Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst Practical

Version 4

Future State of Security Technology

GIAC Enterprises – Fortune Cookie Marketer

GIAC Enterprises – Firewall Policy

Submitted: 8 November 2004

Submitted by: Robert F. McKinney Jr.

Table of Contents

List of Figures

Abstract

This paper contains three sections each addressing an assignment for version 4 of the GIAC Certified Firewall Analyst certification. Section one discusses Host-based Intrusion Prevention Systems (HIPS). This section describes HIPS, discusses what problems HIPS may address, a possible way to classify and compare them, and discusses some considerations for deploying them. This section also discusses what impact HIPS may have on the information security industry and practitioners.

Section two discusses the implementation of an Internet based e-commerce presence for a small business. It begins with a review of management's business criteria applied to the development of possible solutions. Some basic policies are provided for which two solution possibilities are presented to support. Software, hardware, and configuration options are discussed and information flow is presented as well for each recommended solution. Defense-in-depth recommendations and a discussion of the reasoning for solution development are provided to enhance and elaborate on the recommended solutions. This section concludes with a discussion of the selected solution and the basic router and firewall rule sets to support it.

Section three discusses the basic firewall rule set in more detail. It provides an explanation of each rule and its hierarchical placement.

1 Host-based Intrusion Prevention

1.1 Problem

Like many other technologies Intrusion Prevention endeavors to improve network and host information security. This discussion focuses on host protection. The problem this technology tries to address may be better described as a group of related problems rather than a single one.

First, there are a multitude of technologies used to secure information systems. Simply sifting through what is available for a single purpose can be tedious let alone wading through all the technology choices, and their combination to implement a plan. Second, many times products in place or desired to implement these technologies do not interoperate. Thus, personnel must provide manual interface actions or develop in-house automated interfaces. Third, often information security staffs are insufficient to adequately maintain and fully utilize tools in place. Even with the best tools at their disposal personnel can be over whelmed with assigned duties negating the benefits of a well stocked toolbox. Fourth, staffs are not always proficient or possess sufficient knowledge to garner required information from available tools. This is another instance when even with the best tools their full benefit is not realized due to underutilization of capabilities. Fifth, reaction time, the time between vulnerability announcement and available exploit is shrinking.

So, a question vendors may ask is; what can we do to facilitate the selection and implementation of a more efficient and effective information security solution? A possible answer is; develop or integrate existing technologies in a fashion that provides knowledge based output and eliminates or reduces manual intervention, reduces cost of ownership, and provides preventative rather than reactive measures. Enter intrusion prevention.

1.2 What is Intrusion Prevention?

Intrusion prevention (IP) generally refers to the integration of intrusion detection (ID) and firewall technologies.[1,2,3,4] It may also refer to the integration of other capabilities such as anti-virus, spam filtering, or rate limiting.[4,5] Some products are not identified as combining existing ID systems (IDS's) and firewalls but describe functions normally associated with these technologies such as signature based detection and packet dropping.[6] The two basic capabilities found in IP systems (IPS's) ID and firewall encompass two prevention and detection of the three fundamental needs for information security; 1) prevention, 2) detection, and 3) response.[7] By integrating IDS detection with firewall prevention techniques Intrusion Prevention can provide, in an automated fashion, the third information security need, response.

Response can be categorized as passive or active. Where passive might be an e-mail alert to a system administrator and active might be closing a firewall port or aggressive active could be tracing to the source of the alert trigger or launching a counter attack.

An IPS, fundamentally, endeavors to provide automated active response. Some products provide some capabilities for limited aggressive active response, as well.[8]

In addition to this type of IPS one vendor offers a different tack and view of IP. It is described as a firewall but not in the traditional sense. It is called a "memory firewall" and is aimed at a single class of attacks, that is, memory-based attacks.[9]

1.2.1 Classification

1.2.1.1 By IDS

Techniques that can be used for detection; 1) signatures, 2) anomaly detection, and 3) artificial intelligence can be used to further categorize an IPS. Likewise, techniques that can be used for firewalls; 1) packet filtering, 2) stateful, sometimes called dynamic packet filtering, and 3) proxy, sometimes called application or circuit gateways may be used to further categorize an IPS. [10,11]

IDS's often use signatures to determine if unwanted activity is occurring. Signatures are based on what is known. That is, an attack vector is identified then translated into information for which the IDS looks. When a match occurs the IDS produces some type of action such as an alert. In the case of an IPS one action is to tell the firewall to block particular packets or close a port.

Anomaly detection systems, however, detect behavior that is outside of what the system has registered as "normal" behavior. "Normal" behavior is not necessarily the same for any two systems. Anomaly detection systems must "learn" what normal behavior is for each particular system. If the IDS detects something not normal, like the signature based IDS, it produces some type of action.

Another distinction needs to be made for this discussion. Traditional host-based and network-based IDS's monitor different activity to try to determine unwanted activity. Host-based IDS's monitor information pertinent to the particular host such as application and operating system event logs. Network-based IDS's, however, are concerned with activity information that originates from the network, e.g., IP packets or TCP TPDU's. [12,13] So, further distinctions can be made based on the type of information the host-based IDS monitors such as log files, file integrity, or network connections. In general host-based IDS's monitor system and application events, network connections, and file system integrity.[14]

1.2.1.2 By Firewall

Packet filters are widely implemented and the simplest of the firewall techniques. Information in packet headers is compared to a rule set to determine what action to take.

Stateful firewalls are more sophisticated than packet filter firewalls. They allow rule-based traffic flow and maintain defined information in tables on allowed traffic to help determine between wanted and unwanted traffic.

Proxy firewalls again increase the level of sophistication. As the name implies, proxy firewalls act as an intermediary for the user or client in a client-server connection. Since proxy firewalls are generally used at the network level not at the host level they will not be discussed further.

In general host-based firewalls control traffic based on rules applied to local applications.[15]

1.2.1.3 By Additional Capabilities

Additional capabilities that may be useful to further address the problem set discussed above may also be available and used to differentiate IPS'. For example; the capability to monitor remote connections and enforce policies, integration of anti-virus capabilities or awareness of anti-virus products, or consolidation of reporting and or maintenance, can be important discriminators for a particular employment. The ability to centrally manage implementation, administration, and reporting of host-based IPS' is particularly important in large deployments.

1.2.1.4 By Attack Class

Traditional classification is not centered around a particular class of attack but rather on characteristics of the technology. One technology discussed, however, differentiates itself from traditional ones by targeting a specific attack. Since research has only uncovered one such offering classification of this type is limited to memory-based attacks.

1.2.2 Comparison

There are a number of ways to classify or compare IPS's. Does the IPS detect according to signatures, behavior anomalies, or both? Does it detect actions in logs, network connections, file system integrity, or some combination? Is the firewall protection simple packet filtering, stateful, application based, or some combination? What additional active response measures other than firewall centric and complimentary capabilities are available?

1.2.2.1 IDS

Signature based IDS' provide good detection capabilities for known attacks. They are generally perceived to be more accurate than behavior based systems as well but are likely to have false negatives. They are also the most common technique used for host based systems.[16,17]

Behavior based systems, though, may be able to detect unknown attacks where signature based ones cannot. Behavior based systems are more prone to giving false positives, however.[16, 17] User actions vary a great deal making the determination of "normal" behavior on general task hosts difficult. Behavior based systems can be more effective on single purpose hosts such as servers where "normal" behavior can be narrowly defined and implemented with required accuracy.

Hybrid systems are a combination of signature and anomaly detection techniques. Hybrid systems try to take advantage of the potential of the higher accuracy of signature techniques with the ability to be able to detect unknown attacks using anomaly techniques. Following from the above, these systems would likely work well on servers.

1.2.2.2 Firewall

Clearly the objective is to stop or prevent undesired actions on the host. All can block attacks based on analyses done by the ID component. But, as firewalls differ in a "stand-alone" mode they also differ in an IP mode. For example, when the ID component determines there is unwanted activity at the host and sends an alert to a simple packet filter firewall the firewall can block the associated traffic. One could argue that the firewall could compare the alerted traffic against its rule base to determine if it is legitimate traffic. But, simple packet filters typically take action based on IP address, ports, and perhaps other parts of the packet header only. This information may not be enough to actually determine if the alerted traffic is legitimate or not. For instance, traffic from a compromised host on the same network may be legitimate according to the firewall rules but may be causing unwanted actions on the host according to the ID component.

The same can be said for a stateful firewall. The rule base and state table may not have enough information to determine if alerted traffic is legitimate or not. But, a stateful firewall may be able to reduce false positives in comparison to a packet filter firewall. For example, when an ID component sends an alert to a stateful firewall, the stateful firewall can examine its state table. Since the state table maintains connection state as well as other information about the traffic it provides more insight than the simple packet filter. A stateful firewall may be able to override the ID alert and allow the traffic rather than simply blocking on the alert.

Since stateful firewalls also generally provide better traffic analysis and host protection from malicious traffic, IPS' using stateful firewalls may be more desirable.

1.2.2.3 Attack Class

SecureCore is an IPS described by Determina as a "memory firewall." It works within the context of a compiled application monitoring "basic software conventions" to verify the validity of the application while it is running. Determina claims this approach can prevent applications from harmful behavior caused by malicious code with 100% accuracy and no false positives by intercepting and blocking memory based attacks.

