Global Information Assurance Certification Paper

ACME Corp
Network Security Design Study
And Recommendations

Dan Strom
10/13/2004

GSLC, version 2

Introduction

This paper discusses a sanitized real network security architecture design. Company names and identifiable information have been changed. Approval has been secured from management for this to be the subject of this GSLC paper. This is a description, within the framework of the GSLC practical assignment v2, of the points of agreement and disagreement with the existing network security architecture. All of the improvements outlined in the briefing to management have been performed.

Section 1: Executive Summary

To: Wyle E. Coyote, CEO
Subject: Proposed Network Security Changes

While the network security of our organization is generally done well, there are some deficiencies that must be addressed as we continue to conduct business. We are asking for your commitment of $5000 for capital purchases and 500 hours of time to implement these changes.

Generally speaking, the network security of Acme is done well. It supports the normal business operations, as understood by the I.T. department. Done exceptionally well are the VPN connection to Austin, the centralized anti-virus and anti-spyware solutions, the allowing of only valid traffic to pass between us and the Internet (ingress & egress filtering), protection of the corporate database server and the connection to Consolidated Industries.

However, there are some weaknesses in our network security that need to be addressed in order to minimize risk to Acme and to ensure confidentiality of data, integrity of data and availability of resources. A most basic weakness and exposure that we have is **the lack of any information security policy**. The exposure this introduces is that employee behavior, either intentional or unintentional, is the responsibility of Acme. Unless we have policy explicitly stating activities that are allowed or not allowed, we are liable for employee's actions. *Acme needs information security policies*. A second weakness is that **all of our users and servers are located on the same network segment**. The implication is that any activity on the network by one user affects all other users. Similarly, access to certain resources is only limited by authentication and permissions on the server. Acme needs to separate the Trading Group from the rest of the organization. *Acme needs the protection afforded by network segmentation*. A third weakness is that **the firewall access control rules have become loosely defined over time**. Rules currently exist where there is no business need. More access than is required is allowed. *Acme needs stringent firewall access control rules that support the information security policies*. Another weakness is that we have **no means for knowing if our networks have been entered and are being used without authorization**. Intrusion detection acts as an electronic burglar alarm. It watches for anomalous activity on the networks, notifying administrators when it is detected. *Acme needs an intrusion detection system watching the network traffic*. A fifth weakness is that **Acme users endure multiple logins to multiple systems**. At this point, we do not know what options we have to reduce the number of sign-ins or even to get to single sign-on in our organization. *Acme needs to research solutions to multiple authentication mechanisms*. Finally, the convenience of and desire for wireless networking illustrates **the need for Acme to provide secure wireless access to both the internal networks and Internet**. The existing architecture lacks any differentiation between authenticated users and non-authenticated users. *Acme needs to implement a wireless solution providing secure access to the internal corporate networks*.

The remainder of this document provides many additional supporting details.

We would be glad to discuss any questions you might have as the decision is being made.

Section 2: Technical Solution

Description of Company

Acme Corporation (Acme) was established as a membership organization to provide services to its members. These services have historically included financial/insurance services and legislative voice. The company is currently structured so that Acme has two wholly-owned subsidiaries – Acme Traders, and Acme Solutions. These companies are all headquartered in the same building, sharing the same networking resources and personnel.

Most functions of the organization support the activities of the membership. However, there are also the expected support functions such as Human Resources and Accounting. There is a group of people dedicated to lobbying the state and national lawmakers. Also there is a group dedicated to trading stocks and bonds on the domestic and international markets. Additionally, there is a small group establishing some financial instruments designed to reduce risk for the members.

Local offices exist in every county throughout the state. The office housing the legislative lobbyists is located in Austin to be physically near to the state capital.

Network Security Architecture

The current network security architecture design is illustrated in Appendix 1. Note, in particular, that the connection to Barclays is terminated directly on the production network. Also note that wireless access points are attached to the corporate network and also to the Austin network. Finally, note that intrusion detection sensors are conspicuously absent in this diagram.

Business Operations

In January 2003, insurance operations were merged with the insurance operations of another company and they are headquartered in another state. This insurance company is known as Consolidated Industries (Consolidated). Certain amounts of integration are required between the Acme membership systems and the Consolidated insurance systems. There is a connection between the networks.

