Tamirat Atsemegiorgis

Building a Secure Local Area Network

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor’s Thesis

6 May 2013

Author(s) Title Number of Pages Date	Tamirat Atsemegiorgis Building a Secure Local Area Networking 41+ 6 appendices 6 May 2013
Degree	Information Technology
Degree Programme	Bachelor of Engineering
Specialisation option	Communication and Data Networks
Instructor(s)	Erik Pätynen, Senior Lecturer

The goal of this final year project was to study the vulnerability of a small company network system and build a secure Local Area Network that would be capable of providing network resources and services as well as Internet connections to local users and a limited access of network service to public users.

To accomplish the project, a simulated network system was built in the laboratory and network devices were configured for layer 2 and 3 security features, the firewall was deployed to filter out the incoming and outgoing IP traffic, VPN remote client access technology and wireless connection were deployed. The simulated network was found to be security-tight, working for end-to-end client connections, working for Internal connection, working for remote client connections through Internet or wireless connection, and being accessible to the public user.

It can be concluded that unless security measures are planned and implemented, a company network system will be vulnerable to a computer attack that might cause damage to the company's resources and assets. Small companies, which want to build a well secured Local Area Network, will benefited if they adopt the security measures and practices of this project and implement them along with their own companies' specific security policy.

As the network grows in size, a user authentication at the local database is not efficient and here by, it is recommended to anyone who is interested in studying the subject further in the future to enhance the security system of the project by incorporating RADIUS-based authentication and explore advanced encryption methods for wireless networks.

Keywords	Local Area Network, attack, security, vulnerabilities, security policy

Contents

Abbreviations

ACLs	Access Control lists
ASA 5505	Adaptive Security Appliance model number 5505
ASDM	Adaptive Security Device Manager
AH	Authentication Header
ARP	Address Resolution Protocol
CSMA/CD	Carrier Sense Multiple Access Collision Detection
DHCP server	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS attack	Denial of Service attack
ESP	Encapsulating Security Payload
FTP server	File Transferee Protocol server
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol
LAN	Local Area Network
NAT	Network Address Translation
PAT	Port Address Translation
PKI	Pre-shared key Information
SSID	Service Set Identifier
SSL	Secure Sockets Layer
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy

1 Introduction

In today’s interconnected world it is irrational to believe a computer network system is immune from an attacks or think of it as too small to be considered as a predator by intruders to gain whatever advantage they need. Sometimes company owners deceived by thinking that company’s resource are not highly valued and hence, they are not worth to be targeted. The reality is even at this moment companies are losing a significant amount money and wealth because of negligence or lack of awareness about the security issues.

On the other hand smart leaders are taking steps not to be victims of globally-based cyber-attacks. Companies’ managers are spending a considerable amount of money to protect their resources and assets in order to achieve sustainable growth and stability on the course as desired. It is worth spending money and energy on asses’ network vulnerability and to identify the possible threats that might cause damage to the current system and resources. This will help in developing an effective security policy that dictates what to do and by whom in the situation when a system is under an attack coming from inside or outside the company's premises. Hence these days it is absolutely necessary for companies to pay special attention to tightening their security layers to exist as companies and contest at the global level.

The purpose of this project is to design a Local Area Network (LAN) for a small company and study the vulnerability of the system and implement security measures to protect network resources and system services. To do so, I will deal with the physical and logical design of a LAN by building a network in a test laboratory, consisting of computers, a ASA (Appliance Security Appliance) 5505 firewall, and switches and then configuring them for end-to-end connectivity and finally applying security layers on those devices needed to keep the system safe.

The goal of this thesis is to examine the security issues of the Local Area Network set up for a small company and build a secure LAN system and also to recommend the best practices that would help to protect the network system from internal and external attacks.

.

2 Network Topology Design

2.1 Network Design

This day's most organizations build their own LAN infrastructure with special consideration of security measures to protect their resources from any kind of attacks. Building a well-secured LAN requires designing of network topology before deciding which physical devices to be purchased or technologies to deploy. A topology design is defined as the identification of networks and their interconnection points, the size and the scope of the network, and the type of interconnecting devices used.

Basically network design is one of the four phases of PDIOO (Plan Design Implement Operate Optimize) life cycle. In this phase of the network life cycle, the designer's task will be to develop the physical and logical design of the network project. The physical design of the network is concerned with the identification of LAN and WAN technologies and network devices that are supposed to realize the performance of the logical design at large. During this phase, the network designer is responsible for selecting devices such as cabling wires, switches, bridges, routers, wireless access point and others. As we can see the logical design phase is a foundation for the physical network design, and it is where the designer develops a hierarchical and modular network. This phase includes designing of network layer addressing, selection of switching and routing protocols, security planning and network management design. Also the complexity of the topology depends on the size of the network and traffic characteristics of the system. [1,5,283]

2.2 Flat Network Design

A flat network topology is an unstructured type of network designing metrology, which is adequate in designing a small-sized network. It is a non-hierarchical designing model where each inter-networking device performs the same task. This model is easy to plan, design and implement for small-sized networks but it would be difficult to scale up the network when a need for growth arises and also the network might perform unexpected functions as the network expands in size. In addition to that, lack of hierarchy makes network troubleshooting and expansion difficult. Figure 1 below shows flat network design for a local area network. [1,122]

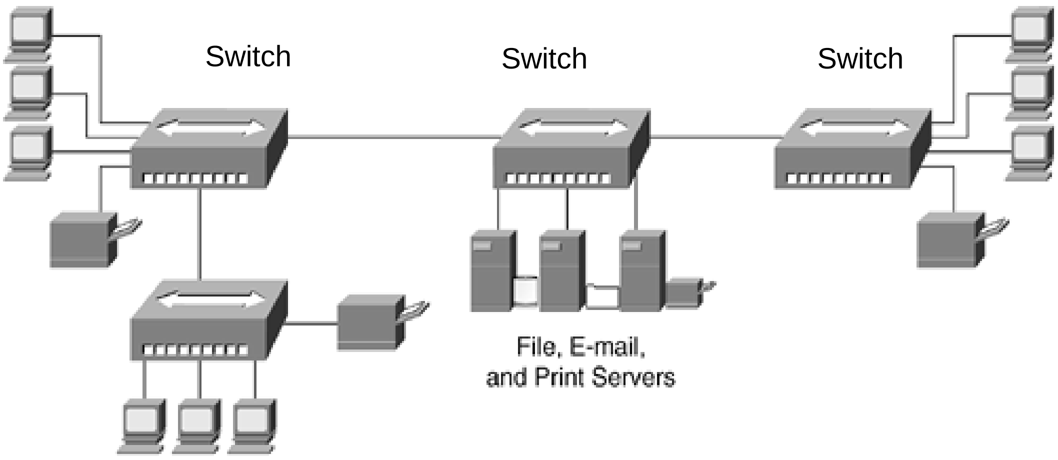


Figure 1. Flat Network Topology Design. Copied from Etutorials (2013) [2]

The design illustrated in figure 1 consists of workstations, printers, servers and switches that belongs to the same broadcast domain and shares the same bandwidth together. Flat topology uses a media-access control process such as carrier sense multiple access collision detection (CSMA/CD) or token passing technology to control access to the shared bandwidth. The absence of modularity in a flat network design courses all network devices to be in the same subnet and receives a copy of every message sent. Besides that, in the case of link failure it is difficult to get an alternative path to the destination. [2]

2.3 Hierarchical Network Design

As discussed in section 2.2, when an organization's network grows and becomes more complex; a flat network designing model would not work. Hence the network designers might need to consider building a network in a modular approach. A modular designing helps to split the huge and complex task by a specific function and makes the design project more manageable. For instance, a company network system might include the company's LANs, remote-access system, wireless connection system and WAN functionalities, in such scenario a hierarchical modelling methods fit well.[4,102]

Basically, a hierarchical model is a three-layer modular and structural design technique used to design a LAN or WAN network. Such a designing model helps to build a company's network into discrete layers consisting of many interrelated components. Technically speaking, a hierarchical model design has three layers, namely Core, Distribution and Access layers, as shown in the figure 2 below. Each layer has its own functions and they are built using network devices like routers or switches or combined in single device. [3,102]

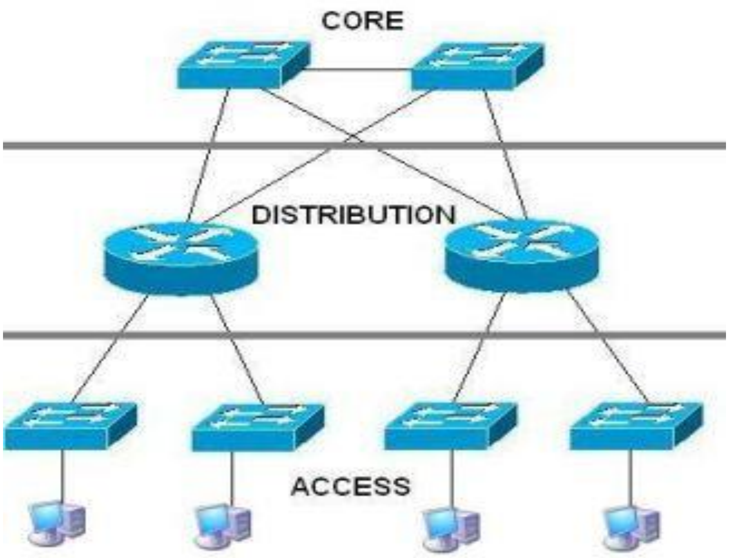


Figure 2. Hierarchical Network. Copied from Dinicolo (2013) [3]

There are many advantages in using a hierarchical model of designing a network, among those bring cost saving, scalability, flexibility, adaptability, simplicity, improved fault isolation and easer network manageability.

Core layer

A core layer is a high-speed switching backbone responsible for interconnecting distribution layers devices. This layer aggregates traffic from all distribution layers devices and is responsible for forwarding a large amount of data with a high speed over the network. To increase the data throughput of the network, packet filtering and other policy-based configurations have to be avoided from the core layer since they add unnecessary latency to the network and also have a significant impact on the network manageability. [4,8]

Furthermore, the core layer needs to be highly reliable and fault tolerant. This happens by establishing a full mesh redundancy link between the core layer routers and between the distribution layer routers and vice versa. Besides that, it is necessary to have backup power supplies in case of power failures. [4,10]

Distribution layer

The distribution layer is a middle layer between the access and core layer of a network. In other words it is considered a demarcation point between these layers. It is at this point where traffic flow control and access control takes place. More often, the distribution layer is a preferred place for designing virtual LANs (VLANs) to create one or more broadcast domains and to configure network devices like routers to route IP packets across VLANs. Besides that, the access layer is used to implement different functionalities that concern about network policies, IP addressing, area aggregation and also quality of services (QoS).

