Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Systems Security Architecture A Novel Approach to Layered Protection

The purpose of this paper is to demonstrate how to develop an information systems security architecture in a complex environment with few security measures in place. The case study illustrated will provide the reader with a set of guidelines that can be used to develop security architecture components that allow for scalable and secure IT infrastructure.

Copyright SANS Institute
Author Retains Full Rights

AD

Information Systems Security Architecture

A Novel Approach to Layered Protection
A Case Study

GSEC Practical Version 1.4b

By: George Farah

© SANS Institute 2005, Author retains full rights.

SANS Institute

September 9, 2004

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract ……..……. 3
Introduction ……..…….. 4

Facts and Assumptions …….. 4
Rationale for Building EISSA ……. 5
Terminology …… 5
Guiding Principles …….. 6

Steps in Designing Security Architecture ……. 7

Phase 1: Conducting Security Assessments ……..…….. 7
Phase 2: Formulation of Target Security Architecture Designs ……..… 8
Phase 3: Construction of Policies and Procedures ……..…. 9
Phase 4: Implementation of Target Security Architecture Design …….. 9
Phase 5: Integration of Security Practices to Maintain Secure Status …… 10

Case Study ……..… 10

Introduction ……..… 10
Background ……..…… 10
Phase 1: Conducting Security Assessments …….. 11

Network and Perimeter Security Assessments ……..……. 11
Existing Application Security Architecture ……. 24
Existing Data Security …… 26
Existing Advisories and Patch Management ……. 29
Current Hardware Security …… 29
Existing Disaster Recovery Plan ……. ……30
Security Administration ……. 31

Phase 2: Formulation of Target Architecture Designs ……..……32

Target perimeter and Internet Architecture Design …….. 33

Phase 3: Construction of Policies and Procedures …… 37

Local area network security (LAN) ……. 37
Incident Handling and Response Team ……38
New Antivirus Policy ……..38

Phase 4: Implementation of Target Designs ……..38

Target Application Security Architecture ……39
Target Data Security ……..39

© SANS Institute 2005, Author retains full rights.

Target Business Continuity Plan and Disaster Recovery Plan ……. 39
Personal Information and Electronic Documents Act ……...39
Security Administration ……. 39

Phase 5: Integration of Security Practices to Maintain Secure Status ……..….40

Discussion ……. 40
Conclusion …….. 41
Works cited ……..... 42
Appendices ……. 43

Appendix A: Security Assessment template …….…….. 44
Appendix B: Kyberpass configuration file and scan results ……..45
Appendix C: Cisco PIX 506e firewall configuration … …….. 50
Appendix D: Cisco PIX 506e second firewall configuration ..……54
Appendix E: Questions asked in security interviews……..……56
Appendix F: Cisco PIX 525 scan results and configurations …… 58
Appendix G: MS proxy 2.0 Internet system scan results…….…….. 62
Appendix H: Cisco VPN 3030 ……64
Appendix I: Cisco IDS 4210 scan results ……..……68
Appendix J: LAN routers and switches scans …… 69
Appendix K: Application Security matrix and assessments……...…71
Appendix L: Recommended data classification system …… 72
Appendix M: Logical data Model structure leveraging IBM webshere ……..…. 73
Appendix N: Logical data Model …….…….. 74
Appendix O: Patch management policy for all systems and devices ….. …….. 75
Appendix P: System builds security templates …….…… 76
Appendix Q: Procedure for wiping out data at DRP site ……85
Appendix R: New MS ISA server configuration recommendations…… 87

© SANS Institute 2005, Author retains full rights.

ABSTRACT

Motivation
The purpose of this paper is to demonstrate how to develop an information systems security architecture in a complex environment with few security measures in place. The case study illustrated will provide the reader with a set of guidelines that can be used to develop security architecture components that allow for scalable and secure IT infrastructure.

Problem statement
The existing infrastructure lacked the structural security elements needed to support the evolving IT infrastructure, emerging legislative regulations, and ever-increasing threats.

Approach
In the case study provided, the reader is guided through five phases of security architecture development. The first details security assessments performed to determine security requirements. The second entails formulation of security architecture designs based on recommendations reached in the assessments. The third involves the development of security policies and procedures. The fourth involves the implementation of target security architecture designs. Finally, the fifth involves the integration of security practices through change management and project management methodology to introduce security as a process.

Results
The end result of the five-phase approach was the development of a security architecture design that spread across data, application and infrastructure architectures. It created consistent, transparent, and cost-effective security components to maintain a secure and robust IT architecture. The integrated security components were cost-effective and helped to achieve compliance to legislation and industry regulations.

Conclusion
The approach described serves as a road map for security architecture. Although described specific to the case study, the approach can be generalized to develop security architecture in other IT environments.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

INTRODUCTION

Although the development of IT security architecture has gained much needed momentum in recent years, there continues to be a need for more writings on best theoretical and practical approaches to security architecture development. Writings that document a practical approach are few.

The main objective of this paper is to provide a case study that will define a novel practical approach to the development of information systems security architecture. The approach can be used by other information systems security architects.

This paper will begin by introducing concepts related to IT security: the rationale for its use, specific terminology and guiding principles. It will then lead the reader through five practical phases to developing secure architecture, followed by a case study to illustrate its applicability to an insurance and investment company. A discussion that includes lessons learned and advice to colleagues concludes the paper.

Facts and Assumptions

Facts:

1. The company already has an IT infrastructure made of different platforms (Windows NT and Y2K, Unix Solaris 8, Cisco IOS, and Mainframe).

2. My role in this project is that of security architect and security practitioner.

3. Security education to increase awareness is needed by all company staff including senior management.

4. A blueprint of enterprise information technology architecture exists. Along with the development of security architecture, all other architectures, data, application and infrastructure (hardware, networks, OS) are being defined and developed by application and infrastructure architects.

5. Corporate security policy and enterprise information technology architecture are out-of-date and do not represent the evolving business and corporate environment and the changes in IT infrastructure.

Assumptions:

1. The reader understands theoretical concepts of risk assessment.

2. The reader understands basic technical terms such as private IP addressing schemes, routing of IP protocol, TCP/IP scans, firewall rule set, LAN, WAN, etc.

3. ACME is the alias used for the company name.

© SANS Institute 2005, Author retains full rights.

4. IS (information systems) and IT (information technology) are used synonymously.

Rationale for Building Enterprise Information Systems Security Architecture (EISSA)

Clients depend on insurance companies to secure their private and personal information. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and all legal and audit regulations require the application of security controls to protect personal and private information. IS security architecture sets the road map for introducing security controls and long-term direction.

Providing a secure architecture ensures that the cost of system failure, recovery, business interruption, and reputation impact is diminished. The cost of building the systems, networks, applications, and databases that provide for the business is measured against the cost of recovery, business interruption and reputation impact. The result is that secure architecture will reduce the cost of interruption and recovery that otherwise would be very costly.

The survival of the company depends on its ability to secure the IT environment from malicious and non-malicious attacks. The unprecedented increase in viruses, spam, hacking attempts, and other malicious threats have emphasized the need for secure architecture.

Terminology

Enterprise Information Technology Architecture (EITA) forms the umbrella framework for all technology used by ACME. The EITA architecture components include application, data, infrastructure architecture (hardware, systems, and networks), and security.

Enterprise Information Systems Security Architecture (EISSA), a component of EITA, forms the overall physical and logical components that make up security architecture in the organization.

National Security Agency/Central Security Service is “America’s cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information” (NSA/CSS website). NSA is a well-recognized source of communications, technology and data processing standards and guidelines. It provides key technical information for the development of security architecture.

“ISO 17799 is a comprehensive information security process” that “provides controls, standards and guidelines that are designed to be used virtually any industry and application” (Info-Tech Research Group).

© SANS Institute 2005, Author retains full rights.

The National Institute of Standards and Technology (NIST) is an agency of the United States government that concerns itself with the development of standards and technology. It is a good source of technical standards and guidelines (NIST website).
Intrusion Detection System/Intrusion Prevention system (IDS/IPS) are systems that detect anomalies and suspicious traffic matching signatures of common attacks. It is used in the detection and prevention of attacks.

Vulnerability assessment involves performing vulnerability scans to uncover weaknesses that can be exploited in various systems, applications and network devices.

Guiding Principles

The *Principle of Least Privilege* involves giving a person or a process the minimal authority necessary to accomplish the job or task. Its objective is to control information flow by protecting against information leakage (Ramachandran 53).

Data classification determines the level of security controls needed to protect data. Data can be classified as confidential, private, public, or unclassified. Confidential data requires more security controls than data classified as private.

The *Separation of Duties* principle is achieved by dividing a task and authority for a specific business process among multiple users. The primary objective is to prevent exploitation and fraud by allowing two people to complete a task. For example, to ensure security when transferring funds online, the password needed to access the online account would be partially entered by two people to complete it.

Confidentiality is the principle of "non-disclosure of information to unauthorized users, entities, or processes" (Ramachandran 53).

Integrity is "the prevention of modification or destruction of an asset by an unauthorized user or entity; often used synonymously with data integrity, which asserts that data has not been exposed to malicious or accidental alteration or destruction" (Ramachandran 52).

Availability "ensures the reliable and timely access to data or computing resources by the appropriate personnel" (Krutz and Vines 3).

Identification is "the means in which users claim their identities to a system. Most commonly used for access control, identification is necessary for authentication and authorization" (Krutz and Vines 4).

Defense in Depth is "a concept used to describe layers of defense strategies. The components at each layer work in tandem to provide one cohesive security mechanism" (Arconati 3).

© SANS Institute 2005, Author retains full rights.

Risk Analysis Approach

The formula for calculating risk is: risk = threats x vulnerability x value of assets (Harris 91). It is always important to assign numerical values or use a convention like high, medium, and low to reach conclusions. One must take into consideration all existing and potential mitigating factors in determining the right numerical value or the residual risk. For example, if risk is calculated as 5 on scale of 1 – 5 (with 5 being the highest), mitigating factors that exist can take risk factor 5 down to 3 or 4 if they are strong in reducing the probability and/or impact of threat, which gives the residual risk factor.

Examples of risk assessment methodologies that will help a security architect develop a process for risk analysis are Kepner Tregoe (Kepner Tregoe website) and NIST's Risk Management Guide for Information Technology Systems (Stoneburner, Goguen, and Feringa).

STEPS IN DESIGNING SECURITY ARCHITECTURE

This section describes the theoretical basis and practical process for the five-phase approach to developing security architecture.

Phase 1: Conducting Security Assessments

Security Assessment takes an account of the current security architecture status. Its goal is to "evaluate threats against and vulnerabilities within the assets of the system and to certify all implemented security controls as adequate, either completely secure or meeting acceptable levels of risk" (Ramachandran 21). Evaluation of the current status includes all levels of security architectures: data architecture, application architecture, and infrastructure architecture (networks, and systems). It involves the following steps:

1. Identification of key personnel to be interviewed for information gathering.

2. Identification of all critical and non-critical security components to be assessed (e.g., firewalls, IDS, proxy, applications, databases, etc.).

3. Design a template for security assessments of all identified security components. Security assessments should include a Business Impact Analysis (BIA) that will be used to "determine the appropriate controls (technical and administrative) described in the policy" (King, Dalton, and Osmanoglu 28). The template used can be found in Appendix A

4. Identification of all threats, vulnerabilities and security issues in each component.

5. Conducting security risk analysis can be done to in this stage as part of security assessment

© SANS Institute 2005, Author retains full rights.

A Modular view is used when conducting security assessments. Each component of security architecture is treated separately. This helps to develop architectures within architectures and emphasizes the coexistence of peer architectures like data and application architectures. It allows a look at security from a “hierarchical view and from an independent component view. With a hierarchical view we can see the underlying architectures. A horizontal view helps us understand the interrelationship between peer component architectures” (Johnston 5).

This modular view is important for us to see how all elements of security architecture interact with each other and with other architectures. Layered in-depth protection methodology also plays a role in that it divides security components into several layers. For example, to assess the security of an overall system structure, one needs to divide security into several layers: operating system security layer, application security layer, database (backend systems) security layer, and network security layer. Each layer is a security component. This layered approach allows one to deal with specific components and isolate issues related to each.

Phase 2: **Formulation of Target Security Architecture Designs**

Target designs are based on results and recommendations as determined in phase 1. As one conducts security assessments, it is imperative to enumerate all necessary architectural elements needed to develop the target security architecture. The recommendations can be used to make necessary architectural changes to existing IT infrastructure design, implementations, and policies and to add security controls to other architectures. It is important to develop two types of security architecture designs:

1. A *logical architecture* of IT security components is needed to organize the physical architecture and implement security in all identified architectures. The logical structure includes processes, technology and people. It consists of perimeter security, a computer incident response team, antivirus policy, security administration, a Disaster Recovery Plan (DRP), risk and threat analysis, data security, application security, and infrastructure security.

2. *Physical architecture* designs include network diagrams illustrating firewalls, mail gateways, proxies, modem pools, VLANs, Demiliterized Zone (DMZ), internal and external connections and devices used, and diagrams of other architectures in relation to security architecture. Especially helpful are diagrams with IP addressing schemes identified.

Phase 3: **Construction of Policies and Procedures**

Once the proposed network infrastructure is designed and all security components to be integrated into other architectures are defined, the third phase can begin. Policies should have a structure starting with corporate policy and then departmental policies and subject policies that deal with what must be protected and all information systems security architecture components. Several important points need to be articulated:

© SANS Institute 2005, Author retains full rights.

According to Merriam-Webster's Online Dictionary, a policy is:

1. A management or procedure based primarily on material interest

2. A definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions and a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body.

Companies develop policies and procedures to guide their employees and external companies on how to behave. While creating polices, one needs to achieve a delicate "balance between security and the ability to conduct business" (King, Dalton, and Osmanoglu 15). Security should never be seen as an impediment but an enabler as one provides solutions and alternatives.

Policies are general in nature and should be distinguished from standards. A policy might read, "All communications must be protected from eavesdropping." The standard will show how this is to be accomplished and what technologies need to be deployed to achieve the policy (King, Dalton, and Osmanoglu 15).

It is very important for policies and standards to have the support of the executive team (King, Dalton, and Osmanoglu 16). It is equally important for people to understand the policy and its objectives so that it gets the support it needs to achieve compliance.

Auditors can use these policies as references when conducting audits as auditing complements all the endeavors of security to achieve compliance by measuring against these policies to uncover any deviation from policy. Findings that are discovered by audit would be deviations from policy and best practices.

It is important to note that in reality many system or device-related policies will end up being translated as configurations on these systems and devices to implement policy. As such, parallel development of polices and architecture is necessary. For example, a policy can say "no surfing of illegal sites." As the Internet server is being built, we have to configure the server to block all illegal sites known. As such, policies are translated to server configurations. Once all policies and standards have been developed, the next phase can begin or the next phase can be done in parallel.

Phase 4: Implementation of Target Security Architecture Design

Once the conceptual design and all related policies and procedures are developed, implementation of target security architecture can begin. Projects that implement architectural changes should have a plan that defines timelines, funding, and resources needed to implement these changes.

© SANS Institute 2005, Author retains full rights.

Phase 5: Integration of Security Practices to Maintain Secure Status

Security is a mindset and a process. In order to maintain a secure environment, one needs to define the role of IT security staff in evaluating all changes to the architecture, systems design, and network structure to maintain secure status in day-to-day operations. In order to achieve this goal, security has to be integrated into two main processes:

1. *Change management process:* Any changes to networks and other infrastructure components must go through this process.

2. *Project management methodology and guidelines* guide the various technology projects in the organization. Security should be integrated into these guidelines at all stages deemed necessary by these guidelines. For example, security can be integrated in Joint Application Development sessions (JAD), business requirement definitions stages, and implementation and development stages of project management methodology. Getting involved in new projects allows the security architect to integrate security controls that implement policy. It also allows the security architect to anticipate and develop new policies and standards.

CASE STUDY

Introduction

This case study will show the approach described above that was followed to develop security architecture at ACME. It is written from the perspective of an information systems security architect and security practitioner who is also a system administrator.

As the project was broad in scope, this case study will focus on defining the existing status of IT security, many of the security assessments conducted and integration of the five mentioned phases to reach recommendations for the new security architecture. It will focus on network perimeter security architecture design and other IT architecture components, such as data, application and infrastructure. It will also focus on key policies and standards like system builds, antivirus, antispam, and data aggregation solutions. The end result will be new physical and logical security architectures.

While reading the case study, one can observe the parallel implementation of target architecture with policy development.

Background

ACME is an insurance and investment company that grew from a mainframe-only shop ten years ago to now integrating a client-server model. The integration of other architectural components like data, application, and infrastructure came after expanding

© SANS Institute 2005, Author retains full rights.

and integrating different applications and systems in the client-server environment. Security was not an integral component from an architectural perspective. As such, many security components were either missing or lacking in security design and implementation, such as IDS, DMZ, VPN implementation, web architecture, system builds, patch management, hardware and software directions, data classifications, encryption policy and standards, firewalls design, operating systems security, etc.

Consequently, I conducted security assessments and introduced security architecture and set the groundwork for implementations and changes in the information systems security architecture and initiated the development of polices and procedures related to security architecture.

The horizontal and random growth in the client-server environment (systems, applications, and databases) made it such that IT infrastructure needed security architecture and controls to sustain secure and scalable information systems architectures.

Phase 1: Conducting Security Assessments

The first step in my approach was to gather information required to complete security assessments to derive requirements for architecture. I conducted onsite interviews with key identified technical and non-technical personnel and developed a list of questions to ask (see Appendix E). Figure 1 depicts the existing Internet and external connectivity.

