CyberGuard Total Stream Protection TSP 7100

A report on CyberGuard's carrier grade and high enterprise security appliance with a full performance test of the Application Inspection features

Testing conducted and report compiled by:

Binary Testing Ltd
Newhaven Enterprise Centre
Denton Island
Newhaven
Sussex
BN9 9BA
t +44 (0)1273 615270

info@binarytesting.com

Introduction

The enterprise firewall market may be relatively mature but the demands on IT security that the latest threats are creating means a drastic rethink is needed to ensure corporate data is fully protected. Traditionally, firewalls have focused on protection at the network layer allowing them to detect and block attacks such as DoS (denial of service). A key advantage of these SPI (stateful packet inspection) firewalls is by only inspecting packets at the network layer they have a minimal impact on network performance, require comparatively low-cost hardware platforms to run on and are relatively simple to install and configure. However, the external threat levels to a network never remain stable and hackers are increasingly looking to the application layer to launch more sophisticated and potentially damaging attacks.

The simple protocol and service based rules used by SPI firewalls are not able to prevent application layer attacks such as buffer overflows so there is a clear need for security solutions to provide deeper packet inspection capabilities allowing them to deliver much greater levels of control into the hands of network administrators. One solution for providing deeper inspection is to partner existing firewalls with specialist products but drawbacks are high costs and increased administrative overheads. Consequently, there is a rapidly growing movement towards a truly integrated approach to network security where a single solution provides multiple services and this is a trend occurring across the entire spectrum of businesses.

For the mid-range business this is relatively easy for vendors to achieve as network traffic levels are lower so performance isn't generally an issue. However, move up to the enterprise level and the dramatic increase in the number of concurrent connections being handled combined with the increased demands of deep packet inspection technology can cause a major issue with service levels. Common ASIC-based hardware may have a problem dealing with these demands so many firewall vendors are embracing an open server architecture allowing them to deliver highly specified and powerful appliance solutions.

Fault tolerance and high availability become critical considerations as the appliance must not represent a single point of failure. It should incorporate component redundancy such as multiple power supplies whilst storage needs to be protected by implementing RAID arrays. For high availability the solution must support deployment of primary and secondary systems to protect against total appliance failure. Where very high levels of traffic are being handled appliance clustering can pay dividends as this provides load balancing and further redundancy as well. As complexity increases with the number of features so management facilities and ease of use for multi-function appliances needs to be addressed to avoid increased running costs. The ability to delegate various day-to-day management functions to different administrators is also a valuable feature and role-based administration can make light work of this.

The bottom line is that as attacks are becoming more sophisticated a standard SPI firewall is no longer enough to protect a business' internal network from being compromised. Deep packet inspection will soon become a requirement rather than a luxury and solutions offering multi-function capabilities will become a key component of an enterprise data security policy.

Executive Summary

Since its inception in 1996 CyberGuard Corporation has specialized in network security and has delivered some highly desirable products to market. The TSP 7100 represents the pinnacle of its product line and brings together a unique firewall solution that incorporates its Total Stream Protection (TSP) technology which offers a unique blend of security features including full application inspection and policy based security. A key feature of this appliance-based solution is the use of a range of application proxies that allows security policies to be enforced at the application level.

Many security solutions that employ basic deep packet inspection merely use sets of signatures to check the application layer. CyberGuard's TSP is far more sophisticated as it doesn't rely on signatures but buffers each session, loads it into memory and runs a full inspection. Performance has always been a major concern due to the processing overheads of application inspection. To overcome these issues the TSP 7100 is delivered as a complete appliance based solution with a hardware specification that offers a high processor density,

This report will focus on the TSP 7100 in order to determine its capabilities and suitability for the enterprise and carrier grade network security market. It will run full performance tests on its application inspection features to ascertain its ability to handle very high traffic loads and concurrent connections using the latest Avalanche and Reflector testing equipment from Spirent Communications. A review will also be conducted that will evaluate the key features that enterprise administrators demand. It will look at the installation procedures and ease of use, general manageability, expansion potential, reporting and fault tolerance.

Testing Scenario

Objective

The test objective was to measure key performance aspects of the CyberGuard TSP 7100 Enterprise firewall appliance in order to ascertain its abilities to handle very high traffic loads when using application inspection. Sets of tests were carried out in both its HTTP Proxy and Circuit Proxy states. A further set of tests was run to measure basic Packet filtering performance. The CyberGuard TSP 7100 was equipped with 4 6-port copper 10/100/1000 bits per second Network Interface Cards (NICs), 4 AMD Opteron processors, and 4 gigabytes of main memory. CyberGuard configured the appliance for optimum performance, with each Opteron processor managing one NIC.

