Global Information Assurance Certification Paper

GIAC Security Leadership Certificate (GSLC)

Practical Assignment

Version 2.0

Evaluation of GCFW Practical Assignment V2.0
"Security Architecture for GIAC Enterprises"
Prepared by Jim Hietala (Submitted March 4, 2004)
http://www.giac.org/practical/GCFW/Jim_Hietala_GCFW.pdf

Connie J. Sadler
SANS 2004, Orlando, Fl
April 2-6, 2004

Submitted July 25, 2004

Connie J. Sadler
July 25, 2004

Table of Contents

Connie J. Sadler
July 25, 2004

List of Figures

Abstract/Summary

This paper's purpose is to evaluate a GIAC GCFW network security design (choosing from those numbered above 400) and to critique it. There are really two goals here. One is to evaluate the network security design on its own merit, calling out its strengths and weaknesses and how the design addresses the needs of the target business. The other goal here is to evaluate the design's merit in the context of the evaluator's needs. In this case, the author of this critique is assessing how the design and implementation of the GCFW proposal might fit the needs of a medium-sized higher educational institution. So it is possible that the design is perfect for the business for which it was conceived, but that it could be a poor solution for a medium sized university.

The network security design chosen to be evaluated was written by Jim Hietala and submitted to GIAC on March 4, 2004. A copy of Jim's paper (in Adobe Portable Document Format) can be found at the following URL: http://www.giac.org/practical/GCFW/Jim_Hietala_GCFW.pdf. Figure 1 below is a network diagram depicting the proposed network security architecture for GIAC Enterprises that is described in Jim Hietala's paper, section 1.5, and included here for reference.

1.5 Network Diagram of Proposed Architecture

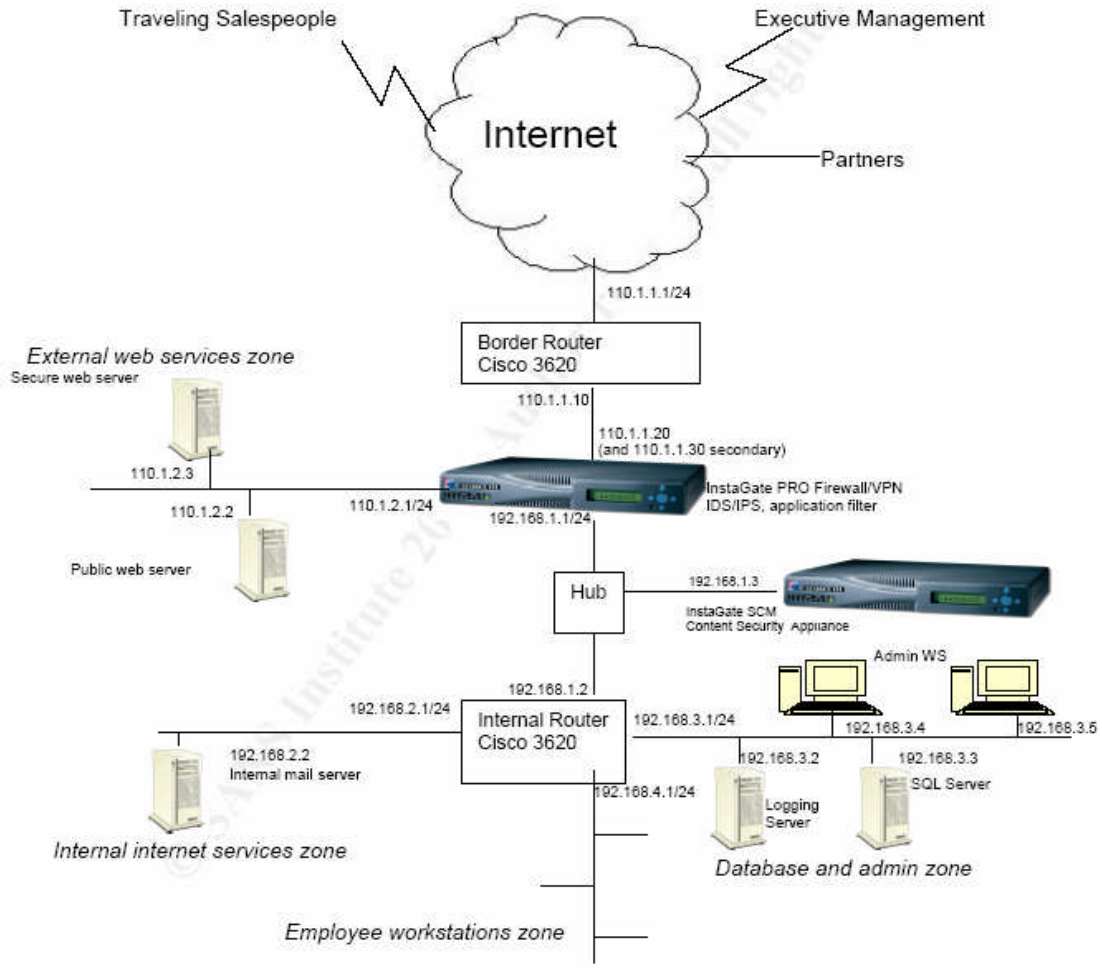

Figure 1

Section 1 - Executive Summary

The proposed solution being evaluated for our medium-sized university environment is a good one. It reflects current strategies (i.e. defense-in-depth), and doesn't rely on any one device or technology to provide protection. Instead, Jim Hietala considers security from all areas of the network - from the Internet and from internal zones, and for all users of its services, including customers, suppliers, internal users, system administrators, partners, etc. The balance that it provides will ensure that attacks that do succeed will be contained to minimize damage. The proposed architecture covers a detailed technical solution, including how devices such as routers, firewalls, and security appliances will work together to offer the best protection for the money. Jim covers perimeter protection, including a border router and an external firewall appliance. Internal protection includes zones that are protected from one another using an internal router and an internal firewall. The zones include a secure web services zone for inbound access from the Internet, an internal e-mail zone, a zone to protect the database servers and a zone for the workstations of administrative support personnel. The design ensures secure transmission of sensitive data with SSL (Secure Socket Layer), secure authentication using Verisign certificates, and secure remote access utilizing VPN (virtual private network) services along with a personal firewall recommendation. Additional layers of defense include anti-virus protection, an IDS implementation, and some SPAM detection.

