Global Information Assurance Certification Paper

Level Two Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Capitol SANS December 10-15, 2000
Version 1.5

Submitted by: Tony Letts

Date: April 5, 2000

TABLE OF CONTENTS

1. Assignment Requirements 3
2. Assignment 1 – Security Architecture 3
   2.1 Overview 3
   2.2 Hardware & Software Components 3
      2.2.1 Cisco 3600 Router 3
      2.2.2 Nortel Contivity 2600 3
      2.2.3 Nokia 440 w/ Checkpoint VPN-1/FW-1 3
      2.2.4 ISS RealSecure Network IDS 4
      2.2.5 BlackICE 4
      2.2.6 Logging Server 5
      2.2.7 Trend Micro Antivirus 5
      2.2.8 SSL Enabled Web Server 5
      2.2.9 DNS Servers 5
      2.2.10 Time Servers 5
   2.3 IP Addressing Scheme 5
      2.3.1 General 5
3. Assignment 2 – Security Policy 6
   3.1 Written Policy 6
   3.2 Border Router – Policy Implementation 6
      3.2.1 Business Impact 7
   3.3 Primary Firewall 7
   3.4 VPN 10
4. Assignment 3 – Audit Your Security Architecture 10
   4.1 Assessment Plan 10
      4.1.1 Considerations 10
      4.1.2 Target Areas 10
      4.1.3 Tools 11
   4.2 Implementation 11
   4.3 Analysis and Recommendations 12
5. Assignment 4 – Design Under Fire 14
   5.1 Firewall Attack 14
   5.2 Denial of Service Attack 15
   5.3 Internal Attack through the Firewall 15

1. Assignment Requirements

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

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

2. Assignment 1 – Security Architecture

2.1 Overview

The security architecture for GIAC has several layers of access control devices designed to provide defense in depth against both external and internal attacks. The graphical depiction of the architecture is displayed on the next page in *Figure 1*. We have implemented the following components in our infrastructure: filtering routers, IDS systems, firewalls, and VPN solutions. Additional measures such as SecurID authentication and logging servers are in place to validate the users and track their progress throughout the network.

To truly provide comprehensive risk management, we have treated our internal network as though a breach is inevitable. Instead of installing a single firewall to protect internal servers, GIAC has installed host level firewall and intrusion detection from Network ICE on all servers, including those servers in the Screened Services Network and Extranet. A Network ICE management console centrally administers all the host level components. We will discuss each hardware component and the roll it plays in our security architecture and discuss how the components interact together to provide the business functions outlined in our requirements.

2.2 Hardware & Software Components

2.2.1 Cisco 3600 Router

We will be using a Cisco 3620 router with IOS 12.1. This is the first level of defense and will reject a large number of basic attacks, also know as "Noise Filtering", through the use of ACLs. Through the use of some rather simple ACLs the router will be used for anti-spoofing, blocking private addresses, controlling ICMP traffic, and blocking source routing.

2.2.2 Nortel Contivity 2600

The Contivity box is a critical piece in our architecture. We will be running two Nortel Contivity 2600s with 3.5-source code on them. They will be load balanced and provide fail over capabilities as well. This component will provide remote access for staff and is the gateway for our partners and suppliers to access the extranet. The VPN appliances were placed outside the firewall so we can be sure that the individual has been authenticated with a secure connection before entering our network.

2.2.3 Nokia 440 w/ Checkpoint VPN-1/FW-1

We chose Nokia 440 boxes for several reasons. First, Nokia provides a "High-Availability" solution, which uses VRRP technology to stay in a hot-standby mode. Second, the Nokia boxes also have a hardened OS already on them and we will be running IPSO 3.3 code on these boxes. Lastly, we will be running Checkpoint 4.1 SP3 as the firewall software.

