

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

GIAC Firewall and Perimeter Protection Practical:
Implementation of Firewall Filters
Heather Bard
Nov 21, 2000

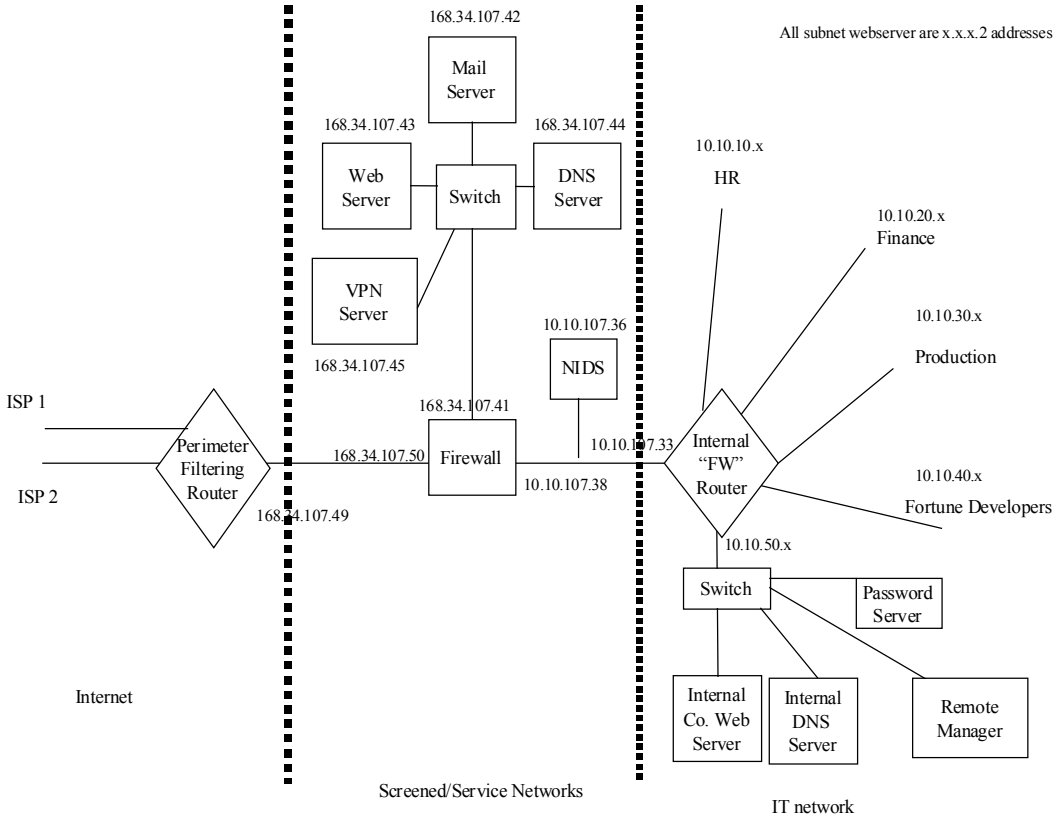
Introduction

This paper will describe a possible security architecture, security policy, and network assessment of this architecture and policy for a simulated company, GIAC Enterprises. GIAC Enterprises is a new Internet Startup that sells online fortune cookie sayings and expects to earn $200 million per year in sales. For the purposes of this paper I chose a "random real" IP address space for the external routes. This is not meant to emulate a real network with these Ips.

I. Define the Security Architecture for GIAC Enterprises.

The recommended Security Architecture for GIAC Enterprises is one of a basic screened or service network(s) approach. The security architecture will have a four-layered defense in depth approach. Refer to Figure 1 and the following text description of the overall architecture that includes a filtering router, firewall with screened network and VPN, internal firewalls, and protected hosts as the four layers of protection.

Figure 1. GIAC Security Architecture



The first layer of protection, the Perimeter Filtering Router, will be a Cisco 3600 router

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and will consist of three Ethernet connections. Two interfaces, e0/0 and e0/1, will be used for external connections providing redundancy in case of network failure. These two interfaces will have the same ingress access control lists (ACLs) applied to them as they are redundant interfaces. The third interface, e0/2, will be for the internal network connection and will connect directly to the external Firewall interface and will have a basic egress ACL applied to it.

The second layer of defense, the Screened Network, will include an Axent Raptor Firewall with 3 NIC cards. The Raptor Firewall provides Proxy Firewall services, as well as the ability to do NAT. The External NIC is connected to the internal interface of the Perimeter Filtering Router. The other 2 NICs are placed in the Firewalls Internal Interface configuration; however 1 of the NICs will be used for the screened services, the VPN and other internal servers. The final NIC will be the connection to the prime internal router, which in this case will be a 7206 router.

The third layer of defense, the internal routers, will have firewalling and IDS features on each of the ethernet interfaces. The 7206 router's Fastethernet port will be for the internal server bank (DNS, Web, and mail) and the other Ethernet connections will go to Ethernet switches connecting the internal user groups subnetworks. All of the http servers (finance, HR, developers, production) and individual mail server accounts will have login restrictions placed on them. Business units will place sensitive http servers on their LANs that they will allow access to via access control lists on the router as well as via password control. This will enable the individual business units to maintain access on a business need to know.

The fourth layer of protection is at the host (workstation) level and not depicted individually in Figure 1.1. This layer however will be based on individual access and restrictions on computers based on login/password to any machine and is controlled by a password server on the IT LAN. The central security manager will update the virus files and other software patches required on the individual machines.

See the Company Security Policy for the specifics on how to configure each of these devices.

II. Define a Security Policy

The Full GIAC Enterprises Security Policy is Attachment 1 to this document and provides indepth detail of a complete Information Assurance Policy.

1. To implement the additional filters that are required through the Policy on the firewall the first thing that needs to be done, after the initial setup of the FW, is to establish the elements that are going to be allowed specific access. These would be either by subnet, specific host, or groups. Once the network entities are created the manager needs to ensure that the specific protocols and or ports are created in the database. If not then the specified information needs to be entered. Once this is done then the specific rule for the policy can be created. These would create the basic firewalling rule bases needed to begin initial connectivity. However, there are many more features available on the Raptor, such as DNS proxy services that would also need to be setup. For more information on this go to: http://www.axent.com – customer support – Raptor Firewall – Configuration Guide.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. The Raptor Firewall permits or denies based on the Best Rule Scenario and therefore the order to apply FW rules does not matter; however to ensure that you have the correct rules applied it is still best to go through a general order. First, locking down the actual Firewall platform, then permitting services external, then permitting services internal to the Screened network, and finally permitting external services directly to the internal either via VPN or direct connections. For examples of the Rule sets for the firewall and routers see the appendices of the Security Policy.

III. Provide the technical plans for an Information Systems Audit for GIAC Enterprises.

1. **Plan the Assessment.** For the Network Security Assessment we will use a combination of free tools such as nmap and a CyberCop Scanner Laptop. The assessment will take place in three phases. The mapping and control phase, the external scan, and the internal scan. First, the Scanner will be placed external to the Perimeter router with no security features in place and will scan the network obtaining data on hosts and network. This will be the "control" for the assessment.

Secondly, all of the protection devices will be implemented and the same tests run. The tests will concentrate on trying to get through the perimeter protection, testing the rule sets, and on scanning/compromising the secuirty hosts, screened hosts, and internal servers and hosts. The data will be collected and compared to the control.

Thirdly, the CyberCop Laptop will be placed internal to the network and will assess the internal to external security policy focusing on the rules as well as trying to assess/compromise the security hosts, screened servers, and internal hosts. The initial tests will be non-destructive and will only identify potential vulnerabilities.

The test will be run during the weekend to give the management an idea of what the security protections of their systems should do and see. This is to ensure that there is minimal impact on network users as these tests do use bandwidth and could slow down service. For the first part of the test the network will be disconnected from the external network connection, so will have to be announced as a "network management" time that users will not be able to connect externally during.

The test will take the full weekend with another week to prepare the reports and will cost approximately $4000 which includes the test report creation and presentation to the company. The first section should take place on Friday evening (after 6PM) as this is the lowest usage time for authorized users). The initial network "normal" usage could be assessed during the week prior to the test to find out what normal traffic is by putting a sniffer in line with the firewall.

2. **Implement the Assessment and validate the policy**. I will assess the external router and FW platforms, and demonstrate that the firewall is performing it's duties in that the IDS will not be impacted. From this one can extrapolate how I would assess all of the hosts. I was not able to get a full complement of hosts due to my test network being pull out from under me to solve real-world issues.

Setup of Cybercop Scanner. Refer to www.nai.com – cybercop scanner – documents "Getting started Guide" for version 5.5. Setup a Fake DNS server. Then setup of IP address ranges to scan. I concentrated on the external to internal view so did a scan on the 168.34.x.x subnet. Would then do a scan on the 10.10.x.x networks for the internal scans.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The scans I will perform are both network and host based scans. To ensure that we have no interfering traffic I will place the Cybercop laptop in the place of one of the external routers (168.34.107.58) and disconnect the other. For the internal scan, to ensure that the perimeter and screened networks are operating as necessary I will put the Cybercop laptop in place of the internal router. Another way to do this is to put the Cybercop laptop as a host off of one of the LANs, or to create a secondary address off of the main router for the Cybercop. For the initial assessment I would perform non-destructive scans. When one goes into Cybercop Scanner the "destructive scans" are readily identifiable. As one looks at the modules, the scans that are highlighted in red are the destructive scans and should only be run on a network that one has permission to run such a scan against. I will use of the module except those that are destructive. Given that I have as much time as necessary, I will start the scan and let it run over night.

