

GajShield 'GS 130d' provides content aware data context, which helps you to secure your enterprise beyond next generation firewalls

CONTENT AWARE DATA CONTEXT

Maps the content of Internet applications into data context templates helping you in decision criteria to prevent threats and data leaks from your organization.

DATA LEAK PREVENTION

Intentional or unintentional leak of information is a major concern for every enterprise. 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 broadband 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 CONTENT 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
Progressive Security



The GajShield 130d appliance is targeted at high speed Internet security device for SME. The 130d appliance manages gigabit traffic with content aware data context platform providing enterprise grade security even to the smallest enterprise.

Small offices do not have enterprise grade security and are limited with basic security applications. Social media marketing has transitioned from being a hobby to a must for business of all sizes to reach out to its current and potential customers. Current grade security solutions do not understand the relevance of this medium and fail to protect enterprises from its risk. They are also unable to protect enterprises with the moving workforce on the field, beyond the perimeters of their network. GajShield 'dc series' provides hardware optimized security software, which enables to provide security features like Data Leak Prevention without compromising on security or throughputs. GajShield 'dc Series' cloud feature enable enterprises to implement the same security policies for mobile workforce without compromising the performance of their mobile devices.

With its intelligent understanding of application data, GajShield 'dc Series' identifies applications regardless of port, protocol, encryption, or evasive tactic. It gives enterprises visibility and policy control over actual applications, not just ports. It also prevents any misuse of application by limiting the use of applications for business.

With its inbuilt cloud security solution, it protects the mobile workforce of an organization from internet threats and intentional or un-intentional leaks without affecting the performance of the end device.

GS 130d FEATURES	SPECIFICATIONS
10/100 Interfaces	-
10/100/1000 Interfaces	4
Concurrent Sessions	1150000
New Sessions Per Second	31000
Firewall Throughput	3.6 Gbps
VPN Throughput	750 Mbps
UTM Throughput	675 Mbps
AntiVirus Throughput	1.1 Gbps
IPS Throughput	775 Mbps
VPN Tunnels	2000
Configurable WAN/LAN/DMZ 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 and Service
- Policy based single window control for Firewall, DLP, BYOD,
- URL Filtering & Application Control.
- 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
- Policy creation based on BYOD

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

VPN CLIENT

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

GATEWAY ANTI-SPAM

- Multiple spam classification
- Image-based spam Filtering
- Recurrent Pattern Detection on POP3, SMTP & SMTPS-SSL
- 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

AUTHENTICATION

- Support for multiple authentication schemes simultaneously
- 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, SMTPS-SSL, 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

IM SECURITY

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

APPLICATION FILTERING

- Control and Visibility of Layer 7 Applications
- Protects your Corporate users as well as BYOD devices
- Inbuilt Application Categories
- 2,500+ Applications Signatures
- Schedule-based access control
- QoS Control over Layer 7 Applications

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
- Visibility & Control over HTTP, HTTPS, SMTP, SMTPS-SSL, IM & Web Chats
- Real-Time Alerts, Monitoring, Reporting
- Mail archiving on SMTP & SMTP-SSL
- Block emails on sender, recipient, subject & content
- Monitor & Control on Social Networking Sites

ENTERPRISE CLOUD

- Visibility & Control over Internet as well as secure access to corporate network
- Enforcing of security policies on roaming users

URL FILTERING

- Inbuilt Web Category Database
- Categories: Default (85+)
- URL, keyword, File type 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
- Web GUI (HTTPS)
- Command Line Interface (Console, SSH)

COMPLETE VISIBILITY & REPORTING

- Complete visibility of evasive applications like P2P and Skype application
- Identify the most bandwidth consuming users
- Identify application mis-use and bandwidth abuse
- Reports based on user's productivity
- 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
- Separate reporting for BYOD devices.
- Email alerts for Admin activity

