Global Information Assurance Certification Paper

GIAC Security Leadership Certificate (GSLC)

Management Review of Recommended Information Technology (IT) Infrastructure for GIAC Fortune Cookies Inc.

Practical Assignment Version 2.0 (revised April 19, 2004)

By Erik J. Mogelgaard

June 2004

Abstract:

Alfredo Lopez proposed an information technology (IT) infrastructure for Global Information Assurance Certification (GIAC) Fortune Cookie Inc. [GFCI], an international company based in Miami, FL engaged in interactive e-commerce. The proposed architecture has a focus on security, as the cookie fortune business is high margin and high pressure, with a short turn around required on information transactions. This industry is characterized by ruthless competition. Infrastructure attacks and efforts to obtain intellectual property by every means are common. This document is an analysis of the design using measurements that include engineering, finance and risk mitigation. A recommendation on incorporation of the design as well as possible improvements is included in the paper.

Table of Contents

1 Executive Summary

The architecture submitted by Alfredo Lopez to GIAC Fortune Cookies Inc. (GFCI) was technically sound and functional. It demonstrates a security strategy of defense in depth. However, the writer advises rejecting the design in its' current form. My recommendation is to use the Lopez design as a foundation for a Request for Proposal (RFP) to be submitted to multiple vendors. The RFP will incorporate additional documentation, design and business process requirements.

This paper will detail the following:

1. Overall design summary – business operations and physical architecture
2. Design strengths
3. Areas of contention
4. Thoughts on specific improvements necessary to develop a secure and robust GFCI information technology (IT) infrastructure.

The improvements that will be presented are based on the understanding that GFCI senior management supports the development of a network that strives for carrier class reliability, availability and serviceability (RAS). RAS is critical to the compressed time frames that the cookie fortune business commands.

Consideration will be given to:

1. Refinements to the business operations and access requirements. The Lopez design, while adequate, requires a level of administration that is onerous and will not meet the needs of the dynamic GFCI operational environment. It also lacks sufficient financial data to develop a ROI model.
2. An ability to manage the network. The industry model of FCAPS (fault management, configuration management, accounting, performance and security) must be incorporated in the final design.
3. Use of third party resources for current and future guidance on network auditing as well as policy development.

It is clear that these improvements will take time to develop and capture. This delay in implementation will create a risk for the company. However, considering the operational expense (OPEX) reflected in the implementation of a new design, as well as the capital expense (CAPEX) of building the architecture, a setback is justified. GFCI can not absorb the cost of retrofitting additional security or operational considerations once a design is implemented.

The success of GFCI is directly tied to its' ability to create, protect and sell fortunes through international e-commerce. Using the Lopez design as a foundation, GFCI must move forward with an RFP to develop a scalable infrastructure that will be the core to our success.

2 Design Analysis

The Lopez design is the source for all information in Section 2 and can be found at the following location:
http://www.giac.org/practical/GCFW/Alfredo_Lopez_GCFW.pdf

The intent of this section is a high level review that provides a clear picture of the operational and technical flow of the Lopez submission. This is a summary only, and specific engineering details will be addressed later in the paper.

2.1 Objectives for the infrastructure

2.1.1 Build a network in Miami, FL

2.1.2 Support the sale of fortune cookies via the internet.

2.1.3 Ensure access to the Latin America Market (LAM), where the GFCI primary revenue stream is located.

2.1.4 Ensure access to the United States for future expansion

2.1.5 Scalable distribution of cookie fortunes.

2.1.6 Uninterrupted access to the fortunes by Partners for cookie production

2.1.7 Access by internal employees to allow upload of fortunes to the public server from the private server after review.

2.1.8 Traveling sales team must be able to check email from remote locations

- No requirement to submit fortunes
- No requirement to retrieve fortunes

2.1.9 Security is paramount, as the fortune cookie business is characterized by ruthless competition, infrastructure attacks and efforts to obtain intellectual property by every means.

2.1.10 Provide the following functional groups access to network resources:

- Partners
- Customers
- Internal Employees
- Suppliers
- Mobile force and teleworkers

2.1.11 Restrict unauthorized access

2.2 Access Review

2.2.1 Partners

- Currently there are four (4) Partners
- Symantec VPN tunnel access to the Partners who are identified by their source IP.

2.2.2 Customers

- The international customer base will be served through www.cookiegiac.com using Hypertext Transfer Protocol (HTTP) through port 80
- Secure Socket Layer (SSL) via Transmission Control Protocol (TCP) port 443 will allow customers to purchase various quantities of fortunes safely using credit cards.

2.2.3 Internal Employees

- Access to the internal database server via Secure Shell (SSH) v2 and Secure Copy (SCP).
  - SSH allowing command line interface (CLI) access to the servers
  - SCP allows files to be copied to/from the server
- Traveling sales team will have a laptop with:
  - Windows 2000 Service Pack 2
  - Symantec Client Security
- IT staff will access equipment:
  - through SSHv2 (TCP port 22)
  - Access to any protocol to the GFCI private network or demilitarized zone (DMZ).
- All non-IT employees:
  - have access to the Internet and the external web server via TCP port 80 and 443 (SSL)
  - Do not have any access to any other port in the services network or DMZ

2.2.4 Suppliers

- Real Academy of the Languages (RAL) is the single contract supplier
  - Partner in writing the fortunes
  - Exist in several international locations and represents various subcontractors
  - Not all RAL employees write fortunes
- Upload fortunes via SSHv2 TCP port 22 and the secure copy (SCP) command.
  - This requires each and every user to have their own directory on the fortunes server

- A tracking and updating process is needed to keep the names and specific information of each user current.

