

Operations

Butler Group Subscription Services

Network Security

TECHNOLOGY AUDIT

Symantec

Symantec Network Security 7100 Series

Abstract *The Symantec Network Security (SNS) 7100 Series of Intrusion Detection and Intrusion Protection appliances have been designed to deal with the ever-growing range of security challenges that threaten the integrity of internal corporate networks. They provide inline, real-time, proactive network intrusion prevention. Internal (behind the firewall) network protection that stops threats from being propagated from any mainstream user source, including Internet, remote client, mobile, wireless, and branch office VPN, etc. The role of SNS is to support business continuity through its ability to deal extremely quickly with the monitoring of high volume traffic flows. SNS combines the use of multiple traffic detection technologies to handle an extensive range of attack models including Denial of Service (DoS), protocol anomaly detection, signature detection, and vulnerability attack interception. SNS monitoring and protection facilities are targeted at medium to large enterprise organisations where the products policy-driven services can be tailored to meet the specific needs of the business.*

KEY FINDINGS

- | | | | |
|---|---|---|--|
| ✓ | Designed to address internal network security challenges. | ✓ | Policy-based solution; uses a central administration console. |
| ✓ | Multi-functional detection engine used to monitor, identify, and block attacks. | ✓ | Delivers integrated intrusion detection and intrusion prevention services. |
| i | Range of three appliance-based solutions supported. | i | Provides one click IDS to IPS functional switching. |

Key: ✓ Product Strength ✗ Product Weakness i Point of Information

LOOK AHEAD

As is the case with most vendors that operate in the security/management sector, Symantec is reluctant to discuss future roadmap strategies for its security products and appliance-based protection solutions. However, it will continue to develop the range of its SNS 7100 Series monitoring and protection services to meet the ever-growing needs of the IDS and IPS area.

► FUNCTIONALITY

Intrusion detection and intrusion prevention are established components of most enterprise security protection and management strategies. The key rationale across the security industry as a whole for providing such solutions, is that organisations can only protect themselves against events and activities that they can first of all detect, then understand, and finally take action against. This is the role of Intrusion Detection Systems (IDSs) and their intrinsically linked reactive components, Intrusion Prevention Systems (IPSs).

The Symantec Network Security (SNS) 7100 Series of appliances have been built to provide real-time, inline, proactive and reactive, network intrusion prevention services that support the IDS and IPS needs of organisations to protect their internal networks, systems, and applications, from all operational threat sources.

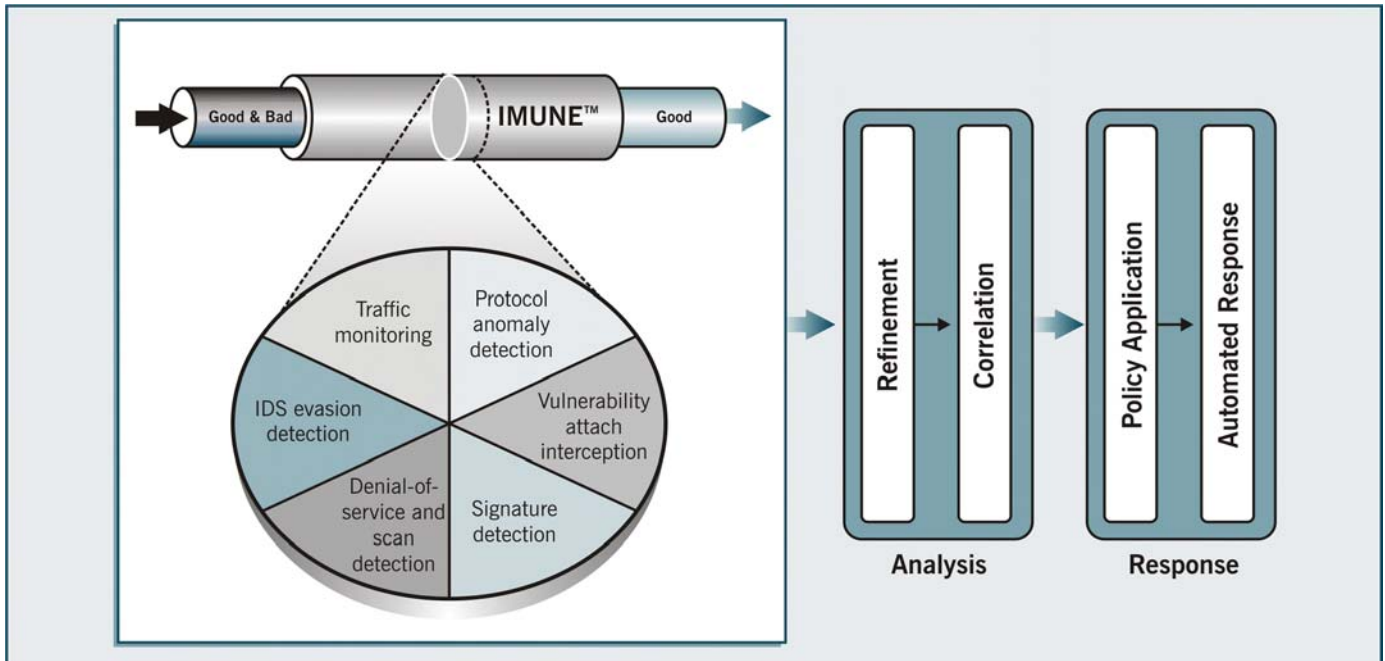
Product Analysis

Real-time protection and service delivery, in the form of network intrusion detection and monitoring, is the starting point for Symantec's SNS solutions. Each of the company's three 7100 Series appliances – 7120, 7160, and 7161 – combines the use of protocol anomaly, signature, statistical, and vulnerability attack interception techniques to identify and then, where appropriate, block known and unknown security attacks. To achieve these objectives, each appliance utilises the services of Symantec's Intrusion Mitigation and Unified Network Engine (IMUNE) that combines the use of anomaly, signature, statistical, and vulnerability attack interception techniques to identify and block network threats as they occur.

SNS appliances are deployed behind the corporate firewall to identify the difference between good and bad traffic, for example, to differentiate between increased traffic flows caused by genuine business traffic peaks, and those caused by malicious Denial of Service (DoS) and distributed Denial of Service (DDoS) activity. SNS appliances have the capability to provide high-speed intrusion detection services (speeds of up to two gigabits per second are achievable), and as a result the solutions multiple detection facilities are able to deal with, control, and contain a wide range of threat types including:

- DoS and DDoS attack detection.
- Stealth attacks.
- Reduction of false positives.
- Worms, Trojans, and Viruses.
- Spyware and Adware.
- Unknown threats identified through the use of Protocol Anomaly Detection techniques, Enhanced Signature Detection (using Stateful Signature Detection), and User Definable Signatures.
- Operating Systems and applications vulnerabilities.
- 'Day zero' attack threats.
- Backdoor detection.
- Instant Messaging (IM) and Peer-to-Peer (P2P) traffic flow identification.
- Ipv6 tunnelled traffic detection.
- Specifically disallowed traffic as determined by an organisation's corporate protection policy.

As highlighted in the following architecture diagram, the challenge for SNS is to detect, identify, and deal with malicious and unacceptable traffic flows and behaviour patterns as they occur, and to determine and deliver appropriate responses on behalf of the business and its users.



Symantec SNS Architecture Diagram

SNS appliances can be deployed to support a flexible range of corporate security and protection initiatives, including passive only inline monitoring for single or multiple devices, real-time intrusion prevention facilities, policy-based monitoring and prevention management services. A flexible range of monitoring and protection services that Butler Groups believes differentiates SNS from many of its more limited competitors.

Symantec's SNS 7100 appliances feature a one-click facility that enables services to switch from a purely detection-based monitoring role to that of a fully-featured IPS with a single mouse click. This approach is easy to control, and can be beneficial for organisations that initially wish to operate their SNS 7100 systems in monitor only mode. We would however, highlight that under these circumstances a manual action needs to be taken in order to switch on IPS protection, and that Symantec offers a fully-automated IDS and IPS facility that provides integrated links between the systems monitoring and protection services.

Each appliance can be centrally managed using the Symantec Network Security Management Console, that provides scalable security management services that are capable of supporting large distributed enterprise-level deployments, providing configuration, policy, threat analysis, visualisation, and reporting services.

SNS provides the flexibility to support a comprehensive range of corporate policy-based protection and security management requirements, and is supported by automated systems maintenance facilities that cover live updating of security content, and real-time security updates through the use of Symantec's Security Response Services.

Product Operation

In operational use SNS 7100 Series appliances are used to monitor and inspect network traffic from every originating source – Internet traffic, wireless users, remote workers, mobile clients, branch staff etc. – providing policy driven reaction to events as they occur.

Responses can range from inline monitoring and alerting through to the real-time blocking of attacks as they are taking place. SNS takes all elements of traditional IDS and IPS monitoring and protection and places them within the hardened boundaries of a black-box system that at the same time still provides the flexibility to support the policy-driven protection needs of the enterprise community, and continues to work towards minimising the incidence of false positives.

The system's protection services have been designed to provide threat visibility and threat identification that can be extended beyond the scope of a single appliance. The systems real-time event correlation capabilities offer the ability to group together related events utilising the solution's user-configurable correlation parameters, and deliver the collected information via the Symantec Network Security Console for analysis by security administrators and security managers.

Event Correlation involves the automated gathering together of event information as an incident. The facility identifies related attributes for example, common source IP or common destination port information. Thereby enabling related information to be grouped together, supporting the speedier identification of threat models, and the actions required to deal with them.

Symantec's Network Security's Analysis Framework (AF) is responsible for delivering event correlation services. AF operates on the systems IPS node, and is responsible for processing all events, across all appliance devices as they occur, and for ensuring that all relevant events are assigned to an existing incident or are used to set up a new incident. In operational use, AF maintains and controls all live and active incidents in memory. Weighted values for event attribution, and policy-driven rules and regulations are used to determine exactly how each event is recorded for an organisation, and into which incident or grouping they are logged.

As each active AF incident is handled in memory, this consumes resources on the SNS node, and therefore maximum resource allocations dictate that there must be a maximum number of incidents that can be allowed to be active at any point in time. If maximum operational levels are reached, AF will open up an overflow incident to capture all excessive activity and deal with this as resources become available. For larger systems deployments cross-node correlation facilities can be utilised to support SNS node clusters, and to ensure that common attack models can be identified across the enterprise, ensuring that such activities are not dealt with as a series of unrelated attacks.

As already discussed, SNS solutions are deployed to support the policy driven IDS and IPS requirements of the business community. Each 7100 Series appliance comes preconfigured with a standard range of detection and protection policies and supporting parameters, these include:

- An all threats policy.
- An all threats and audit policy.
- A critical threats policy.
- A high-level threats policy.
- A medium-level threats policy.
- A Web server threats policy.
- A DMZ threats policy.

Collectively and individually each of these SNS threat policy components are used to drive the out-of-the-box pre-defined monitoring and protection capabilities of each deployed SNS appliance. As a result, at initial deployment, pre-defined SNS monitoring and threat prevention policies are applied to all inline interfaces to provide logging and where appropriate, blocking capabilities.

However, going forward, SNS protection policy management facilities allow organisations to individually tailor specific detection and prevention policies to fit in with their own published policy requirements. In fact, from an operational and service delivery perspective, Symantec recommends that customers should not follow the select all standard signatures approach to deploying SNS policy facilities, but should focus on the key issues, activities, and interface requirements that are relevant to their own business activities. Thereby ensuring that the security processing rules deployed into the live environment match up to corporate security and protection requirements.

The systems single click to protection approach has also been designed to operate alongside Symantec's approach to policy-driven IDS and IPS services. The one click switching from simple detection and monitoring services to full-blown prevention and blocking allows organisations to operate independent, operationally driven, critical threat management services. As required they can deal with all events with a critical severity rating, or those with a high-level threat rating; handle Web-server threat management issues such as, events that are associated with HTTP protocol traffic, regardless of severity levels; and also deal with Worm related threats, network worm propagation etc. Once again, all policy controls and management issues can be controlled from a central management console.

Product Emphasis

The high-level role of IDS and IPS is to capture and, where appropriate, take action on information relating to unexpected and/or unauthorised network activity. Each of the three appliance-based systems in the Symantec SNS 7100 Series has been designed to provide both passive intrusion monitoring, and real-time intrusion protection services.

Butler Group positions the SNS 7100 Series of appliances as a significant range of products that have an important traffic flow management and protection role to play in the enterprise space. We believe that it is no longer good enough to simply provide monitoring and protection services. The delivery of protection service needs to be accompanied by an ability to inform and understand the credentials of the threats that are presented each day. We see SNS as having this ability.

► DEPLOYMENT

The Symantec SNS 7100 Series of appliances have been designed to be utilised in a data centre environment and run alongside other networking devices and systems servers. Installation of basic SNS 7100 functionality is said to be straightforward, and can be undertaken quite quickly by a single technical expert. Ultimately the actual timescales involved will be determined by network complexity within the end-user organisation, and the functionality required.

Once deployed, SNS appliances provide low maintenance protection services. They can be configured to avoid the need for regular additional administrator intervention. Although in Butler Group's opinion the fast moving nature of the threat industry, dictates that all protection services need to come under regular review.

Support for the product set is provided by Symantec, using the company's global Technical Support Services which are located throughout the world. Available support services include:

- Telephone and Web-based services that are able to provide rapid response and up-to-the-minute information facilities.
- Upgradeable insurance services that can deliver automatic software upgrade protection.

- Content protection facilities for the support of virus definitions and security signatures as they need to be updated.
- 24x7 global support from Symantec Security Response experts – a service that can be delivered in a wide variety of languages.
- Symantec Alerting Service and Technical Account Manager facilities to provide enhanced response and proactive security services.

The SNS 7100 Series represents a range of self-contained appliance-based protection solutions that arrive with their software components preloaded. Therefore, there are no direct platform support issues to be considered. From the administration side the use of a central management console is appropriate, and the specifications for that device are as follows:

Processor	Intel® Pentium® or compatible – 1.6GHz or higher.
Operating System	Microsoft Windows® 2000 or XP, Red Hat® Enterprise Linux 3.0 ES.
Memory	Minimum – 256 MB, Recommended – 512 MB.
Disk Space	50 MB for installation, 100 MB post installation.
Screen Resolution	1024 x 768 or higher.
Java	Sun Java™ 2 Runtime Environment (J2RE) version 1.4.2.

SNS 4.0 Security Management Console

The SNS 7100 Series of appliances have been designed to provide network and enterprise protection against a whole range of identifiable threat models including worms, viruses, Trojans, and DoS attacks, and newer ranges of vulnerabilities including spyware etc. Symantec has put together a range of appliance-based offerings that allow organisations to select a solution that fits their individual network protection needs, and given the granularity within the product range there will be an appliance type and delivery model that fits the needs of most medium-to-large enterprise organisations.

► PRODUCT STRATEGY

Symantec's target market for its SNS 7100 Series appliances is, as already stated, medium-to-large enterprise organisations, with a special focus towards organisations that operate in the Financial Services, Healthcare, Managed Services, Technology, Telecommunications, and Utility sectors, where the product has achieved major traction.

SNS 7100 Series appliances are brought to market using Systems Integration and VAR partners at the higher end of the implementation scale, and through GSS partners, and via the OEM route lower down the scale. Appliances are also marketed directly to target customers.

The initial purchase price for the SNS 7100 Series includes the hardware's perpetual licence, and year one maintenance costs (Gold level). Subsequent annual maintenance renewals, that include technical telephone support; software upgrades; security content; and hardware warranty, are charged at 23% of the appliances standard price (MSRP). User organisations have the opportunity to upgrade the level of their support contracts by opting for an optional Platinum contract uplift, that can be selected for one and two year periods.

Within the SNS 7100 Series appliance range (models 7120, 7160, and 7161) a three/four-stage range of usage pricing subsets applies. This Butler Group believes represents a realistic approach to product pricing that will be seen as particularly useful for organisations that expect to grow their licensing requirements for the appliance over time. Entry level pricing for the model 7120 starts at just under UK£5,500 for a 50 Mbps licence with the upper end of the range coming in at just under UK£10,000 for a 200 Mbps user licence. The full SNS appliance pricing strategy is shown in the list below.

Model 7120

- 50 Mbps licence UK£5,433
- 100 Mbps licence UK£6,452
- 200 Mbps licence UK£9,850

Model 7160

- 250 Mbps licence UK£16,306
- 500 Mbps licence UK£23,101
- 1Gbps licence UK£35,333
- 2Gbps licence UK£57,079

Model 7161

- 250 Mbps licence UK£18,344
- 500 Mbps licence UK£25,140
- 1Gbps licence UK£37,372
- 2Gbps licence UK£59,117

Symantec believes that achievable Return On Investment (ROI) from the use of SNS appliances is determined by a number of factors. These include the type of business environment involved; the range of threats posed; and the levels of risk that the organisation finds acceptable. The cost attributed to the average security breach is said by Symantec to be around US\$50,000 (a little over UK£26,000 sterling). This figure includes all elements of the corrective actions including investigation, clean up, and reporting requirements, but as would be expected makes no allowance for intangibles such as, additional reputation and loss of business costs.

In Butler Group's opinion, the problem with any ROI calculation that is made against protection solutions in the security arena is that they can never define a finite value that can be measured against the deployment costs incurred. However, if you accept the average costs for each security breach as previously stated, then it is clear that by comparison Symantec's SNS 7100 appliance-based solution could be expected to pay for its upkeep over a very short time period.

► **COMPANY PROFILE**

Symantec was founded in 1982, and is headquartered in Cupertino, California, USA. Employing around 6,000 staff across 36 countries, the company has offices across North America, South America, Europe, and Asia-Pacific, including: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Ireland, Italy, Japan, Russia, South Africa, Spain, UAE, and the UK.

Symantec is a publicly listed company (NASDAQ = SYMC), and has a corporate mission statement to become the trusted security partner for individuals and enterprises around the world. Currently, Symantec provides comprehensive Internet security products, solutions, and services for more than 125 million users worldwide. These range from the largest corporate enterprises, service providers, government agencies, and higher education institutions, to small business users and individuals.

Reported revenues for the last three fiscal years are as follows:

March year end	2004	2003	2002
Revenues in millions (US\$)	1,870	1,407	1,071

► SUMMARY

Intrusion detection allied to intrusion prevention, has to be seen as cornerstone-stone technology for any enterprise security and protection strategy. Without their inclusion it would be difficult to understand the wider security picture as it relates to the protection requirements of the business.

However, the hard and fixed nature of the enterprise perimeter has now deteriorated to such an extent that it is no longer possible to focus intruder protection services on any single point or style of attack. SNS 7100 Series appliances provide the scope and flexibility to be deployed to suit the internal network traffic flow management and protection requirements of most organisations. As such, the role of each appliance is to provide high-speed traffic-flow monitoring facilities, and to actively stop threats from across all access channels – worms, viruses, Trojans, spyware, and bots, etc. – from propagating inside corporate networks.

IDS and IPS represent an extremely competitive area of the security marketplace. To keep ahead of the competition Butler Group considers that Symantec must continue to build solutions such as the latest SNS 7100 Series, that have the flexibility of purpose, and strength of functionality, to deal with the ever changing protection needs of its customers, and of course, the ever growing range of threats that are presented on a second-by-second basis.

► CONTACT DETAILS

Symantec Corporation
 World Headquarters
 20330 Stevens Creek Blvd.
 Cupertino, CA 95014
 USA

Tel: +1 408 517 8000

www.symantec.com

Symantec United Kingdom Ltd.
 Hines Meadow, St. Cloud Way
 Maidenhead, Berkshire
 SL6 8XB
 UK

Tel: +44 (0)1628 592222

Fax: +44 (0)1628 592393

www.symantec.co.uk

Important Notice:

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

About Butler Group:

Butler Group is the premier European provider of Information Technology research, analysis, and advice. Founded in 1990 by Martin Butler, the Company is respected throughout the business world for the impartiality and incisiveness of its research and opinion. Butler Group provides a comprehensive portfolio of Research, Events, and Subscription Services, catering for the specialised needs of all levels of executive, from IT professionals to senior managers and board directors.