Global Information Assurance Certification Paper

Table of Contents 1
Jamy_Klein_GCFW.doc 2

GCFW Practical v1.6

Jamy Klein

November 12, 2001

Contents

1. **Introduction to GIAC Enterprises ---------- 3**
2. **Assignment 1 – GIAC Security Architecture ---------- 4**
3. **Assignment 2 – GIAC Security Policy ---------- 19**
4. **Assignment 3 – GIAC Security Audit ---------- 41**
5. **Assignment 4 – Design Under Fire ---------- 45**
6. **References ---------- 53**
7. **Appendix 1 ---------- 66**

Introduction

GIAC Enterprises is an online vendor of fortune cookie sayings and related merchandise. Over the past decade, GIAC has become a premier supplier of sayings to nearly all fortune cookie manufacturers, mainly due to the quality of GIAC's sayings. As a major supplier of fortune cookie sayings, GIAC has consistently worked to foster relationships with fortune cookie manufacturers and marketers. These relationships have in turn generated growth for GIAC.

In the past, GIAC has completed all transactions with authors of sayings, resellers, and manufacturers through traditional communication channels such as postal mail. Recently due to economic downturns and a desire foster more effective communication GIAC has decided to allow the individuals and companies they work with to connect to the GIAC network and perform business transactions. To ensure that no GIAC proprietary information is compromised during these transactions the following Information Security procedures and plans have been developed and implemented; Security Architecture Design, Corporate Security policy, and Security Audit.

Assignment 1: Security Architecture

Objectives

The purpose of this section is to provide GIAC enterprises with a security architecture that will safeguard GIAC property from Internet threats while enabling secure communication and transactions with GIAC business partners.

The following areas will be examined; security of internal systems, security of Internet accessible systems, secure remote access, ease of administration, and reduced cost.

Security Architecture Overview

This section provides a description of the security needs of GIAC and the architecture design and components used in implementation of the design. This overview will be divided into four areas of protection, customers, suppliers, partners, and internal users.

Customers: GIAC must be able to provide secure web based purchasing of fortune cookie sayings to customers. To this end the following technologies and services will be utilized.

1. GIAC will acquire certificates from Verisign corporation to ensure that

customers are able confirm our company's identity.

2. Secure Socket Layer (SSL) connections will be used to allow customers to establish encrypted channels with the GIAC e-commerce web server.
3. Each customer will be required to be registered on the e-commerce site, with a unique id and password.

Suppliers: GIAC must be able to allow suppliers to connect to a private site to upload finished fortune cookie sayings. This must be accomplished in a secure manner to protect the property and copyrights of both GIAC and the authors.

1. Suppliers will connect to a secured FTP server through Secure Shell (SSH). The FTP server will not be directly accessible to the Internet. Suppliers will have to SSH to an intermediate host which will than allow authenticated users access to the FTP server.
2. To check the status of submissions and payment for their product, suppliers will be able to connect to a web server via SSL.
3. Each author will be required to have a unique user id and password. The password will be required to contain at least one number, one special character, and be at least 6 characters in length.

Partners: GIAC will supply its partners with VPN connections to our corporate network. GIAC will provide this service to allow our partners easy access from foreign countries to our fortune cookie saying database.

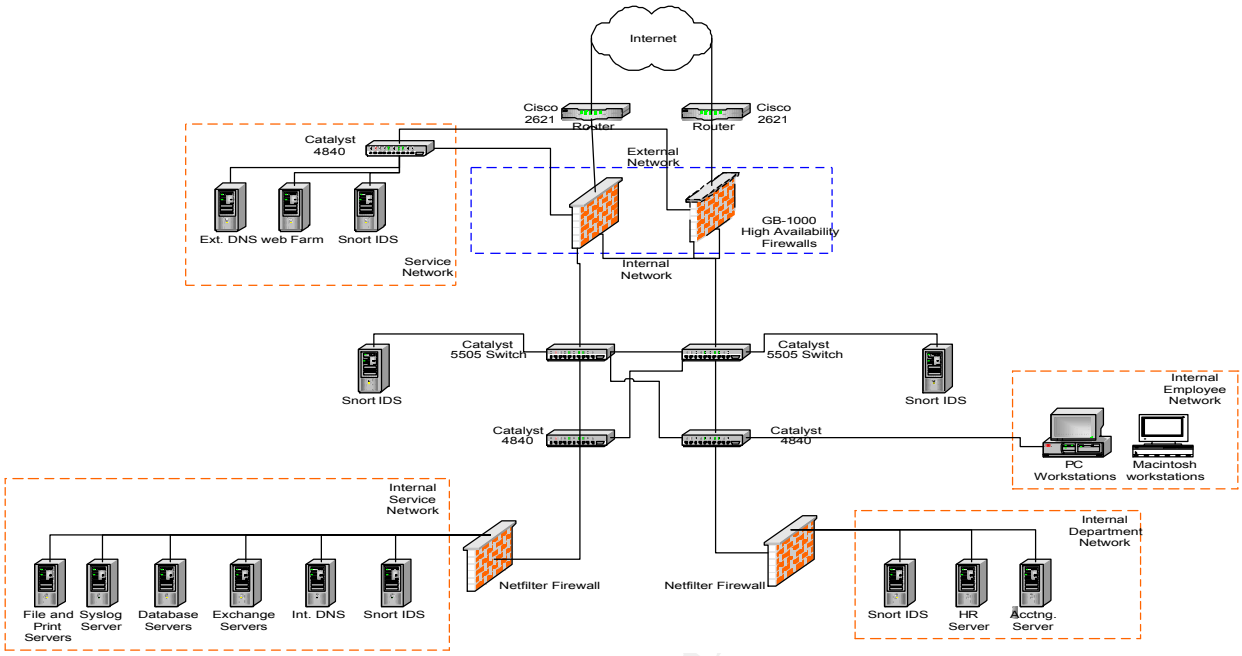
1. GNATBox GB-1000 firewall/VPN appliances will be used to terminate the VPN tunnel on the GIAC side of the connection. These units utilize the IPSec security protocol to ensure compatibility with products from practically any vendor.
2. The partners VPN will be filtered at the GNATbox firewall to restrict access to only the fortune cookie sayings database. This access will be set to read only through access control restrictions on the corporate database server.

Internal Users: GIAC internal employees must have access to Internet resources for job functions. The following services are required for use by internal users.

1. World Wide Web will be provided to allow internal users to browse the web for the latest industry news to search for prospective new customers.
2. Mail access will be allowed to facilitate text communication with customers, partners, prospective customers, and others interested in GIAC Enterprises.

Network Design

Based on the above requirements the network infrastructure will be designed as follows:

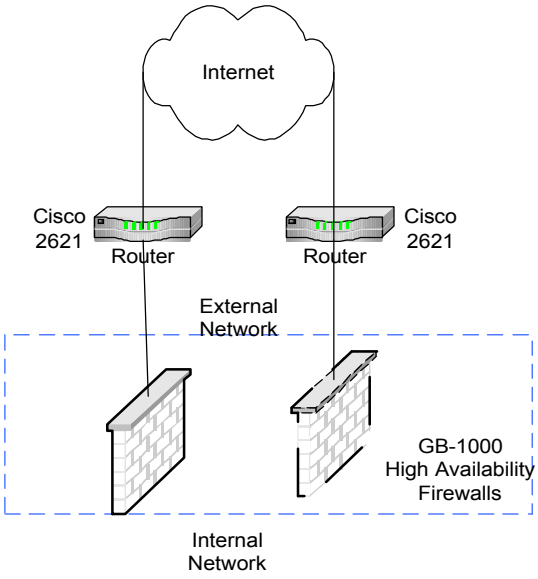


Each area of the GIAC network will be defined in detail below and list the security features and requirements for internal users, partners, suppliers, and customers. Each section will illustrate both the physical equipment topology and the logical topology. The areas to be defined are, External Network, Service Network, Internal Network, Internal Service Network, and the Internal Departmental Network.

External Network

The external network is the area of the GIAC network outside the corporate firewall facing the public Internet. This network uses the Internet protocol address range of 10.20.30.xx/255.255.255.0 assigned by GIAC's Internet Service Provider.

Physical Topology:



Physical Topology: External Network

The external network infrastructure has been designed for performance, security, and redundancy utilizing the following components.

1. Cisco 2621 Router

   The 2621 router has been chosen to handle the connections between the GIAC

perimeter firewalls and GIAC's ISP. This router model was chosen due to its modular design able to handle diverse interface requirements and due to its support of Cisco Access Control Lists (ACL). Each router is configured as a separate connection and route for redundancy.

Each router is configured with a separate routable Internet Protocol address. and The network range that will be used is 10.20.30.1/255.255.255.0. These routers are protected by ACLs that block non-routable address spaces defined by the Internet Assigned Numbers Authority (IANA) in RFC 1918, from entering the GIAC network through the Internet connections. Additionally, the routers are setup to prevent address spoofing by users on the internal GIAC corporate network by restricting outbound Internet Protocol addresses to the routable class C address space provided by our ISP. The routers will log all blocked traffic to a syslog server on the internal service network.

The 2621 routers will be configured with Cisco IOS version 12. This version is not the newest release in the IOS product line. IOS 12 is however the latest release to be listed by Cisco as being in the Mature Maintenance (MM) phase of its life. According to the Cisco IOS website, (**http://www.cisco.com/warp/public/732/releases/release120.shtml**) products designated as MM have "demonstrated a high degree of code stability and will continue to address customer-found defects". This is a benefit to GIAC as it will allow a stable configuration that does not utilize possibly unreliable bleeding edge

technology on the perimeter of the network.

2. GNAT Box GB-1000 Firewall Appliances

Between the External and Internal networks, Global Technology Associates' (GTA) GNAT Box Firewall appliance model GB-1000 will be utilized to perform inbound traffic filtering, outbound traffic filtering, and provide Virtual Private Network (VPN) services for GIACs partner companies.

The GNAT Box appliances were chosen due to their extensive feature set, ease of administration, reliability, and lower total cost as compared to similar solutions.

Features: The GB-1000 features the following technologies.

1. Stateful packet inspection and filtering: This technology helps to ensure more secure and reliable connections by going beyond simply blocking ports and instead keeping track of what connections were opened by an allowed client.
2. IPSec protocol VPN support: This technology is specified by RFC 1825. IPSec's goal is to allow secure interoperable communication through a standards based protocol. This feature will allow GIAC partners to securely connect to the GIAC network using any IPSec based product.
3. Ability to log to a syslog server: This feature will allow centralized log management as the traffic will be sent to our exisiting syslog server.
4. High Performance: GTA states that the GB-1000 can handle 32000

simultaneous connections. It is not expected that GIAC will have this amount of connections active at one time, but this will allow room for increased traffic as GIAC becomes a larger company.

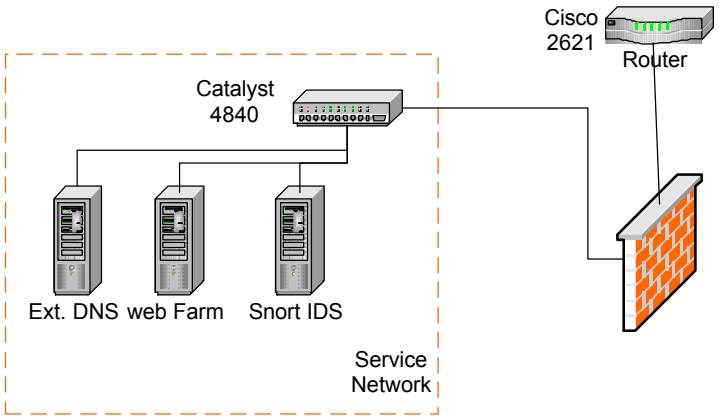
5. High Availability: This technology will allows the GB-1000 units to communicate their status back and forth. This communication allows traffic to be redirected to another GB-1000 unit in the event of connection or firewall failure. (The operation of this feature will be defined in section 2)
6. Variety of supported network interfaces: The GB-1000 supports various network technologies including token ring, 10/100/1000 megabit Ethernet on category 5 wiring, 10/100/1000 megabit Ethernet on fiber optic cable, and also supports ATM technology. This will allow the GB-1000 to be used in the GIAC network now as well as in the future as the infrastructure is moved to new network technologies.
7. NAT: NAT or Network Address Translation allows private addresses to be run on the networks protected by the firewall, and to still enable Internet access.

Configuration: Each GB-1000 will be connected via its external network interface to one of the Cisco 2621 routers. Each GB-1000 external interface will have routable IP addresses assigned as follows; GB-1000-1 = 10.20.30.2, GB-1000-2 = 10.20.30.3. The remainder of the routable class C IP range will be used to translate routable addresses and ports to servers protected on the service network. The GB-

1000 units will be run in tandem to provide high availability, this will ensure network access and traffic filtering is maintained in the event of a failure. The GB-1000 units

Service Network

The Service Network is defined as the network connected to the GB-1000 firewall units that houses GIAC servers that are accessible by the Internet. This network is configured using the private addresses and translated using NAT to the GB-1000 firewall units.



Service Netork Topology

The service network consists of a Cisco Catalyst 4840 load-balancing switch connected to

the service network interface on both GB-1000 firewall appliances. All of GIACs publicly accessible servers are in turn connected to the Catalyst 4840. The Cisco switch provides the capability to direct traffic from the service network to either firewall depending on firewall availability. Additionally this configuration allows traffic to the service network to be filtered inbound and outbound and also segregates the service network from the internal network.

The servers installed on the service network are as follows:

1. External DNS: Provides Domain Name Service lookup for publicly accessible resources.
2. Web Servers: Hosts all publicly accessible GIAC web sites.
3. SNORT IDS: The SNORT intrusion detection server is used to monitor suspicious traffic entering or leaving the service network.

Server Configuration

Each server housed in the service network runs the Redhat Linux operating system, hardened using the Bastille Linux system. The Bastille system disables unnecessary services and implements many of the guidelines specified in SANS Securing Linux Step by Step.

All servers are also configured with the open source Tripwire file integrity system to prevent file replacement hacks. The Tripwire system works by essentially taking a snapshot of a particular file at a given point. This snapshot is used as a baseline to

compare files to. If a file is thought to have been modified by a hacker, the file can be compared to the known good snapshot to determine if it has been compromised.

Each server will be assigned a private Internet Protocol address in the 192.168.0.1/255.255.255.0 class C network range. Ports 22, 53, 80, and 443 will open for use by servers and services. All TCP/IP ports not specifically used by an allowed service will be blocked at the firewall.

Port 22 will be opened to allow authors that work with GIAC to securely connect to the GIAC web server via SSH to upload completed work.

Port 53 will be open to allow the external DNS server to communicate with ISP and Root DNS servers.

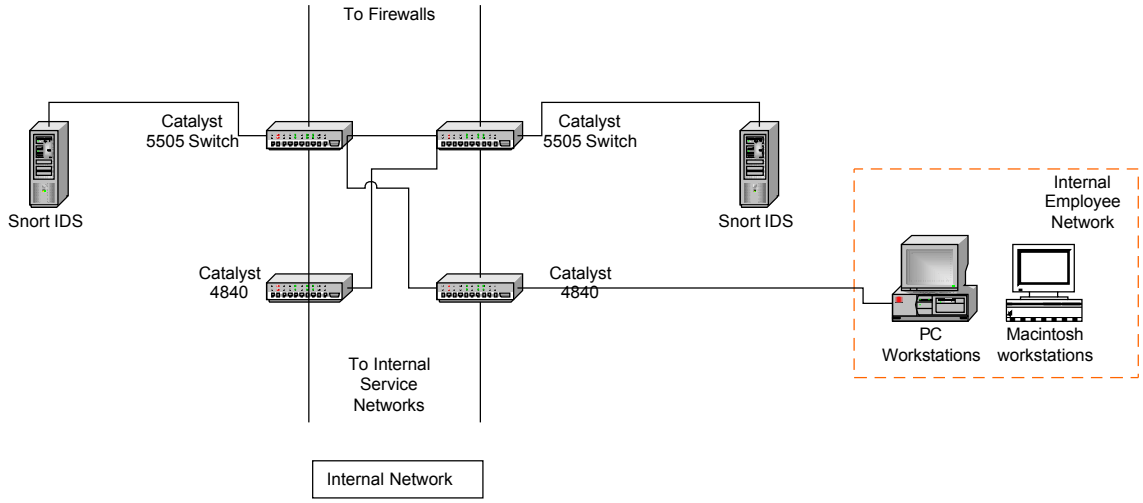
Port 80 will be open to allow access to the GIAC website using the HTTP protocol.

Port 443 will be open to allow Secure Socket Layer access to the GIAC web server for customers placing orders.

The SNORT Intrusion Detection System will be configured to use the ARACHNIDS Signature database found at **www.whitehats.com**.

Internal Network

The internal GIAC network will be used as an inter-connect between the secured Internal service network and the secured Departmental Service Network. In addition the Internal Network will also connect all local user workstations in the GIAC headquarters.



The Internal Network uses the private network range of 172.16.0.0/255.255.0.0 and is composed of two Cisco Catalyst 5505 switches and two Cisco Catalyst 4840 load-balancing switches. Each Catalyst 5505 switch is connected to a GB-1000 firewall and to a SNORT IDS. Each Catalyst 4840 is connected to both Catalyst 5505 switches. This configuration allows a redundant network infrastructure to assure service to all departments and employees.

Two SNORT IDS servers are connected to the Internal Network. These units are connected directly to each Catalyst 5505 switch. The main goal of this SNORT installation

is to attempt to detect any suspicious traffic that is able to pass through the firewall rulebase. Each SNORT machine runs the ARACHNIDS rule database.