2.2.5 Mobile Force and teleworkers

- Use laptops loaded with:
  - Windows 2000 Service Pack 2
  - Symantec Client Security to limit virus infection
- Connect to GFCI private network using Symantec Enterprise VPN Client 7.0.1 (3DES) via a client to site VPN that will set up to communicate with the Velociraptor cluster.

2.3 Architecture review: [see Figure 1]

1. Access – connectivity to the Network Access Point (NAP) of the Americas via a T-3 circuit.
2. A border router and stateful connection-oriented firewall that use specific rules to protect both public and private GFCI networks.
3. An Intrusion Detection System (IDS) that uses packet level analysis that acts as a second layer of defense to the firewall in protecting both public and private GFCI networks.
4. Demilitarized Zone (DMZ) – a separate GFCI network that allows anyone on the internet to connect with the following services:
   a. Domain Name Service (DNS)
   b. Email
   c. GFCI web page
   d. GFCI Fortune Cookie application server
   e. Second Intrusion Detection System (IDS) to identify and respond to attack on the GFCI public network
5. A private GFCI network protected by :
   a. Content Server Switch (CSS) providing load balancing
   b. Dual proxy firewalls that shield internal GFCI IP addresses from the external world.

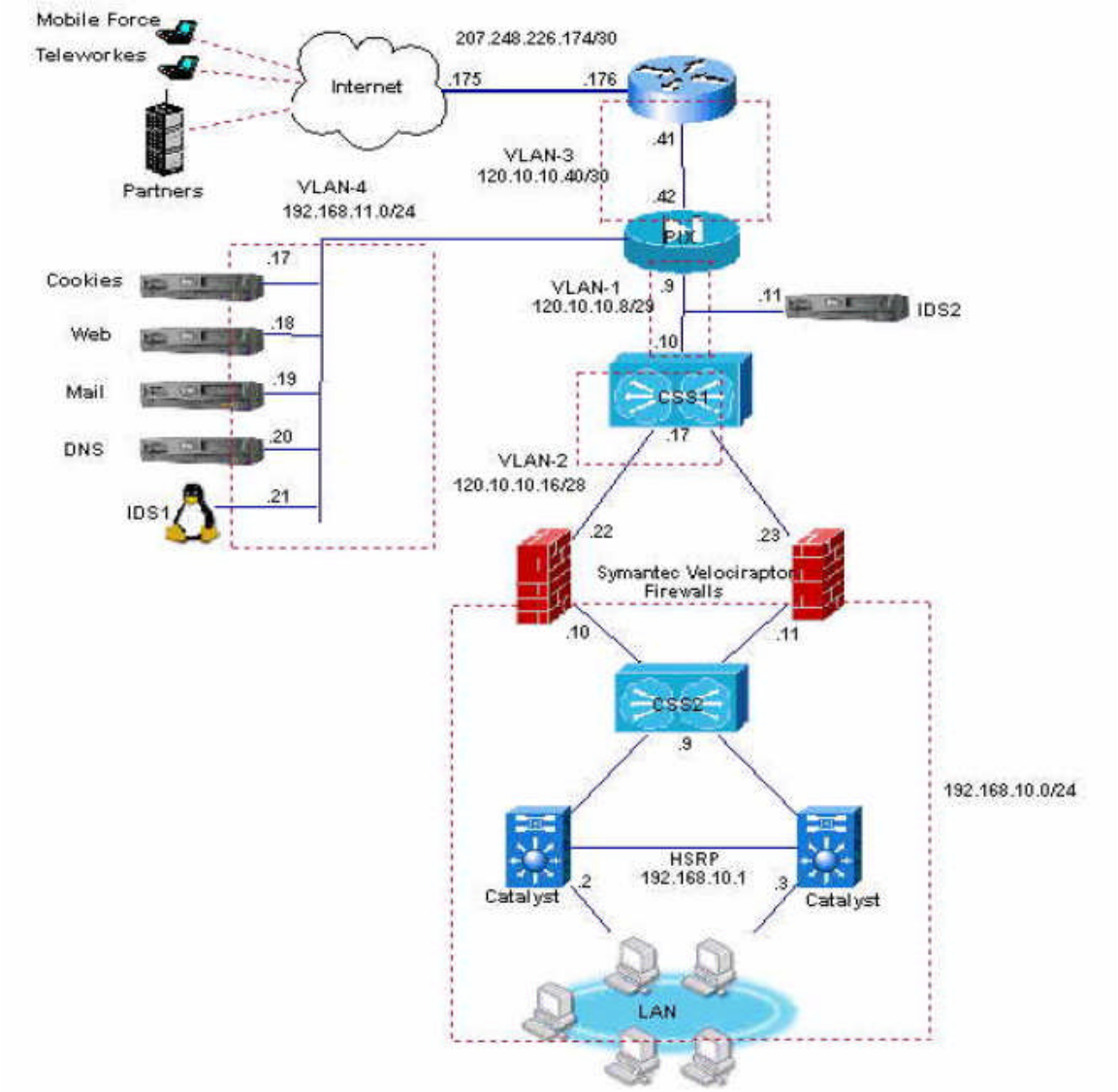

Figure 1 – Lopez Network Design [page 9 Lopez design]

Note: The low level configuration strengths and weaknesses mentioned in Section 3 and Section 4 were discovered using the National Security Agency "Router Security Configuration Guide" Version 1.1 as well as internet searches on specific topics. The lists are not intended to be all inclusive, but only to demonstrate the need and value of having an RFP that would allow GFCI to compare multiple designs and device configuration strategies. While there is a science to device configuration, there is also an art to the selection of a security strategy as well as actual implementation of that strategy. Final architecture and configuration selection will require the highest level of scrutiny and objectivity using defined industry standards and peer review by the entire IT staff at GFCI.

