Global Information Assurance Certification Paper

Securing an Enterprise Using the Symantec Gateway Security 5300 Border Security Appliance

by
Cory Dodds

Global Information Assurance Certification
GIAC Security Essentials Certification (GSEC)
Practical Assignment Option 1
Version 1.4b
Submitted October 20, 2003

Table of Contents

List of Acronyms and Abbreviations

AV	**Anti-virus**
CD	**Compact Disc**
CPU	**Central Processing Unit**
DMZ	**Demilitarized Zone**
DNS	**Domain Name System**
HTTP	**Hypertext Transfer Protocol**
ICMP	**Internet Control Message Protocol**
IDS	**Intrusion Detection System**
IP	**Internet Protocol**
LAN	**Local Area Network**
LED	**Light Emitting Diode**
MMC	**Microsoft Management Console**
NAT	**Network Address Translation**
NIDS	**Network Intrusion Detection System**
OS	**Operating System**
OSI	**Open System Interconnection**
OSPF	**Open Shortest Path First**
RAM	**Random Access Memory**
RIP	**Routing Information Protocol**
SGS	**Symantec Gateway Security**
SMTP	**Simple Mail Transfer Protocol**
SRL	**Secure Remote Login**
SRMC	**Symantec Raptor Management Console**
TCP	**Transmission Control Protocol**
UDP	**User Datagram Protocol**
VPN	**Virtual Private Network**

List of Figures

I. Introduction

Symantec introduced the Symantec Gateway Security (SGS) line of products as an "integrated security" solution. A descendent of the Raptor and Symantec Enterprise Firewall series of security appliances, the SGS series focuses on defense in depth by providing virus protection, intrusion detection, and intrusion prevention, in addition to normal firewall functionality. Symantec combined this feature-set with a hardened version of RedHat Linux as the core operating system (OS) and a Sun server as the platform to create a very impressive package.

While there is no disputing that the SGS contains an impressive feature-set integrated into a single 1U rack-mountable device, the SGS is not without it's weaknesses and drawbacks. Configuration can be a long and tedious process of fine-tuning the SGS to your environment. In addition, some of it's features do not match the functionality available in dedicated devices. This paper will detail the features, abilities, strengths, weaknesses, and proper configuration of the SGS 5310 border security appliance.

II. Overview of components and Features

A. Hardware and Operating System

The SGS 5300 series is based on two core components. The first is the hardware platform. The SGS 5300 series is based on a Sun Microsystems server. The hardware specifications are impressive: one 1Ghz CPU (upgradeable to two CPUs), 512MB RAM (upgradeable to 1GB), one 40GB hard drive (upgradeable to three), and four configurable 10/100 Fast Ethernet ports. Of the four Fast Ethernet interfaces, the first in an inside interface – meaning the network connected to that interface is considered trusted, such as a LAN subnet. The second is an outside interface – meaning the SGS treats the network connected to that interface as a non-trusted network, such as the internet. Sun has once again provided a piece of hardware capable of getting the job done while delivering the reliability and stability it is known for.

The second is the hardened version RedHat Linux that the SGS 5300 series runs as its core OS. Choosing a Linux operating system was an interesting choice, especially considering that competitors in the firewall market, such as Cisco Systems, use proprietary operating systems. Using a Linux operating system opens up a number of very interesting possibilities, such as the ability to run Linux applications such as TCPDump and Snort directly on the SGS. This paper will describe how to run TCPDump on an SGS in a later section.

B. Overview of Features

As mentioned before, the SGS 5300 series has an impressive feature-set. These features include firewall functionality, a network intrusion detection system (NIDS), and Anti-virus scanning. While the aforementioned features collectively make up the core functionality of the SGS 5300 series, it also includes VPN functionality, content filtering, and high availability / load balancing capabilities. These features will only be covered in a peripheral manner in this paper. Keep in mind that, while the SGS can be configured with static routes, it does not support any dynamic routing protocols, such as RIP and OSPF. The following section contains more detailed information on each of the three core functions of the SGS 5300 series.

