GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

CASE STUDY:

Using Multiple Firewalls from Different Vendors for a Defense In Depth Strategy

Jeffrey A. Scott
Track 1 – GIAC Security Essentials (GSEC)
Version 1.4b
Option 2 – Case Study in Information Security

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I. Abstract

Defense in depth is a concept where there are multiple hurdles for an attacker to penetrate before getting to vital information. The use of multiple firewalls is one way of implementing defense in depth. Using firewalls from different vendors is a strategy often used in this scenario. Deciding how to use the features of each firewall and where to place them in the network design can be difficult and often requires testing each firewall in concert with the other in different ways.

I will be discussing the decision to implement a Sonicwall Pro and a GNAT Box GB-1000 as my firewall solutions. I will analyze the features of each and how I was able to utilize them in my design. After testing each firewall as both the external and internal firewall, I settled on using the Sonicwall Pro as the externally connected firewall and the GNAT Box GB-1000 as the internal firewall.

II. Before

When I started employment, my employer's Internet access was via a WebRamp. The WebRamp is an access router that uses modems to connect to standard dial-up accounts via a local ISP. The only security that the WebRamp provided was Network Address Translation (NAT) and minimal filtering that was not flexible. At that time, the company was still small and the requirement for supporting remote access of employees and providing real-time information to our customers/partners was not a requirement.

III. During

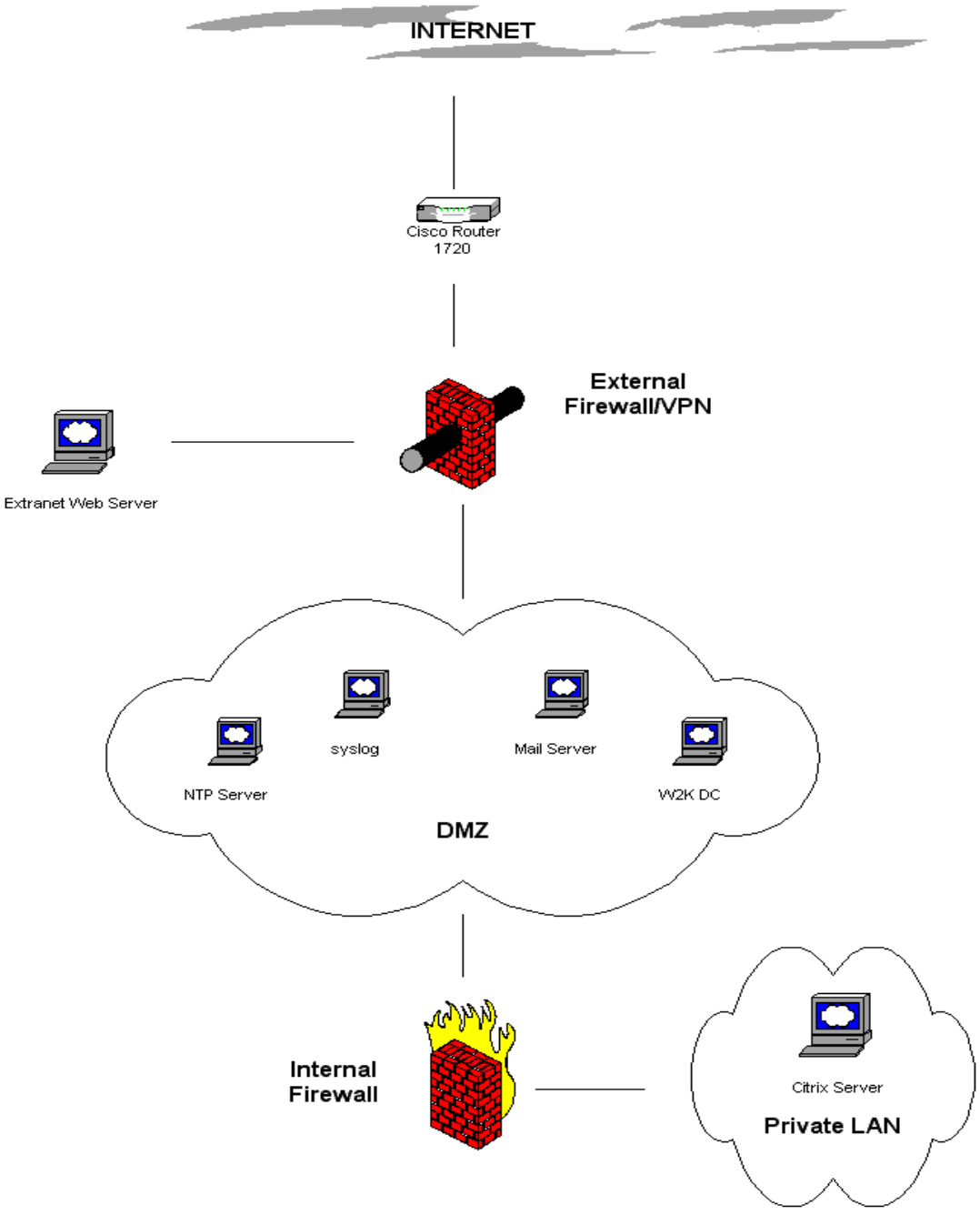
As the size of the company grew, the need to provide Internet services to remote employees, customers, and partners became apparent. Since the WebRamp was an analog dial-up solution, it was also necessary to switch to a higher bandwidth and more reliable solution. We decided to purchase a T1 from a local Tier two provider. We dedicated 16 lines to our phone system and used the remaining 8 lines for our data needs. This gave us a 512 Kb dedicated Internet connection. We also have the option of grabbing more lines for data as the need arises.

At this point, I assessed our needs for security. I knew the developers were working on an Extranet to provide real-time reporting and web based applications for our customers/partners. Other services that we wanted to provide included email, remote access to applications, and remote administration for the IS department. I realized that we needed an external firewall directly behind the Internet router as the first line of defense. However, knowing the risk of having a web server available to the Internet, I wanted a second firewall to isolate the web server from the internal production network. With this main concern in mind, I began my research for firewalls. I restricted my research to firewalls that were ICSA certified. I also used the knowledge I had gained from my GCFW

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Certification, to look for a firewall from two different vendors. The theory behind having firewalls from different vendors is that if a vulnerability is found in one firewall, chances are it won't be found on the other firewall at the same time. Figure 1 shows the original design that I had in mind.

Figure 1:



Since budget was a concern, I looked at the most economical appliance based ICSA firewalls. I ended up purchasing a Sonicwall Pro from Sonicwall, Inc. and a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GNAT Box GB-1000 from Global Technology Associates, Inc. I felt that either firewall would fit the need as the first line of defense behind the Internet router. However, after testing numerous configurations with both firewalls, I found that the Sonicwall offered enticing features for controlling outbound access from the internal network. I also found that the GNAT Box provided greater control for filtering and had features that were a better fit for controlling inbound access to services that we would be providing to the Internet.

There were four services that I wanted to provide to the Internet. The developers in my company were working on an extranet application for our clients as well as our employees. This web application used Microsoft IIS 5.0 and talked to a backend Microsoft SQL 2000 Server. I joined the web server to a separate UnTrusted Windows 2000 domain for administrative purposes. Since the web application also needed to access our internal SQL Server databases for real-time reporting, I decided to set up the backend databases on the same internal SQL Server. The web server needed to be behind a firewall with only port 443 open. However, I also wanted to isolate the web server hosting the Extranet from the internal network using a firewall. This would help prevent an attacker, who may compromise the web server, from then also attacking our internal trusted network. This internal firewall would only allow sql traffic from the web server to the SQL Server and block all other attempts to connect to internal servers.

The next service I wanted to provide was email. We chose to use ipSwitch's iMail Product. This product is an open standard POP and IMAP mail server. I also wanted the email server to be isolated from the internal network. I was not going to open POP or IMAP to the Internet. However SMTP needed to be open to the Internet. I originally was going to set up a SMTP Relay server in the isolated network. But, as I will describe later, I found that this was not necessary. In order to provide remote access to email, I implemented iMail's webmail feature.

I also needed to provide remote access for our employees to applications and files. Since several of my company's most important needs are based on existing client/server applications, I chose to implement a Citrix Terminal Server solution. Using this solution, employees can connect via the Internet to Citrix and see a desktop just like they were sitting at their desk at work. In order to implement this solution, I had to open up the Citrix ports to the Internet.

I also realized that I would need some way of remotely administering the network. I could have used the Citrix solution. However, I had locked down Citrix to prevent unauthorized use and this would limit my administration abilities. Since both firewalls came with a 1 client VPN license, I chose to use a VPN for my remote administration chores. I will discuss later which firewall I chose for this duty.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I will not be going into depth describing all the features and configuration steps of each firewall. I will only be discussing the features that were needed and/or desired for my organization and where they fit in the network design. Figure 2 below is a comparison chart of the features I wanted to use for the two firewalls.