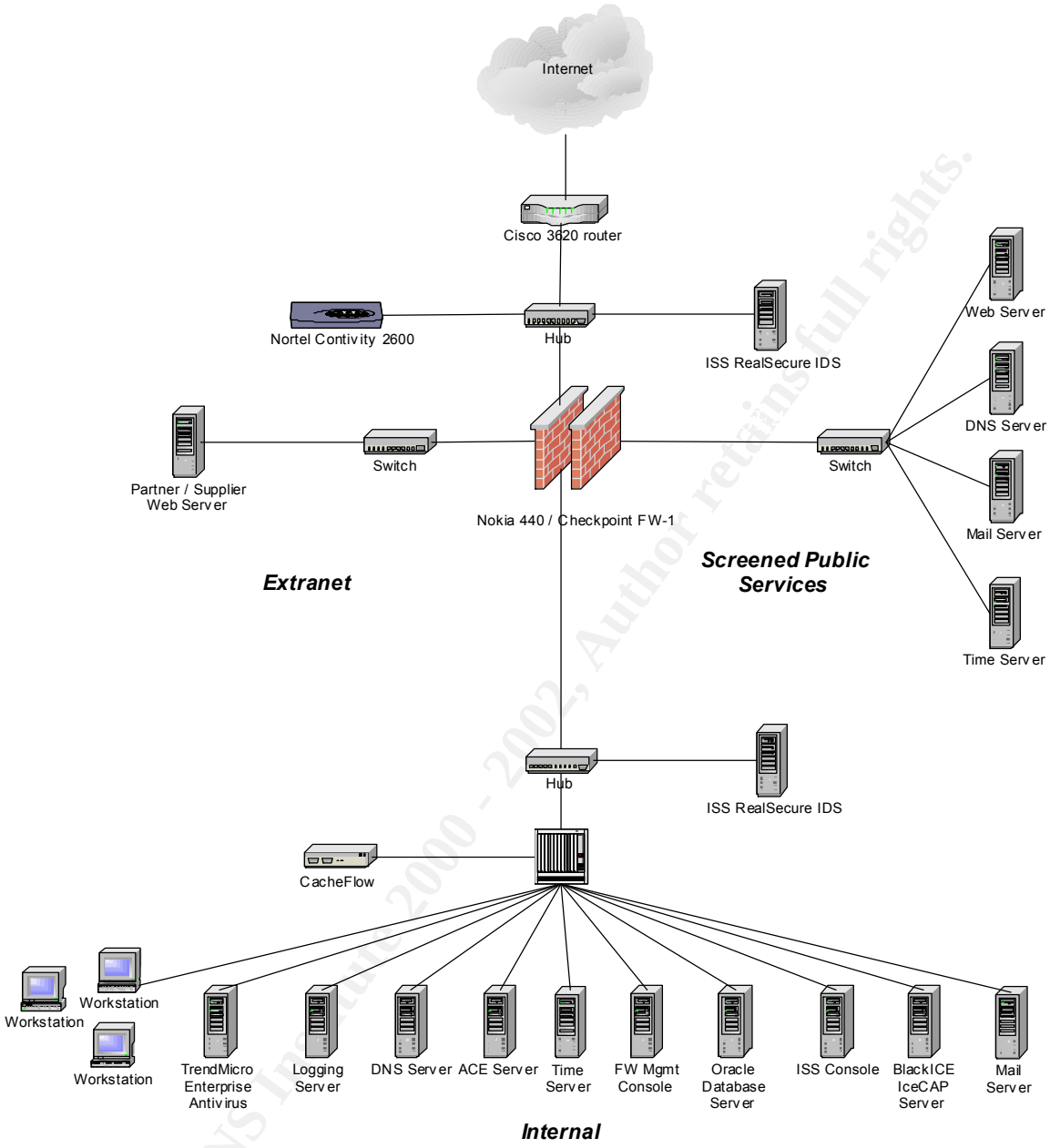


Figure 1 **- Security Architecture Diagram for GIAC**

2.2.4 ISS RealSecure Network IDS

ISS Real Secure 5.0 will be running in promiscuous mode on a Pentium III Windows NT 4.0 with SP6 and hot fixes. There will be two ISS Real Secure 5.0 servers running on the network. One will be between the router and firewall looking for attacks the router missed. The other will be inside the firewall on the internal network looking for attacks the firewall may have missed.

2.2.5 BlackICE

BlackICE (IDS/firewall) agents v2.5 will be deployed on all servers, including the servers in the screened services network, DNS, Mail, and Logging servers. The agents are managed and

automatically updated through the ICEcap management server. This management server also stores all incidents in a SQL 7.0 database for reporting.

2.2.6 Logging Server

A syslog server will be implemented to gather all the logs from all the different security components. Having a consolidated logging server will make it easier to monitor traffic and to trace the steps of a hacker in the scenario of a successful hack.

2.2.7 Trend Micro Antivirus

No good security architecture would be complete without an enterprise antivirus solution. Trend Micro provides an enterprise network solution as well as a plug in for our Checkpoint Firewall. Trend Micro 3.5 will be used to scan all http, ftp and smtp traffic passing through firewall.

2.2.8 SSL Enabled Web Server

Customers will connect to the website using standard HTTP protocol. When performing any e-commerce transactions they will establish a secure connection through HTTPS protocol. This server side certificate will use 128bit encryption. Due to international sales we will allow 40bit client connections but will notify the customer of this detail before they proceed with their transaction.

2.2.9 DNS Servers

GIAC has chosen a split DNS strategy. The two internal DNS servers handle all internal queries and forward external queries to the screened services network DNS server. The ISP is also hosting a second external DNS for redundancy and backup purposes.

2.2.10 Time Servers

Time servers are critical for a complete security architecture. One of the tasks of the Intrusion Response Team is gather the logs and trace where the intruder may have been able to go during their intrusion of the network. If all the logs were not time synchronized that task would be difficult if not impossible. GIAC has placed a time server on the Internal network as well as the Screened Services Network.

2.3 IP Addressing Scheme

2.3.1 General

The GIAC Enterprise network will be divided into 4 segments. The screened public services network will use public/routable addresses and the others will use RFC1918 private addressing schemes as follows.

GIAC Enterprises has been given the following range of public/routable IP addresses: 111.111.111.0- 111.111.111.255 with a subnet of 255.255.255.0.

The ISP has assigned the following address to the external interface of the Cisco router: 200.200.200.200

GIAC will use a private IP address scheme for the 3 secured networks:

Internal: 192.168.10.0 subnet 255.255.255.0
Screened Services: 192.168.20.0 subnet 255.255.255.0
Extranet: 192.168.30.0 subnet 255.255.255.0

3. Assignment 2 – Security Policy

3.1 Written Policy

The policy statements below are by no means comprehensive. These statements have been chosen because of their relevance to this project.