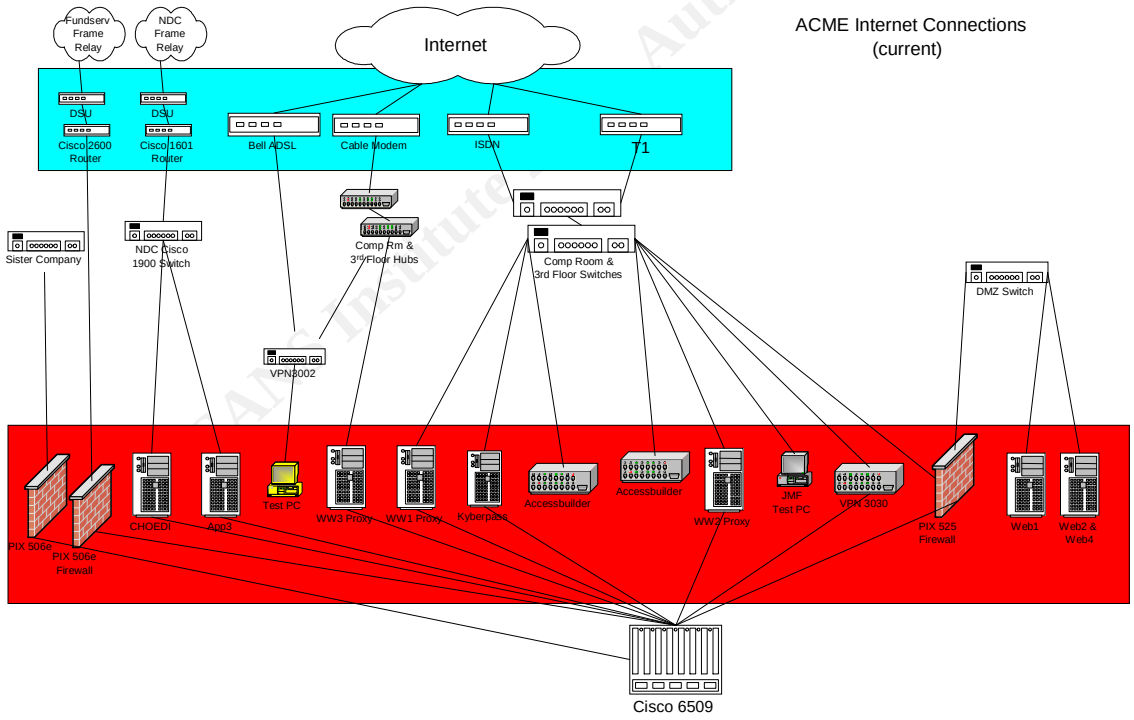


Figure 1: Current Internet and External Connectivity

© SANS Institute 2005, Author retains full rights.

Network and Perimeter Security Assessments

Security assessments were conducted and will be described by their security assessment details, results and recommendations. I used GFILAN guard network security scanner to conduct vulnerability scans. I developed a matrix that contained the names of components that required analysis for the purpose of assessments from Figure 1.

1. Kyberpass Firewall

Assessment Details

The Kyberpass server is a strong authentication proxy server (two factor authentication) using "Privacy Enhanced Mail" encryption algorithm. An outside PC sends a packet to an outside Internet address and port on the Kyberpass server. The Kyberpass server initiates handshaking to authenticate (password and key disk), and establishes an encrypted tunnel if it recognizes a valid user. The outside address and port is proxy passed through the Kyberpass server through the inside interface to a specific inside address and port. Each port going to each address requires a separate proxy and allows external brokers and some of our staff access to our mainframe backend systems and network.

Results

The operating system is not hardened and the system is not patched. Firewall software is out-of-date and no longer supported. The following open ports 135 for netbios and 139 epmap are both needed internally. This system is identified as high risk.

Recommendation

A plan was set for phasing out the system and migrating users to connect through VPN. Continued to monitor the logs until system is phased out. The challenge was providing an alternative way for our external partners to connect to our network remotely. So I developed a policy for external partners that needed to connect to our mainframe through another remote access connection using VPN. The new policy stipulated putting controls like personal firewall, and up-to-date antivirus on each PC that needed to connect using VPN and developed VPN profile to be used by external partners to establish a non-split tunneled connection to hardcoded IP addresses of mainframe systems they needed to access. Phasing out the system was defined as an architectural element. Firewall configurations and scan results are included in Appendix B

2. Cisco PIXes 506e

Two firewalls are deployed. One was used as a connection with a fund company and the other was connected to our sister company and external financial companies that provided investment data to investment office.

© SANS Institute 2005, Author retains full rights.

Assessment Details
All questions used in interviews with network manager are included in Appendix E. Firewall architectures and rule sets were examined and vulnerability scans conducted using GFI LANguard network scanner

Results
Both PIX firewalls were up-to-date with patches. Open ports were needed. Available services were valid. Rule sets were examined. Position in the network was validated and approved. A vulnerability scan was done. Audit logs validated. Appendix C shows the Cisco PIX 506e firewall configuration file that was examined and approved and scan results. Appendix D has the second firewall configuration file and vulnerability scan results.

Recommendations
No changes were required on these firewalls. I developed a policy regarding protocols for secure transfers of data with other companies and put in place a process that defined the party responsible for approving any changes on these firewall configurations and rule sets.

3. National Dental Claims (NDC) connection:

Assessment details
All questions used are included in Appendix E. Connection was established between ACME and National Dental Claims to provide and connect our dental reimbursement systems with the National Dental Claims Network that connected all dentists for online submission of dental assessments and claims. Reviewed the connection diagram and IP traffic flow and assessed controls on the systems connected.

Results
Connection was not separated with a firewall. Systems connected were not up-to-date with patches. This configuration was classified as high risk, as any legal entity connected to the network has to be separated with a firewall. All ports and services have to be defined and controlled through firewall rule set. Separation of IP traffic between the two companies through a Cisco PIX 506e firewall was required.

Recommendations
One of the basic rules of architecture when needing to connect two legal entities is to separate them with a firewall. The firewall will allow only approved IP traffic to pass through. The risk is very high in this case, not only because we can be legally liable and susceptible to any malicious traffic initiated from our network and vice versa, but also because the systems are vulnerable and can be exploited. Cisco PIX 506e is needed in the design architecture between the two entities. The firewall rule set was developed and reviewed with network manager. Systems connected to be updated with all security patches. It was defined as an architectural element.

© SANS Institute 2005, Author retains full rights.

4. Cisco PIX 525

Assessment Details
This firewall was used at our head office and connected to T1 line. I examined the rule set of the firewall and did a vulnerability scan of all secure and non-secure interfaces.

Results
The device was kept up to date with patches. Open ports were valid. Available services used were valid. Rule set analysis revealed all valid rules. Position in the network was correct. TFTP and Pcanywhere remote connection were needed so we had to accept the risk associated. See Appendix F for scan results and configuration files.

Recommendations
Continue checking the logs on a regular basis. Process stipulated to apply updates for any TFTP vulnerabilities. No change was needed. A policy was needed to define IP traffic guidelines to DMZ and internal network. A process for approving changes to firewall configurations by information systems security was also established.

5. Three MS Proxy 2.0 Servers

One proxy server, used for Internet access, was installed on Windows NT. A second was the mail gateway on Windows NT and a third was for redundancy, testing and access to external company that hosts our website.

5a. First Proxy

Assessment details
The first MS proxy server 2.0 was used for Internet access and was installed on Windows NT. Questions used in assessment are included in Appendix E. I identified all secure and non-secure interfaces.

Results
The system was not up-to-date with patches. Several ports were open but not used, such as port 69 for TFTP service. Several services were not used, such as TFTP, SNMP. Its position in the network needed to be changed due to the fact that the firewall module was not used. System acted as a proxy only. Company's Internet policy was out-of-date. System had no antivirus installed. See Appendix G for vulnerability scan results.

Recommendations
The following recommendations were presented:

1. Disable TFTP on port 69

2. Disable SNMP on port 161

© SANS Institute 2005, Author retains full rights.

3. System must be updated with all updates and security patches

4. MS proxy 2.0 to be repositioned in the internal network behind the firewall and upgraded to ISA server

5. Protect all CGI directories

6. Disable netbios ports 137 and 138

7. Disable news port 119

8. Update antivirus software from trendmicro and activate HTTP/FTP virus scanning to virus scan all http traffic.

9. Internet policy to be updated

Server must be upgraded to ISA server as MS proxy 2.0 was no longer supported. The system should be positioned behind the firewall. This was defined as an architectural change.

5b. Second proxy

Assessment details

Server was used as an SMTP gateway directly connected to the Internet. It connected to an exchange server inside the network through the second interface. Same questions for the first proxy were used with similar results to those described above. A review of antivirus and antispam programs was conducted. Review of system patch level and all ports and services was conducted.

Results

The antivirus software being used scanned only email attachments. It was nearing the end of support for the number of updates we were supposed to receive per our agreement with the vendor and needed to be updated to a higher version. The current spam prevention methodology centres on the antivirus e-Manager product. E-Manager was not designed to be a spam prevention tool but was modified and manually maintained to support ACME's spam detection (not prevention) program. Spam detection was done manually with antivirus e-Manager that allowed manual input of key words filtering to stop spam. System was not up-to-date with security patches

Recommendation

An upgrade to the current release of antivirus product we are using would eliminate the need for the proxy server to run with the e-mail gateway and required for accessing external web host for support purposes. Upgrading antivirus software that scans mail and attachments as it was close to end of agreement with vendor and changing policy to include scanning all http/ftp traffic and implementing the appropriate tools and update

© SANS Institute 2005, Author retains full rights.

services to manage spam problem in both the short and long term. Consequently, installation of a new antispam package from the same vendor was the resolution.

Device is to be repositioned in the DMZ with updated new hardware and software to a new MS ISA server. It was defined as an architectural change. I opted not to include the scan results here as they matched those of the first proxy. Identical systems except for port 25 open for SMTP protocol and 110 for POP3 protocol to handle mail as this server served as mail gateway, antivirus and antispam detection. Antispam problem can be demonstrated in the following diagram:

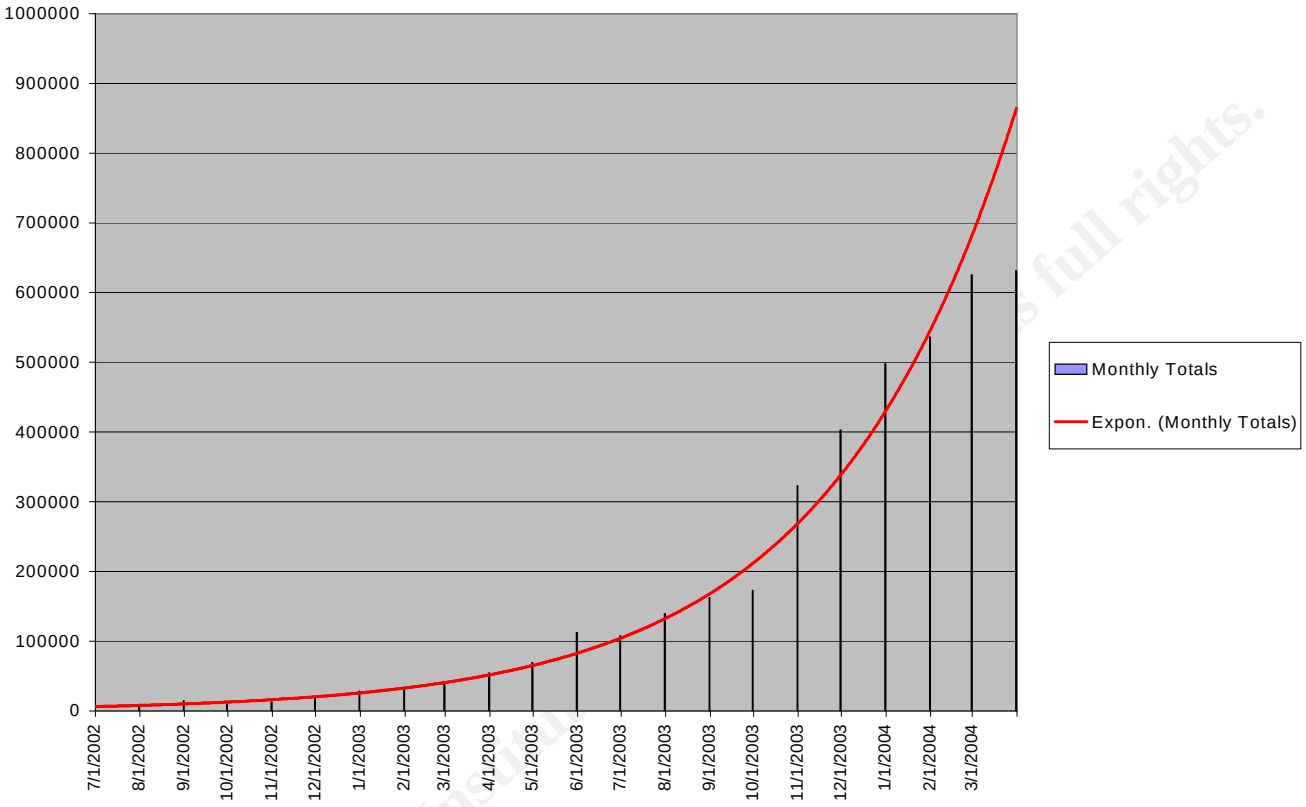


Figure 2: Current Spam Situation

5c. Third MS proxy 2.0 server

The third proxy is an exact replica of the first and the results attained are similar. This server was used for testing and provided another means of connecting our web master to the external host company to avoid having to open ports required for the type of support required.

© SANS Institute 2005, Author retains full rights.

Recommendations
Phase it out and only use for testing in a technical lab and provide an alternative way through the firewall for the function of connection with external website host to manage our website hosted by external web host.

Two of the proxy servers will be decommissioned and the third moved into the technical services lab for offline testing. A new MS ISA server will be positioned behind the firewall with updated antivirus and new antispam software. All three proxies are to be decommissioned. All proxies were defined as high risk; they were vulnerable to attacks as they were not patched and have no antivirus software. It was concluded that there is a need for a new antivirus policy.

6. Cisco Virtual Private Network (VPN) Device Model 3030

Assessment details
Questions included in Appendix E. Cisco VPN concentrator 3030 was connected to an ACE server that does two-factor authentication using RSA secure ID token: something you know (PIN) and something you have (number on the secure ID token). Security assessment included the VPN device and ACE server installed on Windows NT.

Results
Device and ACE server were not up-to-date with patches. Ports were validated except port 21 FTP. Services (processes) were validated. Secure and non-secure interfaces were identified. Configurations of VPN concentrator 3030 were checked and approved. Configurations of VPN software were approved but a banner was added, which is presented to every VPN user at login. Configurations are included in Appendix H. Three Cisco security profiles were used to access the network: the first was a non-split tunnel that hides the connecting computer from any local area network devices, the second, a split tunnel that allows client PC to be seen by other PCs on local LAN but is less secure than non-split tunnel profile, and the third, a NT authentication profile to access through VPN concentrator using LAN ID. VPN implementation policy was not developed.

Recommendations

1. Added a system access banner to VPN configurations so that every user logging in through VPN client can see (see Appendix H).

2. Developed a policy that defined requirements for using split and non-split tunnel to prevent abuse.

3. Policy developed that defined approvals, forms, profiles, controls for home PCs used for VPN (i.e., personal firewall, up-to-date antivirus software).

© SANS Institute 2005, Author retains full rights.

4. Device to be repositioned behind the firewall to force all IP traffic through the firewall. Defined as architectural change. Defined as low risk but need to be included in new architecture design on perimeter network.

7. 3COM Access Builder Devices

A Modem pool that consisted of six dialup modems was used by technical staff to connect remotely to the internal network using access builder device.

Assessment details
Questions are included in Appendix E. These two devices provided a number of modems that our technical staff used to connect to in order to access the network. Authentication was provided by the access builder manager and authorization through Kyberpass firewall server.

Results
Its position in the network was correct. Identified all modem numbers available for use. Normal device configurations for modems provided by Telco. Authentication method used was username and password. There was no policy around its use. It was used mainly by our technical staff as a remote connection before the deployment of VPN and for people who were out of jurisdiction for Internet access (out in the country) to connect via Kyberpass firewall to support internal systems. It was concluded that these devices are no longer needed considering we have an alternative VPN route and Internet became available in remote locations.

Recommendations
An effort to eliminate the need for dial connectivity was made. A small number of users (<10) on this system were migrated to VPN connectivity. To phase it out was defined as an architectural change.

8. ISP connections

Assessment Details:
Currently ACME has three ISP connections:

1. The primary T1 line provided by Bell to support all Internet traffic and access to ACME web services.

2. Bell ISDN service that manages Internet e-mail.

3. Cogeco cable connection used for testing and support of the external web server host.

Results
In the current configuration, none of these connections provide redundancy; failure in one would result in a loss of that service (i.e., HTTP, e-mail, ACME's web services) and difficult migration to an alternative ISP route due to complexity.

© SANS Institute 2005, Author retains full rights.

Recommendations
It was proposed that:

1. The mail traffic be re-routed to the existing Bell T1. Sufficient capacity exists.

2. The Bell ISDN service be cancelled.

3. The Cogeco service be re-routed to the technical services lab and only connected when the lab is disconnected from the network.

4. A second high-speed ISP connection be installed and configured to provide redundant connectivity to the Internet. If primary ISP connection fails, the secondary link will provide access to the company's web services and our internal HTTP and e-mail needs. This may become more critical with the enhancements planned to the group insurance websites called Plan Administrator and member updates services which will change web architecture from a "view only" mode to "update mode" where group insurance administrators can update their employees' data on our websites.

The proposed and updated configuration (Figure 3) provides Internet redundancy cost effectively. Here is the ISP proposed connection recommended. It is an architectural change.

