WHITE PAPER:
CONFIGURING A VIRTUAL PRIVATE NETWORK

Contributed by Caleb Payne May 2014

ABSTRACT

The use of telemetry devices equipped with cellular modems for low-bandwidth measurement and data collection has soared in recent years. There are many aspects to a successful deployment of cellular telemetry devices, from RF-based (signal strength, etc.) to network-based (security, routing, etc.). In some situations, simple static, public IP addressing can be used on cellular devices. In other cases, a private network arrangement must be created in partnership with a cell carrier, to guarantee end device network security. The process of creating a Virtual Private Network (VPN) between a local area network and a remote CDMA wireless service provider is outlined here. For details on GSM set up, download the white paper *Setting Up Custom GSM Cellular Access Points HERE.*

DEFINITIONS

Before beginning the discussion on how to create a VPN with a wireless provider, it is necessary to define a handful of terms. The following terms will be used throughout this white paper:

VPN: (Virtual Private Network) A Virtual Private Network allows a user to join two separate networks over a third and often times public network (typically the Internet). Two nodes are established as the "peering points" or "endpoints" within a VPN and are typically routers used to carry traffic between nodes at either end of the tunnel. What makes a VPN "Private" is that the traffic being sent between the endpoints is encrypted using one of many possible schemes. Without encryption, these networks are simply point-to-point tunnels, such as GRE.

GRE: (Generic Routing Encapsulation) GRE is a tunneling protocol that can be used to establish a point-to-point network between two nodes. Essentially, the protocol encapsulates traffic on top of an existing IP connection and routes it through a private IP address space selected by the user. This is very useful when the public IP addresses between the end points change – any nodes communicating between them will use the private IP address space specified when the tunnel was created, allowing any scripts or any other communication configurations to continue using the private IP address space instead of changing the public IP in each location.

IPSEC: (Internet Protocol SECurity) This is one of many implementations of VPN technology. The IPSEC protocol changes the packet data type at the IP level and encrypts the payload. When the recipient receives an IP packet with the specified IPSEC packet type, it decrypts the payload and forwards it to the desired recipient (or rejects it if authentication fails).

OpenVPN: OpenVPN is another implementation of the VPN technology. This implementation uses a high-security encryption algorithm and routes packets over the UDP protocol.

BGP: (Border Gateway Protocol) The Border Gateway Protocol is a routing protocol that is used to send routing information between two disparate networks. This protocol is used to shape the backbone of the entire Internet.

BENEFITS

The first step in this process is to determine whether or not setting up a VPN is a worthwhile endeavor. Creating a VPN with a CDMA wireless provider can take several months and involves many different steps on both sides of the tunnel. If a user is only planning on deploying a handful of telemetry devices, then perhaps using the carrier's available publicly assigned static (or even dynamic) IP addresses are sufficient. If, on the other hand, the user plans on deploying many hundreds or thousands of telemetry devices, then the costs alone associated with procuring so many public, static IP addresses may be prohibitive. Listed below are some of the benefits for creating a VPN with the wireless provider:

Security: By placing devices inside of a Virtual Private Network, they are no longer accessible "in the wild." The VPN uses a private address space specified by the user and is only accessible by nodes within the network itself.

Figure 1. From left: Boomerang 2S, Pole Mount, Plug-in, 3 phase

WHITE PAPER:
CONFIGURING A VIRTUAL PRIVATE NETWORK

Scalability: When creating a VPN with the wireless provider, the customer is allowed to specify a netmask of varying sizes (from /30 at the smallest, which provides 2 hosts, to a /13 at the largest, allowing 524286 hosts).

Isolation: As mentioned under "security" above, the devices in a VPN are isolated not only from the internet, but from other private networks as well. This can come in extremely handy, especially while troubleshooting.

NECESSARY COMPONENTS AND CONSIDERATIONS

In order to establish a new VPN tunnel with the wireless carrier there are a handful of items that will be needed by the customer. The following are a series of considerations that should be made that will influence the design of the customer's side of the network.

