Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Firewall Analyst Practical (GCFW)

Chris Hayden, GSEC, GCIA

September 24, 2002

Version 1.8

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Figures

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Abstract

The pages that follow cover the practical assignment required for my GCFW certificate. The assignment was four fold and the requirements were as follows:

- Assignment #1 – Design a network architecture to support GIAC Enterprises
- Assignment #2 – Define policies for the Border Routers, VPN Servers, and Primary Firewall for the design in assignment #1 and provide a tutorial on implementing the security policy for one of these devices
- Assignment #3 – Perform an audit of the primary firewall policy specified in assignment #2 and recommend changes to the policy or network architecture
- Assignment #4 – Choose a practical posted in the last six months an attack the network designed for GIAC Enterprises in that practical

Oddly enough Assignment #1 and #2 proved relatively easy when compared with Assignments #3 and #4. I suppose that this was mostly due to the fact that the emphasis of the class was on designing the architecture not auditing or breaking into it.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

GIAC Enterprises is an e-Business startup that deals with selling fortune cookie sayings online. GIAC Enterprises has tasked our firm with designing a network capable of supporting their business requirements. The design must take into consideration access requirements for the following:

- Customers – Companies or individuals that purchase online fortunes
- Suppliers – Companies that supply GIAC Enterprises with fortunes
- Partners – International companies that translate and resell fortunes
- GIAC Employees – located on GIAC Enterprises internal network
- GIAC's Mobile Workforce – "roadwarriors"

Operational Requirements

Customers

Customers need secure access to GIAC Enterprises network to purchase online fortune cookie sayings. A high level of security will be required since customer credit card information will be transmitted for transactions to take place. Private customer information should be protected as much as possible therefore it will be stored encrypted in a database that is not directly accessible from the Internet or internal network. Customers will connect to GIAC Enterprises through a secure web-site to make online purchases.

Suppliers

Online fortune cookie sayings will be purchased by GIAC Enterprises from their suppliers via the most secure method the respective supplier has to offer. GIAC Enterprise employees responsible for fortune cookie saying acquisition will be required to acquire fortune cookie sayings from suppliers and send them to the law department for approval. Once the law department has approved the fortune cookie sayings they will be sent to the data processing department to be manually entered into the retail sales database. GIAC Employees should use the following guidelines when acquiring fortune cookie sayings:

- Whenever possible request a purchase order and send a check
- If online purchasing is the only method of acquisition offered by a supplier make sure that it is a secure web-site using a high-grade encryption key (128bit) before transmitting credit card information

Partners

GIAC Enterprises International partners will connect to GIAC Enterprises network through VPN. Partners will have access to the retail sales database

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

only. Partners are required to replicate the retail sales database to a protected database located on their local networks.

GIAC Employees

Generally GIAC employees will need access to email and outbound web access. The Data Processing department will need access to the database server to update product information. The development team will require access to the database server and production web-site. Network and Computer operations will need access to all infrastructure components.

GIAC's Mobile Workforce

The mobile salesforce will connect to GIAC Enterprises network through VPN. They will need access to email and database access to customer and product information.

Design Guidelines

In the design of the network for GIAC enterprises we tried to adhere to the following guidelines as much as possible:

1. Meet the needs of the Business
2. Deny all traffic except that which is explicitly allowed
3. Be a good Internet neighbor
4. Defense in depth – attempt to provide 2 or more levels of security for every system
5. Plan for growth

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Layout

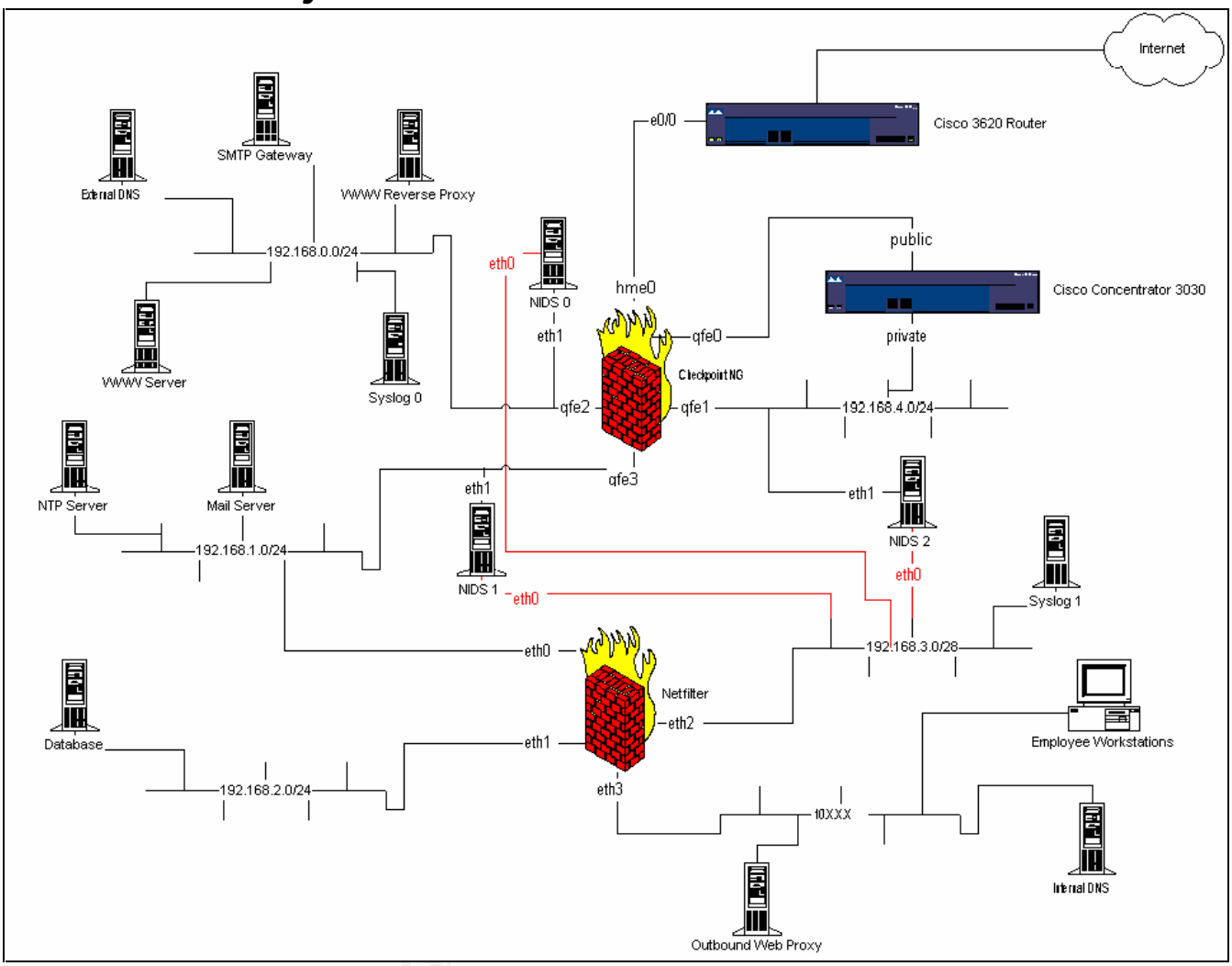


Figure 1 - Network Layout

The network design listed above uses reserved (private) IP addresses to keep from singling out any entity. The implementation of the design above will also keep the same private IP addresses except where public addresses are required. The reason for using private IP addresses is because they are not route-able on the Internet, which provides us with an extra layer of security. In the drawing 172.16.X.X addresses are used in place of public Internet route-able addresses and 192.168.X.X and 10.X.X.X addresses are private addresses used by GIAC Enterprises.

Cisco 3620 Border Router

e0/0 – 172.16.0.1/24

Software Version: IOS 12.2.12

The Cisco 3620 is a relatively inexpensive medium size router. This will provide us with room to grow in case we need more bandwidth at a later date.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We may also leverage this router for its VPN capabilities if the need arises. The size of the router should also help to keep up with processing access lists.

Cisco Concentrator 3030

public interface – 172.16.1.2/30

private interface – 192.168.4.2/24

Software Version: 3.6.1

The Concentrator 3030 is a medium sized VPN appliance. It is capable of supporting connection speeds up to T3 and up to 1500 simultaneous users. We do not anticipate an immediate need for this capacity however this will allow for growth at a later date. The Cisco VPN client for the Concentrator has a built in personal firewall that has centralized policy control from the Concentrator. This allows the Concentrator to query the client and reject connections from a client if the firewall is not turned on or installed.

Checkpoint Firewall

hme0 – 172.16.0.2/24 + static NAT addresses

qfe0 – 172.16.1.1/30

qfe1 – 192.168.4.1/24

qfe2 – 192.168.0.1/24

qfe3 – 192.168.1.1/24

Software Version: Checkpoint FW-1 4.1 SP5

The Checkpoint firewall runs on a Sun e220r with dual 400MHz processors, 1Gb of memory, and a quad-fast ethernet card running on Solaris 8. Increasing the amount of memory in the box, along with modifying some kernel settings, increases the number of connections the firewall is able to handle.

The Checkpoint firewall is a stateful inspection firewall that is relatively easy to configure. This firewall was chosen because of performance, ease of configuration, and good support. Checkpoint firewall also has built-in proxies for http, ftp, telnet, and SMTP, however we will not be using them in this design.

NIDS 0

eth0 – 192.168.3.3/24

eth1 – no ip bound to interface, set to monitor qfe2 interface of Checkpoint firewall

Software Version: Snort 1.8.7 on Redhat 7.3

NIDS 0 has been tuned to watch for and alert on signature based attacks over tcp and udp ports 22 (SSH), 80 (HTTP), 443 (HTTPS), 53 (DNS), 25 (SMTP), and 514 (Syslog). It has been set to alert on all traffic not explicitly allowed by the Checkpoint firewall policy for the 192.168.0.0 service network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The IDS configured in this way will help us be sure that the firewall is configured correctly and that it is not allowing any unwanted traffic through.

NIDS 1

eth0 – 192.168.3.4/24

eth1 – no ip bound to interface, set to monitor qfe3 interface of Checkpoint firewall

Software Version: Snort 1.8.7 on Redhat 7.3

NIDS 1 has been tuned to watch for and alert on signature based attacks over tcp and udp ports 22(SSH), 110 (POP3), 25 (SMTP), 123 (NTP), and 143 (IMAP). It has been set to alert on all traffic destined for the 192.168.1.0/24 service network not explicitly allowed by the Checkpoint firewall policy.

NIDS 2

eth0 – 192.168.3.5/24

eth1 – no ip bound to interface, set to monitor private interface of Concentrator

Software Version: Snort 1.8.7 on Redhat 7.3

NIDS 2 has been setup with the default snort ruleset. The purpose of this sensor is to monitor the unencrypted side of traffic from VPN users. This will help to alert us of a possible VPN server compromise.

Netfilter Firewall

eth0 – 192.168.1.2/24

eth1 – 192.168.2.1/24

eth2 – 192.168.3.1/24

eth3 – 10.0.0.1/24

Software Version: Redhat 7.3

Netfilter was chosen as an internal firewall. It was chosen because it is cheap (free), has great logging, and is different from our primary firewall. Because it is completely different from our primary firewall it is unlikely to fail or suffer from the same vulnerabilities as the primary firewall. It also adds an extra layer of defense to some of our most valuable assets: databases, internal corporate network, and security device management network.

Outbound Web Proxy

Software Version: Redhat 7.3, Squid-2.5_STABLE1, Squidalyser v0.2.55 (http://ababa.org/), squidGuard-1.2.0 (http://www.squidguard.org/)

Squid was chosen as the outbound web proxy for internal user access to Internet web-sites. Squid is nice as an outbound web-proxy because it is free,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

has good support, and allows for caching. Squidalyser was chosen as a log analysis tool for the Squid logs because it allows scrutiny over sites visited by individual users and groups. No IT person wants to be the Internet police for their organization but sometimes this information is necessary when employee performance concerns arise. SquidGuard is used to block access to sites for individual users and/or groups.

SMTP Gateway

Software Version: Redhat 7.3, Sendmail 8.12.6

Sendmail is used to relay email to and from the Internet. It has been configured essentially as an SMTP proxy. Sendmail was chosen because of it's support, wide user base, flexibility, and cost. It has been configured to mask the headers from the internal mail system.

Syslog 0

Software Version: Redhat 7.3

Syslog 0 server is using the default syslog server installed with Redhat 7.3. It is configured to forward log entries to Syslog 1. It is essentially acting as a Syslog proxy for the border router.

Syslog 1

Software Version: Redhat 7.3, Swatch 3.0.4
(http://www.oit.ucsb.edu/~eta/swatch/)

Syslog 1 server is using the default syslog server installed with Redhat 7.3. It is the main log server for all devices. Swatch allows us to easily write filters to look for specific log entries and perform special actions based on the entries seen, such as paging, email generation, etc.

WWW Reverse Proxy

Software Version: Redhat 7.3, Squid-2.5_STABLE1, Jeanne
(http://www.ists.dartmouth.edu/IRIA/projects/d_jeanne.htm)

The www reverse proxy is used to proxy request to the WWW server. Jeanne allows us to configure the proxy to deny requests to urls that aren't explicitly defined in the configuration script. This helps to protect against vulnerabilities based on scripts being installed as part of the default install for the webserver and can also help protect against worms.

WWW Server

Software Version: Redhat 7.3, Apache 1.3.26 + mod_ssl 2.8.10

Apache is used as the webserver because of its cost, large user base, support, and access control abilities. It has been configured to return back bogus server information to keep from making would-be attackers jobs easier in the reconnaissance phase of an attack. It has also been configured to only accept

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

connections from the WWW Reverse Proxy since all requests should be originated from the Proxy.

Note: All devices mentioned above have been hardened for device security. Whenever possible scripts are used to help harden hosts.

© SANS Institute 2000 - 2002, Author retains full rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment #2 – Security Policy and Tutorial

Border Router Policy

Router Hardening

- Hostname

  ```
  hostname chopin
  ```

  Sets the hostname to chopin. We don't want to use a descriptive hostname that may give too much information out to a would-be attacker.

- Disable Unneeded Services

  ```
  no service tcp-small-servers
  no service udp-small-servers
  ```

  Turns off the tcp and udp small servers such as echo and chargen. These are unneeded and could even be used by an attacker to launch an attack against the router such as a denial of service.

  ```
  no service finger
  ```

  Turns off the finger server. Finger gives out information about who is logged on and even where they are connecting from. This gives way too much information to a would-be attacker.

  ```
  no ip http server
  ```

  All connections will be made through telnet or console access (CLI only) therefore we will turn off the http server.

  ```
  no ip bootp server
  ```

  Disable bootp on the router because it is not needed outside the firewall.

  ```
  no ip identd
  ```

  Disable ident (rfc1413).

  ```
  ntp disable
  ```

  We will not be allowing ntp updates on the border router so disable ntp.

- Disable Unused Interfaces

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
int Ethernet 0/1
        shutdown
```

Disable inteface Ethernet 0/1 because it is currently not being used.

- Drop Source Routing

```
no ip source-route
```

Source routed ip packets are considered harmful and should be dropped.

- Encrypt Passwords (Vigenere Cipher)

```
service password-encryption
```

Sets the router to store all passwords in encrypted format to prevent password information from being displayed in clear-text when the configuration of the router is being viewed. This helps defeat casual lookers from seeing router passwords only. The Vigenere Cipher is considered to be a weak encryption algorithm by modern standards.

- Set Passwords

```
line vty 0 4
        login
        password 0 <string>
line con 0
        login
        password 0 <string>
line aux 0
        login
        password 0 <string>
```

Sets a password on each of the lines. The 0 specifies that the cleartext version of the password follows.

```
enable secret <string>
```

Sets the privileged mode (level 15) password for the router. By specifying secret the password will be stored encrypted using an MD5 hash.

- Limit ICMP

```
int Serial 0/0
        no ip directed-broadcast
        no ip unreachables
int Ethernet 0/0
        no ip directed-broadcast
        no ip unreachables
```

Commands must be applied to each interface. Disables directed broadcasts on each interface. No ip unreachables silences the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

router from sending back certain ICMP error messages such as host unreachable and net unreachable. These error messages could help an attacker when probing the network for active machines.

- Set Banners

```
banner login /
WARNING: All unauthorized access is strictly prohibited and may be subject to
prosecution!
/
```

Sets the login banner. This is the banner seen when a user connects to the router before the login prompt is displayed.

```
banner exec /
**********************************************************************

You have logged on to a GIAC Enterprises proprietary device. INFORMATION IN
THIS DEVICE BELONGS TO GIAC ENTERPRISES AND/OR ONE OF ITS
AUTHORIZED CLIENTS AND MAY NOT BE COPIED (IN WHOLE OR IN PART)
IN ANY MANNER WITHOUT EXPRESS WRITTEN AUTHORIZATION. This device
may be used only for the authorized business purposes of GIAC Enterprises and/or its
clients. Anyone found using this device or its information for any unauthorized purpose
or personal use may be subject to disciplinary action and/or prosecution.