Figure 2:

Feature	Sonicwall Pro	GNAT Box GB-1000
Network Address Translation (NAT)	Yes	Yes
Stealth Mode	Yes	Yes
Filter ActiveX	Yes	Yes
Filter Java	Yes	Yes
Filter Java Script	No	Yes
Filter Cookies	Yes	No
Block Known Fraudulent Certificates	Yes	No
Trusted Domains to bypass above filtering	Yes	No
Custom Allowed/Denied Domains	Yes	Yes
Bandwidth Management	Yes	No
Alert for IP Spoofing	Yes	Yes
Specific alerts for Denial of Service (DOS) Attacks	Yes	No
Remote Logging (syslog)	Yes	Yes
DNS Server	No	Yes
Email proxy	No	Yes
Network Time Protocol (NTP) Support	Yes	Yes
IPSec VPN	Yes	Yes
VPN User Authentication	Yes, Radius Available	Yes
Fragmented Packet Control	Yes	Yes
Encrypted Management	Yes, HTTPS	Yes, HTTPS & GUI

I used the above chart in Figure 2 to help break up my requirements into two areas. These two areas are protecting our internal network without negatively impacting performance and protecting the services that will be provided to the Internet. As can be seen in the above chart, two things that the Sonicwall can do that the GNAT Box cannot do are blocking Known Fraudulent Certificates and the ability to create lists of trusted domains that are permitted to bypass filtering. Since Java and Java Script have built in security measures, I was not as concerned with blocking them and thus not concerned that the Sonicwall did not filter Java Script. One of my goals was to also divide the processing load equally between the two firewalls as much as possible.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

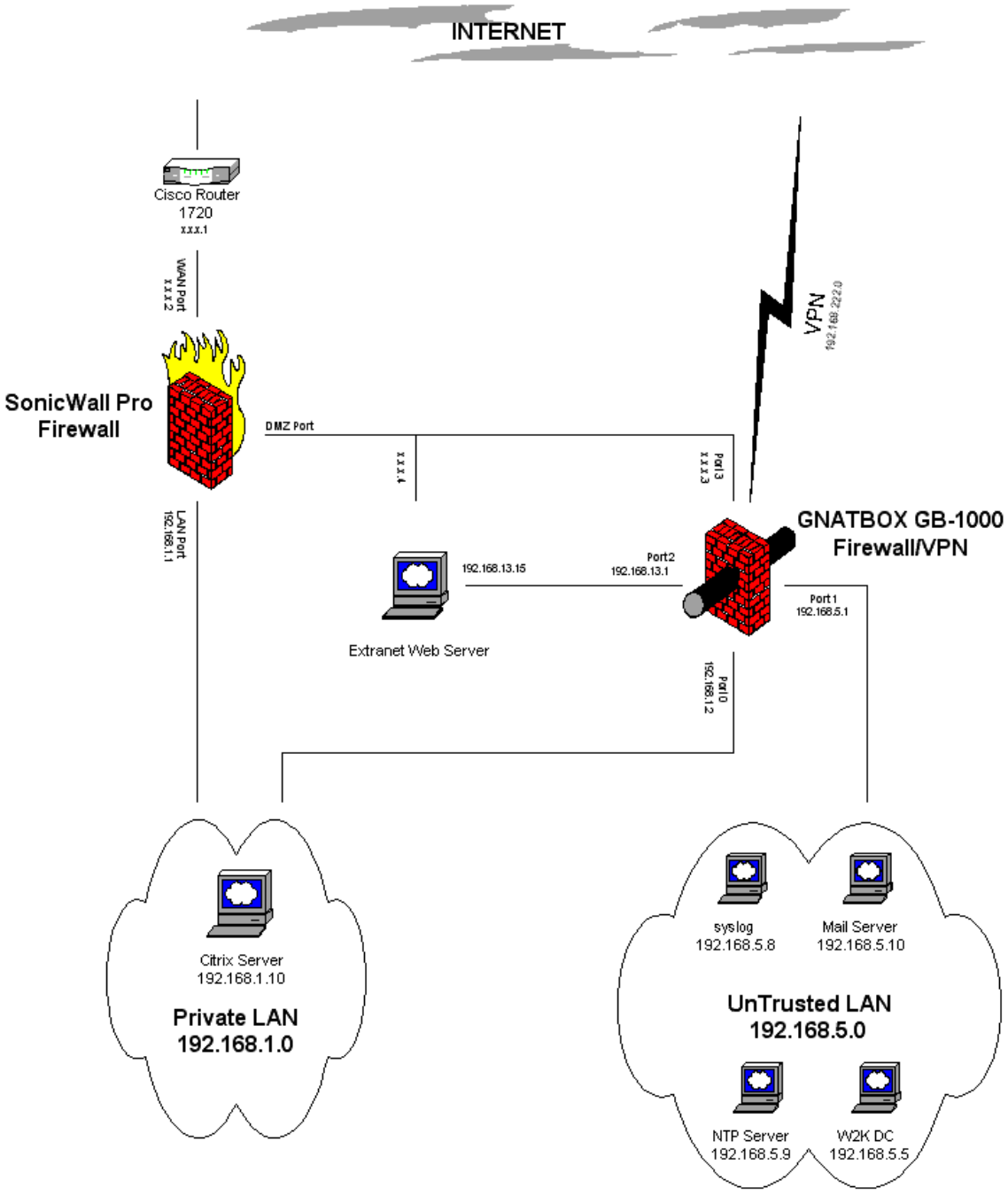
I first looked at making the GNAT Box the external firewall. The GNAT Box could easily handle this configuration. A Private Service Network (PSN) could be setup off one of the GNAT Box's interfaces. I could then place the web server and possibly the email server in this network using private IP addresses. The GNAT Box easily facilitates opening up the Citrix ports to the internal network as well. The GNAT Box could also provide the VPN connection in this configuration. There are a couple of minor drawbacks to this configuration. I would not be able to setup ActiveX filtering, because there are certain web sites that need to have it enabled and I would not want to have to continuously disable and enable ActiveX filtering each time someone wanted to access one of these web sites. The GNAT Box also does not provide any bandwidth management.

In looking at the GNAT Box as the external firewall, I had to simultaneously look at the Sonicwall as the internal firewall. In this configuration, I found the Sonicwall's limitations. The Sonicwall is not well suited as an internal firewall with private non-routable IP addresses on either side not using NAT. When the Sonicwall is configured to operate in standard mode (not NAT), It does not operate like a typical router such that each interface can be assigned a different IP address. It actually operates like a bridge and each interface must be on the same subnet. This would require me to have the DMZ servers on the same subnet as the internal network. This was not desirable because I was using a class C subnet and didn't want to use up addresses on DMZ servers. In this configuration, the GNAT Box would be handling all the processing because I wouldn't be able to offload any of the services to the Sonicwall. The Sonicwall would be acting strictly as a filtering firewall. Even the bandwidth management features would not be fully utilized because the Sonicwall would not know about any traffic going on in the DMZ. In this scenario, it would be just as secure and less administrative overhead to utilize one of the additional interfaces on the GNAT Box in place of the Sonicwall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 3 shows the final design that I decided to implement.

Figure 3:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The main reason I chose to use the Sonicwall as the external firewall was because of the loss of flexibility when using the Sonicwall internally. Friendlier logging and bandwidth management, which is a huge factor for helping performance, also helped make the Sonicwall my choice for the external firewall. Other reasons for using the Sonicwall at the perimeter included:

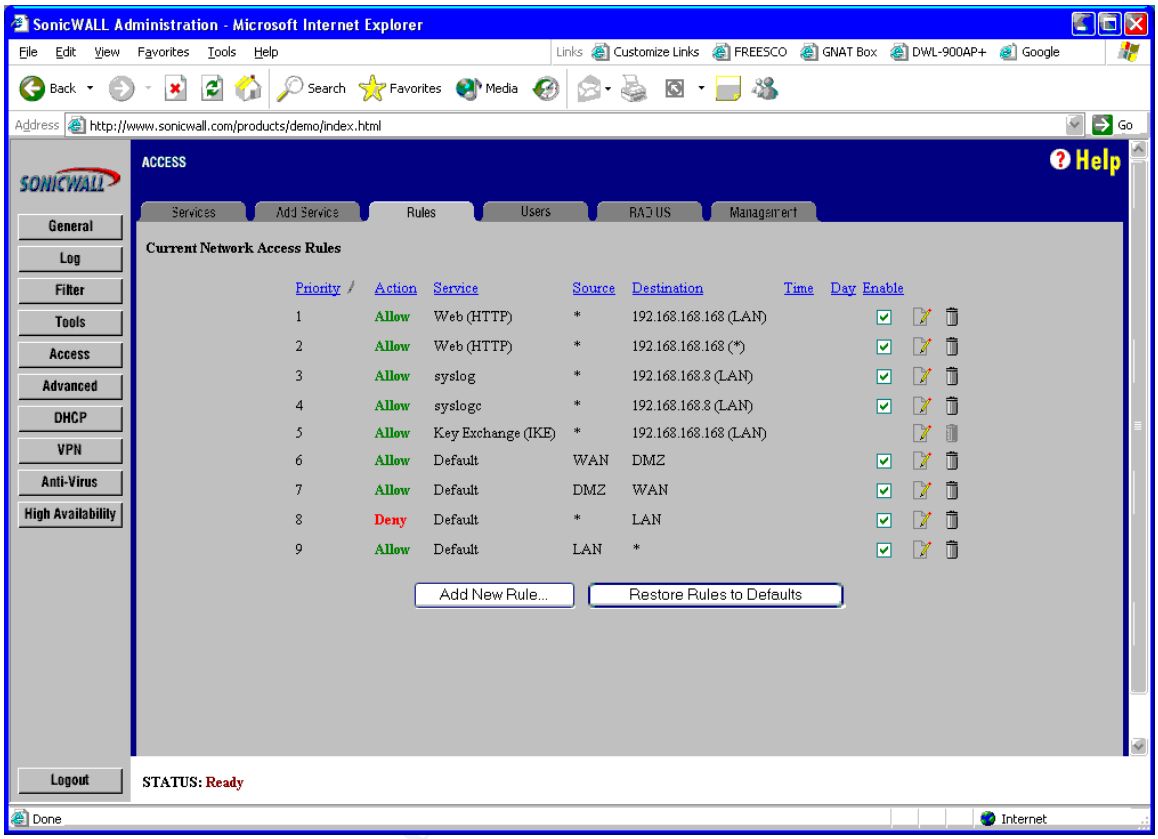
1. The GNAT Box has four fully configurable and equal interfaces compared to the Sonicwall's three interfaces. As can be seen in the final diagram, I needed four interfaces for the internal firewall.
2. The Sonicwall provides bandwidth management that could only be efficiently utilized at the perimeter.
3. The Sonicwall provides filtering that can be bypassed for certain sites and/or certain users. Forbidden domains can be entered and a custom web page shown to users when they try to access these forbidden domains. Domains can also be specified that bypass the ActiveX filters. Users can be created that are authenticated against a radius server, thus making it easier for users to bypass filtered domains, ActiveX, Java, and Cookies.
4. Randomize IP ID Option on the Sonicwall can prevent fingerprinting the Sonicwall appliance. This prevents an attacker from detecting that the firewall is a Sonicwall and thus keeps them from having additional information that they may be able to use in an attack.
5. The rule set at the perimeter is simpler. As explained next, the Sonicwall does not have as flexible of a rule set as the GNAT Box does.

