
FAT Pipe
MPVPN
WHITE PAPERS

FatPipe Multi-Path VPN™ A Router Clustering Device for VPN Infrastructures

Virtual Private Networks are becoming one of the most popular means of communication among companies to achieve higher levels of productivity, service, and cost savings. VPNs use shared data networks that are usually IPenabled (the Internet being the most popular), to securely transfer information among two or more sites for enhanced communication and productivity. Business applications such as ASPs, Intranets, Extranets and Thin Clients typically run over VPNs.

The development and implementation of wide area network (WAN) technologies in general have been steadily increasing due to the growing need for remote LAN access. As businesses become more global, technology becomes a greater tool for increasing productivity and lowering costs. Remote access needs are now mission critical for a majority of businesses.

Considering the growth and popularity of VPNs, FatPipe Networks developed Multi-Path VPN. Multi-Path VPN takes any VPN and makes it up to nine times more secure and up to three times more redundant and reliable, while providing up to three times the speed. Multi-Path VPN is compatible with IPsec protocol and can be seamlessly integrated into any network because it is hardware and technology independent.

The need for FatPipe Multi-Path VPN is described in the next section. The remainder of the White Paper will review Multi-Path VPN's main features, benefits, and its application for business.

VPN Popularity

VPNs are a cost effective and efficient way to transmit data. The number of small and large companies using VPN as a communications tool has increased steadily every year.

According to Frost & Sullivan, the U.S. revenue forecast for IP enabled VPNs has increased two-fold between 1998 and 2000 from a market of $3.54 billion in 1998, and is expected to double again by 2002, reaching $18.77 billion in 2004.

The Need for Secure, Redundant and Fast VPNs

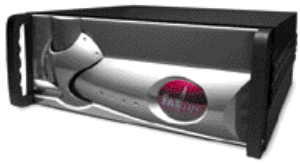
As data communications models evolve using VPN technology, redundancy of WAN infrastructures at the client end becomes an essential issue. It's simple: when the connection to the VPN goes down, offices cannot communicate and customers and remote users cannot access Intranets, e-mail, database, or other internal servers. In other words, productivity is lost.

In recognition of this fundamental shift in business where critical data is stored in remote locations instead of local area networks, FatPipe Networks has developed Multi-Path VPN, a router clustering device that provides high redundancy, reliability and speed for VPNs. By transmitting data over two or three lines together, Multi-Path VPN provides increased speed, reliability and redundancy as well as added security for bi-directional data transfer, without the need for complicated BGPprogramming.

Current VPN Drawbacks

VPN technology has made improvements in addressing concerns about security and sharing of private information over a public network such as the Internet. As a result, more companies are integrating VPN technology into their business models. However, significant drawbacks still exist using the current VPN model. The most common problems associated with VPNs are the following:

- Single points of failure: Intermittent Router, CSU/DSU, last mile failure, ISPand backbone failures
- Security breaches
- Poor WAN infrastructure



Single Points of Failure

When router, CSU/DSU, last mile connection, and ISPor backbone failure occur, business is disrupted and can be very costly. The cost of downtime can be astronomical even detrimental for companies who use their WAN infrastructure for critical interaction with customers, colleagues and other business transactions such as time sensitive financial, medical or legal transactions. The following statistics illustrate the cost of network failures:

- The average corporation has the potential to lose an average of $7.8 million per year in WAN downtime alone. ***
- Average hourly cost of downtime: ***
  Brokerage houses: $6.4 million
  Credit card sales / authorization: $2.6 million
  Catalog sales: $90,00
  Package shipping: $28,000
- WANs fail or degrade on an average of 7.1 hours per month, the cost of which could add up significantly for any company. *

Source of Study:
Infonetics Research*
Comdisco/BellSouth/Oracle Vulnerability **
Contingency Planning Research***

Security Breaches

The issue of security has always been important to the developers of VPN technology. Since the Internet is the most popular shared data network used by companies who have implemented VPNs, extra measures have been taken to try and protect data from sniffers and hackers. A typical VPN device uses a tunneling technique that involves the encryption of data packets, which are encapsulated into an IPpackage by the VPN, and then tunneled through the Internet. A VPN tunnel terminator receives the data on the opposite end of the transmission and decrypts the information. Most VPN products also support multiple forms of authentication, which ensures that the connecting user has rights to enter the network.