3 Design Strengths

3.1 Primary Firewall Selection

Cisco Private Internet Exchange (PIX) 535 UR running 6.2
Connection oriented firewall (Lopez, Page 10, Section 1.2.2)

Lopez provides two primary reasons for selecting the Cisco PIX firewall:

1. Purpose-built firewall appliance running proprietary firmware
2. Stateful connection-oriented firewall

These statements by Lopez will be developed in greater detail to provide supporting facts for the writers' endorsement of the selection.

1. Purpose-built firewall appliance running proprietary firmware
    a. As a purpose-built firewall, the PIX runs on flash memory, which means there is not a hard drive in the device. This increases the Mean Time Between Failure (MTBF), boosting reliability and availability and decreasing the need for a second appliance for redundancy.[1] These features support the availability element GFCI RAS strategy.
    b. Alternative firewalls are often based on the UNIX or Windows NT platforms. Both platforms require a greater level of administration through configuration and patch management.[2] This ability to "set and forget" with a periodic configuration review is attractive, and supports the serviceability element of the GFCI RAS strategy.
2. Stateful connection-oriented firewall
    a. When a host inside the GFCI network makes a TCP connection to the internet, the PIX logs a variety of information (source/destination IP, port, TCP sequencing, etc.) to create a connection object. Inbound packets hitting the firewall are compared to this connection table. The session flow is maintained only while the appropriate connection exits. Symantec has developed what it believes to be an equivalent called "stateful application inspection", demonstrating industry support of the technique.[3] The rigor surrounding this method network protection supports the reliability element of the GFCI RAS strategy.

In addition to the points made by Lopez, the following demonstrate the ability of the PIX to scale[4]:

1. 500,000 concurrent connections
2. 2,000 simultaneous VPN tunnels
3. Dual hot swap power supplies

3.2 Defense in depth with network segmentation

The concept of defense in depth and network segmentation has a developed history.[5] The writer strongly endorses this concept as the foundation for the proposed RFP. The architecture supports modular growth allowing scale, and the proven resiliency to attack meets our RAS requirements. The design layers are broken out below to highlight their function and strength.

Two important points to make clear about the specific components in the design:

1. The writer did not find any literature that would cast doubt or indicate risk in the selection of any of the applications or supporting equipment outlined in Section 3. The Lopez design has strength in the multiple security layers. It does not rely on a single application or device vendor. (Note that the writer did feel the need to research and support the device selection for the first security specific device in the network, the PIX firewall, Section 3.1)

2. There is considerable room for improved documentation surrounding the analysis that supports vendor selection. There are a large number of equipment and application vendors in network and security areas, creating a challenge for accurate comparison. It will become clear when developed in detail Section 4 and Section 5 that this level of scrutiny is required, but is more appropriate in an RFP matrix. Through the RFP process alternate vendors or equipment may be selected, but the design layers must remain intact.

3.3 Intrusion Detection System (IDS)

While the firewall is the first line of defense with defined rules performing basic blocking and tackling, the IDS will perform more complex analysis. This includes traffic rate monitoring to detect denial of service (DoS) attacks, and sophisticated protocol anomaly detection that performs pattern matching by taking advantage of the fact that protocols by themselves are very restrictive. An advantage of protocol anomaly detection over basic signature matching, is that on “zero day” or the first day a new attacked appears on the internet a signature on file is not required in the rule set to block or prevent the attack. This eliminates a window of vulnerability during the time the signature based IDS has not received an update for this new attack.

It is important to note that there are attacks designed without anomalies, and they look 'normal' at the protocol level.[6] Understanding this, Lopez has another IDS in the public network as well as proxy firewalls protecting the private network.

Symantec-ManHunt 2.2 Intrusion Detection System (Lopez, page 10, Section 1.2.3)

- Protocol Anomaly Detection System
- SunBlade 150 (bastion host)
- Solaris 8
- Configured with Smart Agent Event Coordinator that enables accepts of real time data from SNORT (the IDS on the public network)
- Second layer of defense behind the Border Router

3.4 DMZ

The Demilitarized Zone (DMZ) is a network that provides public access to select applications critical to e-commerce. The selections are outlined below to demonstrate that Lopez has engineered each so that it can scale. Solaris and Linux are common in the industry, preventing a complex training and support matrix.

Apache web server 2.0 (bastion host) (Lopez, page 11, Section 1.2.4)

- SunBlade 150
- Solaris 8

Mail Server (sendmail 8.9) (Lopez, page 11, Section 1.2.5)

- SunBlade 150
- Solaris 8

DNS Server (Lopez, page 23, Section 1.2.6)

- Berkeley Internet Name Domain (BIND 8.2.2)

IDS-1 (SNORT 2.0) (Lopez, page 12, Section 1.2.7)

- Linux Red Hat 7.3
- Two 10/100 Ethernet NIC
- One without IP address connected to the SPAN ort of the catalyst were the VLAN to SPAN (DMZ's VLAN)
- Second assigned an IP and connected on any active port in the VLAN 2 to have IP communication with ManHunt IDS 2

Cookie Servers (Lopez, page 13, Section 1.2.9)

- SunBlade 150 with
- Solaris 8
- One public, one private

3.5 Private Network

Isolating the private network behind the Content Services Switch (CSS) and the Velociraptor firewall pair is industry best practice. Load balancing is performed by the CSS, and the firewalls prevent direct connections between clients and servers, and masks the inter IP address scheme from the internet. The RAS components attractive to GFCI are modeled in the application of type CSS architecture in Siemens Medical Solutions. This demonstrates that this application of the CSS in the Lopez design has been field tested. While the implementation is not exactly the same, the functionality/stress applies for comparison.