Employee Segment

The employee network segment of the Internal Network houses all individual employee computers. The GB-1000 firewalls will be configured to allow only HTTP, HTTPS, and GNATBox administration traffic. All traffic traveling from the employee network will be translated at the firewall to routable addresses.

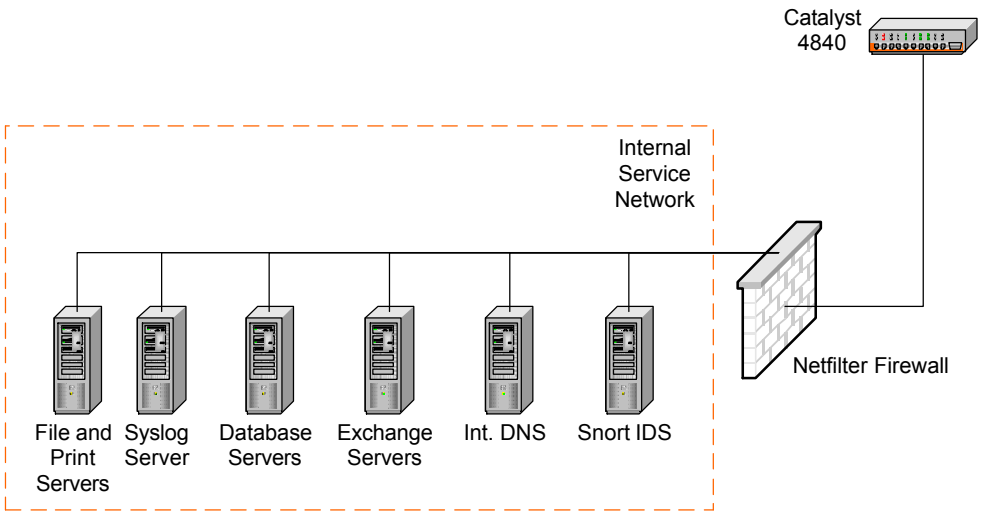
Each workstation will be configured with Sygate managed firewall software and McAfee Anti-Virus software.

The Sygate firewall is configured with a company wide workstation policy that is verified by the Sygate management server upon power on of a workstation. If any changes are found in the workstation policy a log entry is generated and the management server forces the client firewall back to the predefined configuration. In addition, Sygate also verifies the integrity of allowed applications to prevent modification.

McAfee anti-virus will be configured to detect virus infections in email in addition to files on the hard disk of the workstation. Any infections will be reported to the management server by the workstation software.

Internal Service Network

The Internal Service Network is used to house all internal GIAC servers such as the enterprise Database server, Internal DNS, Exchange Email, etc. This network is connected to the Internal network via a Linux NetFilter firewall and a Cisco catalyst 4840 switch.



The internal service network is screened in this manner to reduce unnecessary traffic to corporate server resources and to also prevent attack from compromised hosts on the internal network.

The Netfilter firewall on this network is configured to only allow specific traffic from

specific resources as defined below.

Syslog server: Access to the syslog server is filtered based on IP address. The Cisco routers, SNORT IDS machines, and GB-1000 firewalls are the only equipment allowed to access the syslog server on TCP port 514. All other traffic to the Syslog server is dropped.

Internal DNS: Traffic from any address on the Internal networks is allowed to use TCP port 53 of this server for DNS lookups. All other traffic to this server is dropped.

Database Servers: Access to the database server is limited to internal IP addresses and to GIAC web servers on TCP ports 7000, 7010, 7020, and 7030. All other traffic is dropped.

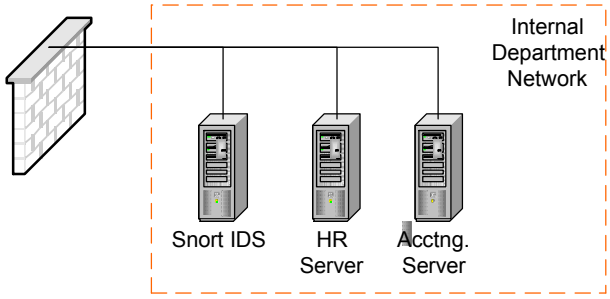
File and Print Server: Access to the file and print servers is limited to internal addresses only on TCP ports 139 and 512 through 1023 for Windows printing and file sharing.

Exchange Server: Access to Exchange will only be allowed from Internal Network Addresses and the GB-1000 email proxy. As such access will only be granted for TCP ports 25,110, and 1024 through 2048. Exchange will be configured to only use these ports.

There will be no traffic directly allowed through the firewall for the SNORT IDS' IP address. The SNORT machine will serve to detect any intrusion attempts that have been able to bypass the firewall.

Internal Departmental Network

Individual department servers for Accounting and Human Resources will be housed on this firewall screened internal network.



This network is protected by a NetFilter Firewall. The NetFilter Firewall will be configured to allow access to each department server based on an IP range given to each department. Accounting will be assigned address range 172.16.0.1 to 172.16.0.100. Human Resources will use address range 172.16.0.101 to 172.16.0.200.

A SNORT Intrusion detection system is installed on this network to detect any intrusion attempts that are able to bypass the firewall.

Assignment 2: GIAC Security policy

Objectives

This section will develop the security policy and configuration for the GIAC architecture defined in Assignment 1. It will focus specifically on inbound and outbound traffic rules for the routers and firewalls and also on the development of the VPN policy as dictated by the network design.

Router

The routers used on the GIAC network will be configured to provide both inbound and outbound filtering. Using inbound and outbound filtering the routers will be able to prevent address spoofing and also prevent and reduce various forms of attacks. In addition filtering on the routers will be kept to a minimum to prevent overload of the router CPU.

Inbound Filtering:

Inbound filtering will be used to block spoofed traffic that originates outside the GIAC network utilizing GIAC routable IP addresses, to block spoofed traffic from private address ranges attempting to enter the GIAC network, to prevent smurf attacks from the hosts on the internet utilizing broadcast addresses, and to deny traffic from a host using the loopback address.

ACL: access-list inbound deny ip 172.16.0.0 0.240.255.255 any log

!denies traffic from private ip range 172.16

access-list inbound deny ip 192.168.0.0 0.0.255.255 any log

!denies traffic from private ip range 192.168

access-list inbound deny ip 10.20.30.0 0.255.255.255 any log

!denies traffic spoofed using GIAC routable class C range

access-list inbound deny ip host 127.0.0.1 any log

!denies traffic with the loopback as its source

no ip direct-broadcast log

!denies traffic with broadcast address as destination

Router Setup: Below is the basic format for a Cisco ACL entry.

Access-list(list name) Action(permit/deny) Protocol(IP,ICMP, etc.) Source(IP address) Mask(network mask) Destination(IP address) Operator(less than, greater than, equal, not equal) Port

Commands: Below are the steps used to install the above ACL on the router.

1. Logon to the router using the Access Server. Enter required logon and password.
2. Type "enable", to enter privilege mode.
3. Enter the enable password and you will get the following prompt; giac1#
4. Type "configure terminal" this allows configuration from the command line terminal.
5. giac1(config)#interface serial 0
   giac1(config-if)#ip access-group inbound in
   giac1(config-if)#exit

   giac1(config)#access-list inbound deny ip 192.168.0.0 0.0.255.255 any log
   giac1(config)#access-list inbound deny ip 10.20.30.0 0.255.255.255 any log
   giac1(config)#access-list inbound deny ip host 127.0.0.1 any log
   giac1(config)#no ip direct-broadcast log

Outbound Filtering

Outbound filtering will be used to prevent internal hosts from being utilized to launch spoof attacks against other networks. As such the ACL will be essentially the same.

ACL: access-list outbound deny ip 172.16.0.0 0.240.255.255 any log

!denies traffic from private ip range 172.16

access-list outbound deny ip 192.168.0.0 0.0.255.255 any log

!denies traffic from private ip range 192.168

access-list outbound deny ip host 127.0.0.1 any log

!denies traffic with the loopback as its source

Commands: Below are the steps used to install the above ACL on the router.

1. Logon to the router using the Access Server. Enter required logon and password.
2. Type "enable", to enter privilege mode.
3. Enter the enable password and you will get the following prompt; giac1#
4. Type "configure terminal" this allows configuration from the command line terminal.
5. giac1(config)#interface Ethernet1
   giac1(config-if)#access-list outbound in
   giac1(config-if)#exit
   giac1(config)#access-list outbound deny ip 172.16.0.0 0.240.255.255 any log
   giac1(config)#access-list outbound deny ip 192.168.0.0 0.0.255.255 any log
   giac1(config)#access-list outbound deny ip host 127.0.0.1 any log

Firewall Policy

GNATBox GB-1000 firewall appliances will be utilized to enforce and control access to servers located on the Service Network, to restrict entry into the GIAC Internal Network, and to restrict outgoing traffic from the network to meet the needs specified in section 1. Both inbound and outbound filtering will be used. A complete printout of all configured rules will be provided in Appendix 1 along with a filter format sample.

The GB-1000 units will be run in tandem in a high availability configuration. Each GB-1000 has been setup with three network interfaces; external (EXT), protected (PRO), and Public Service network (PSN) as a result each interface's policy will be detailed separately. It should be noted that I will not discuss the filters to allow VPN access in to the network in this section, I will instead discuss them as part of the VPN policy section. I will also discuss the configuration in a separate section.

Below is the default behavior of the GNATBox firewall unit as described in the GNAT Box user manual. When an Item below refers to the GNAT Box, it means that access to the actual Interface IP address assigned to the particular GNAT Box network card is not permitted. No filters are installed to induce this behavior, it is instead hard coded in the GNAT Box software.

Implicit rule: "That which is not expressly prohibited is denied." This rule means that if a filter is not in place to allow access from the Internet to the internal network or PSN that the traffic is denied.

Remote Access:

1. All inbound access from the external network is denied, unless expressly permitted by a filter.
2. All access from the external network to the GNATBox is not allowed, unless expressly permitted by a filter.
3. Access to the web browser interface is allowed only from IP addresses on the protected network.
4. Access from the Private Service Network to the GNATBox is not allowed unless expressly permitted by a filter.
5. Access from the Private Service Network to the protected network is not allowed unless expressly permitted by a filter.
6. Access to the console interface requires a user ID and password.
7. Access to the web browser interface requires a user ID and password.
8. GNAT Box filters are processed in order starting at the number one.

Outbound Access:

1. All outbound access from the protected network to the Internet is allowed, unless expressly permitted by a filter. Traffic that does not originate from the network range defined as the protected network is denied.
2. All outbound access from the PSN network to the Internet is allowed, unless expressly denied by a filter. Additionally, GNAT Box automatically denies any

outbound traffic that does not originate from the network range defined as the PSN network.

3. All outbound traffic from the PSN or Internal networks is translated to the routable IP address of the EXT interface or to a separate routable IP address defined in the "aliases" and "static mappings" sections of the GNAT Box configuration.

Creating GNAT Box Filters

The GNAT Box firewall supports three modes of configuration; console interface, web browser, and GB Admin utility. The advantages and disadvantages to each are listed below.

Console: The console resides on the GB-1000 itself. This interface is access through a pc attached to the console port of the GB-1000. All administrative functions can be carried out from this interface. The disadvantages of this interface are that all configuration is done through a text based menu structure, and that you must be attached to the console port.

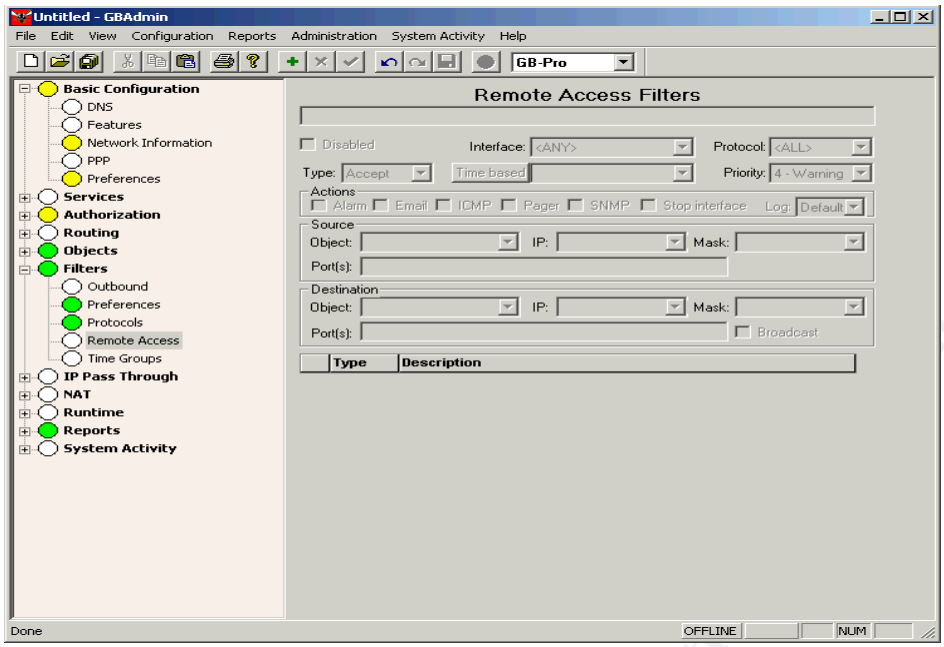
Web browser: With any standard web browser, you can access the built in administration web server of the GB-1000. Normally this server resides on port TCP/IP port 85, but can be changed to any port. The web browser interface allows remote administration of all GNAT Box features from any computer equipped with a web browser provided filters are in place at the GB-1000 to allow this access. The disadvantage to this method is that the as

of this writing, the GNAT Box web server does not support any form of encryption, it simply allows or disallows access based on preset user ids and passwords.

GB Admin: The GB Admin utility is included with all GNAT Box software. GBAdmin provides an administration interface that is remotely accessible and also encrypted. GB Admin accesses the GB-1000 unit on TCP/IP port 77 by default but can be configured to access on any port. Disadvantages of the GB Admin software are that it must be loaded on each machine you wish to administer the GB-1000 from and that the built in encryption appears to be proprietary to GNAT Box products.

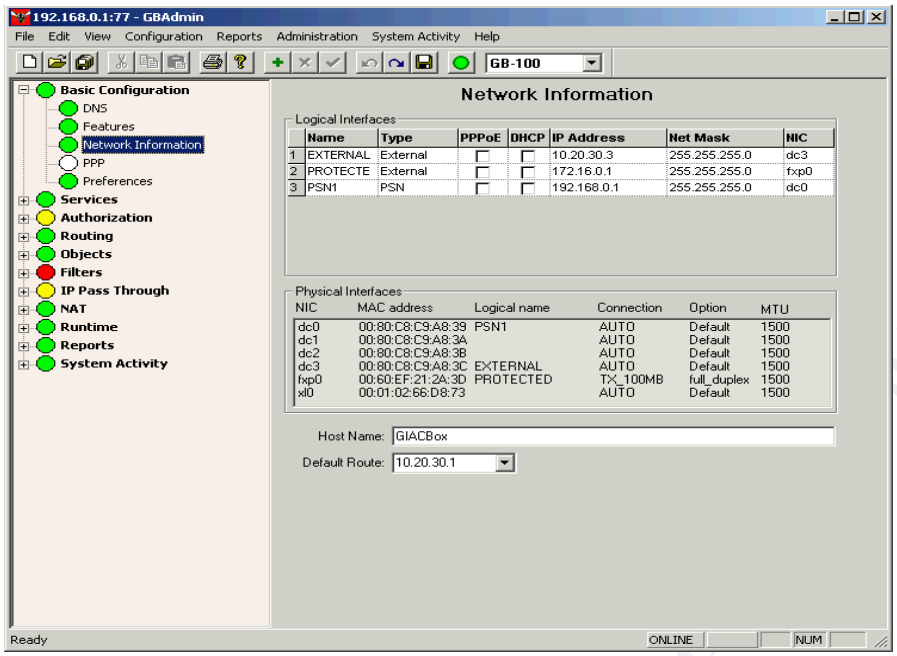
For this tutorial, I have chosen to use GB Admin. The following steps will go through the creation of a filter. For this example, I will be configuring a filter to allow access to a web server that resides on the PSN.

1. By default, GNAT Box opens with blank filters.



2. Before creating a filter, the network interfaces must be configured with IP addresses and you must define each interfaces function, EXT, Protected, or PSN.

Below I have configured my External network as interface one with the IP address of 10.20.30.3. The protected interface is number two with IP address 176.16.0.1. PSN1 is configured as interface three with IP address of 192.168.0.1.