Equipment

We used two pairs of Spirent Communications' Avalanche 2500 and Reflector 2500 systems, running version 6.51 of their Avalanche Commander software. The Avalanche equipment can simulate large numbers of network users, while the Reflector can simulate various types of server and can respond appropriately to the requests made by the Avalanche. It is possible to simulate large numbers of users creating various kinds of traffic, including web browsing, e-mail and file transfer sessions, with the Reflectors returning the appropriate responses for each type, generating realistic network traffic loads. Each Avalanche and Reflector 2500 was equipped with 2 dual-port copper 10/100/1000 bits per second NICs and was capable of generating up to 2 million simultaneous TCP connections and over 2.2 Gbps (Gigabits per second) throughput. Two pairs provided ample testing capacity, being capable of producing throughput in excess of 4 Gbps. Two further pairs were held in reserve to provide extra testing capacity if needed.

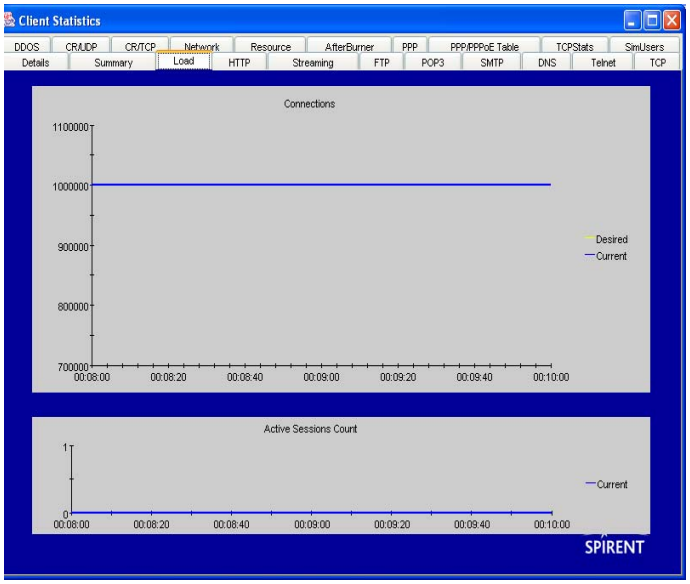
The Spirent Communications' Avalanche and Reflector equipment can generate network traffic loads using a number of parameters which can be set to control both the type of traffic and the rate at which it is generated. System performance can be monitored in real time using various displays, and the data collected by the system can be analysed using Spirent's own analysis programs or by other specially-developed programs. The Avalanche and Reflector pairs were connected directly to the TSP 7100 to eliminate any possible loss of performance that might be caused by any intervening switch equipment.

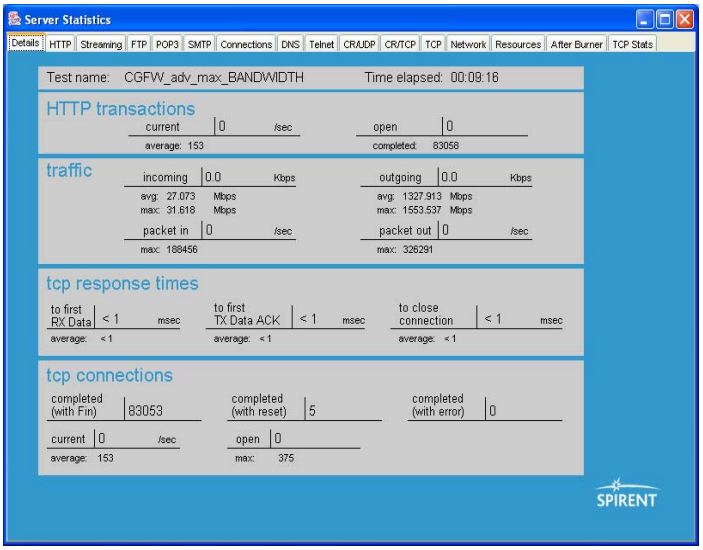
TESTED with SPIRENT

Testing scenario

Plan

The test plan required that the performance factors would be measured in a particular sequence, with each factor determining a parameter for a subsequent test. These factors were determined with the appliance operating in its basic packet-filtering mode.
The first factor to be tested was the maximum connection rate the device could sustain. This factor was then used as a parameter to determine the maximum number of concurrent connections possible, and both of these factors were then used in the final set of tests to determine the system's throughput.
Once these basic performance parameters had been obtained the firewall was then configured to use application inspection. One set of tests was run to determine the maximum connection rate when the system was using HTTP Proxy. This set of tests was then repeated against it using Circuit Proxy. The latter is used for non protocol-specific traffic and provides a proxy for bi-directional TCP connections between two endpoints such as simple client/server connections. It stops the client and server interacting directly by intercepting the traffic and carrying out Layer 5 inspection. System throughput was determined with a second set of tests in the same way; the first set using HTTP Proxy and the second set using Circuit Proxy.
The TSP 7100 was allowed to return to an idle condition determined by monitoring CPU activity, before starting the next test run so that each test would begin with the system in the same state.