To accomplish this SecureCore does not use behavioral or signature based detection techniques. Instead it uses a reference set of rules or conventions called the Application Binary Interface (ABI). Rather than detecting unwanted behavior or indicators of intrusion it prevents the affects of malicious code by ensuring applications only execute in an acceptable manner defined by the ABI conventions. In essence it prevents unwanted behavior by forcing good behavior.

Additional information such as costs, manageability, and performance on general task and server hosts is needed to compare this IPS to typical IPS's. A promise of 100% accuracy with little maintenance even if initial deployment is somewhat laborious is compelling for use on critical servers and worth consideration for testing.

1.2.2.4 Additional Considerations

There is a potential drawback of IPS's that needs to be considered. Namely the accuracy of the system; how many false positives are generated and automatically acted upon thus blocking legitimate traffic? How many false negatives occur allowing attacks to pass?

These questions bring us back to the ID component. It is obviously important that ID be highly accurate. In an ideal world ID would be 100% accurate. Knowing that is not the case, how an IPS handles inaccuracies can have a significant impact on the effectiveness of the deployment and operations. IPS's that allow customization of detection and response parameters, for example, the ability to adjust signatures, types of automated responses, what to respond to and how to respond to it, to easily bypass and reinstate all automated responses, and maintain capabilities such as firewall, IDS, and anti-virus protections without automated responses activated would be desirable.

The decision to deploy host-based IPS's and what type to deploy is also dependent upon a number of other factors such as the sensitivity of the information being protected, the breadth of deployment, and the cost of implementing on each host. For example, the criticality of a server and associated information may be great enough to justify the additional cost of and the higher number of false positives behavior based systems tend to bring with expectation that unknown attacks will be prevented. The additional implementation cost associate with behavior based systems comes from the need to have "clean" hosts, the initial "training" period, and specialized configuration.

In a general setting, however, additional implementation costs and the high number of false positives when leading to automated responses may simply be unacceptable. This may be particularly true in large deployments of thousands of general task hosts.

1.3 Affect on Information Security Industry

This technology should have a positive affect on the industry given some constraints. IPS's like any other single technology does not provide a complete information security solution and should be implemented with that in mind. It is also not a new technology, with the possible exception of the SecurCore product. For sometime IDS' have been described as having automated response capabilities that include router or firewall reconfiguration or closing connections[18] So, current shortcomings of existing products remain in their IPS reincarnations. And while their integration does offer potential improvements over individually implementing the pieces in combination, IPS's may not combine the most desirable or available pieces.

A major caveat is the ability of the IDS to accurately identify unwanted activity at the host. Which is more detrimental false negatives or false positives is debatable and

certainly dependent upon a number of factors such as the type of operation in which the host is employed and the result of the false indication. Unlike active actions typically taken by an IDS such as alerting or generating logs, IPS' impact host activity by blocking network traffic or denying application execution.

False positives may have a significant impact on operations that false negatives may not. For example, a false positive triggered by network traffic may deny the user functionality on the host. However, the IPS will not react and impact the user for a false negative triggered by network traffic. And, if a layered defense includes maintaining the host in a secure fashion and maintaining patches to mitigate vulnerabilities the traffic that triggered the false negative has another layer to overcome. This layer may be enough to stop the attack thus avoiding a detrimental impact on the user.

Currently IPS's limit their automated responses to a subset of IDS alerts to minimize the impact of false positives. Additional work is needed and has been ongoing in the IDS arena for quite some time to improve ID accuracy. As ID improves the impact of IPS's will increase. But, they do provide some immediate benefits by addressing the five problems noted in section 1.1 as follows.

Reliance on IT and attacks on information systems continue to rise, with them demands on IT, in particular security, staffs increase. Security staffs need to find ways to be more productive, streamline processes, and leverage technology in support of themselves to be able to simply keep up. IPS's help staffs be more productive by streamlining processes through leveraged technology. As mentioned except for SecureCore, the underlying technology of IPS's is not new, but IPS's are an integration rather than an interaction of existing technologies. They provide coordinated and automated detection, prevention, and response capabilities. Rather than continually monitoring IDS's and taking actions based on indicators security personnel can rely on IPS's to make decisions and take actions automatically. By integrating technologies and offering automated response capabilities IPS's address problems three and four; dealing with insufficient and / or less knowledgeable staffs.

Addressing the first problem noted above, IPS' offer some consolidation of technology choices. Although it may present a different problem of choice; that is, is it more important if so how much more important is the choice of the IDS capability. And, what affect does the IDS choice have on the firewall capability. By deploying a single technology two capabilities, and the three fundamental information security needs; prevention, detection, and response, are provided, integrated, and interoperable thereby addressing the second problem. Behavior based IPS' address the fifth problem in that they may be able to prevent "zero-day" attacks thus mitigating their impact.

1.4 Affect on Security Personnel

In the long run this technology has the capability to positively impact security personnel. As discussed above, the availability of out-of-the-box integrated and interoperable complimentary technologies makes implementation and maintenance much more

manageable. Having automated response as a capability of that tool can reduce the work load on staffs perhaps reducing the number of off-hour calls / requirements.

1.5 Conclusion

Since host-based IDS's and firewalls are aimed at monitoring users inside the network, host-based IPS' may provide a valuable capability to stop insider attacks. Insiders have the potential to do the most damage and often go undetected by network-based devices.[19]

However, deployment of automated response capabilities needs to be carefully considered. If used over a small set of misuses or attacks such as with dedicated use machines, i.e., dedicated servers, host-based IPS' may be very effective. But, care must be taken with deploying automated response capabilities. The automated nature can be an effective tool for attackers to use against systems for denial of service.[16] And, risk based decisions must be made to determine if this technology is appropriate for enterprise wide host deployment. Without a well-designed and robust centralized management and implementation system a deployment on all but a small scale would likely be more burdensome than beneficial.[12]

Accuracy of these systems is getting better. But they are and should be limited in their range of automated response events according to their accuracy. They may be able to address some needs of information security staffs and have the potential to benefit information security efforts in narrowly defined roles. Host-based IPS's are another step in the right direction, a desired evolution, for existing information security products and should be considered as a component in an information security framework.

2 GIAC Enterprises Security Architecture

2.1 Background

GIAC Enterprises (GE) is a small business that supplies fortune cookie sayings to customers worldwide. It employs 50 people; 30 people at the head office in San Antonio, TX and five at each of the four international offices of Rome, Hong Kong, Sydney, and Brasilia.

After a complete top-to-bottom review of business operations and efficiency, GE management decided their current business operations needed streamlining and modernization to maximize efficiency and improve Return-on-Investment (ROI). As part of that effort management believed they needed to leverage technology as much as possible and move to an Internet based sales transaction model while maintaining a small technology staff and budget.[20]

2.2 Business Criteria

Management developed the following business criteria as a basis for evaluating solutions.

- The technical architecture shall support an easy to use e-commerce professional looking web site for customers and potential customers that also facilitates the activities of the remote sales force.
- The e-commerce application needs to:
  - provide connectivity for suppliers, business partners, and financial institutions allowing customized, manual, automated, ad hoc, and scheduled purchases, payments, and tracking,
  - provide secure interactions and transactions,
  - be relatively easy to maintain,
  - be somewhat customizable,
  - be readily interfaced with a wide variety of possible business software solutions, and
  - provide for emerging e-commerce standards.
- Minimize the training required for the migration and subsequent operations.
- Be scalable.
- Require minimal technology support staff.
- Minimize budget impact.

2.3 Solution Development

To accomplish the transition GE management hired a consultant team called "The Team", Mr. Edgar W. Hat and Ms. Business Gal, to identify applications meeting the above criteria, provide recommendations, design the architecture based on final requirements, and assist in implementation. The Team began by interviewing the staff to determine skills, preferences, and operational processes and functions, inventorying existing hardware and software, and developing a schematic of the current architecture. The following was determined.

2.3.1 Staff Skills and Preferences

The IT staff consisted of one full-time employee who was primarily skilled in Microsoft (MS) products, a Microsoft Certified Systems Engineer (MCSE) NT 4.0, with some basic knowledge of Cisco routers. One member of the financial group had as a collateral duty the maintenance of the standalone legacy financial application code named "The Beast."

Most staff members were very familiar and comfortable with MS Office products and the use of Internet Explorer and the World Wide Web. Many had MS based home systems with dial-up or broadband Internet connection. Several had web based email accounts such as MSN or Yahoo. Members of the financial group were comfortable with command line interface operations.

2.3.2 Hardware and Software Inventory

Office automation products consisted of MS Office 98. Email exchange was limited to communications to the remote offices via the legacy mail system integrated with The Beast. Desktop operating systems (OS's) were all MS Windows 98 and 95. A dial-up modem connection was used for The Beast to connect with remote offices and some business partners. Desktop and server hardware was somewhat old. The hardware

was able to support GE's current OS's but upgrades would be required for newer OS's. Business transactions and financial information storage was accomplished via The Beast.

2.3.3 Operational Processes and Functions

The staff was segregated into five groups; IT support, administrative support, financial / operations, management, and sales.

Sales and operations functions were predominately paper based. Remote offices and some larger business partners conducted transactions via dial up modem to The Beast. The rest of the transactions conducted with suppliers, customers, financial institutions, and distributors were paper based and often facilitated via telephone or fax services. Automated administrative support functions were conducted via Office 98 applications and distributed via shares over workgroups.

