Network Security for a Communications Company

By
Renee M Gunderson

A Research Paper

Submitted in Partial Fulfillment of the
Requirements for the
Master of Science Degree in
Management Technology

Approved for Completion of 3 Semester Credits
INMGT-735 Field Problem

_____
Dr. John Burningham
Research Advisor

The Graduate School
University of Wisconsin-Stout
December 2002

The Graduate School
University of Wisconsin-Stout
Menomonie, WI 54751

ABSTRACT

____ Gunderson Renee M
(Writer)(Last Name) (First) (Initial)

Network Security for a Communications Company
(Title)

Management Technology Dr. John Burningham December, 2002 40
(Graduate Major) (Research Advisor) (Month/Year) (No. of Pages)

__ Publication Manual of the American Psychological Association__ _
(Name of Style Manual Used in this Study)

XYZ Communications (XYZ Communications is a pseudonym for the company's actual name) is a wireless communications company specializing in two-way radio frequency such as cellular and paging systems and is based in the Midwest. Electronic messages are sent throughout the United States via phone, email or http requests. XYZ Communications uses the Internet and Plain Old Telephone System extensively as a transport for their paging and technical support systems.

Due to the company's connection with networks outside of their own Local Area Network , XYZ Communications understands the need for security and has taken some measures to secure their current network infrastructure. However, even with this understanding and their current security measures, XYZ

has recently become the victim of multiple network attacks. In light of these new attacks, XYZ Communications would like to reexamine their current network with the intent of making it more secure from intruders. This research paper will analyze the current network infrastructure and provide suggestions for improving network security on the network's perimeter. The study was conducted by reviewing relevant literature, analyzing the network infrastructure and providing suggestions for improving security.

Table of Contents

List of Figures

Chapter 1

Background and Purpose

The company, XYZ Communications is a wireless communications company specializing in two-way radio frequency such as cellular and paging systems. Their electronic messages are sent throughout the United States via phone, email or http requests. XYZ Communications uses the Internet and Plain Old Telephone System extensively as a transport for their paging and technical support systems.

Due to the company's connection with networks outside of their own Local Area Network (LAN), XYZ Communications understands the need for security and has taken some measures to secure their current network infrastructure. However, even with this understanding and their current security measures, XYZ has recently become the victim of multiple network attacks. In light of these new attacks, XYZ Communications would like to reexamine their current network with the intent of making it more secure from intruders.

While it is impossible to completely thwart all network intrusions, XYZ Communications has requested that I make their network more secure from intruders while still allowing their customers access to use the system. In consideration of a possible Internet attack after the security measures have been implemented, there must also be an emergency backup plan in place so the customers can still continue to use the network unhindered.

Objectives

The goals of this study are to:

1.0 Analyze the current network infrastructure to determine network security weaknesses.

2.0 Provide suggestions for securing the network that will block unauthorized users while maintaining ease of access for authorized users.

3.0 Suggest a backup plan in case the network is compromised by unauthorized users or by internal user error.

Importance of the Study

XYZ Communications is a two-way radio communications company and is therefore entirely dependant upon its computer network for sending and receiving electronic correspondence. XYZ Communications has multiple communication sites with access to the public network. This leaves them vulnerable to external network intruders. If this study is not performed and their network is left unsecured, network security could be compromised with the risk of intrusions bringing the network down. Since the business cannot function or earn money without its network, downtime could virtually eliminate this company (Prescott, T. Personal Communication, May 2002).

Limitations

Due to the sensitive nature of this field project (security), the actual name and IP addresses of the company will not be divulged and the fictitious name of XYZ Communications will be used. The company's network includes both an

internal network and an external network (the telephone system). This study will be limited to securing the perimeter of the companies Local Area Network and not its connection to the nationwide telephone system. It is assumed that the nationwide telephone system will be secured by the service providers themselves. The researcher will only be responsible for providing network infrastructure solutions. The companies current network administrator will address any server required issues. The network equipment being used by the company on the perimeter network is Cisco equipment, therefore all configuration information will be based upon the Cisco Internetwork Operating System.

Chapter 2

Literature Review

Historical Perspective

Computer networks started as a way for government researchers to share information. In the event of a nuclear war, the Department of Defense (DOD) envisioned a network that would not have a single point of failure. To satisfy this desire, the DOD created ARPANET, a national network of computers used to communicate and share data. This small network was comprised of researchers, universities and government agencies. Its sole purpose was to ensure constant connectivity even in times of war. At that time, security of the data wasn't a concern because the only people who were connected with ARPANET were agencies that had contracts with the DOD.

ARPANET grew into what we know today to be the Internet. The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) as a way to get information moved around the network. TCP/IP was created as an open protocol to facilitate communication. TCP/IP was not created to worry about security and therefore has some inherent security flaws just waiting for someone to compromise.

The Internet has grown at a phenomenal rate and now millions of people use this network. With this growth comes more risks and more people who look to compromise businesses that are connected to the Internet. These people are both novice users with active curiosity and professional hackers with sole intent

of stealing information or inflicting damage. For this reason, security is needed to patch up the inherent flaws in TCP/IP and stop attacks to keep data and internal networks safe.