Content Services Switch (CSS) Cisco CSS 11501 (Lopez, page 13, Section 1.2.8)

- Eight 10/100
- One GigE
- Loadbalancing

Two (2) Symantec Velociraptor 1300 firewalls v 1.5 (Lopez, page 13, Section 1.2.10)

- Proxy firewalls
- Do not allow direct communication between clients and servers
- Provides shielding of the internal IP address from the external world
- Allows VPN tunnels client-to-site and site-to-site

Cookie Servers (Lopez, page 13, Section 1.2.9)

- SunBlade 150
- Solaris 8
- One public, one private

3.6 Configuration

The following samples demonstrate that Lopez followed industry best practice during the configuration of sampled network devices. Each implementation of a security practice supports all three elements of the reliability, availability and serviceability of the GFCI (RAS) strategy.

3.6.1 Example 1

Passwords and authentication management

> "To encrypt passwords, use the **service password-encryption** global configuration command." (Lopez, page 17, Section 2.2.2)

Compliant with Router Security Configuration Guide, page 62, Section 4.1.5 Logins, Privileges, Passwords, and Accounts,

> "Enable **service password-encryption**; this will keep passersby from reading your passwords when they are displayed on your screen."

3.6.2 Example 2

Selecting SSH as the preferred method of remote access that provides encryption of the traffic and authentication. (Lopez, page 17, Section 2.2.2)

Compliant with the spirit of Router Security Configuration Guide Section 5.3.1 Configuring a Router for Secure Remote Administration with SSH page 214-215. Note: there are minor deviations, such as ssh time out (60 vs. recommended 120) as well as access list technique.

3.6.3 Example 3

Unnecessary Services. Lopez is to be commended for including this in the design (Lopez, page 18, Section 2.2.3). However, lacking an outside reference, the execution and implementation appears to be lacking. Please see Section 5.3.2 for the specific concerns. This demonstrates that there is an 'art' when implementing a strategy. The strength is that Lopez made the effort to include the exclusion of unnecessary services in his design.

3.6.4 Example 4

Denial of Service (DoS) against the router. Defense in depth is demonstrated by inclusion of this in the design (Lopez, page 19, Section 2.2.4). There is concern when researching the 'art' of implementation. A search of the www.sans.org site for the guide "Securing Cisco routers Step-by-step" was not successful, highlighting the need for GFCI to use external checklists that will updated in a timely manner from their author (like the National Security Agency or Microsoft), and remain accessible for the life of the network.

3.6.5 Example 5

Planning the implementation (Lopez, page 22, Section 2.3.2)
The forms recommended by Lopez are excellent. Please note that to access http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0c6.html
the user needs a current Cisco Support agreement.

3.6.6 Example 6

Verify the Firewall Policy (Lopez, pages 36-74, Section 3). The rigor and attention to detail should be noted and incorporated in the RFP. Especially 3.1.4 Tools to conduct the audit. The presentation of various tool options on two platforms meets the spirit as well as the intent of a robust test environment.

4 Areas of Contention

4.1 Border Router

Border Router (Lopez, page 9, Section 1.2.1)

- Cisco 7206 VXR 12.2.(13)T
- Six high speed port adaptors
- QoS such as committed access rate (CAR)

The author believes that there must be documentation to support the due diligence surrounding the design of the network access point and selection of a border router. This threshold was not met in the Lopez recommendation. To be clear, this contention is not a technical one, but a management requirement that may not have been known to Lopez. The absolute need is to have data available that allows creation of a Return on Investment (ROI) model. Facts are also necessary to demonstrate support of the RAS model.

The author will require a table similar to the one created on the next page from www.telezoo.com . This will allow a quantitative review of equipment during design review.

Table 1

	Cisco 3745 Application Service Router by *CISCO Systems* Description Add to my!Favorites	**NetIron 400 Internet Core Router** by *Foundry Networks* Description Add to my!Favorites	**M10 Internet Backbone Router** by *Juniper Networks* Description Add to my!Favorites	**M20 Internet Backbone Router** by *Juniper Networks* Description Add to my!Favorites
Features				
Image	 View Picture	 View Picture	 View Picture	 View Picture
Type	Rack Mounted, Stackable, Standalone Desktop	Rack Mounted, Stackable	Rack Mounted	Rack Mounted
Supporting Interfaces	10/100BASE-TX, 1000BASE-T, ADSL - CAP, ADSL - DMT, E1 - ATM, E1 - Fractional, E1 - Full, E3 - ATM, HSSI, ISDN BRI - S/T port, RS-232, T1 - ATM, T1 - Fractional, T1 - Full, T3 - ATM, T3 - Full, X.25	10/100BASE-TX, 1000BASE-LX, 1000BASE-SX, 1000BASE-T, 100BASE-FX, 100BASE-TX, OC-12 SM, OC-3 SM, OC-48 SM, STM-16, STM-64, T3 - ATM, T3 - Full	1000BASE-SX, 100BASE-TX, E1- Clear Channel (Unstructured), E3 - Clear Channel (Unstructured), OC-12 MM, OC-12 SM, OC-3 MM, OC-3 SM, STM-1, STM-16, STM-4, T1 - Full, T3 - Channelized, T3 – Full	1000BASE-SX, 100BASE-TX, E1- Clear Channel (Unstructured), E3 - Clear Channel (Unstructured), OC-12 MM, OC-12 SM, OC-3 MM, OC-3 SM, OC-48 SM, STM-1, STM-16, STM-4, T1 - Full, T3 - Channelized, T3 - Full
Networking Features	ATM (UNI), Built-in-CSU, Ethernet Switching, Gigabit Ethernet Switching, IP Forwarding, IP over ATM, PPP over ATM, PPP over Frame Relay, PPP over ISDN, X.25 over TCP	Ethernet Switching, Gigabit Ethernet Switching, IP Accounting, IP Forwarding, Layer 3 Switching, Layer 4 Switching, Packet Over SONET	ATM (AAL5), ATM (UNI), IP Forwarding, IP over ATM, Packet Over SONET, Token Ring LANE, Vitrual Router Redundancy Protocol (VRRP)	ATM (AAL5), ATM (UNI), IP Forwarding, IP over ATM, Packet Over SONET, Token Ring LANE
Supporting LAN Protocols	IP	IP, IP V6	IP	IP
Routing (Features & Protocols)	Dynamic Routing, IP Routing, Static Routing	BGP-4, Dynamic Routing, IP Routing, OSPF, OSPF V.2, PIM, RIP, RIP, RIP II	BGP-4, IS-IS, OSPF	BGP-4, IS-IS, OSPF
Supporting WAN Protocols	ADSL, ATM, Frame Relay, ISDN, PPP, X.25		ATM, Frame Relay, HDLC, PPP	ATM, Frame Relay, HDLC, PPP
Bridging Compliance	802.1p QoS		802.1q VLAN	
Redundancy	Power Supply	1:1, Flash Memory, Hot swappable, Power Supply, Processor	1:1	1:1

