (static)	Original	Gateways	implicit NAT set in object

								definition
19 (implicit)	https.employee-file	Any	Any	10.10.10.161 (static)	Original	Original	Gateways	implicit NAT set in object definition
20 (implicit)	Any	10.10.10.161	Any	Original	https.employee-file (static)	Original	Gateways	implicit NAT set in object definition
21 (implicit)	https.employee-mail	Any	Any	10.10.10.163 (static)	Original	Original	Gateways	implicit NAT set in object definition
22 (implicit)	Any	10.10.10.163	Any	Original	https.employee-mail (static)	Original	Gateways	implicit NAT set in object definition
23 (implicit)	https.partner	Any	Any	10.10.10.150 (static)	Original	Original	Gateways	implicit NAT set in object definition
24 (implicit)	Any	10.10.10.150	Any	Original	https.partner (static)	Original	Gateways	implicit NAT set in object definition
25 (implicit)	https.partner-file	Any	Any	10.10.10.151 (static)	Original	Original	Gateways	implicit NAT set in object definition
26 (implicit)	Any	10.10.10.151	Any	Original	https.partner-file (static)	Original	Gateways	implicit NAT set in object definition
27 (implicit)	https.supplier	Any	Any	10.10.10.140 (static)	Original	Original	Gateways	implicit NAT set in object definition

28 (implicit)	Any	10.10.10.140	Any	Original	https.supplier (static)	Original	Gateways	implicit NAT set in object definition
29 (implicit)	https.supplier-file	Any	Any	10.10.10.141 (static)	Original	Original	Gateways	implicit NAT set in object definition
30 (implicit)	Any	10.10.10.141	Any	Original	https.supplier-file (static)	Original	Gateways	implicit NAT set in object definition
31 (implicit)	https.www.giaccookies	Any	Any	10.10.10.181 (static)	Original	Original	Gateways	implicit NAT set in object definition
32 (implicit)	Any	10.10.10.181	Any	Original	https.www.giaccookies (static)	Original	Gateways	implicit NAT set in object definition
33 (implicit)	smtp.giaccookies.com	Any	Any	10.10.10.164 (static)	Original	Original	Gateways	implicit NAT set in object definition
34 (implicit)	Any	10.10.10.164	Any	Original	smtp.giaccookies.com (static)	Original	Gateways	implicit NAT set in object definition
35 (implicit)	syslog.giaccookies.com	Any	Any	10.10.10.175 (static)	Original	Original	Gateways	implicit NAT set in object definition
36 (implicit)	Any	10.10.10.175	Any	Original	syslog.giaccookies.com (static)	Original	Gateways	implicit NAT set in object definition

FireWall-1 Object Definitions

Network Objects

Name	Type	Location	FW-1	IP Address	Netmask	NAT Address	Members	Comment
Administrative_FW	host	internal	---	172.24.2.10				Administrator's Firewall Management
Administrative_Outgoing	host	internal	---	10.10.10.2				Administrator Usage Only (Bypasses Proxy Server)
AuxiliaryNet	dynamic_net_obj	internal	---					
BorderRouter_1	host	internal	---	10.10.10.253				
BorderRouter_2	host	internal	---	10.10.10.252				
BorderRouter_HSRP	host	internal	---	10.10.10.254				
box1	gateway	internal	FW1 installed	10.10.10.251				Firewall
DAG_range	machines_range	internal	---		0.0.0.1 - 0.0.254.254			
DMZ_1	network	internal	---	192.168.2.0	255.255.254.0			DMZ side of

								Firewall
DMZNet	dynamic_net_obj	internal	---					
dns.giaccookies.com	host	internal	---	192.168.2.170		10.10.10.170 static		
ftp.customer-file	host	internal	---	192.168.2.132		10.10.10.132 static		
ftp.employee-file	host	internal	---	192.168.2.162		10.10.10.162 static		
ftp.partner-file	host	internal	---	192.168.2.152		10.10.10.152 static		
ftp.supplier-file	host	internal	---	192.168.2.142		10.10.10.142 static		
High	sofaware_profiles_security_level	internal	---	3.3.3.3				
http.www.giaccookies	host	internal	---	192.168.2.180		10.10.10.180 static		
https.customer	host	internal	---	192.168.2.130		10.10.10.130 static		
https.customer-file	host	internal	---	192.168.2.131		10.10.10.131 static		
https.employee	host	internal	---	192.168.2.160		10.10.10.160 static		
https.employee-file	host	internal	---	192.168.2.161		10.10.10.161 static		
https.employee-mail	host	internal	---	192.168.2.1		10.10.10.163 st		