- Need-to-Know: Access to information in the possession of, or under the control of GIAC Enterprises must be provided based on the need-to-know. In other words, information must be disclosed only to people who have a legitimate business need for the information.
- Extended User Authentication: Inbound traffic (with the exception of Internet mail and push broadcasts) making access to GIAC Enterprises networks through a firewall must in all instances involve extended user authentication. This strong authentication will be in the form of RSA SecurID tokens assigned to any individual requiring access.
- Anonymous User Connections: Anonymous user connections will be allowed for HTTP, SMTP, and DNS queries to our screened public services network. HTTPS will be required for any e-commerce transactions performed on the public web server.
- VPN: Any authenticated session to GIAC Enterprises will require encryption using VPN technology. This will be provided on an individual basis using the Nortel VPN client software or corporately using an IPSEC VPN to VPN solution. Individual access will only be allowed on GIAC owned hardware with current antivirus software and BlackICE personal firewall software installed. Corporate entities will only be allowed to connect firewall to firewall after a comprehensive review of said company's security policies and implementation practices.
- Posting Updates: Because hackers and other intruders use the latest attack techniques, GIAC firewalls must be running the latest software to repel these attacks. Where available from the vendor, all GIAC firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the Information Security Department Manager, staff members responsible for managing firewalls must install and run these updates after the first week but before the end of the second week of receipt.
- Route Filtering: External gateway routers shall not allow illegal source-routing/IP spoofing. The router will also perform basic ingress and egress filtering
- External Server Connections: Servers on the Extranet and Screened Services Network will only be allowed to connect to the internal network using Oracle SQLNet. Connections initiated from the internal segment will require the use of an encrypted connection using the product SSH.

3.2 Border Router – Policy Implementation

We will use basic ACLs to filter out the "noise" that we know the firewall will drop anyway. We do not want to impede the performance of our router so we will limit the number of filters we will implement. Proper security measures were taken to harden the OS during the setup and logging was turned on and pointed to the syslog server on the screened services network. A warning banner was also implemented on the router.

Link for recommendations on hardening Cisco OS
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Ingress standard ACL which prevents inbound spoofed packets

```
interface serial 0
ip address 200.200.200.200 255.255.255.0
ip access-group 99 in
access-list 99 deny 192.168.0.0 0.0.255.255 any log
access-list 99 deny 172.16.0.0 0.15.255.255 any log
access-list 99 deny 10.0.0.0 0.255.255.255 any log
access-list-99 deny 111.111.111.0 0.0.0.255 any log
access-list 99 deny 224.0.0.0 31.255.255.255 any log
```

access-list 99 deny host 0.0.0.0 log
access-list 99 deny host 127.0.0.1 log
access-list 99 permit any

Egress standard ACL, which prevents GIAC from being used in a DDoS attack

interface ethernet 0
ip address 111.111.111.1 255.255.255.0
ip access-group 99 in
access-list 99 permit 111.111.111.0 0.0.0.255
access-list 99 deny any log

Note: The last line of the egress filter is not required because deny all is default but GIAC would like to log attempts to leave their network using a spoofed address.

3.2.1 Business Impact

There will be no impact on the legitimate business functions defined in the project by implementing these simple ACLs on the border router. Implementing these ACLs only makes us a good neighbor in the Internet community and could protect us from possible legal liability for lack of due diligence.

3.3 Primary Firewall

Listed below are the specific IP address assignments of the servers used in the Rulebase for the Checkpoint Firewall

Firewall: 111.111.111.10, 192.168.20.10, 192.168.10.10, 192.168.30.10
Extranet_Web: 192.168.30.1
SSN_Web: 192.168.20.5 NAT 111.111.111.5
SSN_DNS: 192.168.20.6 NAT 111.111.111.6
SSN_Mail: 192.168.20.7 NAT 111.111.111.7
CacheFlow: 192.168.10.20
Internal_DB: 192.168.10.22
Internal_Mail: 192.168.10.23
BlackICE_Mgmt: 192.168.10.24
Internal_DNS: 192.168.10.25
Internal_Time: 192.168.10.26
Internal_Log: 192.168.10.27

The implementation of the GIAC policy is depicted in *Figure 3*

To implement the Checkpoint Firewall policy you must create objects (*Figure 2)* representing your servers, networks, and services and then create a rulebase.

