Global Information Assurance Certification Paper

(GIAC Enterprises)
GIAC-Online.com

Security Policies & Procedures
for e-commerce

GIAC
Information Security Officer (GISO) Practical,
Version 1.2

Mike Letalien
December, 2002

Summary

GIAC-Online (GIAC) is a company that sells Graphics, Images, Artwork, and Creativity. Over the next few months, GIAC hopes to grow from a relatively small, phone order operation with a presence on the internet to a more powerful entity within the image industry. A project is underway to implement an e-Commerce solution. It is the goal of GIAC to increase the number of images available to customers, and to significantly decrease the turn around time on orders.

This paper was put together as a study of the various security issues that a project of this scope and significance demands. Details about GIAC, the infrastructure and planned security functions will be discussed. Policies and procedural aspects of the e-Commerce project are also included.

Obviously, the release of information about GIAC's planned upgrade, the infrastructure in use, and security issues could seriously damage the company. Damage could be from a hacker attempting to exploit known vulnerabilities of a particular hardware device to GIAC's competition leaping ahead of GIAC knowing what the planned business strategy is. Readers of the document contained herein are encouraged to use it as an educational opportunity only, and not to disperse copies beyond what has been approved in writing by management and ownership of GIAC-Online.

Assignment 1 – Describe GIAC-Online.com

Section 1.1 – Company Description

GIAC-Online.com (GIAC) is a company based in Golden, Colorado that provides Graphics, Images, Artwork and Creativity to consumers of a wide variety of disciplines across the country and around the world. Customers of GIAC include:
Publishers of magazines, books and calendars,

- Web Design companies,
- Media Services - newspapers, television and web-based,
- Educational Providers from Preschool to College, and
- Anyone with an appreciation for original artwork and photography.

Contributors are added every day, and with an emphasis on "up-and-coming" artists GIAC will continue to supply customers with high-quality, cutting-edge graphics. As long as human beings rely on pictures to tell a story, GIAC will strive to provide the means to accomplish that task.

At present, GIAC has a web presence, a catalogue of samples, and processes only phone, mail and fax orders. Printed product is delivered by means of standard shipping. In the case of electronic media, encrypted e-mail services provided by CertifiedMail.com handle all file transfers. GIAC is currently planning to implement an e-commerce solution to enhance the website, and increase market-share by allowing established customers to directly order items via the Internet. A "forklift" upgrade is planned so any discussion of infrastructure will be describing planned activities, rather than existing devices.

GIAC consists of three areas of focus (pun intended): Operations, Customer Service, and Technology. GIAC is headed by a pair of long-time friends...one with a business background and the other a photographer. Decisions regarding company values, goals and direction are approved by both CEO's, along with their group of managers that direct each of the three departments mentioned above. The Operations group consists of general Office Management, Human Resources, and is responsible for the day-to-day internal workflow, as well as hiring and training new employees. Customer Service is responsible for the bottom line at GIAC, consisting of the sub-departments Product Shipping, Customer Inquiries, Sales, and Marketing/PR. The Technology area will be experiencing major growth during this project and is divided into two segments:

- Information Technology, the technical personnel who ensure that orders come in and products go out, and
- Web Development, programmers, and the staff photographers & graphic artists that produce original work exclusively for GIAC.

An important, some would say *the* most important, member of the GIAC family is the photographers and artists that provide GIAC with its enormous inventory. While not directly employed by GIAC, interaction with these talented people is vital to the continued success of GIAC. In the current electronic-enhancement project, plans are to allow artists of all disciplines to directly upload their work to GIAC, rather than

submitting them via mail. This will allow for a quicker time-to-publish and greatly upgrade GIAC's contribution to the current events and 24x7 news coverage that is becoming the industry standard.

Section 1.2 – Communications Infrastructure

Current infrastructure at GIAC consists of internal database and application servers that are networked, but not available outside of the limited, internal network. Orders are taken by our Customer Services staff, whether mail, phone or fax, and processed through traditional means. Credit card orders are phoned in through leased machines provided by the card companies. Checks and money orders are simply deposited, and orders are finalized once those have cleared bank processing.

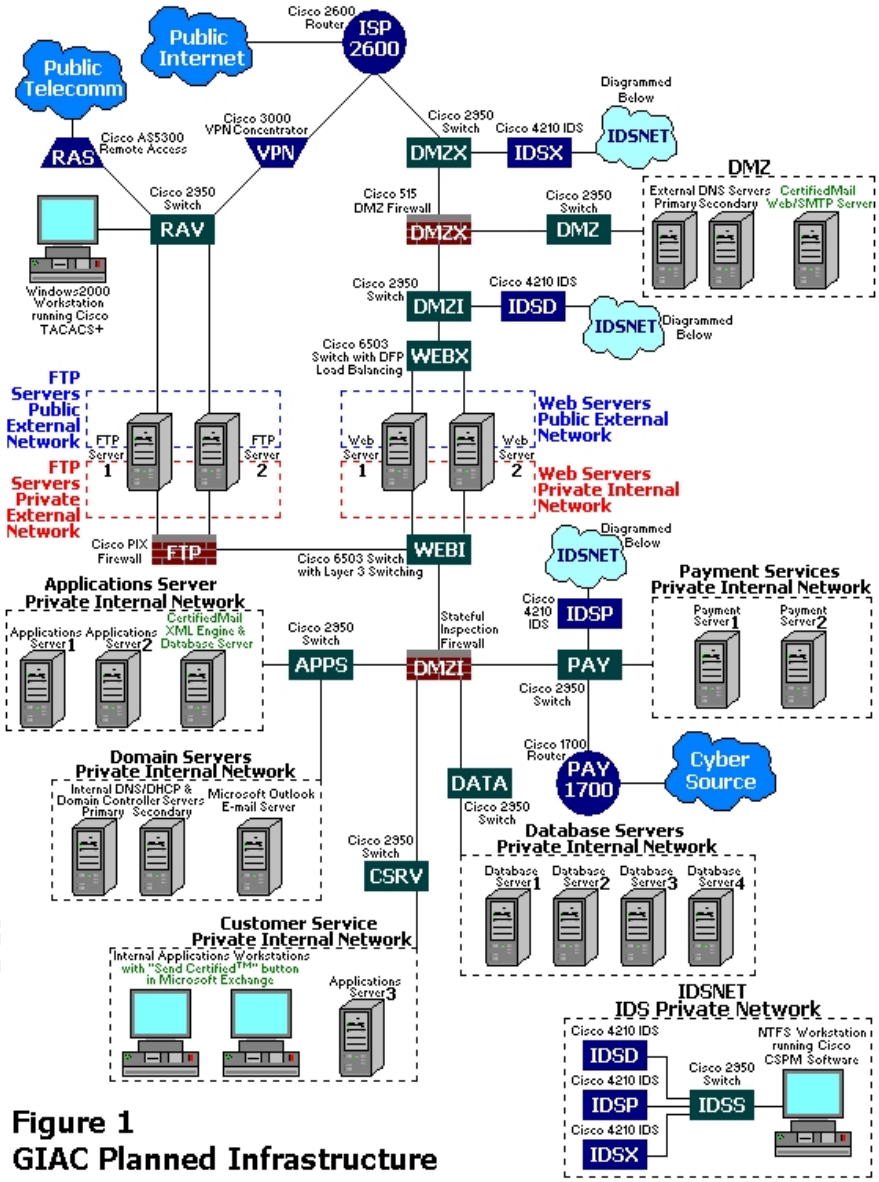


Figure 1
GIAC Planned Infrastructure

Upgraded infrastructure will cover all workstations, servers, and network foundation equipment. All workstations will run the Microsoft Windows 2000 operating system. Servers will also utilize Microsoft's Windows 2000, but will run [1]Advanced Server to allow for clustering across multiple servers providing the same function. Design considerations for an e-commerce facility are strict, and industry standards have been consulted continuously during the planning stages of this project.

