GAJSHIELD

Progressive Security

Sixth Sense UPTM

Data Sheet

- **Data Leak Prevention**
  Intentional or unintentional leak of information is a major concern for enterprises. Identify unauthorized file, data leak user-wise and have the ability to control such leakage.
- **Proactive Security**
  Identify which application, threat vector and user makes the network vulnerable and have control over P2P, Instant Messaging, Email, Web, FTP and other Web 2.0 applications.
- **Complete Visibility**
  User based visibility allows identification of application misuse, Data leak and allows to regain control over applications and more importantly Content traversing out of the network.
- **Unique Gateway Architecture**
  Policy based ISP Failover & Load Balancing to distribute important applications over more robust internet links and less important applications over broad band connections and also to provide redundancy.
- **Zero Hour Protection**
  Signature-less protection to detect and block viruses, malware, spyware, spams, phishing attacks in Real Time.
- **Cloud based URL Filtering**
  Enables real-time protection from emerging Web threats, block or monitor website for better Productivity management and regulate bandwidth through identification and blocking of bandwidth hogging applications.

Time Sense

Identifies the time when any information is sent. Some information may have time sensitivity. For example, you may not want your audited reports to be published or sent before it is publically announced.

Application Sense

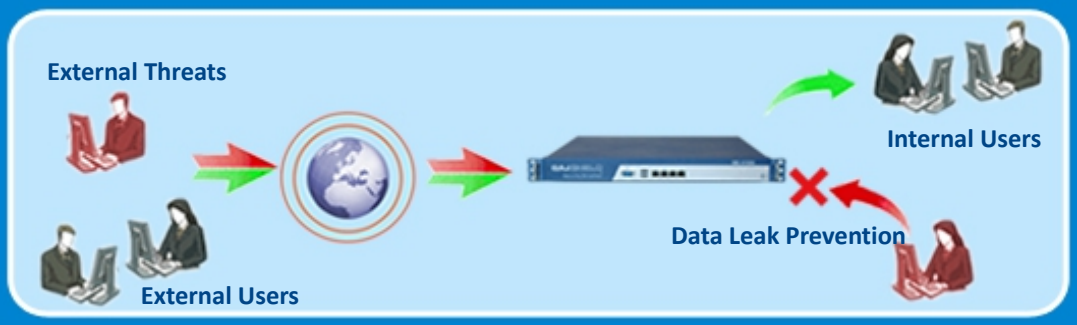
ApplicationSense technology identifies applications regardless of port, protocol, encryption, or evasive tactic. It gives enterprises visibility and policy control over actual applications, not just ports.

Network Sense

Organisation would not want that critical data travel through public networks. For example, when a mobile device is uploading data within the network would need to go through multiple checks of malware detection than data coming from within private networks.

User Sense

Integrates With Enterprise Directories. UserSense technology integrates GajShield's UPTM with enterprises' Active Directory implementations. Meaning that the single policy engine governing application and content security also has the ability to refine that policy with the user and group definitions already used in the enterprise.



Content Sense

Identifies Content – Including Confidential Content. ContentSense technology incorporates 3 key content security elements confidential data (DLP functionality), threat prevention, and a URL filtering capability. The data filtering feature in GajShield makes implementing DLP functionality in the firewall simple. Adding a policy object that scans application traffic is a matter of assigning the data filtering profile to the policy, determining what sort of data to scan for. Enterprises can also use the regular expression capability built into the data filtering feature to create custom patterns. More importantly, ContentSense keeps track of all uploaded data and archives it. This gives an enterprise insight of what is being uploaded even for content where no policy has been set.

Context Sense

Every information has criticality based on the context over which it has been sent. GajShield's ContextSense helps in indentifying the context with the help of the above five senses to categories the criticality of data. For example, when a user is allowed to connect to a POP3 server, he could possibly download mails or any user, but a context sensitive firewall will identify the user using UserSense, the application (POP3) using ApplicationSense, the id it is using to identify to the POP3 server using ContentSense and create a context using the ContextSense engine which enables an organisation to either block or allow the id to connect thus ensuring that only valid users connect to their POP3 ids.

