FATPIPE NETWORKS

IPVPN White Paper

4455 South 700 East • First Floor
Salt Lake City UT 84107
Phone 801.281.3434 • Fax 801.281.0317
Toll Free: 800.724.8521

Fault Tolerance, Security, Speed for Private or Public WANs

Concept

The demand for improved availability of WAN services to support the use of web-based applications has resulted in the steady rise of router clustering technology implementation over the last few years. According to Jim Metzler of Open Reach's *Tackle Your Top 5 Wide Area Network Challenges*[1] report, Internet-based applications' growth rate is doubling every two years, (growing at a rate of 40%- 45% a year). Evidently, many companies use the Internet and/or private WANs as indispensable communication tools and deem their WAN applications and infrastructure as cornerstones to the success of their businesses.

The escalated adoption of TCP-based applications like email, web browsing and file transfers, has increased the need for more bandwidth, additional security of data transmission, and a means to achieve WAN redundancy. The use of more IP based communications has also increased the probability of WAN performance degradation and instability for end users, magnifying the significance of WAN downtime.

Not planning for the possibility of WAN failure is a perilous affair for companies that use WANs to conduct business. Likewise, ISPs, ASPs, VARs and integrators that provide managed IP based services must find ways to ensure WAN connectivity and/or services for their clients. A downed service, core to the functionality of the customer's WAN, may result in customer dissatisfaction and possible termination of contracts if the service they are providing is the root of the malfunction.

The implication of significant losses in productivity and revenue leads companies to prepare contingency plans to avoid the detrimental effects of WAN failures. Companies that use their WAN infrastructures to deploy mission critical applications, and the providers and integrators that service them, are compelled to enhance and fortify their WAN infrastructures.

According to a report from Infonetics Research, two thirds of the respondents to their latest study, *The Cost of Downtime, 2003*,[2] indicated that the two primary factors driving companies to upgrade their WAN infrastucures are the twin desires to lower the cost and to improve the reliability of their WAN services. The question is: how do you accomplish WAN fault tolerance *and* improve security and the speed of data transmission without spending a fortune? What options are available?

FatPipe IPVPN Router-Clustering Technology

This paper will introduce you to FatPipe's IPVPN router clustering product, the most innovative and cost effective solution to the woes of WAN failure that simultaneously improves the security of data transmission and data transmission speed significantly. FatPipe IPVPN offers these advantages to customers without the need for additional hardware, software or applications. FatPipe IPVPN also gives administrators greater control of their networks using web-based management tools supporting private, public wide area networks (WANs) or a hybrid of private and public networks.

The first section of this paper will provide an overview of what FatPipe IPVPN is and how it empowers customers to avoid WAN failures and improve the efficiency of their networks. Short customer scenarios and a case study will follow to illustrate this. The second half of the paper will present more in-depth technical information.

---

[1] *Tackle Your Top 5 Wide Area Network Challenges*, Dr. Jim Metzler, Page 1, November 2002

[2] *The Cost of Downtime 2003*, Infonetics Research, Jeff Wilson, March 2003

What is Router-Clustering Technology?

Several years ago, FatPipe's engineers recognized the need for an easy to deploy and maintain alternative to Border Gateway Protocol (BGP). FatPipe created the concept and category of Router Clustering, and have obtained three patents, with multiple patents pending to date. Router-clustering technology is a relatively easy-to-implement, cost effective and efficient solution to interruptions of WAN services. Router-clustering devices provide fault tolerance for WAN infrastructures and feature several other tools that benefit the customer, such as load balancing methods for inbound and outbound traffic, additional security for data transmissions, and greater bandwidth capability by aggregating two or more lines through the router-clustering device.

How do FatPipe IPVPN and other router-clustering devices do the trick? First, they aggregate any combination of T1, DS3, DSL, Cable, ISDN and/or Wireless connections to achieve combined speed and redundancy. They bond the multiple connections from the same or separate ISPs and backbones, without the need for ISP cooperation or setting up proprietary hardware or software at the ISP site(s). Router-clustering devices also intelligently sense the status of services (ISP, backbone, line, router, etc.), and reroute IP packets automatically when failures occur. The dynamic load balancing and route control features gives control of a wide area network back to the network administrator, without the need for BGP programming.

