Compliance
&
Cross Reference Document
for

GS990nu

Generic

1. Proposed Appliance should be dedicated purpose-built hardware appliance with 64bit hardened OS
   - Please refer 'The power of advanced visibility'
     on below public URL,
     https://www.gajshield.com/index.php/solutions/bulwark
2. Minimum internal storage 200 GB SSD for detailed graphical Logs & Reports on Appliance
   - Please refer Hardware Specifications
     Page 4, Datasheet of GS990nu
3. External /Internal Redundant Power Supply
   - Please refer Data Security Firewall Specifications
     Page 1, Datasheet of GS990nu
4. Solution should have option to support solution that can support the enablement of all next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Malware, VPN, etc.
   - Please refer Datasheet of GS990nu
     Intrusion Protection – Intrusion Prevention System Page 2,
     App control – Application Filtering Page 3,
     URL filtering – URL Filtering Page 3,
     Anti-Malware – Gateway Antivirus Page 3,
     VPN – Virtual Private Network Page 3,
5. Proposed solution should have open standard multicore processor-based architecture and not proprietary ASIC based architecture
   - Please refer Hardware Specifications
     Page 4, Datasheet of GS990nu

Interface Requirement

1. Ethernet Interfaces - 6 no's of 10/100/1000G Ports
2. The proposed system should have HA Active-Active / Active-Passive.
3. Minimum 8*10G SFP+ Port, 2 for core switch, 2 For DMZ zone, 2 for HA and 2 for future, min 64 GB RAM or higher from day 1
   - Please refer Data Security Firewall Specifications
     Page 1, Datasheet of GS990nu
     Also,
     Please refer BOQ for 8*10G SFP+ ports

Performance Capacity from day 1

1. Firewall Throughput - 60 Gbps
2. VPN Throughput - 10 Gbps
3. NGFW Throughput - 30Gbps
4. IPS Throughput - 28 Gbps
5. Firewall IMIX Throughput -35 Gbps
   - ➢ Please refer Data Security Firewall Specifications
     Page 1, Datasheet of GS990nu

Next Generation Firewall Features

1. The proposed system should have firewall with stateful packet filtering technology & must support one-to-one and dynamic user-based NAT with a facility to create rules based on usernames, Source & Destination IP address, Hosts, network, IP Range
   - ➢ Stateful packet filtering –
     Please refer Stateful Inspection Firewall
     Page 3, Datasheet of GS990nu
   - ➢ Please refer
     NAT - Tab 'Networking'
     Rule Creation – Tab 'System Management'
     on below public URL,
     https://www.gajshield.com/index.php/products/features
2. The firewall of the proposed system should be based on a hardened OS, should be capable of delivering network protection services at all layers along with options of network gateway level antivirus /antimalware, anti-spam, intrusion detection and prevention, content filtering, multiple ISP load balancing / sharing, failover and VPN solutions.
   - ➢ Please refer Datasheet of GS990nu
     Gateway level antivirus /antimalware - Gateway Antivirus Page 3,
     Anti-spam - Gateway Anti-spam Page 3,
     Intrusion detection and prevention - Intrusion Prevention System Page 2,
     Content filtering - URL Filtering Page 3,
     Multiple ISP load balancing / sharing, failover - Networking Page 3,
     VPN solutions - Virtual Private Network Page 3,