Per management's requirements, outbound access is controlled via a proxy server, so web access can be configured to minimize risks associated with allowing employees to access inappropriate web sites. This should help to improve productivity, and also to ensure that no employees are offended by what they might see on a display or printer. The ability to set rules for policy is flexible so that policy can be established that fits the environment today and in the future.

Proposed changes to the architecture include providing more redundancy to minimize service outages, including the firewall and an alternative Internet connection, and assuring that the devices can handle the traffic capacity reflected in the larger university environment. Additional recommendations include expanding and improving documented policies and procedures, to ensure secure practices for employees, as well as partners and suppliers.

Additional training and development should also be considered, in support of the plan to implement adequate security protections.

Changes in the plan will result in improved technical capabilities, a much more stable IT environment with less overall risk, and an improved work force.

Section 2 - Technical Solution

2.1 Multi-Layered Approach

The detailed technical proposal described by Jim Hietala for GIAC Enterprises (found at the following URL: http://www.giac.org/practical/GCFW/Jim_Hietala_GCFW.pdf) describes a multi-layered approach that addresses security for the perimeter, for specific machines within the network that house sensitive information, for machines that are used by technical personnel to manage the network, and for users, both local and remote. Jim also attempts to address some of the company's concerns about how their employees may be inappropriately utilizing the Internet. Protection is included to minimize threats to the business such as viruses, worms, peer-to-peer traffic, instant messaging and SPAM. All of these ideas would be appropriate in any enterprise, including a university, but the architectural components would most definitely be implemented in higher education with differing priorities, as will be described throughout this evaluation.

2.2 Border Router

The technical security architecture for the GIAC Enterprises network starts with a border router. A Cisco 3620 is proposed, which is a good choice for GIAC Enterprises, but the university that the author of this paper needs to secure is larger and has many more users, and is going to require more capacity for larger bandwidth. Referencing Cisco's product data sheets[1], perhaps the Cisco 7500 would be a good choice to support the additional capacity necessary. This model should serve to better optimize the increased need for network density, bandwidth aggregation, serviceability, performance, availability and reliability. Since the 7500 was introduced in June of 2003, it has been significantly improved and continues to be a leader in the marketplace.

2.3 Perimeter Firewall

Inside the perimeter router is a firewall. The primary firewall proposed for GIAC Enterprises is the eSoft Instagate PRO unit. It's a firewall "appliance" that sits on a hardened LINUX OS. It is a stateful inspection firewall, and has the capability to analyze traffic inbound and outbound. This will be useful for not only the analysis of inbound traffic (to protect the enterprise), but can also be used to monitor outbound traffic to help management enforce policy designed to control how employees utilize the Internet while at work. While expensive to implement, stateful inspection provides a very powerful mechanism for packet inspection at multiple layers. In "Network Security for Dummies" [2], Chey Cobb discusses the advantages of stateful inspection. Not only are all packets inspected inside and out, the application, the user and the transport method are all checked and

verified. The information is stored in a “state table” and compared to inbound traffic. If the inbound characteristics do not reflect a reasonable match against the previous outbound characteristics, then the connection is refused and the traffic will not flow. The firewall also supports the needs of remote users, who will be able to use its VPN services to access the network from remote sites. The IPsec VPN will encrypt traffic that these users generate into and out of the enterprise network. The high availability option on the Instagate PRO was not proposed for GIAC Enterprises, due to the additional cost, but for the university environment, where downtime cannot be tolerated, this option can and should be used. The university also generates much more traffic than does GIAC Enterprises, so we need to ensure that the Instagate PRO firewall has adequate capacity to support the needs of our environment. According to technical specifications provided by PFW Systems Corporation[3], there is enough capacity in the Instagate PRO appliance to handle traffic to and from the university network. As more systems, services and departments are added behind this firewall, it is conceivable that an additional appliance may be needed. Testing and monitoring logs will enable us to plan accordingly.

2.4 Internal Zones – Web Services and Databases

The third major component in the GIAC Enterprises security design is what Jim Hietala refers to as an "*external web services zone*". This zone is a partitioned (with firewall rules) and protected segment of the network reserved for web services. The systems planned for this zone are for web services that must be Internet-facing – or available to users who will be accessing them over the public Internet. This subnet will come off of the DMZ interface on the Internet firewall (the Instagate PRO) and will be isolated both from unauthorized users on the Internet and from unauthorized access or mistakes coming from the more protected inner zones of the GIAC Enterprises network. With all of the web-based attacks that we’re seeing these days, this is a good idea. It’s an idea that should work well for any enterprise that needs to host web services, including our institution of higher education, which certainly has many web servers necessary for everything from taking early admissions applications from new student prospects to selling tickets for athletic events. In all cases, the databases can be kept deeper in the network, behind an internal firewall, providing them with more protection. In this zone, Jim has proposed that only necessary services be allowed into and out of this zone, and that makes sense for any partition or zone in a network. Besides connections from the databases to the web servers in the DMZ, it is necessary to allow administrative access into the zone for employees who need to manage the web servers. Those employees should use HTTPS and SSH in order to keep sensitive traffic encrypted, so if it is intercepted, data is not in clear text and cannot be compromised.

2.5 Internal Router

Moving from the outer layer of the network inward, the next security device is an internal router. This device is another Cisco 3600 series box proposed for the GIAC Enterprises network, and could work just fine for the university network as well, but more traffic analysis will have to be done to determine what capacity is required for an internal router. It will depend on where the router is placed in the network, and we could start again with what we know can be handled, and plan to add more devices to the internally protected zone as additional resources are introduced.

Other internal network zones described in the design for GIAC Enterprises include a protected zone for internal electronic mail services and a zone for database servers and administrative workstations. This part of the architecture makes sense for most environments, and could certainly work in a university environment. There is also a subnet reserved for the employee workstations, and their information and connectivity is protected, and network administrators are able to control traffic into and out of the employee subnet in support of management's concerns about acceptable use.

2.6 Remote Access

The last layer of defense is with the remote workstation, and the proposed architecture for GIAC Enterprises includes a recommendation for personal firewalls for remote users who will use VPN services off of the concentrator that is integrated into the eSoft Instagate PRO firewall. This seems like a reasonable and secure solution for any remote users who are coming in to access e-mail or sensitive information housed in databases. The VPN will encrypt the traffic and the personal firewall will ensure, if properly configured, that the remote machine can't connect to more than one network at a time, allowing the user to come in to the business network without creating an inadvertent tunnel from an untrusted external network into the trusted internal business network.