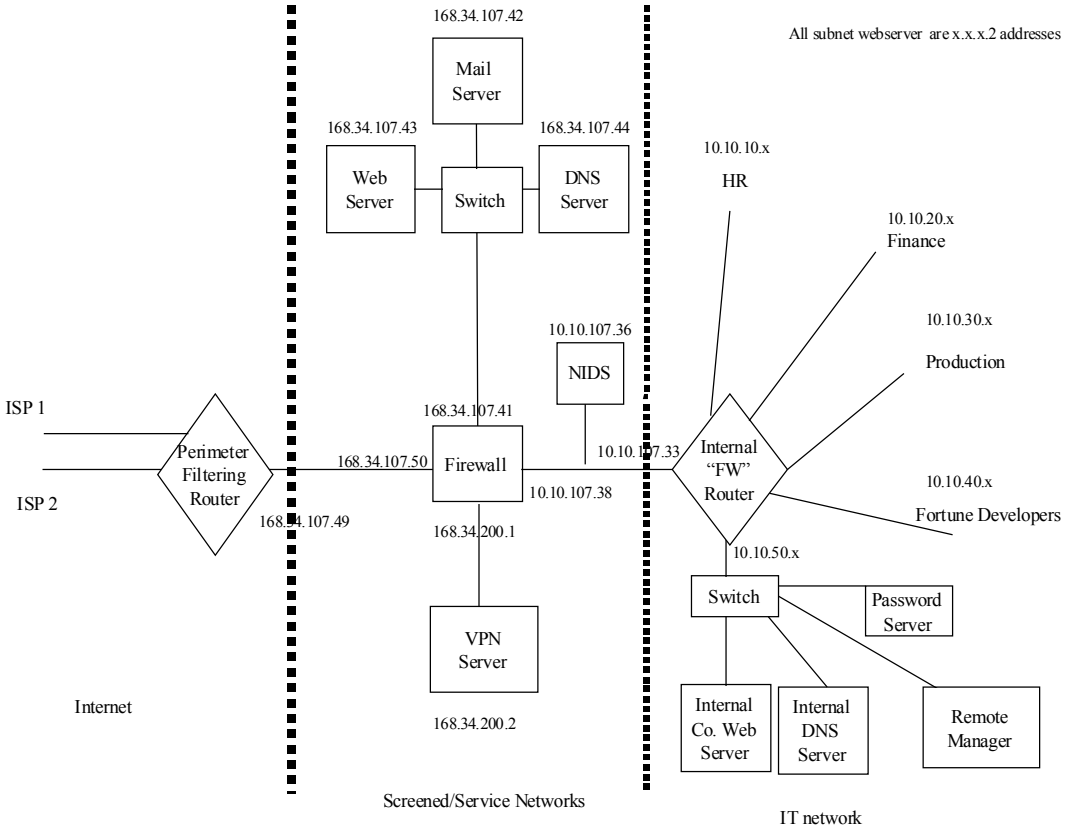
3. **Analyze the Perimeter and make recommendations.** The perimeter is fairly secure; however there is always room for improvement. They network seems to be locked down to the degree that it can be while still affording connectivity. The Cybercop found that telnet banners were implemented, but not ftp banners, especially on the external router. The external router could be more restricted, but that comes with the cost of high maintenance of that configuration file. The hosts are fairly well locked down. There are some minor recommendations made on how to make the hosts more secure as shown in the documentation taken directly from the CyberCop Report and included below.

Given the ability to modify the network I would recommend that the VPN server be placed on a separate NIC off of the Firewall. Depending on how much traffic is really going to go through this interface it could really hamper the flow of data to the other external to internal servers. See Figure 2 for this implementation. Also, would ensure that there is an internal manager to provide virus file updates from which all of the hosts would pull the "live updates".

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 2. VPN on separate NIC



The following is a sample of what one would see coming from a CyberCop report – minus all of the bells and whistles of the graphs and charts that this tool provides.

Network Analysis

Based on information gained from CyberCop Scanner probes to hosts on this network, the following conclusions can be made about the overall security of the network. For more information on interpreting this analysis, see the report introduction.

Total Count of Vulnerabilities	73
Total High-Risk	1
Percentage High-Risk	1
Total Medium-Risk	3
Percentage Medium-Risk	4
Total Low-Risk	69
Percentage Low-Risk	94

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Warning! Some hosts on this network can be completely compromised!

The following hosts were found to have high-risk vulnerabilities impacting system integrity. It is highly probable that a remote attacker can gain complete control over these systems, and use them to leverage access to other resources on the network.

- *168.34.107.58 (this was the Cybercop laptop itself – and it had not gone through any hardening procedures)*

Suggestions for Immediate Repair:

Because some vulnerabilities are easier to address than others, it may be worthwhile to quickly address the simplest vulnerabilities before resolving complex problems. Based on the number of easily-resolved security problems on the following hosts, consider addressing their concerns immediately.

1. *168.34.107.57 (this and 49 were the external router)*
2. *168.34.107.49*
3. *168.34.107.49*
4. *168.34.107.49*

Vulnerability Summary (on the external router)

	Host	Network
High Risk	0 vulnerabilities	1 vulnerabilities
Medium Risk	0 vulnerabilities	3 vulnerabilities
Low Risk	4 vulnerabilities	69 vulnerabilities

Host is on the local network

Ethernet Address: 00:01:96:54:B7:60 Ethernet Vendor : Unknown vendor

---

Host Analysis

Based on information gained from CyberCop Scanner probes to this host, the following conclusions can be made about its overall security.

Design

Many of the threats to this host are due to supported services with fundamentally insecure design. These problems may not be easy to solve, and consideration should be given to entirely replacing insecure services with more secure alternatives.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Vulnerability Analysis

CyberCop Scanner probes indicate that the following individual vulnerabilities are very likely to be present on this host. Vulnerabilities are seperated by "class", representing the different services and implications of the many different problems probed for by the scanner. For detailed information about the vulnerability descriptions and the various classes of problems looked for by the scanner, see the report introduction.

Information Gathering and Recon

1006 : Telnet service banner present (Risk Factor: Low)

Complexity of Attack: *Low*
Ease of Resolution: *Simple*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Misconfiguration*
Impact of Vulnerability: *Intelligence*
Module Output

Access denied.

1041 : Trace route to host (Risk Factor: Low)

Complexity of Attack: *Low*
Ease of Resolution: *Moderate*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

127.0.0.1,localhost 168.34.107.57 V 168.34.107.47

1041 : Trace route to host (Risk Factor: Low)

Complexity of Attack: *Low*
Ease of Resolution: *Moderate*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

127.0.0.1,localhost V 168.34.107.49

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Port Scanning

21001 : TCP port scanning (Risk Factor: Low)

Complexity of Attack: *N/A*
Ease of Resolution: *N/A*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

TCP Port 21 (ftp) active TCP Port 23 (telnet) active TCP Port 25 (smtp) active TCP Port 443 (unknown) active

21003 : TCP SYN port scanning (Risk Factor: Low)

Complexity of Attack: *Medium*
Ease of Resolution: *N/A*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

TCP Port 21 (ftp) active TCP Port 23 (telnet) active TCP Port 25 (smtp) active TCP Port 443 (unknown) active

Vulnerability Summary (on Firewall)

	Host	Network
High Risk	0 vulnerabilities	1 vulnerabilities
Medium Risk	0 vulnerabilities	3 vulnerabilities
Low Risk	5 vulnerabilities	69 vulnerabilities

Host is on the local network

Ethernet Address: 00:01:96:54:B7:60 Ethernet Vendor : Unknown vendor

Based on information gained from CyberCop Scanner probes to this host, the following conclusions can be made about its overall security.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Design
Many of the threats to this host are due to supported services with fundamentally insecure design. These problems may not be easy to solve, and consideration should be given to entirely replacing insecure services with more secure alternatives.

Vulnerability Analysis

CyberCop Scanner probes indicate that the following individual vulnerabilities are very likely to be present on this host. Vulnerabilities are seperated by "class", representing the different services and implications of the many different problems probed for by the scanner. For detailed information about the vulnerability descriptions and the various classes of problems looked for by the scanner, see the report introduction.