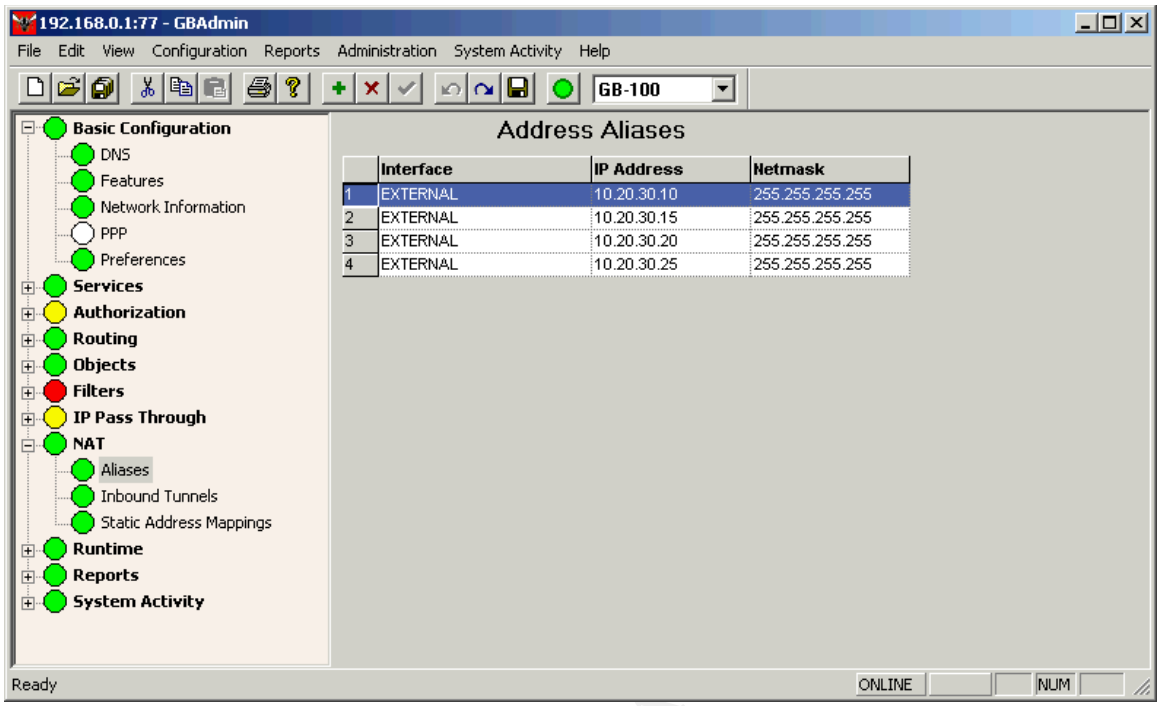
3. Next you must assign an IP alias to the GNAT Box interface. This alias will allow the web server to be accessed on a different IP address than the firewall. Clicking on the green "+" icon causes a blank entry to be added.

. otice the dropdown box option, this allows you to define what interface the IP alias will

reside on. For this web server example I have assigned the alias to the external interface as we wish to allow traffic from the Internet to reach the web server. I have also chosen the IP address of 10.20.30.10 (again this is a non-routable address that I am considering routable for use in this paper).

The following standard buttons are on each page of the GBAdmin client.

1. + icon: this icon inserts a new line at the bottom of the list.
2. x icon: deletes a line
3. check mark: Edits an exisiting row.
4. Arrow to the left: sets an item to default settings.
5. Arrow to the right: reloads a section from the GNAT Box live configuration. This is handy as the GNAT Box software times out administration connections after a period of inactivity.
6. Disk icon: Saves changes
7. Green circle: This icon logs the GBAdmin client on and off of the GB-1000,



4. Next a tunnel needs to be defined to allow traffic to pass from the external interface to the PSN interface where our server resides. Below is the tunnel creation screen

Each tunnel definition requires a protocol, From IP, from port, To IP, and a To Port. Additional options are “automatic accept filter” and “hide source” check boxes.

Protocol: Defines the protocol allowed through the tunnel, in this example TCP.

From IP: This defines the starting address of the tunnel, in this example our external alias of 10.20.30.10.

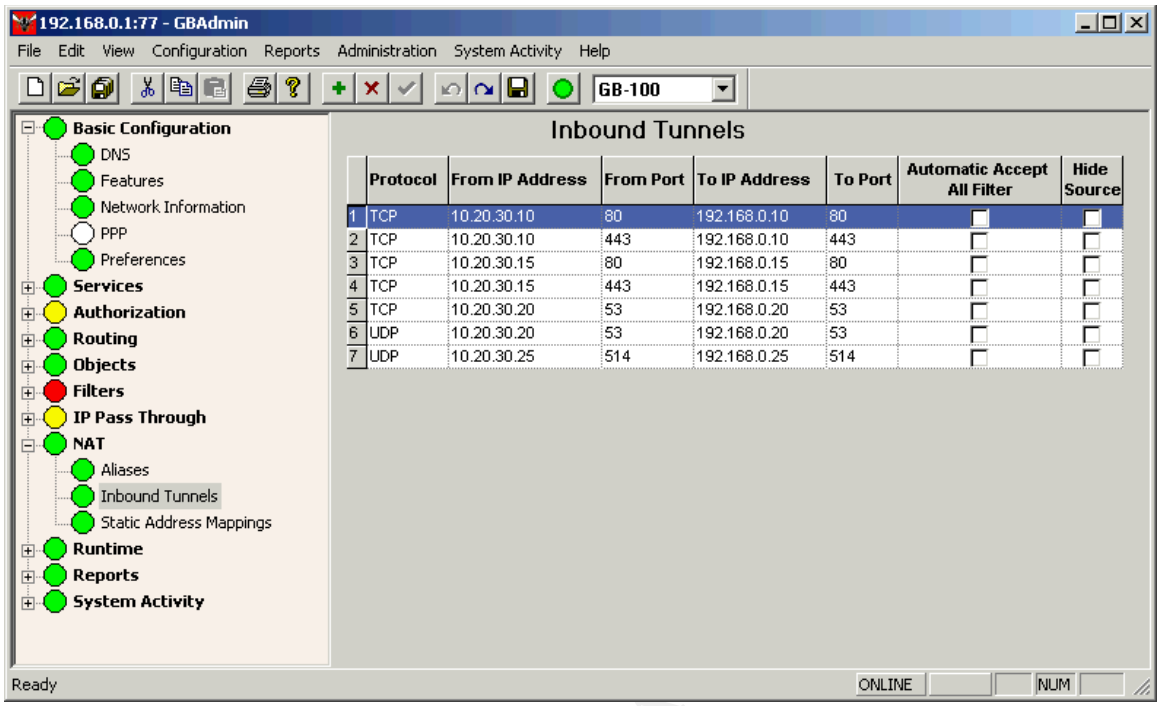
From port: This defines the source port of the tunnel. For this example, I have set it to port 80.

To IP: This defines where the traffic that enters the tunnel should be sent. For this example we are sending the traffic to the PSN address of our web server; IP address 192.168.0.10.

To Port: This defines the port where traffic entering our tunnel should be sent. This does not have to be set the same as the From Port, in this manner port redirection can be performed. For this example we will again be using the standard web port of 80.

Automatic Accept All Filter: This checkbox tells GNAT Box to automatically generate a filter to allow all traffic to this tunnel through to our To IP. This is useful when defining services that will be accessible to all IP addresses, such as our web server. I will not be using this option and instead will be defining the filter maunaly.

Hide Source: This option changes the source address of traffic entering the tunnel to the address assigned to NIC where the tunnel is defined.



4. Last, I will define the filter for the tunnel I have defined.

Here I again add a line by using the "+" icon. The first line of the filter definition is a description section, here I have entered "EXT IN: Allow TCP Access for HTTP".

Interface: Next I selected "external" for the interface. This sets to the filter to apply to the

external interface of the firewall. It should be noted that when a tunnel and corresponding filter is defined GNAT Box allows traffic from the start of the tunnel to the end point of the tunnel through the same definition and filter. As a result, we only need to define one access filter, to allow traffic to the external address.

Protocol: I am defining TCP only. This setting restricts traffic to the alias web server IP address 10.20.30.10. You could set the filter to "any", but if more than one tunnel were defined for port 80 you could potentially allow in unwanted traffic.

Type: This setting defines whether the filter is an accept or deny filter. In the case of this example it is set to accept.

Time based: This option will allow an administrator to set a filter to apply only to certain periods of time. For example 8 am to 5 pm. As I am setting up a publicly accessible web server I will leave it set to default, which allows the filter to always be active.

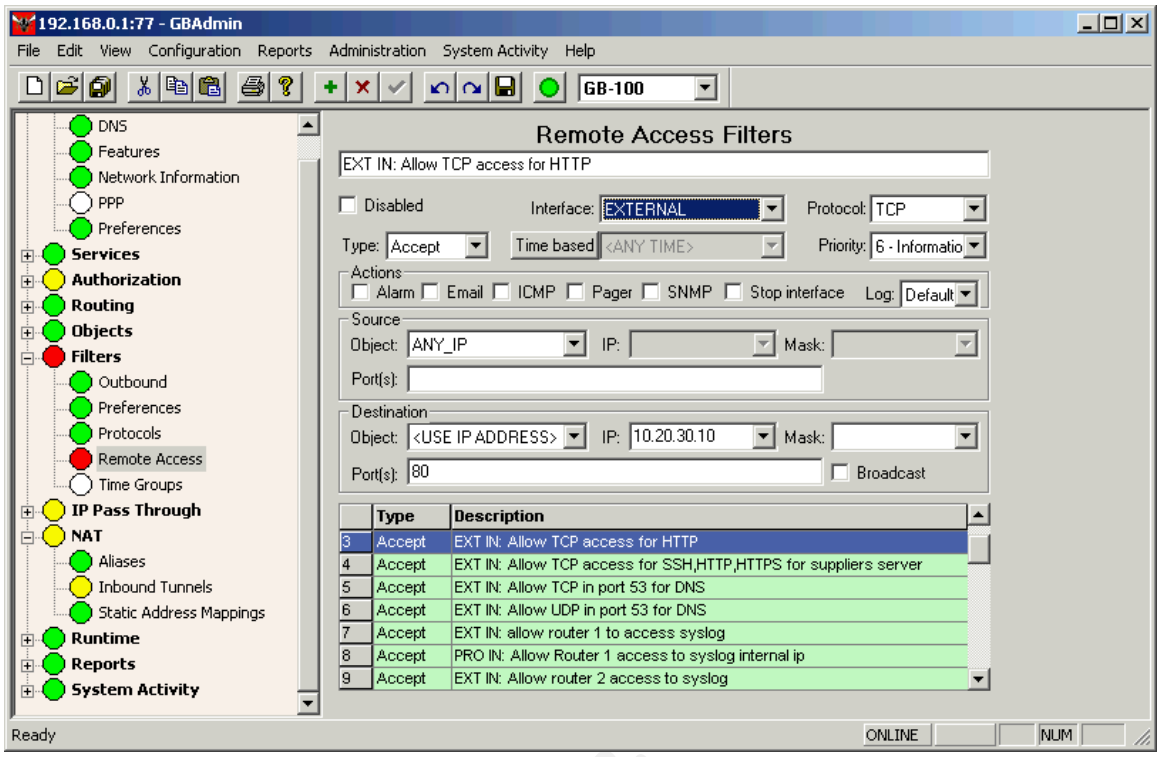
Priority: Priority sets the syslog logging priority of log data generated by the filter. For this example I will leave this setting at default.

Actions: This option tells what action to perform when this filter is matched. This is particularly useful if you have rules setup to block specific attacks. When the condition is met, GNAT Box can page you if a modem is attached, send SNMP traps, send an email, stop all traffic on the interface, or simply log. The log option can be set to "yes" to force

logging, “no”, or to “default”. When set to default the filter uses the default log setting configured globally for the firewall. I this example my default logging is set to log all rejected packets of any protocol. For this example, I will leave log set to default.

Source Object: This item determines what source traffic is allowed to originate from. For this example I am using the setting of “any Ip address” as this filter is to allow access to a public web server.

Destination: This item determines where to allow traffic matching this filter to end. As such I have defined the destination IP as the External alias of the web server. With this filter in place, access to the web server has been completed. Another filter on the PSN interface is not required as the GNAT Box uses a feature called “virtual cracks” to automatically allow reply traffic back to hosts accessing this tunnel.



GIAC Specific Filter setup

Requirements:

Allow customers to access web resources to make purchases.

Allow partners to connect via VPN to the GIAC Database server on the Internal network.

Allow authors to transmit new fortunes to GIAC.

External Interface

The external interface is the network card that connects to the ISP side of the GIAC network. It is used only to filter traffic entering the GIAC network and the PSN; outbound filtering will be accomplished on the PSN and PRO interfaces

EXT Policy:

To accomplish the above requirements, each server will have its address and service port aliased to the EXT interface on each GB-1000. In addition, filtering will be configured to restrict access only to allowed ports/services. To facilitate flow of this document a complete printout out of the GNAT Box configuration, including all filters is attached in Appendix 2

Aliases:

Server	**PSN IP**	**EXT IP**
E-commerce web server	192.168.0.10	10.20.30.10
Supplier's web server	192.168.0.15	10.20.30.15
DNS server	192.168.0.20	10.20.30.20
Syslog server	172.16.0.5 (INT NET)	10.20.30.25

Tunneled Ports:

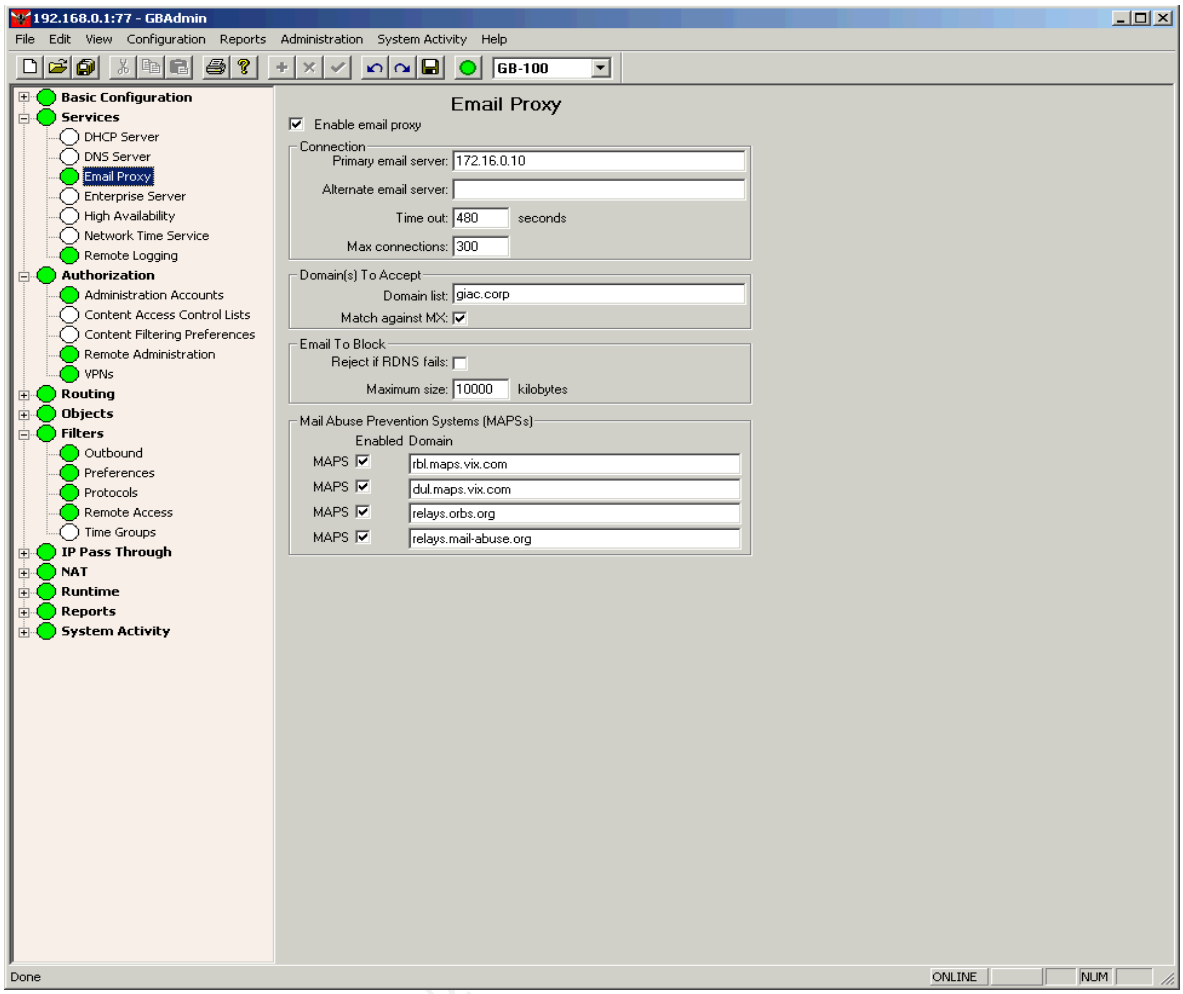
Server	PSN Port(s) Service	EXT Port
E-commerce web server	80T,443T HTTP, HTTPS	80T,443T
Supplier's web server	22T, 80T, 443T SSH, HTTP, HTTPS	22T, 80T, 443T
DNS server	53TU DNS	53T
Syslog server	514U	514U

The letters after the port numbers above are used to designate the TCP/IP protocol type. T = TCP, U = UDP.

Exchange email will be shown below as it is handled by the GB-1000 using a proxy.