Router-clustering devices are application, technology, and router independent, sitting transparently in a network at the edge of the LAN -- there is no need to purchase special routers or additional hardware. FatPipe's IPVPN is the most advanced and sophisticated router-clustering device available in the FatPipe family. It is compatible with private or public networks or a combination of both, giving the user freedom to upgrade, enhance or backup current systems with any other type of system.

The Scoop on FatPipe IPVPN

FatPipe IPVPN 3.0 is a router-clustering device that provides the highest level of redundancy, reliability, speed and additional security for communication between private or public networks, or a mixture of the two types of networks. FatPipe IPVPN provides a cost effective and efficient solution to the interruptions of Wide Area Networks services resulting in WAN downtime. FatPipe IPVPN will keep any type of WAN infrastructure up and running even when a failure occurs to one of its main components including failure of an ISP, a backbone, a line, or a router. FatPipe IPVPN will automatically reroute IP traffic over available lines for inbound as well as outbound traffic. No BGP programming is necessary, although FatPipe IPVPN can work in conjunction with BGP, if it is layered over BGP4 to provide redundant tunnels.

FatPipe IPVPN Benefits

Companies have integrated FatPipe IPVPN in to their network to:

- Prevent WAN downtime
- Achieve higher levels of bandwidth and data transmission speeds
- Acquire up to three times the security of data transmission using FatPipe Patented MPSec® security feature
- Have a choice of robust and intelligent load balancing methods that fit their communication needs

Real World Examples

Customer Scenarios

FatPipe IPVPN is a unique addition to the FatPipe family of products as it works with multiple managed VPN service providers and Customer Premises Equipment (CPE) based VPNs to achieve the highest possible level of reliability, redundancy, speed and security for VPN transmissions. The ability to work with new and existing networks creates a flexible system, balancing load among multiple managed or CPE VPNs, while still being compatible with Internet-based VPNs. The short listed examples below illustrate three main customer scenarios where FatPipe IPVPN would be a good fit for a potential customer.

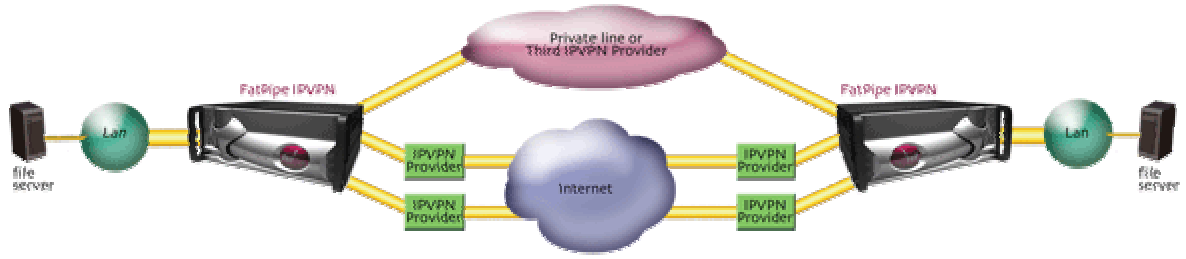


Figure 1 FatPipe IPVPN works with private lines and/or managed (public lines) VPN services and transmits data over multiple ISPs and backbones. Since data is transmitted in any number of permutations and combinations between the routers, hacking becomes extremely difficult.

Backup Frame Relay with a Managed or CPE Based VPN

FatPipe IPVPN works with private and/or managed (public) WANs to meet the redundancy needs of customers. In this scenario, a customer uses a less expensive managed or CPE based VPN to backup its expensive private/frame network via FatPipe IPVPN. (The customer may also be able to use its local Internet connection as a backup to its frame/private line, thus providing a layer of redundancy without increased costs). The company would be able to use the Internet bandwidth at all times or use the backup connection only when the frame connection fails.

Seamless Migration From Frame To IPVPN

A customer can use FatPipe IPVPN to seamlessly integrate managed IPVPN services or Internet connections with an existing Frame Relay network. The customer can migrate from Frame to IPVPN on its own timetable transparently and without interruption by bonding the data connections through a FatPipe IPVPN unit.

