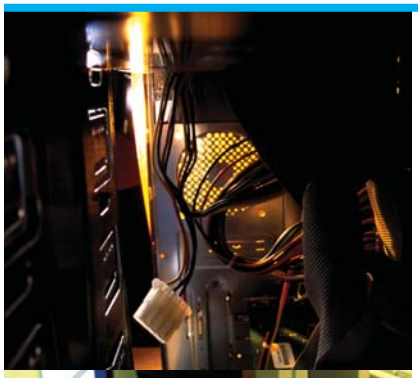
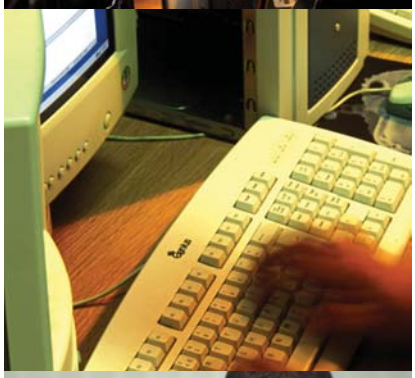
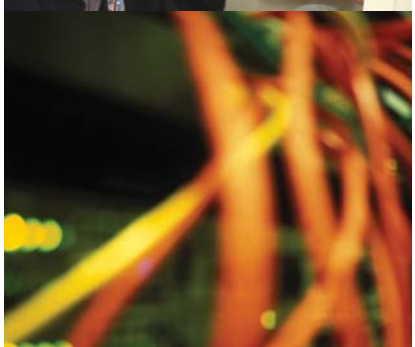
UNIFIED THREAT MANAGEMENT
TECHNOLOGY REPORT

JUNIPER NETWORKS SECURE SERVICES GATEWAY FAMILY







VOLUME 2, ISSUE 1
SEPTEMBER 2006

WEST COAST LABS
www.westcoastlabs.org

CONTENTS

JUNIPER NETWORKS SECURE SERVICES GATEWAY FAMILY

www.juniper.net/ssg

Juniper Networks, 1194 North Mathilda Avenue,
Sunnyvale, California 94089-1206 USA
Tel: +1 408-745-2000, Fax: +1 408-745-2100

West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

EXECUTIVE SUMMARY

SECURE SERVICES GATEWAY FAMILY

SSG 5, SSG 20, SSG 140 (AVAILABLE Q4 2006), SSG 520, SSG 550, SSG 5 WIRELESS AND SSG 20 WIRELESS

From the top down: SSG 5, SSG 20, SSG140, SSG 520 and SSG 550 (The SSG 5 and SSG 20 are also available wireless) The SSG 140 is scheduled for release in Q4 2006.

The Secure Services Gateway (SSG) Family is a new generation of network security appliances from Juniper Networks. The SSG family is designed from the ground up to run a rich set of UTM security features to protect branch offices from all manner of attacks. The product tested in this technology report is the SSG 520 which like the other members in this product range, has advanced security technologies and extensive network protection functionality within a single, easily deployed unit.

This particular device has 13 network interfaces, catering to an extensive range of configurations that meet complex business requirements and scenarios.

At the outset of testing and following a factory reset, the initial configuration of the device – using a console connection to assign an IP address to the internal interface – was a simple process, completed in just a few minutes. From that point onward, all SSG 520 configuration actions were performed using the inbuilt, intuitive web interface, easily accessible from a standard web browser.

The interface is well-designed and made up of two separate panes – the left pane contained all menu options, with the ability to drill down to sub-menu options where applicable, while the right pane displayed the contents of each selected menu option. This design ensured that all menu items were quickly accessible with just a few clicks of the mouse.

Basic, essential configuration tasks were carried out with minimum effort; changing the administrator name and password along with restricting administrator access to the management console by specifying permitted IP addresses, proved a particularly fast and logical process.

It was also possible to change the standard interface ports (HTTP /80, HTTPS / 443, SSH /22, and Telnet /23) to different,

EXECUTIVE SUMMARY CONTINUED

custom port numbers between 1024 and 32767. This shows the inherent flexibility of the unit, while potentially providing an added layer of security. It is also possible to enable the automatic redirection of management interface traffic from HTTP to HTTPS, for improved security and reassurance.

The device was easily updated – via a simple built-in facility – with flexible options to schedule an update at any required time and on any appropriate day. This ensures that the administrator can be confident that the latest firmware and attack signatures are installed.

The unit was deployed with a trusted interface connected to the internal network, an untrusted interface connected to the external network, a DMZ configured interface connected to the DMZ network and a VPN gateway linking the internal and remote networks. Setting up the required network interfaces and the VPN were fast and simple processes aided by the comprehensive online help system and the included documentation. The inbuilt policy and VPN wizards further reduced complexity making the overall set-up a breeze.

Fine-grained control over zones, policies, objects, users, groups, protocols, services, source and destination IP addresses, combine with the advanced screening, profile and filtering options to help ensure the security of both the device and the trusted network it protects.

It was a minor task to setup and activate a profile that screened and filtered out malicious web and email traffic using the internal anti-virus / anti-spyware engine. This testing proved that the unit successfully detected and blocked all samples within the West Coast Labs test suites, comprising an extensive range of malware. The appliance also has the ability to scan HTTP webmail based on URL patterns and parameters – common predefined patterns included America Online (AOL), Yahoo! and Hotmail services.

The set-up of the anti-spam profile proved equally easy – and was activated via a simple checkbox in the relevant policy. It proved to be an effective solution in dealing with the increasing spam problem that currently has such a wide-ranging impact on business productivity and resources.

Tests proved that increasingly essential business tasks, such as web browsing from the trusted network, were available out-of-the-box, providing added ease of use and further reducing administrator intervention. Importantly, these were carefully controlled and balanced with security considerations. It was also quick and simple to disallow or restrict web browsing using the management interface, if appropriate to business requirements.

Testing the device – from firewall, VPN and IPS perspectives – using a variety of real-world port probes and attacks between all internal, external, DMZ and remote networks, revealed only the specific ports open that were expected, and all other attempts to reach any disallowed services failed, as expected.

EXECUTIVE SUMMARY CONTINUED

All methods of allowed administrative activity required a log-in ID and password, further strengthening security. During manual and automated penetration testing and directed DdoS attacks, the SSG 520 continued to allow legitimate traffic flow, while preventing every attempted incursion.

The unit proved its mettle across a broad range of demanding tests, preventing concentrated, targeted attacks designed to compromise the box itself and the protected networks shielded by the device.

Web content filtering was set up by simply selecting the appropriate filtering technology from the management interface. In this instance, the integrated SurfControl protocol was used. For added flexibility, there is another option available to redirect traffic to an external host running either the SurfControl or Websense filtering engines.

Using the built-in engine, content is checked against a predefined category list of banned material, categories included common illegal and offensive subject matter, such as adult / sexually explicit, drugs, alcohol and tobacco, hate speech, violence, weapons, criminal skills and gambling.

In addition to the predefined lists, custom entries could be made in the form of URLs and assigned to a specific category, thus preventing access to any website not already in the database that is deemed unsuitable. The content filtering technology proved extremely effective, successfully blocking all inappropriate web traffic.

WEST COAST LABS VERDICT

An extremely robust, easy to administer device, with advanced protection and security functionality, the SSG 520 proved truly flexible, operating in both simple and complex business scenarios, while successfully detecting and preventing an extensive range of real-world attacks.

TEST OBJECTIVES AND METHODOLOGY

In this Unified Threat Management Technology Report, West Coast Labs is providing a thorough examination of all the main technology components in a UTM appliance through a real world test environment to establish the level of functionality and performance of the solution under test.

West Coast Labs' objective is to provide independently validated, meaningful technical information to a global buying market on which security management and buying decisions can be made.

For the purposes of this Technology Report, West Coast Labs tests the following technologies in the context of a single UTM appliance:

- Firewall and VPN
- Anti-virus
- Anti-spyware
- Anti-spam
- Web Filtering
- IPS

West Coast Labs engineers test the product in a controlled environment. Throughout the test period, the product has internet access and is be configured as recommended to update online. The testing environment mirrors that of a small to medium sized business and the internal interface of the firewall is connected to a 100Mbs network, and traffic loads set accordingly.

Technologies are tested in accordance with the functionality and performance criteria set out in Appendix 2 which form the Checkmark certification programs for Firewall Level 1 and Anti-virus Level 1, VPN, IPS, Web Filtering, Anti-spam and Anti-spyware.

All test methodology are shown in Appendix 2 on page 22.

THE PRODUCT

The Secure Services Gateway Family from Juniper Networks comprises a range of appliances developed for a variety of different business environments. The appliances are the SSG 5, SSG 5 Wireless, SSG 20, SSG 20 Wireless, SSG 140 (available during Q4 2006), SSG 520 and SSG 550.

Juniper Networks describe the products as having been specifically developed for users who want a high performance security platform with proven routing and UTM security features to protect LAN and WAN connections. The target deployment: for the appliances are branch offices and stand-alone small-medium businesses.

JUNIPER NETWORKS DEFINE THE BUSINESS BENEFITS OF THE SSG FAMILY AS:

- Cost effective: Integrates Stateful firewall, IPSec VPN, best-in-class UTM security features, LAN/WAN connectivity and routing into a powerful, all-in-one branch office security appliance. Can be deployed as a stand-alone security appliance or as a consolidated firewall and routing device to reduce IT CAPEX and OPEX
- Easy to manage: Powerful centralized management features reduce the administrative burden and associated costs required to get new devices up and running in branch office locations that lack onsite IT staff.
- Flexible: Broad range of platform options with interface flexibility to address nearly every network deployment scenario without a truck-roll hardware upgrade.

  www.juniper.net/ssg

JUNIPER NETWORKS DEFINE THE PRODUCT TECHNICAL BENEFITS OF THE SSG FAMILY AS:

- Purpose-built security appliances deliver performance required to protect high speed LAN as well as lower speed WAN connections.
- I/O Extensibility delivers LAN connectivity plus WAN I/O options and supporting encapsulations such as PPP, MLPPP, HDLC, FR, MLFR
- Unified Threat Management (UTM) security features including Stateful firewall, IPSec VPN, IPS, Antivirus (Anti-Spyware, Anti-Phishing, Anti-Adware), Anti-Spam, and Web Filtering
- Network segmentation to deploy security policies that isolates guests, wireless networks and regional servers to prevent/contain any attacks that may occur.
- High availability for device redundancy while link layer resiliency is delivered via automatic failover to secondary VPN tunnels.

  www.juniper.net/ssg

TEST REPORT

ANTI-VIRUS

The SSG 520 includes a quality gateway anti-virus (AV) engine, provided by a leading AV vendor. This engine is capable of protecting web traffic, email and web mail from file-based viruses, worms, backdoors, Trojans, and additional malware.

Policy-based management controls are easily implemented to scan inbound and outbound traffic to ensure that the network was safe from a wide range of attack vectors, including those originating from both the external and internal networks. Whilst some integral anti-virus applications primarily rely on a packet or network signature-based approach, the Juniper AV engine actively scans and screens the actual payload – regardless of file type – to detect any potential viruses.

During the testing, it proved to be a simple task to set-up and activate a profile that screened and filtered out malicious web and email traffic. The unit successfully detected and blocked all samples within the appropriate West Coast Labs test suites which comprises of an extensive range of AV malware.

The test samples used included a combination of “in the wild” viruses, worms and additional malware types commonly found in real-world circulation. Considering the overall performance of the device in the area of AV protection and the successful outcome of all AV testing carried out by the West Coast Labs malware team, the SSG 520 was duly certified to the Anti-Virus Checkmark standard, based on a 100% detection rate of the malware in the test suite.

ANTI-SPYWARE

In a similar vein to the integrated anti-virus protection, the SSG 520 uses an inbuilt anti-spyware engine. This actively and successfully detected all the real-world spyware samples within West Coast Labs' test suite, preventing any of the samples from reaching the internal network.

The appliance also has the ability to scan HTTP webmail based on URL patterns and parameters. Common predefined patterns included America Online (AOL), Yahoo! and Hotmail services.

West Coast Labs used an extensive range of spyware samples to test the capabilities of the device in this area, including a combination of “in the wild” backdoors, keyloggers, financials, proxies, password stealers and crackers, downloaders and hijackers.

This round of testing proved that the unit was successful in protecting the internal network from this potentially harmful form of malware. Given that this type of malware can have the ability to surreptitiously use the Internet connection of an infected computer possibly for illegal purposes, as well as monitor user activity and potentially steal personal – including financial – information from compromised hosts, this is an important result.

The device was subsequently awarded the Anti-Spyware Gateway Checkmark as it obtained the required standard of 100% detection in line with the published Checkmark standard.

TEST REPORT CONTINUED...

FIREWALL

The Juniper Networks SSG 520 includes a dynamic packet filtering, Stateful firewall with Deep Inspection capabilities. By default, the firewall settings are configured to allow certain outbound services through the device including HTTP, HTTPS and DNS. This ensures that increasingly essential business tasks, such as web browsing from the trusted network, are available out-of-the-box providing added ease of use and further reducing administrator intervention.

Importantly, all permitted services are carefully controlled and balanced with the security considerations and common business needs of most organizations. It is also quick and simple to disallow or restrict these default services using the intuitive, well constructed web interface that is used for most of the post-install system management tasks.

The unit also allows certain services to connect to the device itself from within the internal network primarily for configuration purposes. These of course, include access to the management interface via the HTTP and HTTPS protocols. By default, all inbound services are disallowed from the external network to both the internal network and the appliance itself, immediately providing increased protection and peace of mind not only for management, but also for security and administration staff.

Using this easily-configured and centralized policy-based management process approach, organizations can define multiple security policies to control traffic flow between connected networks. This is achieved by specifying the types of traffic allowed to pass from nominated sources to nominated destinations – an ability that proved both powerful and flexible during the test process.

The SSG 520 successfully passed all firewall-based tests carried out by the West Coast Labs engineering team including probes, scans, malformed packet attacks, Denial of Service attempts and attempts to circumvent the security of the unit between internal, external and DMZ networks – in line with the published test methodology. West Coast Labs is please to announce that the SSG 520 has been awarded the Firewall Level 1 Checkmark certification.

VPN

The device has an integrated and effective VPN capability. Use of the inbuilt policy and VPN wizards that are easily accessible from the single, unified web GUI significantly reduced the complexity of the VPN implementation, ensuring that the overall set-up was a breeze. A route-based VPN was implemented using the VPN wizard tool, as this option was deemed most appropriate to set-up a site-to-site VPN link between the SSG 520 and a secondary Juniper device located on the remote network.

The implemented VPN connection utilized IPsec and a static IP addressing scheme at both ends of the link, effectively allowing a permanent gateway between the internal and remote networks. Multiple policies were then defined and applied to the VPN tunnel, allowing secured access to a number of resources both to and from the networks.

TEST REPORT CONTINUED...

These resources included common web, file transfer and remote administration services. The SSG 520 passed all VPN-based tests, including various penetration tests, basic encryption verification, checks on the security of the management console, sensor probes assessing tunnel traffic security, and validation that different types of traffic could be allowed and / or denied transport via designated VPN tunnels.

These tests ensured that the SSG 520 performed appropriately, in line with the pre-defined usage policy and the published VPN test methodology. As a result of passing these rigorous real-world tests defined by the West Coast Labs team, the SSG 520 was certified to the VPN Checkmark standard.

IPS

The Juniper device has extensive, built-in IPS functionality that detected and prevented a wide range of real-world attacks at the network perimeter. The technology screens traffic at a deep level, making complex access control decisions based on the content and intent of that traffic. Operating as a true IPS, it successfully prevented a variety of application-level attacks targeted at commonly used protocols.

The SSG 520 ensured protocol conformance and identified attack pattern matches, accepting or rejecting traffic as appropriate, in order to maintain network security. The IPS testing consisted of a rigorous, wide ranging series of tests, probes and scans, designed to emulate real-world attack characteristics. The tests were separated into three distinct test suites: suite one concentrated on device self-protection, suite two looked at device functionality and suite three was concerned with device auditing abilities.

After withstanding a concentrated array of tests and attacks (consisting of over 8000 separate components), including automated penetration tests and real-world replay techniques through commercially available software, the SSG 520 was subjected to a comprehensive, manual verification of all test results, the results of which mean that the SSG 520 was awarded the recently defined IPS Checkmark to complement the other certifications it has achieved.

ANTI-SPAM

The SSG 520 uses an integral anti-spam filter to help prevent the flood of unwanted malicious email. It has the ability to flag and drop any such traffic from known spam and Phishing sources, acting as an effective first line of defense. All known malicious emails were detected at the gateway and the device blocked and flagged each email as appropriate to the anti-spam filter configuration.

The set-up of the anti-spam profile proved equally as easy as the other UTM components tested – and was activated via a simple check-box in the relevant policy. It proved to be a powerful solution in dealing with the increasing spam problem that currently has such a wide-ranging impact on business productivity and resources. Specific custom white and black list entries can also be configured in the anti-spam profile, with the white list identifying messages that are known to be from a trusted email source, and the black list controlling messages that are from a suspected or proven spam source.

TEST REPORT CONTINUED...

West Coast Labs uses a number of exclusive domain names to harvest real-world spam emails that are fed directly into a test network that included the SSG 520 as a gateway anti-spam device. This directly harvested spam email was combined with genuine email from sources on both the internal and external networks that includes both personal and work related emails. Gray email was also thrown into the mix by subscribing users to daily newsletters and numerous mailing lists.

This approach effectively allows West Coast Labs to mirror the varying levels of spam, genuine and gray email found in genuine business environments. Following successful testing in this area, the device was awarded the anti-spam Checkmark at the highest PREMIUM level, achieving a catch rate of over 97% - further information on the test process is set out in the published anti-spam methodology test methodology in Appendix 2.

WEB FILTERING

The SSG 520 device leverages web filtering technologies from both SurfControl and Websense to help protect the corporate network and the business itself from a wide range of potential issues including the potential legal liability associated with downloading copyrighted, inappropriate and illegal material from external websites.

This, of course, has the side effect of increasing overall business productivity, whilst reducing the risks associated with the misuse of company resources and equipment. Web filtering was set-up by simply selecting the appropriate filtering technology from the web management GUI, and in this instance, the integrated SurfControl protocol was used. For added flexibility, there was another option available to redirect traffic to an external host running either the SurfControl or Websense filtering engines.

Using the built-in engine, content was checked against a predefined category list of banned material, categories included common illegal and offensive subject matter, such as Adult / Sexually explicit, Drugs, Alcohol and Tobacco, Hate Speech, Violence, Weapons, Criminal Skills and Gambling. In addition to the predefined lists, custom entries can be made in the form of URLs and assigned to a specific category, thus preventing access to any website not already in the database that is nonetheless deemed unsuitable by an administrator or corporation.

The web filtering technology proved extremely effective, successfully blocking all inappropriate web traffic as expected. Testing was carried out using specialized proprietary web software, based on a real world browser. This software automates the process of web browsing – from the internal to the external network, through the device under test – by loading in known, manually verified websites that contravened a pre-defined acceptable usage policy to a browser window.

A successful pass in this section of testing ensured that the device was certified against the Web Filtering PREMIUM Checkmark the main criteria for which specify that 100% of all attempts to access web sites outside the terms of the security policy should be blocked and that such attempts will be logged. Similarly, 100% of attempts to send emails in contravention of the security policy will fail and that such attempts will be logged.

WEST COAST LABS CONCLUSION

Typical of all the appliances in the Secure Services Gateway Family, the SSG 520 proved to be an extremely robust, simple to administer device, which is easily deployable to both new and existing network infrastructures.

The unit has an extensive, truly flexible array of advanced protection components – integrated within a single, powerful device – designed and proven to secure corporate networks against multiple levels of potential attack, including virus, spyware and hacker based threats. The SSG 520 also has advanced, easily configurable VPN technology to help secure traffic between local and remote networks, facilitating the encrypted transport of corporate data, including web, email and file transfers.

Effective, real-world testing of the built-in firewall, VPN, anti-virus, anti-spyware, anti-spam, web filtering and IPS technologies resulted in the device systematically and accurately detecting and preventing a full range of attack profiles, while operating in both simple and complex business scenarios.

Configuring the device was consistently straightforward and intuitive – even in demanding situations and complicated network environments – aided by the context-sensitive on-line help manual and the well-designed, easily navigable web-based management console.

Clearly, the Secure Services Gateway Family is well suited to any organization that requires a consistently high level of gateway based security.

Checkmark certifications have been awarded for each of the technologies tested as part of this Technology Report, based on the Secure Services Gateway Family achieving the demanding level of performance required.

Full details of the certification criteria for each of the Anti-virus Level 1, Anti-spyware, Firewall Level 1, Anti-spam, IPS, Web Filtering and VPN can be found at www.check-mark.com

Anti-Virus Level 1 | Anti-Spyware GATEWAY | Firewall Level 1 | ANTI-SPAM PREMIUM | Intrusion Prevention Systems | Web Filtering | VPN

APPENDIX 1

FEATURES AND FUNCTIONALITY BUYERS GUIDE – ANTI-VIRUS

AS STATED BY JUNIPER NETWORKS

- Integrates best-in-class gateway antivirus offering from Kaspersky Lab to protect web traffic, email and web mail from file-based viruses, worms, backdoors, Trojans and malware
- Single Antivirus scanning engine detects viruses, Spyware, Adware, phishing and other malware-related programs
- Antivirus scanning engine deconstructs payload and files of all types, evaluating them for potential viruses and then reconstructs the payload or file, sending them to their intended destination
- Protocol support includes SMTP, POP3, FTP, IMAP, HTTP Webmail (yahoo, hotmail, AOL, Comcast, Mail.com, Critical Path, etc.)
- Support for the widest range of file formats and archives that can contain viruses
- More than 400 packers encompassing more than 1100 different versions
- Approximately 40 archives and installers encompassing more than 90 versions and variations
- Three user selectable scanning levels deliver end-user flexibility:
- Standard: The default and recommended option – gives the highest coverage with the lowest false positive rate (includes spyware as well)
- In-The-Wild: Less coverage than standard – offers higher performance by only looking for “in-the-wild” viruses (i.e. does not scan for many of the less frequently seen viruses)
- Extended: Adds some of the traditionally noisier pieces of adware to the scan
- Antivirus signature database is updated as often as every hour. Updates can be delivered to the target SSG platform automatically, per a predefined schedule or manually
- New virus responsiveness averages an industry leading 1.5 hours to deliver a new attack pattern
- Configurable notification (email) to notify the email recipient and sender of virus.
- Policy-based management delivers granular control over traffic scanning to stop attacks that originate from both inside and outside the network
- Email notification is generated if virus found or AV encounters scanning error for SMTP, IMAP, POP3 traffic only.

APPENDIX 1 CONTINUED...

- Create per protocol extension list for targeted scanning
- Create mime list for Targeted scanning
- Create multiple scanning profiles, unique profiler per security zone
- Block files such as exe, .zip, Active X and Java per security zone
- UTM features are manageable by any one of three mechanisms: WebUI, Command Line Interface (CLI) or NetScreen Security Manager (NSM), an optional, extra cost item.
- Apply global UTM security policies via device templates within NSM to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance
- Log Viewer allows logs to be viewed in real time; user-defined filters allow an administrator to perform rapid analysis of security status and events
- Report Manager allows an administrator to generate, view and export predefined and/or custom reports summarizing logs and alarms originating from the managed devices

APPENDIX 1 CONTINUED...

FEATURES AND FUNCTIONALITY BUYERS GUIDE – ANTI-SPYWARE

AS STATED BY JUNIPER NETWORKS

- Powerful Spyware protection is included in the AV scanning engine at no extra charge
- Detects and protects against inbound Spyware attacks such as malicious backdoors, dialers, keyboard loggers, password stealers
- Outbound Spyware protection, delivered through the integration of SurfControl web filtering, blocks users from visiting known Spyware download sites
- Policy-based management delivers granular control over scanning of inbound and outbound traffic to stop attacks that originate from both inside and outside the network
- UTM features are manageable by any one of three mechanisms: WebUI, Command Line Interface (CLI) or NetScreen Security Manager (NSM), an optional, extra cost item.
- Apply global UTM security policies via device templates within NSM to minimize configuration errors by managing any or all aspects of a device or group of devices via a template

APPENDIX 1 CONTINUED...

FEATURES AND FUNCTIONALITY BUYERS GUIDE – ANTI-SPAM

AS STATED BY JUNIPER NETWORKS

- Best-in-class (Symantec) Anti-Spam engine acts as a first line of defense, looking for known spammers and phishers
- Offending spam can be deleted or marked for deletion by the mail server
- Anti-spam engine is derived from analysis of 20-25% of all global email traffic flowing through approximately 3 million Symantec honeypots distributed across more than 25 different countries
- Anti-spam list is updated by Symantec (via Juniper.Net) twice every hour
- User definable tag message with ***SPAM*** default
- Policy-based management delivers granular control over anti-spam
- Enable/disable Anti-spam per security zone
- UTM features are manageable by any one of three mechanisms: WebUI, Command Line Interface (CLI) or NetScreen Security Manager (NSM), an optional, extra cost item.
- Apply global UTM security policies via device templates within NSM to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance
- Log Viewer allows logs to be viewed in real time; user-defined filters allow an administrator to perform rapid analysis of security status and events
- Report Manager allows an administrator to generate, view and export predefined and/or custom reports summarizing logs and alarms originating from the managed devices

APPENDIX 1 CONTINUED...

FEATURES AND FUNCTIONALITY BUYERS GUIDE – FIREWALL AND VPN

AS STATED BY JUNIPER NETWORKS

- Integrated IPS (Deep Inspection FW) protects the network against application level attacks
- Integrated best-in-class Web Filtering (SurfControl) prevents users from visiting malicious Web sites
- Integrated best-in-class Antivirus (Kaspersky Lab) protects the network from penetration and proliferation of viruses, Spyware, Adware, phishing and other malware
- Integrated best-in-class Anti-Spam (Symantec) stops known phishers and spammers.
- Denial of Service protection against over 30 common attacks
- Stateful firewall prevents users and content from entering the network
- IPSEC VPN includes DES/3DES/AES encryption with MD-5 and SHA-1 authentication
- Inline authentication to against Radius, RSA, SecureID, LDAP, local DB in order to access specific resources based on specific protocols
- Web Auth against Radius, RSA, SecureID, LDAP, local DB to require user credentials for access to network resources
- LAN Routing support includes OSPF, RIPv1/2, BGP and source/destination based routing
- Policy-based routing delivers lawful intercept capability by redirecting any type of traffic to an external source (sniffer, scanner, etc) for additional analysis
- WAN encapsulations include PPP, MLPPP, FR, MLFR, and HDLC
- Virtual router, each with their own address table, delivers separate routing domains to manage public/private IP addresses
- Security zones deliver ability to divide network into distinct, secure segments
- VLAN support delivers traffic segmentation capabilities
- NAT, Route and Transparent Layer 2 mode facilitates network integration
- Stafeful High availability for FW and VPN delivers mission-critical device level redundancy
- Redundant VPN tunnel with automatic failover maintains VPN connectivity

APPENDIX 1 CONTINUED...

- SIP, MGCP, SCCP and H.323 application layer gateways help protect VoIP communications
- Optional 802.11 a/b/g Wireless access point support (SSG 5 Wireless / SSG 20 Wireless only)
- Secure 802.11 a/b/g with WPA (AES or TKIP), IPSec VPN, WEP (SSG 5 Wireless / SSG 20 Wireless only)
- Authenticate 802.11 a/b/g with PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x (SSG 5 Wireless / SSG 20 Wireless only)
- When combined with the Juniper Networks Unified Access Controller (UAC), the SSG Family can act as an end point enforcement, redirecting non-compliant systems to a quarantine or remediation VLAN and/or Security Zone for further action.
- All traffic and related events are logged to a central location and time-stamped for analysis and forensic investigation. Logs can be exported to up to four Syslog servers.
- Synchronize internal clock against an external NTP source to ensure accurate log correlation in the event of an attack
- UTM features are manageable by any one of three mechanisms: WebUI, Command Line Interface (CLI) or NetScreen Security Manager (NSM), an optional, extra cost item.
- Apply global UTM security policies via device templates within NSM to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance
- Log Viewer allows logs to be viewed in real time; user-defined filters allow an administrator to perform rapid analysis of security status and events
- Report Manager allows an administrator to generate, view and export predefined and/or custom reports summarizing logs and alarms originating from the managed devices

APPENDIX 1 CONTINUED...

FEATURES AND FUNCTIONALITY BUYERS GUIDE – IPS

AS STATED BY JUNIPER NETWORKS

- Predefined Stateful signatures and Protocol anomalies detect (and stop) a wide range of application level attacks
- Protocol anomalies (decodes) analyze traffic, looking for the underlying behavior of a service to provide zero-day coverage
- Categorized attack signature database (Critical, High, Medium, Low and Informational) for granular policy creation
- Open signatures with regular expression displayed for attack analysis
- Create and enforce appropriate application usage policies for Instant messenger and Peer to Peer applications
- Unique contexts or service fields available (ie. HTTP header or SMTP Subject line) to develop customized signatures
- (7) Attack response mechanisms: Close, Close Server, Close Client, Drop, Drop Packet, Ignore, No action
- (6) Attack logging and notification mechanisms: Session Packet Log, Session Summary E-mail, SNMP, Syslog, Webtrends
- Automatic signature updates delivered weekly and in emergency
- UTM features are manageable by any one of three mechanisms: WebUI, Command Line Interface (CLI) or NetScreen Security Manager (NSM), an optional, extra cost item.
- Apply global UTM security policies via device templates within NSM to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance
- Log Viewer allows logs to be viewed in real time; user-defined filters allow an administrator to perform rapid analysis of security status and events
- Report Manager allows an administrator to generate, view and export predefined and/or custom reports summarizing logs and alarms originating from the managed devices.

APPENDIX 1 CONTINUED...

FEATURES AND FUNCTIONALITY BUYERS GUIDE – WEB FILTERING

AS STATED BY JUNIPER NETWORKS

- Integrated best-in-class (SurfControl) web filtering block access to malicious web sites
- User defined profiles deliver desired levels of web access to different user groups. Profiles can leverage built-in firewall authentication mechanisms for an additional level of control.
- SurfControl supported website for end users to submit new URLs for categorizing
- Option to block or permit all HTTP requests if connectivity to server is lost
- Includes white list (explicitly allowed URLs) and black list (explicitly disallowed URLs) and user definable categories
- URL database of over 19 million (30% are international) covering over 2.5 billion web pages with over 50,000 added every week
- 54 URL categories including Phishing & Fraud, Spyware, Adult/Sexually Explicit, Alcohol & Tobacco, Criminal Activity, Gambling, Hacking, illegal Drugs, Intolerance & Hate, Tasteless & Offensive, Violence, Weapons
- UTM features are manageable by any one of three mechanisms: WebUI, Command Line Interface (CLI) or NetScreen Security Manager (NSM), an optional, extra cost item.
- Apply global UTM security policies via device templates within NSM to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- Audit logs provide a record of configuration changes, supporting central oversight of business policy compliance
- Log Viewer allows logs to be viewed in real time; user-defined filters allow an administrator to perform rapid analysis of security status and events.
- Report Manager allows an administrator to generate, view and export predefined and/or custom reports summarizing logs and alarms originating from the managed devices

APPENDIX 1 CONTINUED...

FEATURES AND FUNCTIONALITY BUYERS GUIDE – OVERVIEW

AS STATED BY JUNIPER NETWORKS

	SSG 5	SSG 20	SSG 140	SSG 520	SSG 550
Targeted deployment location	Small businesses small branch office		Medium businesses and branch offices	Medium businesses and larger branch offices	
Availability	Now	Now	Q4, 2006	Now	Now
Firewall Performance	160 Mbps	160 Mbps	350+ Mbps	650+ Mbps	1+ Gbps
Firewall Packets per second (64 byte packets)	30,000	30,000	100,000	300,000	600,000
IPSec VPN Performance	40 Mbps	40 Mbps	100 Mbps	300 Mbps	500 Mbps
Fixed LAN I/O	(7) 10/100	(5) 10/100	(8) 10/100 (2) 10/100/1000	(4) 10/100/1000	
I/O Options	Factory configured: ISDN BRI S/T or V.92. or RS-232 Serial/Aux	Field installable: T1, E1, ADSL 2+, ISDN BRI S/T, V.92	Field installable: T1, E1, ISDN BRI S/T, Serial	Field installable: 10/100/1000, 10/100, SFP, T1, E1, DS3, Serial	
802.11 a/b/g Wireless	Factory configured option		No	No	No
LAN Routing (RIP/OSPF/BGP)	Yes	Yes	Yes	Yes	Yes
WAN Encapsulations	Yes	Yes	Yes	Yes	Yes
High Availability	Optional	Optional	Yes	Yes	Yes
UTM Security					
Stateful Firewall	Yes	Yes	Yes	Yes	Yes
IPS (Deep Inspection FW)	Yes	Yes	Yes	Yes	Yes
Antivirus (includes Anti-Spyware, Anti-Phishing)	Yes	Yes	Yes	Yes	Yes
Antispam	Yes	Yes	Yes	Yes	Yes
Web Filtering	Yes	Yes	Yes	Yes	Yes

APPENDIX 2

TEST METHODOLOGY AND SPECIFICATIONS

The Juniper Networks SSG 520 appliance was tested at West Coast Labs facility in Swansea, UK and at its accredited test facility in Auburn Hills, Detroit, USA during May thru July 2006.

ANTI-VIRUS AND SPYWARE

Products will be tested in accordance with Checkmark Anti-Virus Level 1 and Checkmark Anti-spyware Gateway specifications to determine their ability to detect all viruses and spyware in the Checkmark certification test suites at the time the test is carried out.

Currently there are over 860 viruses in the Anti-virus Test suite, which is based on the current Wild list and over 1000 in the Anti-Spyware test suite. (See Appendix 3 for detailed descriptions of the malware used in the test suites).

The Anti-Spyware test suite includes a variety of backdoors, downloaders, exploits, proxys, RATs, password stealers, crackers, hijackers and stealers of financial information. West Coast Labs has its own procedures for harvesting and analysing samples on a daily basis.

Infected files will be fed from an external network to an internal network through the device under test or through a gateway machine with the product under test installed. (Where necessary another machine will be provided for the purpose of access to the console, logging, etc.) The product under test will be expected to detect all viruses and spyware while allowing through innocent traffic.

Traffic will be provided using a number of different protocols, as appropriate to the product's specifications. These may include SMTP, HTTP, FTP and/or POP3. A blanket blocking of all files with certain extensions will not be acceptable as an alternative to accurate detection of infections.

FIREWALL

FIREWALL TEST ENVIRONMENT

The test environment will consist of three distinct networks: the external (Internet), DMZ and internal (protected).

The external network may include a telnet host, Web server, FTP server, DNS server and a "hacker" client to simulate the internet. The DMZ network may include a Web server and FTP server. The internal network may include a DNS server, SMTP server, file/print server, Web server and a "hacker" client.

Machines on the internal and DMZ networks are not configured in a secure manner: they rely totally on the protection of the firewall. The firewall is the only link between the DMZ, internal & external networks.

APPENDIX 2 CONTINUED...

The link between the firewall and the external network is via a simple router. No packet filtering will be configured on this router: all protection must be provided by the firewall. Network monitors, protocol analysers and security monitors are employed on the external, DMZ and internal networks.

FIREWALL CONFIGURATION

The firewall is to be configured to provide the various services and enforce the various restrictions specified in this document. All firewalls are to be provided initially with an "out of the box" configuration, although vendors will be invited to remotely access their products if they wish to provide a best fit configuration. Network ranges will be provided to vendors as appropriate.

No patches or configuration options will be allowed which are not available to the general public either in a current release or via a recognised and generally available support source. The configuration of all machines on the three networks will remain constant between tests.

FIREWALL SERVICE CONFIGURATION

The firewall is to be configured to allow the following outbound services:

- Internal to External: DNS, FTP (active and passive), HTTP, SSL/HTTPS, SSH, Telnet, SMTP
- Internal to DMZ: FTP, HTTP, SSL/HTTPS, SSH
- External to Internal: DNS, SSH, and SMTP
- External to DMZ: DNS, FTP, HTTP, SSL/HTTPS, SSH, SMTP
- DMZ to Internal: syslog, SNMP

APPENDIX 2 CONTINUED...

FIREWALL TEST SPECIFICATIONS

The testing is designed to ensure that the firewall technologies under test achieve a basic level of protection against a number of common hostile attacks, from both inside and outside the organization.

A range of tests will be carried out using a variety of firewall scanning tools: these will be configured with full knowledge of both the firewall and network configuration:

- Test that all specified outbound services (and no others) are available from internal clients.
- Test that all specified inbound services (and no others) are available to external clients.
- Test that the firewall management console is not available to any users unless authenticated.
- Test that the firewall is resistant to a range of known Denial Of Service (DOS) tests.
- Test that the firewall does not allow uncontrolled access to either the internal or DMZ networks.
- Test that the underlying OS is hardened and not vulnerable to known OS-specific attacks.