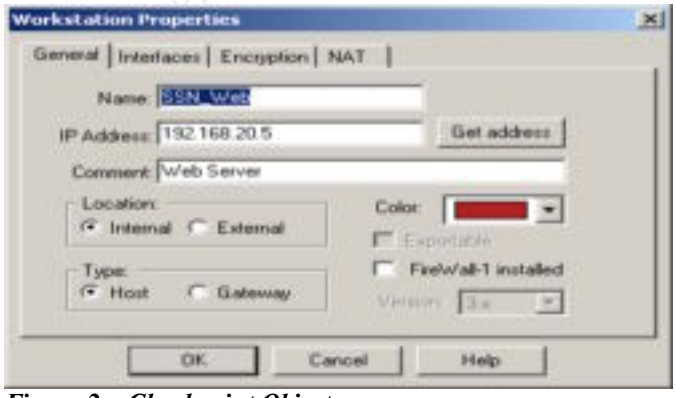
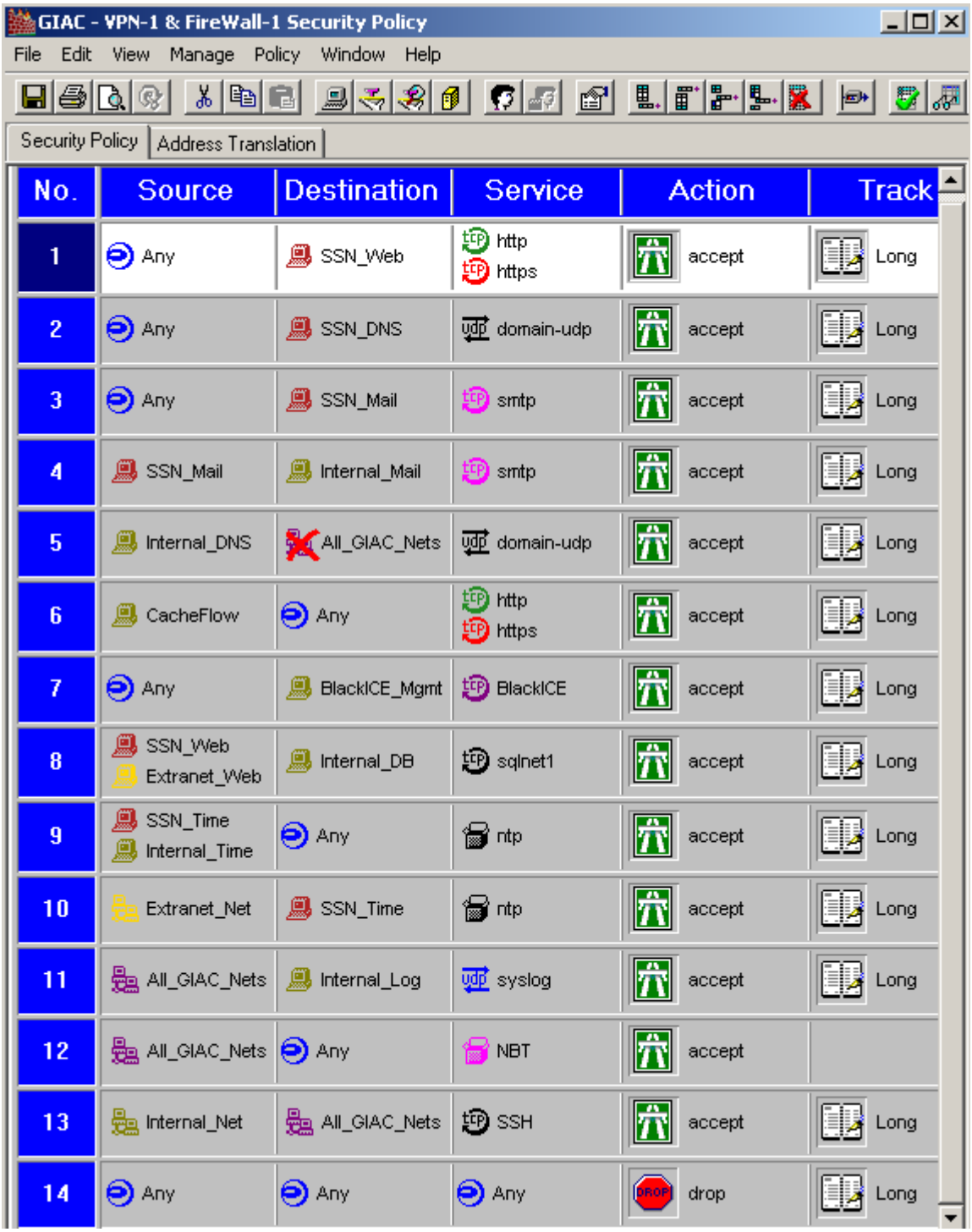


Figure 2 – Checkpoint Object



No.	Source	Destination	Service	Action	Track
1	Any	SSN_Web	http https	accept	Long
2	Any	SSN_DNS	domain-udp	accept	Long
3	Any	SSN_Mail	smtp	accept	Long
4	SSN_Mail	Internal_Mail	smtp	accept	Long
5	Internal_DNS	All_GIAC_Nets	domain-udp	accept	Long
6	CacheFlow	Any	http https	accept	Long
7	Any	BlackICE_Mgmt	BlackICE	accept	Long
8	SSN_Web Extranet_Web	Internal_DB	sqlnet1	accept	Long
9	SSN_Time Internal_Time	Any	ntp	accept	Long
10	Extranet_Net	SSN_Time	ntp	accept	Long
11	All_GIAC_Nets	Internal_Log	syslog	accept	Long
12	All_GIAC_Nets	Any	NBT	accept	
13	Internal_Net	All_GIAC_Nets	SSH	accept	Long
14	Any	Any	Any	drop	Long

Figure 3 – GIAC Checkpoint Rulebase

Below are some notes on selected rules above that may require explanation and some gotchas to watch out for when using a Checkpoint Firewall.

Rule #2: Notice that the UDP protocol is the only one allowed. This prevents a hacker from doing TCP zone transfer of all the details regarding the DNS server.

Rule #7: This rule is in place to allow all the host level IDS/Firewall agents to report back to the BlackICE management console. Parameters are setup on the management console to notify the security administrator of any suspect activity.

Rule #8: This is to allow the web servers to communicate to the Oracle database on the internal network. There is risk involved here but again, risk cannot be eliminated and business requires this functionality.

Rule #12: This rule was added to prevent the logs from filling up with Netbios activity.

Rule #13: This rule is to allow secure connections to the SSN using SSH on tcp port 22. Standard telnet sends information in clear text, which is unacceptable in our architecture.

These rules were ordered based on the frequency they are used.

Checkpoint comes with certain default settings that must be evaluated during setup. The firewall has implied pseudo rules that come from these default settings. It is recommended that these be turned off and traffic controlled exclusively by the rulebase. See *Figure 4*.

