Secure Computing Total Stream Protection TSP 7300

A report on the Secure Computing carrier grade and high enterprise security appliance with a full performance test of the Application Inspection and UTM features

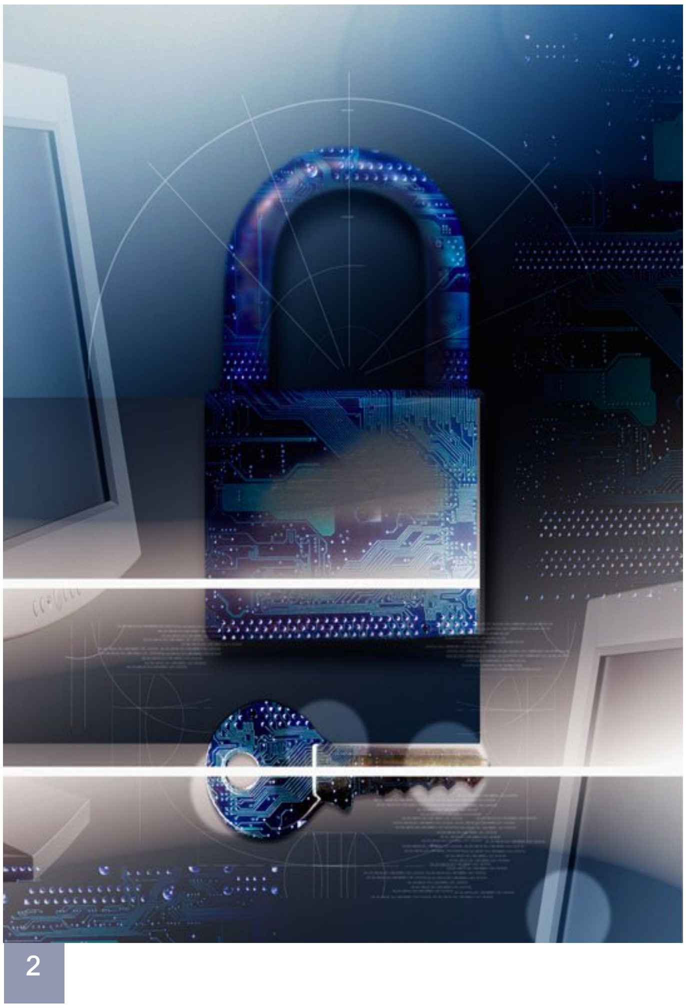
*Testing conducted and
report compiled by:*

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

info@binarytesting.com

Introduction

The dynamic shift over the past few years in the types and variety of threats posed to IT security at the corporate level is presenting CIOs, security officers and support staff with new and ever changing challenges. Attacks have evolved way beyond the relatively simple but undeniably potent DoS (denial of service) to those where the perpetrators are now driven purely by financial gain. The rewards can be considerable and the latest developments are that carefully crafted and highly sophisticated attacks are now being carried out by gangs of organized criminals. Add to this the raft of data security compliance acts such as Sarbanes-Oxley and HIPAA and it's clear that businesses today need to radically overhaul their procedures and systems to ensure corporate data is fully protected.



The diversity of threats means a blended approach to security at the network perimeter is needed. Basic SPI firewalling is insufficient as attacks now focus primarily at the application level. Furthermore, along with the spread of viruses, malware and spyware, the exponential increase in spam now presents a very real threat to productivity. One method is to implement multiple point solutions to protect against each type of threat but this is rapidly losing favour for a number of reasons. Not least are the administrative overheads in corporate environments as support staff attempt to manage, maintain and monitor separate appliances.

A new breed of appliance has risen in response to these challenges which centralizes all security functions into a single solution. Instead of distributing security services across multiple vendors these UTM (unified threat management) appliances encompass all services in one product. The benefits of a single vendor solution are immediate as companies now have a one-stop shop for all their security needs.

The varied interpretations of what a UTM solution should encompass means businesses need to be clear about their requirements. At its foundation the solution will naturally deliver standard SPI firewall functions which focus on the network level allowing them to detect and block attacks such as DoS. However, the simple protocol and service based rules used by SPI firewalls cannot deal with application layer attacks such as buffer overflows so there is a clear need to provide application inspection capabilities. These employ application proxies but their heavy processing demands means a solid hardware platform is required to avoid network performance issues. ASIC-based hardware is sufficient for the SMB but at the enterprise vendors are now embracing an open server architecture allowing them to deliver highly specified and powerful appliance solutions.

Anti-virus scanning is a critical component of a UTM solution and to be effective it needs to encompass all messaging and web traffic. The threats to security and productivity presented by spam requires a proven solution that has the capabilities to deal not only with general nuisance messages but increasingly sophisticated phishing attempts and yet avoid false positives. AUP (acceptable use policies) that restrict an employee's usage of company Internet resources are also a highly desirable feature as these can reduce costs and improve productivity as well.

The benefits of this approach are self evident but to be effective the individual components need to be truly integrated together where they can be easily managed and monitored from a single administrative console.

Unified security solutions can bring clear benefits to business and the ability to offer multiple security functions from a single product are making them a critical part of an enterprise data security policy.

Executive Summary

In order to adhere to data security compliance acts businesses now have a clear responsibility to ensure corporate data is protected. Network security is a key element of this policy but the rapid increase and diversity of attacks means that standard firewalls are not enough. Previously, companies were faced with installing separate, disparate systems to counter each threat but the latest trend is to amalgamate a full range of security services into a single solution. Coined UTM (unified threat management) appliances, these products offer many benefits to business which include centralised management, reduced support overheads and increased productivity.

The merger of Cyberguard Corporation with Secure Computing at the end of 2005 has resulted in a security appliance product line that covers the entire range of business requirements from the SMB right up to the enterprise. The TSP 7300 is the latest to join this extensive family and it focuses on providing a complete, unified security solution to the enterprise and carrier market in a single powerful platform. It achieves this by bringing together Secure Computing's well respected Total Stream Protection (TSP) technology with its Content Security Management (CSM) software solution.

TSP delivers a unique blend of security features including sophisticated application inspection capabilities and policy based security. A key feature of TSP is the use of a wide range of proxies that allows security policies to be enforced at the application level. The processing demands of application inspection can be extreme when dealing with very large volumes of traffic and to overcome these issues the TSP 7300 is delivered with a hardware specification that offers a high processor density. With CSM at the helm the appliance also offers the full gamut of anti-virus and anti-spam measures plus content filtering for both web and email.

This report will focus on the TSP 7300 in order to determine its capabilities and suitability for the enterprise and carrier grade network security market. A full review will be conducted which 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. The report recognises that component integration is a crucial requirement so it will discuss how well the TSP and CSM functions are amalgamated and managed. Full performance tests will be conducted to ascertain its ability to handle very high traffic loads and concurrent connections using the latest Avalanche and Reflector testing equipment from Spirent Communications.

PASSWORD USER LOGGIN I.D.
128 BIT ENCODED
IDENTIFCATION PROCESSOR BINARY CROSS PLATFORM
PASSWORD KEYWORD
IP ADDRESS MAC ADDRESS NIC ADDRESS
CODE
ENCRYPTION
FIREWALL

Testing Scenario

Objective

The test objective was to measure the performance of the Secure Computing TSP 7300 enterprise firewall appliance when subjected to very high traffic loads. Performance would be measured with the firewall configured to handle traffic in both packet filtering and web proxy modes. The web proxy was also configured to operate in two modes, both with and without the CSM features enabled. The same filtering rules were applied to all active interfaces. The TSP 7300 on test was equipped with four 6-port copper Gigabit Ethernet network interface cards, four dual-core AMD Opteron 865 1.8GHz processors, and 4 Gigabytes of main memory. Secure Computing engineers configured the appliance for optimum performance, with one Opteron processor core dedicated to managing each NIC. The operating system software was CgLinux 4.1, with Secure Computing's firewall software version 6.4. The system under test had the CSM software installed, using WebWasher CSM software version 5.3.0.