In 2002 the Computer Security Institute (CSI), along with the Federal Bureau of Investigation, conducted a computer securities survey and received responses from 503 security professionals within the United States. They found that ninety percent of those who responded experienced computer intrusions within the past year and eighty percent incurred financial losses due to those security breaches. Approximately half of those who responded to the survey reported financial losses totaling $455 billion. The largest portion of those losses was $170 billion from information theft (CSI, 2002). Security breaches broadly include everything from simply viewing data, to Denial of Service (DoS) attacks, to data theft, to introducing malicious codes (viruses) into the network. In January 2002, Computer Economics magazine estimated that worldwide, viruses introduced into computer networks would cost $13.2 billion.

According to the IDC, spending on IT products and services is expected to exceed $282.5 billion in 2003 (Computer Security Spending Statistics, 2000). As IT product and services increase, IT network infrastructures and people who want to invade or intrude upon those networks will increase.

Every year, a group of security professionals called the Honeynet Project holds a contest to see who can break into a computer network system the fastest. In March of 2001, the Honeynet Project targeted a university as their point of intrusions. The winner, a math major from the University of Bonn, took less

than a minute to compromise the network, yet it took network professionals more than 34 hours to determine what the student had done (Lemos, R. 2001). This example demonstrates that compromising a computer network is simply too easy and if measures aren't undertaken to secure computer networks worldwide, the cost of network intrusion to government, businesses and individuals will continue to skyrocket.

Current Perspective

According to Micheal Wenstrom, the three main reasons for network insecurities are, "Technology weakness, Configuration weakness and Policy weakness."(Wenstrom, 2001) Technology weaknesses are inherent flaws in the technology being used. This includes the flaws in TCP/IP's implementation of NFS that allows unauthenticated users access to the network. Configuration weaknesses are those that are misconfigured by the network administrator that somehow allows access for those who are not welcome. An example of a configuration weakness would be not shutting down or encrypting Telnet access, thereby allowing others to remotely access the equipment. A policy weakness is a flaw in the company's stated policy identifying computer and network usage. Installation of unauthorized software can lead to viruses and piracy on the network if the security policy does not specifically make a statement against it. This would be considered a flaw in the stated policy and not a mistake of the end users. There are many people out on the Internet willing and capable of taking advantage of a company's network.

According to Wenstrom, some security threats to be aware of include reconnaissance, unauthorized access, Denial of Service and data manipulation. Reconnaissance is the act of monitoring and mapping a network usually with the intent of later using the information gathered to infiltrate the network. Reconnaissance is done to map the network infrastructure, obtain information about the computer operating systems being used, and to gain logins and passwords. Once the intruder knows how to get to the network and has the logins and passwords for the equipment they can gain complete access of the systems; they then become an unauthorized user. Sometimes hackers do not want to access the network, instead their intent may be only to disable the network making it impossible for authorized users to access it.

One way to disable a network is to start a DoS attack. Two variations of DoS are resource overloads and Out-of-Band data attacks. Resource overloads are simply an attempt to overload the resources bandwidth or buffers by sending massive amounts of invalid data. The overload of data will fill the bandwidth and the buffers on the network with useless information, forcing legitimate users to be dropped or redirected from the network. Out-of-Band data attacks manipulate the IP header that in essence confuses the network equipment and causes the equipment to cease operation.

Finally, data manipulation is another broad category of network threats that can manipulate and replay data. Most often the goal with data manipulation is to change or manipulate a website to display something other than what was

intended by the company. Once the researcher is aware of the possible network threats they can begin to defend against those security threats.

Securing the Network

Security Policies and Banner Messages

When starting a security implementation the researcher must first consider the company's security policy. "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide" (Fraser, 1997). The researcher must first find out if there is a security policy in place. If there is a security policy in place, then it must be abided by in the implementation. If there is not a Security Policy in place, then one must be discussed, agreed upon and written. Security Policies have to accomplish three main objectives:

Identify the Organizations objectives.

Document the resources to be protected.

Identify and map the network infrastructure.

(Chapman Jr, Fox, 2001)

Sample security policies can be seen in Barman's book, *Writing Information Security Policies*. After writing and implementing a security policy, the researcher/designer needs to begin considering the actual security measures that need to be implemented.

Most security breaches come from the inside of the company, because of that, the first line of defense against a network attack is to physically secure the network equipment. This requires that the company installs network

infrastructure equipment such as routers, switches and servers in a secure, locked room. Access should only be allowed to those who are trusted and need the access. Once the designer has physically secured the network, they need to become concerned with the configurations of the equipment including the banner messages, password encryption, shutting down unused protocols and ports, configuring VLANs and Access Control lists. Banner messages are messages that a person sees when they enter a router or a switch. Banner messages should warn and make a statement about authorized versus unauthorized use. The Banner message should never welcome the user. Once the administrator has made a statement welcoming the user, even unauthorized users may, in the eyes of the law, become authorized. Legally an intruder may be doing nothing wrong if they are being welcomed as they enter the router or switch. According to Akin (2002), a banner message has four goals:

1.0 Be legally sufficient for prosecution of intruders

2.0 Shield administrators from liability

3.0 Warn users about monitoring or recording of system use

4.0 Not leak information that could be useful to an attacker

A good example of a properly stated banner message is: “This is an actively monitored system. Unauthorized access prohibited” (Depaul University, 2002).