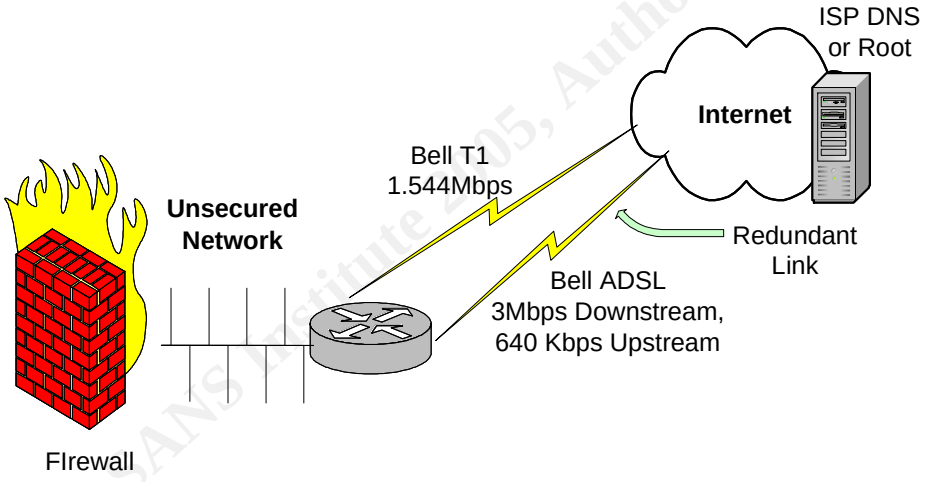


Figure 3. Proposed ISP Connection

9. LAN Extension Device and All Telco VLANs

A turnkey VLANs provided by the local Telco and used in connecting all our remote offices as the following diagram shows:

© SANS Institute 2005, Author retains full rights.

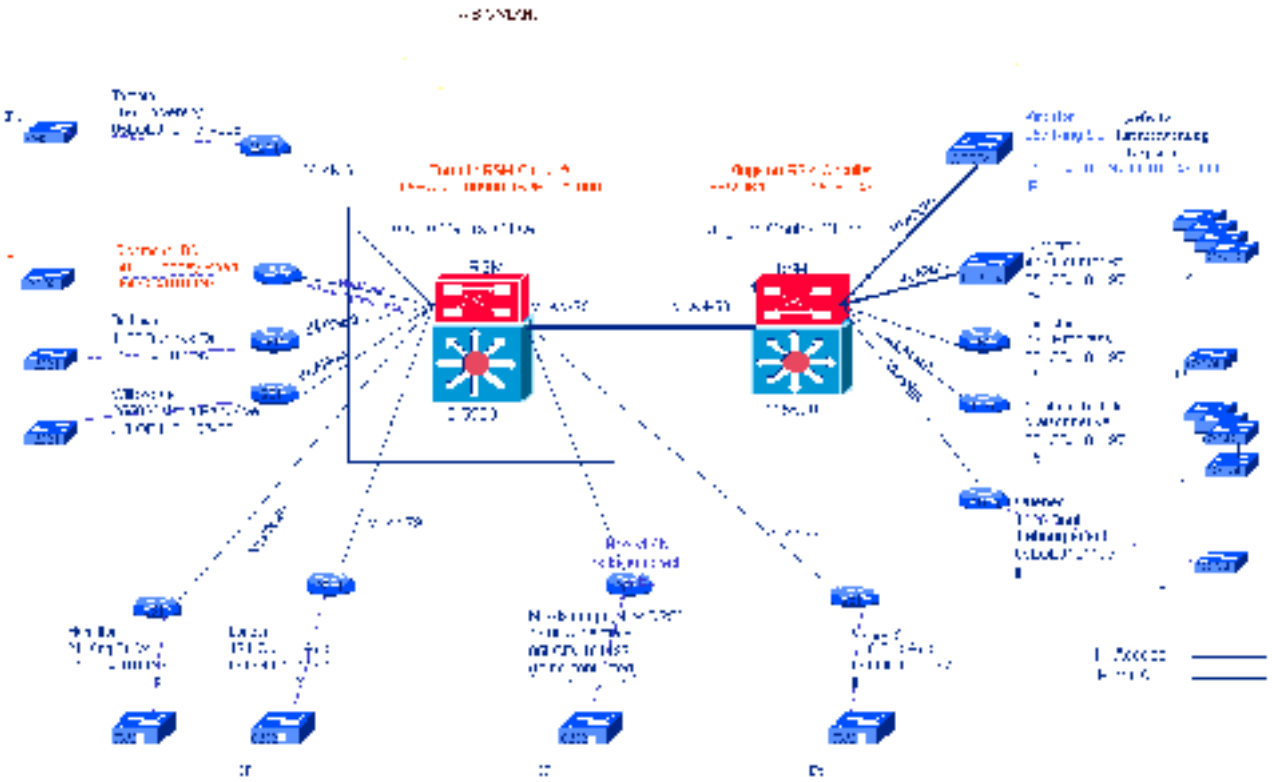


Figure 4: VLANs connecting all local and remote offices across Canada

Assessment details

Questions included in Appendix E. I could not obtain logs from the ISP as it was not included in the contract. Monitoring was done on these connections around the clock (24/7) by ISP. Examined the static routes provided to us by local Telco and examined the contract to be able to recommend amendments to it. Requested statistics on the utilization and use of these connections in addition to snapshots of traffic generated on a regular basis.

Results

Contract was lacking in providing more control on VLANs and lacked an audit section to allow us to audit our configurations and devices used for connecting all remote offices. Utilization stats showed that we were in good standing as far as the speed was concerned on these devices. Assessments shed light on some of the controls the ISP has and resulted in an inventory of all connections with banks of addresses assigned to these VLANs as shown in Figure 4.

Recommendations

The following to be added to the contract:

1. Running regular vulnerability scans on these devices.

© SANS Institute 2005, Author retains full rights.

2. Conducting regular audits on access control, change control, utilization.

3. Collecting statistics regularly on utilization rates.

4. Replacement of some of these VLAN connections for some of our remote offices where we only have minimum number of employees with VPN 3002 device to connect these offices through our VPN concentrator. This was defined as architectural change.

10. Cisco IDS 4210

Assessment details

Questions used are included in Appendix E. Intrusion detection device was introduced as a result of an audit requirement at the time of implementing VPN solution. Device was recommended to monitor all traffic directed to VPN concentrator and head office firewall. The initial implementation is demonstrated in the following diagram:

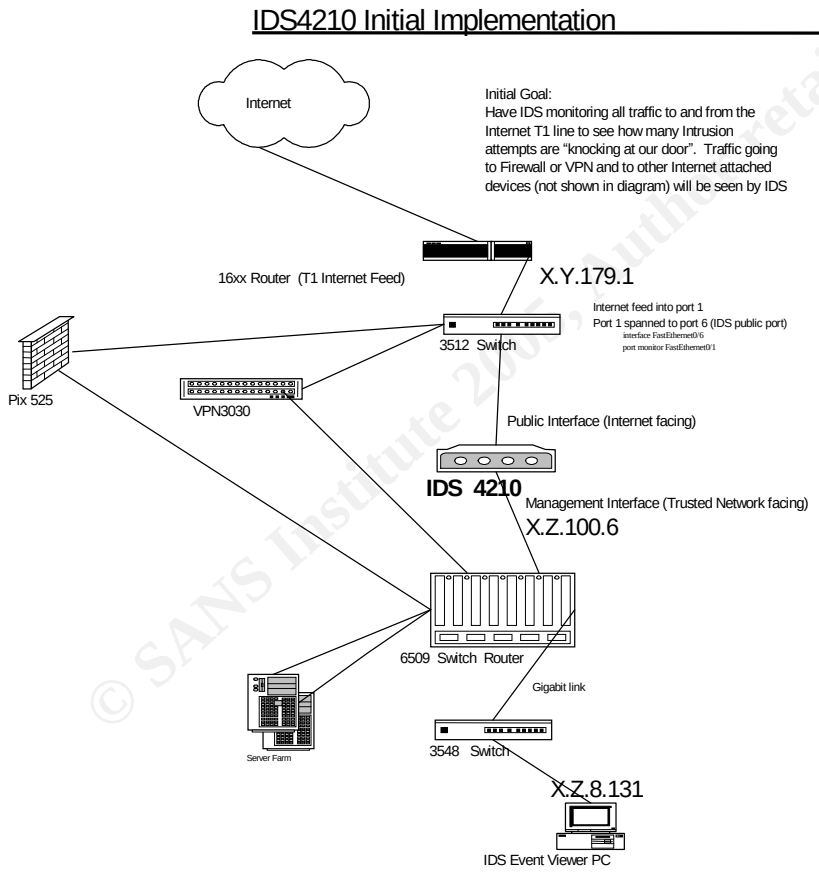


Figure 5: Initial Implementation of Cisco IDS 4210

© SANS Institute 2005, Author retains full rights.

Results
The device was not configured correctly and IP traffic was not benchmarked so as to filter and isolate normal traffic from malicious or abnormal traffic and create filters needed on the IDS. The device scan results are in Appendix I.

Recommendations
Two phases were suggested:

1. Phase One, as depicted above, positions the device at the door of our network in order for us to identify the incoming IP traffic patterns.

2. Phase Two: Positioning IDS device in our DMZ to determine the type of traffic in the DMZ. Also to filter TCP/IP traffic to extract IP packets that match a certain type of IP traffic to be able to isolate normal traffic from malicious or abnormal traffic that matches the IDS sensor signatures. Using IDS event viewer installed on a PC and positioned in the internal secure network to read the IP traffic and events. Also a threat server on the inside of our network was recommended. Cisco IDS 4210s were no longer supported so recommended upgrading to Cisco IDS 4215 sensor. It was defined as an architectural change.

13. Local Area Network Security (LAN):

Assessment details
Questions are included in Appendix E. Assessment entailed examining the configurations of the main routers, cabling layouts, physical security controls and LAN policy. In addition, conducted vulnerability scan using GFI LANguard network scanner on main LAN routers and switches, and examining all related policies.

Results
Ethernet cat 5 10/100 MBPS cables were used for the client server environment. IBM router 2216 connected mainframe to client server environment. Cisco routers and switches were used mainly with Cisco 6509 as main router. Change management was not used to change configurations or update routers. Network manager and other system administrators approved the changes but no formal approval process was written. There was no policy regarding connecting external parties to LAN. There was no software or hardware used for activating ports centrally from head office. Laying out the cable from a live port on the switch and terminating the connection at BIX panels was the only way to add a connection and a port manually every time. Maintenance staff had access to physical space when laying out cabling. Physical security was practiced for granting access to physical space and process for activating and deactivating access badges was established and followed.

© SANS Institute 2005, Author retains full rights.

Part of LAN assessment was evaluating the following main routers:

1. IBM 2216 Router

Assessment details
This router connected the main frame to client server environment.

Results
An older legacy router used which has some limitations in providing connectivity with the speed 10 MBPS as opposed to 100 mbps needed from the mainframe to client-server environment. Vulnerability scan using GFI LANguard revealed ports that are legitimately needed on the router Telnet attempt to the router IP address revealed that router was wide open with no challenge. A Telnet attempt was performed, resulting in a connection to the IBM 2216 prompt as follows:

Copyright Notices:
Licensed Materials - Property of IBM
Multiprotocol Access Services
(C) Copyright IBM Corp. 1996, 1999
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
MOS Operator Console
For help using the Command Line Interface, press ESCAPE, then '?'.
IBM 2216 *
Ready for command input.

All vulnerability scan results are included in Appendix J.

Recommendations:
Add a user name and password on the router to challenge any telnet attempt to access it. Replace it with a Cisco 6509 device since expertise is limited with IBM2216 administration among technical support staff. It was defined as a regular change.

2. Cisco 6509

Assessment details
Vulnerability scan was conducted using GFI LANguard network scanner and did a Telnet to the router and reviewed protocol used.

Results
All are using RIP protocol, with some static routes hardcoded internally. Scan results revealed all legitimate routes and ports. Results of vulnerability scan included in Appendix J. Telnet was challenged with a login screen as follows:

Netlogin:

© SANS Institute 2005, Author retains full rights.

Recommendations
Develop a process for approving any changes and added them to list of devices required to be monitored and included in the patch management program. No other changes were required.

3. LAN Policy Assessment

Assessment details
It was discovered that there was no existing policy.

Results
It was determined that several LAN issues needed to be addressed in a new policy:

1. Activating new LAN ports for new connections.

2. Follow-up process on ports that are not needed.

3. Authorization for activating ports on the LAN.

4. Approving external vendors who need to connect to LAN.

5. Technical controls required to be enforced on any PC or laptop brought in by the vendor or external contractors to be connected to LAN.

6. Authorization for adding static routes to main routers and switches

Recommendations
Use specific hardware such as routers that support remote control of ports in our remote offices to control activating all LAN ports centrally from head office as anyone connecting to remote office LAN would obtain an IP address from the DHCP server and can launch any malicious or discovery software. It was defined as an architectural change since it would change the routers standard we used.

Existing Application Security Architecture

"Application layer security is the enforcement of access control principles within the application to prevent and detect unauthorized access" (King, Dalton, and Osmanoglu 319). Identity, authentication, authorization and audit are principles that need to be achieved when assessing and defining application architecture. "When designing your architecture, target your applications for best results, your applications are the closest to your data as they process, exchange, and store your data. Layers of application security are application, users, systems that host the application, networks where the client and server attach, and physical security infrastructure (King, Dalton, and Osmanoglu 115).

© SANS Institute 2005, Author retains full rights.

Assessment details

Application assessments were conducted by creating a matrix of mission critical applications. Assessment included a review of access control matrices and types of security controls used in each application as they apply to the type of application being reviewed and type of data sensitivity being handled. Authentication and authorization models were reviewed. Security administration of generic and privileged IDs and passwords was reviewed. Application matrix and assessment details are illustrated in Appendix K. Since the number of applications assessed is large (45), I am including only "mission critical applications," which led to development of policies for application security.

Results

Several vulnerabilities were discovered in the applications, authentication and authorization models used. In addition, audit was left unaccounted for. Encryption and code security practices were not integrated in the in-house development of applications.

Recommendations

A new policy regarding the application security was designed to define direction in application security layer. The policy included the following:

1. Certificate-based authentication for any application offered to external community especially when personal and private information protected under privacy act is served through the application. Connection from client to server should be encrypted using secure socket layer SSL. Certificate on the sever should be 1024 bits key allowing only 128 bit level of encryption in the browser.

2. Using different authorization techniques, every user and entity must have a specific set of access authorized based on their roles in the security access control matrix.

3. Reverse proxy is required when providing web access to confidential information through an http server to external client community (e.g., brokers, financial advisors).

4. Secure Electronic Transaction protocol (SET) should be used if the ability to conduct financial transactions on the website is offered, such as buying portfolios or any financial type transactions.

5. Applications should always include audit trails of access control and transaction performed.

6. Specific Application security, such as Websphere security, should be designed by the security architect.

7. Programming language-specific security is crucial to integrate security in code development practices. Security guidelines related to identified and used

© SANS Institute 2005, Author retains full rights.

programming languages should be integrated before development starts, such as JAVA security guidelines and web services security. Sources for some of these can be obtained from vendors such as Sun micros systems, and other resources on the web.

8. Access control to source code was open to all developers and project managers and not protected in Visual Safe Source (VSS), the code library program used. Access to code libraries was not performed by IS Security administration but randomly by developers. A process was developed for access control administration of VSS to code libraries and checking code in and out of the libraries based on developer's level. Security request was required with approvals from project manager and lead developer.

9. All IP protocol traffic to company's web systems in the DMZ need to be network address translated.

10. Application security policies are to be developed that introduce security best practices in code development (i.e. Java, HTML, and Visual Basic), application design, access control, authentication, authorization and audit concepts that need to be accounted for in application design.

11. Introduced role of IS security architect in System Development Life Cycle (SDLC) and defined involvement to integrate application security controls in the various applications being developed in-house or purchased from external vendors.

12. Developed security guidelines for encryption of all data transferred to external partners using secure protocols such as SFTP. The web provided many resources that helped me develop secure code practices, such as Java security guidelines found at the Microsystems Website (Source for Developers). It is important to note that as you develop security guidelines, you need to take into consideration business requirements, protocols, and application functional requirements to create guidelines that can easily integrate into application design.

13. The application policy also enforced authentication, authorization and audit at the application level. Introduced user ID and password and two-factor authentication guidelines based on authentication method required for data and system sensitivity. User verification with challenge questions and answers were added into the application when password resets were required.

    Authorization matrix can be based on codes assigned to a hierarchy of access levels based on roles and business requirements. Introduced role-based access control that can be used to meet authorization of users based on their roles. Security access control matrix needs to be more granular and map roles to flows that execute transactions on systems.

© SANS Institute 2005, Author retains full rights.

14. Documentation and training of staff to take responsibility for application security administration was introduced.

Existing Data Security

Data security is dependent on controls which safeguard the confidentiality, integrity and availability of data.

Assessment details
Reviews were conducted on all database implementations in the environment (MS SQL on Windows, DB2 on Mainframe, UDB and Sybase on Unix). For assessment purposes, I interviewed the database administrators and reviewed the following:

1. Policy regarding database updates and security patches

2. Data classification policy

3. Data modeling

4. Data warehousing and data mining

5. Data protection controls, such as encryption, secure data transfers.

6. Evaluating if best security practices were followed when setting up MS SQL, Mainframe DB2, Sybase and UDB on the various systems.

7. Data Aggregation policy and controls in existing structure

Results

1. Data classification policy does not provide for the needs of different sensitivities of data in the environment. It only has confidential, private and public as classifications.

    1. Database updates and security patches were not applied to any database and there was no process in place to support applying updates and security patches.

    2. Data modeling was not practiced or made an integral part of application development. It was, therefore, introduced to assess the relational structure of identified tables where the information was collected.

    3. Data protection controls were weak as data security measures were not in place and encryption was not considered dependent on data classification and protection of data as it traverses internal and DMZ network segments.

    4. Security guidelines related to database security best practices were not practiced. Several major vulnerabilities were found: views were not created on

© SANS Institute 2005, Author retains full rights.

SQL and Sybase databases, row level security and masking of sensitive columns were not practiced, and the “sa” username and password were used to allow access to database (instead of creating users and assigning roles and permissions to users and objects).

5. With DB2 on the mainframe, access control security software called “top secret” was used to control access to DB2 and Datacom data sets on Mainframe with segregation of roles for granting access to data sets based on their label. Top-secret controlled all access to the Mainframe environment including Datacom and DB2 access.

Recommendations

1. A new data classification system with document controls was recommended. Appendix L contains the new data classification system and document control guidelines put in place.

2. Developed a policy for updating all databases with updates and security patches. Recommended applying critical security patches within a short time frame as the risk was high with the existence of these vulnerabilities.

3. Data modeling was enforced as a prerequisite to any security assessment. This will define the data relations between tables collected from backend systems.