The distribution layer hides detailed topology information of the access layer from the core layer by address summarization, likewise it does core layer destination address summarization and hides the information from access layer devices. The distribution layer helps to improve core layer performance in connecting networks that run different protocols and also by redistributing between bandwidth-intensive access layer routing protocols such as IGRP (Interior Gateway Routing Protocol) and optimized core routing protocols such as EIGRP (Enhanced Interior Gateway Routing Protocol). [1,146]

Access layer

The main task of the access layer is to connect local users to the network so that they can access network resources and services. This layer is designed to deliver local user packets to the targeted end user computer and also to ensure a legitimate access of network resources and services. End devices such as personal computers, printers and IP phones are connected to the access layer. Besides that, interconnecting devices such as routers, switches, hubs and wireless access point can be part of the access layer. [6,5]

3 Overview of Network Security

3.1 Security Analysis

People in a society were used to guard their warehouse where they store their property and valuable treasures. The absence of such security may cause losses of properties and the human life. Likewise computer resources need to be protected from inside and outside intruders or saboteurs [8,201]. The only way of ensuring a complete computer security is by restricting all physical and logical access to a system. Obviously, total segregation of computers from one another creates a safe security zone; on the other hand, the system loses data communications, which makes the system useless. [7,3]

As known, a computer is more useful when it is a part of a network system. A networked environment helps to increase human productivity as well as, to create a conducive environment for the company to compete on the global stage. However it is important to take some security precautions in order to reduce or if possible to avoid the security risks caused by unauthorized access to the system resources and services that jeopardize the company's productivity as well as well-being. [8,6]

Companies work tirelessly to maximize their profits. To do so they use the fastest ways of communication. Today, the Internet is the cheapest, fastest and easiest means of communication to conduct business at global level. The Internet has changed the way people live, and work and has even revolutionized the way business is conducted. Besides the possibilities, Internet misses a security component and hence, a local network without security measures is at great risk of losing resources and assets. [7,3]

Treats are not only from external but also from trusted workers and retired former employees of the company. Hence, today a company needs to implement effective security measures to protect their valuable network resources against attacks. At this point it is worth defining what network security is; it has been perceived and defined in numerous ways in different books but according to cisco, it is defined as follows:

> "Network security includes the detection and prevention of unauthorized access to both the network elements and those devices attached to the network. This includes everything from preventing unauthorized switch port access to detecting and preventing unauthorized network traffic from both inside and outside the corporate network." [7,7]

The main reason for implementing network security is to secure the network and system resources connected to the network. Information in any form is considered a valuable property of the network and losing or releasing it might cost money or a disaster at all. Implementing security controls on a networked environment enables the network system to function properly as designed. Because of this, companies, governments and other organizations have prioritized network security and spent billions of euros on planning and implementing newer technologies. [7,3]

In today's open environment, organizations who want to provide public access to the network resources need to analyse the security threats that might result in an attack to the system. At this point, it is worth to reminding that an attack might happen from inside the network premises by trusted workers as well. A security analyst is concerned about discovering any kinds of vulnerabilities and attacks that might cause threats to today's operation of the system and also to the survival of the organization as well. [7,28]

3.2 Vulnerabilities

Vulnerability is a characteristic of a computer or a network system which poses weaknesses to the overall security system of a computer or a network that can be exploited by a threat. The threat uses the weakness of vulnerability to cause a potential damage to the computer or a network system. [8,6]

Basically, the vulnerability of a system can be traced back to three main sources: lack of effective network security policy, network configuration weaknesses and technology weaknesses.

Lack of Effective Network Security Policy

An organization needs to have a written security police document that clearly states what to do regarding the security issues that matter most to maintain the desired operation standard of the organization. If a policy is characterized by absence of uniformity in the application of polices, absence of continuity in enforcing polices, absence of a disaster recovery plan, absence of patch management, absence of log monitoring and absence of proper access controls, it will create security holes and make the network more vulnerable to an attack. [7,25]

Network Configuration Weaknesses

Humans are prone to comet mistakes in one way or another. Configuration vulnerabilities are human errors caused by lack of knowledge or misunderstanding. Such vulnerabilities happen when a weak password, misconfigured network devices, misconfigured Internet services (HTTP, FTP, Telnet etc.) and default settings are used. Each of them contributes a great opportunity for hackers and saboteurs to misuse the network resources. However, it is possible to prevent the damage before-hand by implementing standard baseline configurations. [7,26]

Technology Weaknesses

The current time technologies are not perfect to provide products and services we need without security holes. Almost all hardware equipment, software products (operating systems and applications), protocols (TCP/IP suits and routing protocols) have defects that can lead to system vulnerability and make the systems they belong to prone to attacks. [8,15]

3.3 Threat

A threat is anything that can be considered a potential cause of event which is capable of exploiting the vulnerability of a network system to harm the organization by disrupting the designed operation of the network. A threat can be initiated intentionally by people or accidentally by natural disasters, by malfunctioning of computers and by system components. [8,22]

Generally threats are grouped into two broad categories: structured threats and unstructured threats. The former type of threats is the most difficult one caused by people who are well organized to attempt a planned attack on a targeted system. Basically, the people are highly skilled and capable of manipulating the vulnerabilities of the system for their own benefit. The latter threats are of the most casual type, and are initiated by any person who is cable of identifying system vulnerabilities using freely available Internet scanning tools. For instance, there are free shall-scripts program and password crackers used by people to crack or steel a password and access the system to seek for any fortunes. Even though the attacks are not in an organized manner like the former, it is still capable of causing serious damage. [7,30]

3.4 Attack

According to the Internet Engineering Task Force (IETF), “an attack is an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system”. The assault can be any attempt to learn or gather information without affecting the system resources (passive attack, like packet sniffing) or it might be a serious one targeting resource manipulation and disruptions of system operation (active attack which include denial of service). Such an attack is initiated either from the inside security perimeters, who are trusted entities (inside attack) or from outside security perimeters, who are not authorized to access the system (outside attack). [7,13]

Technically speaking, with respect to the goals they accomplish, attacks are grouped into three main categories: reconnaissance attacks, access attacks, DoS (Denial-of-Service) attacks.

Reconnaissance Attack

A reconnaissance attack is concerned in accessing a system for any kind of vulnerabilities to launch attacks on the network system. In this case, the loss is not immediate;

however it creates a potential for hackers or intruders to initiate a targeted attack on a network system. A reconnaissance attack is usually aimed at discovering DNS (Domain Name System) information using DNA lookup queries and “Who is” queries, a range of subnets and hosts using Ping sweep software, an open port using port scanner and to examine packet vulnerabilities using packet spoofing. [5,33]

Access Attack

Such type of an attack is targeted to get access to a system or network without legitimate authentication. Intruders use different tools to intercept data traffic and extract important information such as password to get access into the system and misuse the network resources, modify device configurations and add unauthorized body to the system access list. In addition to that, such an attack includes the introduction of fabricated objects usually done by altering the original data, and the injections of malware. [7,33]

Computer malware (including viruses, worms, Trojan horses and others) is malicious software programs designed purposely to destroy or damage a computer system or network resources. Today, a malware developer uses the Internet to spread malicious programs to affect as numerous computer systems as possible. Such programs are capable of slowing down the Internet, wipe out files, affect servers etc. Even though there are a number of malware software programs exiting today, the descriptions of each malicious object mentioned above are presented below:

- Virus is a computer program or code fragment that is capable of attaching itself to the host program and duplicate whenever the host program is excited. A computer virus as a biological virus is not self-propagating. It needs a carrier program to spread from one system to another, like email attachments. [8,22]

- Worm is an independent and self-propagating program which is designed to scan a network for system vulnerability to duplicate itself and then propagate to the next new system. [8,22]

- Trojan horse is a program or pieces of code hiding inside another program to disguise a user to accept it as useful application like commercial games. However, when a program with a Trojan horse is executed it affects the system from miner to total distractions. Some of them are capable of modifying or replacing the existing program, create a back door to hackers, modifying the access list and also upgrade the privilege level. [7,34]

It is very important to note that the definitions of Virus, Worm and Trojan horse change with their development. For example, a computer virus developer is combining a number of viruses' features together to produce a more resilient virus than before.

Denial-of-Service attacks (DoS attacks)

As the name indicates a Denial-of-Service attack is an attack targeted to prevent service access to those individuals who have legal right for it. A system compromised by a Denial-of-Service attack executes a code that generates a number of consecutive requests for a service to create a bottle-neck in data transmission line and, as a result of this the attack makes the service unavailable to the legitimate users [5, 34]. An attack of such a type does not require high level of skill or knowledge; it can be initiated by an individual who has basic skill of the subject matter. Ping of death, synchronize Sequenced Number (SYN) flooding, spamming, and smurfing are among examples of Denial-of-Service attacks. [8,22]

3.5 Risk Analysis

In conducting a risk analysis, first all it is important to understand the basic definition of a computer security risk. A security risk is a probability that a particular threat exploits a particular vulnerability of a computer system that leads to losses of assets and resources. There are many different threats to a network system, but risk analysts have to pay attention to those threats that matter most. At this point, digital log files are the best alternatives to start the process of identification of threats; some of them are listed below:

- Local installation security system
- Software venders
- Local computer records
- Professional computer security organization

- Security newsletter and paper
- Electronic news group and list
- Local system users. [10,17;11,31]

The list might be enough to cover the threats facing the network system, but risk analysts need to widen their horizon to discover organization-specific threats as well.

Conducting a risk analysis primarily involves identification of assets, discovering risks to those assets and deploying controls to mitigate those risks. That means, in the process it is very important to know what kinds of risks exist to the company resources and how those risks be reduced or eventually eliminated. Basically, a security measure in a system has to be in proportion to the risks. Technically, implementing a security system in a computer network is not an easy task and usually, such a process with respect to selecting an appropriate security control is quite subjective. The primary idea of performing a risk analysis is to put those processes into an objective basis. [11,31]

There are a number of distinct approaches to a risk analysis. Basically those approaches are grouped into two categories: quantitative and qualitative risk analysis. Both approaches have their own advantages and disadvantages.

3.6 Risk Analysis Methodologies

3.6.1 Quantitative Risk Analysis

Such an approach of risk analysis is usually expressed in monetary value, and basically it is an estimate value of the probability of an event occurring and the losses it will cause. It is the financial loss expectancy that a company encounters at a time of incidence. Mathematically, the quantitative loses for events are calculated on an annual basis, simply multiplying the potential loss by the likelihood occurrence of a given event. To illustrate it, let us look at a practical example. We suppose the RAM of a computer fails two times every three years and the hardware cost of a RAM is €100. Based on the assumptions, the probability of a RAM fail a year is 2/3; hence the annual loss expectancy will be (2/3)*€100, which is €66,7. [12,4]

Theoretically, it is possible to rank an event based on the calculated risk value which ultimately helps to make the decision about what manner the security controls are going to be deployed. However, a quantitative risk analysis is not feasible when we use unreliable or inaccurate data. For instance, the implemented control and counter measures usually create a number of potential events and those events are mostly interrelated to one another. This makes it difficult to know them at hand and make a prediction about the likelihood probability of the occurrence of an event difficult. [10,4]

3.6.2 Qualitative Risk Analysis

In a qualitative risk analysis one does not assign monetary values to a specific risk, but rather calculate relative values to estimate the potential losses. The analysis is conducted through questionnaires and collaborative workshops involving workers and owners of the company. Risk analysts distribute questionnaires to gather information about the company's assets, deployed controls and other relevant security matters. The collected information is useful in identifying the assets and estimated values of those assets. In the workshop, the participants are tasked in predicting what threats each asset may face and finally imagine what types of vulnerabilities those threats might exploit in the future. [12,5]

3.7 Security Solution

3.7.1 Security Policy

As discussed in section 3.2, a hierarchical network design has three layers. The first one is called the core layer; it is where the critical application and supporting system is located and it needs to be protected from attacker by an additional security layer. The second layer is called the distribution layer where internal users and mostly public resources are located such as web servers and FTP servers. At the distribution layer one may find gateway applications and network systems (such as intrusion detection, virus and content inspections), specialized in providing additional security functions needed to protect the system from outsider as well insiders. The third layer is the access layer where end users are located to access the network resources and services and this layer has to be protected from unauthorized users.