2.7 Software Configurations and Operating Systems

Some of the configurations and operating systems proposed for GIAC Enterprises are described as follows: The secure database server will run Red Hat Linux, removing all unnecessary services. A host-based IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) product will also be installed to offer even more protection for the server's sensitive database information. Attempted intrusions will be blocked at the web server, and this type of service also seems to be appropriate for the university environment. Either Cisco's Okena product or Network Associates' Entercept is proposed and should

work in the university environment as well. The web server will run Microsoft's IIS. All unnecessary services should be removed from this server as well, and a solid patch management process will be critical to ensure that the numerous vulnerabilities that are uncovered for this particular software are taken care of in a timely manner. Proposed for IDS/IPS protection is the eSoft IDS/IPS SoftPak for the Instagate PRO unit. This module will detect and prevent against intrusions. The software was originally developed by Latis Networks and is a commercial implementation of SNORT, a generally popular IDS program in the open source environment. It also supports automatic blocking, based on dynamic rules in the firewall. This module is integrated right into the firewall, and while it represents a single point of failure (as opposed to having two network devices for firewall and IDS/IPS), the risk is deemed acceptable for our purposes.

2.8 eSoft InstaGate SCM Secure Content Management Appliance

The last device proposed for the GIAC Enterprises network protection architecture is provided by an eSoft InstaGate SCM Secure Content Management appliance. This box is proposed to sit between the firewall and the internal network zones, and will provide proxy services, scanning for e-mail-delivered viruses, scanning for SPAM, and filtering of outbound web traffic by URL. This appliance will allow us to set rules for outbound traffic filters based on policy that reflects the concerns of management. This device also offers reporting capability, which can be useful in determining how web and e-mail services are being used, and how many viruses are blocked.

2.9 Addressing Scheme

The addressing scheme proposed for GIAC Enterprises is fairly standard, and uses public and private (non-routable) addressing. Use of campus-wide private addressing is intended to supplement but definitely not replace edge and host-based security measures. For internal systems, Network Address Translation (NAT) will be used to ensure that internal addresses are not exposed to the public Internet. Network Address Translation, according to Network Safety[4], allows your *Intranet* to use addresses that are different from what the outside *Internet* thinks you are using. As an example of something similar, consider a company telephone system with several hundred telephone extensions. Each telephone has its own internal "extension" number, which it uses to call others in the company. When it calls someone on the outside, however, the outside sees the number of the "trunk" line that the system uses and not the extension number of the user's telephone. The actual connection between the outside trunk and the inside user is maintained temporarily by the telephone system. NAT can do the same thing for Internet communications. IP addresses are assigned to internal users, and when they want to connect to the outside network, NAT creates a temporary connection, just like the telephone system would. And, like the

telephone system, the outside doesn't care what sort of internal numbering scheme you create for your users. The only IP address that matters is the one seen from the outside.

2.10 Proxy Server

A proxy server will be used for Internet access as well, so that the firewall and other appliances cannot be effectively “bypassed” by a user trying to access an Internet site that is not allowed by management. It will also help to address issues associated with low productivity stemming from Internet abuse. According to Florida State University’s Campus Security Resource Authority[5], the Eighth Annual Computer Crime and Security Survey taken by CSI/FBI states that (as in previous years), insider abuse of Internet access is as much as 80% of total access.

Section 3 - Agreement

3.1 Adapting to Local University Environment

There are many aspects of this plan for GIAC Enterprises that seem to be a good fit for a medium-sized university environment. A University is a diverse environment, but this architecture can be applied in such a way that most of its proposed policy and structure can be applied to the administrative network that is in place to support staff who keep the business of running a university going and who hold most of the sensitive information that needs to be protected (i.e. admissions information, personnel data, medical records, financial records, student data (subject to regulatory compliance), grant proposals, etc.). The proposal addresses some of the common concerns of a university, including the rising demand for Instant Messaging and concerns regarding large volumes of SPAM, viruses and worms. University IT budgets are often limited, so the fact that the GIAC network was designed with cost in mind certainly makes it attractive. Since staffing is also limited, the solutions offered are easily implemented and managed, also providing a good fit. In addition, the architecture can scale to accommodate larger numbers by adding hardware or upgrading hardware devices.

3.2 Access Control

The standard practice suggested for the GIAC Enterprises user base is one of restricting access to only those systems and services required by each user in order to do a job. This is certainly a good approach for any enterprise, and one that will limit exposure – especially to an inside threat.

3.3 Defense-In-Depth

The most attractive aspect of the design is the strategy *of "Defense-in-Depth".* Defense-in-Depth is widely regarded by IT Security experts as the most effective strategy in an architecture, because there is no one solution that can stand up to all of the threats that a typical network will face today. In "Hacking for Dummies" [6], Kevin Beaver emphasizes the practice of defense-in-depth, and suggests that a designer should not focus efforts on perimeter security alone. A successful security architecture will focus on a layered approach. Kevin uses the analogy of a bank. A bank has security cameras focused on cash drawers, teller stations and systems, and surrounding areas – not just in the parking lot or at the entrance. In a business, a layered approach is best as well, so that just in case one security measure fails, many other barriers will be in place to stop the activities of a malicious attacker.

3.4 SSL

Requiring the use of SSL by suppliers and customers who need to access the secure web server is also a best practice and should be adopted wherever it is necessary and reasonable to do so. The proposal calls for the use of Verisign certificates for remote user authentication. Verisign is perhaps the most highly regarded supplier of certificates in the industry today, and supports customers world-wide, which is important for a global business, but could also be important for a university with a very diverse user base with people from all over the world accessing sites for e-commerce, applications, transcripts, etc. Authentication is important when providing such important services.

3.5 Change Management (Tripwire)

Because the data on some of the GIAC Enterprises servers is critical, and must be protected for confidentiality, reliability and integrity, the fact that a product like Tripwire is recommended is commendable. Tripwire, Inc.'s[7] home page states that "Change Monitoring and Analysis software establishes the foundation for stable IT operations and systems security". As indicated, the presence of a product like Tripwire will also help to ensure that an effective Change Management process is implemented.