[1] Microsoft Windows 2000 Advanced Server "Introducing Windows 2000 Advanced Server"
http://www.microsoft.com/windows2000/advancedserver/evaluation/business/overview/advanced.asp

1.2.1 Network Protection in Publicly Accessible Areas

GIAC will use a Cisco 2600 router (labeled ISP2600) as the first line of defense. Designed to filter packets, it will provide a solution for some basic network security issues. Using Cisco's IOS to create access lists, GIAC will reduce the risk of unwanted and destructive traffic by eliminating the most prevalent and easy to overcome problems. GIAC's internal networks will use private IP addressing (defined in RFC1918) to conserve public IP addresses for devices that actually reside in the public domain. RFC 1918 states that "[2]because private addresses have no global meaning, routing information about private networks shall not be propagated on inter-enterprise links, and packets with private source or destination addresses should not be forwarded across such links. Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured to reject (filter out) routing information about private networks. If such a router receives such information the rejection shall not be treated as a routing protocol error." The SANS Institute (Dan Strom) has also issued recommendations for ingress and egress filtering to fight DoS attacks. [3]The following guidelines should be adhered to:

Ingress – Inbound filtering

- Block packets destined for services that are not being offered to the Internet.
- Block addresses that have a source IP address of:
  - Illegal addresses – e.g. 0.0.0.0/8 (CIDR notation)
  - Broadcast address – 255.255.255.255/32
  - RFC1918 reserved addresses – Private networks use these. There should not be any traffic attempting to access your network with these as source addresses. The IANA reserved blocks are:
    - 10.0.0.0 - 10.255.255.255
    - 172.16.0.0 - 172.31.255.255
    - 192.168.0.0 - 192.168.255.255
  - Multicast, if multicast is not being used.
  - Loopback – 127.0.0.0/8
  - ICMP broadcast per RFC 2644 – This will keep a site from being used as a smurf amplifier.
  - UDP echo
- Block packets from outside the filtering device with a source IP address the same as your internal networks. This blocks packets with spoofed IP addresses. This means that you must know what address space is used internally.

Egress – Outbound filtering

Block traffic with an invalid source IP address. This keeps a denial of service attack using IP address spoofing from originating on the internal network. The filter should only allow traffic to leave your network with a source IP address that is valid on your

---

[2] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E. "RFC1918 - Address Allocation for Private Internets" (1996) http://anreg.cpe.ku.ac.th/rfc/rfc1918.html

[3] Strom, Dan "The Packet Filter: A Basic Network Security Tool" (September 25, 2000) http://rr.sans.org/firewall/packet_filter.php

internal networks. The purpose here is to keep a denial of service attack from originating on the private network.

The next line of defense in GIAC's network infrastructure will be a Cisco 4210 Intrusion Detection System (IDS) labeled in Figure 1 as IDSX (IDS External). Located on a Cisco 2950 switch labeled DMZX (DMZ External), the IDS will monitor all traffic passing through the outer-most router mentioned above. Traffic will be evaluated and categorized as acceptable or malicious. Cisco's website says that with their *Secure Policy Manager* software tool (CSPM), [4]network security administrators can visually create high-level security policies based upon business objectives. Policy definition capabilities include the ability to create security policies that define supported and denied services for Cisco PIX Firewalls and Cisco routers running the firewall feature set. Automatic shutoff of traffic from a specific IP address that is perceived to be malicious is possible, but will only be used in extreme cases by GIAC. In most cases, only after the network security staff has deemed traffic to be of a malicious nature will a particular IP address or addresses be filtered out.

Beyond the IDSX defense, GIAC will place a Cisco 515 packet-filtering firewall, labeled DMZX in Figure 1. Using similar rules to those implemented on the ISP2600 router, this firewall is a more robust line of defense, with specific ports and protocols being brought into play, rather than simply confronting potentially damaging IP addresses. Inbound web traffic (secure and unsecured) will be allowed to connect to servers within the DMZ to permit e-Commerce functions to take place. Aimed at preventing DoS traffic from reaching into, or being sent from GIAC's network, it will follow recommended industry standards. According to the NIST's *Guidelines on Firewalls and Firewall Policy*, [5]the firewall rule set should always block the following types of traffic:

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic.
- Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks.
- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
- Inbound traffic containing IP Source Routing information.
- Inbound or Outbound network traffic containing a source or destination address of 127.0.0.1 (localhost).
- Inbound or Outbound network traffic containing a source or destination address of 0.0.0.0.
- Inbound or Outbound traffic containing directed broadcast addresses.

---

[4] Cisco Systems "Cisco Secure Policy Manager Version 3.1"
http://www.cisco.com/en/US/products/sw/secursw/ps2133/products_data_sheet09186a0080092280.html

[5] Wack, J., Cutler, K., Pole, J. "Guidelines on Firewalls and Firewall Policy" (January 2002)
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

The DMZ includes primary and secondary DNS servers, and the CertifiedMail e-mail server GIAC uses for communications to customers deemed "protected" by GIAC's policies. Any e-mails containing account numbers, credit card information, addresses or telephone numbers, or any other specific account information will continue to be sent via Certified Mail currently in use. DMZ servers are connected to the network as most devices are within the GIAC infrastructure, through a Cisco 2950 switch.
Another Cisco 4210 IDS, labeled IDSD will be located just inside the DMZ firewall attached to another Cisco 2950 switch (DMZI). A redundant measure to be sure, but considered necessary to protect the heart of GIAC's e-Commerce site – the Web Servers. As in the case of IDSX, traffic will be evaluated and categorized as acceptable or anomalous and identical rules being applied to traffic considered malicious.

1.2.2 Web Server Details

Connectivity beyond this point will be achieved through a Cisco 6503 switch (WEBX) attached to the DMZI switch. This particular device was chosen because if its built-in ability to utilize IP load balancing. A Cisco white paper on Dynamic Feedback Protocol (DFP) describes it as "[6]a part of Cisco's ContentFlow architecture and the mechanism by which servers provide feedback to IP load-balancing products. DFP is implemented with workload agents that reside on IP server platforms. Workload agents communicate with the load-balancing manager, which is resident on the LocalDirector chassis or Catalyst® 6000 series switch." Attached to the WEBX switch are the external network cards installed in the web servers.

As mentioned in the beginning of the infrastructure section, GIAC's proposed web servers will be configured with Windows 2000 Advanced Server to allow for clustering across multiple servers providing the same function. Multiple servers, combined with load balancing achieved by the WEBX switch, will give the web server functionality a high level of availability, and provide a backup for this valuable resource in case of failure or attack. The web servers will have a second network card installed, adding security by having a separate physical connection to the internal network. These internal NICs are connected to a second Cisco 6503 switch (WEBI), which contains a Layer 3 Supervisor Engine to act as the internal network router.

1.2.3 Access Via VPN or Remote Dial-Up

A goal of GIAC is to decrease turn-around time for artists and photographers submitting work for the various news services that are customers of GIAC. The new trend in coverage of news events is to focus on breaking news, to cover and publish information about an event as soon after it occurs as possible. GIAC aims to contribute to that customer need in any way possible. Plans call for allowing both VPN and Dial-Up access to FTP servers allowing only communication from users with pre-existing accounts. VPN users will attach to a Cisco 3000 VPN Concentrator, provide account

[6] Cisco Systems White Paper "Cisco Dynamic Feedback Protocol"
http://www.cisco.com/en/US/products/sw/iworksw/ps2769/products_white_paper09186a0080091ea9.shtml

information, and be able to connect to either of GIAC's planned FTP servers via externally-addressed network cards. As with the web servers, the FTP servers will be using Windows 2000 Advanced Server to provide clustering, and therefore redundancy in case of failure. Dial-Up users will connect to the FTP network using a bank of modems available in Cisco's AS5300 Remote Access Server. Authentication for both VPN and Dial-Up access will be through a Windows 2000 workstation running Cisco's TACACS+ software. This authentication server will utilize available encryption to protect account information, and will only be controllable from the workstation itself. Inside the FTP servers, a Cisco PIX Firewall (FTP) will restrict access to the internal networks at GIAC. Following the standard firewall guidelines mentioned in the DMZ firewall description, this will allow internal employees access to the files uploaded by contributors, while protecting internal assets. The inside port of the PIX firewall is connected to the Cisco 6503 switch that hosts the inside NICs of the web servers.

1.2.4 Internal Networks

Attached to the WEBI switch will be another firewall (DMZI). This one will differ from the others in that it will be a stateful inspection firewall, defined by [7]Webopedia.com as "also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested". By design, the stateful inspection firewall is able to track multiple, simultaneous TCP/IP connections, and therefore is essential to place between the public access areas and private internal areas of GIAC's network. Vendors and products are still being evaluated at this time, but leading candidates are [8]Check Point's Firewall-1, [9]Netscreen's Model 500, and [10]NetGuard's Guardian Pro.

