PRACTICAL – FIREWALL AND PERIMETER SECURITY
SANS NETWORK SECURITY 2000 – MONTEREY, CA

CHRIS ROBERTSON

PERIMETER SECURITY FOR GIAC ENTERPRISES

SECURITY AND AUDIT GUIDELINES

TABLE OF CONTENTS

ASSUMPTIONS

The following assumptions have been made in the preparation of this document.

- There are no GIAC Enterprises branch offices
- Physical security of the servers/routers/firewalls is assumed to be adequately covered and is beyond the scope of this document.
- There is only a single data center (has to do with serial cable lengths).
- There are no monetary limitations when deciding on software or hardware.

Notes:

- These guidelines have not been fully tested due to a lack of resources on my part (namely the routers and enough machines to simulate the redundant firewall with a server behind it.)

SECURITY GOALS

The goal of this security definition is to provide a framework that ensures compliance with the VISA Ten Commandments and the SANS Top Ten list while at no time impacts a zero-downtime policy. These definitions should also provide a benchmark against which to measure network security at "a moment in time" and an ongoing manner.

SECURITY POLICY

BASE POLICY

- Permit only authorized traffic in and out of GIAC Enterprises networks.
- Monitor all choke points for possible intrusions.
- Automated monitoring of all servers for intrusion and unauthorized changes (Tripwire).
- All banners should not display any version information.
- All banners should display a warning that unauthorized access is prohibited.
- All VPNs are to terminate at a firewalling device and have a unique restrictive access policy.
- All authentication will be encrypted.
- Require all passwords to be changed at least every 90 days. Passwords are never to be distributed electronically.
- Control all dangerous traffic at each choke point. Exceptions to be made as necessary for required services. Dangerous traffic includes:
    - As defined by the SANS Top Ten list plus:
    - Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
    - Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
    - RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
    - NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)
    - X Windows -- 6000/tcp through 6255/tcp
    - Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
    - Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
    - Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
    - "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
    - Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
    - ICMP-- block incoming echo request (ping and Windows traceroute), block-outgoing echo replies, time exceeded, and unreachable messages.

VISA TEN COMMANDMENT COMPLIANCE

VISA Commandment	Solution
1) Working network firewall	This is addressed at multiple points. All routers filter traffic and FW-A(1&2), FW-C(1&2), and FW-G(1&2) provide host based firewalling. See Firewall Guidelines and Router Configuration.
2) Security patches up-to-date	All systems to have all packages evaluated at least once a week.
3) Encrypt stored data accessible from the Internet	No data is to be stored on any machine accessible from the Internet. All data is stored on back-end server and retrieved at need by the web servers. See Host Security Recommendations.
4) Encrypt data sent across networks	All web traffic is via SSL. All traffic to remote locations is via VPNs. All management and file transfer is via SSHv2. All applications retrieve data via encrypted communication. See VPN Guidelines and Host Security Recommendations.
5) Use and regularly update anti-virus software.	All desktops are managed from one of two centralized Norton AntiVirus (Corporate Edition) servers. One manages the Management Network and the other manages the Corporate Network. All other machines use an equivalent product with centralized management if available (McAffee, F-Prot, etc.). If centralized management is not available virus definitions are to be updated weekly.
6) Restrict access to data by business "need to know."	All users to be granted only the rights required for them to perform their job. All rights are managed from a central location (Netware Directory Services) to prevent errors. Servers that do not connect to NDS (Public Services and firewalls) have a restricted user base and all activity is logged to central syslog servers. See Host Security Recommendations, Router Configuration, and Firewall Configuration.
7) Assign unique IDs to each person with computer access to data	All users have unique logins to a centralized user database (Netware Directory Services) and permissions based on this login. Note: One tree would manage the Corporate Network while a separate tree would manage the Management Network.
8) Track access to data by unique ID.	All access to sensitive data is logged to multiple syslog servers.
9) Don't use vendor-supplied defaults for passwords	All administrative/root/SNMP passwords are to be changed at a minimum of every 90 days. New passwords are never to be distributed electronically. Passwords are to be 8 characters minimum and contain lower, uppercase and non-alpha characters.
10) Regularly test security	Daily automated Nmap scans and Tripwire scans. Regularly scheduled and unscheduled full network vulnerability testing (Nessus/Sara/Saint/etc). Each scan performed with more than one package. See Security Audit Guidelines.

NETWORK DEFINITION

THE NETWORK IS DIVIDED INTO 7 REGIONS BASED ON USE AND NEEDED SECURITY. THESE NETWORK REGIONS ARE:

REGION A – PUBLIC SERVICES

Overview – This region houses all servers (primarily web) who communicate with untrusted computers, particularly e-com shoppers.

Addressing – Network IP range 1.2.1.0/24, publicly addressable.

Access – This region connects to backend services via FW-A1/2 for data and management. Management is accomplished by administrators connecting to a dedicated management station in Backend Services and from there creating a second SSH connection to the server in Public Services. All servers in Public Services (firewalls included) are configured to accept SSH connections from only the management station.. All other connections are made via the DMZ including all http/SSL access.

REGION B – BACKEND SERVICES

Overview – This region houses all servers that provide services to other GIAC Enterprises servers and are never accessed directly (except for DB queries, etc.) aside from the management network.

Addressing – Network IP range 10.2.2.0/24, private address space. This address space is only available via the firewalls. All routers are configured to deny and traffic to or from all RFC 1918 address space.

Access – this region is access by Public Services for data and management via FW-A1/2, by the Management Network for maintenance, development, and management via FW-C1/2, and by Internal Services for data via FW-G1/2.

REGION C – MANAGEMENT NETWORK

Overview – This region exists for the sole purpose of managing secure computers on the network. These are not general-purpose machines (ie- no MS Office installed). The employees using these machines are assumed to have a second computer that is part of the standard corporate network.

Addressing – Network IP range 10.2.3.0/24, publicly addressable. This region also runs IPX for file and print services (NetWare). IPX network 10230.

Access – This region has access to Backend Services and limited access to the Internet. Note that this region has no access to Internal Services. Any employees who need access to both Internal Services and Backend Services must have two computers.

REGION D – DMZ

Overview – This region houses the border and internal routers connecting the various regions.

Addressing – Network IP range 1.2.4.0/24. While this region is allocated a full class C network, in reality it is segmented into 9 /30 networks for the direct connections between routers.

Access – No regions have access to the devices in the DMZ. All management is done via a console server (direct serial connect to the routers) located in Backend Services. All routers are configured to deny any attempts at communication with ACLs (see Router Configuration). See Perimeter Security for filtering details.

REGION E – INTERNAL SERVICES

Overview – This region houses all servers that provide services to the corporate and trusted (VPN/Tunnel) partner networks. This includes all application servers that communication with server in Region B for data and file servers for the Corporate network.

Addressing – Network IP range 10.20.50.0/24. This address space is only available via FW-G1/2. All routers are configured to deny and traffic to or from all RFC 1918 address space. This region also uses IPX for file and print services (NetWare). IPX network 102050. IPX is routed to Corporate Network only via a secondary router running IPX ACLs.

Access – Internal Services is accessible from External Services and the Corporate network. In addition, Internal Services has access to Backend Services.

REGION F – EXTERNAL SERVICES

Overview – This region's sole purpose is to serve as the termination point for VPNs to partner networks. Creating this as its own region is driven primarily by ease of upgrading or increasing the number and/or type of devices terminating the VPNs.

Addressing – Network IP range 10.20.60.0/24. This address space can communicate only with Internal Services via FW-G1/2.

Access – External partners via VPNs. VPNs are to use 3DES encryption as a minimum. All VPN terminating devices deny all traffic to other VPNs allowing only traffic to Internal Services. Access from Backend Services (specifically the management station) is allowed via SSH only for managing the VPN terminators.

REGION G – CORPORATE NETWORK

Overview – This region houses the bulk of the network and all desktop computers (except those that are part of the management network). This region is assumed to have sub-areas that may or may not have secondary internal firewalls. NO CRITICAL OR SENSITIVE DATA IS TO BE STORED IN THIS REGION.

Addressing – Network IP range 1.2.8.0/21. All clients are to use DHCP for IP address assignment. This region also uses IPX for file and print services (NetWare). IPX network 1280 (might be subnetted depending on performance).

Access – IPX is routed to Internal services only via a secondary router running IPX ACLs. This region has access to Internal Services (IP/IPX, filtered) via FW-G1/2 (IP) and IR-04 (IPX) and to the DMZ/Internet via FW-G1/2.

GENERAL NOTES FOR ALL REGIONS

- All regions are fully switched to minimize the risk data being sniffed in transit. Regions do not share switches (no VLANs between regions).
- All managed switches are considered critical systems where their (READ-ONLY) SNMP community is the password. If at all possible SNMP is to be disabled completely.
- Region D consists solely of point-to-point Ethernet links between routers (crossover cables).

PERIMETER SECURITY DEFINITION

OVERVIEW

The perimeter security is defined as securing the interaction between network regions, including the Internet. To implement a secure and robust environment 6 filter routers and 3 firewalls (with fail-over to dedicated machines) are used to filter and monitor network traffic. A brief description of each device and then allowed traffic at each choke point follows:

ROUTER DETAIL

BR-A: This router serves as one of two ingress/egress points to GIAC Enterprises networks. Filtering is performed at this point to deny all traffic not destined to or originating from GIAC networks. RFC 1918 and localhost addressing is also blocked. BGP updates are limited to the upstream and other GIAC border router. In addition all dangerous services are blocked from any source to any destination.

