



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 Certified Firewall Analyst (GCFW)

Practical Assignment Version 3.0

By: Jason D. Gordon

April 18, 2004

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract:

The purpose of this paper is to fulfill the requirements for the practical portion of the GIAC GCFW certification.

This paper focuses on GIAC Enterprises, a fictional corporation that provides fortune cookie sayings, horoscopes, numerology, psychic profiles and other miscellaneous astrological services to the Government of the Northwest Territories in Canada.

The paper consists of four (4) assignments and will outline the business operations, network architecture, and perimeter security of GIAC Enterprises.

DISCLAIMER:

The contents of this paper are completely fictional and are intended for entertainment purposes only. The author is not affiliated with the Government of the Northwest Territories and did not seek their input on the paper. All names have been changed to protect the innocent.

Assignment 1 – Security Architecture

1.1 Business Operations

GIAC Enterprises is an organization that has been contracted to provide various astrological services to the Government of the Northwest Territories in Canada. For the remainder of this paper, GIAC Enterprises will be referenced as GE, and the Government of the Northwest Territories will be referred to as the GNWT. The Canadian territory the Northwest Territories will be referred to as the NWT.

In November 2003, the Legislative Assembly of the Northwest Territories elected a new premier for the territory. One of the topics that this premier campaigned on was the improvement of mental and spiritual health for all citizens of the NWT.

The premier formed a committee and tasked that committee to implement a daring, never been done before concept of bringing astrology to the citizens of the NWT. The catch is that this astrological data must be reflective of the different Aboriginal groups of the NWT.

GE's customer has very simple expectations. The customer lets GE know the type and quantity of the astrological data that they require, GE then acquires, translates and formats this data and makes it available for the customer. The customer's main stipulation is that they would prefer to have their employees be able to get the formatted data from GE in a secure manner. Since this data is paid for with NWT tax money, the confidentiality, integrity and availability of this data is of high importance to the customer.

Once the customer has taken the astrological data off of GE's network, GE has met their SLA and the customer is free to do whatever they like with the data. GE has no knowledge, nor any concern over what happens to the data next.

In going forward with the contract, GE's management needed to put a lot of thought into designing the type of Information System that would meet the customer's requirements and allow GE to deliver the commodity securely and operate efficiently.

GE management decided that the system should also function in a manner that would make it easy for the suppliers and partner companies to interact with GE staff and provide the services that GE has purchased or agreed to from them. GE's management also decided that in order to ensure the integrity and privacy of the commodity, absolutely no astrological data was to leave GE's network, with the exception of the customer getting their data.

GE's management had one other challenge to manage. Currently, the bandwidth available in Canada's arctic is not on par with the rest of Canada. The majority of the communication signals travel over satellite and therefore bandwidth and lag in technology is something that must be considered.

The principals that dictate how GE operates its business are:

- i) **The Company:** GIAC Enterprises (GE), an organization contracted to provide astrological services to the customer.
- ii) **The Customer:** The Government of the Northwest Territories (GNWT), the GNWT is located in Yellowknife, NWT and has a requirement of the astrological data for use in improving constituent morale.
- iii) **The Suppliers:** The two companies that GE purchases the commodity from. The suppliers are located in Vancouver, BC and Toronto, ON.
- iv) **The Partner:** The translation company located in Inuvik, NWT that GE uses to translate the astrological data into various Aboriginal languages.
- v) **The Public:** Everyone else in the general public not affiliated with GE or the GNWT that may be interested in getting information on GE.
- vi) **The Commodity:** The Commodity is the astrological data that GE purchases, translates, formats and delivers to the Customer. The Commodity is in the form of plain text files that gets transferred between all parties.

Each of these principals plays a role in GE's operations, and has different access and communication requirements with regards to GE's network. In addition to the access requirements, there are several access restrictions to be applied to each principal as well.

GE's IT department decided that in order meet all of the above criteria and to give all components the type of access that they require that the network infrastructure would be

built around Citrix Systems' application computing model. The Citrix application-computing model is an extension of Windows 2000 Terminal Services and uses the Independent Computing Architecture (ICA) protocol to pass screen shots, keystrokes and mouse movements back to the remote user. The Citrix ICA protocol is designed to have small bandwidth requirements, so using the Citrix application-computing model makes sense for delivering the access to the Canadian north where bandwidth limitations are an issue.

Implementing a Citrix MetaFrame XP Farm over a Windows 2000 Active Directory would allow GE to deliver their business applications such as e-mail, Internet access, office productivity suites, database access and other miscellaneous applications to all internal and remote employees in a consistent and efficient package.

GE will leverage the Citrix Secure Gateway to provide the customer, suppliers, partner and remote employees remote access to the GE network. A Citrix Web Interface (external web site) listens on port 443 for https requests and provides the remote user with a web page to logon to, and display any applications that the user is authorized to use. The Citrix Web Interface and Citrix Secure Gateway service will be installed on one Windows 2000 Server on a service network that is positioned on a separate burb on the firewall.

The Citrix Secure Gateway communicates with the Citrix MetaFrame XP farm on GE's internal network and acts as an application proxy that streams the remote user's application and access over an encrypted ICA session over https.

The customer and GE have an SLA that requires GE to acquire a predetermined amount of astrological data in the format of standard text files. GE will then contact the suppliers and provision them to provide the amount and type of data that GE requires.

When the supplier is ready to "deliver" the data to GE, the suppliers will navigate their browser to GE's external web address and log onto the Citrix Web Interface. The suppliers will have a standard FTP client published for them to use. The client FTPs the data files from their C:\ drive to their home drive on the GE FTP server. This is all done within an encrypted ICA session.

When the data has been delivered, it is scanned for viruses and malicious content before being moved off of the suppliers' home directories to the internal GE network by GE employees. The GE staff then screen and choose what data they want to make available to the customer. Once a batch of data is ready to be delivered, a copy of this data is placed in the partner home directory for the partner company to translate into the various aboriginal languages.

GE alerts the partner that an order of data is ready for translation and the partner navigates to the same secure web site and logs onto the Citrix Web Interface. The partner will also use the FTP client to "get" the data off of GE's FTP server and "put" it back once the data

has been translated.

The data is scanned again for viruses and malicious content before it is moved off of the partner's home directory back to GE's internal network. GE staff formats the translated data before making it available to the customer. Once the commodity is ready to be delivered to the customer it is placed in the customer's home directory on the same FTP server and made available for the customer to "get" the data.

The customer will navigate to GE's secure web site and logon to the same Web Interface. They will also have access to an FTP client that will allow them to get their data off of GE's network and onto their local PC.

GE chose to use a standard FTP server on a service network to facilitate the movement of the astrological data. The firewall uses an ACL to limit the access to the FTP server to only the Citrix MetaFrame servers. All of the presentation of the application is handled by the Citrix ICA session. GE decided that even though FTP passes user ID and passwords in the clear this would be sufficient as the remote ICA session is encrypted in a 128-bit SSL stream and since it is only mouse movements and keystrokes going back and forth over the Internet, no user information ever leaves GE's wire. The client drive mapping feature of Citrix MetaFrame allows GE to map the customer, suppliers, and partner C:\ drives to their ICA session and therefore have the ability to pass the data files in an encrypted ICA stream.

1.2 Access Requirements

The customer, suppliers and partner are all external organizations to GE. GE is not able to modify the infrastructures of these organizations therefore it was important to create the ability for these organizations to connect to GE securely and efficiently.

GE uses a Citrix MetaFrame XP farm and the Active Directory to provide GE employees access to network resources and applications. Active Directory network accounts and corresponding group memberships determine what applications and network access authenticated users are entitled to.

Using the Citrix Secure Gateway that integrates with existing Citrix MetaFrame XP farms, GE was able to publish a secure web site available for remote users to log onto GE's network and have access to resources and applications.

Since all remote users, including external employees will be using the same secure web site to connect to GE; access requirements are really segmented at the application level and facilitated by the particular Active Directory account.

To connect to GE's secure web site, all remote users need the following items:

- GE's CA Root Certificate
- Internet connection and a web browser that supports 128-bit encryption
- Citrix ICA client
- User ID and password for GE's Active Directory domain

Once a user has these items, the only protocol that they would require to have access to GE's network is https. All communications with GE's network, including the actual Citrix ICA session are encrypted.

1.2.1 The Customer:

The customer communicates with GE via e-mail, traditional phone and fax lines and face to face. The customer does not require any additional changes to their infrastructure in order to connect to GE's network and retrieve their astrological data. The following items are what are specifically required from GE in order for the customer to log onto the GE network.

Customer Access Requirements:

- GE's CA Root Certificate
- HTTPS
- User ID and password for GE's Active Directory domain
- Published FTP client to connect to FTP server
- User ID and password for access to FTP server

The customer only needs access to their FTP home directory in order to "get" their data; therefore their access restrictions basically include everything else. The customer will not have access to any other applications except the FTP client, and the FTP server will be locked down and only allow the customer access to the customer home directory.

Customer Access Restrictions:

- No access to anything except FTP client and FTP server
- Only has ability to "get" data from FTP server

1.2.2 The Suppliers:

The suppliers also communicate with GE via e-mail, over phone and fax lines and face to face when necessary. The suppliers do not have to make any infrastructure changes in order to provide GE with the astrological data. The following items are required for the suppliers to connect to GE's network.

Supplier Access Requirements:

- GE's CA Root Certificate

- HTTPS
- User ID and password for GE's Active Directory domain
- Published FTP client to connect to FTP server
- User ID and password for access to FTP server

Again, since the suppliers are limited to “putting” data in their home directory on the FTP server, their Access Restrictions include everything else.

Supplier Access Restrictions:

- No access to anything except FTP client and FTP server
- Only has ability to “put” data onto FTP server

1.2.3 The Partner:

The partner also communicates with GE via e-mail, phone, fax and face to face. Again, the partner needs access to the same items as the customer and supplier in order to connect to GE's network.

Partner Access Requirements:

- GE's CA Root Certificate
- HTTPS
- User ID and password for GE's Active Directory domain
- Published FTP client to connect to FTP server
- User ID and password for access to FTP server

The main difference between the partner, the customer and suppliers is the fact that the partner needs to first “get” data off of the FTP server, and then “put” the translated data back onto GE's network. Therefore after the partner's ability to “get” and “put” data into their home directory on the FTP server, their Access Restrictions include everything else.

Partner Access Restrictions:

- No access to anything except FTP client and FTP server
- Only has ability to “get” and “put” data onto FTP server

1.2.4 The Public:

Since GE has the GNWT as their primary customer, and this is the first year of a 5-year experimental project, GE does not look to the general public for potential sales. There is a public web site hosted on GE's network that gives the general public information about GE as a company and provides generic contact information. This web site does not contain any private information, and is routinely checked for sensitive information.

Public Access Requirements:

- HTTP

Since the general public can only view non-private information about GE on the public web site, their Access Restrictions include everything else.

Public Access Restrictions:

- No access to anything except public web site

1.2.5 Internal Employees:

GE's internal employees will have access to all of their applications and services via the Citrix MetaFrame farm. Internal users will use their browser to navigate to the internal Citrix Web Interface and log on to have access to their published applications.

This includes all Internet communications such as web browsing (HTTP/HTTPS), e-mail (SMTP) and file retrieval (FTP). The SideWinder G2's various proxy servers manage all Internet bound protocols. For example all HTTP, HTTPS, and FTP requests are sent through a Squid Web Proxy that is hosted on the SideWinder G2 firewall.

The SideWinder G2 firewall's secure split SMTP servers send and receive e-mail to the outside world on behalf of GE's Microsoft Exchange 2000 Server. All outbound mail is sent from the Exchange Server to the internal SMTP server, which passes the mail to the external SMTP server, which forwards it on to the Internet. The reverse order is applied for inbound e-mail.

Finally, the designated internal users will require access to the FTP Server on the service network, and the SideWinder G2 FTP Proxy is configured to allow this communication to take place. Only the Citrix MetaFrame servers are permitted to pass traffic back and forth with the FTP server, but as far as the user knows, they are communicating directly with the FTP server.

All Internet bound traffic is to be filtered through GE's SideWinder G2 firewall. The reasons for this is because the SideWinder G2 has excellent logging capabilities and the stateful application proxies mean that no internal machine is ever exposed directly to the Internet.

Internal Users Access Requirements:

- HTTP/HTTPS
- FTP
- SMTP
- ICA

Internal Users Access Restrictions:

- No internal users or machines are to have a direct connection to the Internet
- Application and file access is determined by Active Directory account

1.2.6 Remote Employees:

GE's remote employees require access to the same applications and services as the internal employees. The only difference is that the remote users are not physically located at GE's head office.

The GE remote employees will use the same secure website as the customer, suppliers and partner to connect to GE's network while off-site. They will logon with their User ID and password and will have access to all of the normal published applications that are required for them to do their jobs. The look and feel and performance of the published applications is identical to internal and remote employees. The only difference between the two parties is that one is located at GE head office, and the others are not. This is possible because of the Citrix Secure Gateway SSL VPN that GE deployed.

Remote Users Access Requirements:

- GE's Root CA Certificate
- Laptop, browser and Internet connection
- HTTP/HTTPS
- FTP
- SMTP/POP3
- ICA

All GE remote employees laptops have been equipped with the latest Microsoft Service Pack and available hotfixes. McAfee Virus Scan is used to protect the laptops and personal firewalls are used on the laptops. This is because the remote users are not physically located at GE and at times must use a direct Internet connection and thus their laptops are not afforded the luxury of being protected by GE's SideWinder G2 firewall.

Therefore there are no real Access Restrictions for the remote employees, except that when they are connected to GE and have launched an ICA session, they are bound by the same Access Restrictions as if they were located inside GE's head office.

1.3 Network Infrastructure

The network infrastructure is composed of three separate network segments. The three network segments are interdependent and complement each other in providing secure, functional and efficient Internet communications.

1.3.1 Standard Components:

GE has standardized on the following components for their network except where noted:

Network Servers Hardware	CPU/RAM	Operating System	Service Pack
HP Proliant DL 360	Intel Xeon 2.8 GHz/2 GB	Windows 2000 Server	Service Pack 4 with up to date patching

Internal Network Workstations Hardware	CPU/RAM	Operating System	Service Pack
HP Compaq dx2000	Intel P4 2.4 GHz/256 MB	Windows 2000 Professional	Service Pack 4 with up to date patching

Monitoring/Logging Servers Hardware	CPU/RAM	Operating System	Service Pack
HP Compaq dx2000	Intel P4 2.4 GHz/256 MB	Red Hat Linux 9.1	Up to date patching

Remote User Laptops Hardware	CPU/RAM	Operating System	Service Pack
HP Compaq Evo610	Intel P3 1.3 GHz/128 MB	Windows 2000 Professional	Service Pack 4 with up to date patching

1.3.2 Network Segments:

The three segments and their components are:

- The Perimeter Network
 - Border Router
 - Firewall
 - VPN
 - DNS*
 - E-Mail Services*
- The Service Networks
 - Citrix Web Interface
 - Citrix Secure Gateway

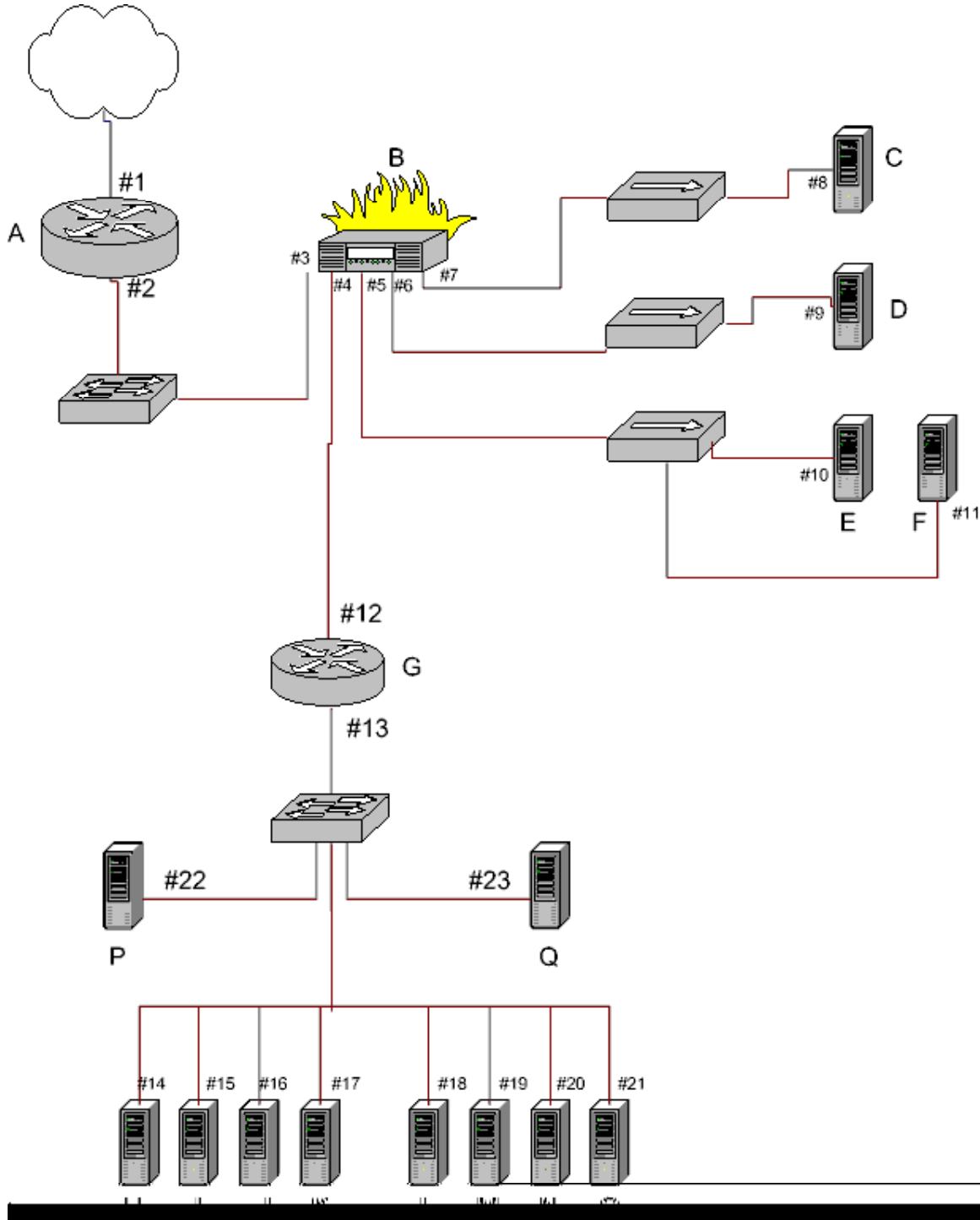
- Public WWW Server
 - FTP Server
- The Internal Network
 - Filtering Router
 - File Servers
 - Databases
 - Application Servers
 - Corporate Mail Server

Following the Defense in Depth principal of architecture design, GE has layered the perimeter components to secure network communications. Layering the perimeter components is preferred because it allows GE to capitalize on the strengths and minimize the weaknesses of each particular device.