Test Methods

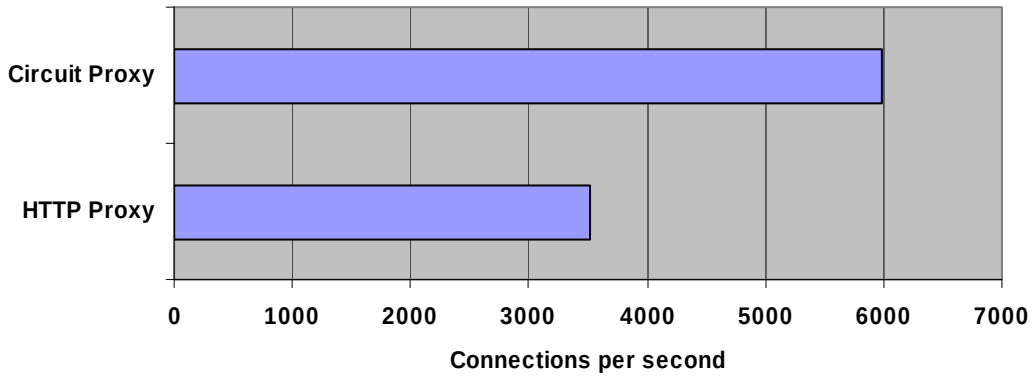
Each test type was run with different sets of parameters to determine which combination would produce the target result without any errors, such as aborted connections, occurring. The tests were set up to generate increasing loads applied in equal steps. Each step could be defined in both quantity and time, and each step was followed by an interval of time during which the system would attempt to maintain the load level. This helped to ensure that the TSP 7100 could adjust to the new load before a further increment was applied. Once the final load level had been reached the system would attempt to maintain the level for several minutes before reducing the load back to zero. Once the correct parameters had been found by adjusting intervals and steps the test was then run with extra steps added to determine if the system could perform successfully beyond its specified limits. More steps were added until the tests began to produce errors. This last test was discarded and the last successful parameter set was used to produce the performance results.

Test Results

Connection rate

The connection rate in the HTTP Proxy state was determined at 3,524 connections per second, while the Circuit Proxy state could sustain a higher rate of 5,992 connections per second. This reflects the extra processing time required to carry out thorough inspection of HTTP packets, which in turn reduces the maximum possible connection rate.

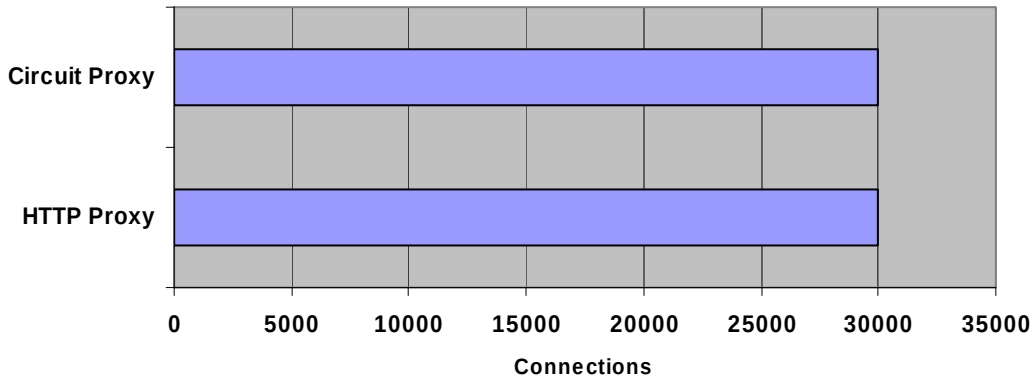
CONNECTION RATE



Concurrent Connections

The system returned average figures of 30,005 concurrent connections in both the HTTP Proxy state and the Circuit Proxy state. The identical results are caused by the system's ability to limit the maximum number of concurrent connections to match the amount of memory available, thus avoiding the potential system instability that can be caused by memory allocation overruns.

