Bloomberg

Transport and Security Specification

19 February 2009
Version: 3.6

Table of Contents

Overview

This document provides network transport and security specifications for the BLOOMBERG PROFESSIONAL® Service.

Bloomberg Access Router

One or more Bloomberg Access Routers are installed at each Client Site. These routers provide the following benefits:

- **Enhanced Data Delivery**
  The Bloomberg Access Router uses the IP network protocol and addressing scheme along with a dynamic access list to deliver data to and from the Bloomberg Private Frame Relay/ATM Network.
- **Seamless Integration**
  Installing a Bloomberg Access Router requires minimal configuration changes and will not impact Client Network topology or performance. Bloomberg requires a CAT5 UTP cable run from the client hub, router or firewall to distribute data to the Bloomberg workstations.
- **Security**
  The Bloomberg Access Router communicates only to the private Bloomberg Network. This is ensured through dynamic access lists on each Bloomberg Access Router in addition to fixed virtual circuit path definitions based on the underlying Data-Link protocol SSL.

The Bloomberg Access Router may reside outside Client Site firewalls to further ensure Client Site LAN integrity.

All connection requests originate from the BLOOMBERG client applications running on the end-user PC. Bloomberg does not send unsolicited connection requests from outside the Client Network; thus, connections are initiated from the Client PC to the Bloomberg.

The BLOOMBERG PROFESSIONAL® Software utilizes both UDP and TCP connections and contains various components and applications such as Bloomberg API, Tradebook, FX and multimedia that utilize multiple ports.

In the event of a Bloomberg hardware/circuit failure, an alternate path is established on the Host end to transport Bloomberg data. For locations with multiple Bloomberg routers and E1/T1 circuits, we support RIP v1 and v2, VRRP and HSRP for redundancy between routers.

Client Site and Desktop Requirements

This section outlines the preferred and minimum desktop requirements to install and run the BLOOMBERG PROFESSIONAL® Service.

DEVICE	RECOMMENDED
Processor	Intel core 2 Duo 2.8 GHZ or AMD Athlon 64X2 2.0 GHZ
Operating System	Microsoft Windows XP Pro Service Pack (SP) 3
Memory:	2 GB RAM
Disk Space:	Minimum 4 GB of free hard disk space
Video Card:	Dual port graphics adapter with 128Mb of memory, 64Mb per port, supporting Direct X version 9.x
Display Settings	1280x1024x32bit or higher
Network Adapter	Integrated network adapter with TCP/IP Services enabled
Software	Microsoft Office 2003 Service Pack 1, Internet Explorer 7
Printer	Local or Network printer that is PCL5 compatible
Monitor	17-inch monitor
Audio	Integrated audio adapter
Keyboard	Available USB port to accommodate the Bloomberg Keyboard

Network Requirements

The following section outlines Client Network requirements to access the BLOOMBERG PROFESSIONAL® Service:

- Ethernet or Token Ring network that supports IP
- CAT5 UTP cable from the client hub, router or firewall to the Bloomberg Access Router
- IP address and subnet mask for the local Ethernet interface on the Bloomberg Access Router (Bloomberg will provide an IP address for clients without an existing IP Address scheme)

Capacity and Bandwidth Requirements

The following table outlines recommended bandwidth requirements per number of Bloomberg connections:

Customer Bandwidth Requirements [1]			
Region	**Terminal Count**	**Router Quantity**	**Tail Circuit Additional T1s/E1s should be diverse**
United States and Tokyo (T1)	1 -8	1	T1
	9 – 24	2	2 x T1 [2]
	25 – 64	2	4 x T1 [2]
	65 – 115	2	6 x T1 [2]
	116 +	2	2 or more DS3 [2]
Asia Latin America Australia and Europe (E1)	1 - 8	1	E1 [2]
	9 - 32	2	2 x E1 [2]
	33 - 84	2	4 x E1 [2]
	85 - 150	2	6 x E1 [2]
	151 +	2	2 or more DS3 [2]
Rate: T1 = 1.544 Mbps ~ E1 = 2.048 Mbps			

[1] The bandwidth matrix is intended as a guideline. Additional bandwidth may be required based on usage.
[2] In the event of a hardware failure, the configuration allows for a single router to accommodate the necessary traffic on a temporary basis until the issue is resolved.