No single perimeter device is capable of providing adequate security by itself, and a layered perimeter is also not without risks, but the risks are calculated and minimal compared to relying on the firewall to be the so called silver bullet to protect the network. Therefore GE has layered the border router, internal router, firewall and segmented networks to achieve the right balance of security, performance and ease of administration.

GE's border router performs the static packet filtering on ingress and egress traffic, while only permitting GE's critical services. Once the traffic has passed the border router it is next screened by the application proxies of the SideWinder G2 firewall. If the traffic is legitimate it is passed on through the firewall to the appropriate network burb on the firewall. For example all traffic for the secure web site and public web site are forwarded to separate network burbs using the firewall's host forwarding options. E-mail and www traffic is passed to the internal network via the firewall's appropriate proxy. The internal filtering router is placed between the firewall and the internal network and its main function is to make sure that only proper traffic leaves GE's network. This includes all of the small services, Microsoft networking services, etc that tend to find their way out to the Internet and all can leak valuable information about GE's network. Finally GE's firewall is divided into several network segments called "burb". These burbs are used to apply different ACLs on different hosts depending on their functions. For example there is an ACL that permits traffic from the Citrix MetaFrame servers on the internal burb to the FTP server on one of the service network burbs. The firewall rules define and regulate the direction that the traffic can travel and this is important to protecting GE's data.

1.3.3 GE Network Diagram:



1.3.4 IP Addressing Scheme (Mapped to Diagram):

Host	Letter / Number	IP Address	Description
Border Router	A 1	201.201.201.99/29	Connected to ISP
	A 2	200.200.200.201/29	Connected to Firewall
Firewall	B 3	200.200.200.202/29	Connected to border router
	B 4	192.168.10.2/30	Connected to internal router
	B 5	192.168.30.33/29	Connected to public service network
	B 6	192.168.40.41/29	Connected to FTP service network
	B 7	192.168.20.25/29	Connected to Citrix Secure Gateway service network
Citrix Web Interface/Secure Gateway	C 8	192.168.20.26/29	Citrix Web Interface/Secure Gateway
GE FTP Server	D 9	192.168.40.42/29	FTP Server
Public WWW	E 10	192.168.30.34/29	Public WWW Server
External Syslog	F 11	192.168.30.35/29	External Syslogd
Internal Router	G 12	192.168.10.3/30	Connected to Firewall
	G 13	192.168.50.10/24	Connected to internal network
File/Print/DC	H 14	192.168.50.20/24	File/Print/DC
Exchange/DC	I 15	192.168.50.21/24	Exchange/DC
Internal Web Interface	J 16	192.168.50.22/24	Internal Citrix Web Interface
Citrix Web Interface	K 17	192.168.50.23/24	Citrix Web Interface
MetaFrame1	L 18	192.168.50.24/24	MetaFrame Server
MetaFrame2	M 19	192.168.50.25/24	MetaFrame Server

MetaFrame3	N 20	192.168.50.26/24	MetaFrame Server
MetaFrame4	O 21	192.168.50.27/24	MetaFrame Server
SNORT IDS	P 22	192.168.50.28/24	SNORT IDS
Internal Syslog	Q 23	192.168.50.29/24	Internal Syslogd

1.3.5 The Perimeter Network:

1.3.5.1 Border Router

- Manufacturer: Cisco Systems
- Make: Cisco 2620 XM Multiservice router
- IOS: 12.3
- Feature Set: IP Base
- Up to date Cisco patches

Role in Defense in Depth

The border router sits between the ISP demarc and the firewall. The border router is configured to “deny any” incoming traffic and to only allow the legitimate Internet traffic that GE requires to do business. This means that the border router will perform ingress static packet filtering on incoming traffic and will not pass any known Internet garbage or bad traffic that should never touch GE’s network, and egress static packet filtering on outgoing traffic and not pass any traffic that should never leave GE’s network.

Items for Ingress Filtering:

- Source IP addresses of internal and service networks
- Source IP addresses with RFC 1918 addresses
- IANA reserved addresses
- Unallocated subnets
- SANS Top 20 List of Scanned Ports

Items for Egress Filtering:

- Source IP addresses that DO NOT belong to GE’s networks
- Small services and Microsoft networking services
- ICMP echo reply and ICMP unreachable messages

This will prevent address spoofing, port scanning and ultimately to lighten the workload

for the firewall. By using the “deny any” on the border router, the SANS Top 20 and other ports will be blocked by default.

© SANS Institute 2000 - 2005, Author retains full rights.

Reasons for using this model:

The Cisco 2620 was chosen because of Cisco Systems' reputation as the industry leader in router products and this model can easily handle the workload of performing static packet filtering of ingress and egress Internet traffic. Cisco routers are easy to configure and deploy, there is good support available from Cisco Systems and there is vast knowledge of Cisco routers amongst GE's IT staff and their professional associates.

There have recently been several vulnerabilities for the Cisco IOS and this is a concern for GE because these vulnerabilities allow attackers to perform DoS attacks, hijacking the router and other attacks that would affect GE's ability to provide service to the customer. Because the border router is the first component in the line of fire, GE's policy on patches for the router are to apply them quickly and to keep up to date with any vulnerabilities and respective patches as they become known. Additionally all router configuration is to be completed on the console of the router. No remote administration is permitted.

1.3.5.2 Firewall

- Manufacturer: Secure Computing Corporation
- Make: Sidewinder G2 Security Appliance
- OS: SecureOS version 6.1
- Hardware: Dell PowerEdge 1750, Intel Xeon 2.8 GHz CPU, 1 GB RAM
- Redundancy: Dual power supply, RAID 0 36 GB HDD
- Up to date patches for SideWinder G2 and SecureOS

Role in Defense in Depth

The firewall is arguably the most important component in the network architecture. The SideWinder G2 firewall ties all of the network segments together and regulates the flow of network traffic through the use of Access Control Lists, application and network level proxies and stateful inspection.

The firewall is positioned between the border router and the internal networks. In addition to GE's traditional internal network, there are 3 service networks that host various services that external and internal users require access to.

Service Network 1: Citrix Web Interface and Citrix Secure Gateway

Service Network 2: Public Web Server and POP Server

Service Network 3: FTP Server

The SideWinder G2 firewall provides two key areas of protection for GE's network; perimeter defense and stealth. Perimeter defense is achieved because all incoming traffic is passed through the firewall and inspected by the applicable intelligent application proxy

and logged. Stealth is achieved because the SideWinder G2 uses NAT to hide the internal addressing scheme. Additionally, any malicious packets that managed to get by the border router will still have to pass through the firewall and its ACL database and state table.

Features of SideWinder G2

- SecureOS: A version of BSD UNIX that Secure Computing has enhanced with their proprietary Type Enforcement technology
- A separate Operational and Administrative Kernel. The Operational Kernel is the default kernel and the Administrative Kernel can only be accessed by rebooting the firewall into the Administrative Kernel from the console
- Type Enforced Domains that keep processes and services running on the system separated
- Intelligent application and network layer proxies, stateful inspection
- SideWinder G2 hosted servers such as Secure Split DNS and Secure Split SMTP
- Extensive and thorough auditing and logging mechanisms

Reasons for using this model:

The SideWinder G2 Security Appliance was chosen because of Secure Computing's reputation for their firewall products. GE's IT manager and staff have all worked with other SideWinder firewalls on other projects and were familiar with administering these types of firewalls. The SecureOS installs on Pentium based hardware, supports standard network interfaces and integrates easily into standard network configurations. The Dell PowerEdge hardware that GE's SideWinder comes with is very powerful and can easily handle user load and workload from the application proxies that GE will use. The support provided with Secure Computing's maintenance contract is superb.

GE has elected to use only one firewall in the network architecture. There are several reasons for this. The number one reason is price. The SideWinder G2 Security Appliance and the maintenance contract is fairly expensive, so purchasing multiple firewalls is not an option.

Another reason for going with a sole firewall is performance. While the SideWinder is expensive, GE felt that it was a worthwhile investment because they were able to run all of their internal and public network services with one SideWinder. Since the SideWinder is capable of hosting split DNS and split SMTP servers, GE was able to justify deciding on the SideWinder G2 because it would be unnecessary to purchase these two additional network servers. Normally it is not recommended to run too many services or servers on a firewall, but since the Dell PowerEdge hardware is capable of handling the workload, and the SecureOS was built to host these servers, and Secure Computing Corporation actually suggests using this feature as part of a secure perimeter, GE's management decided that it would be worth the risk.

There are two 36 GB HDD configured for RAID Level 0 and there are redundant power supplies on the Dell PowerEdge, so in the event of hard disk failure or power supply failure, the stand by would automatically kick in. The configuration and the entire system will be backed up to DAT tapes, and since the SecureOS is compatible with Intel based hardware, GE could have a new system up in running within a few hours in the event of an emergency.

1.3.5.3 DNS:

GE has decided to use the SideWinder hosted secure split DNS servers for the DNS implementation. Secure split DNS is a feature of the SideWinder G2 firewall and is the recommended DNS implementation from Secure Computing. Since GE will be using NAT to hide the internal addressing, using hosted split DNS is mandatory.

SideWinder hosted split DNS consists of two BIND 9 DNS servers residing on the firewall. The external name server is bound to the external burb of the firewall and the other name server, which is called the “unbound” name server, is available for use by the internal burbs on the firewall.

An obvious benefit of using SideWinder hosted split DNS is that both the external and internal name servers are protected by the SideWinder’s hardened operating system. This provides security against attacks on GE’s name servers and hides some of the vulnerabilities found in standard BIND servers.

Using the SideWinder hosted split DNS servers requires that the “named-internet server” must be enabled for the external burb and the “named-unbound server” must be enabled with the DNS Proxy enabled for the internal burbs.

This means that port 53 UDP will be open on the Internet facing interface (external burb) of the firewall. This is necessary in order for GE’s DNS servers to communicate with the Internet.

1.3.5.4 SMTP:

Similarly to DNS, the SideWinder G2 firewall also has the capability to host the SMTP servers securely on the firewall. The SideWinder G2 uses the sendmail message transfer agent to send and receive e-mail messages. With this design all e-mail coming into and going out of the network will be routed through the firewall. This is important because it means the hardened firewall operating system will protect the internal mail server from Internet attacks and mask some of the vulnerabilities of sendmail.

GE has also decided to take advantage of this functionality and use the SideWinder hosted secure split SMTP servers. This means that there will be two sendmail servers running directly on the firewall, which will send all Internet bound e-mail to the Internet through the external burb, and will forward all inbound e-mail from the Internet to the

mail server residing on GE's internal network.

This setup requires that the sendmail server be enabled for the internal and external burb and configured to forward inbound e-mail to the mail server on GE's internal network. This is done during the initial configuration of the firewall.

This configuration means that TCP port 25 will be open on the Internet facing interface (external burb) of the firewall. This is necessary in order for GE's SMTP servers to communicate with the Internet.

Concerns about SideWinder hosted servers:

There can be some concern about overloading the SideWinder G2 firewall by having the DNS and SMTP servers hosted on the firewall. While at a glance it may seem that by hosting these servers on the firewall in addition to using application proxies might have a negative affect on the firewall's performance, the reality is quite different.

Cons:

- Firewall performance can take a hit
- If firewall becomes disabled, critical services will go down
- Configuration of these two servers can be complex

Pros:

- Vulnerabilities of BIND and sendmail are negated by the hardened SecureOS
- Two less network servers need to be purchased and maintained
- All DNS and SMTP traffic is passed through the firewall and logged

While there might be a hit to the performance of the SideWinder G2 by using the hosted DNS and SMTP servers, this really is a small price to pay for the added protection of the hardened operating system, and the Dell PowerEdge 1750 hardware with the SecureOS are really capable of handling the workload. Secure Computing recommends using the SideWinder hosted servers as the best method of achieving maximum network security while using a SideWinder G2 firewall. In the case of the split DNS, this configuration is mandatory because the firewall will be hiding GE's internal addressing through the use of NAT.

There was a heated debate on whether or not use the hosted split SMTP servers of the SideWinder G2 or to use separate mail relay hosts on the service networks. Ultimately it was decided by the GE's management to use the hosted SMTP servers because of the way that the SideWinder G2's Type Enforcement kept the internal mail server and Exchange server (thus e-mail) protected from the Internet. What this means that even if someone did manage to compromise the external SMTP server, Type Enforcement Domains means that they do not get access to the internal SMTP server, or any other

service for that matter. This was a political decision made by GE's executive board because one of the mandates of GE was to operate efficiently, so if there were a way to be efficient while not compromising security it would be explored.

1.3.5.5 VPN

- Manufacturer: Citrix Systems
- Software: Citrix Secure Gateway for MetaFrame version 2.0
- Underlying OS: Windows 2000 SP4
- Hardware: HP Proliant DL 360, dual 36 HDD with RAID 0, redundant power supplies

Role in Defense in Depth:

For the VPN component of the network architecture, GE has decided to implement a non-traditional SSL based VPN as their solution. This is important because by using the SSL based VPN instead of giving another organization an open tunnel into the network with IPSEC, GE does not extend its perimeter to include the other parties, and therefore mitigates the risks associated with persistent VPN tunnels such as viruses, worms, and malicious packets coming from the other corporation's networks. With the Citrix Secure Gateway, GE can manage who has access to their network and what applications they are authorized to use.

Reasons for choosing this model:

Price and the ability to address all remote access needs with one solution was the reason that GE decided to use the Citrix Secure Gateway for MetaFrame for GE's VPN requirements.

GE's IT Department had already decided to use the Citrix MetaFrame for Windows suite to deliver their applications to all GE employees. The GE IT manager had worked with Citrix MetaFrame on previous projects and was very content with how the Citrix product allowed the IT department to centralize time consuming administrative functions such as rolling out new applications and performing software upgrades. Using this centralized model allowed GE to save on hardware costs as all the application processing would take place on the Citrix MetaFrame XP application servers.

The Citrix MetaFrame XP suite that GE purchased included additional features such as the Citrix Secure Gateway (CSG) and the Citrix Secure Ticket Authority (STA). The CSG and STA work together to allow corporations to give remote users access to internal Citrix MetaFrame farms and their applications in a convenient and secure manner. So from a price stand point, GE did not have to purchase separate VPN software or hardware to achieve VPN functionality.

The Citrix Secure Gateway service accepts requests to access GE's internal Citrix

MetaFrame farm from remote users using https. The CSG acts as a proxy between the internal MetaFrame farm and the remote user by passing an encrypted ICA session between the parties.

Requirements to implement CSG:

- Citrix Secure Gateway service and Citrix Secure Ticket Authority
- A MetaFrame XP Server farm
- Root CA Certificate
- External Citrix Web Interface

The MetaFrame farm and the Secure Ticket Authority are located on GE's internal network. The STA service can run on any Windows 2000 Server and requires minimal resources. GE's STA is installed on one of the Windows 2000 file servers.

The Citrix Web Interface and the CSG are located on one of GE's service networks and can be installed on the same Windows 2000 Server. There are a couple of benefits to running both of these services on the same server. First of all, the Web Interface is really only a presentation interface to the end users. It is what the user sees and inputs their User ID and password into. The Web Interface also presents the user with a list of applications that are available to the user once authenticated. The processing power that the Web Interface requires does not justify a separate server. Plus by running both the Web Interface and the CSG on the same server, GE does not have to worry about securing the transmission between the CSG and the Web Interface because their communications never touches the wire.

1.3.6 The Service Networks:

There are three service networks deployed by GE. Each service network is segmented by a NIC on the SideWinder G2 firewall and is governed by separate ACL rules and access groups.