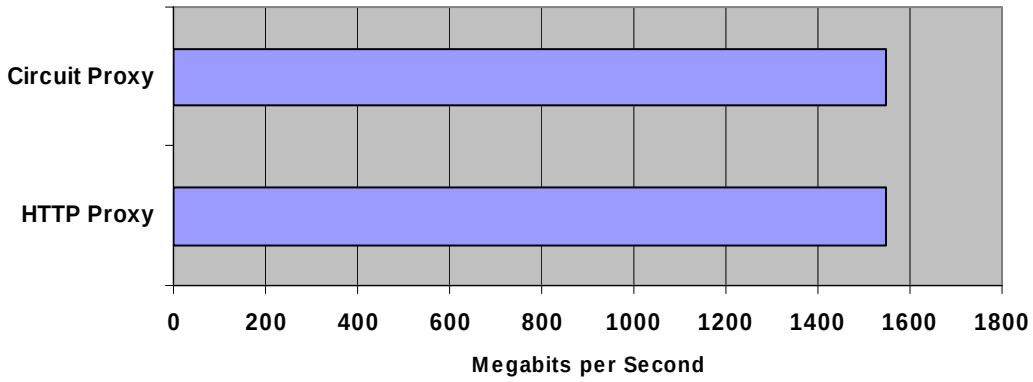
CONCURRENT CONNECTIONS



Bandwidth

The TSP 7100 could maintain an average throughput of 1,546 Megabits per second in both the HTTP Proxy state and the Circuit Proxy state. For these tests the Spirent equipment was set to generate large numbers of users each making ten requests for 1MB data files from the simulated web sites. While this is not a realistic situation, it does have the advantage of generating large amounts of data in a consistent and regular manner and enables the load to be applied in a controlled fashion.

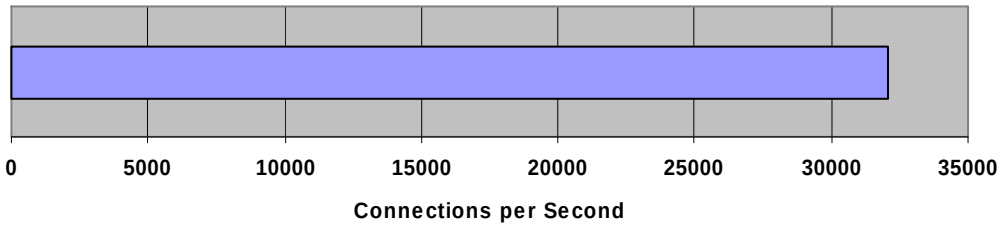
BANDWIDTH



Packet Filtering Connection Rate

The connection rate with the system in its basic packet filtering state was found to be 32,057 connections per second, conforming to the specified rate of 32,000 connections per second.