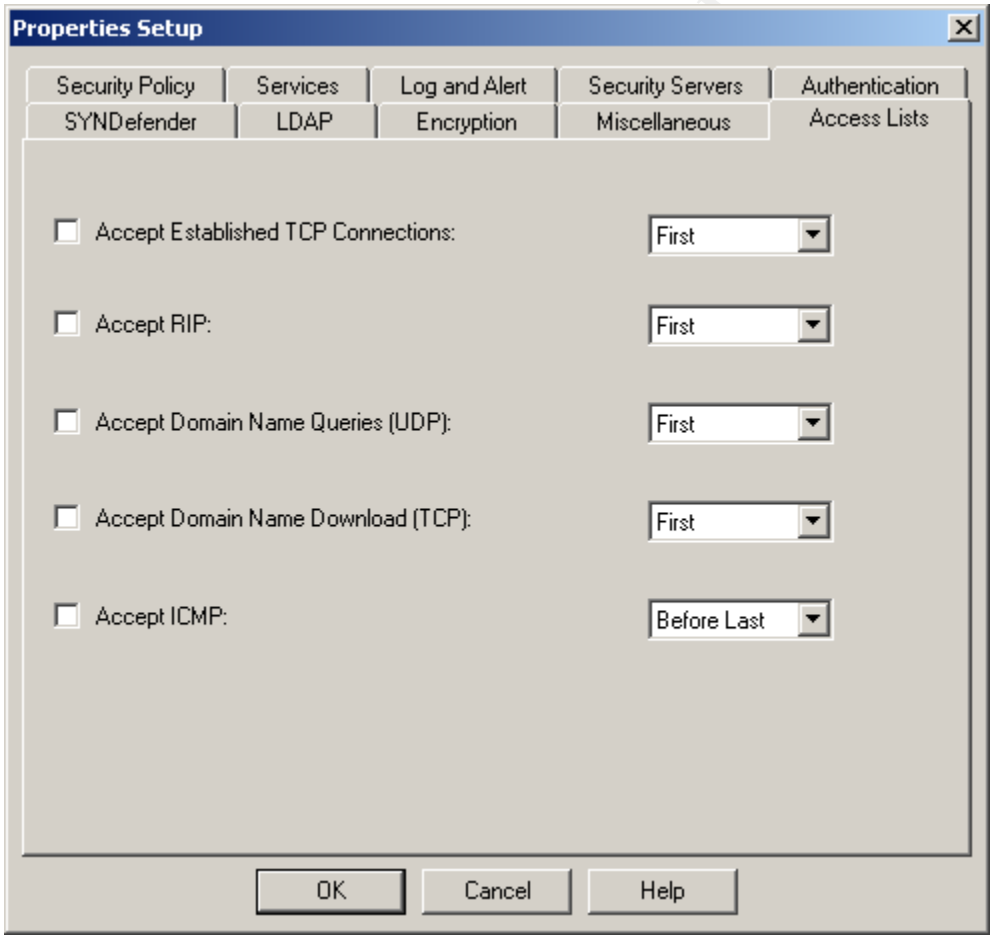


Figure 4 – Access List tab of Checkpoint Firewall properties

3.4 VPN

The VPN implementation is a Nortel Networks solution. This will provide the capability for individual user to connect using IPSEC. 3DES SHA1 will be the encryption algorithm used for all GIAC employees. Split tunneling will be disabled to prevent hackers from connecting to GIAC through a compromised client. Black ICE will also be deployed on any GIAC employee computer along with current antivirus product and definitions. The VPN will also require a SecurID authentication for any user connecting.

The partner/supplier connection may vary. They may choose to use a Nortel client meeting the specifications listed above or a VPN to VPN solution may be implemented. If the VPN to VPN route is taken, careful examination of the partner/supplier security policy will be required. Components like PKI certificates and key exchange will also play a part in this decision.

The Nortel box provides a lot functionality and flexibility. We will be able to control access based on protocol or destination on a per user basis. There is also the option for firewall software running on the VPN box, if that is required.

4. Assignment 3 – Audit Your Security Architecture

4.1 Assessment Plan

4.1.1 Considerations

Assessments should be done on a regularly scheduled basis. Processes should be in place to assess not only your vulnerabilities but also the degree of compliance to your written policy. In some cases penetration tests only provide the vulnerabilities side of your assessment; it is critical to have both.

Best practice would be to have self-evaluations on a monthly or quarterly basis and enlist and outside firm to complete a comprehensive assessment 1- 2 times yearly. For the purposes of this paper we will look at a more comprehensive assessment plan and give targeted examples of that plan in the implementation section of this document. We will also look to provide list of recommendations to improve the security architecture for GIAC.

Due to the nature of the business GIAC is in the assessment will need to take place during non-peak business hours. A comprehensive assessment would take 10 business days at a rate of 1,500 a day. Total assessment fees would run $15,000. It would begin with a review of the current security policy.
The assessment will cover three primary target areas: external, DMZ, and internal networks.

4.1.2 Target Areas

4.1.2.1 External

Included in the external assessment would be the audit of the border router, firewalls, and any backdoors to the network, namely analog phone lines. Several tools will be used to accomplish this assessment as outlined in the tools section. Specifically, we will be looking for open ports, and authentications issues. We will also look to see if all the proper logging is taking place on all the devices including the IDS systems. These tests will be performed to assess any vulnerabilities as well as compliance to written policies.

4.1.2.2 DMZs

Web servers, DNS servers, and Mail servers typically make up DMZs. The assessment here will be made to detect any configuration flaws on these servers or possibly identify services that are active but should be disabled. While on the DMZs we will test the firewall from this segment to make sure the only open ports are those outlined in the policy. Logging will again be assessed on all devices and IDS systems.