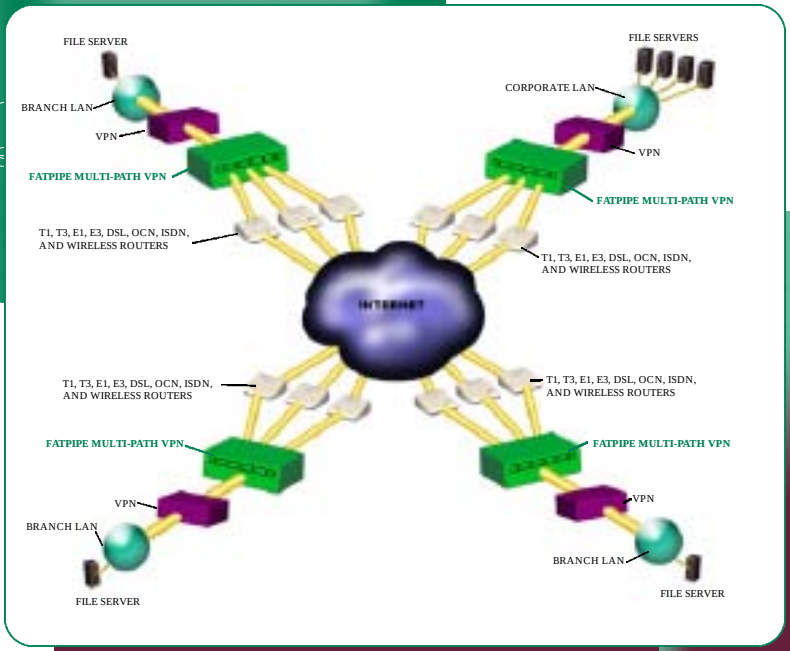
Despite efforts to protect access, security mechanisms can be breached, particularly over the Internet. Capable hackers have broken into and will continue to hack into networks and take valuable information -- such as credit card numbers -- from other people's networks. Knowing the risks involved in sending information over a public network, FatPipe Networks has added its Multi-Path Security technology (MPsec™) to Multi-Path VPN. MPsec delivers packets randomly over multiple paths for up to nine times more security of data packet transmission.

Poor WAN Infrastructure

Poor WAN infrastructure is another issue of VPN technology. It is a challenge to implement VPNs when multiple offices are located in remote areas where bandwidth is not easily available, e.g. factories outside of major cities or international offices where line quality and reliability of Internet connections are poor. The following statistics reflect how costly poor WAN infrastructure can be for business:

- Network downtimes (LAN/WAN) among large companies cost an average of $32.5 million in lost productivity and revenue. *
- One in four companies have experienced a network disaster with a medium length of disaster time of 8 hours. Twenty four percent had outage times over 24 hours. **
- Sixty-four percent of companies do not have sufficient disaster recovery plans for their WANs. **

The employment of VPN is growing rapidly and is expected to continue despite the shortcomings that currently exist. In summary, VPNs that use single links to the Internet are vulnerable to catastrophic failure. FatPipe has developed an easy to implement redundant and reliable solution for VPNs to resolve these common problems. The solution is FatPipe Multi-Path VPN.



FatPipe Multi-Path VPN for Secure, Fast, and Redundant IP Traffic Delivery

FatPipe Networks' Multi-Path VPN takes any VPN and makes it nine times more secure and three times more reliable and redundant, while providing three times the speed

FatPipe Networks set out to eliminate single points of failure for companies implementing VPNs. Multi-Path VPN takes any IP compatible VPN stream and delivers the data over multiple WAN paths, transmitting data over several backbones and routers. The data is received at the other end by multiple routers and then presented as a single stream to the VPN unit, which then decrypts the data and forwards it to the intended IP addresses.