2.3.4 Existing Architecture

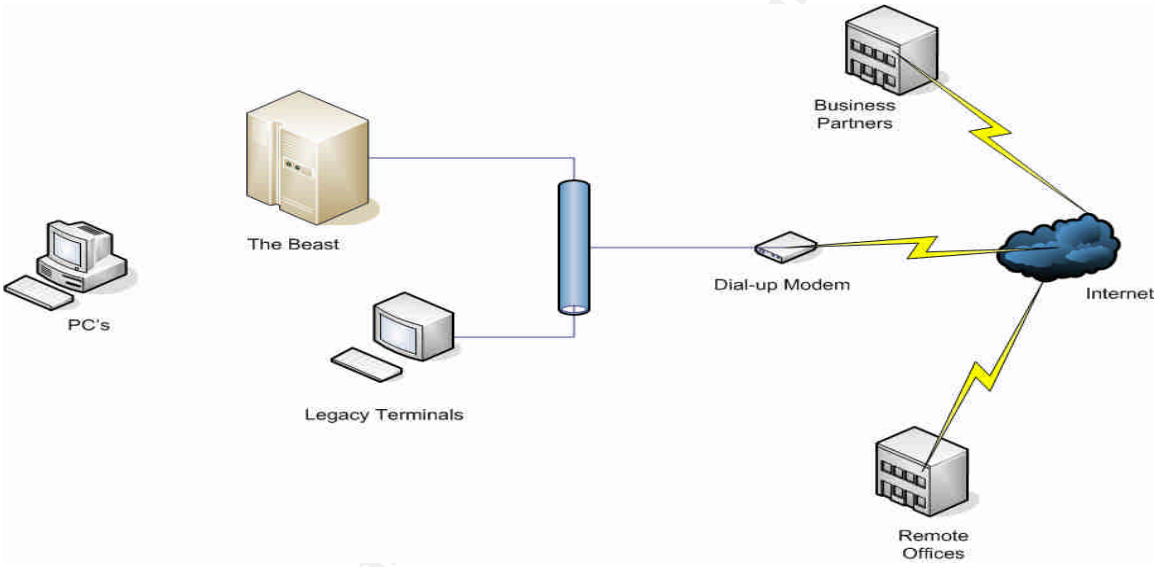

Figure 1. Existing Architecture

2.3.5 Policies and Procedures

No written information security policies, procedures, or practices were available. GE and its employees were not subject to public held company information security requirements such as Sarbanes-Oxley Act of 2002,[21] to industry specific requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[22] or to requirements for federal government entities such as the Federal Information Security Management Act of 2002 (FISMA).[23] However, they were subject to general laws concerning cyber crimes such as California's SB 1386[24] and the CAN-SPAM Act of 2003.[25] Therefore the company needed to ensure proper administrative, operational, and technical controls were in place to protect the information from unauthorized access, use, disruption, modification, or destruction and the company and employees from possible consequences of failure to do so. To address this properly The Team met

with management to develop information security policies and to develop a framework to review and modify policies as necessary.

2.4 Basic Policies

The Team facilitated discussions with management to develop pertinent information security policies. The policies were used to help design the architecture, identify controls, select solutions, and develop procedures and practices. The basic policy premises are as follows.

2.4.1 External to Internal

- Remote connections for e-commerce services shall provide authentication, confidentiality, and integrity services as necessary.
- Remote connections to GE information on internal systems, i.e., not connected to e-commerce services, shall provide authentication, confidentiality, and integrity services.
- Remote users connecting to GE information on internal systems shall only have a single Internet connection active while connected to GE internal systems.
- Sensitive GE business information shall be protected with confidentiality and integrity services when transmitted or stored outside of GE's network.
- Network communications shall be restricted to what is required for business operations.
- Interconnect agreements shall be established for all systems connecting to GE systems to provide an adequate level of information security.
- Remote machines shall conform to established policies before connecting to GE's network.

2.4.2 Internal to GE

- Business groups shall be segregated logically.
- All users shall have unique identification and authentication credentials on all systems required for job functions.
- User accountability shall be enabled.
- Limited personal use of GE resources may be allowed.
- Personal use of GE resources shall not interfere with business operations or expose GE systems to unacceptable risks.
- Only authorized software shall be downloaded and / or implemented on GE systems.
- Complex passwords with a minimum of eight characters shall be used.
- Maintenance on critical servers shall be done locally.
- Physical safeguards shall be implemented and maintained for critical resources.
- Standard hardware and software configurations shall be maintained.
- Configuration change control shall be established and followed.
- Network communications shall be limited and restricted to what is required.
- Adequate, risk-based management, operational, and technical controls shall be used to ensure the confidentiality, integrity, and availability of sensitive GE business information.

2.4.3 Internal to External

- Limited personal use of GE resources may be allowed.
- Personal use of GE resources shall not interfere with business operations or expose GE systems to unacceptable risks.
- Instant Messaging (IM) services are not authorized for business or personal use.
- Peer-to-peer file sharing is not authorized.
- Sensitive GE business information shall be protected with confidentiality and integrity services when transmitted or stored outside of GE's network.
- Only authorized software shall be downloaded and / or implemented on GE systems.
- Communications shall be restricted to what is required for business operations.

2.5 Solution Proposal

2.5.1 E-Commerce Application

A review of available products determined the following. Three options were available; commercial-off-the-shelf (COTS), managed, and build-from-scratch. The build-form-scratch option required the largest upfront commitment, was the most expensive, and required an increase in IT staff just for the maintenance. Managed solutions met most of management's criteria particularly minimizing IT staff and costs; however, most required advertisement banners. COTS solutions met most of management's criteria. But, in general, were more costly than the managed solutions and required additional IT support staff.

The COTS and managed solutions, while less expensive than the build-from-scratch option, provided; integration of business processes into the Internet based commerce model, public facing web pages for general information dissemination, individual ad hoc customer orders, long-term relation customer bulk account orders, automated scheduled purchases, a variety of payment options, and similar capabilities on the supply side.[26] They also provided for remote sales people to access business process applications. In addition to costs, this was another key management requisite.

2.5.1.1 Primary Recommendation

A COTS application was the primary recommended solution. It provided the above capabilities without the necessity for web programming capabilities on staff and provided for a robust suite of existing and emerging standards such as SOPA, UDDI, WSDL, UBL, WS-Security, WS-Reliability, WS Choreography, all the basic XML standards, all the XML security standards: Canonical XML, XML Signature, XML Encryption, XKMS, SAML, all the relevant Java J2EE standards, xCBL, UBL and UML. The solution supported a variety of payment options but the initial recommendation was to handle payments through a credit bureau.[27] In addition the solution offered file, directory, and partition encryption capabilities. This COTS e-commerce system consisted of a front-end Internet Information Server (IIS) web server, a back-end applications server, and a back-end SQL Server 2000 database.

2.5.1.2 Secondary Recommendation

The secondary recommended solution was a managed e-commerce service. The managed service provided most of the capabilities noted above to satisfy management criteria. It also had no advertisement banners and provided merchant account capabilities. This solution, however, was not as flexible in terms of emerging technologies as the COTS application recommended for the primary solution.

2.5.2 Other Software

2.5.2.1 Primary Recommendation

The primary recommended solution implemented Active Directory to provide host management and other services. It implemented Windows Server 2003 and XP Professional SP2 for OS's, split-DNS capabilities, and maintained the current Office products. It deployed Symantec enterprise anti-virus, Microsoft System Management Server for automated patching, Symantec enterprise imaging software for system maintenance and recovery, netForensics for centralized logging, and backbone hardware associated software. It also included Cisco IPSec VPN's for remote clients, Cisco (ZoneAlarm) and MS XP SP2 host firewalls, and policy enforcement via Cisco Security Agent for remote laptop users included with the recommended Intrusion Prevention System (IPS).

2.5.2.2 Secondary Recommendation

The secondary recommended solution implemented workgroups rather than Active Directory and DNS capabilities, implemented Symantec host based anti-virus and automated patching / updates, and Acronis True Image stand-alone imaging application. Logging would be accomplished at the servers only. Cisco IPSec VPN's for remote clients, Cisco (ZoneAlarm) and MS XP SP2 host firewalls, and policy enforcement via Cisco Security Agent for remote laptop users included with the recommended IPS appliance. Also, maintain the current Office products and migrate to Windows Server 2003 and XP Professional SP2 OS's.

2.5.3 Hardware

2.5.3.1 Primary Recommendation

The primary recommendation implemented standard configuration machines suitable for severs, desktops, and laptops respectively. Significant backbone hardware included a Cisco 515E IPS appliance, a Cisco Catalyst 1900 switch, and a Cisco uBR905 cable router.

2.5.3.2 Secondary Recommendation

The secondary recommendation implemented standard configuration machines suitable for desktops and laptops respectively. Significant backbone hardware included a Cisco 506E IPS appliance, a Cisco Catalyst 1900 switch, and a Cisco uBR905 cable router.

2.5.4 External to Internal Solution Sets

2.5.4.1 Primary Recommendation

The Internet based e-commerce solution would be implemented via a COTS web based technology and be maintained onsite. Interaction via the Internet between GE and their customers, suppliers, partners, their sales people, financial services, and the general public would be achieved through this COTS web based product. The COTS product would provide the front end interface to these groups providing services for authentication and SSL VPNs.