BR-B: This router serves as one of two ingress/egress points to GIAC Enterprises networks. Filtering is performed at this point to deny all traffic not destined to or originating from GIAC networks. RFC 1918 and localhost addressing is also blocked. BGP updates are limited to the upstream and other GIAC border router. In addition all dangerous services are blocked from any source to any destination.

IR-01: This router serves as the ingress/egress point to Public Services. IR-01 filters all traffic not destined for or originating from 1.2.1.0/24. IR-01 also limits the ports that are available (see definition below for details) and logs attempted access to deny ports. All dangerous services are blocked from any source to any destination.

IR-02: This router serves as the ingress/egress point to the Management Network. IR-02 filers all traffic not destined for or originating from 1.2.3.0/24. All dangerous services are blocked from any source to any destination.

IR-03: This router serves as the ingress/egress point to Internal Services and External Services. All dangerous services are blocked from any source to any destination.

IR-04: This router routes IPX ONLY between the Corporate Network and Internal Services. This router does not physically connect to any other regions. Note-all dangerous services are not blocked at this router as they are IP based services and this router does not route any IP traffic.

VPN/REMOTE ACCESS

Partner VPNs: Partner VPNs are not mandated by platform, instead they are mandated by encryption. 3DES is the absolute minimum for any semi-permanent or permanent tunnel. Additionally all partners who have VPNs to GIAC Enterprises are required to limit access to the VPN on a user-by-user basis and make this information available to GIAC Enterprises upon request. All partners who have VPNs to GIAC Enterprises are required to show proof of adequate perimeter and internal security. Adequate proof takes two forms, the first is a network vulnerability assessment performed by GIAC computer security personnel, the second is a network vulnerability assessment performed by an agreed upon third party. These assessments must be performed at least once per year. Failure to demonstrate proof of adequate network security shall result in the termination of the VPN to the partner's location(s).

Employee VPNs: Employees on the road shall employee a VPN client that enforces a "split-horizon" (such as Checkpoint). All user authentications at the VPN termination are against the NDS user base. All machines that connect via this method are required to have anti-virus software installed and have the definitions regularly updated. This is to be managed either out of a central NAV server or by a product such as LANDesk that automatically updates the virus definitions (and the anti-virus software) when the machine attaches to the network.

Dial-up Access: Dial-up access does not inherently provide any access to GIAC network resources. All machines that connect via dial-up are also required employ a VPN client as described above. Dial-up authentication is also verified against the NDS user base.

FIREWALL DETAIL

FW-A1: This firewall controls access to the Public Services network region and is primarily concerned with web traffic though the mail gateway and public DNS servers also reside in this region. This firewall also allows access from the Public Services region to the Backend Services region.

FW-A2: This is the fail-over for FW-A1. Up until the point that FW-A1 fails this box will function as an intrusion detection system and not route or firewall at the choke point.

FW-C1: This firewall controls access to the Management Network. Primary concerns at this choke point are allowing the developers and system administrators enough access to the outside world and the Backend Services network region to do their jobs while not risking the integrity of privileged machines.

FW-C2: This is the fail-over for FW-C1. Up until the point that FW-C1 fails this box will function as an intrusion detection system at the choke point.

FW-G1: This firewall has the most complex rule set as it controls access to, and between, 5 regions. These regions are the Corporate Network, Internal Services, External Services, Backend Services, and the internet/DMZ. This is probably the weakest link the perimeter security architecture due to the complexity, paths of attack, and resources vulnerable with a compromised firewall.

FW-G2: This is the fail-over for FW-G2. Up until the point that FW-G1 fails this box will function as an intrusion detection system and not route or firewall at the choke point.

Note: For host descriptions please see the Host Definition Appendix or the Network Map.

HOST: FW-A1

Interface 1: DMZ
Interface 2: Backend Services
Interface 3: Public Services

ALLOWED COMMUNICATIONS

Origination⇔Destination	**Port/Protocol**
DMZ⇔Public Services	80/tcp (HTTP)
DMZ⇔Public Services	443/tcp (SSL)
DMZ⇔Mail Gateway	25/tcp (SMTP)
DMZ⇔Mail Gateway	110/tcp (POP3)
DMZ⇔Mail Gateway	143/tcp (IMAP)
DMZ⇔Public DNS	53/udp (DNS)
Public Services⇔Backend Services	<db app port #>/tcp
Public Services⇔Backend Services	514/udp (syslog)
Public Services⇔Backend Services	<monitoring port #>/tcp
Public DNS⇔Backend Services	53/udp (DNS)
Public Services⇔Management Station	22/tcp
Backend Services⇔FW-A1	22/tcp

HOST: FW-A2

Interface 1: DMZ
Interface 2: Backend Services
Interface 3: Public Services

ALLOWED COMMUNICATIONS (WHEN IN FAIL-OVER MODE)

Origination⇔Destination	**Port/Protocol**
DMZ⇔Public Services	80/tcp (HTTP)
DMZ⇔Public Services	443/tcp (SSL)
DMZ⇔Mail Gateway	25/tcp (SMTP)
DMZ⇔Mail Gateway	110/tcp (POP3)

DMZ⇔Mail Gateway	143/tcp (IMAP)
DMZ⇔Public DNS Servers	53/udp (DNS)
Public Services⇔Backend Services	<db app port #>/tcp
Public Services⇔Backend Services	<syslog-ng port #>/tcp
Public Services⇔Backend Services	<monitoring port #>/tcp
Public Services⇔Backend Services	53/udp (DNS)
Backend Services⇔FW-A2	22/tcp (SSH)
Public Services⇔Management Network	22/tcp (SSH)

HOST: FW-C1

Interface 1: DMZ
Interface 2: Backend Services
Interface 3: Management Network

ALLOWED COMMUNICATIONS

Origination⇔Destination	**Port/Protocol**
DMZ⇔Management Network	80/tcp established (HTTP)
DMZ⇔Management Network	443/tcp established (SSL)
DMZ⇔Management Network	25/tcp established (SMTP)
DMZ⇔Management Network	110/tcp established (POP3)
DMZ⇔Management Network	143/tcp established (IMAP)
Management Network⇔Backend Services	<db app port #>/tcp
Management Network⇔Backend Services	22/tcp (SSH)
Management Network⇔Backend Services	53/udp (DNS)

HOST: FW-C2

Interface 1: DMZ
Interface 2: Backend Services
Interface 3: Management Network

ALLOWED COMMUNICATIONS (WHEN IN FAIL-OVER MODE)

Origination⇔Destination	**Port/Protocol**
DMZ⇔Management Network	80/tcp established (HTTP)
DMZ⇔Management Network	443/tcp established (SSL)
DMZ⇔Management Network	25/tcp established (SMTP)
DMZ⇔Management Network	114/tcp established (POP3)
DMZ⇔Management Network	145/tcp established (IMAP)
Management Network⇔Backend Services	<db app port #>/tcp
Management Network⇔Backend Services	22/tcp (SSH)
Management Network⇔Backend Services	53/udp (DNS)

HOST: FW-G1

Interface 1: DMZ
Interface 2: Internal Services
Interface 3: External Services
Interface 4: Corporate Network
Interface 5: Backend Services

ALLOWED COMMUNICATIONS

Origination⇔Destination	**Port/Protocol**
DMZ⇔Corporate Network	80/tcp established (HTTP)
DMZ⇔Corporate Network	443/tcp established (SSL)
DMZ⇔Corporate Network	25/tcp established (SMTP)
DMZ⇔Corporate Network	114/tcp established (POP3)
DMZ⇔Corporate Network	145/tcp established (IMAP)
Corporate Network⇔Backend Services	<app port #>/tcp
Corporate Network⇔Backend Services	80/tcp (HTTP)
Corporate Network⇔Backend Services	53/udp (DNS)
Corporate Network⇔Backend Services	443/tcp (SSL)
Internal Services⇔Backend Services	<app port #>/tcp
Internal Services⇔Backend Services	80/tcp (HTTP)
Internal Services⇔Backend Services	53/udp (DNS)
Internal Services⇔Backend Services	443/tcp (SSL)

HOST: FW-G2

Interface 1: DMZ
Interface 2: Internal Services
Interface 3: External Services
Interface 4: Corporate Network
Interface 5: Backend Services

ALLOWED COMMUNICATIONS (WHEN IN FAIL-OVER MODE)

Origination⇔Destination	**Port/Protocol**
DMZ⇔Corporate Network	80/tcp established (HTTP)
DMZ⇔Corporate Network	443/tcp established (SSL)
DMZ⇔Corporate Network	25/tcp established (SMTP)
DMZ⇔Corporate Network	114/tcp established (POP3)
DMZ⇔Corporate Network	145/tcp established (IMAP)
Corporate Network⇔Backend Services	<app port #>/tcp
Corporate Network⇔Backend Services	80/tcp (HTTP)
Corporate Network⇔Backend Services	53/udp (DNS)
Corporate Network⇔Backend Services	443/tcp (SSL)
Internal Services⇔Backend Services	<app port #>/tcp
Internal Services⇔Backend Services	80/tcp (HTTP)
Internal Services⇔Backend Services	53/udp (DNS)
Internal Services⇔Backend Services	443/tcp (SSL)

HOSTS SECURITY RECOMMENDATIONS

All firewalls are I386 machines running Redhat 6.2

Latest patches installed.