The configuration of the rule set for the Sonicwall is not as configurable as I would like. For the first generation Sonicwall that we bought it is also limited to 100 rules. Luckily, this should not be a problem since my rules are fairly simple for controlling outbound access. I have two main complaints about the rule configuration. First, the Sonicwall automatically orders the rules. The administrator has no control over rule precedence. Second, there is no group feature. Rules can be created for individual IP address as well as a range of IP addresses. However, the administrator cannot create one rule for many IP addresses that are not consecutive. This task must be done by creating individual rules for each IP address. Since it is preferred to keep the rule set to a minimum for performance reasons, this last inconvenience can, in my opinion, unnecessarily impact the performance of the Sonicwall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 4 shows a sample screen shot of the rules screen from Sonicwall's web site. Since Sonicwall does not have an offline configuration utility, I did not want to give away my company's information by showing the live configuration.

Figure 4:



Listed next is the rule base that I configured for outbound access from the internal network for the Sonicwall. Remember, the Sonicwall automatically orders these rules.

1. Allow HTTPS Management from the LAN
2. Allow HTTP from the LAN to Anywhere
3. Allow FTP from the LAN to Anywhere
4. Allow Authentication from the LAN to Anywhere
5. Allow HTTPS from the LAN to Anywhere
6. Allow NTP from the LAN to Anywhere
7. Allow Ping from the LAN to Anywhere
8. Allow RealAudio from the LAN to Anywhere
9. Allow Citrix from the LAN to Anywhere
10. Allow DNS from the LAN to Anywhere
11. Allow SMTP from Anywhere to the WAN
12. Allow POP3 from the LAN to Anywhere
13. Deny Everything from the LAN to Anywhere

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

a. Deny all other traffic from the internal network

Listed next is the rule set that I configured for inbound access to the web server, mail server, the Citrix server, and the VPN for remote administration.

1. Allow GB Auth (TCP Port 76) from WAN to the GNAT Box
   a. This is the port that the GNAT Box VPN Authentication program uses
2. Allow SMTP from WAN to the GNAT Box
   a. Allow email to be sent from the Internet to the GNAT Box email proxy
3. Allow Citrix from WAN to the GNAT Box
   a. Allow Citrix connections to the GNAT Box. The GNAT Box will then forward the connections to the internal Citrix server.
4. Allow IKE from WAN to the GNAT Box
   a. GNAT Box VPN
5. Allow IPSec (ESP) from the WAN to the GNAT Box
   a. GNAT Box VPN
6. Allow HTTPS from the WAN to the Web Server
   a. Allow SSL Web connections to the web server.
7. Deny Everything from the WAN to Anywhere
   a. Deny all other unsolicited traffic from the Internet

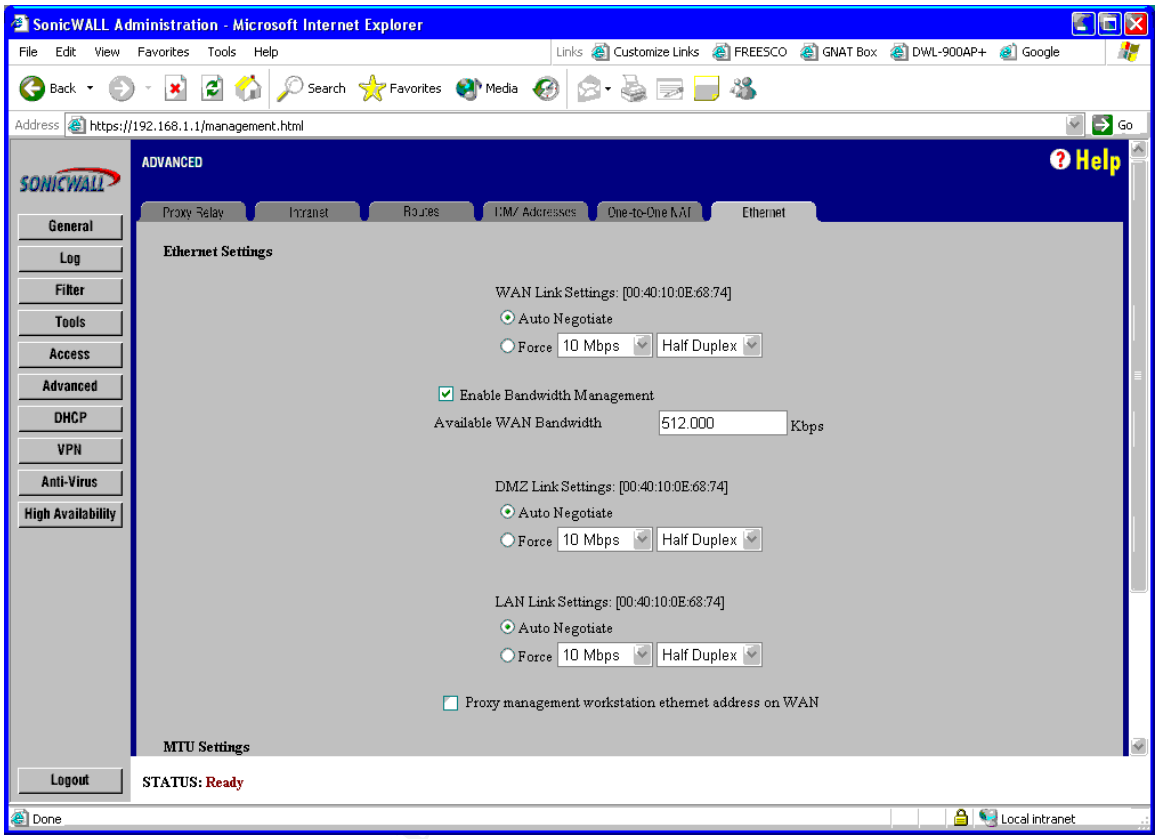
Listed next is the rule set that I configured for outbound access from the DMZ to the WAN.

1. Deny Everything from the DMZ to Everywhere
   a. This will alert me to any unknown connection attempts that the web server makes. These attempts may be the result of a compromised server

© SANS Institute 2003, Author retains full rights.

Figure 5 shows a screen shot of the Ethernet tab under the Advanced Settings for the Sonicwall. Here is where I enabled the bandwidth management feature and filled in the available bandwidth for our T1.

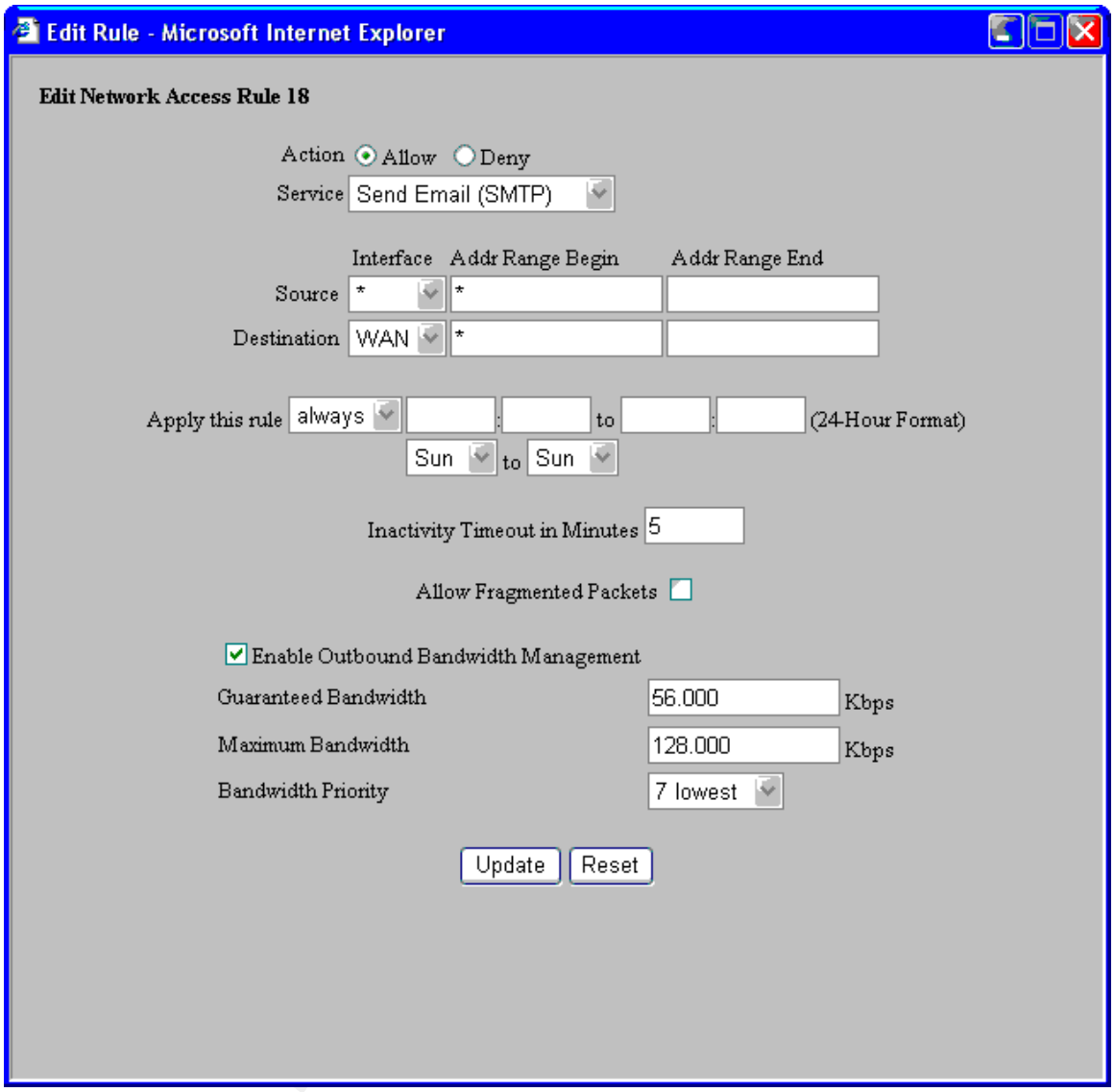
Figure 5:



When enabling bandwidth management for a rule, there are three settings to configure. The first is the Guaranteed Bandwidth. This is the amount of the bandwidth that was specified in Figure 5 that the traffic for this rule is guaranteed. The minimum setting is 20 Kb/s and the sum of all the guaranteed bandwidth entries must be equal to or less that the total available bandwidth configured in Figure 5. The second is the Maximum Bandwidth. This is the total amount of the total bandwidth that the traffic for this rule can consume if it is available. The minimum setting is 20 Kb/s. There is no max limit. The third setting is the Bandwidth Priority. These priorities are ranked from 0 (highest) to 7 (lowest). Figure 6 shows an example rule where I have enabled bandwidth management. The first generation Sonicwall Pro that I purchased supports 20 bandwidth management rules.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 6:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I enabled bandwidth management for three rules. They are as follows:

1. Allow SMTP from Anywhere to the WAN
   a. Guaranteed Bandwidth = 56.000 Kbps
   b. Maximum Bandwidth = 128.000 Kbps
   c. Bandwidth Priority = 0 highest

   This rule guarantees that all outgoing mail is also always guaranteed a 56K portion of the bandwidth and with the highest priority.