Connected to the DMZI firewall will be the various subgroups that comprise GIAC's planned e-commerce support team. Connected through Cisco 2950 switches (PAY, APPS & CSDB), these will further segment GIAC network traffic for speed and security using address subnetting. The Payment Services internal network will have at its core, a pair of Windows 2000 servers running Advanced Server to allow for clustering, just as all the multi-server operations at GIAC. Traffic traveling between this, other GIAC

---

[7] Webopedia "Stateful Inspection" (March, 2002) http://www.webopedia.com/TERM/S/stateful_inspection.html

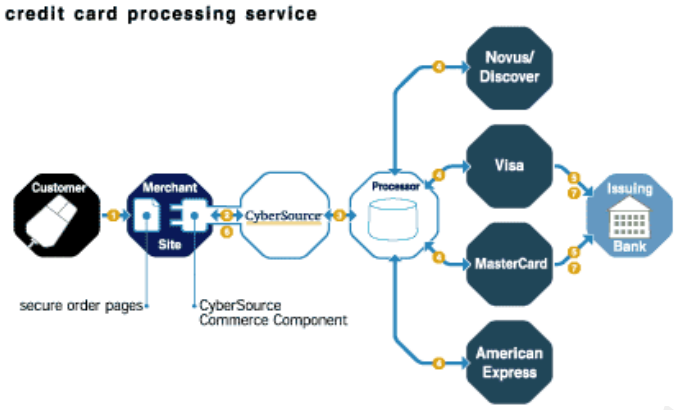
[8] http://www.checkpoint.com/

[9] http://www.netscreen.com/products/NS500.html

[10] http://www.netguard.com/subpages/products_gpro.htm

networks, and CyberSource's credit card processing service will be analyzed by another Cisco 4210 IDS. Since connectivity to CyberSource is through a separate Internet connection, it was deemed necessary to place another security device at this point of ingress/egress.

This diagram and text from CyberSource's website illustrates how real-time, electronic credit card processing works using CyberSource Payment Services.



1. Purchaser places order.
2. Merchant securely transfers order information to CyberSource over the Internet via using a secure, encrypted messaging protocol (SCMP). CyberSource receives order information and performs requested services.
3. CyberSource formats the transaction detail appropriately and securely routes the transaction authorization request through its payment gateway to the processor.
4. The transaction is then routed to the issuing bank (purchaser's bank) to request transaction authorization.
5. The transaction is authorized or declined by the issuing bank or card (Discover, American Express).
6. CyberSource returns the message to the merchant.
7. Issuing bank approves transfer of money to acquiring bank. The acquiring bank, in turn, credits the merchant's account.

The information confirming or denying the order sent by CyberSource to GIAC in Step 6 and is sent via Certified Mail to the ordering customer. This notification process is already in place for the current phone ordering system being replaced by the proposed e-commerce solution.

Also connected to the DMZI firewall will be the Customer Service and Database networks. These will also be segmented by subnet into separate private internal networks. The Database servers are divided into two groups. First is where customer information is stored and used during the ordering process. Unlike the load balancing necessary at the web server connection, this is a simple fail-over setup. Clustering is still employed using Windows 2000 Advanced Server, but server #1 is the active server, and server #2 remaining in standby mode unless a failure occurs on #1. The other servers in the database network are for storage and access of images. These are independent servers, with no clustering involved. Information on all of the database servers is stored in encrypted form and backed up incrementally and daily. The most recent set of tapes remain stored onsite in a fireproof safe, while the previous set of tapes are stored at a secure, fireproof, offsite location. Plans are for images uploaded by individuals via dial-up or VPN to be manually transferred by GIAC staff to the storage servers after certification and encryption. These will be used for waiting projects and made available through the web ordering page when exclusivity agreements allow. The

customer service network will consist of Customer Inquiry staff (existing operators that take phone orders and technical help staff), Product Creation staff (get images to physical form and shipped to customers when ordered in that form), Sales staff, and Marketing & PR staff. GIAC will have an (upgraded) Applications server that runs proprietary software written specifically to interface with customer demographics, image catalogues, and shipping companies.

The third leg off the DMZI firewall consists of the Applications Server network and Domain Servers network. These are segmented by subnet into separate private internal networks. This is where the Office Management staff utilize servers for Human Resources, Payroll, Benefits, and General Administration. Information here is not as volatile as the transaction segment of the company, and therefore live redundancy through clustering or fail-over servers was deemed not necessary. As with all servers though, information on all of these servers is stored in encrypted form and backed up daily. The most recent set of tapes remain stored onsite in a fireproof safe, while the previous set of tapes are stored at a secure, fireproof, offsite location.

GIAC sends routine e-mails through an internal Microsoft Outlook server located within the Domain Servers network. E-mail that contains protected information, such as account information and credit card numbers, is sent using [11]CertifiedMail's "Send Certified™" secure plug-in for Microsoft Outlook. CertifiedMail's product was and is considered the best because of the following [12]advertised features:

- One-click security for e-mail and attachments
- No special software needed to securely read messages
- "Oops" feature retracts sent messages before recipients have read them
- Receive notice when messages were actually opened
- No keys, no certificates required
- Sender determines when message will expire
- Send messages up to 50MB in size

As advised by CertifiedMail case studies, GIAC's CertifiedMail server resides within the Applications Server network discussed previously, and runs an XML engine and database. E-mail recipients connect directly to the CertifiedMail Web server located in the DMZ, also discussed above.

1.2.5 Internal Security and the Intrusion Detection Network

As previously discussed and illustrated in Figure 1, GIAC will employ a force of three Cisco 4210 IDS devices. These will be strategically located to monitor all traffic between mission-critical public and private access points - just inside the border router, between the external firewall and web servers, and between both the Payment Services network and external payment vendors, and the payment servers and the rest of GIAC's assets. Access to the workstation running Cisco's CSPM software is allowed only

[11] CertifiedMail Security Solutions - Secure plug-in for MS-Outlook
http://www.certifiedmail.com/i/products/scbutton.htm
[12] CertifiedMail.com - Moving Fast and Securing a Position in an Emerging Market with .NET Technology (May 2001)
http://www.certifiedmail.com/i/news/Case_Studies/cmcasestudy.pdf

through the local keyboard, rather than network-wide. The network administrators on the technical staff are the only employees that have accounts to access this workstation, as well as the three IDS devices. Network administrators have additional access to the Cisco switches, Remote Access (Dial-Up, VPN) devices, and the firewalls and routers at GIAC. Plans are under development for installing applications that will monitor and report any configuration changes made to network infrastructure devices, but a specific product has not yet been chosen. Existing security on these devices is granted via the Cisco TACACS+ software controlling remote access. GIAC policy requires that when a change is made to the live network devices, a copy of the pre- and post-change configuration is made to the network file server (under applications server network).

Section 1.3 – Business Operations

As GIAC moves toward its goal of an e-commerce presence, maintaining a high degree of availability is obviously key not just to survival, but growth as well. Responsibility for that monumental task will be with the IT staff. By providing for the security and availability of all the components of the e-commerce plan - network infrastructure, servers, remote connectivity – GIAC will have a reliable and profitable facility. Plans for securing availability of and protecting information on the supporting servers supply redundancy, through clustering, and security, by running only those services which are necessary for applications to function, and by allowing controlling access to the servers through limited numbers of restrictive-use accounts. Intrusion Detection is also a big part of the secure business environment, and GIAC's IT staff have provided for three separate traffic monitors to protect against hostile attack and accidental overload. Sensitive information on the servers - credit card numbers, demographics, etc. - has been encrypted to provide additional security in case of accidental disclosure or hostile download. Customers will be able to give vital information to GIAC without fear of compromise.

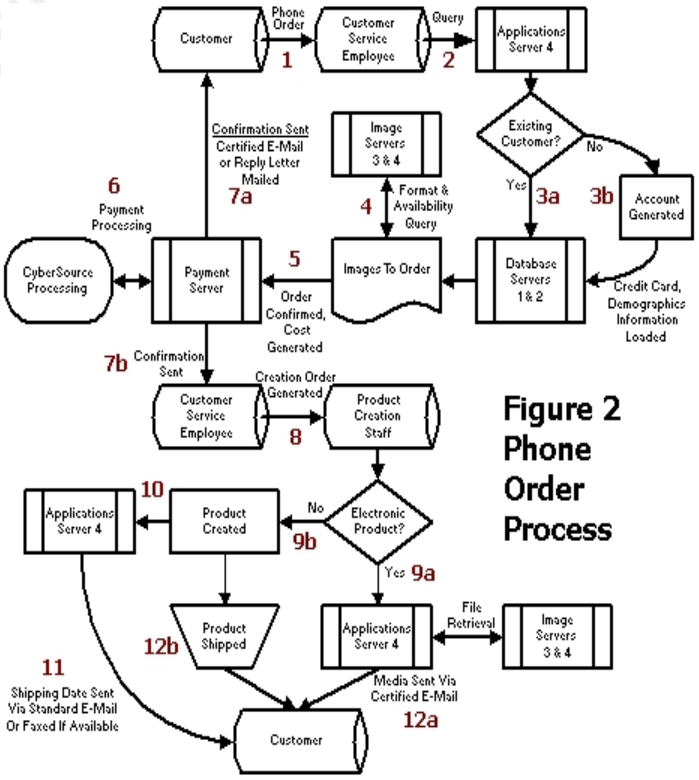


Figure 2 Phone Order Process

1.3.1 Phone Ordering Process

As shown in Figure 2, GIAC will continue to take phone-based orders for its products. Security within the transaction has been increased during the automation of the process. Steps are as follows:

1. Customer calls ordering number, and is connected to

GIAC's customer service team.
2. Customer Service employee uses proprietary application to query for customer demographics.
3a. If customer has existing accounts with GIAC, demographic information necessary for transaction is provided to the customer service employee.
3b. If a new customer, the necessary information is taken down and entered into the GIAC customer data files.
4. Images that customer is requesting are entered into the query initiated on the Image Servers. Customer service staff confirms that the requested format is available.
5. The order is confirmed with the customer, and the order is placed on the payment server.
6. GIAC sends payment information from the payment server directly to CyberSource, using the credit card processing service described in the Internal Networks section above. Data is transferred using SCMP (secure, encrypted messaging protocol). Order approval or denial is sent directly back to the GIAC payment server.
7. An automatic confirmation is generated and sent regarding the status of the customer's order via certified e-mail or if no e-mail is available, a printed copy will be sent via USPS. An additional copy of the order confirmation (if approved) is sent to the customer service employee handling the order.
8. Customer Service then initiates a creation order with the product creation staff. Using proprietary applications, the product creation staff determines how to proceed with delivery of the image(s).
9a. If the request is for electronic copies of an image, the application server retrieves the image files from the image servers.