1.3.6.1 Service Network 1:

The first service network consists of the Citrix Web Interface and Citrix Secure Gateway server. These two services are installed on a single server and their function is to provide a presentation page to remote users (Web Interface), and to authenticate and proxy the remote user's Citrix ICA session using the SSL 3.0 or TLS 1.0 protocol.

- Hardware: HP Proliant DL360, dual 36 GB HDD, 1 GB RAM, redundant power supply
- OS: Windows 2000 Server SP4 and latest hotfixes
- Web Server: IIS 5.0, locked down with Microsoft's IIS Lockdown Tool 2.1
- Software: Citrix Web Interface 2.0, Citrix Secure Gateway 2.0

Three ACL rules are required on the firewall to make this service network functional:

- The HTTPS Proxy Server must forward all external requests on TCP port 443 to the Citrix Web Interface
- The HTTP Proxy Server must allow HTTP traffic on TCP port 80 between the service network and the internal network
- The ICA Proxy Server must allow Citrix ICA traffic on TCP port 1494 between the service network and the internal network

1.3.6.2 Service Network 2:

The second service network consists of the public web server and GE's external Syslog server. The Syslog server is a Red Hat Linux 9.1 box that is patched and only running syslogd.

The Web Server:

- Hardware: HP Proliant DL360, dual 36 GB HDD, 1 GB RAM, redundant power supply
- OS: Windows 2000 Server SP4 and latest hotfixes
- Web Server: IIS 5.0, locked down with Microsoft's IIS Lockdown Tool 2.1

The Syslog Server:

- Hardware: HP Compaq dx2000 workstation, 256 MB RAM, 40 GB HDD
- OS: Red Hat Linux 9.1, patched with all unnecessary services turned off

Two ACL rules are required on the firewall to make this service network functional.

- The HTTP Proxy Server must forward all external requests on TCP port 80 to the public web server
- A Syslog Proxy must be enabled to allow the border router pass Syslog traffic from the external burb to the Syslog server on the service network on the service network 2 burb using UDP port 514

1.3.6.3 Service Network 3:

The third service network is the simplest configuration of the three service networks. It consists of a single FTP Server. The purpose of the FTP server is to act in a warehouse role. Data comes in temporarily and then goes out to the parties that require this data at any given stage of the business process.

The FTP Server:

- Hardware: HP Proliant DL360, dual 36 GB HDD, 1 GB RAM, redundant power supply
- OS: Windows 2000 Server SP4 and latest hot fixes
- Web Server: IIS 5.0, locked down with Microsoft's IIS Lockdown Tool 2.1

There is only one ACL rule required to make this service network functional.

- The FTP Proxy Server must be configured to allow the FTP server to communicate with the internal network on TCP ports 20 and 21

1.3.7 The Internal Network:

GE's internal network is similar to other organizations; there are domain controllers, file servers, print servers, database servers, an Exchange and application and Terminal Servers. GE has standardized on HP Proliant DL360 hardware and Windows 2000 Server SP4 with all the current hot fixes. Employee hardware also consists of various HP desktop and laptop hardware and Windows 2000 Professional SP4 with all the current hot fixes.

1.3.7.1 Internal Router

The internal router is a Cisco 1760 Modular Access Router that is used for internal filtering. The internal router sits between the internal network and the firewall. It is configured to allow all traffic pass from the internal network to the firewall by default except for the egress filtering of known services that should never leave GE's network. These services include small services, Microsoft networking services and other types of traffic that would make GE a good net neighbor. This traffic is screened again at the firewall and border router, but the internal router will lighten the firewall and border router's workload by filtering this traffic out before it even leaves GE's internal network.

- Manufacturer: Cisco Systems
- Make: Cisco 1760 Modular Access Router
- IOS: 12.3
- Feature Set: IP Base
- Up to date Cisco security patches

1.3.7.2 Active Directory Domain Name: `giac-ent.local`

- Domain Controllers: `gefs1.giac-ent.local`, `geex1.giac-ent.local`
- Internal DNS: `gefs1.giac-ent.local`, `geex1.giac-ent.local`
- File/Print Server: `gefs1.giac-ent.local`
- Exchange Server: `geex1.giac-ent.local`
- SQL 2000 Database Server: `gesql1.giac-ent.local`

1.3.7.3 Citrix MetaFrame XPe farm: GIAC-ENT

- MetaFrame Servers: gemf1.giac-ent.local, gemf2.giac-ent.local, gemf3.giac-ent.local, gemf4.giac-ent.local
- Citrix Web Interface: gewi.giac-ent.local

1.3.7.4 Auditing/Logging Servers: SNORT 2.0 and syslogd running on RedHat Linux 9.1

- IDS: SNORT 2.0 running on Red Hat Linux 9.1, patched and unnecessary services disabled
- Syslog: syslogd running on Red Hat Linux 9.1, patched and unnecessary services disabled

The SNORT and syslogd servers are running on HP Compaq dx2000 workstations with Red Hat Linux 9.1 as the base operating system. On both systems all unnecessary services have been disabled and are patched with up to date security patches.

All Windows 2000 Servers are hardened according to CIS and NSA standards, and Active Directory Group Policy is used to enforce GE's security policy on all hosts. Auditing is configured on all Windows 2000 servers and workstations and NTSyslog 1.13 is used to forward all Security Event Logs to the local Syslog server.

Assignment 2 – Security Policy and Component Configuration

2.1 Border Router Policy:

GE's border router is the first component of the layered perimeter. The border router sits between the ISP demarc and GE's firewall and performs ingress and egress static packet filtering on all inbound and outbound Internet traffic.

Since GE's border router is directly exposed to the Internet, it must be hardened to protect GE from external users who may have malicious intent. These types of users can include black hat hackers, paid hackers (corporate espionage), script kiddies, and all the various viruses and Internet worms that could compromise the integrity, confidentiality, availability and integrity of GE's astrological data.

While the router cannot directly prevent any of these types of things from happening, when configured properly in a layered design, the border router can help secure GE's network by enforcing certain restrictions on the traffic that passes through it.

Routers are good static packet filters because of the absolute nature of allowing or denying traffic based on ports, network addresses and other common Internet garbage

that should never enter the internal network.

GE's border router is a Cisco 2620 Access Router running IOS 12.3. There are two interfaces on the router, the serial port to the ISP and the fast Ethernet network card connected to the external interface of the firewall. The border router and firewall are not directly connected; rather they are both on the same IP subnet and on a shared switch.

GE has based the router policy on the NSA/SNAC router configuration guide on hardening Cisco routers. As per NSA recommendations and because GE is a government-funded contractor, GE's border router will be configured to permit only the required protocols and services. An access list will be used to enforce this policy.

"In cases where only certain hosts or networks need access to particular services, add a filtering rule that permits that service but only for the specific host addresses or address ranges. For example, the network firewall host might be the only address authorized to initiate web connections (TCP port 80) through the router."

– From NSA Router Configuration Guide, Applying Packet Filters, page 37

GE's border router is setup with a very simple configuration consisting of two access lists and only the necessary services enabled. The ingress and egress access lists will be configured to allow HTTP, HTTPS, DNS and SMTP in and out.

Ingress Filtering:

Types of Internet traffic that should be filtered at the border router:

- Source IP addresses of internal and service networks
- Source IP addresses with RFC 1918 addresses
- IANA reserved addresses
- Unallocated subnets
- Loopback and multicast addresses
- SANS Top 20 List of Vulnerabilities

Interesting ACL Facts – SANS 2.2 Packet Filters page 5-12:

- ACLs are processed in top down order
- When a match is found, processing ends
- When creating ACLs, new lines are appended to the end of the list
- Modification requires deleting the list and re-entering the entire list
- Common TCP/UDP services and ICMP types are known by name. Values such as telnet, ftp/ftp-data and icmp-echo are valid
- TCP/UDP ports can be a numeric port range rather than just a single value
- Only one ACL per port, per direction

Two of the more common types of ACLs that can be created on a Cisco router are the standard access list and extended access list. GE will be using extended access lists to filtering because extended access lists are more flexible and offer a higher more control because the access list tests for more than just the IP Source as is the rule with standard access lists.

GE will use an extended access list on the external interface (serial 0) of the border router for ingress filtering, and an extended access list on the internal interface (eth 0) for egress filtering. Both access lists will be applied to the applicable “access-group in” for efficiency. This saves CPU resources on the router because the garbage traffic is dropped at the first interface and never crosses the router.

2.1.1 GE’s ingress access list:

```
interface Serial 0
    ip address 201.201.201.99 255.255.255.0
    access-group 101 in

access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.0.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 200.200.200.200 248.255.255.255
access-list 101 permit tcp any 200.200.200.202 eq ssl
access-list 101 permit udp any 200.200.200.202 eq dns
access-list 101 permit tcp any 200.200.200.202 eq smtp
access-list 101 permit tcp any 200.200.200.202 eq www
access-list 101 permit tcp any 200.200.200.200 248.255.255.255 established
deny any
```

GE’s access-list 101 is applied inbound on the serial interface of the border router which is connected to the ISP demarc. The first three rules in the list are necessary to block any traffic that has RFC 1918 source addresses. The fourth rule blocks any traffic that has source address of the loopback address. The fifth rule blocks any traffic with source IPs of GE’s public address space. Any packets with a source IP address matching the first five rules of this list are either malicious in intent or from incorrectly configured hosts on the Internet, neither of which is acceptable on GE’s network. These 5 rules may not be necessary because GE is denying “all” traffic and using the “permit” rule for filtering, but it is possible that the “permit” rule may pass traffic with one of these source IP addresses to the firewall on one of the allowed ports. However with the rules set up this way, these packets will be explicitly denied before the router ever gets to the “permit” rules in the list.

The next four rules are necessary to allow traffic from any source on the Internet to communicate with GE’s Internet services. These services are GE’s secure web site for the customer, suppliers, partner and remote employees, GE’s DNS and SMTP servers and the

public web site. These rules are ordered in a manner that reflects GE's money making services, SSL, DNS, SMTP, WWW in that order. Any traffic bound for any of these services are passed from the border router to the firewall, which then is responsible for getting the traffic to the responsible server.

The next to last rule in the list is important because it allows any traffic that is sent to the Internet from GE's internal network to be returned and passed back into the network. There could be concern about the use of the "permit established" rule in this list. The train of thought is that because the router only looks for the ACK bit to be set when evaluating traffic it could be easy to sneak malicious packets pass the router. This is true, but GE decided that in order to maintain performance it would be best to allow these packets through and have them handled by the SideWinder G2 firewall's application proxies. The firewall will maintain a log of all packets that are dropped.

The final rule is the important catch-all "deny any" rule. Any ingress traffic that does not match any of the first 10 rules on this list will hit the "deny any" rule and be dropped. The "deny any" rule is implicit so it was not necessary to put it in the list, but it is included in the list for affect.

2.1.2 GE's egress access list:

```
interface Ethernet 0
  ip address 200.200.200.201 255.255.255.248
  ip access-group 102 in

access-list 102 deny tcp any any range 135 139
access-list 102 deny udp any any range 135 139
access-list 102 deny tcp any any 445
access-list 102 deny tcp any any range 6000 6255
access-list 102 deny udp any any 69
access-list 102 deny udp any any 514
access-list 102 deny udp any any range 161 162
access-list 102 deny icmp any any echo-reply unreachable
access-list 102 permit 200.200.200.202 248.255.255.255
access-list 102 deny any log-input
```

The first seven rules of GE's egress access list are necessary to prevent any internal traffic that should remain on the internal network. These services include the Microsoft NetBIOS, Microsoft Domain Service, Syslog, SMNP and X-Window System. The eighth rule is necessary to prevent network mapping by external users because any ICMP echo reply and port unreachable packets will be dropped at the internal interface of the border router. The second to last rule permits legitimate traffic from GE's network to pass the router and the last rule denies and logs all spoofed IP addresses from leaving GE's network. The log-input switch is being used with the "deny any" rule so that the MAC address of the spoofed source traffic is logged, this will help GE administrators identify

the source host.

Once the two access lists have been defined it is necessary to further harden the border router by turning off unnecessary services and enabling other Cisco security features. The following list will be applied to GE's border router:

- service password-encryption
- no cdp
- no service tcp-small-servers
- no service udp-small-servers
- no service finger
- no ip unreachable
- no ip direct-broadcast
- no ip bootp server
- no ip http server
- no ip source-route
- no snmp
- logging 192.168.30.35
- no ip proxy-arp
- no boot network
- no service config
- no ip domain-lookup
- no ip mask-reply
- banner / WARNING: Authorized Access Only /

2.1.3 Disabling unnecessary services:

The following commands begin in the appropriate configuration mode.

Passwords:

```
Sanquentin(config) # enable secret IwalkTHEline  
Sanquentin(config) # no enable password  
Sanquentin(config) # end
```

These commands protect the privileged EXEC level by encrypting the password.

```
Sanquentin(config) # service password-encryption  
Sanquentin(config) # no service password-encryption  
Sanquentin(config) # ^Z
```

These commands encrypt the rest of the passwords on the border router. Only the "enable secret password" is encrypted by default when the "enable secret" command is run.

Unnecessary features and services:

CDP

```
Sanquentin(config) # no cdp run  
Sanquentin(config) # exit
```

This turns off Cisco Discover Protocol, a chatty protocol that Cisco routers use to communicate with other Cisco routers. GE does not require this service.

TCP and UDP Small Servers

```
Sanquentin(config) # no service tcp-small servers  
Sanquentin(config) # no service udp-small servers
```

Disables echo, chargen, discard and daytime services. This is now default with IOS version 12.x and up.

Finger Server

```
Sanquentin(config) # no ip finger  
Sanquentin(config) # exit
```

The finger service is used to query a host to see who is logged onto the host. This is obviously a security risk and will not be used by GE.

HTTP Server

```
Sanquentin(config) # no ip http server  
Sanquentin(config) # exit
```

GE will not be administrating the border router through a web browser. All configuration of the border router will be done on the console port.

Bootp Server

```
Sanquentin(config) # no ip bootp server  
Sanquentin(config) # exit
```

Bootp is a protocol that allows hosts to load their operating systems over the network. This feature can allow an attacker to download a copy of the router's IOS. This is a security risk and GE does not need this service.

Configuration Auto-Loading

```
Sanquentin(config) # no boot network
Sanquentin(config) # no service config
Sanquentin(config) # exit
```

This will force the border router to load it's configuration from memory instead of over the network. This will prevent an attacker from loading a different configuration onto GE's border router.

IP Source Routing

```
Sanquentin(config) # no ip source route
Sanquentin(config) # exit
```

GE does not use source routing and disabling this feature will protect the border router against several Internet attacks.

Proxy Arp

```
Sanquentin(config) # interface eth 0/0
Sanquentin(config-if) # no ip proxy-arp
Sanquentin(config) # exit
```

- Repeat this command for all active interfaces

Disabling this feature protects GE's border router from ARP spoofing.

IP Directed Broadcast

```
Sanquentin(config) # no ip directed-broadcast
Sanquentin(config) # exit
```

Disabling this feature protects GE's border router against DoS attacks.

IP Unreachables, Redirects, Mask Replies

```
Sanquentin(config) # interface eth 0/0
Sanquentin(config-if) # no ip unreachable
Sanquentin(config-if) # no ip redirect
Sanquentin(config-if) # no ip mask-reply
Sanquentin(config-if) # end
```

- Repeat this command for all active interfaces

Disabling these features protects GE's network from being mapped as using ICMP

packets is common among attackers.

© SANS Institute 2000 - 2005, Author retains full rights.

SNMP Services

```
Sanquentin(config) # no snmp
Sanquentin(config) # exit
```

GE does not use SNMP for network management.

Router Name and DNS Resolution

```
Sanquentin(config) # no ip domain-lookup
Sanquentin(config) # end
```

GE does not want the border router to do any DNS name resolution.

Disable Unused Interfaces

```
Sanquentin(config) # interface eth 0/3
Sanquentin(config-if) # shutdown
Sanquentin(config-if) # end
```

Disable Auxiliary Port

```
Sanquentin(config) # line aux 0
Sanquentin(config) # exec-timeout 1 0
Sanquentin(config) # transport input none
```

There will not be a modem connected to GE's border router; therefore the auxiliary port will be disabled.

Disable telnet

```
Sanquentin(config) # line vty 0 4
Sanquentin(config) # exec-timeout 1 0
Sanquentin(config) # transport input none
```

GE will be doing all border router maintenance on the console of the border router so it is necessary to disable virtual terminal access.

Logging

```
Sanquentin(config) # logging 192.168.30.35
```

Warning

Sanquentin(config) # banner motd ^/ WARNING: Authorized Access Only /

For legal purposes the warning is to be displayed for all who log in to the border router.

2.2 Firewall Policy:

GE's firewall is a SideWinder G2 Security Appliance from Secure Computing. The underlying Operating System is the SecureOS and the hardware is a Dell PowerEdge 1750 server.

GE's SideWinder G2 is positioned between the border router and the internal networks. The SideWinder G2 is configured with 5 Network Interface Cards to segment GE's network into 5 burbs. A burb is a term that refers to a set of systems that are subject to the same Security Policy and Access Control List.