Password Encryption

By default routers store the telnet and console passwords in clear text, which also means that when someone logs into either a telnet or console session

in a router the passwords are sent across the network in clear, easily obtainable text. When the router gets configured, telnet and console passwords need to be configured using either the "Service Password-encryption" or the "enable secret" command. These commands will change the Telnet and console passwords from their clear text default to an encrypted password that is much more difficult to decipher.

Disabling Ports and Protocols

By default most networking equipment has certain services that are automatically initiated when the equipment is powered up. By using a command such as *nmap* in Linux, an intruder can do a port scan, which will display all open/listening ports on the device (Scambray, McClure, & Kurtz, 2001). Once a list of open ports has been discovered, they can be used to pass or redirect data into the network. Many of the ports and protocols running on equipment are not being used by the network and should be shutdown. Some of the protocols that start up automatically are being used, but they may have some inherent flaws that need to be repaired or shutdown. Protocols such as Internet Control Message Protocol (ICMP), Telnet, Simple Network Management Protocol (SNMP), Cisco Discovery Protocol (CDP) and Network Time Protocol (NTP) are among those that should either be disabled or have their access controlled (Akin, 2002).

ICMP is instrumental in network testing by allowing the technician to ping or traceroute to a device. When a network technician pings a device, the device, if it is valid, working and accepting pings, will respond back with its IP

address and the time it took for the communication. When someone does a Traceroute to a device, all of the devices along the path respond, thereby telling the user exactly what devices it has to go through in order to get to a certain network. The knowledge that Ping and Traceroute provide for a network administrator is invaluable; unfortunately this knowledge is also used by intruders to profile the network.

In an effort to stop intruders from obtaining information from ICMP, a network administrator can deny incoming ICMP requests and shut down the ICMP redirect service. Denying ICMP requests can be done on Cisco equipment by creating an access control list that will deny the traffic. The administrator can issue the command *no ip redirects* at the interface configuration mode to stop ICMP redirects on Cisco equipment.

Telnet is another widely used protocol that allows users to remotely log into network equipment. Telnet does not use encryption; passwords are sent across the network in cleartext and therefore easily discovered by intruders. Telnet should be turned off on all network equipment. If remote access to parts of the network is absolutely necessary, a terminal protocol such as Secure Shell Daemon (Sshd) should be used because it provides authentication and encrypted passwords (Wimpie du Plessis, 2001).

SNMP is used by network administrators to allow them to monitor and manage the network. SNMP sends out an alert message when there is a fault in the network called a "trap" and managers send out messages to get information about the network, these messages are called "requests". These messages use

community strings that are sent across the network in cleartext allowing an intruder to capture the text and use it to change router configurations ("Increasing Security on IP Networks," 2001).

CDP is a Cisco propriety protocol that runs on Cisco routers and switches which allows the routers and switches to create a table of its directly connected Cisco equipment. The command *show CDP neighbors*, displays a table of all the directly connected Cisco equipment, the type of equipment, platform, Operating System, holdtime and which interface it is connected to. Once an intruder has gained access to one router they can then get a good view of the entire network by issuing the *show CDP neighbors* command. See Figure 1 for the response to the *show CDP neighbors* command.

Figure 1: Show CDP Neighbors display

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Lab_B	Ser 0	147	R	2500	Ser 1
CCNA_HubConfigura	Eth 0	156	T S	WS-C2912-X	Fas 0/2
CCNA_HubConfigura	Eth 1	156	T S	WS-C2912-X	Fas 0/1

By reviewing the previous figure, the intruder can determine the equipment platform, equipment type and what interface the equipment is connected to. For example, by looking at figure 1 the intruder knows the the directly connected equipment is a Cisco 2500(Platform) series router(Capability R) connected to a Catalyst 2912(Platform WS-2912-X) switch on FastEthernet 1 and 2(Port ID Fas 0/1, Fas 0/2). Using this knowledge, the intruder can then telnet into the router

or switch and begin to make their way through the network until they have reached their goal. CDP can also be a useful network management tool, but it is extremely vulnerable to intruders and should be shut off whenever security is of concern.

Finally, NTP is another extremely vulnerable protocol that should be disabled. NTP is a protocol that allows all network equipment to be synchronized to the same time. Unfortunately, some security measures depend upon time and if the time is corrupted on the overall system, the security measures can be circumvented. One of the best ways to ward off network attacks is to shutdown ports and protocols that are not being used.

VLANs, Routers and Access Control Lists

Cisco switching equipment allows a user to create Virtual LANs (VLAN) which are a logical grouping of devices and users. VLANs help to secure a network by segmenting the network and only allowing certain users access to the VLAN. For example, a certain VLAN may only contain a select group of users and only those users may be allowed to access the mail server. Security over a VLAN is further enhanced by the use of routers and access control lists over the entire network. Routers can use access control lists to only permit and deny certain traffic. Access control lists are a list of criteria that a packet must meet in order to be forwarded.