Today no computer system is immune to an attack, and companies need to implement effective security measures that are capable of protecting their network system and resources. To confront an attack coming from inside or outside the company's network administrators need to choose adequate security technologies and their placement in the network system. Today there are numerous security technologies available but the choice and deployment has to match to the overall company's goal and security policy. [13,8]

Companies make security-related decision based on their own security goals, which are basically related to the business opportunities which their operation is based. The security goals of the company need to be known to users and employees of the firm through a set of security rules called security policy. According to the Request for Comments (RFC) 2196, a security policy is a formal statement of rules by which people that are given access to an organization's technology and information must abide. The policy has to state clearly everyone's requirements for protecting the company's technology and information assets, and also need to dictate the procedure of how the requirements be met. [13,5]

Before developing a security policy it is necessary to develop a security plan that decides what needs to be protected and from whom. The best way to do it is by conducting a risk analysis to list out what are considered allowable and non-allowable actions and beyond that to determine where and how security issues are addressed .A well-organized security policy includes user access policy, remote access policy, accountability policy, authentication policy, incident handling policy, Internet access policy, E-mail policy, physical security policy, maintenance policy and violation reporting policy. [14,6]

Generally, a policy should not be over-restrictive but rather ease the use of resources with a certain level of restrictions. The depth of our security policy based on how much we trust people, and the policy has to draw a line to balance between allowing users to access company resources to do their jobs and completely denying access to those resources and assets. Usually, network administrators together with senior managers of the company are responsible for designing the security policy. Inputs from users, staff, managers, network administrators and designers are required to develop an effective security policy. Besides that, it is absolutely necessary to seek legal counsel before communicating with users and staff of the company and asking them to abide by the rules of the policy documents. [14,7]

Since companies are in a constant change with respect to technology and business directions, and also risks to the company’s resources and assets changes over time. Hence, the security policy documents needs to be reviewed on a regular basis to support the security needs. According to Cisco security experts, maintaining the security of the company is a non-ending process and puts it in to four stage of a vicious cycle called security wheel. The stages are: implementing, monitoring, testing and improving. After the policy is implemented it needs to be monitored against attacks and then appropriate security measures have to be tested before applying the improved security measures. [1,237]

It might be important to consider exceptions to every rule, and the policy document needs to include those exceptions if they exist. Most often, system administrators might use the same user id and usually they need to have the right to access administrative files to go through a user's files whenever it is necessary.

3.7.2 Security Technologies and Their Placement

Modern network communication and sharing systems requires the deployments of efficient security system that fit with the overall security policy of the company which is capable of protecting the network's assets and resources. Today there are number of technologies available to be used to build a security system, but the biggest challenge to a network administrator is to select the most adequate technology and to decide where the right place would be to deploy it in the network system. Figure 3 below shows the choices of technologies and their placement in the security zone. [16,195]

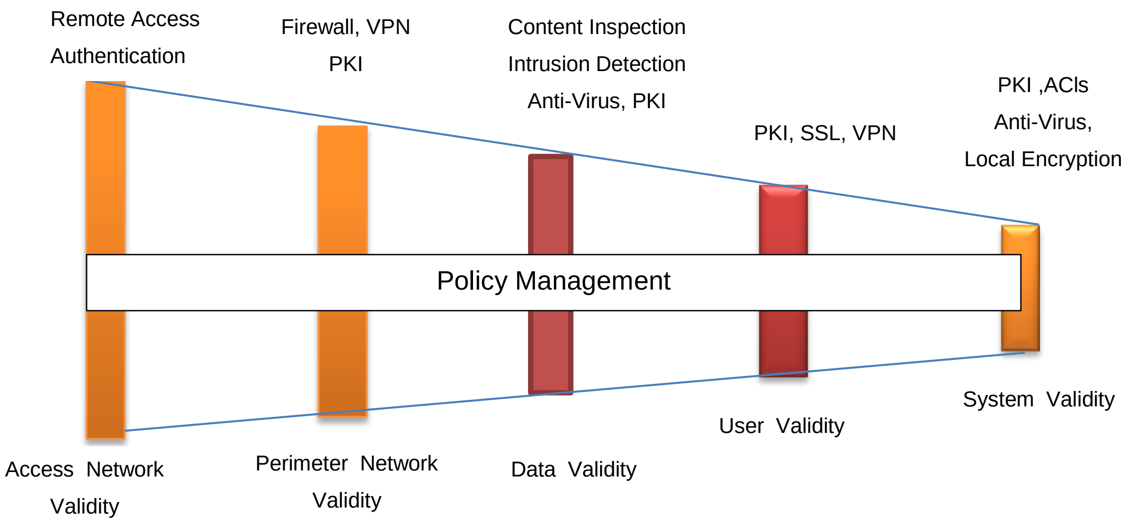


Figure 3. Placement of Security Measures on Security Zone. Copied from Canavan. (2001)[8]

An Unauthorized remote access to a network resource is protected by deploying remote access authentication technologies such as RADIUS (to protect dial-up connections), encryption (to protect leased line connections) and IPsec to protect connection over a public network. Distribution layer devices are usually protected by deploying one or more firewalls as well as a security zone. [16,195]

After a user has been identified and authorized to access the network resources, it is important to check the inbound as well as the outbound data for harmful objects such as viruses that affects the normal function of a computer system. Practically it can be done by deploying content inspection, intrusion detection, anti-virus or PKI (Pre-shared key Information). Finally the system that provides the application service is also needed to protect using access control lists (ACLs), data encryption and anti-virus programs.

3.7.3 Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is an open standard security framework developed by IETF (Internet Engineering Task Force) to provide secure communications over IP networks. That means IPsec offers protection for higher layer protocols and applications that makes it to be the most preferred technology used to secure end-to-end communication over the IP network. Basically, IPsec is designed to offer confidentiality, integrity and authenticity of data communications and devices interoperability. IPsec accomplishes those tasks through two protocols called Authentication Header (AH) and the Encapsulating Security Payload (ESP) along with standard key negotiation and management mechanisms. [9,189;15,5]

The Authentication Header (AH), is designed to provide data integrity (original authentication) for the whole IP datagram and hence it is an effective measure against IP spoofing and session hijacking. Encapsulating Security Payload (ESP), is designed to offer data integrity and confidentiality by encrypting the payload of the IP packets using a shared secret key. [15,201,202]

In addition to AH and ESP, the IPsec suite contains Internet Key Exchange (IKE) that work with Internet Security Association Key Management Protocol (ISAKMP)/Oakley to manage the generation and handling of keys and also it helps to create security associations (SA). A security association is a policy or rules agreed between peer devices concerning how data exchange takes place among them. Besides that, IPsec has two modes of operation: tunnel mode and transport mode. In the tunnel mode, IPsec is implemented between two gateways and the original IP packet is encrypted and becomes the payload of the new IP packet. In the transport mode IPsec is used between hosts and in this case the original header information (source and destination) is unencrypted and it makes it to be visible to intermediate network devices. [15,201,202]

3.7.4 Firewall

Firewalls are either hardware or software based and their main function is to keep a computer or network system secure from an attack. If we look closer, a hardware-based firewall is a dedicated device with its own operating system on a specialized platform, whereas a software-based firewall is an additional program loaded on a personal computer or on a network device like a router to inspect data or network traffic.

A firewall has a great role in the implementation of a company’s security policy and in this case it is considered a system or a group of systems used to control network traffic based on the rules. The firewall is used as a protective bridge that demarks the internal or trusted network to the external untrusted network such as the Internet. As a check point gateway, firewall analyses the IP packets and decides whether to allow through or not, based on the preconfigured rules. Also the firewall determines which information or services to be accessed from outside as well as from inside and by whom. [15,206]

According to cisco, the firewall is helpful for packet inspection, security policy implementation, generation of the audit system and log messages. To operate as desired, the firewall uses one or more of the following technology components: packet-filtering, application level gateway (proxy server) and circuit level gateway (SOCKS). Each of them has different functions and are explained below: [13, 210,211, 219]

- The Packet-filtering components help to limit the flow of information between networks based on the security policy. The Packet-filtering technology uses an access control list to permit or deny traffic fulfilling the rules dictated by the security policy.

- The Application level gateway (proxy server) controls the exchange of data between two networks at the application level. This is done by inspecting a data packet at a higher level of the OSI layers (layer 4, 5, 6 and 7) to control or filter out the content of a particular service according to the security policy.

- The Circuit level gateway (SOCKS) is a special kind of application level gateway, which is designed to examine both TCP/IP and UDP applications without any extra packet processing and filtering. SOCKS is usually used for outbound connections whereas a proxy server is used for both inbound and outbound connections.

To build an effective firewall those components are used together, but depending on the requirements one or more combinations of the components can be used. Even though the firewall is designed to permit or deny a vulnerable service to protect the internal network from external attacks, it is the duty of the network administrator to examine user logs and alarms generated by the firewall and update the security policy as soon as possible.

3.7.5 Physical Security

Physical access to the network facilities has to be monitored and protected in order to avoid unauthorized access, theft, vandalism and misuse of a company's resources and assets. Only the right personnel are needed to be allowed to physically access the network equipment to perform their jobs. This is usually done by keeping the critical network equipment behind locked door, which has protections from natural disasters such as floods, fires, storms, and earthquakes, as well as human disasters like terrorists, hackers and competitors. In a computer room the network equipment should be kept in a rack that is attached to the floor or wall and the room needs to be equipped with uninterruptible power supplies, air-conditioning, fire alarms, fire-abatement mechanisms and water removal systems. [1,238]

4 Research Project and Project Implementation

4.1 Project Analysis

Basically a project analysis includes planning, designing and controlling of a network project. This project focus is on building a local area network for a small company and to apply the security measures to ensure the safety of the network resources and services of a company. The plan of this project is to build a simulation network for a small company in the laboratory network, which consists of one Cisco ASA 5505 firewall as a getaway router, one Cisco 3560 switch as a core switch, two Cisco 2960 switch as workstation switches and workstations.

A computer network is built in the company premises primarily to create a communication channel between users within company to share network resources and services including Internet access safely and easily. Those characteristics are valuable to increase the efficiency of the worker as well as the overall productivity of the company by making resources and services available to users easily whenever needed. That means, building a computer network in a company reduces the time and money spent to get resources and information needed in the traditional manner.

The simulated network is intended to create a communication channel and also to provide file sharing service to the public users with higher security measures. Companies and organizations might need to communicate the public for various reasons. To do so most often they build a web site and make their resources and services available for public usage. Therefore, the project network is employed to offer file sharing service to internal user as well as to the public. This is accomplished by dedicating an FTP server to offer file sharing service for those requisites coming from inside and outside the network.