Firewall Configuration Information:

Burb Number	Interface	Position	IP Address
burb1	em0	internal	192.168.10.2/30
burb2	em1	external	200.200.200.202/29
burb3	em2	service1	192.168.20.26/29
burb4	em3	service2	192.168.30.33/29
burb5	em4	service3	192.168.40.42/29

Setting up and configuring the SideWinder G2 is a fairly straightforward task. When you purchase the SideWinder G2, Secure Computing does the Operating System prep work and the server arrives "ready to turn on". But you cannot just rack the server, plug in your network cables and be up and running. While the firewall OS is preinstalled, all of the network services are turned off by default, and you still have to do the custom configurations specific to your site.

When the SideWinder G2 is initially configured there are two sets of default firewall services that can be placed in the active proxy rule group. The choices are Administration Only and Standard Internet. GE wisely chose the Administration Only services because it only places the minimum administration services required to complete the setup of the SideWinder. The Standard Internet enables several proxy rules that are conflictive with GE's security policy. By using the Administration Only proxy rules, GE is exerting greater control over which proxy rules become active on the firewall.

Administration Only proxy rules:

Proxy Rule Name	Summary
cobra_all	Allows administrators to connect to the firewall using the Admin Console

login_console	Allows administrators to log in directly at the firewall, using an attached keyboard and monitor
deny_all	Denies all connections from any source burb to any destination burb

In order for GE's firewall to become operational in a locked down and functional state, several SideWinder servers and proxies must be enabled on the appropriate burbs. Once the servers and proxies have been enabled, a corresponding rule must be enabled in the rules database.

The ACL rules can be organized in sets called Rule Groups to make it easier for the firewall to process the rules while inspecting incoming and outgoing traffic. Rule Groups can consist of both rules and nested groups. Many rules and Rule Groups can be created but the firewall will only load and use the rules contained in the groups in the Active Rules window of the SideWinder G2 Admin Console. There is one main group called "default" that contains all of the other active groups.

2.2.1 Active Firewall Rules:

GE's active rules group looks like this:

```

default
  SecureGateway
  DNS
  PublicWebServer
  InternetServices
  Administration
  deny_all

```

Within the above rule groups are the applicable rules for that particular group, for example in the InternetServices rule group, there is a rule for the WebProxy that allows the internal burb to pass http/https/ftp Internet traffic to the external burb through the Squid Web Proxy server.

GE's security policy is implemented and enforced by applying rules to all traffic that passes through the firewall. Incoming and outgoing traffic is inspected and compared to a set of criteria established in each rule. There are two distinct rule types that can be configured in the SideWinder G2 firewall; Proxy Rules and IP Filter Rules.

Proxy Rules are used to control the access to the firewall's proxies and servers. Proxy Rules deny or allow traffic to pass based on criteria such as source and destination address. IP Filter Rules are used to configure the firewall to securely forward IP packets between networks. IP Filter Rules allow for filtering of non-TCP and non-UDP traffic because the rules operate directly on the IP packets.

GE only requires Proxy Rules to pass their network traffic. There is no need to turn anything on or off if GE ever needed to use IP Filter Rules in the future. IP Filter Rules are defined in the same administrative section of the SideWinder Admin Console as Proxy Rules.

To enable GE's SideWinder G2 to begin passing traffic in the production environment, 4 SideWinder servers and 5 SideWinder proxies must be enabled. The servers are the DNS, sendmail, SSHD and WebProxy servers. These can be found by launching the Admin Console and clicking on Services Configuration > Servers.

The proxies that are required are the HTTP, HTTPS, FTP, ICA and DNS proxies. These can be found in the Admin Console by clicking on Services Configuration > Proxies.

Before creating the firewall rules, Network Objects must be created for all of the hosts in all of GE's subnets. This is because there are explicit criteria that must be defined when creating the ACL rules. This includes Source and Destination, this is where the IP Address Network Objects are useful for restricting certain services to certain hosts or in this case IP addresses.

The Network Objects that can be chosen from are Domain Network Objects, Host Network Objects, IP Address Network Objects, Netmap Network Objects, Subnet Network Objects and Network Object Groups. For simplicity, GE has elected to use IP Address Network Objects and Network Group Network Objects. Every server gets an IP Address Network Object, and the four Citrix MetaFrame servers also get assigned to a Network Group object because there are two rules that apply to these four servers (ICA proxy rule and https proxy rule).

The basic rule criteria for proxy rules:

Basic Rule Criteria	Comments
Service Type	Software service type: proxy, server, or service group
Service	Type of service: Telnet, FTP, Web (HTTP), etc
Action	Specifies whether to allow or deny a service
Source Burb	Name of the source burb
Source	Name of the source Network Object
Destination Burb	Name of the destination burb
Destination	Name of the destination Network Object

There are several optional settings to configure on each proxy rule such as whether to use NAT, host forwarding or use additional authentication and time restrictions.

GE's Network Objects:

IP Address	Description
200.200.200.201	border_router
127.0.0.1	firewall
192.168.20.26	secure_gateway
192.168.40.42	ftp_server
192.168.30.34	public_www
192.168.30.35	external_syslogd
192.168.50.3	internal_router
192.168.60.10	internal_router
192.168.60.20	gefs1_filesrv
192.168.60.21	geex1_exchsrv
192.168.60.22	gesq1_sqlsrv
192.168.60.23	gewi1_webinterface
192.168.60.24	gemf1_mfsrv
192.168.60.25	gemf2_mfsrv
192.168.60.26	gemf3_mfsrv
192.168.60.27	gemf4_mfsrv
192.168.60.28	snort_ids
192.168.60.29	internal_syslogd

Once the IP Address Network Objects have been created and the Servers and Proxies have been assigned to the appropriate burbs, the next step is to define the appropriate rules to regulate the flow of traffic. These rules are based on the Access Requirements defined in Assignment 1. From the firewall's point of view, the Access Requirements are:

2.2.2 GE's Active Rules Group:

- 1) default
 - a. SecureGateway
 - i. https_csg
 - ii. http_metafarm
 - iii. http_metafarm2
 - iv. ica_metafarm
 - v. ftp_servicenet
 - b. DNS
 - i. dns_self
 - c. InternetServices
 - i. Web_Proxy
 - d. PublicWeb
 - i. http_wwwserver
 - e. Administration
 - i. internal_SSH
 - ii. external_syslog

- iii. login_console
- iv. cobra_all
- f. deny_all

This means that there are 5 Active Rules Groups and 13 ACL rules in the Active Rules of GE's SideWinder G2 firewall. The order and placement of these rules is important because the firewall searches the Active Rules in descending order beginning with the first rule or nested group within the group, then the second, etc. When the firewall hits the first rule that matches the characteristics of the rule, the traffic is processed according to that rule and will not be processed by any other rules.

GE's whole existence hinges on being able to receive astrological data from suppliers, collaborating with the partner and providing the finished product to the customer. This entire line of communication takes place over the Internet and is made possible by GE's SSL VPN (the Citrix Secure Gateway). The CSG uses the https proxy to accept remote connections to the CSG server and to pass an encrypted ICA session back to the remote users using SSL. Internally the CSG uses the http proxy to pass authentication requests and ticketing communication between the CSG on the service network 1 and the Secure Ticket Authority on the internal network. Finally, the CSG uses the ICA proxy to pass the actual ICA session between the Citrix MetaFrame XP farm on the internal network and the CSG on the service network. While not a part of the Citrix Secure Gateway, the ftp_servicenet rule has been placed in the SecureGateway Rules Group as a matter of convenience and by design. This rule allows the Citrix MetaFrame servers on the internal network to establish connections with the FTP server on the service network 2. This is the FTP server that the customer, suppliers and partner use for moving the astrological data during the various stages of the business process.

These four services are critical to the success of GE and therefore have been given the honor of first Rules Group and therefore the first 5 active rules. The second http_metaframe firewall rule is required because of the direction of the service initiating the request to pass traffic. The first rule is to allow the CSG components to pass traffic into the internal network, while the second rule allows the STA to pass traffic back to the CSG service network later as part of a different session.

Next is the DNS Rules Group. The dns_self rule allows DNS clients from the specified internal burb to use the unbound DNS server on the firewall. This one is important for obvious reasons and thus is placed as the number two Rules Group.

The InternetServices Rule Group is for GE employees, internal and remote because as far as the Citrix MetaFrame farm is concerned, all users are "internal" users. The WebProxy server enables the Squid web proxy for HTTP/HTTPS Internet communications. GE chose to use the Web Proxy instead of the HTTP/HTTPS proxies for employee Internet access because the Web Proxy regulates Internet traffic more stringently than the HTTP/HTTPS proxies. Caching is supported, the SmartFilter Internet filter can be used and there are many more filtering options available to the Web Proxy that are not

available with the HTTP/HTTPS proxies. This results in a slightly slower Internet experience for GE employees, but GE senior management decided that since GE is a government-funded contractor, an extensive Internet usage policy would be enforced.

The PublicWeb Rules Group is for the public web site that GE hosts on the third service network. The http_wwwserver requires the HTTP proxy to forward all requests from the external burb to the web server on the service network.

The Administration Rules Group is for GE's firewall administrators. Each rule allows a different method of logging onto the SideWinder G2 firewall and is fairly straightforward. The external_syslog rule is configured to allow the border router to pass syslog traffic to the Syslog server on the service network 2 using UDP port 514.

The last rule in the Active Rules group is the very important deny_all. When traffic that does not match any of the previous rules in the Active Rules Group, it arrives at the deny_all rule and is dropped.

2.2.3 GE's Active Policy:

- 1) https_csg
- 2) http_metafarm
- 3) http_metafarm2
- 4) ica_metafarm
- 5) ftp_servicenet
- 6) dns_self
- 7) Web_Proxy
- 8) http_wwwserver
- 9) internal_SSH
- 10) external_syslog
- 11) login_console
- 12) cobra_all
- 13) deny_all

2.2.4 Configuration of Assigned Rules and Groups:

Please note that these screen shots of the firewall rules DOES NOT include every Active Rule on GE's SideWinder G2 firewall. The most important and significant rules have been shown as screen shots to demonstrate the configuration interface. For a complete list and order of all of GE's rules, see the above list.

Rule 1 – https_csg

Proxy Rules: Proxy Rule

General Source / Dest Authentication Time Advanced

Name:

Service Type:

Service:

Action:

Control:

Audit Level:

Comments:

OK Cancel Help

Rule 1 – Source/Dest Configuration

Proxy Rules: Proxy Rule

General Source / Dest Authentication Time Advanced

Source Burb:

Destination Burb:

Source:

Destination:

All Source Addresses

All Destination Addresses

New

NAT Address:

Redirect Host:

Redirect Port:

OK Cancel Help

Rule 2 – https_metafarm

Proxy Rules: Proxy Rule

General | Source / Dest | Authentication | Time | Advanced

Name: https_metafarm

Service Type: Proxy

Service: https

Action: Allow

Control: Enable

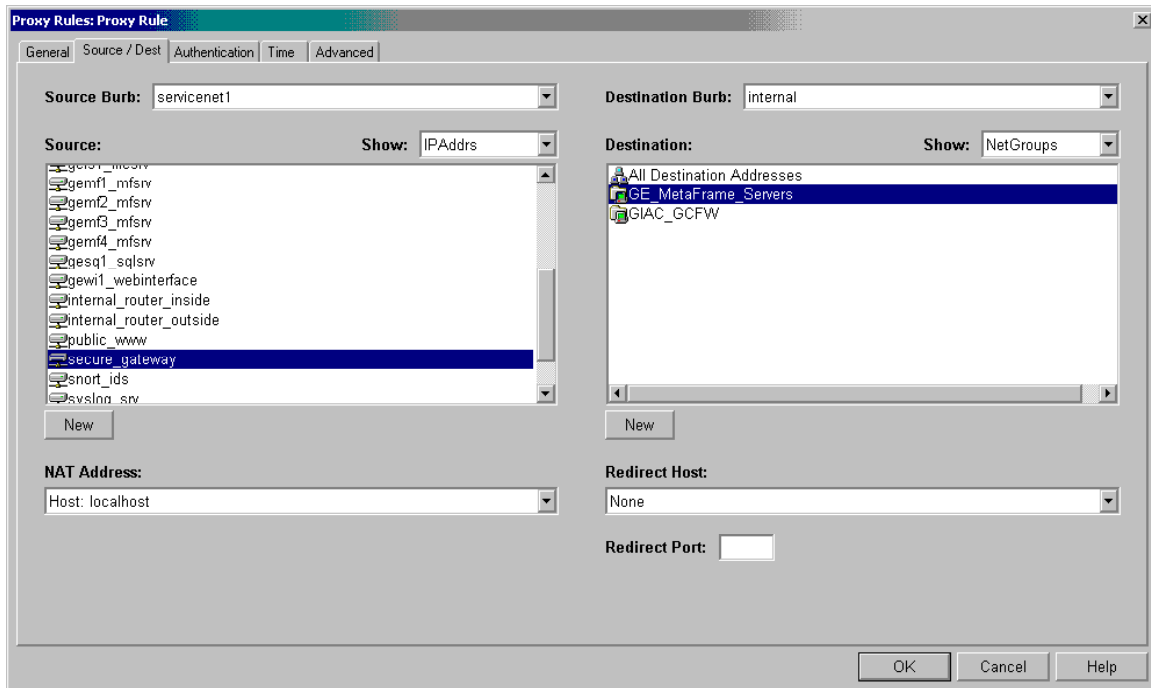
Audit Level: Traffic

Comments: Allow HTTPS Traffic between Service Net 1 and Internal Net

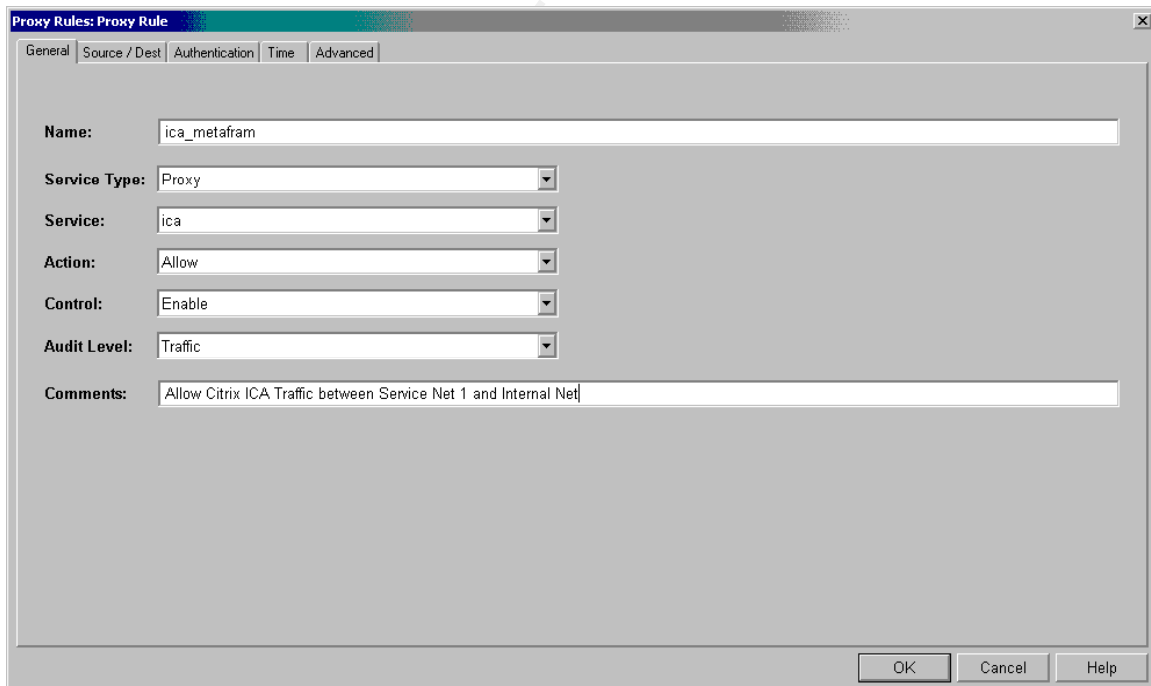
OK Cancel Help

© SANS Institute 2000 - 2005

Rule 2 – Source/Dest Configuration



Rule 3 – ica_metaframe



Rule 3 – Source/Dest Configuration

Proxy Rules: Proxy Rule

General Source / Dest Authentication Time Advanced

Source Burb: **servicenet1** Destination Burb: **internal**

Source: Show: IPAddr Destination: Show: NetGroups

Source list: gem12_mfsvr, gem13_mfsvr, gem14_mfsvr, gesq1_sqlsvr, gewi1_webinterface, internal_router_inside, internal_router_outside, public_www, **secure_gateway**, snort_ids, syslog_srv, WWW_Host

Destination list: All Destination Addresses, **GE_MetaFrame_Servers**, GIAC_GCFW

New

NAT Address: Host: localhost Redirect Host: None

Redirect Port:

OK Cancel Help

Rule 4 – ftp_servicenet

Proxy Rules: Proxy Rule

General Source / Dest Authentication Time Advanced

Name: **ftp_servicenet**

Service Type: **Proxy**

Service: **ftp**

Action: **Allow**

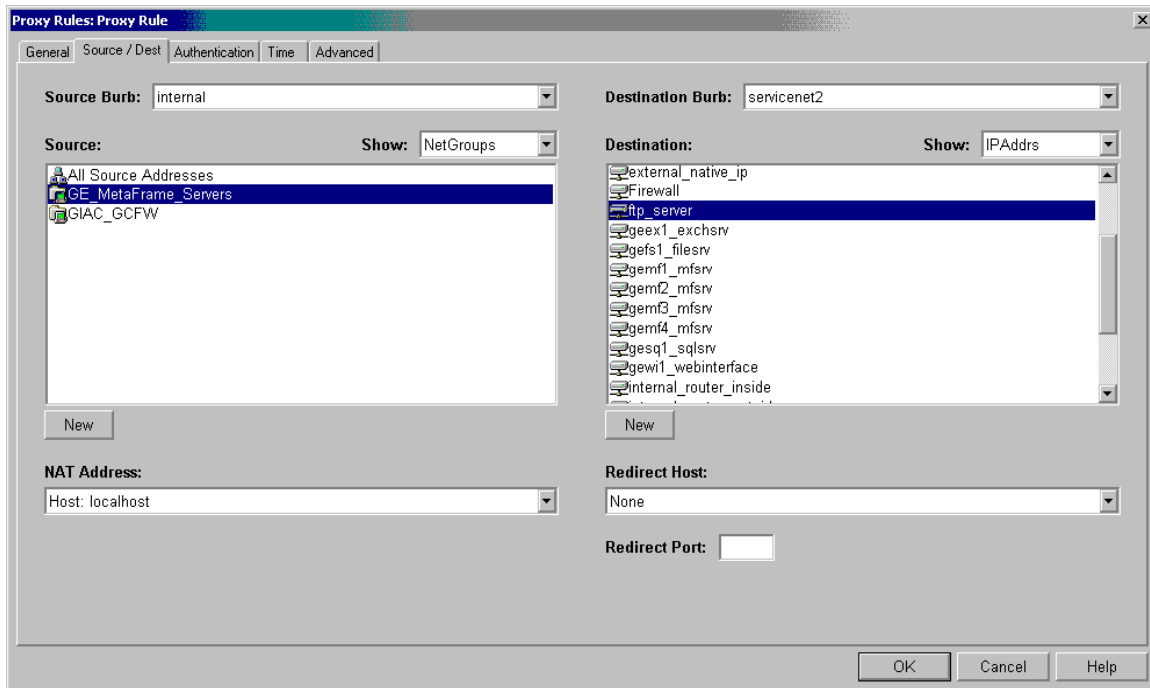
Control: **Enable**

Audit Level: **Traffic**

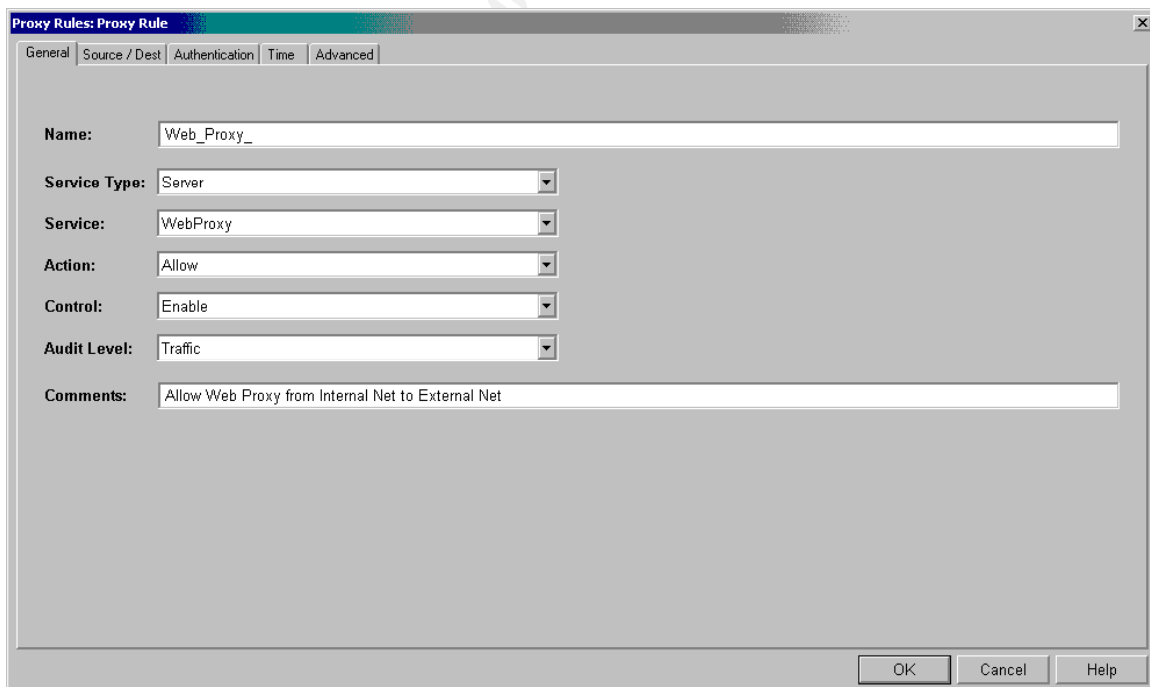
Comments: **Allow FTP from Internal Network to Service Net 2**

OK Cancel Help

Rule 4 – Source/Dest Configuration



Rule 6 – Web_Proxy



Rule 6 – Source/Dest Configuration

The screenshot shows the 'Proxy Rules: Proxy Rule' dialog box with the 'Source / Dest' tab selected. The 'Source Burb' is set to 'internal' and the 'Destination Burb' is set to 'external'. Both have 'Show: NetGroups' dropdowns. The 'Source' list contains 'All Source Addresses', 'GE_MetaFrame_Servers', and 'GIAC_GCFW'. The 'Destination' list contains 'All Destination Addresses', 'GE_MetaFrame_Servers', and 'GIAC_GCFW'. The 'NAT Address' is set to 'Host: localhost' and the 'Redirect Host' is set to 'None'. The 'Redirect Port' is empty. Buttons for 'New', 'OK', 'Cancel', and 'Help' are visible.

Proxy Rules: Proxy Rule

General Source / Dest Authentication Time Advanced

Source Burb: internal Destination Burb: external

Source: Show: NetGroups Destination: Show: NetGroups

All Source Addresses
GE_MetaFrame_Servers
GIAC_GCFW

All Destination Addresses
GE_MetaFrame_Servers
GIAC_GCFW

New

NAT Address: Host: localhost Redirect Host: None

Redirect Port:

OK Cancel Help

Rule 7 – http_wwwserver

The screenshot shows the 'Proxy Rules: Proxy Rule' dialog box with the 'General' tab selected. The 'Name' is 'http_wwwserver'. The 'Service Type' is 'Proxy', 'Service' is 'http', 'Action' is 'Allow', 'Control' is 'Enable', and 'Audit Level' is 'Traffic'. The 'Comments' field contains 'Allow and Redirect HTTP Traffic from External Net to Service Net 3'. Buttons for 'OK', 'Cancel', and 'Help' are visible.

Proxy Rules: Proxy Rule

General Source / Dest Authentication Time Advanced

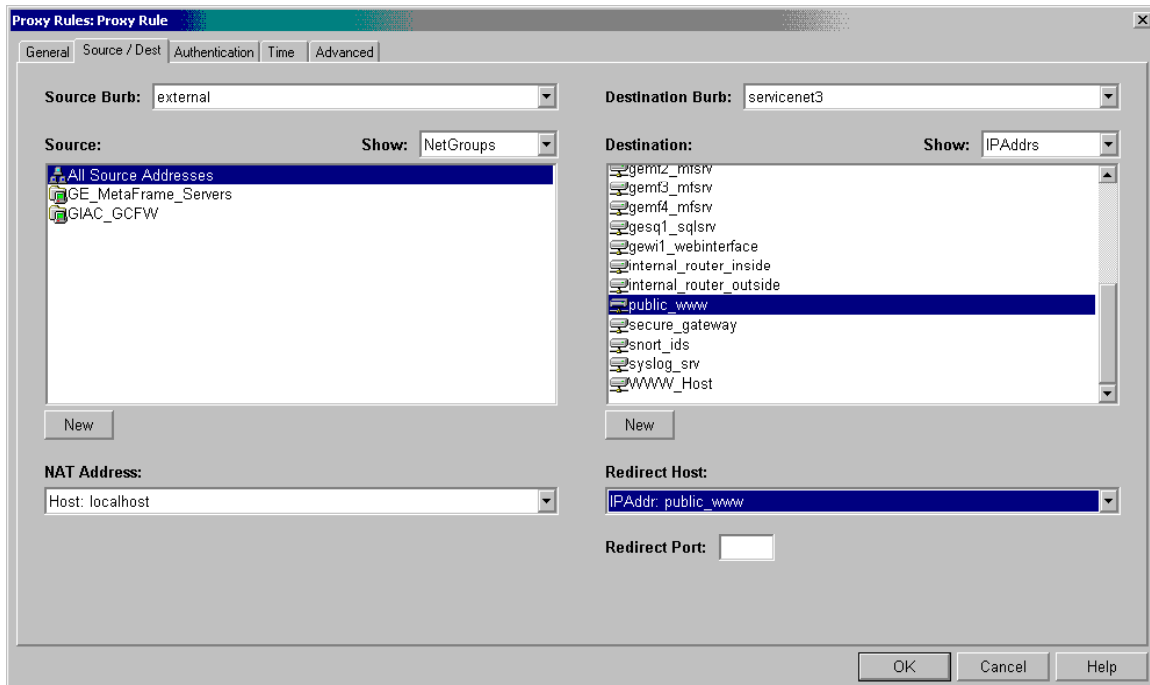
Name: http_wwwserver

Service Type: Proxy Service: http Action: Allow Control: Enable Audit Level: Traffic

Comments: Allow and Redirect HTTP Traffic from External Net to Service Net 3

OK Cancel Help

Rule 7 – Source/Dest Configuration



2.2.5 Summary:

These are the firewall ACL rules that are necessary for GE to do business and meet the access requirements for the customer, suppliers, partner and employees. By using Network Objects (IP Address and Network Group) to define the source and destination of each applicable rule, GE is able to keep the ACL rules database small and still manage the flow of traffic at a granular level. This ensures good performance with little risk to the overall security of GE's network. For the secure web server and the public web server, their respective proxy rules instruct the SideWinder G2 firewall to accept Internet requests on port 80 and port 443 and redirect the requests to the web servers located on the public web server service network and the Citrix Secure Gateway service network.

There are no proxy rules necessary for SMTP because GE is using the SMTP Server, which forwards all outbound e-mail from the internal mail server to the Internet and all inbound e-mail from the Internet to the internal mail server. If GE had enabled the SMTP proxy in addition to using the split SMTP Server, there would be a conflict because both services use TCP port 25 on the external side of the firewall.

The ports that are open on the Internet facing (external burb) interface on the firewall are:

- TCP port 443
- TCP port 80
- TCP port 25
- UDP port 53

These ports are required to be open on the external interface in order for GE to do business.

2.2.6 Additional Hardening:

There are additional configurations required to further harden the SideWinder G2 firewall. ICMP echo and timestamp responses must be disabled, authentication for the administrative kernel should be enabled, netprobe auditing on non-TCP/UDP traffic should be enabled and auditing of all TCP packet discards should be enabled. The following list are based on Secure Computing's recommendations for further hardening of the SideWinder G2 firewall from the SideWinder G2 Administration Guide.

Disabling ICMP echo and timestamp response:

By default the firewall is configured to respond to ICMP echo and timestamp requests on the external burb. This can give external users valuable information about GE's network. Even though the border router should drop all of this traffic, this feature should be disabled on the external interface.

Do the following:

- 1) Start the Admin Console and select Firewall Administration > Burb Configuration
- 2) In the Burbs list, highlight the external burb
- 3) Deselect the Respond to ICMP echo and timestamp check box to disable this parameter
- 4) Click the Save icon to save the changes

Enable authentication for the administrative kernel:

Enabling authentication for the administrative kernel is one more step in protecting the firewall from malicious users. Even though physical access is required to reboot the firewall into the administrative kernel, this feature can protect GE in the event that the physical security has been compromised and a malicious user has access to the firewall console.

Do the following:

- 1) Log in to the Admin Console, and select File Editor
- 2) Click Start File Editor and then select File > Open
- 3) In the Source field, select Firewall File and click OK
- 4) Type /etc/ttys in the File field and click OK
- 5) To enable administrative kernel authentication, edit the following line: console /usr/libexec/getty pccons" ibmpc3 on insecure

- 6) Save and exit the file

Enable auditing of netprobes on non-TCP/UDP traffic:

This feature should be turned on to audit netprobes on the firewall that are non-TCP/UDP traffic.

Do the following:

- 1) At a SideWinder G2 command prompt, log in and enter the following command to switch to the Admn role: `srole`
- 2) Enter the following command to enable netprobes on non-TCP/UDP traffic:
`/sbin/sysctl -w kern.auditnetprobes=2`
- 3) Open the `/etc/rc.local` file and add the command listed in the previous step

Auditing all TCP packet discards:

To enable auditing of all discarded TCP packets, follow the steps below:

- 1) At a SideWinder G2 command prompt, login and enter the following command to switch to the Admn role: `srole`
- 2) Enter the following command to enable auditing for discarded TCP packets:
`/sbin/sysctl -w net.inet.tcp.verbose_audit=1`
- 3) Open the `/etc/rc.local` file and add the command listed in the previous step

2.3 VPN Policy:

GE's VPN implementation will be handled by the Citrix Secure Gateway service. Citrix Secure Gateway is an SSL based VPN that allows remote users to connect to an internal Citrix MetaFrame XP farm over the Internet. This functionality will allow GE to give the customer, supplier and partner access to the astrological data and remote employees access to all GE applications.

“The Citrix Secure Gateway (CSG) functions as a secure Internet-ready gateway for Citrix Independent Computing Architecture (ICA) traffic between MetaFrame servers and Secure Socket Layers (SSL)-enabled ICA client workstations. All data traversing the Internet between the client workstation and the CSG is encrypted, ensuring privacy and integrity of information flow.”

- From Best Practices for Securing a Citrix Secure Gateway Deployment, page 1

Benefits of CSG Deployment:

- 128 bit SSL/TLS encryption
- Authentication (via Web Interface)
- Hidden internal network addresses of MetaFrame servers
- Firewall traversal through a widely accepted port (443)
- Single point of access to network and applications
- Transparent to applications and network devices, no modification or upgrades of existing MetaFrame farm necessary

Implementing is a very straightforward extension to GE's existing Citrix MetaFrame XP farm. There is minimum additional hardware to purchase and there is no additional software required to purchase, as the Citrix Secure Gateway Service, Citrix Web Interface and Citrix Secure Ticket Authority are included with the Citrix MetaFrame base package.

Required Components:

Internal Network

- An existing internal Citrix MetaFrame farm
- Citrix Secure Ticket Authority service (STA)

GE has an established Citrix MetaFrame farm and the Citrix Secure Ticket Authority service is installed on a Windows 2000 Server on the internal network. Besides the actual MetaFrame farm, the STA is the only component of the CSG implementation that is located on the internal network.

The STA is responsible for issuing session tickets to the Web Interface and CSG in the service network. These tickets are used for authentication and validation of ICA sessions. The STA communicates with the Web Interface and CSG over TCP port 80, so this port is required to be open between the internal network and service network 1.

Service Network

- Citrix Secure Gateway service (CSG)
- Citrix Web Interface (WI)
- Windows 2000 Server running IIS 5.0
- Server Certificate for secure.giac-ent.com on CSG/WI server

The CSG and Web Interface are installed on a single server on the service network. The server is a Windows 2000 Server running IIS 5.0. Windows 2000 Service Pack 4 and all current critical updates/hotfixes have been applied on the server. The IIS 5.0 web server has been locked down with Microsoft IIS Lockdown 2.1. Additional hardening of the CSG/WI server has been completed as per "Best Practices for Securing a Citrix Secure Gateway Deployment" from Citrix Systems, INC.

The CSG/WI server communicates with the STA on the internal network over TCP port 80, the Citrix XML Service (part of MetaFrame ICA process) on the internal network over TCP port 80 and the MetaFrame servers on the internal network over TCP port 1494. These three ports are required to be open between the service network 1 and the internal network.

The SideWinder G2 has port 443 open on the external burb and Internet requests for *https://secure.giac-ent.com* are forwarded to the CSG/WI server using the host-forwarding feature of the firewall. The CSG proxies all ICA traffic from the internal network to the remote user on the Internet using 128 bit SSL encryption.

Other

- Root CA Certificate for *secure.giac-ent.com*
- Citrix ICA client for customer, suppliers, partner and remote employees
- TCP port 443 open on external burb of SideWinder G2 firewall
- TCP port 1494 open between internal burb and service network 1 burb of firewall
- TCP port 80 open between internal burb and service network 1 burb of firewall

The CA Root Certificate for *secure.giac-ent.com* is necessary because SSL uses PKI for the encryption/decryption process. The remote user's web browser must have the Root CA Certificate for *secure.giac-ent.com* and the CSG/WI server running on the service network 1 must have this Server Certificate installed.

Remote users need the Citrix ICA client installed on their respective workstations. GE has configured their MetaFrame farm to push the ICA Web Client to any machine connecting to GE that does not have an ICA client installed. This is a handy feature.

2.3.1 Process Flow of GE's CSG implementation:

The following process flow is taken directly from Citrix Systems' Best Practices for Securing a Citrix Secure Gateway Deployment on page 3. It is included to give a clear understanding of how the CSG works. Minor details have been changed to reflect GE's network (specifically with open ports and software versions).

