



## **Application Note:**

### **Adding Network Security For Windows Based ATM's And POS Terminals**

---

*Designed for Financial institutions with ATMs and Point Of Sale (POS) Terminals, the JBM Gateway products provide the added network security needed to protect vulnerable windows-based terminals from hackers and viruses.*

---

### **IP Connectivity Solution**

Over the years, networking of ATM/POS terminals has always been a challenge. With the introduction of so many different manufacturers for terminals and host systems, some form of standardization was necessary in the industry. Demands have prompted most manufacturers to move away from OS/2 and other proprietary operating systems and adopt Windows as a standard operating system. The Windows operating system offers the industry some form of standardization and IP networking capabilities but with a trade off. Windows offers manufacturers increased flexibility with plug and play capabilities, which reduces their development cost; however, this beneficial trade-off for the manufacturers has created a tremendous security risk for financial institutions.

Unfortunately, Windows has been the target of many hackers for years. Hackers of all types are constantly trying to break into corporate networks for various reasons. Whether it's the teenage under achiever or a high tech thief, hackers threaten your system.

In the past, ATM's and POS devices were immune from this threat since most terminals had proprietary operating systems and were on separate leased lines. But now, with the migration of ATM's and POS terminals onto the corporate IP network and the introduction of Windows, the threat of these terminals being hacked into is extremely real and does warrant some level of concern.

Financial institutions deploying these new Windows based ATM/POS terminals in their network are now faced with security risks similar to those that threaten the existing enterprise network. Some manufacturers are finally responding by supplying a software firewall option with new systems, but a software firewall is only as good as the integrity of the underlying operating system.

The reality is for firewall software and Windows security to be effective, timely and complete patch management of all terminals is constantly required. This obviously creates a complex problem for management and technicians to deal with on a daily basis, especially if the financial institutions have thousands of terminals. Unfortunately, even with good patch management, most patches aren't released until after a new threat has been identified, leaving terminals vulnerable for sometime. With new threats being introduced daily, the security risk and manageability problem of patches will always exist.

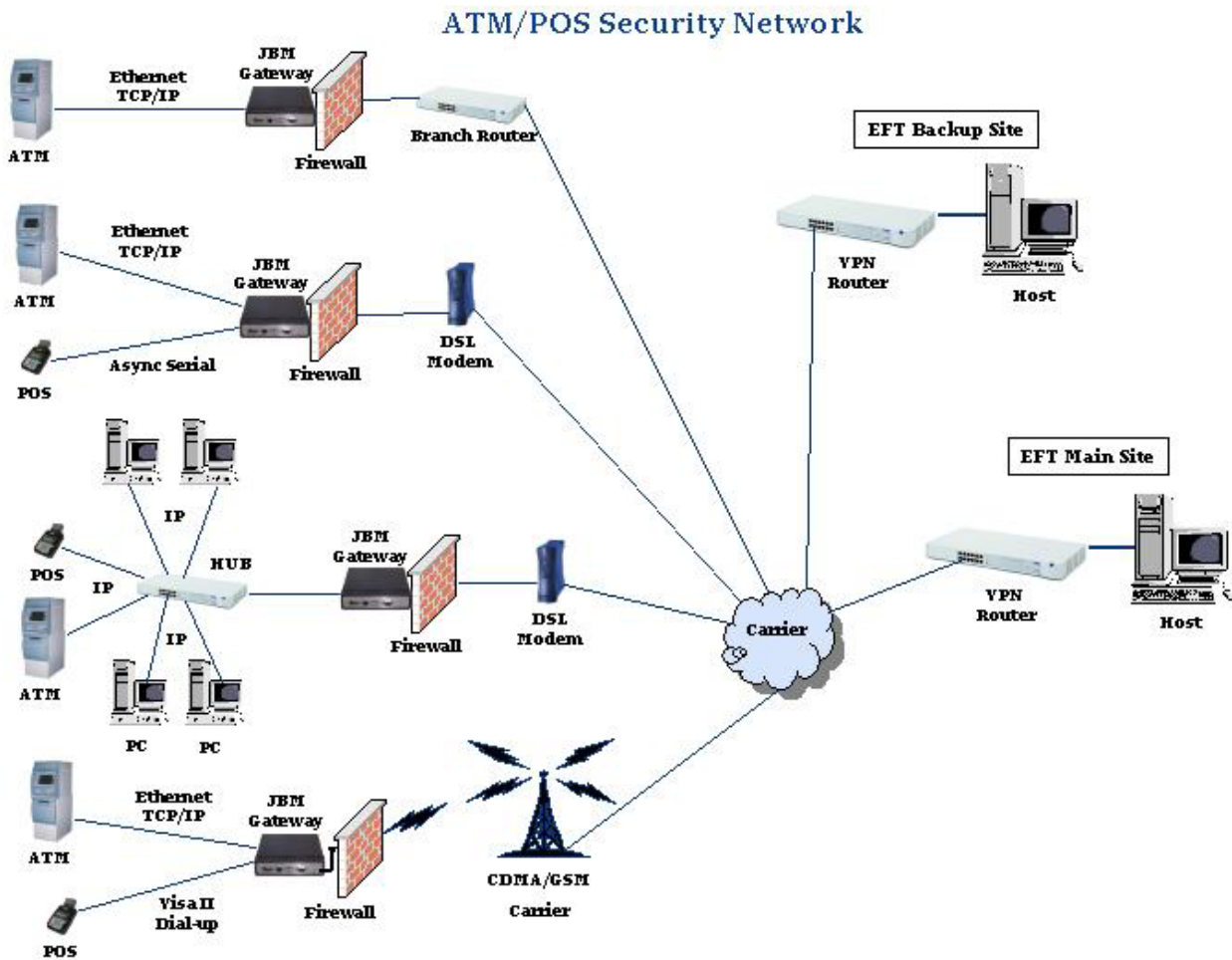
IT security experts agree that locking out an intruder before they can reach the terminal is the best and easiest way to secure a terminal. To do that, a hardware based solution that provides VPN and firewall features is needed and JBM Electronics has that solution. With a low-cost Linux based hardware solution from JBM Electronics, IT managers can drastically reduce their security risk.

