



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 permitted without express written permission.

GIAC Enterprises

**SANS GIAC Certification
GCFW Practical Assignment
Version 3.0**

**Phillip Huereca
9 Aug 2004**

© SANS Institute 2004, Author retains full rights.

Abstract

This paper consists of four assignments.

Assignment one will discuss Security Architecture. In this assignment, a security architecture will be developed that will adequately protect GIAC Enterprises. Components will be added and discussed as to how they enhance the security of the network. Finally defense in depth will be discussed.

Assignment two will develop the security policy. The border router security policy will be discussed as well as its configuration. Next the external primary firewall will be discussed. The configuration and rules will be developed and explained. Finally the VPN policy will be discussed and its policy explained.

Assignment three will be attacking a previous practical that had been submitted in the last 6 months. Reconnaissance, scanning, attacking an internal component and then maintaining control of an internal component will be discussed.

Assignment four will discuss a work procedure for the external firewall. The procedure will be a complete guide that a newly hired security engineer could pick it up and understand how to manage all aspects of the external firewall

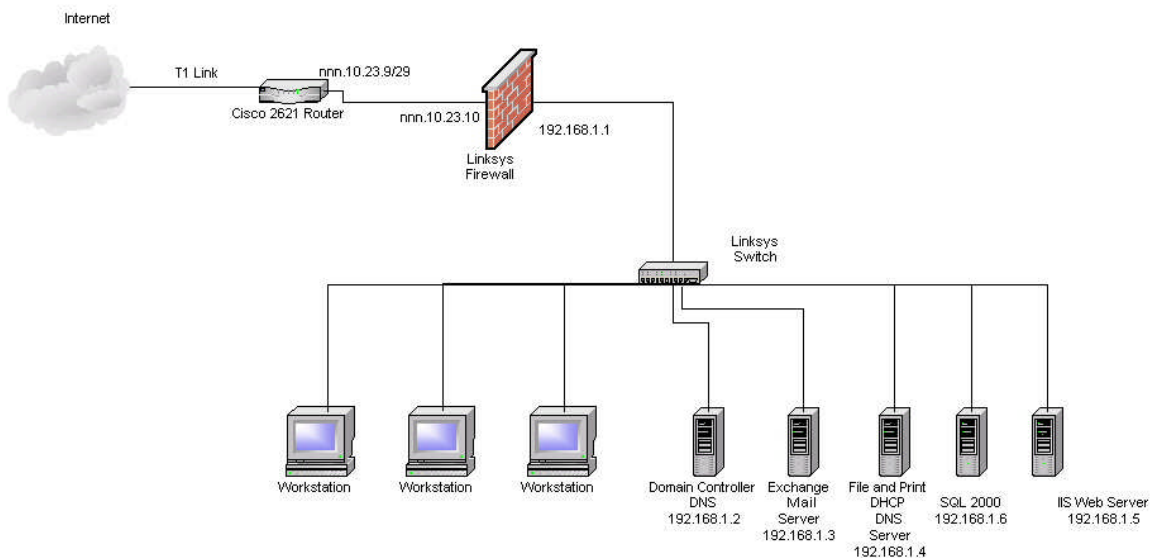
Assignment 1 - Security Architecture

Introduction

GIAC Enterprises is a startup based out of Austin, TX. The company deals with the online sale of fortune cookie sayings, and is a privately held company. Someday the company hopes to go public but in the meanwhile, they have to hold down company expenses and continue to build their cash flow. GIAC Enterprises has built their business and network based on Microsoft Technology. The web server is running IIS 5.0 and is using Microsoft SQL 2000 for the backend. All internal users are using Windows 2000 Professional. Servers are Windows 2000 in an Active Directory configuration. The company currently has a 1 man IT staff who is Microsoft Certified but lacks experience but is highly trainable. Costs will have to be kept low due to the financial status of the company. Currently GIAC Enterprises network consists of a Cisco 2621 border router connected via T1 to their ISP. There is a linksys firewall in place to protect the internal network. The GIAC Enterprises public website was recently defaced and the managers decided that an outside consultant was needed to “tighten security”. They asked for a proposal that will keep costs down but provide the ultimate security. Since this company

is a Microsoft Partner, they preferred to use Microsoft products wherever possible. They also asked to keep any needed changes as simple as possible and easy enough for their current IT staff to learn and maintain. Below is the current GIAC Enterprises network. As their consultant, I will make recommended changes to enhance their security and put into effect the concept of “defense in depth”.

Original GIAC Enterprise Network



Business requirements.

- Customers (whether Companies or individuals) must be able to purchase bulk online fortunes.
- Suppliers that must be able to supply fortune cookie sayings.
- Partners must be able to download fortune cookie sayings.
- Employees of GIAC Enterprise (hereafter called GE) must be able to access the Internet for research and marketing. Web developers must additionally have access to the Web Server in the DMZ.
- Mobile sales employees will travel and must be able to access data back at the company. Certain internal employees will also have the need to be able to access resources at the company from home.

- The general public should only be able to view the company public website.

Business Operation Solution

Once the requirements were known, it was determined the following access requirements would be implemented. For the purpose of this paper, assume that the main website is located at the fictitious site <http://www.giacenterprises.com>.

Customers

Customers will do all transactions using the GIAC main company website located in the DMZ. The protocol being used will be https port 443. Https uses SSL, which stands for “secure sockets layer” for encrypting traffic. The reason we chose SSL is because it’s literally built into everyone’s client browser. All customer transactions will require credit card information and sensitive data of which we will want all these transactions to be securely encrypted. Customers will be accessing the web server at <https://www.giacenterprises.com/customer>. There will be a link from the main website called “customers” for easy access to the customers sections.

Suppliers

Suppliers will supply fortune cookie sayings to GIAC Enterprises using the GIAC main company website located in the DMZ using https port 443. Note that suppliers will access the GIAC website at <https://supplies.giacenterprises.com>. Suppliers can also access the suppliers website thru the main page as there will be a link for easy access. Suppliers will be given a password and will require a digital certificate for access.

Partners

Partners will download cookie sayings from the GIAC main website using https port 443. They will go to URL <https://partners.giacenterprises.com>. There will be a link on the main company website for easy access. Partners be given a password and will require a digital certificate for access.

Internal Employees

Employees of GE will access the Internet for research and marketing purposes. They will only be allowed to browse the Internet. Web developers additionally will be granted access to the files of the web server.

Mobile sales force and teleworkers

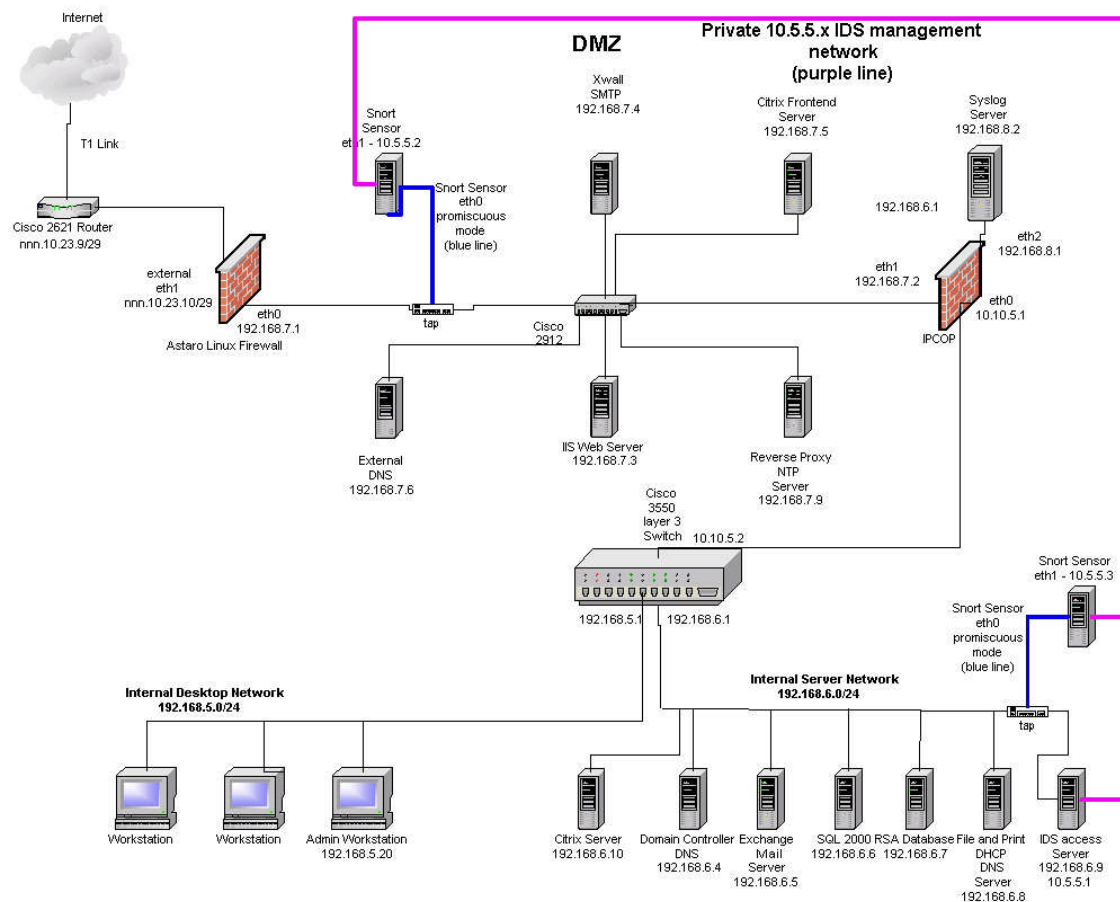
Employees who travel or must work from remote unsecured locations will VPN using SSL to access the Citrix front-end web server. Mobile users will be issued an RSA token for 2-factor authentication. 2 factor authentication deals with the concept of something that a user has (token) and something the user knows (a pin number). Additionally clients

will also have a personal firewall on their machine. We will utilize ez-armor from CA, which provides both anti-virus protection and a personal firewall.

General public

The general public will have access to the public website located at <http://www.giacenterprises.com> or if they chose to become customers can then be linked to <https://www.giacenterprise.com/customers>.

Below is the proposed redesigned network diagram of which we will explain in detail in the following paragraphs



IP Addressing

Note that for the purpose of this paper, our ISP is providing the IP addresses for connectivity of the serial interface of our 2621 Cisco router to the backbone of the ISP. We will assume those IP addresses to be as follows.

nnn.10.25.5 / 30 (ISP backbone router)

nnn.10.25.6 / 30 (GIACenterprise's external serial interface s01)

Our ISP gave us 6 public IP addresses to use. Our assigned network is nnn.10.23.8 / 29
This breaks down as follows

Network: nnn.10.23.8
Broadcast: nnn.10.23.15
First IP: nnn.10.23.9
Last IP: nnn.10.23.14

We will assign these public IP addresses as follows which we will refer to as “external network”

External Network

Cisco 2621 router eth0 – nnn.10.23.9
Astaro Linux firewall eth1 – nnn.10.23.10

DMZ Network

For the DMZ, we will utilize RFC 1918 compliant IP addresses. RFC 1918 compliant addresses can be found at <http://www.iana.org/faqs/abuse-faq.htm#SpecialUseAddresses>.

¹

Current private IP addresses are:

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

I arbitrarily picked 192.168.7.0 /24. This subnet will give more than enough room to grow (254 hosts). Below are the DMZ IP assignments.

Astaro Linux Firewall internal interface (eth0)	- 192.168.7.1
IPCOP Firewall external interface (eth1)	- 192.168.7.2
IIS 5.0 Microsoft Web server	- 192.168.7.3
XWall SMTP server	- 192.168.7.4
Citrix Front-end Server	- 192.168.7.5
DNS server	- 192.168.7.6
Reverse Proxy Server	- 192.168.7.9

Internal Network

¹ <http://www.iana.org/faqs/SpecialUseAddresses>

The internal network is divided between 2 distinct networks. The purpose of this is to put the servers on their own network separate from the desktops. This will give us better control on monitoring the server network particularly with intrusion detection. Below is the IP addressing scheme.

Desktops - dynamically assigned.

Servers

Domain Controller / DNS	- 192.168.6.4
Exchange Mail Server	- 192.168.6.5
SQL 2000 Server	- 192.168.6.6
RSA Database Server	- 192.168.6.7
File and Print /DHCP/DNS Server	- 192.168.6.8
IDS front-end/syslog Server	- 192.168.6.9
Citrix Server	- 192.168.6.10

COMPONENTS in the DMZ

GIAC Enterprises management requested that all additional hardware be racked mounted and consistent. They did not want desktop servers cluttering their very neat server room. They allowed one rack space to be utilized. They also requested that Dell servers be used, as that is whom they are most comfortable with. So it was agreed upon that all Dell Servers would be used and that they would all be 2650 PE Servers with minimum of 1 Gig of RAM and with a raid 1 configuration for fault tolerance. All would come with 2 each 36 Gig Drives with the exception of the syslog server which will come with 3 each 72GIG drives in a raid 5 configuration to insure it has plenty of room for logs. It was also agreed on with the management that Microsoft products would be used where possible and that Windows 2000 Server would be the standard install for all Microsoft Servers. If a UNIX box were required, all boxes would use Red Hat 9.0. This is because Dell servers ship with a CD for each server that can quickly build the box. Red hat 9.0 is the Red hat version currently supported on this CD. Should a UNIX box fail, the box can be easily rebuilt with provided documentation. GIAC has budgeted for 10 servers to be added so as long as I stay under 10 servers, all well be good. 2 Cisco switches were also approved to be added with this budget. A Citrix solution was budgeted for also as the CIO of GIAC insisted this be used, as they needed to give their sales force the most flexibility possible.

Cisco 2621 Router.

GIAC Enterprises already had a 2621 Cisco router in place. As a consultant, I determined that this router would be sufficient. The only thing that will need to be done is to update the IOS version and to train the network administrator the importance of keeping the IOS updated. Exploits do happen and keeping the IOS current is very important to stay secure. A 2600 series router has modular components that can be easily transferred to a

3600 series router should the need arise to upgrade due to increase IP traffic. We will improve on the router configuration by hardening it. The purpose of this router is to interface with the T1 provided by the ISP. It does this by having an internal CSU/DSU module card that interfaces with the T1. The security function that this router will perform will be to use static filters to filter out known absolute traffic that does not need to enter the network such as NetBIOS traffic and spoofed traffic. The security weakness of this component is that it cannot inspect packet payload. It cannot maintain state of a connection. It has problems dealing with certain types of ICMP traffic. The router will also be our first line of defense, as we will use ACL's to control IP traffic.

Astaro Linux Firewall. (www.astaro.org)²

The purpose of this firewall is to protect the networks behind it. This award winning firewall was picked over other contenders because it's robust, secure, easy to use, and easy to rebuild, and not that expensive. It has the important feature of stateful packet inspections. This basically means that the firewall will keep a complete session state information for each session that it uses thru a firewall plus with the additional feature of being application aware. It has a web interface to manage the firewall, which makes it very easy to configure. It can also be used for intrusion detection, Anti-virus, SPAM, and Surf Control. We wanted to pick a firewall that once we configured it properly that we could train a GE employee to take over the task of monitoring it etc.. So we needed a firewall that could quickly be rebuilt if needed. As the company grows, they should be able to afford the HA feature that comes with this firewall. Other firewalls were looked at and considered but the training and learning curve steepened along with the money to afford them. Two examples were Cisco PIX and Checkpoint NG firewalls. OpenBSD has a very nice secure firewall but is not easily rebuilt and it's easy to make a mistake in configuring it. The security weakness of this component is that it can be fooled. Http traffic usually must still flow thru on to the web server and that traffic can have dangerous code for the web server. The component will be GIAC's second line of defense.

Snort Sensor in DMZ (www.snort.org)³

The purpose of the snort sensor is to monitor for intrusions and attacks against the DMZ network. Snort was picked because it's free and widely available and it's what this author is most familiar with. This box will be built with Red hat 9.0 using the latest version of Apache, PHP, ACID and MySQL. There is an excellent document on how-to build this box at http://www.snort.org/docs/snort_acid_rh9.pdf. One of the interfaces will run in promiscuous mode and hook directly into a tap. This will provide optimum traffic capture. This will also make the interface invisible to the DMZ, as it will not be assigned an IP address. The other interface eth1 will be connected to the IDS management network so that an internal management server can manage this sensor privately.

² <http://www.astaro.org>

³ <http://www.snort.org>

Xwall SMTP server. (www.dataenter.com)⁴

The purpose of this server is to provide filtering of all email before the email is allowed to enter the internal network. Therefore the MX record for this server will be the lowest number in the DNS entries. Xwall provides excellent filtering of all emails attachments. They can be checked for viruses before being allowed in. Certain attachments can be blocked. SPAM can be filtered. And best of all, it only costs 350 dollars. It can run on old hardware if that is all you have available. Depending on your volume of email, a 266 Pentium II has been sufficient in the past. Normally though, you will want a more powerful robust server especially if your wanting to use the anti-virus feature which I believe is the most important feature of Xwall. The anti-virus piece can utilize several vendors of your choice. This consultant opted to use the very cheap and available f-prot for anti-virus scanning of email. (www.f-prot.com) Windows 2000 Server will be installed with the latest patches and hardened.⁵ Xwall will run as an application on this server set up as an SMTP relay for the GIAC network ONLY. The security weakness of this device would probably be the configuration of Xwall itself. It is getting lengthier with each version and can be easily misconfigured. It is however, very intuitive and simple to figure out with good documentation at the main website.

DNS Server in DMZ

The purpose of this server is to forward DNS queries from the internal network to the outside world (internet). We will architecture a concept called "Split DNS". Basically this means we let the Internet see only what it needs to see of our network. We do not want to let the world see our internal addressing scheme or any more information about our network than absolutely necessary. This will deter hackers from obtaining any information about our internal network. We will also have an "internal" DNS, which will be discussed later in this paper. Again Windows 2000 server will be used with the latest patches and hardened. Security weakness of this component is that misconfiguration can happen. This could cause zone transfers to servers not intended to get this information. DNS in Windows 2000 has however been reliable and stable.

IIS web server.