4.1.2.3 Internal

This is typically the weakest area in a security architecture. All hosts will be port scanned to identify unnecessary services that are active. Authentication will also be a focus. An overall compliance to the "need-to-know" policy will be assessed. Logging will again be assessed on all devices and IDS systems. Social engineering will be used but only as a last resort.

4.1.3 Tools

It is important that a variety of tools be used during an assessment

4.1.3.1 External

- nmap- used to scan for open ports and policy compliance. Will also be used to test logging activity.
  http://www.insecure.org/nmap/
- ISS Internet Scanner 6.1 – also used to scan for open ports. Will also be used for internal scanning and DMZ scanning
  http://www.iss.net

4.1.3.2 DMZ

- Sam Spade- used to query as much information from your DNS as possible
  http://www.samspade.org
- all tools listed in external tools section

4.1.3.3 Internal

- L0pht Crack – used to crack Windows passwords
  http://www.l0pht.com
- Crack – used to crack Unix passwords
  http://www.users.dircon.co.uk/~crypto

4.2 Implementation

For the purposes of our documentations, we will describe one of the tools used to scan the production Unix web server in the Screened Services Network at GIAC. Remember that a good assessment requires the use of at least 2 different tools. Multiple tools will cover the largest number of vulnerabilities.

ISS Internet Scanner 6.1 is a very useful tool especially for routine self-evaluation scanning. It allows you to configure policies to match your own and save those to allow for repeated testing. Additional scanning should always be done after upgrades or significant changes made to your security policy.

We will select a policy for Unix Web server and perform the scan. This would be done during scheduled downtime since it would affect the performance of the server. After the scan was complete we would be able to see all the discovered vulnerabilities, services running and local accounts on that machine. We would then compare that to the written security policy for validation and possible recommendations for policy change.

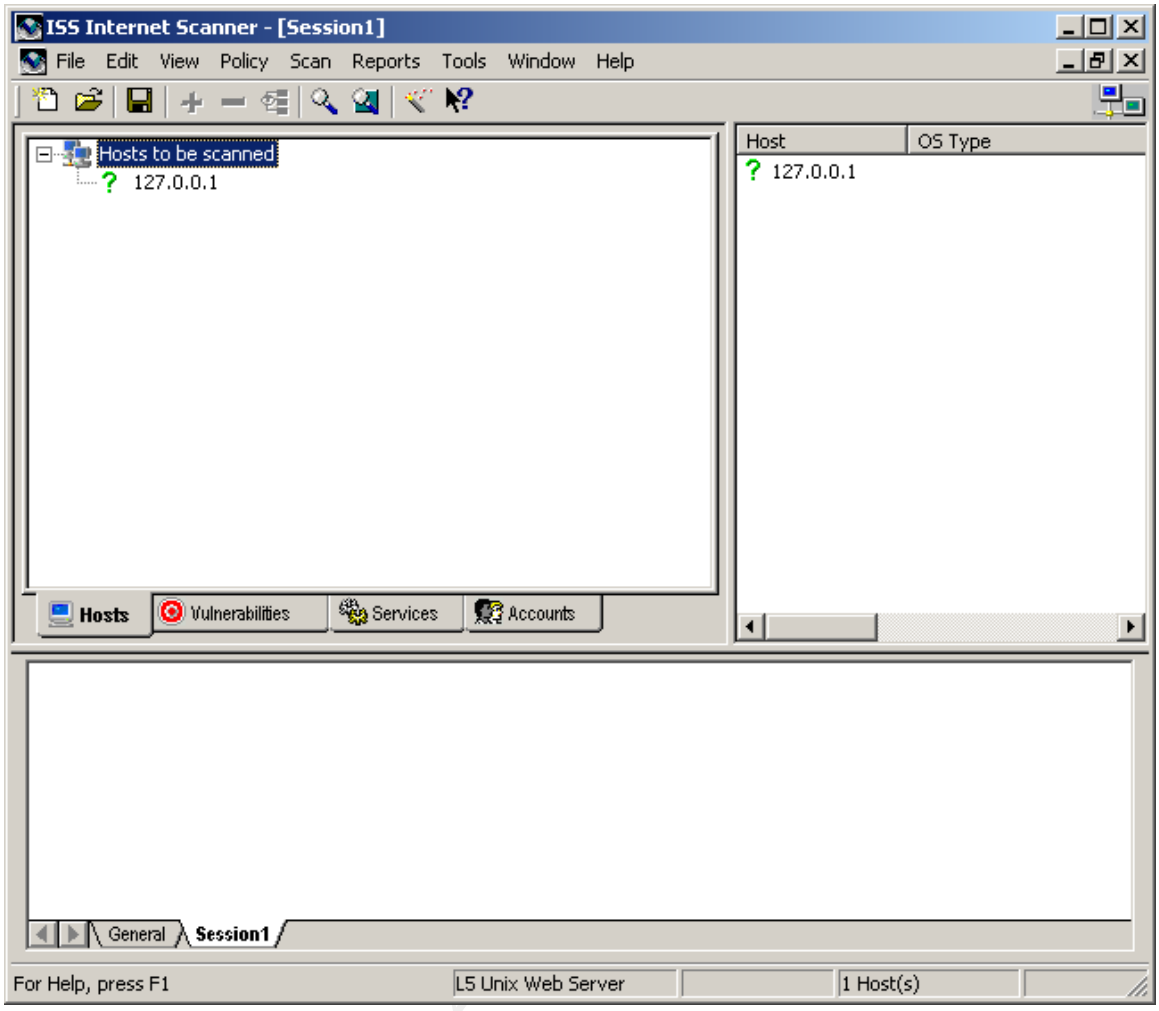


Figure 5 – Interface for ISS Internet Scanner 6.1

This type of implementation would need to be performed for all the different target areas outlined in the plan using a mixture of tools to provide the best possible assessment.