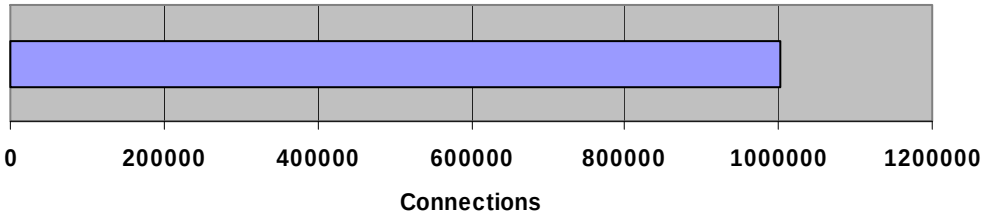
PACKET FILTERING CONNECTION RATE



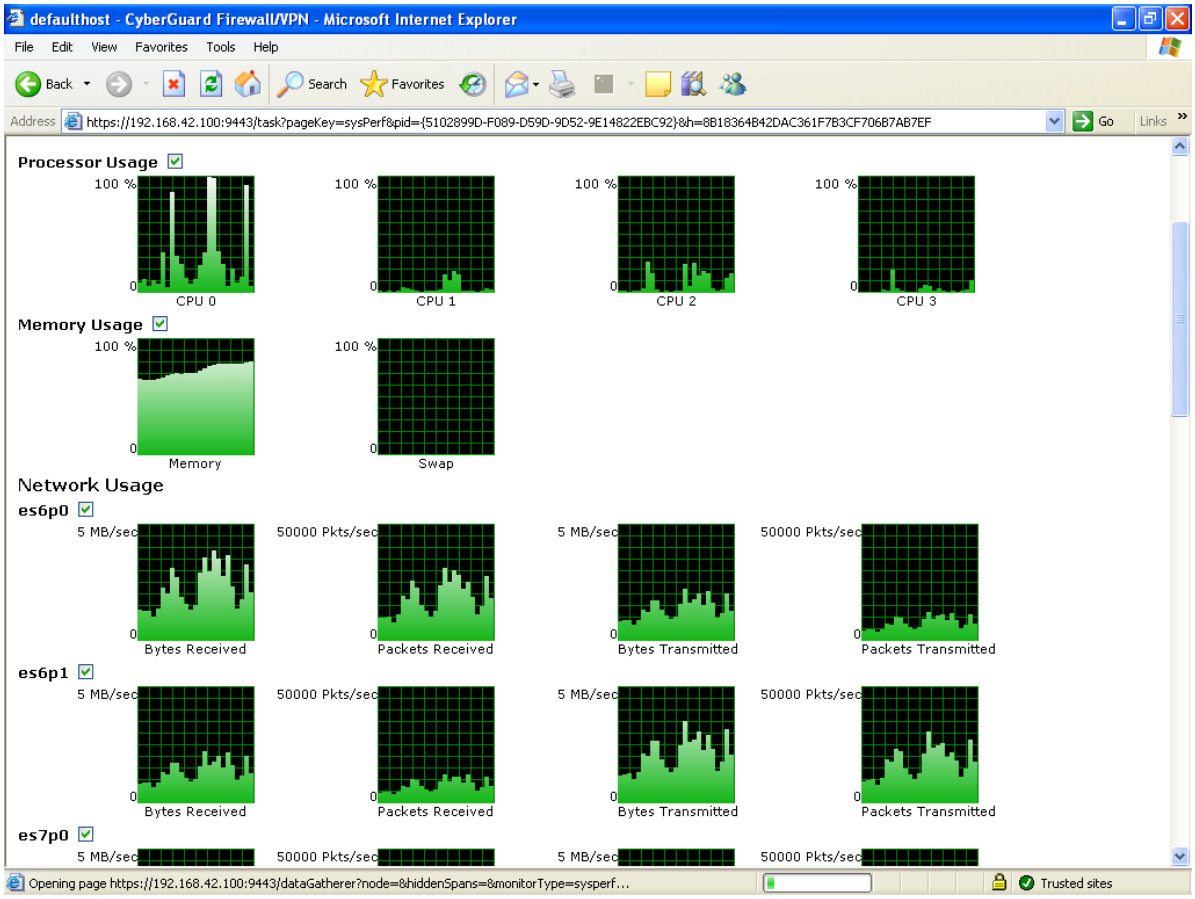
Packet Filtering Concurrent Connections

The system could achieve figures approaching 1,500,000 concurrent connections in bursts, although it could not sustain these levels over time. It was able to maintain an average of 1,001,502 concurrent connections in this condition.

PACKET FILTERING CONCURRENT CONNECTIONS



Test Results



The TSP 7100 real-time monitor display, showing the system under test. The processors are easily handling the traffic load, and in spite of high memory utilisation the system has still not needed to use the swap file.

Testing conclusion

The CyberGuard TSP 7100 Enterprise firewall performed extremely well under test conditions, either matching or exceeding the published performance figures. It showed no sign of instability under high loads, and did not fail even when subjected to loads well in excess of its published limits. It is significant that the system was able to handle all the test loads given to it without resorting to using the swap file. This shows that the system has enough RAM to be able to conduct all its processing in memory without swapping, which in turn allows its CPUs to devote all their capacity to processing traffic, resulting in excellent performance and resilience.

Hardware specification

Physically, the TSP 7100 delivers an impressive hardware specification as it has a Newisys 4300-E enterprise class server as its foundation. The 3U chassis is very well built and designed and delivers the full range of fault tolerant features we would expect to see at this level of the security appliance market. A quartet of 2.2GHz AMD Opteron 848 processors are in the driving seat and these are partnered by a total of 4GB of DDR400 ECC SDRAM memory split equally between all four processors.

Network connections abound as along with a pair of embedded Gigabit Ethernet ports the TSP7100 came supplied with four, six-port Gigabit Ethernet adapters. These 64-bit, 133MHz PCI-X cards from Silicom use Intel dual-controller chipsets and are designed specifically for high-performance servers and mission-critical applications where multiple network segments are required. A key feature is integrated hardware acceleration using a TOE (TCP offload engine) that reduces the load on the main CPUs by performing functions such as TCP segmentation and checksum calculations. As the cards and the server's four 133MHz slots all support PCI hot-plug they can be removed and replaced without requiring any system downtime. A unique advantage offered by the TSP 7100 is that if required it can be configured so that each Opteron processor is dedicated to managing one network card. Furthermore, appliance management access can also be physically separated from general operations by using the embedded network ports purely for these functions. With two more 100MHz PCI slots up for grabs the TSP 7100 can support a total of 38 copper Gigabit Ethernet ports so there is plenty of room to expand with demand.