1006 : Telnet service banner present (Risk Factor: Low)

Complexity of Attack: *Low*
Ease of Resolution: *Simple*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Misconfiguration*
Impact of Vulnerability: *Intelligence*
Module Output

Raptor Firewall Secure Gateway. Hostname:

1008 : FTP banner check (Risk Factor: Low)

Complexity of Attack: *Low*
Ease of Resolution: *Moderate*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Implementation*
Impact of Vulnerability: *Intelligence*
Module Output

220 Secure Gateway FTP server ready.

1041 : Trace route to host (Risk Factor: Low)

Complexity of Attack: *Low*
Ease of Resolution: *Moderate*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

127.0.0.1,localhost 168.34.107.57 168.34.107.50

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Port Scanning

21001 : TCP port scanning (Risk Factor: Low)

Complexity of Attack: *N/A*
Ease of Resolution: *N/A*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

TCP Port 21 (ftp) active TCP Port 23 (telnet) active TCP Port 25 (smtp) active TCP Port 53 (domain) active TCP Port 416 (unknown) active TCP Port 417 (unknown) active TCP Port 418 (unknown) active TCP Port 443 (unknown) active

21003 : TCP SYN port scanning (Risk Factor: Low)

Complexity of Attack: *Medium*
Ease of Resolution: *N/A*
Popularity of Attack: *Popular*
Root Cause of Vulnerability: *Design*
Impact of Vulnerability: *Intelligence*
Module Output

TCP Port 21 (ftp) active TCP Port 23 (telnet) active TCP Port 25 (smtp) active TCP Port 53 (domain) active TCP Port 416 (unknown) active TCP Port 417 (unknown) active TCP Port 418 (unknown) active TCP Port 443 (unknown) active

Below is the partial log file from the Raptor for the period of the scan. In the logs I am sure that it will be noted that I also have some misconfigurations of the Raptor which I did not have the opportunity to completely troubleshoot. However, if one looks at the logs containing the 168.34.107.58 entries, one can see the CyberCop Scans in action.

```
Nov 20 18:54:31.515 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:31.608 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1087->1)
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Nov 20 18:54:31.625 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.28 id=KSR
sent=24 src=168.34.107.58/1087 dst=168.34.107.47/1 proto=1/tcp (failed to get
call addressing information)
Nov 20 18:54:36.484 fw1 ftpd[353]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:36.515 fw1 ftpd[353]: 121 Statistics: duration=5.25 id=N0Z
src=168.34.107.58/1089 proto=ftp (Call startup failure)
Nov 20 18:54:36.532 fw1 telnetd[327]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:36.579 fw1 telnetd[327]: 121 Statistics: duration=5.26 id=P97
rcvd=18 src=168.34.107.58/1088 proto=telnet (Call startup failure)
Nov 20 18:54:38.484 fw1 smtp[346]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:38.515 fw1 smtp[346]: 121 Statistics: duration=5.24 id=Rhf
rcvd=69 src=168.34.107.58/1090 proto=smtp (Call startup failure)
Nov 20 18:54:38.843 fw1 ftpd[353]: 121 Statistics: duration=0.00 id=N12
src=168.34.107.58/21891 proto=ftp (Connection closed immediately)
Nov 20 18:54:38.843 fw1 smtp[346]: 121 Statistics: duration=0.00 id=Rhh
rcvd=18446744073709551615 src=168.34.107.58/21891 proto=smtp (Connection
closed immediately)
Nov 20 18:54:38.843 fw1 telnetd[327]: 121 Statistics: duration=0.00 id=P9a
src=168.34.107.58/21891 proto=telnet (Connection closed immediately)
Nov 20 18:54:42.626 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:42.664 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1092->79)
Nov 20 18:54:42.687 fw1 telnetd[327]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:42.690 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.15 id=KSS
sent=24 src=168.34.107.58/1092 dst=168.34.107.47/79 proto=79/tcp (failed to
get call addressing information)
Nov 20 18:54:42.734 fw1 telnetd[327]: 121 Statistics: duration=5.15 id=P98
rcvd=18 src=168.34.107.58/1094 proto=telnet (Call startup failure)
Nov 20 18:54:42.752 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:42.815 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1093->79)
Nov 20 18:54:42.846 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.29 id=KST
sent=24 src=168.34.107.58/1093 dst=168.34.107.47/79 proto=79/tcp (failed to
get call addressing information)
Nov 20 18:54:42.902 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:42.935 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1095->1)
Nov 20 18:54:42.937 fw1 ftpd[353]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:42.952 fw1 telnetd[327]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Nov 20 18:54:42.968 fw1 smtp[346]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:42.965 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.15 id=KSU
sent=24 src=168.34.107.58/1095 dst=168.34.107.47/1 proto=1/tcp (failed to get
call addressing information)
Nov 20 18:54:43.000 fw1 ftpd[353]: 121 Statistics: duration=5.17 id=N10
src=168.34.107.58/1099 proto=ftp (Call startup failure)
Nov 20 18:54:43.031 fw1 telnetd[327]: 121 Statistics: duration=5.18 id=P99
rcvd=18 src=168.34.107.58/1118 proto=telnet (Call startup failure)
Nov 20 18:54:43.062 fw1 smtp[346]: 121 Statistics: duration=5.20 id=Rhg
rcvd=69 src=168.34.107.58/1120 proto=smtp (Call startup failure)
Nov 20 18:54:43.090 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.125 fw1 ftpd[353]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.216 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.249 fw1 ftpd[353]: 121 Statistics: duration=5.40 id=N11
src=168.34.107.58/1116 proto=ftp (Call startup failure)
Nov 20 18:54:43.278 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1096->2)
Nov 20 18:54:43.340 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.372 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1097->3)
Nov 20 18:54:43.403 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.434 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.52 id=KSV
sent=24 src=168.34.107.58/1096 dst=168.34.107.47/2 proto=2/tcp (failed to get
call addressing information)
Nov 20 18:54:43.465 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1098->4)
Nov 20 18:54:43.496 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.57 id=KSW
sent=24 src=168.34.107.58/1097 dst=168.34.107.47/3 proto=3/tcp (failed to get
call addressing information)
Nov 20 18:54:43.528 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1100->5)
Nov 20 18:54:43.559 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.591 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.65 id=KSX
sent=24 src=168.34.107.58/1098 dst=168.34.107.47/4 proto=4/tcp (failed to get
call addressing information)
Nov 20 18:54:43.621 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.653 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.71 id=KSY
sent=24 src=168.34.107.58/1100 dst=168.34.107.47/5 proto=5/tcp (failed to get
call addressing information)
Nov 20 18:54:43.683 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1101->6)
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Nov 20 18:54:43.715 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1102->7)
Nov 20 18:54:43.746 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.778 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.87 id=KSZ
sent=24 src=168.34.107.58/1101 dst=168.34.107.47/6 proto=6/tcp (failed to get
call addressing information)
Nov 20 18:54:43.809 fw1 tcpap-gsp[229]: 121 Statistics: duration=5.90 id=KT0
sent=24 src=168.34.107.58/1102 dst=168.34.107.47/7 proto=7/tcp (failed to get
call addressing information)
Nov 20 18:54:43.840 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.872 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1103->8)
Nov 20 18:54:43.906 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1104->9)
Nov 20 18:54:43.937 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:43.969 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.06 id=KT1
sent=24 src=168.34.107.58/1103 dst=168.34.107.47/8 proto=8/tcp (failed to get
call addressing information)
Nov 20 18:54:43.999 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.09 id=KT2
sent=24 src=168.34.107.58/1104 dst=168.34.107.47/9 proto=9/tcp (failed to get
call addressing information)
Nov 20 18:54:44.031 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1105->10)
Nov 20 18:54:44.062 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.094 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.21 id=KT3
sent=24 src=168.34.107.58/1105 dst=168.34.107.47/10 proto=10/tcp (failed to
get call addressing information)
Nov 20 18:54:44.124 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1106->11)
Nov 20 18:54:44.156 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.156 fw1 tcp-gsp[317]: 301 Internal warning:
port_receive_control(6,416,2) failed: A device attached to the system is not
functioning.
Nov 20 18:54:44.187 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.31 id=KT4
sent=24 src=168.34.107.58/1106 dst=168.34.107.47/11 proto=11/tcp (failed to
get call addressing information)
Nov 20 18:54:44.218 fw1 tcp-gsp[317]: 301 Internal warning:
port_receive_control(6,416,2) failed: A device attached to the system is not
functioning.
Nov 20 18:54:44.250 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1107->12)
Nov 20 18:54:44.281 fw1 tcp-gsp[317]: 301 Internal warning:
port_receive_control(6,417,2) failed: A device attached to the system is not
functioning.
Nov 20 18:54:44.312 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Nov 20 18:54:44.343 fw1 tcp-gsp[317]: 301 Internal warning:
port_receive_control(6,417,2) failed: A device attached to the system is not
functioning.
Nov 20 18:54:44.375 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.46 id=KT5
sent=24 src=168.34.107.58/1107 dst=168.34.107.47/12 proto=12/tcp (failed to
get call addressing information)
Nov 20 18:54:44.406 fw1 tcp-gsp[317]: 301 Internal warning:
port_receive_control(6,418,2) failed: A device attached to the system is not
functioning.
Nov 20 18:54:44.437 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.468 fw1 tcp-gsp[317]: 301 Internal warning:
port_receive_control(6,418,2) failed: A device attached to the system is not
functioning.
Nov 20 18:54:44.500 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1108->13)
Nov 20 18:54:44.562 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.594 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1109->14)
Nov 20 18:54:44.625 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.656 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.71 id=KT6
sent=24 src=168.34.107.58/1108 dst=168.34.107.47/13 proto=13/tcp (failed to
get call addressing information)
Nov 20 18:54:44.687 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1110->15)
Nov 20 18:54:44.718 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.77 id=KT7
sent=24 src=168.34.107.58/1109 dst=168.34.107.47/14 proto=14/tcp (failed to
get call addressing information)
Nov 20 18:54:44.749 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.781 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1111->16)
Nov 20 18:54:44.812 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.86 id=KT8
sent=24 src=168.34.107.58/1110 dst=168.34.107.47/15 proto=15/tcp (failed to
get call addressing information)
Nov 20 18:54:44.843 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.875 fw1 tcpap-gsp[229]: 239 Sending TCP Reset for packet
(168.34.107.58->168.34.107.47: Protocol=TCP[SYN] Port 1112->17) [(null) log
limit for level 2 reached with 20 messages in the last second -- suppressing
temporarily]
Nov 20 18:54:44.906 fw1 tcpap-gsp[229]: 121 Statistics: duration=6.96 id=KT9
sent=24 src=168.34.107.58/1111 dst=168.34.107.47/16 proto=16/tcp (failed to
get call addressing information)
Nov 20 18:54:44.936 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:44.968 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.02 id=KTb
sent=24 src=168.34.107.58/1113 dst=168.34.107.47/18 proto=18/tcp (failed to
get call addressing information)
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Nov 20 18:54:45.000 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.05 id=KTa
sent=24 src=168.34.107.58/1112 dst=168.34.107.47/17 proto=17/tcp (failed to
get call addressing information)
Nov 20 18:54:45.030 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.11 id=KTc
sent=24 src=168.34.107.58/1114 dst=168.34.107.47/19 proto=19/tcp (failed to
get call addressing information)
Nov 20 18:54:45.061 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:45.093 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:45.125 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.24 id=KTd
sent=24 src=168.34.107.58/1115 dst=168.34.107.47/20 proto=20/tcp (failed to
get call addressing information)
Nov 20 18:54:45.155 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.27 id=KTe
sent=24 src=168.34.107.58/1117 dst=168.34.107.47/22 proto=22/tcp (failed to
get call addressing information)
Nov 20 18:54:45.201 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:45.234 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.37 id=KTf
sent=24 src=168.34.107.58/1119 dst=168.34.107.47/24 proto=24/tcp (failed to
get call addressing information)
Nov 20 18:54:45.310 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
Nov 20 18:54:45.344 fw1 tcpap-gsp[229]: 121 Statistics: duration=7.48 id=KTg
sent=24 src=168.34.107.58/1121 dst=168.34.107.47/26 proto=26/tcp (failed to
get call addressing information)
Nov 20 18:54:45.420 fw1 tcpap-gsp[229]: 343 Interfaces Warning: Unable to
determine tunnel information for destination address 168.34.107.47 - is the
system local and down? -- test connectivity with ping
```

