Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

A Secure By Numbers Approach To An All

Many Small Office / Home Office, (SOHO), networks today are comprised of a combination Broadband Router / Wireless Access Point / Switch. Some of these devices even have a software firewall option that can be enabled. My current network fits this scenario. These multi-functional devices are very simple to setup and use, but may not provide us with the layered Defense In Depth functionality that we desire nor will they provide the additional features of higher end components such as those made by Cisco. With the growing...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

A "Secure By Numbers" Approach To An All Cisco SOHO Infrastructure

Darrell Rogers

January 8, 2004

GIAC Practical Assignment – Option 2

Version 1.4b

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Abstract	**1.0**
In The Beginning… Before	**2.0**
The Hardware	**3.0**
Router	**3.1**
Firewall	**3.2**
Switch	**3.3**
Wireless Access Point	**3.4**
Let's Route Some Data!	**4.0**
Cisco IOS vs. Web Setup	**4.1**
DHCP	**4.2**
NAT	**4.3**
And Prevent Other Traffic! (ACL)	**4.4**
A Firewall – Another Layer of Protection	**5.0**
Cisco IOS vs. PIX Device Manager	**5.1**
DHCP	**5.2**
NAT	**5.3**
Wireless Access Point	**6.0**
Cisco IOS vs. Web Setup	**6.1**
WEP – 128 bit	**6.2**
MAC Address Filtering	**6.3**
Distribute and VLAN – Switching	**7.0**
The End Result	**8.0**
Is it More Secure, Usable, Flexible?	**9.0**
References	**10.0**

© SANS Institute 2004, Author retains full rights.

1.0 Abstract

Many Small Office / Home Office, (SOHO), networks today are comprised of a combination Broadband Router / Wireless Access Point / Switch. Some of these devices even have a software firewall option that can be enabled. My current network fits this scenario. These multi-functional devices are very simple to setup and use, but may not provide us with the layered Defense In Depth functionality that we desire nor will they provide the additional features of higher end components such as those made by Cisco. With the growing use of broadband in homes, home offices and small business, more complex and demanding scenarios are evolving. As these consumers become more reliant and demanding of Information Technologies, their exposure to risk is also higher. Cisco equipment is now being designed and marketed towards these SOHO environments. Some of these Cisco components are a model # 806 router, model # 501 PIX Firewall, and a model # AP352 Wireless Access Point. These components plus an older but usable Cisco model # 1924EN switch make up the hardware that I chose to enable a SOHO with a very capable and securely layered network infrastructure. Since I have recently incorporated, these components will be assembled into "my company's" network.

I think most people are reluctant to use Cisco components in a SOHO because they fear the Cisco IOS. All of the Cisco components that I have identified in this paper have the ability to be configured via a Web interface. This is important for a consumer. The Cisco IOS is a powerful tool. But having the knowledge that I can purchase Cisco products, configure them in a short period of time with a GUI interface and get them on-line and then continue to "tune" the product after it is functional is an empowering concept. This is especially important when you realize that the PIX IOS is similar but different from the Router IOS. So there are multiple skill sets involved. I will take you through a complete ground-up SOHO network build, including all cabling, software and hardware installs and provide a "Paint by Numbers" template which I refer to as a "Secure By Numbers" SOHO. The finished product will provide a very good representation of Defense In Depth that any SOHO would benefit from, and grow with.

2.0 In The Beginning… Before

My current router / switch / wireless access point is a Linksys model BEFW11S4[1]. The physical connections are very simple. It has a WAN port that connects directly to the cable modem via a straight thru CAT5 cable. It also has a 4 port switch for the LAN connections. In addition, it serves as a wireless access point for 802.11b connections.

After powering on the device, it has a default admin login and private IP address of 192.168.1.1 / 24 assigned on the LAN switch. To view the current

[1] Linksys model BEFW11S4; befw11s4_v4_ds.pdf on ftp.linksys.com

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

configuration of the router you simply must connect a client PC with DHCP enabled to one of the switch ports, open a web browser and type in the default private IP address of 192.168.1.1. This will result in a login screen followed by a GUI interface to further configure the device. By default it also functions as a DHCP server. The wireless 802.11b features are configurable from these menus also.