- 1) A remote user launches a web browser and connects to a Web Interface web server on port 443 (HTTPS). The Web Interface portal requires the user to authenticate using valid user credentials.
- 2) Web Interface uses the user credentials to contact the Citrix XML Service, on TCP port 80 by default, running on a MetaFrame server and obtains a list of applications that the user is authorized to access. Web Interface populates the Web portal page with the list of published applications that the user is authorized to access. The communications so far are the normal sequence of events that occur when a Web Interface is deployed to provide ICA client users with access to

- published applications.
- 3) When the user clicks on a link for a published application, Web Interface sends the IP address for the requested MetaFrame servers to the STA and requests a Citrix Secure Gateway ticket for the user. The STA saves the IP address in memory and issues the requested Citrix Secure Gateway ticket to the Web Interface.
 - 4) Web Interface generates an ICA file containing the ticket issued by the STA, and then sends it to the client browser. Note that the ICA file generated by Web Interface contains only the IP address of the Citrix Secure Gateway server and the STA ticket. The address of the MetaFrame server that the ICA client eventually connects to is not exposed.
 - 5) The browser passes the ICA file to the ICA client, which launches an SSL connection to the Citrix Secure Gateway server. Initial SSL handshaking is performed to establish the identity of the Citrix Secure Gateway server.
 - 6) The Citrix Secure Gateway server accepts the ticket from the ICA client and uses information contained in the Citrix Secure Gateway ticket to identify and contact the STA for ticket validation. If the STA is able to validate the ticket, it returns the IP address of the MetaFrame server on which the requested application resides. If the ticket is invalid or has expired, the STA informs the Citrix Secure Gateway server, and an error message is displayed on the ICA client device.
 - 7) On receipt of the IP address for the MetaFrame server, the Citrix Secure Gateway server establishes an ICA connection to the MetaFrame server. After the ICA connection is established, the Citrix Secure Gateway server monitors ICA data flowing through the connection, and encrypts and decrypts client-server communications.

2.3.2 Steps to deploy GE CSG:

The following instructions are a very basic representation of what steps need to be taken to configure and deploy GE's CSG. Where appropriate the following instructions refer to the installation instructions for a particular Citrix product as it is beyond the scope of this paper. Hardening of the CSG focuses on locking down the Windows 2000 Server and IIS 5.0.

- 1) Configure Windows 2000 Server with IIS 5.0 and the Server Certificate for `secure.giac-ent.com`
- 2) Configure the firewall to pass the appropriate traffic between the internal network and the service network 1
- 3) Install and configure the STA on an internal Windows 2000 Server as per the instructions in the Windows Secure Gateway Guide from Citrix Systems
- 4) Install and configure the Web Interface on the CSG/WI Windows 2000 Server as per the instructions in the Windows Secure Gateway Guide from Citrix Systems
- 5) Install and configure the Secure Gateway service on the CSG/WI Windows 2000 Server as per the instructions in the Windows Secure Gateway Guide from Citrix Systems

- 6) Configure the Web Interface to interact with the CSG as per the instructions in the Web Interface for MetaFrame XP Administrators guide from Citrix Systems
- 7) Harden CSG, STA and WI as per the “Best Practices for Securing a Citrix Secure Gateway Deployment” from Citrix Systems
- 8) Use the IIS Lockdown 2.1 tool to lock down IIS on the CSG/WI and STA hosts
- 9) Configure the firewall to accept connections on TCP port 443 on the external burb and forward all requests for <https://secure.giac-ent.com> to the CSG/WI host on the service network 1 using the host redirection feature of the SideWinder G2 firewall
- 10) Test configuration and launch applications from external Internet hosts

2.3.3 Security Best Practices:

The following section deals with hardening the Windows 2000 Server that hosts each component in the Citrix Secure Gateway deployment. These recommendations relate directly to the Windows 2000 Server OS and the IIS 5.0 web server. These recommendations are from the Best Practices for Securing a Citrix Secure Gateway Deployment by Citrix Systems.

Action to take	Importance	Component
Securing the file system	Critical	CSG, STA, WI
Remove Sample Code	Critical	CSG, STA
Authentication	Critical	CSG, STA, WI
User Account	Critical	CSG, STA, WI
IIS Anonymous Access	Critical	CSG, STA
User Account		
Disable Unused Services	Critical	CSG, STA, WI
Remove Windows Components	Critical	CSG, STA, WI
Hot Fixes and Service Packs	Critical	CSG, STA, WI
Remove Unused File Associations	Highly Recommended	CSG, STA
IIS Security	Critical	CSG, STA
Auditing	Critical	CSG, STA, WI
NetBIOS	Critical	CSG, STA, WI
Information Leakage via NULL Sessions	Highly Recommended	CSG, STA, WI
Port Filtering	Highly Recommended	CSG, STA, WI
Denial of Service Registry Entries	Highly Recommended	CSG, STA, WI
Disable Internet Printing	Highly Recommended	CSG, STA, WI
STA TCP/IP Filtering	Highly Recommended	STA

Securing the File System:

Use NTFS; Remove the Everyone Group and substitute with the Authenticated Users Group. Use additional NTFS permissions to protect the server system files

Remove Sample Code:

During the installation of IIS 5.0 a number of sample applications are installed and this is a security hole because the default installation directories are well known.

The following directories and virtual directories should be removed if present:

IIS Samples	\\IISamples	c:\inetpub\iissamples
IIS Documentation	\\IISHelp	c:\winnt\help\iishelp
Data Access	\\MSADC	c:\program files\common files\system\msadc

Authentication:

The recommended method for authentication is using some form of certificate based authentication (eg. SecurID).

Please note that GE is currently only using the Windows 2000 Active Directory User ID and password for authentication at this time. The reasoning is that since it is early in the project and there are less than 10 remote users total, it would be better to leave Strong Authentication for year 2 of the project. GE is aware that both Secure Computing and Citrix Systems have a product called SafeWord for Citrix MetaFrame that will integrate with GE's firewall and MetaFrame farm rather seamlessly.

Until the SafeWord for MetaFrame is implemented, GE will rely Windows 2000 Auditing, IIS Auditing and the firewall logs to monitor the CSG. The Windows 2000 and IIS logs are pushed a syslog server on the service network using NTSyslog.

User Account:

The following settings are recommended for Windows 2000 User Accounts

- Password History – 7 passwords remembered
- Maximum Password Age – 180 days or less
- Minimum Password Age – 1 day or more
- Minimum Password Length – 8 characters
- Passwords must meet complexity requirements – Enabled
- Reverse Encryption – Disabled
- Account Lockout Duration – 3 minutes or more
- Account Lockout Threshold – 3
- Rename Administrator Account - Enabled

All unused local user accounts must be disabled. These include the following:

- IUSR_SERVERNAME
- Guest

IIS Anonymous Access User Account:

Disable the IUSR_SERVERNAME account and create a new user account to allow anonymous access. The default account is well known to the world and prone to exploits.

Disable Unused Services:

It is important to disable services that are not needed because all Windows 2000 services provide a level of vulnerability. The following is a list of services that need to be disabled:

- Application Management
- Clipbook
- Computer Browser
- DHCP
- DFS
- DNS Server
- Fax Service
- File Replication Service
- Index Service
- Internet Connection Sharing
- Intersite Messaging
- Messenger
- Net Meeting Remote Desktop Sharing
- Network DDE
- Network DDE DSDM
- Performance Logs and Alerts
- Print Spooler
- QoS RSVP
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry Service
- RunAs Service
- SMTP
- Smart Card
- Smart Card Helper
- TCP/IP NetBIOS Helper Service
- Telephony
- Telnet
- Terminal Services
- Windows Installer

- WINS

© SANS Institute 2000 - 2005, Author retains full rights.

Hotfixes and Service Packs:

It is important to apply hotfixes and service packs when they become available. GE has standardized all Windows 2000 installations on Service Pack 4.

Remove Unused File Associations:

Malicious users may substitute the original program with a substitute program attempt to breach the IIS server. Remove the following file associations:

- .printer
- .htw
- .ida
- .idg
- .cdf
- .asa
- .htr
- .idc
- .stm

IIS Security:

NTFS permissions should be used on folders and directory browsing should be turned off. Only the newly created anonymous IIS account should have read/write access to the Web Interface Icons folder on the Web Interface and modify permissions to the Scripts folder on the STA. All other directories should have Read Only and no Execute permissions.

Auditing:

Auditing is important. This will be turned on for all of the servers and the Security Event Logs will be pushed to a syslog server using NTSyslog. The default size of the Event Log will be increased to 500 MB.

The following objects will be audited:

- Account Management
- Logon Events
- Policy Change

NetBIOS:

Improper configuration of SMB/CIFS can expose critical system files or give full file system access to any malicious user on the Internet. Access to administrative shares like ADMIN\$, C\$ will be disabled.

Information Leakage via NULL Sessions:

To prevent this from happening the following registry key will be set to limit the amount of information returned:

- HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=2

Port Filtering:

Enabling port filtering on each server NIC will add another layer of security to the CSG components. TCP ports 80, 443 and 1494 should be the only ports that pass traffic between the CSG/WI and STA.

The following commands will allow port filtering and TCP/IP filtering:

- 1) Right click My Network Places and select Properties
- 2) Right click Network Adapter and select Properties
- 3) Select TCP/IP and click Properties
- 4) Click Advanced
- 5) Select TCP/IP Filtering and select Properties
- 6) On the TCP Protocol select Permit Only
- 7) Add the applicable ports

Please note that in GE's case this filtering will be enhanced by the use of the SideWinder G2 firewall rules because when the ports were opened the source and destination hosts were defined.

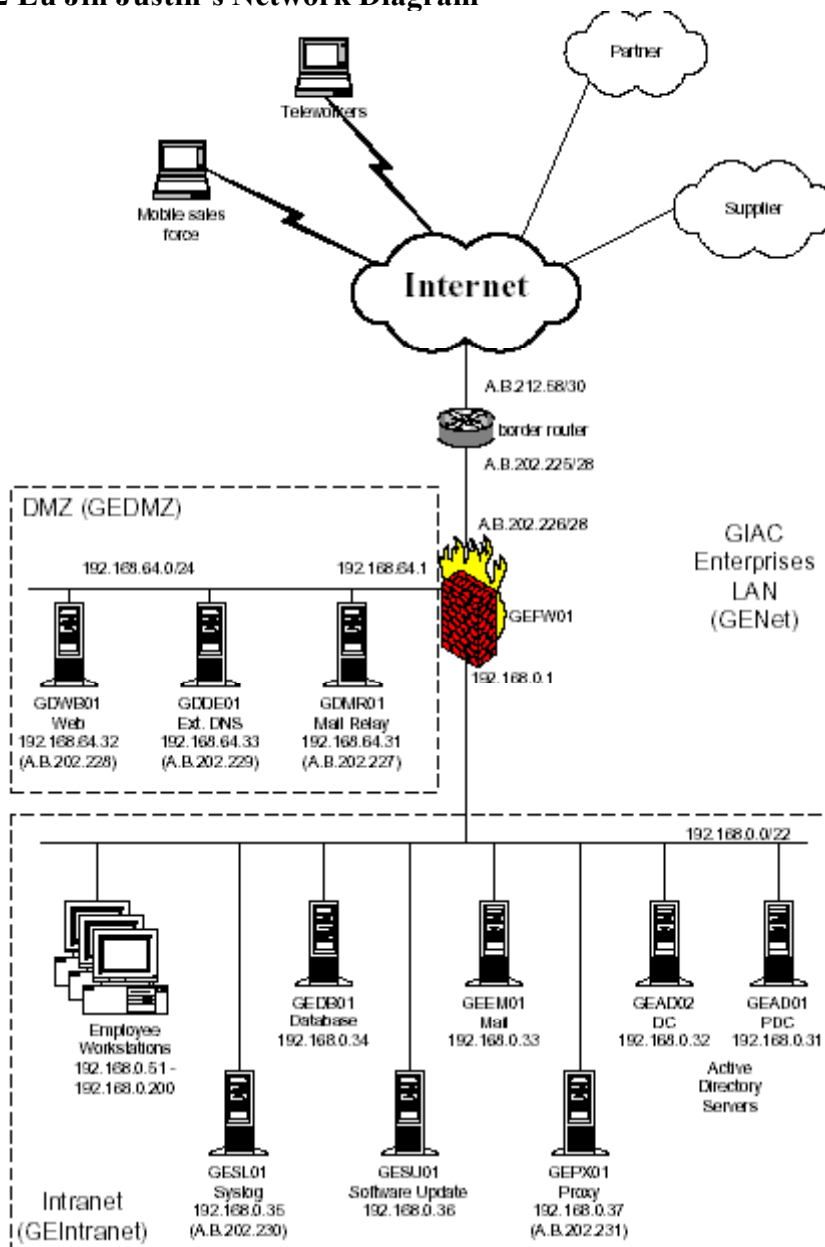
Assignment 3 - Design Under Fire

3.1 Preface:

For this assignment I will be writing the entire document in first person and from my point of view. I have taken on the role of a black hat hacker for hire that has been contracted by GE to conduct some corporate espionage on GIAC Enterprises. GE and GIAC Enterprises are competitors in the fortune cookie industry and are bidding on the same contracts. GE is interested in gaining a competitive edge and would like to know what GIAC's marketing and research departments are currently working on. This is where I come in.

I have chosen Eu Jin Justin Ng's design as the target network. The link to his practical is http://www.giac.org/practical/GCFW/EuJin_JustinNg_GCFW.pdf and the image of his network design is:

3.2 Eu Jin Justin's Network Diagram



3.3 Assumptions:

There are a few assumptions that I will make before and during this assignment. The first assumption that I will make is that both companies are in the same city and that I will have physical access to GIAC's head office because I also am in the same city.

I will also assume that I have the luxury of taking my time in gathering this information for GE. I do not have a specific target of information that I am looking for, only trying to attain internal access to uncover anything that may be interesting.

3.4 Reconnaissance:

Upon accepting the challenge, the first task that I will begin is recon. The first steps that I take will be fairly low technology and I will take advantage of the plethora of publicly available information on any company. Once I have gathered enough information about my mark, I will then begin mapping their network and looking for weaknesses that may be easy to compromise. With an adequate map of GIAC's network I will then attempt to compromise an internal host. This is the ultimate goal because once I have an internal host it will be easy to map the internal network. The keys is attaining internal access and retaining that access so that we can go back to the well as needed in the future.

3.4.1 Internet Whois Databases

The very first thing that I will do is go to GIAC Enterprises' public website at www.giacent.com. GIAC Enterprises has a very helpful website because it provides important information such as the phone numbers and e-mail addresses of key department members such as Sales and Public Relations. This is key for two reasons. A lot of times the structure of a person's e-mail address is similar to their logon ID, and having the person's name, company title and phone number will be helpful with social engineering attacks. Having a block of phone numbers is also good for the social attack, but is important when conducting war dialing to look for unsecured modems. GIAC's public web site also lists their physical address, which is important if dumpster diving becomes an option later.

Some other information that can be gathered from a company's public web site is:

- Business partners and suppliers
- Corporate culture, lingo and projects
- Company history, financial information
- Recent mergers and acquisitions
- Technology in use by the company

Now that I have taken some general information from GIAC's web site, I will use some other methods of gathering more publicly available information. I am specifically looking for information that will make penetrating GIAC's network possible. I will use the following tools for the job:

- Whois databases
 - ICANN (<http://www.internic.net/whois.html>) for registrar info
 - ARIN (<http://www.arin.net/>) for IP address assignment info
 - The registrar (<http://www.webnames.ca/>) for specific info
- Miscellaneous command line tools such as nslookup, dig, whois

Using nslookup I was able to determine the IP address for www.giacenterprises.com was

A.B.202.228 and the DNS server for giacent.com was A.B.202.229. Upon entering these IP addresses into the ARIN database I discovered that GIAC Enterprises has the subnet of A.B.202.224/28 assigned to them, therefore this is what I knew so far:

- A.B.202.224 – network address
- A.B.202.225
- A.B.202.226
- A.B.202.227
- A.B.202.228 – www.giacent.com
- A.B.202.229 – gddn01.giacent.com
- A.B.202.230
- A.B.202.231
- A.B.202.232
- A.B.202.233
- A.B.202.234
- A.B.202.235
- A.B.202.236
- A.B.202.237
- A.B.202.238
- A.B.202.239 – broadcast address

I now use GIAC's registrar whois database to get some technical contact information for the giacent.com domain. Luckily for me there is the name of GIAC's IT manager listed as well as the phone number and e-mail address, more handy information for a social engineering attack. I notice that the contact information has recently been updated so I feel confident that I am dealing with a technically sound organization.

I do one last thing as part of my recon. I will utilize a couple of search engines to see what type of info I can gather. Using google.com and vivisimo.com I do a general search on GIAC Enterprises as well as a link search to see what other companies are linking to GIAC. To do a link search on GIAC I type "link:www.giacent.com" in both search engines for parity. I will next check the Usenet groups to see what residual data I can collect. Sometimes you can get lucky because an administrator posted a question about a technical problem he was having with a particular piece of technology and used his company's e-mail address in the post.