IP: Always defragment is set to yes at compile time

inetd only handles NRPEP connections. All other inbound connections are handled by specific daemons.

Tripwire installed on all hosts.

Automated remote monitoring via Netsaint running NRPEP (Netsaint Remote Process Executor, Perl). NRPEP allows for full system monitoring via secure channels.

Full details on the recommend configuration for each host is shown in Host Definitions.

SECURITY AUDIT GUIDELINES

These security audit guidelines are divided into two parts. The first part is the initial assessment to validate the installed security measures. The second part is the ongoing review and measurement of network security.

INITIAL ASSESSMENT-

Initial assessment consists of vulnerability testing of critical hosts with at least two packages. Critical hosts include all firewalls, routers, intrusion detection systems, public servers, backend servers, and VPN terminators. In other words all systems except those in regions C and G (Management and Corporate networks).

This initial assessment should be performed on a region by region basis at off peak hours, Sunday at 2am or so would be recommended. This is due to the fact that some common vulnerabilities can cause the server to halt/hang/abend etc if not properly patched (Note: Since this is the case the system administrators must be available during the assessment). The initial assessment should be done with tools such as Nessus, ISS, Sara, or Saint. Nmap is not an adequate tool for full vulnerability analysis (though it does have other uses discussed later). These tools, again at least 2 of them, should be run initially from inside the network region. Once all systems in the region show that they are secure from inside the network region a comprehension assessment should be done against the region from all other GIAC network regions.

The Initial Assessment phase should be done begin with the most critical region, Public Services. These are the servers that are accessed by the public and are the most likely to have exploitable security holes; hence they pose the greatest risk of compromise. The recommended order for assessment is; Public Services, Backend Services, Corporate Network, Internal Services, External Services, DMZ, and Management Network. These regions are ordered by a combination of likely hood of attack, risk of compromise, and the amount of damage an attack could do.

Initial assessment highlights are on the next page followed by detailed goals and methods.

THE FOLLOWING LIST ARE HIGHLIGHTS OF WHAT THE INITIAL ASSESSMENT SHOULD BE CONCERNED WITH:

1. Unknown/unauthorized services (aka. Why is port 25 open and accepting connections?) All hosts should have a checklist of what ports should be open (both tcp and udp) and what services run on those ports. See Hosts Definitions for a list of services by host.
2. Outdated versions of software. Particularly those with a history of security holes (BIND and Sendmail come to mind). All systems should have a log of installed software (including, at minimum, date, version, reason for upgrade, and installer). Verify this log against any version information that the assessment software is able to detect. Also verify that anti-virus software is installed and virus definitions are up to date. See Hosts Definitions for recommended versions.
3. Unknown/unauthorized CGI/Perl/Java programs on the web servers. If no one knows what the given script/program does it should be removed (again with a system administrator near-by to verify necessary scripts/programs).
4. Verifying and logging all configurations files.
5. Verifying and logging all user accounts.
6. Verifying that encryption is working properly by capturing transmitted data on the wire.
7. Verifying that all intrusion detection systems noticed the scan and alerted the appropriate parties (as configured).
8. Verifying that all fail-over software/systems work properly. This verification should occur at a time where a system failure would cause minimal disruption in services.
9. Verifying remote access security – partner VPNs
10. Verifying remote access security – employee VPNs
11. Verifying dial-up security.

INITIAL ASSESMENT IMPLEMETATION

UNKNOWN OR UNAUTHORIZED SERVICES

GOAL – Verify that only correct and secure services are running.

METHODOLOGY – Make extensive use of port scanners at all hours of the day to verify that only correct services are accepting connections. Set up a sniffer on a shared segment (inserting a hub between the server and the switch) and verify that no traffic is originating from unknown ports.

OUTDATED SOFTWARE

GOAL – Make sure that no old versions of software are running, especially any that have know security issues.

METHODOLOGY – Have system administrators audit all software installed on the system. The administrators must contact the software vendors (their web site is fine) and verify that no newer version exists or show that a newer version introduces a security risk. Base installed software is to be logged with version information and what the application is used for. This database is to be updated anytime a new piece of software is installed. This includes all new packages, upgrades, patches, and scripts (both shell and web).

INITIAL ASSESMENT CONTINUED

UNKNOWN OR UNAUTHORIZED WEB SCRIPTS/PROGRAMS

GOAL – Verify that no security holes exist in software that is used on the system.

METHODOLOGY – Have the system administrator/webmaster verify all web software. This includes all Apache modules. Any software without definitive purpose is to be removed (In other words, no "We were planning on using that in the next version" or "I think so-and-so uses that for something"). All installed web software is to be logged as system software (see item 2). In addition all source is to be stored in a secure manner that eliminates possible version conflict or over-run. CVS is recommended for tracking software versions.

VERIFY AND LOG ALL CONFIGURATION FILES

GOAL – Verify all configuration files.

METHODOLOGY – Have system administrators verify configuration files. Particular files to pay attention to are all start-up scripts, Apache configuration files, and IP-Chains rule sets. All configuration files will be tracked using a concurrent version system such as CVS. The servers will not have access to the CVS repository. All configuration files will be modified on the system administrator's workstation and then transferred to the server.

VERIFY AND LOG ALL USER ACCOUNTS

GOAL – Prevent unauthorized user accounts and permissions

METHODOLOGY – Have system administrators verify all user accounts on all systems (including NDS). User accounts on critical systems should be logged to a secondary database with the user's name, reason for access, level of access, and who created the account. All root/system accounts are to have a random password of at least 12 characters generated and then sealed for emergency use only. This password should be changed at scheduled audits. All of the system passwords for the last year should be stored in a secure, fire-resistant location.

VERIFY ECRYPTION OF TRANSMITTED DATA

GOAL – Verify that all transmitted data is being encrypted properly. This includes SSL traffic, VPNs, and any applications that communication with the backend databases.

METHODOLOGY – Place a sniffer on the network between communicating devices and verify that all traffic is non-legible. Also verify the configuration of the systems/applications at both ends that proper levels of encryption are being performed.

VERIFY IDS IS WORKING PROPERLY

GOAL – Verify that IDSes will alert staff to possible attacks. This can also be used to create a baseline for normal network traffic.

METHODOLOGY – During the entire assessment period verify that all security scans are detected by the IDS system. During periods where assessments are not running create a baseline of "normal" network traffic. Verify that when the IDS detects a possible security breach that it takes the appropriate action. Appropriate actions include logging the event to an external server (via syslog) and alert system administrators/security staff to the possible intrusion. Logging the data to an external server is critical so that secondary analysis programs can synthesize data from multiple IDS and provide a coherent picture.

INITIAL ASSESMENT CONTINUED

VERIFY FIREWALL FAILOVER WORKS PROPERLY

GOAL – Verify that firewalls fail-over properly in the event of a system failure or compromise (detected by Tripwire).

METHODOLOGY – During off-hours physically disconnect one of the ethernet interfaces and verify that the secondary firewall disable the IDS it is running and start routing traffic properly within 10-15 seconds (any longer and something is mis-configured in the Heartbeat software). If this works properly reconnect the interface and verify that the primary system gracefully enters the cluster with the secondary firewalling releasing firewall duties and resuming as an IDS. Make sure to verify both interfaces. Note, the Heartbeat software communicates via a null modem cable plugged into both machines.

VERIFY PARTNER NETWORK SECURITY

GOAL – Verify that GIAC is not vulnerable from a compromised system at a partners network.

METHODOLOGY – Perform network security assessment of partner's network. This assessment should validate the partner's firewalls and access control to the VPN. If it is not possible for GIAC employees to perform the security assessment a third party should be used. In no case should a partner be given access without this assessment.

VERIFY EMPLOYEE VPN SECURITY

GOAL – Verify that employee's are connecting via a VPN client that uses a "split-horizon" on their computer and that the users have anti-virus software installed on their computer with correct virus definitions.

METHODOLOGY – Remove all possible connection except via an appropriate VPN client and wait for the screams of protest… Also attempt to connect to the VPN terminator with an incorrect client version and verify that access is not granted. Verify that usernames are being authenticated against the appropriate account server (NDS). Try connecting with a computer without anti-virus software and outdated software and verify that the software is installed and virus definitions are updated.

VERIFY DIAL-UP SECURITY

GOAL – Verify that no network access is granted with out a VPN client in place. Also verify that proper authentication is happening to establish the dial-up connection.

METHODOLOGY – Attempt to connect with improper user information and verify that no access is granted. Login with proper credentials but with out a VPN client and verify that no network access is available. Verify that only proper network access is granted with the VPN client properly established.

ONGOING ASSESMENTS

Ongoing assessments are broken into three parts, the first is automated checks, the second is scheduled checks and finally unscheduled checks. Automated checks are generally lightweight and require no intervention from a systems administrator to initiate. Scheduled checks consist of periodic known checks against systems done by systems administrators or security personnel. Unscheduled checks are in effect the same as scheduled checks however they are done with out general knowledge (someone should always know when a security audit is going to happen in case of problems).

AUTOMATED CHECKS

The following checks should be considered a minimum for ongoing checks.

Automated Nmap scans-

Goal – Verify that no new services are being run on critical systems.

Methodology – A nightly scan of all critical systems to verify that no new ports are open. New ports can be automatically detected and forwarded to system administrators by doing a diff with the nightly scan and a known good baseline scan. Make sure that all IDS systems are configured to ignore portscans from the host running the Nmap scans. These scans should be run from inside the firewall in each region to eliminate the possibility of a firewall filtering an unauthorized service.