The front end would interconnect with backend application and database servers. The general public would browse information pages without logging into the system. Customers, suppliers, partners, and GE's sales people would establish accounts and authenticate via the web front end. General browsing would be accomplished over HTTP using port 80. Login and subsequent transaction and financial services would be accomplished over HTTPS using port 443.

A machine digital certificate would be implemented on the web server to provide an assurance mechanism for customers and business partners. An SSL certificate is available that uses 128-bit encryption regardless of how the client browser is configured. For example, it enables 128-bit connections for foreign client browsers that may be configured for 40 or 56-bit encryption for SSL VPN's.[28]

Remote users and satellite offices could connect via an IPSec VPN using ports > 1024 and 500. The VPN connection standard configuration would be: Encapsulating Security Payload (ESP) [3DES, HMAC SHA-1, pre-shared keys, Perfect Forward Secrecy (PFS), main mode] using tunnel mode to the IPS appliance.

DNS queries would be allowed via UPD port 53.

Maintenance on the IPS appliance would be conducted via an SSH v2 connection through the managed service.

Service	Protocol	Port
Web front end	HTTP, HTTPS (SSL / TLS)	80, 443
VPN	IP (ESP), UDP (IKE)	Proto ID 50, 500
DNS	UDP	53
IPS maintenance	TCP	22
Client connections	UPD, TCP	> 1023

2.5.4.2 Secondary Recommendation

The Internet e-commerce solution would be customized, web based and hosted and managed offsite by an e-commerce provider. Customers, suppliers, partners, and financial services would interface with GE through the web based managed solution.

GE personnel would manage the information on the managed site via a web based interface. The managed site would provide the front end interface to these groups also providing services for authentication and SSL VPNs.

Like the onsite COTS application, the front end would interconnect with backend application and database servers. The general public would browse information pages without logging into the system. Customers, suppliers, partners, and GE's sales people and other GE personnel would establish accounts and authenticate via the web front end. General browsing would be accomplished over HTTP using port 80. Login and subsequent transaction and financial services would be accomplished over HTTPS using port 443.

A machine digital certificate would be implemented on the web server to provide an assurance mechanism for customers and business partners. An SSL certificate is available that uses 128-bit encryption regardless of how the client browser is configured. For example, it enables 128-bit connections for foreign client browsers that may be configured for 40 or 56-bit encryption for SSL VPN's.

Remote users and satellite offices could connect to GE's network via an IPSec VPN using ports > 1024 and 500. The VPN connection standard configuration would be: Encapsulating Security Payload (ESP) [3DES, HMAC SHA-1, pre-shared keys, Perfect Forward Secrecy (PFS), main mode] using tunnel mode to the IPS appliance.

DNS queries would be allowed via UPD port 53.

Maintenance on the IPS appliance would be conducted via an SSH v2 connection through a managed service.

Service	Protocol	Port
VPN	IP (ESP), UDP (IKE)	Proto ID 50, 500
DNS	UDP	53
IPS maintenance	TCP	22
Client connections	UPD, TCP	> 1023

2.5.5 Internal to GE Solution Sets

2.5.5.1 Primary Recommendation

GE employees would interact via MS active directory capabilities. Connections would be established to the database, application, file, and development servers. Connections would be allowed between the web server and the application server, and the application server and database server.

Maintenance to the critical servers would be conducted at the machines. Content updates to the web server would be delivered via HTTP on port 80 from the development server only.

netForensics would be used to provide centralized logging for local servers. It would also provide automated log reduction capabilities. The service could be expanded to provide global logging and reduction capabilities for the satellite offices and network components as well. Maintenance would be conducted from the IT administration machine only.[29,30,31]

The cable router would be maintained via console port from IT administration machine only.

Service	Protocol	Port
NetBios	TCP	135, 139
NetBios	UPD	137, 139
SMB	TCP	445
Active Directory, Kerberos v5	UDP, TCP	88
LDAP	UDP, TCP	389
Global Catalog Server	TCP	3268, 3269
File transfer	HTTP	80
D B Connection (SQL)	TCP	1433
D B Connection (SQL)	UDP	1434
DNS	UDP, TCP	53
Logging (netForensics)	TCP	9011, 9012, 9065, 9073, 9076
Client connections	TCP, UDP	> 1023

2.5.5.2 Secondary Recommendation

GE employees would interact via MS workgroup capabilities. The cable router would be maintained via console port from IT administration machine only.

Service	Protocol	Port
NetBios	TCP	135, 139
NetBios	UPD	137, 139
SMB	TCP	445
IPS Maintenance	TCP	22
Client connections	TCP, UDP	> 1023

2.5.6 Internal to External Solution Sets

2.5.6.1 Primary Recommendation

A managed small business web based email service would provide email capabilities. Individual accounts with unique identifiers would be used for each employee. Employees would connect out via HTTP on a port > 1023 or HTTPS (SSL) on a port > 1023. The following security services would be provided for email: spam filtering, and

virus scanning and cleaning for incoming webmail and POP3 attachments, digital signatures, encrypted file storage, and encrypted communications.

Financial services through a credit bureau would be accomplished via HTTPS (SSL) on a port > 1023. Passive ftp would be allowed on a port > 1023. DNS would be allowed on a port > 1023. Time services are provided via Network Time Protocol (NTP) on a port > 1023. IPS events would be allowed on a port > 1023.

Service	Protocol	Port
DNS	UDP	> 1023 to 53
World Wide Web, Webmail	HTTP, HTTPS	> 1023 to 80, 443
General file transfer (PASV ftp)	TCP	> 1023 to 21
NTP	UDP	> 1023 to 123
IPS event monitoring	TCP	> 1023 to 9089

2.5.6.2 Secondary Recommendation

A managed small business web based email service would provide email capabilities. Individual accounts with unique identifiers would be used for each employee. Employees would connect out via HTTP on a port > 1023 or HTTPS (SSL) on a port > 1023. The following security services would be provided for email: spam filtering, and virus scanning and cleaning for incoming webmail and POP3 attachments, digital signatures, encrypted file storage, and encrypted communications.

The managed e-commerce would provide individual accounts with unique identifiers. Employees would connect out via HTTP on a port > 1023 or HTTPS (SSL) on a port > 1023. Financial services through a credit bureau would be accomplished via HTTPS (SSL) on a port > 1023. Passive ftp would be allowed on a port > 1023. DNS would be allowed on a port > 1023. Time services are provided via Network Time Protocol (NTP) on a port > 1023. IPS events would be allowed on a port > 1023.

Service	Protocol	Port
DNS	UDP	> 1023 to 53
World Wide Web, Webmail	HTTP, HTTPS	> 1023 to 80, 443
General file transfer (PASV ftp)	TCP	> 1023 to 21
NTP	UDP	> 1023 to 123
IPS event monitoring	TCP	> 1023 to 9089

2.6 Recommended Defense-In-Depth Components

2.6.1 Remote Operations

- Enable encryption services on laptops for sensitive business information. This would help mitigate the loss of physical protection due to remote operations and open exposure to the public. It would also help prevent loss of sensitive business information in the event a remote user's laptop was lost or stolen.
- Host Firewall
  - Primary
    - Cisco Security Agent would be used on laptops with managed service to provide host firewall, IPS, and policy enforcement to help mitigate the threat of attacks while remote users would be accessing sensitive business information through unprotected Internet connections outside the business perimeter protections. It also would provide internal protection by helping to ensure attackers would not gain access through unprotected network interconnections.
  - Secondary
    - ZoneAlarm firewall/IDS software supplied with Cisco VPN client would be used for laptops to help mitigate the threat of attacks while remote users would be accessing sensitive business information through unprotected Internet connections outside the business perimeter protections. It would also provide internal protection by helping to ensure attackers would not gain access through unprotected network interconnections.
- Laptop OS's and applications would be hardened using National Security Agency (NSA), Defense Information Systems Agency (DISA), or Computer Security Institute (CSI) standards and best practices to reduce threat and attack vectors.

2.6.2 Internal Operations

- Server OS's and applications would be hardened using NSA, DISA, or CSI standards and best practices to reduce threat and attack vectors.
- Desktop OS's and applications would be hardened using NSA, DISA, or CSI standards and best practices to reduce threat and attack vectors.
- Primary
  - Cisco Security Agent would be used on hosts with managed service to provide host firewall, IPS, and policy enforcement to help mitigate the threat of attacks while remote users would be accessing sensitive business information through unprotected Internet connections outside the business perimeter protections. It also would provide internal protection by helping to ensure attackers would not gain access through unprotected network interconnections.
- Secondary
  - XP SP2 firewall would be used on desktops to help mitigate the threat of attacks while remote users would be accessing sensitive business information through unprotected Internet connections outside the business

perimeter protections. It also would provide internal protection by helping to ensure attackers do not gain access through unprotected network interconnections.

- Cisco equipment would be hardened using NSA, DISA, and Cisco standards and best practices to reduce threat and attack vectors.
- Host Intrusion Detection System (HIDS) would be used on critical public facing server to compliment IPS appliance capabilities. The HIDS would monitor events on the server that would provide another opportunity and set of indications that can mitigate attacks.
- Enterprise anti-virus protection would be used to automatically and uniformly protect against malicious software at the host that is not prevented by network capabilities.
- Enterprise auto-patching software would be used to efficiently apply software fixes to all hosts to prevent against attacks that would not be prevented at the network layer on associated discovered vulnerabilities.
- Enterprise data recovery / imaging software would be used to efficiently recover from or protect against attacks that would not be prevented at the network layer on discovered software vulnerabilities that would not have a patch or automated remedial tool.
- Physical controls for critical servers would be used to help prevent attacks locally.