III. Firewall, NIDS, and Anti-virus Scanning: The Details

A. The Firewall

The SGS 5300 series is first and foremost a firewall, and despite all the additional features and frills, it performs this function very well. The firewall component of the SGS functions at the application layer of the OSI model (layer 7) and is considered a hybrid firewall – meaning it has elements of both common statefull packet inspection (SPI) firewalls, and proxy firewalls. This has both positive and negative side effects for this reason: Examining data as it passes through the SGS at all layers (1-7) is a very thorough process, which is good. The downside is in resource usage, since the SGS effectively views every bit of data that passes though at all seven layers. Fortunately, the SGS has the speed to process traffic in this manner with a minimum of latency. When the SGS is configured correctly it can pass traffic at speeds of up to 70Mbps, which is comparable to many routers.

The SGS uses proxies to pass traffic. This is a very useful feature, as it provides NAT-like security. When these proxies are enabled, devices on different interfaces of the SGS will see the nearest SGS interface as the source of the traffic (see Figure 1). Again, this added security comes at a price. If, for example, Host A views a webpage on Server B, the webserver logs on Server B will show the inside interface of the SGS as the source IP address (see Figure 1). While this can be problematic for logging and tracing, the logging capabilities of the SGS offset this weakness by providing a central location to view a log of all traffic.

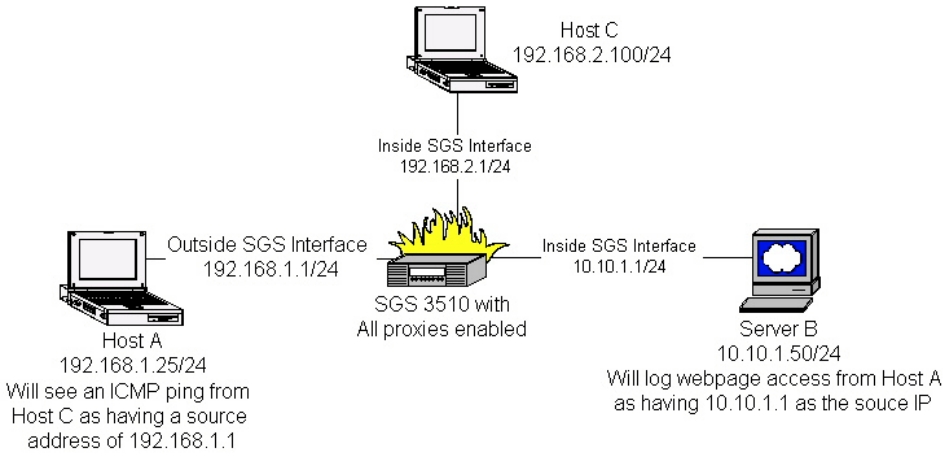

Figure 1 – How the Proxies Work

It is important to mention that the proxy daemons can be disabled. This may be advisable if you have multiple layers of security since the proxy daemons will render source-IP filtering or intrusion detection virtually useless to security devices past the SGS-protected perimeter. Additionally, network entities outside your organization may need to permit or deny traffic to specific network devices inside your perimeter. Keep in mind that it should be considered best practice to keep as many of the proxy daemons enabled as is feasible for your needs.

B. The Network Intrusion Detection System (NIDS)

The SGS 5300 series also includes a NIDS. The NIDS that the SGS uses is a bit unusual. It has nowhere near the reporting abilities or configuration options of other NIDSs, such as the freeware Snort IDS. On the other hand, it is a very simple, easy to configure NIDS with built-in automatic blacklisting capabilities.

Lets start with the configuration options. You cannot write or modify SGS IDS signatures. You can, however, decide which rules are checked and whether the SGS blocks traffic that matches those rules. Updates to the IDS ruleset can either be downloaded manually, or automatically downloaded and installed according to a configurable schedule. Additionally, you can manually change the default severity levels between Low, Medium, and High for each individual signature.

Another useful feature is the ability to configure the SGS to automatically blacklist hosts based on the severity of the IDS alerts they generate. This would enable you to, for example, automatically blacklist hosts that generate High level IDS alerts to prevent a potential intrusions. This can be a two-edged sword. While blocking potential hackers by completely blacklisting them automatically is very appealing, you also run the risk of blacklisting non-malicious activities due to false positives. This may or may not be a major issue for your organization, but it is certainly a consideration to keen in mind.