What size device pool will be needed? A wise rule-of-thumb in this case is to estimate the highest likely node count for the network, then multiply by 1.5. Pick the closest subnet mask that will encompass at least that many nodes.

What address range should be used? Depending on the answer to the question above, there are a series of private reserved address spaces that can be chosen from. For larger blocks, it may be necessary to use the 10.0.0.0/8 (class A) range (even though some wireless providers max out at a /13). Other possibilities are the 172.16.0.0/20 and 192.168.0.0/16 ranges. A quick note: (this will be described in more detail below) the user must actually specify two address ranges, the first for a private /30 GRE point-to-point tunnel, and the other for the device pool itself.

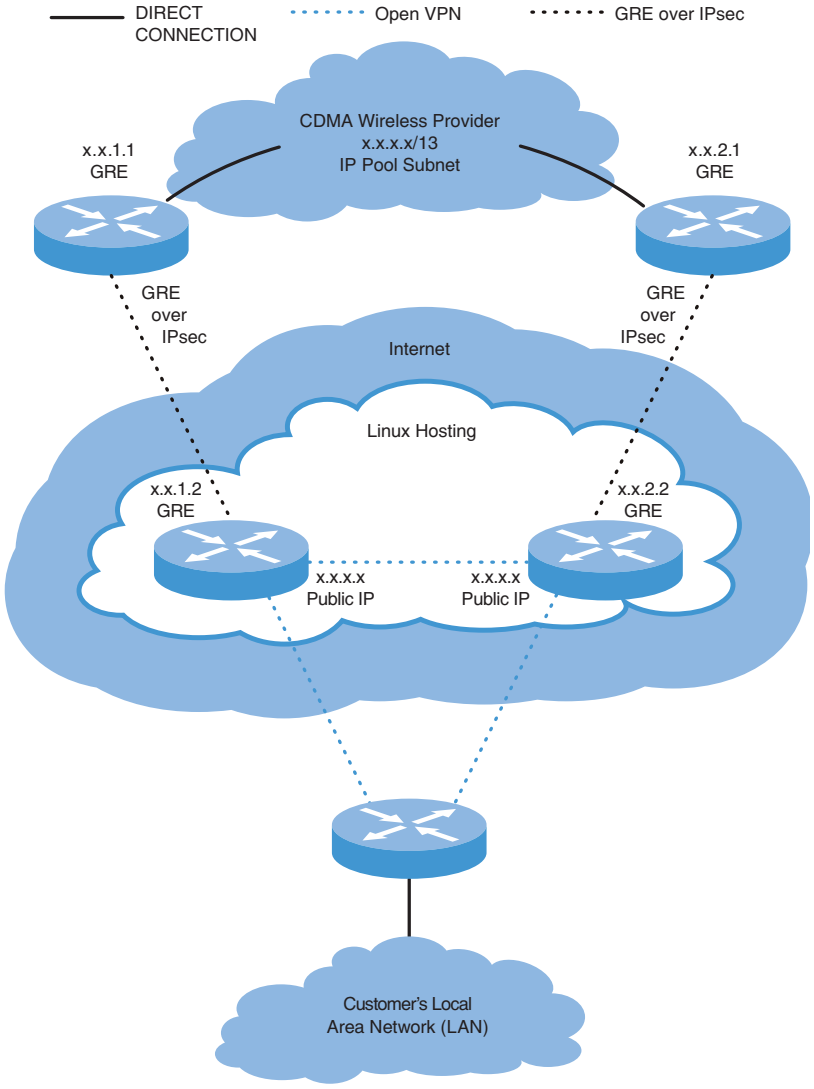

Figure 2. General structure

Where will the VPN tunnel endpoints be physically located? Most wireless providers require at least two end points for fail-over / disaster-recovery scenarios. If the primary tunnel goes down, traffic will be automatically rerouted to the secondary tunnel. It is recommended that the two endpoints be at geographically disparate locations with separate Internet Service Providers (ISPs). With this configuration, if a single endpoint fails, the odds of the other endpoint failing for the same reasons are much slimmer.