Tests will be repeated in the following manner:

- Probe the internal network from the Internet
- Probe the DMZ from the Internet
- Probe the firewall from the Internet
- Probe the external network from the internal network (test security policy)
- Probe the DMZ from the internal network
- Probe the firewall from the internal network

Management of the firewall will be evaluated using the following criteria:

- Local console must be secure.
- Management console should not be open to the external network.
- The firewall configuration should be fully protected and tamper proof (except from an authorised management station).
- Authentication should be required for the administrator for local administration.
- Authentication and an encrypted link should be available for remote administration.
- All attacks should be logged with date and time.

APPENDIX 2 CONTINUED...

TEST METHODOLOGY AND SPECIFICATIONS - VPN

VPN TEST ENVIRONMENT

The VPN Test Environment will be based on the specification for Firewall as shown above, although another network will be specified as a Remote Office (RO). This may contain a telnet host, DNS server, SMTP server, FTP server, file/print server, Web server and client machines. Network monitors, protocol analysers and security monitors will also be deployed on the RO network.

VPN CONFIGURATION AND SERVICE CONFIGURATION

Initial configuration of the RO firewall should allow no inbound traffic to services hosted on the RO network. Clients on the RO should have access to the DNS, HTTP and SSL/HTTPS servers on the External network.

The initial configuration of the VPN should allow unrestricted traffic flow between the RO and the main Internal network. This should include as a minimum ICMP, DNS, FTP (active and passive), HTTP, SSL/HTTPS, SMTP.

VPN TEST SPECIFICATIONS

The testing is designed to ensure that VPN technology achieves a basic level of security performance in that it:

- Allows a secure point-to-point link between two networks and between a roaming client and a network (optional)
- Provides authentication and access control mechanisms to restrict resource access on a per-user or per-group level
- Provides packet filtering or proxy services within the tunnel to restrict tunnel traffic to specific protocols or source/destination points
- Enforces a reasonable level of encryption and data integrity.

PENETRATION TESTS

A range of penetration tests will be carried out using commonly-available scanning tools All tools will be configured with full knowledge of both the VPN and network configuration:

Check that VPN management console is not available to any users unless authenticated and that the remote management link (if available) is encrypted or can be disabled

APPENDIX 2 CONTINUED...

- Check that the VPN configuration is fully protected and tamper proof and that the VPN is resistant to a range of known Denial Of Service (DOS) attacks
- Check that the VPN has no known vulnerabilities and that it does not allow uncontrolled access to the networks behind it if traffic is restricted (see Services)
- Check that the VPN does not pass mis-configured packets to the networks behind it if traffic is restricted (see Services) and that the VPN correctly enforces access control policy on a per user and/or per group basis

ADDITIONAL TESTS

- Stage 1: Probe the VPN from the protected network with no tunnel established
- Stage 2: Probe the VPN from the external network with no tunnel established
- Stage 3: Attempt to establish tunnels using incorrect credentials
- Stage 4: Establish a valid tunnel (gateway-gateway and optionally client-gateway) and ensure that data is being encrypted
- Stage 5: Probe the remote network from the local network with valid gateway-gateway tunnel established – attempt to violate tunnel traffic policy (eg. pass prohibited protocols, etc.)
- Stage 6: Probe the remote network from the local network with valid client-gateway tunnel established – attempt to violate tunnel traffic policy (eg pass prohibited protocols, etc).
- Stage 7: Probe the remote network from the local network with valid gateway-gateway tunnel established – attempt to violate access control policy (eg. user to access restricted resources).
- Stage 8: Probe the remote network from the local network with valid client-gateway tunnel established – attempt to violate access control policy (eg. user to access restricted resources).

MANAGEMENT

Management of the VPN will be evaluated using the following criteria:

- Local console must be secure and the Management console should not be open to the external network
- The VPN configuration should be fully protected and tamper proof (except from an authorised management station)
- Full authentication is required for the administrator for local administration
- Full authentication and an encrypted link is required for remote administration. If the remote link cannot be encrypted, there should be the ability to disable it.

APPENDIX 2 CONTINUED...

TEST METHODOLOGY AND SPECIFICATIONS – IPS

IPS TEST ENVIRONMENT

The network structure will be the same as for the VPN testing (if the DUT supports it, otherwise it should be the same as for firewall testing) with deployments of Network monitors, protocol analysers and security monitors on each network.

CONFIGURATION

The configuration of the DUT should be the same as the VPN testing (if the DUT supports it, otherwise it should be the same as for firewall testing).

TESTING

The IPS testing module is designed to ensure that the technology contributes to a basic level of protection for an organization against hostile attacks.

All IPS testing will be conducted with full knowledge of the configuration of the DUT. The testing will include a variety of different testing methodologies using both proprietary and established tools and code. Further exploration and attempted exploitations will take place dependant upon the DUT and results received from scans made.

The IPS will be expected to monitor all traffic between the external and internal networks. Machines on the internal network are not configured in a secure manner. Network monitors, protocol analysers and security monitors are employed on the external and internal networks. The configuration of all machines remains constant between tests.

A full range of tests will be carried out using tools, which will be configured with full knowledge of the network configuration. Tools used will include port scanners and vulnerability testers. Attacks will be launched including denial of service attacks and targeted buffer overflows. The internal network will also be subject to attack using spyware, worms and Trojans drawn from the West Coast Labs AV, Spyware and Trojan test suites.

The IPS will be tested for reactions to:

- multiple, varied attacks (flood and swarm)
- obfuscated URLs and obfuscated exploit payloads
- speed adjustments in packet sending
- fragmented packets

The testing will also review IPS logs and alerts, matching them to vulnerability scans. They will also be matched to password cracking activity.

APPENDIX 2 CONTINUED...

TEST METHODOLOGY AND SPECIFICATIONS – ANTI-SPAM

WCL has a number of domains available which act as honeypots for spam, receiving genuine, not canned spam. These domains receive varying levels of spam and are intended to mirror different email environments. Within each domain are designated user accounts with a variety of email practices and needs.