A simulated network is also designed to offer a wireless connection to visitors and authenticated users as well. The wireless network helps users to be connected to the network and share resources and services at any place within the radio signal radius. Besides that, the simulated network provides remote access to the network through VPN tunnelling over public Internet. A remote client connection helps authorized users to be connected to the network system as if they were located inside the network premises. Users are able to access the network resources wherever they are as long as they are connected to the Internet.

4.2 Project Design

4.2.1 Topology Design and Implementation

The project topology shown in figure 4 below is designed by considering the characteristics and features of a small company. The topology is assumed to have three departments with the possible future expansion and planned to offer flexible, reliable, secure and fast network services. It is designed to have seven subnets, two of which are workgroup subnets where employees are located, and one subnet is for the network management team, two subnets are for DMZ and internal servers and the remaining two subnets are for a wireless network.

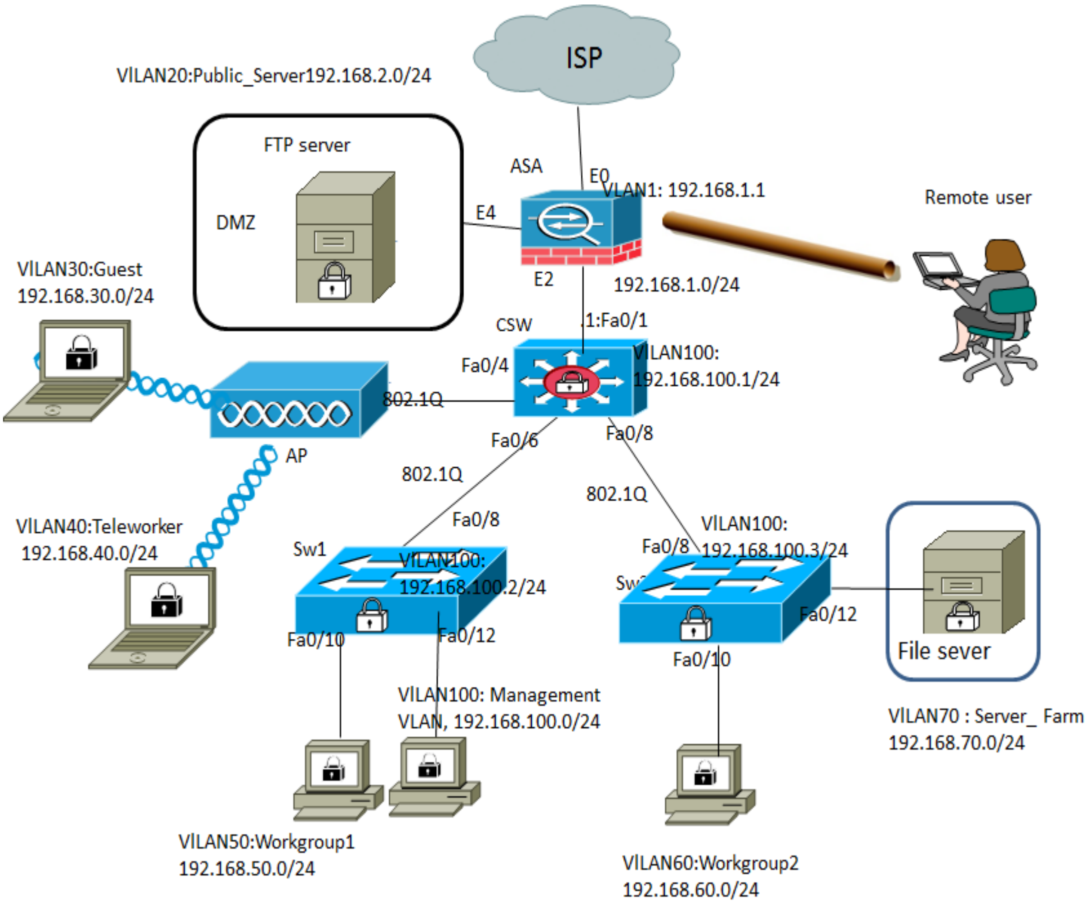


Figure 4. Simulated LAN Network.

The topology presented in figure 4 is an extended star topology where a CSW switch is used as a core switch to centralize all connections going to workstation switches (SW1 and SW2), firewall (ASA) and access point (AP). The extended star topology guarantees the system for future expansions in size whenever the need comes. The network devices are connected to one another using Cat 5 (Unshielded Twisted Pair) cables and RJ-45 connecters.

According to figure 4, the firewall is a gateway to the external network by routing IP traffic in both directions. The firewall is connected to the Internet through test network with a dedicated IP address. A public server is connected to the firewall with its own subnet which is basically planned to offer file sharing services to public users. The firewall is used to translate the private IP addresses of the inside and Public_Server subnets to a public IP address of the outside interface of the firewall and vice versa. Above all, the main task of the firewall is to serve as a check point to filter out incoming and outgoing traffics for the purpose of protection of the internal network against attacks coming from the external network.

Access layer switches (Sw1 and Sw2) shown in the topology figure 4 are used to connect workstations and the internal server to the core switch. Workgroup1 subnet and management subnet are connected to Sw1 switch, and workgroup2 subnet and Server_Farm subnet are connected to Sw2 switch. Workgroup1 and workgroup2 subnets are dedicated to employees, and users in those subnets are allowed to communicate with each other and to the external world through the Internet. The management subnet is dedicated for network administration and management purposes and the Server_Farm subnet is configured to provide file sharing services to the internal user only.

The access point (AP) shown in figure 4 is directly connected to the core switch (CSW) and is configured to provide a wireless connection to visitors and authenticated users within the radio signal range.

4.2.2 IP Addressing

An IP address is a unique 32- bit number which is used to identify a network device on an IP network. Each IP address consists of two parts, the host and the network portion. The network address is used for identifying the network or the subnet where the device is located and the host address helps to identify the individual device.[16,254]

In the simulated network a private IP address 192.168.0.0/24 was used for the internal network subnets and a public IP address 192.94.62.251/24 was used for the outside virtual interface (VLAN2) of the firewall. The VLAN configuration and IP addressing for the firewall (ASA) are presented below.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 10.94.62.251 255.255.255.0
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
```

Listing 1. VLAN configuration on firewall

As listing 1 illustrates, IP address 192.168.1.1/24 is assigned to the VLAN1 of the firewall (inside VLAN) and the 192.1168.2.1/24 is to VLAN3 of the firewall (dmz VLAN). Besides that, according to appendix 1, subnet 192.168.30.0/24 and subnet 192.168.40.0/24 are assigned to the wireless network, subnet 192.168.50.0/24 and subnet 192.168.60.0/24 are assigned to VLAN40 and VLAN50 (workgroup1 and workstation2 VLANs), subnet 192.168.100.0/24 assigned to VLAN100 (management VLAN), and subnets 192.168.70.0/24 and 172.16.10.8/28 are assigned to VLAN70 (Server_Farm VLAN) and to remote clients respectively. The full configuration is provided in appendixes 1,2,3,4 and 5

The firewall (ASA) is also configured to assign a dynamic IP address to remote client who requests for an VPN connection over the Internet. The DHCP pool on the firewall has been configured as follows:

```
ip local pool remote-access 172.16.10.10-172.16.10.15 mask
255.255.255.128
```

According to the above configuration, there are five IP addresses in the address pool, and the firewall (which is a DHCP server for remote clients) is capable of assigning up to five IP addresses to a remote device at the sametime. The rest of the configuration is given in appendix 1.

In addition to that, the core switch (CSW) has been configured for the DHCP server to assign IP addresses dynamically to wireless users. The configuration for the address pools and their default getaways on the core switch (CSW) are presented below:

```
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.40.1
!
ip dhcp pool AP_pool_Guest
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.1
!
ip dhcp pool AP_pool_Worker
   network 192.168.40.0 255.255.255.0
   default-router 192.168.40.1
```

The configuration above is meant to create two IP address pools, namely **AP_pool_Guest** and **AP_pool_Worker**. **AP_pool_Guest** is a pool of IP addresses of a subnet 192.168.30.0/24 that is assigned to the Guest VLAN (VLAN30) and the **AP_pool_Worker** is an IP addresses pool of a subnet 192.168.40.0/24 which belongs to the Worker VLAN (VLAN40). The default gateways (192.168.30.1 and 192.168.40.1) are excluded from pools to avoid address overlap. The rest of the configuration is presented in appendixes 2 and 4.

As stated in section 4.2.2, the inside network uses private IP addresses to identify a network as well as a network device. Private IP addresses are used for intranet connection and they are not routable over the gateway. To make the private IP addresses routable it is necessary to use the NAT (IP Network Address Translation) technology. Basically, NAT is used for translation of a real address (private address) of a device into a mapped address (public address) to be routable over networks.[15] In the simulated network project, the firewall ASA is configured to be a NAT server and some of the configuration is shown below.

```
object network inside-outside
 subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic interface
```

It is important to note that, on the Cisco ASA (Adaptive Security Appliance) 5505 version 8.3 and later, the NAT configuration requires creating a network object which contains a private IP address for a host or a subnet and defines the NAT rule to be followed. In the above NAT configuration, an object **inside-outside** is defined an inside subnet 192.168.0.0/16 and with a NAT rule that dynamically assign the ASA outside interface IP address (10.94.62.251/24) to the internal subnet to connect to the Internet. This and other configuration presented in appendix 1 help to create a working connection to the Internet. Example 1 below shows the output of NAT translations.

Example 1: NAT translation.

```
ASA# show xlate
17 in use, 118 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static,
I - identity, T – twice, e - extended
NAT from inside:192.168.1.0/24 to out-
side:192.168.1.0/24
    flags sI idle 1:15:20 timeout 0:00:00
TCP PAT from dmz:192.168.2.3 21-21 to out-
side:10.94.62.251 21-21
    flags sr idle 0:25:07 timeout 0:00:00
TCP PAT from dmz:192.168.2.0/24 21-21 to out-
side:10.94.62.251 21-21
```

```
flags sr idle 0:25:07 timeout 0:00:00
UDP PAT from inside:192.168.100.4/64375 to out-
side:10.94.62.251/64375 flags ri idle 0:00:55 timeout
0:00:30
TCP PAT from inside:192.168.30.2/50531 to out-
side:10.94.62.251/50531 flags ri idle 0:00:18 timeout
0:00:30
TCP PAT from inside:192.168.30.2/50530 to out-
side:10.94.62.251/50530 flags ri idle 0:00:18 timeout
0:00:30
TCP PAT from inside:192.168.30.2/50529 to out-
side:10.94.62.251/50529 flags ri idle 0:00:18 timeout
0:00:30
```

The output presented in example 1 shows, clients from dmz and inside networks are able to connect to the outside network through the ASA outside interface IP address 10.94.62.251. That means the NAT rule translates the private IP addresses of the internal networks into a public IP address that is routable on the networks.

4.3 Security Desigin and Implementation

4.3.1 Basic Configuration of Network Devices

For the sake of growth and well-being, owners as well as managers of a company need to pay special attention to the security system of their computer network. Network security is concerned with the protection of network resources and services from natural and human caused disasters. To do so, the security designer has to look carefully at the vulnerability of the network system and design security measures to protect disaster on the company.

All network devices used in the simulated lab have been configured with a basic configuration. The basic configuration includes the names of the devices, the IP addresses of the interfaces and VLANs, user names and their encrypted passwords, VTY and console ports passwords, default routes, access and trunk ports, banners of the day and domain names. Some basic configuration of the core switch (CSW) are shown below.