**********************************************************************
/ [1]
```

Sets the banner displayed when a user has successfully logged on to a router.

- Enable Logging

```
logging 172.16.0.5
logging trap debug
logging console emergencies
```

Configures syslog logging to be sent to 172.16.0.5. All messages will be logged to the syslog server and emergencies will be logged to the console as well.

- Disable SNMP

```
no snmp-server
```

Disables SNMP.

- Disable CDP

```
no cdp run
```

Disables the Cisco Discovery Protocol, which is used to gather information about routers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Ingress Filtering

```
int Serial 0/0
        ip access-group 100 in
access-list 100 deny ip 172.16.0.0 0.0.0.255 any log
```

In the above statements we are preventing any packets with source addresses in our public address space from coming in off of the Internet and logging each attempt. These packets would be either crafted or from a misconfigured device so in either case we would not want to allow them into our network. We are using extended access lists (100-199) because only one access list may be applied per port per direction on a Cisco router and we will be adding to this access list later with some more granular statements.

Egress Filtering

```
int Ethernet 0/0
        ip access-group 1 in
access-list 1 permit 172.16.0.0 0.0.0.255
access-list 1 deny any log-input
```

In the above statements we are preventing any packets that do not have a source address in our public address space from exiting our network going to the Internet and logging each attempt with MAC address information. These packets would be either crafted or from a misconfigured device so in either case we would not want to allow them out to the Internet. Logging the MAC address will help us to determine from which device the packets are originating. We are using basic access lists (1-99) because we aren't going to be performing any more granular filtering on this interface and basic access lists do not chew up as many CPU cycles as extended access lists do.

Block Reserved/Private Addresses

```
int Serial 0/0
        ip access-group 100 in
access-list 100 deny ip 0.0.0.0 0.255.255.255 any
access-list 100 deny ip 1.0.0.0 0.255.255.255 any
access-list 100 deny ip 2.0.0.0 0.255.255.255 any
access-list 100 deny ip 3.0.0.0 0.255.255.255 any
…
```

The above statements are being used to drop traffic originating from ip addresses in reserved/private netblocks as defined by IANA in the document found at http://www.iana.org/assignments/ipv4-address-space. Any address originating from one of these netblocks has been either spoofed or is from a misconfigured device so in either case we do not want to allow this traffic into our network. We probably do not want to log this sort of traffic if it is being blocked. If this traffic makes it past our router we can log it at the firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Block Critical Ports