4. Data protection controls were introduced into the environment in a policy. Concepts of data integrity were also introduced to senior management to support policies that deal with securing data transfers and data encryption. Policy stipulated protection of data with encryption that incorporates SHA-1 or MD5 hashes to achieve integrity of data.

5. Introduced database server guidelines, for example, always hide database servers from the domain view, if using ODBC connections, each connection should be accessed using its own user name, block 1433 and 1434 SQL from outside on the firewall.

6. Data aggregation security was required as the company started adopting data aggregation technology. The logical data model software helped us integrate disparate back ends to one front end imaging system using IBM Websphere technology. An example solution for data aggregation can be seen in the view used to develop the data model.

   Data aggregation model leveraging IBM Websphere is illustrated in Appendix M and N. Based on this model, security exists in each of the components in this data aggregation architecture. There is application tier security, logical data model security, web services security and data sources security.

© SANS Institute 2005, Author retains full rights.

Upon reviewing the application security and data model security that was developed using JAVA programming language, a document was developed that introduced controls in the structure of data aggregation such as attribute level security, roles used by the applications, and breaking up all flows of access to backend systems.

The application IBM Websphere security allowed for role-based security for users accessing the logical data model to obtain aggregated data from the back end system and present data to front end system. IBM Websphere security handled the authentication. Authorization and audit required for data aggregation.

Existing Advisories and Patch Management

Assessment details
System and database administrators were interviewed. All practices and policies related to patch management operations were reviewed. This included evaluating test and development environments available for patch management.

Results
There was no process or software used for patch management or any form of tracking advisories to update systems. Consequently all systems, databases and devices were not up-to-date and security patches were not applied.

Recommendations
Developed a process for patching systems based on the classification of advisory (critical, medium and low) and position of system or device in the network. The policy established guidelines for technical staff for applying recommended security patches. The new policy is included in Appendix O. It was defined as an architectural change since it impacts all testing and development environments. Vulnerabilities discovered on Internet facing systems and devices were resolved immediately due to their high risk.

Existing Hardware Security

Assessment details
All system build documentation on Mainframe, Unix Solaris 8, Windows NT and Y2k server were reviewed. The review also included Cisco and IBM routers and switches security policy.

Results

1. Systems were built in different ways without any consistency in system builds and design.

2. Systems did not include any security controls or best practices. For example, audit logs on all servers were turned off. Antivirus was either not installed or not up to date and not running in real time. All services and ports are open by

© SANS Institute 2005, Author retains full rights.

default. Systems were not patched with updates or security patches. System security guidelines provided by their vendors or independent advisors were not followed or adopted as best practices.

Recommendations

1. Developed security system build templates for Unix and Windows platforms and incorporated them in the system build documents to be followed by system administrators when building new systems. Security templates for Unix and Windows can be found in Appendix P. This was defined as a regular change.

Disaster Recovery Plan (DRP):

Assessment details
Reviewed the following:

1. Existing business continuity plan that defined all critical systems and priorities of these systems.

2. Existing disaster recovery plan. Reviewed all disaster recovery tests post implementation reviews (PIRs), DRP documentation, communication channels and procedures and participated in the next DRP test at the hot site.

Results

1. System build documents existed but not system recovery documents.

2. Procedures for validation of all vital records (system build documentation, plans, CDs, tapes) to and from the offsite storage location were not in place.

3. The number of boxes taken from offsite storage to DRP site was not validated.
4. More stringent procedures were required for data eradication.

Recommendations

1. Developed IS security architect role in disaster recovery as a valuator and active participant in data eradication at the end of DRP test.

2. Developed a process that stipulated validation of all vital records (system recovery documentation, tapes, CDs, recovery plans) transferred from head office to offsite storage location and from offsite storage location to DRP site. The policy also introduced guidelines to keeping up to date documentation required before they can be used for DRP.

3. Developed procedures necessary to erase all data on Mainframe, Unix, Windows, Cisco firewalls and routers. Procedures can be found in Appendix Q.

© SANS Institute 2005, Author retains full rights.

4. Validate that eradication of data is completed successfully by obtaining a print out of successful code return=0 on result of Mainframe JCL and personal verification that all data on external and internal disks on Unix, Windows, and Cisco are erased completely. It was defined as architectural change.

Security Administration

Assessment details

Assessment included review of current documentation. Access control administration was performed on:

1. Forty five applications

2. Thirty plus Windows NT and Y2K servers

3. Five Unix systems

4. Databases MS SQL, Sybase, DB2, and UDB.

5. Mainframe access control was performed using Computer Associates "TOP SECRET" software.

Results

1. Documentation of security procedures was lacking and not documented.

2. Training was not provided for to security administration staff.

Recommendations

1. Document all security administration procedures.

2. Train staff on any gaps in their understanding of various procedures related to applications, databases, systems, or tools for security administration

3. Developed a policy for security administration hand over, that stipulated documented procedures, and staff training before security department can own the administration of any new system or application.

4. Developed a document review process that stipulated time cycle for updating security procedures yearly.

Personal Information and Electronic Documents Act (PIPEDA) s

PIPEDA sets out ground rules for how private sector organizations can collect, use or disclose personal information in the course of commercial activities. It is based on the

© SANS Institute 2005, Author retains full rights.

Canadian Standards Association's model code for the “Protection of Personal Information.” Information can be accessed at http://www.privcom.gc

Assessment details

Cooperate policies and procedures affected by this legislation were reviewed.

Results

The legislation impacted some of ACME’s practices as it handled personal and private information in the course of its commercial activities. More controls were needed on system access, protection of data, release of data, disposal of printed and non-printed media where personal and private information is stored.

Recommendations

1. Developed a policy that stipulated shredding all printed material that contains personal and private information.

2. Developed an education program with the legal department to raise awareness of PIPEDA and emphasized all aspects that impacted IT structure and practices. This led to the development of policies and procedures.

3. Encouraged adherence to document controls and developed a policy that handles document control by putting sensitivity of document explicitly with date and owner name.

4. Developed a policy for transferring customer information using protocols that incorporate encryption on any external hard drives where data is stored and transferred to external vendors. SFTP is used instead of FTP when transferring files to other companies.
5. Added a disclaimer to SMTP gateway mail system that was appended to every email sent from the company containing privacy statements. This disclaimer advised the recipient that the message might contain personal information that is protected under PIPEDA.

6. Developed a process for retention of information that contained personal information based on business need, legal regulations and audit guidelines.

Enforcement of this legislation was defined as an architectural change to the logical security architecture.

Phase 2: **Formulation of Target Architecture Designs**

Introduction

The foundation for new security architecture was established based upon security assessment results and recommendations. Two designs were developed:

© SANS Institute 2005, Author retains full rights.

1. Target perimeter and Internet architecture design

2. The Enterprise Information Systems Security Architecture framework defines each security component of ACME's IT architecture. Books containing ISC^2 common body of knowledge, GSEC material, and ISO17799 framework provided help in the base design. The structure integrates three elements: people, process and technology. Policies and procedures that regulate the interaction of these elements are described in the model. These designs are shown as follows:

Target Perimeter, Internet and External Connections Architecture Design

The new perimeter design was formed based on the following recommendations in Phase 1:

1. Repositioning SMTP gateway behind firewall in the DMZ.

2. Setting up a new MS ISA proxy is needed to provide Internet and mail gateway services.

3. Upgrading antivirus package and installing it on the new proxy server to scan all http traffic.

4. Installing new antispam package instead of the manual process of blocking based on keywords only.

5. Upgrading the antivirus package on exchange server and updating exchange.

6. Designing the DMZ IP flow to benchmark IP traffic flowing from the DMZ to the internal network.

7. Establishing dual ISP connections that provide redundancy.

8. Setting up a Cisco Pix firewall for NDC connection.

9. Phasing out Kyberpass firewall and all access builder modem connections, as they are no longer needed.

The following diagrams show new perimeter, Internet and external connections architecture that integrates security recommendations outlined in assessments.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

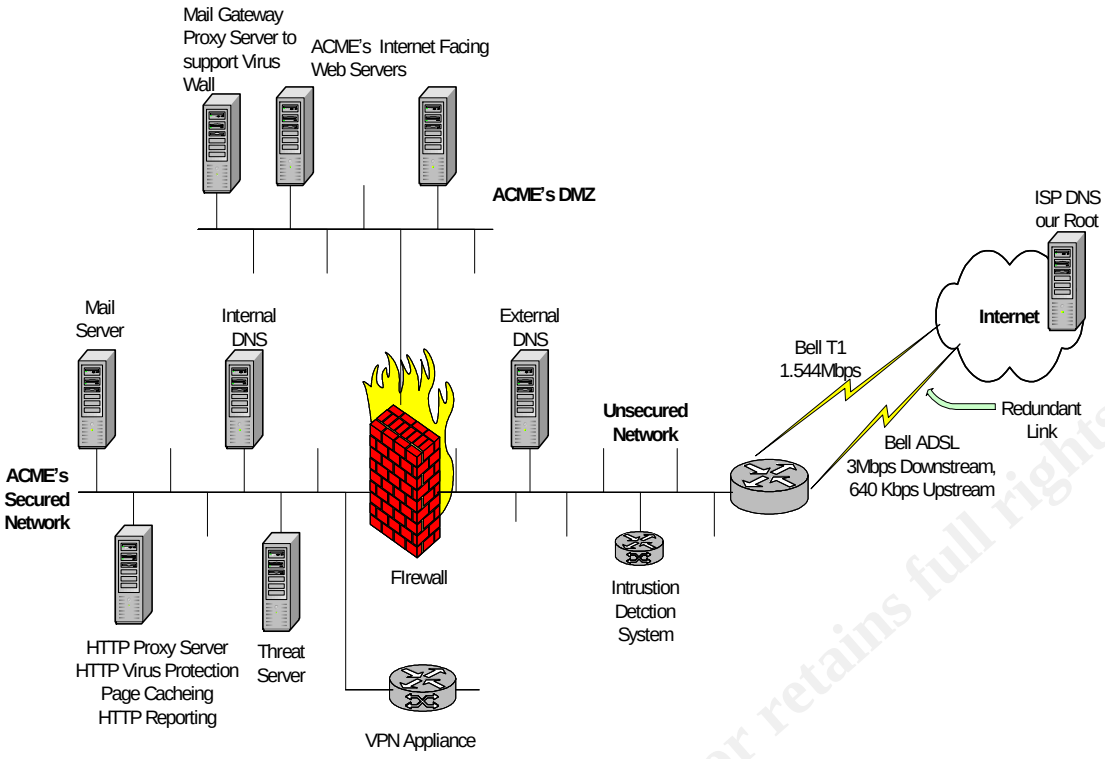


Figure 6: High Level Internet Architecture

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

New External Connections Architecture

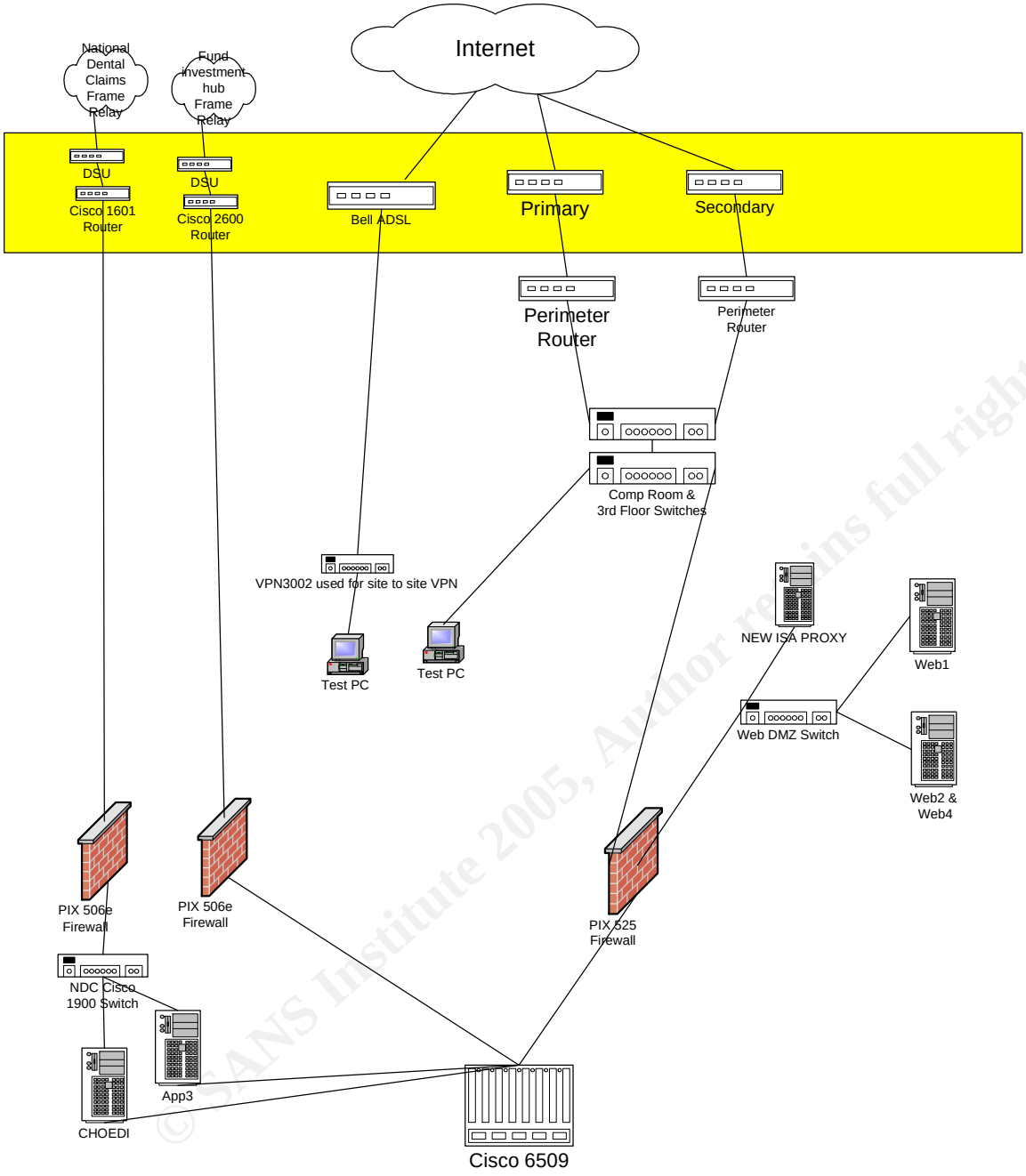


Figure 7: New External Connections Architecture

© SANS Institute 2005, Author retains full rights.

Enterprise Information Systems Security Architecture Framework

The Enterprise IT framework, as depicted below, shows the position of the Enterprise Security Architecture Framework in relation to all other architectures.

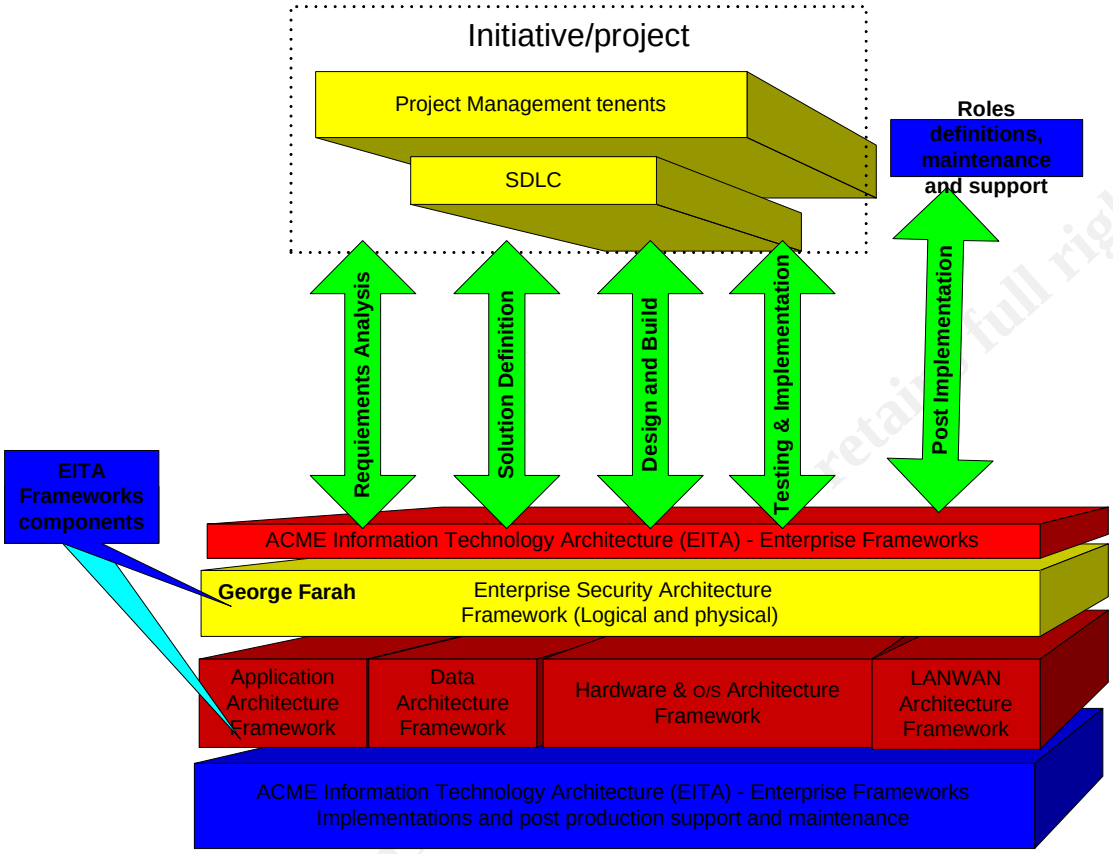


Figure 8: Enterprise Information Systems Architecture

© SANS Institute 2005, Author retains full rights.

Figure 9 below describes the details of the logical enterprise security architecture framework. Each component represents an operational entity that requires policy, standards, and procedures.