```
hostname CSW
!
enable secret 5 $1$Nh/1$bmSgITR31VtxLu.4mc7Wo.
!
ip routing
!

interface FastEthernet0/1
 description "to the ASA device"
 no switchport
 ip address 192.168.1.2 255.255.255.0
!
access-list 1 permit 192.168.100.0
banner motd ^C unauthorized user is not prohibited ^C
!
line con 0
 access-class 1 in
 exec-timeout 0 0
 password 7 06120E2C495A081400
 logging synchronous
 login
line vty 0 4
 access-class 1 in
 exec-timeout 5 0
 privilege level 15
 password 7 06120E2C495A081400
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 no login
```

As stated above, the core switch named CSW configured for a secret privilege mode password, banner of the day, VTY and console port access passwords. A secured remote communication protocol SSH (Secure Shell) has been configured on VTY port and the access has been protected by a standard access list 1. Besides that, the core switch is configured by the command **ip routing** to perform a routing task for the inside subnets. Also, in order to create layer 3 connection between the firewall and CSW Fast Ethernet 0/1 of the CSW is needed to be configured as a routing port with **no switchport** command and assigned to an IP address 192.168.1.2/24. This and other configurations presented in appendix 2, 3 and 4 help to create a working network connection as shown in appendix 5. Examples 2 and 3 present the ip route learnt by the core switch and by the firewall.

Example 2. The ip route table of firewall (ASA).

```
ASA# show route


Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route


Gateway of last resort is 10.94.62.254 to network 0.0.0.0

S    192.168.30.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    192.168.60.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    192.168.40.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    172.16.10.10 255.255.255.255 [1/0] via 10.94.62.118, out-
side
C    10.94.62.0 255.255.255.0 is directly connected, outside
S    192.168.50.0 255.255.255.0 [1/0] via 192.168.1.2, inside
C    192.168.1.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, dmz
S    192.168.70.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    192.168.100.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.94.62.254, outside
```

Example 3. The ip route table of the core switch (CSW).

```
CSW#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter 
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external 
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - 
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, 
l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/1
L        192.168.1.2/32 is directly connected, FastEthernet0/1
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.1/32 is directly connected, Vlan30
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, Vlan40
L        192.168.40.1/32 is directly connected, Vlan40
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, Vlan50
L        192.168.50.1/32 is directly connected, Vlan50
      192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.60.0/24 is directly connected, Vlan60
L        192.168.60.1/32 is directly connected, Vlan60
      192.168.70.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.70.0/24 is directly connected, Vlan70
L        192.168.70.1/32 is directly connected, Vlan70
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Vlan100
L        192.168.100.1/32 is directly connected, Vlan100
```

Example 4 below shows the ping result between the ASA firewall and the management workstation.

Example 4: Connectivity testing

```
ASA# ping 192.168.100.4

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.100.4, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/1/1 ms
```

Examples 2 and 3 presents subnets that are reachable from or through the CSW core switch as well as the ASA firewall. The gateway of last resorts and default routes were configured to route unknown subnets traffics to outside network (that is in the case of the ASA firewall) and to the inside network (in the case of CSW switch). And, example 4 illustrates the connectivity between the management workstation and the ASA firewall.

4.3.2 Securing the Inside Network Using Firewall

As discussed in section 4.2.1, for this project a Cisco Adaptive Security Appliance (ASA 5505) were used as a firewall to protect an attack coming from the outside network to the inside network. ASA 5505 is a full-featured security appliance capable of offering a high-performance firewall, SSL and IPsec VPN, and many other network services for small and medium-sized company networks. ASA 5505 has a flexible eight-port 10/100 Fast Ethernet switch and is capable of supporting up to three VLANs in the security plus license. [15,72]. In the simulated network of this project three VLANs were created: Inside, Outside and dmz VLANs. The Inside VLAN is a trust network assigned to the inside network and is connected to E2 Fast Ethernet interface of the ASA 5505 firewall. The Outside VLAN is the most untrusted network (public network) and is connected to the E0 Fast Ethernet interface of the ASA 5505 firewall, and dmz VLAN is a security zone containing a public server and is connected to the E4 Fast Ethernet interface of the ASA 5505 firewall.

Basically, each interface of the ASA 5505 needs to be assigned a security level between 0 and 100, as shown in appendix 1. The inside interface is assigned to a security level of 100, the outside interface to 0 and the dmz interface to 70. A security-level prioritize the follows of network traffics by applying an implicit permit from a higher security interface to a lower security interface. That means, the host from a higher security-level interface can access any host on a lower security-level interface but not the other way round.

In order to permit the outside hosts to access the FTP server, a network object and an access list is required to be configured to direct the traffic flows against the security level. In the simulated network, a network object **dmz-server-fromoutside** was configured along with an extended access list **outsidetoDMZ** to direct FTP traffic from outside to DMZ VLAN.

```
object network dmz-server-fromoutside
 host 192.168.2.3
nat (dmz,outside) dynamic interface  service tcp ftp ftp

access-list outsidetoDMZ extended permit tcp any host
192.168.2.3 eq ftp
access-group outsidetoDMZ in interface outside
```

As shown above a network object **dmz-server-fromoutside** was created to contain the FTP server IP address and the rule was defined to NAT dynamically using the outside IP address 10.94.62.251 for any ftp connection attempt made from the outside network. The extended access list was also needed to be applied on the outside interface so that the outside network of lower security-level could reach to a higher security-level FTP-server inside the dmz VLAN.

In the same way the ASA 5505 firewall was configured for the DMZ host to access the inside server as well as the inside network hosts to access the DMZ host. The full configuration and a NAT translation is found in appendixes 1 and 5.

4.3.3 Securing Switch

According to the network topology shown in figure 4, the internal network is segmented into subnets based on the function. The core switch CSW is configured to play a role of routing IP traffics to individual segments. Each subnet is a broadcasting domain and this helps to enhance the security of the system by preventing sniffing and ARP (Address Resolution Protocol)attacks between segments [16].

Switch’s ports are gateways to a network system and they need to be protected from strangers. To do so, port security has to be tight and the unused ports have to be monitored regularly and are need to make sure they are shutdown. In the simulated network of this project all unused ports has been shutdown and besides that, to protect the system against MAC flooding and spoofing attack port security was configured on VLAN 50, 60, 70, and 100 ports. To enable port security on the access port, the **switchport port-security** command was used on each access ports of the network system. As an example a configuration for switch Sw2's access port FastEthernet0/10 is shown below.

```
Sw2(config)# interface fastethernet 0/10
Sw2 (config-if)# switchport port-security
Sw2 (config-if)#spanning-tree portfast
Sw2 (config-if)#spanning-tree bpduguard enable
```

Issuing switchport port-security on the access port set the maximum number of MAC address assigned to fastethernet 0/10 port to 1 and the violation rule to shut down. And BPDU (Bridge Protocol Data Unit) is also enabled on a portfast-enabled port using the **spanning-tree portfast bpduguard default** command on configuration mode. This command helps to prevent the desperation of the root bridge function, which is a potential cause of the Denial of Service attacks.

Moreover a management VLAN 100, was assigned to isolate management traffic from the production by assigning each device to the management VLAN. Also the management traffic was encrypted via SSH (Secure Shell) protocol. The entire configuration is found in appendixes 2, 3 and 4.

4.3.4 Securing Remote Client Access

The simulated network was been configured for a VPN remote access to allow privileged users to access the network over the Internet. In such a configuration, before IPsec VPN association was formed a VPN tunnel was created between the remote client and the ASA 5505 firewall over the public Internet and then they negotiate how to build an IPsec security association. To incorporate a remote accessing technology to the simulated network, a VPN connection configuration was done using the web-based GUI (Graphical User Interface) management software ASDM (Adaptive Security Device Manager). The ASDM configuration steps for a remote VPN client connection on ASA 5505 are presented as follows:

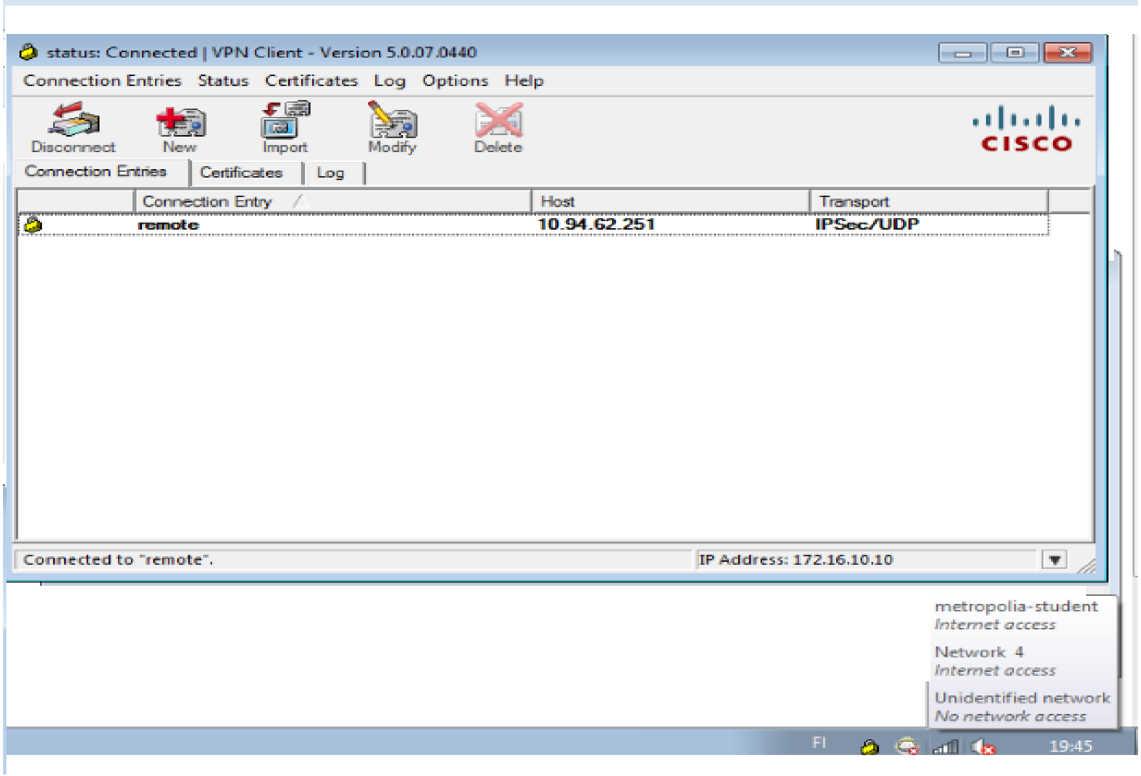
1. On the management host, open an Internet explorer and type https:192.168.1.1 on the address bar.
2. On the Cisco ASDM page, select wizard on the menu bar and select IPsec VPN wizard and select remote access radio button and then click next.
3. On the client type page, select Cisco VPN client and then click next.
4. On the client authentication page, select pre-shared key and type the key then type the tunnel group. (tametame is used for pre-shared key and testgroup for tunnel group) and then click next.
5. Select the authentication on the local user database and then click next.
6. On the user account page, create users with usernames and passwords (tame, tame1 with passwords tametame, tametame1 were used) and then click next.
7. On the address pool page, create a pool of addresses used to be assign to remote clients (a pool of 172.16.10.10-172.16.10.15 were used) and then click next.
8. Type DNS sever in the primary DNS Server (the test network DNS server is used) and then click next.
9. Define the encryption, authentication and Diffie-Hellman group policy and click.
10. Select the inside network to be hide from outside user and select enable split tunnelling and then click next.
11. Finish.

The above configuration was made using the ASA version 8.3(4) and ASDM 6.4 and those steps might not be consistent with other versions.

On the client device after installing VPN client software the configuration were done as follows:

1. Open the VPN client software on the remote client device.
2. Click on new button.
3. On VPN client properties window, type a name on connection entry (like remote-connection), type the public IP address (ASA outside interface IP address 10.94.62.251).
4. On authentication tab, type the tunnel group name used in configuring VPN on ASA (testgroup), enter the pre-shared key in the password box and confirm it (tametame).
5. Save the configuration.

Whenever the client wants to connect to the network remotely, the only task the user does is to plug himself in to the Internet, open VPN client software, select the connection enter name and then press the connect button on the menu bar. Figure 5 below shows a screen shoot of the VPN client desktop while the client is connected to the simulated network through the test network.



Connection Entry	Host	Transport
remote	10.94.62.251	IPSec/UDP

Connected to "remote".

IP Address: 172.16.10.10

metropolia-student
Internet access

Network 4
Internet access

Unidentified network
No network access

Figure 5. Remote Client VPN Connection.

Figure 5 shows that, a remote client was been assigned an IP address 172.16.10.10 and is able to surf on the Internet as well as get connected to the test network. The full configuration and other testing outputs are presented in appendixes 1 and 5.

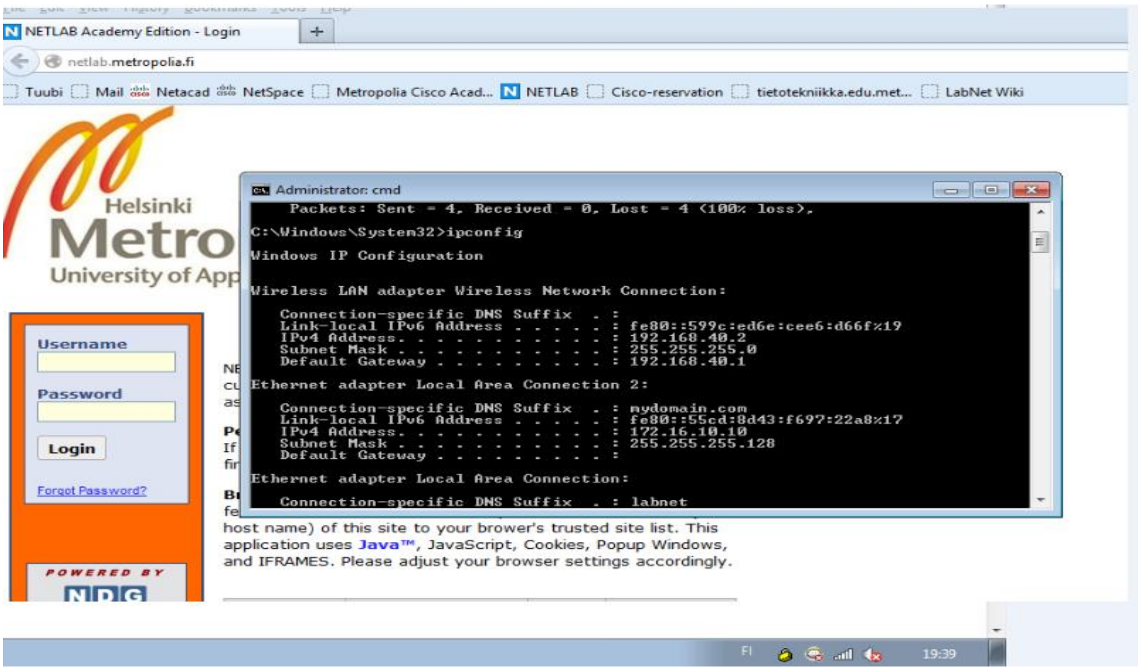
4.3.5 Securing the Wireless Connection

In a simulated network of this project, the wireless network was been implemented and configured for the WEP (Wired Equivalent Privacy) encryption technology to protect a network eavesdropping attack. WEP is widely supported in wireless devices and the VPN technology was deployed for the company users to provide additional security over a wireless connection. As figure 4 shows, the wireless network of this project has two VLANs, the Guest VLAN (VLAN30) for visitor and the Worker VLAN (VLAN40) for employees. Both VLANs were configured for open authentication and the WEP encryption technology. The WEP encryption configuration for VLAN30 and VLAN40 on a wireless access point (AP) was done as follows:

```
AP(config)#interface dot11radio 0
AP(config-if)#encryption vlan 30 key 3 size 128
12345678901234567890123456 transmit-key
AP(config-ssid)#end

AP(config)#interface dot11radio 0
AP(config-if)#encryption vlan 40 key 3 size 128
98765432109876543210123456 transmit-key
AP(config-ssid)#end
```

The above configuration is meant for encrypted data communication between the access point (AP) and the wireless user with a transmittable 128-bite WEP encryption key at slot 3. Figure 6 below shows a screen shoot of a wireless connection using Worker SSID.



```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\System32>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::599c:ed6e:cee6:d66f%19
   IPv4 Address. . . . . . . . . . . : 192.168.40.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.40.1

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : mydomain.com
   Link-local IPv6 Address . . . . . : fe80::55cd:8d43:f697:22a8%17
   IPv4 Address. . . . . . . . . . . : 172.16.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.128
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : labnet
```

host name) of this site to your brower's trusted site list. This application uses Java™, JavaScript, Cookies, Popup Windows, and IFRAMES. Please adjust your browser settings accordingly.

Figure 6: Wireless Connection

As figure 6 shows, the client device was assigned an IP address 192.168.40.2/24 from the Worker subnet and is connected to the simulated network successfully. The yellow closed key icon at the bottom right side of figure 6 represent a VPN connection and that means, a wireless data connection between the client and the access point is made through well secured VPN tunnel. The VPN connection here provides additional protection for the wireless commination between the client and the access point. Besides that, the above client is also connected to the Internet by using the DNS sever in the test network. The full configuration and testing outputs are presented in appendixes 1 and 5.

5 Discussion and Conclusions

At the present time, company’s owners and network administrators are engaged in protecting their resources and assets by prioritizing the deployment of security measures before offering any kind of network-based services. To build a secure network system, a network administrator needs to select the right kind of technology that fit with the company’s goal and security demands. The purpose of this project were to study the susceptibility of small company network system and build a secure Local Area Network system in the laboratory and recommend the best practice presented today.

An attack to a computer system might happen at any time from anywhere and hence securing a computer and a network system of a company is left without choice. Building a security layer on a network system of a company costs money and time, but it is worth it, considering the losses and damages occurring without it. Protection of a company’s network assets require developing a security plan and policy that decide what needs to be protected and from whom and then implementing the right security measures to stop the losses. The system needs to be monitored continuously for the threat and attacks coming from the inside and outside a network system targeting the company’s resources of any kind.

This study found out that no company’s network system is immune from an attack and identified the source of the vulnerabilities of the system to be lack of security policy, and configuration and technology weakness. In order to avoid the occurrences of such problems on a small company’s network system, a demonstration of the basic network devices configuration, layer 2 and 3 security features implementation, firewall deployment, wireless data encryption, secure wireless access for company users through a VPN connection and remote client VPN connection implementation were deployed on a simulated Local Area Network in the test network. The security system built was tested and found to be working very well and security-tight to protect a small company’s network system and resource from internal and external attacks.

As the network grows in size a user authentication at the local database is not efficient and here by, I recommend to anyone who is interested in studying the subject further in the future to enhance the security system of the project by incorporating RADUS-based authentication and explore advance encryption methods for wireless network.

References

1 Priscilla Oppenheimer. Top-Down Network Design. Indianapolis, USA: Cisco Press; 2011.

2 Etutorials. Flat Network Topology [online]. USA: etutorials; January 2013.
URL:http://etutorials.org/Networking/lan+switching/Chapter+10.+LAN+Switched+Network+Design/Flat+Network+Topology/.
Access on April 5, 2013.

3 Dan Dinicolo. Understanding Network Models/The Cisco Network Design Model [online]. Canada: WebProNews; 2013.
URL:http://www.webpronews.com/understanding-network-models-the-cisco-network-design-model-2004-02.
Acess on April 5 8, 2013.

4 Cisco. Network Topology and LAN Design [online]. USA: Cisco press; January 14, 2000.
URL:http://networkworld.com/ns/books/ciscopress/samples/0735700745.pdf.
Access on April 8, 2013.

5 Randy Ivener. CCNP1:Advance Routing. Indianapolis, USA: Cisco Press; 2004.

6 Paul Boger. CCNA Exploration LAN Switching and Wireless version 4.0. Indianapolis, USA: Cisco Press; 2010.

7 Sean Wilkins, Franklin H.Smith III. CCNP Security SECURE 642-637 Offical Cert Guide. Indianapolis, USA: Cisco Press; 2010.

8 John E. Canavan. Fundamentals of Network Security. London, Britain: Artech House; 2001.

9 R. Shirey, editor. Internet Security Glossary [online]. USA: IETF; 2000.

10 Gregory B. White, Eric A.Fisch, UWdo w. Pooch. Computer System and Network Security. USA: CRC press; 2000.

11 Randy Marchany. Computer and network security in Higer Educstion. USA: Jossey-Bass Inc.; 2003.

12 Steve Elky. An Introduction to Information System Risk Management. USA: SANS Institute; May 31, 2006.

13 Joe Harris. Cisco Network Security Little Balack Book. Arizona, USA: The Coriolis Group, LLC; 2002.

14 B. Fraser, editor. Site Security Handbook. USA: IETF; 1997.

15 S. Kent, BBN Corp, R. Atkinson, editor. Security Architecture for the Internet Protocol. USA: IETF; November 1998.

16 Martin W.Murhammer, Kok-Keong Lee, Payam Motallebi, Paolo Borghi, Karl Wozabal. IP Network Design Guide. USA: International Business MAchine; 1999.

17 Microsoft. TechNet:Public and Private Addresses [online]. USA: Microsoft; 2013.
URL:http://technet.microsoft.com/en-us/library/cc958825.aspx.
Access on April 22, 2013.

18 Daniel Oxenhandler. Desining a Secure Local Area Network [online]. USA: SANS Institute; 2003.

URL:http://www.sans.org/reading_room/whitepapers/bestprac/designing-secure-local-area-network_853.
Access on April 8,2013.

19 Cisco. Cisco Security Appliance Command Line Configration Guide. USA: Cisco Press; 2008.

Appendixes

Appendix 1: Firewall Configuration

```
ASA# show running-config
: Saved
:
ASA Version 8.4(4)1
!
hostname ASA
enable password i0kMXuCr6vRaByXN encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
 switchport access vlan 3
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 10.94.62.251 255.255.255.0
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
banner motd # unautherized user is not prohibited #
ftp mode passive
object network inside-outside
 subnet 192.168.0.0 255.255.0.0
object network dmz-outsdie
 host 192.168.2.3
object network dmz-server-frominside
```