4.2 Access

Border Router and T-3 access (Lopez, page 10, Section 1.2.1)

Without supporting documentation, the author finds it difficult to believe the current volume of cookie fortunes produced by GFCI requires a dedicated T-3 with 44.7 Mbps. Depending on local loop charges, this expense could easily exceed $4,000 a month vs. $500 for a dedicated T-1 and less than $400 for a cable modem with a downstream speed of about 3 T-1's . Please see Section 5.1 on for details.

4.3 Configuration

4.3.1 Example 1

Password and authentication management (Lopez, page 17, Section 2.2.2)

> Passwords "2Vmkbrone$" and "very2Vmkbrone$"

Violation of Router Security Configuration Guide Section 4.1.5 Logins, Privileges, Passwords, and Accounts, page 63

> "Avoid more than 4 digits or same-case letters in a row."

4.3.2 Example 2

Services to Block Completely at the Router

Lopez failed to include a comprehensive table similar to Table 3-2, page 38 of the Router Security Configuration Guide.

4.4 Network Event Management

Lopez made it very clear that authentication, authorization and accounting (AAA) and Network Event Management (NEM) are outside the scope of his design.

> Password and Authentication management
> "Authentication via RADIUS is considered in the security roadmap of the network perimeter in the future." (Lopez, page 16, Section 2.2.2)
>
> Unnecessary Services
> "At this time GIAC corporate hasn't installed a monitoring platform that uses SNMP protocol, but it will be deployed in the future, that is why SNMP is disabled in the router." (Lopez, page 18, Section 2.2.3)

The omission of either AAA or NEM would disqualify any design from GFCI consideration in an "all or nothing" RFP.

From a technical perspective, the author believes that a network can not be secure without understanding who, what, where, when, why and how much ***for each and every device and interface***. Those are the elements AAA and NEM provide network engineers and administrators.

From a management perspective, based on a quick CAPEX analysis done by the author (Lopez did not include this data in his design); there is a projected investment of capital in excess of $340,000 to build the network. (See Table 2)

A quick search on www.nextag.com provided 7,400+ matches for network management software priced between $0-$3,500. This equals an investment of approximately 1% of the embedded capital base and does not take into account intellectual property at risk and impact to cash flow that occurs during an outage or compromise. Without question this level of investment, or greater if needed, is necessary to support all RAS elements GFCI finds critical to success.

Note: Lopez failed to provide low level details for a number of elements in the network. Device configuration/build can significantly impact price. Using www.nextag.com , the author developed Table 2 for reference, with the understanding that the RFP will provide significantly more detail to ensure accurate price and ordering. It may be possible to obtain volume discounts if equipment purchases are made through a single vendor/equipment broker.

Table 2

Item	Unit Price	In Network	Total
Cisco 7206	$ 13,000	1	$ 13,000
SunBlade 150	$ 2,000	8	$ 16,000
Pix 535	$ 16,000	1	$ 16,000
Symantec Velociraptor 1300	$ 7,000	2	$ 14,000
Cisco 11501	$ 14,000	2	$ 28,000
Cisco Cat 4506	$ 3,500	2	$ 7,000
Laptop	$ 2,500	100	$ 250,000
		Total	$ 344,000

5 Improvements

5.1 Access Pricing

Page 9 Section 1.2.1 The Border Router, Lopez recommends a dedicated T-3. It was also stated on page 4 that connectivity to the NAP of the Americas is required.

The network access model needs to take into consideration a complex matrix of elements and ideas to include the following:

1. Local Loop pricing
2. physical diversity
    a. building access
    b. router and/or card
3. circuit diversity
4. circuit type (protected/unprotected)
5. bundled services contract to include telephony
6. Accurate utilization history and growth projections
7. contract term
8. waiver of installation fees for an increase in term
9. waiver of upgrade charges
10. expected lead time to upgrade the circuit (vendor capacity models)

A quick search on www.telezoo.com provided seven providers offering dedicated T-1 speeds and higher in the Miami area. After developing and refining the suggested matrix, the 'provider shopping' is best completed by the vendors responding to the RFP.