3.6 Appliances

One of the strengths of the Instagate PRO is that it is a true appliance. Appliances are generally thought of as hardened servers, with just the necessary services enabled on the box. Its updates and security patches are made to the unit automatically, saving time for system and network administrators whose job includes making sure that critical components are patched and updated regularly. This has never been more important than it is right now, with all of the exploits that are loose in the wild. The IDS/IPS component of the appliance is attractive for several reasons, but most especially because it can block peer-to-peer protocols and instant messaging. These capabilities are important for staff networks in a university, but would be less attractive for residential networks, where universities often see themselves as Internet Service Providers. However, some schools are now blocking peer-to-peer traffic due to high volumes of complaints from copyright holders, so this capability could be important to us.

3.7 Requirements for Partners and Suppliers

Another positive suggestion in Jim Hietala's proposal is to ensure that suppliers and customers have implemented firewalls for public access points into their own networks. Since these sites are partners and exchange a lot of data back and

forth between their networks and the GIAC Enterprises network, this practice will help to protect the data and the transactions that move the data back and forth.

3.8 Published Resources Available

The proposed architecture itself is a good one, implementing the defense-in-depth strategy described earlier, as well as encryption for sensitive traffic, hardened operating systems, anti-virus protection, the ability to manage inbound and outbound traffic, authentication and authorization mechanisms, and IDS/IPS to help assess the effectiveness of the architecture in place.

Jim Hietala also did his homework. He looked at threats and vulnerabilities, and looked to address the SANS Top 20 Internet Security Vulnerabilities[8] which are developed independent of any particular type of business or industry. Jim also utilized the Cisco IOS Manual[9], which can be very useful in developing effective and standard policy for the router. This reference (and ones just like them for other versions) will be useful to any site looking to implement Cisco routers.

3.9 Adapting Standard Practices

For all of the network devices, as well as servers and other equipment on the network, Jim was careful to ensure that no vulnerabilities were left open by default, changing passwords and closing unnecessary ports wherever possible.

An approach that Jim Hietala consistently takes throughout his proposal for GIAC Enterprises is that he attempts to utilize standard practices when he can. This makes sense for any site in that it will minimize the level of effort required to train personnel who will then be charged with support and maintenance of the devices and architecture described. It will also keep the costs down. His approach is evidenced by several things. First, he ensures that his design addresses the SANS Top 20 Internet Security Vulnerabilities. He also utilizes the Cisco IOS manual for developing his proposed security policy. Taking these actions will make it easier for system and network engineers in the university environment to focus on the things that are really important and also to get help more easily when things go wrong or when they simply need to understand more about how things work.

Some sound security practices are being suggested for GIAC. Basic controls are addressed, such as ensuring that default passwords are changed to secure passwords, that access to the console and auxiliary ports are restricted, and that all unnecessary protocols and services are disabled. A warning banner is also added to the border router, again using standard language. Other standard controls recommended include logging to a central server (for audit trails). Jim also suggests the application of some class-maps that can help prevent inbound

HTTP attacks. He is also careful to consider the sequence of individual rules in rule sets, keeping in mind how the firewall makes decisions and also how it performs, trying to keep traffic flow as efficient as possible. Backup is also considered, as the work invested in a solid rule base for a firewall or a router should never be lost. All of these practices can and should be applied wherever these devices are used – and would certainly be required in the university environment.

3.10 Documentation

The detail provided by Jim to describe each firewall and router rule, giving its purpose and importance, is very important. This enables someone less technical (i.e. management who control the budget) to read and understand the level of security proposed, and the descriptions allow for more dialogue about the pros and cons of each decision being made. The use of screen shots is also very effective for the reader. Jim describes some of the features of the appliances that are not being proposed for GIAC Enterprises, but wants the reader to know that there are some options, and that some limitations have been applied, based on budget and other resources. For example, Jim suggests that GIAC consider a more restrictive policy for VPN users in the future, perhaps taking advantage of a global roaming agreement with a dial network provider. This could enable GIAC to be selective in what networks they would allow connections to come in from. Without this level of documentation, misunderstandings would be much more likely to occur. So Jim's investment in documentation now can be expected to minimize changes later on – not to mention the challenges of trying to troubleshoot an undocumented rule set. This approach to documentation would certainly be welcome in the university environment, and anywhere else. A designer needs to assume that people involved in the decision making will need to understand the design well enough to make an informed decision. And the reader of the proposal will certainly have more confidence in the designer's ability as he shows he has thought things through and understands and is confident with what he is proposing. This effort now will ensure that the design, once implemented, will serve the environment well – and we shouldn't expect a lot of surprises.

3.11 VPN

For VPN access, the proposal suggests the use of the stronger and more secure IPSEC protocol over PPTP. It's also important to note that no split tunneling will be allowed. In other words, remote clients will not be able to access the Internet directly while they have a VPN connection established. Again, Jim describes why this is important. A secured shared secret is used to provide VPN access, and a "High Security" configuration (Triple DES, SHA-1 hashing and MD5

authentication) has been selected for VPN encryption. These ideas seem to make sense, have industry backing, and should serve the university well.

3.12 IDS/IPS

Another positive aspect of Jim Hietala's configuration is with regard to the implementation of the IDS/IPS module in the Instagate PRO appliance. Jim suggests that we monitor not only traffic coming in through the WAN interface, but also traffic through the LAN interface. This would help to determine if a problem was introduced into the network from inside – via an infected laptop, for example. If internal traffic is monitored, we need to test to make sure that performance is not adversely impacted due to increased logging requirements. Jim also suggests we block Netbios type attacks from leaving the network – using outbound filtering.

3.13 InstaGate Appliances

There is an application filter in the Instagate PRO that will enable us to filter based on application. So management's desire to control the use of Instant Messaging and peer-to-peer traffic can be accomplished using this filter. This type of filtering may not be appropriate for all areas of the university, but could certainly be considered for the administrative zone. For example, the network that is used for residence halls should not be as restrictive as the network used by full-time employees. At any rate, it's nice to know what the options are in case new problems arise that need these types of filters.

The university can also use the InstaGate SCM content security appliance as a key component of our system. Filtering SPAM is certainly something our end users are demanding. A gateway for anti-virus scanning is also a no-brainer. No site today can be without an effective system in place for looking for and containing viruses and worms. Jim's idea to relay all mail through the content security appliance to make sure nothing gets in is a good idea, as well as proxying outbound web traffic. When a virus is identified, both the end user and the system administrator will be notified, which is really important, to make sure that if mail doesn't get delivered, at least the end users can remove the viruses and resend the intended content. For the SPAM filtering module, there is an exception mechanism that can be applied that can help to make sure that legitimate messages will be delivered, even if they contain some characteristics generally found in SPAM messages.