The purpose of this server to provide http web enabled pages to the general public and https web enabled pages to the customers, suppliers, and partners. The GIAC web developers and management are most familiar with IIS 5.0 so that is why it was decided to stay with that version. IIS 6.0 has more improved security but this was a political decision outside the realm of this consultant. By applying the latest patches, we should be fine. Note that Windows 2000 Server will be the operating system. We will also utilize 2 excellent tools to secure our web server, the IIS Lockdown Tool and the URLScan Filter tool. These tools will remove known weaknesses and will provide a layer of defense against attacks. The URLScan Filter tool will filter requests. Note that the DMZ Reverse Proxy Server running SQUID and Jeanne will proxy all requests

⁴ <http://www.dataenter.com>

⁵ <http://www.f-prot.com>

coming to this server so this server will be adequately defended. The security weakness of the server has been that IIS 5.0 has had so many exploits and so that is why all requests to it are filtered. The web application developers also will be receiving additional code training to make their applications more secure and to make them aware of the consequences of bad coding.

DMZ Reverse Proxy Server.

The purpose of this server is to reverse proxy all HTTP and HTTPS traffic from the Internet to the GIAC main web server, which is also located in the DMZ. Squid version 2.5 (<http://www.squid-cache.org/>) will be loaded on a Red Hat Linux box running the agreed upon standard 9.0.⁶ The plug-in Jeanne will also be installed to perform content filtering. All the information about Jeanne can be found at http://www.ists.dartmouth.edu/IRIA/projects/d_jeanne.htm.⁷ The combination should give GIAC the best protection for the highly exploitable IIS 5.0 web server. This component will be third line of defense as the router and firewall precede this component is filtering traffic. Security weakness of this device is making sure the latest patches are applied to the Red Hat Linux box in a consistent manner and also keeping Squid current in the event an exploit is discovered. Note also that the NTP service will be running on this box and will function as the official source of time for the GIAC network.

DMZ Web Interface for Citrix

The purpose of this server is to provide the front-end VPN solution for GIAC's mobile sales force or for any internal employees who must work from home. Authorized users with the RSA token can authenticate against this server and get access to all internal resources that are published for their use. Access will be by utilizing HTTPS using the standard web browser located on most desktops. Internet Explorer must however be version 5.0 or greater. Potential security weakness may be if SSL has an exploit that can be taken advantage of. Other potential security weakness is the operating system itself. However, keeping this server up to date with the latest patches and hardened should offset that factor. The server will be a Windows 2000 Server with the latest patches and of course hardened.

Syslog Server

Note that this server is not in the DMZ and is not in the internal network. It is however on its own segment located off of the internal firewall. The purpose of this server is to have a centralized location to gather all syslogs. Red hat 9.0 running the syslogd will be used to gather all logs. This server will only be used for logging and for nothing else. It will be a stripped down hardened Linux box. This box will have plenty of disk space (note in the hardware discussion above that this box comes with 3 ea 72 Gig Drives in a raid 5 configuration). Should this box be compromised, it is located on it's own segment

⁶ <http://www.squid-cache.org>

⁷ http://www.ists.dartmouth.edu/IRIA/projects/d_jeanne.htm

and will minimize the impact. Security weakness will be if a hacker should get access to this box, a lot of information about the network will be obtained. That is why this box will be stripped down and only running the syslog service.

Components located in the internal network

Internal Firewall – IPCOP

The internal network is further protected by a firewall called IPCOP. (www.ipcop.org)⁸. This firewall was chosen due to its simplicity but yet strong security. It installs very easily simply using an iso image to load with. This firewall uses iptables for stateful packet filtering. IPCOP has snort built in and supports SQUID for http filtering. We will use this firewall to proxy our outbound http connections and to control access to the DMZ from internal servers.

Cisco 3550 Catalyst switch

The purpose of this switch is to separate the servers from the desktops. This is important because a SNORT sensor will be used to watch the traffic on the server network. Excess desktop traffic will only add to the traffic to be analyzed. Using a layer 3 switch allows fast connectivity between desktops and servers. 2 Vlans will be created putting the desktops on one of them and the servers on the other. This particular switch has features that are very desirable for controlling traffic from one vlan to another.

Domain Controller/DNS Server

This server is used to implement Active Directory and provide DNS service for the internal network. This server supports the “Split DNS” architecture previously discussed. Internal desktops will query this DNS server and if necessary, this DNS server will forward the queries to the DMZ DNS server for further information.

Exchange Email

This server will provide email to the internal users. Microsoft Exchange 2000 is very robust and allows collaboration among internal users. All email to this exchange server will come from the Xwall mail server located in the DMZ. That way all email is filtered and screened before arriving. In addition, all email sent outbound will go thru the Xwall mail server to be screened and filtered for viruses. Also as an added level of defense, we will install CA's Etrust mail option to scan for viruses in the information store and can also additionally block certain attachments.

SQL 2000 Server

⁸ <http://www.ipcop.org>

This server provides the backend to the IIS 5.0 web server located in the DMZ. This server was previously located in the DMZ with the IIS 5.0 web server but has now been moved back to the protected internal network. This company prefers Microsoft SQL 2000 database over other vendors since they have several internal employees who are very familiar with this product and are also certified DBA's.

RSA Database Server

This server will provide RSA authentication to RSA token users. We will install RSA 5.01 server version on this particular server. This server will provide token authentication for the VPN Web Interface front-end of Citrix.

File and Print /DNS /DHCP Server

This server will provide regular file and print services to the internal desktop users. In addition this server will provide secondary DNS service for redundancy and also provide DHCP service to the dynamically assigned internal desktop users.

IDS Management Server

This server will provide access to the other Intrusion Detection Servers. We will only allow certain internal desktops access to this server. Operating system will be Red hat 9.0. This server will be running snort center and ACID. This way we have one centralized place to manage all snort sensors. This box will be stripped down and hardened and only Ssh access with RSA keys will be allowed on the box.

Internal Desktops

All internal desktops will be on their own vlan. This will keep unnecessary traffic off of the server vlan. It will also enable any necessary ACL control thru the 3550 switch to the server network if needed. All desktops will utilize Windows 2000 Professional and be dynamically assigned. The only exceptions will be the admin's desktop that will have an assigned IP address for access to the IDS management server/syslog server. All desktops and servers will have CA's Etrust 7.0 Anti-virus installed for protection against viruses, Trojans, etc⁹..

Defense In-Depth

Defense in-depth has been utilized through out the architecture of this network. The first line of defense will be the border router. It will filter all absolute traffic by using static filters. The second line of defense will be the Astaro Linux Firewall. It uses iptables to perform stateful inspection of all packets to screen for proper traffic. For all HTTP and HTTPS traffic, the Reverse Proxy Server will be the third line of defense. It will screen all HTTP and HTTPS requests and direct them to the proper web section on the IIS web

⁹ <http://www.ca.com>

server. Concerning DNS, the split DNS architecture was used. This means that the Internet will only know what is publicly accessible for them and nothing else. The internal network information will not be made available. The DNS server in the DMZ will be non-recursive where as the internal DNS server will be recursive. This means that the DMZ DNS server cannot be used by the Internet to do lookup queries. It will be configured to forward internal queries from GIAC out to the Internet. All logging will be done to a central location. Time will be kept current by a central NTP server so that all logging is accurate with reference to time. VPN access utilized 2 factor authentication and SSL for encryption. A Snort sensor was setup to sniff for any intrusions and a dedicated intrusion network was setup to keep it private and secure. All email will be filtered for viruses and all attachments will be checked before they are allowed to enter the internal network. Certain attachments will be blocked. The internal mail server will also have anti-virus protection for the box itself and protection for the information store. All servers and desktops will have the latest anti-virus signatures on them. Auditing will be installed on all servers and monitored. A baseline will be performed so that normal traffic will be known and a baseline of all servers will be completed. Tripwire will be installed on all Linux servers to monitor critical files.

All servers located in the DMZ and in the internal network will have Etrust Audit installed for real-time auditing.

Assignment 2 - Security Policy and Component Configuration

Border Router Security Policy and Component Configuration

The Cisco 2621 using IOS 12.2(21) will be used.

We will use the NSA Router Security Configuration Guide to configure our router for optimum security. This guide is available at http://www.nsa.gov/snac/routers/cisco_scg.pdf¹⁰

The border router will be our first line of defense against attackers from the Internet. The border router will use static filtering to screen ingress and egress traffic. The security policy for our border router will meet the following objectives.

Protect the router

Protect the internal networks with the router

Protect the router

Physically securing the router.

This is important because if any unauthorized person gets physical access, they can easily do a password recovery procedure on the router and change the password and then be

¹⁰ NSA Router Security, http://www.nsa.gov/snac/routers/cisco_scg.pdf

able to launch attacks once they get access to the console prompt. The router will be placed in a secure server room with console access only by a standalone desktop.

The following commands will limit which hosts or networks can access the router

```
Access-list 10 permit 192.168.5.0 0.0.0.255
  Line vty 0 4
  Access-class 10 in
  Password <password>
  Login
```

The following command will ensure that an automatic timeout will occur after 5 minutes of being idle.

```
Line con 0
  exec-timeout 5 0
```

Authorized users should be the only ones logging in and they should have an account. The following command enforces user log. Be sure user accounts are already created before issuing the login local command.

```
Line con 0
  Login local
```

The auxiliary port should be disabled.

```
Line aux 0
  Login local
  Exec-timeout 0 1
  No exec
```

Passwords will be encrypted.

```
Service password-encryption
Enable secret 5 <password>
```

Using a current stable IOS version.

It is important to use an IOS version that has the “GD” (general deployment) rating. This signifies that the IOS has been tried and proven by customers. So reliability and stability are obtained by using an IOS with this rating. More information can be obtained at http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e06.html.¹¹

Configuration hardening.

¹¹ Cisco IOS,
http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e06.html

It is important to turn off services not required so that an attacker cannot use the service for information gathering or exploitation.

The Cisco Discovery Process is used for identify each router to each other on a network. We will turn this feature as it is not needed and will enhance our security.

No CDP run

Source routing will be turned off as it can be used to exploit our network. An attacker can spoof an internal network IP address. With source routing on, the attacker can then dictate the route back to the spoofing host.¹² Using the following command will turn off source routing.

No IP source-route

The following services are not used and there use could potentially open up security risks. These services will be turned off.

No service tcp-small-serv
No service udp-small-serv
No ip finger
No service finger
No ip bootp server
No ip http server
No ip name-server
No ip domain-lookup
No snmp-server

Cisco routers can load their configuration over the network. This feature will be turned off.

No boot network
No service config

A banner will be added to warn intruders

Banner /
Authorized Use Only
/
Log traffic to syslog server
Logging 192.168.8.2

¹² SANS Track 2 – Firewalls, Perimeter Protection and VPN's, 2-1 TCP/IP for Firewalls Pg 8-25.

Protecting the Network with the Router

Ingress and egress filtering will be put in place to allow or deny certain traffic. Packet filtering will accomplish this by applying ACL rules. Ingress filtering will prevent spoofing, SMURF attacks, DoS to name a few. Egress filtering will block outbound spoofing, will ensure GIAC is a good net neighbor and will block critical services that should never get out on the Internet. The order and the length of the rules are important. Rules are processed from top to bottom. Once a rule is matched, the rest of the list is ignored. More general rules that process the bulk of the traffic should be placed at the top. More specific rules should be placed towards the bottom of the list. If the rule list gets too long, router performance can be affected. Therefore it will be important to select a router that has sufficient power to handle the necessary filter rules that need to be in place to protect the internal networks. Also it must be understood that once an access list is applied to an interface, all traffic will be dropped so it is important that a “permit” rule is placed after all the deny’s. Also only one access list can be applied to one interface in one direction.¹³ With the SANS top 20 vulnerabilities in mind, extended access lists will only be used on GIAC’s border router interfaces.

Access lists are grouped into several categories. Access lists beginning with the number 1 thru 99 or called standard access lists. Also note that standard IP access lists were also extended to use 1300-1399 for IOS 12.1 and greater.¹⁴ They are useful for filtering source addresses. Extended access lists are numbered from 100 thru 199. These extended access lists are useful for filtering source and destination sources and can also filter on specific protocols and on specific ports.

Ingress Filter.

Note: The following rules are placed on the serial interface in the order shown. They will be processed from top to bottom.

Clear the access list and build a new one

```
No access-list 100
```

Deny traffic to router itself

```
Access-list deny ip any host <ext ip address of rtr> log
```

All private IP addresses are filtered out with the below rules

```
Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
Access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
Access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
```

Loop back IP is filtered out.

```
Access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
```

¹³ SANS Track 2 – Firewalls, Perimeter Protection and VPN’s, 2-1 TCP/IP for Firewalls

¹⁴ Managing CISCO Network Security, pg 51 Syngress

Broadcast address is filter out

```
Access-list 101 deny ip <ext ip address of rtr.0> 0.0.0.255 any log
Access-list 101 deny ip <ext ip address of rtr.255> 0.0.0.255 any log
```

Unallocated source IP addresses are filtered out below. A complete list of unallocated IP addresses can be found at <http://www.iana.org/assignments/ipv4-address-space>

```
Access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
Access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
Access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
Access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
Access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
...
Access-list 101 deny ip 255.0.0.0 0.255.255.255 any log
```

Multicast traffic is filtered out.

```
Access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
```

Critical services are filtered at the perimeter.

Access-list 101 deny tcp any any range 135 139 log	(NetBios traffic)
Access-list 101 deny udp any any range 135 139 log	(NetBios traffic)
Access-list 101 deny tcp any any 445 log	(SMB Win2K)
Access-list 101 deny udp any any 69 log	(TFTP)
Access-list 101 deny udp any any 514 log	(SYSLOG)
Access-list 101 deny udp any any range 161 162 log	(SNMP)
Access-list 101 deny icmp any any host-redirect echo	(ICMP traffic)

The following rule permits traffic to flow in.

```
Access-list 101 permit ip any any
```

Finally the ingress filter will be applied to the serial interface

```
Interface serial0/0
  Access-group 101 in
```

Egress Filtering.

```
Access-list 102 deny tcp any any range 135 139 log
Access-list 102 deny udp any any range 135 139 log
Access-list 102 deny tcp any any 445 log
Access-list 102 deny udp any any 69 log
Access-list 102 deny udp any any 514 log
Access-list 102 deny udp any any range 161 162 log
Access-list 102 deny icmp any any echo-reply
Access-list 102 deny icmp any any host unreachable
Access-list 102 deny icmp any any time exceeded
```

```
Access-list 102 permit nmh.10.23.9 0..0.0.255
Access-list 102 deny any log
```

For egress filtering, the access list will be applied to the internal Ethernet interface.

```
Interface Ethernet 0
    Access-group 102 in
```

On all the router interfaces the following will be applied.

```
No ip proxy-arp
Prevent layer 3 to layer 2 broadcast mapping and smurf amplification.
No ip directed-broadcast
Stop ICMP unreachable messages
No ip unreachable
No ip redirect
Ntp disable
```

Finally any unused interfaces will be shutdown.
Shutdown

Primary Firewall Security Policy and Component Configuration

The security policy for the firewall should meet the following goals

1. No direct connections from the Internet to the internal network. In other words, proxy all traffic. The objective here is to secure the network.
2. No direct connections to the interfaces of the firewall except only that internal computer that is allowed to manage the firewall. The objective here is to secure the firewall.
3. Control the flow of traffic
4. Protect the internal network by concealment
5. Log all necessary traffic and have it sent to the centralized Syslog server.
6. No ICMP traffic allowed from the Internet to the firewall.
7. Blocking of all top 10 traffic threats listed in the SANS TOP 10 Threats¹⁵. The border router took care of most of this traffic.
8. Be a good Internet neighbor.
9. Although not done by this firewall, but the internal firewall will proxy all outbound user http traffic.

All traffic for the primary external firewall will first be identified as shown in the tables below.

¹⁵ <http://www.sans.org/top20/>

Inbound from Internet

Source	Destination	Service	Protocol	Port
Public (any)	192.168.7.9	http	Tcp	80
Customers (any)	192.168.7.9	https	Tcp	443
Suppliers	192.168.7.9	https	Tcp	443
Partners	192.168.7.9	https	Tcp	443
any	192.168.7.6	Dns	Udp	53
any	192.168.7.6	DNS	Tcp	53
any	192.168.7.7	Smtpt	Tcp	25
Syslog (border rtr)	192.168.8.2	syslog	udp	514
VPN Citrix	192.168.7.5	https	Tcp	443

Outbound to Internet

Source	Destination	Service	Protocol	Port
Xwall	Any	SMTP	Tcp	25
Ext DNS	Any	DNS	udp	53
Ext DNS	Any	DNS	Tcp	53
Int Network	Any	Any	Any	Any
NTP Server	Stratum server	NTP	Tcp/UDP	123

Configuring and hardening the firewall.

Astaro Firewall is locked down when installed. This is a nice feature of this firewall as some firewalls such as IPCOP allows all outbound traffic upon installation.

Installation of Astaro Linux is very straightforward and simple. During the installation, one of the required items is to designate the internal IP address. This IP address will be accessed after the install to configure the firewall. The IP address for the internal interface of GIAC's firewall is 192.168.7.1. So to configure this firewall, the following URL will be surfed to. <https://192.168.7.1>

The first thing that will need to be configured is to assign an admin password as shown.