5.2 Network Event Management

A method of alerting, alarming and escalation of service impacting events is required to prevent the loss of GFCI revenue and market share during a service impacting network event. An overview of the FCAPS model will highlight key areas to include in the RFP:

This table on the next page from Cisco's "Network Availability" white paper http://www.cisco.com/en/US/netsol/ns206/networking_solutions_white_paper09186a008015829c.shtml will provide a reference as an explanation of how a Telecommunications Management Network (TMN) could be apply to the GFCI network.

A Functional View of TMN Applications and FCAPS

	Fault Management	Configuration Management	Accounting	Performance Management	Security Management
Service Management	Testing, reporting, and notification	Installation and deployment	Pricing	Reporting	Profiling and fraud management
Network Management	Event correlation and filtering; fault testing and isolation; trouble tickets	Connection and installation management	Correlation and storage	Aggregation, trending and characterization; capacity plng	Pattern analysis; breach response and recovery
Element Management	Alarm localization, logging, and correction	Loading, administration, and status	Collection and validation	Collection and analysis; capacity plng.	Alarm and audit trail management
Network Elements	Failure detection, reporting	Configuration validation and enforcement	Usage data generation and storage	State change detection and reporting	Access control; intrusion detection, reporting

Looking at each of the five functional areas in the FCAPS model and how they could fit into a GFCI network[7]:

1. Fault Management – The goal is to detect, isolate and notify the IT staff of faults encountered in the network. A wide range of application software is available to consolidate network events, as well as service failures and security events from the IDS boxes, into a single view. Thresholds can be set that trigger email notification and text messages to a duty pager. The configuration of these traps sent by network devices using Simple Network Management Protocol (SNMP) will be defined by the subject matter experts (SME's) selected during the RFP response. Selection of the device specific Management Information Base (MIB) is a configuration art, much like the security configurations we have discussed in detail. GFCI would expect the vendor selected in the RFP to reference industry standard documents when explaining their configuration plan. The GFCI network does not warrant a fully staffed Network Operations Center (NOC), however a graphical interface for the on call technician to reference will be invaluable to quickly correlate network events and define the scope event impact.

Features that would be desirable in the product would be actual application validation, meaning the software performs DNS, HTTP, POP3, and SMTP, and does not just ping the interface of the device. ICMP would used as well to ensure connectivity is available for the application itself.
A system log (Syslog) server is also required to capture event information from all network devices.

2. Configuration/Change Management – The focus in this area would be a dedicated Trivial File Transfer Protocol (TFTP) server that would contain the standard device configurations, and an automated backup of each device configuration. These are necessary for device recovery in the event of a catastrophic incident.
Other features often available that would be of benefit if included in the software selected are inventory management features, software management summaries as well as the ability to 'diff' configurations, meaning to compare or contrast a configuration in use against a standard in order to identify what changes have been made.

3. Accounting Management – Similar to Performance Management that will be explained in a moment, Accounting Management uses some of the performance metrics to possibly charge back or monitor usage information of network resources. While it is not evident at this time, excessive Partner utilization of server resources could be tracked to monitor for an indication of inappropriate use of GFCI resources.

4. Performance Management- Each interface and each circuit needs a history captured of their utilization. This is necessary for capacity planning as well as supporting data in the event of a DoS attack. A range of other health check from each element are necessary, to include Central Processing Unit (CPU) utilization and packet loss. Specific configuration detail will be listed in the RFP. Internal Service Level Agreements can be created and tracked to ensure server response times, application availability and overall network status.

5. Security Management - Without question, each of these "triple A" sections must be present in the GFCI network. This will provide various levels of access to network devices to authorized users, and track actions taken on the equipment. The goal of GFCI would be development of a 'single sign on' process. To outline the embedded requirements of the process:

- Authentication - the process of identifying users, including login and password dialog, challenge and response, and messaging support. Authentication is the way a user is identified prior to being allowed access to the device. There is a fundamental relationship between authentication and authorization. The more authorization privileges a user receives, the stronger the authentication should be. The RFP should stress this point and possibly expand the scope to all

users of the network. Consideration should be given to two factor authentication of some type. The wide range of products in this space requires analysis of the RFP response matrix to effectively select a solution that fits the unique circumstances of GFCI.

- Authorization - provides remote access control, including one-time authorization as well as authorization for each command that is requested by the user. On a Cisco router, the authorization level range for users is 0 to 15 with 0 being the lowest level and 15 the highest. With the small IT staff at GFCI, this is not expected to be a complex task.
- Accounting - allows for the collecting and sending of security information used for billing, auditing, and reporting, such as user identities, start and stop times, and executed commands. Accounting enables network managers to track the services that users are accessing as well as the amount of network resources they are consuming. Tracking each keystroke made on all network devices is an invaluable audit tool when reconstructing a network event. Network change is the root cause of more outages than hardware and software problems combined.

5.3 Configuration

The following two improvement opportunities are presented to demonstrate the need for a more thorough scrub on the configurations presented by Lopez. It is not intended to be an all inclusive review, and is not meant to question the designers' ability to set up a network. The intended spirit is that no one of us is smarter than all of us, and peer review and following checklists developed by recognized technology experts are the best method to avoid omission of simple steps that increase the security of the network.

5.3.1 Example 1

Page 17 Section 2.2.2 Password and authentication management

SSH set up. There was no steps provided to verify SSH is operational.