GAJSHIELD

Progressive Security

GajShield Infotech (I) Pvt. Ltd.
4, Peninsula Center, S.S. Rao Rd,
Parel, Mumbai – 400012,
Tel:- 022 – 66607450,
info@gajshield.com, www.gajshield.com

GajShield 1030d Features	Specification
- 10/100/1000 Interface	20/16
- Fiber Ports	4/8
- Concurrent Sessions	4000000
- New Sessions/Second	250000
- Firewall Throughput	30 Gbps
- VPN Throughput	15 Gbps
- UTM Throughput	7 Gbps
- Antivirus Throughput	8 Gbps
- IPS Throughput	11.5 Gbps
- VPN Tunnels	25000
- Configurable WAN / DMZ / LAN ports	Yes

Networking
- Transparent Mode, Route Mode, Layer3 Bridge mode
- Static IP Address, PPPoE, DHCP support
- Policy based Multiple Link Auto Failover
- Policy based Load balancing
- Policy based routing based on Application and User
- DDNS/PPPoE Client
- Policy based NAT, Port Address Translation
- HTTP Proxy Mode, Parent proxy support
- IPv6 Ready
- Dynamic Routing: RIP v1& v2, OSPF
- Multicast Forwarding

Stateful Inspection Firewall - ICSA Certified
- UserSense UTM - Policy combination of User, Source, IP address and Service
- Policy based control for Firewall, IPS, URL Filtering
- Anti virus, Anti spam, DLP and Bandwidth Management
- Access Scheduling
- Policy based Source & Destination NAT
- H.323 NAT Traversal, 802.1q VLAN Support
- DoS, DDoS, Syn Flood Attack prevention

DATA Leak Prevention
- Identifies Who is accessing, Which application, What content is sent out
- know what information has been sent in attachments on Webmail, Blogs, P2P, web uploads
- User based Policy control to prevent Data Leak
- Control over HTTP, HTTPS, SMTP, Instant Messaging
- Monitor & Block unwanted applications like P2P, Open proxies
- Real-Time Alerts, Monitoring, Reporting
- Incoming & Outgoing Mail archiving
- Block emails on sender, receipent, subject & content

Bandwidth Management
- Application and User based Bandwidth allocation
- Prioritize, shape or Limit bandwidth
- Priority based bandwidth allocation
- Multi WAN bandwidth reporting

High Availability
- Active-Passive with state synchronization
- Stateful Failover
- E-mail Alert on Appliance Status change

IM Security
- User wise allow/block IM
- Live Chat Monitoring
- User wise allow/block file transfer
- User based IM Archiving

System Management
- Web UI (HTTPS)
- Command line interface (Console, SSH)

Authentication
- Local database
- Windows Domain Control & Active Directory Integration
- External LDAP/RADIUS/TACAS+ database Integration
- RSA, VASCO secure tokens

Intrusion Prevention System
- Signatures: Default (6000+), Custom signatures
- Policy Based IPS, Anomaly Detection
- Automatic real-time updates & e-mail notification
- P2P applications signatures

VPN Client
- IPSec compliant
- Inter-operability with major IPSec VPN Gateways
- Supported platforms: Windows 98, Me, NT4, 2000, XP, Vista, Windows 7

Gateway Anti-Virus
- ZERO hour Virus protection
- Inline HTTP, FTP, SMTP, POP3, IMAP scan
- Virus, Worm, Trojan Detection & Removal
- Spyware, Malware, Phishing protection
- Automatic Real Time virus signature databatse update
- Individual user scanning
- Scan by file size

Gateway Anti-Spam
- Multiple spam classification
- Image-based spam Filtering
- Recurrent Pattern Detection
- Independent of Content, Format, Language
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient
- Subject line tagging
- Zero hour Virus Outbreak
- Quarantine folder for Spam

URL Filtering
- Inbuilt Web Category Database
- Categories: Default(85+)
- URL, keyword, File type block
- HTTP , HTTPS Upload block
- Mime type blocking
- Protocols Supported – HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Block Java Applets, Cookies, Active X
- URL Exempt/White List

Virtual Private Network – VPN
- IPSec, L2TP, PPTP
- Encryption - 3DES, DES, AES
- Hash Algorithms - MD5, SHA-1, SHA-2
- Authentication - Preshared key, Digital certificates, Xauth
- IPSec NAT Traversal
- Dead peer detection and PFS support
- Diffie Hellman Groups - 1,2,5,14,15,16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support for tunnel end points
- Hardware Token : RSA, Vasco
- VPN connection failover

Administration
- Web-based configuration wizard
- Role-based administration
- Multiple administrators and user levels
- Upgrades & changes via Web UI
- On Appliance Analytics
- Graphical real- time and historical monitoring
- Email notification of reports, viruses and attacks
- Syslog support

Complete Visiblity & Reporting
- Complete visibility of evasive applications like P2P and Skype application
- Identify the most bandwidth consuming users
- Identify application mis-use and bandwidth abuse
- Identify work or non-work related browsing
- Application Traffic , Total Traffic, Application set and application detail
- Trend Analysis of applications, users and bandwidth
- Current, Daily, Monthly, Year reports
- Intrusion events reports
- Policy violations reports
- Search Engine Keywords reporting
- Data transfer reporting (By Host, Group & IP Address)
- Virus reporting by User and IP Address

Environmental

- Operating Temperature	0 to 50 °C
- Storage Temperature	-25 to 75 °C
- Relative Humidity (Non condensing)	10 to 90%