The Trading Group requires real-time data transfers between Bloomburg and Barclays. Bloomburg is used primarily for market data and Barclays is used for executing trades on both domestic and international markets. This function is time-sensitive. In addition to staff executing the trades, there is an automated trading application that responds to market conditions in real-time. Because of the automated trading application, the trading staff accesses the trading pc remotely via Windows Remote Desktop across a virtual private network (VPN). Monitoring of this trading activity is critical to the business.

Virtually all of the local Acme offices are co-located with an insurance agency. These local Acme offices connect to the Internet via either a local ISP, or via the Consolidated wide area network. Local Acme offices use the Internet for accessing the corporate Acme membership applications and the Acme email system. Confidential membership information is encrypted as it passes over the public Internet.

One person in the Acme organization acts as a travel agent, making airline, hotel and transportation reservations via a reservation system through the contracted travel agency. The connection is made through a VPN and uses specialized application software.

The Austin office needs to have all of the internal network resources of the headquarters office available to them. A VPN is established between the Austin office and the headquarters office. All data is tunneled across this VPN. Files and printers are shared between users at both locations via the network servers. There are currently only 7 employees located in the Austin office.

The business requires generalized Internet access for all internal employees. This is used as a part of research and in the creation of organizational environmental positions and policies. SMTP/POP email is also used by all internal and field staff. Internal users are also given the availability of sharing their Outlook calendars on an internal server. External, non-VPN users do not have this capability.

Network Infrastructure

The Acme network is primarily Windows-based. The following servers are used internally.

Server	Description	Operating Environment
Johndeere	Domain controller acting as a file and print server	Win2K SP4
FordNewHolland	Database server	Win2K SP4
Harvestor	Accounting application server	Win2K3 Standard Edition
Helpme	Internal documentation server	Win2K SP4
Viroscanner	Development server and management applications	Win2K SP4
Combine	Web server	Win2K3 Standard Edition
Mail	Mail server	RedHat Enterprise Linux v3

The internal LAN switches are Dell PowerConnect 3248's. The corporate firewall is a NetScreen 208 running software version 4.0.1r6.0. The Austin office uses a NetScreen 5GT firewall.

The NetScreen 208 has 8x10/100Mbps Ethernet ports available. Port 1 is connected to the internal trusted networks. It's IP address is 172.27.1.10. Port 2 is connected to the DMZ network. It's IP address 172.26.1.1. Port 3 is connected to the Internet segment as IP address A.B.C.30. Port 5 is used for connecting to the Consolidated networks.

The internal networks and the DMZ are configured to use the private IP address space of 172.27.0.0/16 and 172.26.0.0/16 respectively. The Internet connection is under control of one of our business partners. They maintain the router and the ingress/egress filtering of the router.

Windows-based servers and workstations form the basis for this network. It was chosen primarily because of market share and administrator familiarity with the products. The

end-users are familiar with the user interface and the basic Microsoft Office applications.

The only non-Windows server in the network is the mail server. It is a Red Hat Enterprise Linux v3 server. It provides SMTP and POP access to email using the Postfix mail system. SMTP requires authentication to keep the server from being used as an open relay. The mail server also gives web access to email using SquirrelMail. IMAP access is allowed for internal users only.

Two Macintosh G4 workstations exist on the network, also. They run OS X 10.3.5.

The Windows workstations are all configured to download critical updates automatically. Installation of these critical updates is dependent upon the user installing them. The Windows servers are also configured for the automatic download of critical updates. Installation of the updates on the servers is performed every Monday and Thursday morning prior to the beginning of the arrival of the office staff.

The FordNewHolland database server is used solely for database activity. It runs Windows2000 Service Pack 4 and MySQL v.4.1.

The Harvestor application server is used for the accounting functions of the company. It runs Windows 2003 Standard Edition.

The Combine web server runs Windows 2003 Standard Edition. It is used for all web applications that are to be accessed from the Internet. This includes the expected corporate presence web site and also the Membership Application. The Membership Application is written in Java and is accessed via the web browser. It passes information to the FordNewHolland database server and executes queries against the data on FordNewHolland.

All servers are backed up using the Veritas backup systems on a VXA tape library. The agents to copy open files are running on each of the servers.

The centrally-managed Symantec Anti-Virus v8.1 application is installed on each Windows workstation and Windows server. Updates to the application and virus definition file are pushed out daily, if needed. The centrally-managed Webroot Spysweeper is also installed on each Windows workstation and server. Updates are pushed out daily, if needed. Spysweeper is scheduled to execute a sweep of the workstation each day at noon.

DNS for the internal network is served as a part of the Active Directory controller on JohnDeere. It defers to the external authoritative DNS server for external names. External DNS is hosted by Network Solutions.