2.7 Anticipated Training

2.7.1 Primary Solution

- Active directory – operations and security
- MS XP, 2003 – operations and security
- Enterprise software
- Financial and sales operations and application interface
- E-commerce application

2.7.2 Secondary Solution

- XP operations and security stand-alone software
- Financial and sales operations and application interface

2.8 Recommended Solution Reasoning

The recommended solution may not be what would be considered a traditional architecture. But, it is suitable for a small business application.[32] A dedicated firewall for the internal LAN and separate IDS's were not used. Instead a single appliance that provided stateful firewall, IDS, and IPS capabilities was selected. This single appliance (IPS) provided the security capabilities noted on traffic flowing between all network segments while meeting management's primary concern, minimizing costs. It was acknowledged this device was a single point of failure as was the cable router. The decision to not use redundant systems was a risk management decision keeping in line with management's desire to minimize costs.

The IPS provides immediate response to known harmful network traffic as opposed to the typical delayed response associated with IDS' detect and response process. However, the IPS capability of the appliance triggers on a limited set of known signatures to minimize false positives thereby minimizing self or feature-based attacker launched denial of service. In addition it is an in-line appliance that therefore is able to immediately drop the triggering packets rather than trying to shunt them as typical separate, and some integrated, IDS and firewall interactions occur, which improves network protection with regard to these architectures.

The firewall is the Cisco Pix stateful inspection firewall that includes, in particular for this architecture, the following application and protocol inspection capabilities; HTTP, FTP, DNS, SQL, and Microsoft Networking (SMB). The Pix provides excellent firewall capabilities that are enhance by its protocol inspection capabilities. The appliance incorporates Cisco's IDS that provides alerts and packet dropping capabilities beyond the IPS function. It also provides IPSec VPN capabilities for remote access to internal file systems. Figure 5 gives a representation of remote IPSec VPN connections.

To keep costs low, the Pix stateful inspection firewall with protocol inspection capabilities was used in lieu of adding on dedicated proxy firewall capabilities for the web, database, and application servers. The use of a single appliance in this configuration provided firewall and IDS capabilities for traffic flowing between the Internet, internal LAN, database back-end segment, application back-end segment, maintenance segment, and the web interface front-end and DNS segment. The selected appliance provided these services, reduced initial and long-term costs, and provided additional IPS capabilities. The model selected provided the necessary interface capabilities as well as abundant processing capabilities to aptly handle these functions for the anticipated near and future network load.

While this device can monitor traffic flowing between network segments it cannot monitor traffic on the individual segments. To mitigate this weakness VLANs will be employed. Although VLANs have their own weaknesses the risks associated with them were determined to be less than those associated with not employing them.[33] Also, the separation of the web front end, the application server, and database server through separate interfaces on the IPS forced their interaction traffic to flow through the IPS. This and the fact that the database and application server were isolated on their own network segments mitigated the need for separate IDS's on each segment. Host IPS's (HIPS's) are recommended for these critical servers as well which further mitigates the need for NIDS on these segments.

In addition to the IPS appliance, two more network based defense-in-depth layers were incorporated into the design. Some limited network traffic filtering possible through the ISP provided the first layer. The cable router provided the second layer of network traffic filtering as well as network and port address translation. The default packet filtering capabilities of the cable router, combined with the ISP traffic filtering, provided the desired traffic screening services in the architecture. This screening was intended

to reduce undesired traffic on the network and the load on the IPS appliance. Additional stateful firewall capabilities on the router were not incorporated due to costs and increased load on the router.

HIPS's were selected for use on critical servers. This proved an additional layer of protection from network as well as host based attacks.

MS XP SP2 was selected to upgrade from current desktop OS's and for implementation on laptops. The upgrade to XP was recommended to provide required user authentication and accountability not provided by current OS's. It was also selected due to the planned reduction and eventual near term end of support for Windows 2000 as well as for the additional security capabilities of XP SP2. MS was recommended due to staff preferences, skills, and knowledge.

netForensics was selected to consolidate logs for the local servers and provide automated reduction capabilities to minimize the impact on current IT staff. It was also selected for its ease of installation and use again to minimize the impact on current IT staff. In addition, it is capable of integrating these services for network components as well as the satellite offices for future expansion.

2.9 Selected Solution

Overriding criteria for management solution selection was to keep IT costs to a minimum by maintaining minimal IT staff and minimizing maintenance and investment costs. Management chose a phased approach in an effort to implement the desired Internet e-commerce initiative balanced against costs and an opportunity to measure ROI in terms of productivity and sales. The initial phase was also considered a pilot for remote office integration into the long-term solution and upgrade.

2.9.1 Phase One

Management decided on the following for the initial phase of implementation based on reasons and defense-in-depth components discussed above as well as follow-up discussions.

- Managed e-commerce application and service
- Managed email service
- Upgrade desktop PC's hardware and implement with XP Professional SP2
  - Harden according to recommendations
  - Use firewall capabilities of XP SP2
  - Use MS auto update feature
  - Use host based antivirus
- Remote laptops with XP Professional SP2
  - Harden according to recommendations
  - Encrypt sensitive company information using MS Encrypting File System (EFS)
  - Use Cisco supplied ZoneAlarm and policy enforcement in conjunction with XP SP2 firewall

  - Use MS auto update feature
  - Use host based antivirus
- Cisco IPS – 506E
  - Harden according to recommendations
- Cisco cable router uBR905
  - Harden according to recommendations
- Cisco catalyst 1900 switch
  - Harden according to recommendations
- SMC7008ABR router

The Beast and the dial-up connection would be maintained to service remote sites and current customer connections until Phase One components were fully online, tested, and operational with the new configuration. A small router with simple filtering capabilities was recommended to add to the legacy network for improved security in the interim. An SMC7008ABR router, capable of connecting to the external dial-up modem, was selected.[34]

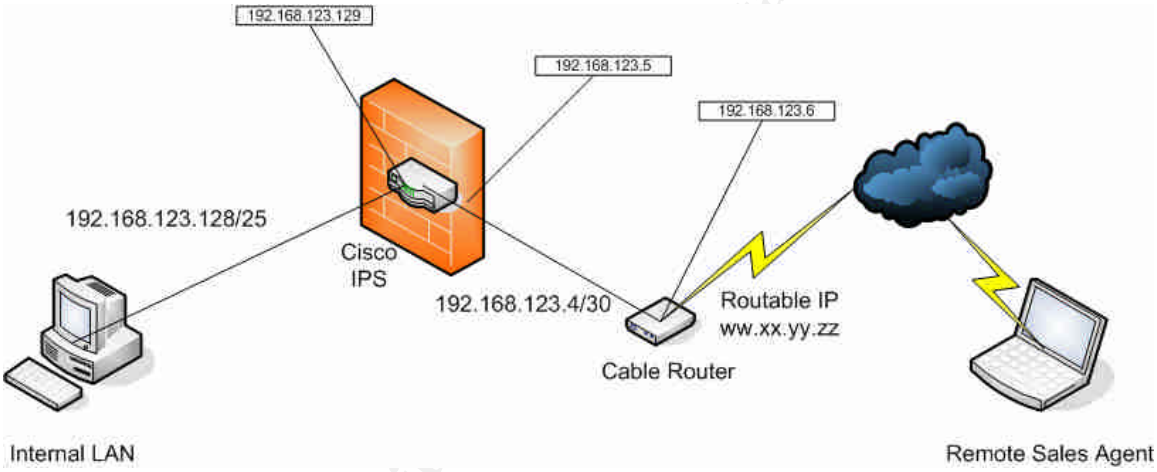

Figure 2. Phase One Architecture

2.9.1.1 Reasoning

Keeping costs to a minimum was paramount for management. To help achieve that goal managed services were selected for reasons noted and to minimize training, maintenance, and personnel costs. The managed e-commerce and e-mail services also provided 24/7 coverage which management felt was necessary. Management believed that risks associated with the loss of direct control of security functions associated with the managed services was far outweighed by the risks associated with the costs to initially provide those functions is house.

The managed e-commerce service provided a solution with all desired capabilities including security. Figure 6 gives a representation of remote or local SSL VPN connections to the e-commerce solution when hosted by GE. A similar connection is provided by the managed e-commerce service. Authorization was coordinated between GE and the managed service provider.

This managed approach gave GE management an opportunity to evaluate the move to an e-commerce solution without investing heavily in hardware, software, or personnel. Should the desired ROI and business growth be achieved then migration to phases two and three could be implemented.

An outsourced email service was selected that costs a fraction of hosting internally. The service provided flexible, reliable, business-wide email capabilities accessible from remote locations with spam filtering, virus scanning and cleaning for incoming webmail and POP3 attachments, digital signatures, encrypted file storage, and encrypted communications.[35]

While XP's EFS does not provide a complete encryption service for the hard drive, it does provide some protection for sensitive business information by encrypting file systems and folders.[36] Management determined the risks associated with the loss of information on laptops did not justify the costs of additional available COTS solutions.

