



Application Notes

Policy Routing

FatPipe Networks continues to provide the best-of-breed products and technology for our customers. To that end, FatPipe has enhanced the WARP and MPVPN products.

One of the improvements implemented in FatPipe's WARP and MPVPN 2.0 versions is the addition of the Policy Routing innovation. Policy Routing allows users to direct outbound traffic based on specific criteria. It uses prioritized rules that define what the criteria are and what is done when a data stream matches the criteria. One can use specific protocols and/or ports to designate data transmission.

In effect, Policy Routing allows the Administrator to set router policy according to specific parameters. For example, if an e-commerce company wanted to have all of its customers' credit card information sent over a Secured Socket Layer (SSL) using one line only, the company's administrator would set rules directing that specific type of traffic to the specified port.

Another good example: using the router policy feature to back up a frame connection with a VPN. An administrator can set rules that will multiplex the site-to-site traffic across the two lines or set up in failover mode where primary is frame and secondary is VPN. At the same time, all Internet traffic will be directed to the Internet line only. See Figure 1.

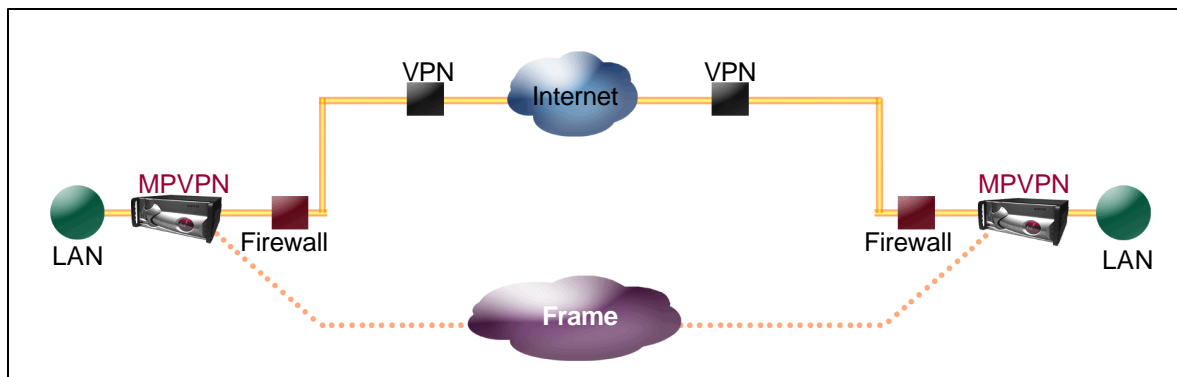


Figure 1

Each rule has the following criteria

Source IP/Mask – single IP, whole IP subnet, or all IPs

Source Port(s) – single port, port range, or all ports

Destination IP/Mask – single IP, whole IP subnet, or all IPs

Destination Port(s) – single port, port range, or all ports

Protocol(s) – specific protocol or all protocols

Source IP/Mask and **Destination IP/Mask** can use an asterisk (*) to indicate all IPs. **Source** and **Destination Port(s)** can use a hyphen to specify port ranges (e.g. 1-1024) or an asterisk (*) to specify all ports.

Each rule also has the following action

NAT: User can specify whether the traffic gets masqueraded as the IP of the port it goes out or if the traffic goes out untouched (keeping the IP of the source machine).

Traffic Mode: There are two modes: Interface Priority or Interface Specific.

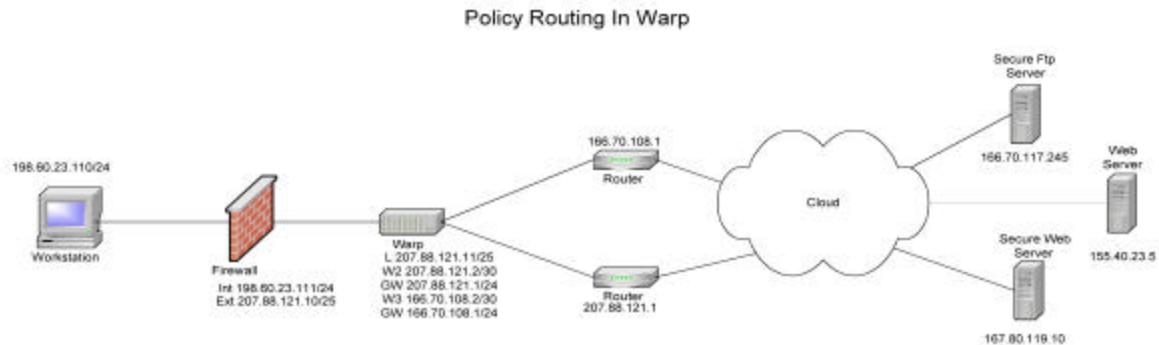
1. **Interface Priority** directs traffic out the first live line, using order: port 2, 3, or 4
2. **Interface Specific** directs traffic out only through the line or lines specified

The rules are prioritized, which means that the first rule that matches is applied. If the top rule is not matched, the next rule is checked, and on down the rule-set until it reaches the bottom. If no rule is matched, then the default rule is applied. The default rule is to masquerade (NAT) and multiplex (send out all live ports) outbound traffic.

Note: The most restrictive rule must be listed first and the least restrictive rule last. If the order is reversed, the most restrictive rule will be disregarded. To use policy routing, click on Policy Routing under the Advanced Configuration section listed on WARP's remote configuration window. On the Policy Routing page, click Add to add a new Policy Routing Rule.

Policy Routing Examples

You will find four policy routing examples, which are illustrated in Figure 2 and outlined below.



Order of rules is very important. All rules must descend most restrictive to most lenient. Failure to do so will result in a specific rule being disregarded. For example, if policy 4 is put ahead of any of the other policies, the other policies will never be checked because policy 4 allows everything.

Figure 2

Policy 1

207.88.121.10/32 Src Port *
166.70.117.245/32 Dest Port 20-21
Protocol Tcp
NAT Disabled
Interface Specific Port 2

Policy 1: This policy states when the device with address 207.88.121.10 connects to 166.70.117.245 on ports 20-21 (FTP) not to use NAT and send traffic only through port 2.

Policy 2

207.88.121.10/32 Src Port *
167.80.119.10/32 Dest Port 80
Protocol TCP
Interface Specific Port 2

Policy 2: This policy states when the device with address 207.88.121.10 connects to 167.80.119.10 on port 80 (HTTP) not to use NAT and send traffic only through port 2.

Policy 3

0.0.0.0/0 Src Port *

155.40.23.5/32 Dest Port 80

NAT Enabled

Protocol TCP

Interface Priority

Policy 3: This policy states any connection going to 155.40.23.5 for HTTP should NAT these connections and use only 1 WAN port until it fails then use the next in order.

Policy 4

0.0.0.0/0 Src Port *

0.0.0.0/0 Dest Port *

Protocol All

Default

Policy 4: This policy states any source bound for any destination should NAT and multiplex all connections.

Legend

* = All ports

Src = Source port

Dest = Destination port

Definitions

- **Interface Priority** = Use only the first port. If the first port fails use the second etc. If the First port comes back on line it will utilize it again
- **Interface Specific** = Utilize only the specific ports enabled. Whether NAT is enabled or disabled, if more that one port is checked than the connections are executed in a round robin fashion
- **Default** = All connections NAT and are multiplexed