Backup VPN With a Second CPE based VPN or a Managed IPVPN

The customer can use a second CPE based VPN or a managed IPVPN services to backup its current VPN (CPE or Managed) infrastructure.

The last scenario described in this paper is an actual FatPipe customer success story. Read below to discover how the client, Next Generation Radiology, uses FatPipe to improve network system efficiency, increase bandwidth and security.[3]

[3] Please visit FatPipe Network's website to read more customer success stories (http://www.fatpipeinc.com/casestudies/)

FatPipe Case Study: Next Generation Radiology Uses FatPipe IPVPN to Ensure Efficient Access to Patient Medical Information and Data Security to Surpass HIPAA Compliance Regulations

Next Generation Radiology (NGR) is taking part in a new, sophisticated movement in medical imagery technology. The conversion from film to digital media for storage, display, and archival of patient information has had a tremendous impact on companies such as NGR in streamlining workflow, reducing operating expenses and improving overall patient care. NGR uses FatPipe IPVPN as a solution to ensure fault tolerant Internet access and by default surpass HIPAA's standards and requirements for security by utilizing FatPipe IPVPN's security feature, MPSec®.

Solution Overview

Situation
NGR was using Frame Relay to transfer digital patient files to each of its locations, but suffered from faulty Internet access and poor bandwidth conditions. Every time NGR's network failed, information transfers among doctors and staff were lost.

Solution
NGR integrated FatPipe IPVPN into their network to improve system efficiency. NGR now has at each office, one public connection strictly for Internet connectivity and two Frame links for greater bandwidth and reliability of their private network, via FatPipe IPVPN.

Benefits
NGR achieves high network availability and efficient delivery of patient data. FatPipe's unique MPSec technology also allowed NGR to surpass HIPAA compliance issues by providing additional security for data transmission.

Next Generation Radiology uses a Frame Relay network to connect all three of its branch offices to their main facility, which is the repository for X-Rays, MRI's and patient data. NGR was facing poor quality of service and bandwidth limitations due to restricted service options. Every time NGR experienced a circuit failure, information transfer among doctors and hospital staff were completely lost. Receiving data in a timely manner is a constant critical issue for doctors in assessing patient "risk" information. Bandwidth "bottlenecking" was also a major issue.

NGR wanted to find a solution that could improve system capability and provide redundancy and reliability while increasing overall bandwidth at a reasonable cost. After considering more complicated and expensive alternatives, NGR implemented FatPipe IPVPN to bond an Internet connection and an additional Frame link with their existing single line, Frame network. FatPipe aggregates the two Frame connections for additional speed for their private network, and has the Internet lines available purely for Internet connectivity (DSL/T1 mix). FatPipe IPVPN is a complete solution, providing WAN redundancy and network flexibility resulting in a more efficient performance.

"There is no other product as well suited as FatPipe IPVPN to mix public and private networks while maintaining network security," said Dan Castalado, NGR's System administrator.

By adding a public circuit to their network, NGR was required to meet HIPAA compliance regulations, which address the security and privacy of patient health care data. FatPipe's unique MPSec technology provided the additional security in data transmission allowing NGR to go above and beyond certification.

With FatPipe IPVPN, NGR provides efficient delivery of mission critical patient health care data.