The SGS can be configured to either email IDS alerts or send them to a mobile device. The latter is not recommended due to the volume of alerts that will be seen in a production environment. Additionally, the alerts are not as informative as one would hope. They consist of a two to five line message with the time, rule name, source address/port, and destination/port (see Figure 2)

From: Root@device_name.domain_name

Subject: IDS Alert High

Oct 1 10:33:33.314 *device_name* kernel: 575 IDS Alert:
1066415613.312985:128:BugBearB_Worm_Propagation:192.168.1.25:61000:10.10.1.52:25

Figure 2 – Sample IDS Alert from a SGS 5310

Due to the limited amount of information available in the SGS IDS logs, it is recommended that a defense in-depth style strategy be taken when determining your NIDS needs. The SGS certainly has strength in its ability to block traffic matching IDS rules and its automated blacklisting, but it should not be considered a replacement for much more informative and thorough NIDSs such as Snort. One advisable NIDS configuration is in Figure 3.

Figure 3 – One Advisable NIDS Configuration.

C. Anti-virus Scanning

As you might expect of a product from Symantec, the SGS 5300 series includes an anti-virus (AV) scanning engine that uses Symantec's AV definitions. This is one function of the SGS that would be hard to improve on. AV scanning can be enabled or disabled on the device as a whole. If enabled, you have the ability to enable or disable AV scanning on individual firewall rules.

You could, for example, configure an SGS with three internal interfaces and one outside interface. Two of the internal interfaces could be internal LAN segments – Subnets A and B. The third internal interface could connect to a DMZ subnet containing mail and web servers – Subnet C (see Figure 4). With this configuration, you may not want to enable AV scanning between your two internal subnets, Subnet A and Subnet B, due to resource usage on the SGS. On the other hand, you would probably want to enable HTTP/HTTPS (TCP

80/443) and SMTP (TCP 25) AV scanning to all of your mail and web servers in Subnet C. The SGS gives you the ability to fine-tune your AV scanning to give you a maximum level of protection, while maintaining a minimum level of latency.

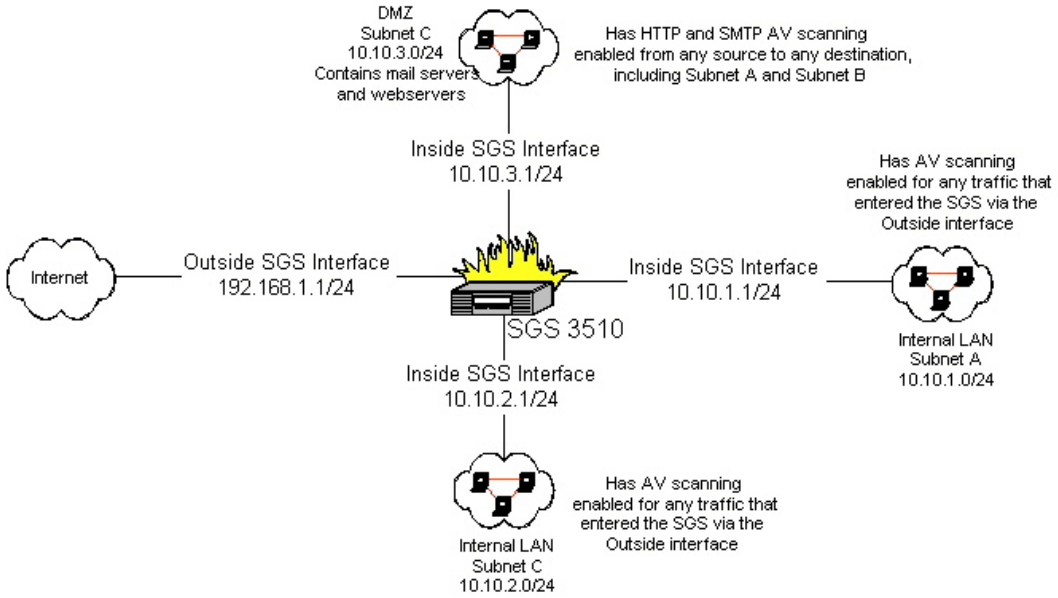

Figure 4 – SGS Anti-virus Scanning Scenario

In addition to being very flexible in exactly what is and is not scanned, the SGS AV system also comes with an easy method for updating virus definitions. Much like updating the IDS signatures, the SGS AV system uses a LiveUpdate feature. You can either manually run LiveUpdate or it can be scheduled to run automatically. Scheduling a daily update during low traffic hours is highly recommended. The updates themselves are very small and take very little time or bandwidth to download and install. It is important to remember that neither the IDS update feature nor the AV LiveUpdate will function without a properly configured connection to the internet and a DNS server specified on the SGS. It is critical to manually check the update features before relying on a scheduled update or after any DNS configuration changes.