12a. The application server will automatically send the files via certified e-mail (described later) to the customer, updating all pertinent sections of the internal applications.

9b. If the order is for a printed copy of an image, the production staff will process the order as requested, and the order is prepared for shipping.
10. Change of an order to a status of "completed" will prompt the applications server to generate all shipping labels, and update all pertinent sections of the internal applications.
11. The shipping date for the order is sent to the customer via standard e-mail or via fax if indicated, with sensitive information not included.

12b. The product is shipped by whatever means requested by the customer.

1.3.2 Online Ordering Process

As shown in Figure 3, GIAC will be accepting online ordering as well. Steps are as follows:
1. Customer goes to website (GIAC-Online.com), and is queried regarding interest in signing up for GIAC's customer list, required if orders are to be placed.
2. Web Server uses proprietary application to query for customer demographics.
3a. If customer has existing accounts with GIAC, demographic information necessary for transaction is made available for updating the database servers.

3b. If a new customer, the necessary information is entered by the customer and encrypted and stored in the GIAC customer data files.

4. Customer enters image selections into the query initiated on the image servers. The image servers confirm that the requested format is available and confirms sizing and pricing.

5. The order is confirmed with the customer, payment information is then requested and the order is sent to the payment server.

6. GIAC sends payment information from the payment server directly to CyberSource, using the credit card processing service described in the Internal Networks section above. Data is transferred using SCMP (secure, encrypted messaging protocol). Order approval or denial is sent directly back to the GIAC payment server.

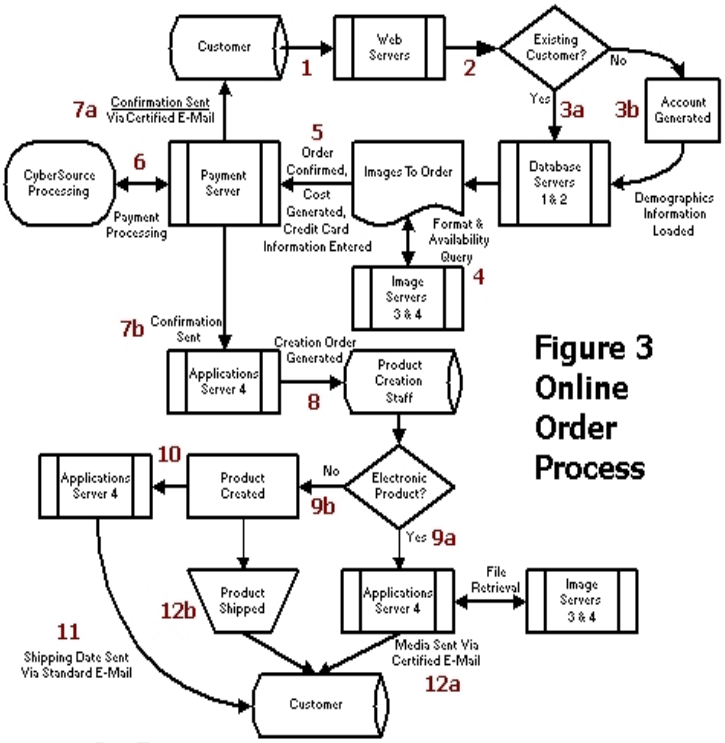


Figure 3 Online Order Process

7. An automatic confirmation is generated and sent regarding the status of the customer's order via certified e-mail or if no e-mail is available, a printed copy will be sent via USPS. An additional copy of the order confirmation (if approved) is sent to the customer service employee handling the order.

8. The application server then initiates a creation order with the product creation staff. Using proprietary applications, the product creation staff determines how to proceed with delivery of the image(s).

9a. If the request is for electronic copies of an image, the application server retrieves the image files from the image servers.

12a. The application server will automatically send the files via certified e-mail (described later) to the customer, updating all pertinent sections of the internal applications.

9b. If the order is for a printed copy of an image, the production staff will process the order as requested, and the order is prepared for shipping.

10. Change of an order to a status of "completed" will prompt the applications server to generate all shipping labels, and update all pertinent sections of the internal applications.

11. The shipping date for the order is sent to the customer via standard e-mail or via fax if indicated, with sensitive information not included.

12b. The product is shipped by whatever means requested by the customer.

1.3.3 Image Upload Process

Contributors to GIAC's vast stock of images are encouraged to upload their own work directly to storage servers at GIAC. In addition to saving time in getting the product to customers, the artist/photographer has more control on how the image is displayed. Connectivity is provided using a bank of modems or via the internet and a VPN tunnel. Both methods use the same database (Cisco's TACACS+) of pre-established accounts to authenticate and encrypt access to the FTP servers. Once authorized, contributors are asked to provide FTP account and password to their individual storage area on the server. Different levels of access are provided at varying costs to meet the individual contributor's need for storage space. Once the files have been uploaded, the contributor must notify GIAC that they are available via phone call or e-mail. GIAC support staff regularly check incoming files to the FTP server for new images to attribute, but final proofs can only be made available to the public after the contributor has provided the file names to GIAC. This protects GIAC against releasing an image not yet ready for distribution.

1.3.4 Certified Mail Process

GIAC uses a CertifiedMail Server running Windows 2000 Advanced Server and a Microsoft-SQL database to provide communications for sensitive materials sent between GIAC and ordering customers. Certified e-mail is sent just like standard e-mail, except that instead of just clicking send, GIAC employees click a "Send Certified" button. A notice is sent to the customer's e-mail address that they have a certified e-mail to retrieve at GIAC-Online.com. A link is provided that directs the addressee to the appropriate server, authenticates that they are indeed who they claim to be, and the e-mail is displayed. Customers also have reply functions available from the CertifiedMail server as well.

Assignment 2 – Identify Risks

At GIAC-Online, there are several areas of risk to deal with upon entering the realm of e-commerce. The National Institute of Standards & Technology (NIST) has published a risk management guide that deals with every aspect of risk management and organized a step-by-step checklist for companies. After comparison with other documents, GIAC has deemed this publication "the most useful of its kind" and employees should "refer to this publication as the ultimate guide" for analyzing and minimizing risk.

Section 2.1 – GIAC Risk Management Study

GIAC consulted with NIST's *Risk Management Guide for IT Systems* to determine what should be considered at-risk, and how these concerns should be addressed. A checklist was created keeping in mind that it should "[13]contain the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, information), non-automated procedures,

[13] Stoneburner, G., Goguen, A., Feringa, A "Risk Management Guide for Information Technology Systems" (October 2001) http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

processes, and information transfers associated with a given IT system in the following security areas:
Management Security covers the following risks: Assignment of responsibilities, Continuity of support, Incident response capability, Periodic review of security controls, Personnel clearance and background investigations, Risk assessment, Security and technical training, Separation of duties, System authorization and reauthorization, and System or application security plan.

Operational Security deals with risks from the following: Control of air-borne contaminants (smoke, dust, chemicals), Controls to ensure the quality of the electrical power supply, Data media access and disposal, External data distribution and labeling, Facility protection (e.g., computer room, data center, office), Humidity control, Temperature control, and Workstations, laptops, and stand-alone personal computers.

Technical Security addresses risks from: Communications (e.g., dial-in, system interconnection, routers), Cryptography, Discretionary access control, Identification and authentication, Intrusion detection, Object reuse, and System auditing.