```
int Serial 0/0
        ip access-group 100 in
access-list 100 deny tcp any any range 135 139
access-list 100 deny udp any any range 135 139
access-list 100 deny udp any any eq 69 log
access-list 100 deny udp any any eq 514 log
access-list 100 deny udp any any range 161 162 log
access-list 100 deny tcp any any eq 23 log
access-list 100 deny tcp any any eq 22 log
access-list 100 deny tcp any any range 20 21 log
access-list 100 deny udp any any range 20 21 log
access-list 100 permit any any
```

The above statements are being used to block traffic to ports that are critical to our environment and should not be accessible from the Internet. The first two access-list statements block all NetBios traffic, the next few lines block TFTP, Syslog, SNMP, Telnet, Secure Shell, and FTP. The final line permits all other traffic. This line is necessary because when an access list is used it implies a default "deny all" policy.

Order of Rules

It is important to note that access list rules are processed in sequential order on a Cisco router. When creating access lists one must take care that a previous rule doesn't allow/deny traffic that was intended to be denied/allowed by a subsequent rule (known as shadowing a rule). When access lists are employed on a Cisco router a default "deny all" policy is implied so be sure to add a statement to allow all other traffic at the bottom of the access list if appropriate.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Checkpoint Firewall Policy

Firewall Rules

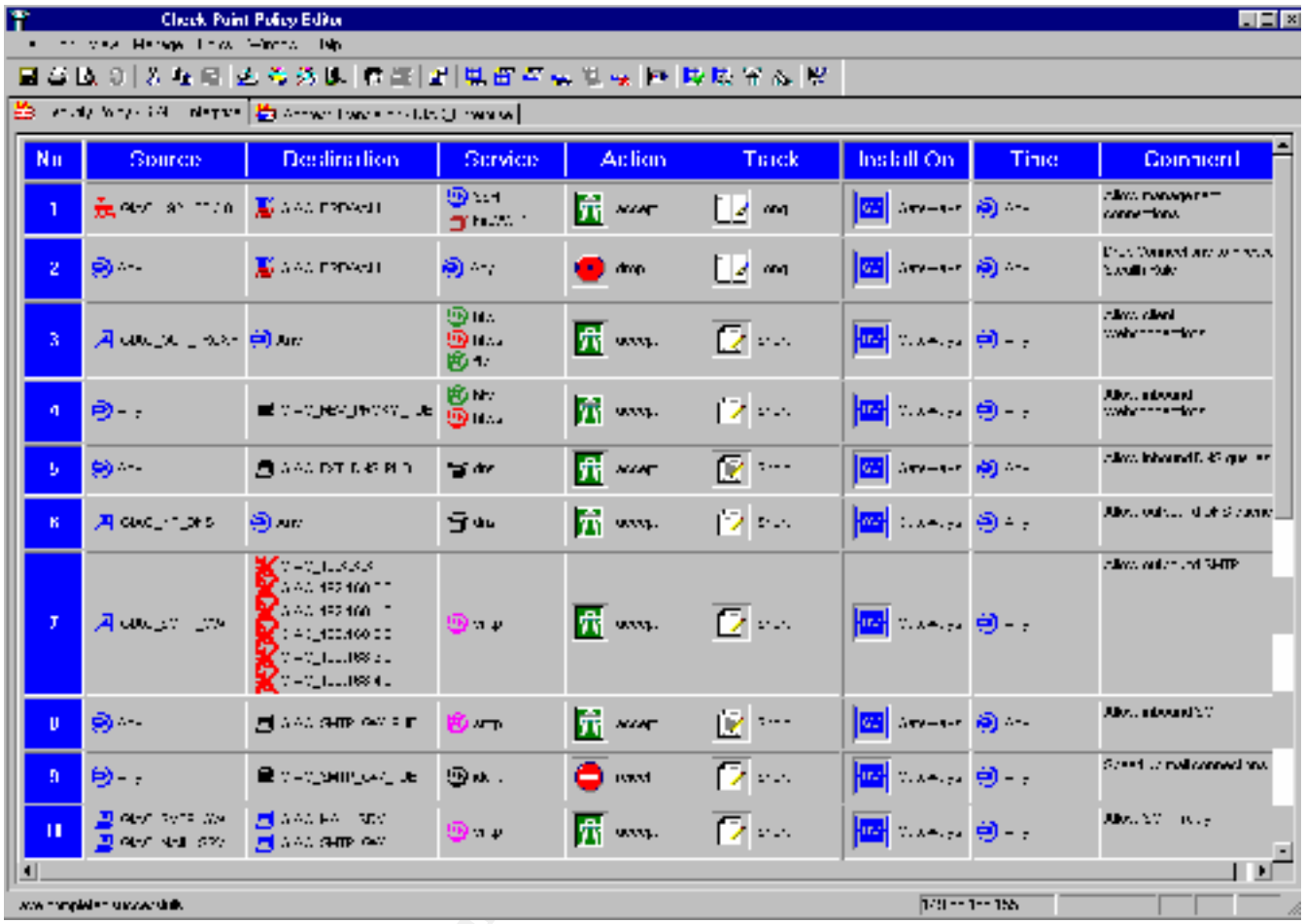


Figure 2 - Firewall Rules

© SANS Institute

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

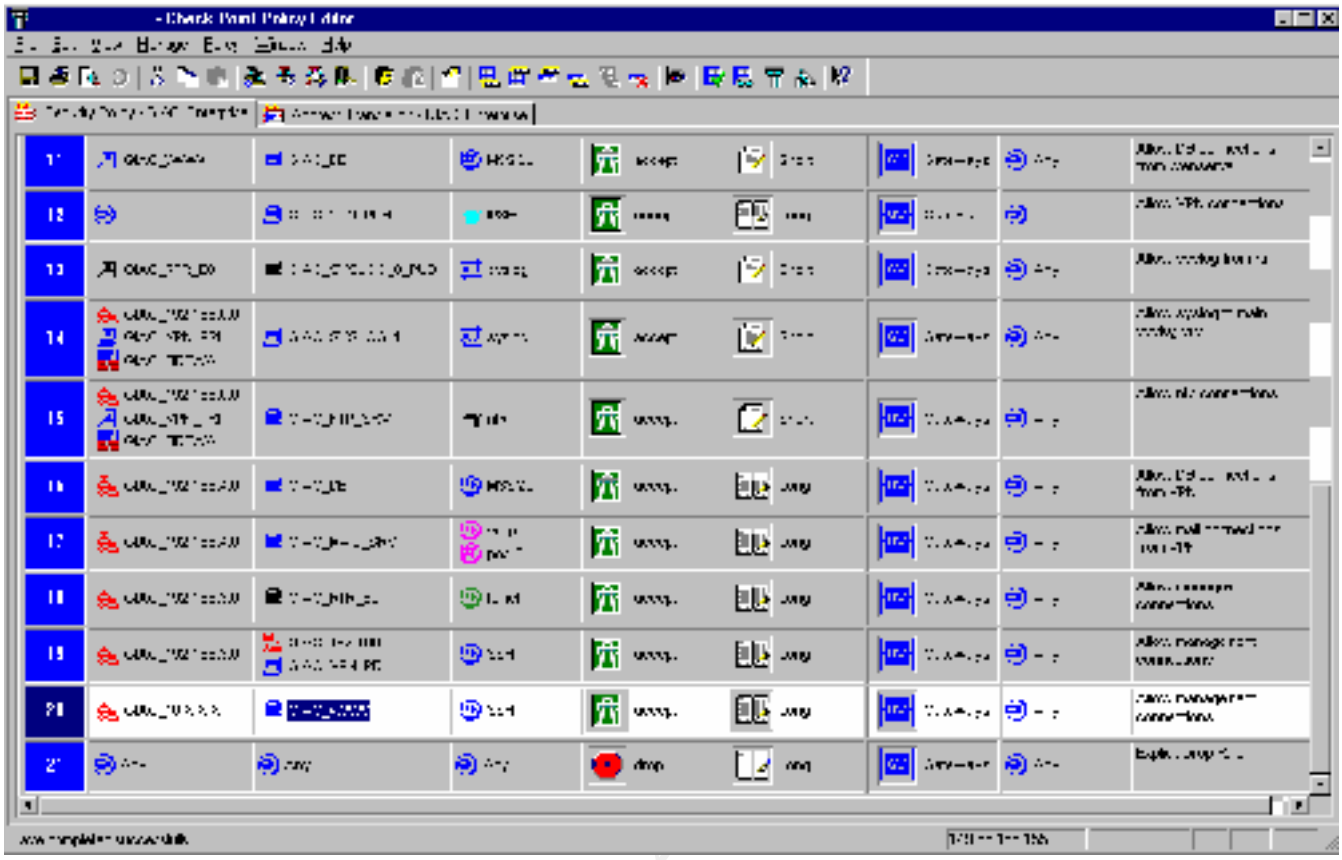


Figure 3 - Firewall Rules (cont)

The firewall rule policy is shown in the figures above. Each rule will be referred to by its rule number in the explanation that follows. Descriptive names have been used to define each object in the policy.

1) This rule allows connections from our management network 192.168.3.0. This allows ssh connections as well as FW1 connections, which include GUI Client connections. This rule must go above the stealth rule since connections are being made to the firewall itself.
2) This is what as known as the stealth rule. Named so because the firewall just drops connections directed at it instead of resetting connections, etc. This rule is pretty much standard in every firewall policy.
3) This rule allows outbound http, https, and ftp connections from the outbound www proxy. This rule is required to support outbound web connections from our internal network.
4) This rule allows inbound http and https connections to the inbound reverse web proxy. This rule is required to support inbound connections to the production website. Notice that the rule allows connections to the public address of the proxy, this is required because of the way Checkpoint performs NAT.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5) This rule allows queries to the external DNS server. This is required for users to be able to browse the production website from the Internet.

6) This rule allows outbound DNS queries from the internal DNS server. This is required for internal users to browse Internet websites.

7) This rule allows the SMTP gateway to send email to the Internet. The negation of all internal networks is used to specify the destination of the rule.

8) This rule allows inbound SMTP connections to the SMTP gateway.

9) This rule speeds up inbound SMTP connections by rejecting inbound connections to the ident service. By rejecting the connections the firewall will send a tcp reset which keeps from having to wait for the ident connections to timeout before continuing the SMTP connection.

10) This rule allows the SMTP gateway to send mail to the internal mail server and vice versa.

11) This rule allows connections from the production website to the database server. This is required for completing transactions and displaying webpages because no data is kept on the production website.

12) This rule allows inbound VPN connections to the Concentrator.

13) This rule allows the border router to log to the syslog server on the service network.

14) This rule allows devices on private networks to log back to the main syslog server.

15) This rule allows devices on private networks to connect to the ntp server for ntp updates.

16) This rule supports database connections from VPN users.

17) This rule supports mail connections from VPN users.

18) This rule allows management connections to the border router from the management network.

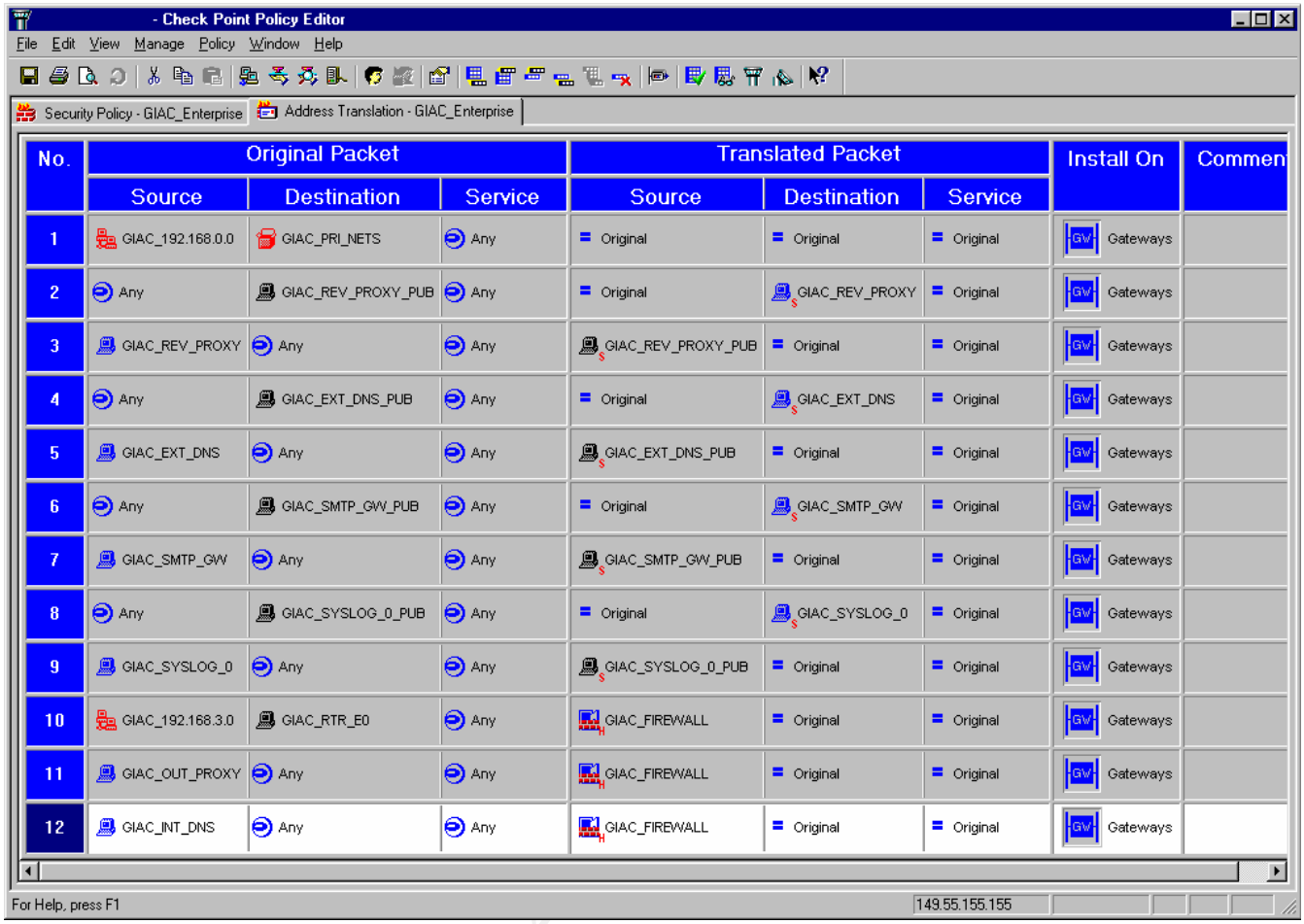
19) This rule allows management connections from the management network to the VPN Concentrator and to the 192.168.0.0 service network.

20) This rule allows management connections from the internal network to the www server. This is required for developers to update the website.

21) This rule is the explicit drop rule. This is required because we took the security posture to drop all traffic except for that which is explicitly allowed. This is a pretty much standard in every firewall policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Nat Rules



No.	Original Packet			Translated Packet			Install On	Commen
	Source	Destination	Service	Source	Destination	Service		
1	GIAC_192.168.0.0	GIAC_PRI_NETS	Any	= Original	= Original	= Original	Gateways	
2	Any	GIAC_REV_PROXY_PUB	Any	= Original	GIAC_REV_PROXY	= Original	Gateways	
3	GIAC_REV_PROXY	Any	Any	GIAC_REV_PROXY_PUB	= Original	= Original	Gateways	
4	Any	GIAC_EXT_DNS_PUB	Any	= Original	GIAC_EXT_DNS	= Original	Gateways	
5	GIAC_EXT_DNS	Any	Any	GIAC_EXT_DNS_PUB	= Original	= Original	Gateways	
6	Any	GIAC_SMTP_GW_PUB	Any	= Original	GIAC_SMTP_GW	= Original	Gateways	
7	GIAC_SMTP_GW	Any	Any	GIAC_SMTP_GW_PUB	= Original	= Original	Gateways	
8	Any	GIAC_SYSLOG_0_PUB	Any	= Original	GIAC_SYSLOG_0	= Original	Gateways	
9	GIAC_SYSLOG_0	Any	Any	GIAC_SYSLOG_0_PUB	= Original	= Original	Gateways	
10	GIAC_192.168.3.0	GIAC_RTR_E0	Any	GIAC_FIREWALL	= Original	= Original	Gateways	
11	GIAC_OUT_PROXY	Any	Any	GIAC_FIREWALL	= Original	= Original	Gateways	
12	GIAC_INT_DNS	Any	Any	GIAC_FIREWALL	= Original	= Original	Gateways	

Figure 4 - NAT Rules

The firewall NAT (Network Address Translation) policy is shown in the figure above. Each rule will be referred to by its rule number in the explanation that follows. Descriptive names have been used to define each object in the policy.

1) This rule is required so that return traffic from the 192.168.0.0 network to GIAC's private and internal networks is not translated to the respective public address.

2) This rule translates inbound connections to the public address for the reverse www proxy to the private address for the reverse www proxy. This rule uses static NAT, which is a one-to-one translation.

3) This rule translates outbound traffic from the reverse www proxy to the public address for the reverse www proxy. This is required for return traffic for inbound requests.

4) This rule translates inbound connections to the public address for the external DNS server to the private address for the external DNS server.

5) This rule translates outbound traffic from the external DNS server to the public address for the external DNS server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6) This rule translates inbound connections to the public address for the SMTP gateway to the private address for the SMTP gateway.
7) This rule translates outbound traffic from the SMTP gateway to the public address for the SMTP gateway.
8) This rule translates inbound connections to the public address for the syslog 0 server to the private address for the syslog 0 server.
9) This rule translates outbound traffic from the syslog 0 server to the public address for the syslog 0 server.