2. Allow DNS from the LAN to Anywhere
   a. Guaranteed Bandwidth = 56.600 Kbps
   b. Maximum Bandwidth = 128.000 Kbps
   c. Bandwidth Priority = 7 lowest

   This rule Guarantees that DNS lookups are always guaranteed a 56.6K portion of the bandwidth. However, it is at the lowest priority

3. Allow HTTPS from the WAN to the Web Server
   a. Guaranteed Bandwidth = 128.000 Kbps
   b. Maximum Bandwidth = 512.000 Kbps
   c. Bandwidth Priority = 1

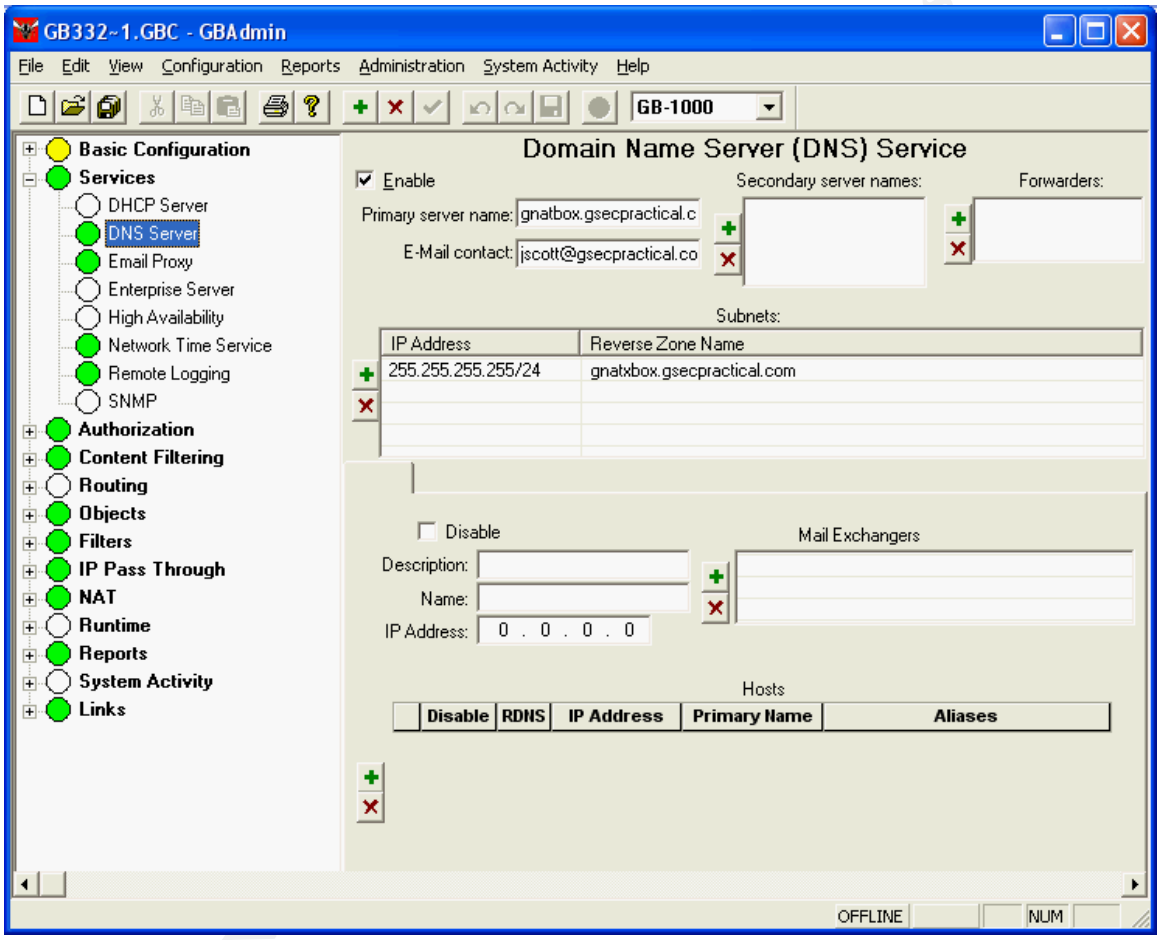
   Since bandwidth management only applies to outgoing traffic, this rule guarantees that all response packets get a 128K portion of the bandwidth with a high priority.

4. By default all other traffic uses spare bandwidth in a first-in-first-out scenario with a hidden priority of 8.

© SANS Institute 2003, Author retains full rights.

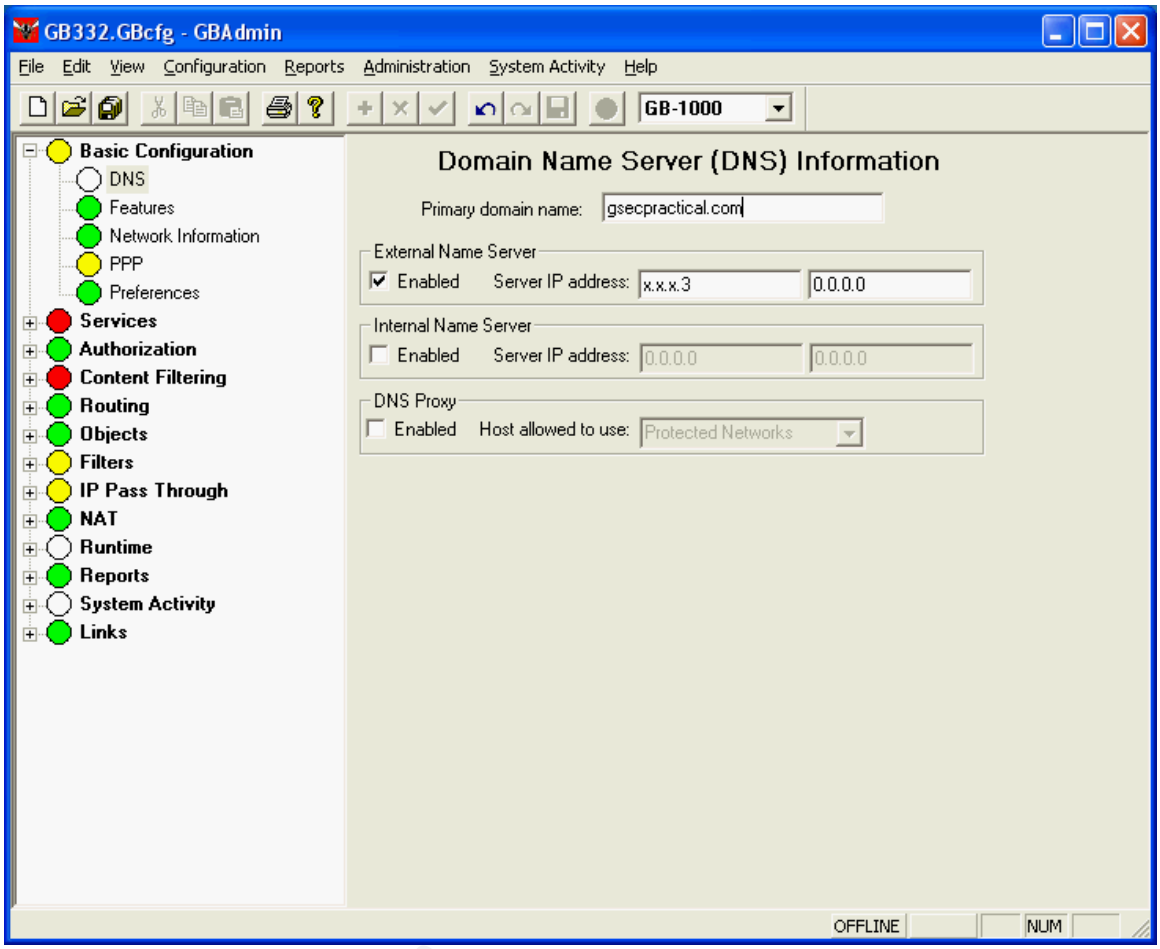
As can be seen in the chart from Figure 2, the GNAT Box jumps out as having the advantage for providing services to the Internet. The GNAT Box runs a hardened version of bind for the DNS Server and suits my company's needs perfectly for hosting our domain name. This also keeps us from having to build another machine for this purpose. Figures 7 and 8 show the configuration for setting up the DNS Server.