Everything described above in this section calls out parts of the proposed design that seem to be good suggestions and that would appear to be a good fit for the university. The following section will detail things that may be weak in the proposal or that don't seem to be a good fit for the university environment.

Section 4 - Disagreement

4.1 Redundancy and Failover

It's understood that Jim Hietala's proposed design for GIAC Enterprises was done with a very tight implementation budget in mind. The economic constraints might line up against acceptable risks in a small business environment, but be less acceptable in a larger environment such as a medium sized university. One area where risk needs to be carefully considered is in the area of redundancy and failover. Jim's design touches on some recommendations for redundant devices for critical architectural components, but he also says that those recommendations will not be implemented due to budget constraints. Because failure of some of these devices will affect every user and process in the network, I think that Jim should have looked at the costs associated with deciding not to implement some of these measures. For example, if the border router ceases to function, management at GIAC Enterprises should know how long the outage could last, and what affect such an outage could have on business. This sort of analysis should be done for every critical component in the design. In fact, if this were done consistently, it could be that a different type of design would result. Perhaps managers would decide it's more important to have the network up 7 by 24 than to implement filters for SPAM and Instant Messaging. Perhaps some open source code could be found (i.e. SPAM Assassin) that could free up some resources to apply against some redundancy and failover capabilities. For our medium sized university environment, some of these tradeoffs will have to be carefully considered. Because of the nature of research and higher education, the network really must be redundant and the major components of perimeter security as well (i.e. routers and firewalls). Any downtime at all could affect critical research, patient care, classroom work, etc., and so risks associated with availability have to be taken into account. I'm not convinced that Jim's proposal really considered the repercussions of downtime or failures to the GIAC business, which he says is very competitive.

4.2 Single Points of Failure

Another thing that Jim should consider carefully and communicate in his design is the concept of having too many eggs in one basket. Again, to save money, single devices are providing multiple key services. Ideally, separate boxes would be introduced to minimize the impact of losing a single box, but GIAC Enterprises can't afford it. Again, I think it would be prudent for Jim to further analyze the pros and cons of setting up his architecture in this manner, giving budget managers a chance to better understand what they are risking with the decisions being made.

4.3 Scope of Design Planning

Jim describes in several places the scope of the project, but does not tell the reader how the scope was arrived at. We don't know how much the customer was involved in defining the scope, and it would be useful to know. The more the customer is involved in these decisions, the more successful we can expect implementation of the design to be.

It could also be useful to know whether or not Jim considered recommending some level of outsourcing for this project – either for training or for monitoring, logging, firewall protection, etc.

Jim also talks about some of the things that are out of scope for the project, such as firewalls and anti-virus for customers and suppliers, but if these solutions are out of scope for GIAC Enterprises, then I would be interested in what alternatives he might suggest for remote users. Even if the project can't afford commercial solutions, there might be other ways to mitigate the risk associated with this type of access. In an article written by Salvatore Salamone, published by TechRepublic[10], products like ZoneAlarm can be configured to check to see if vendors and others have certain settings before being allowed to connect. When a remote user connects to the network utilizing VPN, even though the transmitted text is encrypted, an intruder could gain access to the remote computer and then enter the business network from that point. If the remote system is compromised, it could also inadvertently introduce malicious code into the internal environment (i.e. viruses, worms, Trojans, and spyware).

4.4 Assessing Risk

Jim says that GIAC Enterprises is growing rapidly, it's a customer-driven business, and the competition is fierce, but there is no budget for redundancy or failover. In the absence of these important features in the design, it would have been prudent for Jim to describe the risk, and what losses could be expected if this doesn't change. Are there plans to expand in the future? What do the maintenance contracts look like in terms of turnaround time for telephone or onsite support, for hot spares, replacement parts, etc.? Would it be better to exclude the internal firewall in favor of a redundant perimeter box? Maybe lower-cost software firewalls could work internally – to help manage internal risk. These would all be important questions for me to know the answers to as I consider this design for my enterprise.

Jim keeps two critical databases on the same server. If the hardware or operating system experiences a problem, both sets of data are unavailable, and this could be avoided. I would like to see some options here – perhaps two boxes that are smaller but able to carry the load of both databases in an emergency.

The web server to be used at GIAC Enterprises is an IIS server. Jim is recommending some improvements for the web server, suggesting that it be moved to another Internet-facing zone. Another thought I have is that he might consider a safer configuration for the web server, if possible, as IIS has been the target of many types of attacks. There is helpful information available publicly (see Cindy Souders'[11] article on TechRepublic's web site) as well as coursework that will provide more professional and complete material (reference SANS Training for Securing IIS Servers[12]).

4.5 Third Party Involvement

Jim's recommendation to have GIAC personnel manage the access router instead of a service provider is a good one. This is a critical component in this design. For services that must come through third-party providers, I'd like for Jim to discuss the contractual agreement in more detail, giving the reader more "peace of mind" in terms of what the business can expect from third parties, and what compensation can be obtained should service be interrupted, data lost or compromised, etc. Jim also mentions that the service provider has been asked to implement filtering on the access router, to prevent non-essential protocols and services, but it isn't clear who decides what the configuration will be, how it will be documented, controlled, etc. This should be in writing and formally agreed to.

4.6 Certificates and Authentication

Verisign certificates are proposed for customer and supplier assurance as to the authenticity of the GIAC web server, but we also should consider authentication of the persons who are accessing that server, and it isn't really addressed. Also, I think it would have been prudent for Jim to recommend a procedure for managing the certificates, because if certs are not managed responsibly, then they really lose their effectiveness.

4.7 Patch Management

Jim Hietala's proposed architecture, due no doubt to budget constraints, makes some things recommended when they really should be mandatory, given the nature of the GIAC Enterprises business. For example, active patch management is recommended, but what Jim doesn't say to GIAC management is that patch management needs to be done one way or the other – it really isn't an option. Utilizing tools in a patch management strategy can benefit an organization in many ways, improving efficiency and saving labor as well as dollars. Microsoft offers information about the importance of managing updates and patches in a timely manner. Microsoft asserts in one of their TechNet webcasts[13] that "Used properly, they can prevent downtime, loss of data, and

other costly problems resulting from an improperly patched infrastructure." Whether it's done manually or in an automated fashion is really the question here, and I'm not sure that point is clear in the proposal.