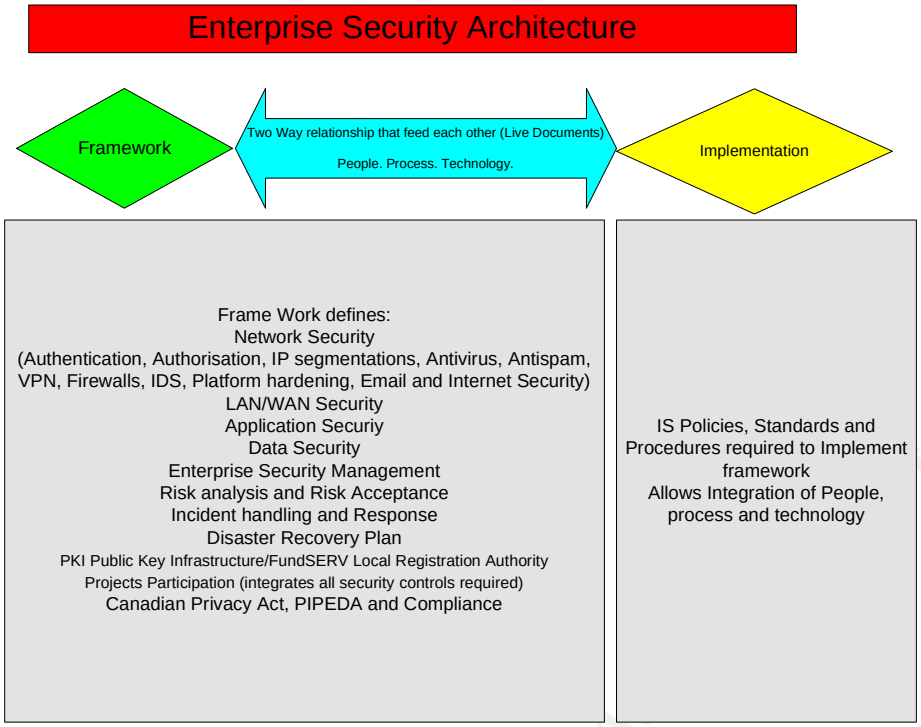


Figure 9: Enterprise Information Systems Security Architecture (Enterprise Security Architecture)

Phase 3: Construction of Policies and Procedures

During this phase policies and procedures were written and updated to regulate the above components of the Enterprise Security Architecture. This task can be done while developing the architecture framework itself. Some policies can be developed at or near the conclusion of a certain assessment. A sample of policies that support the framework is provided below.

1. Local Area Network Security (LAN)

LAN policy emphasized central control of all LAN ports and stipulated authorization for any new connection by the network manager who became accountable to all new ports. Authorization forms were developed for that purpose. Policy also stipulated

© SANS Institute 2005, Author retains full rights.

authorization of any laptops brought by external vendors or contractors to make sure they are checked for viruses, malware and spyware before they are connected to the LAN. An NT domain group was created for contractors who only needed access to the Internet and configured proxy to allow http access. Authorization was required for any additional routers and firewalls ACLs. Every router and switch must have a user name and password to challenge any Telnet access attempt.

1. Incident Handling and Response Team

The IS security manager was added to the team involved with critical escalation of technical and security issues. Security escalation procedures were integrated into existing procedures. The new escalation procedure defined time thresholds, reporting and team structure for making decisions when security issues occur. The incident response process detailed needed resources, responsibilities, and defined communication channels with higher management.

2. New Antivirus Policy

New policy enforced daily updates of virus signatures on the antivirus gateway server, automated push of scan engine updates, and virus signature updates to all workstations. Login script was modified to start antivirus scan at login. While email and attachments were already being scanned, the new policy enforced http/ftp scans on the http/ftp traffic. The upgrade of antivirus package and the upgrade in hardware to greater horsepower allow for the new level of scanning without impacting Internet performance.

Phase 4: Implementation of Target Designs

My role involved the following:

1. Providing the desired security configurations of systems and software required for installing all new hardware and software.

2. Providing all security policies, standards and procedures for application, data, and infrastructure architectures.

Implementation of target architectures began once all architectural changes were defined. New projects were initiated with the infrastructure manager to obtain the necessary approvals and budget allocation. Project plans and timelines for implementation were developed with infrastructure manager. Implementation involved the following:

1. Presenting the new physical and logical architectures to senior management to obtain approval on required changes, involve them in the decision-making process, and discuss budget requirements.
2. Implementing the desired network architecture involved consultation with the technical infrastructure manager and staff about required system configurations.

© SANS Institute 2005, Author retains full rights.

3. Providing the new ISA server security documents containing configurations of new MS ISA server, antivirus and antispam software.

4. Participating with network manager to add a new Cisco PIX firewall between National Dental Claim and dental claims system for group insurance.

5. Writing policies, standards and procedures required for target enterprise information systems security architecture.

Target Application Security Architecture

The target application security architecture outlines guidelines and security controls required by the new policy (p. 22)**.** All identified regular changes requiring security controls on applications related to identity management were introduced through change management.

Target Data Security Architecture

Target data security architecture was borne out of recommendations from initial assessments, leading to the development of a new policy (p. 25). Data protection controls based on value of data and its importance are introduced in the policy and the design of databases. This became part of enterprise security architecture.

Target Disaster Recovery Plan

The DRP was headed by the operations manager. The role of IS security was then introduced in the process as a valuator and participant in defining acceptable security procedures. Upon completing the DRP assessment, procedures were introduced to erase all data on Mainframe, Unix, Windows, and Cisco PIX firewalls and routers. The security architect became an active participant with the DRP team to erase all data. This role constituted a component in the enterprise security architecture described above.

Personal Information and Electronic Documents Act PIPEDA

As a result of assessment, several policies were developed. The security architecture now has privacy compliance as one of its components.

Security Administration

Recommendations mentioned in the security administration assessment (p. 30) were implemented, making the security department responsible for security access control processes for the organization. As a result, security administration became a component in the enterprise security architecture.

© SANS Institute 2005, Author retains full rights.

Phase 5: Integration of Security Practices to Maintain Secure Status

In order to maintain the security and integrity of all IT architectures, IS security involvement was defined. Review of all changes on systems, network, architecture projects, new projects, and privacy-related issues became part of the role of the security architect.

I integrated security sign off in two major areas:

1. Change management process

2. Project management methodology - integrated security in project management life cycle at initial stages in the project definition phases, in JAD sessions, risk analysis phases, project development, and completion phases.

DISCUSSION

The major constraints to introducing security controls were budgetary, resource and time constraints. It is important achieve a balance without compromising important security controls.

Advice to colleagues:

1. Always remember to secure senior management support for security changes.

2. Never assume that people understand security concepts or believe in their applicability.

3. The security architecture you are developing should be borne out of existing IT structure elements and geared toward future directions.

4. Always start with existing corporate policies. If there are none, develop your own and obtain senior management support.

5. People can be resistant to change. It is important to convince people of the value of your work

6. Educate company employees of security policies and articulate their value so that people can adopt them and be mindful of them, otherwise, they will end up on paper only.

7. Keep up-to-date with new technology solutions.

© SANS Institute 2005, Author retains full rights.

CONCLUSION

This paper describes a novel methodology for developing security architecture, which was developed through my experience as a security architect and practitioner. The approach consists of five phases that are best followed in sequence but can accomplished in parallel. In the case study provided, the steps are illustrated as they were implemented in an insurance and investment company that was lacking a security architecture.

The first phase involves conducting security assessments to gather information, attain assessment results and develop recommendations that detail requirements for security architecture. The second phase is the formulation of target architecture designs for both logical and physical architectures. It constitutes the skeleton for the target architecture. The third phase is the development of policies, standards and procedures, which add form and are necessary for implementation and operations of security architecture.

The fourth phase involves implementing the desired security architecture in relation to all other architectures within the environment. The fifth phase is the maintenance of the security architecture. It involves definition of the role of the security architect and integration of security practices into company processes such as change management and project management methodology.

Through this approach, new security architecture resolved security issues with the development of new Internet, perimeter and external connections able to handle identified threats. With this model, security becomes a process based on developed policies, standards and procedures related to identified security components. Security is a mindset and education is of crucial importance to impact on practice.

It is my hope that this paper proves to be helpful to my colleagues as they endeavour to develop and implement IT security architecture in their practice.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

WORKS CITED

Arconati, Nick. “One Approach to Enterprise Security Architecture.” 14 Mar. 2002. SANS Information Security Reading Room. SANS Institute. 7 Sept. 2004. <http://www.sans.org/rr/policy/approach.php>

Harris, Shon. CISSP Certification: Exam Guide. New York: McGraw-Hill/Osborne, 2002.

Info-Tech Research Group. ISO 17799: A Standard for Information Security Management. London, ON: Info-Tech, 2003.

Johnston, John David. "Architecting, Designing and Building a Secure Information Technology Infrastructure: A Case Study.” 24 Aug. 2003. SANS Information Security Reading Room. SANS Institute. 9 Sept. 2004. <http://www.giac.org/practical/GSEC/John_Johnston_GSEC.pdf>

King, Christopher, M., Curtis E. Dalton, and T. Ertem Osmanoglu. Security Architecture: Design, Deployment & Operations. New York: Osborne/McGraw-Hill, 2001.

Krutz, Ronald L., and Russell Dean Vines. CISSP Prep Guide: Mastering the Ten Domains of Computer Security. New York: Wiley, 2001.

Ramachandran, Jay. Designing Security Architecture Solutions. New York: Wiley, 2002.

Kepner-Tregoe. 2003. Kepner-Tregoe Inc. 9 Sept. 2004. <http://www.kepner-tregoe.com>

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. “Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30. Oct. 2001. National Institute of Standards and Technology. 9 Sept. 2004. <http://www.tarrani.net/InfoSysRiskManagement.pdf>

Source for Developers. 2004. Sun Microsystems. 9 Sept. 2004. <http://developers.sun.com/techtopics/security/index.html>

National Security Agency/Central Security Service. 7 Sept. 2004. <http://www.nsa.gov/about/index.cfm>

National Institute of Standards and Technology. 2 Aug. 2004. National Institute of Standards and Technology. 7 Sept. 2004. <http://www.nist.gov/public_affairs/general2.htm>

© SANS Institute 2005, Author retains full rights.

Appendix A

Security Assessment template**:**

Security assessments	
Results	
Recommendations	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix B
Kyberpass configuration file and scan results

Configuration file:

Proxy Type	Proxy In Address		Server	Policies	Type
Certificate Manager P...	X.Z.2.18:7070			Logon Authentication	CERT
Ms Network Proxy	G.T.166.12:139	External	X.Z.3.4:139	Full Packet Encryption	MSNet
Ms Network Proxy	G.T.166.12:239	External	X.Z.3.4:139	Full Packet Encryption	MSNet
Generic Proxy	G.T.166.12:4631	External	X.Z.2.12:4631	Full Packet Encryption	PCA
Generic Proxy	G.T.166.12:5631	External	X.Z.3.4:5631	Logon Authentication	PCA
Certificate Manager P...	G.T.166.12:7070	External		Logon Authentication	CERT
Generic Proxy	G.T.166.200:5631	External_CHOSQLPR1	X.Z.2.13:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.201:23	External_EMPDG	X.Z.20.2:23	Full Packet Encryption	Telnet
Generic Proxy	G.T.166.203:5631	External_CHOSQLPL3	X.Z.2.15:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.204:21	External_CHO_MAIN_SERVER	X.Z.3.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.204:5631	External_CHO_MAIN_SERVER	X.Z.3.1:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.205:21	External_ESTON_SERVER	X.Z.2.7:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.206:21	External_QHO_MAIN_SERVER	X.Z.23.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.206:5631	External_QHO_MAIN_SERVER	X.Z.23.1:5631	Logon Authentication	PCA

© SANS Institute 2005, Author retains full rights.

Generic Proxy	G.T.166.200:21	External_ MTLRS_ SERVER	X.Z.36.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.208:21	External_ MLSLA_S ERVER	X.Z.35.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.209:21	External_ 3QDIS_S ERVER	X.Z.37.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.210:23	External_ CHOMFD V1	X.Z.3.2	Full Packet Encryption	Telne t
Generic Proxy	G.T.166.210:87	External_ CHOMFD V1	X.Z.3.2	Full Packet Encryption	TTY
Generic Proxy	G.T.166.211:21	External_ TORINV_ SERVER	X.Z.20.3:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.211:5631	External_ TORINV_ SERVER	X.Z.20.3:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.212:21	External_ TOCOL_ SERVER	X.Z.31.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.212:5631	External_ TOCOL_ SERVER	X.Z.31.1:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.213:21	External_ TO_SER VER	X.Z.39.1:21	Full Packer Encryption	FTP
Generic Proxy	G.T.166.214:21	External_ TOD_SE RVER	X.Z.32.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.215:21	External_ NIA_SER VER	X.Z.33.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.216:5631	External_ EBSVR	X.Z.41.1:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.217:21	External_ PRC_SE RVER	X.Z.29.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.218:5631	External_ SGR	X.Z.8.84:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.219:21	External_ VAB_SE RVER	X.Z.26.1:21	Full Packet Encryption	FTP

© SANS Institute 2005, Author retains full rights.

	G.T.166.220				
Generic Proxy	G.T.166.221:21	External_ EBLAN2	X.Z.3.11:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.221:23	External_ EBLAN2	X.Z.3.11:23	Full Packet Encryption	Telne t
Generic Proxy	G.T.166.221:2025	External_ EBLAN2	X.Z.3.11:2025	Full Packet Encryption	SYB
Generic Proxy	G.T.166.222:23	External_ ENTLAN1	X.Z.2.1:23	Full Packet Encryption	Telne t
Generic Proxy	G.T.166.222:2025	External_ ENTLAN1	X.Z.2.1:2025	Full Packet Encryption	SYB
Generic Proxy	G.T.166.223:21	External_ ENTAVE 1	X.Z.2.5:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.223:23	External_ ENTAVE 1	X.Z.2.5:23	Full Packet Encryption	Telne t
Generic Proxy	G.T.166.224:21	External_ GRP_SE RVER	X.Z.24.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.225:21	External_ GRPL_S ERVER	X.Z.21.1:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.226:21	External_ GRN_SE RVER	X.Z.22.2:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.227:21	External_ CHOMFS VR1	X.Z.1.2:21	Full Packet Encryption	FTP
Generic Proxy	G.T.166.227:87		X.Z.1.2:87	Full Packet Encryption	TTY
Generic Proxy	G.T.166.228:23	External_ C_MAINF RAME	X.Z.1.2:23	Full Packet Encryption	Telne t
Generic Proxy	G.T.166.229:23	External_ SUNSTA G1	X.Z.2.3:23	Packet Authentication	Telne t
Generic Proxy	G.T.166.230:5631	External_ STA_SE RVER	X.Z.5.1:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.231:5631	External_ ASTE	X.Z.8.161:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.232:5631	External_ CHOSQL PL4	X.Z.2.17:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.233:5631	External_	X.Z.8.97:5631	Logon	PCA

© SANS Institute 2005, Author retains full rights.

		JF		Authentication	
Generic Proxy	G.T.166.234:5631	External_DC	X.Z.8.98:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.235:5631	External_PJ	X.Z.8.99:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.236:5631	External_CHOSQLPL2	X.Z.2.14:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.237:5631	External_CHOTECHSVR1	X.Z.10.1:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.238:5631	External_p	X.Z.8.96:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.239	External_CHOIST1SVR	X.Z.2.9:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.240	External_CHOIUA1SVR	X.Z.8.169:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.241	External_MB	X.Z.8.90:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.242	External_CPR	X.Z.8.93:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.243	External_ISO	X.Z.8.86:5631	Logon Authentication	PCA
Generic Proxy	G.T.166.244	External_pcAGateway	X.Z.8.85:5631	Logon Authentication	PCA

Vulnerability Scan Results:

Scan target: X.Z.2.18 [1 computers found]

IP Address Details Hostname Username Operating System
X.Z.2.18 [ ] Windows 9x/XP
  IP Address : X.Z.2.18
  Operating System : Windows 9x/XP
  Time to live : 128
  TCP ports - 2 open ports
        139 [Netbios-ssn => NETBIOS Session Service]

        135 [epmap => DCE endpoint resolution]

External Interface showed the following results:

© SANS Institute 2005, Author retains full rights.

```
Scan target : G.T.166.12 [ 1 computers found ]
--------------------------------------------------------------------------------
IP Address Details Hostname Username Operating System
G.T.166.12         undetermined

G.T.166.12 [ ]  undetermined
  IP Address : G.T.166.12
  Operating System : undetermined
  Time to live : 0
   TCP ports - 1 open ports
        5631 [ pcANYWHEREdata => Remote Control Software ]
 220 KyberPASS
    UDP ports - 7 open ports
        67 [ bootps => Bootstrap Protocol Server ]
        69 [ TFTP => Trivial File Transfer Protocol ]
        135 [ epmap => DCE endpoint resolution ]
        137 [ Netbios-NS => Netbios Name Service ]
        138 [ Netbios-DGM => Netbios Datagram Service ]
        445 [ Microsoft CIFS => Common Internet File System ]
        1434 [ ms-sql-m => Microsoft SQL Monitor ]
  Alerts
     Service alerts
   Trivial FTP service running
 Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable
file. You should remove this service, unless you really need it.
http://www.cert.org/tech_tips/usc20_full.html#2.17
```

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix C

Cisco 506e Firewall connection with another fund company: Configuration file:

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password VStNDcDirpEb5DVg encrypted
passwd RnDlqNZhQ8hpCaBc encrypted
Hostname Fundfire
Fix protocol ftp 21
Fix protocol h323 h225 1720
fix protocol h323 RAS 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list acl_out permit tcp host X.Y.10.35 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.35 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.35 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.35 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.35 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.35 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.36 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.36 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.36 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.36 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.36 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.36 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.56 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.56 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.56 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.56 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.56 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.56 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.57 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.57 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.57 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.57 host L.M.254.5 eq ftp
```


© SANS Institute 2005, Author retains full rights.

```
access-list acl_out permit tcp host X.Y.10.57 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.57 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.59 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.59 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.59 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.59 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.59 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.59 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.69 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.69 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.69 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.69 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.69 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.69 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.73 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.73 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.73 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.73 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.73 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.73 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.74 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.74 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.74 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.74 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.74 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.74 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.76 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.76 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.76 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.76 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.76 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.76 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.77 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.77 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.77 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.77 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.77 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.77 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.85 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.85 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.85 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.85 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.85 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.85 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.98 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.98 host L.M.254.4 eq ftp
```


© SANS Institute 2005, Author retains full rights.

