



Configuring a Firewall for Access via the Internet/VPN

PROTOCOLS:

TCP/IP (Protocols 6 & 4)
 Nortel Contivity VPN Client Only (IPsec) UDP (Protocol 17)
 ISAKMP: UDP protocol on port 500 IPsec: ESP & AH (Protocols 50 & 51)
 UDP Source Port 4500 to UDP Destination Port 4500 (only required, In some cases where IPsec is used over PAT and NAT Traversal)

DESTINATION DNS Name & IP ADDRESSES for VPN Switches:

There are two 'connection points' available to Galileo's VPN There are advantages and disadvantages to the following connection points.

Connection Destination	Connection Type
fpnetipsec.galileo.com 198.151.32.105	Nortel Contivity IPsec VPN Client. Use this if your routers or firewalls do not require or support IPsec over PAT
fpnetnatt.galileo.com 198.151.32.110	Nortel Contivity IPsec VPN Client. Use this if your routers or firewalls require support for IPsec over PAT (NAT Traversal)

DNS SUPPORT:

The computer running the Nortel VPN client software must be able to 'resolve' and 'reach' the appropriate DNS name.(see above). If you have ICMP turned on, you should be able to ping the appropriate name and receive a reply. If, for some reason, ICMP is disabled on your network, you will not be able to ping the following two 'destinations'. Option #1 PING fpnetipsec.galileo.com (Nortel IPsec Client, default)

Option #2 PING fpnetnatt.galileo.com (Nortel IPsec Client, use with IPsec over PAT) Once the VPN tunnel has been established, you MUST be able to ping the following by DNS names. Even if your firewall(s), router(s) or both have ICMP disabled, you should be able to "ping" inside the VPN tunnel. It's important to be able to ping by DNS name, and not just by IP address. The Focalpoint and Galileo Print Manager software may not work properly if DNS is not properly configured, allowing you to ping the following two 'names'.

'Config' Server vpnipcs.galileo.com (should respond and resolve to 172.20.200.2)
 IP Concentrator vnpipc.galileo.com (should respond and resolve to 172.20.200.1)

Example how to configure an access-list

Source	Destination	Protocol	Port
LAN IP or 3rd party Router Public IP	198.151.32.0/24	udp (17)	500
LAN IP or 3rd party Router Public IP	198.151.32.0/24	ipsec esp (50)	N/A
LAN IP or 3rd party Router Public IP	198.151.32.0/24	udp (17)	4500
198.151.32.0/24	LAN IP or 3rd party Router Public IP	udp (17)	500
198.151.32.0/24	LAN IP or 3rd party Router Public IP	ipsec esp (50)	N/A
198.151.32.0/24	LAN IP or 3rd party Router Public IP	udp (17)	4500