Goal – Verify firewall ruleset.

Methodology – Nightly scans of all firewalls from each region. The scans should target machines that are known to be running services that are to be blocked by the firewall. A good example would be running the scan from inside either External Services or the Corporate Network against the database servers in Backend Services (or any other server for that matter). These scans should again be compared to known good baseline scans and the results automatically emailed to the firewall administrator.

Goal – Verify no dangerous services are running on desktops/workstations.

Methodology – A nightly scan of desktops/workstations for dangerous services that are running. See the Security Policy for a list of dangerous services. Exceptions should be made and recorded for required services (NetBIOS for example). As doing this scan on an entire network would be prohibitive a more efficient solution is to do a ping sweep on the entire network and parse the output of that back into the scan so that only active hosts are scanned. Scans should be done and reported by logical port groupings. For example one scan looks for common web services on port 80/tcp, 443/tcp, 8000/tcp, 8008/tcp, etc. Another scan might look for ftp, telnet, trojans, etc. By scanning the network by port groupings it makes it much easier for support staff to notice any changes and allows the system running the scans to execute the scans in parallel. The entire contents of the scan to be emailed to the desktop support staff. This scan should also be done during regular business hours occasionally to catch any machine that might get turned off at night. I would not recommend to this on a regular basis during business hours due to the traffic it can create.

Tripwire-

Goal – Verify file integrity on critical systems.

Methodology – A semi-hourly file scan (CRC) and a daily full integrity check. Where possible the full integrity checks should be scheduled in such a way that overall performance is not affected. The results of the scan should be logged to a remote server (via syslog if possible) running a log watching program such as Swatch.

SCHEDULED CHECKS

Again these should be considered a minimum.

Full vulnerability assessment-

Goal – Verify continuing system integrity against new attacks.

Methodology – A full assessment, as per the initial assessment, should be done on all critical systems at least once per quarter. The results should be compared against previous scans to attempt to detect any trends (such as wow, another vulnerability in BIND, maybe we should use different software, or, wow that system still has holes in it. Maybe someone should talk with the system admin…).

Goal – Verify that new software does not introduce new security holes.

Methodology – All new software (including patches) should first be applied to test servers that are identical to the production servers. A full assessment should then be performed upon the test system to verify the system's security before applying the software to other systems. If this is not possible the software upgrade should happen off-hours (though after a full, verified, back-up has completed) and a full vulnerability analysis should be performed (assuming time permits). If there is not enough time to do the full assessment time should be made in the immediate future to complete the assessment.

RECOMMENDED IMPROVEMENTS

The first improvement that could be made is to use stateful proxies. The current setup is susceptible to engineered packets that could bypass the firewall (requiring that only the SYN flag be set). Implementing this would be most useful in front of the Corporate and Management Networks as they are the most likely to have insecure machines. Implementing a stateful proxy in front of the public web servers would not be recommended due to load and response times.

Another improvement, particularly at the Management Network, would be to require authentication at the firewall before you computer is allowed to other regions. While this provides significantly more security and would be ideal for high security areas it would not be recommended for the Corporate Network due to the number and technical sophistication of employees involved.

If performance becomes an issue I would look into moving the public servers into the DMZ behind heavy packet filtering at the router level. If this was done it would be possible to use high speed layer 3 switches as routers, load balancers, and firewalls providing greater redundancy and performance. I considered using this type of architecture but did not have the resources to do any type of hands on. A trade off to using this type of architecture is that either the web servers must be dual-homed into the Backend Services network or you must allow traffic through the firewall to the database servers (something that is severely frowned upon). Creating links into backend servers this way introduces another avenue of access, read attack, to the severs that need to be most secure and eliminates one layer of defense. However the performance gained by not having a choke point on the public servers might be worth the risk.

One of the major weakness of the architecture presented here is that the public servers are limited to the amount of traffic that FW-A1/2 can handle. If GIAC Enterprises has the equivalent of an OC-12 (155 Mbps) coming into the data center the single, most likely 100Base-T, ethernet adapter in the firewall is going to be quickly overwhelmed. Replacing the ethernet card with a faster piece of hardware is possible it just means that the secondary firewall is going to have to be an extremely powerful machine to do real time IDS on that amount of traffic.

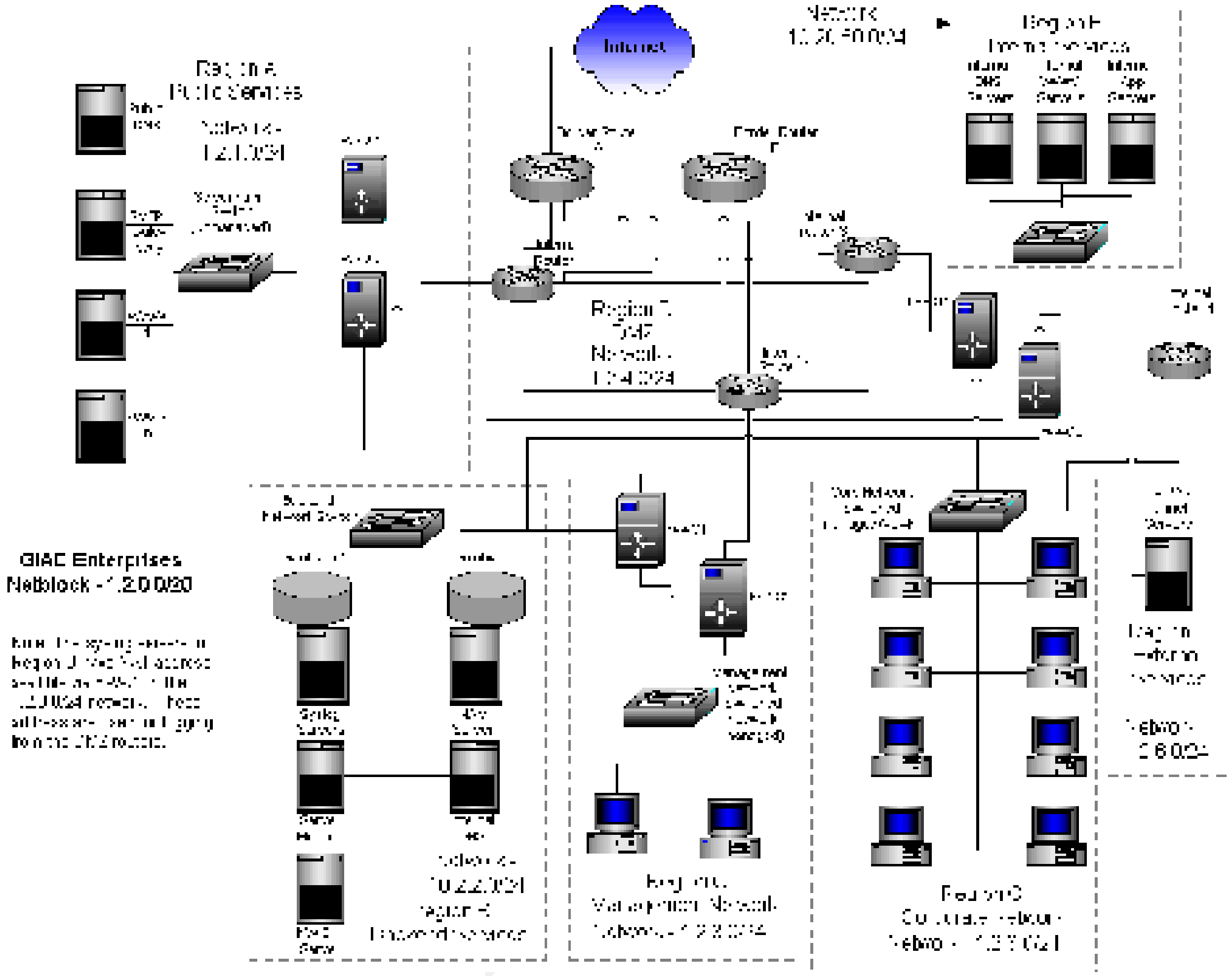
Likewise the connection into Internal Services is limited to the speed of the PCI bus (400 Mbps), a speed that could quickly become a major bottleneck with heavy utilization of application servers located behind the firewall. The solution for this would to be to go to a series of distributed firewalls and allow a high speed routing switch to do port based filtering in front of the application servers. The trade-off here is again security. More firewalls means more places something could be mis-configured.

It should be noted that the placement of the VPN terminators causes all traffic on the VPNs to transverse the firewall twice. While the place does increase the utilized bandwidth it reduces processor load on the firewall by having all the encryption done on a separate host. Also by having the VPNs terminate at a different device you can be extremely limiting in the amount of access to the firewall itself (note the described rule sets allow only ICMP traffic to target the firewall with SSH allow from a single host).

Another improvement, not directly related to perimeter security, would be to use a secure logging feature such as syslog-ng between all hosts. Syslog-ng allows for encrypted and verified communication when logging system events, always a good thing if someone is trying to erase your logs.

APPENDICIES

NETWORK MAP


Internet
Region A
Public Services
Network 1.2.1.0/24
Region D
DMZ
Network 1.2.4.0/24
GIAC Enterprises
Netblock - 1.2.0.0/20
Network 10.22.2.0/24
Management Network
Region G
Corporate Network
Network - 1.2.3.0/24

FIREWALL RULE SETS

Note: All rule sets are named by the region they connect to (meaning that there are rule sets on different firewalls with the same name). Also while the same rule set loads on both firewalls the aliased IPs do not become active on the secondary firewall until the Heartbeat software detects that the primary firewall has stopped communicating on at least one interface (the firewalls are connected via a null modem cable to ensure communication). All firewalls have the "forward" IP-Chain set to DENY by default.