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Attachment 1 to Firewall and Perimeter Protection Track Practical – GIAC Enterprise's Security Policy

Table Of Contents

Nov 20, 2000 ..... **i**
Introduction i
Figure 1. GIAC Security Architecture i
II. Define a Security Policy ii
III. Provide the technical plans for an Information Systems Audit for GIAC Enterprises. iii

Figure 2. VPN on separate NIC ..... **v**
Network Analysis v
Vulnerability Summary (on the external router) vi
Host Analysis vi
Vulnerability Analysis vii
1006 : Telnet service banner present (Risk Factor: Low) vii
1041 : Trace route to host (Risk Factor: Low) vii
21001 : TCP port scanning (Risk Factor: Low) viii
21003 : TCP SYN port scanning (Risk Factor: Low) viii
Vulnerability Analysis ix
1006 : Telnet service banner present (Risk Factor: Low) ix
1008 : FTP banner check (Risk Factor: Low) ix
1041 : Trace route to host (Risk Factor: Low) ix
21001 : TCP port scanning (Risk Factor: Low) x
21003 : TCP SYN port scanning (Risk Factor: Low) x

1. Scope **6**

2. Applicable Documents **6**

3. Physical Security **6**

4. Personnel Security **6**
4.1 GIAC Network Managers 6
4.2 Maintenance Personnel 7

5. Information Assurance Considerations **7**
5.1 Protection Requirements 7
5.1.1 Information Protection 7
5.1.2 Network Availability Protection 8
5.2 Threats to Information Assurance 8
5.2.1 Unintentional Threats and their impacts 8
5.2.2 Internal Threats and their impacts 8
5.2.3 External Threats and their impacts 9
5.2.4 System Vulnerability Threat and their impacts 9
5.3 Risk Management 9
5.3.1 Operator Trust Level 9
5.3.2 Network Encryption Level 9
5.3.3 Network Operator versus Manager Trust Level 10
5.4 External Interface Requirements 10

6. IA Architecture Description **10**
6.1 External Filtering Router 10
6.2 External Firewall and Screen Network Information Assurance Features 10
6.2.1 External Firewall Services 10

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6.2.2 External NIDS Services 11
6.2.3 VPN Server 11
6.3 Backbone Network Information Assurance Features 11
6.3.1 Backbone Network Firewall Services 12
6.3.2 Backbone Network IDS Services 12
6.4 Host Level Information Assurance Features 12

7. Information Assurance Management 12
7.1 IA Management Plan 13
7.1.1 IA Management - Attack Notification and Response 13
7.1.2 Primary IA Management - IA Software Updates 13
7.2 Network Management 14
7.2.1 Network Management Plan 14
7.2.2 Network Management - Attack Notification and Response 14
7.2.3 Network IA Management - IA Software Updates 14

8. Areas of Responsibility 14
8.1 Company CEO 14
8.2 Information Assurance Managers 14
8.3 Internal Network Operators 14
8.4 System Administrators and System Security managers 15
8.5 Network Subscribers 15

9. Acceptable Use Guidelines 15
9.1 Additional Guidance 15
9.2 Enforcement for Misuse 15

Appendix A. Acronym List 15

Appendix B External Router Configuration and Access Controls 17

Appendix C Raptor Configuration Rules 19

Appendix D Internal Router Access Controls 26

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Executive Summary

This document serves as the Information Assurance (IA) Policy for GIAC Enterprises. Its purpose is to summarize the Security Policy while accounting for the architectural framework at the same time. It defines the security architecture and roadmaps the security actions needed to support GIAC Enterprises requirements.

GIAC Enterprises network IA provides information protection and network availability to ensure the integrity of all data being passed into, out of, and through their network and that the network is maintained and operational. The GIAC network IA Policy is a multi-tiered architecture consisting of four layers, each consisting of a different configuration of security tools to provide a rugged defense-in-depth strategy of protection. The four IA layers are the following: (1) external filtering router layer, (2) external firewall and screening layer, (3) backbone network layer, and (4) host layer.

The external filtering router layer provides for the first layer of defense while being fairly permissive. This layer is to deny those well-known attacks and "hacker Ips".

The external firewall layer is the strongest of the four layers. The external firewall layer IA mechanism consists of a a full-function firewall and Network Intrusion Detection System (NIDS) to protect the internal network from unauthorized access from external connections. It also has a VPN server that allows data to tunnel through external networks to remote suppliers and partners, as well as the "untrusted" servers.

The backbone network IA layer mechanisms consist of Cisco routers with an embedded Firewall Feature Set (FFS), which includes a Context Based Access Control (CBAC) firewall and Intrusion Detection Systems (IDS).

Finally, host layer IA mechanisms use Command and Control (C2) Protect tools to allow secure protocols to encrypt traffic sessions via an authorized encryption mechanism, to perform workstation configuration checks, and to send alerts. Virus protection via anti-virus software is an important part of this layer. UNIX and Windows New Technology (NT) workstations will adhere to the appropriate security, and hardening, documents.

At each GIAC local and remote network site physical and personnel security policies must be strictly enforced. The physical security policy is based on an analysis of mission criticality, sensitivity levels of the information being processed, security threats, and the vulnerability of the network to the security threats. The personnel security policy focuses on network operators who must follow the security features of the system for which they are responsible. The manager in charge of each unit is responsible for the actions of the people under his control.

Both internal and external threats are addressed by the IA Policy. They include data theft, data corruption, network flooding, denial of service, espionage, and virus attacks. Internal threats originate from within the network and are mitigated by granting a level of trust to the network operators as well as through authentication, firewalls, and IDSs. External threats will be blocked at the external layer. IA management is the key to the security and functionality of the network. The primary IA manager will work with the network and local IA managers in managing the entire GIAC network. Each manager will have different responsibilities with regard to plan implementation, attack response, obtaining and loading attack file updates, and ensuring network integrity.

Heather Bard 01/16/05

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Scope

This document defines the Information Assurance (IA) policy GIAC Enterprises. It describes GIACs network equipment and information that will be protected, the threats to this information, and the potential risks. It also addresses the IA architecture, including the methods and mechanisms used to protect the information and network, the responsibilities of the IA staff, the physical and procedural security requirements, and acceptable use guidelines. The overall security objective of the policy is to protect GIACs network from malicious activities or nonmalicious accidental actions that can lead to the network being compromised.