Firewalls

A Firewall is computer that controls access between networks and is most often placed at the perimeter of the network between the Public and Private

networks. There are three types of firewalls: packet filter, proxy filter and stateful. A packet filtering firewall filters packets at Layer 2 and 3 of the Open Systems Interconnect (OSI) model and closely resembles a router with access lists defined. A proxy filtering firewall runs at the Application layer of the OSI model and responds to requests from outside users while never allowing the users to actually enter the network. Stateful firewalls use the best from both proxy and packet filtering firewalls with the ability to both filter and log packets.

Many different vendors such as Cybergaurd, Ascend and Cisco offer firewall hardware. Cisco offers what they call the PIX Firewall. The PIX Firewall is a stateful hardware firewall. By default, the PIX Firewall does not allow any traffic through to the protected network. If it is desired to allow traffic through, the firewall must then be configured using translations to allow traffic through. Some PIX Firewall models have a failover feature that allows another firewall to take over if the main firewall goes down. For this reason, the PIX Firewall will be the firewall of choice for this project. As stated earlier, the PIX Firewall can also be configured for logging and authentication. This is another valuable asset because it allows the administrator to monitor access and usage of the network for any unusual activity.

Many reported cases of information theft occur from within the network and not from external intruders. This knowledge makes it necessary to log network activity. This activity is often recorded to a logging server. Allowing the network administrator to view the network activity at any time. Logging and

authentication should be done with a server that is separate from both the routers and firewalls.

Redundancy

When securing a network, an administrator also needs to consider what will happen in the event their network is compromised. Generally, this contingency plan incorporates redundant equipment, redundant links and server clustering to be sure that if one piece of equipment or one link fails, that another one comes online with a minimal interruption in service. When provisioning links from an ISP each link should be obtained from separate providers. This way, if one of the ISPs has a network problem that causes the network link to go down, the other link provided by an error free ISP can come up and continue to provide users with service.

Cisco routers use Hot Standby Routing Protocol (HSRP) that allows redundant routers on the network. When a network is using HSRP, a second router can come online and take over the routing job of the compromised router. Spanning Tree protocol allows for redundant switch links on a network. This protocol is on by default in most switching equipment.

Finally, once the network infrastructure itself is redundant, the servers should be made to have backups. Servers can be clustered to provide redundancy and load balancing. Clustering is a method of connecting two or more computers to provide a singe service (Bookman, 2003). For example, by connecting two computers both running as Email servers, to provide backup and load balancing for the email system. Load balancing is when two or more

computers are connected to distribute data across more than one server (Bookman, 2003). Load balancing allows communication between users and services to speed up because the data has more than one connection to traverse.

Chapter 3

Research Methodology

The purpose of this study is to identify and eliminate insecure areas of XYZ Communication's internal LAN. The methodology used to accomplish these goals were a review of literature, an analysis of the current network infrastructure and recommendations for correctly securing the network. Cisco recommends the following steps for network security:

Know your enemy:

Understand who may want to infiltrate the network.

Count the cost:

Securing a network always incurs costs, either from usage delays or equipment costs.

Identify assumptions:

This involves knowing what your assumptions are, because making assumption may cause you to misidentify the threats to your network.

Control your secrets:

Secrets are things like passwords that will allow intruders to circumvent your security measures.

Remember human factors:

This step involves understanding that people want change and policies to be as easy and pain free as possible. This means that if their passwords are too difficult to remember they will write them

on their computers (huge security leak). If your servers are locked in a closet people will probably prop the door open instead of bothering with locking the door.

Know your weaknesses

Know the networks weaknesses and how intruders can exploit them.

Limit the scope of access:

If intruders do enter the network limit how far they can get in and how much damage they can do.

Understand your environment:

This step involves base lining your network or simply finding out what its normal operational levels are. When you know what is normal you will more easily be able to see if someone is trying to infiltrate your network.

Limit your trust:

Know what software you company can't do without and don't assume that its bug free.

Physical Security:

This involves physically securing computer and network hardware. The general public or company population does not need, nor should it have access to the company's routers and servers; lock it down.

Security is pervasive:

> Know that any change that you make to your computers or network infrastructure will have an affect on the networks security. Before making any changes, consider the affect it will have upon the computer network security ("Increasing Security on IP Networks," 2001).

Once the network has been analyzed, suggestions for securing the network will be based upon the previous review of literature and the network analysis.

Chapter 4

The Study

The suggested Cisco steps for analyzing the network, revealed threats, costs, assumptions and weaknesses at XYZ Communications. People who may interested in infiltrating the network would be competitors or people just interested in being able to compromise a network for the thrill of it. Given the current network infrastructure and the nature of the business the benefits of securing network far outweigh the costs. It is assumed that the ISP are securing their end of the network connection. XYZ Communication's points of weakness are their connections to the public Internet and this will become an area where the network will be secured.

The study began by analyzing the current network infrastructure. Figure 2 shows the current network setup. There are currently about 150-200 users both internal and external. The users have access to multiple email, web and paging servers. The users and servers are provided with an outside Internet connection via a router that is connected to the central switch and a T1 provisioned from Internet Service Provider 1 (ISP1). If ISP1 were to fail, Internet Service Provider 2(ISP2) would become live (ready to send and receive data) and the user traffic would all be transferred to ISP2. There are currently two separate address allocations being used inside the network, a Class B, 172.16.x.x and a Class C, 197.12.74.x. The network currently uses Enhanced Interior Gateway Routing Protocol (EIGRP) and Telocator Network Paging Protocol (TNPP) for

network transport. EIGRP is a routing protocol that transports data across the network. TNPP is a paging protocol used to move paging data inside the network and between paging terminals. TNPP is the protocol of choice because it is a protocol that can be used with all kinds of different paging terminals and it is not a propriety protocol.