IV. Setup and Initial Configuration

A. Initial Setup

The initial configuration of the SGS 5300 series is done through the front panel. There are six buttons and a small LED screen that enables you to enter an IP address, subnet mask, management console IP address, and other basic configuration information (see Figure 5). During this process, you are given three passwords: one for accessing the SGS through the Symantec Raptor Management Console (SRMC), one is the password to the root account in the

OS, and the last is a password for Secure Remote Logon (SRL) client. This paper will not go into detail on the initial setup since the Symantec Gateway Security Appliance Installation and Configuration Guide (the SGS manual) already contains step-by-step instructions for this portion of the setup. Keep in mind that any time you edit settings on the SGS from the front panel, you will be required to reboot.

Figure 5 – SGS 5300 Front Panel. Image © Symantec Corporation
Symantec Corporation. Symantec Gateway Security Appliance Installation and Configuration Guide. Symantec Corporation, 2002. Page 14.

B. Introduction to the SRMC and Setup Wizards

Symantec Raptor Management Console (SRMC) is a Microsoft Management Console (MMC) snap-in. It is more than likely that you will be performing the bulk of configuring, administrating, and monitoring from this console. As shown in Figure 6, the SRMC is a single, simple interface for accessing the SGS. The SRMC is included on the CD that comes with the SGS 5300 series.

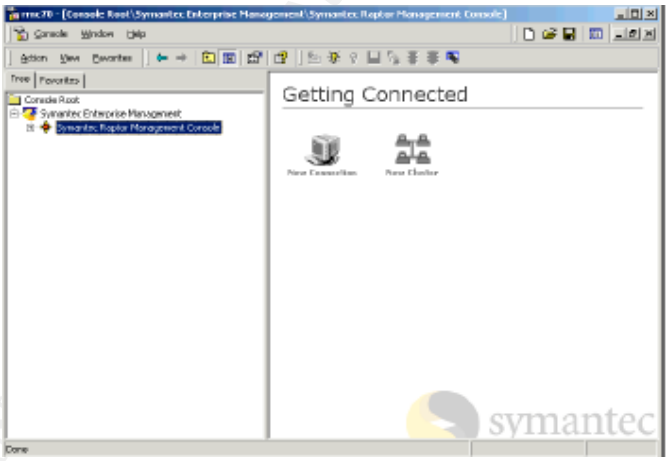

Figure 6 – Symantec Raptor Management Console (SRMC). Image © Symantec Corporation
Symantec Corporation. Symantec Gateway Security Appliance Installation and Configuration Guide. Symantec Corporation, 2002. Page 54.

It is important to remember that the SRMC has not been approved for use with Windows XP or Windows Server 2003. Configuring an SGS from a SRMC located on a non-Windows 2000 computer may cause serious configuration errors. In addition, you should always check for and install the latest SRMC patch before you connect to an SGS. You can check on SRMC patches and service packs for the SGS 5300 at this website:
"Symantec Enterprise Support - Symantec Gateway Security 1.0 - Model 5200/5300"

http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_1_52005300/files.html
Patches and service packs for the SGS 5310 can be found at this website:
"Symantec Enterprise Support - Symantec Gateway Security 1.0 - Model 5310"
http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_1_5310/files.html
Using the SRMC on the correct operating system (Windows 2000) and patching it with the latest updates are two of the most critical steps to ensure the proper configuration and long-term stability of your SGS.

After you install and patch your SRMC, the next step is to connect to the SGS with the SRMC for the first time. Once you connect, your first task is to complete the initial Setup Wizard. In this wizard, you will perform basic configuration tasks such as naming the SGS and configuring the interfaces. More information about this Wizard can be found in the Symantec Gateway Security Appliance Installation and Configuration Guide (the SGS manual). At the end of the wizard, the SGS will reboot.

Now that the SGS has a basic configuration, you have the option to use the other built-in wizards, such as the SMTP wizard, to further configure the SGS. While these wizards may seem very helpful, a more precise configuration can be achieved manually. Therefore, the wizards are best suited for people with little experience configuring firewalls, or those who will not have the opportunity to familiarize themselves with the SGS before it is put into a production environment. For those with more time and/or experience, manually creating rules and editing proxy daemon settings is recommended.