Access Requirements and Restrictions

The following access permissions and restrictions are configured on the NetScreen 208 firewall for the network. The permissions and restrictions of individual users on each server are intentionally omitted from this work. Also intentionally omitted is any discussion concerning OS hardening on any of the servers or workstations.

External to DMZ

General public	The general public needs to access the www.acme.org web server to gather news and policy development information	
Any	A.B.C.20 – VIP to 172.26.1.10 (web server)	http (tcp 80) http (tcp 8080)
Acme Offices and traveling staff	This group needs access to the www.acme.org web server for the Membership Application and to the email server. The email server also hosts a web interface to mail.	
Any	A.B.C.20 – VIP to 172.26.1.10 (web server)	http (tcp 80) http (tcp 8080)
	A.B.C.22 – VIP to 172.26.1.11 (mail server)	http (tcp 80) smtp (tcp 25) pop3 (tcp 110)

DMZ to External

DMZ servers	Servers in the DMZ need general Internet access	
172.26.x.y/16	Any	Any

External to Internal via VPN (bi-directional)

Austin Office	Users in the Austin office need access to all of the LAN resources in the headquarters office.	
172.22.215.0/24	A.B.C.30 – VPN to 172.27.x.y/16	Any protocols
Dial-Up VPN Users	These users are corporate users connecting to the LAN resources in the Headquarters office.	
Any	A.B.C.30 – VPN to 172.27.x.y/16	Any protocols

Internal to External

Internal Users	Users in the headquarters office need general Internet access	
172.27.0.0/16	Any	Any protocols
Internal Users	Users in the headquarters offices needing access to the old airline reservation system	
172.27.0.0.16	Any	PPTP – tcp 1723
Reservation clerk	The user in the headquarters needing access to the primary airline reservation system	
172.27.4.22	Any	IPSec • IP 50 • IP 51 • UDP 500

Internal to DMZ

Internal Users	Internal users need to access servers contained in the DMZ area	
172.27.0.0/16	Any	Any

DMZ to Internal

DMZ Servers	One of the servers in the DMZ needs specialized access to a database server on the Internal network	
172.26.1.10	172.27.3.7	ftp (tcp 20, 21) MySQL (tcp 3306)

Internal to Consolidated

Internal Servers	These servers need to transfer files to servers with Consolidated	
172.27.0.0/16	172.16.12.14 172.16.12.18 192.168.202.1	ftp (tcp 20, 21)
Internal Users	Many internal users continue to need access to the Consolidated mainframe	
172.27.0.0/16	172.16.1.111	http (tcp 80)
	172.16.1.10	telnet (tcp 23)

Section 3: Agreement

The aspects of the previously described security design that are well done are discussed below. An attempt is made to balance the business requirements with the security specifications. This list is not exhaustive.

VPN connection to/from Austin

The connection between the headquarters office and the Austin office utilizes an IPSec VPN. ESP (for confidentiality) and AH (for non-repudiation) are both a part of the tunnel negotiation. All traffic at the Austin site that is destined for any network other than the 172.22.215.0/24 network is sent through the tunnel to the headquarters office. Split tunneling is not allowed. The Austin network is effectively an extension of the networks in the headquarters office.

Internet service at the Austin office is via a 1.5M synchronous DSL circuit provided by SBC. The SLA (service level agreement) from SBC allows for the use of VPN protocols. Traffic logs show that this circuit rarely is used at more that 10% of capacity.

As mentioned earlier, there are only 7 employees located in the Austin office. There are plans to increase this staffing to 9 at the most over the next 3 years. Taking into account the usage of the VPN connection and the response times across the VPN, scaling up to 9 users will not present a problem.

The VPN is a cost-effective solution to the requirement of extending the work environment[1]. A firewall with VPN capabilities is installed at the Austin office. It had a purchase cost of $1200. A private T1 line between locations is $1900/month while the DSL circuit with this bandwidth is only $170/month. Acme would not be able to afford this connectivity without the VPN solution.

[1] Bird, p. 99ff.

Centralized AntiVirus and Anti-Spyware

A centrally managed Symantec corporate anti-virus server is deployed in the headquarters office. All workstations located in the headquarters and Austin offices are configured to pull antivirus updates from this server. The workstations report back to the server of any virus that is found on the workstation.

Similarly, the Webroot corporate SpySweeper server is deployed in the headquarters office. All workstations located in the headquarters and Austin offices are configured to pull SpySweeper updates from this server. The workstations report back to the server of any spyware that are found on the workstation.