The time to deploy this unit out of the box is less than 10 minutes. It serves as a router / gateway. It provides DHCP service for the LAN. It uses NAT to allow multiple clients with private IP addresses to utilize the one routable IP address assigned by the ISP for internet access. It also has the option of using a software firewall at the router level that can be enabled with a product key. It has logging capabilities. It can be very useful, yet also has weaknesses.

Unlike a Cisco router, the options for LAN configuration are limited to the 192.168.1.0 / 24 IP range. Classful routing is the only option. This can become a problem if more than one router is used within the same network. For example, the ability to segment a network to separate wireless clients from wired clients is not easily done without additional equipment. Each router will require a different network segment on the LAN. This is not currently possible on the Linksys. Access Control Lists, (ACL's), are not possible. An ACL gives one the ability to restrict traffic either inbound or outbound on a specific interface based upon the IP address of the data. This is akin to blocking a telemarketer's phone calls from getting to your phone. As we progress, more functionality will be discussed and compared.

It is a single device providing some of the functions of multiple devices, doing some things well, and not doing others at all. For a network that is just being birthed the Linksys is a good starting point. When additional functionality and security is required it is time to look for something else.

3.0 The Hardware

I made my choices with respect to hardware based on my current skill set, my business needs, a fair amount of research on what tools work well together and of course how much is it going to cost. One of the components, the Cisco 806[2] router was made available to any Cisco Networking Academy[3] students for about one-half the normal retail cost. It is a Cable / DSL Broadband router with a CAT-5 WAN port and a 4-port switch on the LAN side. The 4-port switch is seen as a single interface, Ethernet 0, so in addition to the single WAN interface there are only two interfaces to configure. The router has a full featured Cisco IOS[4] that you can update for additional feature sets that may suit your needs. It also has a Web based interface for quick initial setups.

---

[2] Cisco 806 Product Data
[3] Cisco Networking Academy
[4] Cisco IOS Software - Cisco Systems

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

My second component, a Cisco PIX 501 DES (K8)[5] firewall, was obtained via a well known on-line auction process. I chose the PIX for several reasons. I wanted a hardware firewall that allowed for stateful packet inspection. Since I am an instructor at a Cisco Networking Academy the training for the PIX is available to me. Price was a negative. After I discovered that I could purchase one via auction a lower dollar amount I preceded with the PIX 501.

This product is has been officially[6] "sunset" by Cisco. This means that they have placed a "Press Release" on their web site stating their intent to cease production / sale of this product. The last date to order this model is March 11, 2004. The PIX 501 3DES (K9) will still be produced. The most obvious difference is the fact that mine has only "single" DES encryption and the PIX 501 3DES (K9) model has "triple" DES. However, there is a benefit to getting one of the older units if 3DES is a feature you desire. The 3DES feature used for encryption on the PIX 501 K9 model is normally an upgrade that you have to pay about $100USD for, can now be activated[7] for free with a key obtained at the Cisco website. If you supply an existing serial number you will be given a key needed to activate 3DES on the cheaper unit. You can do this on-line in about 3 minutes. So I too now have 3DES.

This unit has an integrated 4-port switch and is configured much like the 806. The terminology with a firewall is somewhat different. Instead of WAN or LAN interfaces there are inside and outside interfaces. They are still referred to as Ethernet 0 and Ethernet 1 for the purposes of configuration. This unit can also be used as a stand alone device without a router. It has the ability to be a DHCP server and can provide NAT/PAT functionality.