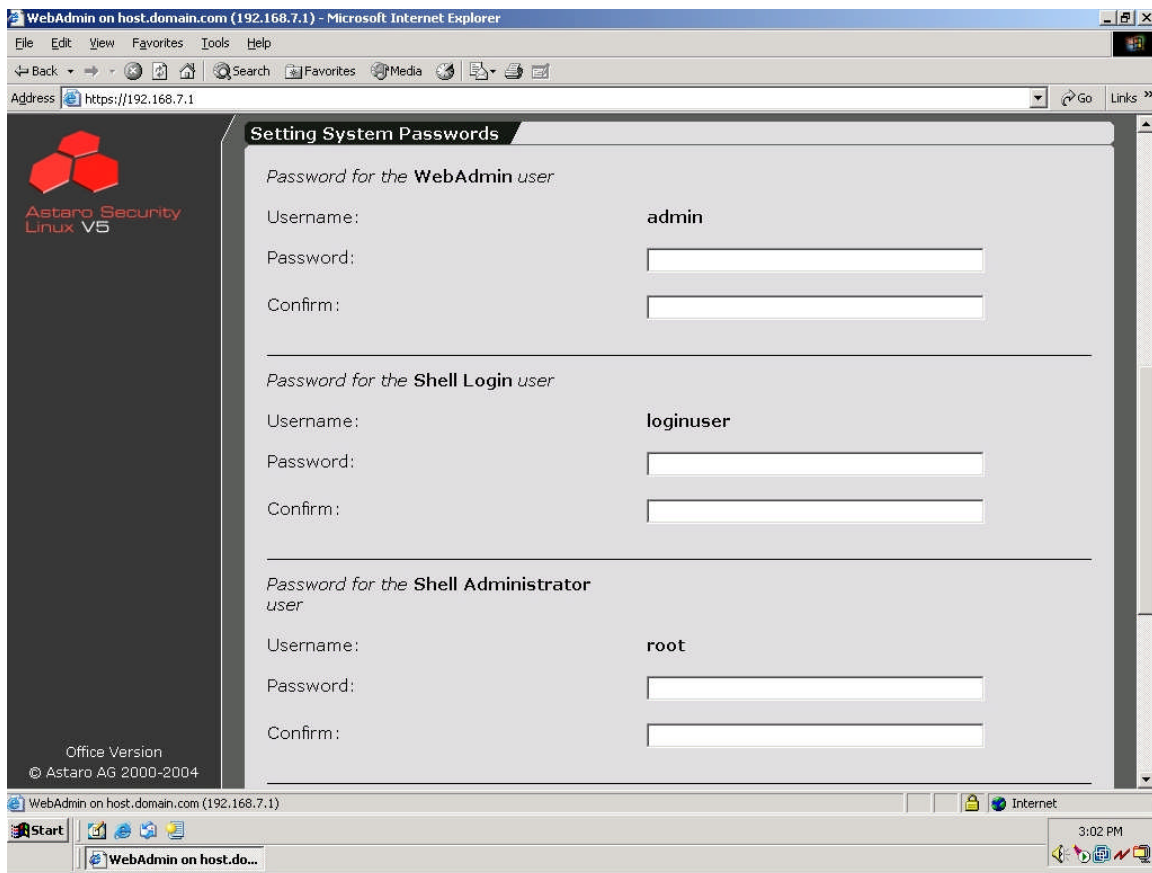


Figure 1

Also the Shell Login user and Shell Administrator passwords will be required. The Shell Login user is for the purpose of Ssh and the Shell Administrator is “root” which is only allowed to physically logon on to the server itself. Passwords will be lengthy and complex for optimum security. Note that SSL encryption is utilized to administer this firewall for added protection.

After assigning the passwords, the rest of the configuration can be done. Below is the menu with the configuration choices.

	System
	Definitions
	Network
	Intrusion Protection
	Packet Filter
	Proxies
	IPSec VPN
	Reporting
	Local Logs
	Online Help
	Exit

Figure 2

Starting with “System” the following menu choices are available as shown below.

Settings
Licensing
Up2Date Service
Backup
SNMP Access
Remote Syslog
User Authentication
WebAdmin Settings
WebAdmin Site Certificate
High Availability
Shut down/Restart

Figure 3

First thing that needs to be done is to update the firewall. This is required to make sure the firewall has the latest patches and is secure. But before we can do that, the external interface must be configured as shown below.

Current Interface Status				New ...
Admin	Oper	Name/Type	Parameters	Actions
<input checked="" type="checkbox"/>	Up	Astaro_DMZ_Interface (Standard ethernet interface) on eth0	192.168.7.1 / 255.255.255.0 Gateway: none	edit delete
<input checked="" type="checkbox"/>	Up	Astaro_External_Interface (Standard ethernet interface) on eth1	211.10.23.10 / 255.255.255.248 Gateway: 211.10.23.9	edit delete
Hardware List				
Sys ID	Name/Parameters			PCI Device ID
eth0	Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] irq=10 type=eth mac=00:0c:29:51:e9:a7			
eth1	Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] irq=9 type=eth mac=00:0c:29:51:e9:b1			
eth2	Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] irq=5 type=eth mac=00:0c:29:51:e9:bb			

Figure 4

Once the interfaces are good, it is time to update the firewall.

Prefetch Up2Dates now: Click "Start" to prefetch available system Up2Date packages now Start

Prefetch Up2Dates automatically: ☒ Disable

Interval: Every day

Import from File: Browse... Start

Unapplied Up2Dates		
Version	File Name	Actions
5.011	5.011.tar.gpg	[install]
5.012	5.012.tar.gpg	[install]
5.013	5.013.tar.gpg	[install]
5.014	5.014.tar.gpg	[install]
5.015	5.015.tar.gpg	[install]
5.016	5.016.tar.gpg	[install]
5.017	5.017.tar.gpg	[install]

Figure 5

As shown, there are some updates available right away to be applied. Clicking the “start” button will fetch any available Up2Date packages. After they are all fetched, then simply click the “install” button next to each package to install.

Next access to the firewall for administration purpose will be secured as shown below. A network host object will be created for the desktop that will administer this machine.

Access and Authentication

Allowed Networks:

Selected	Available
firewall admin machine	Any external (Address) external (Broadcast) external (Network) External SMTP Relay

Authentication Methods:

1 ☒ Local Users ⚙️

Allowed Users:

Selected	Available
admin	phil

Figure 6

Note that only one user is currently allowed to access the firewall. Should there be more than one user, more users can easily be added. Should that be the scenario, the best practice would be to create a user for each person who will administer the firewall and then to remove the admin user. This way there is accountability for each administrator who changes the firewall policy as all changes can be logged.

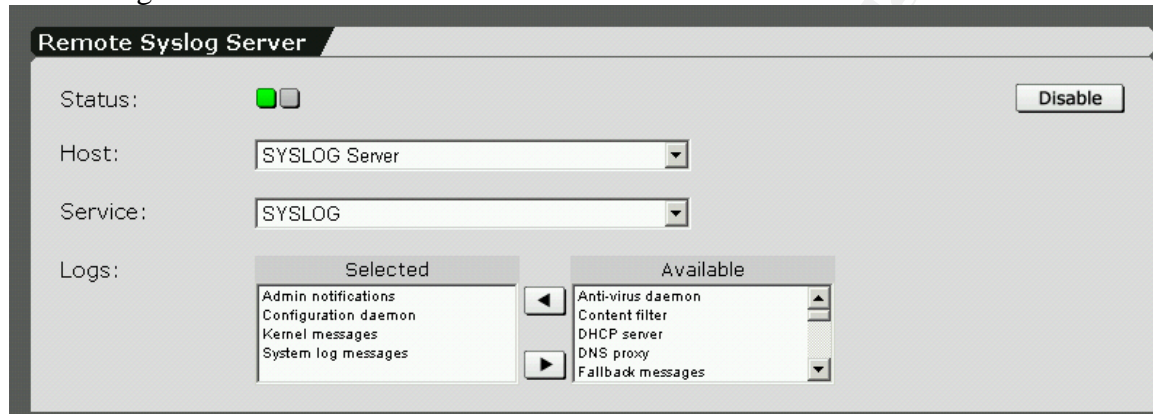
Under “Settings” the time zone will be set to the local time zone.
Also note that the NTP server in the DMZ is setup here also to maintain correct time.



The Time Settings window shows two dropdown menus. The first is labeled "Time Zone:" and has "America - Chicago" selected. The second is labeled "Use NTP Server:" and has "NTP Server" selected.

Figure 7

Next the syslog server will be specified. Note that there is a quite a list of items to choose from to log.



The Remote Syslog Server window has a "Status:" section with a green square and a "Disable" button. Below are "Host:" and "Service:" dropdown menus, both set to "SYSLOG Server" and "SYSLOG" respectively. The "Logs:" section contains two lists: "Selected" and "Available". The "Selected" list includes "Admin notifications", "Configuration daemon", "Kernel messages", and "System log messages". The "Available" list includes "Anti-virus daemon", "Content filter", "DHCP server", "DNS proxy", and "Fallback messages". Arrows between the lists allow for moving items.

Figure 8

Now all ICMP traffic will be turned off. By default most of this traffic is off.



This block contains three separate settings windows. The "ICMP Settings" window has three rows: "ICMP Forwarding:", "ICMP on Firewall:", and "Log ICMP Redirects:", each with a red square and an "Enable" button. The "Traceroute Settings" window has three rows: "Firewall is Traceroute visible:", "Firewall forwards Traceroute:", and "Traceroute from Firewall:", each with a red square and an "Enable" button. The "Ping Settings" window has three rows: "Firewall is Ping visible:", "Firewall forwards Pings:", and "Ping from Firewall:", each with a red square and an "Enable" button.

Figure 9

Set the hostname for the firewall as shown below.

Figure 10

Now all that is left is to define the network objects and create the rule base. This completes the configuration portion of setting up the firewall.

Creating the Rule Base

Referring to figure 2, under “Definitions”, all network objects will be created. There are five types of network objects that can be created.

Host – used for specifically defining servers and desktops.

Network - used to identify the different networks in your enterprise







Network group – used to group the various networks. For example all RFC1918 networks can be grouped under “Private Networks”

DNS hostname – used with dynamic DNS... not used.










IPSEC user group – used for incoming IPSEC traffic... not used.







































































The following network objects will be created and they will be used in the rule base.

Network Definitions				Total 22 entries	▽ New Definition ... ▽	▽ Filters ▽
▽ Name		Value		Comment		
All Networks		255.255.255.255/32		Broadcast to all networks		
Any		0.0.0.0/0		[none]		
Astaro_DMZ_Interface (Address)		Interface up	192.168.7.1	Address of interface 'Astaro_DMZ_Interface'		
Astaro_DMZ_Interface (Broadcast)		Interface up	192.168.7.255	Broadcast address on interface 'Astaro_DMZ_Interface'		
Astaro_DMZ_Interface (Network)		Interface up	192.168.7.0/24	Network on interface 'Astaro_DMZ_Interface'		
Astaro_External_Interface (Address)		Interface up	211.10.23.10	Address of interface 'Astaro_External_Interface'		
Astaro_External_Interface (Broadcast)		Interface up	211.10.23.15	Broadcast address on interface 'Astaro_External_Interface'		
Astaro_External_Interface (Network)		Interface up	211.10.23.8/29	Network on interface 'Astaro_External_Interface'		
Border Router		211.10.23.9		Border Router		
DMZ DNS Server		192.168.7.6		DNS server in DMZ		
DMZ SMTP Server		192.168.7.4		SMTP Server in DMZ		
firewall admin machine		192.168.7.20		[none]		
IPCOP External Interface		192.168.7.2		IPCOP external interface		
IPCOP Internal Interface		10.10.5.1		IPCOP Internal Interface		
NFUSE Web Interface		192.168.7.5		Frontend to Citrix		
NTP Server		192.168.6.9		Server to keep time on network		
ntp3.tamu.edu		128.194.254.9		Time Server from which to get time from		
PPTP-Pool		10.68.59.0/24		Autogenerated random PPTP-Pool network.		
Public Website		192.168.7.3		www.giacenterprises.com		







 Reverse Proxy Server	 192.168.7.9	Reverse Proxy Server with Jeanne
 Syslog Network	 192.168.8.0/24	Syslog Network
 SYSLOG Server	 192.168.8.2	IDS Management/Syslog Server

Below is the completed rule set. The rules are processed from top to bottom. The order of the rules is very important. The more specific rules are placed towards the top and then works down to the more general rules. This will make processing the rules more efficient and not consume so much cpu processor power. Astaro like Checkpoint firewalls, have implied rules built in. ICMP traffic is one such rule. The best practice here is to turn off all ICMP traffic at the menu configuration and use rules to allow or deny ICMP traffic. Also it should be noted that Astaro puts in anti-spoofing rules for every internal network that is created. Underneath Astaro is simply iptables. Astaro just provides a very nice front-end to quickly configure a hardened firewall.

Packet Filter Rules									
Total 23 entries					▽ New Rule ... ▽		▽ Filters ▽		Live Log
	Δ	Group		Source	Service	Action	Destination		Comment
	1	[none]		firewall admin machine	 HTTPS		 Astaro_DMZ_Interface (Address)		Allow admin machine to manage firewall by secure web browser
	2	[none]		firewall admin machine	 ping-request		 Astaro_DMZ_Interface (Address)		Allow admin machine to ping firewall
	3	[none]		firewall admin machine	 SSH		 Astaro_DMZ_Interface (Address)		Allow admin machine to ssh to firewall
	4	[none]		Any	 Any		 Astaro_External_Interface (Address)		Drop any traffic directed at external interface
	5	[none]		Any	 Any		 Astaro_DMZ_Interface (Address)		Drop any traffic directed at internal interface
	6	[none]		Astaro_DMZ_Interface (Network)	 Any		 Astaro_DMZ_Interface (Broadcast)		All DMZ broadcasts dropped
	7	[none]		Astaro_DMZ_Interface (Network)	 Any		 All Networks		All Network broadcasts dropped (DHCP and Bootp requests)
	8	[none]		Astaro_DMZ_Interface (Network)	 NetBIOS/IP Services		 Any		Drop any DMZ outbound Netbios traffic 135:139
	9	[none]		Astaro_DMZ_Interface (Network)	 TFTP		 Any		Drop any DMZ outbound TFTP traffic

10	[none]		Astaro_DMZ_Interface (Network)		SYSLOG			Any		Drop any DMZ outbound Syslog traffic
11	[none]		IPCOP External Interface		Any			Any		Allow internal users out to internet
12	[none]		Border Router		SYSLOG			SYSLOG Server		Allow border router logs to get to syslog server
13	[none]		Any		DNS			DMZ DNS Server		Internet access to DMZ DNS server
14	[none]		Any		HTTP			Reverse Proxy Server		Internet access to public website
15	[none]		Any		HTTPS			Reverse Proxy Server		Internet secure access to website
16	[none]		Any		SMTP			DMZ SMTP Server		Internet access to DMZ mail server
17	[none]		Any		HTTPS			Citrix Web Interface		VPN access to Citrix
18	[none]		Any		NetBIOS/IP Services			Any		Drop inbound NetBIOS traffic
19	[none]		Any		IDENT			DMZ SMTP Server		Reject IDENT to DMZ SMTP Server
20	[none]		DMZ NTP Server		NTP			ntp3.tamu.edu		Allow NTP server to get time
21	[none]		DMZ DNS Server		DNS			Any		Allow Outbound DNS traffic
22	[none]		DMZ SMTP Server		SMTP			Any		Allow Outbound SMTP traffic
23	[none]		Any		Any			Any		Drop and log any other traffic not allowed

This is the NAT rules..













NAT Rules					SRC Translation		DST Translation		Actions	
State	Name	Match Parameters								
	Citrix Frontend	Any -> Astaro_External_Interface (Address) / HTTPS			None		Citrix Web Interface		edit	delete
	DMZ DNS Server	Any -> Astaro_External_Interface (Address) / DNS			None		DMZ DNS Server		edit	delete
	DMZ NTP Server	ntp3.tamu.edu -> Astaro_External_Interface (Address) / NTP			None		DMZ NTP Server		edit	delete
	DMZ SMTP Server	Any -> Astaro_External_Interface (Address) / SMTP			None		DMZ SMTP Server		edit	delete
	Reverse Proxy Server	Any -> Astaro_External_Interface (Address) / HTTPS			None		Reverse Proxy Server		edit	delete
	Router syslogs	Border Router -> Astaro_External_Interface (Address) / SYSLOG			None		SYSLOG Server		edit	delete

Nat rules 1, 2, 4 and 5 allow for proper translation to access the private addressed web servers from the Internet.






















Nat rule 3 allows for proper translation for accessing the private addressed NTP server.

Nat rule 6 allows the border router to translate properly in route to the syslog server.

Breaking down and explaining each rule are as follows.

1	[none]		firewall admin machine		HTTPS		Astara_DMZ_Interface (Address)		Allow admin machine to manage firewall by secure web browser
2	[none]		firewall admin machine		ping-request		Astara_DMZ_Interface (Address)		Allow admin machine to ping firewall
3	[none]		firewall admin machine		SSH		Astara_DMZ_Interface (Address)		Allow admin machine to ssh to firewall

Rules 1 thru 3 allow the designated admin machine to manage the firewall. All traffic to the firewall is encrypted. Note also that the admin machine is also allowed to ping the firewall for maintenance and troubleshooting purposes. The rest of the users on the network are not allowed to ping the firewall. This traffic is logged.

4	[none]			Any	Any		Astara_External_Interface (Address)		Drop any traffic directed at external interface
5	[none]			Any	Any		Astara_DMZ_Interface (Address)		Drop any traffic directed at internal interface
6	[none]		Astara_DMZ_Interface (Network)		Any		Astara_DMZ_Interface (Broadcast)		All DMZ broadcasts dropped
7	[none]		Astara_DMZ_Interface (Network)		Any		All Networks		All Network broadcasts dropped (DHCP and Bootp requests)
8	[none]		Astara_DMZ_Interface (Network)		NetBIOS/IP Services		Any		Drop any DMZ outbound Netbios traffic 135:139
9	[none]		Astara_DMZ_Interface (Network)		TFTP		Any		Drop any DMZ outbound TFTP traffic
10	[none]		Astara_DMZ_Interface (Network)		SYSLOG		Any		Drop any DMZ outbound Syslog traffic

Rules 4 thru 10 all drop traffic.

Rules 4 and 5 drops any traffic directed at either interface of the firewall. Only the admin machine designated in the previous rules is allowed to access the internal interface of the firewall.











































Rules 6 and 7 drops broadcast traffic and specifically bootp and DHCP traffic, which will broadcast to all networks. Notice that this traffic is not logged as this kind of traffic could fill up our syslog server in a hurry.

Rule 8 drops any outbound NetBIOS traffic. This will also be dropped at the border router but it does not hurt to be thorough and adds another layer of making sure we are being good Internet neighbors. This traffic is logged.

Rule 9 drops any outbound TFTP traffic. Again the border router is also configured to drop this traffic also. Any sign of this traffic usually means trouble and should be looked

at quickly. The only reason some would be using TFTP is if a hacker compromised one of our boxes and was attempting to get a root kit or some other executables. This traffic is logged.

Rule 10 drops any outbound SYSLOG traffic. Syslog traffic is only allowed in the direction of our syslog server. This traffic is also blocked at the router but it does not hurt to be paranoid. This traffic is logged.

	11	[none]		IPCOP External Interface		Any			Any		Allow internal users out to internet
	12	[none]		Border Router		SYSLOG			SYSLOG Server		Allow border router logs to get to syslog server
	13	[none]		Any		DNS			DMZ DNS Server		Internet access to DMZ DNS server
	14	[none]		Any		HTTP			Reverse Proxy Server		Internet access to public website
	15	[none]		Any		HTTPS			Reverse Proxy Server		Internet secure access to website
	16	[none]		Any		SMTP			DMZ SMTP Server		Internet access to DMZ mail server
	17	[none]		Any		HTTPS			NFUSE Web Interface		VPN access to Citrix

Rule 11 allows our internal users access to the Internet. Note that before the users are allowed out that all traffic that needed to be dropped such as NetBIOS and TFTP was dropped before letting the users out. All internal users will have the IP of the IPCOP external interface. IPCOP proxy's all web traffic for the internal users. This traffic is logged.