FW-A1 and FW-A2 have the following IPChains rules:

TO THE DMZ. INTERFACE ETH0 (1.2.4.1 ALIASED)

```
/sbin/ipchains -N dmz
/sbin/ipchains -A dmz -s 10.0.0.0/8 -i eth0 -j DENY
/sbin/ipchains -A dmz -s 127.0.0.0/8 -i eth0 -j DENY
/sbin/ipchains -A dmz -s 172.16.0.0/12 -i eth0 -j DENY
/sbin/ipchains -A dmz -s 192.168.0.0/16 -i eth0 -j DENY
/sbin/ipchains -A dmz -d 10.2.2.254 -i eth0 -p TCP -j DENY
/sbin/ipchains -A dmz -d 10.2.2.254 -i eth0 -p UDP -j DENY
/sbin/ipchains -A dmz -d 1.2.1.0/24 :80 -i eth0 -p TCP -j ACCEPT
/sbin/ipchains -A dmz -d 1.2.1.0/24 :443 -i eth0 -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.1.2 :53 -p UDP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.1.1 :25 -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.1.1 :110 -p TCP -j ACCEPT
/sbin/ipchains -A dmz -d 1.2.1.1 :220 -i eth0 -p TCP -j ACCEPT
```

TO BACKEND SERVICES. INTERFACE ETH1 (10.2.2.254 ALIASED).

```
/sbin/ipchains -N backend
/sbin/ipchains -A backend -i eth1 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A backend -i eth1 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A backend -i eth1 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A backend -i eth1 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A backend -i eth1 -d 10.2.2.254 :22 -s 10.2.2.8 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.254 -p !ICMP -j DENY
/sbin/ipchains -A backend -i eth1 -d 1.2.1.0/24 :80 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 1.2.1.0/24 :443 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 1.2.1.2 :53 -p UDP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 1.2.1.1 :25 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 1.2.1.1 :110 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 1.2.1.1 :220 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.5 :617 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.6 :617 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.3 :514 -p UDP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.4 :514 -p UDP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.8 :22 -p TCP -j ACCEPT
```

TO THE PUBLIC SERVICES REGION. INTERFACE ETH2 (1.2.1.254 ALIASED).

```
/sbin/ipchains -N mgmnt
/sbin/ipchains -A mgmnt -i eth1 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.4.254 -p TCP -j DENY
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.4.254 -p UDP -j DENY
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :80 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :20 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :21 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :443 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.1.1 :25 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.1.1 :110 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.1.1 :220 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 10.2.2.8 :22 -s 1.2.4.0/24 -p TCP -j ACCEPT
```

Notes: The only connections that should be initiated in public services are DB requests to backend services and SMTP connections to other mail servers. Also it is possible for packets destined for RFC 1918 (other than the ones we are using) could be sent from this region, however the upstream routers are configured to drop such traffic. This traffic is not dropped at the firewall to help simplify the rule set.

THE RESULTING RULE SET FOR FW-A1 AND FW-A2

```
Chain dmz (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
DENY       tcp  ------  anywhere             10.2.2.254            any ->   any
DENY       udp  ------  anywhere             10.2.2.254            any ->   any
ACCEPT     tcp  ------  anywhere             1.2.1.0/24            any ->   0:www
ACCEPT     tcp  ------  anywhere             1.2.1.0/24            any ->   0:https
ACCEPT     udp  ------  anywhere             1.2.1.2               any ->   0:domain
ACCEPT     tcp  ------  anywhere             1.2.1.1               any ->   0:smtp
ACCEPT     tcp  ------  anywhere             1.2.1.1               any ->   0:pop3
ACCEPT     tcp  ------  anywhere             1.2.1.1               any ->   0:imap3
Chain backend (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
DENY       tcp  ------  anywhere             10.2.2.254            any ->   any
DENY       udp  ------  anywhere             10.2.2.254            any ->   any
ACCEPT     tcp  ------  anywhere             1.2.1.0/24            any ->   0:www
ACCEPT     tcp  ------  anywhere             1.2.1.0/24            any ->   0:https
ACCEPT     udp  ------  anywhere             1.2.1.2               any ->   0:domain
ACCEPT     tcp  ------  anywhere             1.2.1.1               any ->   0:smtp
ACCEPT     tcp  ------  anywhere             1.2.1.1               any ->   0:pop3
ACCEPT     tcp  ------  anywhere             1.2.1.1               any ->   0:imap3
ACCEPT     tcp  ------  anywhere             10.2.2.5              any ->   0:617
ACCEPT     tcp  ------  anywhere             10.2.2.6              any ->   0:617
ACCEPT     udp  ------  anywhere             10.2.2.3              any ->   0:syslog
ACCEPT     udp  ------  anywhere             10.2.2.4              any ->   0:syslog
ACCEPT     tcp  ------  anywhere             10.2.2.8              any ->   0:ssh
Chain public (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
DENY      !icmp ------  anywhere             10.2.2.254            any ->   any
ACCEPT     tcp  !y----  1.2.1.0/24           anywhere              0:www ->   any
ACCEPT     tcp  !y----  1.2.1.0/24           anywhere              0:https ->   any
ACCEPT     tcp  ------  1.2.1.0/24           10.2.2.0/24           any ->   0:321
ACCEPT     udp  ------  1.2.1.2              anywhere              0:domain ->   any
ACCEPT     tcp  ------  1.2.1.1              anywhere              0:smtp ->   any
ACCEPT     tcp  !y----  1.2.1.1              anywhere              0:pop3 ->   any
ACCEPT     tcp  !y----  1.2.1.1              anywhere              0:imap3 ->   any
ACCEPT     tcp  !y----  anywhere             10.2.2.5              any ->   0:617
ACCEPT     tcp  !y----  anywhere             10.2.2.6              any ->   0:617
ACCEPT     udp  ------  anywhere             10.2.2.3              any ->   0:syslog
ACCEPT     udp  ------  anywhere             10.2.2.4              any ->   0:syslog
ACCEPT     tcp  !y----  anywhere             10.2.2.8              any ->   0:ssh
```

FW-C1 AND FW-C2

TO THE DMZ. INTERFACE ETH0 (1.2.4.5 ALIASED)

```
/sbin/ipchains -N dmz
/sbin/ipchains -A dmz -i eth2 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A dmz -i eth2 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A dmz -i eth2 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A dmz -i eth2 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A dmz -i eth2 -d 1.2.3.0/24 :80 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth2 -d 1.2.1.0/24 :443 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.3.0/24 :20 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.3.0/24 :21 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth2 -d 1.2.1.2 :53 -p UDP -j ACCEPT
/sbin/ipchains -A dmz -i eth2 -d 1.2.1.1 :25 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth2 -d 1.2.1.1 :110 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth2 -d 1.2.1.1 :220 ! -y -p TCP -j ACCEPT
```

TO BACKEND SERVICES. INTERFACE ETH1 (10.2.2.253 ALIASED)

```
/sbin/ipchains -N backend
/sbin/ipchains -A backend -i eth1 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A backend -i eth1 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A backend -i eth1 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A backend -i eth1 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A backend -i eth1 -d 10.2.2.253 :22 -s 10.2.2.8 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.253 -p TCP -j DENY
/sbin/ipchains -A backend -i eth1 -d 10.2.2.253 -p UDP -j DENY
/sbin/ipchains -A backend -i eth1 -d 10.2.2.5 :80 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.6 :80 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.5 :617 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.6 :617 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.3 :514 -p UDP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.4 :514 -p UDP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.8 :22 -p TCP -j ACCEPT
```

TO THE MANAGEMENT NETWORK. INTERFACE ETH2 (1.2.3.254 ALIASED)

```
/sbin/ipchains -N mgmnt
/sbin/ipchains -A mgmnt -i eth1 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.4.254 -p TCP -j DENY
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.4.254 -p UDP -j DENY
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :80 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :20 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :21 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 0/0 :443 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.1.1 :25 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.1.1 :110 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 1.2.1.1 :220 -s 1.2.4.0/24 -p TCP -j ACCEPT
/sbin/ipchains -A mgmnt -i eth1 -d 10.2.2.8 :22 -s 1.2.4.0/24 -p TCP -j ACCEPT
```