The third component is a Cisco AP352 Wireless Access Point. The reasons this product was chosen are power, power and power. It is by far the most powerful transceiver on the market at 100 milliwatts. Most retail store products are in the 10 to 16 milliwatt range. In addition it has the ability to be configured in the way the Lee Barken[8] discusses in chapter 1 of his book. Summarizing, he suggests that for a SOHO application you should consider turning off the broadcast SSID, use MAC filtering, use WEP and attempt to reduce your transmitted signal to the needed work area. Like the PIX 501, I found this unit on a favorite auction web-site at a great price. This device is fully configurable via a Web interface and can be on-line in minutes.

There are several models to choose from. When looking for Cisco equipment with respect to WEP, the Cisco part number identifies what if any WEP is

---

[5] Cisco PIX 501 Product Data
[6] EOS PIX 501 Security Appliance DES (K8) Bundles-Cisco PIX 500 Series Firewalls - Cisco Systems
[7] Encryption Software Export Distribution Authorization Form
[8] Barken, Lee. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi Lan. New Jersey: Prentice Hall PTR. 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

enabled on the device. For example, this unit is an AP352. The “2” indicates 128 bit WEP. There is also an AP351. The “1” indicates 40 bit WEP. If it were an AP350, the “0” would indicate no WEP.

The fourth piece of equipment is a Cisco 1900 series Catalyst switch. It is configured with 24 ports and is an enterprise model. It was picked up used as well, but is an excellent choice for my SOHO. It is WEB configurable as well as console via the Cisco IOS. It is menu based even via the Cisco IOS and is very intuitive. I can setup a “sniffing port” on this switch so that I can use an IDS at the switch level if I desire. It also has the ability to be broken up into VLAN’s. This is important to me for a couple of reasons. I do a lot of multicasting. When I do I get complaints from my co-habitors, my family. Multicasting via the Linksys switch quickly brought the other users to a crawl. With a different segment on it’s own VLAN, I found that this problem goes away. It has two ports that are 100 megabit and 24 ports that are 10 megabit. This might seem slow but most of the work done from my SOHO involves crossing the WAN so the bottleneck won’t be the switch. Your needs will vary and a higher bandwidth switch may be required.

I did not say finally when I spoke of the fourth piece of equipment. There are other peripheral pieces that I chose to install while completing this upgrade. I used a Black Box Rack Mount Patch Panel to connect the various devices together. This will make it easier to move components in and out of use. And even though some of the equipment that I am using is not rack mountable, I am placing all equipment in a standard width 7 foot tall rollable rack. Of course, there are lots of cables. Straight-thru cables work for most of the equipment but you will need several cross-over cables if you use a patch panel. For many of the cables I made my own. With the varying lengths needed and the various types, this made sense. While making the cables it was good to be able to test them. I used a Fluke OneTouch[9] to be sure the cables worked as I wanted them to. While working on network issues you want to be sure that you can rule out physical layer problems.

4.0 Let’s Route Some Data!

The first thing to do is physically connect the Cisco 806 router. Connect one end of a straight-thru CAT-5 cable to port 4 of the switch and the other end to a NIC on the computer that you will use to configure the switch. Port 4 has a special feature that will allow you to cross the connection internally if needed. Initially it will not be important to connect to the console port on the router. The router has a default configuration out of the box that will allow you to use a web browser for generic configuration changes. The initial configuration looks like this:

```
version 12.2
no service single-slot-reload-enable
no service pad
```

[9] Fluke OneTouch

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

```
service timestamps debug uptime
service timestamps log uptime
service password-encryption

hostname Router

logging rate-limit console 10 except errors

ip subnet-zero
ip dhcp excluded-address 10.10.10.1

ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1

no ip dhcp-client network-discovery
lcp max-session-starts 0

interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 no cdp enable
 hold-queue 32 in

interface Ethernet1
 ip address dhcp
 ip nat outside
 no cdp enable

ip nat inside source list 102 interface Ethernet1 overload
ip classless
ip http server

access-list 102 permit ip 10.10.10.0 0.0.0.255 any

line con 0
exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local

scheduler max-task-time 5000
end
```

© SANS Institute 2004, Author retains full rights.