```
 subnet 192.168.2.0 255.255.255.0
object network dmz-server-fromoutside
 host 192.168.2.3
object network int-server
 host 192.168.70.3
object network NETWORK_OBJ_172.16.10.8_29
 subnet 172.16.10.8 255.255.255.248
object network NETWORK_OBJ_192.168.1.0_24
 subnet 192.168.1.0 255.255.255.0
access-list outsidetoDMZ extended permit tcp any host 192.168.2.3 eq
ftp
access-list internal-server extended permit tcp any object int-server
eq ftp
access-list testgroup_splitTunnelAcl standard permit 192.168.1.0
255.255.255.0
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
ip local pool remotepool 172.16.10.10-172.16.10.15 mask
255.255.255.128
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (inside,outside) source static NETWORK_OBJ_192.168.1.0_24 NET-
WORK_OBJ_192.168.1.0_24 destination static NETWORK_OBJ_172.16.10.8_29
NETWORK_OBJ_172.16.10.8_29 no-proxy-arp route-lookup
!
object network inside-outside
 nat (inside,outside) dynamic interface
object network dmz-outsdie
 nat (dmz,outside) dynamic interface
object network dmz-server-frominside
 nat (dmz,outside) static interface service tcp ftp ftp
object network dmz-server-fromoutside
 nat (dmz,outside) static interface service tcp ftp ftp
access-group outsidetoDMZ in interface outside
access-group internal-server in interface dmz
route outside 0.0.0.0 0.0.0.0 10.94.62.254 1
route inside 192.168.30.0 255.255.255.0 192.168.1.2 1
route inside 192.168.40.0 255.255.255.0 192.168.1.2 1
route inside 192.168.50.0 255.255.255.0 192.168.1.2 1
route inside 192.168.60.0 255.255.255.0 192.168.1.2 1
route inside 192.168.70.0 255.255.255.0 192.168.1.2 1
route inside 192.168.100.0 255.255.255.0 192.168.1.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authorization exec authentication-server
```

```
http server enable
http 192.168.100.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
```

```
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh 192.168.100.0 255.255.255.0 inside
ssh timeout 10
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd auto_config outside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
group-policy testgroup internal
group-policy testgroup attributes
 dns-server value 10.94.1.4
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value testgroup_splitTunnelAcl
 default-domain value mydomain.com
username tame password iOr58rasLrrZeZhx encrypted
username tame attributes
 service-type admin
username tame1 password iOr58rasLrrZeZhx encrypted privilege 0
username tame1 attributes
 vpn-group-policy testgroup
tunnel-group testgroup type remote-access
tunnel-group testgroup general-attributes
 address-pool remotepool
 default-group-policy testgroup
tunnel-group testgroup ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
```

```
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:ee11514827e8bf7c2946c10d1e8eced2
: end
```

Appendix 2: Core Switch Configuration

```
CSW# show running-config

Building configuration...

Current configuration : 5317 bytes
!
! Last configuration change at 03:00:03 UTC Mon Mar 1 1993
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname CSW
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$Nh/1$bmSgITR31VtxLu.4mc7Wo.
!
username tame password 7 071B20414B1D180812
no aaa new-model
system mtu routing 1500
ip routing
no ip domain-lookup
ip domain-name mydomain.com
!
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.40.1
!
ip dhcp pool AP_pool_Guest
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.1
!
ip dhcp pool AP_pool_Worker
   network 192.168.40.0 255.255.255.0
   default-router 192.168.40.1
!
!
!
!
crypto pki trustpoint TP-self-signed-2871021440
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2871021440
 revocation-check none
 rsakeypair TP-self-signed-2871021440
!
!
crypto pki certificate chain TP-self-signed-2871021440
 certificate self-signed 01
  3082024C  308201B5  A0030201  02020101  300D0609  2A864886  F70D0101
04050030
```

```
  31312F30  2D060355  04031326  494F532D  53656C66  2D536967  6E65642D
43657274
  69666963  6174652D  32383731  30323134  3430301E  170D3933  30333031
30303031
  30375A17  0D323030  31303130  30303030  305A3031  312F302D  06035504
03132649
  4F532D53  656C662D  5369676E  65642D43  65727469  66696361  74652D32
38373130
  32313434  3030819F  300D0609  2A864886  F70D0101  01050003  818D0030
81890281
  8100BE4A  A175F73F  5386F919  11AB8945  5B497A79  B45136BE  B6CFD58B
062C46F2
  F38C06DD  00052170  D5964B8E  7CE2C021  AC44FB28  EF7EF583  48BDA045
15BBCDAD
  2822CF7E  5495D032  71E59E73  44CFE70E  F305DC4D  EAFD246F  34D97CA6
62F2A054
  906C5291  D4DA6C80  9234C51B  18384B8B  4AD02E35  D743CC87  3932750E
611D986A
  4A2D0203  010001A3  74307230  0F060355  1D130101  FF040530  030101FF
301F0603
  551D1104  18301682  14436F72  655F5377  2E6D7964  6F6D6169  6E2E636F
6D301F06
  03551D23  04183016  801466C6  33FE8BB8  2D166D86  C32FBE33  CC2C7499
1CCE301D
  0603551D  0E041604  1466C633  FE8BB82D  166D86C3  2FBE33CC  2C74991C
CE300D06
  092A8648  86F70D01  01040500  03818100  872E2A78  C8EC8034  EF632F43
8BB282B3
  B24011BB  00FFB7D7  873861FF  F5AEAFA6  3087A870  B931E379  96030151
4838A5C1
  5CDAA100  52C6DD71  1A9BB8CF  6FDD123E  F136D649  C9077668  31528960
8A495BFB
  A38DA12F  A51B433A  95F6C18F  C8D1327F  61B7F3CE  35372032  E894F7F1
9FE994BD
  30F9F5C2 53C060C4 CF90E666 A754874D
        quit
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,30,40,50,60,70,100 priority 0
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
interface FastEthernet0/1
 description "to the ASA device"
 no switchport
 ip address 192.168.1.2 255.255.255.0
!
interface FastEthernet0/2
 shutdown
```

```
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 description " to the AP"
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 30,40,100
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 description " to switch 1"
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 description " to switch 2"
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
```

```
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 description "Guest vlan"
 ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
 description "mobile worker vlan"
 ip address 192.168.40.1 255.255.255.0
!
interface Vlan50
 description "workstation one vlan"
 ip address 192.168.50.1 255.255.255.0
!
interface Vlan60
 description "workstation two vlan"
 ip address 192.168.60.1 255.255.255.0
!
interface Vlan70
 description "server farm vlan"
 ip address 192.168.70.1 255.255.255.0
!
interface Vlan100
 description "management vlan"
 ip address 192.168.100.1 255.255.255.0
!
no ip http server
```

```
ip http access-class 1
ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
logging esm config
access-list 1 permit 192.168.100.0
!
!
banner motd ^C unauthorized user is not prohibited ^C
!
line con 0
 access-class 1 in
 exec-timeout 0 0
 password 7 06120E2C495A081400
 logging synchronous
 login
line vty 0 4
 access-class 1 in
 exec-timeout 5 0
 privilege level 15
 password 7 06120E2C495A081400
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 no login
!
End
```

Appendix 3: Access Switch (SW1) Configuration

```
SW1# show running-config

Building configuration...

Current configuration : 4308 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$G6/O$eoEkanvGfe6nCsCUlqw5w.
!
username tame privilege 15 secret 5 $1$H/Z2$wkFjs2z5SjmrcTNwVOZf6/
aaa new-model
!
!
!
!
!
aaa session-id common
system mtu routing 1500
ip subnet-zero
!
ip domain-name mydomain.com
!
!
crypto pki trustpoint TP-self-signed-2876515968
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2876515968
 revocation-check none
 rsakeypair TP-self-signed-2876515968
!
!
crypto pki certificate chain TP-self-signed-2876515968
 certificate self-signed 01
  30820248 308201B1 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 32383736 35313539 3638301E 170D3933 30333031
30303030
  34365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32
38373635
  31353936 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100B266 A4DA86C3 4B259BB5 8250DBED 077258E3 3F87B1AB 1B7CC99B
0CF0BD4E
```

```
  C7CCEEB3  DC0791F0  C9D4313F  614D10F8  FE40BBE6  006DBB3A  2C56FF66
7757A665
  55D32D53  83F0B397  0A0211E4  A5D72EB3  8204A138  C3E2D4DD  5CAF9D50
6AF46A2C
  FC0D2195  915C3E10  FC2B9197  081E54D7  01CBFC95  AEC564DB  DF458FFD
626F7250
  F3B90203  010001A3  70306E30  0F060355  1D130101  FF040530  030101FF
301B0603
  551D1104  14301282  10535731  2E6D7964  6F6D6169  6E2E636F  6D301F06
03551D23
  04183016  8014E236  018E8541  BBA6A323  C59B0BFC  7BA03AB2  0E62301D
0603551D
  0E041604  14E23601  8E8541BB  A6A323C5  9B0BFC7B  A03AB20E  62300D06
092A8648
  86F70D01  01040500  03818100  4AFA61A3  8A0E0257  1D1F0A68  87D8AFD8
7A054A10
  999235D3  9B29595A  1CCBCC13  C4229593  D729088F  0DFB824C  CD63FD6E
D2C9B238
  B9C6C236  52AC2CED  4058A6A5  DCBC0996  F37C1553  87647CB1  8745DCA7
6D7EF50A
  5B91D6A2  944D987F  F83FFA88  DDD42651  86647C88  AC569FEA  DCCDC781
F629F8D8
  39ECD3BD DA1F4270 8291D717
  quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 description "to core switch"
 switchport trunk native vlan 100
 switchport trunk allowed vlan 30,40,50,60,70,80,100
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 description "workstation one access port"
 switchport access vlan 50
 switchport mode access
 switchport port-security
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 description "management workstation access port"
 switchport access vlan 100
 switchport mode access
 switchport port-security
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
```

```
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.100.1
no ip http server
ip http access-class 1
ip http secure-server
access-list 1 permit 192.168.100.4
!
control-plane
!
banner motd ^C unauthorized user is not prohibited ^C
!
line con 0
 access-class 1 in
 exec-timeout 5 0
 password 7 0010120B014F0A0B0A
 logging synchronous
line vty 0 4
 access-class 1 in
 exec-timeout 5 0
 password 7 021205560E
 logging synchronous
 transport input ssh
line vty 5 15
!
end
```

Appendix 4: Access Switch (SW2) Configuration

```
SW2# show running-config
Building configuration...