The benefits of centrally manages systems is well known. It eases the burden on the network administrators. This is especially important when the number of support staff is small. We have only 2 network administrative staff and they are often very busy. When a virus outbreak occurs, there is not enough time in the day for these staff to visit every workstation. Therefore, the centrally managed solution simplifies the work and saves real dollars. It also gives the users the assurance that even if they don't see a person at their desk fixing the virus problem, it **is** being fixed.

Spyware gets installed on users workstations amazingly frequently. SpySweeper is scheduled to do a complete system scan daily on each workstation. Since this was started in June, 2004, the support calls related to system performance degradation due to spyware have dropped significantly. Whereas formerly we averaged 8 spyware incidents per week, we now deal directly with .5 incidents per week. This has freed the administrators to concentrate on other work.

Some of the users have complained about the SpySweeper scan occurring each day on their workstation. We have helped them become more accepting by showing them that the short amount of time required for the scan is small in comparison to the time lost in dealing with the sypware application.

Ingress/Egress Filtering

Ingress filtering and egress filtering are used as a first level determination of what is allowed in and what is allowed out of the protected network from any other network that is connected. It is implemented both in the Internet router and the Internet firewall.

Filtering is necessary both to protect the internal networks and to protect the Internet. It keeps illegitimate traffic from entering or leaving the internal networks. Only in-bound traffic from routable, unicast ip addresses that are destined to addresses/ports that are used are allowed through. Egress filtering keeps a compromised system on the internal networks from launching attacks against other hosts on the Internet.[2]

There are no additional costs associated with implementing ingress and egress filtering. The Internet router and firewall are required portions of the infrastructure. The implementation of filtering is simply a configuration change on both.

[2] Brenton

The router and firewall are sufficiently sized so as to be able to handle several times the number of current connections.

Protection of Database Server

The database server contains the membership information for the organization. It is vitally important that this information be protected from unauthorized access. The web server sits in the DMZ area and needs to access and update information that is stored on the database server. The database server resides on the protected internal network. Access from the DMZ to the database server is limited by the firewall and only allows access on the MySQL ports from the web server. Access is not allowed directly from the Internet to the database server. The Windows operating system is hardened and the configuration is periodically checked to verify the continued correct configuration.

Veritas does not have a MySQL-specific agent for backing up the MySQL tables. Each night, the database tables are dumped to produce a flat file that can be backed up using the tape library system.

Although Acme is not subject to GLB or HIPAA, it is important that membership data not be leaked. Personal data that is stored on the database server must be protected. The reputation and integrity of the organization is at stake. The measures that have been taken to secure the data at rest on the server are sufficient and use previously acquired hardware and software.

Connection to Consolidated Industries

The connection to the Consolidated networks is accomplished by a double-firewalled Ethernet connection. The Consolidated networks and the Acme networks both reside in the same physical facility, yet are owned and controlled by two distinct companies. Each company controls a firewall on their end of the connection. Thus, anytime there is a requirement for hosts and/or protocols to reach the other network, it must be expressly permitted by each company. However, because we are business partners, there is a certain level of implied trust.

Practically speaking, the firewalls controlling access are in equipment racks that sit beside each other. A simple Ethernet patch cord is connected from one equipment rack to the other. Data moving between the networks is less than 500 MB per day. The data transfer speeds are capable of 100 Mbps. There are no plans to significantly change the amount of data that is transferred each day. However, if there were, this connection would easily handle 10-times the amount of data. This solution scales well.

The only significant issue with this connection is the difficulty in making changes. Consolidated has a strict change management policy that requires approval by a committee. This committee meets twice per week. They must approve any changes that are required for this connection. Acme, likewise, has change management policy. Changes must be approved by a manager. This is very flexible. Occasionally, problems have arisen requiring an immediate change. This is delayed until the next meeting of the

Consolidated change management committee. This is the only significant issue with the connection.

Section 4: Disagreement

Just as there are portions of the network security design that were done well, there are some aspects that are not done so well.

Loose firewall rules

The first aspect of the network security design that should be improved is that of the firewall rules. Several of the rules allow access that is not required for the business and that may be completely inappropriate. They should **all** be reviewed for applicability.

As an example, there is one rule for the “DMZ to External” controls. It allows any host on the DMZ to access any Internet host using any protocol. This is *much* more than is required. In actuality, the only access that is needed is http, https, and dns query. This rule should reflect the actual needs.

