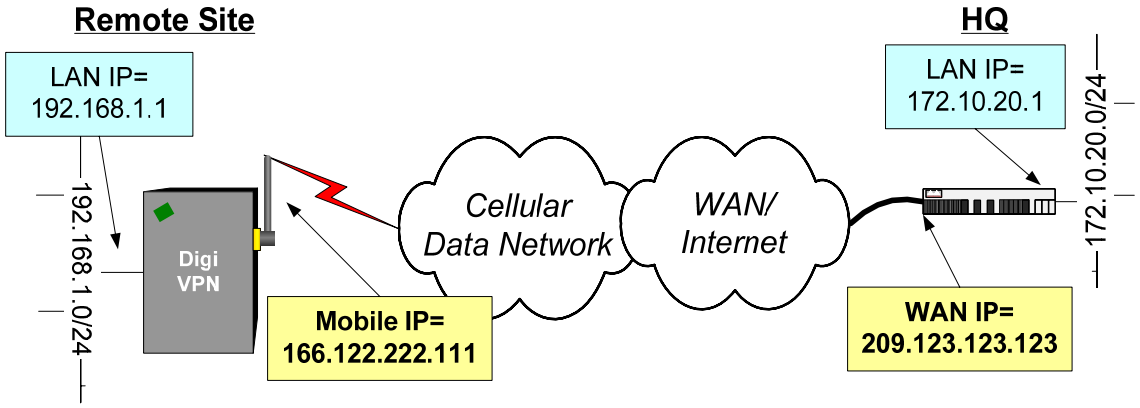
Digi Cellular Router Application Guide:
Configuring a VPN connection between a Cisco IOS Router and a Digi Cellular Router

Introduction

This is a sample configuration of an IPsec VPN tunnel from a Digi VPN device, such as a ConnectPort WAN VPN, to a Cisco IOS-based router. Sections in this document are:

1. Example diagram and VPN parameters used.
2. Cisco VPN configuration settings. Knowledge of Cisco IOS is assumed and required. Digi does not provide support for non-Digi device configuration. Embedded notes in the sample config file help describe the settings.
3. Digi cellular device's IPsec WebUI configuration
4. Testing and basic troubleshooting

1. Example Diagram and VPN Parameters



VPN Parameters:

- Identity: Mobile IP address (FQDN/FQUN if dynamic IPs are used)
- Pre-Shared Key: 1s3d4f5g
- Main mode
- Encryption/Hash transforms: 3des/md5; des/MD5
- Diffie-Helman Group: 2
- Perfect-Forward Secrecy (PFS) enabled
- SA Lifetime 86400 secs.

2. Cisco Sample Config File:

This configuration file describes how to setup a configuration to accept a VPN connection from a Digi Connect VPN. Two pre-shared key definitions are listed:
(1) Is for a single static mobile IP address. Multiple entries are needed for each mobile IP address. (2) Covers either a range of static IPs or more likely is used when *dynamic* mobile IP addresses are used. See the Key section a few lines down.

```
! Cisco Local IP address is 172.10.20.1/24
! Digi Unit Local IP address (Ethernet) is 192.168.1.1/24
!
! ISAKMP Phase 1 config:
crypto isakmp policy 2
 encr 3des
 hash md5
 authentication pre-share

! KEY SECTION
! (1) Define the key if a STATIC mobile is used:
crypto isakmp key 1s3d4f5g address 166.122.222.111 no-xauth

! (2) Define the shared key for a number of mobile devices that share an address
! range. This shared key will work for all devices that have an IP address in
! the subnet: 166.122.0.0/16 This is useful for dynamic IPs in this range.
crypto isakmp key 1s3d4f5g address 166.122.0.0 255.255.0.0 no-xauth

! Define the transforms that can be used.
crypto ipsec transform-set tset-des-md5 esp-des esp-md5-hmac
crypto ipsec transform-set tset-3des-md5 esp-3des esp-md5-hmac
crypto ipsec transform-set tset-aes256 esp-aes 256
crypto ipsec transform-set tset-aes256-md5 esp-aes 256 esp-md5-hmac

! Setup the dynamic crypto map that will be used as a template
crypto dynamic-map digivpn 10
  set transform-set tset-des-md5 tset-3des-md5 tset-aes256 tset-aes256-md5
  set pfs group2
  match address101
  reverse-route

! Setup the crypto map that will be applied to the interface
crypto map digi-crypto-map 10 ipsec-isakmp dynamic digivpn

! Configure the access list that will define the VPN
! This map defines what data is going to be protected by the VPN
! The form is
!
!  <LAN on the Cisco router> <inverse-subnet-mask> <LAN on the Digi unit> <inverse-
subnet-mask>
!
! Access list 101 says that if a packet matches source 172.10.20.0/24 to
! destination 192.168.1.0/24 (from the Cisco perspective), then it should be
! run through the VPN.  The Cisco configuration will automatically set up
! the reverse of this to allow traffic from the other direction.

access-list 101 permit ip 172.10.20.0 0.0.0.255 192.168.1.0 0.0.0.255

! Finally, apply the transform to the ethernet interface:
interface Ethernet0/0
  description Public IP connected to the Internet
  ...
  crypto map digi-crypto-map
```