Current configuration : 4328 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9u6H$Y33Dbas7.NTucwQ2BxJES1
!
username tame password 7 120D041A171F0D092F
aaa new-model
!
!
!
!
!
aaa session-id common
system mtu routing 1500
ip subnet-zero
!
ip domain-name mydomain.com
!
!
crypto pki trustpoint TP-self-signed-2878419584
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2878419584
 revocation-check none
 rsakeypair TP-self-signed-2878419584
!
!
crypto pki certificate chain TP-self-signed-2878419584
 certificate self-signed 01
  30820248  308201B1  A0030201  02020101  300D0609  2A864886  F70D0101
04050030
  31312F30  2D060355  04031326  494F532D  53656C66  2D536967  6E65642D
43657274
  69666963  6174652D  32383738  34313935  3834301E  170D3933  30333031
30303030
  34365A17  0D323030  31303130  30303030  305A3031  312F302D  06035504
03132649
  4F532D53  656C662D  5369676E  65642D43  65727469  66696361  74652D32
38373834
  31393538  3430819F  300D0609  2A864886  F70D0101  01050003  818D0030
81890281
  8100A1DC  D170542B  245EDCD1  DC993EED  CB5FC320  D764AF42  85286AA0
401DA57A
```

```
  E3202617  830828A6  395074F2  0089CB14  09337048  A5E878A0  E4C07E47
934FE8A4
  D2D4AEA9  BB1A31AB  AA9ABCD4  81EC72C3  D7D17F3A  1A8DAF9D  150CF31E
4AD65FC7
  B0B63029  CAE3460D  E1E68071  1EFBF2EA  ED256D21  9BC8376A  0BD3CEFC
B01A4C30
  27550203  010001A3  70306E30  0F060355  1D130101  FF040530  030101FF
301B0603
  551D1104  14301282  10535732  2E6D7964  6F6D6169  6E2E636F  6D301F06
03551D23
  04183016  8014FC46  FAD07283  742702AB  2A7539F9  E77347F1  1139301D
0603551D
  0E041604  14FC46FA  D0728374  2702AB2A  7539F9E7  7347F111  39300D06
092A8648
  86F70D01  01040500  03818100  0B5971C6  0DF1382E  1CA59FB4  B6E5E30F
CD9C10BE
  D814F4CD  361FD35D  97C2783B  773FAD13  D7DEB374  F5B64D1E  CE3582C7
6EBE839D
  68C11940  29515570  D2244880  821B6DA1  D4E6033D  B90F6AB4  C2333F3E
AB841EE9
  18850678  36F20FD7  D4581828  66C90F42  96A885A3  2764ED50  F27CCB6A
8C05EE4A
  CFA572AE E09108C8 347DF3F9
  quit
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 10
!
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
```

```
 description "to core switch"
 switchport trunk native vlan 100
 switchport trunk allowed vlan 30,40,50,60,70,100
 switchport mode trunk
 switchport nonegotiate
 storm-control broadcast level 50.00
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 description "workstation two access port"
 switchport access vlan 60
 switchport mode access
 switchport port-security
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 description "internal serve access port"
 switchport access vlan 70
 switchport mode access
 switchport port-security
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
```

```
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan100
 ip address 192.168.100.3 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.100.1
no ip http server
ip http access-class 1
ip http secure-server
access-list 1 permit 192.168.100.4
!
control-plane
!
banner motd ^C unautherized user is not prohibited ^C
!
line con 0
 access-class 1 in
 exec-timeout 5 0
 password 7 051F070224584F041C
 logging synchronous
line vty 0 4
 access-class 1 in
 exec-timeout 5 0
 password 7 051F070224584F041C
 logging synchronous
 transport input ssh
line vty 5 15
 exec-timeout 0 0
!
end
```

Appendix 5: Access Point Configuration

```
AP#show running-config
Building configuration...

Current configuration : 6194 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP
!
!
ip subnet-zero
ip domain name mydomain.com
ip name-server 10.94.1.4
!
!
aaa new-model
!
!
aaa group server radius rad_eap
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
dot11 ssid guest
   vlan 30
   authentication open
   mbssid guest-mode
!
dot11 ssid worker
   vlan 40
   authentication open
   mbssid guest-mode
!
!
crypto pki trustpoint TP-self-signed-3139600724
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3139600724
 revocation-check none
 rsakeypair TP-self-signed-3139600724
!
!
crypto ca certificate chain TP-self-signed-3139600724
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 33313339 36303037 3234301E 170D3133 30343232
31353331
  33305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33
31333936
  30303732 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100E081 0480ACB9 92D5E4E5 5D4311F5 DE462CF8 B58E0B8D C792A58B
5403DF84
  E27D17FE 66269146 5F43A7A5 CDF54913 FEF46420 9D036439 A59D4D43
64453426
  5EA474F2 23A5AE8B BBB4D476 231EDA9B 824C4C4A D120F2D5 4EF54E6F
658D0F4B
  66DD8309 A5AF25EE 028537AA 066FFD62 DE0B7856 17CD242B 1CAB65E1
8DF89D82
  2FEB0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 148D41AC 6EEF8A7A 835873CB B8C3543E 6C2CEC20
93301D06
  03551D0E 04160414 8D41AC6E EF8A7A83 5873CBB8 C3543E6C 2CEC2093
300D0609
  2A864886 F70D0101 04050003 81810003 CEA0FC6A 70A758C2 AA4183A6
5D12CC84
  1E059CC0 035DCD47 8B5E1B4D 13C82F0B 6E26EDBE 95BB8912 E77DB4BB
AB64C826
  A27004A3 B10F8D8D 4EA418EF 7158CC07 2E7B414B D8A941E5 331F6B7E
42BBE77E
  514630DE C499A855 70E61EF7 3779CE0D 39BE34E4 4BD13DF4 B9DAEB3F
340B1B0F
  23971EC3 9AFCAB2B 88616BAA 959E41
  quit
username tame privilege 15 password 7 120D041A171F0D092F
username tame2 password 7 09584F041C11161F0E5E
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 encryption vlan 30 key 1 size 128bit 7 F70212836BFB29783FA0A5E65A95
transmit-key
 encryption vlan 30 mode wep optional
 !
 encryption vlan 40 key 1 size 128bit 7 E6150A7B949EC21B725817485642
transmit-key
 encryption vlan 40 mode wep mandatory
 !
 encryption vlan 100 key 1 size 128bit 7 B40E12774AB6C52D1761DC68F37A
transmit-key
 encryption vlan 100 mode wep mandatory
 !
 broadcast-key vlan 30 change 300 membership-termination capability-
change
 !
 broadcast-key vlan 40 change 300 membership-termination capability-
change
 !
 broadcast-key vlan 100 change 300 membership-termination capability-
change
 !
 !
 ssid guest
 !
 ssid worker
 !
 mbssid
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0
36.0 48.0 54.0
 station-role root
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
 bridge-group 40 spanning-disabled
!
interface Dot11Radio0.100
 encapsulation dot1Q 100 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 hold-queue 160 in
!
interface FastEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
!
interface FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 no bridge-group 40 source-learning
 bridge-group 40 spanning-disabled
!
interface FastEthernet0.100
 encapsulation dot1Q 100 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.100.5 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.100.1
no ip http server
ip http authentication aaa
ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
access-list 1 permit 192.168.100.4
access-list 111 permit tcp any any neq telnet
radius-server local
  no authentication eapfast
  no authentication mac
  nas 192.168.100.5 key 7 06120E2C495A081400
  user tame nthash 7
040B2D5329751A175D3D5D36475A5B257C7E007B10637044574353537380A0676
```

```
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.100.5 auth-port 1812 acct-port 1813 key 7
03105A06031B20414B
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
banner motd ^C unautherized user is not prohibited ^C
!
line con 0
 access-class 1 in
 password 7 1403130609102B2621
line vty 0 4
 access-class 1 in
 password 7 010707095E1F070224
 transport input ssh
!
End
```

Appendix 6: Testing Listing

Verification of Inside Network Connection

```
SA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.94.62.254 to network 0.0.0.0

S    192.168.30.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    192.168.60.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    192.168.40.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    172.16.10.10 255.255.255.255 [1/0] via 10.94.62.118, outside
C    10.94.62.0 255.255.255.0 is directly connected, outside
S    192.168.50.0 255.255.255.0 [1/0] via 192.168.1.2, inside
C    192.168.1.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, dmz
S    192.168.70.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S    192.168.100.0 255.255.255.0 [1/0] via 192.168.1.2, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.94.62.254, outside
```

```
CSW#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l -
LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*     0.0.0.0/0 [1/0] via 192.168.1.1
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.1.0/24 is directly connected, FastEthernet0/1
L         192.168.1.2/32 is directly connected, FastEthernet0/1
       192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.30.0/24 is directly connected, Vlan30
L         192.168.30.1/32 is directly connected, Vlan30
       192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.40.0/24 is directly connected, Vlan40
```

```
L        192.168.40.1/32 is directly connected, Vlan40
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, Vlan50
L        192.168.50.1/32 is directly connected, Vlan50
      192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.60.0/24 is directly connected, Vlan60
L        192.168.60.1/32 is directly connected, Vlan60
      192.168.70.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.70.0/24 is directly connected, Vlan70
L        192.168.70.1/32 is directly connected, Vlan70
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Vlan100
L        192.168.100.1/32 is directly connected, Vlan100


ASA# ping 192.168.100.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Verification of VPN Connection

```
ASA# show vpn-sessiondb remote

Session Type: IKEv1 IPsec

Username     : tame1                  Index        : 1
Assigned IP  : 172.16.10.10           Public IP    : 10.94.62.113
Protocol     : IKEv1 IPsec
License      : Other VPN
Encryption   : AES256 AES128          Hashing      : SHA1 SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Group Policy : testgroup              Tunnel Group : testgroup
Login Time   : 15:06:52 UTC Mon Apr 29 2013
Duration     : 0h:09m:18s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Verification of Wireless Connection

```
AP#ping 192.168.100.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Verification of NATs Translation

```
ASA# sh xlate
16 in use, 118 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T
- twice
       e - extended
NAT from inside:192.168.1.0/24 to outside:192.168.1.0/24
    flags sI idle 1:16:58 timeout 0:00:00
TCP PAT from dmz:192.168.2.3 21-21 to outside:10.94.62.251 21-21
    flags sr idle 0:26:45 timeout 0:00:00
TCP PAT from dmz:192.168.2.0/24 21-21 to outside:10.94.62.251 21-21
    flags sr idle 0:26:45 timeout 0:00:00
TCP PAT from inside:192.168.100.4/1907 to outside:10.94.62.251/1907
flags ri idle 0:00:57 timeout 0:00:30
TCP PAT from inside:192.168.100.4/1901 to outside:10.94.62.251/1901
flags ri idle 0:00:58 timeout 0:00:30
TCP PAT from inside:192.168.100.4/1893 to outside:10.94.62.251/1893
flags ri idle 0:00:58 timeout 0:00:30
TCP PAT from inside:192.168.100.4/1885 to outside:10.94.62.251/1885
flags ri idle 0:00:59 timeout 0:00:30
UDP PAT from inside:192.168.100.4/64375 to outside:10.94.62.251/64375
flags ri idle 0:02:33 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50535 to outside:10.94.62.251/50535
flags ri idle 0:00:31 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50532 to outside:10.94.62.251/50532
flags ri idle 0:00:31 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50530 to outside:10.94.62.251/50530
flags ri idle 0:01:56 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50528 to outside:10.94.62.251/50528
flags ri idle 0:01:56 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50524 to outside:10.94.62.251/50524
flags ri idle 0:01:56 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50522 to outside:10.94.62.251/50522
flags ri idle 0:01:57 timeout 0:00:30
TCP PAT from inside:192.168.30.2/50510 to outside:10.94.62.251/50510
flags ri idle 1:05:47 timeout 0:00:30
UDP PAT from inside:192.168.70.3/52291 to outside:10.94.62.251/52291
flags ri idle 0:05:06 timeout 0:00:30
```