4.8 Technical Personnel

System administrators, network administrators and DBAs are very important to the security of these systems and databases, but we don't know much about the capabilities of the technical personnel. To me, this would be important to consider. Do we need more technical people? Do the people we have need more training for new hardware and software? What is their development plan and how will they work together to achieve expected results? How will they manage access? Hopefully, these administrators will also get a chance to participate in the review of this proposal and be given the opportunity to point out issues or weaknesses in it.

4.9 Capacity

Jim Hietala's assessment is that the Cisco 3620 has enough capacity to handle requirements for the foreseeable future, but he doesn't provide bandwidth capability against estimated bandwidth needs, and we aren't sure how much time we have before we need to consider an upgrade. In other words, what does the *"foreseeable future"* really mean in terms of time?

4.10 Encryption

It's clear that administrators will need access to both web servers from the administrative workstations, and that they will use HTTPS and SSH to access the servers, but another important point to be made here is that SSH, in particular, needs to be kept up-to-date, as there are numerous exploits available for older versions of SSH. Someone needs to be responsible and accountable for regular updates – and needs to subscribe to the right mailing lists in order to stay well informed about patches, critical updates, etc.

4.11 Addressing and Access Control

Regarding the internal router described in the proposed design, access controls are described to limit access to the databases and to restrict access based on a need to know basis. There isn't much discussion about whether or not IP addresses will be static or dynamic, and how that might affect how access is granted. I would have liked to have seen this discussed in a bit more detail.

4.12 Remote Access

There is a statement in the design proposal that requires partners and suppliers to use firewalls to protect their own networks, and there is also a requirement for remote employees to utilize personal firewalls and anti-virus software along with VPN. But there is no discussion about how GIAC will be able to enforce this. We don't even know for sure if these folks will be asked to sign a contract or agreement with the requirements clearly stated. Also related to the VPN implementation is a statement that the authentication protocol to be used will be MS-CHAP2 but we don't know why. The Computer Technology Documentation Project[14] contains computer documentation and information in various technical areas including authentication protocols like CHAP and MS-CHAP. The documentation is suited for all levels, including experts. It might have been helpful for Jim to utilize a resource like this one to briefly describe the differences between the various authentication protocols and why this particular one was chosen as a good fit for GIAC Enterprises. It would also be helpful to have the VPN configuration shown in the network diagram depicted in Section 1.5 of the proposed design.

One last thing about the VPN configuration: it would be helpful to know whether or not this VPN implementation supports access for different groups – so that group policy can be applied based on need-to-know.

4.13 Monitoring and Logging

When Jim references logging in Section 2.1.4 of his design document, it would be helpful for him to discuss in more detail a logging strategy. Who reads the logs, how much data is kept and for how long, and what happens if anomalies are found? These are questions I'd want to ask about the logging capabilities. Also in the table in the same section, under the "Importance" column, Jim makes many comments like *"Strengthens security"* or *"More secure to disable"*, but it's not clear *why* in some cases – and a more detailed message in the "Importance" column would be helpful. Jim's tables are great, and very helpful, but in some places, they are not totally complete. The same thing can be said for the firewall table near the front of Section 2.2.2.

4.14 Managing Access Control Lists

At the end of Section 2.1.6 in the proposal, Jim talks about the importance of sequence in the access control lists, but he doesn't really tell us *why*. Is it for protocol – for readability – for performance?

4.15 Physical Security

One question I'm left with after reading through Jim's design is that of physical security. I would like to see a section dedicated to the planned access controls for hardware, environmental controls, etc.

4.16 Application Filtering

Related to the application filter configuration, the design document for GIAC Enterprises references a list of applications that will be blocked. It would be helpful to know where this list came from, how it is updated and by who, whether it can be customized, and what the customization process would look like. The list is composed of applications used for Instant Messaging and peer-to-peer file sharing applications, and it is well known that there are many changes and additions to this list as developers try to stay ahead of the filters.

4.17 Proxies

The InstaGate Pro will act as a proxy server for several types of traffic, and Jim states that "*using a proxy server is the preferred mode of operation from a security standpoint"*, but he doesn't explain why. He might have discussed this more – the role of a proxy server in this context and how it works to increase the security of the network and/or control the behavior of the users. Jim also recommends hardening of all servers and network devices, but really doesn't address how client configurations should be controlled. Workstations can be vulnerable to attack and a plan to keep them properly configured and protected needs to be addressed.

4.18 Vulnerability Scanning

Jim recommends that an outside vendor be brought in periodically to scan the network for vulnerabilities. This could be costly, and since cost is a major issue for GIAC Enterprises, it might be worthwhile to explore what it would take to run self-scans – from an internal machine as well as from something on the Internet side. There are several good open source scanners available that could be evaluated for this purpose. Tony Bradley[15] has written a good article on vulnerability scanning, its importance and the options involved that can be found on one of the many network security web sites available. Jim also recommends automated patch management, but there is no discussion regarding the different types and which one might be a good fit for GIAC. Since Jim now knows the GIAC Enterprises business environment very well, he might be in a position to make a more specific recommendation.

4.19 Maintenance

Another topic for discussion in this design document might be maintenance. What should administrators sign up for? What mailing lists should be subscribed to and what web sites would be useful to monitor regularly?

4.20 Business Continuity

There might be some concern about having too many services running on the appliances. It might be fine if we had some backup or failover capability, but we don't in this case. So I think that there should have been a discussion included to address the worst-case scenario associated with losing any one of these machines identified as a single point of failure. Management at GIAC Enterprises should be clear on the level of risk they are accepting. In other words, if one of these boxes goes down, the impact should be fully understood ahead of time, and a detailed plan in place to address recovery of services in a timely manner that is also understood by GIAC Enterprises' customers and partners.

4.21 Managing E-Mail

The InstaGate SCM appliance holds infected e-mail messages in a quarantine folder, and they can be released, but Jim doesn't describe how that release mechanism would work. Users might be concerned about privacy or loss of important e-mail, so a procedure for handling these quarantined messages should be communicated and fully understood. I would have liked to see a more complete coverage of how SPAM filters are set as well. What are the criteria for high, medium and low? If any messages are to be deleted (and they will be if they score in the "high" category), then we should be given very solid assurance that these messages will indeed be SPAM – as close to 100% as we can get. Users need to know what risks they are facing as these policies are implemented.

4.22 Legal and Regulatory Compliance

Jim did not address legal or regulatory compliance issues in his design proposal. For the university implementation, it is recommended that legal counsel review the proposed design, considering issues associated with filters, monitoring, logging, etc. that could impact privacy or compliance with state and federal regulations. Students have different rights than employees, and requirements change from state to state.