The IA features of GIACs network will consist of four layers, each layer consisting of different configurations of access lists, firewalls, Network Intrusion Detection Systems (NIDS), and/or host-based IA features, to provide a rugged defense-in-depth strategy of protection. The four layers are the following: (1) external filtering router, (2) external firewall and screened networks, (3) backbone network layer (hereafter referred to as the backbone layer), and (4) host layer.

2. Applicable Documents

Request for Comment (RFC) 2196 Site Security Handbook – Network Working Group, September 1997.
RFC 1918 on Spoofed Ips.
RFC 2267

3. Physical Security

The GIAC network hardware, software, documentation, firmware, and all classified and Sensitive-But-Unclassified (SBU) data processed and stored will be protected to prevent the threat of unauthorized (intentional or unintentional) disclosure, destruction, or modification. Physical security is one of the principal means used to protect against this threat.

Physical security at each GIAC network site is based on an analysis of mission criticality, sensitivity levels of the information being processed, security threats, and the vulnerability of the GIAC network to the security threats. It is the responsibility of the site commander/IA manager to establish and enforce the site's physical security policy.

The objectives of physical security at each site are to prevent unauthorized access to equipment, facilities, material, media, and documents; safeguard against espionage, terrorism, sabotage, damage, misuse, and theft; and reduce the exposure to threats that could result in a denial of service or unauthorized alteration of data.

4. Personnel Security

4.1 GIAC Network Managers

GIAC network managers are those personnel responsible for operating the network equipment such as the switches, routers, and network management systems. They

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

should conduct themselves in accordance with the approved security procedures of the system for which they are responsible.

Network managers will be familiar with the personnel in their subnet. However, it is not the network managers responsibility to check on the identity and need-to-know of each individual requesting access to the GIAC network. They are not responsible for granting or denying access. This is the responsibility of overall Security Manager.

4.2 Maintenance Personnel

The IA manager will be responsible for any exceptions that are made that allow uncleared personnel access to the GIAC network for the purpose of maintenance. All maintenance personnel, whether they are cleared or not, will be escorted and observed during maintenance procedures by someone with technical expertise to detect obvious unauthorized modifications.

If maintenance personnel must remove GIAC network components, property accountability and security procedures will be followed. If any GIAC network components with sensitive data must be removed, the site IA manager or operator must backup and then purge them. If maintenance personnel need to remove components that cannot be fully purged, operators will advise the maintenance personnel of the sensitivity of the material stored on the components and handling procedures for the sensitive material. The IA manager and network managers will be notified if uncleared maintenance personnel inadvertently gain access to sensitive data during the course of their maintenance actions.

5. Information Assurance Considerations

5.1 Protection Requirements

The GIAC network IA provides information protection and network availability protection. The information/data being protected consists of the following:

- E-mail.
- Personnel data.
- Network configuration data - DNS and Webserver information
- Fortune Cookie saying development information.
- Company financial data.

5.1.1 Information Protection

The defense-in-depth strategy of protection will ensure the integrity and accuracy of all data being passed on the internal network. This entails ensuring the authenticity of the information and ensuring that all information passed retains its classification level.

The backbone layer uses secured VPN connections to remote sites. The NIDS and firewalls at the backbone and external layers will inspect the Internet Protocol (IP) streams for packet integrity and provide network access controls. VPN encrypted network to network traffic that stays within the GIAC network branches will not

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

be checked by firewalls or NIDS as it is a packet that will not be decrypted before reaching the router. The router cannot look into this packet.

Host layer security consists of C2 Protect tools (Paragraph 6.4 contains a list of required tools), physical and personnel security.

5.1.2 Network Availability Protection

Protection of the network path availability and component configurations will help to ensure transmission through the network. Protection is accomplished primarily at the backbone layer using firewall access lists, dynamic filtering with packet inspection, network router authentication, and near real-time NIDS alerts. This will ensure that the hardware, software, and firmware that support the backbone remain undamaged.

5.2 Threats to Information Assurance

There are multiple means of attack that will be protected against by using other methods already in the backbone system (e.g., trunk encryption). These threats are presented in the following paragraphs in the order of likelihood and severity of damage that could occur.

5.2.1 Unintentional Threats and their impacts

Unintentional threats are those caused by operator error. Protection will be provided to reasonably ensure that an operator does not unwittingly pass classified or SBU information to those not cleared or without a need to know. This protection will be accomplished using the firewall's access control mechanisms at the external interface to block outgoing traffic to unauthorized hosts, using mail servers, web servers, and DNS servers to pass traffic down to a lower level (this will occur primarily through the screened network, and using VPNs throughout the system to pass traffic to parties at the same level.

Unintentional threats are also those caused by an operator that result in a network slowdown or interference with data or network availability. These threats are controlled through the implementation of the IA Policy, monitoring audit trails set through the NIDS, and the use of firewalls to stop flooding and synchronization attacks.

The likelihood of unintentional errors is high, but the protection afforded through the implementation of the IA Policy greatly reduces the likelihood of harmful disclosure of information or network malfunction.

5.2.2 Internal Threats and their impacts

Internal threats may include data theft, data corruption, network flooding, denial of service, espionage, and virus attacks. Within the network, there is a level of trust granted to operators. Contractors and partners will be subject to the same policies as the company personnel. A level of protection will be provided at the backbone and subnetwork layers for denial of service and flooding attacks through firewall features and intrusion detection. Additionally, at all layers, operator authentication requirements, permission settings, and audit trails provide other methods of security.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The likelihood of an insider attack is fairly small, but the damage that could be caused by a knowledgeable insider is disproportionately large. Therefore, adherence to the IA Policy and the continual use of physical and personnel security protections are necessary.

5.2.3 External Threats and their impacts

The difference between external and internal threats, from a network assurance perspective, is where the attack originates and where the attack needs to be blocked. External threats will be blocked at the external network connection point with full feature firewalls and NIDS. An external threat includes the possibility of a shelter or operator workstation being compromised.

The likelihood of an external attack is very high, and the damage that could be accomplished if the attacker gains access would be very great. With the SECRET high backbone and defense-in-depth approach, the success of this type of attack is much less likely than the success of an insider attack.

5.2.4 System Vulnerability Threat and their impacts

System vulnerability threats are external threats that are caused by security holes in operating systems, Web applications, office products, etc. Patches to address these problems are routinely developed, updated, and published. Patches may not be installed if they adversely impact mission critical functionality. The system manager will make the decision regarding the installation of security patches. Installing patches when users are remoted is an extremely rare event and will occur only if it is absolutely vital to the security of the network.

To minimize the system vulnerability threat, not all network operators will have a need-to-know for this information.

The likelihood of system vulnerability attacks is very high, and the damage that could be accomplished if the attacker gains access would be very great. With the defense-in-depth approach, the success of this type of attack is less likely than the success of an insider attack.

5.3 Risk Management

5.3.1 Operator Trust Level

The level of trust given to GIAC network operators is directly proportional to the level of management responsibility of the system given to the operator. GIAC will trust the network managers to a very high degree, and those operators internal the the base network to a high degree allowing a fairly open internal network (i.e., subnet to subnet). The operators will be regulated from the command level with the Acceptable Use Guidelines and enforcement of those policies (see Section 0 for more details).

5.3.2 Network Encryption Level

Hosts at external connections use on time passwords and VPNs for tunneling into the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

network. The management interface to the hosts will use Secured Shell (SSH) and Secure Sockets Layer (SSL) as an added layer of protection for router management.

5.3.3 Network Operator versus Manager Trust Level

Due to the complexity of router configuration setups in a mobile, ever changing environment and the need to provide one source for network management, the router, firewall, and NIDS setups will be provided by the IA manager to the network managers for implementation.

There will be general-purpose default configurations for the router firewall feature set, firewalls, and NIDS provided internally to the boot-up databases. These defaults provide the initial protection and detection configurations and ease the amount of configuration that the IA manager must perform on a recurring basis.

5.4 External Interface Requirements

All connections external to the GIAC Enterprises Network must obtain the approval of the System Administrator prior to opening the connection. If a connection is found that is not approved it will immediately be disconnected and the operator's computer and/or network equipment will be seized until it is completely inspected for compromise.

6. IA Architecture Description

GIAC Enterprises network IA implementation will consist of four IA layers, each consisting of a different configuration of firewalls, Intrusion Detection System (IDS), access controls, and/or host-based IA features to provide a rugged defense-in-depth protection. Physical security and proper storage of configuration databases are applicable throughout each layer with IA management being key to the security and functionality of the network.

6.1 External Filtering Router

The Cisco 3600 Router will provide routing between the external interfaces and the firewall. The only security features used at this level are some basic ACLs to stop some of the most blatant attacks. Appendix B contains the specific default access list settings. These basic ACLs are used to minimize the risk of IP spoofing and to minimize the ability to login to and mange this external router.

6.2 External Firewall and Screen Network Information Assurance Features

The strongest IA layer will be on connections external to the local GIAC environment. These connections will be secured using a FW. This layer will also provide VPN server, network servers, and a NIDS. This strong approach is used to prevent external operator access into the GIAC network unless the internal operators initiate the contacts or knowingly allow them in, as well as to ensure that the internal operators do not inadvertently pass traffic out of their network.