After connecting the computer to the router switch port 4, make sure that the computer's Network Interface Card is set to DHCP, then reboot. Your computer will get an IP address on the same segment as the router when it reboots. By default the Cisco 806 acts as a DHCP server. Now you should open a Web browser on you computer and type in 10.10.10.1 for the URL. This will open a Web based interface that you can use to make basic setups / changes to the router. This GUI interface will not allow you to customize the Access Control Lists, or other customizations that can be done via the Cisco IOS. A nice feature is that you can change the LAN IP range which will automatically effect a change to the Access Control list and the DHCP scope. It is a little more time consuming at the IOS level. One thing you should choose to do at this point is select the security option and add passwords. This will help prevent users from making unwanted changes to your router. Once again, anything that you can do at the GUI level is probably easier to do than at the IOS command line. However, most things can't be done from the GUI interface. The existing default configuration and the password and LAN changes that you have tuned will be sufficient to begin operations.

During the life of your new router you will begin to tune and use additional features, this is where it will be necessary to connect your computer to the router via the console interface. You should use a flat roll-over cable to connect a com port on you computer to the console port on the back of the router. Once the physical connections are made you should start a communication program such as HyperTerminal. The port settings should be set to 9600, 8, none, 1 and hardware. Once the session is established it will prompt you to press enter to continue. You will then see a prompt that looks like this:\

Router>

At this point you are in "Exec" mode. You can't make any configuration changes in this mode. One of the things that you have to learn with the Cisco IOS is what mode you have to be in to make certain changes. If you type ena and then press enter you should be prompted for the password you created above. You will then be in privileged mode. Then type "config t". This will place you into global configuration mode. This is a good starting point that will allow you to tune the configuration. When you are ready to begin using the Cisco IOS to make configuration changes Cisco has a document[10] entitled "Feature by Feature Router Configurations" that can be downloaded in PDF format. It is specifically written for the Cisco 806. This document picks up in global config mode. It is 38 pages long and give a great feature by feature description and setup commands.

My initial thoughts were to use the 806 for DHCP and NAT. After you read further you will understand why that reasoning changed. A few of the changes that I made were to change the hostname to Rogers806, removed the configuration for DHCP and NAT functions and added passwords. The Access Control List will be

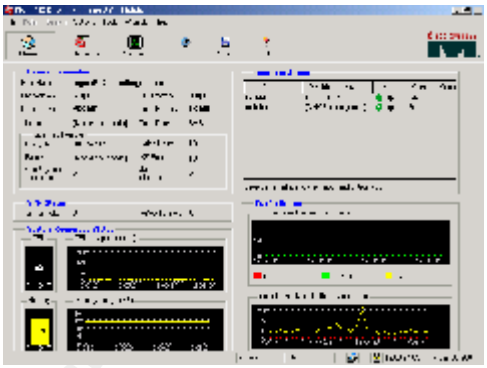
[10] Feature by Feature Router Configurations - 806

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the focus of most of my time spent tuning this device. That is the area where a router can benefit me the most in my attempts to secure my network.

5.0 A Firewall – Another Layer of Protection

The PIX 501 Firewall, as stated in the Cisco PIX 501 Quick Start Guide,[11] comes with a default configuration for most broadband SOHO environments that will allow you to simply plug-in and go. As with the router, it has a GUI Web based configuration screen so that it can be configured, as well as the IOS command line method. The Web interface is much more robust with the PIX. It has a great deal of charting and graphing activity that you can tune to your desires. It also has more configuration choices than the 806 Web setup.



You should connect the PIX 501 in much the same way as you did for the 806. Connect to a computer with a CAT-5 straight-thru cable. Power on the PIX and make sure that your computer is set to DHCP. You will need to reboot your computer to obtain a DHCP address from the PIX. The default configuration on the PIX is set to a different subnet than the 806 so the same address won't allow you to connect to the PIX. More about that later. Once you have re-booted you should open the Web browser of your choice and enter this for the URL: https://192.168.1.1

A username and password screen appears. At this point leave them both blank and press enter. Next you should accept the certificate and follow the directions. It has a very nice startup wizard that will guide you through the final tunings of the install. During the startup wizard you will be allowed to setup passwords. Once again you should be sure to do this.