The Cisco 506E was selected to provide firewall, IDS, IPS, and VPN capabilities. This model was selected to; reduce initial costs during the initial phase and concept evaluation period, better evaluate the anticipated traffic requirements of remote offices, be used at one of the remote offices should the concept prove successful, and better match the anticipated traffic handling capabilities required for the initial phase

In-house maintenance and monitoring of the IPS was selected by management due to risk and cost considerations. Management decided the risks associated with network or system compromise was low and the layered defense provided by network devices and host configurations mitigated the need to employ 24/7, on-call, or off-site maintenance and monitoring of the network for this phase. These managed services are planned for phase three when the e-commerce solution will be brought onsite.

The MS auto update feature on XP Pro hosts was selected for the initial phase for costs considerations. The auto update feature will be part of the standard configuration to mitigate the need to rely on users to conduct updates. The risks and costs associated with not testing updates was determined to be minimal compared to the risks and costs associated with not updating in a timely fashion and adding additional requirements on the current support staff.

Like the MS auto update feature, Norton's (Symantec) Antivirus 2005 host based antivirus solution, with auto update enabled, was selected for the initial phase for costs considerations and avoidance of adding additional requirements on current support staff.

The XP SP2 and ZoneAlarm hosts based firewalls provide an additional layer of protection with no additional costs other than IT staff support. Management decided these controls provided additional protection that outweighed the impact on IT staff.

The support requirements was mitigated through the use of standard configurations and Acronis' True Image 8.0 data recover and imaging tool.

The SMC7008ABR router provides NAT, filtering, and stateful packet inspection firewall capabilities.[37] In general the threat to systems connected to the Internet via dial-up connections is less than that of systems connect through "always on" broadband connections. The threat is also reduced due to the nature of the legacy system. Most, if not all, of the malicious software a business is typically concerned with does not affect the legacy OS and application. However, the residual threat has been considered and mitigated. This device should provide adequate protection on the legacy dial-up connection for the short period anticipated until the Phase One solution is operational.

2.9.2 Phase Two

- Implement Active Directory
- Implement in-house enterprise antivirus, patching, and data imaging
- Implement logging server
- Implement screened subnet with split DNS configuration
- Implement physical controls for servers
- Upgrade remote office PC's
- Implement Phase One solution at and integrate remote offices

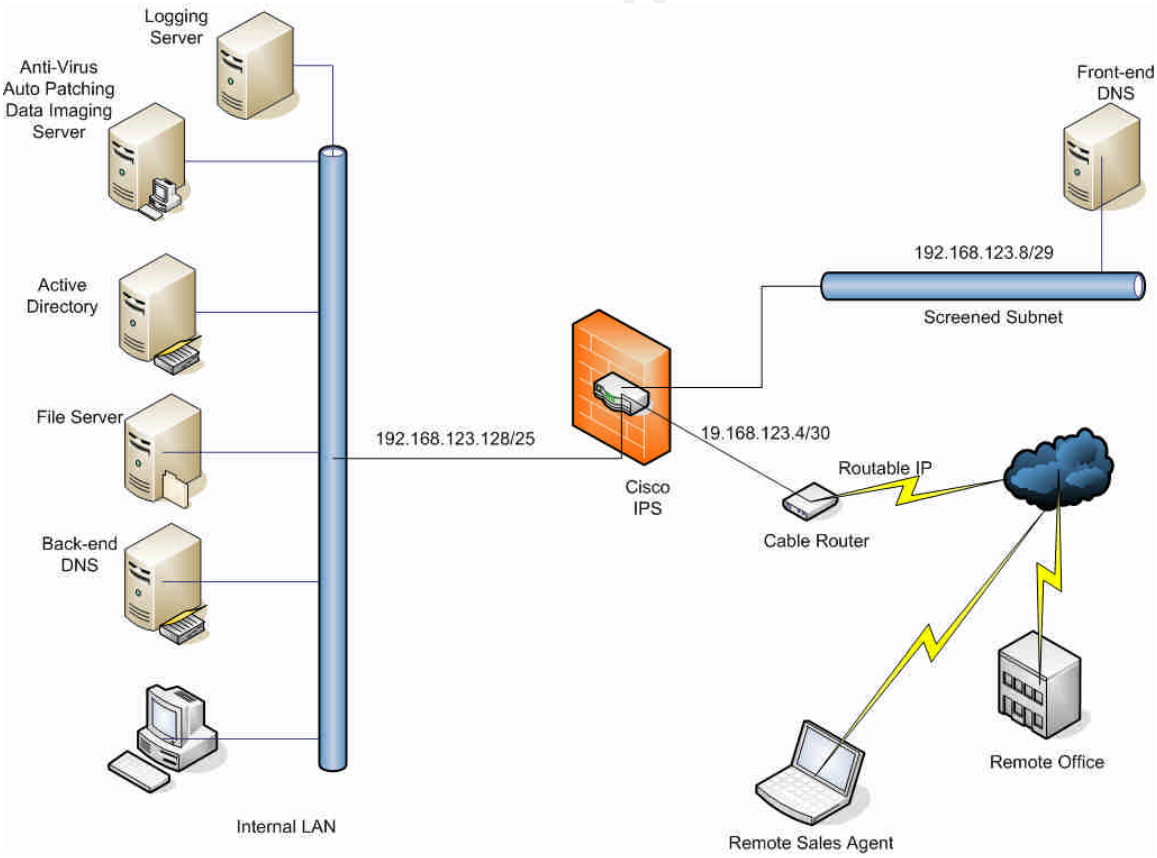

Figure 3. Phase Two Architecture

2.9.3 Phase Three

- Implement COTS e-commerce solution
  - Implement HIPS on critical servers
- Cisco catalyst 1900 switch
  - Harden according to recommendations
  - Use to provide VLANs on Screened Subnet; subnet traffic not detected by the IPS appliance
- Upgrade to Cisco IPS – 515E at home office
- Implement managed IPS maintenance and monitoring service; selected for the reasons noted above, to minimize training, maintenance, and personnel costs while providing 24/7 coverage
- Implement Cisco Security Agent on hosts with managed services
- Upgrade Rome site to serve as backup location