After the researcher performed the physical analysis of the current network, an analysis of the company goals was required. The company was expanding rapidly and the leaders were looking for a network design that was scalable, secure, redundant and cost effective. Their desire was to keep intruders out of their network while allowing trusted users in and providing a backup plan if a part of the network goes down or if an area of the network is compromised by an intruder.

As previously stated, the first step in securing the network is to create a security policy to define acceptable use, authorization, Internet usage, campus usage and remote access and what to do when a problem is noticed. A security policy should be individual and specialized to the company implementing it; therefore this study did not provide an exact policy to follow. Internet links to sample security policies are provided in Appendix or can be found in Barman's book, "Writing Information Security Policies."

Once a security policy has been written the company can move on and begin to make changes to secure the network. XYZ Communications already has a banner message, but it is suggested that the banner message be changed to include an indication of privacy and logging. The banner message should be

changed from " No unauthorized Access is permitted," to "This is a private system. No unauthorized access is permitted. All accesses to this service is logged." Changing the message will better follow banner message generally accepted rules and allow for a more thorough warning to unauthorized usage, thereby allowing for a better opportunity to prosecute unauthorized users.

Unused IP address offer the opportunity for a intruder to become a client on the network by "stealing" an IP address from the companies address range and then masquerading as a host on the internal network. The IP addressing should be changed from the Class B, 172.16.x.x scheme to a Class C, 192.168.1.x to trim away any unused IP addresses.

XYZ Communications needs to configure VLANs 1, 2, 10, 20, 30, 40, 50 and 60 to logically separate users and workgroup functions. The VLANs should be assigned as followed:

1 – Default Management VLAN	30 – General Users
2 – DMZ	40 – Accounting and Paging
10- Backbone	50 – ISP
20 – Core	60 – Airport

VLAN 1 is a default management VLAN for managing the network devices internally. VLAN 2 will be used for the Demilitarized Zone (DMZ) that will hold the general access web, mail and paging servers. The other VLANs will be used to separate the network devices, general internal users and the airport from one another.

Inter-VLAN communication requires routers, therefore, once the VLANs have been created all traffic going outside the VLAN must pass through a router. In order to secure the network after creating VLANs the company will begin to "harden" the routers. Hardening the routers is simply the process of making the routers difficult for intruders to enter via router configuration. Unused ports on the router will be shutdown and will not be listening for requests. The company currently uses telnet, which is widely known to be an insecure protocol. The telnet port will be shutdown on the perimeter routers and in place of telnet, Sshd will be configured and used. See below for the required configuration commands to shutdown telnet and allow Sshd.

```
Router(config)#  hostname Router1
Router1(config)# ip domain-name  xyzcommunicationsrouter1.com
Router1(config)#crypto key generate rsa
!Allows the router to generate ras keys
Router1(config)# ip ssh time-out 60
!Sets the session timeout
Router1(config)# line vty 0 4
Router1(config)# transport input ssh
!Allows Ssh connections instead of telnet
```

(Configuring Secure Shell, n.d.)

Other protocols that will be shutdown are CDP, Proxy ARP, Finger and ICMP redirects. The following displays configuration commands to shutdown the previous protocols on the companies Cisco routers.

```
Router(config-if)# no ip redirects
!Stops ICMP redirects
Router(config-if)# no cdp enable
!Disables the Cisco Discovery Protocol on the specified
 port
Router(config-if) #no ip proxy-arp
!Disable proxy arp on the selected port
Router(config-if) # no ip service finger
!Disables finger on the selected port
```

XYZ needs to configure access control lists on the perimeter routers to provide access to the users from the ISP, VLAN 20, 30 and the airport wireless, while denying access to all other users. An access control list configuration sample is below:

```
Router(config)# ip access-list 1 permit 207.204.1.0 0.0.0.255
!Permits access to  users from the ISPs
Router(config)# ip access-list 1 permit 207.204.2.0 0.0.0.255
!Permits access to users on VLAN 20
Router(config)# ip access-list 1 permit 207.204.3.0 0.0.0.255
!Permits access to users on VLAN 30
```

By default all traffic that is not permitted in the access list will be denied.

After the routers have been configured to disable ports and deny certain traffic two Cisco PIX 525 hardware firewalls with three Gigabit Ethernet

interfaces can be installed. The three interfaces will be used for the internal, external and DMZ networks. The PIX 525 will be configured to only allow general users into the DMZ, web, mail and paging servers. All internal users will be allowed access to the DMZ, while only users coming from VLANs 40 and 60 will be allowed access to the outside network.

At this point the network perimeter is considered secure from intrusion. It is, however, not secured from various network disasters or internal users. In order to achieve true security of internal networks and data redundant links and equipment need to be added.