Recommendation: follow the steps provided in Router Security Configuration Guide Section 5.3.2 Advanced SSH Commands, page 216, when using Cisco IOS 12.2:

To verify SSH has successfully been enabled, execute the command, **show ip ssh**

To verify SSH has been successfully enabled and that your session is actually using SSH, execute the command **show ssh**

5.3.2 Example 2

Page 18 Section 2.2.3 Unnecessary Service
Recommendation: Referencing the NSA Router Security Configuration Guide Executive Summary Card, follow the *Specific Recommendations: Router Access*, section 1-3 in their entirety. Lopez as omitted safeguards (**no ip bootp server**) as well as presented typographical errors that can not be implemented by the router (**no service udp-small services** vs. the correct **no service udp-small servers**). This **services** vs. **servers** is present in the tcp-small command as well.

5.3.3 Example 3

During the RFP, there should be detailed review of Table 3-1, page 38 and Table 3-2, page 39, Router Security Configuration Guide to gain a deeper understanding of the services allowed to traverse the border router.

The lesson is that GFCI wishes to use reputable external sources as checklists for auditing our network. Review of the version of these sources on a periodic cycle allows GFCI administrators to focus on providing service to our customers vs. maintaining currency in all facets of security and technology.

5.3.4 Example 4

Sections 2.2.5 through 2.2.7, recommend the RFP reference Cisco IOS Firewall to review the possibility of using Context Based Access Control (CBAC)

5.4 Miscellaneous additional items

5.4.1 Five Step Risk Assessment Model

While it is clear that Lopez does have some understanding of GFCI, restructuring the information into a Risk Management model allows an objective analysis of the business and the supporting network to ensure all security needs are being met.

The National Infrastructure Protection Center provides the following five steps to develop a comprehensive assessment[8]:

1. Asset Assessment – the most important of the five steps, all assets, tangible (equipment, facilities, etc.) as well as all others (intellectual property contained in the fortunes, the process surrounding their development and deployment, etc.) are identified. Identify possible events that would damage or destroy each asset and then define the impact that would have on GFCI.

2. Threat Assessment – Develop a matrix of adversaries using the events identified in the Asset Assessment. Based in Miami, the threat of a hurricane is and obvious event that would impact GFCI. To determine if our competitors are adversaries, each must be measured to determine if they have the intent as well as the capability to cause an unwanted event, as well as a history of successful attacks.
3. Vulnerability Assessment – This will characterize the vulnerabilities related to specific equipment, as well as exploitable situations created by poor process or inadequate policy enforcement. The Threat Matrix will also identify the relevant vulnerabilities most likely to be exploited by specific adversaries, and allow a priority in testing and threat protection development. This was partially addressed by Section 3 of the Lopez design.
4. Risk Assessment – This step combines all the information from the prior three steps. Simply put, Risk = Consequence x (Threat x Vulnerability). This can provide the basis for a numerical ranking for rating the risks. "Threat x Vulnerability" represent the probability of the event, and the "loss effect" represents the impact to the organization.
5. Identification of Countermeasure Options – This step is the purpose of the RFP, which is to develop the secure infrastructure to meet the business needs of GFCI. The value in developing the risk analysis is it will allow management to conduct consequence assessment. Simply put, this is a Return on Investment model with a security spin defining the impact of a loss.

5.4.2 Login Banners

Lopez fails to address the creation of the login banner for any of the devices in the network. While this may appear simplistic, a simple banner with strong legal language is vital for prosecution if an attacker is identified. This is especially useful for unauthorized access or use by a disgruntled GFCI employee.

5.4.3 Backups

While this is related more to process than physical network design or equipment configuration, mention of backing up data is vital to securing the integrity of the intellectual property of our fortunes. The Risk Assessment will assist in determining the periodicity of the data capture, but off site storage will be a requirement.

5.4.4 Physical Security

Building access and equipment room access are outside the design scope. However, to meet the spirit of developing a totally secure network, mention of something as elementary as a locking equipment rack http://www.racksunlimited.com/louver_door.html would enhance the design. Console port access is hands down the best way for a malicious individual to gain access to a piece of equipment.

5.4.5 Creativity

The writer would like to see forward thinking solutions that strive to keep GFCI one step ahead of our competition. An example would be the limited deployment of steganography software such as Crytobola, where a single copy is only $29.00 http://www.cryptobola.com/index.htm . Clearly the intent would not be to replace sound security practices displayed in the Lopez design, but it could be the edge needed to prevent 'prying eyes' from reading a clear text message in an email. This product could be installed for senior executives and key fortune developers.

6 Conclusion

The Lopez design is not a viable solution for GFCI. The writer believes that if GFCI had provided a Risk Management Model and defined key network requirements for our reliability, availability and serviceability strategy, Mr. Lopez would have presented an acceptable solution that would include the data necessary to develop financial justification for the investment.

The fundamental design elements that are missing and make the architecture unacceptable is the lack of basic network event management, and the absence of the "AAA" critical security features of authentication, authorization and accounting. These elements were consciously excluded by Lopez and mentioned as being on the roadmap for development. The writer is of the opinion that these elements are a requirement for creating a network. They are the essence of core security process.

The other concerns with the design could be easily addressed. They can be can be grouped into two main areas – failure to provide financial or engineering justification, and configuration flaws discovered during the design review that demonstrate the need to reference best practice guidelines that are kept current by reputable external resource. Basically this means facts for justification and references for validation of best practice when implementing the configurations.

The next step for GFCI is to retain an expert to create a Risk Management Model. This would be the key to establishing design and process priorities and requirements. It would also provide data to complete the ROI for the various elements that support and protect each business process.

The RFP that follows development of the model needs to be managed by GFCI. An external resource may be necessary to expedite the development, distribution and analysis, but the accountability must rest squarely on the shoulders of the IT Management team. The work to compare and contrast solutions, pricing and implementation strategies of the various vendors submitting bids is more than just and exercise. It will expand the knowledge base of our staff, justify the OPEX and CAPEX expenditures, and identify areas of improvement that do need to be on our roadmap.