ANTI-SPAM TEST METHODOLOGY

During the course of testing, test engineers use several different internal and external accounts to send emails that simulate real life email transactions common in a business environment. These include requesting meetings, distributing notifications to groups and sending non-business related social emails.

Emails are also sent from web-based accounts to simulate external users sending non-business related emails and home workers. Individual user accounts are subscribed to several mailing lists and daily newsletters for grey mail purposes.

The appliance is configured initially to fit in with the test network using the vendor's recommendations and is placed into the stream of live mail to ascertain how it copes in an "out-of-the-box" situation. The only alteration made to standard working practices is that all emails should be forwarded on (although with altered headers or some sort of flag marking the offending mail as spam) to allow for later classification.

For ascertaining the level of performance, the appliance receives a set number of emails. These are then classified by hand into genuine, spam and grey mail by test engineers with full knowledge of the mailing lists that have been previously signed up for. These figures are then compared with the figures given by the solution to give an overall detection rate.

PRODUCT TESTING AND REPORTING

The appliance under test is assessed in three specific areas – Management/Administration, Functionality, and Performance.

1. Management/Administration.

- Ease of Setup/Use; Logging and reporting function; Rule creation.
- Customization; Content Categories; Product Documentation

2. Functionality

- Email Processing; Allow/Blocking of Email; Quarantine Area; Blacklist/Whitelist

APPENDIX 2 CONTINUED...

3. Performance

- Volume or % of spam detected; False positive rate
- Spam incorrectly passed thru; Legitimate mail blocked

TEST METHODOLOGY AND SPECIFICATIONS – WEB FILTERING

WEB FILTERING TEST METHODOLOGY

The Web Filtering tests replicate in a short space of time a number of hits on sites that fall outside of a prescribed Acceptable Usage Policy, along with providing genuine sites as a control group.

TEST I - A proprietary piece of software has been developed that will load in a list of URLs from a file. This switches through the list changing web page every 6 (six) seconds until it either runs out of URLs or receives an END command. The HTML code from each web page is appended to a log. The designated test engineer examines these logs to ascertain if any undesirable pages have been passed through the appliance.

TEST II - The url list from TEST I is re-run through the appliance. This is accompanied by a manual check following a pre-specified list of URLs in a pre-specified order, and also by a background load provided by specialist hardware. The logs are then appended again to a log file and will be checked further.

Assessment of the appliance under test will consist of attempts to access material via the web in contravention of the security policy. A standardised user session will be employed for this purpose with reproducible http requests beiing generated.

It is expected that attempts to access web sites outside the terms of the security policy will be blocked, and that all such attempts will be logged and recorded.

- The appliance's web filtering technology will also be assessed on:
- The extent to which the security policy is enforced.
- The level of false positives recorded (innocent actions blocked or prohibited)
- The completeness and accuracy of the logs produced.

WCL will also comment on :

- The ease with which the solution can be configured to support the security policies tested
- The level of technical knowledge required to implement and maintain the solution tested.
- The extent to which the solution can be customised in regard to warning messages, logging and content definition.

APPENDIX 3

MALWARE USED IN THE WEST COAST LABS TESTS

MALWARE - A GENERIC DEFINITION

The word Malware is short for malicious software, which is a program designed specifically to damage or disrupt a computer system or its usage, therefore creating a security risk. In the context of this Technology Report, the term Malware includes Viruses, Worms, Trojans and Spyware.

VIRUS

A Virus is a program or piece of code attached to a file or diskette's boot sector; it is loaded onto a computer without the user's knowledge. Viruses are manmade (though they can be corrupted in use to form new variants of the virus) and replicate themselves by attaching themselves to files or diskettes, often soaking up memory or hard disk space and bringing networks to a halt. Most recent viruses are internet-borne and capable of transmitting themselves across and bypassing security systems. Minor variants of the same virus are classed as families of viruses.

WORM

A Worm is an insidious program or algorithm that replicates itself over a computer network or by email system and usually performs malicious actions, such as using up the computer's resources or distributing pornography and possibly shutting the system down. Unlike Viruses, Worms copy themselves as standalone programs and do not attach themselves to other objects.

TROJAN

Trojan Horses or Trojans are destructive programs that pretend to be benign applications. Unlike Viruses or Worms, Trojan Horses do not replicate themselves; they can be damaging to networks by delivering other types of Malware.

SPYWARE

Spyware is a form of software that makes use of a user's internet connection without his or her knowledge, usually in order to covertly gather information about the user. Once installed, the Spyware may monitor user activity on the Internet and transmit that information in the background to someone else. Spyware can also gather information about addresses and even passwords and credit card numbers. Spyware is often unwittingly installed when users install another program, but can also be installed when a user simply visits a malicious website.

APPENDIX 3 CONTINUED...

TYPES OF SPYWARE

BACKDOOR

A Backdoor is a secret or undocumented way of gaining access to a program, online service, computer or an entire computer network Most Backdoors are designed to exploit a vulnerability in a system and open it to future access by an attacker. A Backdoor is a potential security risk in that it allows an attacker to gain unauthorised access to a computer and the files stored thereon.

KEY LOGGERS

A Key Logger is a type of surveillance software that has the capability to record every keystroke to a log file (usually encrypted). A Key Logger recorder can record instant messages, email and any information typed using the keyboard. The log file created by the Key Logger can then be sent to a specified receiver. Some Key Logger programs will also record any e-mail addresses used and Web Sites visited.

FINANCIALS

A Financial is a program that has the capability of scanning a PC or network for information relating to financial transactions and then transmitting the data to a remote user.

PROXIES

Proxies are designed to enable an external user to use a computer for their own purposes, for example, to launch DDoS attacks or send spam, so that the true originator of the attack cannot be traced.

PASSWORD STEALERS AND CRACKERS

A Password Stealer is a program resident on a computer which is designed to intercept and report to an external person any passwords held on that machine. A Password Cracker has the ability to decode any encrypted passwords.

DOWNLOADERS

A downloader is a file which when activated, downloads other files on to the system without the knowledge or consent of the user, those other files then carrying out malicious functions on the system.

HIJACKER

A Hijacker is a file with the ability to change your default Internet home page and/or to create or alter other Web browser settings such as bookmarks and redirection of Internet searches or Internet browsing to commercial sites that could offend the user or breach corporate policies on inappropriate or illegal content.

West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org