What type of hardware will be used? In general, any routers capable of GRE tunneling, IPSec tunneling, BGP routing, basic firewalling and packet forwarding / redirection will be sufficient. Some wireless providers can provide a specific list of Cisco and Juniper hardware models as known, working examples, but software defined routers running Linux (CentOS, which is a Red Hat Enterprise Linux clone) is known to work as well.

How will internal nodes be connected to the VPN? The CDMA carrier will be hosting all of the telemetry devices behind their VPN endpoint. The rest of the nodes, however, will be the responsibility of the end user. Remember that there will need to be machines capable of reaching this network for device configuration, probing, monitoring, etc. One practice is to create a second VPN from the CDMA endpoint back into the customer's LAN. This will be described in more detail below.

WHITE PAPER:
CONFIGURING A VIRTUAL PRIVATE NETWORK

GENERAL STRUCTURE

The general structure of the network is as follows: an IPSec tunnel is established between the customer's endpoint on a public, static IP address and is terminated at the public, static IP address of the CDMA wireless carrier's endpoint. See Figure 2. Some carriers may require that transport mode be used instead of tunnel mode for the IPSec tunnel and that a PSK (Private Shared Key) be used instead of certificates.

Once the IPSec tunnel has been established and traffic is flowing, the GRE tunnel can be brought up. The GRE (Generic Routing Encapsulation) tunnel (point-to-point) is established between the customer's endpoint through the IPSec tunnel on a public, static IP address and is terminated at the public, static IP address of the CDMA wireless carrier's endpoint. The subnet for this small network, as directed by the wireless provider, must be a /30 (to allow only the two endpoints). The customer's endpoint will be the x.x.x.2 while the CDMA provider will be the x.x.x.1 in the tunnel.

Having established both the IPSec and GRE tunnels between the endpoints with traffic flowing, it is now time to bring up the BGP (Border Gateway Protocol) service. At this point, any internal routes that the telemetry devices will need to know about (i.e., if the customer wishes the telemetry devices to be able to tunnel through the VPN back into the customer's LAN) must be specified and broadcast through the BGP router. Additionally, the BGP service should be configured to accept the incoming routes (which were selected as part of the device pool determination mentioned earlier) and update routing tables accordingly.

After the BGP service has been configured and is running, routes should be being broadcast between the customer's endpoint and the remote CDMA wireless provider's endpoint. At this time, traffic from any network that the customer is broadcasting through the BGP service should be routed through the tunnel and delivered to the CDMA provider's endpoint. A simple ICMP ping will likely be sufficient during testing.

It was mentioned earlier under the "Considerations" section that more details would be provided regarding the OpenVPN configuration. A hypothetical configuration could use two CentOS virtual machines as software defined routers for VPN endpoints. These routers will be geographically disparate and on separate networks. To join these disparate networks together and link them back with the customer's LAN, an OpenVPN tunnel can be set up on the endpoints (this is not a requirement by the wireless provider). The OpenVPN tunnel's network can be the actual network that is broadcast through BGP back to the CDMA provider's network. This serves several purposes, security being primary among them. By using OpenVPN to create a new network and broadcasting that network to the peer, the customer will be able to successfully allow the telemetry network to tie into the customer's LAN, but only through nodes connected through OpenVPN (prohibiting all other nodes on the customer's LAN from communicating with the telemetry network).

CONCLUSION

Setting up a VPN with a CDMA wireless provider can be a long and somewhat tedious process, but provides several benefits, and may be required in some security situations. With a router that meets the minimum capabilities, the system can be set up for a minimal cost (Linux) – or the user can opt to use a more widely used piece of hardware (such as that available from Cisco and Juniper).

Caleb Payne
Manager of Software Development
cpayne@powermonitors.com
www.powermonitors.com
800.296.4120

RECOMMENDED READING

The following publications are useful creating secure VPNs to cell carriers:

Bantoft, Ken. *OpenSwan: Building and Integrating Virtual Private Networks*

Zhang, Randy. *BGP Design and Implementation*