4.23 Web Access and Policy

The only other shortcoming I might identify in Jim Hietala's design would be that he doesn't describe how the filters that block access to unauthorized web sites will be maintained. We should assume that there will be additions, exceptions, etc., and this will have to be addressed. None of the databases created for this purpose are static – the world-wide web is very dynamic, and the database will change along with it.

Section 5 - Improvements

Jim Hietala's design for GIAC Enterprises has a very thorough approach, utilizing defense-in-depth, and much of his proposed solution would convert easily to many other environments. My plan to improve on Jim's design (and to adapt it to a larger environment) would include the elements described below which should be included in a management briefing.

5.1 Suggestions for Improvement

Suggestions for Upper Management Briefing

What are the recommended changes?

Technical
- Improve redundancy and failover capability
- Assess current capacity (and planning) for Cisco 3620 (testing)

Procedural
- Harden the web and database servers and document the procedures for doing so
- Improve documentation
- Address procedure for certificate management
- Strengthen agreements with partners and suppliers (include requirements like firewalls on their networks)
- Emphasize patch management, which is even more important in a larger environment
- Address change management (and include desktop workstations)
- More fully flush out a logging strategy (who, what and how often and what's done when an anomaly is found)

Managerial
- Perform some additional risk assessment
- Articulate who manages what and assign accountability
- Assess technical capabilities and training needs
- Add some consideration for physical security
- Develop internal scanning mechanisms with separation of responsibilities
- Develop some simple business continuity plans
- Establish more detail regarding the handling of quarantined e-mail and SPAM filtering (addressing risks associated with dropped e-mail messages)

5.2 Reasons for Recommending Change

Why are the changes important?

All of the proposed changes are recommended because of the significant difference between the business described in Jim Hietala's design proposal and that of an institution of higher education. There are differences in size, culture, purpose and risk that need to be addressed in order to apply the work completed for GIAC Enterprises to that of the university environment.

5.3 Proposed Actions

What needs to be done?

- Consider additional hardware – possibly an additional router and perimeter firewall. If no money can be obtained to pay for the hardware, the risk of replacing the internal firewall with some perimeter hardware should be assessed. Lack of an internal firewall could be compensated for with host IDS or host firewall solutions – targeted at servers with sensitive information on them. The logging from these servers could be sent to the centralized server.
- Establish a secondary Internet connection – after determining the absolute minimum bandwidth necessary to maintain critical connectivity.
- Assess capacity of the perimeter router and firewall for additional bandwidth needed to support the university environment.
- Perform some additional risk assessment – to assess the level of risk that no failover or redundancy will bring to this new university environment, which is assumed to be greater than that of GIAC Enterprises.
- Have technical personnel harden the servers and document what was done.
- Document secure procedures for certificate management.
- Have Legal support review contracts to strengthen agreements and responsibilities of suppliers and partners.
- Plan for additional training for technical staff. Online training should be considered as well as some certifications for senior staff. Training should be looked at as a motivational incentive for more junior staff. To save on cost, a "train the trainer" approach can be taken, where senior staff take formal courses and then bring what they've learned back to share (in the context of the local environment) with more junior staff. This practice also reinforces the knowledge of the senior staff.
    - Target subjects that will include patch management, change management and centralized logging – fundamental system administration and security.
- Assign an individual to document improved procedures and policies for the environment. This individual should be someone on staff who can write well and understands the importance of positive communication at all levels of the organization. In a university, the training and communications departments can be tapped as well, where in a smaller business, these types of resources may not be available at all.

5.4 Benefits of Change

What are the benefits?

- Less overall risk
- Clear understanding of who manages what (accountability)
- Improved technical capabilities – for now and for the future
- More knowledge about how efficient the network is performing
- Similar cost – better application of existing resources based on risk
- A better trained staff that is not only ready to take on current challenges, but should be ready to take on changes or additions related to capacity planning as well.

5.5 TCO and ROI

Total Cost of Ownership (TCO)

The following is taken from About.com's[16] online library:

A good cost model helps track down everything relevant and helps to minimize overlap in spending plans. It also includes business drivers for the various costs and benefit items. We should generally start with collecting costs for our proposed improvements. Both labor and technical expenses related with the *"entire project lifecycle stages -- acquisition, operations, growth/change -- covering costs at owning, deploying and upgrading"*, should be included.

Cost Model	Acquisition and Implementation	Operations	Ongoing Growth and Change
Hardware (maintenance, support)	$6200 (router and firewall appliance)	20%/year	
Software (deployment, upgrading)	OS' provided		
Network and Communications	$1200 for Redundant Internet connection	$1200/year	10%/year
Personnel Costs: IT Staff	0.5 FTE - $27,500.	$27,500/year	5%/year
Personnel Costs: Users	Open Source (some time for training)	N/A	N/A
Consulting Fees	$1000	None	N/A
Training (administration, end-users)	$5000 per person per year (average)	$5000 per person per year (average)	10%/year
Other Costs: Infrastructure Facilities, etc.	None	None	Reassess annually
Total ($)	$40,900		

Key Aspects of TCO:

- an annual cost figure does not cover the benefits of asset usage or ownership.
- most analysts consider it unwise to use TCO alone for evaluating potential technology initiatives.
- the cost of the hardware and software, according to many TCO studies, cover only 15% of the total cost of asset ownership, while Management, Support and other Indirect expenses claim the rest - 85% of the total cost.

How do I calculate ROI?

Information for the ROI formula used below was obtained from CIOview's[17] web site.

Return on Investment (ROI) may be the best measure of how one business practice compares to another. Return on investment results from the current value of your net benefits (gross benefits less ongoing costs) over a period of time divided by initial costs. The result is a percentage over a given amount of time. In the world of IT, a period of three years is most generally used because technology is usually considered to be obsolete after three years. The calculation for a 3-year ROI could look like the following:

(net benefit year 1 / (1+discount rate) + net benefit year 2 / (1+discount rate) + net benefit year 3 / (1+discount rate)) / initial cost.