THE RESULTING RULE SET FOR FW-C1 AND FW-C2

```
Chain dmz (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
ACCEPT     tcp  !y----  anywhere             1.2.3.0/24            any ->   0:www
ACCEPT     tcp  !y----  anywhere             1.2.1.0/24            any ->   0:https
ACCEPT     tcp  !y----  anywhere             1.2.3.0/24            any ->   0:ftp-data
ACCEPT     tcp  !y----  anywhere             1.2.3.0/24            any ->   0:ftp
ACCEPT     udp  ------  anywhere             1.2.1.2               any ->   0:domain
ACCEPT     tcp  !y----  anywhere             1.2.1.1               any ->   0:smtp
ACCEPT     tcp  !y----  anywhere             1.2.1.1               any ->   0:pop3
ACCEPT     tcp  !y----  anywhere             1.2.1.1               any ->   0:imap3
Chain backend (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
ACCEPT     tcp  ------  10.2.2.8             10.2.2.253            any ->   0:ssh
```

```
DENY       tcp  ------  anywhere             10.2.2.253           any ->   any
DENY       udp  ------  anywhere             10.2.2.253           any ->   any
ACCEPT     tcp  ------  anywhere             10.2.2.5             any ->   0:www
ACCEPT     tcp  ------  anywhere             10.2.2.6             any ->   0:www
ACCEPT     tcp  ------  anywhere             10.2.2.5             any ->   0:617
ACCEPT     tcp  ------  anywhere             10.2.2.6             any ->   0:617
ACCEPT     udp  ------  anywhere             10.2.2.3             any ->   0:syslog
ACCEPT     udp  ------  anywhere             10.2.2.4             any ->   0:syslog
ACCEPT     tcp  ------  anywhere             10.2.2.8             any ->   0:ssh
Chain mgmnt (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere             n/a
DENY       all  ------  127.0.0.0/8          anywhere             n/a
DENY       all  ------  172.16.0.0/12        anywhere             n/a
DENY       all  ------  192.168.0.0/16       anywhere             n/a
DENY       tcp  ------  anywhere             1.2.4.254            any ->   any
DENY       udp  ------  anywhere             1.2.4.254            any ->   any
ACCEPT     tcp  ------  1.2.4.0/24           anywhere             any ->   0:www
ACCEPT     tcp  ------  1.2.4.0/24           anywhere             any ->   0:ftp-data
ACCEPT     tcp  ------  1.2.4.0/24           anywhere             any ->   0:ftp
ACCEPT     tcp  ------  1.2.4.0/24           anywhere             any ->   0:https
ACCEPT     tcp  ------  1.2.4.0/24           1.2.1.1              any ->   0:smtp
ACCEPT     tcp  ------  1.2.4.0/24           1.2.1.1              any ->   0:pop3
ACCEPT     tcp  ------  1.2.4.0/24           1.2.1.1              any ->   0:imap3
ACCEPT     tcp  ------  1.2.4.0/24           10.2.2.8             any ->   0:ssh
```

FW-G1 AND FW-G2

TO THE DMZ. INTERFACE ETH0 (1.2.4.9 ALIASED)

```
/sbin/ipchains -N dmz
/sbin/ipchains -A dmz -i eth0 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A dmz -i eth0 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A dmz -i eth0 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A dmz -i eth0 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A dmz -i eth0 -s 20.20.20.20 -d 1.2.6.1 -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :80 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :443 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :20 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :21 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :53 -p UDP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :25 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :110 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A dmz -i eth0 -d 1.2.8.0/21 :220 ! -y -p TCP -j ACCEPT
```

Notes: Rule 5 is a typical example of access granted to an off-site partner located at 20.20.20.20 to access the other end of a VPN tunnel at 1.2.6.1. Each partner that has a VPN to GIAC would have their own rule.

TO BACKEND SERVICES. INTERFACE ETH1 (10.2.2.252 ALIASED)

```
/sbin/ipchains -N backend
/sbin/ipchains -A backend -i eth1 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A backend -i eth1 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A backend -i eth1 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A backend -i eth1 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A backend -i eth1 -d 10.2.2.252:22 -s 10.2.2.8 -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.252 -p TCP -j DENY
/sbin/ipchains -A backend -i eth1 -d 10.2.2.252 -p UDP -j DENY
/sbin/ipchains -A backend -i eth1 -s 10.2.2.9 :321 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -s 10.2.2.10 :321 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.3 :514 -p UDP -j ACCEPT
/sbin/ipchains -A backend -i eth1 -d 10.2.2.4 :514 -p UDP -j ACCEPT
```

TO THE CORPORATE NETWORK. INTERFACE ETH2 (1.2.8.1 ALIASED)

```
/sbin/ipchains -N corp
/sbin/ipchains -A corp -i eth2 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A corp -i eth2 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A corp -i eth2 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A corp -i eth2 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A corp -i eth2 -d 1.2.8.1 -p TCP -j DENY
/sbin/ipchains -A corp -i eth2 -d 1.2.8.1 -p UDP -j DENY
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 -d 0/0 :80 -p TCP -j ACCEPT
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 -d 0/0 :443 -p TCP -j ACCEPT
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 :20 -p TCP -j ACCEPT
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 :21 -y -p TCP -j ACCEPT
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 -d 1.2.1.1 :25 -p TCP -j ACCEPT
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 -d 1.2.1.1 :110 -p TCP -j ACCEPT
/sbin/ipchains -A corp -i eth2 -s 1.2.8.0/21 -d 1.2.1.1 :220 -p TCP -j ACCEPT
```

TO INTERNAL SERVICES. INTERFACE ETH3 (10.20.50.254 ALIASED)

```
/sbin/ipchains -N internal
/sbin/ipchains -A internal -i eth3 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A internal -i eth3 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A internal -i eth3 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A internal -i eth3 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A internal -i eth3 -d 10.20.50.254 -p TCP -j DENY
/sbin/ipchains -A internal -i eth3 -d 10.20.50.254 -p UDP -j DENY
/sbin/ipchains -A internal -i eth3 -d 1.2.6.0/24 -s 10.20.50.0 :80 -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :80 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :443 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :20 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :21 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :53 -p UDP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :25 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :110 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A internal -i eth3 -d 1.2.8.0/21 :220 ! -y -p TCP -j ACCEPT
```

Notes this assumes that all served applications are via http (rule 7).

TO EXTERNAL SERVICES. INTERFACE ETH4 (1.2.6.254 ALIASED)

```
/sbin/ipchains -N external
/sbin/ipchains -A external -i eth4 -s 10.0.0.0/8 -j DENY
/sbin/ipchains -A external -i eth4 -s 127.0.0.0/8 -j DENY
/sbin/ipchains -A external -i eth4 -s 172.16.0.0/12 -j DENY
/sbin/ipchains -A external -i eth4 -s 192.168.0.0/16 -j DENY
/sbin/ipchains -A external -i eth4 -d 1.2.6.254 -p TCP -j DENY
/sbin/ipchains -A external -i eth4 -d 1.2.6.254 -p UDP -j DENY
/sbin/ipchains -A external -i eth4 -s 1.2.6.1/24 -d 10.20.50.0 :80 -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :80 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :443 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :20 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :21 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :53 -p UDP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :25 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :110 ! -y -p TCP -j ACCEPT
/sbin/ipchains -A external -i eth4 -d 1.2.8.0/21 :220 ! -y -p TCP -j ACCEPT
```

Notes: 1.2.6.1 represents the end of a VPN with a partner site. Each VPN should have its own rule.

THE RESULTING RULE SET FOR FW-G1 AND FW-G2

```
Chain dmz (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
ACCEPT     all  ------  20.20.20.20          1.2.6.1               n/a
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:www
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:https
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:ftp-data
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:ftp
ACCEPT     udp  ------  anywhere             1.2.8.0/21            any ->   0:domain
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:smtp
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:pop3
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21            any ->   0:imap3
Chain backend (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
ACCEPT     tcp  ------  10.2.2.8             10.2.2.252            any ->   0:ssh
DENY       tcp  ------  anywhere             10.2.2.252            any ->   any
DENY       udp  ------  anywhere             10.2.2.252            any ->   any
ACCEPT     tcp  !y----  10.2.2.9             anywhere              0:321 ->   any
ACCEPT     tcp  !y----  10.2.2.10            anywhere              0:321 ->   any
ACCEPT     udp  ------  anywhere             10.2.2.3              any ->   0:syslog
ACCEPT     udp  ------  anywhere             10.2.2.4              any ->   0:syslog
Chain corp (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
DENY       tcp  ------  anywhere             1.2.6.254             any ->   any
DENY       udp  ------  anywhere             1.2.6.254             any ->   any
ACCEPT     tcp  ------  1.2.8.0/21           anywhere              any ->   0:www
ACCEPT     tcp  ------  1.2.8.0/21           anywhere              any ->   0:https
ACCEPT     tcp  ------  1.2.8.0/21           anywhere              0:ftp-data ->   any
ACCEPT     tcp  -y----  1.2.8.0/21           anywhere              0:ftp ->   any
ACCEPT     tcp  ------  1.2.8.0/21           1.2.1.1               any ->   0:smtp
ACCEPT     tcp  ------  1.2.8.0/21           1.2.1.1               any ->   0:pop3
ACCEPT     tcp  ------  1.2.8.0/21           1.2.1.1               any ->   0:imap3
Chain internal (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere              n/a
DENY       all  ------  127.0.0.0/8          anywhere              n/a
DENY       all  ------  172.16.0.0/12        anywhere              n/a
DENY       all  ------  192.168.0.0/16       anywhere              n/a
DENY       tcp  ------  anywhere             10.20.50.254          any ->   any
DENY       udp  ------  anywhere             10.20.50.254         any ->   any
ACCEPT     tcp  ------  10.20.50.0           1.2.6.0/24           0:www ->   any
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:www
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:https
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:ftp-data
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:ftp
ACCEPT     udp  ------  anywhere             1.2.8.0/21           any ->   0:domain
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:smtp
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:pop3
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:imap3
Chain external (0 references):
target     prot opt     source                destination          ports
DENY       all  ------  10.0.0.0/8           anywhere             n/a
DENY       all  ------  127.0.0.0/8          anywhere             n/a
DENY       all  ------  172.16.0.0/12        anywhere             n/a
DENY       all  ------  192.168.0.0/16       anywhere             n/a
DENY       tcp  ------  anywhere             1.2.6.254            any ->  any
DENY       udp  ------  anywhere             1.2.6.254            any ->  any
ACCEPT     tcp  ------  1.2.6.0/24           10.20.50.0           any ->  0:www
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->  0:www
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->  0:https
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:ftp-data
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:ftp
ACCEPT     udp  ------  anywhere             1.2.8.0/21           any ->   0:domain
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:smtp
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:pop3
ACCEPT     tcp  !y----  anywhere             1.2.8.0/21           any ->   0:imap3
```

HOST LISTING

FW-A1, FW-C1, FW-G1

Platform: Redhat 6.2 on Intel P-III
Software: IP-Chains version 1.3.9
SSH version 2.3 (www.ssh.com/products/ssh/)
High Availability Linux Server – Heartbeat v 0.4.8 (http://www.linux-ha.org/download/)
Netsaint NRPEP (http://www.netsaint.org/docs/0_0_6/addons.html - nrpep)

Initialization Scripts
(rc3.d): K92ipchains, S10network, S20random, S30syslog, S40crond, S99local
(rc.d): rc, rc.local, rc.sysinit

Notes:
NRPEP is the only service listed under inetd.conf (see configuration line below).

```
nrpep stream  tcp     nowait  netsaint   /usr/local/netsaint/libexec/nrpep
```

SSH is not controlled via inted.conf due to performance issues at startup.