Equipment

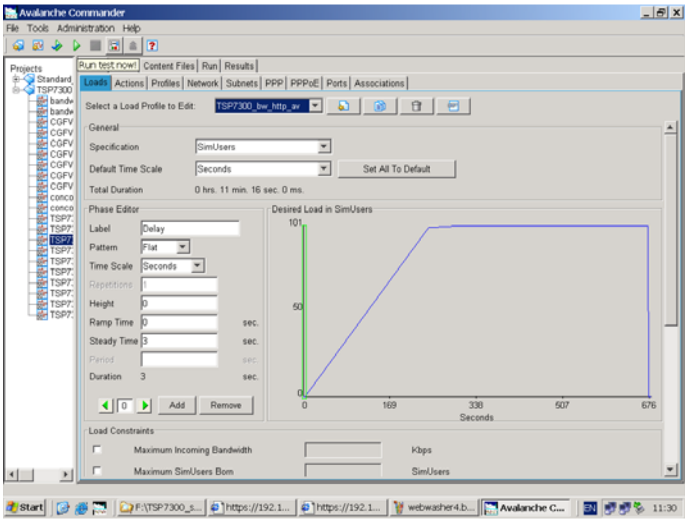
We used two pairs of Spirent Communications' Avalanche 2500 and Reflector 2500 systems, running version 6.51 of their Avalanche Commander software. The Avalanche equipment can simulate large numbers of network users, while the Reflector can simulate various types of server and can respond appropriately to the requests made by the Avalanche. The systems can emulate the actions of large numbers of users engaged in various activities, including web browsing, e -mail and file transfer sessions, with the Reflectors returning the appropriate responses for each type, generating realistic network traffic loads. 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 7300's Ethernet ports to eliminate any loss of performance that might be caused by passing the traffic through an intervening switch. Each Avalanche and Reflector 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.

Test Plan

The TSP 7300 was subjected to test loads under both HTTP Proxy and Packet Filtering rules, but with all CSM features disabled. A further set of tests was performed to determine throughput under the HTTP Proxy rules but this time with the CSM anti-virus scanning feature enabled. All three anti-virus scanning engines were in use during this particular test cycle.

The test plan ensured that the performance factors would be measured in a particular sequence, with each factor determining a parameter for a subsequent test. Although Packet Filtering is used for non protocol-specific traffic, all the tests would generate HTTP requests irrespective of the firewall rules in force at the time. This would ensure that the results would be directly comparable across all tests.

The first factor to be tested was the maximum connection rate the device could sustain. This factor was then used as a parameter in the next test to determine the maximum number of concurrent connections possible, and both of these factors were then used in the final test to determine the system's throughput. The first set of tests was conducted with the device operating under Packet Filtering rules, with all CSM features disabled. The next set of tests was run to determine performance using HTTP Proxy rules, again with all CSM features disabled. The HTTP Proxy rule was then configured to use the anti-virus scanning feature of the CSM software, and a further set of tests was run to determine the effect of this part of the CSM system on the device’s overall throughput.



Select a Load Profile to Edit: TSP7300_bw_http_av

General

Specification: SimUsers

Default Time Scale: Seconds

Total Duration: 0 hrs. 11 min. 16 sec. 0 ms.

Phase Editor

Label: Delay

Pattern: Flat

Time Scale: Seconds

Repetitions: 1

Height: 0

Ramp Time: 0 sec.

Steady Time: 3 sec.

Period: sec.

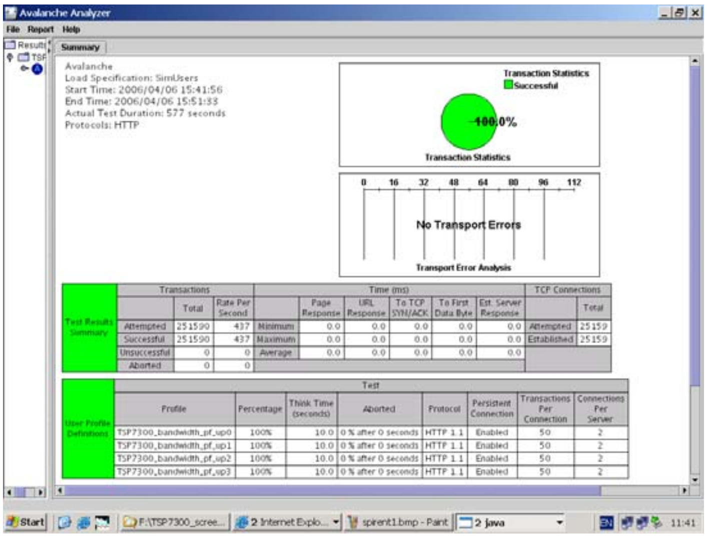
Duration: 3 sec.

0

Load Constraints

☐ Maximum Incoming Bandwidth Kbps

☐ Maximum SimUsers Born SimUsers



Avalanche
Load Specification: SimUsers
Start Time: 2006/04/06 15:41:56
End Time: 2006/04/06 15:51:33
Actual Test Duration: 577 seconds
Protocols: HTTP

Test Results Summary	Transactions			Time (ms)						TCP Connections	
		Total	Rate Per Second		Page Response	URL Response	To TCP SYN/ACK	To First Data Byte	Est. Server Response		Total
	Attempted	251590	437	Minimum	0.0	0.0	0.0	0.0	0.0	Attempted	25159
	Successful	251590	437	Maximum	0.0	0.0	0.0	0.0	0.0	Established	25159
	Unsuccessful	0	0	Average	0.0	0.0	0.0	0.0	0.0		
	Aborted	0	0								

User Profile Definitions	Test							
	Profile	Percentage	Think Time (seconds)	Aborted	Protocol	Persistent Connection	Transactions Per Connection	Connections Per Server
	TSP7300_bandwidth_pf_up0	100%	10.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2
	TSP7300_bandwidth_pf_up1	100%	10.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2
	TSP7300_bandwidth_pf_up2	100%	10.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2
	TSP7300_bandwidth_pf_up3	100%	10.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2

Test Methods

Each test type was run with different sets of parameters to determine which combination would produce the highest result without errors, such as aborted connections, occurring. The tests were set up to generate increasing loads applied in equal steps. Each step was defined in both quantity and time, and each step was followed by a further interval of time during which the system would attempt to maintain the load level. This helped to ensure that the TSP 7300 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 at a higher level. More steps were added until the test began to produce errors. This last test was discarded and the previous successful parameter set was used to produce the performance results. The TSP 7300 was rebooted before each test run to ensure that the test began with the system in the same state each time to avoid any variation in performance that might be caused by any residual resource allocation, such as memory, remaining from the previous test run.

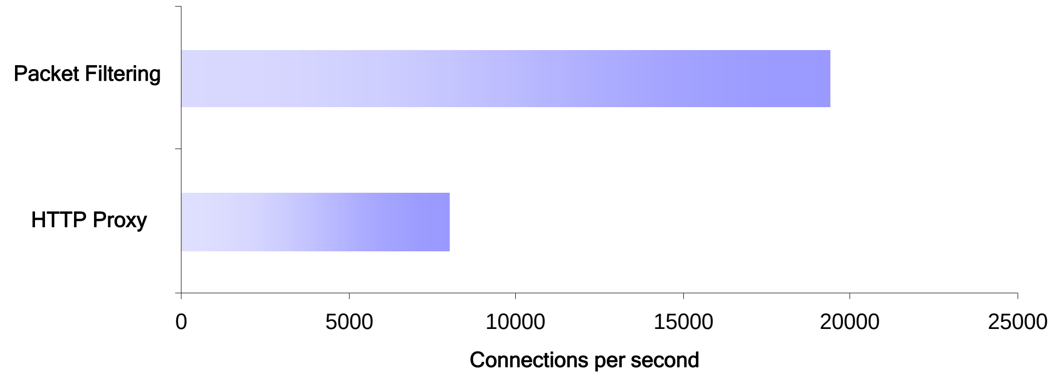
TESTED with SPIRENT

Test Results

Connection rate

The maximum connection rate with the system operating with Packet Filtering rules was found to be 19,398 connections per second. The maximum connection rate with HTTP Proxy rules was determined at 8,017 connections per second.

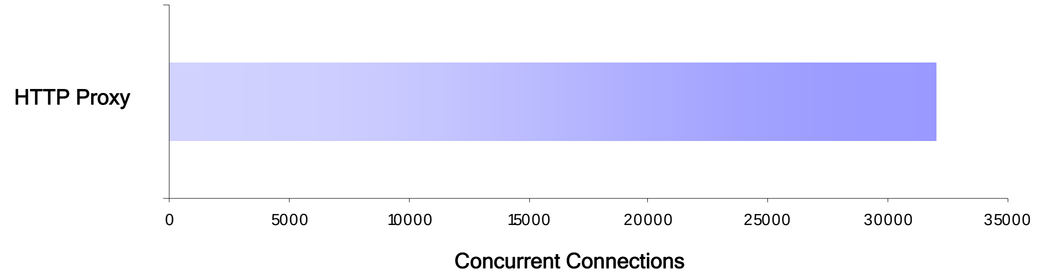
CONNECTION RATE

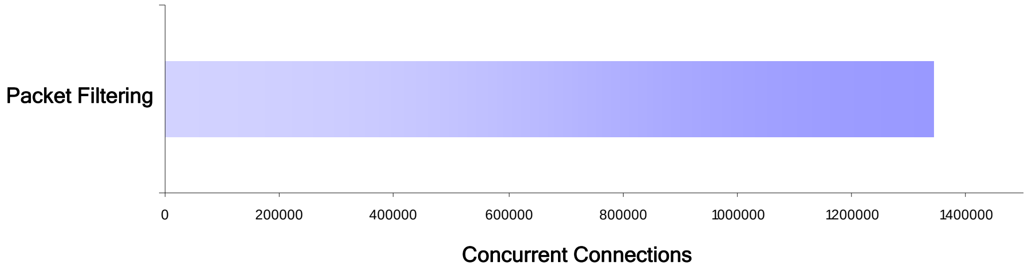


Concurrent Connections

The system was able to attain a peak load of 1,344,255 concurrent connections while operating with Packet Filtering rules. The system returned a peak load of 32,000 concurrent connections operating with HTTP Proxy rules in force.

CONCURRENT CONNECTIONS



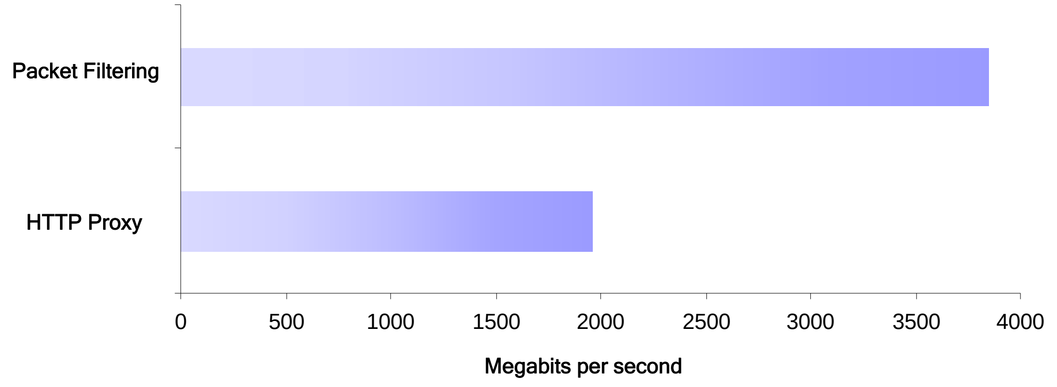


Test Results

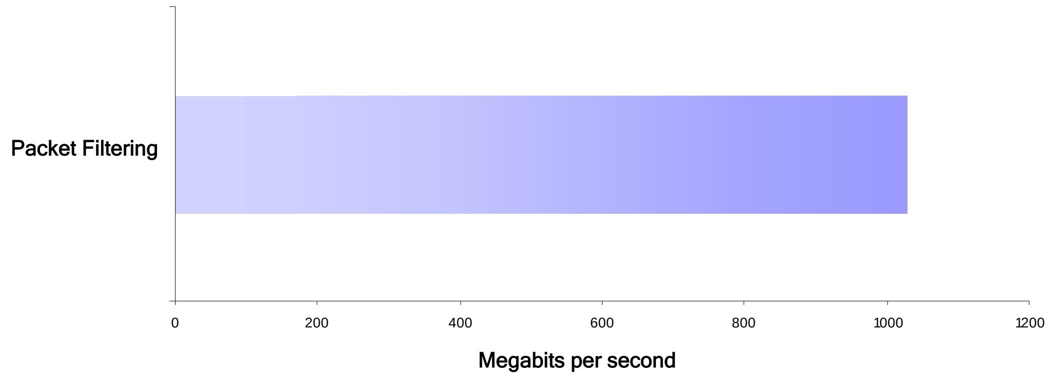
Bandwidth

The TSP 7300 could achieve a maximum throughput of 1,959 Megabits per second in the HTTP Proxy state, and this reduced to 1,030 Megabits per second when the anti-virus scanning engines were enabled. When operating with Packet Filtering rules, the device achieved a maximum throughput of 3,845 Megabits per second. This last figure is approaching the maximum that the interface cards could achieve, and indicates that it is possible that the device might be capable of reaching even higher throughput. 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.

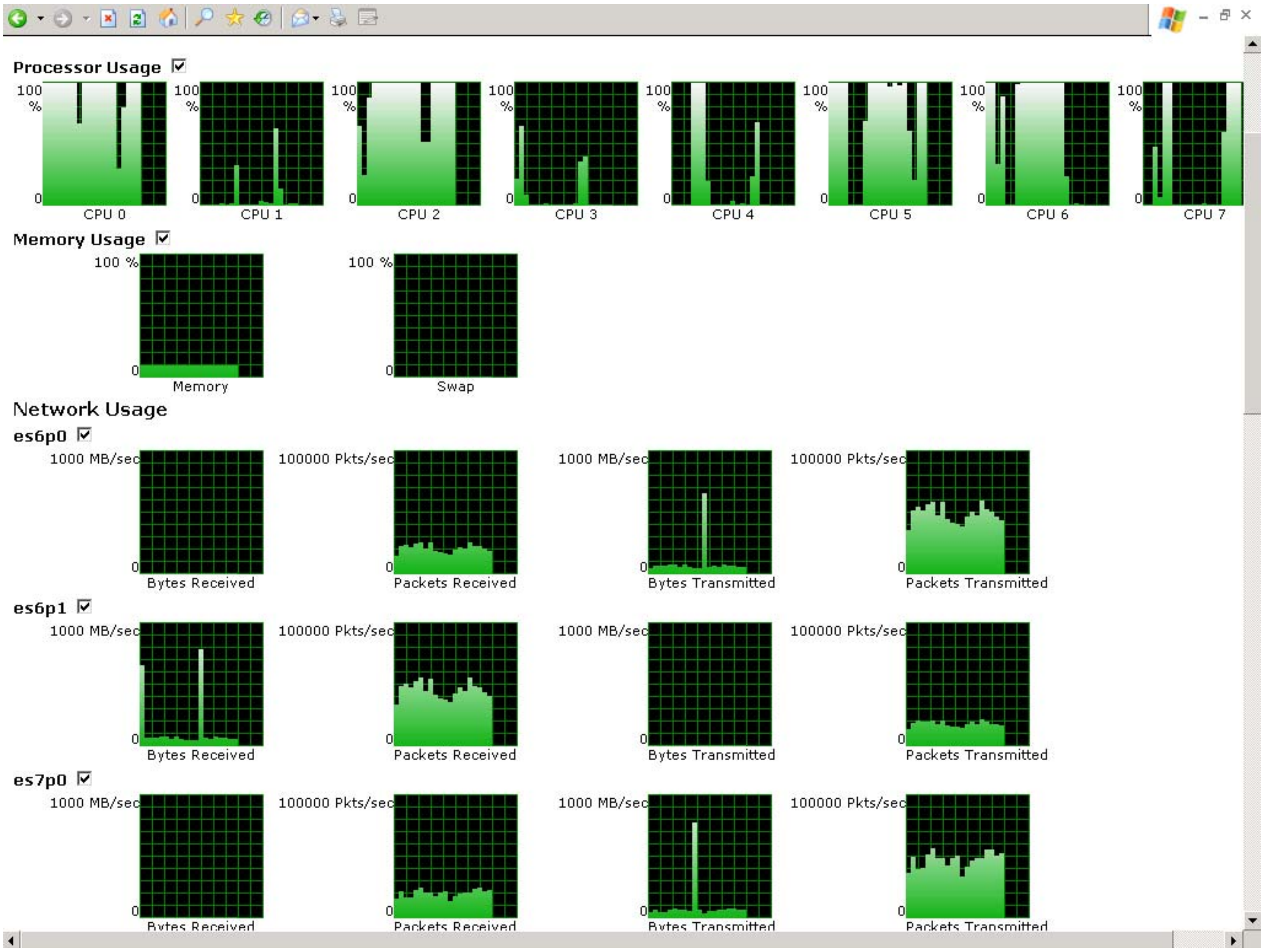
BANDWIDTH



BANDWIDTH WITH ANTI-VIRUS ENABLED



Test Results



The TSP 7300 system performance monitoring display showing the system during a test. Although traffic levels through the interfaces are high and the associated processor cores are working hard, the system still has plenty of spare

Testing Conclusion

The TSP 7300 performed very well under test and our results compare favourably with Secure Computing's TSP 7100 appliance, although the differences in configuration and software between the two models preclude any direct comparisons.

When we reported on the TSP 7100 we found performance across the board was particularly impressive and so it is with the TSP 7300. The key differences between the two test platforms is that although the TSP 7100 now has the capability of running the CSM components, at the time of review it was tested with only the TSP firewall and application inspection features running. In general, we found the superior hardware specification of the TSP 7300 delivered a considerably higher performance with it only falling back marginally when the three anti-virus scanning engines were engaged.

Hardware Specification

The decision to use an AMD Opteron based appliance is a smart move as this processor is a mature product with a proven track record. Furthermore, the dual-core Opteron 800 series processors were released nearly a year ago giving AMD a significant lead over Intel which only delivered its dual-core Xeon MP processors this year.

The TSP 7300 uses a Newisys 4300-E enterprise class server which we found provides excellent build quality along with all the fault tolerant features we would expect to see at this level of the security appliance market. Furthermore, at only 3U high it offers one of the lowest form factors for eight-way processing currently available. The system under test was supplied with a quartet of dual-core 1.8GHz AMD Opteron 865 processors along with 4GB of PC3200 ECC SDRAM memory made up of eight 512MB modules. The Newisys motherboard provides no less than sixteen DIMM sockets and with qualified 4GB modules can support up to 64MB of memory.

Storage options abound as the chassis has room for up to five hard disks mounted in easily accessible hot-swap carriers and the system under test came fitted with four 74GB Hitachi 10K Ultra320 SCSI drives. The motherboard does offer an embedded Ultra320 SCSI chipset which provides basic RAID-1 mirroring but Secure Computing opted to fit an LSI Logic MegaRAID Ultra320 RAID PCI-X card complete with 64MB of cache memory. Full storage fault tolerance is provided as the drives were pre-configured in a triple-disk RAID-5 array with hot-spare.

Plenty of component redundancy is provided as the chassis is supplied with a pair of 760W hot-swap power supplies. These are accessed easily from the rear and the entire power assembly is contained in a separate cage that mates with a single power socket on the motherboard and can also be removed if required for maintenance or complete replacement. With this much horsepower under the lid cooling needs to be good and the TSP 7300 doesn’t disappoint. It is equipped with twelve fans located in key positions and all are hot-swappable in the event of a failure.

High availability is on the menu as the TSP 7300 supports two modes of appliance clustering. In active/passive mode two appliances are used where one is designated as active whilst the second remains in standby. Should the primary unit suffer a complete failure then the secondary unit will take over all operations. Where traffic volumes are particularly high then multiple appliances can be used in active mode where sessions are assigned to specific systems. A new feature that makes the TSP 7300 well suited to high demand environments is the ability to cluster application proxies.

The appliance offers an extensive range of network connection options as the four 64-bit, 133MHz PCI-X expansion slots are each fitted with Silicom six-port Gigabit Ethernet adapters. These are designed specifically for mission-critical applications and high-performance servers where multiple network segments are required and each utilise Intel dual-controller chipsets. 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. A unique feature introduced in the Secure Computing TSP 7100 appliance and also offered with the TSP 7300 is that network adapter cards can be dedicated to individual processors if required. Furthermore, if any card fails it can be replaced without incurring any system downtime as the adapters and the four 133MHz expansion slots all support hot-plug capabilities. A new feature on the TSP 7300 is network link aggregation for high speed, redundant pipelines.

Installation

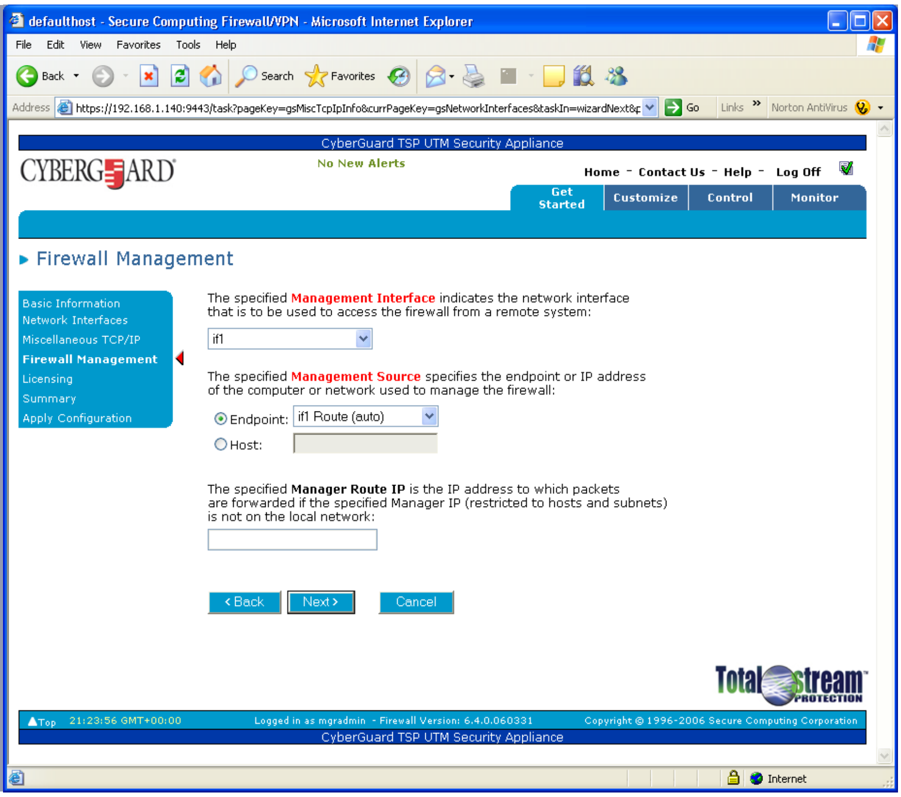
Initial installation of the TSP 7300 starts by attaching a local keyboard, mouse and monitor and accessing the well designed and remarkably intuitive GUI. We were impressed with the ease with which this could be conducted as a Getting Started Wizard guides you through defining the network interfaces, securing management access and getting the system started. A useful feature is that you can select the interface that your remote management station is to access and the Wizard will automatically set up a firewall access policy specifically for this function. Along with this you can add host and domain names and decide how the physical network interfaces are to be used.

Each interface can play a number of roles and you can designate them as internal, external, DMZ (demilitarized zone) or heartbeat for appliance clustering. DHCP server and client services can also be activated on internal or external interfaces. Should you choose to add more network interfaces you can rerun the Wizard to configure them ready for use.

Each feature on the appliance requires a license code to activate it and this can be run during the initial configuration phase. As this is the final step you are presented with a summary of the initial configuration for review after which you can apply all changes. A valuable feature – particularly for a system already running in a 'live' environment - is that all modifications are only applied to the system after they have been reviewed and then activated. 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.

The overall ease with which the TSP 7300 can be configured from start-up is impressive. We found the assistance provided by the Wizard combined with the detailed documentation and extensive on-line help avoids the complexity of installation and deployment inherent in many of these types of appliances. Our experiences with other Secure Computing TSP and CSM appliances reveals that ease of use is a key feature of all its security appliances making them stand out from many competing products.

General remote management is conducted over secure encrypted links where the browser interface is identical to the local GUI. The home page presents four tabbed folders for access to wizard based assistance, manually customizing the firewall, controlling the TSP and CSM functions and system and monitoring all activity. Management access needs to be strictly controlled and along with locking this down to one port you can also designate specific systems or hosts attached to the chosen network interface that are allowed to access the system.



Address: https://192.168.1.140:9443/task?pageKey=gsMiscTcpIpInfo&currPageKey=gsNetworkInterfaces&taskIn=wizardNext&p

▸ Firewall Management

The specified **Management Interface** indicates the network interface that is to be used to access the firewall from a remote system:

if1

The specified **Management Source** specifies the endpoint or IP address of the computer or network used to manage the firewall:

● Endpoint: if1 Route (auto)

○ Host:

The specified **Manager Route IP** is the IP address to which packets are forwarded if the specified Manager IP (restricted to hosts and subnets) is not on the local network:

21:23:56 GMT+00:00 Logged in as mgradmin - Firewall Version: 6.4.0.060331 Copyright © 1996-2006 Secure Computing Corporation

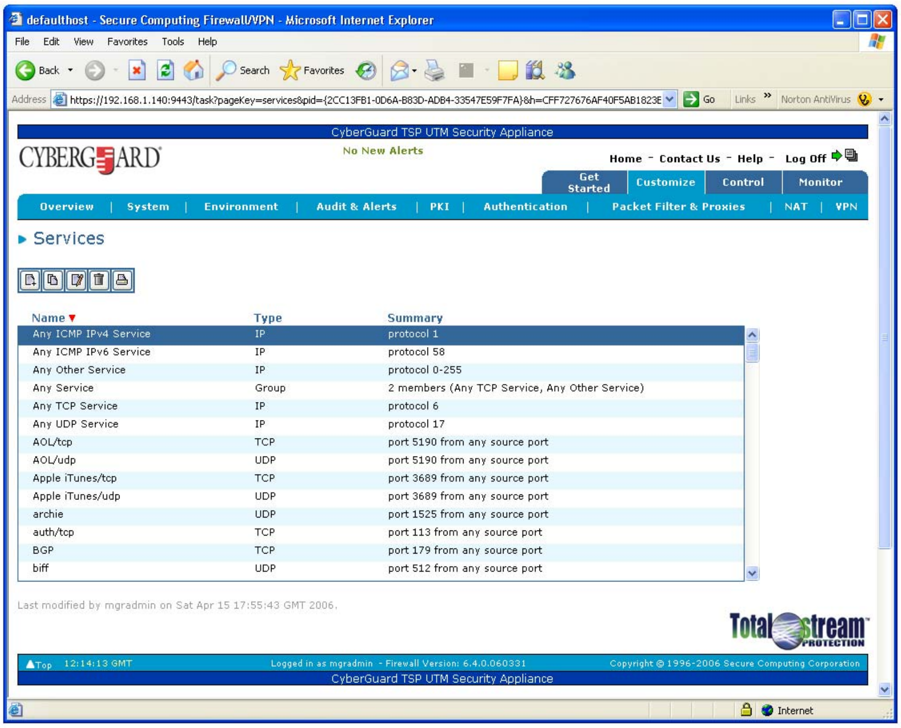
CyberGuard TSP UTM Security Appliance

An object lesson

All configuration functions are accessed directly from the Customize tab in the appliance's management home page. From here, you can view and modify system settings such as network interfaces, auditing and alerting, user authentication and, of course, packet filtering and application proxies.

After initial setup the TSP 7300 automatically blocks all general network traffic in both directions and requires packet filtering rules to be created to allow access to any service. Each rule comprises an action, service, source, destination and time period and a key feature of the Secure Computing method that makes configuration a cinch is that each of these elements only needs to be defined once as objects which can then be selected for use in multiple access rules. Furthermore, objects can be modified at any stage and these changes will be automatically propagated to all rules that are using them.

A wide range of actions are available and can be as simple as allowing, blocking or dropping packets or using one of the many proxies provided. Service categories include ICMP, IP, TCP and UDP plus groups comprising multiple categories. You can create your own custom services if you wish but we found the wealth of predefined services should cover most requirements. The same applies to sources, destinations and time periods and each one provides a list of predefined objects for immediate selection. If you need to create an object during rule creation just click on the small cross above each section and a new window opens up allowing a new one to be swiftly created. All rules are maintained in a list in order of processing priority and new access security features in the TSP 7300 allow administrators to block rules being promoted, demoted or deleted and you can also add comment lines to the packet filtering rule table.


defaulthost - Secure Computing Firewall/VPN - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://192.168.1.140:9443/task?pageKey=services&pid={2CC13FB1-0D6A-B83D-ADB4-33547E59F7FA}&h=CFF727676AF40F5AB1823E
Go
Links
Norton AntiVirus
CyberGuard TSP UTM Security Appliance
CYBERGUARD
No New Alerts
Home - Contact Us - Help - Log Off
Get Started
Customize
Control
Monitor
Overview | System | Environment | Audit & Alerts | PKI | Authentication | Packet Filter & Proxies | NAT | VPN
Services
TotalStream PROTECTION
Internet

Name ▼	Type	Summary
Any ICMP IPv4 Service	IP	protocol 1
Any ICMP IPv6 Service	IP	protocol 58
Any Other Service	IP	protocol 0-255
Any Service	Group	2 members (Any TCP Service, Any Other Service)
Any TCP Service	IP	protocol 6
Any UDP Service	IP	protocol 17
AOL/tcp	TCP	port 5190 from any source port
AOL/udp	UDP	port 5190 from any source port
Apple iTunes/tcp	TCP	port 3689 from any source port
Apple iTunes/udp	UDP	port 3689 from any source port
archie	UDP	port 1525 from any source port
auth/tcp	TCP	port 113 from any source port
BGP	TCP	port 179 from any source port
biff	UDP	port 512 from any source port

Last modified by mgradmin on Sat Apr 15 17:55:43 GMT 2006.

▲Top 12:14:13 GMT Logged in as mgradmin - Firewall Version: 6.4.0.060331 Copyright © 1996-2006 Secure Computing Corporation

CyberGuard TSP UTM Security Appliance

The Environment sub section in the management interface provides easy access to object creation. Sources and destinations are categorized as endpoints and can be anything from an IP address or address range, a fully qualified hostname, a subnet or a network interface. All rules can have a schedule applied that determines when they are active and these are defined simply as time period objects which encompass date ranges and specific times for each day. Time periods add considerable flexibility to the TSP 7300 as standard rules can be applied to normal working hours whilst other time periods can be used to activate access rules on particular minutes, hours, days, weeks or months. A good example of the power of objects is that that a time period only needs to be modified once and all rules that include this object will automatically use the new values.

Change management is now a standard practise within enterprises and in many cases is a legal requirement for data security compliance. All configurations are tracked and audited within the TSP 7300 and any changes requested can have compliance enforced by the use of descriptions and reasons for the modifications. Further tracking is provided by the use of tickets that clearly identify the administrator that made the changes.

Objects also come into play when defining the levels of access that are granted to different administrators. These define roles with different permissions allowing you to dictate what each user can do and what menu options they are allowed to see. 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.

The TSP 7300 also maintains all configuration files locally and provides facilities to compare different files where any differences are highlighted. If a configuration change results in an adverse effect on firewall operations then a previous version can be easily restored.

Application Proxies

The TSP 7300 delivers an impressive range of application proxies covering services including HTTP, FTP, SMTP, Lotus Notes and LDAP along with H.323 for VoIP services and a Circuit option for non protocol-specific proxies. These are all accessed and configured from the packet filtering and proxy menu tab where we found them to all provide a good range of functions.

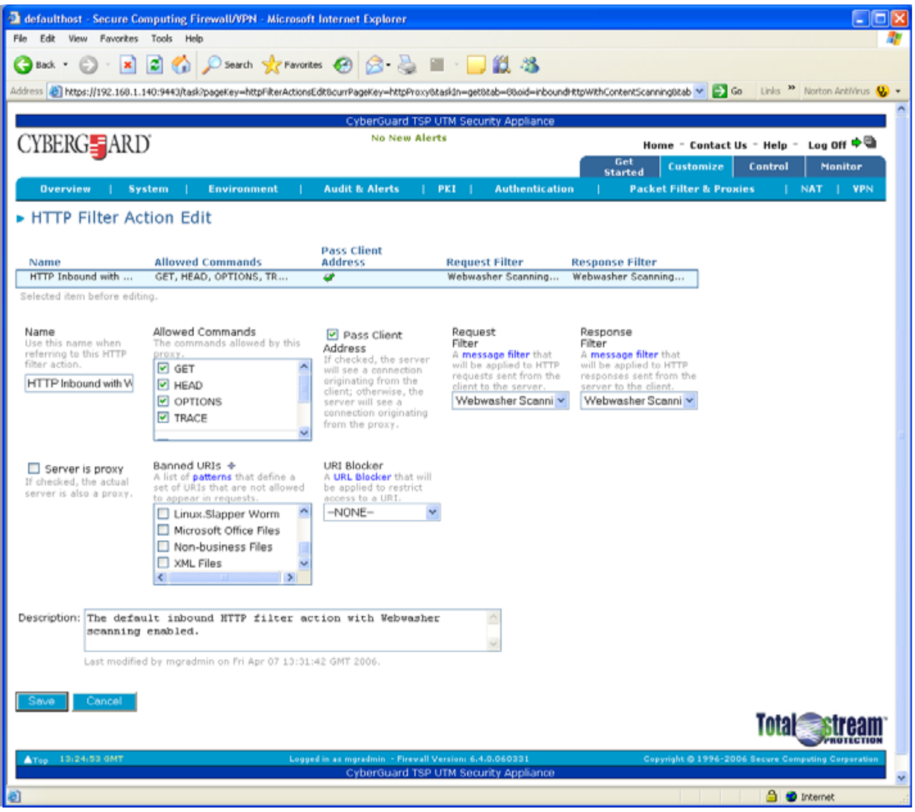
Messages can be filtered for specific HTTP commands, banned URIs and resources that are not to appear in message bodies. Once again, objects come into play as resources are defined once as patterns which can be used in multiple filter actions and can be anything from a file type extension to a web page. Operating in transparent or non-transparent modes, the HTTP proxy and its deep packet inspection allows extensive filtering to be applied to inbound and outbound traffic.

Actions extend to blocking ActiveX controls, Java applets, JavaScript and VBscript. CSM comes into the picture here as the TSP 7300 also allows filter actions to be created to allow, for example, the HTTP filter to apply CSM scanning on inbound and outbound traffic.

Extensive controls over how email is handled are provided by the SMTP proxy which can inspect mail headers, attachments and body content and, as with the HTTP proxy, pass messages to the CSM scanners for functions such as virus and spam checking. You can determine which users are allowed to receive and send mail from within the company and the proxy can be configured to replace message headers with predefined ones allowing it to conceal information about internal mail servers. Message filters extend to checking for banned subjects and attachments.

As usual, Secure Computing'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 are supported by detailed on-line help files and clear documentation.

It's a well known fact that application proxies requires a lot of processing horsepower with many companies separating out SPI firewall and proxy functions into independent solutions to reduce the load. However, our performance tests show the TSP 7300 has the power to handle all these functions allowing it to deliver a single, easily manageable solution


defaulthost - Secure Computing Firewall/VPN - Microsoft Internet Explorer
File Edit View Favorites Tools Help
CyberGuard TSP UTM Security Appliance
CYBERGUARD
No New Alerts
Home - Contact Us - Help - Log Off
Get Started | Customize | Control | Monitor
Overview | System | Environment | Audit & Alerts | PKI | Authentication | Packet Filter & Proxies | NAT | VPN

▸ HTTP Filter Action Edit

Name	Allowed Commands	Pass Client Address	Request Filter	Response Filter
HTTP Inbound with ...	GET, HEAD, OPTIONS, TR...	✓	Webwasher Scanning...	Webwasher Scanning...

Selected item before editing.

Name: HTTP Inbound with W

Allowed Commands: ☑ GET ☑ HEAD ☑ OPTIONS ☑ TRACE

☑ Pass Client Address

Request Filter: Webwasher Scanni

Response Filter: Webwasher Scanni

□ Server is proxy

Banned URIs: □ Linux.Slapper Worm □ Microsoft Office Files □ Non-business Files □ XML Files

URI Blocker: –NONE–

Description: The default inbound HTTP filter action with Webwasher scanning enabled.

Last modified by mgradmin on Fri Apr 07 13:31:42 GMT 2006.

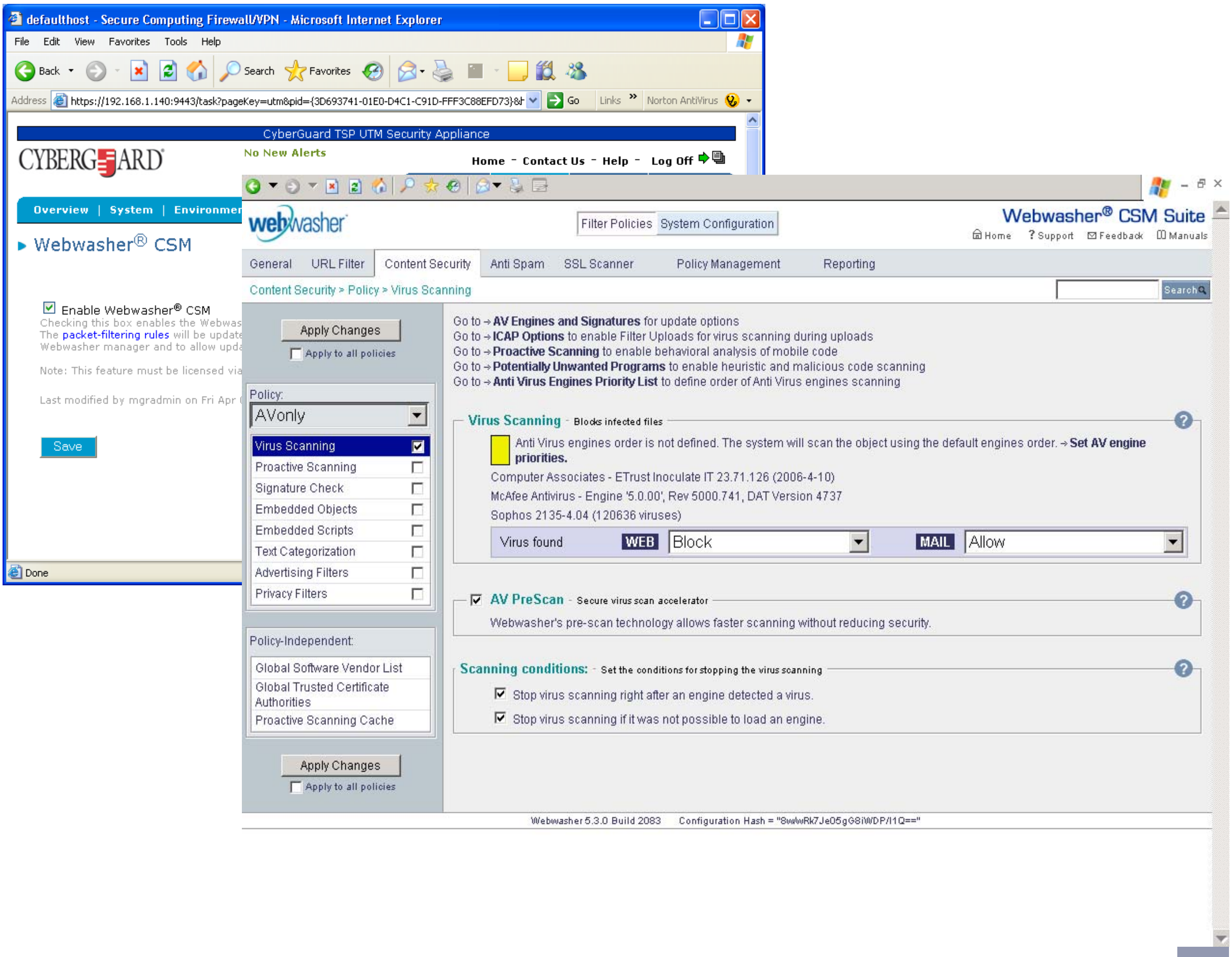
Save
Cancel
Top 13:24:53 GMT
Logged in as mgradmin - Firewall Version: 6.4.0.060331
Copyright © 1996-2006 Secure Computing Corporation
Internet

Content Security Management
The complete UTM picture

The inclusion of Secure Computing's Webwasher CSM technology allows the TSP 7300 to provide a complete UTM solution and during testing we found that it has been neatly integrated with the TSP components making for easy management.

A new option is provided under the System sub-menu where the CSM can be activated directly. One very smart feature is that once this has been achieved the appliance automatically creates and applies new filtering rules to open up management access to the CSM and pass anti-virus signature updates through the firewall. Furthermore, packet filtering and application proxies are updated to include objects for the CSM features where they can be immediately incorporated into new or existing rules.

The CSM components allow the TSP 7300 to function as HTTP and FTP proxies and a mail relay. Admittedly, management access does require a new browser session to be run but this is simply pointed at the appliance's secure management interface address and a different port number used.


defaulthost - Secure Computing Firewall/VPN - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.140:9443/task?pageKey=utm&pid={3D693741-01E0-D4C1-C91D-FFF3C88EFD73}&h
Go Links Norton AntiVirus
CyberGuard TSP UTM Security Appliance
CYBERGUARD
No New Alerts
Home - Contact Us - Help - Log Off
Overview | System | Environmen
Webwasher® CSM
Save
Done
webwasher
Filter Policies System Configuration
Webwasher® CSM Suite
Home ? Support Feedback Manuals
General URL Filter Content Security Anti Spam SSL Scanner Policy Management Reporting
Content Security > Policy > Virus Scanning
Search
Apply Changes
☐ Apply to all policies
Policy-Independent:
Global Software Vendor List
Global Trusted Certificate Authorities
Proactive Scanning Cache
Apply Changes
☐ Apply to all policies

☑ Enable Webwasher® CSM
Checking this box enables the Webwas
The packet-filtering rules will be update
Webwasher manager and to allow upda

Note: This feature must be licensed via

Last modified by mgradmin on Fri Apr

Policy: AVonly

- Virus Scanning ☑
- Proactive Scanning ☐
- Signature Check ☐
- Embedded Objects ☐
- Embedded Scripts ☐
- Text Categorization ☐
- Advertising Filters ☐
- Privacy Filters ☐

Go to → **AV Engines and Signatures** for update options
Go to → **ICAP Options** to enable Filter Uploads for virus scanning during uploads
Go to → **Proactive Scanning** to enable behavioral analysis of mobile code
Go to → **Potentially Unwanted Programs** to enable heuristic and malicious code scanning
Go to → **Anti Virus Engines Priority List** to define order of Anti Virus engines scanning

Virus Scanning - Blocks infected files

Anti Virus engines order is not defined. The system will scan the object using the default engines order. → **Set AV engine priorities.**

Computer Associates - ETrust Inoculate IT 23.71.126 (2006-4-10)
McAfee Antivirus - Engine '5.0.00', Rev 5000.741, DAT Version 4737
Sophos 2135-4.04 (120636 viruses)

Virus found WEB Block MAIL Allow

☑ **AV PreScan** - Secure virus scan accelerator

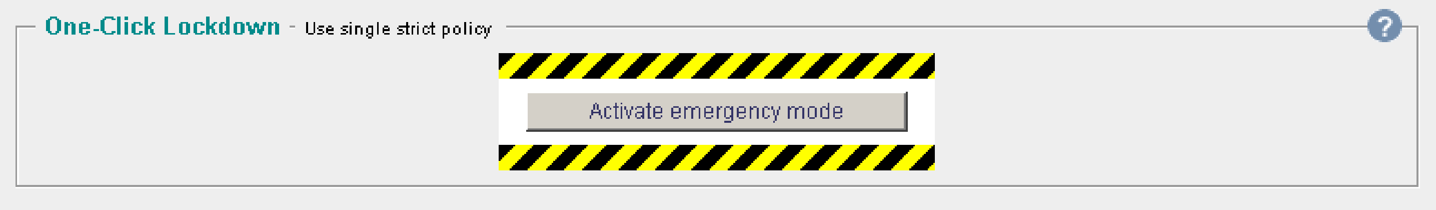
Webwasher's pre-scan technology allows faster scanning without reducing security.

Scanning conditions: - Set the conditions for stopping the virus scanning

☑ Stop virus scanning right after an engine detected a virus.
☑ Stop virus scanning if it was not possible to load an engine.

Webwasher 5.3.0 Build 2083 Configuration Hash = "8wwRk7Je05gG8iWDP/I1Q=="

Content Security Management
The complete UTM picture



We found the CSM web interface as well designed and as intuitive as the TSP version. A key concept of CSM is the use of corporate filtering policies which are applied at the gateway for selected email senders and recipients, IP addresses, users or groups. Effectively, corporate filtering policies contain multiple policies with each one describing a range of filtering actions for each CSM component. You can include content filters plus actions for the anti-spam and anti-virus modules and the policies can be applied to selected users. Usefully, when modifying a CSM component you can either declare the changes as global or only apply them to a specific policy.

You can swap between system configuration and setting up filtering policies using a couple of buttons at the top of the web interface. All HTTP, HTTPS and FTP proxy services are accessed from the system configuration page along with the mail gateway and delivery details plus ICAP server parameters. Anti-virus signatures and engines plus anti-spam and content filtering database updates are all carried out automatically. You can specify intervals for each individual component but they can also be run manually.

A common practise for virus scanning in enterprise networks is to use a multi-pronged attack with a combination of different scanning engines. The TSP 7300 certainly doesn't disappoint in this department as it employs solutions from Sophos, Computer Associates and McAfee and you can decide in which order they are applied for filtering. All three don't have to be used as you can select only those you want, license them from the web interface and then use content filtering policies to determine their behaviour.

With signature updates coming from three independent sources new viral outbreaks should be contained but the Lockdown feature could prove invaluable as all Internet access can be blocked with a single press of a button located on the CSM home page. This uses a predefined emergency policy which immediately overrides all currently active policies. Once the danger has passed the button is simply pressed once more which will restore all policies back to active duty.

Spam gets a tough time from CSM as its defences start with Mailshell's SpamCatcher and are stiffened up with a wide range of other measures including RBLs, header and message body rules, URL filters and Bayesian analysis. Secure Computing also includes the Habeas SWE DNS based service which provides safe-lists of audited and certified senders and aims to reduce false positives.

For URL filtering the appliance uses a database of undesirable web sites and all user requests are checked before being allowed through. The list is extensive as it currently contains over sixty pre-defined categories which can be customised with your own black lists. These can include URLs, file types such as media and keywords within a URL whilst specific web page content can be blocked using the Generic Body Filter feature. With time schedules in the mix you can easily create AUPs (acceptable use policies) which are active at different times of the day or working week. Time and volume quotas can make your AUPs even more powerful as these can be applied to user types allowing you to restrict their browsing time on a daily, weekly and monthly basis and also limit their download quota to so many MB over the same periods. Individual user sessions can even be limited to a specific number of minutes. A highly important feature that puts the TSP 7300 ahead of much of the competition is that is can scan encrypted SSL content and the scanner can perform certificate validation so removing the decision process from the employee.

Monitoring and Reporting

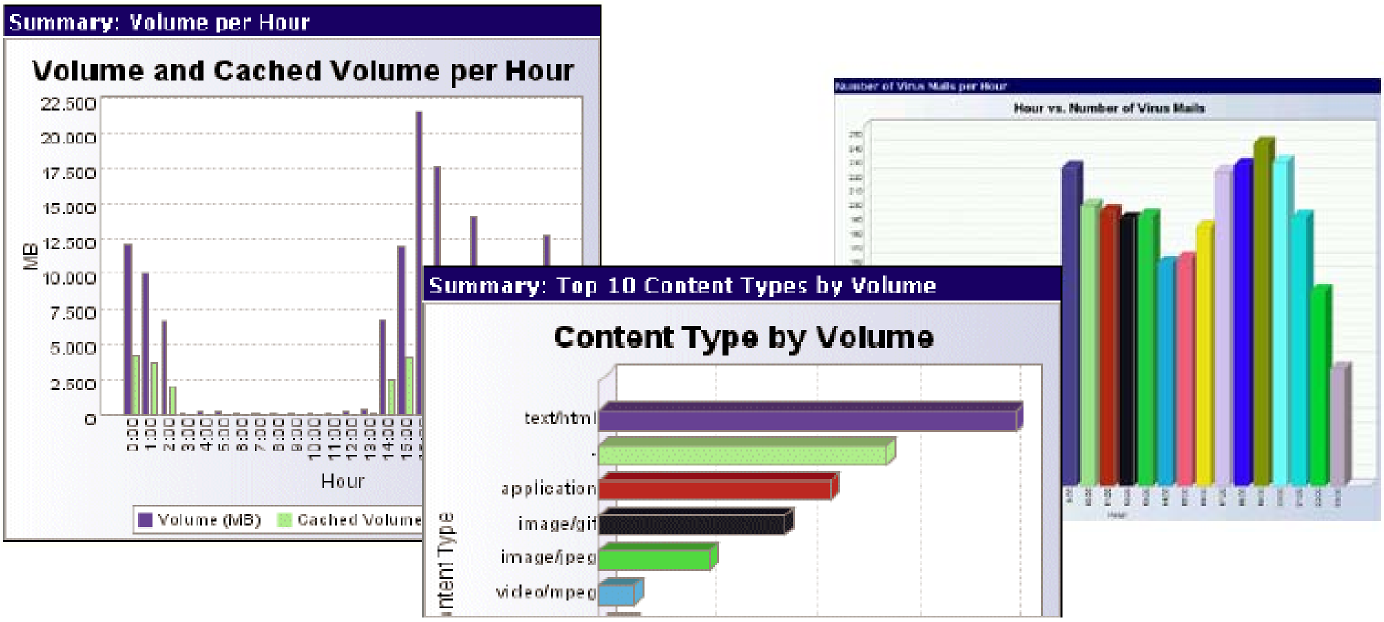
With so many data security compliance acts in force reporting now takes on a far more critical role and we found the TSP 7300 provides an impressive range of facilities for gathering information about performance, security status, user activity and change management.

You can keep a close eye on the system and components as the TSP interface provides plenty of information in tabular format about general operations with views on an extensive range of functions including active connections, interface and protocol statistics, hard disk utilization and system performance. We found the system performance option extremely useful as it provides a single screen showing real-time graphs on areas such as individual CPU utilisation, memory and swap file status, internal temperatures, fan operations and a complete rundown on all network interface traffic.

Everything you need to know about firewall activity is provided from the Monitor tab and any new alerts are highlighted with a quick access option at the top of the screen which provides a full summary. 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. The configuration tracking feature also allows administrators to view a complete change history and fine tune it with data and time filters.

The TSP 7300 provides full audit logs on firewall and system activity. These are used to generate reports that can be viewed directly from the management interface and extensive filtering actions and time periods can be used to weed out extraneous data. Secure Computing also provides an audit dictionary which contains categories, saved audit filters and events allowing administrators to facilitate precise data extractions. Audit logs will naturally grow substantially over time and archiving facilities are provided to allow these to be copied off the appliance to avoid wasting internal storage space. The appliance will automatically create packet filtering to allow archives to be copied to a remote location and even better is the fact that all audit logs can be security encrypted when they are archived.

Secure Computing also offers its Webwasher Content Reporting tool which provides a wealth of information about all the various components. It does require some extra manpower to set up as it comprises a separate server which is accessed remotely via a browser and requires a log source which, in this, case would be the TSP 7300. However, it's worth the extra work as it is capable of providing highly detailed reports on all activities. Trends in network and user activity can be identified easily and Internet resource usage and email tracked closely. The Content Reporter is quite sophisticated as it can access logs from both the TSP and CSM components. It can also display results in tabular and graphical format, export them into HTTP, PDF and text formats and also distribute them directly via email or to an FTP site.



Conclusion

As networks are faced with an ever increasing number and variety of security threats the means to combat them must grow in sophistication. Whilst SPI firewalls provide basic levels of protection the exponential growth in viruses, worms and spam has driven a fragmented approach where many companies have resorted to installing multiple point solutions that deal with each specific threat. There are further problems as unmonitored Internet access in the workplace is costing businesses far too much to be ignored. Without an AUP (acceptable use policy) in place Internet misuse can have a serious impact on employee productivity, storage and network bandwidth. This means businesses also must look at mail and web content filtering solutions to allow them to monitor user activity and enforce strict policies.

The multi-vendor approach is rapidly losing favour as the cost of implementing the various solutions is prohibitive whilst the manpower overheads incurred in managing and maintaining multiple systems is unacceptable. It may be a relatively new phenomenon but the UTM solution is an inevitable evolution of the firewall in response to these demands. However, to be effective it must master all elements of security and show no signs of weakness in any specific areas.

By neatly amalgamating Secure Computing's TSP and CSM technologies the TSP 7300 aims to deliver a complete UTM solution in a single hardware platform. TSP delivers standard SPI firewall functions and powerful application inspection capabilities which are far more sophisticated that the common signature based deep packet inspection (DPI) technologies used by much of the competition. CSM brings in a complete arsenal of virus scanning, anti-spam and web and message content filtering and even scanning of SSL encrypted content - a feature that few competing appliances offer.

Clearly, to be able to handle the demands of these myriad features without impacting on network performance and productivity the appliance itself needs to be something special and we found the platform selected delivers an excellent specification that centres round AMD's proven dual-core Opteron processor technology. The TSP 7300 is well built and provides all the fault tolerance you'd expect to see in an enterprise solution but backs this up with support for high availability clustering as well.

A critical requirement of a UTM solution is not just the number of features on offer but how well they have been integrated together. In our review we found the TSP and CSM functions worked hand in hand so facilitating easy management. Initial installation is handled extremely well with the use of wizards and automatic rule creation. 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.

The results from our performance tests show clearly that the TSP 7300 is capable of dealing with the heavy processing demands of deep packet inspection. It coped well with the heavy traffic loads applied using the Avalanches and Reflectors and even with the extra burden of the CSM services running in the background delivered significant performance improvements over the TSP 7100.

Along with top performance and manageability the TSP 7300 has plenty of room to expand memory and network connections allowing it to grow with demand and making it an excellent solution for enterprises that want all their security managed by a single UTM solution.

Binary Testing Limited believes the information in this publication to be accurate as of its publication date and retains the right to make changes to this publication at any time without notification.
Binary Testing Limited makes no warranty with respect to the information that appears in this publication, assumes no responsibility for any errors that may appear and does not make a commitment to update the information contained therein.