Source and Destination Ports

The BLOOMBERG PROFESSIONAL® Service uses the following source and destination port numbers (destination is from the customer perspective):

UDP Source Ports	UDP Destination Port
48129 — 48137	48129 — 48137

TCP Source Ports	TCP Destination Ports
8194 — 8395 and 1024 — 5000[1]	8194 — 8198
8194 — 8395 and 1024 — 5000[1]	8209 — 8220
8194 — 8395 and 1024 — 5000[1]	8290 — 8294

From the Bloomberg Connection Wizard (CONN <GO>) deselect the box titled “Use specific TCP port(s)" to allow for toggling between the source port range of 1024-5000. Selecting this box restricts the source port range to 8277-8294.

[1] This is the Microsoft default for ephemeral ports.

Network Address Specifications

The Client PC can connect to the BLOOMBERG PROFESSIONAL® Service over a private connection or over the public Internet. The port requirements are the same in both cases; however, the registered network address ranges of the Bloomberg servers differ.

Private Bloomberg Network

For a private connection, the Client PC must be able to connect to the following Bloomberg subnets:

208.134.161.0	using the subnet mask of	**255.255.255.0**
205.183.246.0	using the subnet mask of	**255.255.255.0**
199.105.176.0	using the subnet mask of	**255.255.248.0**
199.105.184.0	using the subnet mask of	**255.255.254.0**
69.184.0.0	using the subnet mask of	**255.255.0.0**

The above network prefixes are advertised using RIP v1 or v2 from the Ethernet ports of the Bloomberg Access Routers installed at the Client Site. Alternatively, clients wishing not to receive RIP can configure their networks to route statically to the above prefixes through the Ethernet ports of the Bloomberg Access Routers.

Internet

For Internet connections, the Client PC must have Internet connectivity and the ability to resolve the following DNS names:

- pdir.bloomberg.net
- sdir.bloomberg.net
- api1.bloomberg.net
- api2.bloomberg.net

Additionally, the Client PC must be able to connect to the following Bloomberg subnets:

160.43.250.0	using the subnet mask of	**255.255.255.0**
206.156.53.0	using the subnet mask of	**255.255.255.0**
205.216.112.0	using the subnet mask of	**255.255.255.0**
208.22.56.0	using the subnet mask of	**255.255.255.0**
208.22.57.0	using the subnet mask of	**255.255.255.0**
69.191.192.0	using the subnet mask of	**255.255.192.0**

Bloomberg Anywhere Non-Configured

BLOOMBERG ANYWHERE allows you to access your Bloomberg login from any desktop or Internet based terminal, ANYWHERE in the world with the same settings and defaults you have on your own desktop.

Basic Connectivity Requirements

The following is a list of minimum requirements for Bloomberg Anywhere Non-Configured running on Intel PCs with Microsoft Operating Systems:

Network Requirements

- HTTP Port 80 must be allowed to access any proxy server or firewall
- HTTPS Port 443 must be allowed to access any proxy server or firewall
- Broadband Internet access or better

Hardware Requirements

- Pentium III 1.0GHz processor or better
- Windows 98SE or better
- 512MB RAM
- 20MB of free hard drive space for the installation of Java Web Client, temporary Java files and temporary Internet files
- B-unit for additional authentication to complete the login process

Software Requirements

- Internet Explorer 6 with Security set to medium or lower
- ActiveX enabled
- PC must allow JavaScript, Cookies and pop ups to install the Citrix Client
- VeriSign Root certificate installed
- Java Platform 1.4.2 or better
- Citrix or Java Client

A customer may choose to install the Citrix Full Program Neighborhood version 7.0 or better rather than accepting the download of the Citrix or Java Client. For an administratively disabled PC that does not allow for the installation of the Citrix Web Client, Bloomberg Anywhere Non-Configured will utilize Java.

Technical Specifications for the Connection Process

Bloomberg Anywhere Non-Configured uses a Citrix MetaFrame environment to achieve connectivity to Bloomberg. A Citrix server emulates the user's mouse movements and keyboard commands, processes the user's interactions locally on the server and "paints" the results back to the user's desktop. These servers are on a private Bloomberg network and are not accessible from the Internet.

To access Bloomberg Anywhere Non-Configured go to http://www.bloomberg.com and click the Bloomberg Anywhere button which initiates an HTTPS connection to https://bba.bloomberg.net.

A Security Alert dialogue box will inform the user: You are about to view pages over a secure connection. Any information you exchange with this site cannot be viewed by anyone else on the Web.