C. Pre-configuration Tasks

Once the SGS has been configured with the initial setup wizard, there are two very important tasks that should be completed before any other configurations are made. Failure to perform these tasks can cause anything from serious configuration errors to poor performance. These are perhaps the two most important steps to ensuring the SGS functions properly.

The first is to patch the SGS itself. Unfortunately, this is one process that can not be automated. It is, nonetheless, as simple procedure. To begin, check the website that is appropriate for the particular model of the SGS you are running.
Patches and service packs for the SGS 5200 and 5300 can be found at this website:
"Symantec Enterprise Support - Symantec Gateway Security 1.0 - Model 5200/5300"
http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_1_52005300/files.html

Patches and service packs for the SGS 5310 can be found at this website:
"Symantec Enterprise Support - Symantec Gateway Security 1.0 - Model 5310"

http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_1_5310/files.html
The above links are the same websites used to download SRMC patches and service packs.

Once the appropriate patch is downloaded in .zip format, unzip it using WinZip or a comparable application and place the unzipped .tar file on a computer which has the SRMC installed on it. Connect to the SGS using the SRMC, then right-click the name of the SGS in the left of the console, expand All Tasks and click Patch. You will be prompted to browse to the location of the .tar patch file. Select the .tar file and then follow the on-screen directions.

After you patch the SGS you should tune your SGS. This is the second of the two very important configuration tasks mentioned earlier. Symantec has provided a document on this matter that can be here:
"How to tune your firewall after applying hotfixes - Symantec Gateway Security 1.0"
http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003061017501054

The instructions from Symantec can be difficult to follow, due to their vagueness. Below are some of the most commonly edited settings, and their recommended values.

- udp-gsp.csvr.max_conns= By default, this is set to 256. If have a mid- to large-sized network and send DNS queries through SGS, you should probably increase this to 512 or 1024. Also, if you have a considerable amount of LAN traffic passing through the SGS (NetBIOS, for example), you should increase this to 512 or 1024. If you have both, or have large amounts of UDP traffic passing though the SGS for any other reason, you may want to consider increasing this to 1536 or 2048. Check the logs on the SGS to make sure you are not getting udp-gsp thread limit exceeded warnings. If you are, increase this setting further. If you run out of UDP threads, you will begin to see high latency in UDP traffic.
- pingd.csvr.max_conns= By default, this is set to 256. If you permit ICMP into your network, you may want to increase this to 512. Worms like Welchia can tie up 256 ping threads pretty quickly and prevent normal ICMP traffic from passing.

- ScanThreads= By default, this is set to 10. If you are scanning all HTTP and/or SMTP traffic on a mid- to large-sized network, you will want to increase this to 200 or 300. Leaving this at it's default will cause extreme latency for all AV scanned traffic.

If at any point you find you are experiencing latency, be sure to check the logs on the SGS for any sort of "threads exceeded" errors or warnings. If you see any warnings that match that criterion, you should take the time to visit the link above and consider boosting some of the settings. In most cases, the SGS

has the extra resources to allocate to add additional threads; it's just a matter of adding them.

V. How To…

A. Keep from Exceeding License Limits

If you suspect you may be running out of licenses, you can check by right-clicking the name of your SGS on the left side of the SRMC and going to properties. If you have in fact exceeded your license limit, you should scroll down the list of Opened and Closed connections on the same properties tab. Look for anything that has a large number of open connections and investigate to see if this is normal for your environment. If it is not, consider blocking the port(s), if possible. If you need the port(s) open, consider moving the resource to the same network as the traffic is originating from. Symptoms of exceeded licenses is as follows: some hosts will be able to pass traffic through the SGS without any problems – because they already have a session – while other hosts will have their traffic completely dropped by the SGS – because you are out of licenses, no more sessions can be created.