From groups.google.com I enter a search for giacent.com, GIAC Enterprises and the e-mail addresses that I harvested from GIAC's public web site and rolled the proverbial dice. I lucked out because there were a few posts containing information about GIAC's internal network. It seems that one of the network administrators was having trouble making configuration changes to their Active Directory implementation and was asking for help specifically about applying Group Policies. There was nothing incriminating in the post, but it was important because I was able to deduce that GIAC has an Active Directory implementation internally, and are using Windows 2000 or Windows 2003 Servers. The fact that they are using Group Policy means that it is very likely that the end

user workstations are either Windows 2000 Professional or Windows XP. This may or may not be true, but it has been my experience. Now I have a good idea of what type of internal systems that my mark is using. It has also been my experience that internal systems, particularly end user workstations are less likely to be patched and are therefore more vulnerable to compromise. These systems are also less likely to be thoroughly logged and audited.

3.5 Scanning GIAC:

Now that I have completed my recon, it is time to map GIAC's network and look for weak points. I already know that there are two live Internet hosts and would like to know if GIAC is using their 12 remaining addresses.

The very first thing that I do before doing a network scan is use a war dialer to check for modems on GIAC's network. From my information gathering I was able to get several phone numbers and I will scan numbers in this range to see what I come up with. There were no modems found in the batch of numbers that I tried.

I want to know what type of server www.giacent.com is running on, so I use Netcraft (<http://www.netcraft.com/>) to find out this information. Netcraft indicates that www.giacent.com is running on IIS 6.0, so this means that the underlying OS is Windows Server 2003.

I have decided that I will use Nmap to try and determine if there are any other hosts live on GIAC's subnet. Nmap can scan multiple network addresses using traditional ICMP echo requests and is capable of conducting TCP scans for when ICMP is blocked.

This command from Nmap will perform a ping sweep on GIAC's subnet range and return any info. Nmap has discovered other hosts on the subnet. Using an educated guess based on the IP addresses of the web server and DNS server I pick one of the hosts to begin probing to determine if it is the firewall. Using passive scanning with Nmap and sticking to the common ports such as WWW, DNS and SMTP I determine that A.B.202.226 is in fact the firewall and that the firewall has TCP ports 25, 80 and 53 open. This is standard for the majority of companies and leads me to believe that internal employees have access to the public Internet using standards ports on the firewall.

I next spend a bit of time reading up on the latest vulnerabilities and other types of attacks for ideas. I determine that it is likely the public web server has been patched because there have been so much attention paid to Microsoft security problems lately and Microsoft has been doing a lot of work to change the public conscience about patching and keeping servers secure. So I decide that I will not try to attack the web server. The same is true for the firewall and router because most companies actually are very good at keeping these components up to date, plus if I did manage to compromise one of the external hosts it still does not guarantee me access to the data I am looking for.

I go back to the search engines and luckily come across an article about this online sales consortium that GIAC belongs to and is actually a leading member. I decide that my best bet for immediate results is to take advantage of GIAC's membership in this consortium and attempt to trick them using this information. I decide that I will call someone from GIAC, probably someone from marketing or sales because they are less technical and are more likely to fall for a well planned social attack. I will pretend that I am from this online consortium and try to convince my mark that I am conducting a survey about all members and try to get the individual to go to a web site. Obviously this web site is malicious and if successful will give me remote access to GIAC's internal network.

3.6 The Attack:

The attack on GIAC to try to gain internal access will rely on a couple of factors. Using the contact information gathered during the recon phase, I will make a call to the Sales contact and attempt to get the user to install a program on his workstation that will allow me to place a backdoor on the system. The program is the Reverse WWW Shell by van Hauser.

Information on the Reverse WWW Shell can be found here:

<http://www.thc.org/papers/fw-backd.htm>

The Reverse WWW Shell is a Perl script that places a program on a target machine that acts as a slave to a program on a remote master machine. The attacker inputs commands into the remote master server and the target machine GETS the commands over the Internet in standard HTTP requests. This backdoor program is successful because GIAC employees are allowed to access the Internet and to the firewall this traffic looks like legitimate HTTP traffic.

There are two Perl files that are needed to execute this program. First I must get the rwwwshell.pl file and edit it with the correct values of my target slave and my master server. Next I run the rwwwshell.pl program on my master server to accept the target's http requests.

The hard part is getting the rwwwshell.pl slave file to be executed on the target workstation. This will take luck. I phone the Sales contact and introduce myself as Joe So and So from some sales and marketing organization that is conducting a survey. I ask if he has the time to do the survey now, or if he's too busy I can e-mail him a link to our online survey that he can complete at his convenience. I make sure to phone at a time that he is likely to be busy and does not want to be disturbed. The Sales contact agrees to have me e-mail him the survey and gives me his e-mail address.

I e-mail him a link to a web server that has the master program running and at this point I have to wait for him to click on the link and launch the slave program.

3.7 The Result:

When the user clicks on the link his Anti-Virus software picks up the threat and my attack fails. Looks like I'm going dumpster diving.

3.8 Mitigation:

In this case I was able to gather a lot of information from GIAC's public web site, particularly with regards to the phone numbers and e-mail addresses. This can be prevented if a company has a policy restricting the type of information put on the public web site. For example only using the main phone number instead of publishing the direct lines exposing the exchange to a war dialing effort.

E-mail addresses and contacts for important departments are important, but if at all feasible business wise, a company should consider funneling all calls and e-mails through a generic number or address. This can also cut down on all the spam and virus threats as well.

I was able to convince the Sales contact to click on the link because I was able to convince him that I was doing a survey. I phoned at a time that I knew he would be busy and offered him the opportunity to complete the survey online at his convenience. I would just e-mail him the link. I might even entice him to complete the survey by offering some type of reward, or say something like everyone who completes the survey gets their name put in a draw for dinner at a local restaurant. The key is to sound convincing, not hard to do if you are in the same city or know the lingo.

The workstation's Anti-Virus detected the malicious Perl script and aborted the download. But this could have been avoided by educating the users about the dangers of clicking on links in e-mails, opening attachments, etc. This is especially important for non-technical staff as they are less savvy when it comes to the dangers of the Internet. All staff should be trained to be suspicious of anyone who calls them and asks if they can e-mail them something and all they have to do is open the attachment, click on the link etc.

Assignment 4c – Work Procedure (Firewall Tutorial)

This tutorial is a working document on the Active Rules of GE's SideWinder G2 firewall. It is designed to assist new GE firewall administrators to manage GE's firewall policy properly.

4.1 Assumptions:

This tutorial assumes that the firewall policy is defined and active and that the SideWinder G2 Admin Console has been installed on a Windows PC and is configured to communicate with GE's firewall securely over port 9003. This is done as part of the configuration of the firewall admin tools.

This tutorial does not purport to contain intricate instructions on the configuration of the SideWinder G2 firewall rules. This tutorial is meant to get the reader familiar with GE's Active Rules and what GE would likely require in terms of adding a new rule. The reader is advised on the order of the rules and the different types of proxies that are relevant to GE.

GE's firewall rules are established in the following order:

- 1) https_csg
- 2) http_metafarm
- 3) http_metafarm2
- 4) ica_metafarm
- 5) ftp_servicenet
- 6) dns_self
- 7) Web_Proxy
- 8) http_wwwserver
- 9) internal_SSH
- 10) external_syslog
- 11) login_console
- 12) cobra_all
- 13) deny_all

Following these assumptions and these firewall rules, this tutorial will show the reader how to log onto the Admin Console, navigate around the Admin Console, view the Active Rules and make and apply changes.

4.2 SideWinder ACL Policy Configuration:

“Your site's security policy is implemented and enforced by applying rules to all traffic that passes through the SideWinder G2 firewall. Each rule is basically a mini policy which contains criteria that is used to inspect incoming or outgoing traffic. Rules determine whether that traffic will be allowed to continue to its destination.”

- From SideWinder G2 Administration Guide, page 4-1

There are two types of rules that can be configured on the SideWinder G2 firewall:

- Proxy Rules – allow you to control the firewall's proxies and servers. Proxy Rules use criteria like source and destination addresses to make decisions on passing traffic
- IP Filter Rules – allow you to configure the firewall to securely forward IP packets between networks. Use IP Filter Rules for non-TCP/UDP traffic such as IP Protocol 50

Firewall rules are organized in Rule Groups. A Rule Group can consist of both rules and nested Rule Groups. You can create multiple rules and Rule Groups, but the firewall will only load and use the rules and groups contained in the Active Rules window. The Active Rules is the Rules Group named “Default”.

Rules in the active groups are processed in sequential order from top to bottom.

“When a request arrives at the firewall, it will first be forwarded to the active IP Filters Rules. If the request does not match any IP Filter Rules, the request is forwarded on to the Active Proxy Rules. If a rule match is found, the traffic is processed according to that rule and will not be processed by any other rules. Therefore, the order of the rules and nested rule groups within an active rule group is very important.”

- From SideWinder G2 Administration Guide, page 4-3

If you add, remove or rearrange any firewall proxy rules it is important to think about how the changes you make will affect the existing firewall rules and the flow of traffic in and out of the firewall.

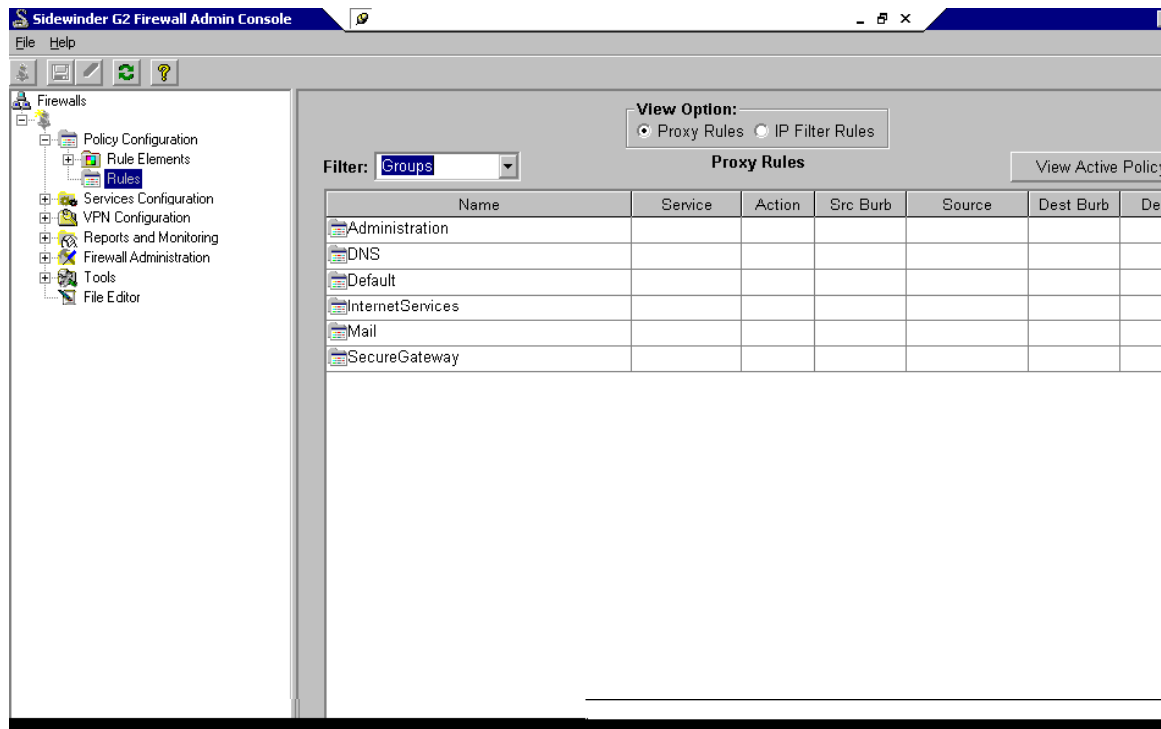
4.3 Viewing GE’s Active Policy:

In order to view the Active Rules on the firewall, do the following:

- 1) From the Windows desktop select Start > Programs > Secure Computing > SideWinder G2 6.1 > Admin Console
- 2) Select the firewall and click Connect. Make sure the IP address is correct and that the port is 9003 and NOT 9002. Traffic sent to port 9002 is not encrypted and therefore is against GE policy
- 3) Input the administrator User ID and password and click OK
- 4) In the left node expand the Policy Configuration tab and select Rules
- 5) From the right node click on the View Active Policy button

This will display the Active Rules for the firewall. The top pane contains any Active IP Filter Rules while the bottom pane contains the Active Proxy Rules. GE has not enabled any IP Filter Rules so you will only be concerned with the Proxy Rules.

When you click on Admin Console\Policy Configuration\Rules your window will look like this:



This view has been filtered to only display the Active Groups. All of the above Active Groups are nested in the Default Active Group. Note that if a rule is not in an Active Group, the rule IS NOT enabled on the firewall.

The Active Rules are displayed in the following tabular format:

Proxy Rules										IP Filter Properties
Active Group: Default										Set...
Pos	Name	Service	Action	Src Burb	Source	Dest Burb	Destination	Attributes		
1	dns_self	dns	Allow	int	All	All	All	Allow misconfigu		

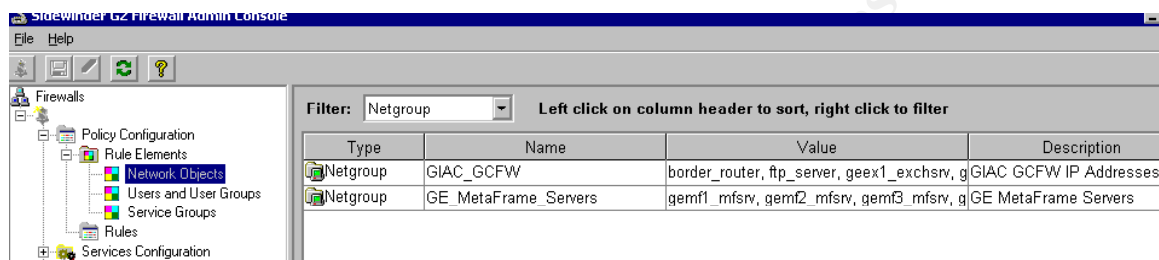
Remember that positioning of the firewall rules is important because it affects how traffic is processed. If traffic is going to be high and the type of traffic is important to GE's business operations, rules should be placed higher on the list. Remember to place any explicit denies before any occurrences of rules that may permit this traffic before the firewall gets to the deny rule. Once the firewall matches a rule for traffic, it will not compare the traffic to the remaining rules in the list.

4.4 Viewing Network Objects:

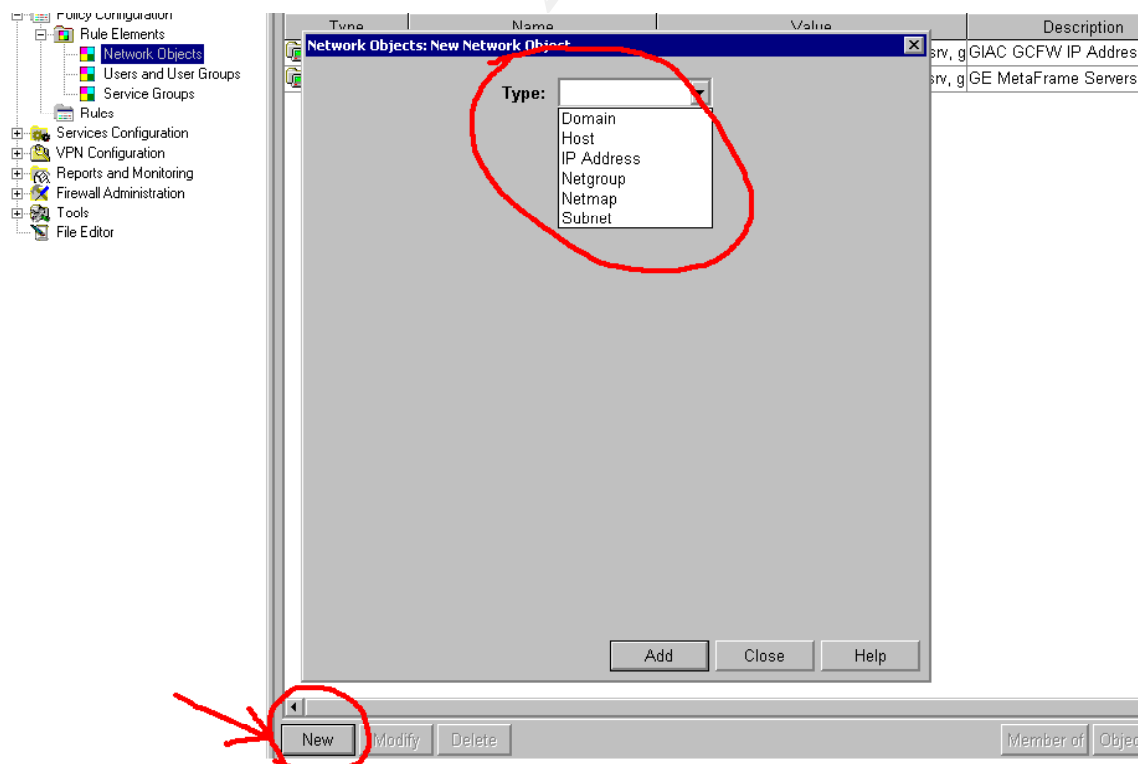
Occasionally you may need to add Network Objects to facilitate in the management of a

new firewall rule. These types of objects help you define source or destination hosts, IP addresses or entire Network Groups of other objects. This is very helpful when trying to limit the type of traffic that a particular host on GE's network will be permitted to pass through the firewall. For example you may have a host on the internal network that needs access to a certain service on the Internet, but you do not want to open up this service to all hosts on GE's network. You could create a Network Object if one did not already exist, enable the necessary proxy and create a new rule. In the source field of the firewall rule you would select the appropriate Network Object for the applicable host.