Figure 7:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 8:

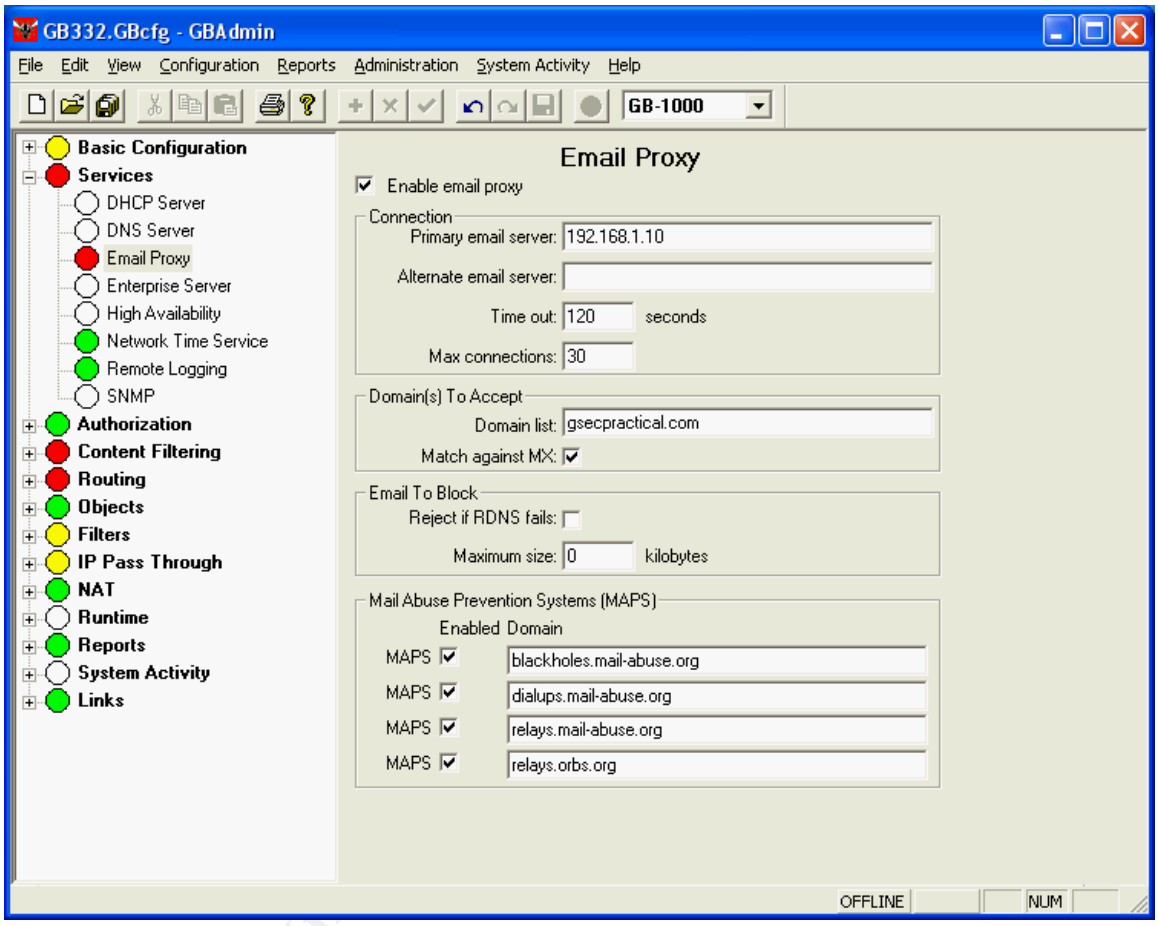


© SANS Institute

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The GNAT Box also includes an smtp email proxy that protects the internal email server from unauthorized access attempts. The email proxy also provides features for fighting SPAM. This eliminated the need for having an SMTP relay in the DMZ. Figure 9 shows the configuration for the email proxy.

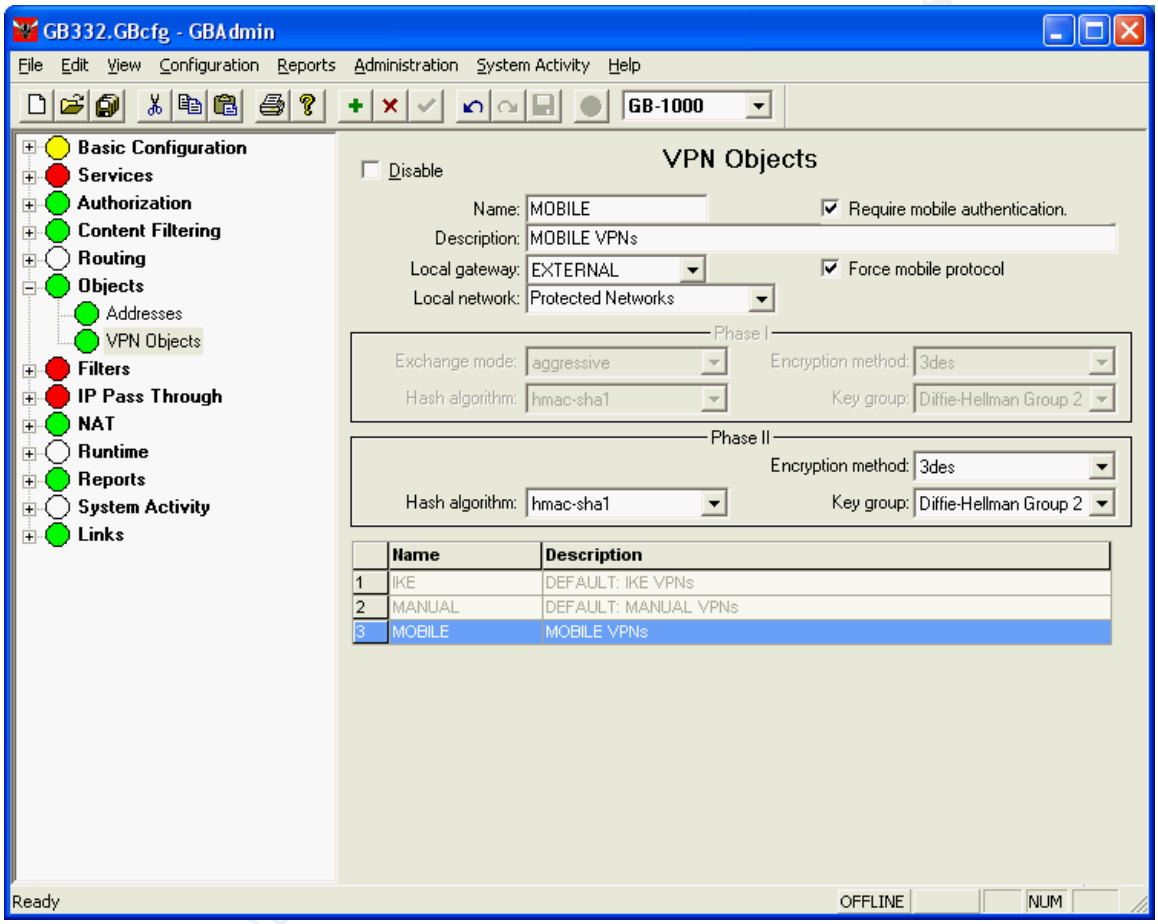
Figure 9:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

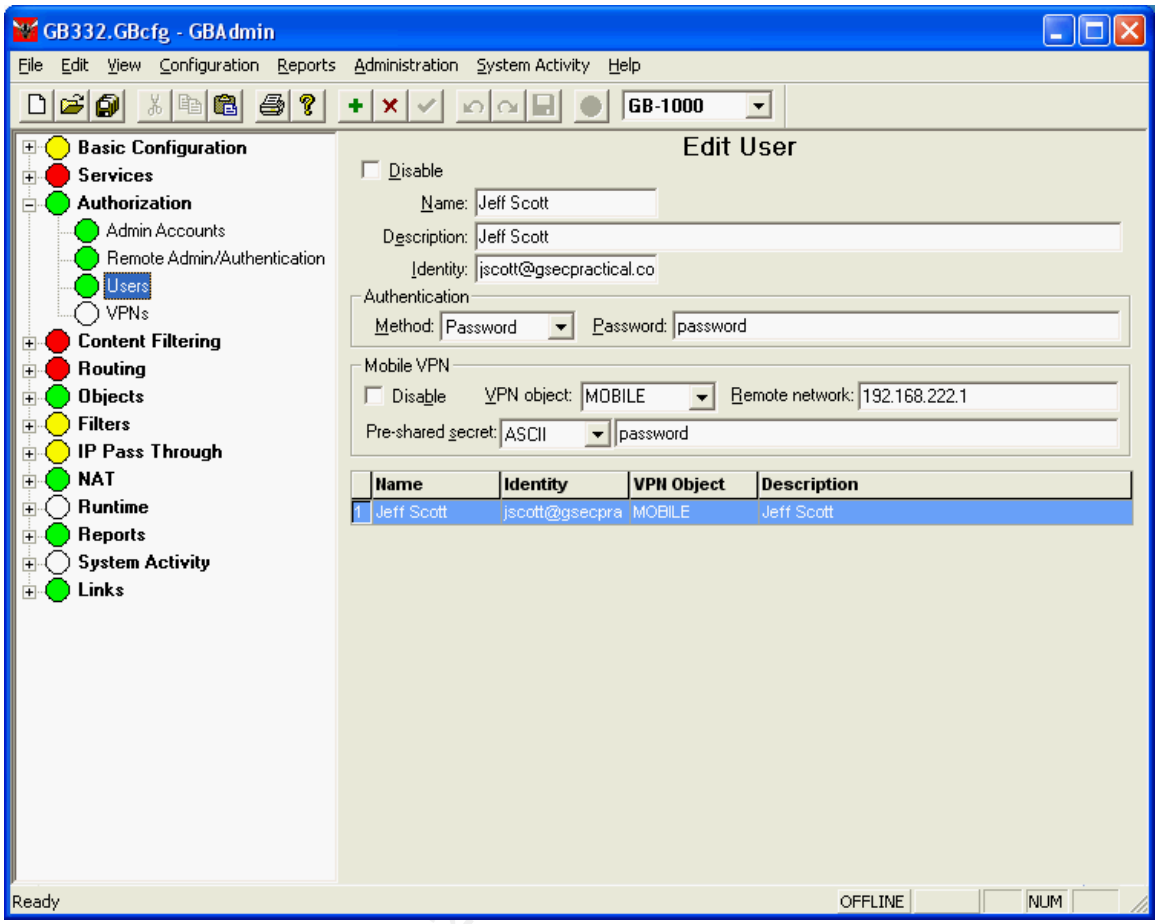
While I actually felt that the Sonicwall had a better VPN solution because of the fact that it supported RADIUS for user authentication and client certificates, I didn't want to burden the Sonicwall with the overhead of maintaining a VPN. Since I only needed a VPN solution to provide the Information Systems department with remote management, I felt the GNAT Box VPN would suffice. Figures 10 and 11 show the screens necessary for setting up the VPN.