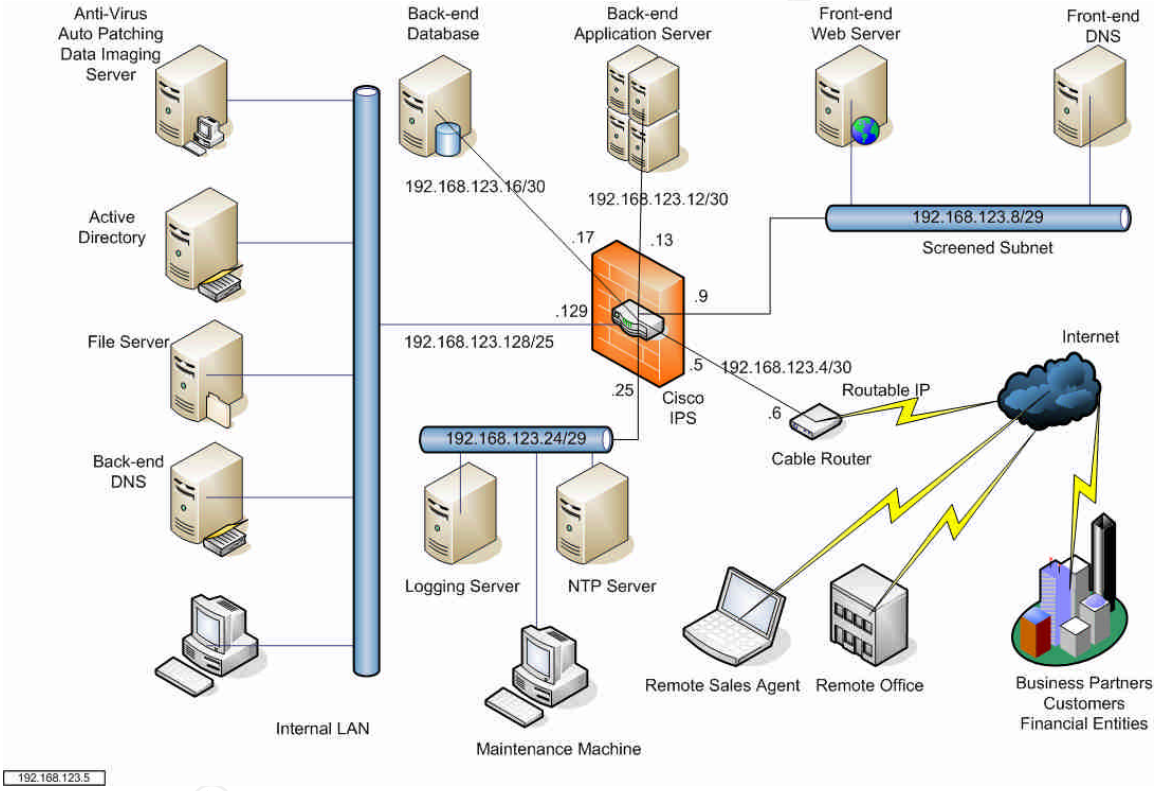

Figure 4. Phase Three Architecture

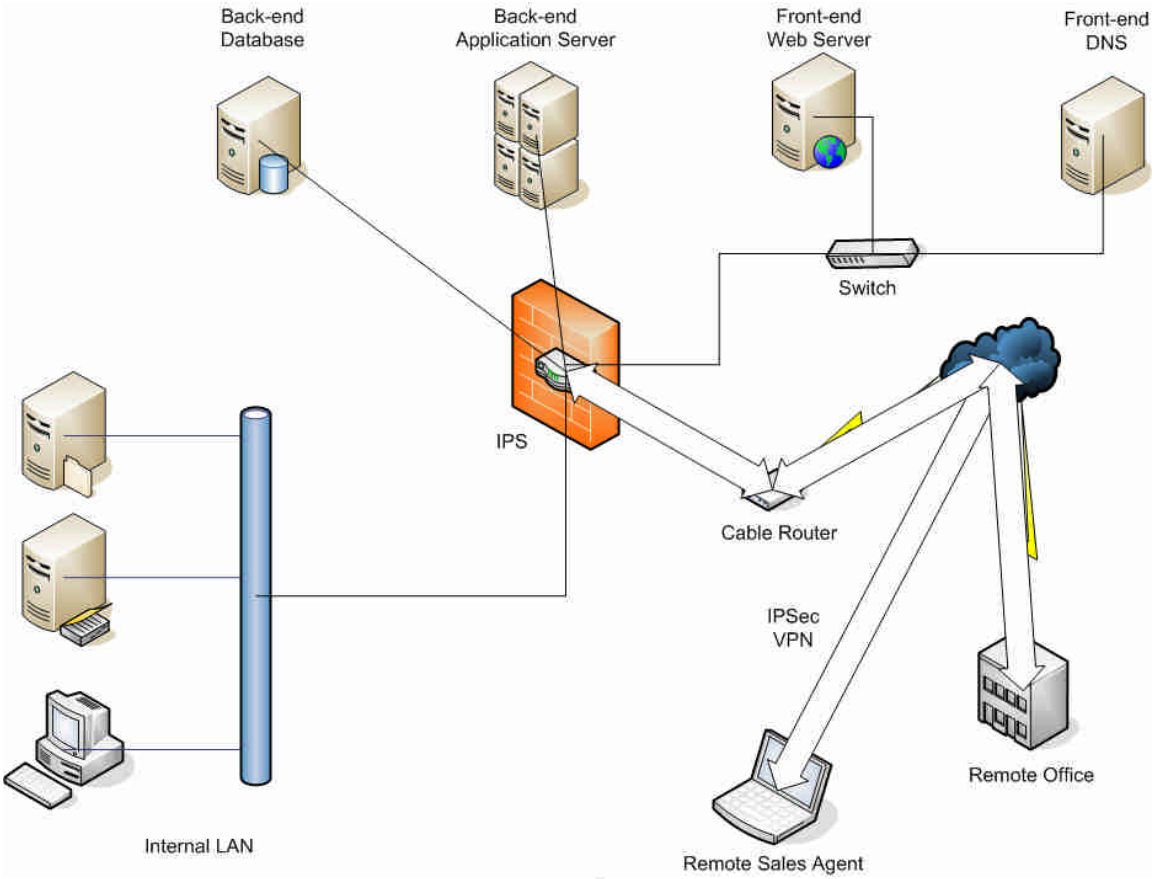

Figure 5. IPSec VPN Connection

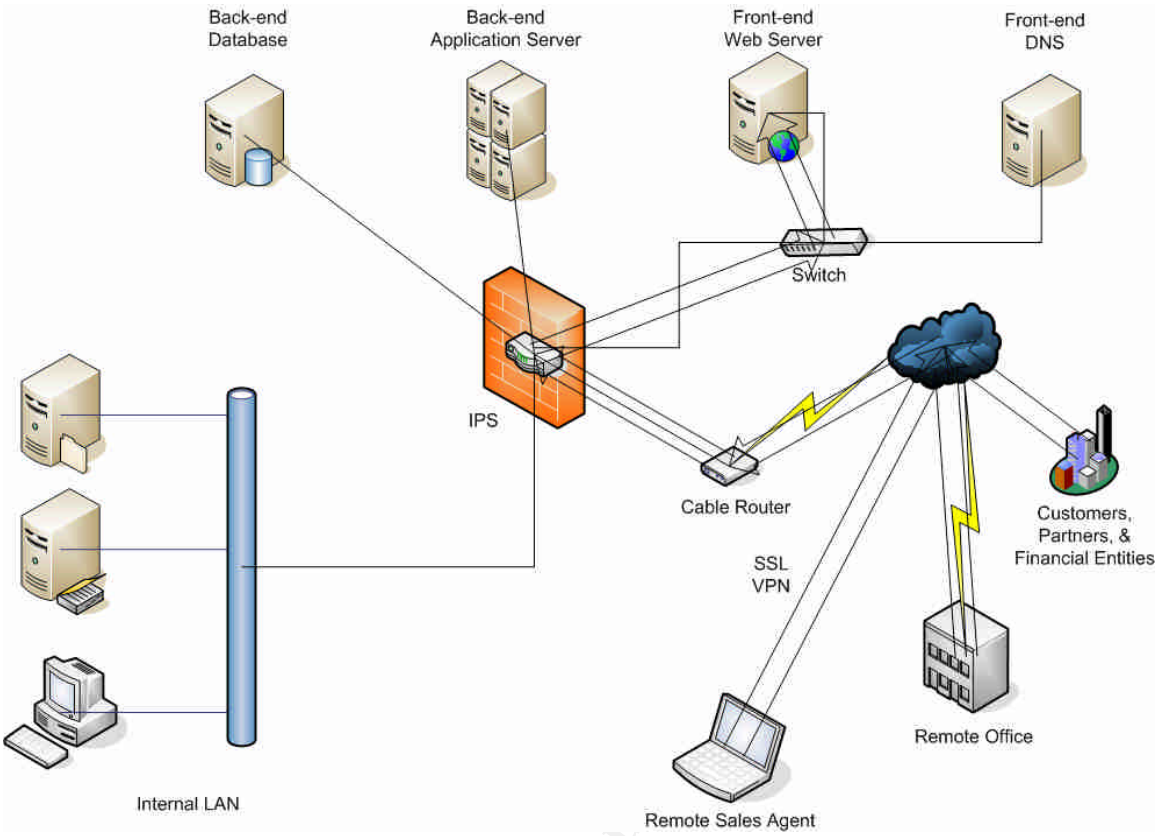

Figure 6. SSL VPN Connection

2.10 Phase One Firewall Rule Set

no fixup protocol ftp
fixup protocol http 80

Internal to external – in internal interface

permit icmp 192.168.123.128 255.255.255.128 any packet-too-big
permit udp 192.168.123.128 255.255.255.128 gt 1023 any eq 53
permit tcp 192.168.123.128 255.255.255.128 gt 1023 any eq 80
permit tcp 192.168.123.128 255.255.255.128 gt 1023 any eq 443
permit upd 192.168.123.128 255.255.255.128 gt 1023 any eq 21
permit tcp host 192.168.123.130 host 192.168.123.129 eq 22
permit tcp host 192.168.123.130 host 192.168.123.6 eq 22
deny ip any any log-input

External to Internal – in external interface

permit icmp any any packet-too-big
permit esp 192.168.123.32 255.255.255.224 host 192.168.123.5
permit udp 192.168.123.32 255.255.255.224 host 192.168.123.5 eq isakmp
deny ip any any log-input

2.11 Phase One Cable Router Configuration

Internal to External – in internal interface

```
permit tcp host 192.168.123.130 host 192.168.123.6 eq 22
deny tcp any host 192.168.123.6 eq 22
permit ip 192.168.123.128 0.0.0.255 any
deny ip any any log-input
```

Internal to External – out external interface

```
permit tcp any any eq 21 reflect packets
permit tcp any any eq 53 reflect packets
permit tcp any any eq 80 reflect packets
permit tcp any any eq 443 reflect packets
permit udp any any eq 53 reflect packets
permit icmp any any packet-too-big
```

External to Internal – in external interface

```
deny ip 10.0.0.0 0.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
deny ip host 0.0.0.0 any
permit icmp any any packet-too-big
permit esp 192.168.123.32 0.0.0.30 host 192.168.123.5
permit udp 192.168.123.32 0.0.0.30 host 192.168.123.5 eq isakmp
evaluate packets
deny ip any any log-input
```


3 GIAC Enterprises Firewall Policy

3.1 Phased Approach Selected

Overriding criteria for management solution selection was to keep IT costs to a minimum by maintaining minimal IT staff and maintenance and investment costs. Management chose a phased approach in an effort to implement the desired Internet e-commerce initiative balanced against costs and an opportunity to measure ROI in terms of productivity and sales. The initial phase was also considered a pilot for remote office integration into the long-term solution and upgrade.

3.2 Phase One Firewall Configuration

The following are the firewall rules affecting IP traffic. The overarching policy is to deny all.

Fixup commands implement the additional application inspection capabilities of the Pix firewall. The following fixup commands were specifically used.

no fixup protocol ftp –Disables FTP fixups which restricts outbound users to passive mode only and all inbound FTP is disabled.[38]
fixup protocol http 80 – Implements application inspection for http.