You can find Network Objects here in the Admin Console:



To create a new Network Object, from the Network Objects pane, click New and a New Network Objects dialog box pops up. From the drop down menu select the type of Network Object you want to create and click Add.



It is unlikely that you will need to add any additional Network Objects, but in the event

that this is necessary, using IP address Network Objects will more than likely suffice.

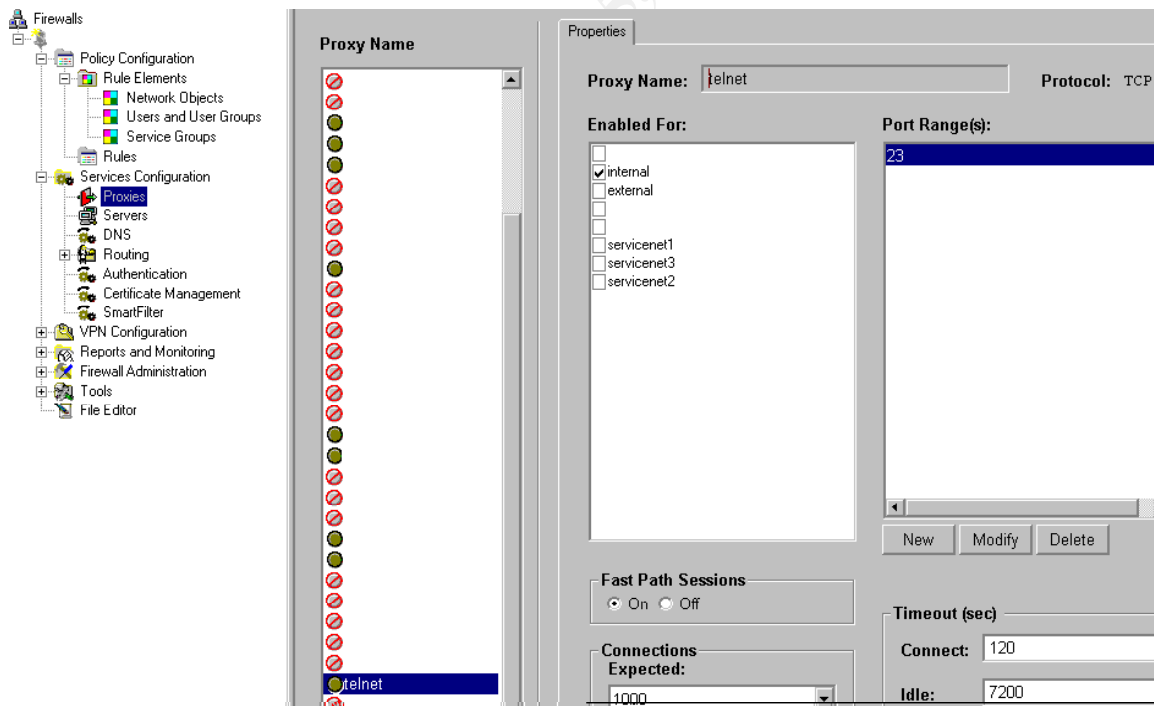
4.5 Creating new Proxy Rules:

Now on to the good stuff. This is where you will spend most of your time. There are four steps to creating a new proxy for the firewall.

- Enable appropriate proxy
- Create the firewall rule for the combination of proxy and service
- Move the new rule into the Active Rules group
- Save your changes

Enable appropriate proxy:

To turn a proxy on for a particular burb, from the Admin Console select Services Configuration > Proxies. You will have a choice of several available proxies, and burbs to apply to open up the proxy on. For our example we will open up the Telnet proxy on the internal burb. It is our intention to telnet to a host on one of the service networks. The first step is to open up the Telnet proxy on the internal burb.



To verify that port 23 on the internal burb is open we can use nmap to scan port 23. From an internal host, run nmap with the following command:

```
nmap -P0 -p 23 -vvv 192.168.10.2
```

You will get a response from nmap indicating that this port is open on the internal interface of the firewall.

Create the new rule:

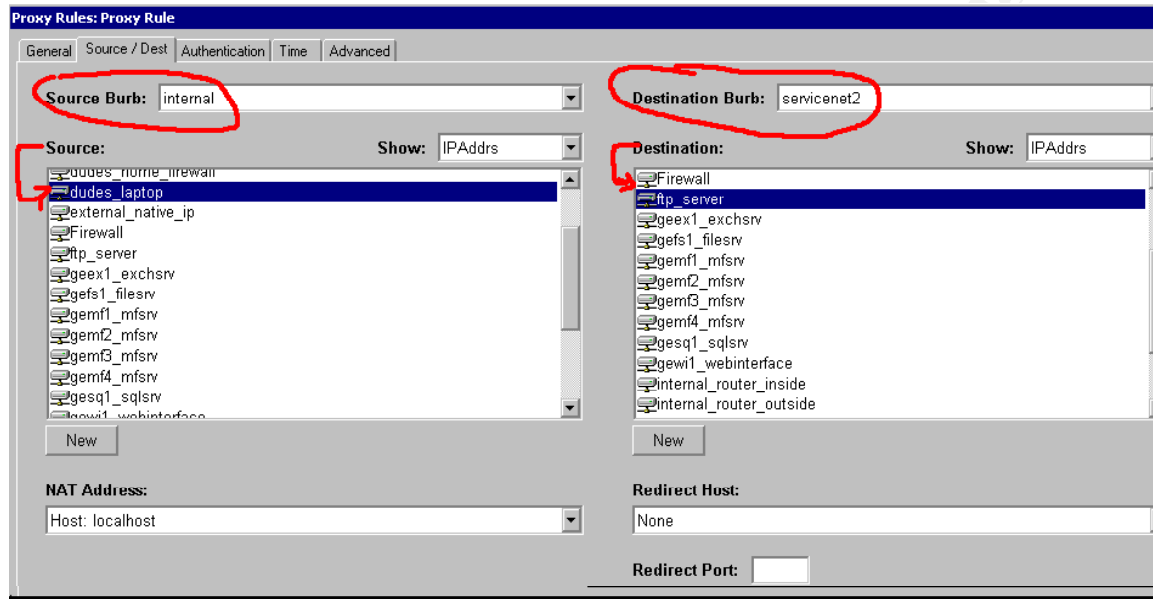
From the same context in the Admin Console used to View Active Policy, at the bottom pane select New > Proxy Rule



A “Proxy Rules: Proxy Rule” dialog box will pop up. Fill in an appropriate name and select Proxy for Service Type, Telnet for Service and Allow for Action. This is illustrated in the following picture. Pay close attention to the Type, Service and Action.

A screenshot of the 'Proxy Rules: Proxy Rule' dialog box. The 'General' tab is selected. The 'Name' field contains 'telnet_out'. The 'Service Type' dropdown is set to 'Proxy', the 'Service' dropdown is set to 'telnet', and the 'Action' dropdown is set to 'Allow'. These three fields are circled in red. The 'Control' dropdown is set to 'Enable' and the 'Audit Level' dropdown is set to 'Traffic'. The 'Comments' field contains the text 'Allow telnet access from burb internal to burb service network|'. The dialog box has tabs for 'General', 'Source / Dest', 'Authentication', 'Time', and 'Advanced'.

The final step in creating the firewall rule is to define the Source and Destination directions. In the case of our telnet rule, our Source Burb is internal, the Destination Burb is servicenet2, the source IP address object is dudes_laptop and the destination IP address object is ftp_server. This means that the host on GE's internal network that is defined as the dudes_laptop IP Address Object is permitted to telnet into the FTP Server on the service network 2.



Activating the rule:

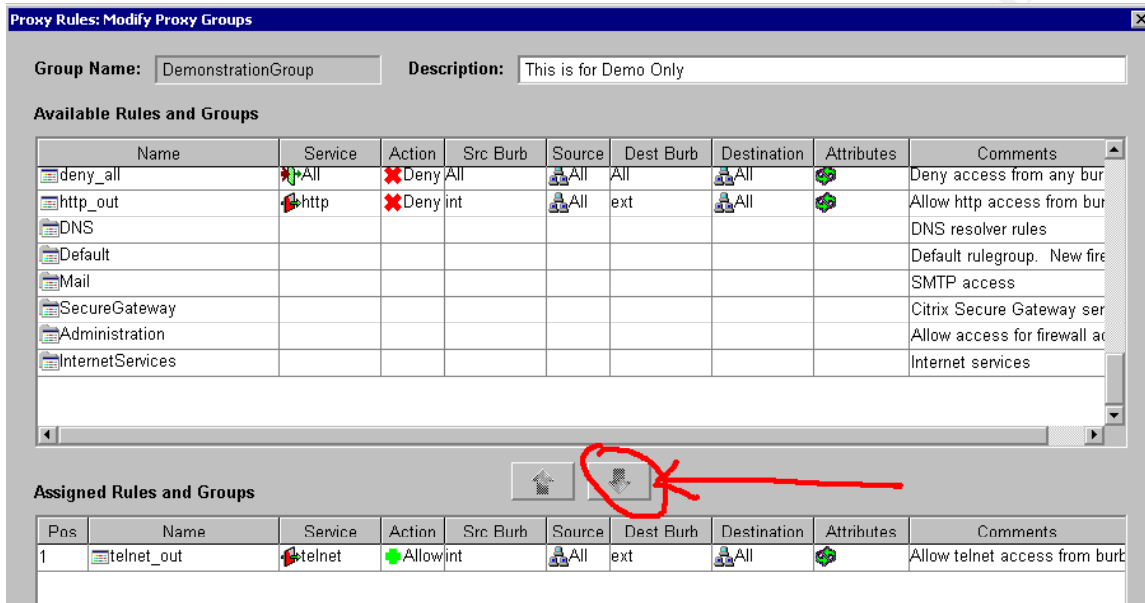
Now that the proxy has been enabled, the new firewall rule has been created it is time to put the firewall rule into the Active Rules group. There are two choices, you can either add the new rule to an existing Active Group that is already in the Default Active Group, or if the rule does not fall into one of the established categories, you can create a new Active Group and place the new group in the Default Active Group. Either way, the new firewall rule needs to be in an Active Group that is in the Default Active Group in order to be in the Active Rules.

This is done from the Policy Configuration/Rules node in the Admin Console. If you need to add a new Proxy Group select New > Proxy Group. Enter an appropriate name and then open the Proxy Group by double clicking on it in the Proxy Rules pane. You can filter the view to only display Proxy Groups if this is easier to view.

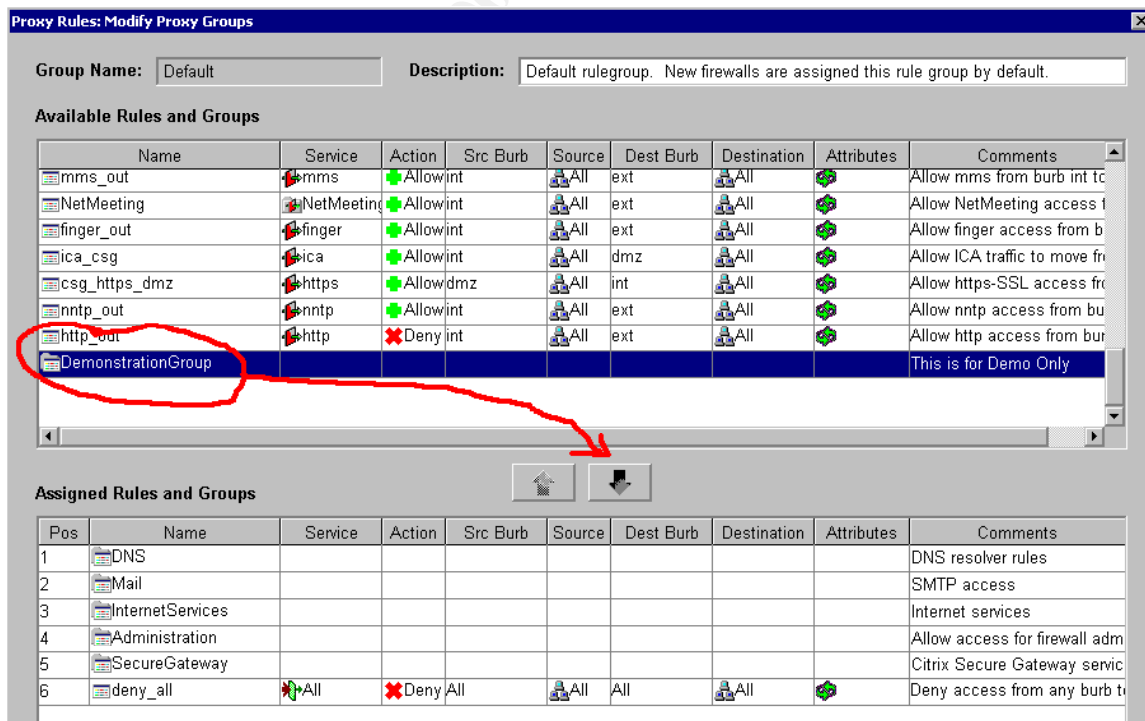
The following picture shows how to add a firewall to a rule group. You open the Rules Group, select your rule and click the down arrow to move the rule into the group. If the rule group is new, you will do a similar action to move the new Proxy Group into the Default Rules Group.

Remember that the order you place the new proxy group in the Default Rules Group will

affect the performance of the firewall. The order that you place the firewall rules in the Rules Group also affect the firewall performance because of the sequential nature of how traffic is processed against the Active Rules. The firewall checks every rule in every group sequentially until it finds a match or until it hits the deny all. This is important so proper planning of new firewall rules is necessary.



Moving a new proxy group into the Default Rules Group:



Apply the rule:

The last thing to do is to apply your changes. This is very easy. Close any open dialog boxes, and click the Save Icon on the Admin Console toolbar. That's all it takes to apply your changes. Your rule is now active. You can view the Active Policy again to verify that your newly created rule is active.

4.6 Backup the configuration file:

Though this is not necessary to create and apply rules, but it is good change management procedure, you should always make a backup copy of the firewalls configuration files following any ACL changes. Configuration changes can be backed up to floppy disk, the local SideWinder hard drive or another SideWinder G2 hard drive.

To backup the configuration files do the following:

- 1) Start the Admin Console and select Firewall Administration > Remote Administration > Configuration Backup
- 2) From the Configuration Backup dialog box in the Action field, select Backup
- 3) In the Backup To or Restore From field select Floppy Diskette
- 4) Put a blank formatted floppy diskette in the SideWinder G2 firewall
- 5) To begin the backup process click the Save icon on the toolbar
- 6) Label the floppy disk and file with the other SideWinder G2 disks

4.7 Summary:

These steps are all that are necessary to create and apply new rules on the SideWinder G2 firewall. Consult the SideWinder G2 Administration Guide for more complex custom proxies and rules.

This document only describes using SideWinder proxies because at this time this is the only service on the firewall that may require additions or subtractions.

4.8 Tips:

- The order of rules in a Proxy Group are important and the order of Proxy Groups in the Default Rules Group are important. Both affect firewall performance
- Use Network Objects to granularly permit or deny traffic. IP Address Network Objects will be sufficient in most cases, but use Network Group Network Objects to apply the same rule to multiple IP Address Network Objects
- When creating new Proxy Groups remember to add the new group the Default Rules Group
- Add new firewall rules to the Active Rules by adding the rule to one of the

- established Rules Groups or create a new Proxy Group
- Consult the SideWinder G2 Administration Guide or take advantage of our maintenance contract with Secure Computing for complex or custom proxies and rules
- Make a backup of the current configuration
- Keep a sense of humor and have fun

References:

Here are the references of the material that I used to assist in writing this paper organized by assignment. Some material has been used for more than one assignment.

Assignment 1 – Security Architecture

- The complete SANS Track 2 course material
- SideWinder G2 Administration Guide - Secure Computing
- Perimeter Security Planning Guide (SideWinder G2 Edition) - Secure Computing
- Cisco Certified Network Associate Training Guide – Lammle/Sybex
- Citrix Secure Gateway Getting Started version 1.0 – Citrix Systems
- Windows Secure Gateway Guide – Citrix Systems
- Citrix Secure Gateway Checklist – Citrix Systems
- <http://www.securecomputing.com/>
- <http://www.citrix.com/>
- <http://www.cisco.com/>

Assignment 2 – Security Policy and Component Configuration

- The complete SANS Track 2 course material
- SideWinder G2 Administration Guide - Secure Computing
- Windows Secure Gateway Guide – Citrix Systems
- Citrix Secure Gateway Checklist – Citrix Systems
- Best Practices for Securing a Citrix Secure Gateway Deployment – Citrix Systems
- Cisco Certified Network Associate Training Guide – Lammle/Sybex
- http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf

Assignment 3 – Design Under Fire

- Counter Hack – Skoudis
- Security + Study Guide – Pastore/Sybex
- Hacking Exposed – McClure
- <http://www.thc.org/papers/fw-backd.htm>
- <http://groups.google.com/>
- The Art of Deception - Mitnick

Assignment 4c – Work Procedure (Firewall Tutorial)

- SideWinder G2 Administration Guide – Secure Computing
- <http://www.securecomputing.com/>

© SANS Institute 2000 - 2005, Author retains full rights.