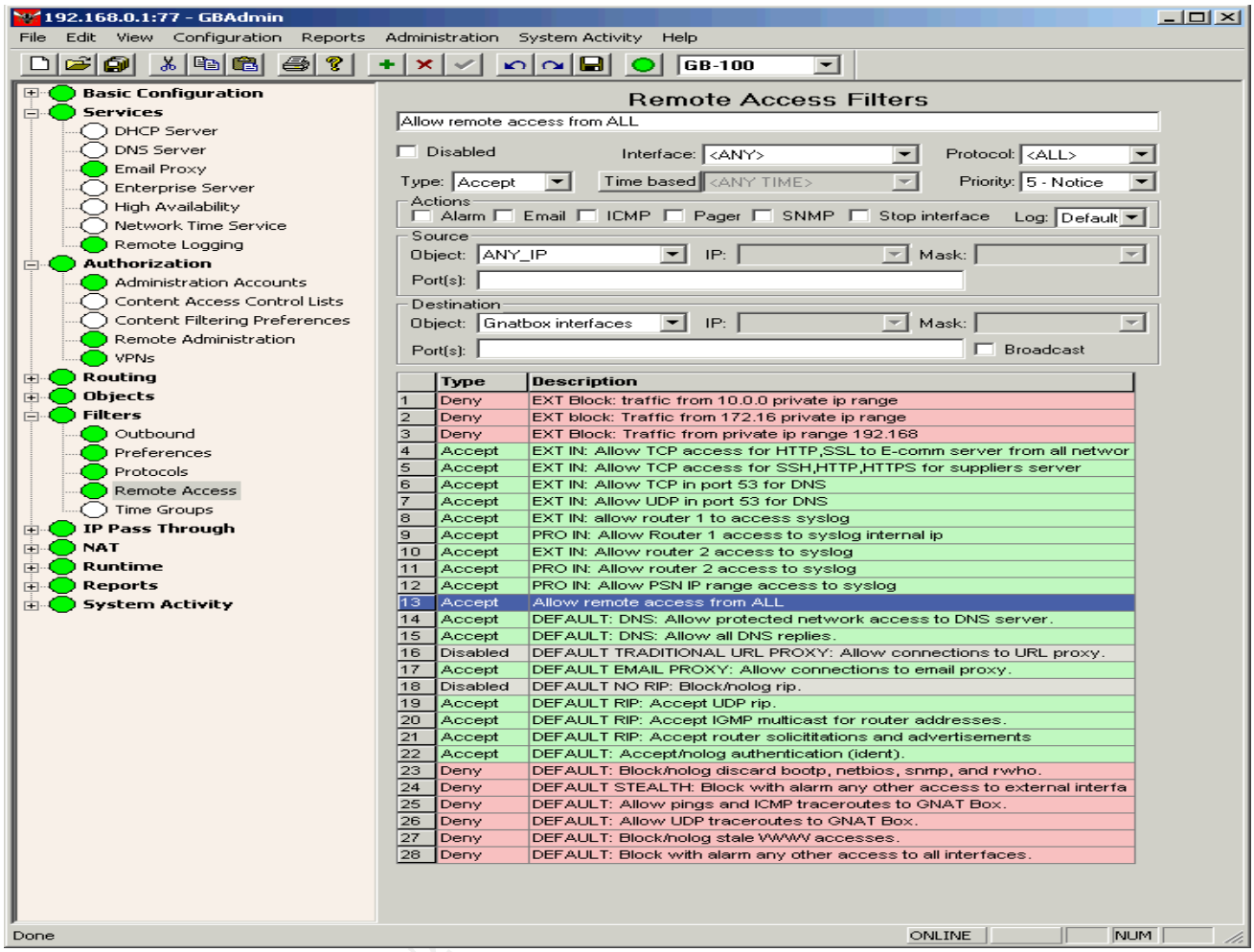
Exchange E-mail

The giac.corp email server will be accessed through the GB-1000 email proxy. The proxy automatically forwards smtp and pop3 traffic to the internal email server at address 172.16.0.10. Additionally, the email proxy also provides spam and other mail abuse prevention through the maps.org. The configuration screen for the proxy is shown below.



Filters

All inbound filters, or Remote Access filters as they are referred to by the GNATBox firewall, are configured from one central screen. Filters can apply to all interfaces, or to only one interface. They can be restricted to ranges of IP addresses or to a single IP address. In this section I will provide the details of the filters that apply only to the External interface. Note that filter 13 is highlighted, this is not a filter I would use in this configuration, it is in place temporarily to allow me to complete this assignment without building a separate network.



Filters 1 to 3: These filters deny (a stealth block) and log all private IP ranges attempting to access GIAC resources from the Internet.

Filter 4: Allows and logs HTTP and HTTPS traffic on ports 80 and 443 respectively to traverse the external interface to the ecommerce server on the PSN.

Filter 5: Allows and logs SSH, HTTP, and HTTPS on ports 22, 80, 443 to traverse the external interface to the suppliers server on the PSN.

Filters 6 and 7: Allows and logs DNS traffic on port 53 to traverse the external interface to the DNS server on the PSN.

Filters 8 and 10: Allows and logs syslog traffic from the border routers to the internal syslog server.

Filters 14 and 15: Allows and logs replies to Internet DNS servers.

Filter 17: Allows access by mail servers to the GNATBox email proxy.

PSN Interface

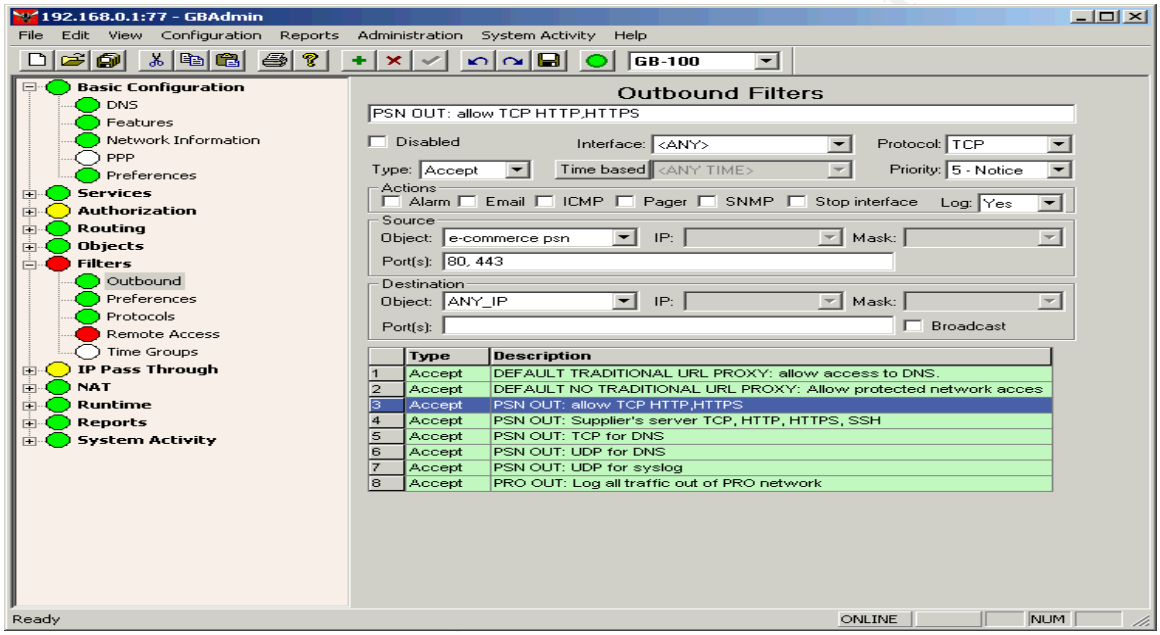
The PSN interface is the network card of the GB-1000 that connects to service network portion of the GIAC network. It is used to filter traffic entering and leaving the GIAC network.

PSN Filters

Remote access filters for this interface are handled by the EXT facility, in that any port tunneled from EXT to PSN are automatically allowed in. Outbound traffic is only allowed on ports listed in the above section for services. As a result I will only cover outbound filters in this section. By default the GNATBox allows all outbound traffic leaving the

PSN (outbound filter 3). In my configuration filter 3 will be disabled, I am leaving it on here to facilitate my home networks access to the gnatbox.

Outbound filters



In this screenshot, only filters 4,5,6,7 apply to the PSN interface. Even though the tunneling facility allows traffic in and out on the tunneled ports, I have created specific

outbound filters to facilitate better logging functionality.

Filter 4: Allows out and logs traffic from the ecommerce server on TCP ports 80, and 443 for HTTP and HTTPS to any IP address and port.

Filter 5: Allows traffic and logs traffic out from the supplier's server on TCP ports 22, 80, and 443 for SSH, HTTP, and HTTPS to any IP address and port.

Filter 6: Allows and logs traffic out from the external DNS server on TCP port 53 to any IP address and port.

Filter 7: Allows and logs traffic out from the external DNS server on UDP port 53 to any IP address and port.

Filter 8: Allows and logs traffic from PSN addresses to UDP port 514 of the internal syslog server.

Vulnerability: These services could be vulnerable, as numerous exploits exist for various web server products, and for SSH. However as Filters 1 through 7 would be the least vulnerable of the seven filters, as they allow traffic from the PSN to the Internet. The largest concern for services on the PSN is filter 8 as it allows traffic from the PSN network range to the syslog server on the internal service network. If a PSN server were to be compromised this rule could possibly used to compromise the internal network as it would allow communication with a machine on the internal network.

PRO Interface

The PRO interface is the network card of the GB-1000 that connects to internal or protected network portion of the GIAC network. It is used to filter traffic entering and leaving the GIAC internal network.

Pro Filters

Filters on the PRO interface are configured to perform both inbound and outbound filtering.

Inbound

Please refer to the filter screen capture shown in the above EXT section to see the PRO network Remote Access filters.

Filter 9 and 11: Allows and logs inbound syslog traffic from the border routers only to the internal syslog server on UDP port 514 only.

Filter 12: Allows and logs inbound traffic from the PSN servers to the internal syslog server on UDP port 514 only.

Vulnerability: These filters present the possibility to be exploited if either traffic were to be spoofed using the external router addresses or if a PSN server were to be compromised. If either were to happen, communication would be allowed to take place with the syslog server on the internal network. This would potentially allow further compromise.

Outbound

Please refer to the screen capture of outbound filters above and to Appendix 1 see the actual filters.

Filter 9: Allows access out and logs traffic from the internal network on ports 21, 22, 77, 80, and 443. This allows FTP, SSH, GBAdmin, HTTP, and HTTPS traffic from the internal network to the Internet or the PSN.

Vulnerability: This filter would allow outbound communication if an internal host were to be compromised. In addition, this filter would of course allow internal users to potentially download malicious code.

VPN Policy

The GB-1000 appliances will serve as GIAC's VPN servers in addition to performing the firewall function. The VPN policy will enforce control over GIAC partners entry into the GIAC internal network.

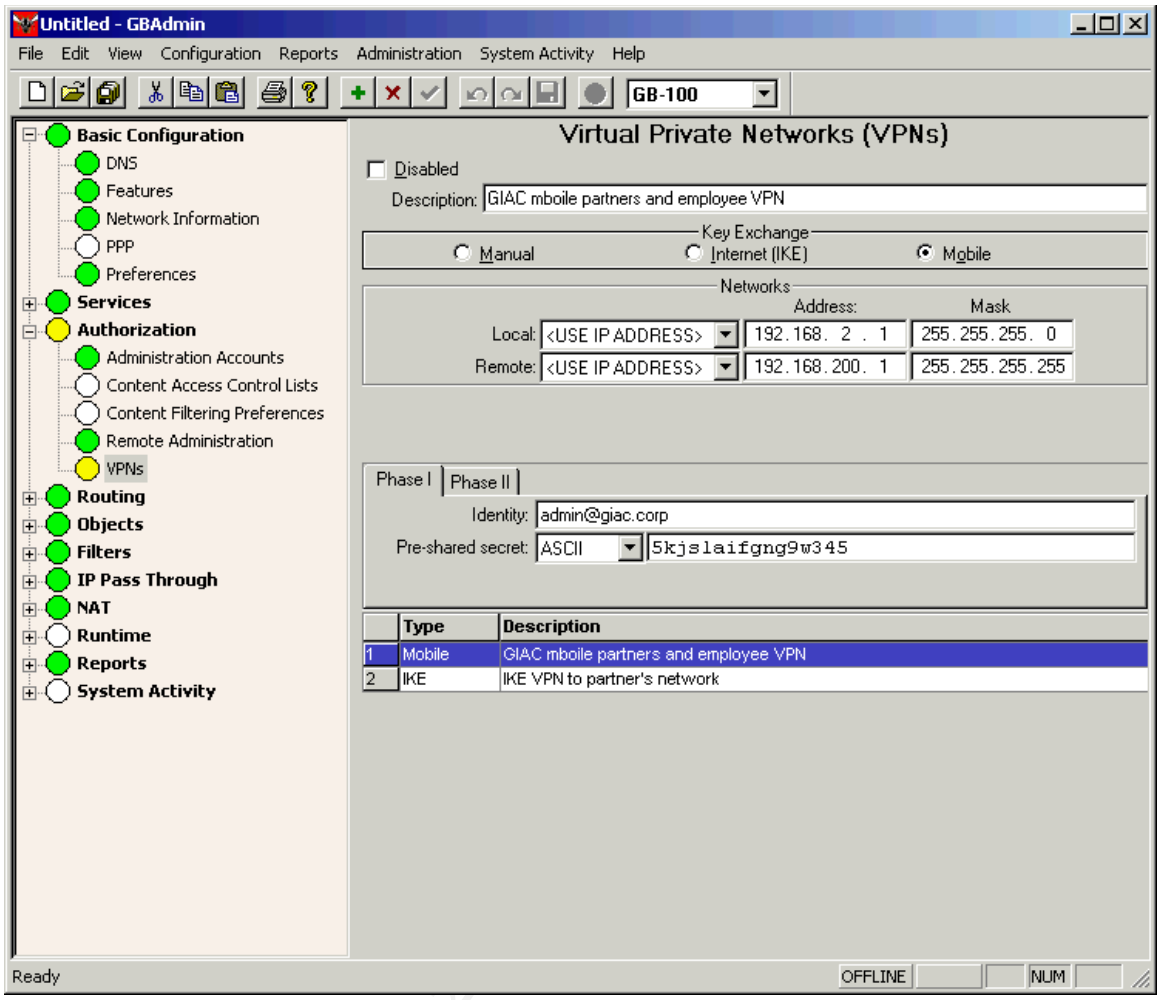
The VPN will assign a private IP address to each successful VPN connection made to the GIAC network. The ESP protocol will be utilized along with triple DES for mobile client encryption to encrypt the data in VPN traffic packets for partners and mobile employees as this is the highest encryption supported by the GNATBox VPN client software. An Internet Key Exchange (IKE) VPN will be established between the GIAC network and

our partner's network using Blowfish 448 bit encryption. Authentication Header (AH) protocol will not be used this is to allow better interoperability with networks that utilize NAT and to better facilitate mobile client connections. I have arbitrarily chosen the class c network 204.86.186.0/255.255.255.0 as the network of GIAC's partner company.

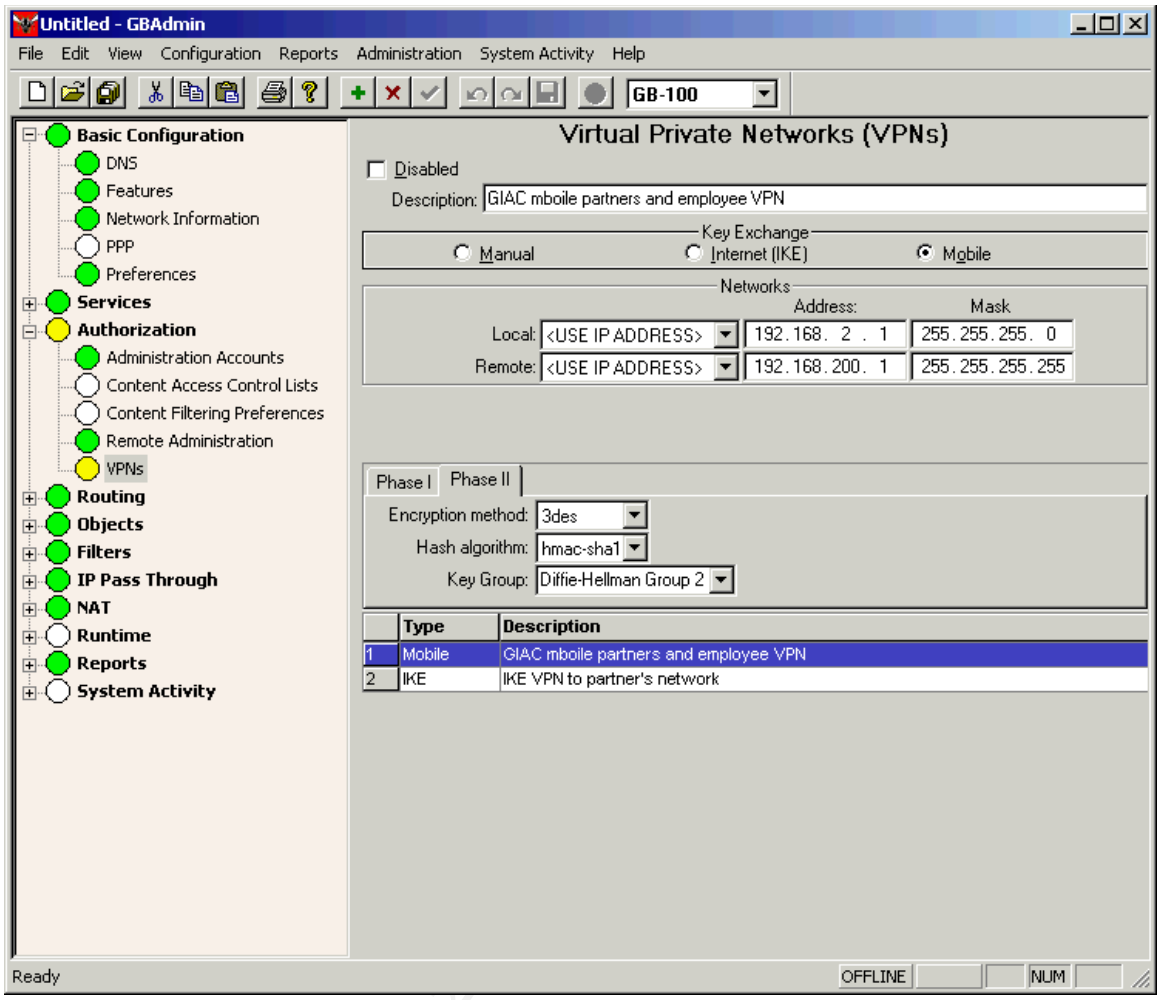
The VPN policy is shown below.