Other examples occur in the “Internal to External” controls listing. The first rule is to allow any internal user to access any Internet host using any protocol. A well-known listing of the actual required protocols for conducting business is available. This rule allows access using protocols that are not necessary, nor recommended, to access the Internet. This rule should reflect the actual needs.

Another “Internal to External” rule specifically allows any internal host to access any Internet host on tcp port 1723. There is no current business requirement for this rule.

Good security practice dictates that only access that is required is allowed. However, at this point in time, several users are using protocols that are not required for the business. Streaming audio and video have been used for personal enjoyment for quite some time. If this is to be limited, buy-in from the executives must be acquired. The firewall access control lists should be reviewed and made more restrictive.

Intrusion Detection/Prevention

The next aspect of the network security design that should be improved is that of intrusion detection and prevention. Currently there is no intrusion detection or prevention built into the network.

The problem introduced is that there is no knowledge or understanding of what is actually happening on the network. The network perimeter could have been violated and there would no awareness of that.

Just as a burglar alarm in a building has no impact on legitimate occupants, so the implementation of network intrusion detection would have no apparent impact on the users. It has not been implemented due to time and staffing constraints, but in order to adequately protect the organization, it must be determined how to do this.

The cost justification and ROI analysis for the implementation of intrusion detection and protection must take into account the cost of a security breach and the resultant loss of

data. IDS has traditionally been viewed in the same light as a building burglar alarm. The expense is simply a cost of doing business. Likewise, at Acme the expense of the IDS should be viewed as a cost of doing business.

Intrusion detection should be implemented both on the network and each server.

Wireless Architecture

Another portion of the network security design that ought to be improved is the wireless networking architecture. As with many organizations, wireless networking has crept into the Acme networks without thorough consideration as to the implications of the technology and how to secure it.

The 802.11b/g access points that we use are configured similarly. They reside on the internal network. The SSID broadcast is disabled. The connection is 128-bit encrypted. Thus anyone wanting to connect to the internal network wirelessly needs to know the SSID and the WEP key. However, the weaknesses of WEP are well documented[3].

Since wireless access points have appeared in the network architecture, they have become a regular and expected service. Many staff use laptop computers with wireless technologies built in. It is common practice to take the wireless laptop to meetings and continue to have access to the expected network resources.

This is an example of where the business needs must be weighed against the security implications of that need. The business need for wireless networking has grown. The convenience is a big part of this requirement.

Secure wireless network access should be a priority for the organization. An informal risk analysis has been performed and the risk of an insecure wireless architecture is unacceptable. The solution should allow for growth in the number of wirelessly connected devices up to 150 hosts at any time.

Network Segmentation

The Trading Group is an important part of our business operations. It handles financial transactions that our organization depends on. Connections facilitating the real-time trades are made to partner organizations throughout the day and night. However, the connection to one of the partners is made directly on the internal network.

Although the partner, Barclays, is a trusted partner, this is not good practice. The Barclays router terminates directly on the network that is used for all of the other business operations. There is risk both to Barclays and Acme with this connection. The access rules are implemented on the Barclays router by Barclays staff. We are dependant upon them for limiting access to our network and for limiting our access to their resources. The Trading Group also implements real-time computerized trading. These servers conducting the trading reside on the general internal networks and are subject to events that occur on the general network.

The architecture of the connection to Barclays and the fact that the Trading Group is not segmented on the networks should be reconsidered.

[3] Borisov

Divergent Authentication Mechanisms

Windows Active Directory is used as the primary authentication mechanism within the organization. However there are systems that are not configured to authenticate against Active Directory. This results in administrative overhead and introduces opportunity for configuration mistakes.

Authentication of the VPN that is used for the Trading Group is performed by an internal database on the VPN terminating firewall. The VPN firewall *does* have the capability to check Active Directory for the user/password for access.

The Linux server hosting the email application performs electronic mail authentication. It does have the capability of checking Active Directory for authentication information.

Various applications that are in use within the organization also perform their own authentication. One web application that is particularly important requires user authentication into the application. The userid/password database is stored on the MySQL database server. The login objects for this application have been written in-house.

The desired end-result is to minimize the number of login credentials that a user has to remember and to simplify system administration. Where appropriate, all authentications should be based on Active Directory.

Information Security Policy

Although not strictly a part of the network security design, a significant point of disagreement with the existing architecture is policy. There is no formal, written information security policy for the organization.