3. The firewall should be able to support deployment in transparent mode, Bridge mode, layer 3 transparent proxy mode
    - ➢ Please refer Networking
      Page 3, Datasheet of GS990nu
4. The firewall of the proposed system should provide Predefined services based on port numbers and Layer 7 application and ability to create user-definable services which can be used to define firewall rules
    - ➢ Please refer Tab ‘System Management’
      on below public URL,
      https://www.gajshield.com/index.php/products/features
5. The proposed system must provide inbuilt PPPoE client and should be capable to automatically update all required configuration (NAT Policies, VPN Configuration, Firewall Rules) whenever PPPoE IP get changed.
    - ➢ Please refer Tab ‘Networking’
      on below public URL,
      https://www.gajshield.com/index.php/products/features
6. The firewall of the proposed system should support 802.1q based VLAN tagging to segregate devices logically
    - ➢ Please refer Stateful Inspection Firewall
      Page 3, Datasheet of GS990nu
7. The proposed solution should have option to configure firewall policies to block or allow rules based on Country based Geo Location
    - ➢ Please refer Tab ‘System Management’
      on below public URL,
      https://www.gajshield.com/index.php/products/features
8. The proposed solution must have control mechanism to perform policy-based control for Application, traffic shaping and visibility for Users, Groups, IP address & Network.
    - ➢ Please refer
      Policy based control - Tab ‘System Management’
      traffic shaping - Tab 'Bandwidth Management'
      on below public URL,
      https://www.gajshield.com/index.php/products/features

9. The proposed solution should be able to detect & block known applications like P2P & IM.
    - Please refer 'Features'
      on below public URL,
      https://www.gajshield.com/index.php/solutions/application-filtering
10. The proposed solution should limit upstream and downstream bandwidth based on application, users etc
    - Please refer Bandwidth Management
      Page 3, Datasheet of GS990nu
11. Should have Role based and multi factor authorization for Administration
    - Please refer Administration
      Page 3, Datasheet of GS990nu
12. The proposed solution should be able to detect & block known applications based on time schedule.
    - Please refer Application Filtering
      Page 3, Datasheet of GS990nu

URL Filtering & Web Protection

1. Should support 85+ Web categories
    - Please refer URL Filtering
      Page 3, Datasheet of GS990nu
2. Should support blocking of category-based HTTPS sites without having to provide the URL of the site to be blocked
    - Please refer 'Features'
      on below public URL,
      https://www.gajshield.com/index.php/solutions/url-filtering
3. Should support HTTPS transparent proxy
    - Please refer Tab 'Networking'
      on below public URL,
      https://www.gajshield.com/index.php/products/features
4. Should support HTTPS transparent / explicit proxy. The proposed system should support browsing proxy and gateway mode simultaneously
    - Please refer Tab 'Networking'
      on below public URL,
      https://www.gajshield.com/index.php/products/features

5. The proposed solution should block HTTPS URLs with complete path instead of only sites names
   - ➢ Please refer URL Filtering
     Page 3, Datasheet of GS990nu
6. The proposed solution should support regular expression in blocking of HTTPS sites
   - ➢ Please refer 'Features'
     on below public URL,
     https://www.gajshield.com/index.php/solutions/url-filtering
7. Should enforce Google/Yahoo Images strict filtering through a web interface.
   - ➢ Please refer 'Features'
     on below public URL,
     https://www.gajshield.com/index.php/solutions/url-filtering
8. Web based management through https and command line interface support
   - ➢ Please refer Administration
     Page 3, Datasheet of GS990nu

Intrusion Prevention System

1. Intrusion Prevention system should be appliance based or integrated with the NGFW solution
   - ➢ Please refer Intrusion Prevention System
     Page 2, Datasheet of GS990nu
2. The proposed IPS system should have signature and anomaly base intrusion detection and prevention system
   - ➢ Please refer Intrusion Prevention System
     Page 2, Datasheet of GS990nu
3. The proposed system should have prevention option for more than 30 common attacks. Real- time intrusion detection for minimum 11000+ signatures.
   - ➢ Please refer Tab 'Intrusion Prevention System'
     on below public URL,
     https://www.gajshield.com/index.php/products/features