The company currently has a backup connection to their ISP (ISP1 and ISP2), however in order to properly use the connection, HSRP will have to be configured between the two perimeter routers and both of the Internet connections will need to be provided by separate ISPs. This way, if one ISP fails the other can take over with little interruption to internal and external users. Configuring HSRP on two routers allows one router to be the main router and the other to be the backup router. The hosts on the network will always point to a virtual router address so, when one of the routers goes down the backup will take over with the virtual address resulting in no interruption to end users. Configuration of HSRP on the perimeter routers will be done on the Fast Ethernet 0/0 interface of the routers as follows:

Router 1:

```
Standby 10 ip 207.204.10.1
!assigns a standby group and virtual ip address
```

Standby 10 priority 120 preempt

!assigns a priority and allows the router to become the

!active

!router when its priority is greater than the other

!routers in

!the HSRP group.

Standby 10 track serial 0

!tells the interface to track S0, if serial 0 goes down Router 2

!will take over and begin to route the traffic.

Standby [group number] authentication string

Router 2:

Standby 10 ip 207.204.10.1

!assigns the standby group and virtual address

Standby 10 preempt

!allows the router to take over when its priority is greater than the other routers in the group

Standby 10 track Serial 0

!tells the router to track the Serial 0 interface.

Dynamic Domain Name System (DDNS) will have to be added to allow communication throughout the internal network from the backup ISP connection. If DDNS is not used Border Gateway Protocol will have to be used and this is

considered undesirable to the company. Configuring DDNS will be done on the Windows clients and servers by the current system administrator.

Finally in order to complete the redundancy plan, adding a backup paging and email server is suggested to allow for backup and load balancing. The servers will be configured for backup and load balancing by the current Network Administrator.

Once all equipment has been configured and/or install it will to be necessary to test the network for connectivity issues and its ability to keep intruders out of the network. (See Figure 3 for the physical layout of the suggested perimeter network.) This will be initiated by testing connectivity from inside the network. Begin with a computer inside the network and access all perimeter interfaces and to the external Internet. Once connectivity is established, test to be sure that intruders from the Internet cannot infiltrate the internal, protected, network. In order to test that the security measures work and everything is configured properly, a representative of XYZ Communications needs to perform the following steps:

1.) Access Web, Email and Paging servers by trying to receive a Web page, Email message and Page. Remember the user will be unable to ping these servers because ICMP has been shutdown. If you are unable to ping any of the servers then the PIX Firewall is not properly configured to allow internal users access to the DMZ.

2.) Access a Web page that is external to the network. If the user is able to access the internet then internal users have the required connectivity. If the

user is unable to access the Internet, either the firewall is not allowing communication to the internal network from the Internet or HSRP is not working correctly on the network.

3.) Once internal connectivity has been verified go to a computer that is on an external network and try to access the Web, Email and Paging servers. The servers are inside the DMZ so this communication should work. If this does not work the firewall may not be configured to allow communication to the DMZ from the Internet.

4.) Ping the perimeter routers and PIX Firewall. This should not be successful. If this has been successful then the router has not been correctly configured to shutdown ICMP.

5.) Telnet to the perimeter routers. Once again this should not be successful. If this is successful then Telnet has not been shutdown on the routers.

6.) Ping and telnet to the firewall. This should not be successful. If this is successful then reexamine the firewall, it is not configured correctly.

7.) Use packet capturing software to try to discover usernames and passwords. If any passwords are sent across the network in clear text then encryption is not properly set on the routers.

8.) Once you are convinced the perimeter is secure check the router redundancy by shutting down router1. Watch to see that router2 has taken over control and begin testing the network again, starting at step 1.