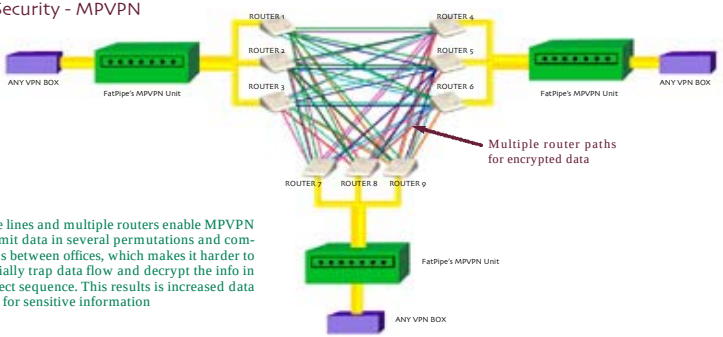
FatPipe developed Multi-Path VPN to give customers control over their WAN networks and keep their VPNs up and running despite any line failure. Multi-Path VPN enables bi-directional data transmission over multiple VPN paths, providing up to three times the reliability, redundancy, and speed of a VPN while enhancing security.

Security – FatPipe MPsec™

FatPipe Multi-Path VPN provides the highest levels of redundancy and reliability for VPN infrastructures. Multi-Path VPN also provides added security of data transmission -- up to nine times -- with its patented MPsec™ technology. As data is transmitted over different permutations and combinations between the routers, snooping becomes extremely difficult because a random number of IP combinations and physical paths are involved. This makes it virtually impossible to trap data in the correct order and to decrypt the information in the correct sequence. Random placement of data as well as the separation of data over multiple streams increases data security. The less secure alternative is to use one line for transmitting data using a single data path, which makes it is easier to trap and decode data. Figure below demonstrates the innumerable paths for data to travel using FatPipe's MPsec™.

There are three offices connected via VPN diagram below. Even if only two offices are connected, each office would have up to nine times more security by using three connections at each location. MPsec routes packets randomly over the three available lines from each router, thus creating nine distinct data paths over three separate ISP/backbones. Should a hacker successfully break into one of the lines, the hacker will only receive one-ninth of the data from a data stream placed over three connections.

High Security - MPVPN



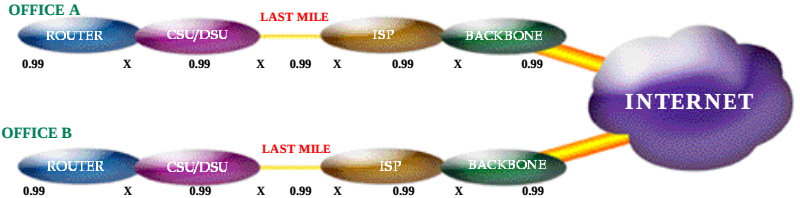
Multiple lines and multiple routers enable MPVPN to transmit data in several permutations and combinations between offices, which makes it harder to sequentially trap data flow and decrypt the info in the correct sequence. This results is increased data security for sensitive information

Redundancy and Reliability

Multi-Path VPN gives customers the ability to transmit data over multiple lines, bypassing failures along its route when necessary, including router, ISP, line or backbone failures. Users enjoy faster speeds when all lines are available and can be rest assured that their connection to the outside world will be up 24 hours a day, 365 days a year even when intermittent failures occur.

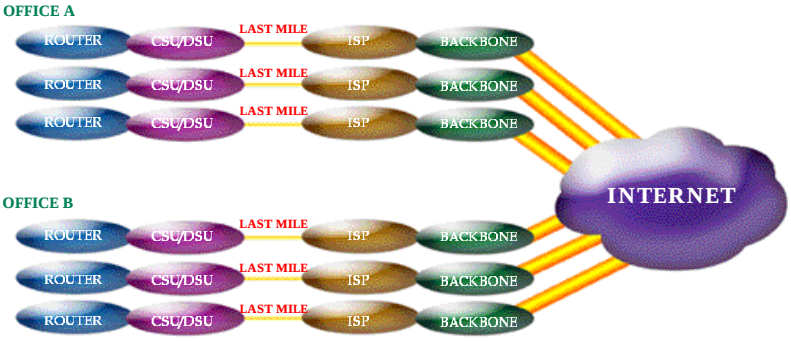
Integrating Multi-Path VPN as part of a VPN solution significantly enhances system reliability. The figure below shows the potential cost associated with VPN models that do not have the advantage of Multi-Path VPN as part of their VPN network. Money, time and productivity even when every single point of failure is 99 percent reliable can be lost. Integrating Multi-Path VPN into the network increases system reliability.