4. The IPS should be able to detect, respond to and alert any unauthorized activity. Product detects the attacks and the network misuse that represent risk to the customer.
   - ➢ Please refer Tab ‘Intrusion Prevention System’
     on below public URL,
     https://www.gajshield.com/index.php/products/features
5. NIDS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.
   - ➢ Please refer Tab ‘Intrusion Prevention System’
     on below public URL,
     https://www.gajshield.com/index.php/products/features
6. Support at least 11000+ or more signatures with online download support of newer signatures.
   - ➢ Please refer Intrusion Prevention System
     Page 2, Datasheet of GS990nu
7. The proposed system should automatically update the attack signatures database from a central database server
   - ➢ Please refer Intrusion Prevention System
     Page 2, Datasheet of GS990nu
8. The proposed system should be able to detect and block HTTP proxy traffic both from Content filtering solution & also from IDP
   - ➢ Please refer Tab ‘Intrusion Prevention System’
     on below public URL,
     https://www.gajshield.com/index.php/products/features
     Also,
     Please refer ‘Features’
     on below public URL,
     https://www.gajshield.com/index.php/solutions/url-filtering

Gateway Anti-Malware

1. The proposed system should scan for viruses even for downloads from HTTPS sites
   - ➢ Please refer Gateway Antivirus
     Page 3, Datasheet of GS990nu

2. Proposed solution should be cloud based Anti-APT solution to scan for zero-day malwares
   - ➢ Please refer Gateway Antivirus
     Page 3, Datasheet of GS990nu
3. Embedded Anti Malware support. Should have option to automatically update the new virus pattern updates. Anti-Malware should be supported for HTTP, HTTPS, FTP, POP3, SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3. Anti-Malware scanning should be signature/Hash based and should provide ZERO HOUR Anti Malware support.
   - ➢ Please refer Gateway Antivirus
     Page 3, Datasheet of GS990nu
4. Gateway level Anti Malware should provide high-performance protection against viruses in SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3, HTTP, HTTPS and FTP traffic. It should block viruses and worms from penetrating into an organization's internal network through e-mail attachments, malicious Web pages, and files obtained through FTP.
   - ➢ Please refer Tab 'Gateway Anti-Malware'
     on below public URL,
     https://www.gajshield.com/index.php/products/features
5. Virus gateway should provide real-time detection of viruses and malicious code at the gateway for IMAP SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3, HTTP, HTTPS and FTP Internet traffic.
   - ➢ Please refer Tab 'Gateway Anti-Malware'
     on below public URL,
     https://www.gajshield.com/index.php/products/features
6. The proposed solution should be licensed per unit as against per user.
   - ➢ Please refer Tab 'Firewall'
     on below public URL,
     https://www.gajshield.com/index.php/products/features

Logging and Reporting solution

1. The proposed system should have reporting solution VM/Appliance based
   - ➢ Please refer Tab 'Appliance based Security Analytics'
     on below public URL,
     https://www.gajshield.com/index.php/products/features

2. The proposed system should provide individual users download & Upload data usage report.
    - Please refer Tab ‘Appliance based Security Analytics’
      on below public URL,
      https://www.gajshield.com/index.php/products/features
3. The proposed system should email daily group browsing reports to respective group heads in pdf format.
    - Please refer Tab ‘Appliance based Security Analytics’
      on below public URL,
      https://www.gajshield.com/index.php/products/features

4. The proposed system should provide user and IP address-based reports.
    - Please refer Tab ‘Appliance based Security Analytics’
      on below public URL,
      https://www.gajshield.com/index.php/products/features
5. The proposed system should have options to create users with different access rights (E.g. users who can only view reports and not manage the system)
    - Please refer Administration
      Page 3, Datasheet of GS990nu
6. The reporting solution of the proposed system should be able to provide detailed Audit log for auditing and tracking system
    - Please refer Tab ‘Logging and Reporting’
      on below public URL,
      https://www.gajshield.com/index.php/products/features
7. Should support logging on the Next Generation Firewall internal or external. It should provide various kinds of reports like Malware/Virus reports, URL filtering reports, Top visited websites, Systems infected by Spywares, User or IP wise download for the day. It should have graphical reports of usages ISP wise, Application wise and IP wise.
    - Please refer
      Tab ‘Logging and Reporting’ and
      Tab ‘Appliance based Security Analytics’
      on below public URL,
      https://www.gajshield.com/index.php/products/features