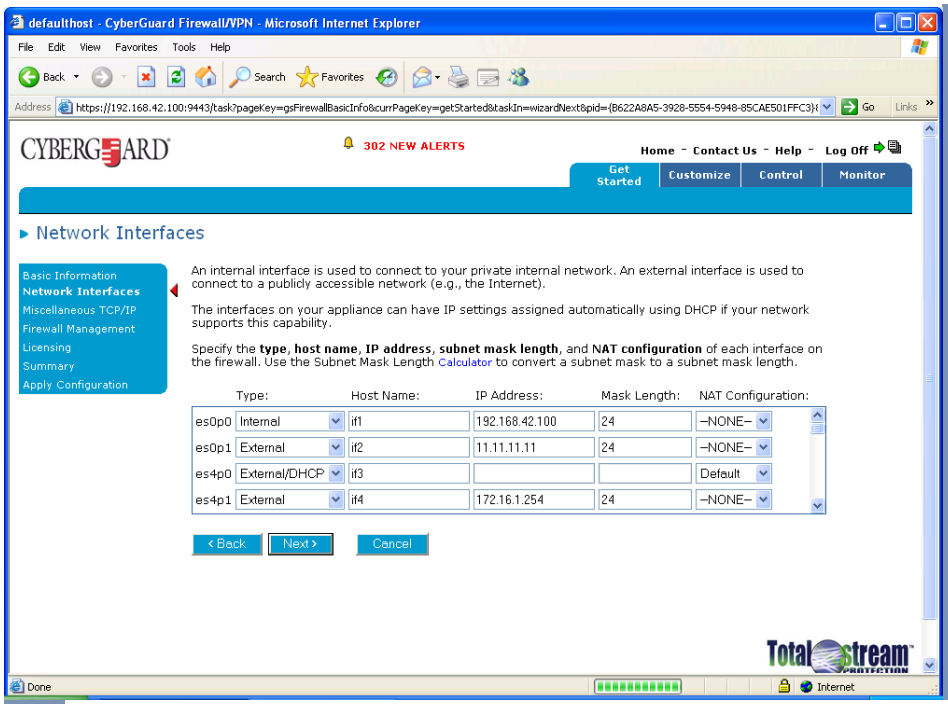
Storage is handled by an LSI Logic MegaRAID Ultra320 SCSI RAID controller card equipped with 64MB of embedded cache memory. There's space for up to five hard disks in the front panel and the system comes supplied with four 73GB Hitachi Ultrastar Ultra320 drives mounted in sturdy hot-swap carriers. Storage fault tolerance is good as the drives are configured in a triple-disk RAID-5 array with hot-spare.

Internal cooling doesn't get any better as the chassis incorporates no less than twelve strategically placed fans and all are hot-swappable. Power gets the same attention as the TSP 7100 is equipped with two 760W hot-swap supplies and these are located in a separate housing that mates with the motherboard and can also be easily removed.

Appliance clustering is fully supported allowing the TSP 7100 to operate in two different high availability modes. In its simplest form two appliances can be configured so that one is designated as active whilst the second remains in standby. If the active appliance fails then the standby immediately takes over all operations. In high demand environments multiple appliances can also be used to share the load where sessions are assigned to a particular device.

Installation

The TSP 7100 may be aimed at the carrier grade and high enterprise markets but it neatly avoids the complexity of installation and deployment inherent in many of these types of appliances. In fact, ease of use is a key feature of all CyberGuard security appliances and this makes them stand out from many competing products. CyberGuard is also to be commended on the excellent documentation provided which covers all areas of configuration in extreme detail.
The appliance can be managed locally by attaching a monitor, keyboard and mouse or remotely via a secure web browser interface. Both methods present the same GUI which we found very well designed and intuitive. The home page presents four tabbed folders for access to wizard based assistance, manually customizing the firewall, controlling both the firewall and system and monitoring all activity.
Installation is helped along nicely by a Getting Started wizard that takes you through the initial processes of defining the network interfaces, securing management access and getting the system up and running. From here you step easily through entering host and domain names and deciding how each physical network interface is to be used. For the latter, each one can be designated as internal, external, DMZ (demilitarized zone) or heartbeat for appliance clustering whilst DHCP client and server services can also be activated on internal or external interfaces. A smart feature is that as you add more network interface cards the wizard can be used to configure them with the minimum of fuss.
Securing firewall management comes next and you can lock down remote access to a selected network interface and a filtering rule will be automatically created for this. Security goes much further as you can designate specific systems or hosts attached to the chosen network interface that are allowed management access. The final job is to enter the license codes purchased for each feature, review a summary of the initial configuration and then apply all changes. It's important to note that no changes are made to firewall operations on the fly so you can easily review any modifications before activating them. Furthermore, any configuration changes that have not been applied are highlighted and the soft button at the top of the management interface used to apply these only appears when any changes to the current configuration have been detected.