```
access-list acl_out permit tcp host X.Y.10.98 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.98 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.98 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.98 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.101 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.101 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.101 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.101 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.101 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.101 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.120 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.120 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.120 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.120 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.120 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.120 host L.M.254.6 eq ftp
access-list acl_out permit tcp host X.Y.10.123 host L.M.254.4 eq 4446
access-list acl_out permit tcp host X.Y.10.123 host L.M.254.4 eq ftp
access-list acl_out permit tcp host X.Y.10.123 host L.M.254.5 eq 4446
access-list acl_out permit tcp host X.Y.10.123 host L.M.254.5 eq ftp
access-list acl_out permit tcp host X.Y.10.123 host L.M.254.6 eq 4446
access-list acl_out permit tcp host X.Y.10.123 host L.M.254.6 eq ftp
pager lines 24
logging on
logging buffered debugging
logging trap debugging
logging history debugging
logging facility 23
logging host inside X.Z.3.9
logging host inside X.Z.3.25
icmp deny any outside
mtu outside 1500
mtu inside 1500
ip address outside L.M.254.2 255.255.255.0
ip address inside X.Z.100.9 255.255.0.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 L.M.254.3 netmask 255.255.255.0
nat (inside) 1 X.Z.0.0 255.0.0.0 0 0
static (inside,outside) L.M.254.4 X.Z.2.40 netmask 255.255.255.255 0 0
static (inside,outside) L.M.254.5 X.Z.254.50 netmask 255.255.255.255 0 0
static (inside,outside) L.M.254.6 X.Z.254.51 netmask 255.255.255.255 0 0
access-group acl_out in interface outside
route outside X.Y.10.0 255.255.255.0 L.M.254.1 1
```


© SANS Institute 2005, Author retains full rights.

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host inside X.Z.3.9
no snmp-server location
no snmp-server contact
snmp-server community quartz7
snmp-server enable traps
floodguard enable
telnet X.Z.0.0 255.255.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:9e24565385689d9436d96d7a7160274c
: end
```

Scan results of internal interface:

```
Scan target : X.Z.100.9 [ 1 computers found ]
-------------------------------------------------------------------------------
IP Address Details Hostname Username Operating System
X.Z.100.9

X.Z.100.9 [ ]
  IP Address : X.Z.100.9
  Operating System : Cisco Pix
  Time to live : 255
   TCP ports - 1 open ports
        23 [ Telnet => Remote Login Protocol ]
User Access Verification
Password:
   Alerts
     Service alerts
Telnet service is running
 This service is dangerous because it doesn't encrypt data. Sensitive information
(usernames+passwords) can be sniffed. If possible use SSH instead.
```


© SANS Institute 2005, Author retains full rights.

Appendix D

Cisco PIX 506 configuration file (Connection with sister company):

```
pixfirewall# wr t
Building configuration...
: Saved
:
PIX Version 5.3(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password VStNDcDirpEb5DVg encrypted
passwd RnDlqNZhQ8hpCaBc encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 101 permit icmp host L.M.1.3 any echo
access-list 101 permit icmp host L.M.1.2 any echo
no pager
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered debugging
logging trap debugging
logging history debugging
logging facility 23
logging queue 512
logging host inside X.Z.3.9
logging host inside X.Z.3.25
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside L.M.1.1 255.255.255.0
ip address inside X.Z.20.110 255.255.0.0
ip audit info action alarm
ip audit attack action alarm
arp timeout 14400
```


© SANS Institute 2005, Author retains full rights.

```
nat (inside) 0 X.Z.0.0 255.255.0.0 0 0
static (inside,outside) X.Z.0.0 X.Z0.0.0 netmask 255.255.0.0 0 0
access-group 101 in interface outside
route inside X.Z.0.0 255.255.0.0 X.Z0.20.18 1
route outside H.N.176.0 255.255.248.0 L.M.1.2 1
route outside H.N.184.0 255.255.254.0 L.M.1.2 1
route outside M.S.246.0 255.255.255.0 L.M.1.2 1
route outside A.B.161.0 255.255.255.0 L.M.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
snmp-server host inside X.Z.3.9
no snmp-server location
no snmp-server contact
snmp-server community quartz7
snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet X.Z.0.0 255.255.0.0 inside
telnet X.Z.0.0 255.255.0.0 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:fe1478c3c6f436ccdcfc123f6989099d
: end
[OK]
```

Scan results of internal interface:

```
Scan target : X.Z.20.110 [ 1 computers found ]
-------------------------------------------------------------------------------
IP Address Details Hostname Username Operating System
X.Z.20.110 [ ]
  IP Address : X.Z.20.110
  Operating System : probably Unix
  Time to live : 255
   TCP ports - 1 open ports
        23 [ Telnet => Remote Login Protocol ]
   Alerts
     Service alerts
   Telnet service is running
 This service is dangerous because it doesn't encrypt data. Sensitive information
(usernames+passwords) can be sniffed. If possible use SSH instead.
```


© SANS Institute 2005, Author retains full rights.

Appendix E

Security Assessments Questions:
Is system up to date with patches?
What ports are open?
Are the open ports needed?
What services are open and why?
Firewall Rule set analysis?
Is the device positioned correctly in the network?
What are all secure and non-secure interfaces?
What is the history of the device
Is there a process for making aqny changes?
Who is responsible for creating accounts, deleting accounts?
Are the logs being checked?
Who is responsible for reviewing the logs?

Proxy servers questions:
Is system up to date with patches?
What ports are open?
What services are open and why?
Is the position in the network correct?
What is the company's internet policy?
IS firewall module turned on?
Was http traffic being scanned for antivirus?
What is the latest spam list updates?
how are we doing updates and stopping Spam? And how often?

Extra questions related to VPN 3030:
What are Configurations of Cisco security profiles used by users to access the network?
What is VPN implementation policy?
What is the distribution policy?
Who qualifies to get VPN access and what controls need to be on every PC?

Questions related to 3COM modem pool:
What is the connection diagram, and phone numbers?
How is it positioned in the network?
What is the device configuration?
What is the authentication method used?
What is the policy around its use?
Who uses and is authorized to use it?
Why is it needed?
How does someone obtain an IP address once connected?

WAN devices related questions:
What types of logs can we get from our provider as per our contract with them?
What type of monitoring they have for the connections?

© SANS Institute 2005, Author retains full rights.

Can we do any type of vulnerability scans on these devices?
Can we get the routing tables?

LAN security related questions:
What is the layout of cabling and devices?
What are the standards of cables used?
What is the network topology?
What is the main network connection from mainframe to client server environment (through IBM router 2216)?
What types of routers, hubs and switches are used?
Do they have user name and password to access?
Is change management used when changing routers or switch configurations?
Who approves these changes?
What is the policy regarding connecting to LAN?
What is the policy regarding activating ports?
Who has access to physical space?
Is there a policy for connecting external vendors to the LAN?
Is physical security practiced properly for accessing premises and process for activating and deactivating badges, LAN ports and LAN connection drops?

Cisco IDS 4210 Assessment questions:
where is the device positioned?
is it up to date with software updates and attack signatures?
Do we understand the traffic we are trying to detect coming to our DMZ or external and internal network?
Has the device been positioned in different places on the network to understand the type of traffic we can detect?
What is the configuration of the device?
Is it configured to send an alarm to network administrator?

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix F

Cisco PIX 525 Scan results of internal interface:

Scan target : X.Z.100.4 [1 computers found]

IP Address Details Hostname Username Operating System
X.Z.100.4 probably Unix

X.Z.100.4 [ ] probably Unix
IP Address : X.Z.100.4
Operating System : probably Unix
Time to live : 255

TCP ports - 1 open ports
23 [Telnet => Remote Login Protocol]
password
Alerts
Service alerts
Telnet service is running
This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

Cisco PIX 525 Scan results of external interface:
scan target : G.T.166.12 [1 computers found]

IP Address Details Hostname Username Operating System
G.T.166.12 undetermined

G.T.166.12 [ ] undetermined
IP Address : G.T.166.12
Operating System : undetermined
Time to live : 0
TCP ports - 1 open ports
5631 [pcANYWHEREdata => Remote Control Software]
220 KyberPASS
UDP ports - 6 open ports
69 [TFTP => Trivial File Transfer Protocol]
135 [epmap => DCE endpoint resolution]
137 [Netbios-NS => Netbios Name Service]
138 [Netbios-DGM => Netbios Datagram Service]
445 [Microsoft CIFS => Common Internet File System]
1434 [ms-sql-m => Microsoft SQL Monitor]
Alerts
Service alerts
Trivial FTP service running

© SANS Institute 2005, Author retains full rights.

Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable file. You should remove this service, unless you really need it.
http://www.cert.org/tech_tips/usc20_full.html#2.17

Cisco Pix 525 Firewall Configuration file: used at head office:

```
PIX passwd:

Welcome to the PIX firewall

Type help or '?' for a list of available commands.
pix_empire> en
Password: *******
pix_empire# wr t
Building configuration...
: Saved
:
PIX Version 5.2(5)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
enable password VStNDcDirpEb5DVggg encrypted
passwd RnDlqNZhQ8hpCaBc encrypted
hostname pix_empire
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list acl_out permit tcp any host C.D.179.250 eq www
access-list acl_out permit tcp any host C.D.179.251 eq www
access-list acl_out permit tcp any host C.D.179.250 eq 443
access-list acl_out permit tcp any host C.D.179.251 eq 443
access-list acl_out permit tcp any host C.D.179.251 eq 442
access-list acl_out permit tcp any host C.D.179.249 eq www
access-list acl_out permit tcp any host C.D.179.249 eq 443
access-list acl_out permit tcp any host C.D.179.249 eq 442
access-list acl_dmz permit tcp E.F.254.0 255.255.255.0 any eq www
access-list acl_dmz permit udp E.F.254.0 255.255.255.0 any eq domain
access-list acl_dmz permit tcp host E.F.254.3 host E.F.254.200 eq 8993
```


© SANS Institute 2005, Author retains full rights.

```
access-list acl_dmz permit tcp host E.F.254.3 host E.F.254.200 eq 8081
access-list acl_dmz permit tcp host E.F.254.2 host E.F.254.201 eq 1433
access-list acl_dmz permit tcp host E.F.254.4 host E.F.254.200 eq 8993
access-list acl_dmz permit tcp host E.F.254.4 host E.F.254.200 eq 8081
access-list acl_dmz permit tcp host E.F.254.3 host E.F.254.200 eq 9094
access-list acl_dmz permit tcp host E.F.254.4 host E.F.254.200 eq 9094
no pager
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered debugging
logging trap debugging
logging history debugging
logging facility 23
logging queue 512
logging host inside X.Z.3.9
logging host inside X.Z.3.25
interface ethernet0 auto
interface ethernet1 100full
interface ethernet2 auto
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside C.D.179.230 255.255.255.0
ip address inside X.Z.100.4 255.255.0.0
ip address dmz E.F.254.1 255.255.255.0
ip address intf3 L.M.0.1 255.255.255.255
ip address intf4 L.M.0.1 255.255.255.255
ip address intf5 L.M.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
arp timeout 14400
global (outside) 1 C.D.179.231 netmask 255.255.255.0
global (dmz) 1 E.F.254.254 netmask 255.255.255.0
nat (inside) 1 X.Z.0.0 255.0.0.0 0 0
nat (dmz) 1 E.F.254.0 255.255.255.0 0 0
static (dmz,outside) C.D.179.251 E.F.254.3 netmask 255.255.255.255 0 0
static (inside,dmz) E.F.254.200 X.Z.3.32 netmask 255.255.255.255 0 0
```


© SANS Institute 2005, Author retains full rights.

```
static (dmz,outside) C.D.179.250 E.F.254.2 netmask 255.255.255.255 0 0
static (inside,dmz) E.F.254.201 X.Z.2.13 netmask 255.255.255.255 0 0
static (dmz,outside) C.D.179.249 E.F.254.4 netmask 255.255.255.255 0 0
access-group acl_out in interface outside
access-group acl_dmz in interface dmz
route outside 0.0.0.0 0.0.0.0 C.D.179.1 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
route inside X.Z.0.0 255.255.0.0 X.Z.100.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
snmp-server host inside X.Z.3.9
no snmp-server location
no snmp-server contact
snmp-server community quartz7
snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet X.Z.0.0 255.0.0.0 inside
telnet timeout 30
ssh timeout 5
terminal width 80
Cryptochecksum:39fbd9769d71c809e88962fb53a23c6c555V
: end
[OK]
```


© SANS Institute 2005, Author retains full rights.

Appendix G

MS proxy 2.0 Internet system Scan results of external public interface:

```
Scan target : G.T.166.254 [ 1 computers found ]
-------------------------------------------------------------------------------
IP Address Details Hostname Username Operating System
G.T.166.254      WWWSVR    Windows 2000
G.T.166.254 [ WWWSVR ]  Windows 2000
  IP Address : G.T.166.254
  Hostname : WWWSVR
  Operating System : Windows 2000
  Time to live : 0
  SNMP info (system)
     sysDescr - Hardware: x86 Family 15 Model 2 Stepping 9 AT/AT COMPATIBLE -
Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)
     sysUpTime - 56 days, 5 hours, 20 minutes, 36 seconds
     sysName - webserver
     Object ID - 1.3.6.1.4.1.311.1.1.3.1.2.3.2.6.5 (NT Server)
     Vendor - Microsoft
    TCP ports - 6 open ports
         21 [ Ftp => File Transfer Protocol ]
 220 wwwsvr Microsoft FTP Service (Version 5.0).
          25 [ Smtp => Simple Mail Transfer Protocol ]
 220 wwwsvr.ACME.ca Micro InterScan Messaging Security Suite, Version: 5.5 (build
1141) ready at Fri, 06 Aug 2004 13:46:01 -0400
          80 [ Http => World Wide Web, HTTP ]
 HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 06 Aug 2004 17:46:07 GMT
Content-Type: text/html
Content-Length: 87
          119 [ News ]
 200 NNTP Service 5.00.0984 Version: 5.0.2195.6702 Posting Allowed
          443 [ HttpS => Secure HTTP ]
          3389 [ Terminal Services ]
    UDP ports - 8 open ports
         67 [ bootps => Bootstrap Protocol Server ]
         69 [ TFTP => Trivial File Transfer Protocol ]
         135 [ epmap => DCE endpoint resolution ]
         137 [ Netbios-NS => Netbios Name Service ]
         138 [ Netbios-DGM => Netbios Datagram Service ]
         161 [ SNMP => Simple Network Management Protocol ]
         445 [ Microsoft CIFS => Common Internet File System ]
         1434 [ ms-sql-m => Microsoft SQL Monitor ]
   Alerts
```


© SANS Institute 2005, Author retains full rights.

CGI abuses
Frontpage check (1)
Frontpage extensions are installed on this computer
Frontpage check (2)
Some versions of Frontpage are vulnerable to denial of service attacks
http://www.securityfocus.com/bid/1608
Frontpage check (3)
Some versions of Frontpage are vulnerable to denial of service attacks
http://www.securityfocus.com/bid/1608
Service alerts
SNMP service is enabled on this host
Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. You should check if your system is vulnerable.
http://www.cert.org/advisories/CA-2002-03.html
Trivial FTP service running
Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable file. You should remove this service, unless you really need it.
http://www.cert.org/tech_tips/usc20_full.html#2.17

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix H

Cisco VPN 3030

Scan results of internal (secure) Interface of VPN concentrator 3030:

```
Scan target : X.Z.100.5 [ 1 computers found ]
-------------------------------------------------------------------------------
IP Address Details Hostname Username Operating System
X.Z.100.5        probably Unix
X.Z.100.5 [ ]  probably Unix
  IP Address : X.Z.100.5
  Operating System : probably Unix
  Time to live : 128
   TCP ports - 4 open ports
         21 [ Ftp => File Transfer Protocol ]
 220 Session will be terminated after 600 seconds of inactivity.
         23 [ Telnet => Remote Login Protocol ]
 Login:
         80 [ Http => World Wide Web, HTTP ]
 HTTP/1.1 400 Bad Request
Server: Virata-EmWeb/R5_3_0
         443 [ HttpS => Secure HTTP ]
   Alerts
     CGI abuses
   Leif M. Wright ad.cgi
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2103
   Aglimpse
 Possible Force the web server to send the password file back to the attacker
http://www.securityfocus.com/bid/2026
   AnyForm2
 Possible Force the web server to send the password file back to the attacker
http://www.securityfocus.com/bid/719
   eXtropia bbs_forum.cgi
 Possible Run arbitrary commands, view files
http://www.securityfocus.com/bid/2177
   Brian Stanback bsguest.cgi
 Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2159
   Brian Stanback bslist.cgi
 Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2160
   NCSA HTTPd campas
 Possible View remote files (web server level privileges)
http://www.securityfocus.com/bid/1975
   iCat Carbo Server File Disclosure
```


© SANS Institute 2005, Author retains full rights.