NIST defines risk as being a result of multiplying the likelihood of an occurrence by the impact of that occurrence.
Definitions of levels of likelihood are:

- High: The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
- Medium: The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- Low: The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Definitions of magnitude of impact are:

- High: Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
- Medium: Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
- Low: Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

All planned systems and associated processes at GIAC were analyzed subject to these standards, and the following areas were determined to be of greatest risk to compromise:

- ❖ Database/Image Servers (the "crown jewels" of GIAC's treasury)
- Web Servers
- Internal Applications

Section 2.2 – Risk 1: Database/Image Servers

Risk 1 Overview

In upgrading GIAC's mission to include e-commerce, few assets and processes will remain as they currently exist. One of these will be in the area of storage and usage of the images upon which GIAC depends for existence. GIAC does not own the majority of these images, the original contributing artist does, with GIAC is acting as a broker for the marketing and distribution of the products. Therefore, compromise of these assets GIAC has been entrusted with would be fatal to the integrity of the company, and more than likely, the company itself. Compromise could result from:

1. Images stolen and used for profit by someone not legally able to do so. This could include other artists, other image provider companies, internal GIAC staff or external individuals/entities with either an axe to grind against GIAC or its contributing artists, or just randomly hacking to find vulnerabilities in internet servers.
2. Credit card information stolen/modified/corrupted and used to charge items illegally or prevent business transactions from taking place at all. This could result in the worst case scenario of legal action being taken against GIAC. Most likely would be the loss of trust in GIAC and its services. In this business, customers gain knowledge of a company and refer others to that company by word-of-mouth. Negative publicity would be passed just as effectively as a recommendation, and the results would be disastrous.

Risk 1 Damage Potential

Overwhelming potential for damage exists if information on GIAC's database servers was compromised by internal or external means. Potential damage to data files could occur from several threatening scenarios:

- Malicious External Attack - A hacker that penetrates GIAC's defensive layers (external router and firewalls and/or remote-access devices) would be able to access files on the database/image servers and either steal or corrupt them. While the files are protected during storage using encryption, damage could still occur to the server itself through outright deletions or virus attachment.
- Internal Destruction or Theft – A disgruntled employee could do far more damage than an external attacker. Since GIAC has entrusted the particular employee with access, the software used to encrypt the data/images within GIAC would be available to decrypt and steal images. While similar to an external attack, damage could occur far more quickly given local access to servers.
- Accidental Destruction - System/server failure could potentially damage files being processed, or files that have been added or modified since the last backup.

Loss of existing and future customers and possible legal action against GIAC would be the death knell of this growing business. Of the threats to the database/image servers, the one that is the most crucial at this point is from internal damage, either malicious or

accidental. These servers are not accessible from outside GIAC, so there is no identified risk of external exploitation. As GIAC moves to make images available online, emphasis will shift to protecting these servers from external attacks. Massive damage to existing files of images and customer information would be costly in both fiscal and public image areas.

Risk 1 Mitigation

GIAC's proposed infrastructure and procedural upgrade will mitigate the risk involved in protecting the integrity of the database/image servers by use of the following:

1. Database/image servers are segmented into their own private network internally. Access from internal systems is only through a stateful inspection firewall.
2. External access to the database/image servers adds several more layers of defense. Through the internet access is either through the border router and external firewall, or the border router, remote access server and FTP firewall. Dial-Up access would be through the remote access server and FTP firewall.
3. Servers located in the DMZ (DNS & E-Mail) are blocked from initiating any connections beyond the stateful inspection firewall, or anywhere on the internal network.
4. Queries to the data stored on the database/image servers will be performed by separate applications located beyond the stateful inspection firewall.
5. Database/image servers will be single-function devices, performing only those tasks and rejecting any other traffic.
6. Data on the database/image servers is incrementally backed up to onboard files several times daily. Those files are backed up to tape daily, after end-of-business-day processes have been run (closing books, settling of batch files, etc.). Those files are deleted after confirmation of a clean backup has been achieved. Current backup policy is only once a day, just before end-of-business-day processes.
7. Direct access to the database/image servers will be restricted to need-to-know personnel. Only those IT personnel with job-specific functions (i.e. server administrators) will be granted accounts. Password expiration will be weekly, upgrading the current policy of monthly password generation.
8. Audit trails will be used within the proprietary applications to enforce accountability for Customer Service staff. Current application software has no means of performing audit trails.
9. In addition to checking references and a lengthy interview for Customer Service personnel, a simple credit history and legal background check will be performed. This is an upgrade of current policy, which requires only the interview and reference check process. Current policy only requires the interview and a reference check.
10. Servers are kept behind controlled-access doors in a climate-controlled room.
11. Power is provided through multiple uninterruptible power supplies (UPS) that condition the energy source and provide battery backup to allow for orderly shutdown of servers in the event of a total power loss.

Steps 1-5 are part of the new implementation project and therefore will be new procedures that must be developed. Steps 6-9 represent an upgrade in protection strategy that will enhance current policies and/or procedures. Steps 10 and 11 reflect current practice at GIAC.

Risk 1 Overall Assessment

Given the extreme potential for damage should an exploitation occur, the impact for this risk has been classified as High. The more mitigation steps that are taken as listed, the more the likelihood is reduced to Low, categorizing this as an overall Medium Risk. Using all of the mitigation factors will reduce threat likelihood to bare minimum, ensuring that GIAC's data will be protected and providing GIAC documentation to back up that claim.

Section 2.2 – Risk 2: Web Servers

Risk 2 Overview

Although GIAC currently maintains a web presence, e-commerce will be a radical change in terms of security. Images will retain the GIAC watermark (see example 1) and any artist-provided copy right notations (see example 2).

Example 1

Example 2

The services provided by the web servers are the originating interface with new customers, and GIAC's lifeline for existing customers. Loss of confidence in the integrity of what is posted would be disastrous for this growing company. Incorrect or altered pricing and misspelled or mismatched images and descriptions would certainly make a customer hesitant when deciding to utilize GIAC for images and online purchases. Potential contributors to GIAC would also question whether their work would be safe in GIAC's hands if appropriate protective measures were not obvious.

The integrity of these servers is crucial to maintaining the integrity of GIAC. GIAC must consider the following when planning web server security:

- Artists and photographers will cease to employ GIAC to distribute their images if original works are not protected from unauthorized use.

    - Image Integrity: Contributors will discontinue using GIAC as their image broker. Without fresh material, GIAC will be unable to meet its goal of providing the graphic edge it promotes in media-targeted advertising, and therefore lose a mission of the company. GIAC's business depends on news sources to a large degree to meet its day-to-day income projections.
- Customers enter credit card and image details on the web servers during the ordering process. If the web servers aren't functioning properly, orders can't occur or be processed and customers will be forced elsewhere for their products.
    - Web Servers Functionality Disabled: GIAC will lose existing customers if downtime occurs frequently. New customers have already made their judgment if web servers are down – "*It doesn't work...guess I'll look elsewhere*".
- GIAC's bottom line depends on sales, and prices must reflect contractually agreed upon values or business will suffer. Pricing changed maliciously or through typing errors by GIAC staff will have detrimental effects on sales.
    - Content errors/alteration: The web server is GIAC's first and only opportunity to reach new online customers. Pricing and/or content errors will hurt GIAC by discouraging the customer unfamiliar with GIAC and the quality services that could be offered... "*if only the website was available and I could trust what I see*". Returning customers will likely reach a point where they begin shifting orders away from GIAC to competitors.

Risk 2 Damage Potential

Overwhelming potential for damage exists if information on GIAC's public web servers is compromised by internal or external means. Potential damage to web servers could occur from several threatening scenarios:

- Malicious External Attack - A hacker that penetrates GIAC's outer defensive layers (external router and firewall) and server account security could potentially access files on the public web servers and alter information on them or damage them through deletions or virus attachment. Damage in this scenario could range from merely embarrassing, in a case of vandalism, to the completely destructive, where the entire web server could be taken over and destroyed.
- A Denial of Service (DoS) attack could render GIAC's servers unavailable to customers. Lack of sales would affect GIAC rather quickly, since many news services depend on GIAC for products and would take their business elsewhere.
- Internal Error – Incompetent employees with poor typing and/or editing skills would be damaging to GIAC as well. Enough errors and customers would no longer trust the web server content, driving them to other providers rather quickly.
- Accidental Destruction - System/server failure could potentially damage information being processed.

Risk 2 Mitigation

GIAC's proposed infrastructure and procedural upgrade will mitigate the risk involved in protecting the integrity of the web servers by use of the following:

1. Web servers are restricted-use devices, running only those services necessary to provide web functionality and only through port 80 and any others deemed necessary by web server applications.
2. Web servers have separate network interface cards providing different points of access from external and internal sources.
3. Access to internal networks is also restricted by a stateful inspection firewall.
4. Traffic that is suspicious, particularly denial-of-service attacks, will be blocked by the IDS located between the web servers and the internet.
5. Failover and redundancy is achieved through the use of multiple servers running Windows 2000 Advanced Server.
6. Local access to the web servers will be restricted to need-to-know personnel. Only those IT personnel with job-specific functions (i.e. server administrators) will be granted accounts. Password expiration will be weekly, upgrading the current policy of monthly password generation.
7. Data on the web servers is incrementally backed up to onboard files several times daily. Those files are backed up to tape daily, after end-of-business-day processes have been run (closing books, settling of batch files, etc.). Those files are deleted after confirmation of a clean backup has been achieved. Current backup policy is only once a day, just before end-of-business-day processes.
8. Servers are kept behind controlled-access doors in a climate-controlled room.
9. Power is provided through multiple uninterruptible power supplies (UPS) that condition the energy source and provide battery backup to allow for orderly shutdown of servers in the event of a total power loss.