10) This rule hides connections from the management network to the Cisco router behind the firewall's external interface. This hide mode address translation is a many-to-one address translation.
11) This rule hides connections from the outbound web proxy behind the external interface address of the firewall.
12) This rule hides connections from the internal DNS server behind the external interface address of the firewall.

One thing to note about address translation rules is that only one object may be used in the source or destination of each rule. Groups may be used to combine more than one item and used in the source or destination of address translation rules.

Order of Rules

The rules in a Checkpoint policy are applied in sequential order. One nice feature of using the Checkpoint GUI is that if a rule shadows another rule it usually will indicate this to the user before saving the policy. It is best to put rules that are used the most at the top of the rulebase in order to speed up processing on the firewall.

VPN Concentrator Policy And Tutorial

Connection Requirements

(As stated from Assignment #1)

Note: because the easiest method of configuring a Cisco Concentrator is through the web interface, we will be creating the policy as we walk through the tutorial for creating it.

Partners - GIAC Enterprises International partners will connect to GIAC Enterprises network through VPN. Partners will have access to the retail sales database only. Partners are required to replicate the retail sales database to a protected database located on their local networks.

- Need to connect to the Database Server (192.168.2.2) for MS SQL ODBC – tcp/1433

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Database security ensures that Partners' userid and password restricts access to retail sales data only
- IP addresses partners will be connecting from are as follows: 1.1.1.1, 2.2.2.2, 3.3.3.3, and 4.4.4.4
- Partners will connect using Groupid: partner and Group password: g1aCr0ck5!

GIAC's Mobile Workforce - The mobile salesforce will connect to GIAC Enterprises network through VPN. They will need access to email and database access to customer and product information.

- Need to connect to the Database Server (192.168.2.2) for MS SQL ODBC – tcp/1433, Mail Server for SMTP – tcp/25 and POP3 – tcp/110
- Database security ensures that Sales Peoples' userid and password restricts access to customer and product information
- Users will connect with Groupid: roadwarriors and Group password: g35Al3s#1
- Users will also use static login and password stored on the concentrator
- Users are required to carry a linksys router for firewall protection on client side

Create Network Lists

The first step is to create network lists on the Concentrator to make writing rules easier. We will create network lists as follows:

Partners: 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4

DB_Server: 192.168.2.2

MAIL_Server: 192.168.1.2

1) We start by connecting to the web interface through IE 5 or above and logging in as admin. The interface works with other browsers but the recommended is IE5.0+.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

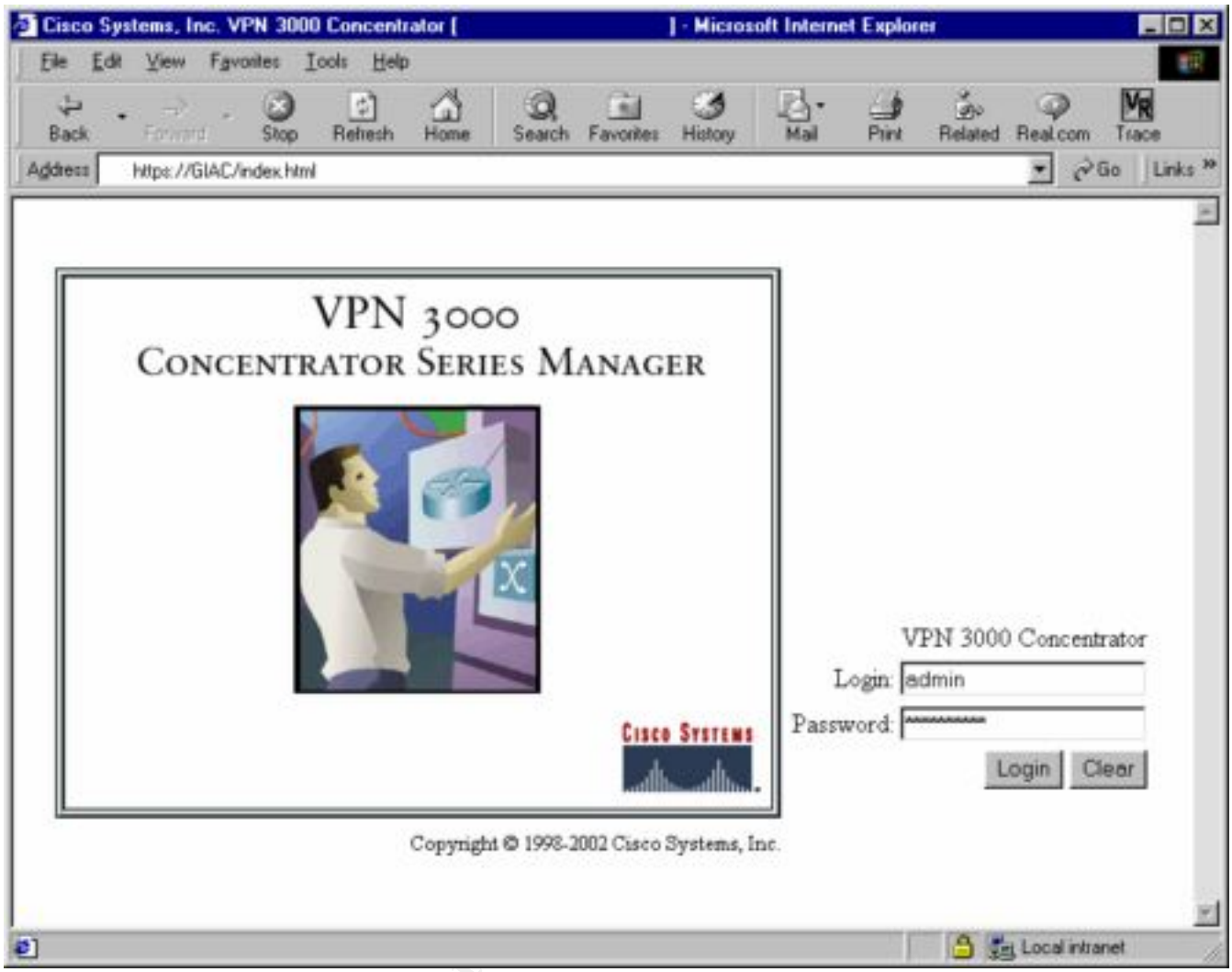


Figure 5 - Concentrator Login Screen

2) After logging in go to Configuration -> Policy Management -> Traffic Management -> Network Lists. Click the Add button to add new lists.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

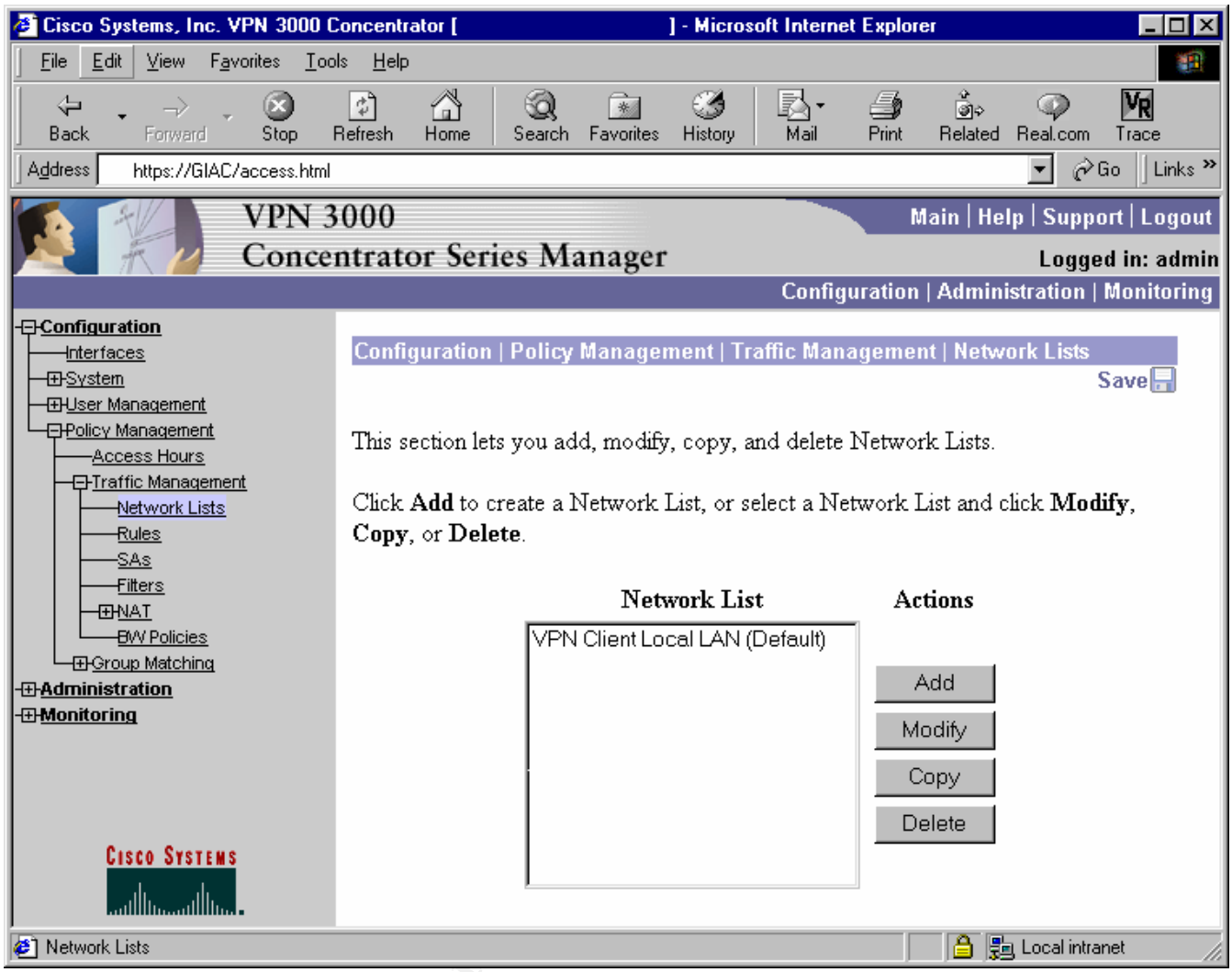


Figure 6 - Network Lists

3) We will create a list called Partners that contains the ip addresses 1.1.1.1, 2.2.2.2, 3.3.3.3, and 4.4.4.4. We first type the name Partners in the "List Name" text box. Next we add the addresses to the list in the "Network List" scrollbox. The addresses need to be added with appropriate wildcard (not subnet) mask. After entering the ip address/wildcard mask pairs press the "Add" button to add the list. Repeat these steps for the DB_Server and MAIL_Server lists.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

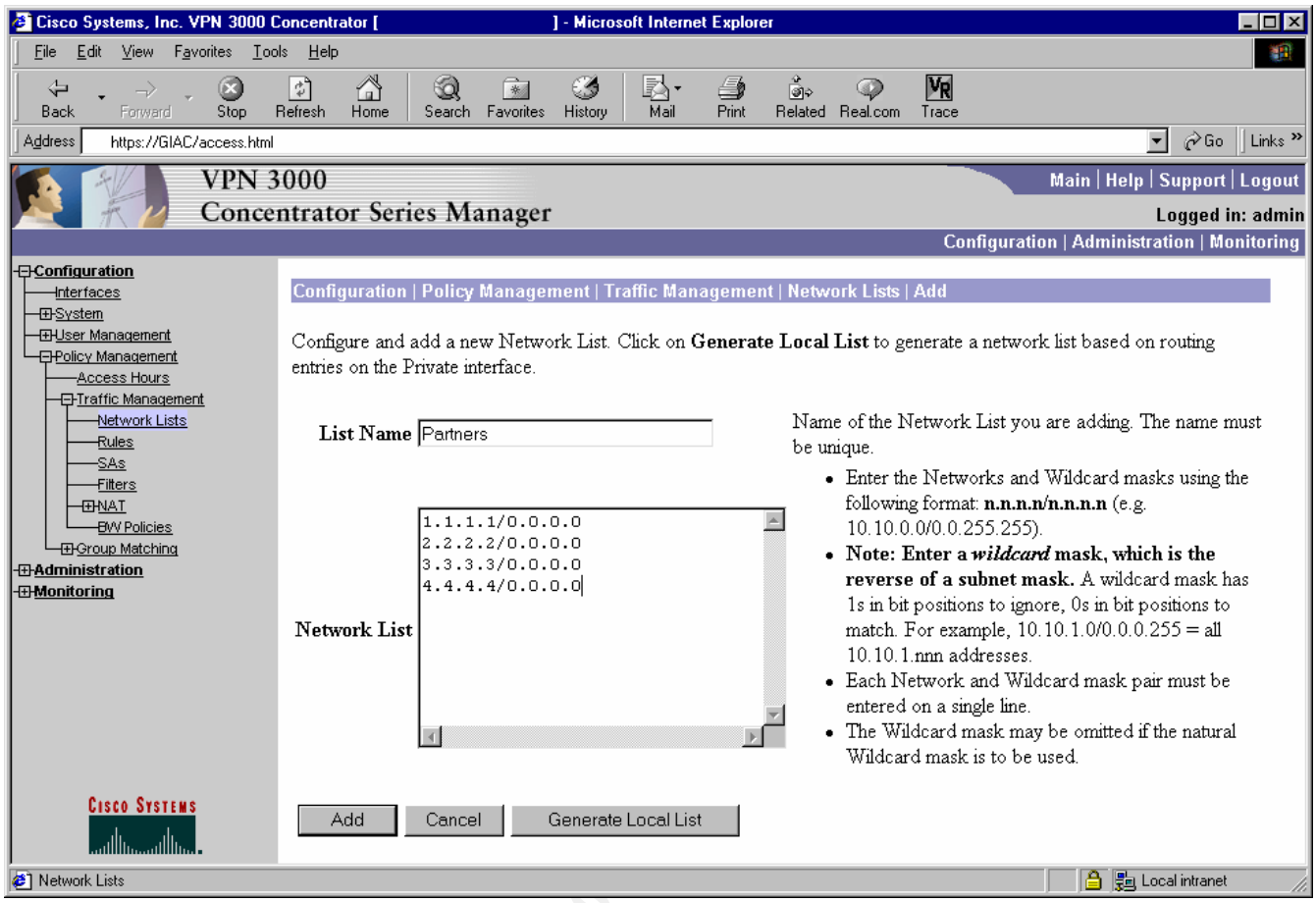


Figure 7 - Add Network List

Upon completion we should see all of the lists just created in the main network lists window as follows:

© SANS Institute 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

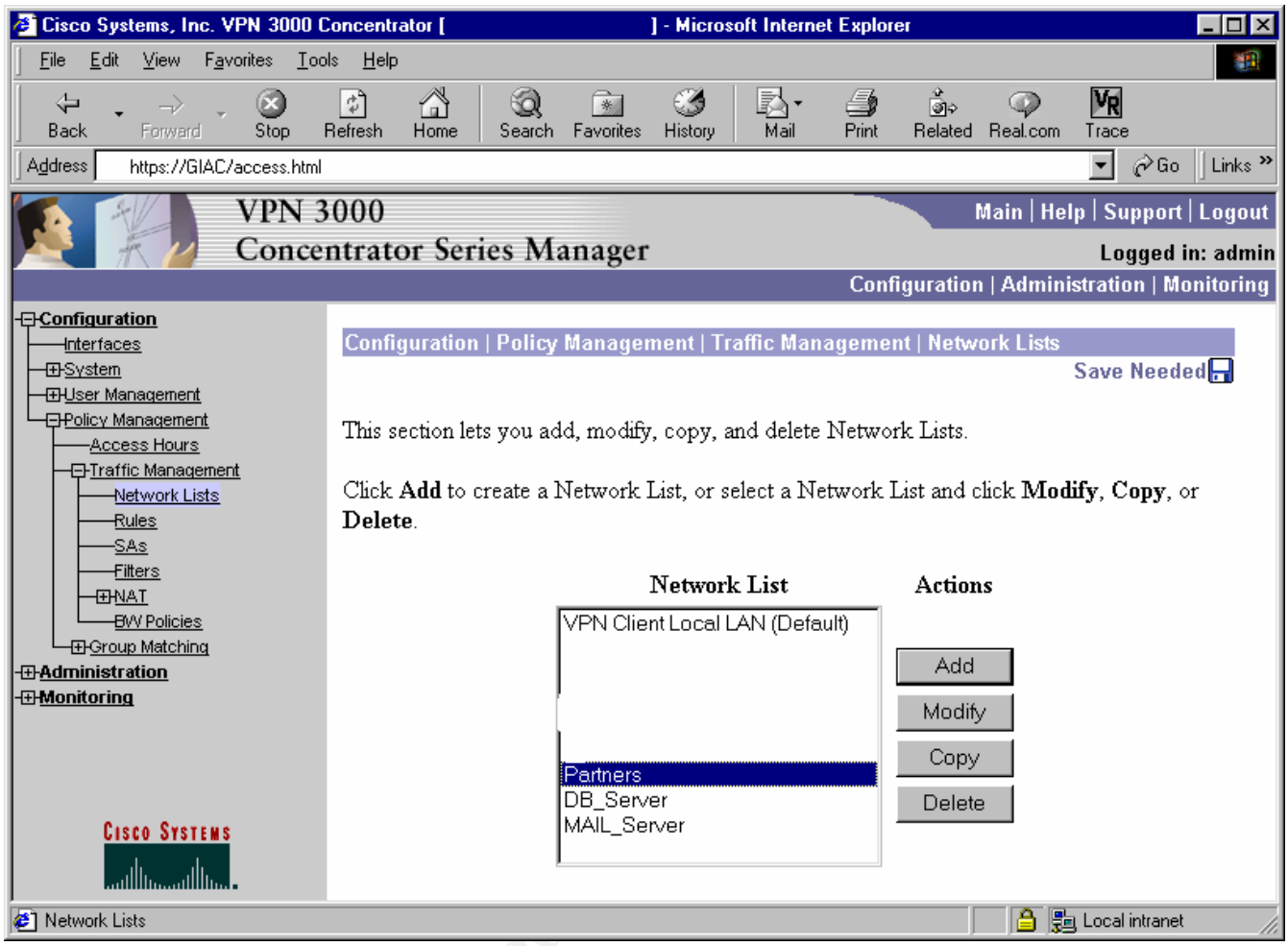


Figure 8 - GIAC Network Lists

Create SA's

The next step will be to create our SA's governing the connection requirements for VPN.

1) Go to Configuration -> Policy Management -> Traffic Management -> SAs. Click the Add button to add a new SA.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

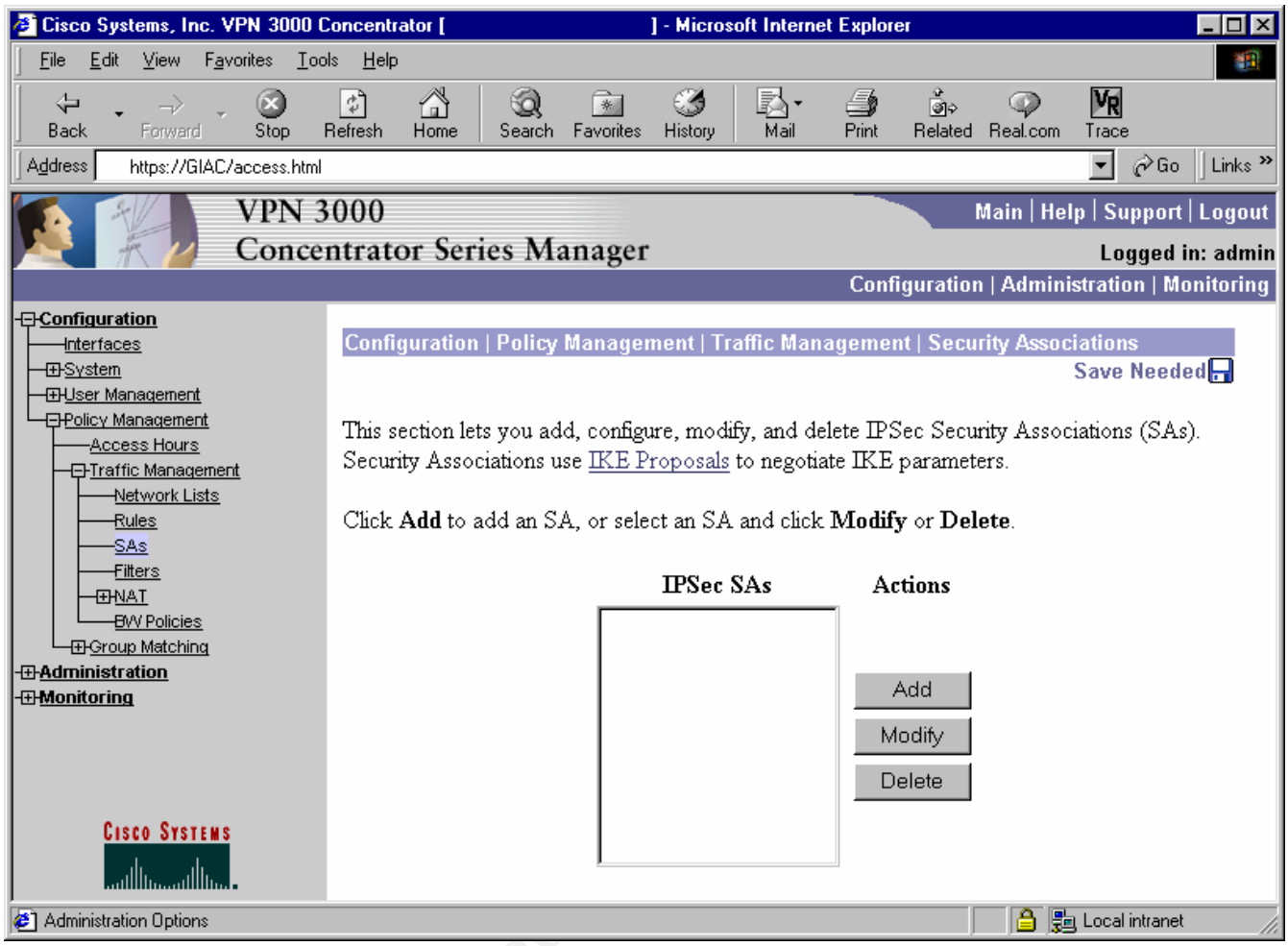


Figure 9 - SA List

2) Fill in the appropriate information as follows:

- SA Name – name given to the security association, we will call this one GIAC
- Inheritance – specifies how many tunnels to build for this connection. Each tunnel uses a unique key. From rule specifies to use one tunnel for each rule in a connection. From data specifies to use one tunnel for each address pair in the ranges specified in a rule
- Authentication Algorithm – specifies the data (packet) authentication algorithm to use. Choices are ESP/MD5/HMAC-128 and ESP/SHA/HMAC-160.
- Encryption Algorithm – specifies the type of encryption used to encrypt data. Choices are None, DES-56, and 3DES-168
- Encapsulation Mode – specifies the type of mode Tunnel or Transport to use. Since all of our connections are essentially Client-to-LAN connections we will be using Tunnel mode.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Perfect Forward Secrecy – specifies whether to use Perfect Forward Secrecy and the size of the keys to use in generating Phase II IPSec keys. The options are Disabled, Group 1 (768-Bit), Group 2 (1024-Bit), and Group 7 (ECC). We will be disabling Perfect Forward Secrecy since it must be configured exactly the same on both ends and we are not certain that our partners will be configuring this option.
- Lifetime Measurement – specifies how to measure the lifetime of keys, the length of time before a new set of keys are generated for a SA. The options are Time – use time to measure, Data – use amount of traffic in Kbytes to measure, Both – use Time and Data, which ever occurs first, and None – keys last until session is terminated or for up to 24 hours.
- Data Lifetime – if Data or Both was chosen the number of KB that is allowed to pass before new keys are generated
- Time Lifetime – if Time or Both was chosen the number of seconds before the keys expire
- IKE Peer – applies only to LAN-to-LAN connections so we will ignore it
- Negotiation Mode – IPSec negotiation mode, Aggressive or Main. We will use Main.
- Digital Certificate – specifies whether to use pre-shared keys or PKI. We will be using pre-shared keys (Group passwords)
- Certificate Transmission – we are not using digital certificates so we ignore this option
- IKE Proposal – specifies the attributes that govern Phase I negotiations. We will use CiscoVPNClient-3DES-MD5. This option allows for Pre-shared keys (XAUTH), MD5/HMAC-128 for authentication, 3DES-168 bit encryption, and uses Diffie Helman Group 2 (1024-bits) to generate SA keys.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 10 - SA Name

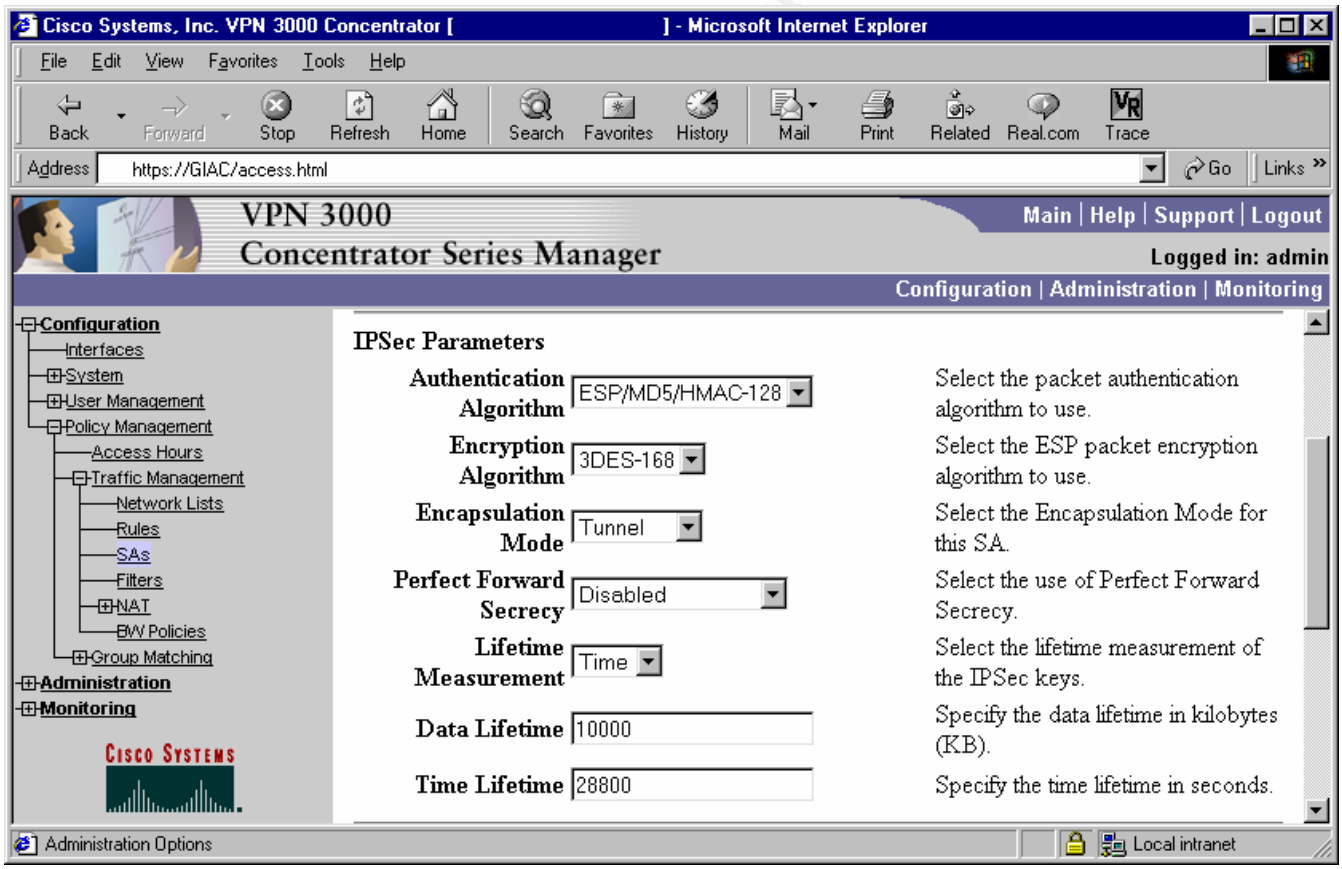


Figure 11 - SA IPSec Parameters

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

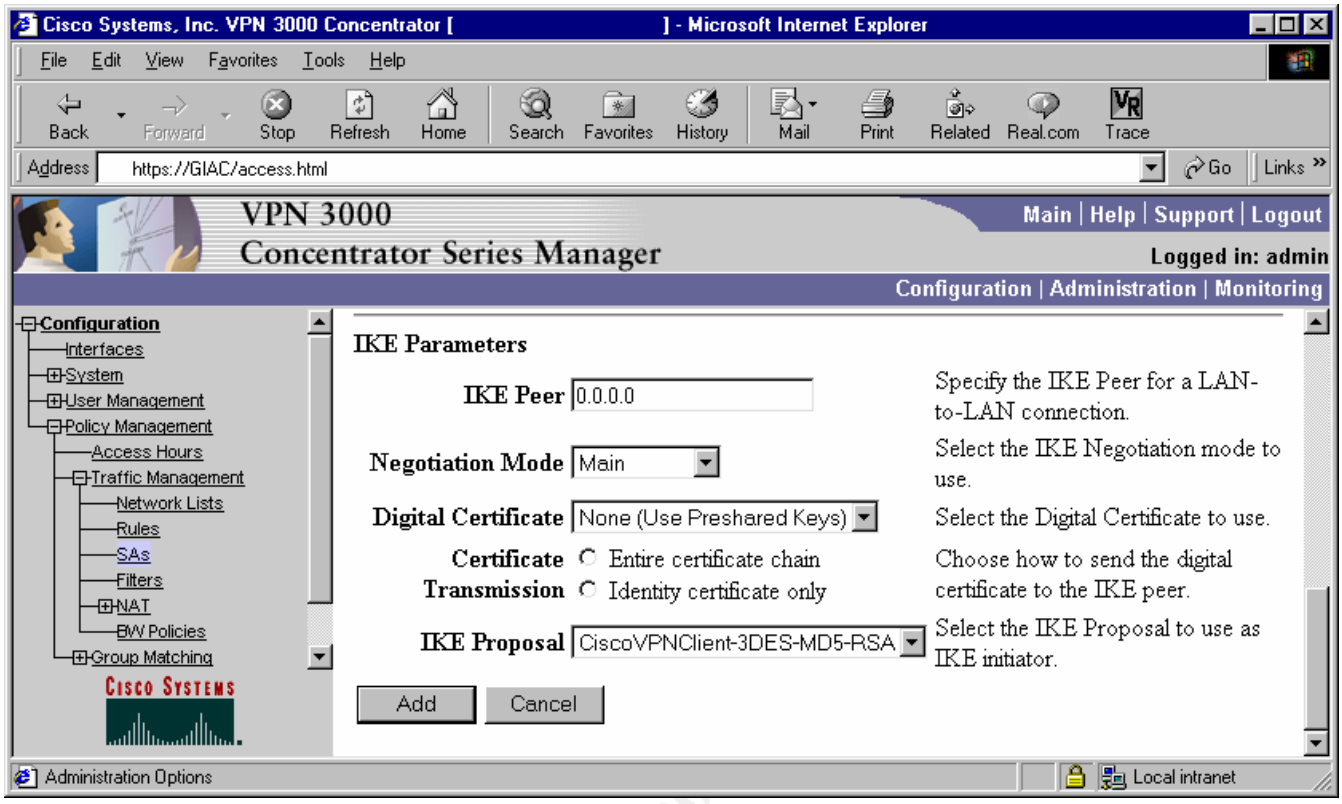


Figure 12 - SA IKE Parameters

3) After all the information has been entered click add to add the SA. We should now see the new SA in the SA list.

© SANS Institute 2000 - 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

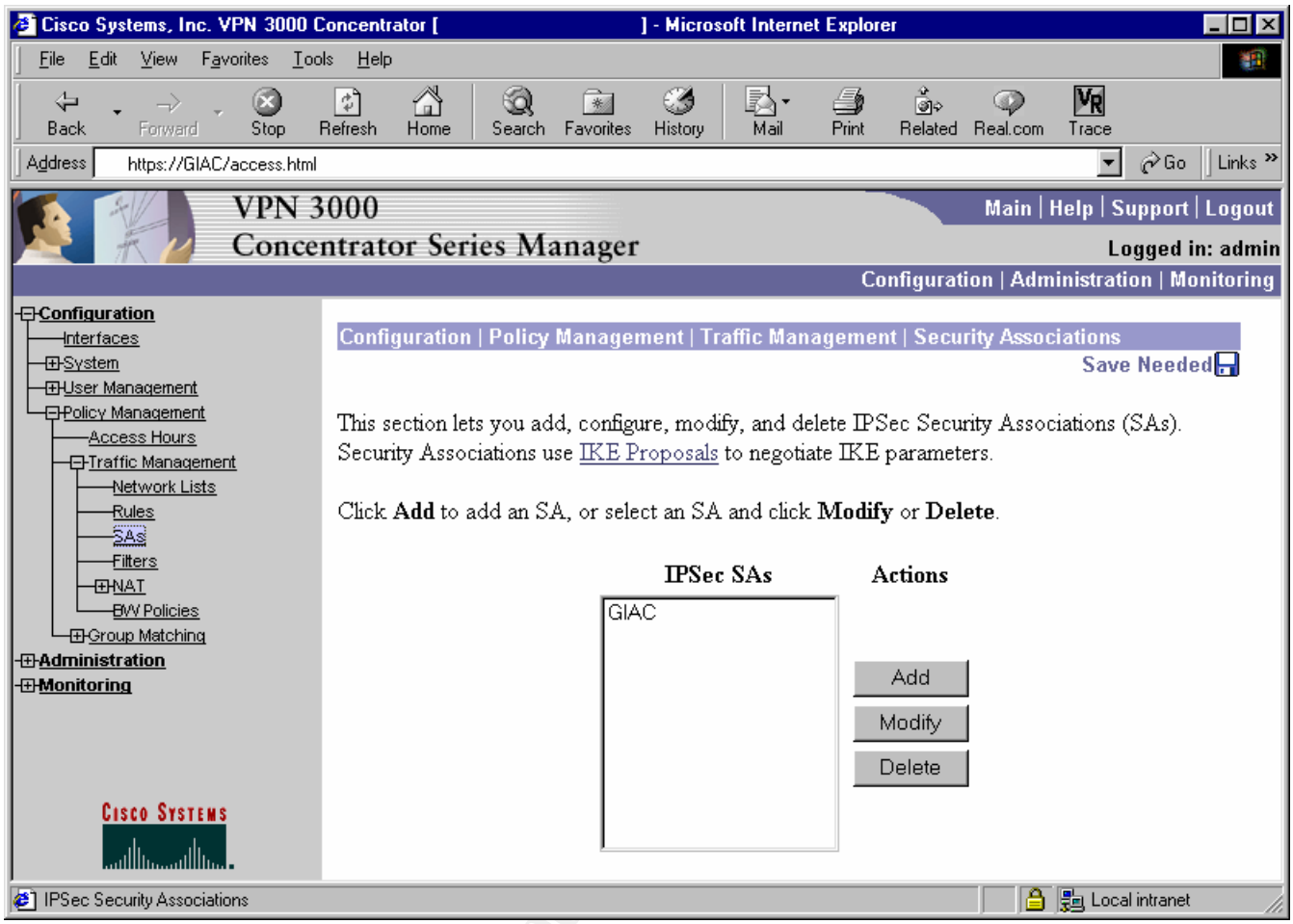


Figure 13 - GIAC SA List

Create Rules