Figure 10:



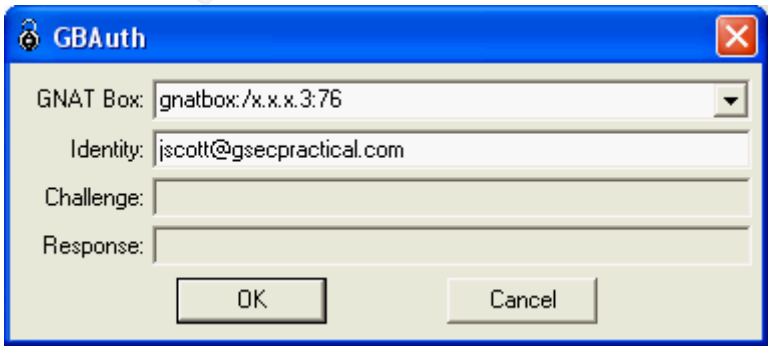
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 11:



The client side of the VPN uses the SafeNet client. As an additional protection for the VPN, GNAT Box provides the GBAuth program. This is a preliminary authentication mechanism for the VPN. If the "Require mobile authentication" checkbox as shown in Figure 10 is enabled, then the VPN cannot be initiated without first authenticating with GBAuth. Figure 12 shows a screenshot of the GBAuth program on the client.

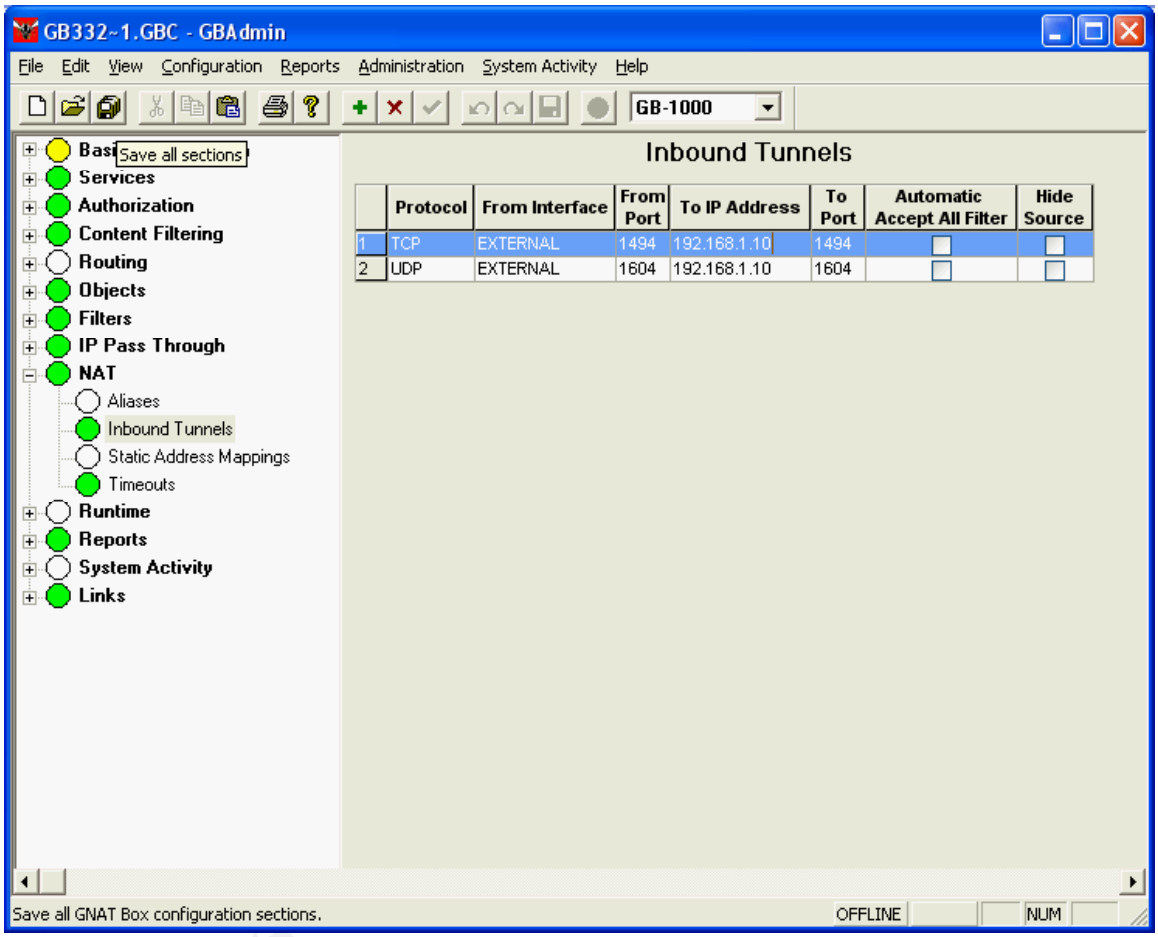
Figure 12:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The need for employee remote access was addressed by using Citrix. In order for clients on the Internet to access the Citrix server on the Private LAN, a tunnel needed to be created on the GNAT Box. Tunnels are only created for inbound unsolicited connections. Figure 13 shows the necessary tunnels that were configured to forward connections to the Citrix server.

Figure 13:

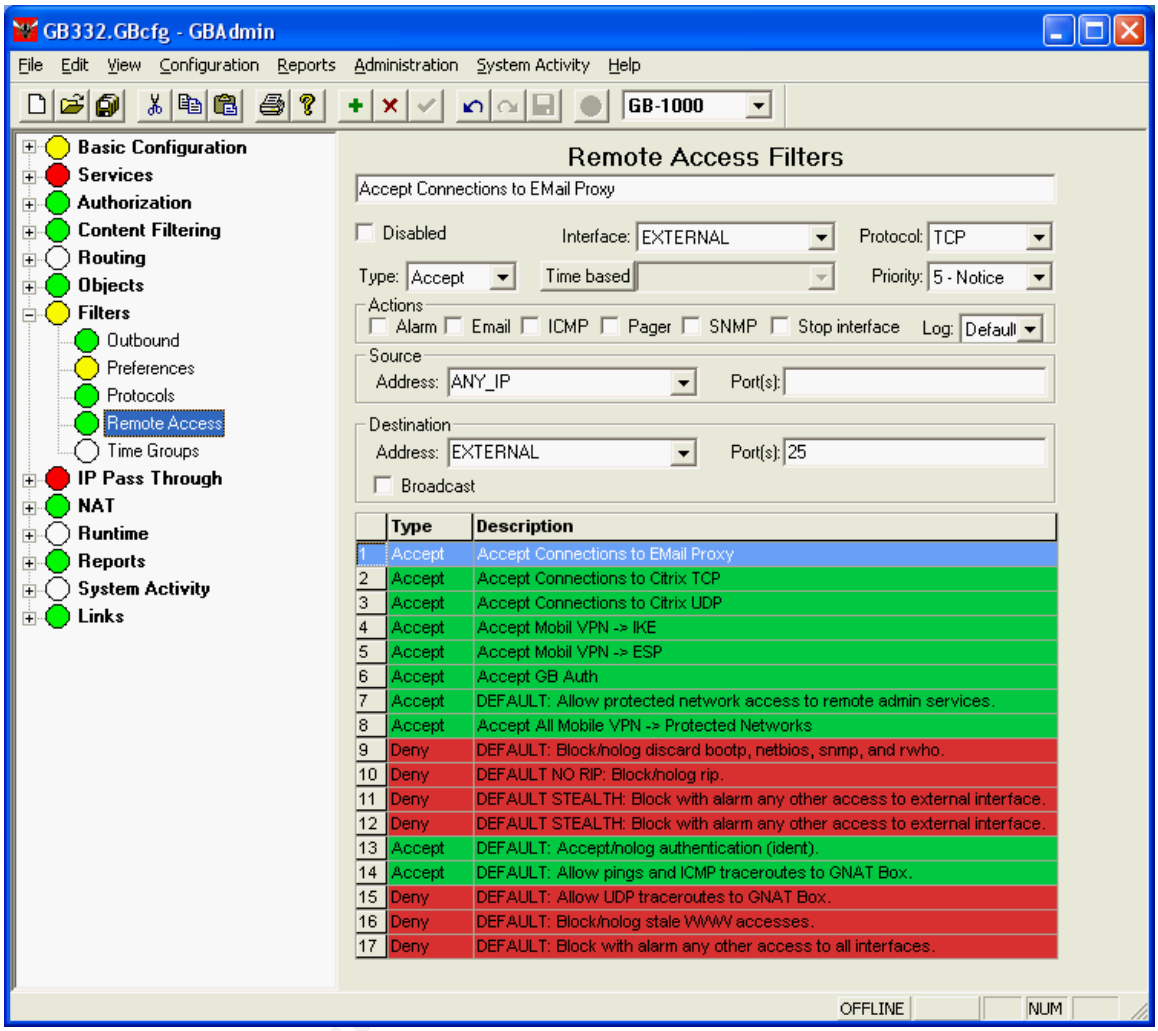


Tunnels require a corresponding Remote Access Filter that permits use of the tunnel. The Remote Access Filters for Citrix will be covered in Figure 14. I could have opened the Citrix server up to the Internet directly through the Sonicwall, but I didn't want to open up any ports to pass directly through the Sonicwall to the protected network. Therefore, I am passing the Citrix traffic as well as the VPN traffic through to the GNAT Box. The GNAT Box then takes all the processing hits for forwarding traffic.

