



## Review: Secure SnapGear SG565

By Steve Ragan

The Secure Computing® Secure SnapGear SG565 is a small and almost invisible device when it is sitting in the back of a desk doing its job. However, the little blue box lives up to the “good things come in small packages” saying, because despite some faults, there is nothing to be ashamed of if you replace several rack based appliances with this tiny device.

This review will cover the aspects of the Secure SnapGear SG565, both good and bad, while explaining some of its core functions. The SG565, as it will be referenced during this review, is aimed at medium businesses and can mix well with existing hardware. Tech Herald had arranged a demo of the SG565, and Secure Firewall Reporter (log monitoring and auditing software) before we met with them at RSA. The testing of the device started April 21, 2008. Over the past few weeks, the SG565 has managed and defended a network that contained the following:

### Hardware:

- Gateway Laptop (Vista SP1)
- Dell GX 150 and GX 280 (XP SP2 on both)
- Non-branded computer (XP SP3 and Ubuntu 8.04)

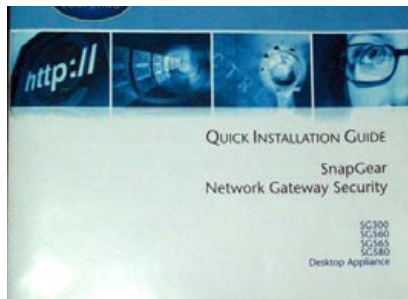
### Virtual:

- Windows Server 2003 SP1 (w/IIS at one point)
- Windows XP SP 3 (x2)
- CentOS 5.5 (Webserver)

While not scientific, the goal was to use the lab computers and virtual computers to mirror a small business. Several aspects of the SG565 were tested including the firewall, IPS and IDS protections, and VPN, to name a few. The lab was assigned its own domain name, and all efforts were made to mirror a solid business network. This review should only be used as one part of a company's overall research into Secure Computing or any network security device. With that said, lets move on to the good stuff.

### Deployment:

Out of the box deployment and setup is a snap. The SG565 earns its name because with a little effort, and easy to follow instructions, you can deploy this in a matter of minutes. In this test, the complete setup took fifteen minutes.



There is network storage available on the SG565, as you can see in the image. Attaching a USB drive to one of the two slots in the rear of the unit allows you to setup log storage. The image shows a 1GB USB flash drive. (You can use a USB hard drive as well.)

The software setup is straight forward. Once the hardware is configured, you go through the wizard to complete the setup.



One interesting aspect of the SG565 is the ability to isolate the ports for more advanced networking. This feature was not used during most of the test but configured originally to test the abilities of the unit. The performance of this feature worked well, and behaved as expected.

Once the wizard is finished, you will want to check the Network Setup area of the administration console to double check the settings. Another area to check is the Diagnostic section, and look for a state of up on the connections area.

Other aspects of the network setup area include, DHCP server, Shares for management of network storage and printing, QoS Traffic Shaping, SIP Proxy management, and Web Cache, which as the name suggests, allows storage of Web sites in cache on the SnapGear unit.

Once network setup is set to spec, you can start getting security in place.





authentication. (Note: To use the authentication you must set the browser to use the Secure SnapGear unit as the default proxy. There is help in the administration manual to cover this.)

When using ACL (Access Control Lists) on the SG565, the definitions you created earlier are helpful. Here you can allow or block access based on the definitions and control the browsing this way. You can restrict access to URL's, or allow them with Web Lists, or use NSAL scripts, which are a part of the Nessus Vulnerability Scanner, to manage access. Lastly, you can purchase a subscription to Webwasher and perform content filtering and logging from there.

Webwasher is an old brand name for what Secure Computing now calls Secure Web. In the control panels for the SG565, Webwasher is the name listed, and will be referred to as such. If you are doing research on content filtering, then the product you need to check for is now named Secure Web. (<http://www.securecomputing.com/index.cfm?skey=22>)

Webwasher was simple to setup and configure. In the SG565 control panel, you can access Webwasher and its settings. However, until they are licensed and activated, they are worthless. Once activated, you can filter internet traffic using category based detection and filtering. There are over sixty categories to pick from, and they cover what you would expect in a URL filter.

The AV protection offered on the Secure SnapGear unit comes by the way of ClamAV. The AV database can be automatically updated, ensuring coverage, but you will be limited to what signatures ClamAV offers. This is by no means a replacement for network wide AV protection. With that said, you can use the AV protection on the SG565 to cover POP, SMTP, Web downloads, and FTP. You have the option of selecting a network share or USB share on the SnapGear unit to provide storage for the AV database and temporary files when scanning. (Network Share is recommended for effective scanning.)

Anti-Spam features on the SG565 run from TrustedSource™, which was not tested during this review. However, if you want to learn more, visit the TrustedSource Web site. (<http://tinyurl.com/6l472x>) The lack of Anti-Spam testing had no impact on the overall review of the SG565. The reason for no testing was do to licensing. During the review, there was no license made available to test the TrustedSource component.

## VPN Control

The SG565 offers a couple of options for the VPN settings. PPTP and L2TP VPN access is offered, and you can configure both servers and clients for either method. The setup is wizard based, and easy to complete. IPSec VPN, and SSL VPN are options for port tunneling as well.

## Testing

### IDS/IPS

SNORT worked as expected, blocking all known types of scans and attacks. While some port scanners were able to obtain information there is nothing that was able to bypass the SG565 that would not bypass other network appliances. Likewise, direct attacks using PHP vulnerabilities were stopped by matching signatures in SNORT. In addition, attacks that rely on the user taking action to exploit a computer locally or remotely worked. One example is taking advantage of the "Print Link Tables" flaw in Internet Explorer. In various tests using this exploit, the Windows XP SP3 computers were exploited with the user being the cause.