The absence of written information security policy introduces several exposures to the organization. There is no basis for limiting activities on the networks. There are no boundaries defining where abuse starts. Employees do not know whether their desired activity is allowed or not. Policies set the expectations of behavior in the organization.[4]

Information security policy should be developed and approved by top-level management for the organization.

[4] Canavan, p3.

Section 5: Improvements Briefing to Management

Current State

The current network security architecture came about as the result of needing to quickly build a network to conduct business. It has been in place for 20 months. During that time, some improvements have occurred and enhancements have been implemented. In general the network we have is robust and secure. However there are some important deficiencies that must be addressed. The final go-ahead for changes must come from upper management. It is hoped that management will be convinced by this presentation.

Early on, it became evident that we needed to extend access to the computing resources to the Austin office. A virtual private network (VPN) was implemented using the public Internet as a transport for the private connection between our offices. This VPN follows industry best-practices for the configuration. This was done very well. The implementation of the VPN has a monthly cost of $75 for the DSL Internet connection in Austin, as compared with the previously installed private T1 costing $1700 per month.

Our business, like many others, is dependant upon a steady and reliable connection to the Internet. This requires that we protect ourselves from Internet-based attacks, and that we act as good citizens. Ingress and egress filtering of Internet traffic is a component of this.

Another part of a good defense is protection against viruses and spyware. Licenses for the Symantec corporate centrally-managed anti-virus software were purchased. The software was pushed to every workstation and server. The WebRoot SpySeeper centrally-managed spyware detection and removal system was installed. The SpySweeper client was pushed to every workstation and a scan is executed each day between 11:00am and 1:00pm. This combination of Symantec Anti-Virus and SpySweeper has reduced the number of support calls by 93%. This is a *huge* savings!

Protection of the corporate data is of utmost importance. We have taken appropriate steps to make sure that the membership data that is stored on the MySQL server is protected. The server is well configured. Tape backups of the data occur nightly. The backup tapes are tested regularly for the ability to recover the database.

The connection between Acme and Consolidated has been made very well. While very simple, it also is robust. This connection is necessary to the ongoing business, but was able to be established at no additional cost to Acme.

Weakness Overview

There are six significant areas in which we need to make some necessary improvements. The first of these is the configuration of the perimeter firewall rule sets. They include rules that are no longer needed, rules that allow unnecessary computers and protocols to pass, and rules that we are not sure why they are included.

We have no means for knowing whether our networks have been compromised. We think that we are secure, but we really don't know. Network intrusion detection acts as

an alarm when certain traffic thresholds are exceeded. Normally this would indicate compromise.

Wireless network access onto our internal networks is not secure. The wireless networks were installed to meet some very specific requirements and were intended to be installed for only a limited amount of time. The usefulness of wireless networking, however, has taken hold. The equipment and configurations we are currently using are very susceptible to compromise. In fact, someone with a laptop can be in the parking lot and wirelessly access the internal networks without any sort of authentication!

The segmentation, or separation, of the workgroups on the network is non-existent. Sensitive data is created within the Trading Group. The router giving a connection to Barclays is connected directly onto the internal networks. The Trading Group has reliability requirements that differ from the remainder of the organization. It is not wise to connect a partner network directly to the internal networks without some sort of perimeter protection.

Users within our organization are required to know several different login/password combinations to conduct their work. Network, email, web server and applications all require different passwords. Not only does this generate support calls, but it increases the likelihood that users will create simple passwords and write them down at their desk.

Our organization does not have any formal information security policy. It has been shown that this could put us in a legal bind with respect to employee behavior at the workplace. This needs to be addressed.

Proposed Changes

Security Policy

The first change that must be done is the creation and adoption of a corporate information security policy. The policy will be defined through meetings with the executives and division directors. The objective here is to define what is acceptable and expected. Additionally, services that are unacceptable should be defined. Once draft policies are defined, then they will be reviewed by the Chief Executive Officer for his agreement. Following sign-off by the CEO, the policies will be disseminated to the employees and will be used as the basis for network and computer configurations, and usage of company-owned computer and technology resources.

The cost of developing these policies is time-only.

Project Lead	60 hrs @ $45/hr	$2,700
Division Directors (6)	15 hrs each @ $60/hr	$5,400
CEO	5 hrs @ $120/hr	$600
TOTAL		**$8,700**

The policies should be viewed as a necessary first step in improving the network security architecture of the organization. Annual and on-demand review of the policies should be done.

Segmentation

Segmentation of the network must be addressed. The proposed network security architecture is presented in Appendix 2. The Trading Group should be given their own subnet, and virtual LANs (VLAN) should be implemented in the network. The VLANs are in preparation for the wireless architecture modifications. This will give the immediate benefit of separating the trading network traffic from the general corporate traffic.