Step 1 is currently in place with existing web servers. Steps 2-5 are part of the new implementation project and therefore will be new procedures that must be developed. Steps 6 and 7 represent an upgrade in protection strategy that will enhance current policies and/or procedures. Steps 8 and 9 reflect current practice at GIAC.

Risk 2 Overall Assessment

Given the potential for financial damage should an exploitation occur, the impact for this risk has been classified as Medium. Mitigation steps that are taken as listed will further reduce the likelihood Low, placing this risk in the Low-Medium category. Using all of the mitigation factors will reduce threat likelihood to a negligible level, ensuring that GIAC's web servers will continue to function and a reliable web presence will result.

Section 2.3 – Risk 3: Internal Applications

Risk 3 Overview

GIAC currently utilizes proprietary software for customer server applications - placing orders, answering questions, assisting contributors in delivering products – but the proposed e-commerce project will demand more applications, more personnel, and more security. GIAC must consider the following risks when planning Internal Application security:

- Sensitive Information Protection
    - Customer Service staff will be accessing sensitive materials, such as credit card numbers, through queries.
- Accurate Ordering Information
    - Customer Service Staff will be assisting phone order customers and must have accurate product information to perform quality work.
    - Customers ordering products online must also have accurate information to complete the ordering process.
- Customer Service Support
    - Customer Service Staff will be entering credit card numbers during the phone order process. Accuracy must be achieved to ensure the correct customer gets what is ordered and that GIAC doesn't lose money in faulty transactions.
    - Customers ordering products online will be entering credit card numbers during the order process. Accuracy must be achieved to ensure the correct customer gets what is ordered and that GIAC doesn't lose money in faulty transactions.
    - Product Creation and Delivery staff must have accurate information to produce images that the customer has ordered, whether it is electronic transfer or physical reproductions.
- Financial Transactions
    - Credit card information submitted to CyberSource for processing must be accurate and submitted in a timely fashion.

Risk 3 Damage Potential

Potential damage to data files could occur from several threatening scenarios:

- Malicious External Attack - A hacker that penetrates GIAC's defensive layers (external router and firewalls and/or remote-access devices) could potentially access files on the application servers and either steal or corrupt them. Theft of information, both financial and image data, would seriously damage GIAC's reputation as a secure processor.
- Internal Destruction or Theft – A disgruntled employee could do far more damage than an external attacker. Since GIAC has entrusted the particular employee with access, the software used to encrypt the data/images within GIAC would be available to decrypt and steal images. While similar to an external attack, damage could occur far more quickly given local access to servers.
- Internal Error – Inaccuracy during the online and phone ordering process could lead to excessive frustration by the customer and propel them to GIAC's competitors. Inaccuracy during the product creation stage, can cause a multitude of errors: incorrect electronic file format, image size, incorrect images, or incorrect shipping to name a few. Customers could likely request a refund of money and try another vendor rather than wait for a resolution from GIAC.
- Accidental Destruction - System/server failure could potentially damage files being processed, or files that have been added or modified since the last backup.

- Delays in order processing through CyberSource could cause customers to reject GIAC's services as well.

Risk 3 Mitigation

GIAC's proposed infrastructure and procedural upgrade will mitigate the risk involved in internal application functionality by use of the following:

1. Application servers are segmented into their own private network internally. Access from internal systems is only through a stateful inspection firewall.
2. External access to the Application servers adds several more layers of defense. Through the internet access is either through the border router and external firewall, or the border router, remote access server and FTP firewall. Dial-Up access would be through the remote access server and FTP firewall. All access points listed block unauthorized traffic.
3. Servers located in the DMZ (DNS & E-Mail) are blocked from initiating any connections beyond the stateful inspection firewall, or anywhere on the internal network.
4. Applications servers will be single-function devices, performing only those tasks and rejecting any other traffic.
5. Failover and redundancy is achieved through the use of multiple servers running Windows 2000 Advanced Server.
6. Data on the application servers is incrementally backed up to onboard files several times daily. Those files are backed up to tape daily, after end-of-business-day processes have been run (closing books, settling of batch files, etc.). Those files are deleted after confirmation of a clean backup has been achieved. Current backup policy is only once a day, just before end-of-business-day processes.
7. Local access to the application servers will be restricted to need-to-know personnel. Only those IT personnel with job-specific functions (i.e. server administrators) will be granted accounts. Password expiration will be weekly, upgrading the current policy of monthly password generation.
8. Audit trails will be used within the proprietary applications to enforce accountability for Customer Service and IT staff. Current application software has no means of performing audit trails.
9. In addition to checking references and a lengthy interview for IT Applications personnel, a simple credit history and legal background check will be performed. This is an upgrade of current policy, which requires only the interview and reference check process. Current policy only requires the interview and a reference check.
10. Servers are kept behind controlled-access doors in a climate-controlled room.
11. Power is provided through multiple uninterruptible power supplies (UPS) that condition the energy source and provide battery backup to allow for orderly shutdown of servers in the event of a total power loss.

Steps 1-5 are part of the new implementation project and therefore will be new procedures that must be developed. Steps 6-9 represent an upgrade in protection

strategy that will enhance current policies and/or procedures. Steps 10 and 11 reflect current practice at GIAC.

Risk 3 Overall Assessment

Given the potential for financial, legal and public image damage should an exploitation occur, the impact for this risk has been classified as High. Mitigation steps that are taken as listed will further reduce the likelihood Low, placing this risk in the Medium category. Using all of the mitigation factors should reduce threat likelihood to essentially none, ensuring that customers can place a high degree of trust in GIAC's ordering and payment process. Retention of current customers and the promise of confidentiality of new customer data will result in continued growth for GIAC.

Assignment 3 – Evaluate and Develop Security Policy

GIAC used the SANS Institute's "[14]*Server Security Policy*" as the template for its own policy. GIAC's existing policy has been included in Appendix B.

Section 3.1 – Evaluation of Existing Security Policy

GIAC has policies on file pertaining to Information Security. With the implementation of an e-commerce solution, whole new sections of policy will need to be added and existing sections will need to be updated. GIAC's policy on server security has both good and points and these will be compared in the evaluation section.

Purpose Statement

This section is very direct and precise. The purpose is described without going into large discussions about intentions beyond what is needed to achieve the objective of protecting information and the people that access it. Unfortunately, the text could expanded somewhat to further describe exactly from whom/what is the policy protecting the servers. This might provide added incentive about the seriousness of this policy.

Scope Statement

The scope section is also efficient in limiting the text to a generalized "what is a covered server" approach. GIAC will probably need to expand this scope to include descriptions of the various server segments within its network infrastructure and the differences inherent in their functionality. GIAC should also include the DMZ servers. A separate DMZ policy can be established, but since all of the equipment located in the DMZ (DNS and E-mail) is server-based, it should not be excluded entirely from policy discussion about security aspects and requirements of servers.

Policy – Ownership and Responsibility

[14] SANS Institute "The SANS Security Policy Project" http://www.sans.org/newlook/resources/policies/Server_Security_Policy.pdf

The section of the policy that pertains to ownership of assets establishes accountability, as it should, but fails to mention specifically which assets are controlled by which operational group. Since GIAC has only one technical support group, it would seem obvious that the IT group is responsible for maintenance and setup of these servers. However, application support staff within the management group are considered the owners of their systems (HR, payroll). In fact, the IT group is comprised of several sub-groups, each of which is responsible for different servers within GIAC. Inclusion of such detail may pack unnecessary information into the text and make the purpose of this section less clear.

Policy – Configuration Guidelines

This section is a good starting point for directing the various responsible groups on practices to follow when configuring a server. GIAC policy should be more restrictive when it comes to server configuration (and testing) in an e-commerce environment. Patches should not be applied directly to live systems, but tested on an isolated server to confirm its viability. GIAC has, in its IT department, a server set aside for this purpose, so it should be mentioned in this policy. Another item that perhaps needs to be addressed is the use of the vague "if possible", "where practical" and "If a methodology is available". If such guidelines are unable to be met, the reasons for non-compliance should be documented by the responsible group. A statement about this needs to be included in this policy.

Policy – Monitoring

The monitoring section is clear, concise, and descriptive. It is also lacking in spots for a facility engaging in e-commerce. Logs and backups of log data must be maintained for a considerably longer period of time to ensure business operational integrity, and to have proof if an incident should occur that would threaten said integrity. Compromise of sensitive data could lead to legal action, and forensic evidence could provide clues and point to a perpetrator, whether it be intentional, accidental, or mechanical. Disputed charges on a credit card must also be dealt with, and without a specific timeframe mentioned, could occur months or even years beyond GIAC processing time.