During the wizard you will be allowed to configure DHCP and NAT / PAT. Since both devices provide some of the same functionality you will have to decide on which device will provide DHCP and NAT / PAT functions. In my case I chose to use the 806 as a border router and supply the functionality that this implies. The router will provide all NAT / PAT functions, Access Control List functionality, and DHCP. The PIX will be left alone to provide stateful packet inspection. I disabled these features on the PIX using the setup wizard.

The PIX 501 can be used as a stand alone device or in tandem. I almost decided to remove the 806 from the line but felt that the layered approach utilizing the 806 to limit unwanted traffic was still better. Defense In Depth.

[11] Cisco PIX 501 Quick Start Guide

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Now more about the LAN segments. I initially spent considerable amount of time trying to make something work that I now know simply can't. I guess we put two different hats on, one at work which makes us very calculated and unwilling to fail, and the one we wear at home where we let our defenses down and become reckless.

I was not sure if the PIX really acted like a router, even though the documentation states that it does. After all it is a PIX, it's not called a router. So I attempted to place both the router and the pix on the same LAN segment. I configured the 806 to DHCP from my cable provider. Then 806 was to simply be the border component that supplied DHCP addresses, did NAT / PAT translations and blocked unwanted traffic via the ACL's. Directly connected was the PIX. E0 to E0. I setup the PIX on the same subnet as the 806 and was able to ping interfaces. All is well. Knowing that DHCP clients would find the closest DHCP server on the same network segment I knew that the LAN on the other side of the PIX would be able to get an IP address from the router. Worst case, I might have to enable the PIX as a DHCP listening agent. It did not work. When I configured the internal interface of the PIX with an IP address on the same subnet as the external interface, it balked. I had spent considerable amount of time configuring the servers with static IP's on the subnet I thought I was going to use. I had already set the Wireless Access Point to default on the LAN segment I thought I was going to use. I spent considerable amount of time trying to defeat the electrons in those wires. I created a VLSM IP range hoping to somehow summarize the route to allow me to continue to use everything as configured. Don't do as I did. Simply plan on using two different segments. It really does act like a router! Bottom line is that I now have the PIX doing DHCP and stateful packet inspection.

Something that I found while looking at sample configurations at Cisco's website was a document with ways to use the PIX 501 to block file sharing programs[12] like Gnutella and Kazaa. I live in a home with 3 kids so this is of interest to me. I read the article and found that it was a little mis-leading. It did confirm for me that I made the right decision to leave the 806 router in as a border filter. The article clearly gave configuration statements that could be used on the PIX for various kinds of peer to peer file sharing programs like Blubster or Piolet. It then stated that Kazaa could not be stopped by the PIX firewall.

It further stated that NBAR[13], (Network Based Application Recognition), could be used at the router level and gave sample ACL's. I had not heard of NBAR but did some research at Cisco's website to learn that it could be used to identify mission critical applications. These mission critical applications would then be given preferential treatment so that at least a minimum amount of bandwidth could be guaranteed. Conversely, you could use the same technology to identify

[12] Blocking Peer to Peer File Sharing Programs with the PIX
[13] NBAR

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

applications that you wanted to get no bandwidth like Kazaa. Below is a sample IOS router configuration from the referenced article above to work with NBAR to block Kazaa specifically:

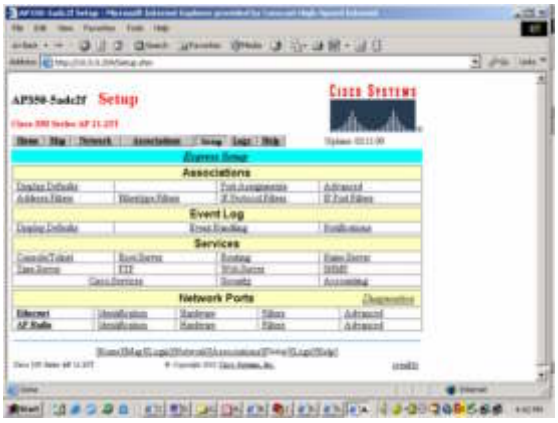
```
class-map match-any p2p
  match protocol fasttrack file-transfer *

policy-map block-p2p
  class p2p
    drop

int FastEthernet0
  description PIX-facing interface
  service-policy input block-p2p
```

This is something that I will continue to try an implement for future improvement.

6.0 Wireless Access Point

Out of all the 4 components, this is probably the one that excited me the most. I have used these in business situations for other people and businesses, but could not justify the expense for myself. Once again, my favorite on-line auction place allowed me to fit it into my budget.

The initial setup is a little different for the AP352. It is set to DHCP. Unless you have the DHCP logs available you can't readily identify the IP address. The easiest way to identify / configure is to connect via the serial connection. Connect to the AP352 and start a HyperTerminal session using the same settings as with the other Cisco devices. Connect the AP352 via CAT-5 to a DHCP server. Then remove power from the AP352 and re-apply power – in other words reboot the WAP. You will see the AP352 go through the POST and the IP will scroll by. Once you have the IP you can use a Web browser to configure the WAP.



Once again the Web based interface is a great tool. As I stated earlier there are really four things that I want to do to make the AP352 as secure as I can.

Before we harden the AP352, lets establish a User Manager. After clicking on the setup tab the next menu will have a section entitled Services. Under Services is a selection named Security. Click on Security. At this page you first need to select User Information and then

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

choose to Add New User. Be sure and select the capability settings that you should allow yourself – all of them. Select apply and then select the “back” button on your browser to get back to Security Setup. Choose User Manager and select enabled on the next page to enable a login. After navigating back to the Security Setup screen you should select Login and login. Otherwise none of you changes will be effective from this point forward and some of the screens start to generate some errors.

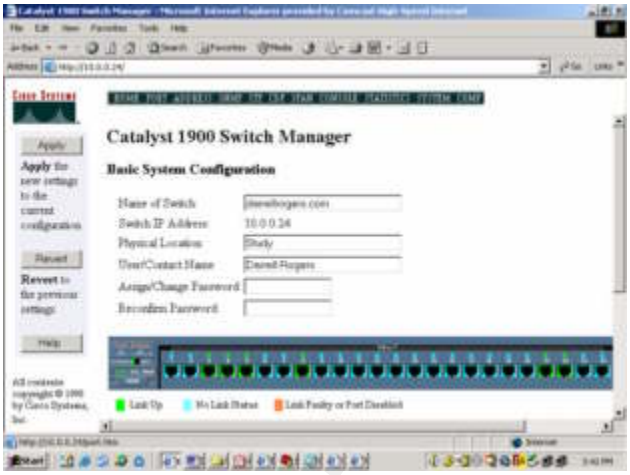
Now that we have a User Manager established and are logged in, from the Security Setup screen select Radio Data Encryption. Note: As soon as you enable WEP you will no longer be able to access the AP352. You will have to enable WEP on your Wireless Card as well. I prefer to do WEP first so that I can still see the SSID and am sure that I must have mis-keyed the encryption key if it doesn’t allow me to connect. At the AP Radio Data Encryption page you should enter at least one WEP key. If you are using 128 bit WEP the key must be entered as 26 digit hexadecimal digits. Be sure and select 128 bit for the key size. There is a choice on the AP352 to use 40 or 128 bit. I am using 128 bit. Please be sure you right down the encryption key as you enter it – then double check it. Once entered and saved the only way to recover is to reset the AP352. Select OK and go to your wireless card settings and enter the same key. Note: While you are in the process of re-connecting make a note of the MAC address on you wireless card. You will need the MAC address of it and any other wireless cards that you want to have access to you WAP. After correctly entering the WEP key in the security settings of your wireless connection you should be allowed to re-connect.