Possible View known files (web server level privileges)
http://www.securityfocus.com/bid/2126
Count.cgi (wwwcount) Buffer Overflow
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/128
DCScripts cgforum.cgi Arbitrary File Disclosure
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/1951
Hylafax Faxsurvey Remote Command Execution
Possible View remote files, run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2056
gbook.cgi Remote Command Execution
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/1940
ht://dig Arbitrary File Inclusion
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/1026
Miva htmlscript 2.x Directory Traversal
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/2001
JJ sample CGI program Escape Character
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/2002
Technote Inc Technote 'filename' Variable File Disclosure
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/2156
Endymion MailMan Remote Arbitrary Command Execution
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2063
Ibrow newsdesk.cgi File Disclosure
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/2172
Technote Inc Technote 'board' Function File Disclosure
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/2155
ikonboard Arbitrary Command Execution
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2157
Leif M. Wright simplestguest.cgi Remote Command Execution
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2106
OmniHTTPD File Corruption and Command Execution
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2211
WEBgais Remote Command Execution
Possible Run arbitrary commands (web server level privileges)

© SANS Institute 2005, Author retains full rights.

http://www.securityfocus.com/bid/2058
Microsoft IIS 4.0 IISADMPWD Proxied Password Attack
Possible Unauthorized access to your computer
http://www.securityfocus.com/bid/2110
WEBgais Remote Command Execution
Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/2058
Perl.exe
Possible Run perl commands (web server level privileges)
Perl.exe
Possible Run perl commands (web server level privileges)
Perl.exe
Possible Run perl commands (web server level privileges)
SGI InfoSearch fname
Possible Run arbitrary commands (web server level privileges)
http://www.securityfocus.com/bid/1031
Webcom Datakommunikation CGI Guestbook rguest/wguest
Possible View arbitrary files (web server level privileges)
http://www.securityfocus.com/bid/2024
Alex Heiphetz Group EZShopper Directory Disclosure
Possible directory listing , probably view arbitrary files
http://www.securityfocus.com/bid/2109
Merchant Order Form 1.2 Order Log Permissions
Possible view shopping orders
http://www.securityfocus.com/bid/2021
a1stats CGI script _show files_
Possible view arbitrary files
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0561
DCforum allows remote file retrieving and command execution
Possible remote file retrieving and command execution
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1132
nhp-maillist.cgi script
Remote command execution
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0400
Adcycle
Possible Weak authentification
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0425
BBS Forum vulnerability
Possible Remote file retrieving
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-1208
mailnews.cgi
Possible Remote command execution
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0271
newsdesk.cgi
Possible Remote file retrieving
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0231

© SANS Institute 2005, Author retains full rights.

Pals-cgi
Possible Remote file retrieving
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0217
DCShop vulnerability
Possible Retrieve sensitive information
http://www.securityfocus.com/archive/1/191834
get32.exe
Possible Remote command execution
Service alerts
Telnet service is running
This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

Scan results of external Interface of Cisco VPN 3030:
NETBIOS discovery ...
Done sending, waiting for responses ...
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
Ready
No computers found.
Ready

Configurations of VPN device:
VPN device was configured to accept Cisco VPN Client triple DES – MD5 hash and Cisco VPN client AES-128 SHA and IKE Cisco CPN client triple DES –MD5-RSA.
IPSEC was used to establish secure tunnels.
Protocols allowed were:
FTP on port 21
http on port 80 /https on port 443
Telnet and telnet/SSL o poret 992
SNMP was enabled on port 161
SSL was enabled with RC4-128/MD5, 3DES-168/SHA, DES-56/SHA, RC4-40/MD5 Export, DES-40/SHA Export
SSL version 2 and V3 supported
Generated certificate Key size 1024 bit RSA Key
SSH enabled on port 22 using 3DES-168. RC4-128 and DES-56
Enabled SCP secure copy over SSH.
Logging was enabled
Received all security 1-3 issues by email
Syslog servers were receiving logs from VPN device

© SANS Institute 2005, Author retains full rights.

Banner added to Cisco VPN device to appear for eceryone logging in via VPN:

This System is an ACME resource and is for authorized use only. If you are not authorized to access this resource, disconnect now. Unauthorized use of, or access to this resource is strictly prohibited and may subject you to disciplinary action or criminal prosecution. By accessing and using this resource, you are consenting to monitoring, keystroke recording and/or auditing."

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix I

Cisco IDS 4210 Scan Results:

Scan results of intenal interface of IDS**:**
Scan target : X.Z.100.6 [1 computers found]

IP Address Details Hostname Username Operating System
X.Z.100.6 probably Unix

X.Z.100.6 [ ] probably Unix
IP Address : X.Z.100.6
Operating System : probably Unix
Time to live : 64
TCP ports - 2 open ports
22 [Ssh => Remote Login Protocol]
SSH-1.99-OpenSSH_3.7.1p2
443 [HttpS => Secure HTTP]

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix J

LAN Routers and switches scans:

IBM 2216 scan results:
Scan target : X.Z.2.2 [1 computers found]

IP Address Details Hostname Username Operating System
X.Z.2.2 [IBM 2216] IBM
  IP Address : X.Z.2.2
  Hostname : IBM 2216
  Operating System : IBM
  Time to live : 64
  SNMP info (system)
    sysDescr - IBM 2216-400 Multiprotocol Access Services S/N : 57-60669 Level : 2216-MAS Feature 2899 V3.3 Mod 0 PTF 0 RPQ 0 MAS.FF1 cc50_13a Firmware : cc4:BUILD:cc4_32l
    sysUpTime - 237 days, 3 hours, 7 minutes, 3 seconds
    sysContact - Jim French
    sysName - IBM 2216
    sysLocation - Computer Room
    Object ID - 1.3.6.1.4.1.2.6.131.32.36
    Vendor - IBM
   TCP ports - 1 open ports
        23 [Telnet => Remote Login Protocol]
 _____
   Alerts
    Service alerts
   SNMP service is enabled on this host
Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. You should check if your system is vulnerable.
http://www.cert.org/advisories/CA-2002-03.html
   Telnet service is running
 This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

CISCO router 6509 scan results:
Scan target : X.Z.2.16 [1 computers found]

IP Address Details Hostname Username Operating System
X.Z.2.16 [ ] probably Unix
  IP Address : X.Z.2.16 Operating System : probably Unix
  Time to live : 32
   TCP ports - 1 open ports
        23 [Telnet => Remote Login Protocol]

© SANS Institute 2005, Author retains full rights.

NetLogin:
Alerts
Service alerts
Telnet service is running
This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix K

Application Security matrix and assessments:

Application name	***Authentication***	***Authorization***	***Audit***	***Critical System (Low-Medium-High)***	***Administration***
General Ledger	Y	Y	Y	H	Y
Imaging Application	Y	Y	Y	H	Y
Life Insurance Application	Y (Needs controls on password expiry)	Y	Y	H	Y
Portfolio Management application	Y	Does not provide for business need. Requires update	Y	H	Y
Accounting application	Y	Y	Y	H	Y
HR System	Y	Y	Y	H	Y
Employee Benefits Application	Y	Y	Y	H	Y
Employee Benefits Web access (SSL enabled site)	Y	Y	Y	H	Y
Individual Business web sites	Y	Y	Y	H	Y

© SANS Institute 2005, Author retains full rights.

Appendix L

Recommended data classification system:

A - Confidential: Information that is considered very sensitive in nature. Its unauthorised disclosure could seriously and negatively impact the company. Example, Information about new product development, trade secrets, Network diagrams, IP addressing schemes used in the organisation, Application architecture, Source code Programs, etc.

B- Sensitive: Information that requires higher level of classification than normal data. This type of information need to be protected from unauthorised alteration that might cause loss of confidentiality or integrity.

C - Private: Information that is considered of a personal nature, and is intended for company use only, its disclosure could affect company and its employees.

D - Public: Information that is considered neither sensitive nor classified, all of the companies information that doesn't fit in the previous categories can be considered public, This information should not be disclosed, however, if it is disclosed, it is not expected to seriously or adversely impact the company

Once the owner has defined the Classification level of the document, it is their responsibility to make sure that the following is implemented on the document at all times:

1 - Document Classification level explicitly visible on the document at the top or bottom of document (Confidential, Sensitive, so on ...)
2 - Name of Owner or creator of the document
3 - Date Document created
4 - Date document last modified done by any person that modifies the document.

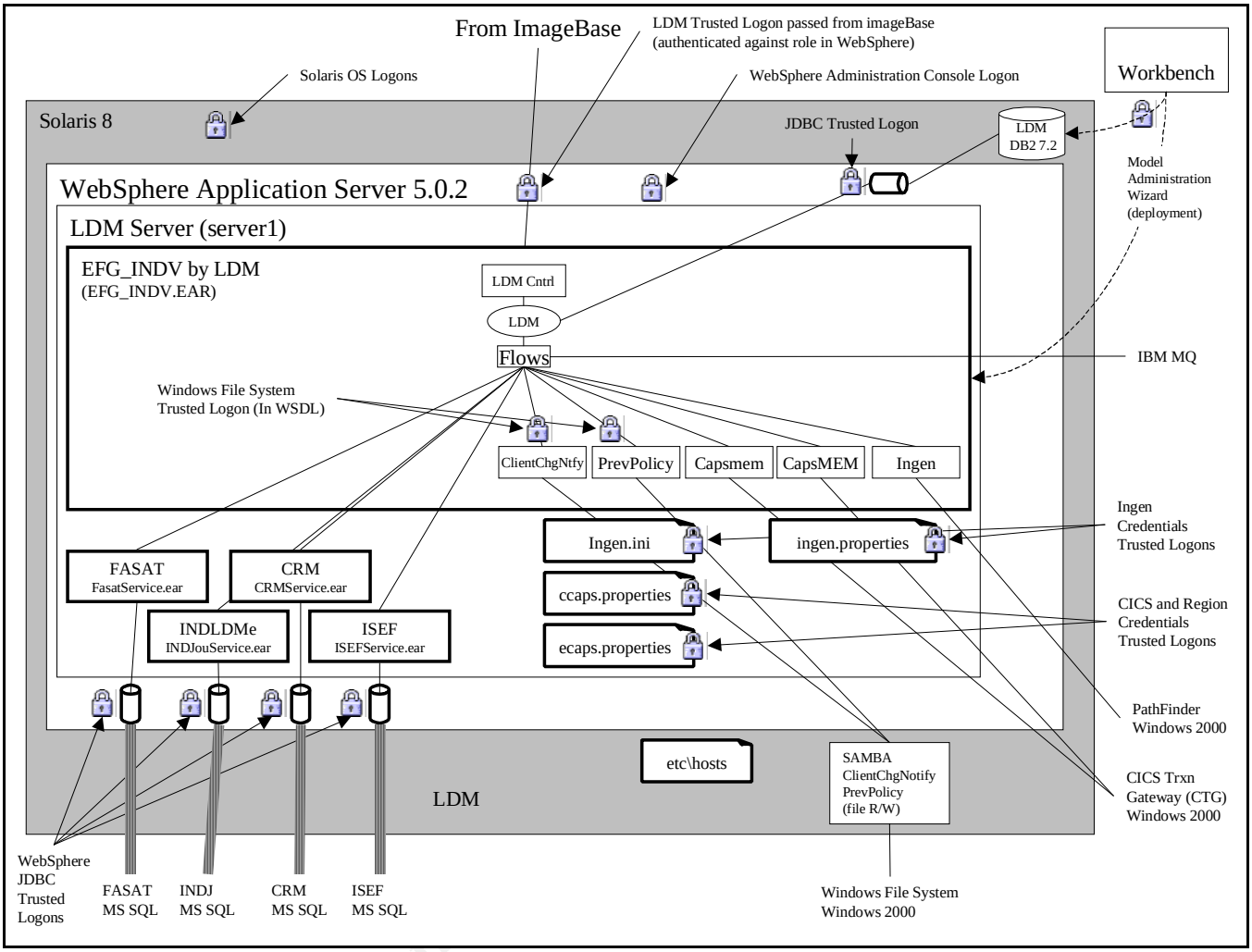
It is also the responsibility of the custodian of the document to maintain any change on the document and indicating last modified date on it.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix M

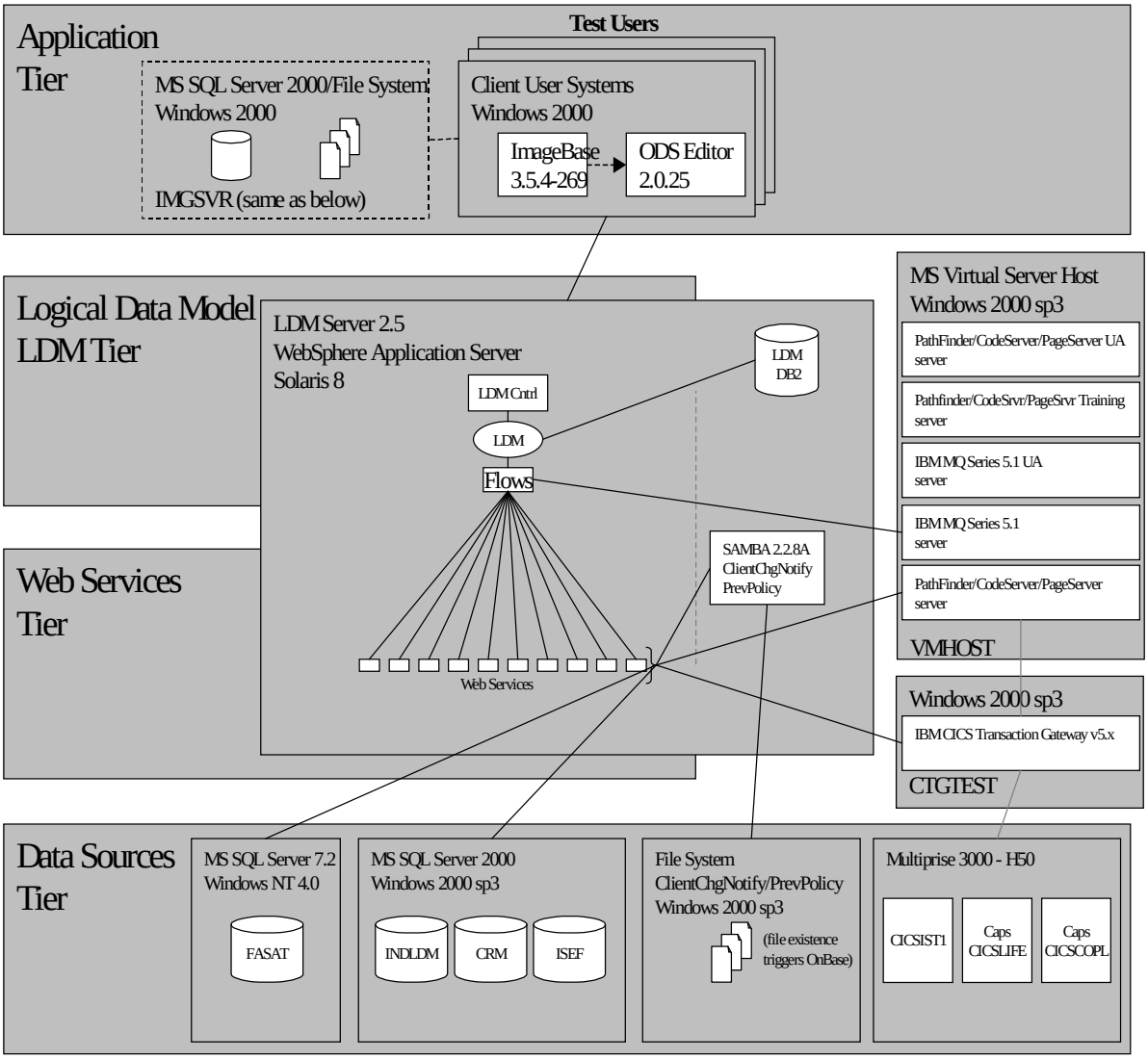
Logical data Model structure leveraging IBM webshere:



© SANS Institute 2005, Author retains full rights.

Appendix N

Logical data Model:



© SANS Institute 2005, Author retains full rights.

Appendix O

Patch management policy for all systems and devices.

Sensitivity of advisory	Network Position	Time Frame for Implementation
Critical Advisories	Internal Network	One week
Critical Advisories	DMZ and External	24 - 48 hours
Moderate Advisories	Internal Networks	Two Weeks
Moderate Advisories	DMZ and External	One week
Low Advisories	Internal Network	Three Weeks to One Month
Low Advisories	DMZ and External	Two Weeks

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix P

System builds security templates:

Windows Security Guidelines:

Operating System Security Guidelines

1. Is system up to date with updates and security patches?
2. Are all the ports and services needed?
2. Is antivirus software installed and running in real time?
3. Are the security guidelines provided by the vendor or NSA being followed in system configurations?
4. Resource sharing protection using NTFS permissions (share Level)
5. Partitioning hard disk for data and system files in two separate partitions
6. Security audit logs need to be configured for all successes and failures and kept for 60 days then archived.
7. Following guidelines and best practices as provided by Microsoft and NSA as fits our architecture.

Unix System Security Guidelines:

UMASK : should be set up the umask value as **022**, execute the **umask 022** command.

IF Global Security Kit is used, the following table lists the directory location of the Global Security Kit (GSKit) installation image files for Websphere plug-ins for Web servers that are running on a distributed platform. The appropriate file must be downloaded to the workstation on which the Web server is running.

install_root/ DownloadPlugins/Solaris/ gsk/gsk5bas.tar.Z_bin

There should be a separate partitions for root /, /usr /var, and /opt. **Is there** ?

No remote root login, every user should login with their user ID and su to root if they need root privileges.

Auditing

1. Enable the Basic Security Module (BSM):
   /etc/security/bsmconv

2. Configure the classes of events to log in /etc/security/audit_control:
   dir:/var/audit
   flags:lo,ad,pc,fc,fd,fm
   naflags:lo,ad
   #
   # lo - login/logout events
   # ad - administrative actions: mount, exportfs, etc.
   # pc - process operations: fork, exec, exit, etc.

© SANS Institute 2005, Author retains full rights.

```
#   fc - file creation
#   fd - file deletion
#   fm - change of object attributes: chown, flock, etc.
```

3. Create /etc/security/newauditlog.sh:

```
#!/sbin/sh
#
# newauditlog.sh - Start a new audit file and expire the old logs
#
AUDIT_EXPIRE=30
AUDIT_DIR="/var/audit"

/usr/sbin/audit -n

cd $AUDIT_DIR # in case it is a link
/usr/bin/find . $AUDIT_DIR -type f -mtime +$AUDIT_EXPIRE \
   -exec rm {} > /dev/null 2>&1 \;
```

4. Run the script nightly from cron:

```
chmod 500 /etc/security/newauditlog.sh
/usr/bin/crontab -e root
0 0 * * * /etc/security/newauditlog.sh
```

5. The audit files generated are not human readable. The praudit(1M) command can be used to convert audit data into several ASCII formats.