Figure 2

Current Network Perimeter

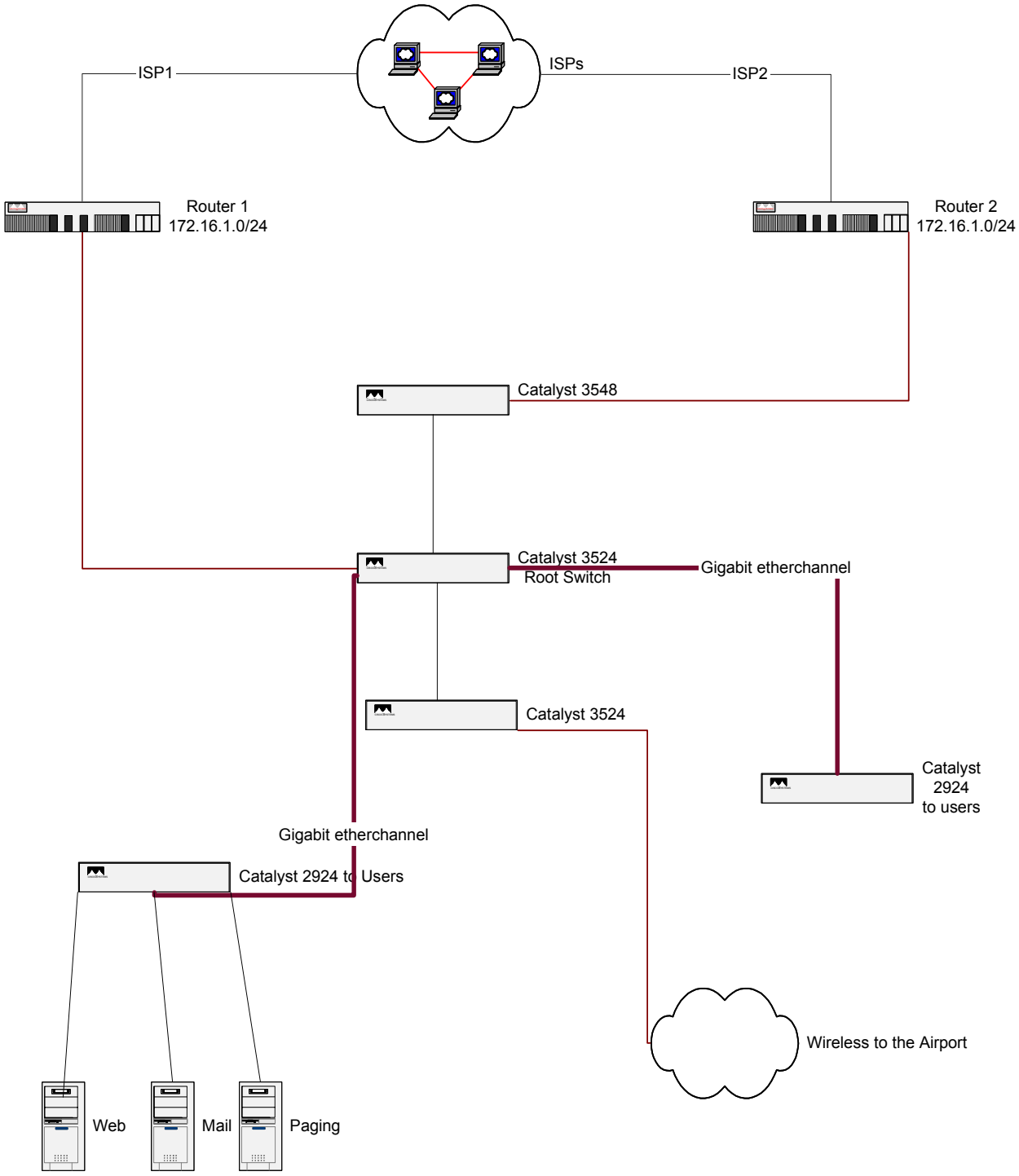
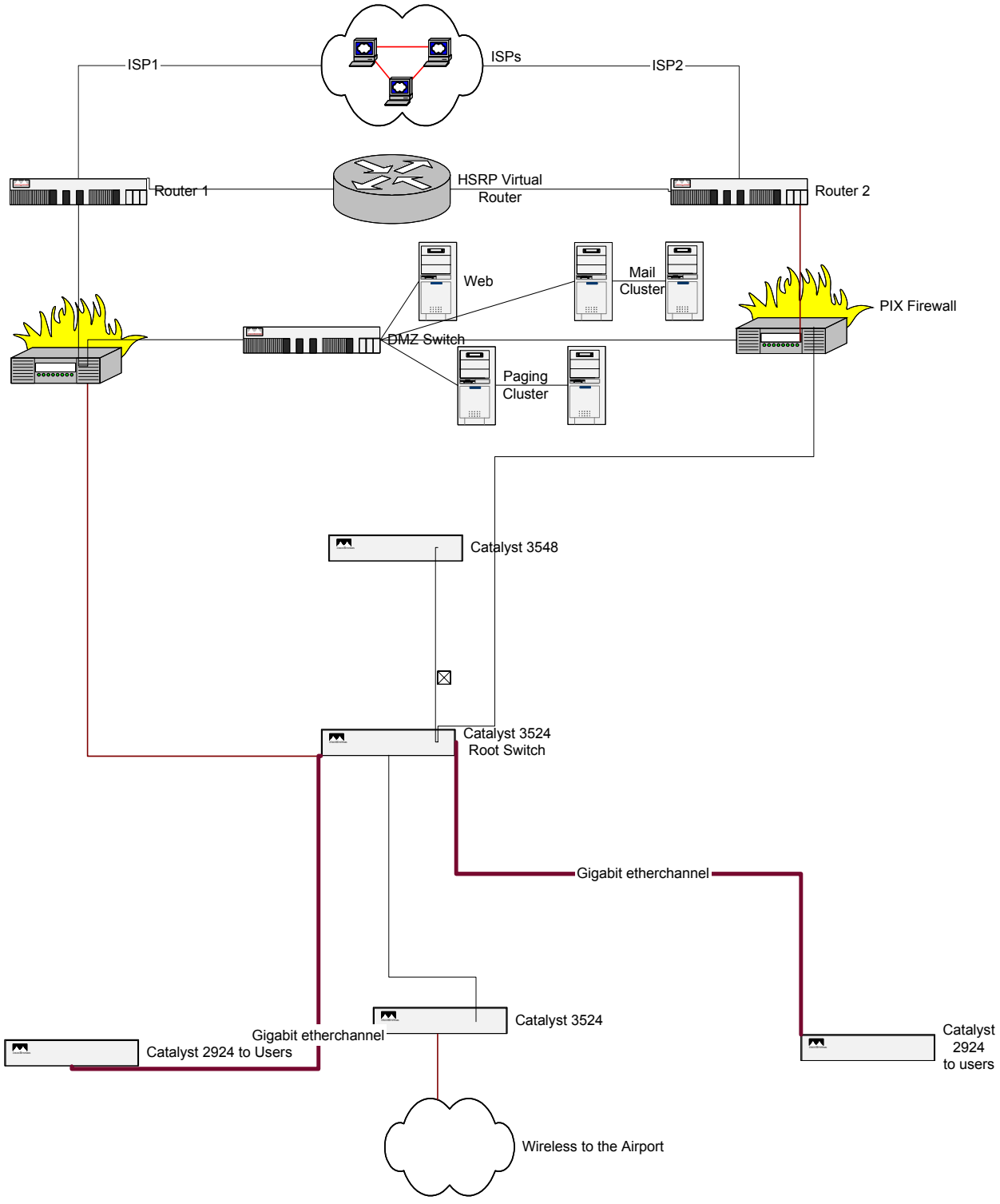