3. Digi VPN Config:

1. Using a browser, access the Digi's WebUI (e.g. http://192.168.1.1)
2. In the left column, select "Configuration" -> "Network"
3. Select the "Virtual Private Network (VPN) Settings" link in the middle of the page.
4. Select the first link ("VPN IKE Settings")
5. Identity: select "Use the Mobile IP address as the identity"
6. General Security Settings

   a. "Connection Mode": Main
   b. "Diffie-Hellman": Group 2
   c. Check to "Enable Perfect Forward Secrecy (PFS)"

7. Under “Internet Key Exchange (IKE) Security Settings”
   a. Select "Use the following policies to negotiate Internet Key Exchange (IKE) security settings"
   b. Remove any items
   c. Select 3DES and MD5 for Encryption and Authentication. Leave the SA Lifetime at 86400. Click "Add".
   d. Select DES and MD5. Leave the SA Lifetime at 86400. Click “Add”.
8. Click “Apply”
9. Select "VPN Policy Settings" link just below the Apply button. (Make sure you clicked the Apply button as mentioned above or your changes will be lost).
   a. Remove any unneeded tunnels by selecting the "delete" link.
   b. Click "Add" to add a new tunnel
   c. Enter the WAN IP address or hostname of the Cisco router at the other end of the tunnel, in this example 209.123.123.123. The IP address must usually be a public IP address reachable from the wireless address of the Digi Connect unit.
10. Under "VPN Tunnel:" Select "ISAKMP"
11. Under the heading: "Tunnel Network Traffic FROM the following Local Network" (this is the local subnet attached to the Digi router):
    a. Verify the IP address corresponds to the subnet of the local Ethernet address (in this case 192.168.1.0/255.255.255.0). If the address is not the same, change the local Ethernet IP address/subnet to the proper address under the Configuration->Network link on the left side of the page.
    b. Verify the subnet mask is appropriate for the tunnel you want to create.
    c. Note that the IP address and subnet mask define the SOURCE address range for traffic that will be sent through the tunnel from the remote network.
12. Under the heading "Tunnel Network Traffic TO the following Remote Network" (this is the subnet attached to the Cisco router)
    a. Enter the IP address of the network that the data will be flowing TO. This is the network part of the address that is defined on the LOCAL side of the Cisco Router. In this case 172.10.20.0.
    b. Enter the appropriate Subnet Mask that defines the LOCAL side of the Cisco Router – in this case 255.255.255.0.
13. Click “Apply” to save the information.

The Digi VPN configuration is now complete.

4. Testing and Basic Troubleshooting

By default the VPN tunnel does not initiate automatically[1]. Follow the information below to help initiate the tunnel and diagnose connection problems.

1. Select the Diagnostics link at the bottom of the page. Enter an IP address of a host on remote end of the tunnel (the local side of the Cisco router), e.g. 172.10.20.1. The IP address needs to be an actual interface IP address. Click on the Ping button. Wait for the connection to respond correctly.
   --or--
   Generate traffic from the remote subnet to the HQ subnet. For example from 192.168.1.100 try pinging 172.10.20.1. The first few pings will say "Destination Host Unreachable" as 172.17.1.100 does not yet know the route to the remote site until the VPN tunnel is built. After the VPN tunnel is established, the ping will likely timeout but should respond after a few pings. If you continue to get "Destination Host Unreachable" messages, the tunnel in never being built.
2. If you do not get a valid response, verify the IP address is ping-able (i.e. not filtering ICMP).
3. Cross-check and re-check the VPN parameters on both units. They ahould match exactly (except for possibly the life-time settings; make them the same anyway).
4. Check the Cisco router logs. (*As of this writing the Digi router has no VPN logs*).
5. Check the VPN connection status from the Digi's command line via the "display vpn" command. Look for the SADB Table which shows the active connection. See the Digi *Command Reference* for more details.

5. Where to Get More Information

Further details and information are available in the *User's Guide*, *Command Reference* and **Application Docs** available from Digi's support (www.digi.com/support) and product website docs links (http://www.digi.com/products/wireless/cellular.jsp, select the appropriate product, then click on the "Documents" tab). For example, a more detailed generic VPN doc is available here: http://ftp1.digi.com/support/documentation/appguide_digiconnectvpn.pdf.

Refer to the Digi Connect WAN user documentation and Digi technical support website at www.digi.com/support for more information. Technical assistance is available at http://www.digi.com/support/eservice/.

For sales and product information, please contact Digi International at 952-912-3444 or via www.digi.com.

[1] Traffic generated by Digi's SureLink Link Integrity Monitoring or Connectware Manager remote management traffic can be used to 'automatically' initiate the VPN negotiation. See the Digi application note on Using SureLink to Initiate a VPN Tunnel at the "documents" link above.