

## GajShield Case Study - SBI Capital Markets

"How a leading finance company used GajShield to protect their network and provide online broking/ trading through VPN Access"

### • Organization

SBI Capital Markets



### Mr. Vinod Jha

(Associate Vice President  
- Technology )

" GajShield is the only company to offer everything in e-security in one suite. All updates are automatic through their centralized server. The product is wonderful compared to other products available in the market, with comparison on cost v/s features. Their after sales service is excellent and the best thing is that round the clock you just call them and they give you necessary solutions to the queries you have. "

### • Customer Profile

**SBI Capital Markets Ltd. (SBICAP)** is amongst the oldest players in the Indian Capital Markets and for a number of years the bank has achieved a dominant market position in the Indian Primary Capital Markets. Over the years, anticipating the changing needs of clients in a rapidly opening economy, SBICAP has evolved an array of advisory services in almost all sectors of the economy. SBICAP, known for professionalism and business ethics, provides the full range of Investment, Advisory and Financial Services under one umbrella.

A pioneer in privatization in India, SBICAP has established itself as a leader in providing financial and advisory services in core sector and infrastructure industries.

**As regards its capital markets related operations, SBICAP is registered with the Securities Exchange Board of India for its various services.**

### • The Requirements

Being a part of SBI group and a leading financial company security was paramount at SBI Capital Markets. Looking at the increased threats of intrusions, viruses, worms, trojans and blended attacks with the network being connected to the internet Mr. Vinod Jha, AVP- Technology – SBI Capital Markets Ltd, actively started scouting for Security solution for protecting their network from Internet-borne viruses, malicious hacker attacks and VPN Access.

SBI Capital Markets uses Lotus mail server as email is the preferred mode of communication it needed scanned for viruses & Trojans at the Gateway itself. Their network is managed by a team whose job is to manage network, security and applications. SBI Capitals has around 15 branch offices, which needed to connect to head Office to do online trading in secure manner without having to invest in high cost VSAT, Leased Line or Single ISP VPN connections.

Being a large organization with critical applications they were looking for a security solution, which would be robust, high performance and provide utmost security.

SBI Capital evaluated different Security solutions like Checkpoint, Checkpoint/Nokia, Sonicwall, StoneGate & Astaro along with GajShield. GajShield was selected based on Price to Feature comparison. GajShield at that time was one of the few products available which had Stateful Inspection Firewall, IPS, Gateway Anti-Virus, URL Filtering, VPN and Bandwidth Management integrated in one security appliance.

SBI Capital did a proof of concept (demo) along with checking references from experiences of other customers before freezing on GajShield Security Appliance.

### • The Solution

SBI Capital Markets implemented GajShield Integrated Security Appliance – GS 5100 at the Head office's Internet Gateway to ward of hackers and protects their network from viruses, spywares etc.

**GAJSHIELD**

Progressive Security

**CHALLENGE:**

Stop threats like data leak, spam, phishing, intrusions, viruses, improve network performance, free up bandwidth for business purposes, and gain visibility of application traffic. Deploy appropriate levels of Application visibility and control, Data Leakage Visibility and control.

**BENEFITS:**

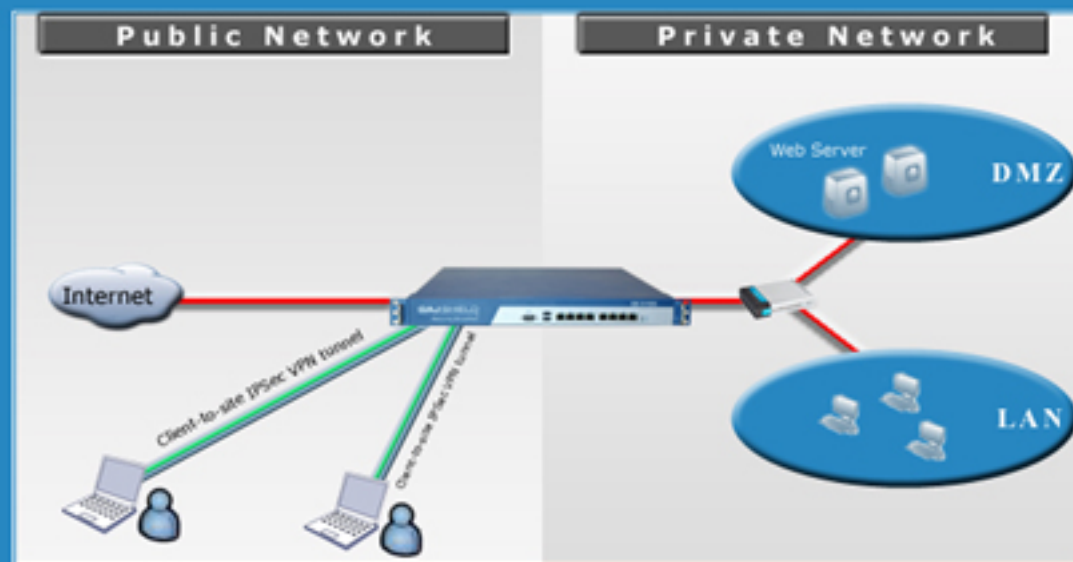
- Granular visibility of who is using what
- Control over Data traversing out of network
- Reduced operational costs
- Increased Application and user productivity
- Ability to enforce and monitor appropriate use policies

Firewall policies were defined to allow access for specific applications from the corporate LAN network to the internet and vice versa. Intrusion Prevention System was deployed to deeply inspect the packets for identifying malicious packets and intrusions. As they wanted to expose some of the web based application to the internet, a DMZ (De-Militarized Zone) was created and a secure reverse Proxy redirector was set up. The reason for this architecture was to ensure that no user from the internet would connect to the Database server directly.

URL Filtering was implemented enabling the IT staff to set and enforce web access policies across an entire network without creating huge hurdles to deployment or maintenance. Groups were created based on department, seniority etc and they were provided with time based browsing access. SBI Capital Markets felt that allowing users to upload files to internet could cause serious security concerns and hence all users were disallowed to do upload files.

Client-to-site VPN tunnels were established with branch office to allow them to use Financial technologies ODIN server for online trading. To authenticate the users, IKE based certificate authentication was used. These branch offices were allowed to only access the ODIN server on specific ports only. Hence by using certificate based authentication if a user would leave the organization the administrator can revoke the certificate issued to that particular user and from then on that particular user would not be able to connect via the VPN. The encryption used was standard based 3DES (168 bit).

Gateway Anti-Virus was implemented hence all the emails are scanned for viruses and only virus free mails reach the Lotus Notes server. Similarly the Browsing and FTP traffic are also being scanned to protect the users from viruses.



- **About GajShield**

GajShield is a leading innovator of UTM appliances offering powerful & integrated protection, Data Leak Prevention, Application, user visibility & control, granular policy definition, zero day protection. GajShield delivers pro-active security to networks delivering real-time protection against fast moving threats like spyware, phishing, masked applications like Malware, Adware, P2P, Instant Messaging and provide visibility and control over content going out of an organizations network. GajShield UTM appliances are used by more than 1000, Small businesses, enterprises, educational and government institutions to protect their networks proactively. For more information call 91-22-6660 7450 or email [info@gajshield.com](mailto:info@gajshield.com)