Next Generation Radiology Network Setup

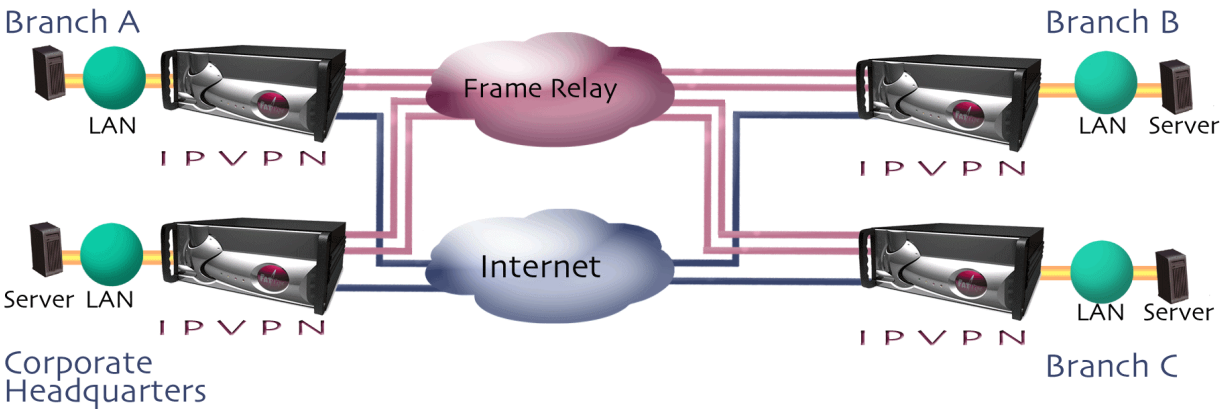


Figure 2 The illustration above is a simplified diagram of NGR's wide area network. NGR runs two frame and one Internet connections through FatPipe IPVPN units at the headquarters and branch office sites. Each site is setup identically, with FatPipe IPVPN bonding two frame connections for aggregate speed while allowing end users to use each Internet connection for browsing capabilities.

FatPipe IPVPN's Functionality

At the nucleus of FatPipe IPVPN is a number of patented and patent pending FatPipe technologies. These features are discussed in the next section followed by a real world diagram that illustrates how some of the FatPipe features can be configured to aid the customer to setup a more cost effective and efficient WAN.

Redundancy and Reliability

FatPipe IPVPN's patented and patent pending technology is designed to work seamlessly over multiple backbones and ISPs for redundant and reliable WAN connectivity. FatPipe IPVPN can dynamically sense when an interruption of service occurs due to router, line, ISP or backbone failure, and automatically reroutes the packets to available lines.

Speed

FatPipe IPVPN load balances Internet traffic over multiple connections dynamically, according to the load-balancing method chosen by the administrator. FatPipe IPVPN can combine up to three (or more) DS3, T1, DSL, Cable, ISDN and/or Wireless connections for aggregate speed. It works with any brand of routers including Cisco, NetSpeed, Ascend, and 3COM. FatPipe IPVPN works at the network level and does not require any special changes to the existing router tables or bridges. Additionally, software changes are not required on the network servers either, as FatPipe IPVPN works transparently over any operating system. It does not matter what operating system or network platform you are using as long as it is IP enabled or the data packets are encapsulated into IP packets.

Load Balancing Options

FatPipe IPVPN load balances Internet or private/frame traffic over multiple connections dynamically. Four different methods for load balancing are possible:

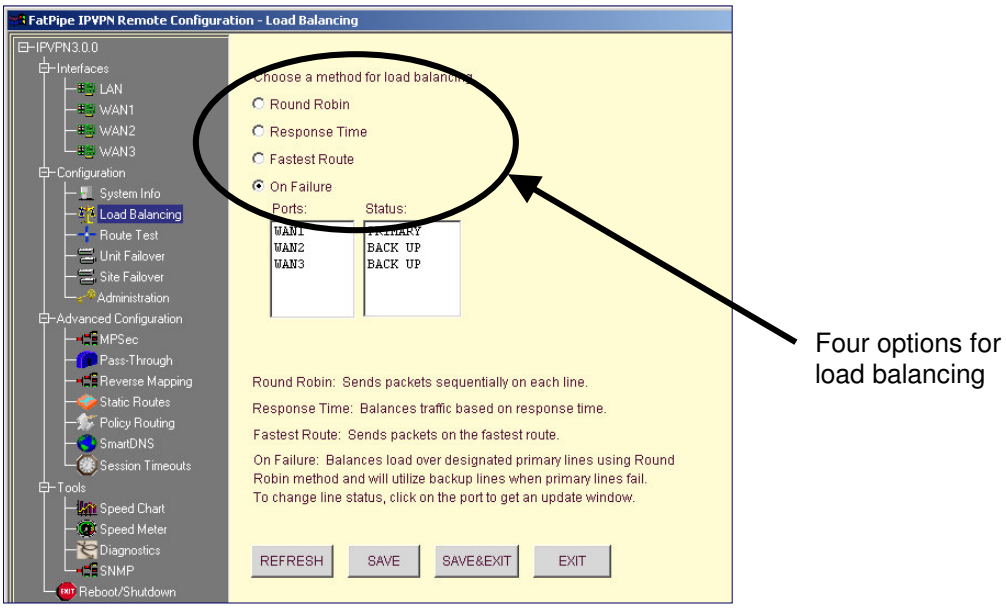


Figure 3 FatPipe's Graphical User Interface makes installation and general management simple and easy for the administrator. The above screenshot is of the main load balancing configuration page.

Round Robin: (default) Sends packets in order of succession over each connection to the Internet. This method is recommended for similar speed connections to the Internet, even if the connections are not the same kind (i.e.: combining a 1.5 Mbps Cable connection with one or two same speed T1s).

Response Time: Balances network Internet traffic based on each line's average response time for the Internet request. This method is recommended for extremely unequal speed connections. The Response Time method utilized the fastest connection the most.

On Failure: Balances the network's load based on the primary line's current availability. All traffic will be directed to the primary lines. In case the primary lines fail, all traffic will then be directed over the backup lines. This option is used when combining a primary and standby-metered communication line.

Fastest Route: Configures FatPipe IPVPN to balance load on a per destination basis. Each session will go over the fastest line for its destination.

Load balancing is achieved without the need for BGP programming.[4] The routers do not have to be BGP compatible, e.g. DSL routers and cable modems can also work well with FatPipe IPVPN.

[4] If the client is already using BGP, note that in most cases FatPipe IPVPN can work in conjunction with BGP4 without making any changes to BGP tables or routers.

Security

FatPipe IPVPN uses its patented Multi-Path Security (MPSec) feature to provide up to three times the security of data transmission on private and a combination of private and public networks, and nine times more security for entirely public networks. MPSec transmits data in several permutations and combinations between offices, which make it virtually impossible to trap data and decrypt information in correct sequence.

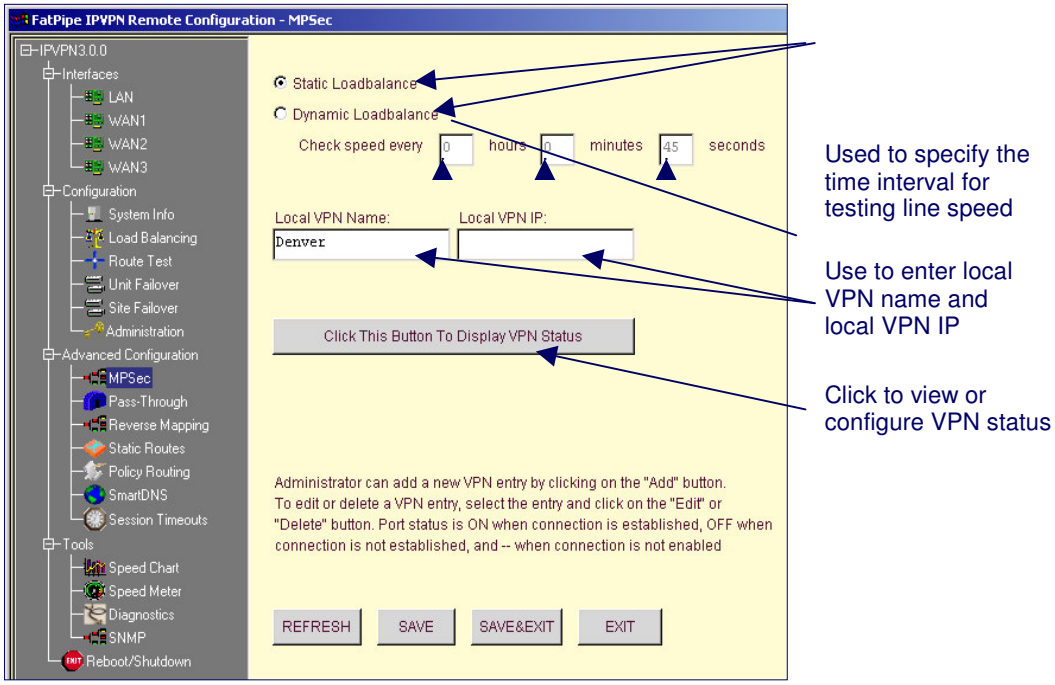


Figure 4 FatPipe IPVPN's MPSec security feature adds up to three times more security of data transmission. The above screenshot is of the main MPSec configuration page.