B. Capture packets with TCPDump

Running TCPDump – a very powerful and well-known packet sniffer – on an SGS is just like using it on any other Linux system. Since the SGS comes with TCPDump pre-loaded, no installation is required. Simply connect to the SGS using the SRL, then use the tcpdump command. Symantec has provided a set of instructions in the event that you are unfamiliar with the TCPDump utility: "How to use the Tcpdump utility"
http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2002021911533154?Open&src=ent&docid=2003061809255154&nsf=ent-gate.nsf&view=38e56e3d471fe42c88256bc1005cd7d4&dtype=corp&prod=Symantec%20Gateway%20Security&ver=1.0%20-%20Model%205310&osv=&osv_lvl=

C. Protect Against IP Spoofing

These are some general tips that can help mitigate the danger of IP spoofing on any firewall.

1. DO NOT allow internal (LAN) addresses to enter you network through the external interface. This keeps malicious hackers from successfully spoofing their source IP to match the IP of a trusted host on the inside of your network to gain unauthorized access to your network.
2. DO NOT allow private IP ranges, such as 192.168.0.0/16, to enter your network.

3. DO write "tight" firewall rules. This means that if you want to permit Subnet A (interface eth0) to have outgoing access any protocol and any port on Subnet B (interface eth2), create a rule that allows exactly that. Here is an example:
   Permit any IP traffic. Source: Subnet A. In via: Eth0.
   Destination: Subnet B. Out via: Eth2.
   As opposed to this sloppy rule:
   Permit any IP traffic. Source: Subnet A. In via: any.
   Destination: Subnet B. Out via: any.
   Or:
   Permit any IP traffic. Source: Universe. In via: Eth0.
   Destination: Universe. Out via: Eth2.

And while this is not specifically related to IP spoofing, you should try to avoid using the *all** protocol in your rules (basically all IP protocols). Instead, create custom protocols that have specific TCP or UDP port ranges.

D. Make the Most of Your Logs

The SGS has amazing logging capabilities. Depending on what you choose to log, you could maintain a log of all traffic passing through the SGS until it runs out of storage space – at which point you could archive them to another storage device. You will find that manually sorting through the logs is a daunting, if not impossible task. Symantec included a simple yet effective filtering function with the SRMC. To use it, simply right-click any log file from inside the SRMC and then click Filter. You can filter by event type – Information, Warning, Error, etcetera – and by text patterns, among other options. To see what traffic has been coming from or going to a particular IP, just filter with the IP in question as the Text Pattern and check all the event types (Information, Error, etcetera). The SGS will then filter the logs and display the results. You may then click any of the other log files and have your filter automatically applied to them. This is an excellent tool for tracking down suspicious activities on your network.

E. Automatically Blacklist Based on IDS Alerts

You can configure the SGS to automatically blacklist IP addresses that are the source of IDS alerts. To do this, create a new notification with a Source of IDS and an Action of Blacklist. You can also configure the severity of IDS alert that will result in blacklisting – High, Medium, or Low (you can select any combination of the three levels). Keep in mind that one false positive could result in blacklisting an innocent user.

VI. Conclusions

The Symantec Gateway Security 5300 border security appliance is an excellent product, especially for businesses that cannot afford a dedicated firewall, a dedicated NIDS, and gateway-level anti-virus scanning. While it can be a tedious process to learn the basics and then get the SGS configured properly for your environment, it works like a dream once everything is configured properly. If you do encounter problems, you will find the Symantec support helpful – especially if you purchased the Platinum Support option.

With a properly configured SGS running at your border, you won't find yourself wondering at night whether your firewall is actually providing protection. Perhaps that is the highest praise that can be bestowed upon a firewall.

Works Cited

Symantec Corporation. Symantec Gateway Security Appliance Installation and Configuration Guide. Symantec Corporation, 2002. Pages 14, 54**.**

“Symantec Enterprise Support - Symantec Gateway Security 1.0 - Model 5200/5300” 11 June 2003. URL: http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_1_52005300/files.html (18 October 2003)

“Symantec Enterprise Support - Symantec Gateway Security 1.0 - Model 5310” 11 June 2003. URL: http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_1_5310/files.html (18 October 2003)

“How to tune your firewall after applying hotfixes - Symantec Gateway Security 1.0” 26 June 2003. URL: http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003061017501054 (18 October 2003)

“How to use the Tcpdump utility” 16 May 2003. URL: http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2002021911533154?Open&src=ent&docid=2003061809255154&nsf=ent-gate.nsf&view=38e56e3d471fe42c88256bc1005cd7d4&dtype=corp&prod=Symantec%20Gateway%20Security&ver=1.0%20-%20Model%205310&osv=&osv_lvl= (18 October 2003)