6.2.1 External Firewall Services

The FW firewall will be configured to allow only necessary traffic into the backbone

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

network from external sources. The screened network will provide for DNS, web, and mail servers.
Some of the defaults filters incorporated into the firewall include the following:

- block incoming echo ping requests,
- allow web service out of the network to anywhere,
- allow external web requests into the screened web server,
- allow DNS requests to the screened DNS server,
- allow DNS requests out,
- allow mail out,
- allow incoming mail into the screened web server,
- allow file sharing through VPN tunnels,
- allow video teleconferences through VPN tunnels,
- allow any ftp requests out,
- allow incoming ftp requests to the ftp server,
- allow the IA manager and the network manager to manage the external router, screened servers, and protection devices.

Appendix C contains the specific firewall settings.

6.2.2 External NIDS Services

The NIDS will contain the most recent full attack signature list and attack scenarios. Updates of the latest attack signatures and scenarios will be added to the NIDS as they are released by the vendor. The NIDS is placed behind the FW for the initial deployment to allow the managers to become familiar with the attacks, but not to be overwhelmed with false positives. The NIDS will be able to be configured outside of the firewall and behind the external router if and when the management deems necessary.

6.2.3 VPN Server

The VPN server encrypts data for tunneling through the Internet to remote users and partners.

6.3 Backbone Network Information Assurance Features

The backbone network IA features will be less stringent than that of the External FW. A Context-Based Access Control (CBAC) firewall and IDS are embedded on the Cisco 7206 router. The firewall and IDS functionality are part of the Cisco Firewall Feature Set (FFS) which is built into Cisco's Internetwork Operating System (IOS).

CBAC will provide:

- a layer of defense in depth,
- allowing departments to restrict other departments access to their workstations and servers.

The IDS will be more narrowly focused, configured to detect only the most likely attacks. NetRanger Director will be hosted on the management workstation(s) to monitor the routers.

The backbone provides internal Domain Name Server (DNS)/Dynamic Host

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Configuration Protocol (DHCP), mail, other servers, as well as development and management capabilities. This approach provides IA to the operator level, while having a fairly open routing scheme between subnets.

6.3.1 Backbone Network Firewall Services

The CBAC firewall at ANCS and ASEN routers will be configured to only block unauthorized intra-network traffic (tandem router traffic only, not ATM-only traffic). CBAC will also be used to ensure that small services have global timeouts implemented on them to ensure that those services are not being misused.Appendix D contains the specific firewall settings.

6.3.2 Backbone Network IDS Services

Updates to which attack signatures are implemented will be handled by IA management personnel as those updates become available from the vendor.

6.4 Host Level Information Assurance Features

Host level IA mechanisms will be implemented at the workstation level. C2 Protect Tools will be integrated on all workstations providing:

- Secure protocols can be used to encrypt traffic sessions via an authorized encryption mechanism (i.e., SSH, SSL).
- Identification and authentication will be accomplished via passwords to allow access to the host and network and for certain privilege levels for host and network control.
- All workstations will have a warning banner on them to ensure a user is aware of the consequences of improperly using the workstation or information contained therein.
- All workstations will have a password that has a minimum of 8 letters and has at least 2 non-letter characters. Passwords will be changed at a minimum every 90 days, and can not be reused for at least 3 iterations.
- Only servers will allow file sharing.
- All workstations that connect up to the GIAC network (whether company owned or private) will undergo a security screen to ensure that all non-essential services are not enabled.

The UNIX workstations will be provided with software packages to include the following: Transmission Control Protocol (TCP) Wrapper, Tripwire, Swatch, SSH, a password checker, and anti-virus software.

The Windows New Technology (NT) servers and workstations will include anti-virus software and will use the Microsoft Security Configuration Manager (SCM) software package to set policies for user accounts, user rights, auditing, event logs, password parameters, etc.

7. Information Assurance Management

There will be an IA management team made up of the overall system administrator, security manager, and network administrator. IA manager will determine the IA implementation plan and distribute the necessary information to the network managers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Two identically configured management workstations (MWs) will configure/reconfigure, monitor, and manage the ISS Real Secure NIDS, Eagle Raptor Firewall, Cisco CBAC FFS/IDS products, and VPN products locally and at any remote locations.

7.1 IA Management Plan

The MW will be connected to the IT subnet and will be used to manage all network and host security assets within the network. Using the MWs, the IA manager will be capable of the following:

a. Provide IA policy updates via Microsoft Word documents
b. Configure the preferences of the C2 Protect tools for the hosts
c. Configure/reconfigure and monitor the IDS and firewall within the network routers
d. Configure/reconfigure and monitor the NIDS and firewall within the Screened Network
f. Monitor host security events
g. Shut down any of the above devices in response to an attack
h. Perform vulnerability scans of the network (with separate laptop)
i. Download and provide virus file and IDS file updates for retrieval
j. Collect event/incident reports and send to the Computer Emergency Response Team (CERT).
k. Update the VPN server with information as it changes with the growing and changing demands of the company.

7.1.1 IA Management - Attack Notification and Response

The IA manager will be the end authority for attack response, and will report the attack information to network authorities upon resolution.

The MW will be the central collection point for all NIDS alerts. The primary IA manager may pass this information to the subnetwork managers who may then determine what action to perform, such as shutting down operators, ports, or services. The primary and network managers may coordinate with each other in determining the attack response.

7.1.2 Primary IA Management - IA Software Updates

The IA managers will be the source of datafile updates for C2 Protect tools and will ensure that updates are sent to the subnetwork managers for implementation in a timely manner. The IA managers will install them in the server workstations. This activity should occur primarily during non-peak

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.2 Network Management

The network managers will be part of the management team and exchange information with the IA managers on the status of network equipment, including the switches and workstations.

7.2.1 Network Management Plan

The network manager's responsibilities include providing IP addresses for the routers, firewall, and IDS and C2 Protect Tool configuration updates from the IA manager to download to their equipment.

The network managers will determine the required logical network diagram for the external network connections, what type of connections they are and which will be connected to the FW. The network manager ensures that people preparing work remotely know how they can reconnect with the proper configuration.

7.2.2 Network Management - Attack Notification and Response

The network manager often works with the IA managers to determine a network attack response.

7.2.3 Network IA Management - IA Software Updates

The network managers will receive datafile updates for C2 Protect tools from the IA managers and distribute them to each router for installation as soon as possible. This activity should occur primarily during non-peak hours.

8. Areas of Responsibility

8.1 Company CEO

The CEO is responsible for adapting the IA Policy to the needs of the current network requirements, ensuring that all operators and managers are briefed on the IA Policy and adhere to the Acceptable Use Guidelines in Section 0, and enforcing the IA Policy.

8.2 Information Assurance Managers

The IA managers are responsible for advising the commander on recommended IA Policy updates; determining and distributing the IA network plan for all layers; downloading and distributing the appropriate FW firewall and NIDS, FFS, ACL, IDS, and C2 Protect tools configurations; monitoring the NIDS events and reconfiguring the network as necessary; downloading and distributing the current COTS NIDS attack files, virus files, and COTS software security patches to the relevant equipment; knowing and adhering to the Acceptable Use Guidelines (see Section 9).

8.3 Internal Network Operators

Operators are responsible for monitoring the network equipment for signs of intentional/unintentional failures at the individual shelters, assisting in the configuration of the network equipment, knowing and adhering to the Acceptable Use Guidelines, and maintaining password integrity.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8.4 System Administrators and System Security managers

The system administrator is a trusted, highly privileged and skilled operator, who oversees the operation of the GIAC network systems and configures the GIAC network system components. Additional responsibilities include the following: creating and maintaining the access control databases, using all of the operating system commands, and having the authority to make emergency repairs to the system. Since the GIAC network connects to the Internet, the GIAC network system administrator must also work closely with the system administrators at the ISPs to assure proper configurations.

The ISSM is responsible for all network security matters and procedures required by the CEO and shareholders. The GIAC network managers assesses the GIAC with the assistance of the system administrator. The ISSO will (a) ensure compliance with all DAA requirements and (b) investigate anomalous or suspicious behavior.

8.5 Network Subscribers

All GIAC network operators are responsible for knowing what data can be transmitted to whom, using the appropriate IA measures for data transmission, knowing and adhering to the Acceptable Use Guidelines, and maintaining password integrity.

9. Acceptable Use Guidelines

All the Information Systems (ISs) in the GIAC are company assets; therefore, they are subject company policies and regulations. Limited personal use of company telephones, e-mail systems, and Internet communications is permitted on the ISs, so long as such use is on a not-to-interfere basis and is not-for-improper purposes.

The company network and IA managers have the right to monitor activities on any connected IS.

9.1 Additional Guidance

Unacceptable use of the GIAC network may include, but is not limited to, "spoofing" of IP addresses, inappropriate Web surfing, or playing network games. Also, network operators may not load any unauthorized software.

9.2 Enforcement for Misuse

A malicious attack on the network including, but not limited to, denial-of-service attacks, theft of data, and data corruption is punishable under local and Federal laws.

Anyone found violating the Acceptable Use Guidelines will be reprimanded accordingly by their local manager. If the misuse continues it could lead to cause for termination of employment.