Rule 12 allows the border router Syslog logs to travel thru the firewall onto their destination of the Syslog Server, which is behind the IPCOP firewall. This traffic is logged.

Rule 13 allows the Internet to resolve names against GIAC's DMZ DNS server using only the DNS service. This traffic is logged.

Rule 14 allows anyone to browse to port 80 on the public web server but only after they have been filtered thru the reverse proxy server. This traffic is logged.

Rule 15 allows anyone who has been directed to a secure connection to access the website but again only after being filtered by the reverse proxy server. This traffic is logged.

Rule 16 allows the Internet to send email to GIAC's DMZ SMTP server. This traffic is logged.

Rule 17 allows GIAC's VPN users to access the front end of the Citrix server. This traffic is logged.

18	[none]		Any	NetBIOS/IP Services		Any	Drop inbound NetBIOS traffic
19	[none]		Any	IDENT		DMZ SMTP Server	Reject IDENT to DMZ SMTP Server

Rule 18 drops any inbound NetBIOS traffic. This traffic should have already been dropped at the border router but it does not hurt to have layered defense. Since this kind of traffic can fill logs, it was determined not to log this traffic.

Rule 19 rejects any Ident that our outbound SMTP may begin. This could potentially cause delays on outbound mail delivery. This traffic is logged.

20	[none]		DMZ NTP Server	NTP		ntp3.tamu.edu	Allow NTP server to get time
21	[none]		DMZ DNS Server	DNS		Any	Allow Outbound DNS traffic
22	[none]		DMZ SMTP Server	SMTP		Any	Allow Outbound SMTP traffic
23	[none]		Any	Any		Any	Drop and log any other traffic not allowed

Rule 20 allows the NTP server to get updated time from the designated stratum 3 NTP server. This traffic is logged

Rule 21 allows outbound DNS for the GIAC network. Note that IPCOP will only allow the internal DNS server to forward requests only to the DNS server in the DMZ. (This is not shown, as this rule would be located in the IPCOP rule set). This traffic is logged.

Rule 22 allows outbound email to the Internet from the DMZ SMTP server. This traffic is logged.

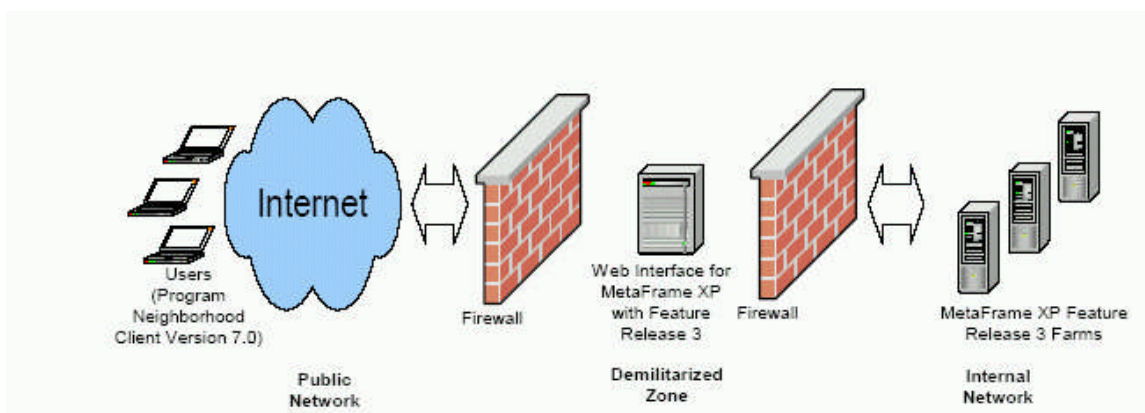
Rule 23 drops any other traffic not allowed. The traffic will be logged.

VPN Policy

GIAC Enterprise VPN solution will be accomplished using Citrix MetaFrame XP architecture.¹⁶ Below is an example diagram showing a high level view of the VPN solution.

GIAC Enterprise's mobile sales force will use their web browser to access the designated Citrix web interface. The connection will be totally secured using SSL. This solution gives the sales force complete mobility in accessing resources back at the corporate office.

¹⁶ <http://www.citrix.com>

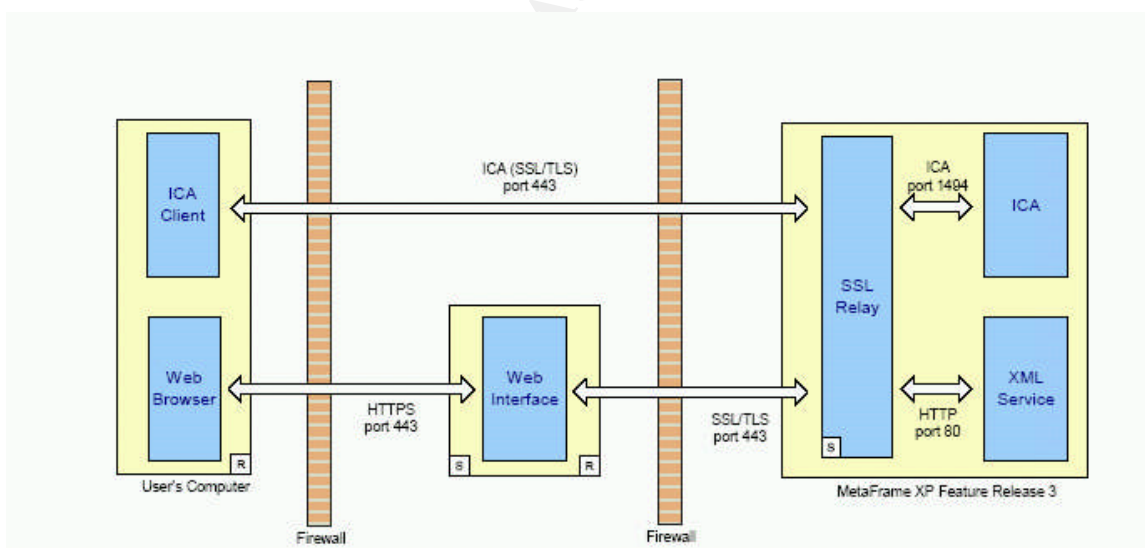


17

The clients will require client software called ICA (Independent Computing Architecture). This client can easily be downloaded when accessing the VPN website the first time. Or it can be downloaded from the Citrix website.

To further strengthen the VPN solution, two-factor authentication will be used by utilizing RSA SecurID token from RSA Security. Two factor authentication deals with combining something the user knows with something the user has.¹⁸

Below is an example showing how the communication between the client and the Web Interface takes place.



19

Note that the client uses https traffic (SSL) over port 443 to access the web interface located in the DMZ. The client will then logon to the front-end using their username, password, domain and then their PASSCODE. This is the SecurID token that is generally

¹⁷ <http://whitepapers.zdnet.co.uk/0,39025945,60081408p-39000457q,00.htm>

¹⁸ <http://www.rsasecurity.com/node.asp?id=1173>

¹⁹ <http://whitepapers.zdnet.co.uk/0,39025945,60081408p-39000457q,00.htm>

setup to require a 4-digit pin and the 6-digit passcode displayed on the token. An example is shown below.

The web interface will then communicate to the backend Citrix server using SSL. The Citrix server and the client then respond back and forth using the ICA protocol over SSL.

The user will browse to <https://www.giacenterprisesapps.com> and will be shown the below.



After authenticating, the client will have access to all the applications made available to that client. The client will be able to access all email, and perform all normal tasks that are published to the client.

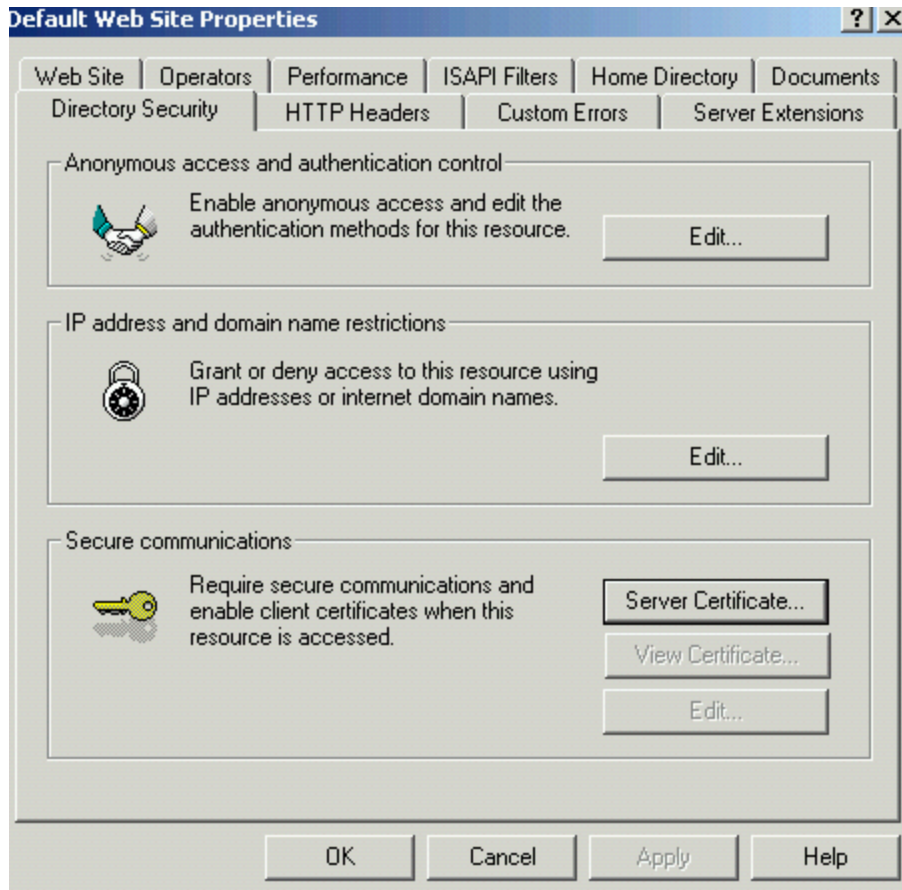
Configuring the VPN solution.

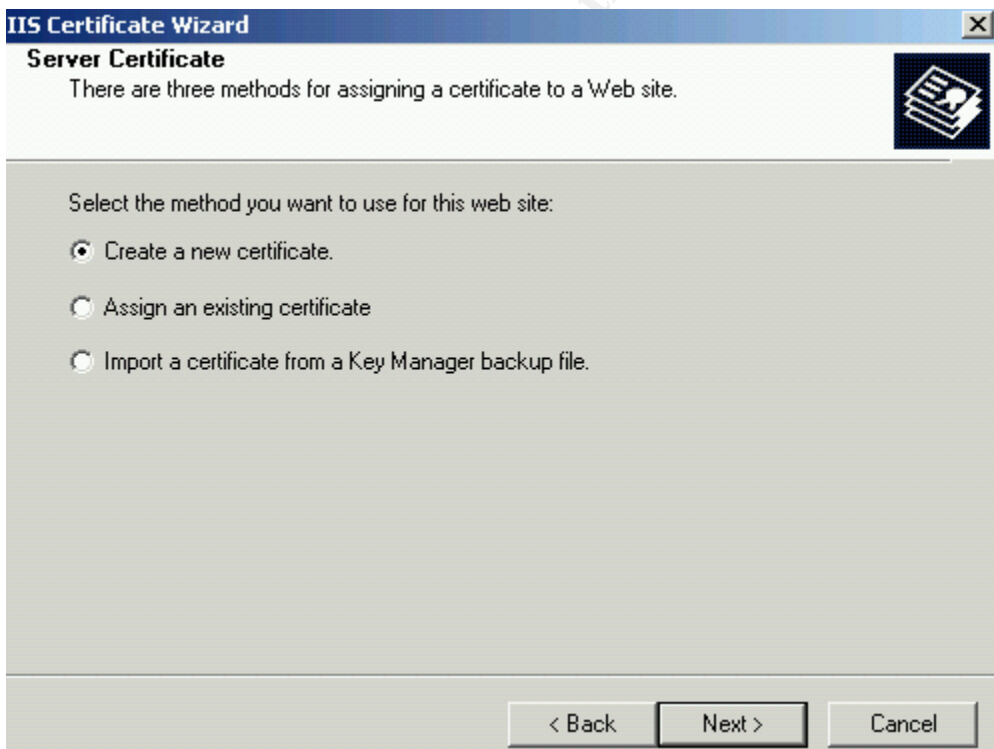
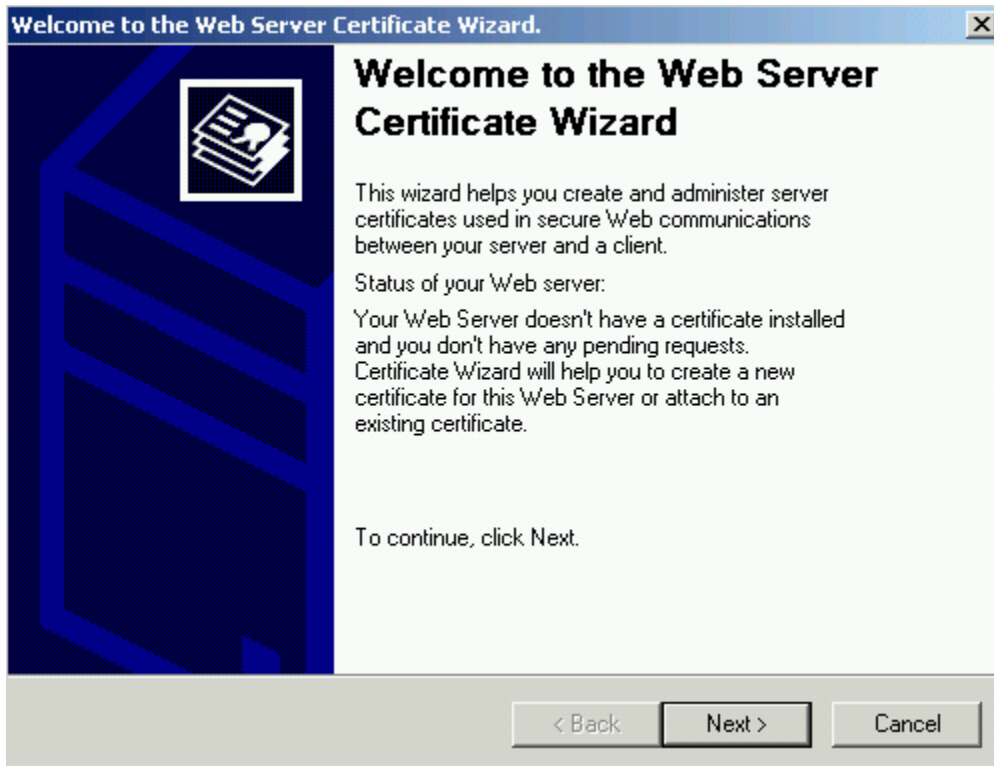
The configuration of the VPN solution will assume that the Citrix server farm and that the RSA Server database has already been installed and configured. This configuration will be for the Web Interface located in the DMZ.

Windows 2000 with the latest service pack running IIS 5.0 will be installed on a server. The server will then be hardened and locked down. There are numerous documents on the web on how to harden and lock down a Windows 2000 server. One such site is http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1²⁰

²⁰ http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1

SSL will now be configured for the IIS server. A certificate must be generated to accomplish this. Open up Internet Service Manager and right click on the website ->properties and click on the "Directory Security" tab.





IIS Certificate Wizard

Delayed or Immediate Request

You can prepare a request to be sent later, or you can send one immediately.

Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

☒ Prepare the request now, but send it later

☐ Send the request immediately to an online certification authority

< Back Next > Cancel

IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

GiacEnterpriseApps

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length:

1024

☐ Server Gated Cryptography (SGC) certificate (for export versions only)

< Back Next > Cancel

IIS Certificate Wizard [X]

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:
GiacEnterprises.com

Organizational unit:
GiacEnterprises.com

< Back Next > Cancel

IIS Certificate Wizard [X]

Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:
GIAC_VPN

< Back Next > Cancel

IIS Certificate Wizard [X]

Geographical Information

The certification authority requires the following geographical information.

Country/Region:
US (United States) [v]

State/province:
Texas [v]

City/locality:
Austin [v]

State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back Next > Cancel

IIS Certificate Wizard [X]

Certificate Request File Name

Your certificate request is saved as a text file with the file name you specify.

Enter a file name for the certificate request.

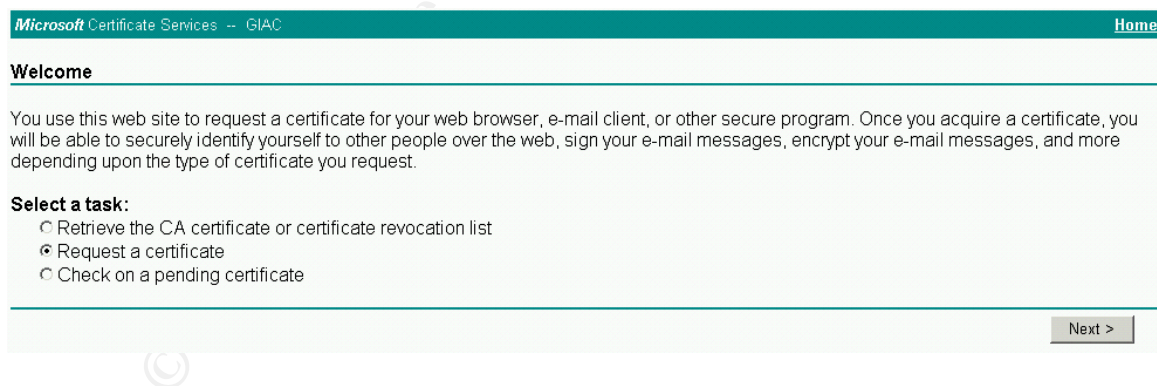
File name:
c:\certreq.txt [v] Browse...

< Back Next > Cancel



Now to process the certificate request, I need a CA (Certificate of Authority). Just so happens that with Windows 2000, that is easily accomplished by simply installing the certificate services.

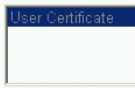
Once the CA has been installed, the request can now be processed,



Choose Request Type

Please select the type of request you would like to make:

☐ User certificate request



☒ Advanced request

Next >

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

☐ Submit a certificate request to this CA using a form.