Configuration
The object advantage

Commendably, the appliance defaults to blocking all inbound and outbound traffic and requires packet filtering rules to be created before any access is granted. Each rule comprises an action, service, source, destination and time period and it's at this stage you start to see how easy it is to configure the TSP 7100. All these elements are defined once as objects that can be employed in multiple access rules and if the object itself is modified at a later stage then these changes are automatically propagated to all other rules that are using them.

Actions can be as simple as allowing, blocking or dropping packets or using one of the many proxies provided, whilst service categories include ICMP, IP, TCP and UDP plus groups comprising multiple categories. Each one comes with a wealth of predefined services which will cover virtually all eventualities but it's easy enough to create custom services if required. The same applies to sources, destinations and time periods and each one provides a list of predefined objects for immediate selection. If there isn't one that suits then you just click on the small cross above each section and a new window opens up allowing a new object to be swiftly created. As you'd expect, each packet filtering rule is placed in a list in order of processing priority but it's easy enough to promote or demote them.

All objects are accessed from the Environment tab in the Customize section. Endpoints describe all sources and destinations and can be anything from a fully qualified hostname, IP address or address range to a subnet or a network interface - the firewall itself is also available as an endpoint. Time period objects add considerable versatility to access rules as they can define a date range and this can include a specific period of hours for each day. A simple example would be a standard working week with a 9-5 time period. Alternatively, schedules can be used to activate access rules on particular minutes, hours, days, weeks or months. Changing a time period give a simple example of how powerful objects can be. If you decide the working week time period should start at 08:00 a.m. instead of 09:00 a.m. then simply change the relevant time period and all rules that include this object will start an hour earlier as soon as the changes have been applied.

In today's enterprises change management is an important process and the TSP 7100 includes facilities for tracking and auditing configuration changes. When enabled, this feature requests that descriptions of the changes being made and possibly the reasons are entered before they can be applied, and a ticket can also be used as an identifier for the administrator making the changes. All previous configuration files are maintained on the appliance along with details of the changes made in them and you can compare files to see the differences. If a configuration change results in an adverse effect on firewall operations then a previous version can be easily restored.

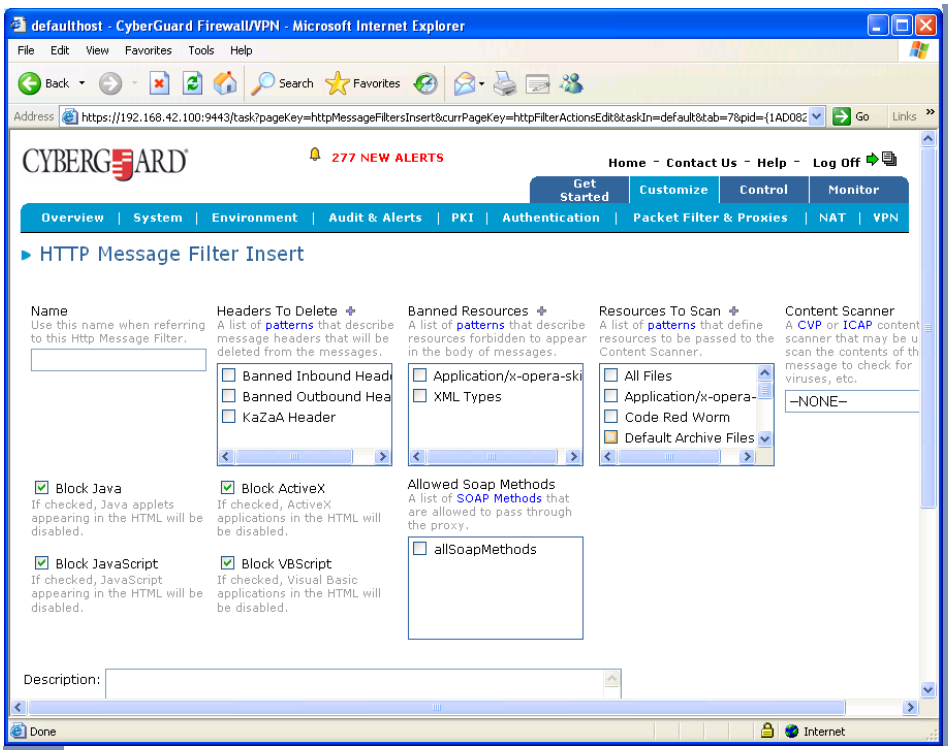
Along with change management the levels of access for different administrators can be easily controlled. Even here objects are used as you define each role with different permissions that determine which menu options can be accessed. When creating users you designate which role objects are to be assigned to them thus determining what menu options they are allowed to see and edit. Security clearances can be modified easily as any changes to a role object will be automatically propagated to all users that have it declared in their profile.