Click OK to initiate a detection process where the Citrix Web Interface (CWI) used for initial connectivity attempts to detect which type of Client the user's PC has and also checks that service packs and any other updates are correct for a successful connection.

The user is then prompted to enter login credentials, which include login name, password and a B-Unit screen sync.

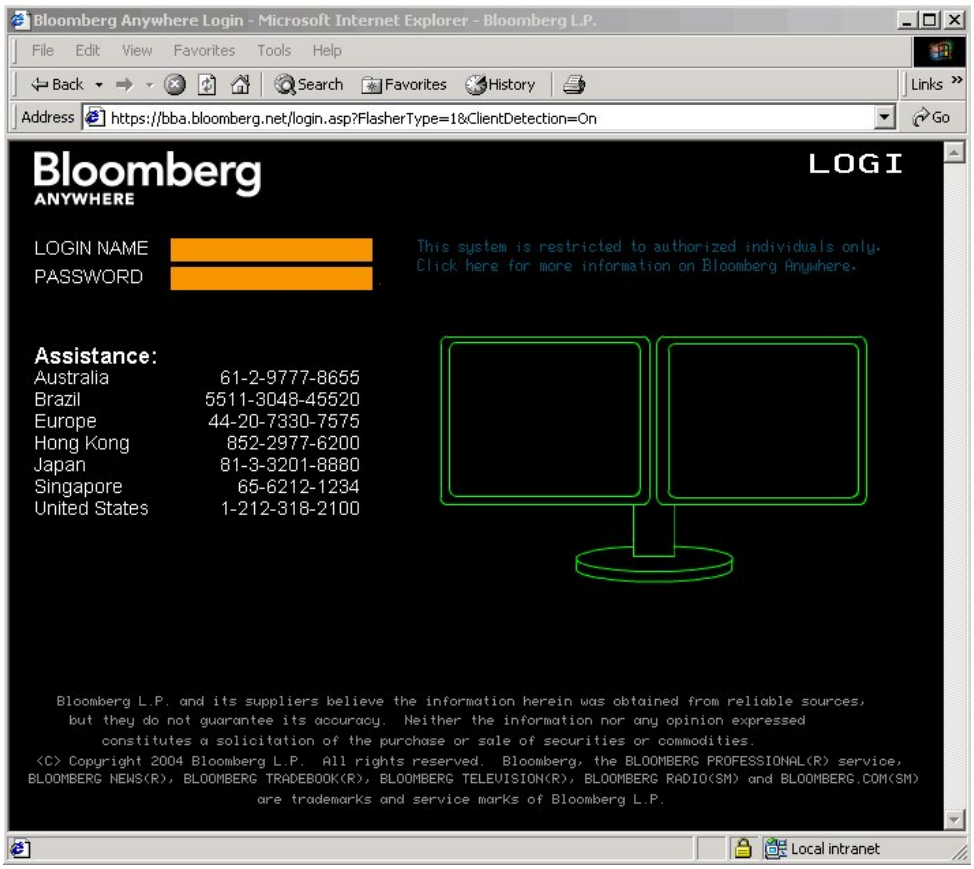

Figure 1 Bloomberg Anywhere Login

1. The CWI authenticates the user's credentials with Bloomberg. If a Citrix Client 7.0 or better is detected, Bloomberg Anywhere Non-Configured will use this Client to connect. If not, the CWI will use a Java Client to connect and push the Citrix ICA Web Client (minimal install) for the next connection.
2. The Java Client is pushed to the Temporary Internet Files folder on the user's PC. Therefore, it is necessary for a user to have full administrative rights to this folder. The first connection will use the Java Client and subsequent connections use the Citrix Web Client. Once either of these processes is completed a session is established at TCP port 443/SSL to a Citrix Secure Gateway (CSG).