4.3 Analysis and Recommendations

After all the implementation phase is complete all the reports from all the different tools are compiled to provide a list of all vulnerabilities and policy variances. All these items will be assigned the following attributes with a rank of Low, Medium, or High:

- Risk
- Probability of Risk Occurrence
- Change Effort
- User Impact

Looking at the GIAC perimeter security architecture the following vulnerability was noted:

Vulnerability: Single Firewall Vendor. Even though the firewalls have load balancing and fail over, GIAC is still relying on one vendor. If a vulnerability was discovered by the hacker community and that information was disseminated quickly as it normally is, the network could be compromised overnight before the whitehat community every discovered it.
Recommendation: Deploy a second firewall between the current firewall and internal network. See *Figure 6*.

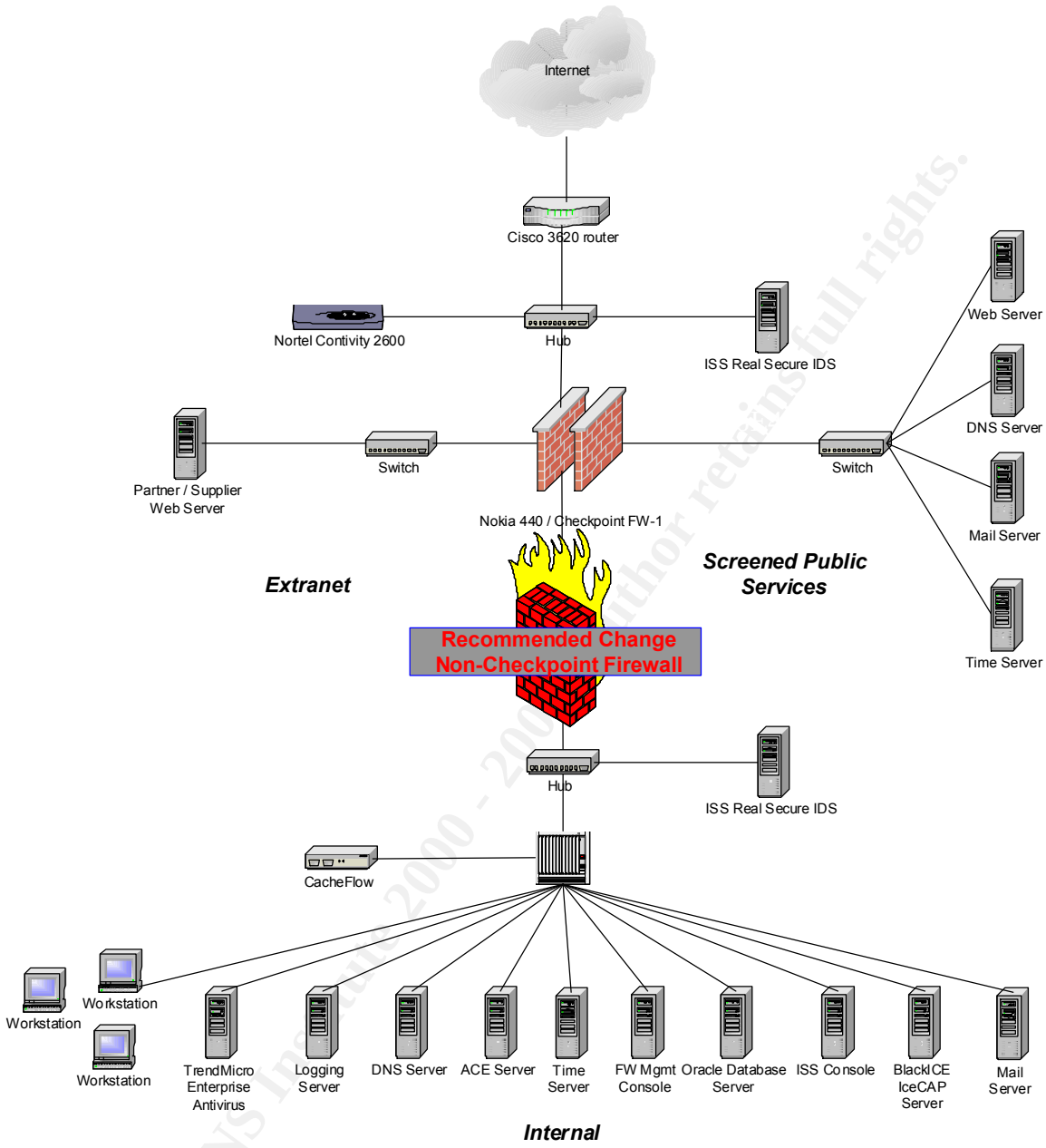
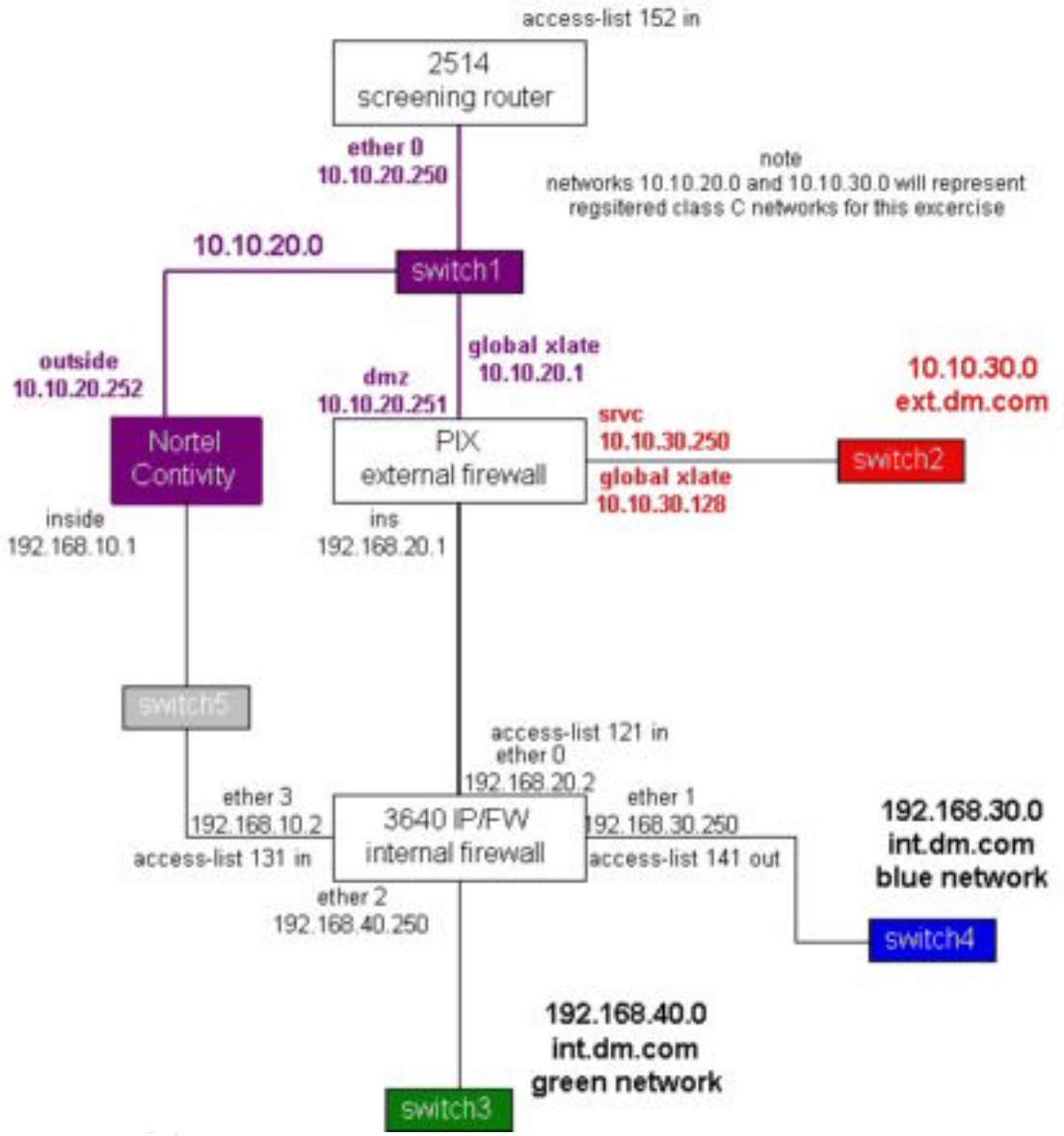