Next we will create rules to define traffic that will be allowed. This part is kind of tricky because for each connection we must create a rule to allow the traffic in one direction and then create a separate rule to allow traffic in the other direction.

1) Go to Configuration -> Policy Management -> Traffic Management -> Rules. Click the Add button to add a new Rule.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

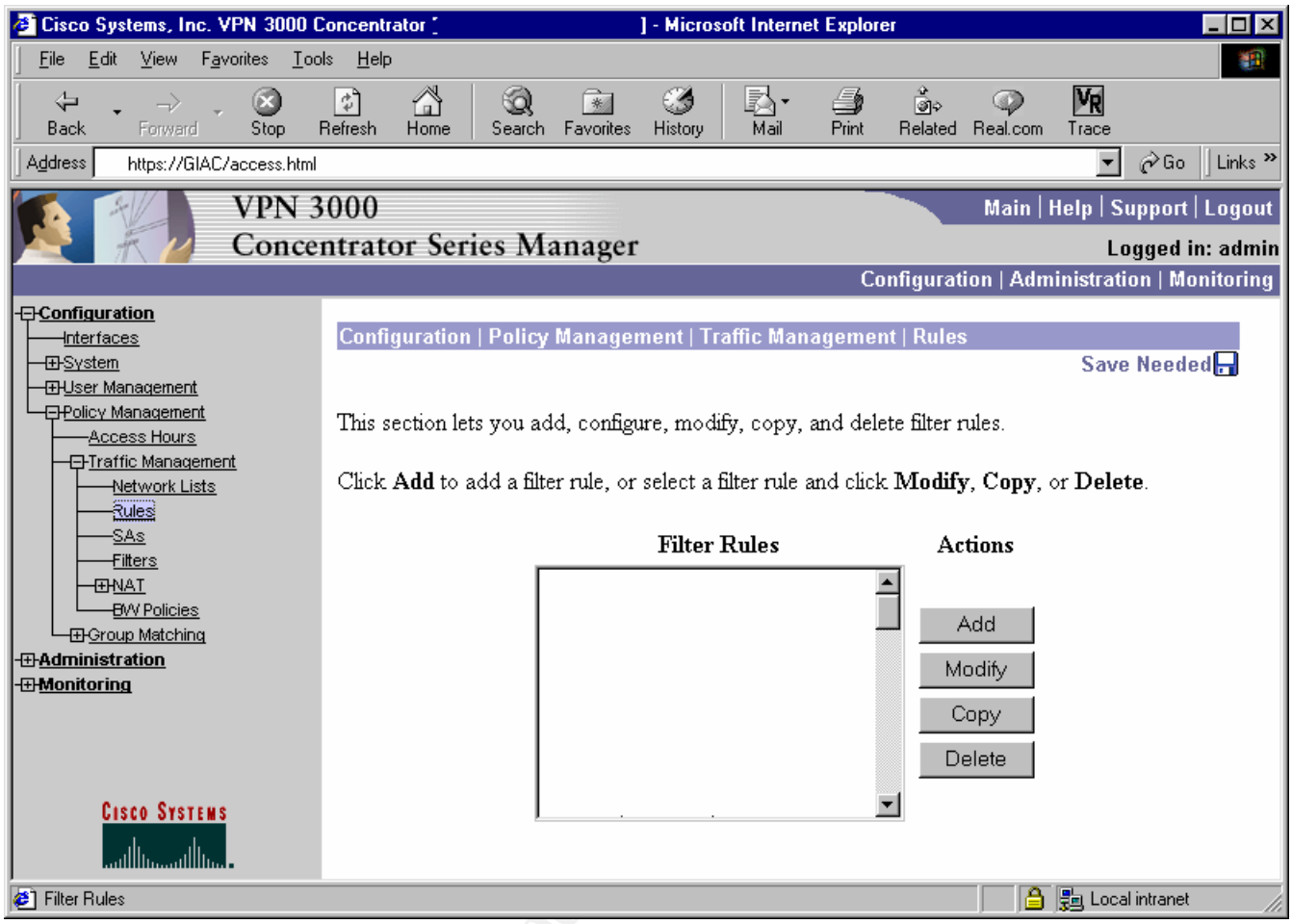


Figure 14 - Rules List

2) First we will create an inbound rule to support tcp/1433 connections to the database server. Directions correspond to the direction of traffic flowing through the concentrator interface. For instance Inbound refers to traffic coming from a remote client into the concentrator. Outbound refers to traffic going to a remote client. Fill in the fields as appropriate using the following guidelines:

   - Rule Name – name of the rule, we will call this one DB_Server_in
   - Direction – direction of traffic to which this rule applies, Inbound
   - Action – action to perform on the traffic, options include drop, drop and log, forward, forward and log, apply IPSec, apply IPSec and log. The logging options are intended to only be used for debugging purposes. The IPSec options only apply to LAN-to-LAN connections. The other options are to drop the traffic or forward it through the box. We will choose forward.
   - Protocol – specify the protocol we are referring to, TCP

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- TCP Connection – specifies whether the rule applies to established connections or any connection, in order to allow new connections we must select Don't Care
- Source Address – specify the source address of the rule. Our users will be tunneling and will be assigned a DHCP address on the 192.168.4.0/24 network, hence this will be the source of the rule. One may use either a pre-defined network list or IP/wildcard mask pair.
- Destination Address – specify the destination address of the rule. This will be the address of the DB_Server for which we have a pre-defined network list.
- TCP/UDP Source Port – specifies the source port for the rule. This can either be a specific pre-defined port or a range of ports. We will be using a range of all possible port values since this refers to the client side of the connection.
- TCP/UDP Destination Port – specifies the destination port for the rule. Since tcp/1433 is not one of the pre-defined ports we will use a range from 1433 to 1433.
- ICMP Packet Type – specifies the type number associated with various types of ICMP packets. This rule does not refer to ICMP therefore we will ignore this option.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

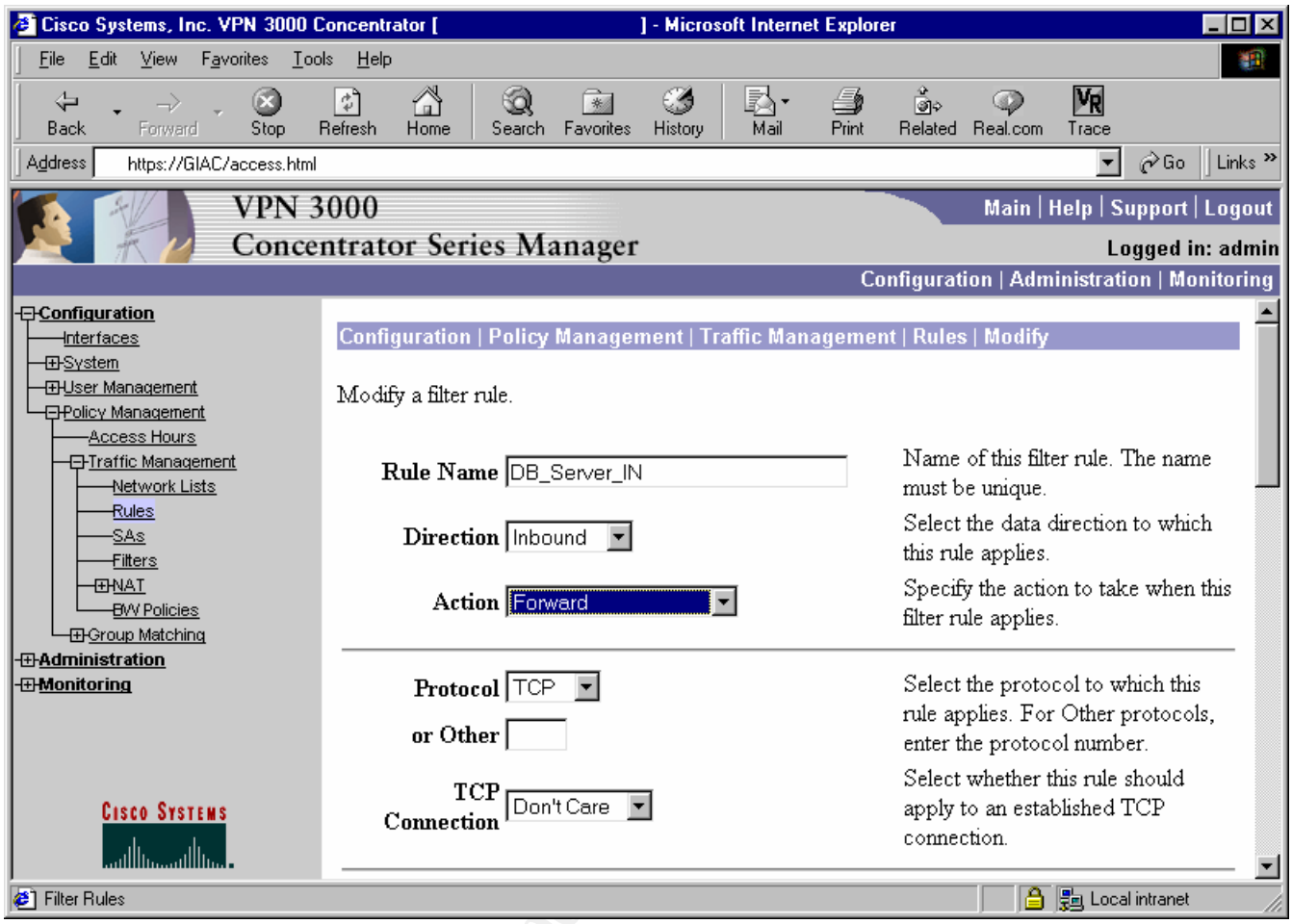


Figure 15 - Rule Name

© SANS Institute 2000 - 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

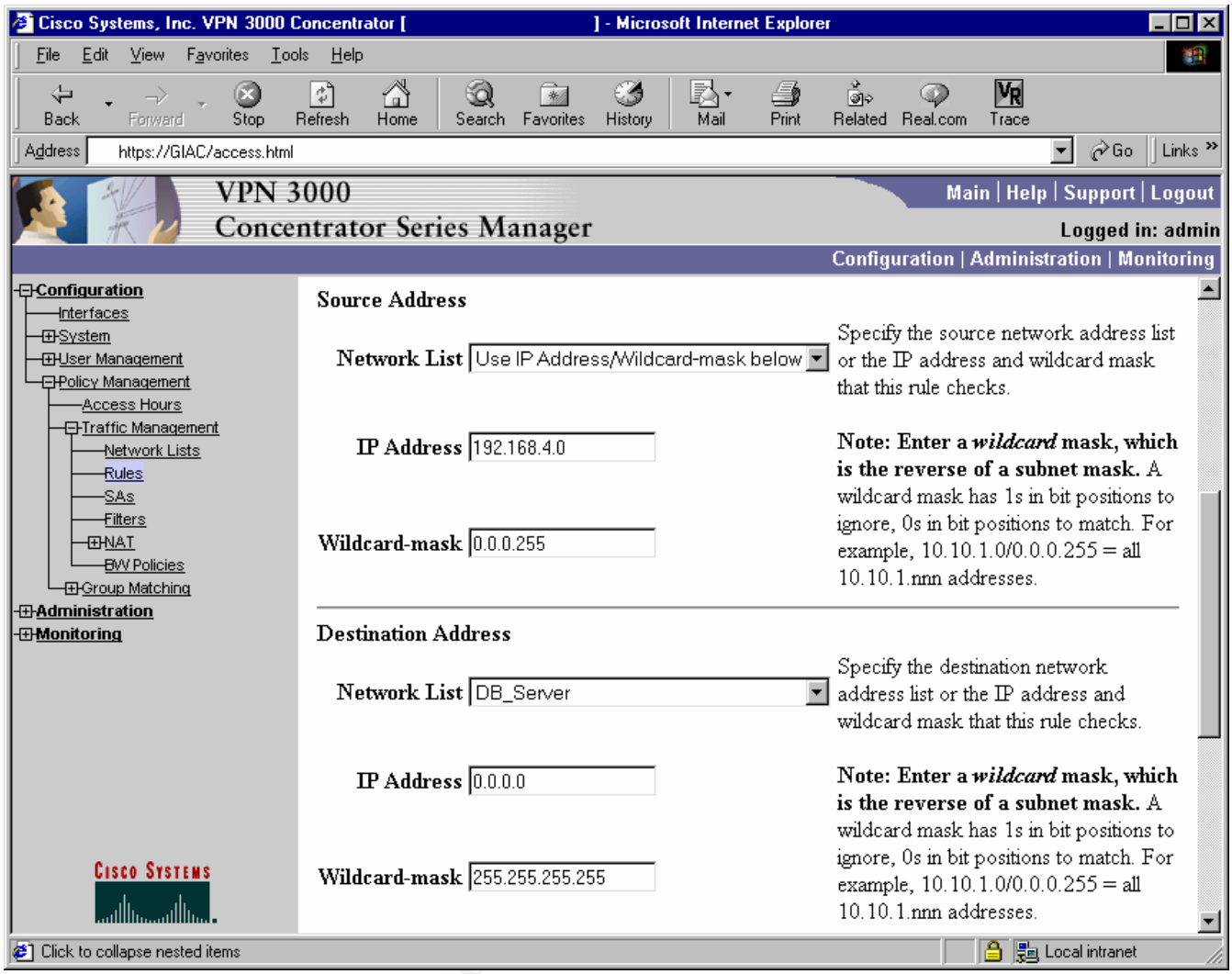


Figure 16 - Source/Dest Address

© SANS Institute

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

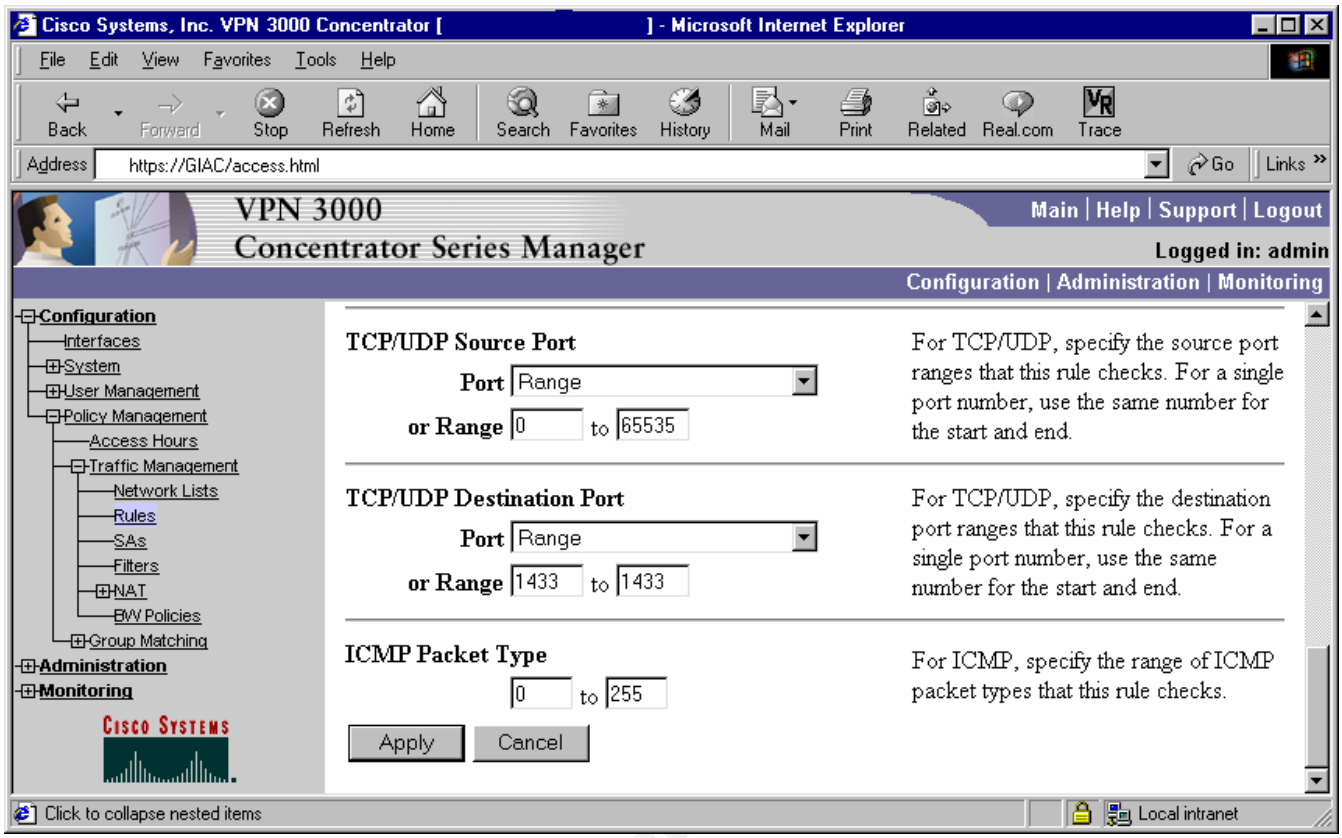


Figure 17 - Port Information

3) Create an outbound to support database connections. This rule will essentially be the opposite of the inbound rule. Repeat this procedure for MAIL_SRV_SMTP_in, MAIL_SRV_SMTP_out, MAIL_SRV_POP_in, and MAIL_SRV_POP_out.

© SANS Institute 2000 - 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

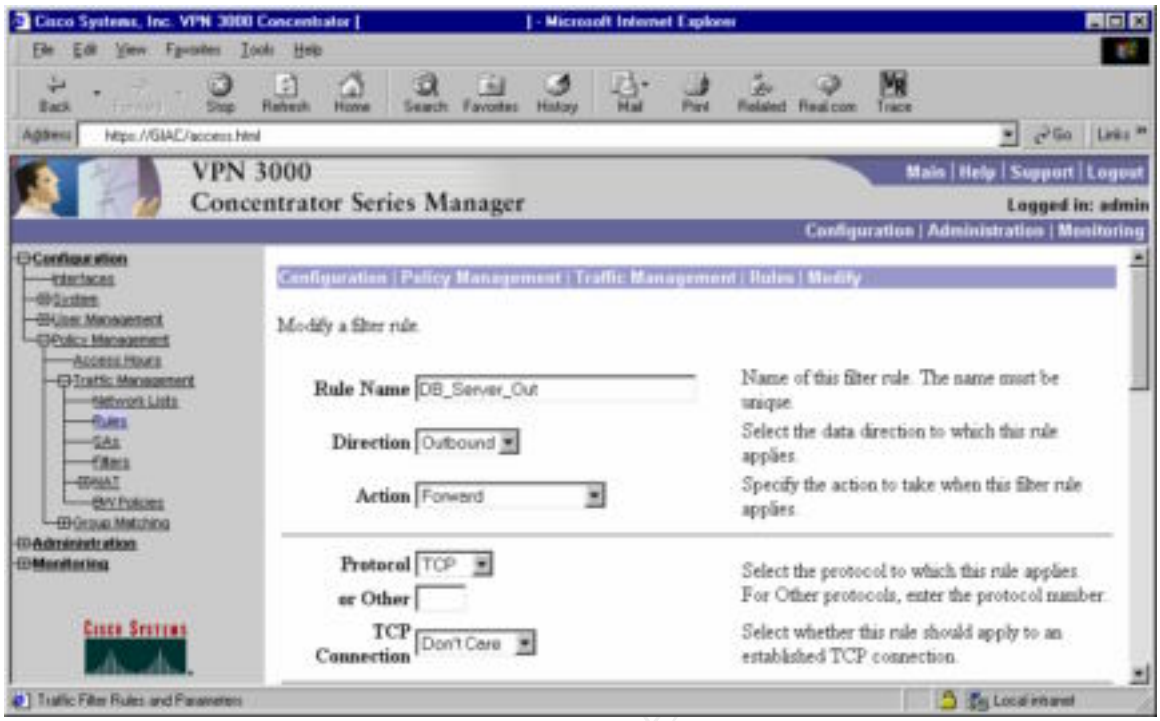


Figure 18 - Rule Name Outbound

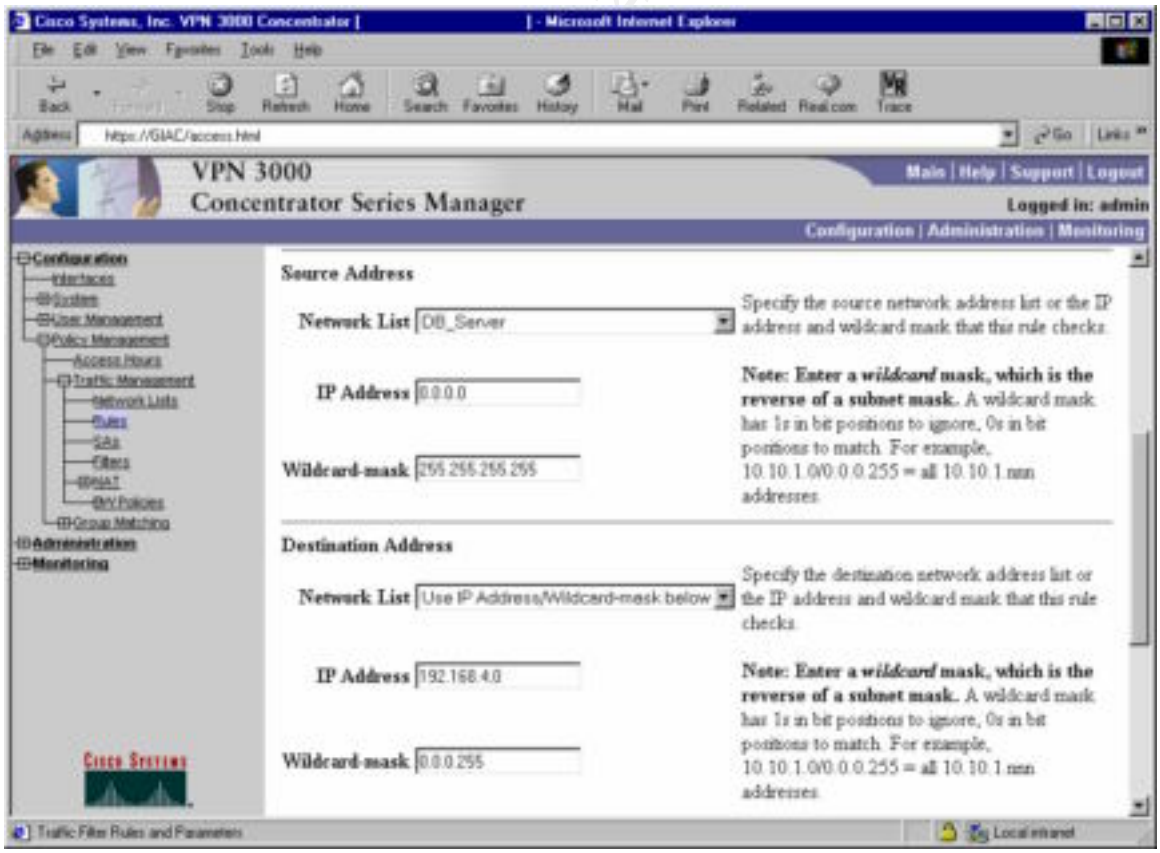


Figure 19 - Source/Dest Address Outbound

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

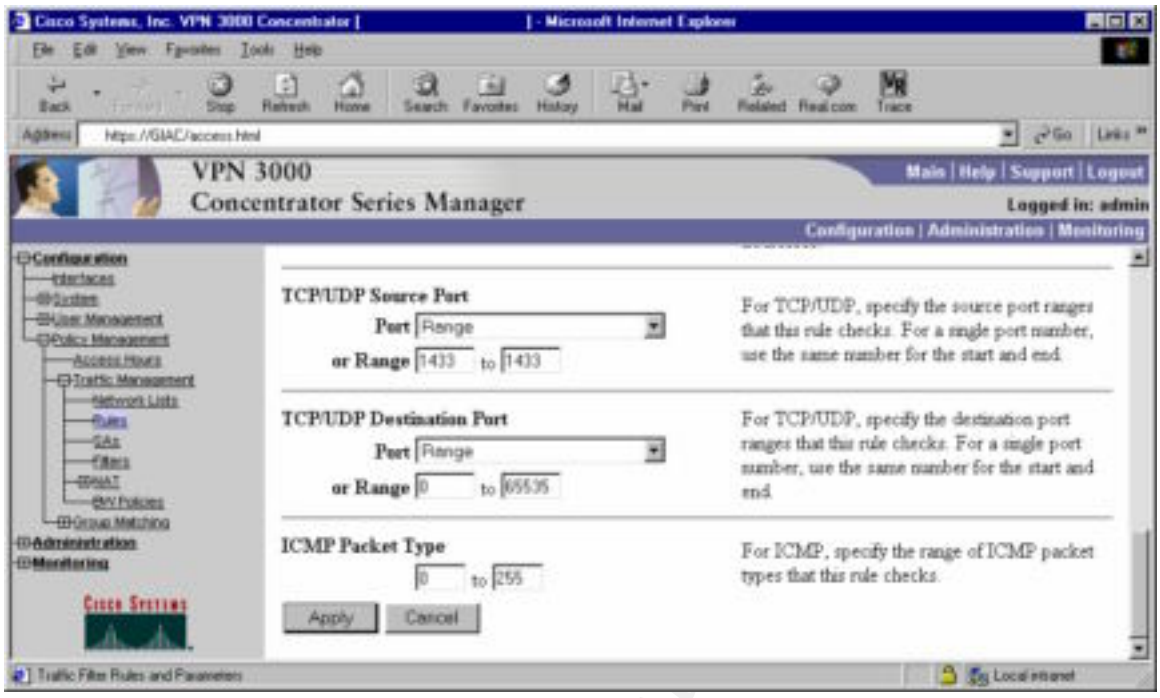


Figure 20 - Port Information Outbound

4) After creating all of the rules we should be able to see them in the main Rule List screen.

Figure 21 - GIAC Rule List

Create Filters

Next we will create filters for each group. These filters are basically collections of rules that act as a firewall policy. We will create a partners

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

filter that allows traffic to and from the database server and an appropriate roadwarriors filter.

1) Go to Configuration -> Policy Management -> Traffic Management -> Filters. Click the Add button to add a new Filter.

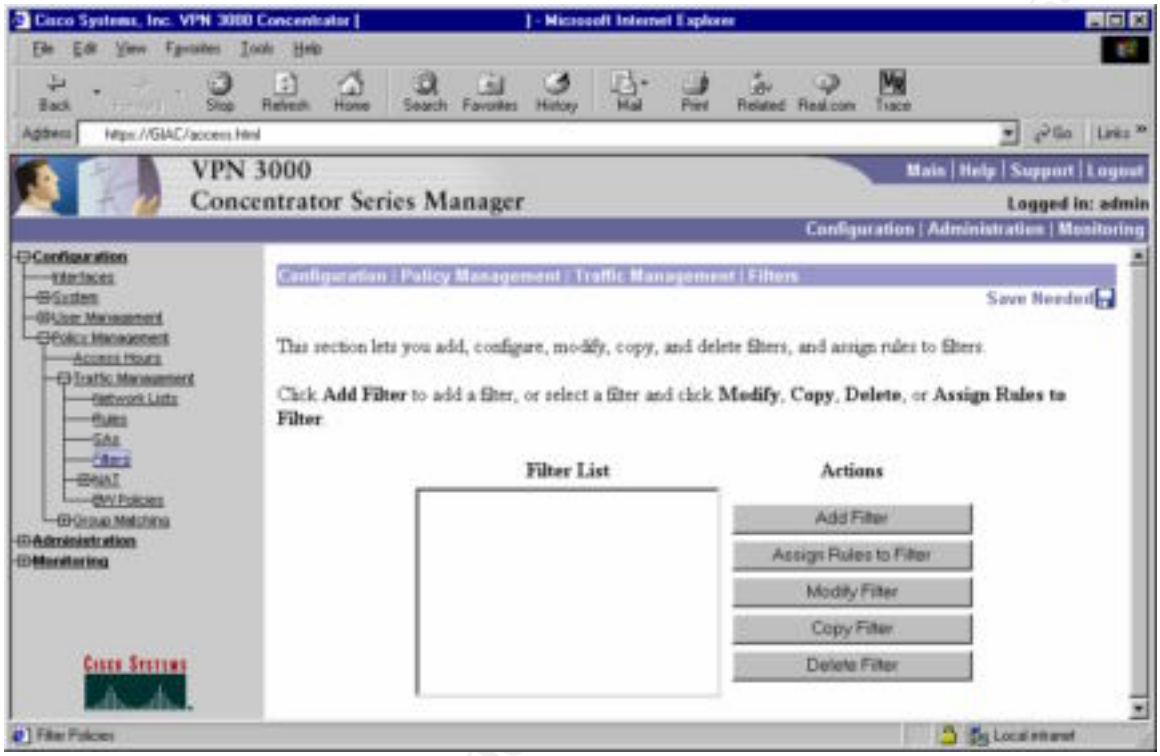


Figure 22 - Filter List

2) Fill in the appropriate information according to the following guidelines and click Add:

- Filter Name – specifies a name for the filter, we will call it partners
- Default Action – the default action for the filter. Options include Drop, Forward, Drop and Log, or Forward and Log. We will choose to Drop since we want to drop traffic not explicitly allowed.
- Source Routing – check this box to allow ip source routing, we do not want to allow source routed packets into our network so leave the box unchecked
- Fragments – check this box to allow fragmented packets to pass
- Description – enter a description for this filter

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

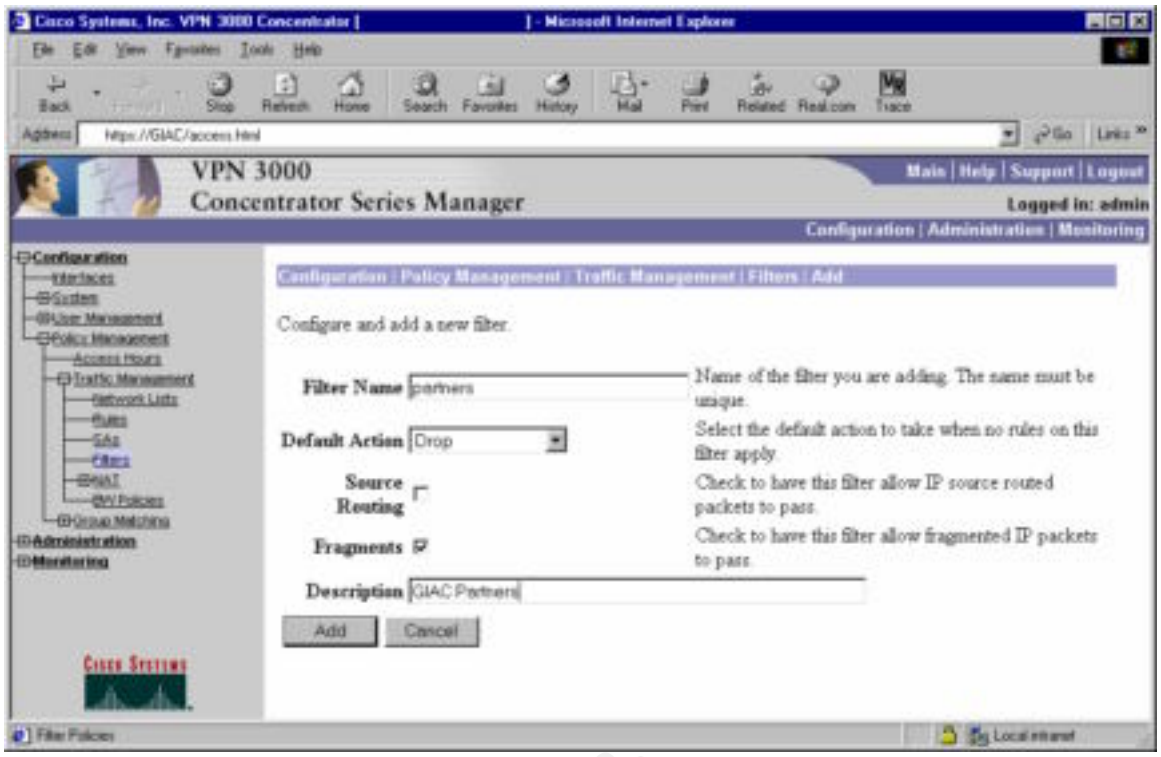


Figure 23 - Add Filter

3) Find the rules created for this filter, select the appropriate rule and click add to add the rule to the filter. When finished adding the rules to the filter click done.

© SANS Institute 2000 - 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

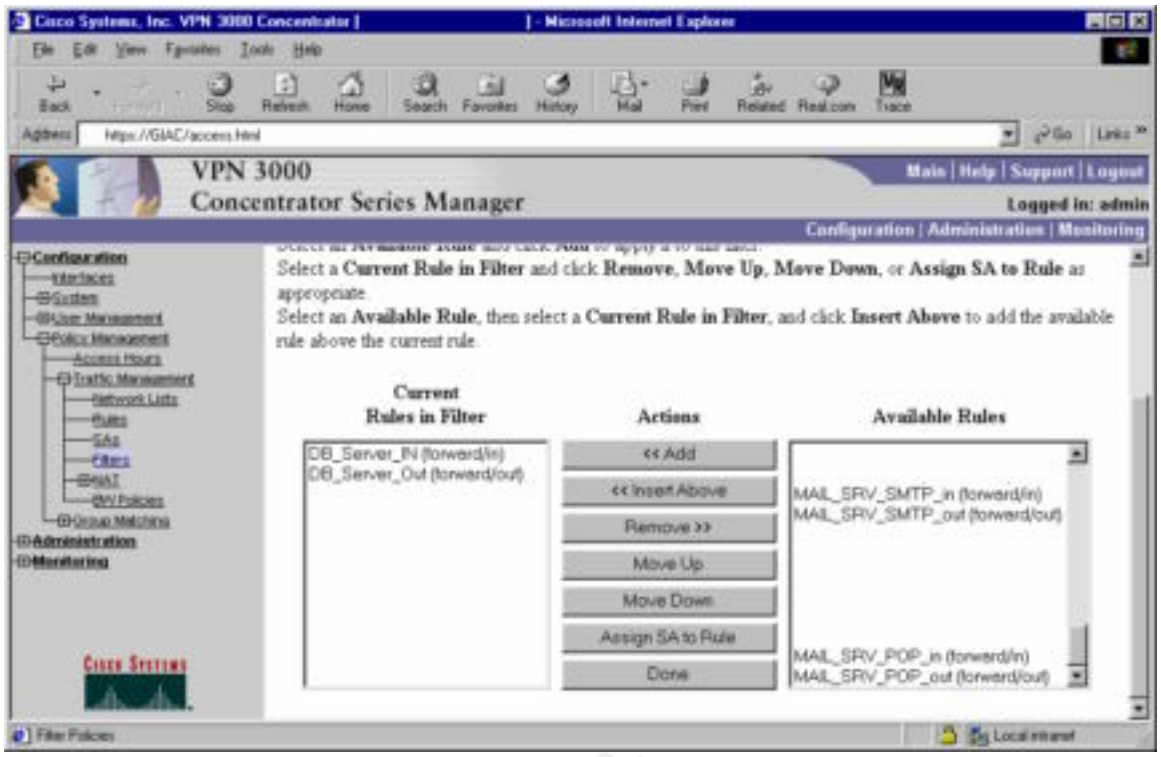


Figure 24 - Assign Rules to Filter

4) Repeat for the roadwarriors group. Upon completion we should see the newly created filters in the main filter list screen.

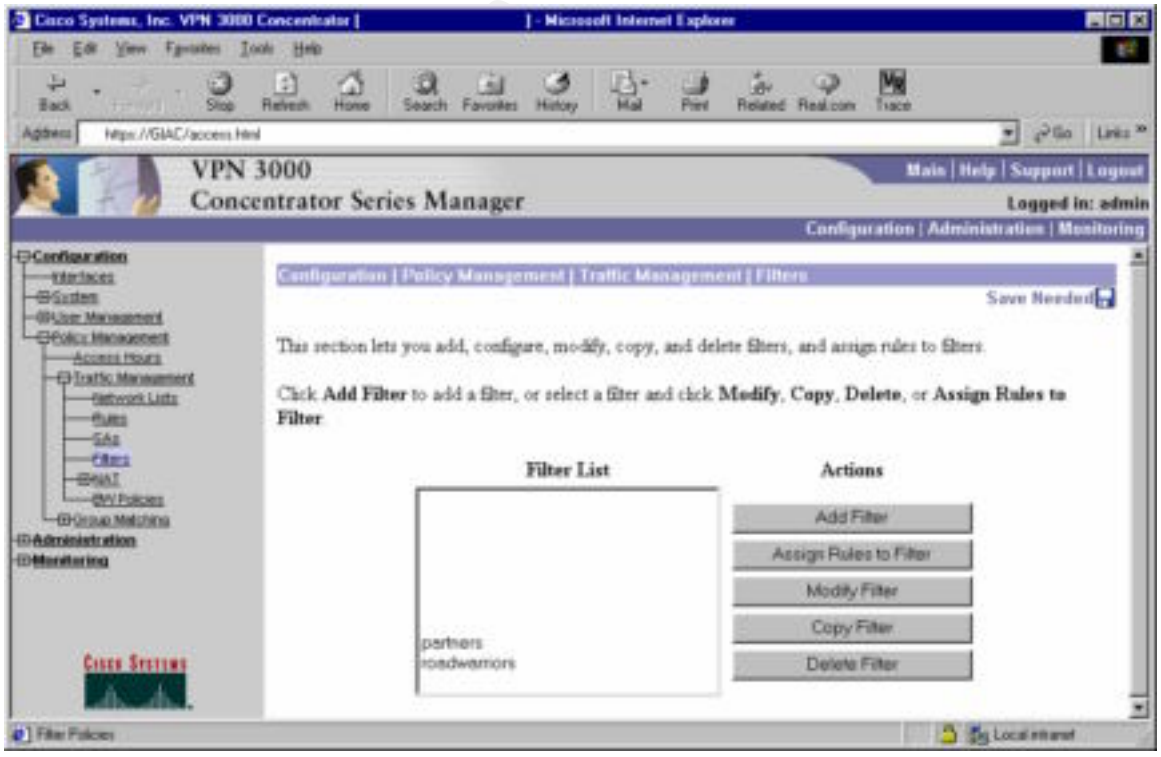


Figure 25 - GIAC Filter List

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Create Groups

Next we will create groups as defined in the connection requirements.

1) Go to Configuration -> User Management -> Groups. Click the Add Group button to add a new Group.

2) Fill out information according to the following guidelines:
   - Identity Tab
     - Group Name – the name of the group, partners
     - Password – the group password
     - Verify – verify the group password
     - Type – whether the group is defined internally (on the concentrator) or externally (in RADIUS), this group is defined internally

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

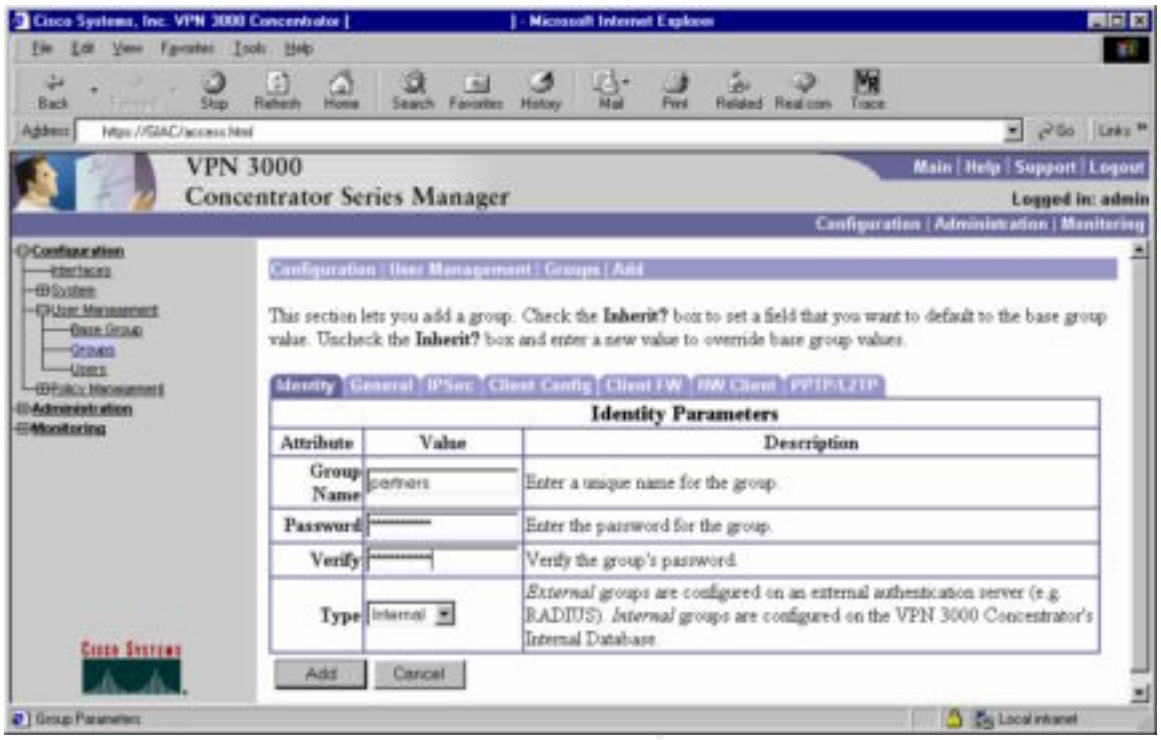


Figure 26 - Group Identity Tab

- General Tab
  - Access Hours – defines times that users in the group are allowed to connect to the concentrator. We have set this to Business Hours, which is a built in group that allows connection M-F from 9-5.
  - Simultaneous Logins – specifies the number of simultaneous logins allowed per user in a group. Set to 1.
  - Minimum Password Length – specifies the minimum password length for internally configured userids and passwords.
  - Allow Alphabetic-Only Passwords – check this box to allow passwords that only contain alphabetic characters. Obviously we do not want to do this because it allows for weak passwords.
  - Idle Timeout – specifies the number of minutes a user may remain idle before being kicked off the server
  - Maximum Connect Time – specifies the minutes a user may remain connected for any one time
  - Filter – specifies the filter that is to be used for this group. Set to partners filter that we created before.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Primary & Secondary DNS – specifies the primary and secondary DNS information sent to clients who were given a DHCP address from the pool configured internally on the concentrator.
- Primary & Secondary WINS – specifies the primary and secondary WINS information sent to clients who were given a DHCP address from the pool configured internally on the concentrator.
- SEP Card Assignment – a SEP is a special hardware processor used for encrypting and decrypting. One may have up to 4 SEPs in a Concentrator 3030. This specifies which SEPs a group is able to use when connecting.