☒ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

☐ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

Microsoft Certificate Services -- GIAC

Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
AAAAwDQYJKoZIhvcNAQEFBQADgYEAZtoYXSP2uFk4
/CChbIBOHuwjQyBPd5C3RxKNYXLb6nFO5EXMc3xX
tt3MQ4HoEaeD3Qx2mv2FT/t5K8AVXi6UteATeZV/
HSCZdp0=
-----END NEW CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Microsoft Certificate Services -- GIAC

Home

Certificate Issued

The certificate you requested was issued to you.

☒ DER encoded or ☐ Base 64 encoded




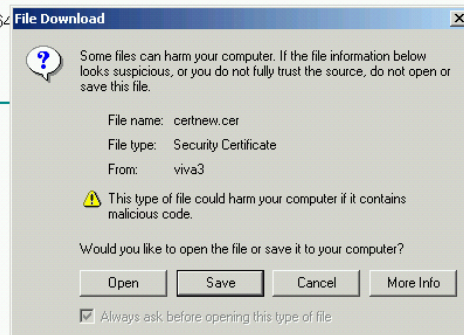
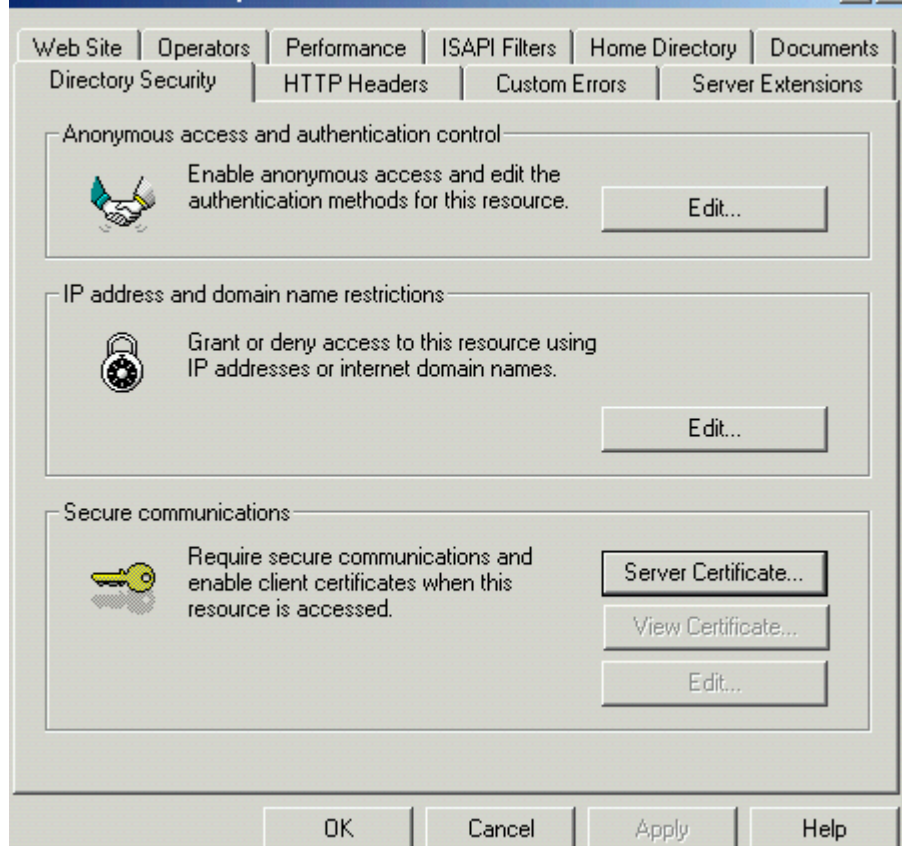
[Download CA certificate](#)

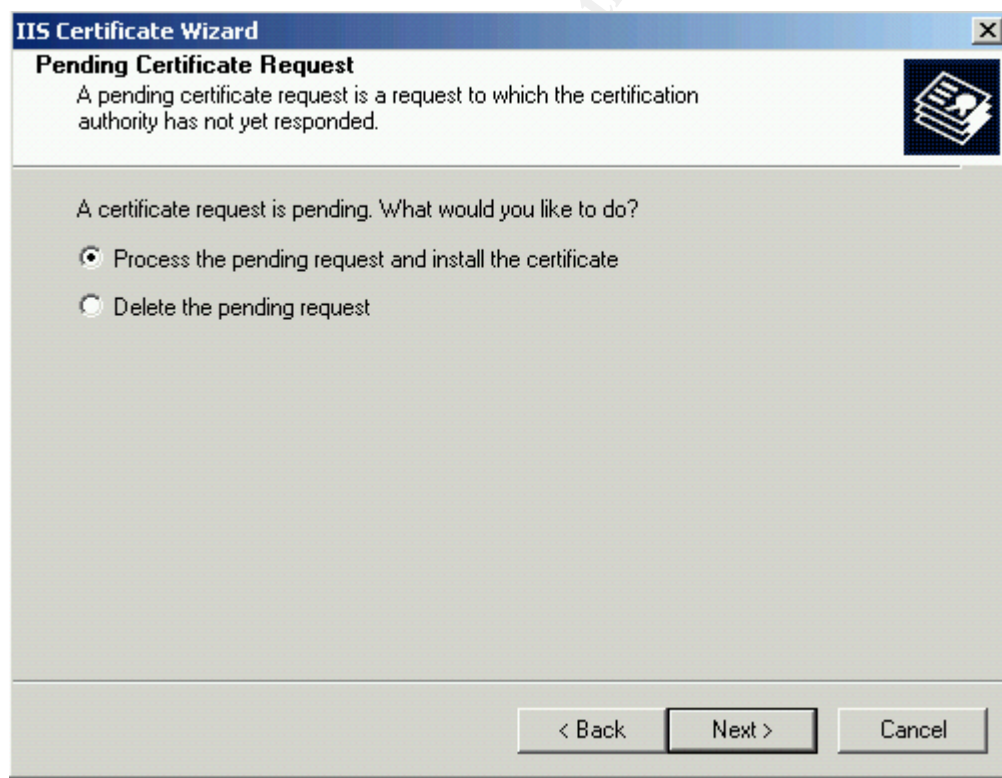
[Download CA certification path](#)

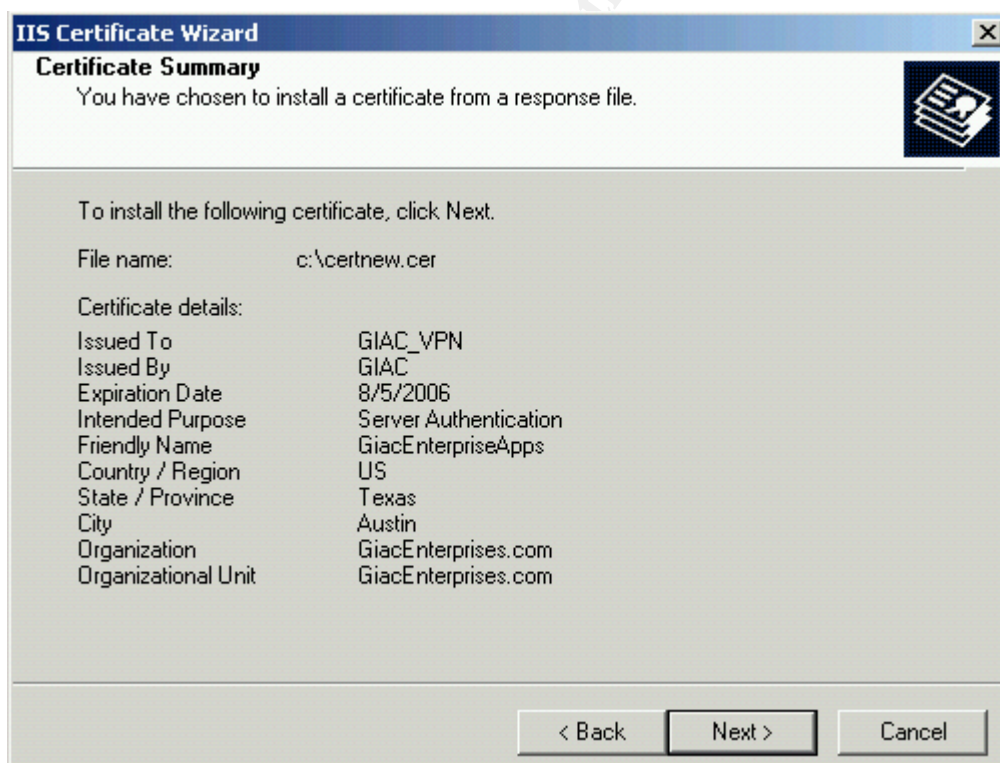
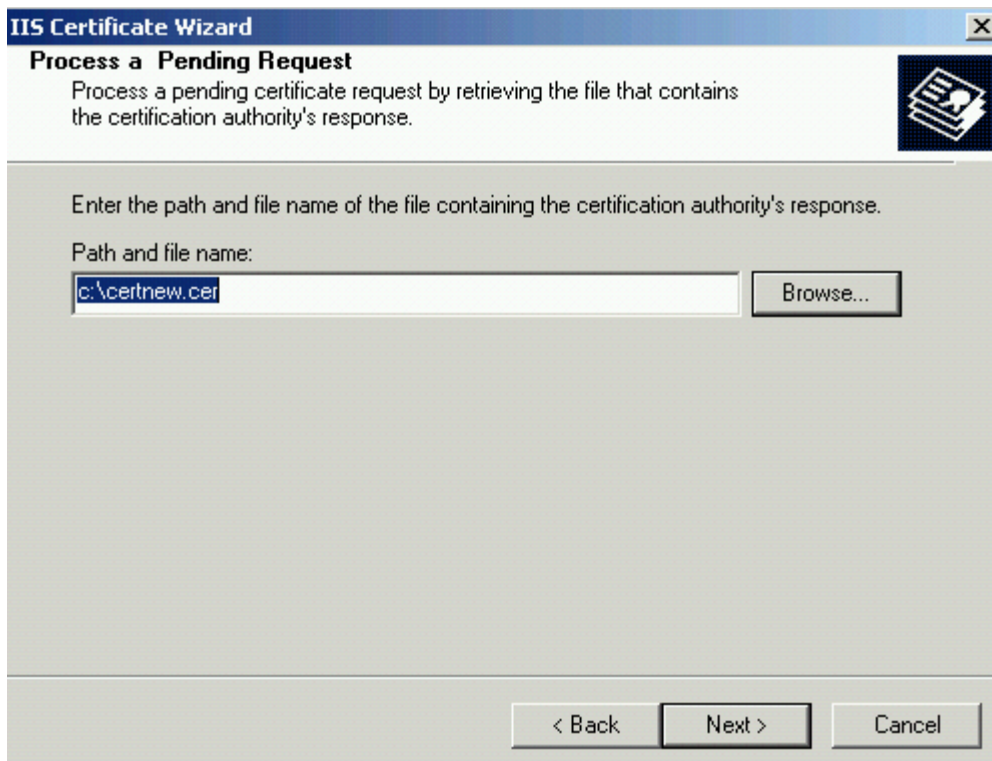
Certificate Issued

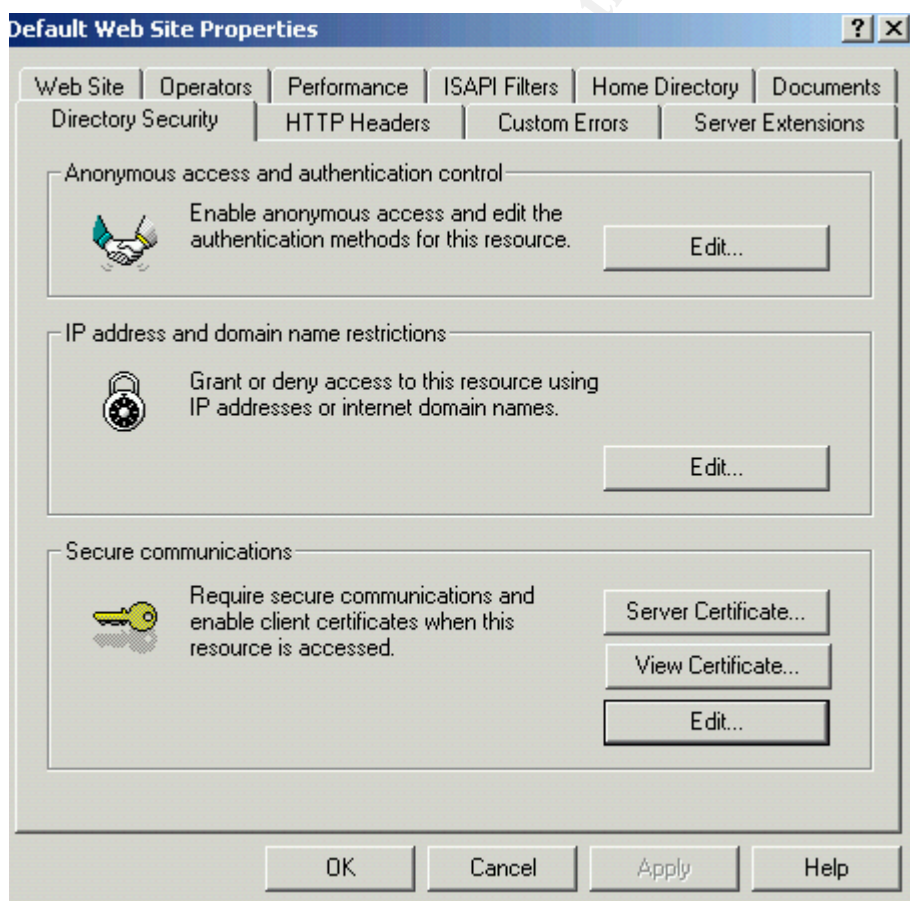
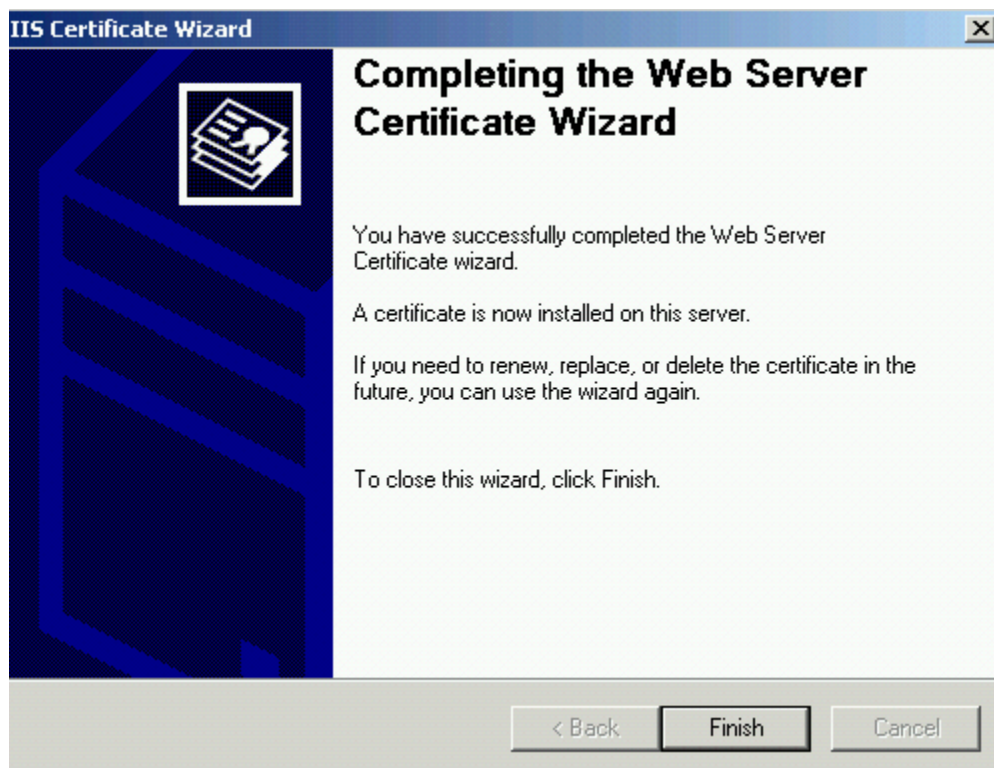
The certificate you requested was issued to you.

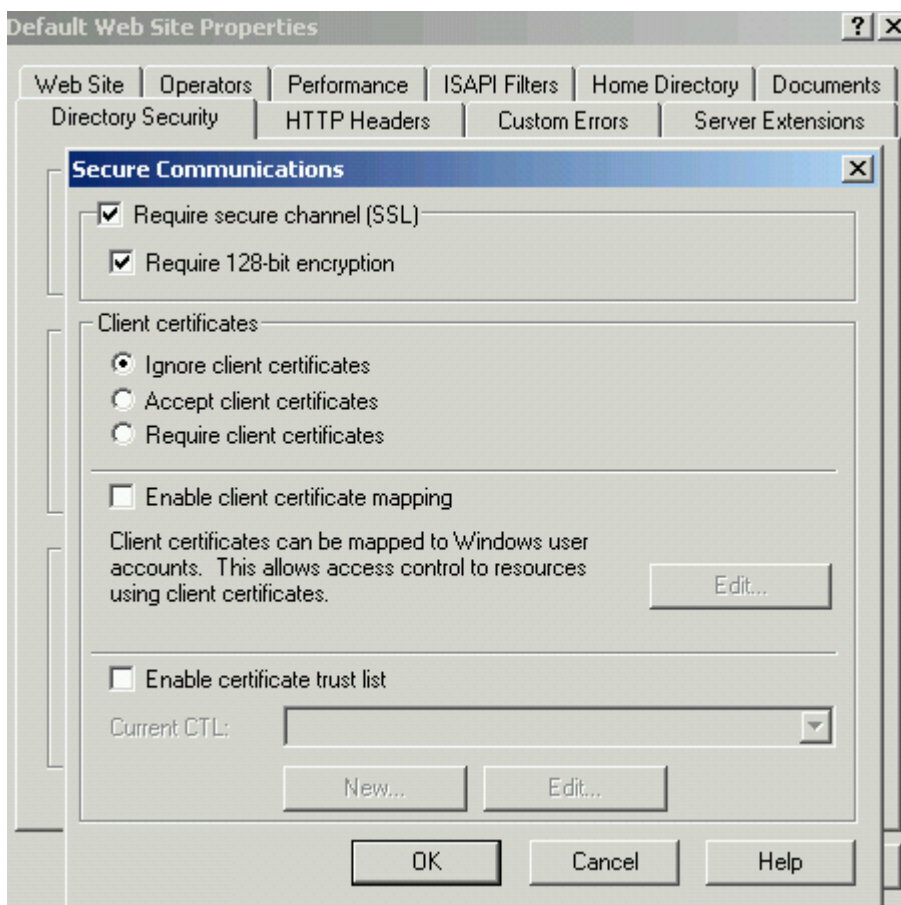
☒ DER encoded or ☐ Base 64
 [Download CA certificate](#)
[Download CA certification path](#)

**Default Web Site Properties**









Click OK and now SSL is installed on our web server.