3.2.1 Internal to external – in internal interface

These rules restrict access to the internal IP address space to tighten the security by eliminating all other IP addresses in the *permit* statements. All other traffic is denied by default. Their order can be adjusted according to use, for instance, the ftp rule would probably be used less than the http rule.

permit icmp 192.168.123.128 255.255.255.128 any packet-too-big – "(A)llows outbound information to other routers who send acceptable return traffic, but with too large of a packet size."[39] This rule supports the security policy by allowing traffic that is required for normal operations.

permit udp 192.168.123.128 255.255.255.128 gt 1023 any eq 53 – Allows requests from the internal network to DNS servers. This rule supports the security policy by allowing traffic that is required for normal operations.

permit tcp 192.168.123.128 255.255.255.128 gt 1023 any eq 80 – This rule supports the security policy by allowing users on the internal network to browse the world wide web.

permit tcp 192.168.123.128 255.255.255.128 gt 1023 any eq 443 – This rule supports the security policy by allowing users on the internal network to browse the world wide web using SSL tunnels.

permit upd 192.168.123.128 255.255.255.128 gt 1023 any eq 21 – This rule supports the security policy by allowing users on the internal network to use any ftp server.

permit tcp host 192.168.123.130 host 192.168.123.9 eq 22 – This rule supports the security policy by allowing only the maintenance machine on the internal network to access the firewall (IPS) using SSH tunnels.

permit tcp host 192.168.123.130 host 192.168.123.6 eq 22 – This rule supports the security policy by allowing only the maintenance machine on the internal network to access the cable router using SSH tunnels.

deny ip any any log-input – This rule supports the security policy by filtering out all other traffic. This rule must come after the permit statements to allow desired traffic. It is applied last as a catch all after desired traffic. It also logs traffic that may be of interest for investigation.

3.2.2 External to Internal – in external interface

The order of these *permit* statements probably does not matter and can be adjusted according to use.

permit icmp any any packet-too-big – Allows inbound information from other routers who send acceptable return traffic, but with too large of a packet size. This rule supports the security policy by allowing traffic that is required for normal operations.

permit esp 192.168.123.32 255.255.255.224 host 192.168.123.5 – This rule supports the security policy by allowing remote laptops to connect to the IPS by IPSec tunnels.

permit udp 192.168.123.32 0.0.0.224 host 192.168.123.5 eq isakmp – This rule supports the security policy by allowing remote laptops to connect to the IPS by IPSec tunnels.

deny ip any any log-input – This rule supports the security policy by filtering out all other traffic. This rule must come after the permit statements to allow desired traffic. It is applied last as a catch all after desired traffic. It also logs traffic that may be of interest for investigation.

A. References

[1] Internet Security Systems, RealSecure Desktop, http://www.iss.net/products_services/enterprise_protection/rsdesktop/protector_desktop.php, (10 July 2004)
[2] Cisco, Cisco Security Agent, http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html, (12 July 2004)
[3] Gupta, S. D., *Open Source – Intrusion Prevention System,* White Paper, http://puzzle.dl.sourceforge.net/sourceforge/lak-ips/OpenSource-IPS-NAT.pdf, (15 July 2004)
[4] DeepNines Technologies, Slueth9, http://www.deepnines.com/corefunc.html, (15 July 2004)
[5] Internet Security Systems, Proventia Integrated Security Appliance, http://www.iss.net/products_services/enterprise_protection/proventia/m_series.php, (15 July 2004)
[6] Juniper Networks, Netscreen-IDP, http://www.juniper.net/products/intrusion/dsheet/110010.pdf, (15 July 2004)
[7] Proctor, Paul E., *Practical Intrusion Detection Handbook,* Upper Saddle River: Prentice Hall PTR, 2001, pp. 1, 78
[8] Internet Security Systems, RealSecure Desktop, *Desktop Protector User Guide Version 7.0,* Atlanta: Internet Security Systems, Inc. pg. 47, http://documents.iss.net/literature/RealSecure/RSDP-UG_70.pdf, (15 July 2004)
[9] Determina, *Introducing Memory Firewall Technology*, White Paper, http://www.determina.com/tech/overview.asp, (25 July 2004)
[10] Northcutt, Stephen, Zeltser, Lenny, Winters, Scott, Frederick, Karen K., Ritchey, Ronald W., *Inside Network Perimeter Security,* Indianapolis: New Riders Publishing, 2003, pp. 23-101
[11] Cheswick, William R., Bellovin, Steven M., Rubin, Aviel D., *Firewalls and Internet Security 2nd Ed.* Boston: Addison-Wesley, 2003, pp. 175-193
[12] Proctor, Paul E. *Practical Intrusion Detection Handbook,* Upper Saddle River: Prentice Hall PTR, 2001, pp. 32-77
[13] Tanenbaum, Andrew S., *Computer Networks 3rd Ed.,* Upper Saddle River: Prentice Hall PTR, 1996, pp. 28-30
[14] Northcutt, Stephen, Zeltser, Lenny, Winters, Scott, Frederick, Karen K., Ritchey, Ronald W., *Inside Network Perimeter Security,*. Indianapolis: New Riders Publishing, 2003, pp. 280-289
[15] Northcutt, Stephen, Zeltser, Lenny, Winters, Scott, Frederick, Karen K., Ritchey, Ronald W, *Inside Network Perimeter Security,* Indianapolis: New Riders Publishing, 2003, pp. 263-280
[16] Proctor, Paul E., *Practical Intrusion Detection Handbook,* Upper Saddle River: Prentice Hall PTR, 2001, pp. 101-127
[17] Cheswick, William R., Bellovin, Steven M., Rubin, Aviel D., *Firewalls and Internet Security 2nd Ed.,* Boston: Addison-Wesley, 2003, pp. 279-283
[18] Proctor, Paul E., *Practical Intrusion Detection Handbook,* Upper Saddle River: Prentice Hall PTR, 2001, pg. 11
[19] Peiter Mudge Zatko, *Inside The Insider Threat,* COMPUTERWORLD, June 14, 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,93757p3,00.html, (3 Aug 2004)
[20] Dai, Qizhi and Kauffman, Robert J., *Business Models for Internet-Based E-Procurement Systems And B2b Electronic Markets: An Exploratory Assessment,* Carlson School of Management University of Minnesota, Last revised: July 27, 2000, http://misrc.umn.edu/wpaper/WorkingPapers/dk_hicss2001_misrc_72700.pdf, (4 September 2004)
[21] Public Law 107–204, July 30, 2002, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf, (12 September 2004)
[22] Health Insurance Portability and Accountability Act of 1996, http://www.hhs.gov/ocr/hipaa/, (12 September 2004)
[23] Federal Information Security Management Act of 2002, http://csrc.nist.gov/policies/FISMA-final.pdf, (12 September 2004)
[24] California SB 1386, http://www.legalarchiver.org/sb1386.htm, (12 September 2004)
[25] CAN-SPAM Act of 2003, http://www.legalarchiver.org/cs.htm, (12 September 2004)
[26] E-Commerce Digest, Software Packages, http://www.ecommerce-digest.com/ecommerce-software-packages.html, (4 September 2004)
[27] E-Commerce Digest, No Merchant Account, http://www.ecommerce-digest.com/no-merchant-account.html, (4 September 2004)
[28] Thawte Digital Certificates, http://www.thawte.com/ssl/, (18 September 2004)
[29] *CiscoWorks SIMS Engine 3.1*, Release Notes, OL-4379-01, http://www.cisco.com/application/pdf/en/us/guest/products/ps5209/c1178/ccmigration_09186a008019d562.pdf, (6 November 2004)

[30] *Configuration and Maintenance Guide,* Version 3.1.1, December 2003, OL-3902-02, http://www.cisco.com/application/pdf/en/us/guest/products/ps5280/c1067/ccmigration_09186a00801f9ba4.pdf, pp. 129-131 (6 November 2004)
[31] *Understanding and Implementing netForensics*, Version 3.1, April 2003, OL-3904-01, http://www.cisco.com/application/pdf/en/us/guest/products/ps5209/c1626/ccmigration_09186a008017e180.pdf, (6 November 2004)
[32] Convery, Sean and Saville, Roland, *SAFE Extending the Security Blueprint to Small, Midsize, and Remote-User Networks*, http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8a0.shtml , (26 September 2004)
[33] Northcutt, Stephen, Zeltser, Lenny, Winters, Scott, Frederick, Karen K., Ritchey, Ronald W., *Inside Network Perimeter Security,* Indianapolis: New Riders Publishing, 2003, pp. 348-353
[34] SMC7008ABR - Barricade™ 8 Port 10/100 Mbps Broadband Router, http://www.smc.com/index.cfm?sec=Products&pg=Product-Details&prod=243&site=c, (31 October 2004)
[35] Yahoo Small Business Email Service, http://smallbusiness.yahoo.com/email/business_mail.php, (2 September 2004)
[36] Microsoft Encrypting File System, http://www.microsoft.com/windows2000/techinfo/planning/security/efssteps.asp, (15 September 2004)
[37] *SMC Networks Cable/DSL Broadband Router User Guide*, 23-28, http://www.smc.com/drivers_downloads/library/7008ABR_MNv2.pdf, (31 October 2004)
[38] Cisco, Cisco PIX Firewall and VPN Configuration Guide, Version 6.2, *Configuring Application Inspection (Fixup),* http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb727.html#wp1063623, (17 October 2004)
[39] Northcutt, Stephen, Zeltser, Lenny, Winters, Scott, Frederick, Karen K., Ritchey, Ronald W., *Inside Network Perimeter Security,* Indianapolis: New Riders Publishing, 2003, pg. 636