				63		atic		
https.partner	host	internal	---	192.168.2.150		10.10.10.150 static		
https.partner-file	host	internal	---	192.168.2.151		10.10.10.151 static		
https.supplier	host	internal	---	192.168.2.140		10.10.10.140 static		
https.supplier-file	host	internal	---	192.168.2.141		10.10.10.141 static		
https.www.giaccookies	host	internal	---	192.168.2.181		10.10.10.181 static		
InternalNet	dynamic_net_obj	internal	---					
LocalMachine	dynamic_net_obj	internal	---					Check Point Local Machine
Low	sofaware_profiles_security_level	internal	---	3.3.3.1				
Medium	sofaware_profiles_security_level	internal	---	3.3.3.2				
Proxy	network	internal	---	10.10.10.0	255.255.255.248			Proxy Side of Firewall
Proxy_Server	host	internal	---	10.10.10.1				
smtp.giaccookies.com	host	internal	---	192.168.2.164		10.10.10.164 static		
syslog.giaccookies.c	host	internal	---	192.168.2.1		10.10.10.175 st		

om				75		atic		
VPN	network	internal	---	172.24.2.0	255.255.254.0			VPN side of Firewall
VPN_Office_Mode	network	internal	---	172.31.0.0	255.255.255.0			
VPN_SERVICES	host	internal	---	172.24.2.5				DNS & WINS services for VPN clients

Service Objects

Name	Type	Port/ Program	S_Port from	S_Port to:	Match	Prolog	Members	Comment
dns	group						domain-tcp domain-udp	Domain Name System (TCP/UDP)
domain-tcp	tcp	53						Domain Name System Download
domain-udp	udp	53						Domain Name System Queries
ftp	tcp	21						File Transfer Protocol
http	tcp	80						Hypertext Transfer Protocol
https	tcp	443						HTTP protocol over TLS/SSL
nntp	tcp	119						Network News Transfer Protocol
smtp	tcp	25						Simple Mail Transfer Protocol
syslog	udp	514						UNIX syslog Protocol, control system log

Desktop Security

Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENTS
1	VPN	Remote_Access@Any	Any	Encrypt	Log	Encrypt (Accept) inbound traffic to the Desktop from the VPN network.
2	Any	AllUsers@Any	Any	Block	Log	Block inbound traffic to the Desktop.

Outbound Rules

RULE	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENTS
3	Remote_Access@Any	VPN	Any	Encrypt	Log	Encrypt (Accept) outbound traffic from the Desktop to the VPN network.
4	AllUsers@Any	Any	Any	Accept	Log	Accept outbound traffic from the Desktop to anywhere else.