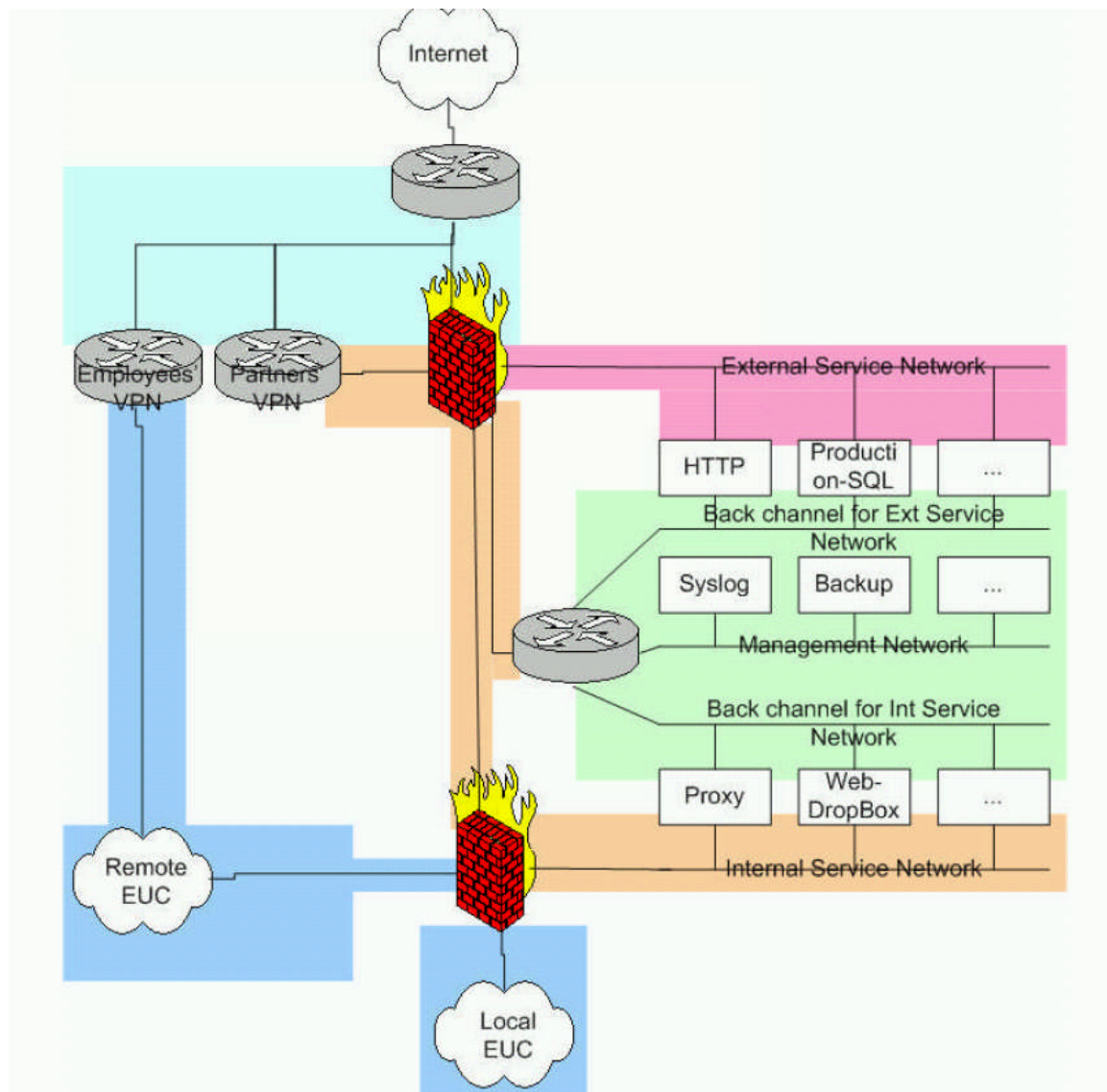
Next the RSA agent will be installed on the web server. The latest RSA Agent can be obtained from the RSA Security website located at <http://www.rsasecurity.com>. Be sure to copy the sdconf.rec file located at the RSA database server to c:\winnt\system32 directory, as it will be needed during the install.

Finally the Web Interface for Citrix can be installed.

In summary, SSL was installed on the web server. GIACEnterprise clients who have an RSA SecurID token can now log in from virtually anywhere in the world and access all the resources available to them in a very secure manner.

Assignment 3 – Design Under Fire

The practical that I will attack was done by Marc-Andre Frigon dated 18 May 2004. The network design is shown below. The URL is http://www.giac.org/practical/gcfw/marc-andre_frigon_gcfw.pdf



The plan of attack will be as follows.

1. Reconnaissance of the site.
2. Scan the site.
3. Attempt to compromise an internal system
4. Attempt to retain access to the compromised system.

Reconnaissance

At this stage, all that is known about this network is that it consists of the name GIAC Enterprise. With this information, we will start gathering information.

The first step that will be done to see if this site has a public website. Assuming that a public website, is found, a tool called wget located at <http://www.gnu.org/software/wget/wget.html> can be used to download the complete site so that it can be studied for information.²¹ Other things that can be done is to a whois on the public website once known. One good place to do this is to go to http://www.networksolutions.com/en_US/whois/index.jhtml and do a search on the domain name. This will give us a wealth of information to work with. Some of the information that will be shown could be the IP address of an external DNS server. A sample website is shown below.

IP Address:	65.173.218.144 (ARIN & RIPE IP search)
IP Location:	US(UNITED STATES)-MARYLAND-BETHESDA
Record Type:	Domain Name
Server Type:	Other
Web Site Status:	Active
DMOZ	5 listings
Y! Directory:	see listings
Secure:	Yes
E-commerce:	Yes
Traffic Ranking:	3
Data as of:	08-Jun-2004

Also a phone number could be listed to the administrator of this domain. That could be used to attempt social engineering in an attempt to get a password or more information. Another site that can be utilized is www.samspade.org as shown below.

System outages SamSpade.org has been increasingly unreachable for the past couple of months. This has been due to several reasons - general network problems, blackholing of SamSpade.org by several RIRs and general heavy usage.

This is a slightly trimmed down version of the SamSpade.org site, while I deal with some of the other issues.

- [The SamSpade.org FAQ](#)
- [Lots of online tools](#)
- [Sam Spade for Windows](#)
- [The Library](#)
- [Link to SamSpade.org](#)

[Get SamSpade.org stuff](#) - T-shirts, mugs, mouse pads, boxer shorts, frisbees....

Who is the real Sam Spade? A character created by writer [Dashiell Hammett](#).

<input type="text"/>	Do Stuff
<input type="text"/>	at <input type="text" value="Magic"/> Whois
<input type="text"/>	IP Whois

What was interesting when I went to this site is that it has been experiencing network problems. Note the message on the above site.

So what we know so far is that we have an IP address to work with. Assume that this IP is 207.99.32.2 (IP is listed in the practical) and that this is the IP of the public DNS server for GIACEnterprise.org. We also have a phone number to use for social engineering

²¹ McClure, p.7

purposes. We also discovered the physical location of GIAC Enterprises. War dialing could perhaps be used to dial all numbers in that area looking for any vulnerability.

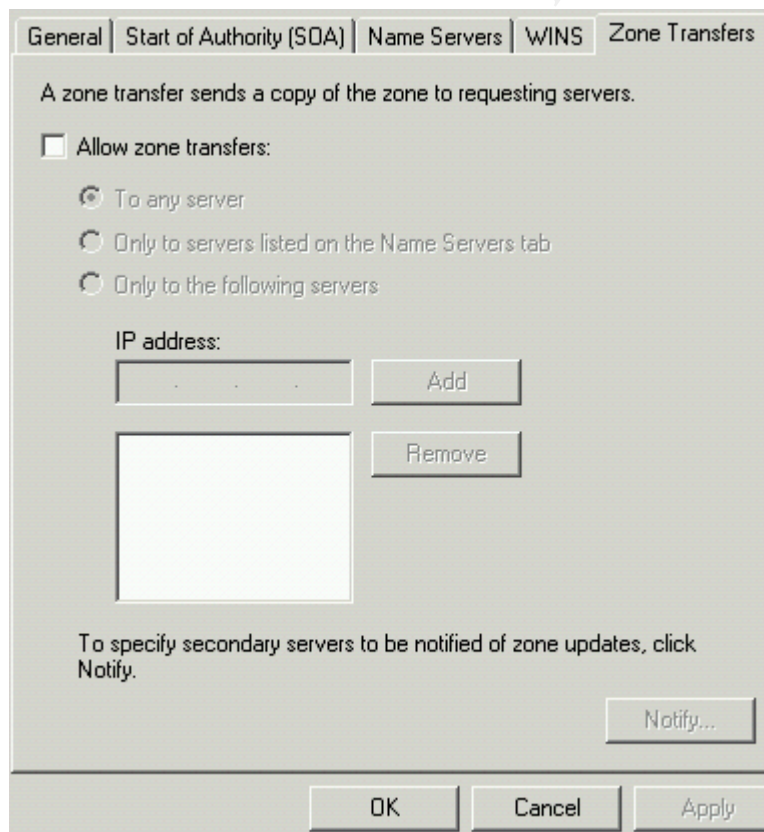
A countermeasure against reconnaissance is to be sure that the company knows what information is disclosed publicly. The public website should be scrutinized to be sure nothing is inadvertently disclosed.

Now that the DNS server of GIAC Enterprise is known, nslookup will be used to gather more information as shown below. Nslookup can be used to look for any DNS misconfiguration. Windows NT 4.0 DNS servers were fairly susceptible to misconfiguration if the administrator was not paying attention. To begin interactive mode simply type in “nslookup” at the DOS prompt on a Windows 2K desktop. At the nslookup prompt then issue the following commands.

```
>>Server “IP Address”  
>> set type=any  
>>ls -d GIACEnterprise.org
```

If the DNS server is misconfigured, there will be a wealth of information displayed.

The countermeasure for the above is to be sure the public DNS server is properly configured. As an example, on a Windows 2000 Server DNS, the following should be checked to make sure no zone transfer information is leaked.



If a zone transfer is not required, uncheck the “Allow zone transfer” box so that no transfer happens at all. If this is an external DNS in the DMZ, there should be no reason to transfer with any other DNS server.

Also as discussed in the SANS material, uptime.netcraft.com can be utilized to gather information about a particular site.²² A wealth of information can be obtained such as the operating system and type of web server software that is running on this particular site. Let’s assume for this attack on GIAC Enterprises that we determine that the website is running Apache 2.0.49 and the same IP address listed above was shown here also. This tells us that probably private IP addresses are being utilized behind a firewall and that the only public IP being seen is the outside interface IP address of the external firewall.

Scanning the site.

With all the information gathered, probing of the site can now begin. First Fping will be used to see what responds. This will help determine what the status of ICMP is at the targeted site. Some sites do not restrict ICMP traffic and this could work to our advantage. Also another excellent tool that could be used is SuperScan. This utility will identify open ports by attempting TCP connect scans.

Countermeasure for Fping scanning is to properly configure the border router and primary firewall for ICMP traffic. ICMP traffic should be filtered so that no outbound ICMP traffic goes out.

We will next use Firewalk to determine what other information can be discovered. This utility increments TTL values as traceroute does. Essentially this utility attempts to discover additional information.

Countermeasure is to simply deny ICMP time exceeded traffic.

Next nmap will be used to probe the perimeter to see what we have. The following syntax 99999999 will be used against GIACEnterprise.org.

Nmap -sS -n -v -p 100 -P0 www.GIACEnterprise.org

-sS is a SYN attempt

-n is to never do reverse DNS resolution.

-v is verbose

-p is port range. In the above example, port 100 is being scanned.

-P0 turns off pinging before scanning.

If a RST is not returned, a stateful or proxy firewall is protecting the host. That is the case in this scan against GIACEnterprise.org.

²² 2.6 Network Design and Assessment, p.4-8. 99999

Next nmap will be used to scan the subnet of the known DNS server.

Nmap -sS -n -v T 3 207.99.32.0/24. Note that paranoid mode is being used to attempt to avoid detection. A partial example output could be like below.

```
host 192.168.5.9 appears to be down, skipping it.  
host 192.168.5.10 appears to be down, skipping it.  
host 192.168.5.11 appears to be up ... good.
```

The above scan was done against an internal system behind no firewall but let's say for example that with the GIACEnterprises.org that we find the following addresses live.

207.99.32.2

Banner grabbing can now be attempted to find out what type of software is running. From a Windows 2K box, the following command will initiate a SMTP connection with GIACEnterprise.org.

```
Telnet 207.99.32.2 25  
Trying 127.0.0.1...  
Connected to 127.0.0.1.  
Escape character is '^I'.  
220 linux.local ESMTP Postfix
```

For the purpose of this attack on Marc-Andre's practical, it will be assumed that it is learned from the above banner-grabbing attempt that this site is running Sendmail 8.12.11. In this practical, no external mail relay is mentioned so it will be further assumed that this mail server is in the internal network and so an attempt to exploit this will now begin

Attempt to compromise an Internal System

One of the first places to look for vulnerability could be <http://packetstormsecurity.org>. So we will search that site for any known issues concerning Sendmail 8.12.11.

After a thorough search, no exploits were found concerning this version. However, a critical security flaw was found in Sendmail versions 8.12.9, which was fixed by version 8.12.10. So this means that if we tried again in a month or so, more than likely there will be an exploit found in this current version. Sendmail has had its share of exploits so the wait should not be long. The main Sendmail website has more information on the required patches. <http://www.sendmail.org>

Also two more versions of Sendmail have come out since 8.12.11. Below is the new features of 8.13.0 that 8.12.11 did not have.

Some of the interesting new features are:

- New map "socket" to query maps via TCP/IP sockets.
- Connection rate control as well as control over the number of incoming open connections.

Of interest is the “control over the number of incoming open connections”. Perhaps that can be exploited by spamming the administrator’s email address that we learned from the whois query above. Flooding the SMTP port could result in a denial of service for GIACEnterprise.org and achieve one attack on this site. Of course the sending email address would be spoofed to mask our identity.

Another possibility is to send an email to the administrator account and attempt to get that person to click on a link to an infected website that was setup.

The best countermeasure would be to disable Sendmail and not use it. Sendmail has had many exploits over the past and more will be found. The fact that in this practical that there does not seem to be a relay email system in front of this mail server will make it more dangerous for GIACEnterprise in the future. It will be just a matter of time. And time is on this hacker’s side.

Now this hacker will attempt to compromise the web server that was identified when using uptime.netcraft.com. The apache version identified was Apache 2.0.49. This version was released to fix the vulnerabilities as stated on packetstormsecurity.org.

Apache 2.0.49 has been released to address three security vulnerabilities. A race condition that allows for a denial of service attack, a condition that allow arbitrary strings to get written to the error log, and a memory leak in mod_ssl have all been addressed.²³

Searching the main Apache website, it is learned that Apache 2.0.50 has been recently released to fix two vulnerabilities. Of the most interest is the following.

A remotely triggered memory leak in http header parsing can allow a denial of service attack due to excessive memory consumption

With that information, it appears that if we browse to the main GIAC website, we can cause a denial of service attack by using a large number of spaces and tabs as detailed at <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0493>. Depending on how the reverse proxy is configured would determine if this attack could be successful or not.

In our last attack, we will attempt social engineering. We have the contact number to the administrator of GIACEnterprises.org. We discovered that number when we did the whois query earlier. One trick may be to call the administrator and to get him talking. Some people I have worked around will talk your ears off. We might get lucky and find a talker who once he/she gets comfortable with you, may start to give off valuable

²³ <http://packetstormsecurity.org>

information about the organization. The information learned can then be used to attack the site.

Attempt to maintain access to the compromise system.

All that could be accomplished against GIAC Enterprises is denial of service attacks. No systems were compromised in the sense that no root kits could be installed.

Assignment 4a – Work Procedure

In this assignment, I will write a work procedure that a newly hired security engineer could follow. It will be assumed that any security engineer knows the basics of TCP/IP but is not familiar with the particular brand of firewall that this enterprise has. As noted, the procedure will be on the firewall and will cover all aspects of this firewall and in particular how to implement the policy. The goal will be to be able to hand this document to a newly hired engineer and he/she should be able to properly implement the security policies by following the guidelines and instructions written down in this document. This procedure will be based on the GIAC Enterprise network.

Procedure Document on Astaro Linux Firewall.

Introduction

This working level procedure will cover all aspects of administering the Astaro Linux Firewall. Items that will be covered will be the following.

1. Building the Firewall
2. Firewall initial configuration
3. How to create firewall objects.
4. How to create and apply policy rules
5. Firewall backup and recovery procedure.
6. Day to day administration procedure

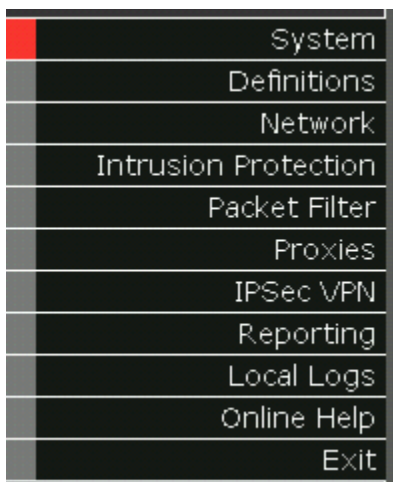
Note: The latest documents for this firewall can be found at <http://docs.astaro.org>.²⁴

Only the features that GIAC Enterprises uses will be covered. Intrusion Protection, Proxies, and IPSEC VPN are not covered.

General Information

The Astaro Linux Firewall uses the below general menu for all action items. For each item in the menu, there will be submenus. This main menu will be referred to as “**Main menu**” thru out the work procedure.

²⁴ <http://docs.astaro.org>



The “System” menu covers all aspects of anything that has to do with the firewall box itself. For example the backup menu will be found here. Also user accounts and basic system settings will be here.

Definitions are where you define the various network objects, service objects, and user objects. These objects are what are used to makeup the rule base.