Interfaces: eth0 (all systems) – DMZ

Eth1 (all systems) – Backend services

FW-A2, FW-C2, FW-G2

Platform: Redhat 6.2 on Intel P-III
Software: IP-Chains version 1.3.9
SSH version 2.3 (www.ssh.com/products/ssh/)
High Availability Linux Server – Heartbeat v 0.4.8 (www.linux-ha.org/download/)
Snort version 1.6.3 patch2 (www.snort.org)

Initialization Scripts
(rc3.d): K92ipchains, S10network, S20random, S30syslog, S40crond, S99local
(rc.d): rc, rc.local, rc.sysinit

Notes:
NRPEP is the only service listed under inetd.conf (see configuration line below).

```
nrpep stream  tcp     nowait  netsaint   /usr/local/netsaint/libexec/nrpep
```

SSH is not controlled via inted.conf due to performance issues at startup.

SYSTEM INTERFACE LISTING-

REGION A-

FW-A1 - PRIMARY FIREWALL

eth0- DMZ Connection - 1.2.4.1 (alias), 192.168.1.1 (real)
eth1- Backend Connection - 10.2.2.254 (alias), 192.168.2.1 (real)
eth2- Public Services - 1.2.1.254 (alias), 192.168.3.1 (real)

FW-A2 - SECONDARY FIREWALL/IDS

eth0- DMZ Connection - 1.2.4.1 (alias), 192.168.1.2 (real)
eth1- Backend Connection - 10.2.2.254 (alias), 192.168.2.2 (real)
eth2- Public Services - 1.2.1.254 (alias), 192.168.3.2 (real)

PUBLIC DNS

eth0- 1.2.1.3

SMTP GATEWAY

eth0- 1.2.1.4

WEBSERVER 1

eth0- 1.2.1.5

WEBSERVER N

eth0- 1.2.1.4+n

REGION B -

PRIMARY SYSLOG SERVER

eth0- 10.2.2.3

SECONDARY SYSLOG SERVER

eth0- 10.2.2.4

PRIMARY MONITORING SERVER

eth0- 10.2.2.5

SECONDARY MONITORING SERVER

eth0- 10.2.2.6

MANAGEMENT STATION

eth0- 10.2.2.8

DATABASE SERVER 1

eth0- 10.2.2.9

DATABASE SERVER N

eth0- 10.2.2.8+n

REGION C -

FW-C1 - PRIMARY FIREWALL

eth0- DMZ Connection - 1.2.4.5/30 (alias), 192.168.4.1/24 (real)
eth1- Backend Connection - 10.2.2.253/24 (alias), 192.168.5.1/24 (real)
eth2- Management Network - 1.2.3.254/24 (alias), 192.168.6.1/24 (real)

FW-C2 - SECONDARY FIREWALL/IDS

eth0- DMZ Connection - 1.2.4.5 (alias), 192.168.4.2 (real)
eth1- Backend Connection - 10.2.2.253 (alias), 192.168.5.2 (real)
eth2- Management Network - 1.2.3.254 (alias), 192.168.6.2 (real)

NAV SERVER

eth0- 10.2.2.3

WORKSTATION 1

eth0- 10.2.2.4

WORKSTATION N

eth0- 10.2.2.4+n

REGION D -

BR-A - BORDER ROUTER 1

Serial 0/0- IP given by ISP

Ethernet 0/0- IR-01 - 1.2.4.9/30

Ethernet 0/1- IR-02 - 1.2.4.13/30

Ethernet 1/0- IR-03 - 1.2.4.17/30

BR-B - BORDER ROUTER 2

Serial 0/0- IP given by ISP

Ethernet 0/0- IR-01 - 1.2.4.21/30

Ethernet 0/1- IR-02 - 1.2.4.25/30

Ethernet 1/0- IR-03 - 1.2.4.29/30

IR-01 - INTERNAL ROUTER 1

Ethernet 0/0- BR-A - 1.2.4.10/30

Ethernet 0/1- BR-B - 1.2.4.22/30

Ethernet 1/0- FW-A1/2 - 1.2.4.2/30

IR-02- INTERNAL ROUTER 2

Ethernet 0/0- BR-A - 1.2.4.14/30

Ethernet 0/1- BR-B - 1.2.4.26/30

Ethernet 1/0- FW-C1/2 - 1.2.4.6/30

IR-03 - INTERNAL ROUTER 3

Ethernet 0/0- BR-A - 1.2.4.18/30

Ethernet 0/1- BR-B - 1.2.4.30/30

Ethernet 1/0- FW-G1/2 - 1.2.4.34/30

IR-04- INTERNAL ROUTER 4

Ethernet 0/0- Internal Services - NO IP - IPX 102050

Ethernet 0/1- Corporate Network - NO IP - IPX 1280

REGION E -

INTERNAL DNS SERVERS

various

INTERNAL WWW SERVERS

various

INTERNAL APPLICATION SERVERS

various

REGION F -

HOST 1 - VPN TERMINATOR/FIREWALL 1

Ethernet 0 – 1.2.6.1

HOST N - VPN TERMINATOR/FIREWALL N

Ethernet 0 – 1.2.6.1+n

REGION G -

FW-G1 - PRIMARY FIREWALL

eth0- DMZ Connection - 1.2.4.35 (alias), 192.168.7.1 (real)
eth1- Backend Connection - 10.2.2.252 (alias), 192.168.8.1 (real)
eth2- Corporate Network - 1.2.8.1/21 (alias), 192.168.9.1 (real)
eth3- Internal Services - 10.20.50.254 (alias), 192.168.10.1 (real)
eth4- External Services - 1.2.6.254 (alias), 192.168.11.1 (real)

FW-G2 - SECONDARY FIREWALL/IDS

eth0- DMZ Connection - 1.2.4.35 (alias), 192.168.7.2 (real)
eth1- Backend Connection - 10.2.2.252 (alias), 192.168.8.2 (real)
eth2- Corporate Network - 1.2.8.1/21 (alias), 192.168.9.2 (real)
eth3- Internal Services - 10.20.50.254 (alias), 192.168.10.2 (real)
eth4- External Services - 1.2.6.254 (alias), 192.168.11.2 (real)

WORKSTATION 1

eth0 – DHCP

WORKSTATION N

eth0 – DHCP

ROUTER CONFIGURATION

All routers have telnet disabled and are managed via a console server in the Management Network. The console server authenticates against a Radius server. All routers also have ACL statements to deny any traffic destined for the routers themselves.

Border routers are assumed to be Cisco 4000 series routers. Internal routers are assumed to be Cisco 2621 routers (though I may have some interface numbers incorrect on the 2621s).

The philosophy behind the ACLs is to eliminate unwanted traffic as early as possible without straining any filtering/firewalling device. To this end the border routers (BR-A and BR-B) eliminate any traffic not destined for GIAC networks (1.2.0.0/20) or from obviously spoofed address (RFC1918 and 127.0.0.0/8). Additionally BGP updates are limited to the upstream neighbor and the other border router. Other than BGP no port filtering is done at the border routers for performance and management reasons. Port filtering is handled by the internal routers and firewalls.

Internal routers (IR-01, IR-02, and IR-03) restrict traffic to traffic originating or destined to the regions behind them. No inter-region traffic passes between the internal routers except for traffic destined to Public Services. Traffic destined to Public Services is treated as traffic from the internet with the allowance for users to retrieve email either via POP3 or IMAP.