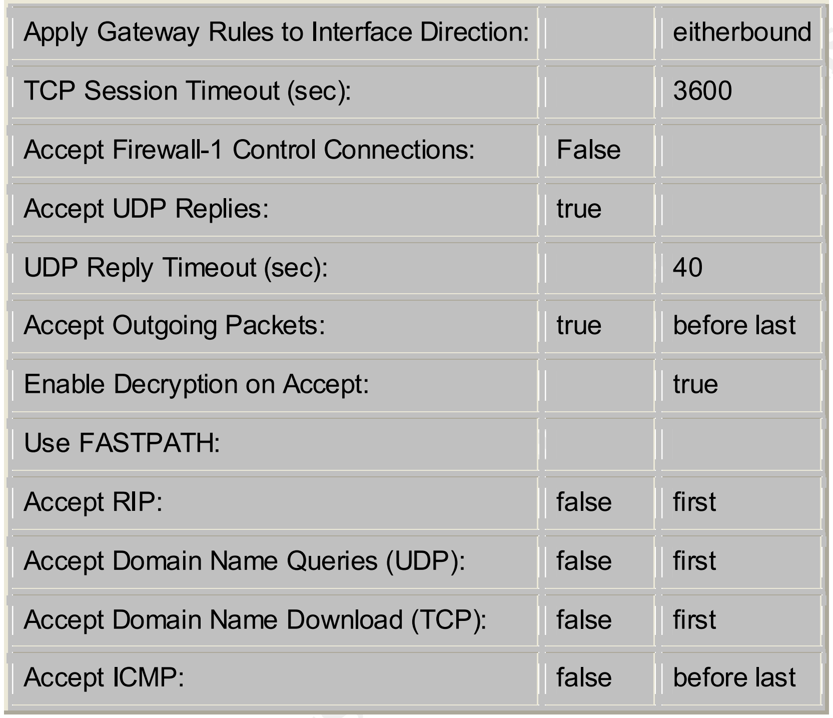
User Objects

Name	Type	From	To	Auth	Day	Expires	Members	Comment

Property Settings

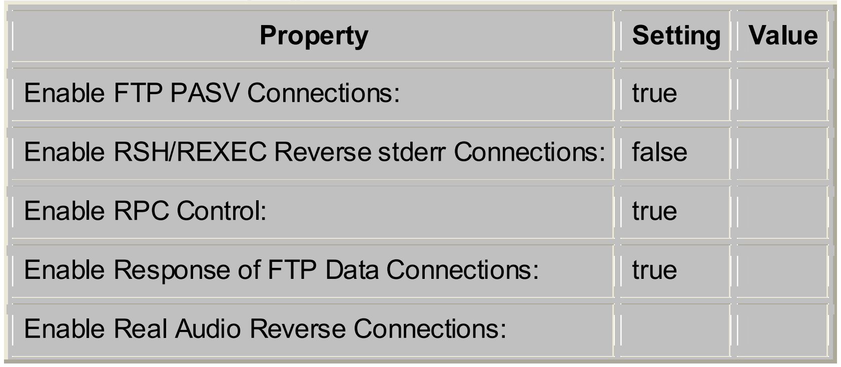
Security Policy

Property	Setting	Value



Apply Gateway Rules to Interface Direction:		eitherbound
TCP Session Timeout (sec):		3600
Accept Firewall-1 Control Connections:	False	
Accept UDP Replies:	true	
UDP Reply Timeout (sec):		40
Accept Outgoing Packets:	true	before last
Enable Decryption on Accept:		true
Use FASTPATH:		
Accept RIP:	false	first
Accept Domain Name Queries (UDP):	false	first
Accept Domain Name Download (TCP):	false	first
Accept ICMP:	false	before last

Services



Property	Setting	Value
Enable FTP PASV Connections:	true	
Enable RSH/REXEC Reverse stderr Connections:	false	
Enable RPC Control:	true	
Enable Response of FTP Data Connections:	true	
Enable Real Audio Reverse Connections:		

Enable VDOLive Reverse Connections:		
Enable CoolTalk Data Connections (UDP):		
Enable H.323 Control and Data Connections:		

Log and Alert

Property	Setting
Excessive Log Grace Period (sec):	62
PopUp Alert Command:	
Mail Alert Command:	internal_sendmail -s alert -t mailer root
SNMP Trap Alert Command:	internal_snmp_trap localhost
User Defined Alert Command:	
Anti Spoof Alert Command:	internal_sendmail -s alert -t mailer root
User Authentication Alert Command:	internal_sendmail -s alert -t mailer root
Log Established TCP Packets:	true
Enable Active Connections:	false

Resolving

Property	Setting
Lookup Priorities:	1. sys (current system settings) 2. none 3. none

	4. none
BIND Timeout (sec):	10
BIND Retries:	1
Log Viewer Resolver Properties:	20