For our business to remain stable in our current Latin America Market, and to expand into North America, our network must emerge from this redesign as close to carrier class as possible. It must be resilient to infrastructure attacks and protect the intellectual property that is the life blood of our business.

List of References

Broderick, Stuart. "Implementing and Managing a VPN Security Policy." Information Security Technical Report. Article ID: 1298. 23 April 2002. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=1298&EID=0 (June 2004)

Cisco. "Cisco CSS 11500 Series Content Services Switches Case Study." Siemens Medical Solutions Deploys Content Networking Solutions. URL: http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_case_study09186a00800a3bc4.shtml (June 2004)

Cisco. "Cisco Internet OSS Overview White Paper." An overview of the approach, strategy, and products needed to build a packet-based OSS infrastructure. URL: http://www.cisco.com/en/US/netsol/ns341/ns396/ns108/ns30/networking_solutions_white_paper09186a00800e0266.shtml (May 2004)

Cisco. "Cisco IOS Firewall." Technical Support Cisco IOS Firewall. URL: http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Software:Cisco_IOS_Firewall&s=Implementation_and_Configuration#Software_Requirements (June 2004) Note: Reader needs CCO username/password to view.

Cisco. "Cisco PIX 535." URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2119/index.html (May 2003)

Cisco. "Cisco's PIX Firewall and Stateful Firewall Security White Paper." 30 June 2000. URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm (May 2003)

Cisco. "Network Availability White Paper." Network Availability: How much do you need, now much do you get? URL: http://www.cisco.com/en/US/netsol/ns206/networking_solutions_white_paper09186a008015829c.shtml (May 2004)

Cisco. "Network Management System: Best Practices White Paper." Document ID: 15114. URL: http://www.cisco.com/warp/public/126/NMS_bestpractice.html (June 2004)

Conry-Murray, Andrew. "New Public Network: Network Security's Not-So-Secret Ingredients." 09 August 2001. URL: http://www.networkmagazine.com/showArticle.jhtml?articleID=8703199 (May 2003)

Conry-Murray, Andrew. "Special Report: Firewalls for All." 05 June 2001. URL: http://www.networkmagazine.com/showArticle.jhtml?articleID=8703117 (May 2003)

Della Maggiora, Paul L. Performance and Fault Management. Indianapolis: Cisco Press, June 2000.

Dornan, Andy. "Networking for Managers." 01 January 2000. URL: http://www.networkmagazine.com/article/NMG20000426S0021 (June 2004)

Dubie, Denise. "FCAPS for real?" 19 May 2003. URL: http://www.nwfusion.com/weblogs/management/002787.html (June 2003)

Fraser, B. "Network Working Group Request for Comments: 2196." September 1997 URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (June 2004)

Future Software Limited, India. "FCAPS White Paper." 2003. URL: http://www.futsoft.com/pdf/fcapswp.pdf (May 2004)

Hernacki, Brian. "Intrusion Detection Systems: Defining Protocol Anomaly Detection." Symantec Enterprise Security White Paper. 2003

Lopez, Alfredo. "GIAC Certified Firewall Analyst (FCFW) Practical Assignment Version 1.9 (revised January 20, 2003)." 02 April 2003. URL: http://www.giac.org/practical/GCFW/Alfredo_Lopez_GCFW.pdf (May 2004)

National Infrastructure Protection Center. "Risk Management: An Essential Guide to Protecting Critical Assets." November 2002. URL: http://www.nipc.gov/publications/nipcpub/P-Risk%20Management.pdf (May 2004)

National Security Agency. "Router Security Configuration Guide." Router Security Guidance Activity of the System and Network Attack Center (SNAC). Version 1.1 Report Number: C4-040R-02, 27 September 2002. URL: http://www.nsa.gov/snac/routers/cisco_scg.pdf (May 2004)
National Security Agency. "Router Security Configuration Guide Executive Summary Card." NSA/SNAC Router Security Configuration Guide. Version 1.1. 10 February 2003. URL: http://www.nsa.gov/snac/routers/cisco_exec_sum.pdf (May 2004)

The Network Reliability and Interoperability Council. "NRIC Best Practices Selector Tool." URL: http://www.bell-labs.com/cgi-user/krauscher/bestp.pl (June 2004)

Endnotes

[1] Cisco. "Cisco's PIX Firewall and Stateful Firewall Security White Paper." 30 June 2000. URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm (May 2003)

[2] Ibid

[3] Conry-Murray, Andrew. "Special Report: Firewalls for All." 05 June 2001. URL: http://www.networkmagazine.com/showArticle.jhtml?articleID=8703117 (May 2003)

[4] Cisco PIX 535 http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a008007d05d.html

[5] Section 3.2.3 Protecting the Network http://www.ietf.org/rfc/rfc2196.txt?number=2196

[6] Hernacki, Brian. "Intrusion Detection Systems: Defining Protocol Anomaly Detection." Symantec Enterprise Security White Paper. 2003, Page 5

[7] Cisco. "Network Management System: Best Practices White Paper." Document ID: 15114. URL: http://www.cisco.com/warp/public/126/NMS_bestpractice.html (June 2004)

[8] National Infrastructure Protection Center. "Risk Management: An Essential Guide to Protecting Critical Assets." November 2002. URL: http://www.nipc.gov/publications/nipcpub/P-Risk%20Management.pdf (May 2004)

Last Updated: July 25th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Banff MGT512	Banff, AB	Oct 23, 2017 - Oct 27, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced