Secure Network Access System

Computer Division, B.A.R.C has developed an indigenous integrated security appliance called as **Secure Network Access System (SNAS)**. SNAS secures any enterprise network by intelligently sensing security threats and responding to them automatically. SNAS provides end point security policy compliance by taking policy based decisions regarding who gets admission into the network and with what level of network access privileges. SNAS identifies the “who, what and where” of the end systems connected in a network. It can identify almost everything on the network – the devices, their operating systems and the applications running on them. SNAS combines the features of a perimeter firewall, network management system and endpoint security solution to provide a bird's eye view of the entire network as well as detailed information about each entity connected to it. SNAS can be easily configured to suit the network security requirements of different types of enterprises.

SNAS can be deployed in enterprise networks to replace the existing firewalls between intranet segments (LAN) and various demilitarized zones and WAN. SNAS will ensure that the devices in the user segment comply with security policy and all internal network attacks are identified and mitigated. The SNAS security suite provides a comprehensive solution for mitigation of attacks.

In April 2012, SNAS was launched as a commercial product at national level by Dr. Srikumar Banerjee in the presence of Dr. Rajagopala Chidambaram in Delhi.

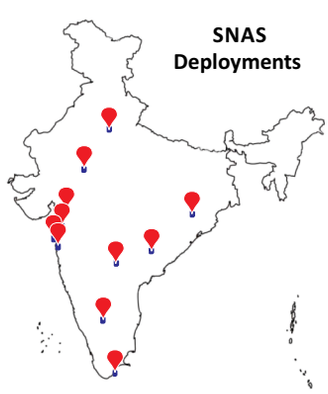
S.No.	SNAS Versions	**Moonlight**	**Sunlight**
1	Network Interfaces*	4 x 10 Gbps 4 x 1 Gbps	4 x 10 Gbps 4 x 1 Gbps
2	Max Supported End Points	5000	20000

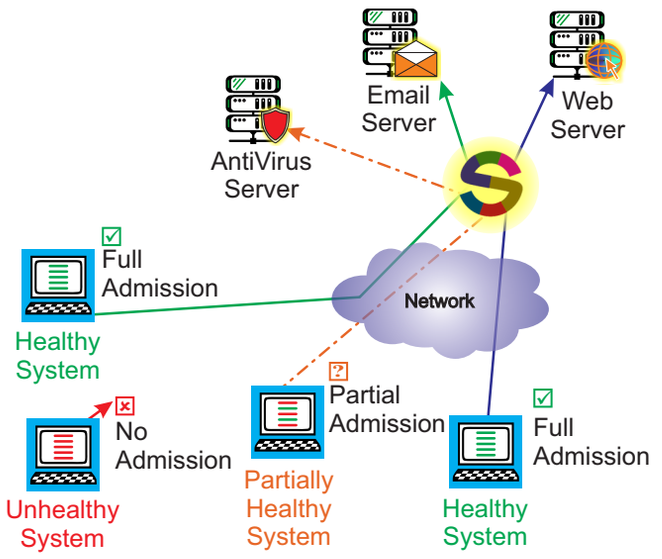
* Custom configurations are also available

Developed By:

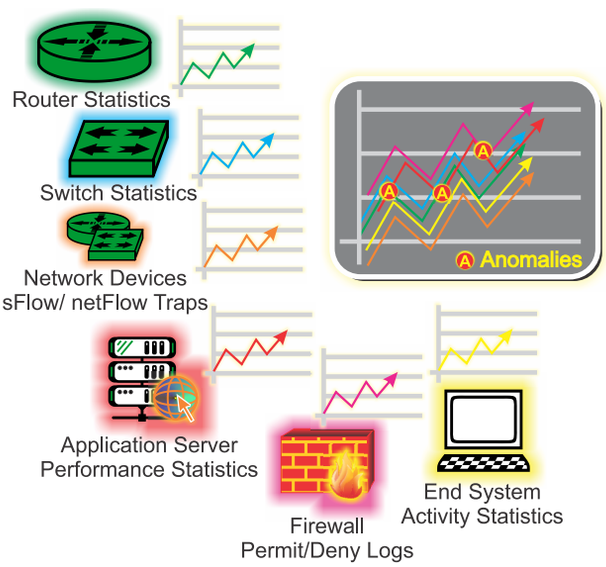
भाभा परमाणु अनुसंधान केंद्र
BHABHA ATOMIC RESEARCH CENTRE

SNAS Appliance





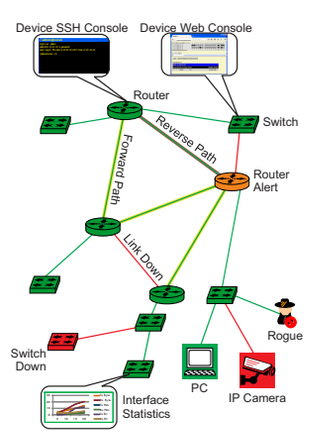
Network Admission Control



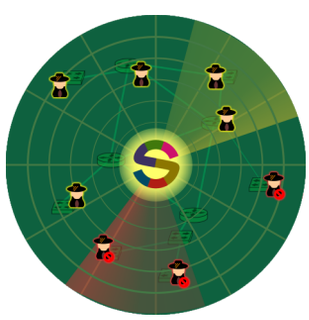
Network Behaviour Anomaly Detection Architecture

Salient Features

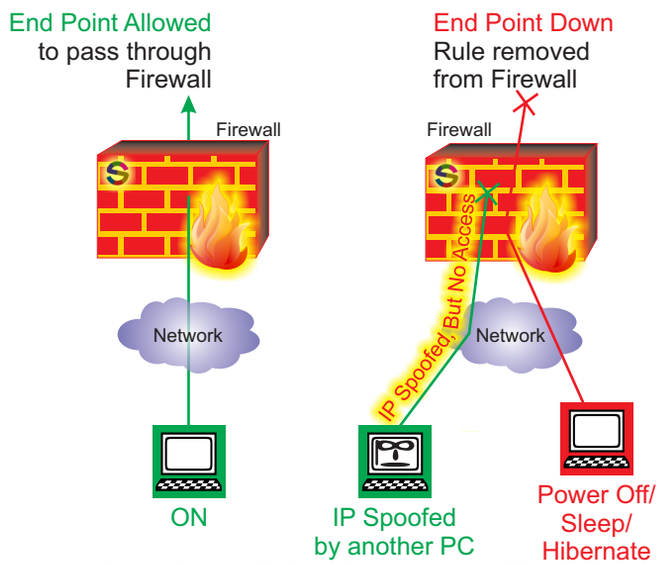
- Enterprise Network Security Policy Enforcement
- Profile based access control
- Removable Media Control
- Agent / Agent-less support
- Detection of network behaviour anomalies
- Identifies and mitigates internal attacks
- Security visualization of complete network
- Network monitoring & management
- Supports wide variety of network devices
- Detects routing mirrors in network
- Identification and isolation of unauthorized devices in the network
- Identification and mitigation of bridging of isolated networks
- End-system Health Monitoring
- Continuous monitoring of network-devices and end-systems
- Dynamic Host-aware Firewall
- Bandwidth Control & Connection Limiting
- Captive Portal
- Multiple 1G/10G ports available
- Firewall Permit/Deny Logs Analysis
- Firewall rules correction support
- High Availability
- Integration with open source IDS
- Support of deployment life-cycle
- Support for asset management of the network
- Scalable to small, medium and large enterprises with varying security requirements



Network Monitoring and Management



Continuous Network Scanning



Host Aware Policy Enforcement Firewall