Mobile VPN

Phase 1: Validates the VPN tunnel from the mobile client and sets the parameters. During authentication of a mobile client tunnel, a pre-shared secret is exchanged to establish the VPN tunnel. Once established the client is assigned a virtual IP address in the network range 192.168.2.1/255.255.255.0, the GB-1000 performs routing of these packets automatically.



Phase 2: This phase sets the encryption level to 3DES, 192 bit encryption. Additionally, the VPN is set to allow only the Diffe-Hellman Group 2 hash algorithm for key exchange as it is the hash supported by the GNATBox VPN client.

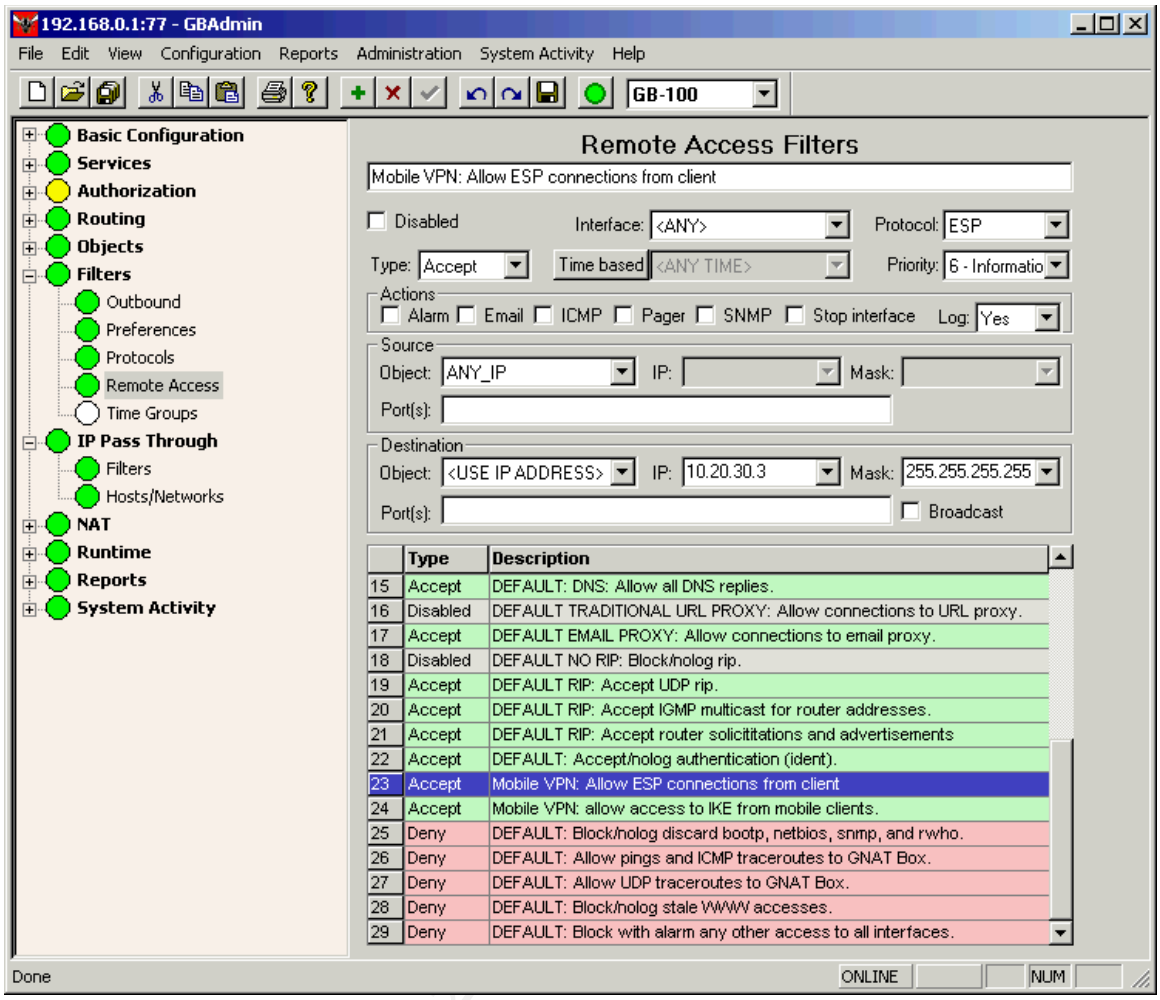


Mobile VPN filters

Filters are set as follows to allow the mobile VPN to operate.

Filter 23:Allow ESP connections from mobile client. ESP traffic from any IP address is accepted

Filter 24: Allow IKE for mobile connections. This filter allows traffic to UDP port 500 of the GB-1000 external interface IP address of 10.20.30.3 for Internet Key Exchange.

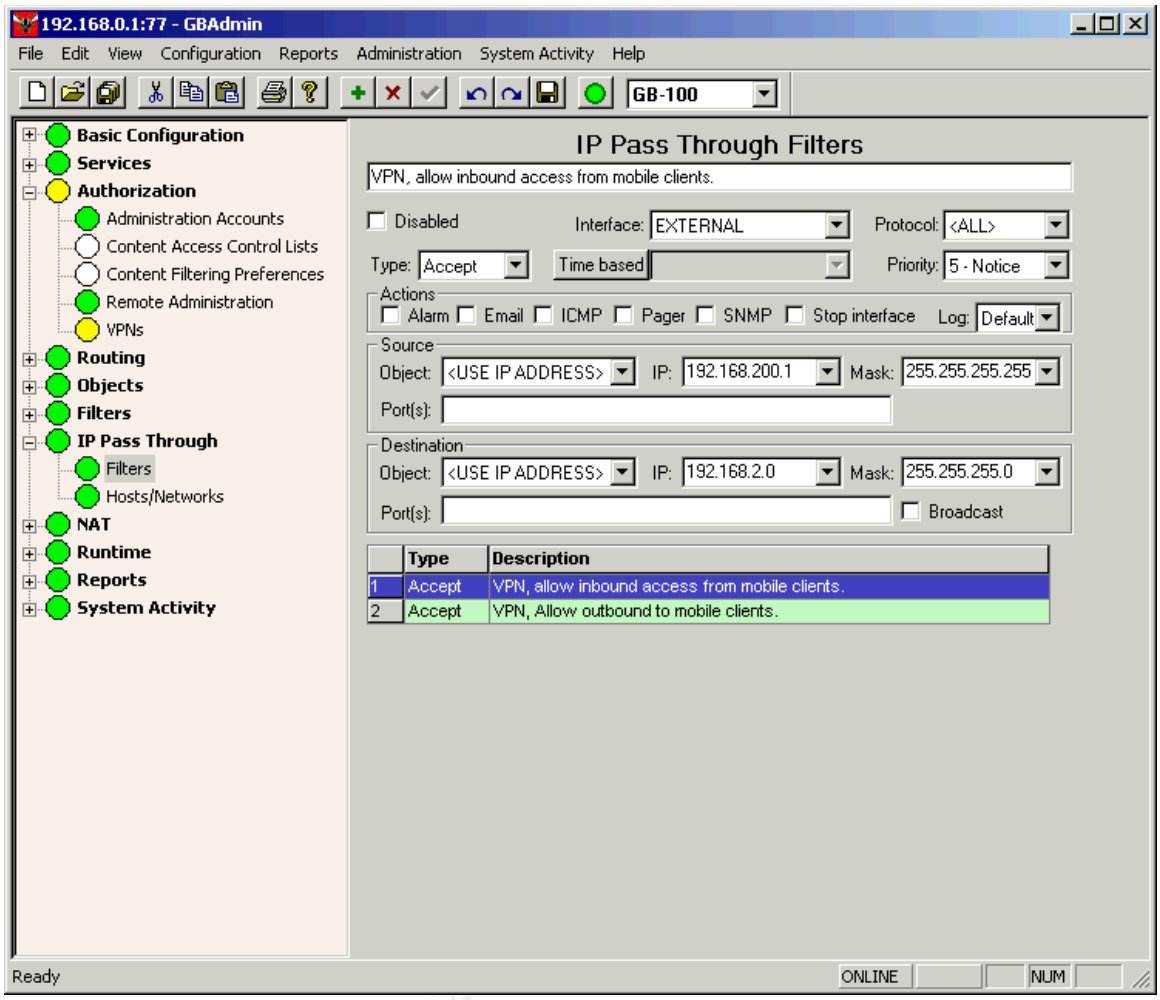


GNATBox IP pass through filters are configured to allow traffic from the protected network to go back through the VPN without being translated by NAT built into the GB-1000.

Pass through Filters

Filter 1: Allows all traffic from the mobile client IP addresses on the 192.168.200.1 network to enter the GB-1000 firewall.

Filter 2: Allows traffic to return out to the mobile clients without experiencing translation by the firewall software.

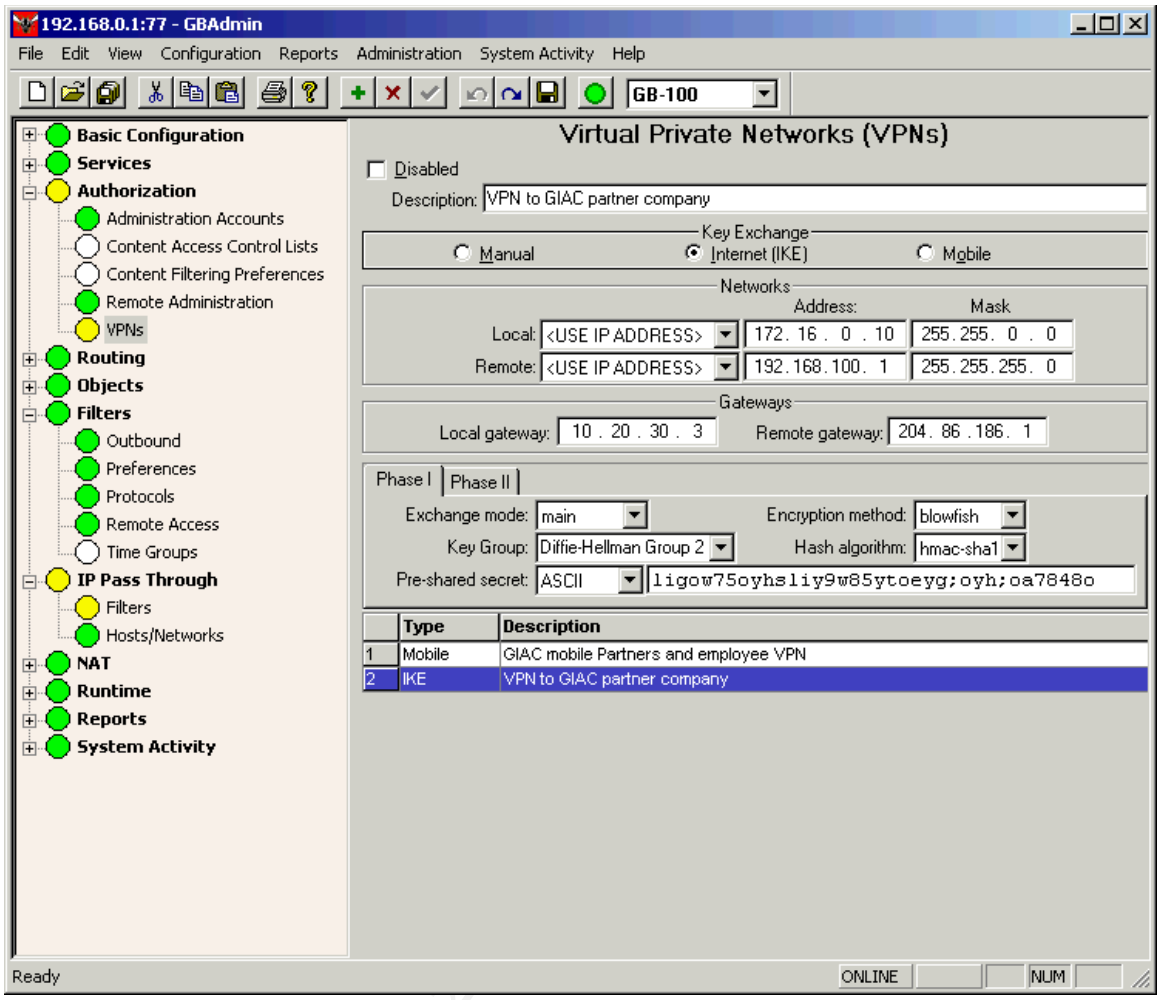


Partners VPN

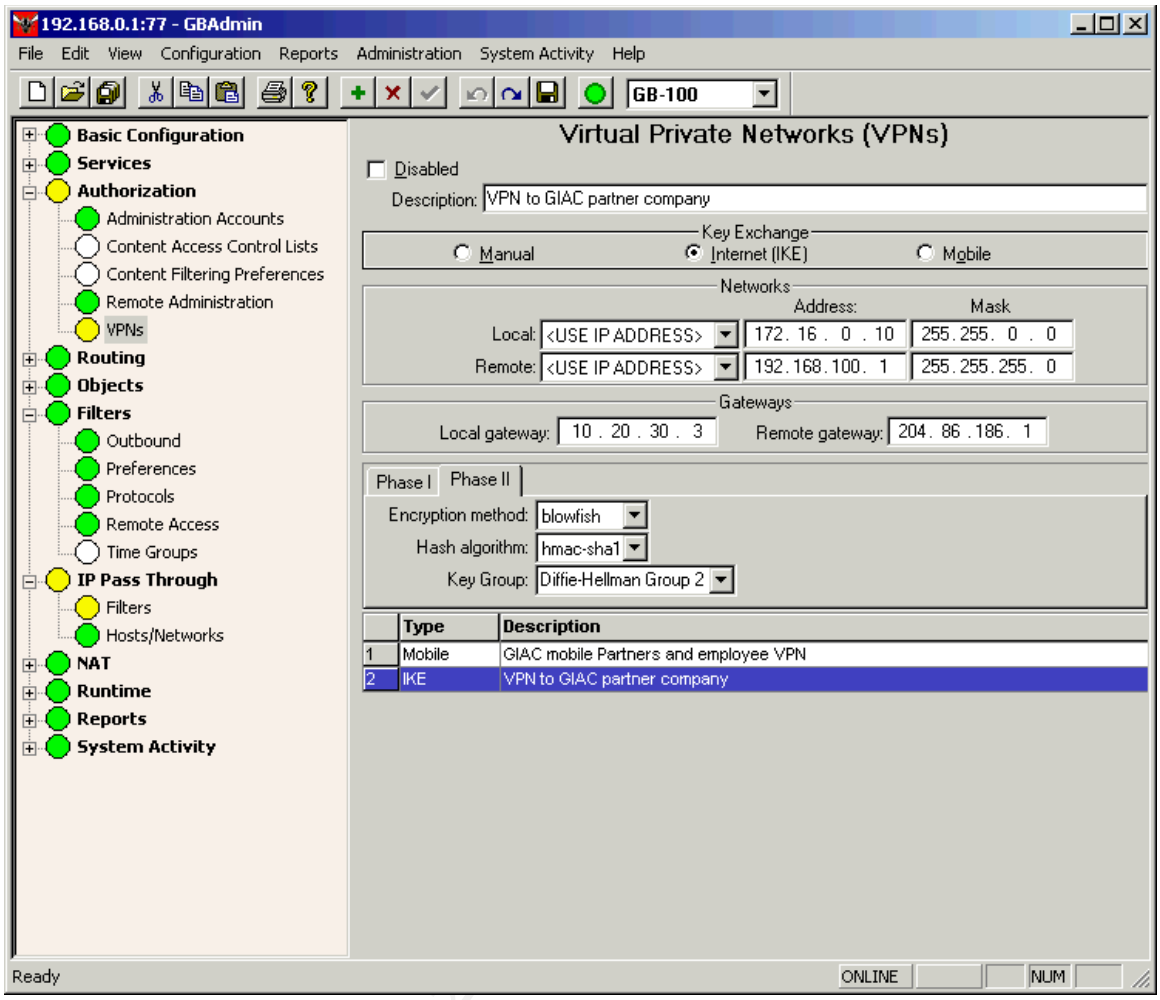
The partners VPN uses blowfish encryption for phases one and two of the VPN. IT also uses IKE to create dynamic encryption keys during phase two. This VPN is setup between the GIAC network and the Partner company network. The partners network will only be allowed to access the corporate database server on the Internal service network on ports 7000 through 7030 as defined in section one.

Note: in the screen capture below the VPN section is shown as yellow instead of green, this is due to the non-valid IP addresses that I have chosen to use in this project. Due to my equipment limitations, I am showing the setup of the partner gateway side of the VPN on the same firewall as the GIAC gateway.

Phase 1: Validates the VPN tunnel from the partner company network and sets the parameters. During authentication of a partner network tunnel, a pre-shared secret is exchanged to establish the VPN tunnel. Once established the client is assigned a virtual IP address in the network range 192.168.2.1/255.255.255.0, the GB-1000 performs routing of these packets automatically.