The Linux-based Gateways can now offer IT managers a low-cost solution for protecting their most important assets. The hardware-based Gateways provide Virtual Private Network (VPN) Client, 3DES encryption, SSL Client, Transparent Bridging, In-line Intrusion Protection, Network Address Translation (NAT), Stateful Inspection and an extremely flexible Firewall. The JBM Gateways are standard-based and are compatible with any industry standard based VPN router or server.

### Operation

All of the JBM Gateways offer security features and are easy to install with zero impact on the terminal's software or configuration. A change to the terminal's software is not required, which eliminates the requirement for re-certification of the terminal's application. The Gateways are self-contained and connect to the terminal through the Ethernet, Serial, or Dial-Up Modem ports. The network Ethernet port connects to the LAN, Branch Router, DSL Modem, or through a wireless PCMCIA card. Installation of a JBM Gateway is a simple process. Simply drop the Gateway in between the terminal and the network. The Gateway can be configured for VPN or SSL, 3DES encryption, and Stateful firewall.

The Linux Operating System adds an additional layer of protection. The introduction of a second, dissimilar operating system creates a heterogeneous environment, which can frustrate the efforts to compromise, the terminal.



**ATM/POS Security With VPN and Firewall**

## Features and Functionality of the Gateway Products

### Security Features

ATMs and POS devices are open for attack by hackers and JBM realizes this, so we have added additional security by incorporating VPN capabilities with Firewall functionality into our products. We provide a Linux based hardware solution, which is a secure way of preventing hackers from retrieving critical transaction data. Our Gateway products are easy to install; and in most cases, no reconfiguration of the ATM or POS device is required. The Gateways include:

- Stateful Inspection Firewall
- VPN Client/Server
- SSL Client/Server
- 3DES Encryption
- Dynamic Keys
- DHCP Client/Server
- PAT for IPsec
- NAT
- PPP and PPPoE
- Transparent Bridging Capability

### Router Functionality

The Gateway Series offers full IP routing functionality supporting Static, RIP, OSPF, and BGP routing. The Gateway also supports DHCP, DHCP client, PPP, and PPPoE for broadband users.

### Compatibility

Compatibility is never an issue with the Gateway since JBM uses all standards based protocols. Interoperability between JBM and other router/VPN vendors is fully supported.

### Dial Backup

The V.92 modem can be used for dial backup in case the primary link goes down. This feature provides reliability for a customer's most important data. Also, the V.92 Modem can be used as a primary dial out circuit.

### Management

The JBM Gateways can be configured through CLI Command entered via console port or Telnet. The Telnet connection provides command, control, and monitoring of the Gateways. SNMP is supported with SNMP Traps providing notification of major events in the Gateways. SSH is also supported for security of the management connection. Extensions to the Telnet or SNMP commands are available as a special order

### Fallback Routing

One of the Gateway's key features is the ability to perform fallback routing. Fallback routing enables a user to configure alternate paths to the host or to several hosts for disaster recovery. The fallback path can be to a different IP server or with a properly equipped Gateway, through a different connection such as a cell or dial modem.

### Wireless Support

Some of the Gateways provide an integrated cell modem for CDMA or GSM/GPRS wireless communications. The wireless connections provide simple, low-cost communications to the network. All that is required to get connected is a carrier account and the Gateway.

### CO-Modem Support

All of the modems support both async Legacy protocols and async PPP. The CO-Modem provides a dial tone for dial-only async devices. This dial tone simulator and associated modem allows for a simple, non-disruptive connection of these devices. The Gateway can route the connection based upon the data or phone number (DTMF recognition). The V.92 modem component of the CO-Modem can also be used as a normal async modem.

### Frame Relay

The Gateway expansion cards provide the option for a 56K DSU or T1/E1 DSU with full Frame Relay or X.25 support. The software supports up to 100 Logical Channels (DLCIs) with flow control using individual Committed Information Rate (CIR) for each DLCI. Our Frame Relay support is certified to ISO and ITU standards by major network laboratories and is compliant with ANSI T1.617 Annex D, Q.933 or LMI Link Management. The ROLAND Laboratory certifies the X.25 to European NET2 standards.

### Protocol Conversion

All of the JBM Gateway products support protocol conversion, and when it comes to protocol conversion, JBM is the industry leader with over 50 different protocols in our software library. Protocol conversion is necessary when converting a host to IP or introducing a new Transaction Switching System. Our Gateway products provide our customers with an efficient and non-disruptive migration to IP. The Gateways support conversion of most financial protocols. In addition, the Gateways support Data and Header manipulation allowing seamless access into many host systems. Below is a list of the most Common Protocols Converted to TCP/IP:

- Bisync 3270
- SNA/SDLC
- Poll Select TC500
- Uniscope
- Bisync 2780/3780
- Visa I & II

For more information, please contact us.