Digi Connect® WAN Application Helper

NAT, GRE, ESP and TCP/UPD Forwarding and IP Filtering

Introduction

The Digi Connect WAN supports five features which provide security and IP traffic forwarding when using incoming or mobile terminated connections:

1. Network Address Translation (NAT)
2. Generic Routing Encapsulation (GRE) forwarding
3. IPsec ESP protocol forwarding
4. TCP/UDP port forwarding
5. IP Filtering

This document describes each function, how they are used in conjunction with each other, how they are used, and what issues can occur with each if not used properly.

Network Address Translation (NAT)

NAT allows the Digi Connect WAN to have a single public IP address on the mobile link, while allowing multiple private IP-addressed devices connected to the Ethernet interface.

Outgoing traffic (mobile initiated) from the private network to the public mobile network assumes the IP address of the public mobile interface. An internal table tracks which internal IP address made the outgoing request so that responses get sent to the proper requestor.

For example, a workstation at IP address 192.168.1.15 sends a request to www.digi.com. The source IP address is changed by the Digi Connect WAN address translation to the public

Incoming (mobile terminated) traffic is either designated to the Digi Connect WAN itself (i.e. HTTP or telnet connections for configuration or monitoring), or is forwarded to hosts via the Ethernet interface based either on GRE or TCP/UDP port forwarding, which is covered below.

NAT provides two main benefits:

1. **Security:** NAT hides the private IP addresses of the devices on the Digi Connect WAN's Ethernet network.
2. **IP Address Availability**: IP addresses are in short supply and cost money. The Digi Connect WAN need be provided only one IP address from the wireless carrier.

NAT is enabled by default on the Digi Connect WAN. It should not be disabled unless there is a specific reason to do so.

Generic Routing Encapsulation (GRE) forwarding

GRE is a transport layer protocol, designated as IP protocol number 47, is used by many routers, WAN switches and VPN concentrators, to effectively tunnel traffic over a WAN between routers. Note that GRE itself provides no encryption but protocols such as PPTP

can use GRE. IPsec can be encapsulated in GRE (and vice-versa).GRE uses IP-in-IP and allows private IP addresses to be “tunneled” through a public network.

The Digi Connect WAN provides a simple checkbox to turn on GRE forwarding to pass GRE traffic from the mobile interface through to a router on the Ethernet interface. Note the Digi Connect WAN only passes GRE traffic and does not terminate it.

Following is an example diagram:

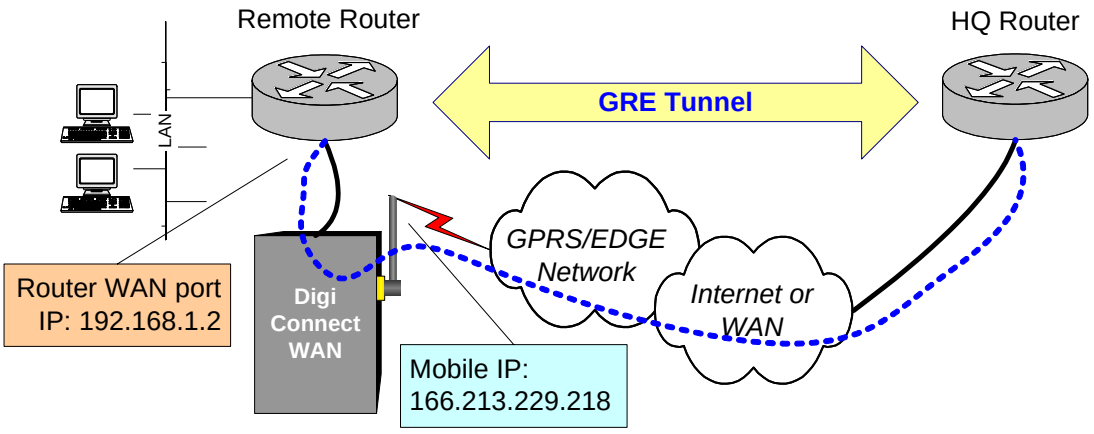

Figure 1 - GRE Forwarding

The HQ router’s peer GRE address is the mobile IP address of the Digi Connect WAN, which in this case is 166.213.229.218. The Digi Connect WAN has GRE forwarding enabled and will send to the router’s Ethernet WAN port, in this case 192.168.1.2. Typically this connection is a directly connected Ethernet cable.

An example similar to the above is where GRE tunneling is used to create a *backup* WAN connection to a primary Frame Relay connection through the Digi Connect WAN and wireless network. See the Digi Connect WAN application notes on primary and fail-over connection scenarios.

IPsec ESP Forwarding

IPsec ESP tunnel-mode traffic can be forwarded to a router or VPN appliance in the exact same manner as GRE. Simply check the ESP forwarding box and enter the IP address of the router/VPN appliance. UDP Port 500 may also be needed to forward IKE/ISAKMP traffic. See next section for details.