- Tunneling Protocols – specifies which tunneling protocols may be used by the group. In our case only IPSec is used.
- Strip Realm – strips the realm from a username when performing authentication. For instance if the box is checked and the userid is given in the form user@realm, the realm is stripped and the user alone is used to authenticate.

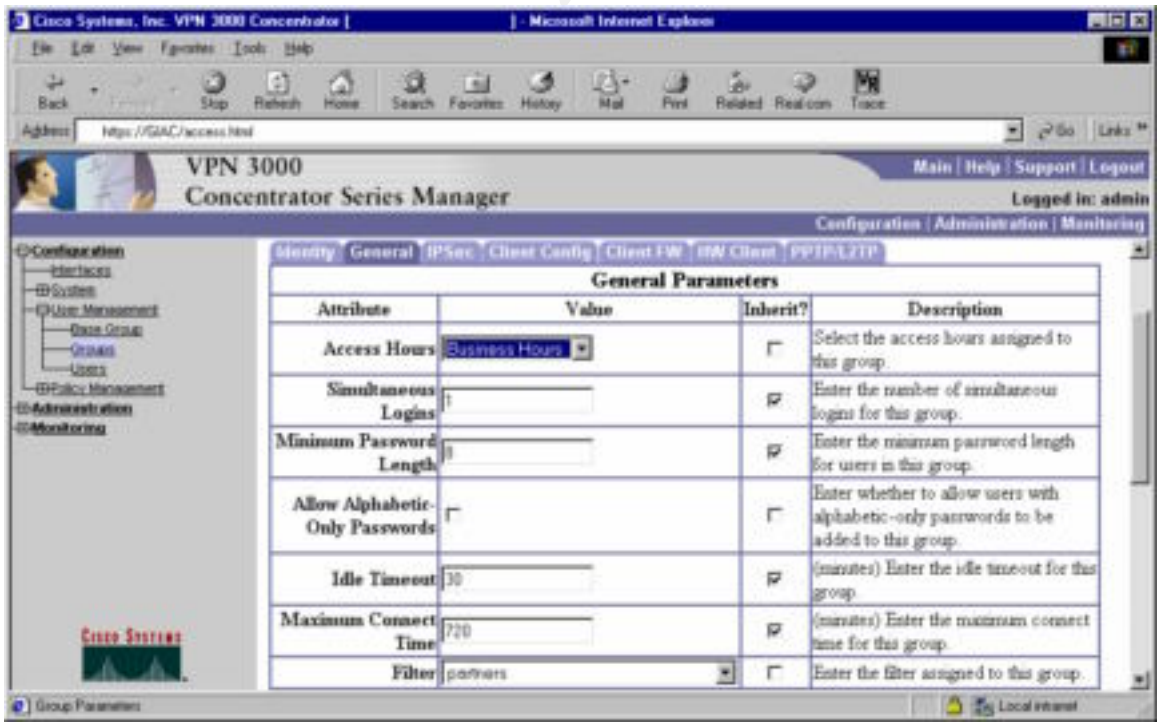


Figure 27 - Group General Tab

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

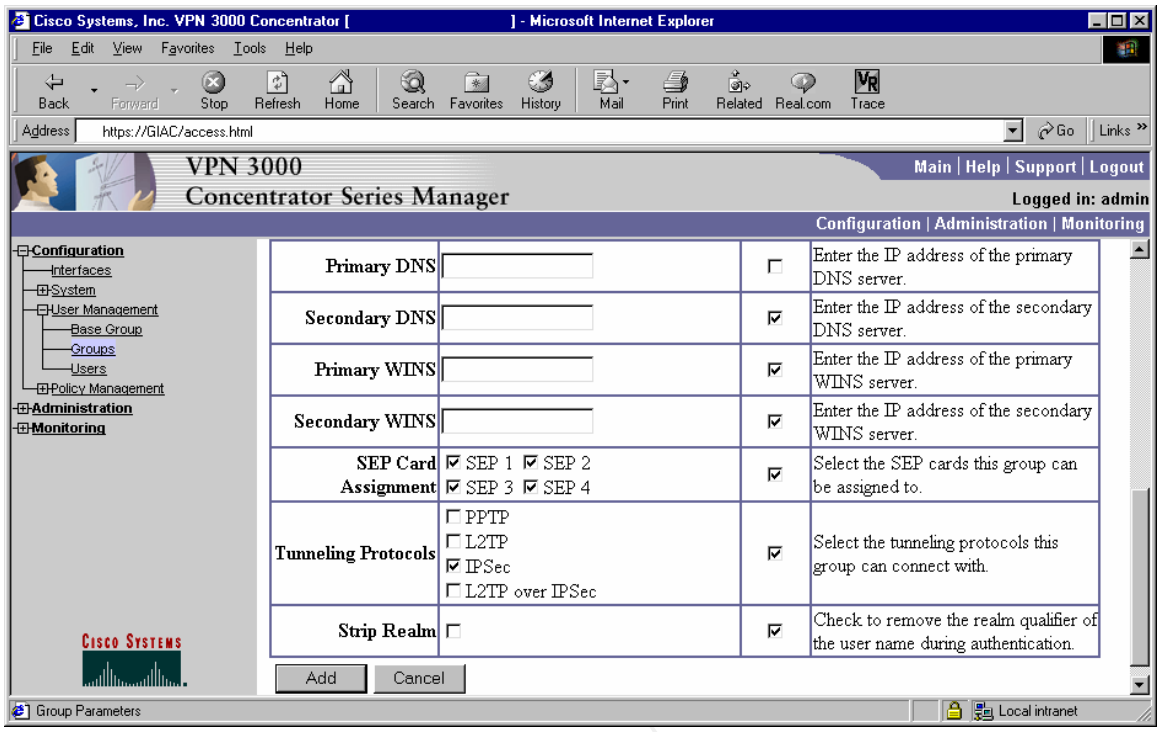


Figure 28 - Group General Tab (cont)

- IPSec Tab
  - IPSec SA – specifies the SA to use for the group. Set to the GIAC SA created earlier.
  - IKE Peer Identity Validation – checks the identity of the connecting system to the like value specified in the certificate for that system. Since we are not using certificates we will disable this by setting to "Do not check".
  - IKE Keepalives – sends keepalives to the remote client to make sure the client is still there, prevents hung connections
  - Tunnel Type – sets the tunnel type for the group, this is either LAN-to-LAN or Remote Access
  - Group Lock – if checked forces the client to authenticate through this group only
  - Authentication – specifies the type of authentication to use for users in this group. This can be None, RADIUS, RADIUS with expiry, NT Domain, SDI, and Internal
  - IPComp – specifies the method of IP Compression for this group. Can be either none or LZS.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Reauthentication on Rekey – if checked requires users to reauthenticate when a rekey occurs
- Mode Configuration – if checked enables Mode Configuration with IPSec clients

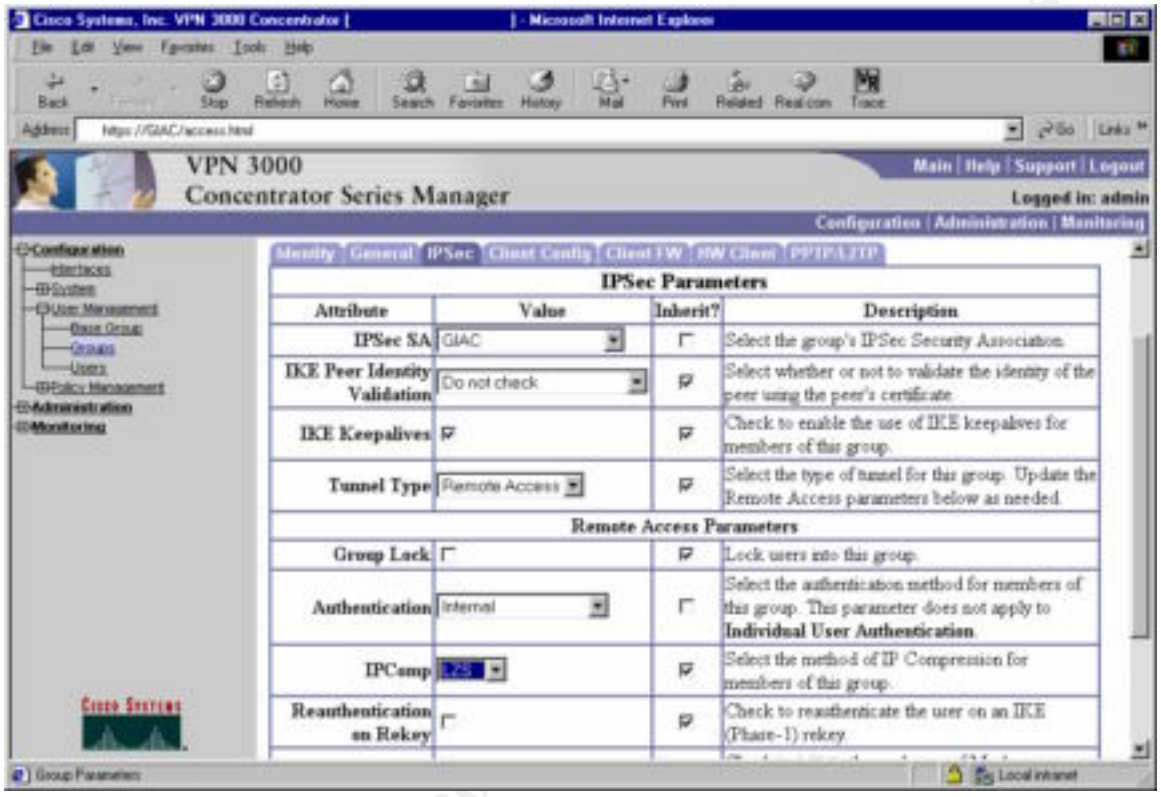


Figure 29 - Group IPSec Tab

Figure 30 - Group IPSec Tab (cont)

- Client Config Tab
  - Banner – sets the banner displayed to users of this group upon login

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Allow Password Storage on Client – if checked allows the client to save their password in the client software. This is better left unchecked since if a client saves his/her password on the local client and their machine gets stolen the thief would have access to our network.
- IPSec over UDP – allows a client to operate through a NAT device. This is necessary because our remote users should be behind Linksys routers.
- IPSec over UDP Port – specifies the UDP port to use for IPSec over UDP connections
- IPSec Backup Servers – we will ignore this option as it only pertains to the 3002 hardware client
- Intercept DHCP Configure Message – allows the concentrator to intercept DHCP packets and rewrite some of the information specified in the packets
- Subnet Mask – specifies subnet mask given to clients requesting Microsoft DHCP options
- Split Tunneling Policy – specifies whether to allow split tunneling and to which addresses. We want to tunnel everything because split tunneling could provide an attacker with a back door into our network. If an attacker has compromised a machine that has connected to our network via VPN, that attacker could then possibly launch attacks against our internal network from that machine.
- Default Domain Name – specifies the default domain name that the concentrator passes to the IPSec client
- Split DNS Names – used with split tunneling to allow tunneled traffic to be resolved through the internal DNS and non-tunneled traffic to be resolved through some other DNS such as the user's ISP.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

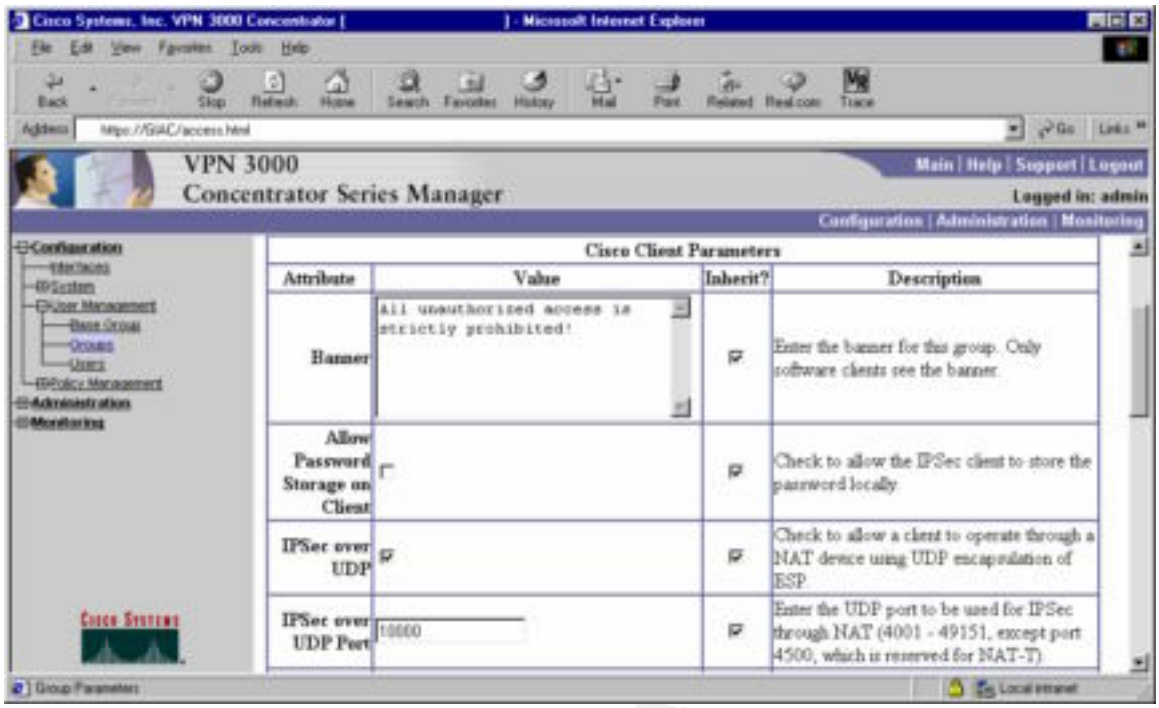


Figure 31 - Group Client Config Tab

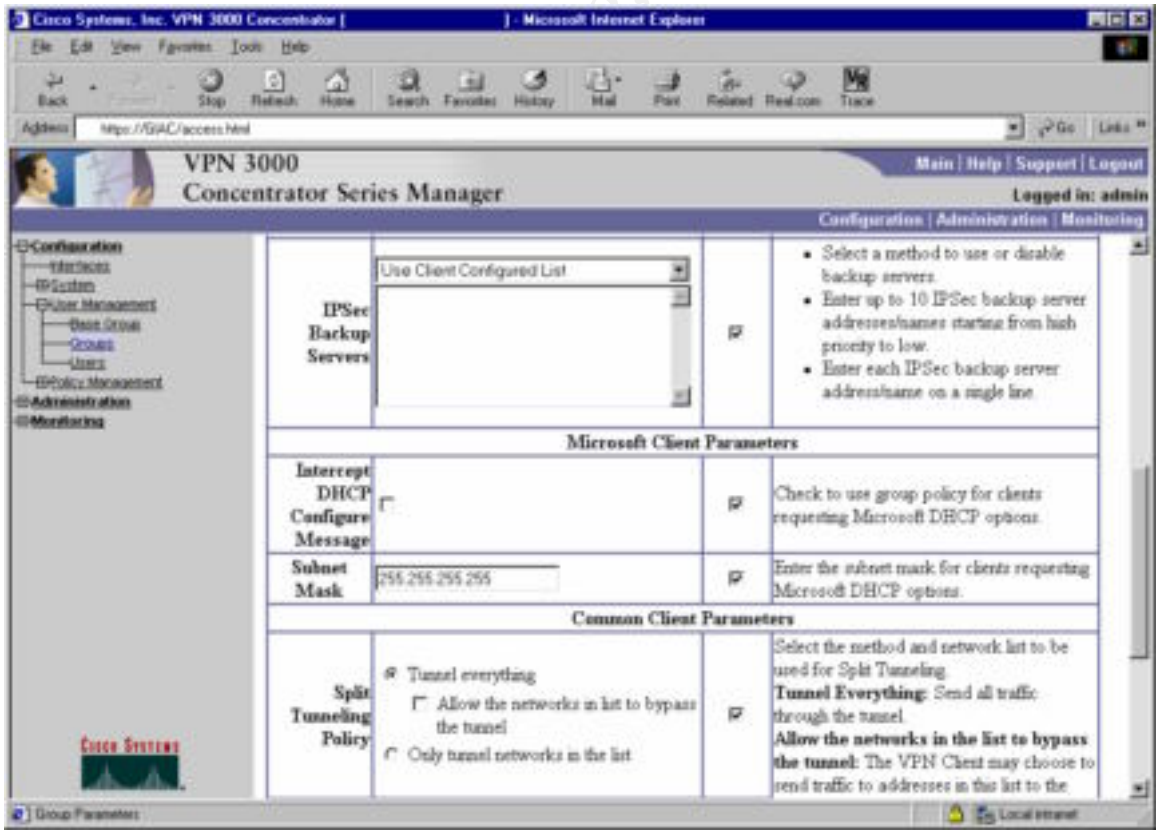


Figure 32 - Group Client Config Tab (cont)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

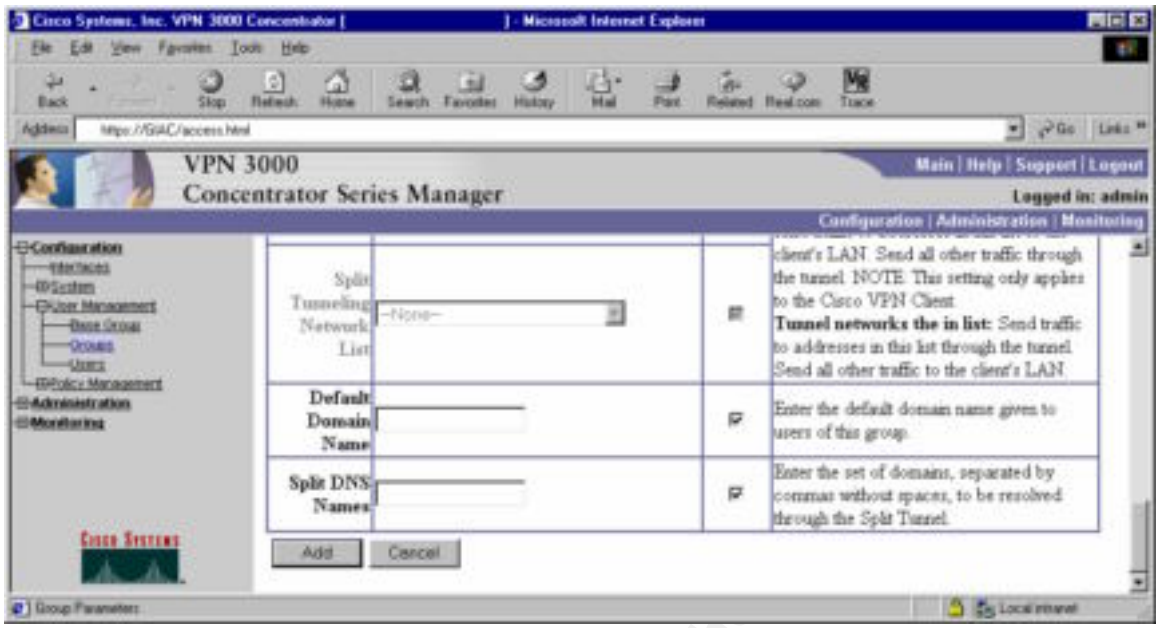
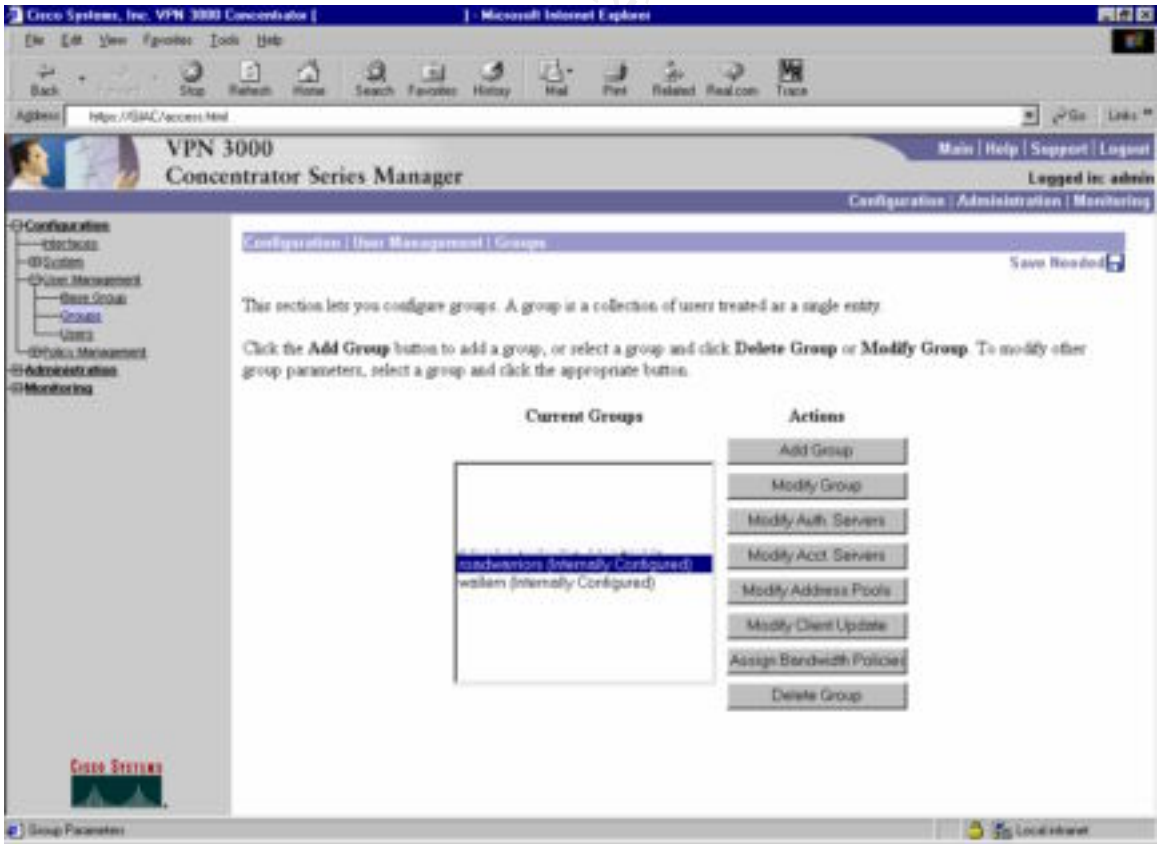


Figure 33 - Group Client Config Tab (cont 1)

3) Repeat these steps for the roadwarriors group. Upon completion we should see all groups we have configured in the main Groups screen.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Order of Rules

When rules are added to a filter they are processed sequentially. Inbound rules are processed first and then outbound rules.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment #3 – Verify the Firewall Policy

Planning

The purpose of this audit is to verify the firewall policy. In performing the audit we need to verify two things: 1) the firewall is indeed blocking traffic we intend for it to, and 2) the firewall is allowing legitimate traffic. We will verify the policy using the following guidelines:

1) verify connections are being dropped to the firewall from each network except the 192.168.3.0 network (for practicality we will consider connections from our public network to be the same as Internet addresses)
2) verify that appropriate connections are being allowed from the 192.168.3.0 network to the firewall
3) verify that appropriate connections are being allowed from the 192.168.3.0 network to other networks (172.16.0.0/24, 192.168.4.0/24, 192.168.0.0/24)
4) verify connections from outside to the service network
5) verify connections from inside
6) verify connections from VPN private network (192.168.4.0/24)
7) verify connections from server to server

In performing the tasks mentioned above we would use nmap running on a laptop. I believe nmap will be all we need to use because we are not required to perform a vulnerability analysis rather we are just concerned that the firewall is performing as expected. With this in mind, we need only be concerned about verifying access up to layer 4 (of the OSI model) since we are not using any proxies on the primary firewall. The firewall could be audited at any time, however it is preferred to perform the audit at a time when we are able to disconnect the internal network and the Internet connection so it is easier to verify that only the traffic from the audit is being seen on the network. The audit is expected to take roughly 6 hours using 2 people. Since there is no cost for software or hardware the costs for the audit come down to 12 man-hours. The firewall is located in the GIAC Enterprises Data Center which has restricted access and is staffed 24x7, therefore physical security is assumed.

Before we perform our audit we must obtain written permission from the CIO or another appropriate Executive for GIAC Enterprises.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Execution

Connections to the firewall

The first step in our audit is to verify connections to the firewall from the management network 192.168.3.0/24 and another network namely the 172.16.0.0/24 network. From each network we will perform a UDP scan (-sU), a TCP half-open SYN scan (-sS), OS detection, and a ping to check for ICMP.

- 172.16.0.0/24 Network

  nmap –sU –p 1-65535 172.16.0.2

  This scan checks for listening UDP ports in the range of 1 – 65535 (all possible ports). This scan can take a long amount of time to complete. Because we are dropping all traffic directed at the firewall except from the 192.16.3.0 network, all ports were in state filtered.

  nmap –sS –p 1-65535 172.16.0.2

  This scan checks for listening TCP ports in the range of 1 – 65535 (all possible). Again all ports were in state filtered because we are dropping all traffic directed at the firewall except from the 192.16.3.0 network.

  nmap –O 172.16.0.2

  This scan attempts to remotely identify the operating system of the target host. Because it could not find at least one open and one closed port the scan failed.

  ping 172.16.0.2

  This scan attempts to send an ICMP echo request to the target and looks for an ICMP echo reply packet to be returned. This scan failed because all traffic to the firewall is being dropped.

- 192.168.3.0/24 Network

  nmap –sU –p 1-65535 192.168.1.1