Application Inspection
CyberGuard's Application Proxies

Application layer inspection has traditionally placed a heavy burden on security appliances. Performance has always been a major concern resulting in many companies taking a two-fold approach by implementing separate appliances for packet and application inspection. However, this report shows clearly that CyberGuard's implementation delivers excellent performance for both technologies allowing the TSP 7100 to deliver a single solution that covers stateful packet inspection, packet filtering and application layer gateways.

The TSP 7100 delivers a wide range of application proxies covering services including FTP, HTTP, SMTP, Lotus Notes and LDAP along with H.323 for VoIP services and a Circuit option for non protocol-specific proxies. Each one is configured separately from the packet filtering and proxy menu tab where we found them to all provide an impressive range of functions. The HTTP proxy can operate in transparent or non-transparent modes and its application inspection capabilities allow extensive filtering to be applied to inbound and outbound traffic. Messages can be filtered for specific HTTP commands, banned URIs and resources that are not to appear in message bodies. Resources are defined as pattern objects which can be used in multiple filter actions and can be anything from a file type extension to a web page. Actions also extend to blocking ActiveX controls, Java applets, JavaScript and VBscript. A neat feature is that filter actions can include the option to pass a message to an external ICAP or CVP compliant content scanner for virus checks and so on.

The SMTP proxy offers extensive controls over how email is handled and can inspect mail headers, attachments and body content and, as with the HTTP proxy, pass messages to other scanners for functions such as virus checking. Strict verification controls can be applied to determine which users are allowed to receive and send mail from within your organization and the proxy can be configured to replace message headers with predefined ones allowing it to conceal information about internal mail servers. Message verification options extend to filtering messages for banned subjects and attachments and sending out mail notifications. Once again, CyberGuard's objects come into play as subjects and attachment types are defined as pattern objects. Overall, we found the various proxies simple enough to configure and use and as with general appliance configuration they are supported by detailed help files and documentation.



Monitoring and Reporting

This is one area that many security appliances fall down on but the TSP 7100 provides high levels of information from the Monitoring menu option. You can keep a close eye on system operations with views on an extensive range of functions including active connections, interface and protocol statistics, hard disk utilization and system performance. The hardware health option is particularly impressive as it provides a matrix of over sixty graphs detailing component and chassis temperatures, fan operations and voltages.

We found information about firewall activities to be just as detailed and opening with a complete summary of all firewall related alerts. With configuration tracking activated you can browse through all changes made to the appliance and view change history which can be fine tuned using time and date filters. A list of all packet filters is provided so you can see how many hits each one has received and packet filter sessions can be viewed using attributes such as the protocol, filter action or client address.

At this level of the security market reporting needs to be very good and the TSP 7100 doesn't disappoint as it maintains full audit logs on firewall and system activity. Reports can be generated and viewed directly from the administrative interface and fine tuned using extensive filtering actions and time periods. CyberGuard provides an audit dictionary which contains categories, saved audit filters and events allowing administrators to extract only the information they require. We would have liked to have seen an option to show report data in graphical format but you can choose to display the final report in the administrative interface, write it out in WELF format or export it into a spreadsheet in CSV format.

Conclusion

The results from our performance tests show that the TSP 7100 is more than capable of handling the demands of application inspection. It not only delivered the quoted speeds and connection rates but in most cases exceeded them and also impressed our testers with the stability it demonstrated whilst under extremely heavy loads.

Physically, the TSP 7100 is a very well built appliance which delivers a high performance specification. It ticks all the right boxes for fault tolerance and supports a number of high availability scenarios making it even more versatile.

In our review of the key features we found that CyberGuard has made every effort to ensure that installation is achieved with the minimum of fuss and the use of wizards makes this process even easier. The well designed web interface ensures general configuration parameters are very accessible and the supplied documentation is a cut above much of the competition. We were particularly impressed with the object oriented method of creating security policies as this ensures that any changes can be quickly propagated to all relevant polices so reducing the management burden. Add to this the extensive auditing and reporting facilities and it's clear the TSP 7100 is offering a complete enterprise and carrier grade level network security solution that has the ability to cope with current requirements but also has the expansion potential and the capabilities to grow easily with demand.