Appendix A. Acronym List

ATM Asynchronous Transfer Mode

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

C2	Command and Control
CBAC	Context Based Access Control
COTS	Commercial Off-the-Shelf
CP	Capability Package
DHCP	Dynamic Host Configuration Protocol
FFS	Firewall Feature Set
FTP	File Transport Protocol
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance
IDS	Intrusion Detection System
IOS	Internetwork Operating System
IP	Internet Protocol
IPSec	IP Security
IS	Information System
ISS	Information Systems Security
ISSM	Information System Security Manager
LAN	Local Area Network
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NT	New Technology
RFC	Request for Comment
SCM	Security Configuration Manager
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SPI	Security Profile Inspector
SSH	Secure Shell
SSL	Secure Socket Layer
FW	Firewall
TCP	Transmission Control Protocol
VPN	Virtual Private Network

Appendix B External Router Configuration and Access Controls

```
This is an entire default external router configuration.

version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname GIACrtr
!
enable secret 5 $1$aEej$pLdDt7eCSW9uwqCawljbW/
!
username giacmgr privilege 15 password 7 141A13050D032F7A76
username giacops password 7 02000557080901701E
!
memory-size iomem 15
ip subnet-zero
no ip source-route
no ip finger
no ip domain-lookup
no snmp
no service tcp-small-servers
no service udp-small-servers
no ip bootp

ip audit notify log
ip audit po max-events 100
!
interface Ethernet0/0
 description GIAC router exterior interface to ISP1
 ip address 168.34.107.57 255.255.255.248
 no ip directed-broadcast
 no shutdown
 no cdp enable
 no ip unreachables
 ip access-group 40 in
 !access list 40 filters incoming traffic

interface Ethernet0/1
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
 description GIAC router exterior interface to ISP2
 ip address 168.34.107.49 255.255.255.252
 no ip directed-broadcast
 no shutdown
 no cdp enable
 no ip unreachables
 ip access-group 40 in
 !access list 40 filters incoming traffic
!
interface Ethernet0/2
 description GIAC router interior interface to FW
 ip address 168.34.107.53 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no shutdown
 no cdp enable
 ip access-group 50 in
!access list 50 filters FDD traffic exiting the GIAC network to prevent
!source IPspoofing in accordance with RFC 2267.
!
autonomous-system 4087
!
ip classless
ip route 168.34.0.0 255.255.0.0 168.34.107.50 permanent
no ip http server
!
no cdp run

access-list 40 deny 192.168.0.0 0.0.255.255
access-list 40 deny 172.16.0.0 0.15.255.255
access-list 40 deny 10.0.0.0 0.255.255.255
access-list 40 permit any !Could specify ranges if desired
access-list 40 deny all

!Access list 40 is applied against the perimeter router's outside
!interface.

access-list 50 permit 168.34.0.0 0.0.255.255
access-list 50 deny all

!Access list 50 is applied against the perimeter router's inside
!interface and allows only GIAC traffic to pass.  This prevents IP
!spoofing in accordance with RFC 2267.
!
access-list 15 permit 168.34.0.0 0.0.255.255 !IA Manager
access-list 15 deny all
!
! Access list 15 is applied against VTY lines 0-4 to limit TELNET
! access of the GIAC routers to the IA Manager only.

line con 0

 transport input none
 speed 115200
 login local
 logging synchronus
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
line aux 0
 !This interface is not utilized

line vty 0 4
 access-class 15 in
! Only IA MANAGER shall have authorization to access the perimeter
!router via TELNET Access list 15 blocks all TELNET connections to the
!VTY lines 0-4 at the perimeter router except those from the from the
!IA MANAGER.

no scheduler allocate
end
```

Appendix C Raptor Configuration Rules

Provide below is only the Rules Report for the basic firewall. It does not include the rest of the firewall configuration that is necessary for the foundation of the rules. The text version is not nearly as easy to read as the GUI version; however the reader can at least get the idea of what Raptor Firewall Rules entail.

Rules Report

```
       Rule ID: 12
       Description: Fortune VideoTelecons
       Services: h323*
       Service Limits:  h323
       Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
       Advanced Services:
       Application Scanning: 1
       In Via: Any VPN
       Out Via: El90x2 (internal interface)
       Source: Fortunes
       Destination: Fortunes
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold: 3
       Alert 15 minutes threshold: 5
       Alert Hour threshold: 10
       Alert Day threshold: 25
       Alert Week threshold: 100
       Log Normal Activity: 1
       Application Data Scanning: 1
==================================================
       Rule ID: 10
       Description: allow hosts on inside network to send
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
mail to all systems
       Services: smtp*
       Service Limits:  smtp
       Proxy Limits:  smtp.rlimit.soft: smtp.rlimit.hard:
smtp.hide: smtp.read: smtp.check_orig_domain:0
smtp.no_srcroutes:0 smtp.no_telnet:0 smtp.loose_recip:0
smtp.loose_orig:0
       Advanced Services:
       Application Scanning: 0
       In Via: El90x3 (Screened interface)
       Out Via: Any
       Source: Universe*
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 0
==================================================
       Rule ID: 2
       Description: Denying internal access to FW
       Services: all*
       Service Limits:  .all-protocols
       Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
       Advanced Services:
       Application Scanning: 1
       In Via: Any
       Out Via: Any
       Source: Universe*
       Destination: Firewall
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 1
================================================
       Rule ID: 1
       Description: Manage the FW
       Services: all*
       Service Limits:  .all-protocols
       Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
       Advanced Services:
       Application Scanning: 1
       In Via: El90x2
       Out Via: El90x2
       Source: IAMGR
       Destination: FWInternal
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 1
================================================
       Rule ID: 3
       Description: External Router Management
       Services: ftp* ping* telnet*
       Service Limits:  ftp telnet ping
       Proxy Limits:  ftp-disallow-gets:0 ftp-disallow-
puts:0
       Advanced Services:
       Application Scanning: 1
       In Via: El90x2
       Out Via: El90x1 (external interface)
       Source: IAMGR
       Destination: Universe*
       Time:
       Authentication:
       User:
```


© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 1
================================================
       Rule ID: 4
       Description: allow hosts on inside network to send
mail to all systems
       Services: smtp*
       Service Limits:  smtp
       Proxy Limits:  smtp.rlimit.soft: smtp.rlimit.hard:
smtp.hide: smtp.read: smtp.check_orig_domain:0
smtp.no_srcroutes:0 smtp.no_telnet:0 smtp.loose_recip:0
smtp.loose_orig:0
       Advanced Services:
       Application Scanning: 0
       In Via: El90x2
       Out Via: Any
       Source: Universe*
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 0
================================================
       Rule ID: 5
       Description: allow hosts on inside network to send
mail to all systems
       Services: smtp*
       Service Limits:  smtp
       Proxy Limits:  smtp.rlimit.soft: smtp.rlimit.hard:
```


© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
smtp.hide: smtp.read: smtp.check_orig_domain:0
smtp.no_srcroutes:0 smtp.no_telnet:0 smtp.loose_recip:0
smtp.loose_orig:0
       Advanced Services:
       Application Scanning: 0
       In Via: El90x3
       Out Via: Any
       Source: Universe*
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 0
==================================================
       Rule ID: 6
       Description: Allow all internal systems to access
HTTP and FTP services
       Services: ftp* http*
       Service Limits:  ftp http http-allurl http-allext
       Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
http:1 http-https:0 http-tunnel:any http-tunnel.list: http-
dcom-tunnel:0 http-ftp:0 http-gopher:0 http-finjan:0 http-
allurl:0 http-allext:0 http-proxy: http-proxy.ipaddress:
       Advanced Services:
       Application Scanning: 1
       In Via: El90x2
       Out Via: Any
       Source: Universe*
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 1
================================================
       Rule ID: 7
       Description: Allow all internal systems to access
HTTP and FTP services
       Services: ftp* http*
       Service Limits:  ftp http http-allurl http-allext
       Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
http:1 http-https:0 http-tunnel:any http-tunnel.list: http-
dcom-tunnel:0 http-ftp:0 http-gopher:0 http-finjan:0 http-
allurl:0 http-allext:0 http-proxy: http-proxy.ipaddress:
       Advanced Services:
       Application Scanning: 1
       In Via: El90x3
       Out Via: Any
       Source: Universe*
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 1
================================================
       Rule ID: 8
       Description: Allow all systems to send mail to the
internal mail server
       Services: smtp*
       Service Limits:  smtp
       Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
smtp.rlimit.soft: smtp.rlimit.hard: smtp.hide: smtp.read:
smtp.check_orig_domain:0 smtp.no_srcroutes:0
smtp.no_telnet:0 smtp.loose_recip:0 smtp.loose_orig:0
       Advanced Services:
       Application Scanning: 0
```


© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
       In Via: Any
       Out Via: Any
       Source: Universe*
       Destination: 168.34.107.42
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 0
==================================================
       Rule ID: 9
       Description: Allow internal mail server to send mail
to all systems
       Services: smtp*
       Service Limits:  smtp
       Proxy Limits:  smtp.rlimit.soft: smtp.rlimit.hard:
smtp.hide: smtp.read: smtp.check_orig_domain:0
smtp.no_srcroutes:0 smtp.no_telnet:0 smtp.loose_recip:0
smtp.loose_orig:0
       Advanced Services:
       Application Scanning: 0
       In Via: Any
       Out Via: Any
       Source: 168.34.107.42
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 0
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
================================================
       Rule ID: 11
       Description: allow hosts on inside network to send
mail to all systems
       Services: smtp*
       Service Limits:  smtp
       Proxy Limits:  smtp.rlimit.soft: smtp.rlimit.hard:
smtp.hide: smtp.read: smtp.check_orig_domain:0
smtp.no_srcroutes:0 smtp.no_telnet:0 smtp.loose_recip:0
smtp.loose_orig:0
       Advanced Services:
       Application Scanning: 0
       In Via: El90x2
       Out Via: Any
       Source: Universe*
       Destination: Universe*
       Time:
       Authentication:
       User:
       User:
       Group:
       Group:
       Alert 5 minutes threshold:
       Alert 15 minutes threshold:
       Alert Hour threshold:
       Alert Day threshold:
       Alert Week threshold:
       Log Normal Activity: 1
       Application Data Scanning: 0
================================================
```

Appendix D Internal Router Access Controls

The following examples are the CBAC/FFS/IDS commands that could get implemented through a Cisco router running IOS/FW. This is not the entire internal router configuration, as that would take up too many pages of this document and this is not a routing paper. This is an example of how complex internal "permissive" ACLs can become when all of the pieces are implemented. In this example we are not running IPSEC as the internal network is trusted and VPNs are used for external "trusted" connections.

```
! XXXXXXXX  INTRUSION DETECTION SYSTEMS GLOBAL CONFIGURATIONXXXXXXXXXXX
! MAX # OF HALF OPEN SESSION WILL CAUSE ROUTER TO STOP DELETING
ip inspect max-incomplete low 1000
! MAX # OF HALF OPEN SESSION WILL CAUSE ROUTER TO START DELETING
ip inspect max-incomplete high 1200
! MAX RATE OF HALF OPEN SESSION WILL CAUSE ROUTER TO STOP DELETING
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
ip inspect one-minute low 5000
! MAX RATE OF HALF OPEN SESSION WILL CAUSE ROUTER TO START DELETING
ip inspect one-minute high 10000
! MANAGED TIME AFTER NO SESSION ACTIVITY [UDP]
ip inspect udp idle-time 200
! MANAGED TIME OF DNS LOOKUP AFTER NO ACTIVITY
ip inspect dns-timeout 20
! MANAGED TIME AFTER NO SESSION ACTIVITY [TCP]
ip inspect tcp idle-time 2000
! MANAGED TIME AFTER FIREWALL DETECTS A FIN-EXCHANGE
ip inspect tcp finwait-time 10
! WAITING TIME TO REACH ESTABLISHED STATE BEFORE DROPPING THE SESSION
ip inspect tcp synwait-time 40
! # OF HALF OPEN SESSIONS WITH SAME DESTINATION IP CAUSES SESSIONS
DROPPED
ip inspect tcp max-incomplete host 60 block-time 30
!
!  XXXXXXXXXXXXXX  INSPECT DEFINITIONs  XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
ip inspect name Inspect_102 fragment maximum 250 timeout 600
ip inspect name Inspect_102 udp
ip inspect name Inspect_102 h323
ip inspect name Inspect_102 ftp
ip inspect name Inspect_102 tftp
ip inspect name Inspect_102 smtp
ip inspect name Inspect_102 http java-list 1 timeout 360
ip inspect name Inspect_103 fragment maximum 250 timeout 600
ip inspect name Inspect_103 tcp
ip inspect name Inspect_103 udp
ip inspect name Inspect_103 h323
ip inspect name Inspect_103 ftp
ip inspect name Inspect_103 tftp
ip inspect name Inspect_103 smtp
ip inspect name Inspect_103 http java-list 1 timeout 360
ip inspect name Inspect_104 fragment maximum 250 timeout 600
ip inspect name Inspect_104 tcp
ip inspect name Inspect_104 udp
ip inspect name Inspect_104 h323
ip inspect name Inspect_104 ftp
ip inspect name Inspect_104 tftp
ip inspect name Inspect_104 smtp
ip inspect name Inspect_104 http java-list 1 timeout 360

! XXXXXXXXXXXXXX  DIRECTOR INTERFACE XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
ip audit notify nr-director
ip audit notify log
ip audit po max-events 100
! ip audit po remote hostid TEAMLABEL orgid 1 rmtaddress  IP FOR WSP
localaddress IP FOR FA0/0 port 45000 preference 1 timeout 5 application
director
ip audit po remote hostid 25360 orgid 1 rmtaddress 168.033.053.2
localaddress 168.033.053.001 port 45000 preference 1 timeout 5
application director
ip audit po local hostid 160 orgid 1
ip audit name AUDIT.1 info action alarm
ip audit name AUDIT.1 attack action alarm
process-max-time 200
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
! XXXXXXXXXXXXXXXXXXXXXX  FIREWALL ACCESS LIST  DEFINITIONS XXXXXXXXXXX
!
! XXXXXXXXXXXXXX ACCESS LIST 2  XXXXXXXXXXXXXXXXXXXXXXXXXXX
! INTENDED FOR APPLICATION ON THE FA0/0 INTERFACE
access-list 102 permit ip 10.0.0.0 0.255.255.255 any
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any established
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 45000
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq snmp
access-list 102 permit icmp 168.0.0.0 0.63.255.255 any
access-list 102 permit igmp 168.0.0.0 0.63.255.255 any
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 427
access-list 102 permit udp 168.0.0.0 0.63.255.255 eq 427 any
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 7640
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 7642
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 7648
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 7648
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 24032
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 1503
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any range 1718 1720
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 1710
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 1710
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 1812
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 1813
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 56800
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 1424
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 1414
access-list 102 permit udp 168.0.0.0 0.63.255.255 any range 1718 1720
access-list 102 permit udp 168.0.0.0 0.63.255.255 any range 53002 53009
access-list 102 permit udp 168.0.0.0 0.63.255.255 any range 53016 53019
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 5050
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 6000
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 7000
access-list 102 permit ospf 168.0.0.0 0.63.255.255 any
access-list 102 permit pim 168.0.0.0 0.63.255.255 any
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq bgp
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq domain
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq domain
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq tftp
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq snmptrap
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq www
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq syslog
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq smtp
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any range 416 418
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 901
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 2998
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 61161
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 22
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 63
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 69
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any range 103 104
! access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 162
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any range 381 383
access-list 102 permit udp 168.0.0.0 0.63.255.255 any range 381 383
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 389
access-list 102 permit udp         168.0.0.0 0.63.255.255 any eq 389
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq pim-auto-rp
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 639
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 647
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any range 989 990
access-list 102 permit udp 168.0.0.0 0.63.255.255 any range 989 990
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 992
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 992
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any range 1095 1096
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 2240
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 2468
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 2490
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 2643
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 3025
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 3025
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 3030
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 3030
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 5000
! access-list 102 permit tcp 10.10.10.2 0.0.0.0 168.033.053.2 0.0.0.0
eq 5000
 access-list 102 permit tcp 168.0.0.0 0.63.255.255 10.10.10.0 0.0.0.255
eq 5000
 access-list 102 permit tcp 10.10.10.0 0.0.0.255 168.0.0.0 0.63.255.255
eq 5000
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 5001
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 5757
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 7001
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 40000
access-list 102 permit ip host 168.033.053.2 host 168.033.053.001
access-list 102 permit ip host 168.033.053.001 host 168.033.053.2
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq 3001
access-list 102 permit udp 168.0.0.0 0.63.255.255 any eq 3001
access-list 102 permit ip host 168.033.053.4 any
access-list 102 permit ip any host 168.033.053.4
access-list 102 permit tcp 168.0.0.0 0.63.255.255 any eq telnet
access-list 102 permit udp  168.0.0.0 0.63.255.255 any eq 1757
access-list 102 permit tcp  168.0.0.0 0.63.255.255 any eq 1757
access-list 102 permit udp  168.0.0.0 0.63.255.255 any eq 1552
access-list 102 permit udp  168.0.0.0 0.63.255.255 any eq 110
access-list 102 permit udp  168.0.0.0 0.63.255.255 any eq 5402
!
! access-list 110 to 150 would be implemented on the incoming internal
! ethernet routes to allow specific users into other departmental
! subnetworks. All of 10.10.50 would be allowed as they are the
! management network
access-list 110 permit tcp any any established
access-list 110 permit ip 10.10.50.0 0.0.255.255 any any
access-list 110 permit ip any host 10.10.10.2 any
!

! TELNET ACCESS LIST
access-list 15 permit 10.10.50.2 0.0.0.255
!
! XXXXXXXXXXXXXXXXXXXXXXXX BANNER WARNING
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
banner motd  ^ ATTENTION!
THIS IS A GIAC Enterprises         COMPUTER SYSTEM. BEFORE PROCESSING
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SENSITIVE INFORMATION, CHECK THE SECURITY POLICY. DO NOT PROCESS, STORE OR TRANSMIT SENSITIVE INFORMATION IF IT IS NOT AUTHORIZED FOR THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED GIAC USE. GIAC COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS GIAC COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS GIAC COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.
!

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.