Figure 14 shows the Remote Access Filters configuration for the GNAT Box. "Remote Access Filters control the access of packets that are directed at an IP address assigned to any of the network interfaces on the GNAT Box system" (GNAT Box User's Guide, p. 22).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 14:



Custom Rule Descriptions:

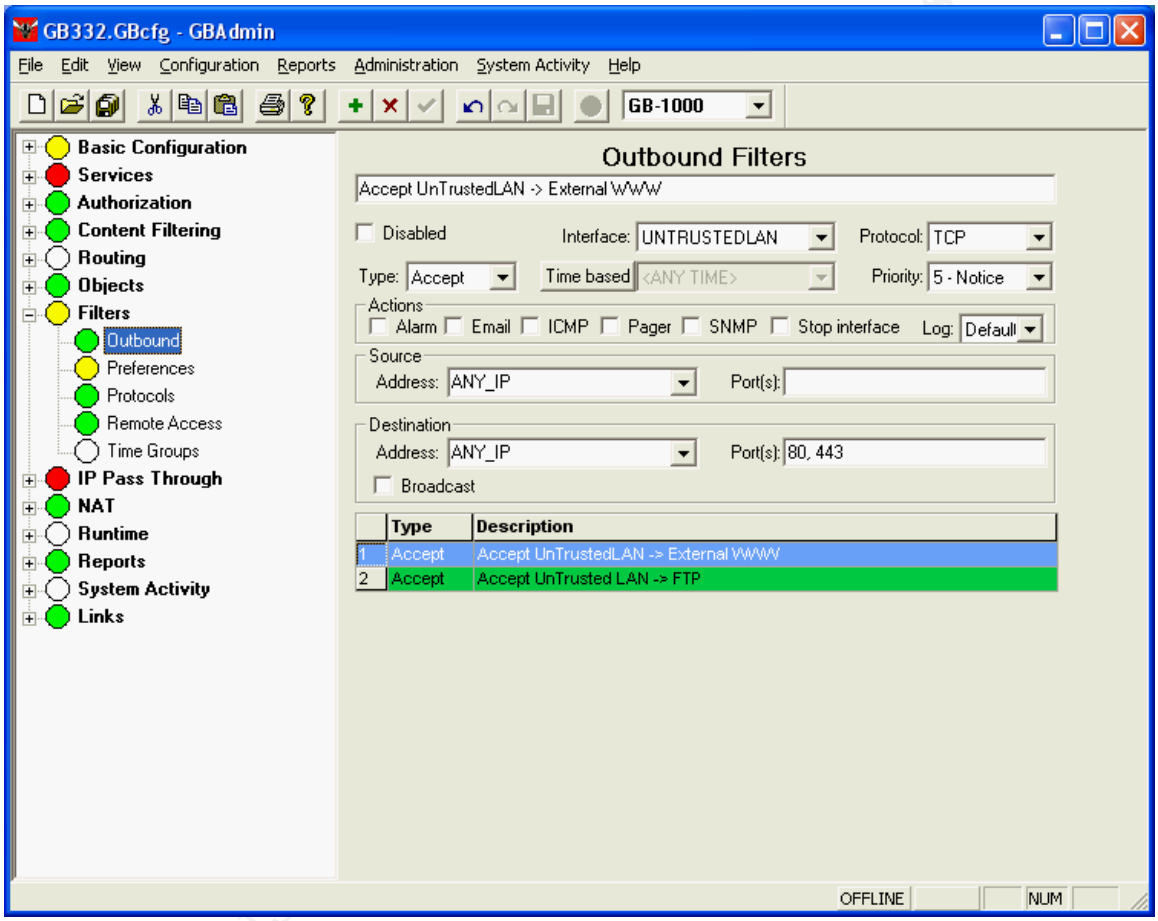
1. Accept Connections to Email Proxy
    a. Allow connections from anywhere to x.x.x.3 TCP Port 25
2. Accept Connections to Citrix TCP
    a. Allow connections from anywhere to x.x.x.3 TCP Port 1494
3. Accept Connections to Citrix UDP
    a. Allow connections from anywhere to x.x.x.3 UDP Port 1604
4. Accept Mobile VPN -> IKE
    a. Accept connections from anywhere to x.x.x.3 UDP Port 500
5. Accept Mobile VPN -> ESP
    a. Accept connections from anywhere to x.x.x.3 ESP Protocol
6. Accept GB Auth
    a. Accept connections from anywhere to x.x.x.3 TCP Port 76
8. Accept All Mobile VPN -> Protected Networks

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

a. Accept connections from VPN to Protected networks

Figure 15 shows the Outbound Filters. "The Outbound Filters control access of packets directed to IP addresses on an External network and to a PSN (if one exists)." (GNAT Box User's Guide, p.23). Only the UnTrusted LAN utilizes these filters to access the Internet.

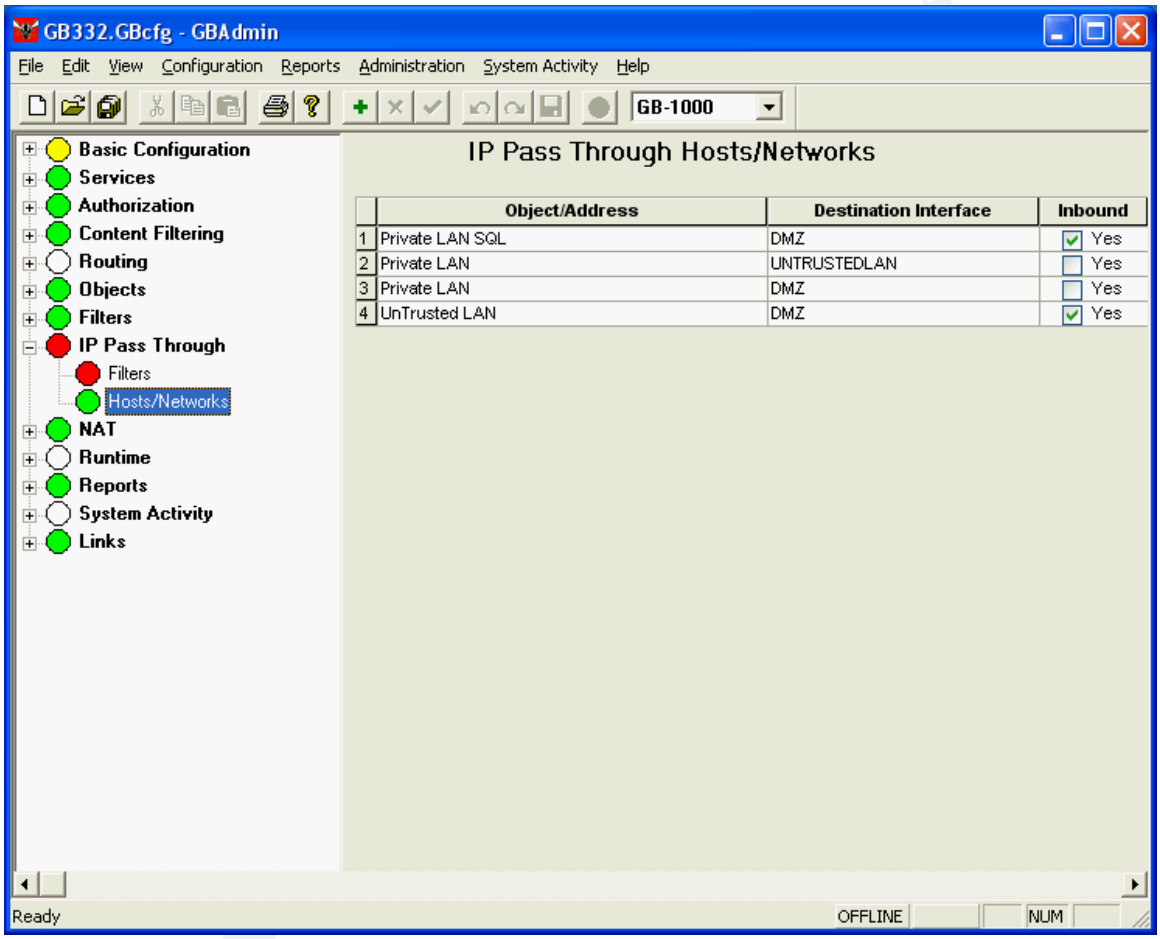
Figure 15:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IP Pass Through Hosts need to be defined in order to use IP Pass Through Filters. IP Pass Through is GNAT Box's term for NO-NAT. I did not want the communication between the UnTrusted Domain and the web server and between the Private LAN SQL server and the web server having Network Translation applied to it. Therefore IP Pass Through needed to be setup. Figure 16 shows the IP Pass Through Hosts/Networks that I defined.