Overall, the straight forward attacks on the network failed for the most part due to SNORT catching a known signature, or the systems being fully patched.

(Note: Remember this test was aimed at replicating a real business network, the systems in a proper environment are patched fully and properly managed in IT. The systems that were left unpatched fell to various issues including XSS, SQL Injection, and other vulnerabilities that targeted various services. This is to be expected, and even on the unpatched systems SNORT logged the attacks, an in some cases blocked what the rules were designed to block.)

### Secure Web (Webwasher)

Webwasher worked so well it at one point stopped all internet traffic during the test. You must take care when selecting what categories to filter. One of the sites that ended up being filtered the most during the test was iGoogle. Because of the various gadgets in place and various feeds from Google Reader, the pages would end up blank.

This is not necessarily a bad thing. This proves that the filtering does work. Using the DeepThroat script from Untangle, Webwasher earned a 98% block rating, effectively killing off almost all of the sites loaded from the script. The testing script and source is available on the Untangle blog if you want to try this at home.

One odd occurrence during testing proves that you have to be careful with what you filter. Selecting the "Information Security" as well as, "Web Hosting/IT Services" and "Business/Services" services categories ended up filtering several legit applications. Once, when a Web site was blocked, the SG565 offered to check the URL. When the link was clicked to submit the URL to the Secure Computing Web site, it was blocked by the filtering. This happened once, but we have not been able to recreate the issue, nor have we seen the submission page again.

When enabling Webwasher, it was nice to see that it worked well with the rest of the options on the SG565 security matrix. However, that was also a minor annoyance. When setting up, a filtering mistake killed access to the SnapGear unit on all but the SSH port.



During the test, aside from the testing with the Untangle script, Webwasher categories were enabled one at a time, and various well known sites were visited to record the pass or fail rating. For example, the Music/Web Radio category blocked AOL, Yahoo, Shoutcast, and various online radio stations.

Sensitivity was not noticed until three or more categories of various degrees were selected. If you intend to lockdown internet traffic, then Webwasher will do this, but the ACL option, which does not require a license, is a reliable method. The catch is you have to be detailed, and it would take a good bit of effort to manage and maintain.

However, with that said, the ability to have this type of granular content control without Webwasher is a huge plus for the SG565.

### Anti-Virus

AV was tested on a limited basis. The AV engine detected known Virus files as they were downloaded from the web, so the protection works as designed. If you chose to use this in conjunction with other network AV protection, use the network share option for better performance. Remember, this is NOT a viable replacement for network scanning and protection. Use the ClamAV engine on the SG565 as a layer of security, not as the magic bullet.

### VPN

Testing of VPN was relatively simple. A PPTP and L2TP client and server were each created and configured according to documentation from Secure Computing. Both worked as designed, and management was simple. The ability to assign DNS and WINS to the VPN makes the entire function work like other devices found in a network. There were no glitches or problems connecting with either protocol or accessing the LAN remotely.

### Overall:

The SG565 has a good deal of options for such a small package. The experience with deployment and management has been a positive one the last few weeks. The security aspect of the SG565 is typical, as almost all of the similar products offer IDS/IPS/Virus/Spam protections. However, adding TrustedSource instead of normal Spam filtering that is blacklist based is a bonus. (Even without testing, reputation based management for Spam is faster and stronger than blacklist solutions.)

The granular level of control to some aspects is also a decent plus considering some of the similarly priced devices on the market do not offer all the controls you will get with the SG565. However, the layered controls and the feature rich contents of the unit might sway some from using it to its full ability.

In each section and on each tab there is a link to built-in help. The built-in help functions covered many areas, but some sections were lacking in clear documentation. One example of where documentation would have helped was the custom IPTABLES rule section. The help simply explains that, "...only experts on firewalls and IPTABLES will be able to add effective custom firewall rules. It is preferable to use the rules defined on the Packet Filter Rules page instead."

This is true, however giving even a basic example of how to use that area would have helped. This lack of clear documentation can be offset by the detailed administration manual and online knowledge base. However, the Knowledge-base, which the internal help refers to, is also hard to navigate and it too lacks some clear information when researching help to a problem. There is community help, but that is really a Yahoo discussion group that has little traffic to it.

Now, documentation gripes aside, the SG565 is \$629.00 and Webwasher will cost \$149.00 extra. For this cost, this device is worth every penny, especially for the small company who needs an extra layer of security but cannot afford it. Add to that the VPN offering, and you have a good package for the price. (Cisco offerings can be almost twice the cost of the SnapGear SG565.)

### Ratings:

The SG565 was rated according to the following list worth twenty points each.

1. Features and options
2. Adaptability with other devices
3. Security – How well can it protect the network
4. Usability – How easy was it to set-up and manage
5. Overall performance
  1. 20 (TrustedSource, VPN, UTM security, all equal an impressive feature set.)
  2. 20 (There is nothing on a network that the SG565 cannot work with.)
  3. 20 (SNORT acted exactly as advertised. The only issues were user created.)
  4. 15 (Documentation on the internal help. However, it is easy to use on your own.)
  5. 15 (Solid performance and strong features make the SG565 worth looking at.)

With a total score of 90, the SG565 is worth looking in to and more than worth your time. The price point and features make this a good investment for a small company or office, and offers great room to grow.