BORDER ROUTERS

BR-A, BR-B

Interfaces: Serial 0/0 – Connection to upstream ISP (Note-should be different for BR-A and BR-B)

Ethernet 0/0 – Connects to IR-01 fwain (inbound), fwaout (outbound)

Ethernet 0/1 – Connects to IR-02 fwcin (inbound), fwcout (outbound)

Ethernet 1/0 – Connects to IF-03 fwgin (inbound), fwgout (outbound)

Ethernet 1/1 – Connects to other border router brin(inbound), brout(outbound)

ACLs: (note: All ACLs are inbound on their respective ports and are named by the region they connect to.)

```
worldin:    access-list worldin permit any 1.2.0.0 0.0.15.255
            access-list worldin deny 10.0.0.0 0.255.255.255 any log
            access-list worldin deny 192.168.0.0 0.0.255.255 any log
            access-list worldin deny 172.16.0.0 0.15.255.255 any log
            access-list worldin deny 127.0.0.0 0.255.255.255 any log
            access-list worldin permit icmp any <S0/0 IP>
            access-list worldin deny ip any any log

worldout    access-list worldout permit any 1.2.0.0 0.0.15.255
            access-list worldout deny 10.0.0.0 0.255.255.255 any log
            access-list worldout deny 192.168.0.0 0.0.255.255 any log
            access-list worldout deny 172.16.0.0 0.15.255.255 any log
            access-list worldout deny 127.0.0.0 0.255.255.255 any log
            access-list worldout permit icmp <S0/0 IP> any
            access-list world deny ip any any log

fwain:      access-list fwain permit tcp 1.2.1.0 0.0.0.255 any gt 1023
            access-list fwain permit icmp any 1.2.4.9 0.0.0.0
            access-list fwain deny ip any any log

fwaout      access-list fwaout permit tcp any 1.2.1.0 0.0.0.255 eq 80
            access-list fwaout permit udp any 1.2.1.2 0.0.0.0 eq 53
            access-list fwaout permit tcp any 1.2.1.0 0.0.0.255 eq 443
            access-list fwaout permit tcp any 1.2.1.1 0.0.0.0 eq 25
            access-list fwaout permit tcp any 1.2.1.1 0.0.0.0 eq 110
            access-list fwaout permit tcp any 1.2.1.1 0.0.0.0 eq 220
            access-list fwaout permit icmp 1.2.4.9 any 0.0.0.0
            access-list fwaout deny ip any any log


fwcin:      access-list fwcin permit tcp 1.2.3.0 0.0.0.255 any eq 80
            access-list fwcin permit tcp 1.2.3.0 0.0.0.255 any eq 443
            access-list fwcin permit tcp 1.2.3.0 0.0.0.255 any eq 20
            access-list fwcin permit tcp 1.2.3.0 0.0.0.255 any eq 21
            access-list fwcin permit icmp any 1.2.4.13 0.0.0.0
            access-list fwcin deny ip any any log

fwcout      access-list fwcout permit tcp any 1.2.3.0 0.0.0.255 gt 1023 established
            access-list fwcout permit udp 1.2.4.13 0.0.0.0 1.2.2.3 0.0.0.0 eq 514
            access-list fwcout permit udp 1.2.4.13 0.0.0.0 1.2.2.4 0.0.0.0 eq 514
            access-list fwcout permit icmp 1.2.4.13 0.0.0.0 any
            access-list fwcout deny ip any any log

fwgin:      access-list fwgin permit tcp 1.2.3.0 0.0.0.255 any eq 80
            access-list fwgin permit tcp 1.2.3.0 0.0.0.255 any eq 443
            access-list fwgin permit tcp 1.2.3.0 0.0.0.255 any eq 20
            access-list fwgin permit tcp 1.2.3.0 0.0.0.255 any eq 21
            access-list fwgin permit icmp any 1.2.4.17 0.0.0.0
            access-list fwgin deny ip any any log

fwgout      access-list fwgout permit tcp any 1.2.8.0 0.0.7.255 gt 1023 established
            access-list fwgout permit icmp 1.2.4.17 0.0.0.0 any
            access-list fwgout deny ip any any log
```

CONFIGURATION NOTES:

Example configuration highlights for BR-A:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no snmp
no ip unreachables
no ip direct-broadcast
no ip bootp server
no ip http server
no ip source-route
no telnet
!
logging 1.2.2.3
logging 1.2.2.4
!
interface Ethernet 0/0
      ip address 1.2.4.1 255.255.255.252
ip access-group fwain in
ip access-group fwaout out
interface Ethernet 0/1
      ip address 1.2.4.4 255.255.255.252
ip access-group fwcin in
ip access-group fwcout out
interface Ethernet 1/0
      ip address 1.2.4.7 255.255.255.252
ip access-group fwgin in
ip access-group fwgout out
interface Serial 0/0
      ip address <given by ISP>
ip access-group worldin in
ip access-group worldout out
```

INTERNAL ROUTERS-

The primary purpose of the internal routers is two fold. First they allow the firewalls not to have to do any routing in connecting to multiple border routers and running dynamic routing protocols. The second and more important function is that they provide a screening layer between the world and the networks running private address space. Having the internal routers allows for very secure screening of any traffic destined to, or originating from, one of the private networks.

For the sake of brevity I'm not going to develop full ACLs for all the internal routers. Instead here are the guidelines to be applied to each interface. For the traffic that should be allowed to each router please see the border router ACLs.

Deny all traffic originating from or destined to RFC 1918 addresses and 127.0.0.0 addresses. This should be applied inbound and outbound on all interfaces.

Allow only traffic destined for the publicly addressable network directly behind the router. For example IR-01 should only accept traffic destined for 1.2.1.0/24. The ACL should also enforce proper ports and connections. Again IR-01 should only accept traffic on ports that servers are running and should not allow outbound web connections, but should allow outbound sendmail. This should be applied to both border router connections inbound and outbound.

Allow only traffic originating from the GIAC network directly behind the router outbound. Example IR-02 should only allow traffic from 1.2.3.0/24 outbound. Port filtering should occur as well as connection filtering (not allowing inbound web connections for example).

SAMPLE SCAN OUTPUT

Note both of these scans are from inside the firewall.

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
 Interesting ports on  (10.2.2.5):
(The 1518 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        listen

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=18610 (Worthy challenge)
Remote operating system guess: Windows 2000 RC1 through final release

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

```
Nessus Scan Report
------------------
SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 6
 - Number of security notes found : 1

TESTED HOSTS

 10.2.2.5 (Security holes found)

DETAILS

+ 10.2.2.5 :
 . List of open ports :
   o unknown (135/tcp)
   o netbios-ssn (139/tcp) (Security hole found)
   o unknown (445/tcp)
   o unknown (1025/tcp)
   o netbios-ns (137/udp) (Security warnings found)
   o general/udp (Security notes found)
   o general/tcp (Security warnings found)
   o general/icmp (Security warnings found)
. Vulnerability found on port netbios-ssn (139/tcp) :

    . It was possible to log into the remote host using a NULL session.
    The concept of a NULL session is to provide a null username and
    a null password, which grants the user the 'guest' access

    . All the smb tests will be done as
     ''/''

 . Warning found on port netbios-ssn (139/tcp)

    Here is the browse list of the remote host :

    DUALCELERON -

    This is potentially dangerous as this may help the attack
    of a potential hacker by giving him extra targets to check for

    Solution : filter incoming traffic to this port
    Risk factor : Low

 . Warning found on port netbios-ssn (139/tcp)

    The host SID can be obtained remotely. Its value is :
    DUALCELERON : 5-21-1177238915-725345543-1417001333

    An attacker can use it to obtain the list of the local users of this host
    Solution : filter the ports 137 to 139
    Risk factor : Low

 . Warning found on port netbios-ssn (139/tcp)

    The SID could be used to enumerate the names of the users
    of this host.
    (we only enumerated users name whose ID is between 1000 and 1200
    for performance reasons)
    This gives extra knowledge to a cracker, which
    is not a good thing :
    - Administrator account name : Administrator (id 500)
    - Guest account name : Guest (id 501)

    Risk factor : Medium
    Solution : filter incoming connections to port 139

 . Warning found on port netbios-ns (137/udp)

    . The following 6 NetBIOS names have been gathered :
     DUALCELERON     = This is the computer name registered for workstation
     services by a WINS client.
     DUALCELERON
     WORKGROUP       = Workgroup / Domain name
     WORKGROUP
     WORKGROUP
       __MSBROWSE__
    . The remote host has the following MAC address on its adapter :
       0x00 0xe0 0x7d 0x71 0xe3 0xb8

    If you do not want to allow everyone to find the NetBios name
    of your computer, you should filter incoming traffic to this port.

    Risk factor :
     Medium

 . Information found on port general/udp

    For your information, here is the traceroute to 10.2.2.5 :
    1.2.1.254
    10.2.2.5

 . Warning found on port general/tcp

    The remote host uses non-random IP IDs, that is, it is
    possible to predict the next value of the ip_id field of
    the ip packets sent by this host.

    An attacker may use this feature to determine if the remote
    host sent a packet in reply to another request. This may be
    used for portscanning and other things.

    Solution : Contact your vendor for a patch
    Risk factor :
     Low

 . Warning found on port general/icmp

    The remote host answers to an ICMP timestamp
    request. This allows an attacker to know the
    date which is set on your machine.

    This may help him to defeat all your
    time based authentifications protocols.

    Solution : filter out the icmp timestamp
    requests (13), and the outgoing icmp
    timestamp replies (14).

    Risk factor : Low
    CVE : CAN-1999-0524
------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

REFERENCES

Syslog-ng	http://www.balabit.hu/products/syslog-ng/
Linux HA	http://www.linux-ha.org/
IP-Chains How-to	howto.tucows.com
Netsaint	http://www.netsaint.org/
Nessus	http://www.nessus.org/
Saint	http://www.wwdsi.com/saint
Sara	www-arc.com/sara
Snort	http://www.snort.org/
SANS Top Ten	http://www.sans.org/topten
Nmap	http://www.insecure.org/
Tripwire	http://www.tripwire.com/
SSH	http://www.ssh.com/