Security Features for Bloomberg Anywhere Non-Configured

Bloomberg's software and systems architecture are under continuous information and software security review by a dedicated internal team of software security and information security personnel. Bloomberg also contracts with outside suppliers and auditors for security reviews and audits. Following are specific security features:

- All communication is encrypted and available only through SSL.
- Initial connections are to a secure website utilizing a Citrix Web Interface (CWI) product that is further enhanced, hardened and secured by Bloomberg.
- Authentication to the web interface is through Bloomberg User Name, Password and B-unit.
- The BLOOMBERG PROFESSIONAL® is the only application published by the Citrix environment. This is the same software installed locally on client PCs worldwide.
- The Citrix Presentation servers (MetaFrame XP) that run the BLOOMBERG PROFESSIONAL® are on private IP addresses that are not accessible from the Internet. All communication to these servers is through the Citrix Secure Gateway using TCP 443/SSL.
- In order to take advantage of enhanced security features, the Bloomberg Anywhere Non-Configured Microsoft environment is entirely Windows Server 2003 based.
- Connectivity from the Citrix Presentation Servers and the Bloomberg network are secured and firewalled in the same manner as all existing configured Bloomberg connections using private network or Internet. Client side X.509 certificates, SSL based communication and Bloomberg proprietary session authentication secures this connectivity.
- All of the Internet facing DMZs utilize the same infrastructure as existing Bloomberg Internet facing DMZs. Both firewalls and intrusion detection systems are utilized. These systems are continuously operated and monitored by two separate teams (one internal and one outsourced).
- User activity logs such as login attempts, source IP addresses, Serial Numbers used and Citrix Servers used are coupled with existing BLOOMBERG PROFESSIONAL® software logs and recorded, correlated and processed through use of various management systems. Both proprietary and vendor specific systems such as Citrix's CMC and Microsoft's IIS logs are utilized.
- All traces are removed if bitmap caching is off; however, if bitmap caching happens to be on, the cache is encrypted (not in plain text).
- Citrix's bitmap caching is disabled server side to ensure that traces of a user's activity cannot be removed from a remote computer that was used to access the BLOOMBERG PROFESSIONAL® Service.

Email Security

Bloomberg protects end-user Internet mail data utilizing the following measures:

- The Bloomberg proprietary message system transmits Internet email using several Bloomberg maintained SMTP Gateways. These Gateways also support other messaging protocols such as X.400, X.500, and SMTP/MIME. All incoming and outgoing email targeted for the Bloomberg message system must pass and be authenticated through these Gateways. All users are first authenticated on the Bloomberg Mail Gateways, residing on the private Bloomberg network.
- All data (including mail data) must traverse the Bloomberg Host network before exiting to, or entering from, the Internet. This Host network employs a Bloomberg proprietary protocol to send and receive data. Data packets foreign to this protocol format will not be able to enter the Bloomberg Host Network.
- All Internet email traverses Bloomberg's private network only and is then sent to the Bloomberg proprietary mail system (**MSG<GO>)** for user retrieval.
- Users accessing a Bloomberg session through the Internet must also traverse and be authenticated on the Bloomberg SMTP Gateways.
- All Internet messages targeted for the Bloomberg message system are scanned for known viruses before entering the private Bloomberg network. If a virus is found, the infected file is removed and the intended recipient is notified via an incoming Internet message.
- All Bloomberg and Internet messages traversing the Bloomberg private network are stored on proprietary mail servers thus prohibiting any unauthorized modification of data.
- Bloomberg maintains and updates every 24 hours an X.500 directory of all valid users, including their unique login name and associated Customer and Firm number. All users and messages are authenticated against this database outside of the Bloomberg Firewall. If a message does not authenticate against this directory / database, it does not enter the private Bloomberg network.

Socks5 Proxy Server

For customers utilizing a SOCKS5 Proxy Server, the Client PC will communicate only with the proxy server and the proxy server will in turn communicate to the Bloomberg servers.

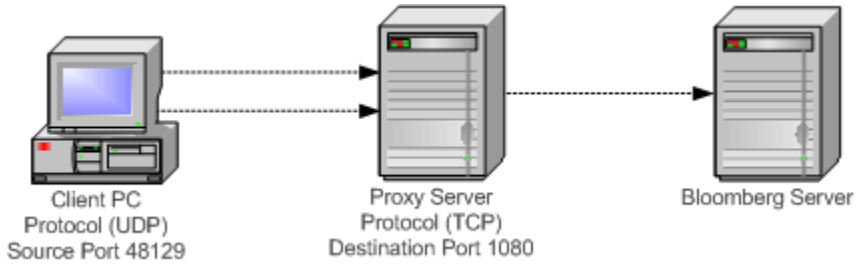

Figure 2 Example of the Client PC to Proxy Server Communication

Client to SOCKS5 Proxy Server Communication

The Client PC will send TCP communication to port 1080 on the SOCKS5 Proxy Server. Upon initial connection, the Client PC will select the source port for this connection. This destination port 1080 may be different if the proxy server administrator has configured the proxy server to run on a different port. The communication back from the proxy server to the Client PC will be from port 1080 to the port selected by the Client PC based upon server configuration.