Phase 2: This phase sets the encryption level to Blowfish, 448 bit encryption. Additionally, the VPN is set to allow only the Diffe-Hellman Group 2 hash algorithm for key exchange, this is simply for simplicity as we are already using this algorithm on the client VPN.



Remote Access Filters

Filters 25 through 28 allow VPN traffic to take place between GIAC and the partner network.

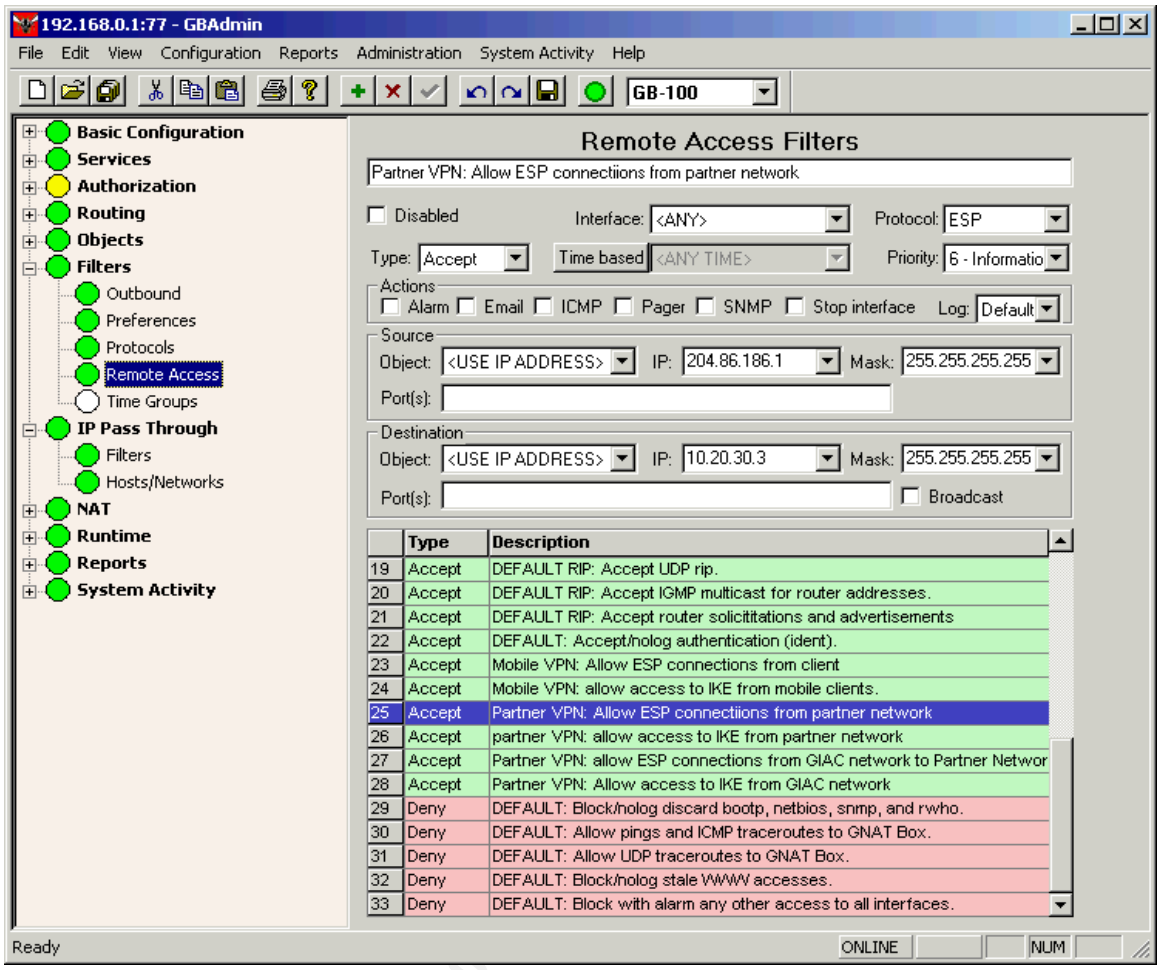
Filter 25: Allows ESP traffic from the partner gateway at 204.86.186.1 to the GIAC GB-1000 at 10.20.30.3.

Filter 26: Allows IKE to take place on UDP port 500 between the partner gateway at 204.86.186.1 and the GIAC GB-1000 at 10.20.30.3

Filters 27 and 28 would be installed on the partner VPN gateway.

Filter 27: Allows the GIAC network to establish VPN connections and communicate with the partner gateway using ESP.

Filter 28: Allows the GIAC network to initiate IKE with the partner gateway on UDP port 500.



Pass through Filters

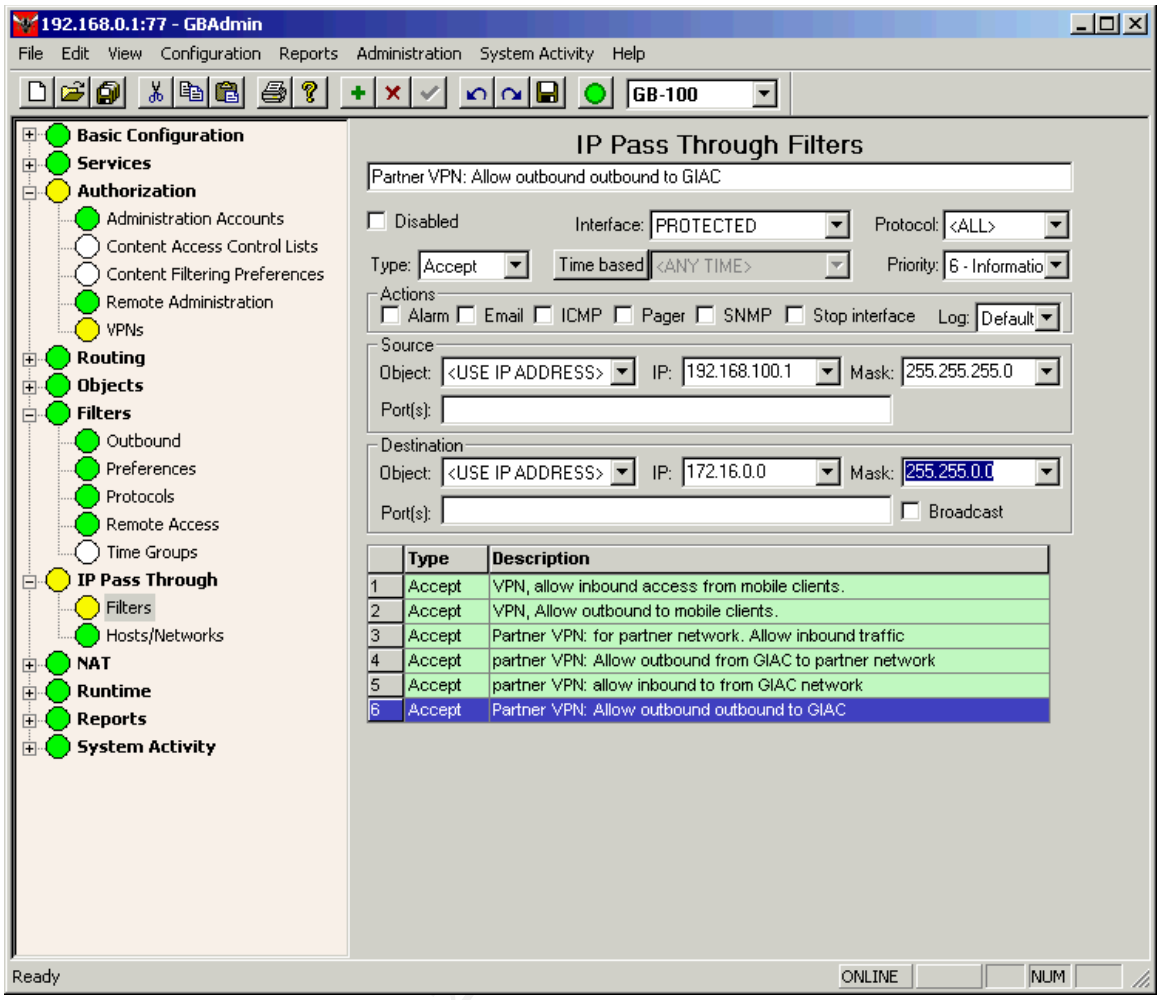
Filter 3: Allows inbound traffic from the partner network on IP addresses 192.168.100.1/255.255.255.0 to enter the GB-1000 firewall.

Filter 4: Allows traffic to return out to the partner network without experiencing translation by the firewall software.

Filters 5 and 6 would be installed on the partner VPN gateway.

Filter 5: Allows inbound traffic from the GIAC internal network to the partners network on TCP ports 7000-7030

Filter 6: Allows out bound traffic from the internal partner network back to the GIAC network on ports 7000-7030



Vulnerability: The most significant risk to the GIAC network from the VPN filters would be based on the compromise of a mobile client machine or the compromise of a machine on our partner's network. In the case of the mobile client compromise, the attacker would have almost complete access to the GIAC network. In the case of compromise of a host on the partner's network, the internal GIAC database would be compromised at a minimum to access to confidential GIAC data and at worst the attacker could possibly damage the database.

High Availability

The GB-1000 units are configured in what Global Technology Associates calls a H_2O configuration. The GB-1000 units are configured as a single virtual firewall. In this manner, one unit acts as the master (GB-1000/10.20.30.3) and a second unit (GB-1000/10.20.30.4) acts as the slave this is configured through a priority structure with master being a higher priority. The GNAT Box firewalls constantly communicate using HA UDP/77 and IGMP on both the external and internal interfaces. The master unit continually broadcasts to the slave unit to let the slave know that it is operating, if this broadcast ever ceases on either interface, the slave takes over. During the swap-over, connection state information is not exchanged and as a result current connections are not maintained. When the master begins broadcasting again, the slave receives HA traffic and compares the embed priority of the received traffic to its own priority, if the priority of the received traffic is higher than its own priority a swap-over occurs to the unit with the

higher priority. In this way, the GB-1000 units operate under one virtual IP address and the changes are relatively seamless to hosts traversing the firewall.

The following rules have been put in place to allow HA traffic on the external and internal interfaces.

Filter 28: Allows UDP traffic from Firewall 2 to Firewall 1. From any source port to port 77 of the external address of firewall 1.

Filter 29: Allows IGMP from firewall 2 to firewall 1. From

Rules Test

To test the functionality of the rules, I have chosen remote access filters 4, 5, and 8.

Filter 4 would be tested by attempting to access HTTP, and HTTPS from a host on the Internet, this would demonstrate allowed traffic to the ecommerce server. To verify denied ports, an attempt to connect to telnet or various other non-allowed services could be made.

Filter 5 would be similar to filter 4 with the addition of a test to verify that SSH operates correctly. The test for denied traffic would be the same as filter 4.

Filter 8, allows syslog traffic from the PSN servers to the internal syslog server. This functionality could be verified at the syslog server after the verification of filters 4 and 5. If

the allowed access has happened, the syslog server should show a log entry for it.

A test of the high availability function could be accomplished by disconnecting the primary firewall and verifying that traffic is still able to leave the network. Once the test firewall is returned to service, the remaining firewall could be disconnected. This test would verify that each firewall is able to take over for the other.

Assignment 3: Audit

The GIAC audit will be conducted in three phases; the planning phase, test phase, and evaluation phase. The three phases will be conducted by GIAC network support staff and outside contractors. The planning phase will be conducted during normal business hours. The Test phase will be conducted after normal business hours. The evaluation phase will be conducted during normal business hours.

Planning

Planning will consist of an evaluation of the physical and logical network design to ensure that it matches the GIAC design diagrams. The auditors will also review the GIAC security policy of allowed services as a baseline for testing. This portion will be conducted during normal business hours.

The following costs are associated with the planning phase:

Contractors: 8 hours onsite analysis of the diagrams and planning the tests. Cost of $150.00 per hour.

Network Support staff: 8 hours of analysis of diagrams and test planning. Cost of $75.00 per hour.

When planning is finished the GIAC plan will be presented to management to receive by in, as the tests performed in the audit could cause disruption of network services. In addition the plan will also be brought to GIAC's ISP to ensure disruptions of the ISP network are not caused.

Test

The tests of the GIAC firewall would be conducted on a weekend to avoid interruption of business critical applications and services. As with any test of a system, a particular function could inadvertently be taken offline. To eliminate any internal mis-configurations of the firewall, the audit shall be performed from a host residing on the Internet and additionally from a host on the PSN.

To assess the GIAC firewall, the tool NmapNT will be used. NmapNT is the Windows port of the UNIX Nmap port scanning and assessment tool. NMap supports scanning of host machines using non standard packet types to discover not only what ports are open, but also what operating system the target is running. TCP SYN stealth and UDP ports scans will be used with the OS fingerprinting option enabled.

It is estimated that this phase will require 8 hours of work from GIAC network support staff at a rate of $75 per hour.

PSN Scans

Below is the output from the Nmap TCP SYN stealth scan run from inside the PSN.

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security (http://www.eEye.com)

based on nmap by yodor@insecure.org (www.insecure.org/nmap/)

Interesting ports on (192.168.0.1):

(All 65535 ports scanned but not shown below are in state: filtered)

Port	State	Service
25/tcp	open	smtp
77/tcp	open	priv-rje
85/tcp	open	mit-ml-dev
113/tcp	open	auth

TCP Sequence Prediction: Class=random positive increments

Difficulty=22898 (Worthy challenge)

Remote OS guesses: Acorn RiscOS 3.7 using AcornNet TCP/IP stack, Borderware 6.0.2 firewall, Gnat Box Light 3.0.3 (from the inside interface), FreeBSD 2.2.1 – 3.2, Juniper Router running JUNOS, Mirapoint M1000 (OS v 1.0.0), Cabletron Systems SSR 8000 System Software, Version 3.1.B.16

Nmap run completed – 1 IP address (1 host up) scanned in 288 seconds

From this scan we can see that TCP ports 25, 77, 85, and 113 are listed as open.

Port 25: Is the SMTP port utilized by the GNATBox email proxy, which is by default allowed on all interfaces.

Port 77: Is used by the GNATBox encrypted remote administration client.

Port 85: Is the GNATBox administration webserver, this function duplicates the admin

client but through a web browser.

Port 113: Is used by the GNATBox to provide IdentD protocol authentication to devices that are being translated using NAT.

The scan also guessed that our firewall is running one of eight operating systems, one of which is listed as GNATBox light, the free version of GNATBox.

Below is a UDP scan of the same interface.

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security (http://www.eEye.com)

based on nmap by yodor@insecure.org (www.insecure.org/nmap/)

Warning: No TCP ports found open on this machine, OS detection will be MUCH less reliable

All 65535 scanned ports on (192.168.0.1) are: filtered

Too many fingerprints match this host for me to give an accurate OS guess

Nmap run completed – 1 IP address (1 host up) scanned in 13139 seconds

EXT Interface Scans

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security (http://www.eEye.com)

based on nmap by yodor@insecure.org (www.insecure.org/nmap/)

Interesting ports on (192.168.0.1):

(the 65531 ports scanned but not shown are in state: filtered)

Port	State	Service
25/tcp	open	smtp
77/tcp	open	priv-rje
85/tcp	open	mit-ml-dev
113/tcp	open	auth

This scan is of the IP address 10.20.30.3, the external NIC of the GB-1000 unit. This scan used the SYN stealth option of NMap. The scan shows identical results of the PSN NIC.

UDP Scan

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security (http://www.eEye.com)

based on nmap by yodor@insecure.org (www.insecure.org/nmap/)

Warning: No TCP ports found open on this machine, OS detection will be MUCH less reliable

All 65535 scanned ports on (10.20.30.3) are: filtered

Too many fingerprints match this host for me to give an accurate OS guess

Nmap run completed – 1 IP address (1 host up) scanned in 13139 seconds

Evaluation

Evaluation will consist of both the Auditors and GIAC network support staff analyzing the NmapNT security scan results, comparing them to the GIAC security policy, and providing recommendations for improvements.

It is estimated the evaluation will take 6 hours at a cost $150 per hour for the contract auditors and $75 per hour for GIAC network staff.

Audit Results

Based on the NMap scans, the GIAC security policy is in place and providing the desired security. The firewall is passing traffic as designated by the filter policy, and is not answering to port scans. With only the abnormal results being open ports 77, and 85 which are used for the GNAT Box remote administration tools.

Recommendations

After this audit, it can be determined that filtering on the GIAC PSN network should be improved. Specifically, ports 25,77, and 85 have no reason to open. Having PSN access to the GNATBox administration functions could be a security risk if any of the hosts on the PSN were to be compromised. The fact that our firewall can be identified within eight operating systems, could make it easier for a skilled hacker to penetrate our system. The random TCP sequence generation, judge to be a "worthy challenge" by NMap would hopefully mitigate some of the risk of having a reasonably easy to guess firewall operating system. The UDP scan shows all ports filtered and NMap is unable to guess the operating system.

After auditing the EXT interface, again the results are the same as the PSN interface. As such, it may be wise to also add explicit filters to deny access to the GB-1000 admin interface ports.

The only real concern is the unexpected ports open for the administration interface. After this scan it may be wise for GIAC to put explicit filters in place to block the admin ports on the PSN interface.

Based on the analysis of the GIAC design diagrams, the following changes are recommended.