After re-establishing your wireless connection open the Web browser and type in the IP address to continue securing your wireless access point. Now I want to apply a MAC Address Filter. You will find this option after going back to the Home menu and then selecting Setup. At the Setup page under Associations select Address Filters. One by one enter the MAC addresses, select allowed and select Add. The list will grow at the bottom of the page and will reflect the only MAC addresses that will be allowed to connect to the AP352. When done select apply. The one part of this software that I don’t like is that you have to click on the back button to navigate. The menu choices are not always there to select.

There is one additional measure that I wanted to take to secure my wireless. I say wanted because it appears that I cannot. I had wanted to disable the broadcast of the SSID. It does not appear that the Cisco AP352 has this functionality. Can’t have everything – or can you?

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

7.0 Distribute and VLAN – Switching



The 1900 EN is capable of Web based setup and monitoring. The way I began is by using a com port on a computer to connect to the console port of the switch. I established a HyperTerminal session using the same settings used for the other Cisco products. Once the session is established I selected "I" for IP configuration. I input the IP address and subnet mask that I selected for the switch along with the default gateway. I found that the DNS info had already been auto populated as well as the domain name. Pretty smart. RIP is also enabled. After completing these tasks I opened the Web browser and input the IP address assigned to the switch and the Catalyst 1900 Switch Manager page opened.

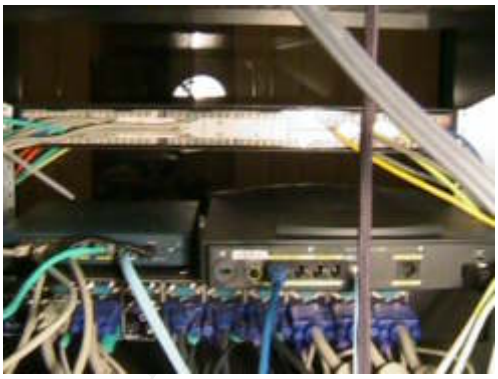
I am using my switch to segregate traffic. As my network is structured the true gateway is the Cisco 806 router. The PIX 501 is directly connected to the 806. From the PIX I have ran a single CAT-5 cable to the "B" port on my switch. I elected to connect the AP352 to a second switch port on the PIX. I will only use the 1900 for cabled connections. I have connected two Microsoft 2000 Domain Controllers to the switch – just enough to see if it works. By default the switch has one VLAN with all ports in the VLAN. I created a second VLAN with ports 9 through 16 for Multicasting. I have tried and it does work. One of the servers is multi-homed so I created an additional network segment using the second NIC and connected it to port 9. I connected a client to port 16. The lights were going crazy on all ports 9 thru 16 indicating steady traffic. The lights were very lazy on all other ports. I attempted to gain access to the internet and found no problem. Clearly this worked!!!

8.0 The End Result

I have to keep in mind as I review this document that many things changed as the project evolved. My initial thoughts and plans were tossed aside in many cases. So let's summarize what actually happened. I have now installed a ground-up installation SOHO including all new cabling, router, PIX firewall, 1924 switch and an AP352 wireless access point. I got most of what I wanted in terms of a secure network and at the same time got more than I expected in terms of a secure network. This has been a mind bending experience. Each of these components is by itself an endeavor that could t and will continue to take considerable amounts of time to configure and tune. But I now have the tools and ability to tune my network to do things it could never do before. Before I go on to the checklist of "Secure By Numbers" let me go over my checklist of mistakes:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Not believing that the PIX would behave like a router.
- Pre-Building all the components separately based on a plan.
    - Since my plan was flawed it cost me time to setup twice.
- Not taking into account that my family would notice the network was down – no tougher customers.