So if the initial cost for the university's network design improvement plan is $40,900, and the annual benefits minus annual costs are constant at $20,000 for the next three years, and the discount rate is 10%, your 3-year ROI would be:

($20,000 / (1 + .1) + $20,000 / (1 + .1)^2 + $20,000 / (1 + .1)^3)/$40,900 = 133%

ROI can help us to estimate what percentage of return we can expect to get over a specified period of time. It will not tell us anything about the magnitude of the project. In other words, a 133% return may seem very positive, but what's more attractive - a 133% return on a $40,900 investment or a 60% return on a $400,000 investment? So again, this is only one tool that can be utilized when considering technology spending, and should never be used independently of other tools and information.

5.6 Training and Awareness

Suggestions for Training and Awareness:

- Online training
- Vendor training and certification
- SANS Track Training and web site resources
- Books and other publications for system administration and security
- Technical mailing lists and online forums
- White papers
- Web pages for communication
- Newsletters and e-mail status notices
- Periodic briefings

5.7 Policy and Procedures

Proposed changes to policy: (to back up procedural recommendations)

- Require documentation for configuration management, patch management and logging strategy (could be part of a records retention policy)
- Document procedure for certificate management
- Develop checklist to include standard language in agreements with partners and suppliers (include requirements like firewalls on their networks) and have legal experts review it
- Require annual risk assessment
- Develop policy for physical security of computing equipment
- Require at least some simple business continuity planning

5.8 Additional Recommendations

Adjunct Actions:

- Review technical job descriptions and strengthen requirements as necessary
- Develop internal scanning mechanisms with separation of responsibilities
- Establish more detail regarding the handling of quarantined e-mail and SPAM filtering (addressing risks associated with dropped e-mail)

Section 6 - Conclusion

6.1 Basic Conclusions

After studying and analyzing Jim Hietala's proposed network security design for GIAC Enterprises, I believe that his approach will work as a good starting point for just about any enterprise. He considers defense-in-depth, and does not rely on any one particular solution, device or technology to secure his business. If an individual wants to design an architecture for a site, that individual could benefit from Jim's plan. Then some adjustments would have to be made, but it will be much less effort than starting "from scratch". The things that should be considered for any other site would include the size of the enterprise (to adjust for increased capacity needs), as well as the culture of the organization, because what will be accepted by users at one site or location cannot be assumed to be acceptable for everyone. Defense contractors can be expected to have employees with a different mind-set than those who work in a research institution. Other considerations should include numbers and experience of technical personnel, risk, the type of information stored and/or transmitted by the organization, and the sophistication of the end users.

6.2 Value of Design Analysis

Any design proposal will benefit from an analysis just like the one we did here – looking at pros and cons, strengths and weaknesses, how the technology works together, what can be adopted right away and what cannot – and how to improve on the weaknesses. The format really makes the designer or manager think about what applies and what doesn't, and helps to facilitate a thorough analysis of options and how they might apply to one's own work environment.

So I agree that Jim Hietala's design is a good one, but that its value lies more in its approach than in its actual implementation. The analysis that he has done is fairly complete, and anyone who studies it will learn a great deal about his thought process, and how he has considered risks to the organization.

References

[1] Cisco Systems, Inc. “Cisco Gigabit Ethernet Solutions for Cisco 7x00 Series Routers.” Cisco Systems, Inc. 1992-2004. URL: http://www.cisco.com/en/US/products/hw/modules/ps2033/products_data_sheet09186a0080091ce7.html (15 May 2004).
[2] Cobb, Chey. Network Security for Dummies, 1 edition. For Dummies, 10 October 2002. Page 92.
[3] PFW Systems Corporation. “InstaGate PRO™ Product Specifications.” PFW Systems Corporation. 2004. URL: http://www.pfw.com/solutions/productpdfs/instagate_pro.pdf (20 May 2004).
[4] Network Safety. “Network Address Translation.” 1996, 1997, 1998, 1999, 2000. URL: http://www.safety.net/indnat.html (09 June 2004).
[5] Florida State University. “CSI/FBI Eighth Annual Computer Crime and Security Survey.” 2003. URL: http://www.security.fsu.edu/docs/FBI2003.pdf (04 July 2004).
[6] Beaver, Kevin. Hacking for Dummies. Wiley Publishing, Inc. 2004. Page 309.
[7] Tripwire, Inc. “Tripwire, Inc.”. Tripwire, Inc. 2004. URL: http://www.tripwire.com (28 May 2004).
[8] SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus.” Version 4.0, October 8, 2003. SANS Institute. 2001-2003. URL: http://www.sans.org/top20/ (16 June 2004).
[9] Cisco Systems, Inc. “Cisco IOS Release 11.1.” Cisco Systems, Inc. 1992-2004. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/ (07 July 2004).
[10] Salamone, Salvatore. “Lock IT Down: Integrated VPNs can help secure remote workstations.” 05 August 2002. CNET Networks, Inc. TechRepublic. 1995-2003. URL: http://techrepublic.com.com/5100-6296-1059707.html (06 June 2004).
[11] Souders, Cindy, MCSE. “Fifteen tips for securing IIS Web servers”. 11 August 2003. CNET Networks, Inc. TechRepublic. 1995-2003. URL: http://techrepublic.com.com/5100-6313-5055458.html (06 June 2004).
[12] SANS Institute. “Securing Microsoft’s IIS Web Server.” SANS Institute. 2001-2003. URL: http://www.sans.org/IIS/sec_IIS.htm (06 June 2004).
[13] Microsoft Corporation. “TechNet Webcast: Security Patch Management Tools (Part 2) - MBSA and SUS - Level 200.” Microsoft Corporation. 2004. URL: http://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032255030&Culture=en-US (07 July 2004).
[14] The Computer Technology Documentation Project. ”Authentication Protocols.” The Computer Technology Documentation Project. 2003. URL: http://www.comptechdoc.org/independent/networking/protocol/protauthen.html (07 July 2004).
[15] Bradley, Tony, CISSP, MCSE2k, MCSA, A+. “Introduction to Vulnerability Scanning.” About, Inc. A Primedia Company. 2004. URL: http://netsecurity.about.com/cs/hackertools/a/aa030404.htm (15 June 2004).
[16] Internet Technology. “Steps for an Effective ROI Analysis -1 Understanding ROI Essentials.” About, Inc. A Primedia Company. 2004. URL: http://internet.about.com/library/aa_roi2_022403.htm (15 July 2004).
[17] CIOview Corp. White Papers. “Financial Primer: How to Calculate ROI, NPV, Payback and IRR.” CIOview Corp. 1999-2004. URL: http://www.cioview.com/resource_whitepapers_financial.asp (15 July 2004).