Network menu will cover any item that has to do with network configuration. Items located here will be such things as configuring the interfaces or setting static routes.

Intrusion Protection will deal with the built-in intrusion prevention system.

Packet Filter is where the rules are created and the policies are implemented. This menu item along with the “Definition” menu will be the most used menus.

Proxies menu covers the various proxies that this firewall has built-in. None of these are used at GIAC Enterprises as there is concern that the firewall box could get too busy and not do it’s primary job which is to protect the network.

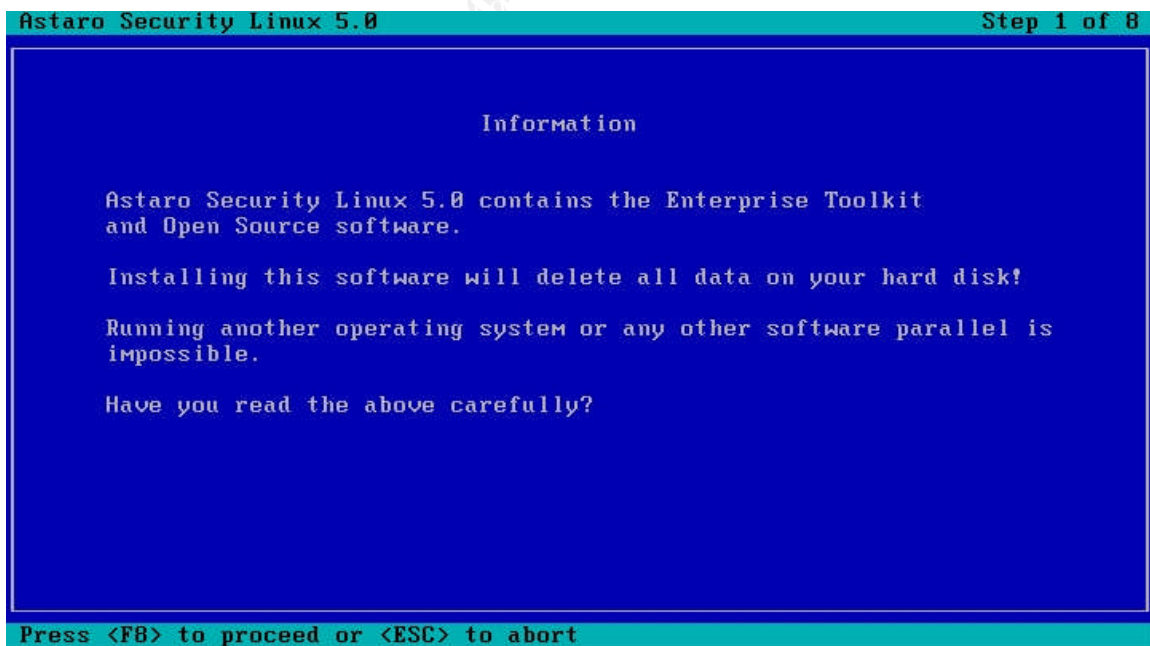
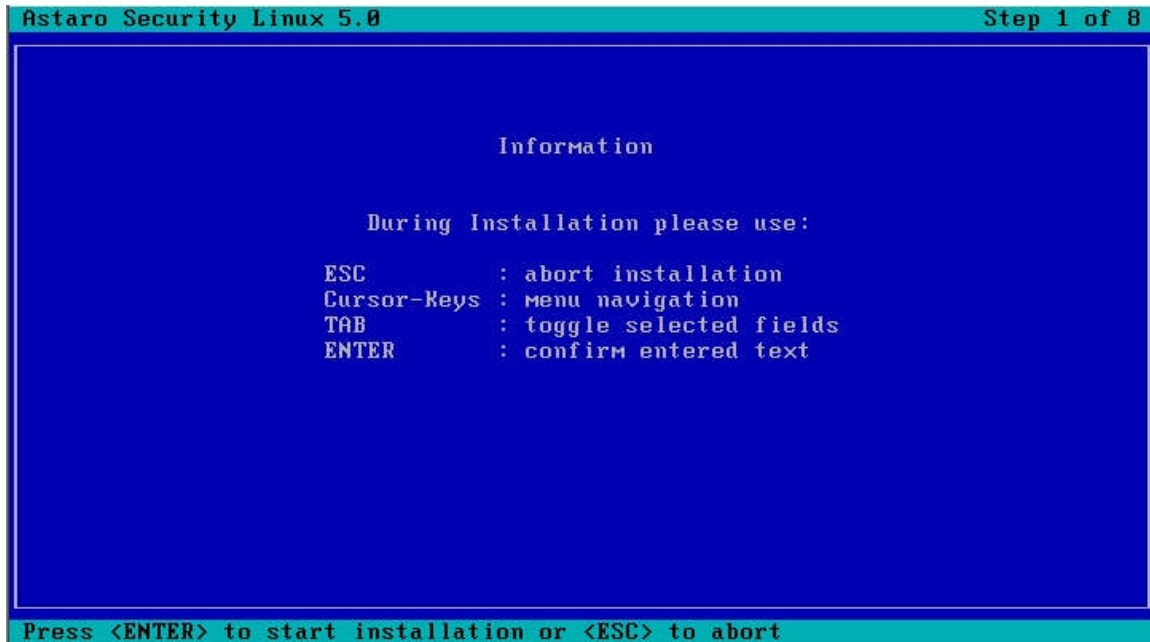
IPSec VPN covers all aspects of IPSec and VPN capabilities. None of these features are currently used as GIAC Enterprises uses a Citrix solution.

Reporting menu has all kinds of statistics and graphs about administration, packet filter, network, and hardware to name a few.

Local logs menu will be where log settings can be made and then also browsed.

How to build the firewall

Should the firewall need to be rebuilt for any reason; below is the procedure on how to do this. Rebuilding an Astaro Firewall is very simple and the screen shots below are self-explanatory and no explanations are needed. Simply put Astaro CD into server and reboot to it.



Please select the keyboard layout

English (USA)
Dutch
English (UK)
French
German
Italian
Spanish
Swedish/Finnish

Use arrow keys to navigate and <ENTER> to select

Detected hardware

Processor(s):

- Intel(R) Xeon(TM) CPU 3.06GHz, 3056 MHz

Disk(s):

- Size: 10240 MB, VMware Virtual S

CD-ROM drive(s):

- Model: VMware Virtual IDE CDROM Drive

Network card(s):

- Model: Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]

Press <ENTER> to accept, <ESC> to abort

License agreement

IMPORTANT--READ CAREFULLY BEFORE OPERATING THIS SOFTWARE

BY USING THE ENTER KEY OR USING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, USE THE ESC KEY AND PROMPTLY RETURN THE SOFTWARE TOGETHER WITH ALL ACCOMPANYING ITEMS TO YOUR SUPPLIER FOR A FULL REFUND OF YOUR PAYMENT.

Astaro License Agreement 4.3

The installation and use of the Astaro Enterprise Toolkit is subject to the following terms and conditions which constitute a license agreement between Astaro AG, Germany or Astaro's subsidiary, together ("Astaro") and the contracting individual or company ("User"). By installing the Astaro

Press <F8> to accept or <ESC> to abort

Please select your area

Africa
America
Antarctica
Arctic
Asia
Atlantic
Australia
Brazil
Canada
Chile
Etc
Europe
Indian
Mexico
Mideast

Use arrow keys to navigate, <ENTER> to select, <ESC> to abort

Astaro Security Linux 5.0Step 5 of 8

Please select your time zone

Catamarca
Cayenne
Cayman
Chicago
Chihuahua
Cordoba
Costa_Rica
Cuiaba
Curacao
Danmarkshavn
Dawson
Dawson_Creek
Denver
Detroit
Dominica

Use arrow keys to navigate, <ENTER> to select, <ESC> to abort

Astaro Security Linux 5.0Step 5 of 8

Please enter the current date and time

Year: 2004
Month: 6
Day: 23
Hour: 13
Minute: 57
Second: 28

Press <ENTER> to take over the current values or <ESC> to abort

Please configure the administrative network interface

Address: 192.168.7.1

Netmask: 255.255.255.0

(*) Gateway: 192.168.7.2

(*) optional, only needed if management PC is outside
of the network range entered above

Press <ENTER> to accept the current settings or <ESC> to abort

Information

To comply with the license regulations, we are obliged to offer you
the possibility of installing only the Open Source software.

However, we advise you to also install the Enterprise Toolkit, so
you can use the full functionality of Astaro Security Linux 5.0.

Do you wish to install both software packages?

Press <ENTER> to install both or <ESC> to do not

WARNING!

The next step will erase all data from your harddisk.
This is your last chance to stop the installation.

Press <F8> to continue, <ESC> to abort or <F12> to start over

Installation progress:

Verifying package checksums:

```
Astaro Security Linux 5.0 Step 8 of 8

Installation progress:

Verifying package checksums .....: OK
Partitioning the hard disk .....: OK
Formatting SWAP .....: OK
Formatting ROOT-Filesystem .....: OK
Formatting Boot Partition .....: OK
Formatting Install Partition .....: OK
Formatting Storage Partition .....: OK
Formatting Up2Date Partition .....: OK
Formatting Secure Partition .....: OK
Formatting Log Partition .....: OK
Formatting Temp Partition .....: OK
Creating base environment .....: OK
Copying install files .....: OK
Installing packages .....: OK
Post-Install configuration .....: OK

Press any key to finish the installation
```

```
Astaro Security Linux 5.0 Step 8 of 8

Installation finished

Please remove the CD-ROM, connect the selected
administrative network interface to your local network
and restart the system.

After the system restarted please browse to
https://192.168.7.1/
and complete the configuration.

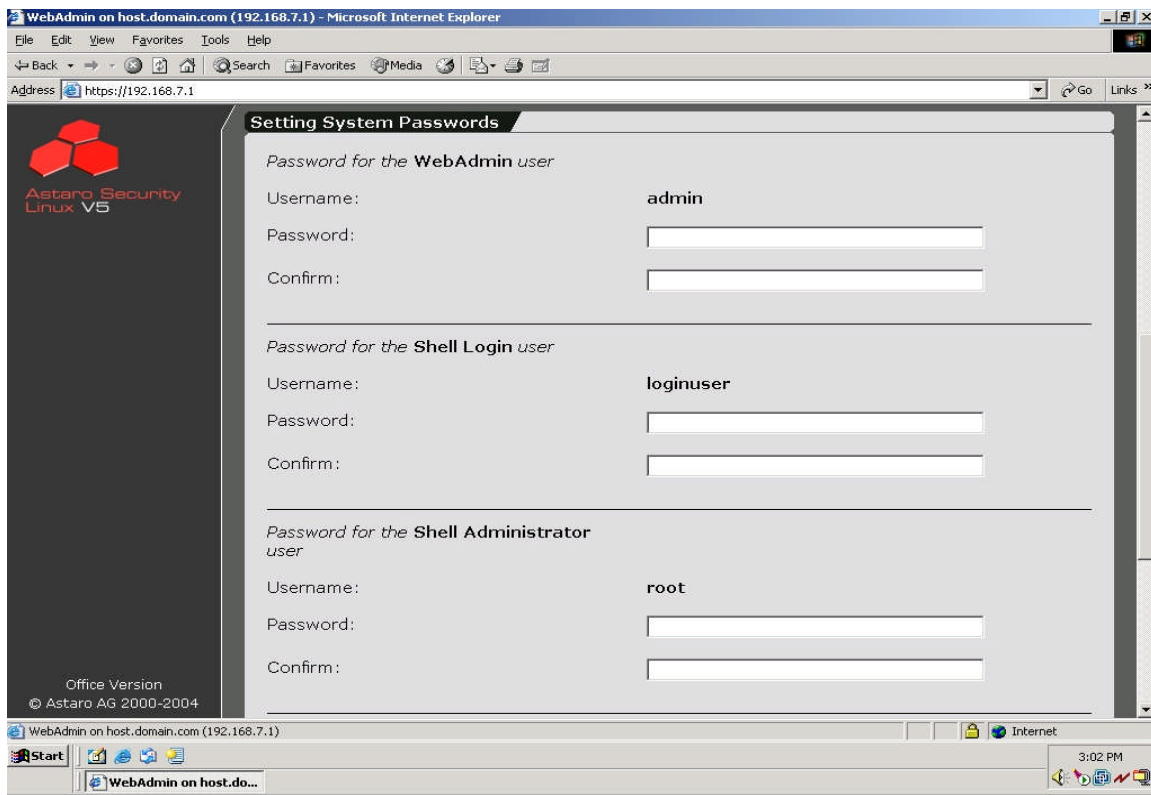
Thank you for installing Astaro Security Linux 5.0.
```

Rebuilt complete.

Firewall initial configuration

Note: This assumes a fresh install of Astaro Linux

Step 1. Browse to <https://192.168.7.1> and you will see the below menu. Enter passwords for the admin, login user, and root accounts.



Step 2. Initialize Access and Authentication by going to the following "Main Menu"->"System"->"WebAdmin Settings".

IMPORTANT: Allowed Networks and Allowed Users is initially set to "any". Leaving it at this setting will could potentially expose the firewall to any network (internal and external). Be sure to remove "any" and replace it with an appropriate object. For initial configuration, use "internal network" and "admin" After a specific machine is created, then be sure to come back here and update the "allowed Networks". This will be covered in "How-to create Firewall Objects".

Access and Authentication

Allowed Networks:

Selected	Available
firewall admin machine	Any external (Address) external (Broadcast) external (Network) External SMTP Relay

Authentication Methods:

1	<input checked="" type="checkbox"/> Local Users	⚠⚠⚠
---	---	-----

Allowed Users:

Selected	Available
admin	phil

Step 3. Upload your license file. “Main Menu” -> “System” -> “Licensing” License file can be obtained from main Astaro website at <http://www.astaro.org> and then login in with user account.

License File

Upload License File:

Step 4. Set email address of administrator and set NTP server so that firewall has correct time. NOTE: If NTP server object has not yet been created, then see work procedure “How to create Firewall Objects”.

Administrator Contact

E-Mail Addresses:

	<input type="text"/>	<input type="button" value="Add"/>
1	admin@giacenterprises.com	⚠⚠⚠
2	do-not-reply@fw-notify.net	⚠⚠⚠

Time Settings

Time Zone:

Use NTP Server:

Step 5. Configure the interfaces by going to “Main Menu”->“Network” -> “Interfaces” as shown below. Click “edit” for each interface and enter required information.

Current Interface Status				New ...
Admin	Oper	Name/Type	Parameters	Actions
<input checked="" type="checkbox"/>	Up	Astaro_DMZ_Interface (Standard ethernet interface) on eth0	192.168.7.1 / 255.255.255.0 Gateway: none	edit delete
<input checked="" type="checkbox"/>	Up	Astaro_External_Interface (Standard ethernet interface) on eth1	211.10.23.10 / 255.255.255.248 Gateway: 211.10.23.9	edit delete

Hardware List		
Sys ID	Name/Parameters	PCI Device ID
eth0	Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] irq=10 type=eth mac=00:0c:29:51:e9:a7	
eth1	Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] irq=9 type=eth mac=00:0c:29:51:e9:b1	
eth2	Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] irq=5 type=eth mac=00:0c:29:51:e9:bb	

Step 6. Update the system by going to “Main Menu” -> “System” -> “Up2Date Service” as shown below. Simply click “Install” next to each update to update the system.

Prefetch Up2Dates now: Click "Start" to prefetch available system Up2Date packages now Start

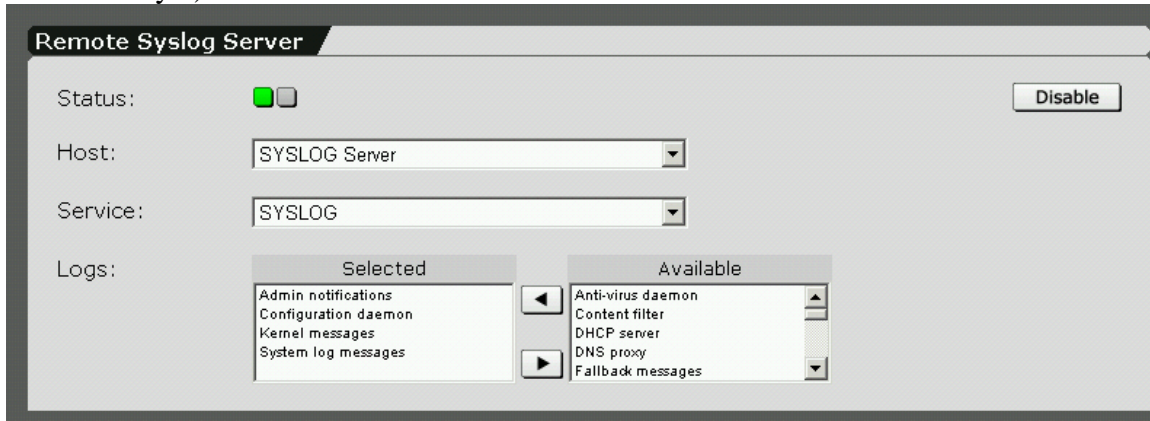
Prefetch Up2Dates automatically: ☒ Disable

Interval: Every day

Import from File: Browse... Start

Unapplied Up2Dates		
Version	File Name	Actions
5.011	5.011.tar.gpg	[install]
5.012	5.012.tar.gpg	[install]
5.013	5.013.tar.gpg	[install]
5.014	5.014.tar.gpg	[install]
5.015	5.015.tar.gpg	[install]
5.016	5.016.tar.gpg	[install]
5.017	5.017.tar.gpg	[install]

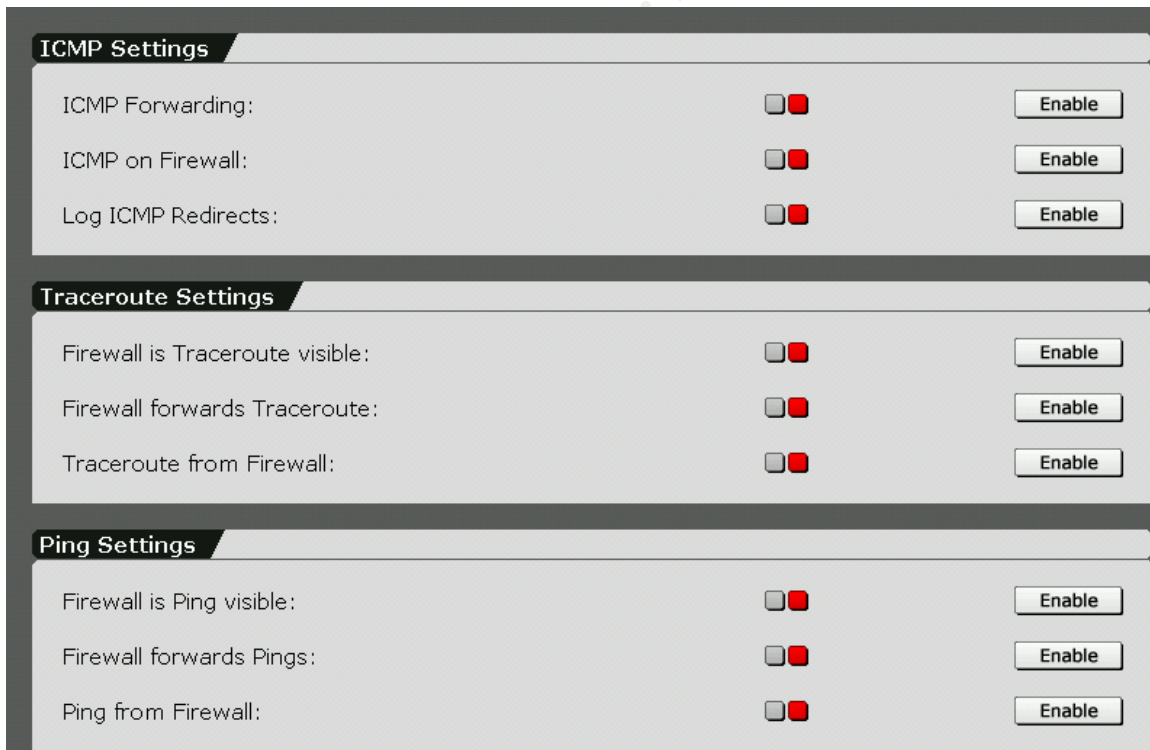
Step 7. Setup remote syslog. “Main Menu” -> “System” -> “Remote Syslog”. Next the syslog server will be specified. (See “How to Create Firewall Objects” is syslog host is not created yet)



The "Remote Syslog Server" configuration window shows the following settings:

- Status: ☒ (Green indicator)
- Host: SYSLOG Server
- Service: SYSLOG
- Logs: A list of log categories with "Selected" and "Available" columns. The "Selected" column contains: Admin notifications, Configuration daemon, Kernel messages, System log messages. The "Available" column contains: Anti-virus daemon, Content filter, DHCP server, DNS proxy, Fallback messages.
- Buttons: "Disable" (top right), "Enable" (bottom right).