Availability of Systems



System reliability = 0.9910 = 90.43% i.e. the system will be down 9.56% of the time, or 168 hours in an 8am - 5pm period (220 days/yr). At $10,000/hr, the cost to the company = 168 x $10,000 = $1,680,000/year for a two office connection

Availability of Systems with MPVPN



For multiple (3) parallel systems as shown above, the system reliability is 0.999995 x 0.999995 = 99.999% I.e. system will fail only 0.001% or 0.0176 hours in a year (8 hour day, 220 days/yr.). Potential loss averted = $1,680,000 - $176 = $1,679,824

FatPipe's RAIL™ Technology for Outbound Redundancy

FatPipe's patented technology called Redundant Array of Independent Lines bonds any combination of multiple T3, E3, T1, E1, DSL, ISDN, and Wireless connections for increased speed and redundancy. Should any of the services fail along the route of transmission, IPpackets are automatically rerouted, circumventing points of failure to keep WAN infrastructures intact and functional while the failure is active.

FatPipe's SmartDNS™ for Inbound Redundancy

FatPipe's patent-pending SmartDNS™ provides redundancy for incoming traffic by allowing the host on the network to be accessible through multiple connections. SmartDNS makes adjustments to the DNS records when connections fail, and will not resolve host names to IPaddresses that are associated with the failed connection. Multi-Path VPN uses a short Time to Live (TTL) to ensure that information about the IP addresses for the host that it serves is accurate. When a line goes down, SmartDNS will not broadcast the IP address that is associated with the failed line. Instead, it guides queries to available lines, thus providing redundancy for inbound traffic. Administrators can change the TTL according to their preference.

Load Balancing and Speed

FatPipe's RAIL and SmartDNS technologies not only provide redundancy, they also balance load over available lines and add speed to the delivery of bi-directional data transactions through bonding.

Multi-Path VPN dynamically load balances inbound and outbound traffic using all available lines. There is no need to setup router tables or use the more traditional BGP programming. Multi-Path VPN also speeds up the delivery of information over VPN infrastructures. Regardless of size, FatPipe Multi-Path can provide speed, reliability, and security for WANs at a minimal cost and effort.

FatPipe RAIL™

For outbound IP traffic, Multi-Path VPN automatically senses load on each line and dynamically balances load according to line availability using FatPipe's patented RAIL technology. There are no complicated router tables to configure; BGP programming is not required. RAIL enables Multi-Path VPN to balance the load of data transmission over WAN connections of similar or dissimilar speeds.

Fatpipe Multi-Path also aggregates multiple connections forming a single, virtual fatpipe for combined speed. It bonds any combination of lines, including T3, E3, T1, E1, DSL, Wireless, ISDN, 56K for outbound IP transmissions. The result is cost savings for companies, as they can backup expensive T3 and T1s lines with cheaper alternatives such as DSL or Wireless.

FatPipe SmartDNS™

Inbound IP traffic is balanced by FatPipe's SmartDNS™ technology. SmartDNS balances load by allowing the host on the network to be accessible through multiple connections. The host appears to be at different IP addresses at different times, thus using all available lines to transmit data. FatPipe's SmartDNS also speeds up the delivery of inbound traffic by intelligently choosing the fastest connection of available lines.

Easy Management

FatPipe Multi-Path VPN offers a secure networking environment that lends flexibility and control to help Administrators accomplish their tasks. Multi-Path VPN's web-based management tools allow Administrators to access the network, view routers, the speed meter and the speed chart, and the status of connections from any location worldwide. Multi-Path VPN comes with paging and e-mail alert software that can be installed on any computer on the LAN to notify Administrators of ISP, router, line, or backbone failures. Multi-Path VPN even offers the ability to send SNMPtraps to select SNMP manager stations.

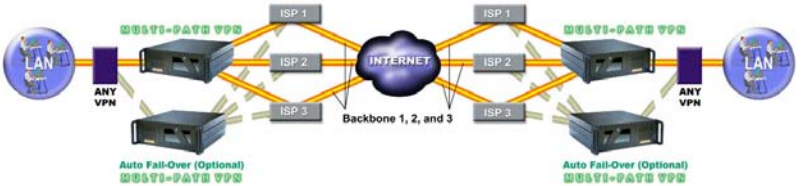
Reverse Port Mapping for Efficient Delivery of Inbound IP Traffic

Reverse Port Mapping is an efficient way to deliver IP packets and requests from the outside world into a LAN. Reverse Port Mapping allows specifically assigned servers on a LAN to be accessible to machines on the Internet by assigning multiple private IP address to a public IP address. Reverse Port Mapping conserves public IP addresses. Asingle public IP address can be mapped based on port number to multiple internal servers.