Auto Failover

All FatPipe products provide three auto failover options for customers. Clients have several choices, and depending on their level of sensitivity regarding redundancy, they can choose among the following:

- Single unit with dual fans for superior cooling
- Single unit with hot-swappable power supplies. If the primary power supply fails, the secondary power supply takes over automatically with no interruption to services.
- Dual FatPipe units in auto-failover setup, where the primary and secondary units are sitting at the customer premises, constantly communicating with each other. Should the primary unit fail, the secondary unit automatically takes over instantaneously.

FatPipe IPVPN Features

Listed below are the principal features that make up FatPipe IPVPN's unique core technology.

- ✓ **RAIL:** FatPipe's Redundant Array of Independent Lines or RAIL is a patented technology that dynamically balances load over multiple lines for outbound IP traffic without BGP, thus creating a virtual *fatpipe.*

- ✓ **SmartDNS:** A patent pending technology from FatPipe, SmartDNS intelligently selects the fastest connection for inbound traffic as well as provide **Inbound IP Traffic Line Failover.** SmartDNS detects when lines are down and will automatically reroute inbound traffic to available lines.

- ✓ **Policy Routing:** Allows the client to direct outbound traffic based on specified criteria. Administrators use this feature to setup and prioritize rules that define the actions taken when a data stream matches the criteria. Administrators can direct traffic based on port, IP address, or a combination of the two with or without NATting, using the Policy Routing feature.

- ✓ **Reverse Mapping:** Allows the client to conserve IP addresses and directs application traffic to specific servers. Reverse Mapping will allow inbound access to servers on the LAN side of FatPipe IPVPN.

- ✓ **Pass-Through:** Allows administrators to integrate FatPipe IPVPN into their networks with minimal changes to existing network addressing. Pass-Through will allow inbound access to servers on the LAN side of FatPipe IPVPN.

- ✓ **Proxy ARP:** Saves time and money by allowing administrators to integrate FatPipe IPVPN into their networks without having to reset gateways on client computers in their LANs.

- ✓ **Web-based management tools:** For remote monitoring from any location to view the status of local or remote office sites.

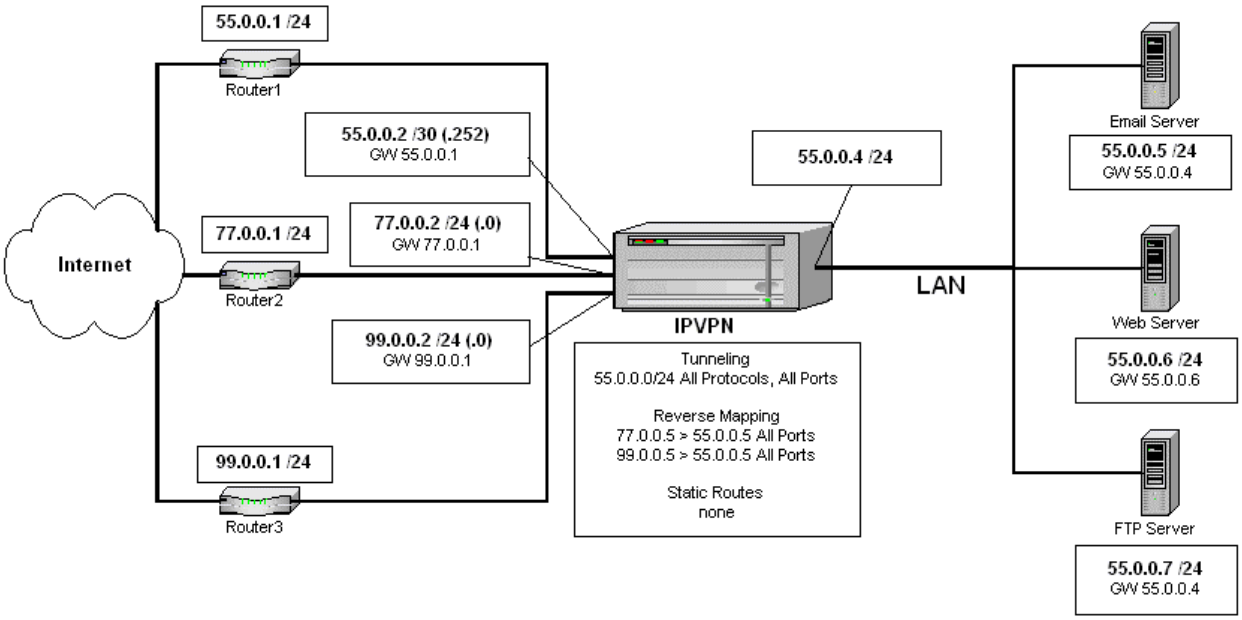
- ✓ **Paging and e-mail:** Emergency notification to administrators if a failure occurs to their wide area networks.