  ```
  Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
  Interesting ports on 192.168.1.1 (192.168.1.1):
  (The 65533 ports scanned but not shown below are in state: filtered)
  Port       State       Service
  259/udp    open        firewall1-rdp
  500/udp    open        isakmp
  ```

  nmap –sS –p 1-65535 192.168.1.1

  ```
  Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
  Interesting ports on 192.168.1.1 (192.168.1.1):
  (The 65529 ports scanned but not shown below are in state: filtered)
  ```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Port State Service
22/tcp open ssh
256/tcp open rap
257/tcp open set
258/tcp open yak-chat
259/tcp open esro-gen
900/tcp open unknown

nmap –O 192.168.1.1

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Interesting ports on 192.168.1.1 (192.168.1.1):
(The 1543 ports scanned but not shown below are in state: filtered)
Port State Service
22/tcp open ssh
256/tcp open rap
257/tcp open set
258/tcp open yak-chat
259/tcp open esro-gen
900/tcp open unknown

Remote operating system guess: Sun Solaris 8 early acces beta through actual release

ping 192.168.1.1

The ping test failed.

Connections from the management network

Next we configured a box on the 192.168.3.0/24 network and scanned the 192.168.4.0/24, 192.168.0.0/24, and the 172.16.0.0/24 network. The results of the scans are as follows:

IP	UDP Scan	TCP Scan	Ping Scan
192.168.0.1	259,500	22,256,257,258, 259,900	no response
192.168.0.2	All filtered	22	no response
192.168.0.3	All filtered	22	no response
192.168.0.4	All filtered	22	no response
192.168.0.5	All filtered	22	no response
192.168.0.6	All filtered	22	no response
192.168.4.1	259,500	22,256,257,258, 259,900	no response
192.168.4.2	All filtered	22	no response
172.16.0.1	259,500	22,256,257,258, 259,900	no response
172.16.0.2	All filtered	23	no response
172.16.0.3	All filtered	25	no response

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

172.16.0.4	All filtered	80,443	no response
172.16.0.5	All filtered	All filtered	no response
172.16.0.6	53	53	no response

Connections to the Service Network

From the 172.16.0.0/24 network we ran the following commands to test connectivity to the service network(s). First we ran the following commands against the 172.16.0.0 network these are the public addresses for the 192.168.0.0/24 network.

nmap –sU –p 1-65535 172.16.0.0/24

nmap –sS –p 1-65535 172.16.0.0/24

nmap –O 172.16.0.0/24

nmap –sP 172.16.0.0/24

The results of the scan were as follows:

IP	UDP Scan	TCP Scan	OS Scan	Ping Scan
172.16.0.3	All filtered	25	no closed ports found	No response
172.16.0.4	All filtered	80, 443	no closed ports found	No response
172.16.0.5	All filtered	All filtered	no open or closed ports found	No response
172.16.0.6	53	53	no closed ports found	No response

Next we performed a scan against the 172.16.1.0/30 network:

nmap –sU –p 1-65535 172.16.1.0/30

nmap –sS –p 1-65535 172.16.1.0/30

nmap –O 172.16.1.0/30

nmap –sP 172.16.1.0/30

The results of the scan were as follows:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IP	UDP Scan	TCP Scan	OS Scan	Ping Scan
172.16.1.1	All filtered	All filtered	no open or closed ports found	No response
172.16.1.2	500	All filtered	no closed ports found	No response

Connections from inside network

Next we performed nmap scans from the 10.x.x.x network to the 192.168.0.0/24, and the 192.168.4.0/24. To perform testing of outbound http, https, DNS, and ftp we simply started a web browser configured to use the outbound http proxy and attempted to connect to an http site, an https site, and download a file from an ftp site. Since all sites had URLs that were required to be resolved this verified that the internal DNS server is able to resolve external names. Since we were able to get to a few of each type of site, this verified that outbound http, https, and ftp are working through the firewall.

The results of the scans are as follows:

IP	UDP Scan	TCP Scan	Ping Scan
192.168.0.6	All filtered	22	No response
192.168.4.0/24	All filtered	All filtered	No response

Connections from VPN

Next we connected our laptop to the VPN private subnet and assigned it an address on the 192.168.4.0/24 network. We ran scans against the 192.168.1.0/24 and the 192.168.2.0/24 network. The results of the scans are as follows:

IP	UDP Scan	TCP Scan	Ping Scan
192.168.1.2	All filtered	25,110	No response
192.168.2.2	All filtered	1433	No response

Connections from Server to Server

Next we verified connections from server to server to make sure that the proper connections are set up between devices.

The results of our findings are as follows:

Source	Destination	UDP Ports	TCP Ports

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Router e0/0	Syslog 0	514	None
SMTP Gateway WWW Reverse Proxy External DNS WWW Server Syslog 0 VPN Private	Syslog 1	514	None
SMTP Gateway	Mail Server	None	25
Mail Server	SMTP Gateway	None	25
SMTP Gateway WWW Reverse Proxy External DNS WWW Server Syslog 0 Syslog 1 VPN Private	NTP Server	123	None
WWW Server	Database	None	1433

Evaluation

For the most part the firewall is configured correctly, however some interesting results came out of the firewall audit that cause some concern.

Connections to the Firewall

The requirement for management connections from the management network is for SSH (tcp/22) and FW1_mgmt (tcp/258). The audit revealed that in addition to these ports the following ports were open as well:

tcp/256,257,259,900

udp/259,500

We should remove the Firewall1 group from the services column in rule #1 on the firewall and replace it with the FW1_mgmt. This will

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

get rid of these unwanted ports that are currently accessible from the management network.

Connections to VPN public

As part of the scan of the service networks we scanned the VPN devices public interface. The result of this scan revealed that port udp/500 (IKE) is open. The only problem is that we require our roadwarriors to use a Linksys router when connecting their company laptop to the Internet outside of work. Since a Linksys router performs NAT we must support NAT'd IPSec connections. In order to accommodate this requirement we specified that we were going to use udp/10000 in the VPN policy. The problem is that apparently connections to port udp/10000 are being blocked by the firewall which leads one to conclude the following: 1) no roadwarriors are connecting through VPN, or 2) our roadwarriors are not using their Linksys routers. In either case we need to resolve this issue by adding a rule to allow connections from the Internet to the VPN public interface for udp/10000.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment #4 – Design Under Fire

The architecture I have chosen for this portion of the assignment is from the practical submitted by Stephen Monahan for his GCFW Certification. This practical may be found at http://www.giac.org/practical/Stephen_Monahan_GCFW.doc.

Internal Machine Compromise

First we will attempt to compromise an internal system in the hopes that we may use this system in an attack against the firewall itself. A lot of people do not consider VPN users to be internal, but once a VPN tunnel is established the network perimeter has been extended and that user very much becomes a part of the internal network. All the more reason to closely scrutinize VPN connection requirements for security. Since a Secure Pix firewall is being used as the primary firewall and for a VPN server as well, I think it is safe to assume that clients will be using some form of the Cisco VPN client software.

Time for some social engineering. Let's go in to drop off a bogus resume for a job. While we are there let's try to pick up on as much information about the company as possible. You would be surprised as to how much information people will disclose if you are inquiring about a position at the company. Also, have you ever noticed that a lot of companies require employees to wear ID badges? For instance my company requires me to wear an ID badge and on that badge is my name and employee ID. It is usually a good bet that companies use employee ids as userids for logging on to systems. This way people don't have to remember a bunch of different ID's and numbers. A quick glimpse around and we have a pretty good idea of what operating systems are being used on company laptops. So just from a quick visit to the company for a bogus job application we were able to find the following information:

- Bob Man is the HR hiring person
- His employee id is t123456
- His work number is 123-1111
- Bob runs Windows95 on his company laptop
- Bob just got cable modem access through ABC Communications and it is the best thing since sliced bread, I can email questions to him at bman@abccom.com

After speaking to bob, I go out to the parking lot and wait for him to leave for the day so we can follow him home to find out his address (123 Man St). To make the process of finding Bob out of all the other cable modem users easier we give ABC Communications a call:

> **Ted:** Hello, this is Bob Man. My machine blew up and I had to rebuild it but lost the piece of paper that had my IP address listed on it. Can you give me that information so I can get back up and running?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Op: What was the name on the account sir?

Ted: It is Bob Man, 123 Man St.

Op: That number is 1.2.3.4. Is there anything else I can help you with today sir?

Ted: No thanks, that will be all, thank you.

NOTE: An alternative method of finding Bob's IP would be to write a perl script to scan the netblock for ABC's broadband users using nbtstat, checking for Bob's employee ID. Something similar to the following would work:

```
#perl –w
use NetAddr::IP;

print "Enter search string: ";
chomp($search=<STDIN>);
print "Enter Network Addres: ";
chomp($netaddr=<STDIN>);
print "Enter Subnet Mask: ";
chomp($netmask=<STDIN>);

$ip = new NetAdd::IP($netaddr,$netmask);
@iplist = $ip->hostenum();
foreach $ipaddr (@iplist) {
        open(NBTSTAT,"nbtstat –A $ipaddr|") or warn;
        while($line=<NBTSTAT>) {
                if($line =~ /$search/i) {
                        print "Found at $ipaddr\n";
                        exit 0;
                }
        }
        close(NBTSTAT);
}
```

Anyone who has ever dealt with the phone operators at the local cable company knows that it is that easy to get information.

So now what? Since social engineering has gotten us this far lets see if it continues. Lets send an email to Bob:

To: Bob Man

From: Ted

Attachments: runme.bat game.exe patch.exe

Check this out Bob. Just detach all to a folder and run runme.bat.

Now if Bob runs the program we have just nailed him with netbus (patch.exe). With netbus installed we can download files particularly the connection profile used to store VPN information. For a Cisco VPN Client this information is typically stored in C:\\Program Files\Cisco Systems\VPN Client\profiles\ directory. The profiles are stored in the format <connection name>.pcf. By grabbing the connection profiles we have all of the connection and group information needed to connect to the system. All we need to get now is Bob's password. Bob uses

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the same userid and password to logon everywhere so using netbus we grab the PWL files (cached passwords) stored on Bob's machine in the Windows directory and use PWLTools to crack his password.

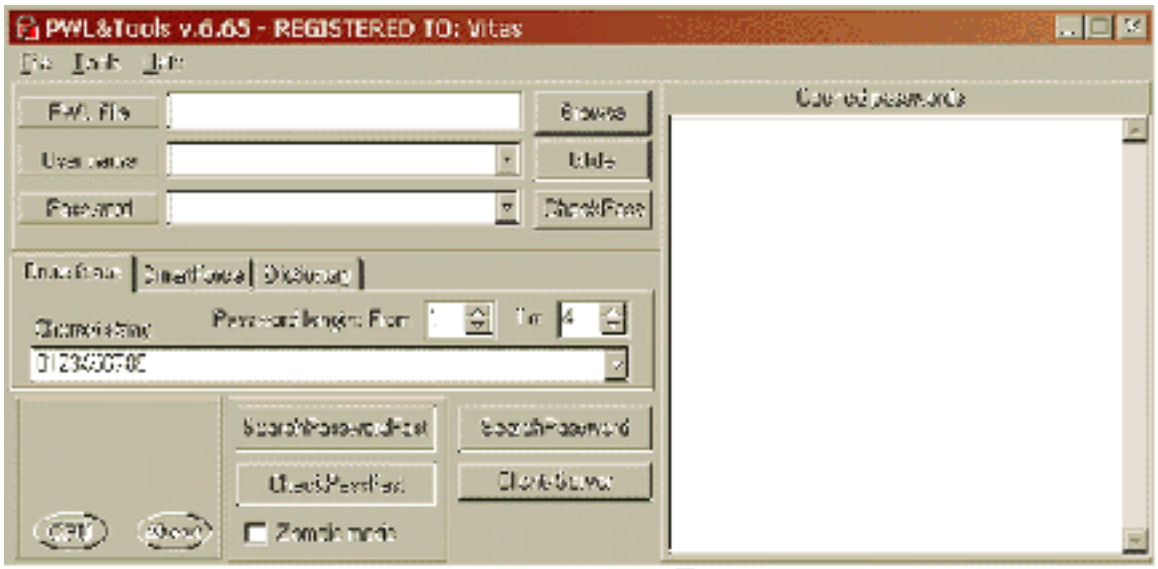


Figure 34 – PWLTools

Now all we have to do is grab a copy of the Cisco VPN Client software, available on Cisco's website and voila, we are able to VPN into the network.

Firewall Attack and DOS Attack

The version of firewall being used is Cisco Pix running software version 5.2. After searching Cisco's website we came across the following vulnerability:

http://www.cisco.com/warp/public/707/SSH-scanning.shtml

> Summary
>
> While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (http://www.cisco.com/warp/public/707/SSH-multiple-pub.html) we inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.

So it turns out that we can cause a denial of service against the firewall simply by sending a large packet to the SSH service running on the PIX firewall. Code for exploiting the CRC32 vulnerability may be found at:
http://downloads.securityfocus.com/vulnerabilities/exploits/ssh-exploit-diffs.txt

This code works by applying the changes included in the diff to the ssh client and recompiling. Then reconfigure the second program included with the path to the modified ssh program and compile. No one is able to run the exploit against the firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Since the DOS attack was against the firewall itself I am going to include a third attack that is indirectly an attack of the firewall. This attack is against the Mailguard feature on the PIX firewall. Mailguard is enabled by entering the command:

```
fixup protocol smtp
```

Mailguard is used to protect against unsecure mail servers by not allowing certain commands to be issued that are considered a security risk such as HELP, EXPN, etc. The advisory for the vulnerability may be found at:

http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml

The issue is due to the pix not requiring the appropriate MAIL FROM and RCPT TO commands required before issuing the DATA command. If one issues the DATA command before entering either of the aforementioned commands the server will respond with error 503, however the firewall thinks everything is ok and will allow everything through until receiving <CR><LF><CR><LF><CR><LF>. This allows an attacker to get around the security provided by the firewall for the SMTP server and possible issue an attack against the server itself. This is why one should always use defense in depth. One may be tempted to install a default server without hardening simply because the firewall takes care of securing SMTP. An example of the attack follows:

```
telnet <mail server> 25
        220 <mail server> ESMTP Service ready
EHLO world
        250-<mail server> Hello world([my ip]), pleased to meet you
Mail from: ted@hacker.org
        250 ted@hacker.org… Sender OK
Data
        503 Issue RCPT TO: command before DATA command
Now we are able to enter any command we want…
```

The are a few ways to help prevent these attacks.

1) educate users against social engineering techniques and about security in general
2) always keep software up-to-date
3) restrict connections to explicitly allowed hosts only
4) Defense in depth – always use as many layers of security as is practical

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

[1] Dana Graesser. "Cisco Router Hardening Step-by-Step". July 25, 2001. http://rr.sans.org/firewall/router2.php.

[2] IANA. "INTERNET PROTOCOL V4 ADDRESS SPACE". 2002-08-06. http://www.iana.org/assignments/ipv4-address-space.

[3] SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities". May 2, 2002. http://www.sans.org/top20.htm.

[4] M. St. Johns. "Identification Protocol". February 1993. http://www.rfc-editor.org/rfc/rfc1413.txt.

[5] Cisco Systems. "SC: Cisco IOS Security Configuration Guide, Release 12.2". May 6, 2002. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm.

[6] Cisco Systems. "SR: Cisco IOS Security Command Reference, Release 12.2". May 6, 2002. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm.

[7] Cisco Systems. "Cisco Security Advisory: Cisco Secure PIX Firewall Mailguard Vulnerability". 2000 October 5. http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml.

[8] Stephen Monahan. "GCFW Firewall Practical". October 26, 2001. http://www.giac.org/practicals/Stephen_Monahan_GCFW.doc.

[9] Emily Gladstone. "GCFW Firewall Practical". April 30, 2002. http://www.giac.org/practical/Emily_Gladstone_GCFW.zip.

[10] Cisco Systems. "Security Advisory: Scanning for SSH Can Cause a Crash". 2002 June 27. http://www.cisco.com/warp/public/707/SSH-scanning.shtml.

[11] SecurityFocus Online. "Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability". Sep 19, 2000. http://online.securityfocus.com/bid/1698/.

[12] SecurityFocus Online. "SSH CRC-32 Compensation Attack Detector Vulnerability". Feb 08, 2001. http://online.securityfocus.com/bid/2347/.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.