

GajShield GS 250A

Complete Network Security for
SOHO & Remote Offices



GajShield UPTM Appliances - The next generation UTM

Threat patterns have changed over a period of time, attacks have become blended in nature & change their patterns rapidly. The new evolving threats are distributed through viruses, malware, spams, phishing, P2P, web, Email, FTP, Chat and inflicts a network to leak information, reduce application & system performance and grind them to a halt.

GajShield's UPTM appliances integrates sophisticated technology and contextual analysis to bring highest level of security, performance, control and prevents data leakage, mitigate threats and increases productivity.

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
- Dynamic Routing: RIP v1& v2, OSPF
- Multicast Forwarding

Stateful Inspection Firewall -ICSA Certified

- UserSense UTM - Policy combination of User, Source, IP address & Service
- Policy based control for Firewall, IPS, URL Filtering
- Antivirus, 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

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
- User wise allow/block file transfer
- Live Chat Monitoring
- 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

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 database update
- Individual user scanning
- Scan by file size

VPN Client

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

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
- 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 Visibility & Reporting

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

GajShield Unified Performance & Threat Management (UPTM) Appliances

Provides complete visibility into various threats and performance inhibitors allowing organization to make informed and proactive security measure. Threat Management incorporates an ICSA certified firewall, VPN, URL Filtering, Gateway Antivirus, Intrusion Prevention System and Performance Management has Traffic Analysis, Network behavior analysis, Policy based ISP Failover and Load Balancing as well as Bandwidth Management.

GajShield 250A Features	Specification
- 10/100 Interfaces	4
- Concurrent Sessions	140000
- New Sessions/Second	2200
- Firewall Throughput	110 Mbps
- VPN Throughput	75 Mbps
- UTM Throughput	30 Mbps
- Antivirus Throughput	35 Mbps
- IPS Throughput	70 Mbps
- VPN Tunnels	10
- Configurable WAN / DMZ / LAN ports	Yes

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, 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. .

User Sense

UserSense technology integrates GajShield's UPTM with enterprises' AD implementations. helps single policy engine governing application & content security.

Content Sense

Identifies Content – Including Confidential Content. Incorporates - confidential data (DLP functionality), Threat prevention, URL filtering capability. track of all uploaded data and archives it.

Context Sense

Every information has criticality based on the context. It helps in identifying the context with the help of the above five senses to categories the criticality of data. ContextSense engine enables block or allow the id to connect, only valid users connect to OP3 ids.

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 has 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.



GajShield Infotech (I) Pvt. Ltd.

4, Peninsula Centre,
S.S. Rao Road,
Parel, Mumbai – 400 012.

:- 022 - 66607450/51/52/53