Boot Files:

1. Disable all startup files for services that are not needed from /etc/rc2.d and /etc/rc3.d. Services may be disabled by changing the capital 'S' in the name of the script to a lowercase 's'. The following startup files should **not** be disabled:

```
S01MOUNTFSYS   S69inet       S72inetsvc     S74xntpd       S80PRESERVE
S05RMTMPFILES  S71rpc        S74autofs      S75cron        S88utmpd
S20sysetup     S71sysid.sys  S74syslog      S75savecore    S99audit
S30sysid.net
```

2. In order to ensure that all of the startup scripts run with the proper umask, execute the following script:

```
umask 022  # make sure umask.sh gets created with the proper mode
echo "umask 022" > /etc/init.d/umask.sh
chmod 544 /etc/init.d/umask.sh
for d in /etc/rc?.d
do
  ln /etc/init.d/umask.sh $d/S00umask.sh
done
```


© SANS Institute 2005, Author retains full rights.

3. In order to log as much information as possible, add the following lines to your /etc/syslog.conf:

```
mail.debug          /var/log/syslog
*.info;mail.none    /var/adm/messages
```

Note: Tabs **must** be used to separate the fields.
This will log mail entries to /var/log/syslog and everything else to /var/adm/messages.

4. Log failed login attempts by creating the /var/adm/loginlog file:

```
touch /var/adm/loginlog
chown root /var/adm/loginlog
chgrp sys /var/adm/loginlog
```

5. Set the permissions on the log files as follows:

```
chmod 600 /var/adm/messages /var/log/syslog /var/adm/loginlog
```

6. Configure syslogd to not listen on port 514/udp by specifiing the -t flag in /etc/rc2.d/S74syslog (Solaris >= 8):

```
/usr/sbin/syslogd -t > /dev/msglog 2>&1
```

7. Configure logs files to be rotated daily archiving old versions for 30 dain /etc/logadm.conf:

```
/var/log/syslog -A 30d -p 1d -z 1 -a 'kill -HUP `cat /var/run/syslog.pid`'
/var/adm/messages -A 30d -p 1d -z 1 -a 'kill -HUP `cat /var/run/syslog.pid`; \
logger -t logadm Begin new logfile'
```

8. Enable hardware protection for buffer overflow exploits in /etc/system (sun4u, sun4d, and sun4m systems only).

```
* Foil certain classes of bug exploits
set noexec_user_stack = 1
* Log attempted exploits
set noexec_user_stack_log = 1
```

Network Services:

1. IF the /usr/lib/sendmail daemon is not running, you should add the following line to root's crontab file:

```
0 * * * * /usr/lib/sendmail –q
```

2. Replace /etc/mail/sendmail.cf with the following:

```
# Minimal client sendmail.cf

### Defined macros
# The name of the mail hub
DRmailhost

# Define version
```


© SANS Institute 2005, Author retains full rights.

```
V8

# Whom errors should appear to be from
DnMailer-Daemon

# Formatting of the UNIX from line
DlFrom $g $d

# Separators
Do.:%@!^=/[]

# From of the sender's address
Dq<$g>

# Spool directory
OQ/usr/spool/mqueue


### Mailer Delivery Agents
# Mailer to forward mail to the hub machine
Mhub,   P=[IPC], S=0, R=0, F=mDFMuCX, A=IPC $h
# Sendmail requires these, but are not used

Mlocal, P=/bin/mail, F=rlsDFMmnuP, S=0, R=0, A=mail -d $u
Mprog,  P=/bin/sh,   F=lsDFMeuP,  S=0, R=0, A=sh -c $u

### Rule sets
S0
R@$+    $#error $: Missing user name
R$+ $#hub $@$R $:$1        forward to hub

S3
R$*<>$*     $n            handle <> error address
R$*<$*>$*   $2             basic RFC822 parsing
```

This configuration should be sufficient for servers where no local mail delivery is required.

1. Create /etc/init.d/nddconfig and create a link to /etc/rc2.d/S70nddconfig.

```
touch /etc/init.d/nddconfig
ln /etc/init.d/nddconfig /etc/rc2.d/S70nddconfig
chmod 544 /etc/init.d/nddconfig
```

Add the following lines to the /etc/init.d/nddconfig file:

```
#!/bin/sh
#
# /etc/init.d/nddconfig
#
```


© SANS Institute 2005, Author retains full rights.

```
# Fix for broadcast ping bug
/usr/sbin/ndd -set /dev/ip ip_respond_to_echo_broadcast 0

# Block directed broadcast packets
/usr/sbin/ndd -set /dev/ip ip_forward_directed_broadcasts 0

# Prevent spoofing
/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1
/usr/sbin/ndd -set /dev/ip ip_ignore_redirect 1

# No IP forwarding
/usr/sbin/ndd -set /dev/ip ip_forwarding 0
# Drop source routed packets
/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0

# Shorten ARP expiration to one minute to minimize ARP spoofing/hijacking
# [Source: Titan adjust-arp-timers module]
/usr/sbin/ndd -set /dev/ip ip_ire_flush_interval 60000
/usr/sbin/ndd -set /dev/arp arp_cleanup_interval 60

# The following tweaks are from 'Tuning Solaris for FireWall-1' by
# Rob Thomas.
#
# Do not respond to queries for our netmask
/usr/sbin/ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
#
# Do not issue redirects -- fix the routing table instead
/usr/sbin/ndd -set /dev/ip ip_send_redirects 0
#
# Increase our defense against SYN floods.
# The "q" queue is the completed socket holding pen where sockets
# remain until the application issues accept().
/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q 1280
# The "q0" queue is the half-open socket queue.
/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q0 10240
#
# --
```

A sample nddconfig file can also be found on the Sun BluePrints site at http://www.sun.com/blueprints/tools/nddconfig.tar

1. Deny services executed by inetd(3) the ability to create core files and enable logging for all TCP services by editing the /etc/rc2.d/S72inetsvc:

```
# Run inetd in "standalone" mode (-s flag) so it doesn't have
# to submit to the will of SAF.  Why did we ever let them change inetd?
ulimit -c 0
/usr/sbin/inetd -s -t&
```


© SANS Institute 2005, Author retains full rights.

2. Configure RFC 1948 TCP sequence number generation in /etc/default/inetinit:
   TCP_STRONG_ISS=2

3. Comment out or remove all unnecessary services in the /etc/inet/inetd.conf file including the following:

shell	login	exec
comsat	talk	uucp
tftp	finger	sysstat
netstat	time	echo
discard	daytime	chargen
rquotad	sprayd	walld
rexd	rpc.ttdbserverd	
ufsd	printer	dtspc
rpc.cmsd		

4. Create /etc/rc3.d/S79tmpfix so that upon boot the /tmp directory will always have the sticky bit set mode 1777.

```
#!/bin/sh
#ident  "@(#)tmpfix 1.0    95/09/14"

if [ -d /tmp ]
then
/usr/bin/chmod 1777 /tmp
/usr/bin/chgrp sys /tmp
/usr/bin/chown sys /tmp
fi
```

[Source: Titan psfix module]

Access Controls

1. Disable network root logins by enabling the "CONSOLE" line in /etc/default/login.

2. Remove, lock, or comment out unnecessary accounts, including "sys", "uucp", "nuucp", and "listen". The cleanest way to shut them down is to put "NP" in the password field of the /etc/shadow file.

3. Require authentication for remote commands by commenting out the following line in /etc/pam.conf:
   #rlogin auth sufficient /usr/lib/security/pam_rhosts_auth.so.1
   and changing the rsh line to read:
   rsh auth required   /usr/lib/security/pam_unix.so.1
   [Source: Titan pam-rhosts module]

4. Only add accounts for users who require access to the system. If using NIS, use the compat mode by editing the /etc/nsswitch.conf file:
   passwd: compat

© SANS Institute 2005, Author retains full rights.

Add each user to the /etc/passwd file

```
+nis_user:x::::/home_dir:/bin/sh
```

and the /etc/shadow file

```
+nis_user::10626::::::
```

5. Create an /etc/issue file to display the following warning banner: WARNING: This System is an ACME resource and is for authorized use only. If you are not authorized to access this resource, disconnect now. Unauthorized use of, or access to this resource is strictly prohibited and may subject you to disciplinary action or criminal prosecution. By accessing and using this resource, you are consenting to monitoring, keystroke recording and/or auditing**."**

   And in French: Ce système est une ressource du ACME et il doit être utilisé sur autorisation seulement. Si vous **n'avez pas** l'autorisation d'accéder à cette ressource, veuillez en interrompre l'utilisation immédiatement. L'utilisation non autorisée de cette ressource, tout comme l'accès à celle-ci, sont strictement interdits et peuvent vous exposer à une action disciplinaire ou à des poursuites au criminel. Si vous accédez à cette ressource et l'utilisez, vous consentez à un contrôle, à un enregistrement des saisies au clavier et/ou à une vérification.

   Add the banner to the /etc/motd file:

```
cp /etc/motd /etc/motd.orig
cat /etc/issue /etc/motd.orig > /etc/motd
```

1. The Automated Security Enhancement Tool (ASET) checks the settings and contents of system files. Many of the setuid and setgid programs on Solaris are used only by root, or by the user or group-id to which they are set.
   Run aset using the highest security level and review the report files that are generated in /usr/aset/reports.

```
/usr/aset/aset -l high
```

   Use of the FixModes program available from the Sun BluePrints site at http://www.sun.com/blueprints/tools/ is recommended.

2. Create a master list of the remaining setuid/setgid programs on your system and check that the list remains static over time.

```
/bin/find / -type f \( -perm -4000 -o -perm -2000 \) \
        -exec ls -ldb {} \;
```

3. Execution of the su(1M) command can be controlled by adding and configuring a wheel group such as that found on most BSD derived systems.

```
/usr/sbin/groupadd -g 13 wheel
/usr/bin/chgrp wheel /usr/bin/su /sbin/su.static
/usr/bin/chmod 4550 /usr/bin/su /sbin/su.static
```

   The GID for the wheel group does not need to be 13, any valid GID can be used. You will need to edit /etc/group to add users to the wheel group.

© SANS Institute 2005, Author retains full rights.

4. Create an /etc/ftpusers file:

```
cat /etc/passwd | cut -f1 -d: > /etc/ftpusers
chown root /etc/ftpusers
chmod 600 /etc/ftpusers
```

Remove any users that require ftp access from the /etc/ftpusers file.

5. Set the default umask so that it does not include world access. Add "umask 027" to the following files:

```
/etc/.login            /etc/profile
/etc/skel/local.cshrc  /etc/skel/local.login
/etc/skel/local.profile
```

Enable the "UMASK" line in the /etc/default/login file and set the value to 027

6. The files in /etc/cron.d control which users can use the cron(1M) and at(1) facilities.

Create an /etc/cron.d/cron.allow file:

```
echo "root" > /etc/cron.d/cron.allow
chown root /etc/cron.d/cron.allow
chmod 600 /etc/cron.d/cron.allow
```

Create an /etc/cron.d/at.allow file:

```
cp -p /etc/cron.d/cron.allow /etc/cron.d/at.allow
```

Create an /etc/cron.d/cron.deny file:

```
cat /etc/passwd | cut -f1 -d: | grep -v root > /etc/cron.d/cron.deny
chown root /etc/cron.d/cron.deny
chmod 600 /etc/cron.d/cron.deny
```

Create an /etc/cron.d/at.deny file:

```
cp -p /etc/cron.d/cron.deny /etc/cron.d/at.deny
```

7. If CDE is installed, replace the default CDE "Welcome" greeting. If the /etc/dt/config/C directory does not exist, create the directory structure and copy the default configuration file:

```
mkdir -p /etc/dt/config/C
chmod -R a+rX /etc/dt/config
cp -p /usr/dt/config/C/Xresources /etc/dt/config/C
```

Add the following lines to /etc/dt/config/C/Xresources:

```
Dtlogin*greeting.labelString:       %LocalHost%
Dtlogin*greeting.persLabelString:   login: %s
```

8. If CDE is installed, disable XDMCP connection access by creating or replacing the /etc/dt/config/Xaccess file:

```
#
# Xaccess - disable all XDMCP connections
#
!*
```

Set the permissions on /etc/dt/config/Xaccess to 444:

```
chmod 444 /etc/dt/config/Xaccess
```


© SANS Institute 2005, Author retains full rights.

Time Synchronisation

Edit the /etc/inet/ntp.conf file:

```
#
# /etc/inet/ntp.client
#
# An example file that could be copied over to /etc/inet/ntp.conf; it
# provides a configuration for an ntp server that uses three public sources
# with an internal fallback (L.M.1.0).
#
# A simple NTP client would specify one or more network servers in your
# organization:
#
#    server ntp.example.com
#
# Public NTP Server list: http://www.eecis.udel.edu/~mills/ntp/clock1a.htm
#
server L.M.41.40  # tick.usno.navy.mil
server L.M.5.250  # clock.isc.org
server L.M.176.30 # timekeeper.isi.edu
server L.M.1.0  # internal clock
fudge L.M.1.0 stratum 10
```

Recommended Tools to be installed

1. Sudo: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments.

2. TCP Wrappers: With this package you can monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services. TCP Wrappers is included in Solaris 9.

3. Secure Shell (ssh): Ssh is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels. It is intended as a replacement for rlogin, rsh, and rcp.

4. Titan: Titan is a collection of programs, each of which either fixes or tightens one or more potential security problems with a particular aspect in the setup or configuration of a Unix system.

Logcheck: Logcheck is a perl script that monitors system logs for unusual activity.

Are all OS and Security patches installed up to date? Provide details.

© SANS Institute 2005, Author retains full rights.

Appendix Q

Procedure for wiping out all data at DRP site:

1. Mainframe: Delete all data on all Mainframe DASD addresses to wipe out the VTOC and all volumes on the DASD. NOT only the VTOC(Table of contents). We usually use about 2X volumes during our DRP exercise. Using ICKDSF tool in verbose mode that will wipe out the data completely and zero all the used volumes.

2. Sun Platform: Solaris 8. procedure:
   Start the format program. Select the disk we want to scrub, example a14l5c2. Enter the Analyze utility. Then run verify. Verify will write data to the entire disk, twice. Once we have identified all disks we need to do the same on each. Or script it with all the names of the drives.
   Details of procedure as developed per our system configurations we have on these systems:
   # mount to see all mounted partitions
   # format
   Choose partition 5 first , so start with 5, then 4, then 3, then 2, then 1.
   You need to umount any partitions that might be mounted if system sees them as mounted.
   Then boot from CD . insert CD in CDROM and do the command
   #init 0 to boot from CD in single user mode to get the OK
   # OK
   type
   OK boot cdrom –s
   Once boot from CD is up system will boot is single user mode
   Do Format on partition 0, all drives attached to 0 will be unmounted during reboot from CD.
   # format
   #analyze
   #verify
   say yes to corrupt data
   and see it fly through all sectors
   once done do a
   # format
   #print
   to see all hex 0 across especially on partition 0 which is disk 1 that will be mostly used.
   All disks are in /dev/dsk
   # ls /dev/dsk
   Hot site vendor will reload the OS, and wipe out the disk array controller

3. Intel Platform:
   We require that all data on all internal and external drives are deleted. Recommended using gdisk utility that will allow us to run and wipe out all data on

© SANS Institute 2005, Author retains full rights.

all disks in the array along with deleting all controller information and get a default partition of I gig back on the main drive and also swap all the drives in the array afterwards. Gdisk can run on the 4th or 8th bit. We need the job completed in parallel on XX(Number) Intel servers in about 2 hours
Procedure using gdisk utility:
gdisk 1 or 2 /diskwipe command (after booting with a gdisk boot disk)
Then the hotsite vendor reloaded their own partitions and delete all array controller configurations
Result is *DELETED* on each partition.

4. Cisco Platform procedure:
Using Cisco Management Console: delete all Vlans maped to ports. Do a write erase on all routers and reset to factory default.
There are 5 VLANs that need to be deleted and write erase done on the routers.
Do the following on routers and firewalls: login in privileged mode: en
#Write erase
reload
show Run (Will show you running configs)
show startup-config (will show all startup configurations of device
#boot config
Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).

5. All workstations used have to be ghosted with a generic windows operating system.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Appendix R

MS ISA Server configuration recommendation taken from vendor manuals, and NSA document of best practices and changed to meet the need of new proxy configurations:

1. Do not install services and applications on the ISA Server other than Trend micro Spam Application
2. Harden the Windows 2000 OS by using hardening tools as used on MERIT Database server and MS Security analyzer that can be downloaded free from Microsoft
3. Install the latest security updates to Win2k and ISA Server to date
4. Disable all services that aren't required by the base operating system and ISA Server
5. Do not install ISA Server on a domain controller unless it's a dedicated ISA Server domain and forest
6. Change the method for resolving unqualified names by choosing the Append these DNS suffixes (in order) option in the DNS tab in the Advanced TCP/IP settings Properties dialog box
7. Determine whether your network infrastructure requires enabling the Microsoft Client, File and Printer sharing, and NetBIOS on the internal interface. If you do not require these features, turn them off.
8. Turn on packet filtering
9. Do not enable IP Routing unless absolutely required
10. Enable fragment filtering
11. Enable intrusion detection
12. Enable filtering of IP Options
13. Remove all Incoming Web Proxy listeners since we do not plan to use Web Publishing Rules
14. Change the default anonymous access Site and Content rule so that it applies to domain users, and delete the rule entirely.
15. Use the principle of least privilege
16. Create Protocol Rules for only required protocols
17. Limit access to protocols only to users that require them
18. Do not allow access to Publishing Rules
19. If server used for publishing, configure the published server to allow access only to those that require access to the server
20. Harden the published server as you would if the server were directly connected to the Internet
21. Configure important Alerts with response actions as determined by your corporate security policies Email to support personnel.
22. Store Logs and Summaries on a dedicated, extendable disk 90 Days minimum
23. Increase the number of saved log files
24. Copy the log files each day to a safe location
25. Increase the number of saved summaries 90 days
26. Enable the DNS, POP and SMTP application filters

© SANS Institute 2005, Author retains full rights.

27 Use the SMTP Message Screener as we require detection of more than SMTP command buffer overflows
28 Disable the SOCKS filter. **No winsock proxy** (Case by case basis based on business need).
29 Put only internal network addresses in the LAT
30 Put only internal network domains in the LDT
31 Do not "loopback" access to internal network resources through the ISA Server

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced