GRE Tunnel over IPSec Configuration

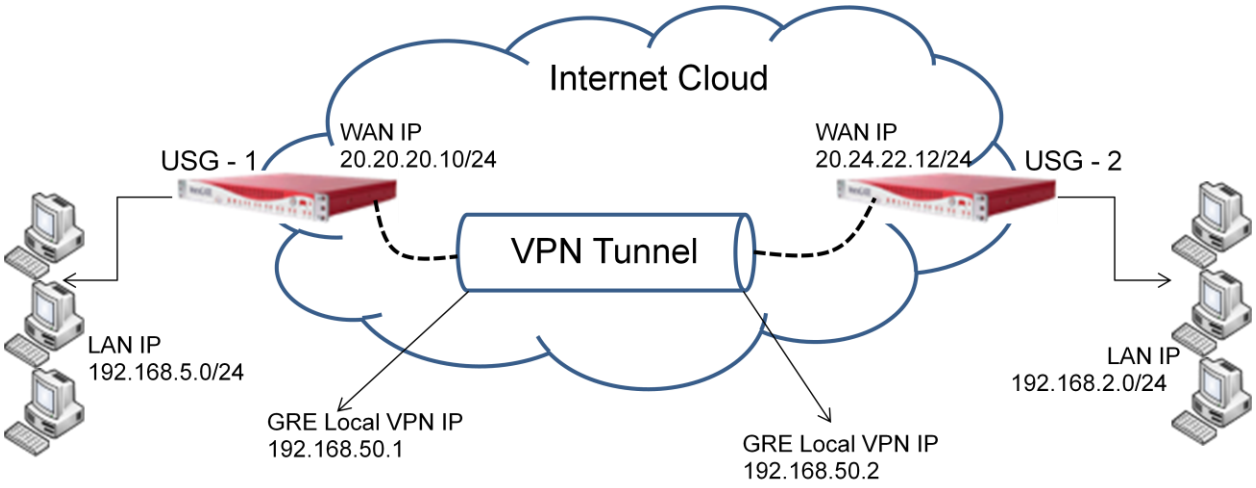
This document helps with

- a brief explanation of GRE Tunnel over IPSec
- step by step procedure with screenshot to configure in USG
- steps to verify the configured tunnel is working

Generic Routing Encapsulation (GRE) is a tunneling protocol that allows the encapsulation of many different network layer protocols between two endpoints. Packets are sent through a virtual tunnel on a point-to-point link.

It is important to understand that GRE tunnels do not encrypt traffic in any way; they are simply encapsulated within an additional GRE and IP header. If a secure tunnel is required, IPSec can be used with GRE to provide data confidentiality.

GRE over IPSec tunnels are different from stand-alone IPSec VPN tunnels. GRE over IPSec tunnels support multicast IP traffic, which strict IPSec VPNs do not. This is important when routing protocols need to send routing information across the tunnel since they use multicast for their control information.



Few points to remember

- GRE Tunnel over IPSec has two modes
  - Tunnel Mode : This work with dynamic IP
  - Transport Mode: Only work with Static IP on both ends.
- MTU setting in GRE Tunnel interface in general set as 1400 - 1420. This is to avoid any fragmentation problems over the transport networks. Remember that GRE adds an additional 20-byte IP header as well as a 4-byte GRE header to each packet in the tunnel.

How to configure IPSec VPN Tunnel for Transport GRE in USG?

- Ensure whether you are ready with phase I and phase II details before configuring the IPSec VPN Tunnel
- This is not a generic IPSec VPN tunnel, hence care need to be taken while configuring the tunnel.

Example Phase I & Phase II Requirement document

Phase I Configuration		Phase II Configuration	
IKE Encryption	3DES	IPSec Encryption/HMAC	3DES/SHA
Hash Algorithm	SHA1	D H Group	Group 2
Security Association Lifetime	7200	Security Association Lifetime	3600
DH Group	Group2	Perfect Forward Secrecy	Enabled
Authentication Method Pre-Share –Key	<Need to create one and share the same to remote end>	Note: The WAN IP of both the locations are required for this configuration.	