Figure 6 **- Modified Security Architecture Diagram for GIAC after Assessment**

5. Assignment 4 – Design Under Fire

The practical for this portion of the project is http://www.sans.org/y2k/practical/Blair_Perry.doc. Below is a diagram of his network design.



5.1 Firewall Attack

Blair has chosen a Cisco PIX version 4.4 as the firewall for this network design. We will be using the known vulnerability found at http://www.securityfocus.com BugTraq ID of 1454, CVE-2000-0613

The vulnerability is the described as the following: A connection through a Cisco Secure PIX Firewall can be reset by a third party if the source and destination IP addresses and ports of the connection can be determined or inferred. This can be accomplished by sending a forged TCP Reset (RST) packet to the firewall, containing the same source and destination addresses and ports (in the TCP packet header) as the connection to be disrupted.

To take advantage of this exploit we need to find out the IP address of some partners or suppliers. This could be done through research and some social engineering. We could easily identify the IP address of the web servers and ftp servers through DNS queries. Once we have this information we can begin to guess what protocols would be used starting with http, https, ftp. This would allow us to interrupt some of the business-to-business traffic that this company relies on.

5.2 Denial of Service Attack

The assumption is made here that the network in question here is under a DDoS attack from 50 compromised systems using TCP SYN floods and the question is posed as to what can be done to mitigate this attack. I will reference the follow article and present some options of defense. http://razor.bindview.com/publish/papers/DDSA_Defense.html

- Get physical access to your perimeter devices during the attack and determine the origin and destination of the packets. You can then create rules to block or divert this traffic.
- Turn logging off for these new rules to prevent the logging process from taking up valuable processor cycles.
- Contact your ISP with the information.
- Develop an architecture using 2 different ISPs each with its own router and firewall.

5.3 Internal Attack through the Firewall

There is a new vulnerability out listed for Microsoft's IE 5.5 found at http://www.securityfocus.com BugTraq ID of 2524, CAN-2001-0154

The way I would go about exploiting this would be to contact and HR recruiter for the company and ask them for their email address to send a resume.

Once the email address scheme is known, I would call the company after hours and hopefully be prompted to enter a names directory. Using this information, an email could be drafted posing as a legitimate business linking to a web page with the exploitation code on it. I could then execute a trojan or virus on that system and have an open door to the network.