TCP/UDP Port Forwarding

Normally, traffic initiated from a host site to a Digi Connect WAN is blocked by NAT, unless the traffic is destined for the Digi Connect WAN itself. Port forwarding provides a means to pass traffic from the mobile interface to devices connected to the Digi Connect WAN’s Ethernet port. There are two main applications where port forwarding is required:

1. Pass application data traffic, such as polls or requests, to Ethernet connected devices
2. Pass VPN traffic, such as IPsec-in-UDP, through to routers or VPN appliances

For example, three devices are attached to the Digi Connect WAN's Ethernet port:

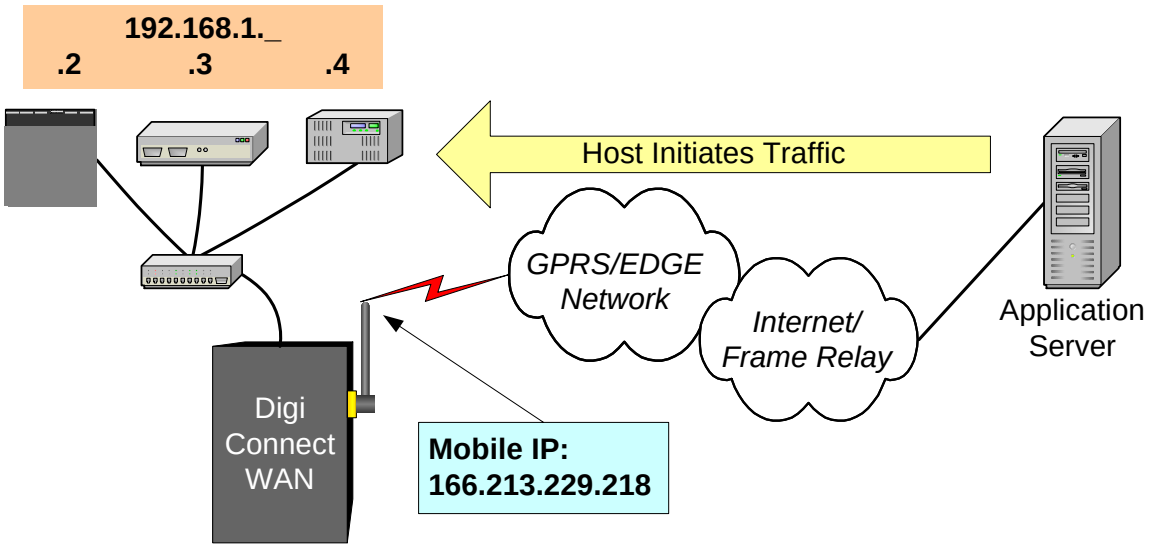

Figure 2 - TCP Port Forwarding

The application uses a protocol that polls the devices using the device IP address and TCP Port 502 (which is Modbus). On local LANs and publicly routable IP addresses this is not a problem.

NAT hides the private Ethernet IP addresses of the devices connected behind the Digi Connect WAN's Ethernet port. The application can then only send polls to one IP address – the mobile IP – in this case 166.213.229.218.

TCP port forwarding is used to forward the IP polls to one or more devices on the Digi Connect WAN Ethernet port. Different TCP port numbers are used to designate which device gets the proper traffic.The application *must* be able to support changing the TCP protocol port number from the default of 502. In this case the application is configured to poll according to this table:

Remote Device	Destination IP Address	Destination TCP Port
One	163.213.229.218	12001
Two	163.213.229.218	12002
Three	163.213.229.218	12003

Notice the destination IP address is the Digi Connect WAN's mobile IP address.

The Digi Connect WAN is configured with a TCP/UDP forwarding table as follows:

Source TCP Port	Destination IP Address	Destination TCP Port
12001	192.168.1.2	502
12002	192.168.1.3	502
12003	192.168.1.4	502

Incoming traffic is then 'routed' to the proper device. The devices can use their standard TCP port of 502.

The main issue with port forwarding in this case is when the polling application does *not* allow the user to specify the TCP or UDP port used. The workaround is to use

routers that support GRE, VPN or other forms of tunneling that can be forwarded through the Digi Connect WAN.

Another example of port forwarding is forwarding of IPsec-in-UDP traffic to a VPN appliance or router attached to the Digi Connect WAN's Ethernet port. Figure 1 above shows a GRE tunnel. In much the same way, IPsec traffic can be encapsulated in UDP to prevent NAT from modifying the IPsec headers (which would invalidate the traffic). IPsec-in-UDP implementations always use UDP Port 500 for IKE/ISAKMP, but can use various UDP port numbers for the AH/ESP traffic. Following is an example of UDP port forwarding entries on a Digi Connect WAN for IPsec in UDP:

Protocol	Source Port	Destination IP Address	Destination Port
UDP	500	192.168.1.2	500
UDP	4500	192.168.1.2	4500

IP Filtering

IP Filtering is a security feature that allows the user to block all incoming, mobile terminated traffic into the Digi Connect WAN, except for traffic from specific IP addresses and/or subnets. There are three IP filtering settings on the Digi Connect WAN:

1. Only allow access from the following devices and networks. When checked this blocks ALL incoming traffic except for the traffic from the IP address/subnets listed in the "allow access" tables.
2. Automatically allow access from all devices on the local subnet. This allows outbound traffic from the private Ethernet network out to the mobile network and beyond.
3. Allow access from the following devices and/or subnets. When the "Only allow access from the following devices and networks" box is checked, you must provide entries here to allow in-coming mobile traffic to be passed through the Digi Connect WAN.

CAUTION: Incorrect settings here can stop some or all traffic. For example, checking "Only allow access from the following devices and networks" without adding IP addresses or subnets to the "allow access" tables will block ALL incoming traffic – even responses – from outgoing requests.

Furthermore, the Digi Connect WAN is not a *stateful* firewall. That is, it does maintain a state table of out-going connections. For example, you attempt to open www.digi.com, but the IP address of www.digi.com is not in the "allow access" table. Responses back from www.digi.com are blocked.

Additional Assistance

If you have any questions or need assistance, please contact your Digi Connect WAN vendor or Digi International at 952-912-3444, or Digi technical support at http://www.digi.com/support/eservice/eservicelogin.jsp.