1. Install a proxy server to limit access on the GIAC webservers to only allowed HTML page names and directories, this will prevent exploits such as code red which rely on the input of Unicode into the HTTP GET request.
2. Provide for more secure authentication at the start of mobile client VPN tunnels with a smart card or biometric authentication system.

Section 4: Design under Fire

For this section I have chosen to evaluate the design proposed in Tim Daly's Practical, available at www.sans.org/y2k/practical/Tim_Daly_GCFW.zip. Mr. Daly's design is shown below.

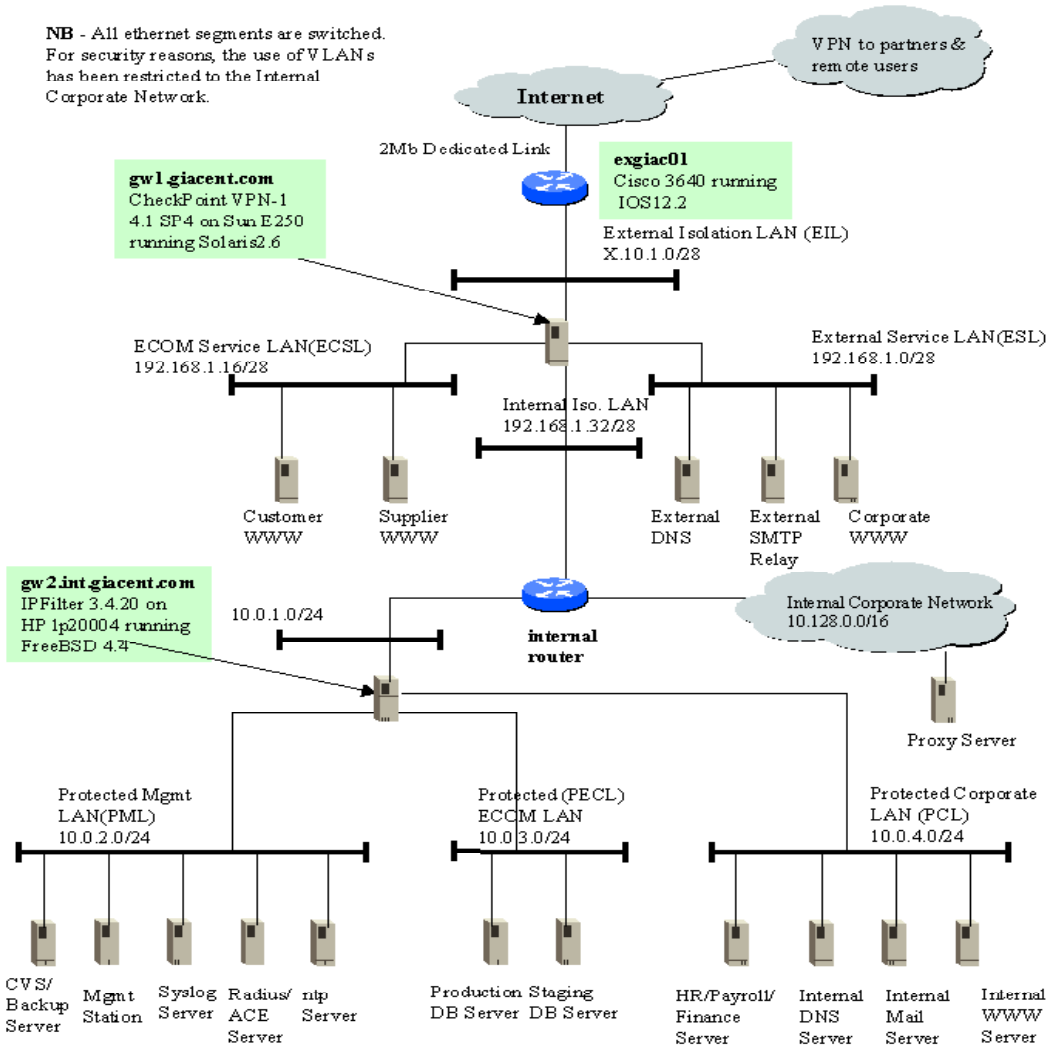


Figure 1

Mr. Daly lists his perimeter firewall as CheckPoint VPN-1 v4.1 SP4 running on Solaris v2.6. aAs such, my attacks will focus on Firewall-1.

Attacks

Attack 1: IP Fragment-Driven Denial of Service Vulnerability

Description: A stream of IP fragments can be used to consume all CPU cycles on the Check Point Firewall unit. Listed on Check Point's Support site at http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

Check Point states in this document that this vulnerability will be fixed in Service Pack 6 hot fix, as of this writing only service pack 5 is available.

Attack 2: Improper stderr Handling for RSH/REXEC

Description: "Specially formatted RSH/REXEC connection requests could cause an unauthorized connection to be opened from an external RSH/REXEC server to an internal (protected) RSH/REXEC client. This applied only if the FireWall-1 administrator specifically enabled the RSH/REXEC setting in the Properties window." Found on Check Points site at http://www.checkpoint.com/techsupport/alerts/list_vun.html#Improper_stderr

Attack 3: RDP Communication Vulnerability

"Description: Check Point has become aware of a condition with RDP Protocol in

VPN-1/ FireWall-1 4.1 and Next Generation (NG) that may affect system stability. If the error occurs on a 4.1 module, certain management functions, such as logging and administrator communications, will halt. On NG modules, encryption key processing may be briefly interrupted. At no point is security compromised, and the firewall continues to enforce the security policy and allows appropriate traffic. No unauthorized access, information leakage or breach of security occurs. Check Point knows of no organizations that have had systems affected by this issue. However, Check Point recommends the hot fix below be immediately installed. QinetiQ SHC Research reported this issue to us." Information on this vulnerability was found at http://www.checkpoint.com/techsupport/alerts/rdp_comms.html

Actual Attack: The attack will focus on the RDP Communication vulnerability.

As shown below by rule two, the Firewall is set to allow RDP traffic in from any address.

This vulnerability would allow a Denial of service attack to take place against the Firewall-1 unit, by halting logging and administrator functions. This would also allow other attacks to take place unnoticed. This attack could be accomplished by crafting RDP packets and sending them at the firewall by using a tool such as Libnet, available at http://www.packetfactory.net/Projects/Libnet/. Proof of concept code for a previous RDP exploit was constructed by the German security web site www.inside-security.de. The exploit that this code was meant to prove, allowed packets to be sent through a Firewall-1

unit and targeted at hosts behind the firewall. This same proof of concept code could easily be run against Firewall-1 to exploit this new RDP communication vulnerability.

The code available from Inside-security, works by crafting a RDP header with arbitrary RDP commands and adding it to a UDP packet. This code has the additional benefit of being able to spoof the source address of the sent packets. The checkpoint RDP protocol operates as a subset of UDP on port 259. The information at inside-security shows the RDP packet structure as follows:

```
************************
*       IP Header              *
************************
*       UDP Header             *
************************
*        RDP Header            *
************************
*        Payload                *
************************
```

The RDP header consists of the RDP Magic number and the RDP command. Inside Security states, that "the RDP magic number has turned out to be irrelevant", meaning that to either RDP exploit the RDP number does not affect whether or not the exploit can take place. Inside security also states that the "RDP commands that will be permitted to pass the firewall follow straight from the INSPECT include file $FWDIR/crypt.def."

```
************************
*  RDP Magic Number       *
************************
*  RDP Command            *
************************
```

To prevent this attack, an interim solution would be to not allow RDP traffic to the firewall from Internet hosts. I specify Internet, as not allowing RDP from the Internal network would prevent remote administration of Firewall-1 from inside the protected network. As a patch to correct this vulnerability is not currently available, if RDP were required from the Internet such as for Check Point's secure remote VPN client, the only way to reduce this eventuality would be to specify VPN access by IP address. If remote VPN clients use dial up Internet access, the only thing that could be done is to review logs and check for periods where the log shows no traffic and setup and active monitoring program using intrusion detection to attempt to monitor traffic entering the protected or PSN networks. Another solution would be to install another brand of firewall before the checkpoint unit to monitor traffic in the event Firewall-1 logging is disabled by this exploit. I have not run and tested this exploit as I do not have a Firewall-1 unit available in my test environment.

DDoS Attack

Fifty compromised machines on DSL or cable modem connections could be used to disastrous affect to launch a Distributed Denial of Service attack against the Firewall-1 unit. Utilizing a tool such as the Tribe Flood Network, or by compiling the tool I mentioned in the previous section, compromised machines could generate and send to the firewall malformed IP fragments or utilize the RDP Communication vulnerability. Either would deny service to a degree. The IP fragment vulnerability, would effectively take

down GIAC's internet connection, while the RDP communication vulnerability could be used to mask other attacks.

Execution of the attack:

First download and install Tribal Flood Network 2000 (TFN2K). I downloaded this tool from www.paketstormsecurity.org. TFN2K operates in a client/server configuration, with one exception, the TFN2K client controls the server, the server is the machine that actually generates the attack. In this attack, the client and server reside on the same machine. A screen capture of the TFN2K options output is below.

```
[Root@evilcomputer /]# ./tfn
usage: ./tfn <options>
[-p protocol]    Protocol for server communication. Can be ICMP, UDP or TCP. Uses a random
                 protocol as a default
[-P protocol]    Send out n bogus requests for each real one to decoy targets
[-S host/ip]     Specify your source IP. Randomly spoofed by default, you will need to use
                 your real IP if you are behind spoof-filtering routers
[-f hostlist]    Filename containing a list of hosts with TFN servers to contact
[-h hostname]    TO contact only a single host running a TFN server
[-I targetstring]Contains options/targets separated by '@', see below
[-p port]        A TCP destination port that can be specified for syn floods
<-c command ID>  0 - Halt all current floods on server(s) immediately
                 1 Change IP antispoof- level (evade rfc2267 filtering)
                 2 Change packet size, usage: -i <packet size in bytes>
                 3 Bind root shell to a port, usage -i <remote port>
                 4 UDP flood, usage: -i victim@victim2@victum3
                 5 TCP/SYN flood, usage: -i victim@…
                 7 ICMP/SMURF flood, usage: -i victim@…
                 8 MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@…
                 9 TARGA3 flood (IP stack penetration), usage: -i victim@…..
                 10 Blindly execute remote shell command, usage -i command
```

The actual command is as follows: ./tfn –h 127.0.0.1 –c8 –i www.giac.com

-f serverlist :tells TFN2K to contact all the servers listed in the file "serverlist"
-h 127.0.0.1 :tells TFN2k to additionally contact the server on the local machine
-c8 :tells TFN2K to send a mixed attack of UDP,TCP, and ICMP traffic
-i :tells TFN2K to the machine to attack.

If the true goal of the attack is to deny service, I would launch the attack during the middle of the business day. The reason for this is that during the middle of the business day, there is more than likely going to be business critical traffic taking place. If our attack

were truly meant to damage GIAC and deny use of their systems it would be most effective to cause disruptions during the most critical time periods. In addition with customers and partners of GIAC residing overseas, the attacks could also be launched during off hours to disrupt transactions by foreign customers.

Compromised Host

This attack will be carried out against the web server located on the E-commerce Service LAN. As shown below in rule 9, Mr. Daly is allowing access on ports 80, and 443 to the e-commerce web server located on the E-Commerce service LAN.

This rule would allow scans of the web server to take place on ports 80, and 443. These scans could be utilized to determine what operating system and web server software this server is running.

The first task of this exploit is to determine what web server software and operating system are being used. The following scans and tools would aid in this discover.

First: A traceroute and DNS lookup utility would be run to determine the public IP address of the server. Next a very basic attempt to discover the web server and operating system being run could be accomplished by using the "What's that site running?" tool available at www.netcraft.com. The potential problem with this

method is that the web server could possibly be set to send false version information.

Second: Nmap scans would be run with the following command lines.

Nmap –sS –O -p 80 <webserver IP address>

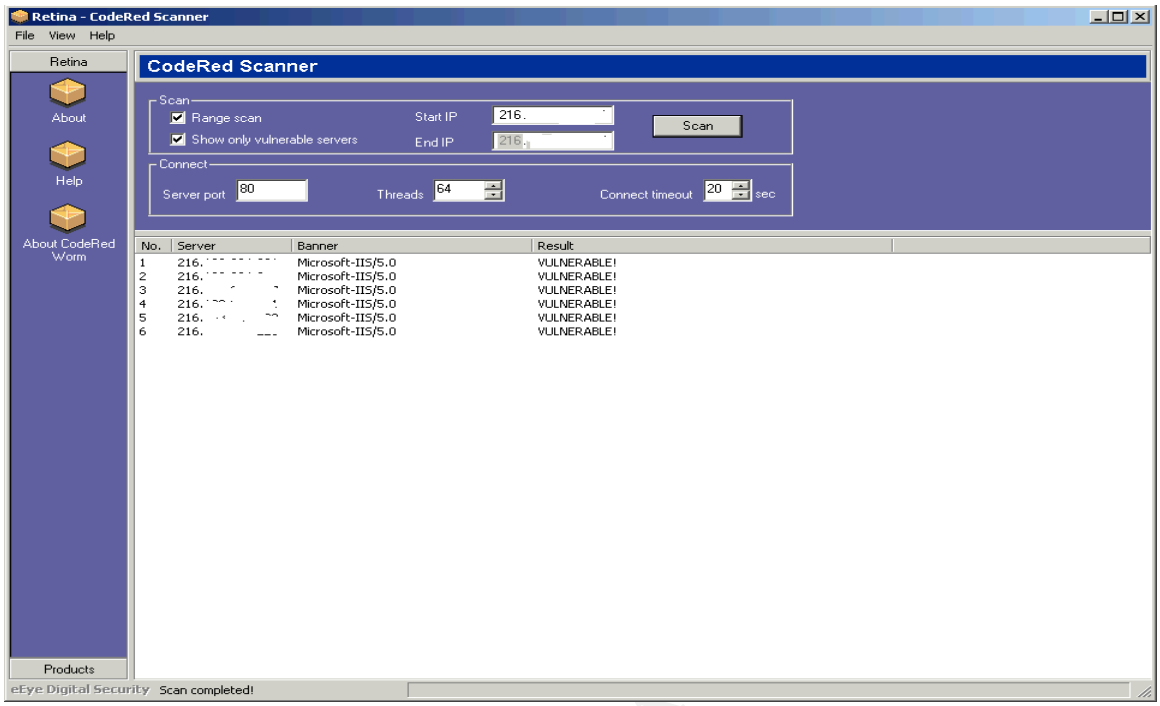
Nmap –sS –O –p 443 <webserver IP address>

The –sS option tells nmap to run a stealth port scan. Ths means that nmap sends a TCP packet with the SYN flag set and waits for a response, if a SYN ACK is received back Nmap immediately sends a RST to tear down the connection. The advantage of this scan is that many operating systems do not log connection attempts of this nature.

The –O option tells nmap to use TCP fingerprinting to attempt to identify the operating system. Nmap attempts to guess the operating system through TCP packet sequence prediction and by sending a TCP packet with non-standard flags set such as RST as the first packet. No standard way of responding to packets with non-standard flags set has been established, and as a result each operating system responds in a different way.

The –p option tells nmap to scan only specified ports, in the command lines above we are scanning only port 80 and port 443. By limiting scans to know open ports, the scans can be hidden as normal HTTP and HTTPS requests.

Third: A tool such as the eeye.com code red scanner could be run to determine if the site is vulnerable. Below is output of the Code Red scanner's discovery of vulnerable servers. I have sanitized the IP addresses, as this scan was not performed on test servers.



Last, now that the server is known to be vulnerable the code red worm code can be transferred to the server. This is accomplished by send an HTTP GET request that contains the code red source. A sample of the code follows:

GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801

%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u0

0c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

If this code is successfully executed, code red will attempt to replace files on the system including w3svc.dll and cmd.exe this would allow other tools to be transferred to the compromised server to be used to launch attacks from inside the perimeter. Older versions change the default webpage to standard page containing obscenities; this would be an indication that the site has been hacked. Newer versions of the exploit do not change the default web page, in this case the only indication of compromise would be if the administrator noticed increased activity or if other administrators reported that their sites were being scanned by the server's IP address.

Rule 10 shown below allows traffic from the web server to the corporate database server as shown below, this would allow damage to the database, transfer of corporate data to take place, or access to the entire network if the database server is vulnerable to exploit.

References

Brenton, Chris; Firewalls, *Perimeter Protection, and Virtual Private Networks,* The SANS Institute, 2001.

Brotzman & Ranch, *Securing Linux Step-by-Step version1.0*, The SANS Institute, 2000

http://www.bastille-linux.org/ - Information on the Bastille Linux configuration.

www.cert.org – Various articles on vulnerabilities.

www.checkpoint.com – Checkpoint Firewall Vulnerabilities.

http://www.cisco.com/ - Information on Cisco routers, switches, and IOS software.

www.eeye.com – Information on NmapNT, Code Red, LibnetNT and the Code Red Scanner.

www.gta.com – The manufacturer of the GNAT Box firewall system.

www.gnatbox.com – Information and user manuals for the GNAT Box firewall system.

www.insecure.org/nmap – Information on the NMap port scanning tool and its features.

www.maps.org – Information on the mail abuse prevention system.

www.microsoft.com – Information on the Code Red Unicode exploit.

www.netcraft.com – Information on Web server software and the "what is that site

running" tool.

www.redhat.com – Source of the Red Hat Linux operating system.

www.snort.org – Information on the SNORT Intrusion Detection System.

www.sygate.com – Manufacturer of the Sygate managed firewall.

www.tripwire.org – Information on the Tripwire file verification tool.

www.whitehats.com – Source of Arachnids IDS signatures for SNORT.

www.sans.org/y2k/practical/Tim_Daly_GCFW.zip – Tim Daly's GCFW practical.

