12. Intrusion prevention system

12.1 Network Intrusion Prevention System

Sr. No.	Item	Minimum Requirement Description
NIPS.REQ.001	Network Intrusion Prevention System	**Platform Requirement**
NIPS.REQ.002	Network Intrusion Prevention System	The device should be a purpose built dedicated appliance (not a subset of firewall or UTM appliance).
NIPS.REQ.003	Network Intrusion Prevention System	The device should operate in transparent (Bridge) mode.
NIPS.REQ.004	Network Intrusion Prevention System	The device should have separate dedicated interface for management.
NIPS.REQ.005	Network Intrusion Prevention System	The device should have external / internal Redundant Power Supply (RPS).
NIPS.REQ.006	Network Intrusion Prevention System	L2
NIPS.REQ.007	Network Intrusion Prevention System	The device should perform traffic inspection based on:
		a) Signatures
		b) Protocol anomaly
		c) Behavior anomaly
		d) Reputation
NIPS.REQ.008	Network Intrusion Prevention System	The device should accurately detect the following Attack categories:-
		a) Unauthorized access attempts
		b) Pre-attack probes
		c) DoS
		d) Vulnerability exploitation
		e) Zero-day attacks.
NIPS.REQ.009	Network Intrusion Prevention System	The device should employ full seven-layer protocol analysis of over 100 internet protocols like HTTP, FTP, SMTP, etc.
NIPS.REQ.010	Network Intrusion Prevention System	The device should support more than 2500 signatures.
NIPS.REQ.011	Network Intrusion Prevention System	The device should handle following traffic:
		a) IPv6
		b) IPv4
		c) Asymmetric / Symmetric Traffic

DRAFT

NIPS.REQ.012	Network Intrusion Prevention System	The device should support:
		a) Bi- directional inspection
		b) Detection of Shell Code
		c) Advanced evasion protection.
NIPS.REQ.013	Network Intrusion Prevention System	The device should have the ability to identify/block individual applications (eg. Facebook or Skype) running on one protocol (eg. HTTP or HTTPS).
NIPS.REQ.014	Network Intrusion Prevention System	The device should identify SSL Protocol based attacks.
NIPS.REQ.015	Network Intrusion Prevention System	The device should have the ability to scan malware within files such as PDF, MS office Documents.
NIPS.REQ.016	Network Intrusion Prevention System	The device should be capable of providing network-based detection of malware by checking the disposition of known files in the cloud.
NIPS.REQ.017	Network Intrusion Prevention System	The device should support Protection against Client side attacks.
NIPS.REQ.018	Network Intrusion Prevention System	The device should protect:
		Web applications
		Web 2.0
		Databases
NIPS.REQ.019	Network Intrusion Prevention System	The device should support both IPv4 & IPv6 simultaneously (Dual Stack).
NIPS.REQ.020	Network Intrusion Prevention System	The device should support botnet protection based on:
		a) BOT detection
		b) Command and control database
NIPS.REQ.021	Network Intrusion Prevention System	The device should protect against DOS/DDOS attacks based on Threshold based detection.
NIPS.REQ.022	Network Intrusion Prevention System	**Performance**
		Should have minimum Inspected throughput of 1 Gbps for all kinds of traffic.
		Should support minimum 500,000 Concurrent Connections.
		Should have dedicated 10/100/1000 RJ45 Management Interface.
		The device should have 8 10/100/1000 ports.
NIPS.REQ.023	Network Intrusion Prevention System	**Reporting and Alerting**
NIPS.REQ.024	Network Intrusion Prevention System	The management platform should provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
NIPS.REQ.025	Network Intrusion Prevention System	**Availability**

DRAFT

NIPS.REQ.026	Network Intrusion Prevention System	Sensors should support built-in capability of failing close and failing open, such that communications traffic is still allowed to pass if the inline sensor goes down.
NIPS.REQ.027	Network Intrusion Prevention System	**Third-Party Integration**
NIPS.REQ.028	Network Intrusion Prevention System	The management platform should include an integration mechanism, to enable respond to threats.
NIPS.REQ.029	Network Intrusion Prevention System	**Network Behavior Analysis (NBA)**
NIPS.REQ.030	Network Intrusion Prevention System	The solution should provide NBA capability to detect threats emerging from both outside the network & inside the network.
NIPS.REQ.031	Network Intrusion Prevention System	**Threat Protection**
NIPS.REQ.032	Network Intrusion Prevention System	Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.
NIPS.REQ.033	Network Intrusion Prevention System	The detection engine should be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).
NIPS.REQ.034	Network Intrusion Prevention System	Sensors should be capable of performing packet-level forensics and capturing raw packet data in response to individual events without significant performance degradation.
NIPS.REQ.035	Network Intrusion Prevention System	**Policy Configuration**
NIPS.REQ.036	Network Intrusion Prevention System	The device should have facility to enable/disable each individual signature. Each signature should allow granular tuning.
NIPS.REQ.037	Network Intrusion Prevention System	The device should support granular management. Should allow policy to be assigned per device, port, VLAN tag, IP address/range.
NIPS.REQ.038	Network Intrusion Prevention System	The device must have facility to exempt IPS inspection for a particular signature based on
		a) Source or Destination IP/Subnet
		b) Between two IP/subnet
NIPS.REQ.039	Network Intrusion Prevention System	The device should support a wide range of response actions:
		a) Block traffic
		b) Ignore
		c) TCP reset
		d) Packet capture
		e) Email alert
		f) SNMP alert