1. Creating IPSec Tunnel in Transport GRE mode in USG

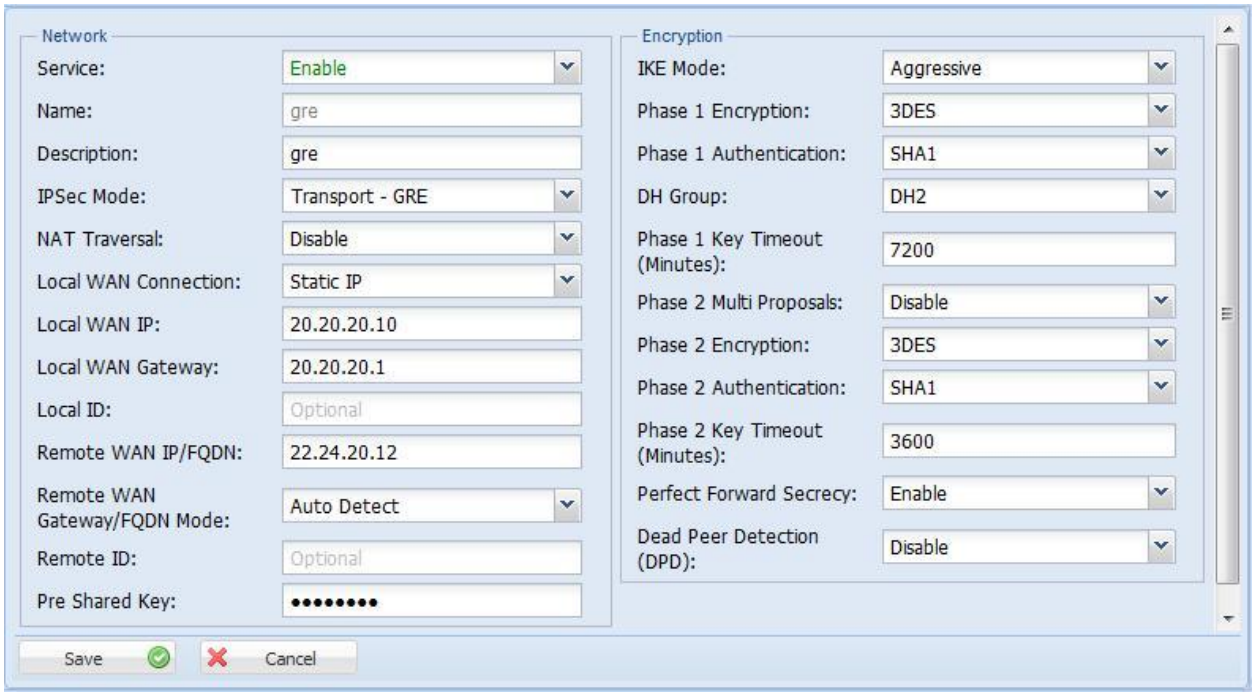
As mentioned above, GRE provides no form of payload confidentiality or encryption. If the packets are sniffed over the public networks, their contents are in plain-text.

IPSec solves the security concerns by encrypting part or all of the GRE packets. There are two IPSec tunnel modes – tunnel and transport. This configuration steps below shows, Transport GRE mode IPSec.

Step 1:

- In configuration menu, choose VPN and select IPSec VPN
- Click “Add” which opens up “IPSec VPN – New Tunnel” tab
- Service by default “Enable”
- Provide a name to the tunnel. For example “gre”
- Description is optional field. Enter “USG-1” for easy identification
- Choose IPSec Mode as “ Transport GRE”
- NAT Traversal by default “disable”. Choice is based on remote end configuration
- Choose “Static IP” for Local WAN Connection tab
- Enter Local WAN IP, in this example it is “20.20.20.10”
- Enter Local WAN GW, in this example it is “20.20.20.1”
- Local ID is also optional field. This field is used mostly in dynamic IP configuration.
- In Remote WAN IP / FQDN field enter remote end WAN IP. In this example it is “20.24.22.12”
- Remote WAN Gateway by default is “Auto Detect”. If GW IP is known and need to be entered, choose “Specify” to enter.
- “Remote ID” is optional and used only if Local ID is used

- Pre Shared Key is the password key need to be generated by the HO side IPSec VPN Tunnel and the same need to be passed to the branch end. In this example USG-1 considered as HO and hence a Pre Shared Key is entered and the same is passed on to USG-2 end. It can of alpha, numeric and special characters.
- Phase I and Phase II as per the configuration table provided above choose the appropriate values
- Dead Peer Detection (DPD) by default is “Disabled” and most of the cases remains “Disabled”. If the HO side is enabled then the branch end also need to be enabled.