Step 8. Turn off ICMP traffic. “Main Menu” -> “Packet Filter” -> “ICMP”



The configuration windows show the following settings:

- ICMP Settings:**
 - ICMP Forwarding: ☒ (Red indicator) [Enable]
 - ICMP on Firewall: ☒ (Red indicator) [Enable]
 - Log ICMP Redirects: ☒ (Red indicator) [Enable]
- Traceroute Settings:**
 - Firewall is Traceroute visible: ☒ (Red indicator) [Enable]
 - Firewall forwards Traceroute: ☒ (Red indicator) [Enable]
 - Traceroute from Firewall: ☒ (Red indicator) [Enable]
- Ping Settings:**
 - Firewall is Ping visible: ☒ (Red indicator) [Enable]
 - Firewall forwards Pings: ☒ (Red indicator) [Enable]
 - Ping from Firewall: ☒ (Red indicator) [Enable]

Step 9. “Main Menu” -> “Network” -> “Hostname”. Set the hostname for the firewall as shown below.



The "Firewall Hostname" configuration window shows the following settings:

- Hostname: giacfw
- Buttons: "Save" (bottom right).

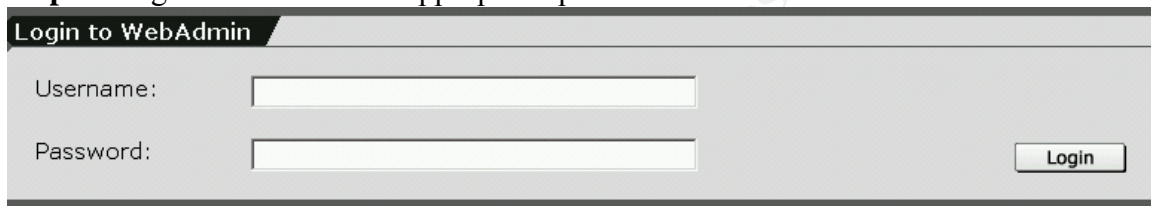
This completes how to configure the initial setup of the firewall.

How to create Firewall Objects.

Firewall objects reflect the design of the network. Each internal network is represented by an object. Objects also must be created for servers that need access to from the public. Also user objects can be created for specific purposes such as users who will administer the firewall.

Step 1. Browse to <https://192.168.7.1>

Step 2. Login as “admin” and appropriate password.



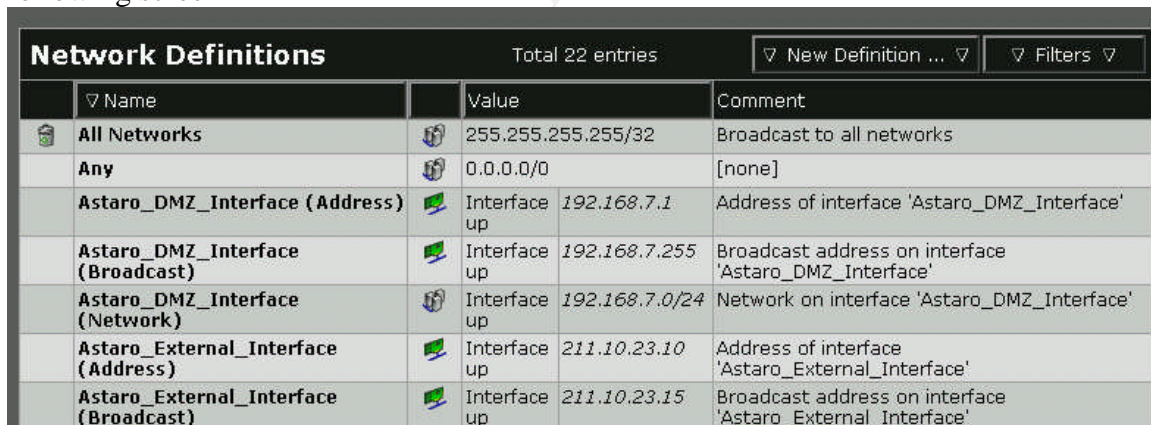
Login to WebAdmin

Username:

Password:

Login

Step 3. Go to “Main Menu” -> “Definitions” -> Networks” You should be at the following screen



Network Definitions		Total 22 entries	New Definition ...	Filters
	Name		Value	Comment
	All Networks		255.255.255.255/32	Broadcast to all networks
	Any		0.0.0.0/0	[none]
	Astaro_DMZ_Interface (Address)		Interface up 192.168.7.1	Address of interface 'Astaro_DMZ_Interface'
	Astaro_DMZ_Interface (Broadcast)		Interface up 192.168.7.255	Broadcast address on interface 'Astaro_DMZ_Interface'
	Astaro_DMZ_Interface (Network)		Interface up 192.168.7.0/24	Network on interface 'Astaro_DMZ_Interface'
	Astaro_External_Interface (Address)		Interface up 211.10.23.10	Address of interface 'Astaro_External_Interface'
	Astaro_External_Interface (Broadcast)		Interface up 211.10.23.15	Broadcast address on interface 'Astaro_External_Interface'

Step 4. Click on “New Definition” located at top right of screen.

Step 5. To create a host, make sure “host” is selected and then enter name of desktop and IP address. Fill in comments and click “Add Definition”

Network Definitions Total 22 entries △ New Definition ... △



Name:

Type:

Address:

Comment:

Step 6. Going back to the main menu, click on “Definitions” but this time click on “users” You should have the below menu.

Local User Definitions Total 2 entries ▽ Add Definition ... ▽ ▽ Filters ▽									
▽ Username	Password							PPTP Address	Comment
 admin	HTTP	SMTP	SOCKS	WebAdmin	L2TP-IPSec	PPTP	[from pool]	[none]
 phil	HTTP	SMTP	SOCKS	WebAdmin	L2TP-IPSec	PPTP	[from pool]	administrator

Step 7. Click on “Add Definition” and enter username, password and click “Add Definition” when done.

Local User Definitions Total 2 entries △ Add Definition ... △ ▽ Filters ▽

Username:

Password:

Comment:

Step 8. Go back to main menu and click on “System” and then “WebAdmin Settings” Add your desktop and username as shown below. Select your desktop on the right side and then click the left arrow so that it shows up under “Selected”. Do the same with your username.




IMPORTANT: Do not leave “ANY” as shown below. This could open a potential hole.

Access and Authentication

Allowed Networks:

Selected	Available
Any firewall admin machine	All Networks Astaro_DMZ_Interface (Address) Astaro_DMZ_Interface (Broadcast) Astaro_DMZ_Interface (Network) Astaro_External_Interface (Address)

Authentication Methods:

1	<input checked="" type="checkbox"/> Local Users	  
---	---	---

Allowed Users:

Selected	Available
admin phil	jack

Step 9. Have the newly added user browse to <https://192.168.7.1> and login with their new account.

That completes the tutorial on how to setup accessing the firewall.

How to create policy rules.

Policy rules are what permit or deny traffic thru the firewall. Rules are processed from top to bottom. The rules once created are not activated. The rules must be activated to be in effect. Specific rules should be placed before more general rules. Placement of the rules is very important. Network objects must be all created before creating rules. See “How to create Firewall Objects” if this has not been done yet.

Step 1. Browse to <https://192.168.7.1>

Step 2. Login as “admin” and appropriate password.



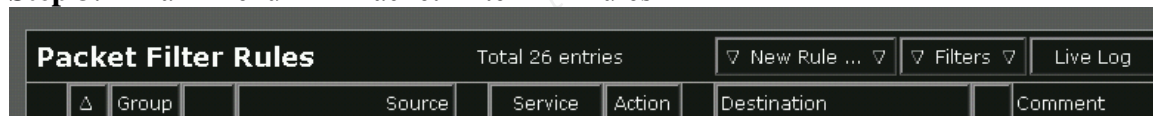
Login to WebAdmin

Username:

Password:

Login

Step 3. “Main Menu” -> “Packet Filter” -> “rules”



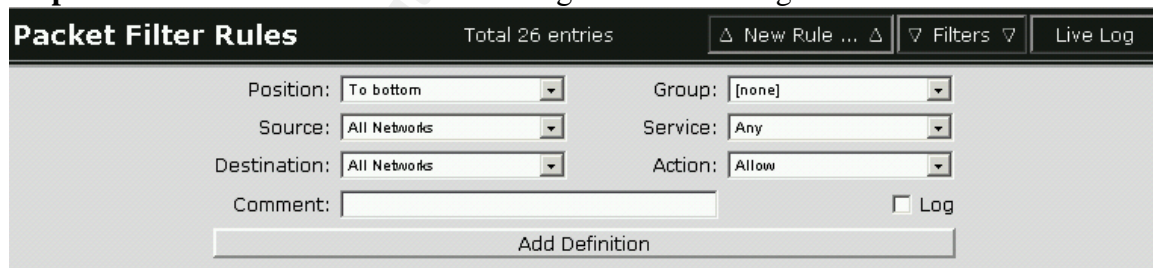
Packet Filter Rules

Total 26 entries

New Rule ... Filters Live Log

Group	Source	Service	Action	Destination	Comment
-------	--------	---------	--------	-------------	---------

Step 4. Click on “New Rule” You should get the below diagram.



Packet Filter Rules

Total 26 entries

New Rule ... Filters Live Log

Position: To bottom Group: none

Source: All Networks Service: Any

Destination: All Networks Action: Allow

Comment:

Log

Add Definition

Step 5. Fill in the above information. Position is important. For example, if allowing the internet to access the DMZ mail server, the set source to “any” and destination” to “DMZ SMTP Server”. Set Service to “SMTP”. Finally click “Add Defniition”. Note that the rule is not activated as shown below. To activate, click square box to left of red box. It will turn green indicating it is now active.



16	[none]	Any	SMTP	→	DMZ SMTP Server	Internet access to DMZ mail server
----	--------	-----	------	---	-----------------	------------------------------------

Step 6. For servers to be accessible to the public, DNAT/SNAT must be set properly. Since GIAC Enterprises is using private IP addresses, the following must be done for any service external to the firewall needing to access DMZ resources. Click Add when done.

“Main Menu” -> “Network” -> Nat/Masquerading

Add new NAT Rule

Name:

Rule Type:

Packets to match:

Source address: Destination address: Service:

Change Source to: Address:

Change Destination to: Address: Service destination:

NAT Rules

State	Name	Match Parameters	SRC Translation	DST Translation	Actions
:: No NAT rules defined ::					

This completes how to build firewall rules.

Firewall Backup and Restore Procedure.

Step 1. Login and then go to main menu and click on “System” and then “Backup”

Step 2. Enter a comment in the section “Create a Backup”. Click “start”

Restore a Backup

Upload Backup File:

Create a Backup

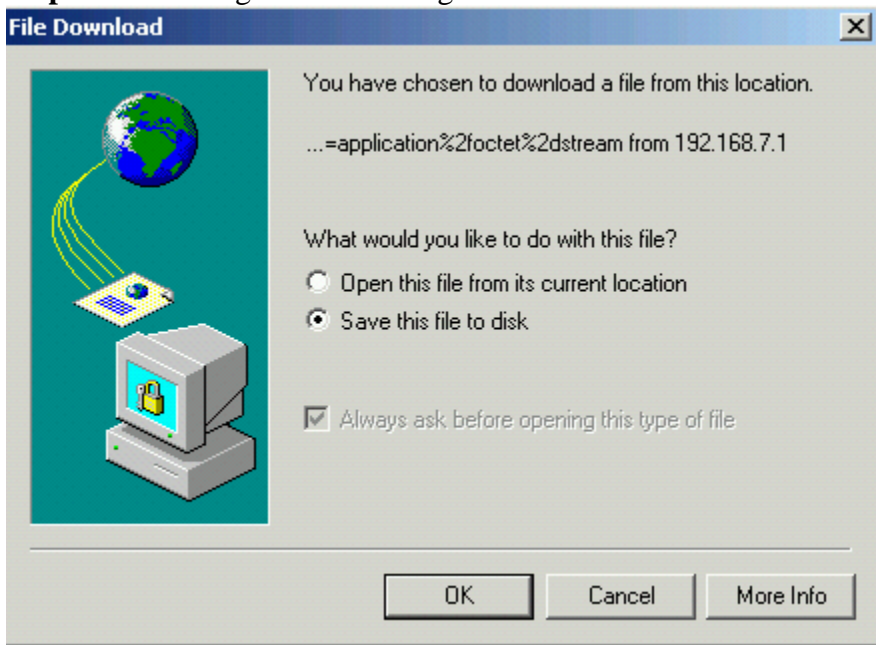
Comment:

Advanced

Encryption: ☐ ☐

Send Backups by E-Mail: ☐ ☐

Step 3. You will get the following.



Step 4. Save file to your desktop.

If you want to restore your system from a last known backup, simply “Upload Backup File” as shown above and your system is restored.

That completes the backup and restoration of Astaro Linux Firewall.

Firewall Daily Procedures.

The following should be performed daily.

1. Check for the latest patches. “Main Menu” -> “System” -> Up2Date Service.
2. Review Reporting reports. “Main Menu” -> “Reporting”
3. Review local logs. “Main Menu” -> “Local Logs” -> “browse”
4. Review local logs disk space as shown below. “Main Menu” -> “local logs” -> settings.

Local Log File Archive

Log file partition status: 2% full (36 MB used)

0 MB 2537 MB

0% 50% 100%

Delete Log Files: After 10 days

Threshold One:

When usage reaches: 85%

do this: Send Notification

Threshold Two:

When usage reaches: 90%

do this: Delete oldest log files

Threshold Three:

When usage reaches: 95%

do this: Shutdown system

Save

This concludes the work procedure on how to administer and manage the Astaro Linux Firewall.

In summary, all four assignments were completed. A thorough discussion of Defense In-Depth was discussed protecting GIAC Enterprises. A network solution was architected. A complete configuration of three key components was presented. A peer's network design was attacked. Finally a complete work procedure was written for one of those key components which was the Astaro Firewall.

List of References

IANA.ORG, 8 Aug 2004

<http://www.iana.org/faqs/SpecialUseAddresses>

Snort, 8 Aug 2004

<http://www.snort.org>

Astaro, 8 Aug 2004

<http://www.astaro.org>

Xwall, 8 Aug 2004

<http://www.dataenter.com>

F-prot, 8 Aug 2004

<http://www.f-prot.com>

Squid, 8 Aug 2004

<http://www.squid-cache.org>

Jeanne, 8 Aug 2004

http://www.ists.dartmouth.edu/IRIA/projects/d_jeanne.htm

IPCOP, 8 Aug 2004

<http://ipcop.org>

Cisco, 8 Aug 2004

<http://www.cisco.com>

Microsoft, 8 Aug 2004

<http://www.microsoft.com>

NSA Router Security, 8 Aug 2004

http://www.nsa.gov/snac/routers/cisco_scg.pdf

Cisco IOS, 8 Aug 2004

[http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterpr
ise0900aecd800a4e06.html](http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e06.html)

SANS Track 2 – Firewalls, Perimeter Protection and VPN's, 2-1 TCP/IP for Firewalls,
2004 Pg 8-25.

IANA Address Space, 8 Aug 2004

<http://www.iana.org/assignments/ipv4-address-space>

Lusignan, Robert; Steudler, Oliver; Allison, Jacques; Managing Cisco Network Security, Syngress , 2000, pg 51.

SANS Top 20, 8 Aug 2004
<http://www.sans.org/top20/>

Citrix, 8 Aug 2004
<http://www.citrix.com>

Zdnet Citrix MetaFrame XP Security Standards and Deployment Scenarios, 8 Aug 2004
<http://whitepapers.zdnet.co.uk/0,39025945,60081408p-39000457q,00.htm>

RSA SecurID for Windows, 8 Aug 2004
<http://www.rsasecurity.com/node.asp?id=1173>

Microsoft Windows 2000 Guides, 8 Aug 2004
http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1

Packetstorm.org, 8 Aug 2004
<http://packetstormsecurity.org/>

Astaro Documents, 8 Aug 2004
<http://docs.astaro.org/>

CA website, 8 Aug 2004
<http://www.ca.com>

© SANS Institute 2004, Author retains full rights.