The Client PC will also send UDP communication to the Proxy Server. The source UDP port for this communication will be 48129, and the proxy server will pick the destination port upon initial connection. This destination UDP is picked from a range defined by the server administrator. The communication from the proxy server to the Client PC will be from the port picked by the proxy server upon initiation to UDP port 48129.

In order for the Bloomberg software to connect with the proxy server, type CONN <GO> within the Bloomberg application to open the connection box. Under the settings tab, check the box “Connect through a SOCKS Version 5 Proxy Server” and enter the appropriate DNS or IP addresses. To allow API/DDE connectivity, click Start Button\Programs\Bloomberg\BBComm Configuration to open the configuration window. Click the SOCKS5 button and enter the appropriate DNS or IP addresses.

The communication between the SOCKS5 servers to Bloomberg is the same as defined above for PC to Bloomberg communication, except the source ports used will be defined and limited by the server administrator.

Virtual Private Network (VPN)

Customers may choose to use a VPN for traveling users which allows users to connect to the Client Network using an Internet connection. In order for the application software to connect over a VPN connection, type CONN <GO> within the Bloomberg application to open the connection box. Under the settings tab, check the “Connect to Bloomberg using a Private IP Network” and “Use any local IP address” boxes. The VPN server must be configured to forward the network traffic to the Bloomberg Access Routers. In some cases, the VPN connection must also pass through a proxy server; therefore, the proxy settings need to be configured as well.

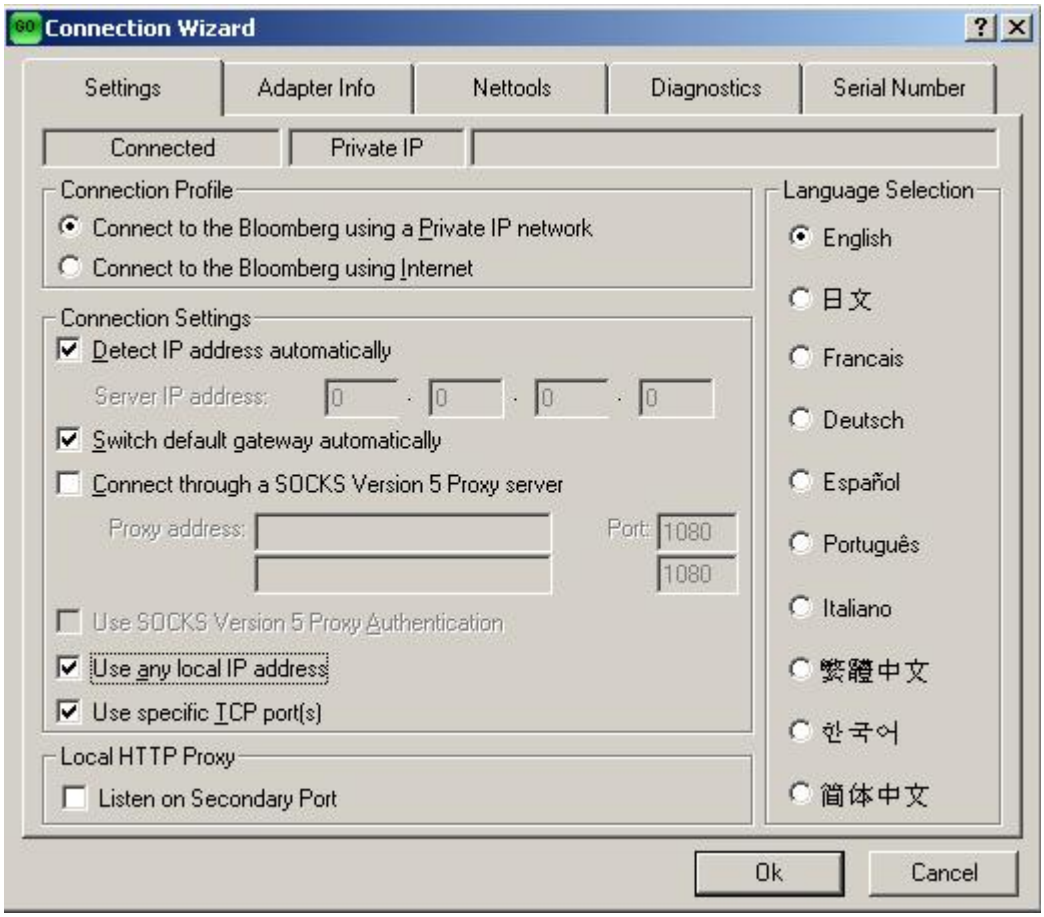

Figure 3 Connection Box (CONN <Go>)