Note: Follow the same steps above to create the IPSec Tunnel in Branch end, in this example in USG-2 end. Ensure the Local IP and Remote IP is entered correctly .For USG-2, USG-1 is remote end.

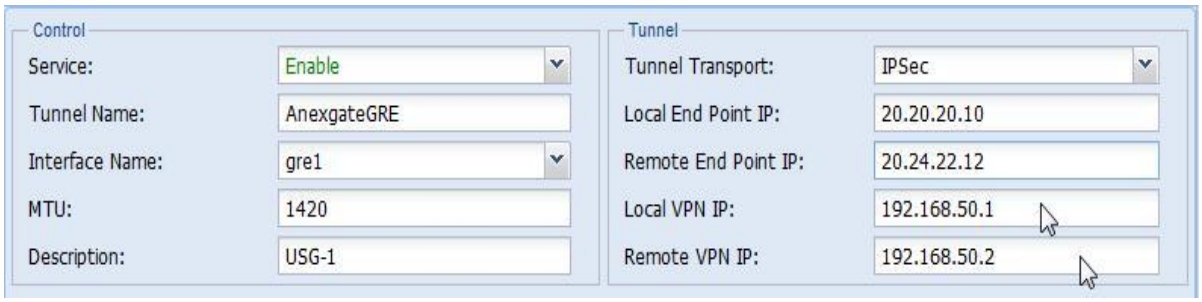
2. Creating GRE Tunnel Interface in USG

A GRE tunnel uses a virtual tunnel interface, configured with an IP address where packets are encapsulated / de-capsulated as they enter and exit the GRE tunnel. The IP address must be in the same subnet on both USG tunnel interfaces. Ensure the IP Segment used in GRE is unique and not used in the existing network. Same is named in USG as “Local VPN IP” and “Remote VPN IP”

Step 1:

- In configuration menu, choose VPN and select GRE Tunnel
- Click “Add” which opens up “GRE Tunnel – New Tunnel” tab
- Service by default “Enable”
- Provide a “Tunnel Name” which is used to easily identify the created tunnel.

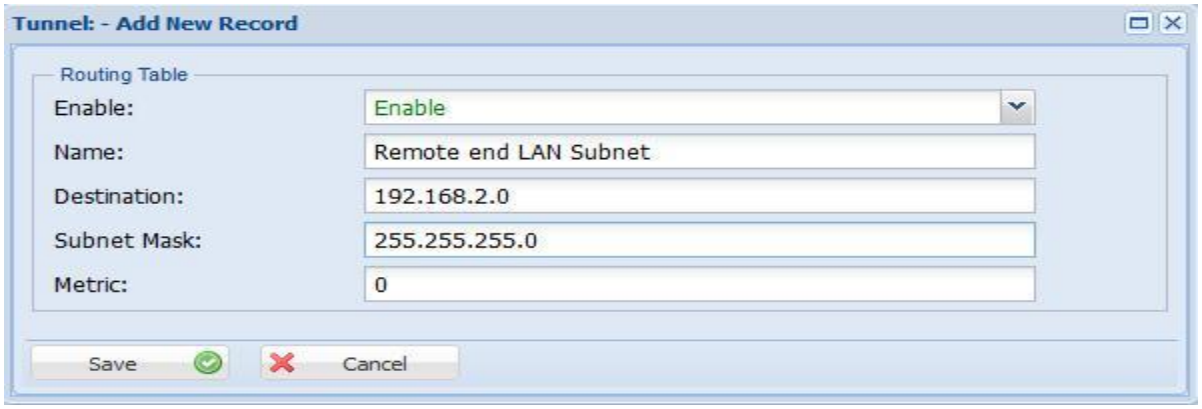
- Interface Name: Choose “gre1” or one of the available GRE interface.
  - *Note: USG support 5 GRE interfaces*
- MTU default set to “1420”
- Description is an option field used to mention the location name for the created tunnel
- In Tunnel Transport: Choose “IPSec”
- Local end point IP is the WAN IP of USG-1 location
- Remote end point IP is the WAN IP of the USG-2 location (Remote end)
- Local VPN IP is the GRE Tunnel Interface IP for USG-1
- Remote VPN IP is the GRE Tunnel Interface IP for USG-2 (Remote end)
- Press “Save” to add remote end LAN subnet route.