Security Servers

Property	Setting
Telnet Welcome Message File:	
Rlogin Welcome Message File:	
FTP Welcome Message File:	
Client Authentication Welcome Message File:	
HTTP Next Proxy:	:

Authentication

Property	Setting
User Authentication Session Timeout (min):	15
AXENT Pathways Defender Server Setup:	IP: Agent ID: Agent Key:

SYNDefender

Property	Setting
Method:	0
Timeout:	10
Maximum Sessions:	5000
Display Warning Messages:	1

Miscellaneous

Property	Setting
Load Agents Port:	18212
Load Measurement Interval:	30

Access Lists

Property	Setting	Value
Accept Established TCP Connections:	true	first
Accept RIP:	false	first
Accept Domain Name Queries (UDP):	false	first
Accept Domain Name Download (TCP):	false	first
Accept ICMP:	false	before last

Generated with the help of FW1rules (7.3.29)

References

Cisco Command Summaries books

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_summaries_books_list.html

CS1: Cisco IOS Command Summary, Volume 1 of 3, Release 12.2

http://www.cisco.com/application/pdf/en/us/guest/products/ps4032/c1106/ccmigration_09186a0080133d12.pdf

CS2: Cisco IOS Command Summary, Volume 2 of 3, Release 12.2

http://www.cisco.com/application/pdf/en/us/guest/products/ps4032/c1106/ccmigration_09186a0080133d18.pdf

CS3: Cisco IOS Command Summary, Volume 3 of 3, Release 12.2

http://www.cisco.com/application/pdf/en/us/guest/products/ps4032/c1106/ccmigration_09186a0080133d17.pdf

INTERNET PROTOCOL V4 ADDRESS SPACE
http://www.iana.org/assignments/ipv4-address-space

IANA Port listings
http://www.iana.org/assignments/port-numbers

Information on blocking IM
Dalton, Curtis E. & Kannengeisser, William, "Instant Headache" August 2002 issue of InfoSecurity Magazine http://www.infosecuritymag.com/2002/aug/cover.shtml

Microsoft Internet Security and Acceleration Server information
http://www.microsoft.com/ISAServer/

Netscaler (Secure Application Switch)
http://www.netscaler.com/product/sa_switch_datasheet.html

General Checkpoint (Firewall-1 NG) Information
http://www.checkpoint.com
http://www.secwiz.com/ASPX/Default.aspx?tabindex=11&tabid=22
http://www.phoneboy.com/fom-serve/cache/519.html

Checkpoint Firewall configuration dump tool
FW1Rules http://www.wyae.de/software/fw1rules/

Tools

Foundstone Tools	www.foundstone.com/knowledge/free_tools.html
NMAP	www.nmap.org
Languard	www.gfisoftware.com/languard
Nessus	www.nessus.org
ISS	www.iss.net
Retina	www.eeye.com
Spike	http://www.immunitysec.com/spike.html
WebLoad	http://www.radview.com/products/WebLOAD.asp

Packet Sniffing and Analysis

Ethereal	http://www.ethereal.com/
Iris	http://www.eeye.com/html/Products/Iris/index.html
Observer Suite	http://www.networkinstruments.com/

Design under fire paper

Robert K. Alley #360 http://www.giac.org/practical/GCFW/Robert_Alley_GCFW.pdf

Vulnerability information Resources

Astalavista	http://astalavista.box.sk
CERT coordination center	http://www.cert.org/
Church of the Swimming Elephant	http://www.cotse.com/
Exploits Archive	http://exploits.no-ip.com/
Foundstone, Inc	http://www.foundstone.com
Google Search Engine	http://www.google.com/
ICAT Metabase	http://icat.nist.gov/icat.cfm
Immunity Security	http://immunitysec.com
Internet Security Systems Dbase	http://www.iss.net/security_center/search.php
Microsoft knowledge base	http://support.microsoft.com
Microsoft Security Center	http://www.microsoft.com/security
Neohapsis	http://www.neohapsis.com/
NewOrder	http://neworder.box.sk/
Packet Storm	http://packetstorm.widexs.nl/
Securiteam	http://www.securiteam.com/
Security Focus	http://www.securityfocus.com/