DRAFT

		g) Syslog alert
NIPS.REQ.040	Network Intrusion Prevention System	**Real-Time Awareness**
NIPS.REQ.041	Network Intrusion Prevention System	The solution should be capable of gathering information about network hosts and their activities.
NIPS.REQ.042	Network Intrusion Prevention System	The solution should be capable of employing an extensive set of contextual information (e.g., behavior of the network) to improve the efficiency and accuracy of analysis of detected events.
NIPS.REQ.043	Network Intrusion Prevention System	The solution should be capable of providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
NIPS.REQ.044	Network Intrusion Prevention System	**High Availability**
NIPS.REQ.045	Network Intrusion Prevention System	The device should support High Availability.
NIPS.REQ.046	Network Intrusion Prevention System	The device should support both Active/Passive and Active/Active configuration
NIPS.REQ.047	Network Intrusion Prevention System	**Management and Usability**
NIPS.REQ.048	Network Intrusion Prevention System	The solution should support centralized, life cycle management for all sensors.
NIPS.REQ.049	Network Intrusion Prevention System	The solution should be accessible via a web-based SSL interface.

12.2 Host based Intrusion Prevention System

Sr. No.	Nature of Requirement	Minimum Requirement Description
HIPS.REQ.001	General Requirement	The proposed solution should be a virtualization aware solution that provides advanced protection for systems.
HIPS.REQ.002	General Requirement	The proposed solution should be supported on multiple operating systems: Microsoft Windows, Solaris , Red Hat Enterprise & Suse Linux, etc.
HIPS.REQ.003	General Requirement	The proposed solution should be able to provide protection such as Antimalware real time, IDS/IPS, Firewall, Integrity changes, and Inspection of system critical logs for all the systems and should be able to achieve with the single Agent.
HIPS.REQ.004	General Requirement	The proposed solution should have management console and provide Prevention and Monitoring support for all the operating systems in the heterogeneous environment.

DRAFT

HIPS.REQ.005	General Requirement	Should provide intrusion detection and protection by analysing events, operating system logs and inbound/outbound network traffic on enterprise servers.
HIPS.REQ.006	General Requirement	The proposed solution should employ full, seven-layer, state-based protocol decoding and analysis. Analyses all packets to and from the server for and propagation. To detect and prevent attacks, both known and unknown intrusion attempts. Should prevent the following: a) Prevents the delivery and installation of kernel-level Root kits. b) Prevents cross-site scripting (XSS) attacks. c) Prevents SQL injection attacks. d) Prevents DOS, DDOS, worm, botnet and Trojan attacks. e) Prevent Buffer overflow attacks f) Decodes backdoor communications and protocols. g) Inspect and block attacks that happen over SSL (HTTP & HTTPS).
HIPS.REQ.007	General Requirement	The proposed solution should have rule based protection, and for servers.
HIPS.REQ.008	General Requirement	The proposed solution should have Application based Control rules provide increased visibility into the applications that are accessing the network. These rules shall be used to identify malicious users / software accessing the network and provide insight into suspicious activities such as allowed protocols over unexpected ports (FTP traffic on a mail server, HTTP traffic on an unexpected server, or SSH traffic over SSL, etc.)
HIPS.REQ.009	General Requirement	The proposed solution should have detailed events data to provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit, shall be logged.
HIPS.REQ.010	General Requirement	The proposed solution should be capable of blocking and detecting of IPv6 attacks.
HIPS.REQ.011	General Requirement	The solution should allow blocking based on thresholds.
HIPS.REQ.012	General Requirement	The proposed solution should have detection capability of reconnaissance activities such as port scans and also detect protocol violations of standard protocols.
HIPS.REQ.013	General Requirement	The proposed solution should have an auditable reporting should generate within the solution, along with alert generations, and automated report creation and delivery.
HIPS.REQ.014	General Requirement	The proposed solution should have Agent installation methods to support manual local installation and distribution through LDAP / Active Directory. No restart should be required once the agent is installed on the Servers.
HIPS.REQ.015	General Requirement	The proposed solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.

DRAFT