Summary Illustration

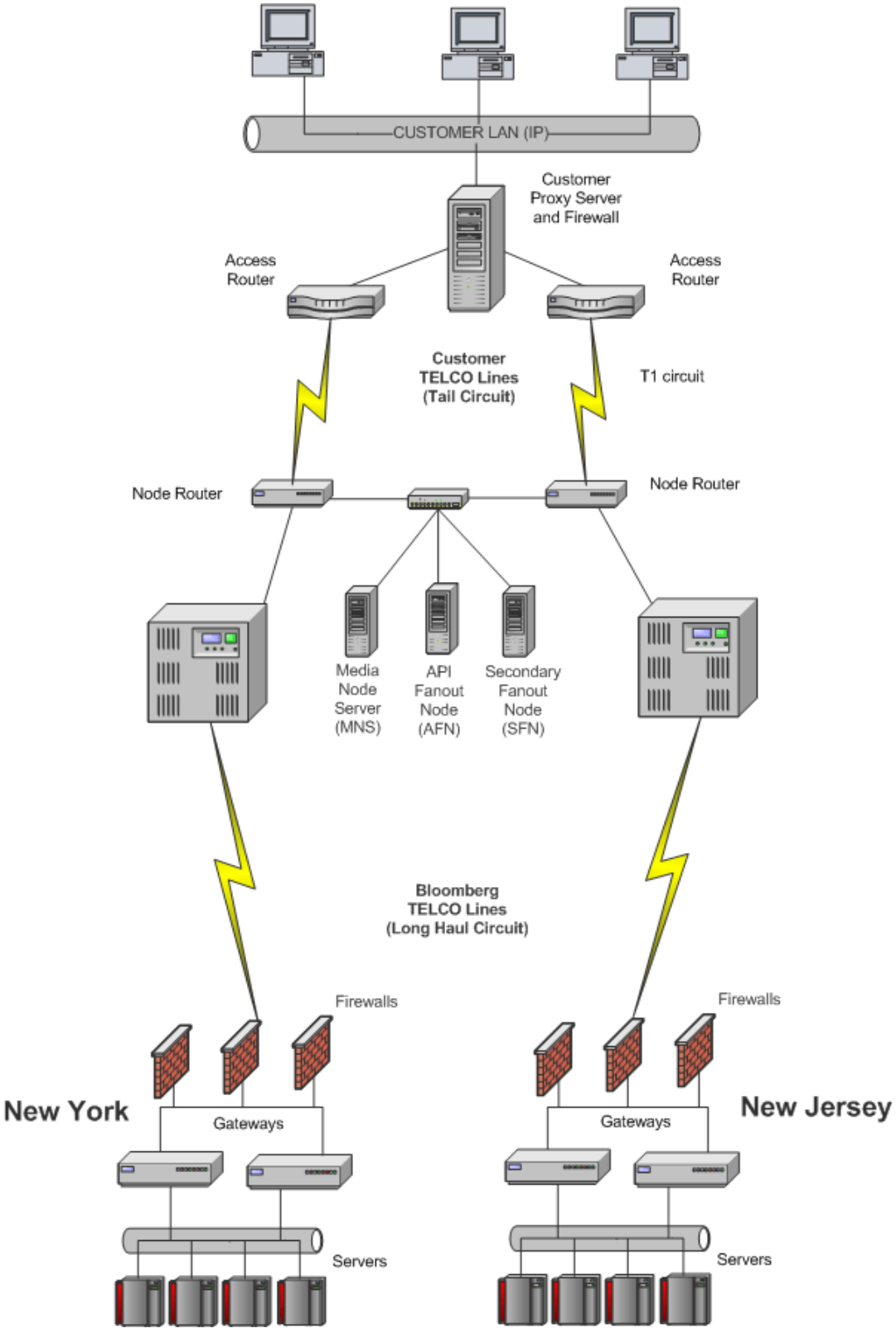

Figure 4 Bloomberg through a Customer Firewall