Appendix 1

GNAT Box Software Configuration Summary

GNAT Box Version: GB-100 3.2.0 Fri 2002-01-04 17:49:46

Basic Configuration

DNS

External name server: 10.20.30.20
Internal name server: 0.0.0.0
Domain:

Features

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa - GB-100 3.2 - Registered
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa - GB-100 3.2 - Multiple interfaces

Network Information

LOGICAL INTERFACES

Name	Type	IP Address	Netmask	NIC
EXTERNAL	EXTERNAL	10.20.30.3	255.255.255.0	dc3
PROTECTED	EXTERNAL	172.16.0.1	255.255.255.0	fxp0
PSN1	PSN	192.168.0.1	255.255.255.0	dc0

NETWORK INTERFACE CARDS

NIC	MAC Address	MTU	State	Connection
dc0	00:80:c8:c9:a8:39	1500	up	AUTO
dc1	00:80:c8:c9:a8:3a	1500	down	
dc2	00:80:c8:c9:a8:3b	1500	down	

```
dc3    00:80:c8:c9:a8:3c  1500   up     AUTO
fxp0   00:60:ef:21:2a:3d  1500   up     TX_100MB full_duplex
xl0    00:01:02:66:d8:73  1500   up

Default route (gateway): 10.20.30.1
            Hostname: GIACBox
```

Preferences

```
ADMINISTRATOR CONTACT INFORMATION
         Name: Jamy Klein
      Company: GIAC Fortune cookies
Email Address: jamy@giac.corp
 Phone number: 555-555-6555
Serial number: 5555555555

Support email: gb-config@gta.com

Default character set: ISO-8859-1

KEYBOARD LAYOUT
 United States ISO-8859-1

SCREEN SAVER
 Timeout: 600 seconds
```

Services

DHCP Server

disabled

DNS Server

```
       Enabled: no
 Primary name:
    Secondary:
   Forwarders:
Email contact:

DOMAINS
 1
  #
        State: enabled
  Domain address: 192.168.2.1
  Mail exchangers: sttint3 lists hq

  HOSTS
   Index  Disabled  RDNS  IP Address       Names
   -----  --------  ----  ---------------  --------------------------------
     1           X   192.168.2.9      sttint3  lists  hq

NETWORKS
 Index  Network Address  Netmask          Reverse Zone Name
 -----  ---------------  ---------------  ------------------------------
   1  192.168.2.9      255.255.255.0
```

Email Proxy

Enabled: yes
Primary server: 172.16.0.10
Alternate server:
Time out: 480 seconds
Maximum connections: 300
Domain: giac.corp
Use MX: yes
Verify RDNS: no
Maximum size: 10000 kilobytes
MAPS 1: enabled rbl.maps.vix.com
MAPS 2: enabled dul.maps.vix.com
MAPS 3: enabled relays.orbs.org
MAPS 4: enabled relays.mail-abuse.org

Enterprise Server

disabled

Remote Logging

Logging system messages to server: 192.168.2.7:514
Use non-standard date format: enabled

Filter facility: local1
NAT facility: local0
WWW facility: local2
Open priority: emerg
Close priority: emerg
WWW priority: alert

Authorization

Admin Accounts

Index	User	Permissions
1	gbadmin	admin console www remote
2	sysadmin	admin www remote

Content Filtering Preferences

disabled

MOBILE CODE BLOCKING
JAVA blocking: disabled
JAVA script blocking: disabled
ActiveX blocking: disabled

Content Access Control Lists

none

Remote Administration

WWW Server: enabled
Updates: enabled
Port: 85

RMC Server: enabled
Updates: enabled

Port: 77

VPNs

1 #VPN to GIAC partner company
Key exchange: IKE main mode
Networks: 172.16.0.0/255.255.0.0 -> 192.168.100.0/255.255.255.0
Gateways: 10.20.30.3 -> 204.86.186.1
Phase 1: blowfish hmac-sha1 group 2
Phase 2: blowfish hmac-sha1 group 2

2 #GIAC mobile Partners and employee VPN
Key exchange: MOBILE
Networks: 192.168.2.0/255.255.255.0 -> 192.168.200.1/255.255.255.255
Identity: admin@giac.corp
Phase 1: 3des hmac-sha1 group 2
Phase 2: 3des hmac-sha1 group 2

Routing

Gateway Selector

disabled

RIP

Enabled: yes

Interface	Enabled	Input	Output	Password
EXTERNAL		none	none	none
PROTECTED	X	both	both	none
PSN1	X	both	both	none

Advertise default route: yes

Static Routes

Index	IP Address	Netmask	Gateway

Objects

Addresses

1 ANY_IP - DEFAULT: Matches all IP addresses.

Index	Type	Beginning	Ending
1	range	0.0.0.0	255.255.255.255

2 e-commerce ext - ecommerce webserver external ip

Index	Type	Beginning	Ending
1	host	10.20.30.10	

3 e-commerce psn - psn net ip address of e-commerce server

Index	Type	Beginning	Ending
1	host	192.168.0.10	

4 EXT DNS IP - External DNS: EXT ip

Index	Type	Beginning	Ending

Index	Type	Beginning	Ending
1	host	10.20.30.20	

5 EXT DNS PSN IP - PSN ip address of external DNS server

Index	Type	Beginning	Ending
1	host	192.168.0.20	

6 EXT IP range - External ip address tnage

Index	Type	Beginning	Ending
1	range	10.20.30.1	10.20.30.255

7 Gnatbox interfaces -

Index	Type	Beginning	Ending
1	host	192.168.0.1	
2	host	172.16.0.1	
3	host	10.20.30.3	

8 PRO Net IP range - IP addresses for the internal network

Index	Type	Beginning	Ending
1	range	172.16.0.1	172.16.255.255

9 PSN IP range - IP address range for the service network

Index	Type	Beginning	Ending
1	range	192.168.0.1	192.168.0.255

10 supplier's ext - external ip of supplier server

Index	Type	Beginning	Ending
1	host	10.20.30.15	

11 supplier's int - PSN net address of supplier's server

Index	Type	Beginning	Ending
1	host	192.168.0.15	

12 Syslog EXT - external IP of syslog

Index	Type	Beginning	Ending
1	host	10.20.30.25	

13 Syslog INT - IInternal address of syslog

Index	Type	Beginning	Ending
1	host	172.16.0.5	

Filters

Outbound

1 #DEFAULT TRADITIONAL URL PROXY: allow access to DNS.
Accept "PROTECTED" UDP log

```
    from "ANY_IP"
      to "ANY_IP" 53

2 #DEFAULT NO TRADITIONAL URL PROXY: Allow protected network access to anywhe
  Accept "PROTECTED" ALL  log genICMP
    from "ANY_IP"
      to "ANY_IP"

3 #DEFAULT PSN: Allow PSN network to access anywhere.
  Disabled - Accept "PSN1" ALL  log
    from "ANY_IP"
      to "ANY_IP"

4 #PSN OUT: allow TCP HTTP,HTTPS
  Accept ANY TCP  log
    from "e-commerce psn" 80 443
      to "ANY_IP"

5 #PSN OUT: Supplier's server TCP, HTTP, HTTPS, SSH
  Accept ANY TCP  log
    from "e-commerce psn" 22 80 443
      to "ANY_IP"

6 #PSN OUT: TCP for DNS
  Accept ANY TCP  log
    from "EXT DNS PSN IP" 53
      to "ANY_IP"

7 #PSN OUT: UDP for DNS
  Accept ANY UDP  log
    from "EXT DNS PSN IP" 53
      to "ANY_IP" 53

8 #PSN OUT: UDP for syslog
  Accept ANY UDP  log
    from "PSN IP range" 514
      to "Syslog INT" 514

9 #PRO OUT: Log all traffic out of PRO network
  Accept "PROTECTED" TCP  log
    from "ANY_IP"
      to "ANY_IP" 21 22 77 80 443
```

Remote Access

```
1 #EXT block: Traffic from 172.16 private ip range
  Deny   "EXTERNAL" ALL  log
    from "ANY_IP"
      to "172.16.0.0/255.255.0.0"

2 #EXT Block: Traffic from private ip range 192.168
  Deny   "EXTERNAL" ALL  log
    from "ANY_IP"
      to "192.168.0.1/255.255.255.0"

3 #EXT IN: Allow TCP access for HTTP,SSL to E-comm server from all networks
  Accept ANY TCP
```

```
    from "ANY_IP"
      to "e-commerce ext" 80 443

4 #EXT IN: Allow TCP access for SSH,HTTP,HTTPS for suppliers server
  Accept ANY TCP  log
    from "ANY_IP"
      to "supplier's ext" 22 80 443

5 #EXT IN: Allow TCP in port 53 for DNS
  Accept ANY TCP  log
    from "ANY_IP"
      to "EXT DNS IP" 53

6 #EXT IN: Allow UDP in port 53 for DNS
  Accept ANY UDP  log
    from "ANY_IP"
      to "EXT DNS IP" 53

7 #EXT IN: allow router 1 to access syslog
  Accept "EXTERNAL" UDP  log
    from 10.20.30.1/255.255.255.255 514
      to "Syslog EXT" 514

8 #PRO IN: Allow Router 1 access to syslog internal ip
  Accept "PROTECTED" UDP  log
    from 10.20.30.1/255.255.255.255 514
      to "Syslog INT" 514

9 #EXT IN: Allow router 2 access to syslog
  Accept "EXTERNAL" UDP  log
    from 10.20.30.2/255.255.255.255 514
      to "Syslog EXT" 514

10 #PRO IN: Allow router 2 access to syslog
  Accept "PROTECTED" UDP
    from 10.20.30.2/255.255.255.255 514
      to "Syslog INT" 514

11 #PRO IN: Allow PSN IP range access to syslog
  Accept "PROTECTED" UDP  log
    from "PSN IP range" 514
      to "Syslog INT" 514

12 #Allow remote access from ALL
  Accept ANY ALL
    from "ANY_IP"
      to "Gnatbox interfaces"

13 #DEFAULT: DNS: Allow protected network access to DNS server.
  Accept "PROTECTED" UDP  log
    from "PRO Net IP range" 53
      to "EXT DNS PSN IP" 53

14 #DEFAULT: DNS: Allow all DNS replies.
  Accept ANY UDP
    from "ANY_IP" 53
```

```
      to "ANY_IP" 1024:65535

15 #DEFAULT TRADITIONAL URL PROXY: Allow connections to URL proxy.
  DISABLED - Accept "PROTECTED" TCP
    from "ANY_IP"
      to 0.0.0.0/0.0.0.0 2784

16 #DEFAULT EMAIL PROXY: Allow connections to email proxy.
  Accept "EXTERNAL" TCP
    from "ANY_IP"
      to "ANY_IP" 25 110

17 #DEFAULT NO RIP: Block/nolog rip.
  DISABLED - Deny   ANY UDP  nolog
    from "ANY_IP"
      to "ANY_IP" 520

18 #DEFAULT RIP: Accept UDP rip.
  Accept ANY UDP
    from "ANY_IP"
      to "ANY_IP" 520

19 #DEFAULT RIP: Accept IGMP multicast for router addresses.
  Accept ANY 2
    from "ANY_IP"
      to 224.0.0.0/255.255.255.0

20 #DEFAULT RIP: Accept router solicititations and advertisements
  Accept ANY ICMP
    from "ANY_IP"
      to 224.0.0.0/255.255.255.0 9 10

21 #DEFAULT: Accept/nolog authentication (ident).
  Accept ANY TCP  nolog
    from "ANY_IP"
      to "ANY_IP" 113

22 #Mobile VPN: Allow ESP connections from client
  Accept ANY 50   log
    from "ANY_IP"
      to 10.20.30.3/255.255.255.255

23 #Mobile VPN: allow access to IKE from mobile clients.
  Accept ANY UDP  log
    from "ANY_IP" 500
      to 10.20.30.3/255.255.255.255 500

24 #Partner VPN: Allow ESP connectiions from partner network
  Accept ANY 50
    from 204.86.186.1/255.255.255.255
      to 10.20.30.3/255.255.255.255

25 #partner VPN: allow access to IKE from partner network
  Accept ANY UDP  log
    from 204.86.186.1/255.255.255.255 500
      to 10.20.30.3/255.255.255.255 500
```

```
26 #Partner VPN: allow ESP connections from GIAC network to Partner Network
  Accept ANY 50
    from 10.20.30.3/255.255.255.255
      to 204.86.186.1/255.255.255.255

27 #Partner VPN: Allow access to IKE from GIAC network
  Accept ANY UDP  log
    from 10.20.30.3/255.255.255.255
      to 204.86.186.1/255.255.255.255

28 #Allow High Availability Protocol
  Accept ANY UDP
    from 10.20.30.4/255.255.255.255
      to 224.0.0.18/255.255.255.255 77

29 #Allow: IGMP for High availability
  Accept ANY 2    bcast
    from 10.20.30.4/0.0.0.0
      to 224.0.0.18/0.0.0.0 77

30 #DEFAULT: Block/nolog discard bootp, netbios, snmp, and rwho.
  Deny   ANY UDP  log
    from "ANY_IP"
      to "ANY_IP" 9 67 68 137 138 161 513

31 #DEFAULT: Allow pings and ICMP traceroutes to GNAT Box.
  Deny   ANY ICMP log
    from "ANY_IP" 8
      to "ANY_IP" 8

32 #DEFAULT: Allow UDP traceroutes to GNAT Box.
  Deny   ANY UDP  log genICMP
    from "ANY_IP"
      to "ANY_IP" 32767:65535

33 #DEFAULT: Block/nolog stale WWW accesses.
  Deny   ANY TCP  log
    from "ANY_IP" 80
      to "ANY_IP" 1024:65535

34 #DEFAULT: Block with alarm any other access to all interfaces.
  Deny   ANY ALL  log
    from "ANY_IP"
      to "ANY_IP"
```

Time Groups

None

Protocols

Index	Name	Number
1	IGMP	2
2	ESP	50
3	AH	51

Preferences

DEFAULT LOGGING
Log ALL packets rejected.

ALARMS
Send email for alarms when 10 seen within 120 seconds.
Send a maximum of 500 alarms per email.
Do not attempt to log host names using reverse DNS.
Do not attempt to send page when alarm threshold reached.

GENERAL
Stealth mode: disabled
Doorknob twists generate: alarm logMessage
Address spoofs generate: alarm logMessage

EMAIL SERVER
Server name: mail.giac.corp
From: GB-1000
To: sysadmin@giac.corp

SNMP TRAPS
disabled

PAGER
disabled

IP Pass Through

Hosts/Networks

Index	Object or Address Range	Interface	Options
1	ANY_IP	PROTECTED	inbound

Filters

1 #VPN, allow inbound access from mobile clients.
Accept "EXTERNAL" ALL
from 192.168.200.1/255.255.255.255
to 192.168.2.0/255.255.255.0

2 #VPN, Allow outbound to mobile clients.
Accept "PROTECTED" ALL log
from 192.168.2.0/255.255.255.0
to 192.168.200.1/255.255.255.255

3 #Partner VPN: for partner network. Allow inbound traffic
Accept "EXTERNAL" ALL
from 192.168.100.1/255.255.255.0
to 172.16.0.10/255.255.0.0

4 #partner VPN: Allow outbound from GIAC to partner network
Accept "PROTECTED" ALL
from 192.168.100.1/255.255.255.0
to 172.16.0.10/255.255.0.0 7000:7030

5 #partner VPN: allow inbound to GIAC network

Accept "EXTERNAL" TCP
from 172.16.0.0/255.255.0.0
to 192.168.100.1/255.255.255.0

6 #Partner VPN: Allow outbound, outbound to GIAC
Accept "PROTECTED" TCP
from 192.168.100.1/255.255.255.0
to 172.16.0.0/255.255.0.0 7000:7030

NAT

Aliases

Index	Interface	IP Address	Netmask
1	EXTERNAL	10.20.30.10	255.255.255.255
2	EXTERNAL	10.20.30.15	255.255.255.255
3	EXTERNAL	10.20.30.20	255.255.255.255
4	EXTERNAL	10.20.30.25	255.255.255.255

Inbound Tunnels

Index	Protocol	From IP Address	Port	To IP Address	Port	Options
1	TCP	10.20.30.10	80	192.168.0.10	80	filter
2	TCP	10.20.30.10	443	192.168.0.10	443	
3	TCP	10.20.30.15	80	192.168.0.15	80	
4	TCP	10.20.30.15	443	192.168.0.15	443	
5	TCP	10.20.30.20	53	192.168.0.20	53	
6	UDP	10.20.30.20	53	192.168.0.20	53	
7	UDP	10.20.30.25	514	192.168.0.25	514	

Static Address Mappings

Index	From - Object or Address Range	To IP Address
1	e-commerce psn	10.20.30.10
2	supplier's int	10.20.30.15
3	EXT DNS PSN IP	10.20.30.25

Timeouts

ICMP: 15 seconds
TCP wait for ACK: 30 seconds
TCP: 600 seconds
TCP keep alive enabled: yes
UDP: 600 seconds
Wait after close: 20 seconds

Filter Format:

Filters are listed in the configuration printout in the following format.

```
<filter number>  <description>
      <Action>   <interface> <protocol>  <log action>
        <source object or IP> <source port(s)>
          <destination object or IP> <destination port(s)>
```