Proxy ARP

Multi-Path VPN uses Proxy ARPto help the Administrator integrate Multi-Path VPN into their network with very little change to the existing LAN/WAN IPconfiguration. It is designed to minimize changes to the network. By subnetting the existing IPrange into a smaller network, Proxy ARP"fakes out" the Multi-Path VPN unit into thinking all of its interfaces (WAN and LAN) are on different networks (Subnets). Multi-Path VPN will take the traffic intended for the router's IP address.

FatPipe Multi-Path VPN in auto fail-over mode



FatPipe MPVPN combines multiple routers into a single, high-speed Internet connection. In this diagram, two MPVPN units are used at each location (called Dual MPVPN) for ultimate reliability.

Auto Failover
In addition to automatically rerouting information when lines fail, Multi-Path VPN also has other redundancy features such as hot-swappable power supplies and a Dual Multi-Path VPN setup option.

The Dual Multi-Path VPN setup is comprised of two units installed at one site. Amaster - slave configuration allows each unit to talk to the other and check availability on a consistent basis. If the master unit fails, the slave unit will takeover until the Administrator can pinpoint the master unit's cause of failure. (If the master unit needs rebooting, the Administrator can reboot from a remote location). In failover mode, the maximum possible system redundancy is achieved, resulting in maximum uptime for the VPN system.

Seamless and Transparent
Multi-Path VPN™ is technology and application independent and does not require proprietary components. Therefore, it does not matter what type of hardware or software technology is used in the LAN. Multi-Path VPN is router hardware independent and works seamlessly with any type of firewall, caching and server load balancing devices. It works with any VPN technology that uses IPsec protocol and over any operating system and platform.

Scalable and Flexible
FatPipe makes it easy for companies to get the support they need for their VPN infrastructures. It comes in three versions, 135Mbps, 50Mbps and 2Mbps throughput, making reliability, redundancy and speed available to companies according to their individual needs.

Multi-Path VPN provides a solution for companies who have branch offices in remote areas where high bandwidth is not readily available. Bonding lower speed lines adds up to a fast connection for these offices and provides the redundancy they need. Abank, for example, can use the 135Mbps version at its head office while its branch offices in the US and abroad utilize the 50Mbps or the 2Mbps version, where broadband is either too expensive, unavailable, or not needed. VPN is scalable and can grow as the company grows.

Easy Setup
FatPipe Multi-Path VPN™ is easy to install using its Graphical User Interface. Unlike BGP programming, there's no need to contact the ISP or for the ISPto have proprietary hardware or software at their site.

Ease of Setup

Review of Multi-Path VPN's Benefits and Features

Features

- Combines multiple T3, T1, DSL, Wireless, ISDN connections for aggregate speed
- Works over multiple ISPs and backbones for reliability
- Auto load balancing and auto failover for inbound and outbound IP traffic
- FatPipe's patent pending Multi-Path Security (MPsec™) for up to nine times more security of IPdata stream transmissions
- SmartDNS™ provides redundancy and dynamically balances incoming traffic load
- RAIL™ technology for redundancy and load balancing of outgoing IPtraffic
- Reverse Port Mapping to conserve IP addresses
- Proxy ARP designed to minimize changes to the network
- No BGP programming or additional router programming or hardware needed
- Web-based management tools for remote monitoring
- Paging and e-mail emergency notification
- No new or specialized hardware or software at the ISP site
- Remote r eboot
- Easy Install

Benefits

- Increases security of IPdata stream transmission up to nine times with FatPipe's MPsec™
- Provides the highest level of redundancy and reliability of VPN infrastructures
- Aggregates any combination of T3, E3, T1, E1, DSL, ISDN and/or Wireless connections, with speeds up to 135 Mbps
- Seamless technology that is application and technology independent

Conclusion

FatPipe Networks' Multi-Path VPN takes any VPN and makes it nine times more secure and three times more reliable and redundant, while providing three times the speed. Whether you have offices all over the country or all over the globe, FatPipe's Multi-Path VPN will keep your WAN infrastr ucture up and running despite intermittent ISP, router, line, or backbone failures.