Policy – Compliance

The compliance section is good, but can also be improved. Audits "performed on a regular basis" need to have the timeframe and modality defined here. Random audits are also a good idea to catch things that might occur between a lengthy audit period. Information Security staff are mentioned as those responsible for managing the audits. To avoid any appearance of impropriety, there should be one individual responsible for overseeing this task, and they should directly report findings to the managerial group, or CEO-level personnel. This would decrease the possibility that the process could be corrupted in some manner by a mid-level manager.

Policy – Enforcement

The enforcement section needs to be expanded upon. Detailed descriptions of violations and consequences need to be provided for employee education and guidance.

Policy – Revision History

Existing GIAC server security policy has (according to documentation) undergone no revisions. To be effective, annual or semi-annual review of policy will be made a separate policy and procedures for doing so will be created. An effective date must be included in the revision history section as well. Without a start date, the policy hasn't ever really been in effect.

Section 3.2 – Revised Security Policy Update

Changes to GIAC's Server Security Policy have been made and are highlighted within the following policy.

Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by GIAC-Online. Effective implementation of this policy will minimize unauthorized access to GIAC-Online proprietary information and technology. This includes non-GIAC personnel with malicious intent that would seek to harm GIAC as a business, as well as GIAC employees that are responsible but put task completion speed ahead of security and accuracy.

2.0 Background
Servers house the foundation of GIAC's business. Without servers, GIAC provides no images to its customers. Without customers, GIAC does not exist. The protection of the servers and the images contained therein must be the highest security priority in GIAC's inventory. This policy on securing database/image servers must be known by all employees at GIAC, not just technology-oriented departments. Security training is addressed in other sections of policy but is just as vital to the success of this policy, and therefore the company. Security incidents are also addressed in other sections to serve as a guide for managers and employees.

3.0 Scope
This policy applies to server equipment owned and/or operated by GIAC-Online, and to servers registered under any GIAC-owned internal network domain. Support staff in each group (Applications Support, Customer Service, Information Technology, Office Management) are responsible for abiding by this policy. This policy is specifically for equipment on the internal GIAC-Online networks and servers located in the DMZ.

Expanded detail on secure configuration of equipment external to GIAC-Online on the DMZ can be referenced in the Internet DMZ Equipment Policy.

4.0 Policy

4.1 Ownership and Responsibilities

All internal servers deployed at GIAC-Online must be owned by an operational group that is responsible for system administration. Approved server configuration guidelines are established and maintained by each operational group, based on business needs and approved by personnel responsible for Information Security. Designated security personnel within operational groups must monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group has established a separate process for changing the configuration guidelines, which includes review and approval by a member of the Information Security staff.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow established change management procedures as set forth in GIAC policy and procedures.

4.2 General Configuration Guidelines

- Operating System configuration will be in accordance with approved Information Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services will be logged and/or protected through access-control methods if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers are to be physically located in an access-controlled environment.

- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- Configuration guidelines that are required but are not able to be achieved due to software, hardware, or other technical limitations will be documented and included in the particular operational group's setup guide.

4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 4 weeks.
- Every-3-Hour incremental tape backups will be recycled no sooner than 48 hours after backup.
- Daily full tape backups will be retained for at least 4 weeks.
- Weekly full tape backups of logs will be retained for at least 1 year.
- Monthly full backups will be retained for a minimum of 3 years.

Security-related events will be reported to Information Security staff, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

4.4 Compliance

- Audits will be performed
    - On a regular basis by authorized organizations within GIAC-Online.
    - At random intervals not scheduled by procedures.
    - As soon as technically feasible after an incident has occurred.
- Audits will be managed by the internal audit group or staff responsible for Information Security, in accordance with the Audit Policy. Information Security staff will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification. A monthly report will be made to managerial staff outlining incidents, resolutions, trends, and necessary policy changes.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. The direct supervisor of an employee is responsible for documenting policy violations and forwarding information to Human Resources for inclusion in the employee's file when deemed appropriate. Server security violations and sanctions are defined as follows:

I. Level I Breaches (Least Severe):
    a. Sharing passwords,
    b. Failing to logout of a console when left unattended,
    c. Unlicensed use of software,

i. Corrective action: Retraining with verbal or written warning.

II. Level II Breach:
    a. Repeated Level I breach (a trend of non-compliance),
    b. Accessing customer records without a legitimate "need-to-know" as described in the employee's job description,
    c. Using another employee's login without the employee's authorization,
    d. Accessing personnel records, payroll or other confidential Human Resources information without a legitimate reason,
    e. Verbal or written disclosure of confidential information without proper reason or authorization.
        i. Corrective action: Written warning with possible termination.

III. Level III Breach (Most Severe)
    a. Acquiring/releasing information for personal gain,
    b. Destroying or altering information intentionally,
    c. Acquiring/releasing information with the intent to harm an individual or the organization.
        i. Corrective action: Termination with possible legal action.

6.0 Definitions

Term Definitions

1. DMZ De-militarized Zone: A network segment external to the corporate production network.
2. Server: For purposes of this policy, a Server is defined as a networked GIAC-Online owned and operated Server.
3. Desktop machines and Lab Testing equipment are not relevant to the scope of this policy.

7.0 Revision History

Effective Date: December 1st, 2002
Revised Effective Date: February 28th, 2003*

* Effective upon completion of e-Commerce project. This date will be revised to reflect actual, rather than target, date once it has been achieved.

Assignment 4 – Develop Security Procedures

Server Data Backup Procedures

Effective date: February 1st, 2003

1.0 Purpose

To define processes and procedures involved in backing up data on GIAC servers.

2.0 Background

As detailed in GIAC's Server Security Policy, data integrity is an important component in services that are provided at GIAC. The following guidelines will be used to ensure that current copies of data on any servers at GIAC will be protected from destruction.

3.0 Scope
This procedure applies to any server deployed at GIAC-Online, including application, data, domain, payment and e-mail servers.

4.0 Ownership and Responsibilities
Information Technology staff are required to follow these guidelines and to report any failures involved using the backup log sheet (Appendix C). Partnered with GIAC in this endeavor is The Fortress, an offsite data storage facility. The Fortress operates on a 24x7x365 availability, but courier service is not available on weekends.

5.0 Procedure

5.1 Software/Hardware
GIAC uses [15]Yosemite Technologies' Tapeware software to backup all server data to tape. Daily backups are full coverage, that is, all data on a server. Incremental backups will occur every 3 hours, and will only backup files that have been altered since the last backup procedure. All servers have their own tape drive and individual tapes are labeled for each server using the following nomenclature:

- Daily Full Backups
  - (Week#)-(DayofWeek)-(ServerCode)
  - Example: "2-THU-PAY1" is week 2 of 4, Thursday evening's backup of Payment Server #1.
- Incremental Backups
  - (DayofWeek)-(ServerCode)
  - Example: "MON-IMG2" is Monday's incremental backup tape for Image Server #2.

5.2 Process
The IT Server backup designee (IT personnel rotate through this position) will perform all server backup duties for their assigned day. Duties follow this schedule:
8-9 am

- Review system logs from night before, noting any inconsistencies or failures and follow-up measures taken on the backup log sheet (Appendix C).
- Recover successful tapes for storage in onsite fire-proof vault.
- Recover previous day's tapes for transport by Fortress personnel to off-site storage.
- Prepare tapes for incremental backups scheduled for 10:00, 13:00, 16:00, 19:00, 01:00, 04:00 and 07:00. All servers must have appropriate tapes for incremental backup loaded and in working order.

After every scheduled incremental backup during the day (10:00, 13:00)

[15] Yosemite Technologies "Tapeware" Software http://tapeware.com

- Review system logs, noting any inconsistencies or failures and follow-up measures taken on the backup log sheet (Appendix C).
- Evening shift (4pm – Midnight) IT personnel will follow similar review practices for the 16:00 and 19:00 incremental backups.

10-11 am (Monday-Friday Only)

- Receive off-site stored tapes from Fortress courier. Store tapes in onsite fire-proof vault until ready for use. Deliveries should include incremental tapes for two days after, and daily tapes for the next day based on the following schedule:
    - Monday: Wednesday and Thursday's incremental tapes and Monday & Tuesday's daily tapes
    - Tuesday: Friday's incremental tapes and Wednesday's daily tapes
    - Wednesday: Saturday's incremental tapes and Thursday's daily tapes
    - Thursday: Sunday's incremental tapes and Friday's daily tapes
    - Friday: Monday & Tuesday's incremental tapes and Saturday & Sunday's daily tapes
- Hand over tapes to Fortress courier to be stored off-site based on the following schedule:
    - Monday: Wednesday, Thursday & Friday's incremental tapes and Thursday, Friday & Saturday's daily tapes
    - Tuesday: Saturday's incremental tapes and Sunday's daily tapes
    - Wednesday: Sunday's incremental tapes and Monday's daily tapes
    - Thursday: Monday's incremental tapes and Tuesday's daily tapes
    - Friday: Tuesday's incremental tapes and Wednesday's daily tapes

9pm

- Evening shift IT personnel will load appropriate tapes for full daily backup. All servers must have appropriate tapes for full backup loaded and in working order.