Costs of this segmentation are as follows:

VLAN configuration	8 hrs @ $45/hr	$360
Firewall purchase		$1,000
Bloomburg re-configuration	8 hrs @ $45/hr	$360
Firewall installation	12 hrs @ $45/hr	$540
Ruleset modification	8 hrs @ $45/hr	$360
TOTAL		**$2,620**

The Trading Group will use the Cox internet connection. This currently costs $230/month, but is included in a different budget.

Segmentation of the Trading Group provides benefit to the entire organization by (1) restricting trading network access to only authorized trading personnel, (2) keeping sensitive financial information off the general business network, (3) providing a redundant internet connection, and (4) integrating into the new wireless network architecture.

Firewall Rules

The organization needs to commit the time to review and modify the access control rules that are in the perimeter firewalls. Access rules necessary for the on-going business of the organization should be accurately reflected in the firewall rules. This should be done immediately upon completion of the development and adoption of the security policies. The improved rule set should encapsulate the requirements as defined in the security policies. The firewall rule set is a means for the application of the adopted security policy.

The cost for the improvement of the firewall rules is time-only.

Project Lead	40 hrs @ $45/hr	$1,800
TOTAL		**$1,800**

The benefit to the organization is that we now know that appropriate access to the Internet is applies consistently across the company. Also, we now have a control point for the security policies.

Intrusion Detection

Both network and host intrusion detection should be implemented. A network intrusion detection system (N-IDS) watches the packets on the wire and a host intrusion detection system (H-IDS) watches the actual server for signs of compromise. These are analogous to burglar alarms and security systems in the corporate environment.

Implementation of IDS can be done concurrently to the network segmentation portion of the project. Initially, only N-IDS will be implemented. Research is required to determine the impact on the business applications prior to implementing H-IDS on the servers.

The N-IDS should be implemented with Snort. The primary advantages are that (1) it is open-source, (2) there is wide-spread usage of Snort, (3) it is low-cost, and (4) we already have expertise in Snort.

A minimal implementation of Snort requires that sensors be deployed on the internal network immediately inside the firewall and on the DMZ. This implies that we need to have a Linux host at each of these locations to gather traffic information and a Linux server on a management network to process the information and issue alerts.

The costs associated with implementing the Snort N-IDS are as follows:

Snort sensor hosts	2 @ $700	$1,400
Snort console	1 @ $1200	$1,200
Hubs	3 @ $200	$600
Installation and Configuration	80 hrs @ $45/hr	$3,600
TOTAL		**$6,800**

The costs associated with the H-IDS impact research follows:

Evaluate critical applications	30 hrs @ $45/hr	$1,350
Research H-IDS products	40 hrs @ $45/hr	$1,800
Implementation Recommendation	10 hrs @ $45/hr	$450
TOTAL		**$3,600**

A single incident of compromise can easily cost the organization upwards of $15,000 in lost productivity and availability. The cost of lost business is much more difficult to quantify. However lost trust may never be recovered.

Authentication

Multiple network and application authentication mechanisms are costly to maintain. They are also a source of weak credentials which can lead to a more easily compromised network. Various authentication mechanisms in use need to be reviewed and recommendations made to simplify the process for users.

Much of the time required will be spent in research to make the determination of how to proceed.

Research implemented authentication methods	50 hrs @ $45/hr	$2.250
Integration Analysis	20 hrs @ $45/hr	$900
Recommendations	20 hrs @ $45/hr	$900

Report		
TOTAL		**$4,050**

When the report detailing recommendations for authentication is complete, a decision will be made as to whether to pursue implementing centralized user authentication and authorization for the various systems and applications within our organization. The cost for implementing this cannot be determined at this point because there are too many unknowns that should be uncovered during the Integration Analysis portion of the research.

Wireless

Improvements must be made to the wireless infrastructure in the organization. This will build upon the work that is to be performed in the segmentation portion of these recommendations.

The wireless infrastructure needs to be re-designed to allow authenticated access to the internal networks and unauthenticated access to the Internet. This will be accomplished by having two wireless networks. At this point it is the most cost-effective solution to us. When budget time rolls around next year, we will be presenting a more robust solution to the problem

The costs associated with the implementation of this follow:

Access point – Restricted zone	2 @ $200	$400
Access point – Unrestricted zone	2 @ $200	$400
VLAN configuration	15 hrs @ $45/hr	$675
TOTAL		**$1,475**

The benefit is that risk is reduced for a relatively low cost.

