

# GAJ SHIELD

Security Simplified



## Integrated Security

- ICSA Certified Firewall
- VPN (Virtual Private Network)
- Intrusion Prevention System
- Gateway Anti-Virus
- Anti-Spyware / Anti-Malware
- URL Filtering
- Bandwidth Management
- Bandwidth Profiling
- Multiple ISP Support
- Load Balancing & Auto Failover
- Strong Authentication
- Monitoring and Reporting
- Multi DMZ Support

## Features

- Enterprise Gateway UTM functionality
- Multi-layer Security Services
- Inline POP3, SMTP virus scanning
- HTTP, FTP virus scanning
- Policy based IPS
- DHCP Server
- P2P Blocking
- ISP automatic link failover
- Filters millions of URLs
- IPSec, L2TP, PPTP VPN tunneling
- Radius, Tacas+, LDAP authentication for VPN & Proxy
- Static and Dynamic NAT
- IPsec Nat Traversal
- High Availability
- PPPoE support
- Spyware protection
- ISP Load Balancing
- SNMP Management
- Remote Syslog support
- Web Management Console

Delivering powerful, easy to use, and affordable network protection

It took only a few years for network security to become a critical strategic concern for successful organizations. Yet many companies remain totally vulnerable. The equation is simple, if you have something to lose, you have something to protect.

Due to recent revolutions in broadband, mobility and Virtual Private Networks (VPNs), firewall performance is now crucial. Ultimately, however, good security is as much about protection as it is about reaping the benefits of improved information flow. In short: the safe exchange of intellectual property and confidential information is a top-line business priority.

Enterprises are subjected every day to a wide variety of Internet threats - hackers, viruses, worms, spyware, spam, phishing, botnets, Trojans, application exploits, identity and information theft. These can infect computers, reduce productivity, and increase costs. Traditional firewalls and intrusion protection products filter network traffic, but are not designed to protect against these new content-based attacks.

## UNIFIED THREAT MANAGEMENT

GajShield UTM appliances reduce complexity and protect users from multiple internally and externally generated threats by combining multiple protection measures into a single appliance.

GajShield UTM appliances is powered by ICSA Certified GajSecureOS operating system. Scalable and modular architecture enable enterprises to scale up cost-effectively and to meet expanding needs without increasing management overhead. GajShield appliances are automatically updated with the latest security intelligence to effectively stop a full spectrum of Internet threats.

## AN IDEAL FIT FOR ANY ORGANIZATION

GajShield UTM appliances are rated for the number of users, with models for large enterprise deployments as well as small office/home office (SOHO) or remote office environments.



**Security Features**

- ICSA Certified Firewall
- URL Filtering
- Virus Screening
- IM Security
- Virtual Private Network
- Spyware, Adware protection
- Intrusion Prevention System

**Network Behavior Analysis**

- Identify fast moving exploits
- Detection of rouge or stealth activity
- Detects Protocol Abuse
- Detects Bandwidth Abuse
- Give Global Visibility

# Education



**Application Performance**

- Policy based ISP Failover
- Policy based ISP Load Balancing
- Bandwidth Optimization
- Policy based Application Shaping
- QoS for VOIP services
- Managed greedy or abusive users
- Limit or eliminate rouge applications

**Analytics**

- User Specific Reports
- Real Time Monitoring
- Automated Alerts
- Historical Visibility
- IM Archiving
- Analyze the impact on your network

GajShield 800E Features	Specifications
10/100 Interfaces	2
10/100/1000	2
Concurrent Sessions	400000
New Sessions/Second	15000
Firewall Throughput	400 Mbps
VPN Throughput	75 Mbps
UTM Throughput	150 Mbps
Antivirus Throughput	240 Mbps
IPS Throughput	210 Mbps
Branch Office VPN – maximum	500
Mobile User VPN	500
Configurable WAN / DMZ / LAN ports	Yes
High Availability ( Active-Passive)	Yes
<b>Mode Of Operation</b>	
Transport Mode, Route Mode	Yes
FNAT ( Forward NAT)	Yes
Policy based NAT, Port Address Translation	Yes
Time based Scheduling of policies	Yes
<b>Networking</b>	
Static IP Address	Yes
PPoE	Yes
DHCP Server	Yes
Policy based WAN-WAN Failover	Yes
Policy based WAN-WAN Load balancing	Yes
RIP v1, RIP v2, OSPF support	Yes
<b>Gateway Anti-Virus Support</b>	
Inline POP3, SMTP Virus Scan	Yes
HTTP & FTP virus Scan	Yes
Automatic Virus update	Yes
<b>URL Filtering</b>	
Category based Blocking	Yes
URL Exempt List	Yes
URL White List	Yes
Mime Type Blocking	Yes
Groups based Scheduling	Yes
Automatic updates to the URL Categories	Yes
<b>Authentication</b>	
Internal user Auth	Yes
Radius, TACAS+, LDAP, ADS	Yes
RSA, VASCO secure tokens	Yes
<b>IM Security</b>	
User wise allow/block IM	Yes
User wise allow/block file transfer	Yes

<b>Intrusion Prevention System</b>	
Policy based IPS	Yes
6,000+ signatures	Yes
Anomaly Detection	Yes
Automatic updates for new threats	Yes
Notification via email	Yes
<b>Virtual Private Network</b>	
PPTP, L2TP, IPsec VPN	Yes
IPsec NAT Traversal	Yes
DES, 3DES, AES encryption	Yes
Manual key, IKE, PKI	Yes
Diffie Hellman Groups – 1,2,5,14,15,16	Yes
Dead Peer Detection	Yes
<b>Spyware/P2P prevention</b>	
Multi-level scanning for Spyware	Yes
Stop connection to Sypware site	Yes
Automatic updates of new threats	Yes
Deny Access to Kaaza, Bit Torrent, Gnutella	Yes
<b>Bandwidth Management</b>	
Prioritize, shape or Limit bandwidth	Yes
Guaranteed bandwidth	Yes
Maximum bandwidth	Yes
Priority based bandwidth allocation	Yes
<b>System Management</b>	
Web GUI ( HTTPS), SSH console	Yes
Remote Syslog, SNMP support	Yes
Multi-Role Administrators	Yes
Firewall rules, System Backup/Restore	Yes
<b>Reporting</b>	
Security reports include Firewall, IPS & VPN	Yes
Real time reporting of bandwidth and users	Yes
Policy violation reporting	Yes
Virus filtering reporting	Yes
Bandwidth usage User, ISP & Application wise	Yes
URL Filtering reporting	Yes
Historical reporting	Yes
Internal HDD	Yes
<b>Certification</b>	
ICSA Certified	Yes
CE/FCC	Yes