- ✓ **Fast Disaster Recovery:** FatPipe IPVPN allows administrators to save configuration files to a safe location – either a secondary backup FatPipe unit or any other PC – for quick recovery of configuration information and restoration of the WAN network.

- ✓ **MPSec:** Significantly improves data transmission security with its patented technology that splits data streams at the packet level, randomly send the packets over multiple connections where the data is reassembled at the receiving end.

FatPipe IPVPN Real World Diagram

The diagram below portrays an example of a real-world setup. Both Pass-Through and Reverse Mapping are used to bring traffic into the servers. The Email Server, Web Server, and FTP Server all have public IP addresses. FatPipe IPVPN provides redundancy to these servers by passing the 55.0.0.x IPs back to the LAN using Pass-Through and translating the 77.0.0.x and 99.0.0.x IPs back to 55.0.0.x IPs using Reverse Mapping. This way, there are multiple paths into those servers, thus multihoming the servers is unnecessary. The existing public IP space can be used as was prior to installing FatPipe IPVPN.



Conclusion

FatPipe has engineered FatPipe IPVPN to provide the world's highest flexibility, reliability, redundancy, security and speed for wide area networks that surpasses all technologies available in the market today. Corporations can now obtain up to 99.999988% reliability for their WANs.

For more information about FatPipe IPVPN and FatPipe's line of router clustering products, please visit www.fatpipeinc.com or contact FatPipe by telephone: 800.724.8521 or email your request to info@fatpipeinc.com.

Product Specifications

Specifications

General
4U high, 19" rack-mount chassis
Meets EIA RS-310C Rack-mounted standard
Front Panel power switch, reset switch and Power LED

Load Balancing
Round Robin
Response Time
0n failure
Policy Routing
Fastest Route

Management
Java interface
Network configuration
Emergency Paging and e-mail alerts
Speed Chart and Speed Meter
Automatic failover
SNMP Ready

Security
Inherent NAT-based Firewall
Reverse Mapping

In The Box
Owners Manual

Warrantee
90 days of free technical support
Premier packages can be purchased

Physical Specifications

Dimensions
7"H x 19"W x 17.8"D
4U Industry standard rack-mount chassis

Weight
40 lbs. 18.1kg

Network Interface
Four 10/100 BASE Fast Ethernet
Fast Ethernet Fiber and Gigabit Ethernet available
Additional WAN ports available

Operating Temperature
32° to 122° F (0° to 50° C)

Relative Humidity
10 to 96% @ 104° F (40° C, non-condensing)

Power Supply
90-132 VAC or 180-264 VAC
** Dual power supply units available -- hot swappable

Cooling Fan
Two front cooling fans

Vibration
Sweeping frequency: 5~35~200Hz
Amplitude: 0.6mm (zero to peak)
Acceleration: 1.5 m/s^2

FatPipe Networks Patents
Please see below for the FatPipe Patents. Go to http://patft.uspto.gov/ to read about each patent in detail.

The patent numbers are as follows:

6,295,276
6253,247
6,493,341