Section 6: Conclusion

What has been presented in the paper is a description of the network security environment at Acme, Corp, a discussion of the strengths and weaknesses of that environment and a briefing to management outlining the necessary improvements.

The improvements presented to management, while not exhaustive, are a necessary starting place to improving the network security of the organization. These recommendations have been thoroughly considered and ought to be done.

References

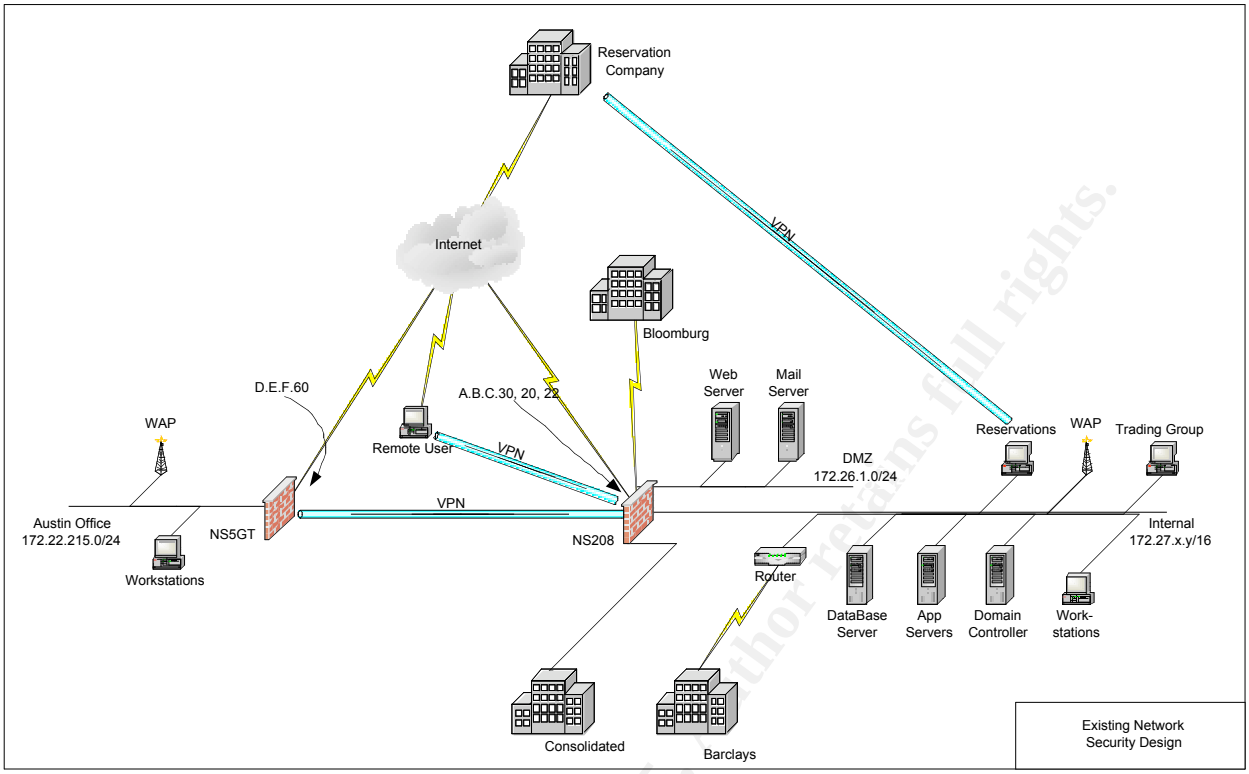
Bird, Christina, “An Introduction to Secure Remote Access.” Published in Information Security Management Handbook, 4th Edition. Tipton and Krause, ed. 2001.

Brenton, Chris. “Whatis Egress Filtering and How Can I Implement It?” Feb. 29, 2000. URL: http://www.sans.org/rr/papers/index.php?id=1059 (October 13, 2004).

Borisov, Nikita, Goldgerg, Ian, Wagner, David. “Security of the WEP algorithm.” Date unknown. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html. (October 13, 2004).

Canavan, Sorcha. “An Intformation Security Policy Development Guide for Large Companies.” Nov 18, 2003. URL: http://www.sans.org/rr/papers/index.php?id=1331. (October 13, 2004).

Appendix 1: Existing Network Security Architectural Design



Appendix 2: Improved Network Security Architectural Design