- The patch panel is a nice "pretty concept" but caused many errors that I assumed were caused by router or pix misconfigs. After I caught on it all worked out.
- Assuming that Cisco would allow me to turn off the broadcast SSID on the AP352. I was so focused on the output and WEP that this slipped under my radar screen. Strangely the AP341 does have the ability to turn off the broadcast SSID.

My Secure checklist went like this: (by device):

Router:

- Review and tweak the default configuration (LAN address, DHCP, etc.)
- Enable passwords
- Review the ACL to be sure that unwanted traffic was refused at the WAN interface. (It should be configured to deny all but incoming traffic from your WAN by default).

PIX

- Review and install using the default configuration. Utilize the Cisco PDM and the initial setup wizard to tweak the LAN address, DHCP, NAT / PAT, etc.
- Enable Passwords.

AP 352

- Perform Initial Default setup, tweak LAN address, set default address, gateway.
- Establish a User Manager, and require a login for changes.
- Turn on 128 bit WEP using at least one Key.
- Activate MAC address filtering.
- Change default SSID.
- Tune the power output – Reduce to just enough to maintain bandwidth in SOHO area.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

1924

- Perform initial setup via console.
- Establish IP address for Web based config and monitoring.
- Web based monitoring provides excellent data per port.
- Establish VLANS to segregate bandwidth hogs.

9.0 Is it more Secure, Usable, Flexible?

There can be no question that my SOHO network is more secure and more flexible than it ever was before. The fact that I was able to put it together by myself with only referential material is a huge plus. My objective was to validate the fact that Cisco devices that were perceived as complex and only for use in the large enterprise can be utilized in SOHO situations.

I have access to more data and logging than I ever possibly could have obtained from the "old" network. I have the ability to react to specific problems with a multi-layered defense in place. I have the infrastructure in place to continue to train myself with IDS tools, etc. This certainly was not as easily done prior to the "new" network. Additionally, this certainly more closely mirrors what "regular" companies are using for IT infrastructure, therefore my "network tuning" at home equates to real experience.

10.0 References

Paquet, Catherine and Diane Teare. Building Scalable Cisco Networks. Indiana: Cisco Press, 2001.

Barken, Lee. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN. New Jersey: Prentice Hall PTR, 2004.

Cisco PIX Firewall Command Reference Version 6.3. California: Cisco Systems, 2003

McGregor, Mark. CCNP Cisco Networking Academy Program: Semester Five Companion Guide Advanced Routing. Indiana: Cisco Press, 2001.

Cisco Systems, Feature By Feature Router Configuration, 806 URL:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/806/806swcg/routconf.pdf

Linksys, A Division of Cisco Systems, BEFW11S4 Product Data Sheet, URL:
befw11s4_v4_ds.pdf on ftp.linksys.com

Cisco Systems, Cisco 806 Broadband Router Data Sheet, URL:
Cisco 806 Broadband Router - Cisco Systems

Cisco Networking Academy Program, URL:
Academy Connection

Cisco Systems, Cisco IOS Software, URL:
Cisco IOS Software - Cisco Systems

Cisco Systems, Cisco PIX 501 Datasheet, URL:
Cisco PIX 501 Firewall - Cisco Systems

Cisco Systems, Cisco PIX 500 Series Firewalls, URL:
EOS PIX 501 Security Appliance DES (K8) Bundles-Cisco PIX 500 Series Firewalls - Cisco Systems

Cisco Systems, Cisco PIX Firewall Quick Start Guide, URL:
http://www.cisco.com/application/pdf/en/us/guest/products/ps2030/c1616/ccmigration_09186a0080177094.pdf

Cisco Systems, Blocking Peer to Peer File Sharing Programs With The PIX Firewall, URL
Blocking Peer-to-Peer File Sharing Programs with the PIX Firewall-IPSec - Cisco Systems

Cisco Systems, Cisco IOS Network Based-Application Recognition (NBAR) URL:
Cisco - Cisco IOS® Technologies - Cisco IOS NBAR

© SANS Institute 2004, Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

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

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