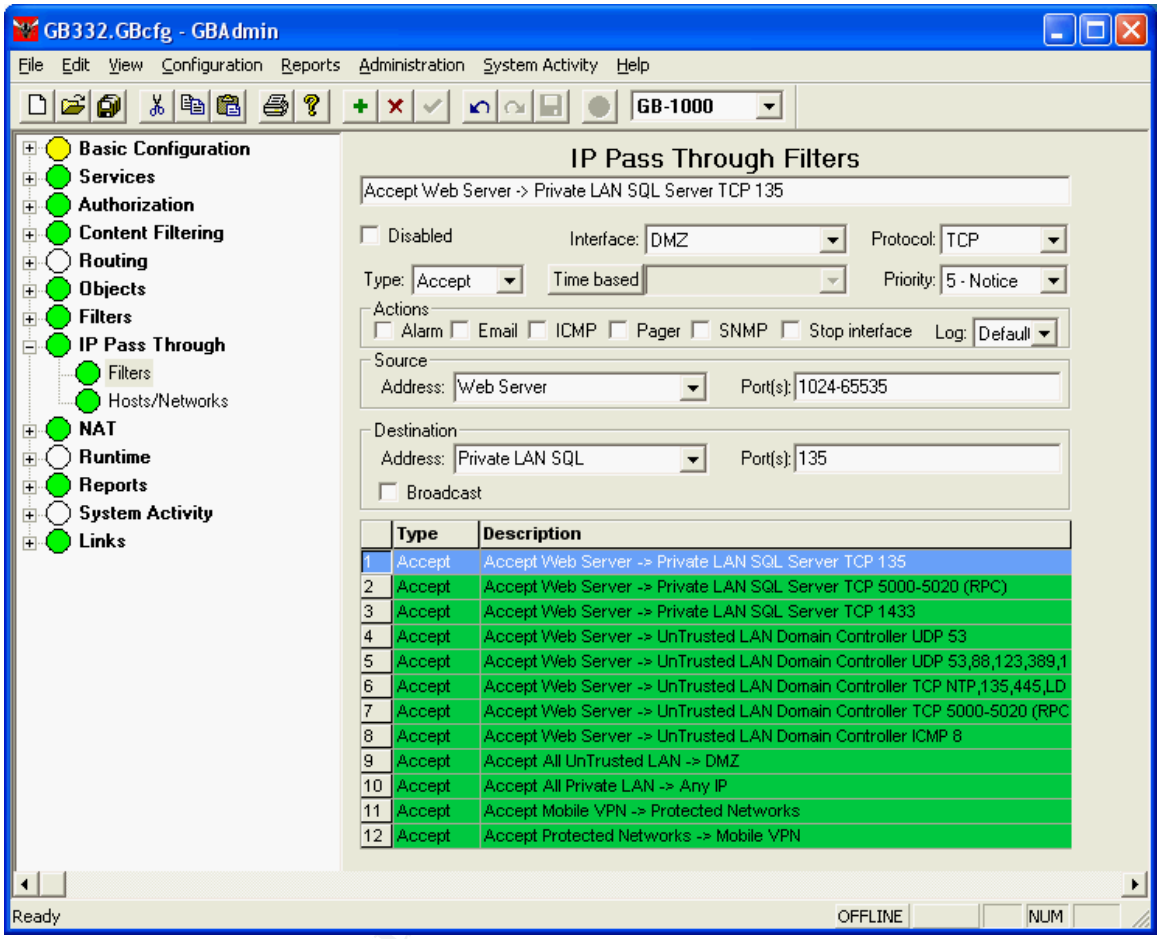
Figure 16:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 17 shows the actual rules for the IP Pass Through Filters.

Figure 17:



Custom Rule Descriptions:

The first three rules allow the Web Server to access the Private LAN SQL Server for the extranet application to function.

Rules 4 – 8 contain all the protocols and ports necessary for the web server to communicate with the UnTrusted LAN Domain Controller that the web server is a member of.

Rules 9-12 allow full access from the internal networks and the VPN

This configuration can be considered a defense in depth strategy because all inbound services need to navigate two firewalls. However, all outbound traffic is only passing through one firewall, in this case the Sonicwall. This helps to reduce the latency of traffic accessing the Internet from the internal network. I also implemented a third line of defense in the router. I enabled access lists on

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the Cisco 1720 router to filter the most common attacks. Listed below are the most important commands and access-lists to protect the router and the network.

Create an encrypted enable password for configuration changes:

```
enable secret 5 1234567890ABCDEFGHIJKLMNOPQRST
```

Prevent a packet from determining it's own path through the network:

```
no ip source-route
```

Disable the web interface on the router:

```
no ip http server
```

Disable the Cisco Discovery Protocol:

```
no cdp run
```

Turn on warning banners:

```
banner exec ^C Unauthorized Access Is Prohibited ^C
banner incoming ^C Unauthorized Access Is Prohibited ^C
banner login ^C Unauthorized Access Is Prohibited ^C
```

Configure the LAN Interface to only accept packets from our IP address range:

```
interface FastEthernet0
 description connected to EthernetLAN
 ip address x.x.x.1 255.255.255.0
 ip access-group 12 in
 no cdp enable

access-list 12 permit x.x.x.0 0.0.0.255
```

Configure the Internet interface:

```
interface Serial0
 description connected to Internet
 ip address y.y.y.1 255.255.255.0
```

Deny packets coming from the Internet that match private, loopback, and broadcast addresses. Deny packets destined for the Microsoft netbios ports:

```
 ip access-group 111 in
```

© SANS Institute 2003, Author retains full rights.

```
access-list 111 deny   ip 192.168.0.0 0.0.255.255 any
access-list 111 deny   ip 172.16.0.0 0.15.255.255 any
access-list 111 deny   ip 10.0.0.0 0.255.255.255 any
access-list 111 deny   ip 127.0.0.0 0.255.255.255 any
access-list 111 deny   ip 255.0.0.0 0.255.255.255 any
access-list 111 deny   ip 224.0.0.0 7.255.255.255 any
access-list 111 deny   ip x.x.x.0 0.0.0.255 any
access-list 111 deny   ip host 0.0.0.0 any
access-list 111 deny   tcp any any eq 135
access-list 111 deny   tcp any any eq 137
access-list 111 deny   tcp any any eq 138
access-list 111 deny   tcp any any eq 139
access-list 111 deny   tcp any any eq 445
access-list 111 deny   udp any any eq 135
access-list 111 deny   udp any any eq netbios-ns
access-list 111 deny   udp any any eq netbios-dgm
access-list 111 deny   udp any any eq netbios-ss
access-list 111 deny   udp any any eq 445
access-list 111 permit ip any any
```

Deny responses to ping and trace route from our network :

```
ip access-group 120 out

access-list 120 deny   icmp any any time-exceeded
access-list 120 deny   icmp any any echo-reply
access-list 120 permit ip any any
```

Prevent the router from sending ICMP unreachable messages:

```
no ip unreachables
```

Configure Telnet access with an encrypted password (password is sent in clear text across the network) only from the Sonicwall Pro.

```
line vty 0 4
 access-class 10 in
 password 7 1234567890ABCD
 login
access-list 10 permit x.x.x.2
```

© SANS Institute 2003, Author retains full rights.

These additional steps help to keep the firewalls from having to deal with the most basic and very common attacks. However, since the router is a small router, it needs to be monitored to make sure it is not being overloaded.

I then setup a syslog server using Kiwi Enterprise's Syslogd program running on Windows 2000 Server. All the firewalls and other network devices are configured to send their log messages to this server. This allows me to maintain and review all the logs in one place. Since it is very important that this server is not also compromised, this server was hardened by removing all unnecessary services and protocols and has ZoneAlarm Personal Firewall running on it to prevent any unauthorized access.

Being able to trace an event from different devices relies heavily on having accurate time on all the devices. Therefore, I then setup a Network Time Server running the NTP protocol. I configured this server using a stripped down version of Linux with no other services running on it. I again configured all firewalls, devices, and services to synchronize their time with this server.

IV. After

The bandwidth management features of the Sonicwall have proved to be valuable. The rules have kept the performance at an acceptable level. It is worth note that the Sonicwall I purchased was a first generation of the Sonicwall Pro. Later generations of the Sonicwall Pro appliances have faster processors and thus can handle more rules, more bandwidth management rules, and more VPN connections.

After completing the firewall setup, I ran Nmap and Nessus scans both from the Internet and internally against our configuration. These scans verified that the firewalls were configured correctly Since the Sonicwall is logging all connections inbound to the web server as well as all blocked attempts outbound from the web server, I should be alerted to when the web server may possibly be compromised and have a log for when it happened. In conjunction, if the attacker then tries to use the web server to launch attacks against the internal network, the GNAT Box will log all such attempts. While both firewalls support and have been configured to send alert email to me, it is important not to rely on the email. For the time being, I have resorted to manually looking over the syslog files for suspicious activity. However, this is where a vulnerability still exists and I realize I need to develop a more automated solution. I also want to implement an internal Intrusion Detection System (IDS) for monitoring the traffic inside the firewalls, particularly traffic coming from the web server. Overall this design has worked well and continued monitoring has created an effective defense in depth security perimeter.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

V. References

Global Technology Associates, Inc. GNAT Box Firewall System Software User's Guide. Orlando: Global Technology Associates, Inc., August 2001.

SonicWALL, Inc. SONICWALL Internet Security Appliances. Sunnyvale: SonicWALL, Inc., August 2001.

SonicWALL, Inc. SonicWALL 6.3.1.0 Addendum. Sunnyvale: SonicWALL, Inc., March 2002.

Brenton, Chris. SANS Institure 2.2 Firewalls 101: Perimeter Protection with Firewalls. Baltimore: SANS Institute, May 2001

Brenton, Chris and Spitzner, Lance. SANS Institute 2.3 Firewalls 102: Perimeter Protections and Defense, In-Depth. Baltimore: SANS Institute, May 2001

Global Technology Associates, Inc. Company's Home Page.
URL: http://www.gta.com

GNAT Box.com User Forum.
URL: http://www.gnatbox.com/cgi-bin/Ultimate.cgi

SonicWALL, Inc. Company's Home Page.
URL: http://www.sonicwall.com

Ramp Networks. Company's Home Page.
URL: http://www.webramp.com

Citrix Systems, Inc. Company's Home Page.
URL: http://www.citrix.com

SafeNet, Inc. Company's Home Page.
URL: http://www.safenet-inc.com

TruSecure ICSA Labs. Home Page.
URL: http://www.icsalabs.com

Internet Software Consortium. Home Page.
URL: http://www.isc.org/products/BIND/

Cisco Systems, Inc. Company's Home Page.
URL: http://www.cisco.com

© SANS Institute 2003, Author retains full rights.

Cisco Systems, Inc. “Improving Security on Cisco Routers.” Firewalls and VPN’s. (16 Oct. 2002).
URL: http://secinf.net/info/fw/cisco/add.html#sched

SANS Information Security Knowledge Base
URL: http://www.sans.org/resources/

Ipswitch, Inc. Company’s Home Page.
URL: http://www.ipswitch.com

Kiwi Enterprises. Company’s Home Page.
URL: http://www.kiwisyslog.com

Zone Labs, Inc. Company’s Home Page.
URL: http://www.zonelabs.com
Insecure.org. Nmap Home Page. (19 Mar. 2003)
URL: http://www.insecure.org

Nessus.org. Nessus Home Page.
URL: http://www.nessus.org

© SANS Institute 2003, Author retains full rights.