Appendix A: GIAC-Online Planned Network Infrastructure

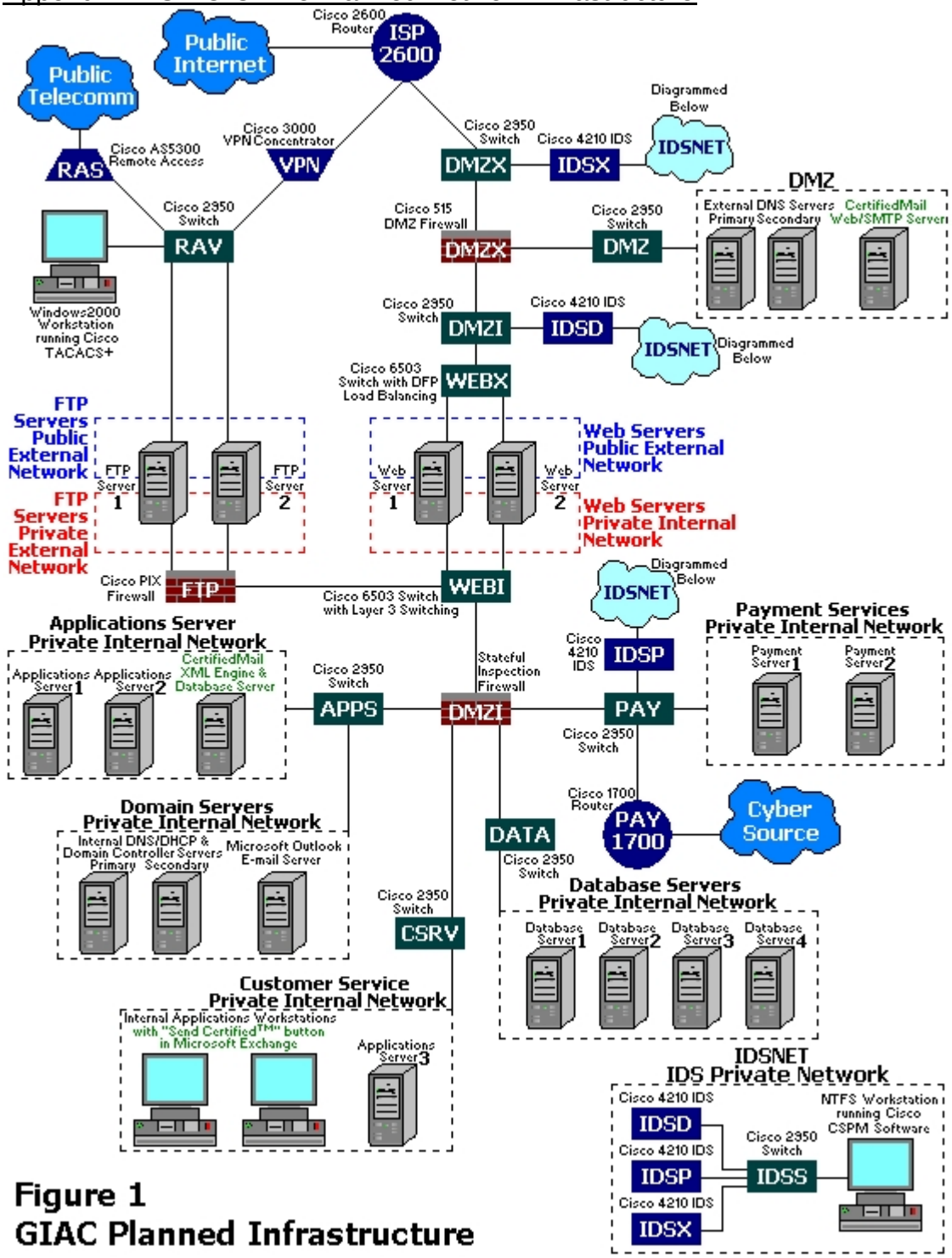


Figure 1
GIAC Planned Infrastructure

Appendix B: Policy Example

Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by GIAC-Online. Effective implementation of this policy will minimize unauthorized access to GIAC-Online proprietary information and technology.

2.0 Background
Servers house the foundation of GIAC's business. Without servers, GIAC provides no images to its customers. Without customers, GIAC does not exist. The protection of the servers and the images contained therein must be the highest security priority in GIAC's inventory. This policy on securing database/image servers should be known by all employees at GIAC, not just technology-oriented departments. Security training is addressed in other sections of policy but is just as vital to the success of this policy, and therefore the company.

3.0 Scope
This policy applies to server equipment owned and/or operated by GIAC-Online, and to servers registered under any GIAC-owned internal network domain.
This policy is specifically for equipment on the internal GIAC-Online networks. For secure configuration of equipment external to GIAC-Online on the DMZ, refer to the Internet DMZ Equipment Policy.

4.0 Policy

4.1 Ownership and Responsibilities
All internal servers deployed at GIAC-Online must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by personnel responsible for Information Security. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the Information Security staff.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.

- Configuration changes for production servers must follow the appropriate change management procedures.

4.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved Information Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

Security-related events will be reported to Information Security staff, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

4.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within GIAC-Online.
- Audits will be managed by the internal audit group or staff responsible for Information Security, in accordance with the Audit Policy. Information Security

staff will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

5.0 Enforcement

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

6.0 Definitions

Term Definitions

1. DMZ De-militarized Zone: A network segment external to the corporate production network.
2. Server: For purposes of this policy, a Server is defined as an internal GIAC-Online Server.
3. Desktop machines and Lab equipment are not relevant to the scope of this policy.

7.0 Revision History

Appendix C: Server Backup Log Sheet

Date: _____

Time: 01:00	Anomalies?: No	Yes	(Explain below)
Time: 04:00	Anomalies?: No	Yes	(Explain below)
Time: 07:00	Anomalies?: No	Yes	(Explain below)
Time: 10:00	Anomalies?: No	Yes	(Explain below)
Time: 13:00	Anomalies?: No	Yes	(Explain below)
Time: 16:00	Anomalies?: No	Yes	(Explain below)
Time: 19:00	Anomalies?: No	Yes	(Explain below)
Time: 22:00	Anomalies?: No	Yes	(Explain below)

Details (remember to include Server & tape name, detailed description of failure/problem and resolution, and your signature)

References

Microsoft Windows 2000 Advanced Server "Introducing Windows 2000 Advanced Server"
http://www.microsoft.com/windows2000/advancedserver/evaluation/business/overview/advanced.asp

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E. "RFC1918 - Address Allocation for Private Internets" (1996)
http://anreg.cpe.ku.ac.th/rfc/rfc1918.html

Strom, Dan "The Packet Filter: A Basic Network Security Tool" (September 25, 2000) http://rr.sans.org/firewall/packet_filter.php

Cisco Systems "Cisco Secure Policy Manager Version 3.1"
http://www.cisco.com/en/US/products/sw/secursw/ps2133/products_data_sheet09186a0080092280.html

Wack, J., Cutler, K., Pole, J. "Guidelines on Firewalls and Firewall Policy" (January 2002)
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

Cisco Systems White Paper "Cisco Dynamic Feedback Protocol"
http://www.cisco.com/en/US/products/sw/iworksw/ps2769/products_white_paper09186a0080091ea9.shtml

Webopedia "Stateful Inspection" (March, 2002) http://www.webopedia.com/TERM/S/stateful_inspection.html
http://www.checkpoint.com/
http://www.netscreen.com/products/NS500.html
http://www.netguard.com/subpages/products_gpro.htm

CyberSource "How It Works – Credit Card Processing"
http://www.cybersource.com/products_and_services/electronic_payments/credit_card_processing/howitworks.xml

CertifiedMail Security Solutions - Secure plug-in for MS-Outlook
http://www.certifiedmail.com/i/products/scbutton.htm

CertifiedMail.com - Moving Fast and Securing a Position in an Emerging Market with .NET Technology (May 2001)
http://www.certifiedmail.com/i/news/Case_Studies/cmcasestudy.pdf

Stoneburner, G., Goguen, A., Feringa, A "Risk Management Guide for Information Technology Systems" (October 2001)
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

SANS Institute "The SANS Security Policy Project" http://www.sans.org/newlook/resources/policies/Server_Security_Policy.pdf

Yosemite Technologies "Tapeware" Software http://tapeware.com