Figure 3

Proposed Secure Network Perimeter



Chapter 5

Conclusions and Recommendation

The purpose of this study was to provide suggestions for securing the network infrastructure from internal and external intruders while still providing a high quality of service to authorized users of the network. The goals of the study were to:

1.0 Analyze the current network infrastructure to determine network security weaknesses.

2.0 Provide suggestions for securing the network that will block unauthorized users while maintaining ease of access for authorized users.

3.0 Provide a backup plan in case the network is compromised by unauthorized users or by internal user error.

Conclusions

The current network infrastructure uses Cisco equipment. Standardization on one set of network equipment will make a transition from a relatively insecure network to a secure and redundant network relatively easy. Securing the network will require adding a Cisco PIX Firewall and creating a DMZ. Web, paging and mail servers will be moved to within the DMZ. After making those changes to the devices on the network infrastructure, the only steps necessary will involve changing some configurations on the currently existing network infrastructure devices.

Recommendations

When a company is wholly dependant upon its network infrastructure in order to run its business the cost of someone either internally or externally compromising the network can be too much. If network downtime is experienced long enough in a company such as this, it may shut the company down altogether. Before considering any changes to this network the company must do a cost vs. benefit analysis and decided for themselves whether the suggestions provided in the study are feasible. However, given the vital nature of XYZ Communications network, it is suggested that the company purchase the necessary equipment and make the configuration changes to the network that are necessary for securing the perimeter of the network. Once the perimeter is secured it may be desirable to perform another network analysis and consider the steps necessary for securing the internal network.

Appendix

Links to Internet Sites Offering Sample Security Policies

The SANS Institute has provided a multitude of sample security policies in downloadable template formats at:
http://www.sans.org/newlook/resources/policies/policies.htm#template

Sample security policies offered online by author Scott Barman for his book "*Writing Information Security Policies*":
http://www.panix.com/~barman/wisp/

RFC 2196 provides a blueprint for writing Security Policies. RFC 2196 can be viewed online at: http://www.ietf.org/rfc/rfc2196.txt?number=2196

References

Akin, Thomas. (2002). Hardening Cisco Routers. California: O'Reilly & Associates.

Barman, S. (2002). Writing Information Security Policies. Indianapolis, IN: New Riders.

Bookman, C. (2003). Linux Clustering, Building and Maintaining Linux Clusters. Indianapolis, IN : New Riders.

CEI, Computer Economics (2002). The Computer Economics Security Review 2002. Retrieved June 30, 2002 from: http://www.computereconomics.com/article.cfm?id=356

Chapman Jr, D. & Fox, A. (2001). Cisco Secure PIX Firewalls. Indianapolis, IN: CiscoPress

Computer Security Spending Statistics. (2000). Retrieved June 30, 2002 from: http://www.securitystats.com/sspend.asp.

Configuring Secure Shell. (n.d.). Cisco Systems, Inc. Retrieved November 20, 2002 from: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

CSI (2002). Cyber crime bleeds U.S. corporations, survey shows: financial losses from attacks climb for third year in a row. Retrieved July 2, 2002 from: http://www.gocsi.com/press/20020407.html

Depaul University, Information Security Team. (2002, August). Logon Banners for Computer Systems. Retrieved September 9, 2002 from:

https://infosec.depaul.edu/doc/policy/pub/logonbanners.pdf

Fraser, B. (1997). Site Security Handbook: Request for Comments 2196. Retrieved September 2, 2002 from: http://www.ietf.org/rfc/rfc2196.txt?number=2196

Increasing Security on IP Networks. (2001). Cisco Systems, Inc. Retrieved June 30, 2002 from: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Lemos, R. (2001). Digital sleuthing uncovers hacking costs. Retrieved June 30, 2002 from: http://news.com.com/2100-1023 254561.html?legacy=cnet&tag=ch_mh

Scambray, J. & McClure, S. & Kurtz, G. (2001). Hacking Exposed: Network Security Secrets and Solutions. California: Osborne/McGraw-Hill.

Wenstrom, Michael. (2001). Managing Cisco Network Security. Indianapolis, IN: Ciscopress

Wimpie du Plessis. (April, 2001). Internet Daemon (inetd) – What it is and Securing it. Retrieved September, 09 2002 from: http://rr.sans.org/unix/inetd.php