Note: Follow the same steps above to create the GRE Tunnel in Branch end, in this example it is USG-2 end. Ensure the Local End Point IP / Local VPN IP and Remote End Point IP / Remote VPN IP is entered correctly. For USG-2, USG-1 is remote end.

Step 2: Adding routes to access the remote end LAN client machines

- Once the GRE basic configuration is saved, click on the “Add Route” in the submenu
- The route is “ENABLED” by default
- Provide a name for the Route entry, which is use to understand the requirement of this route
- Provide the destination LAN segment IP (ex: 192.168.2.0) in the Destination tab.
- In the SUBNET MASK tab, provide the subnet mask of the destination LAN segment
- Metric is provided as “0” by default.



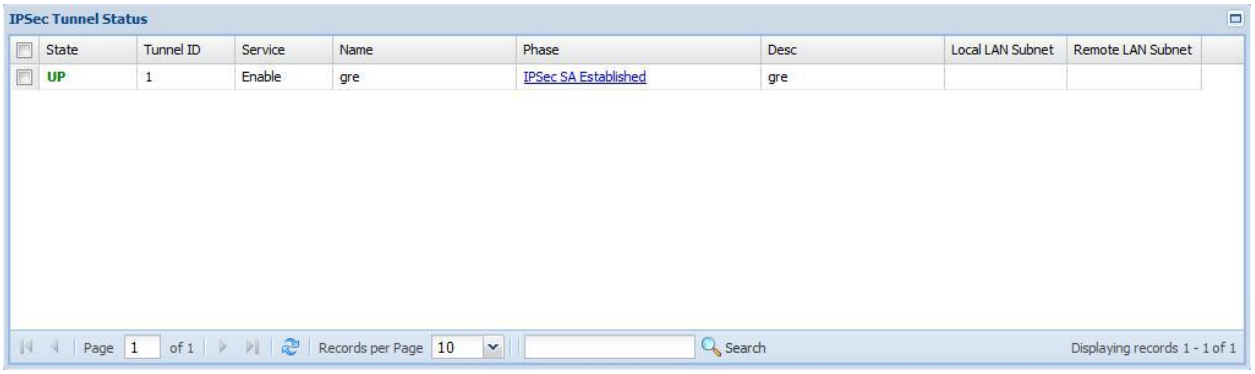
Note: Follow the same steps above to create the Routes for GRE Tunnel in Branch end, in this example it is USG-2 end. The Remote end LAN subnet IP is 192.168.5.0/24.

3. Verifying the created GRE over IPSec Tunnel in USG

Configuration of both USG-1 and USG-2 are done. Next question is how to verify whether the configuration is done correctly and its working as expected. Below steps provide the information about the established tunnels and also how to verify.

Step1: Verifying Created IPSec Tunnel

- In USG main window, click on "Status"
- Choose VPN and then IPSec VPN to view the "Tunnel Status"
- Tunnel status state show as "UP" and the phase should show "IPSec SA Established"



Step2: Verifying Created GRE Tunnel

- In USG main window, click on "Status"
- Choose VPN and then GRE Tunnel to view the "Tunnel Status"
- If the tunnel is created correctly, it will display the status like below with the local and peer end WAN IP and with the 2 routes in the routing table. One for the USG-2 end GRE VPN IP and second for USG-2 end LAN subnet.

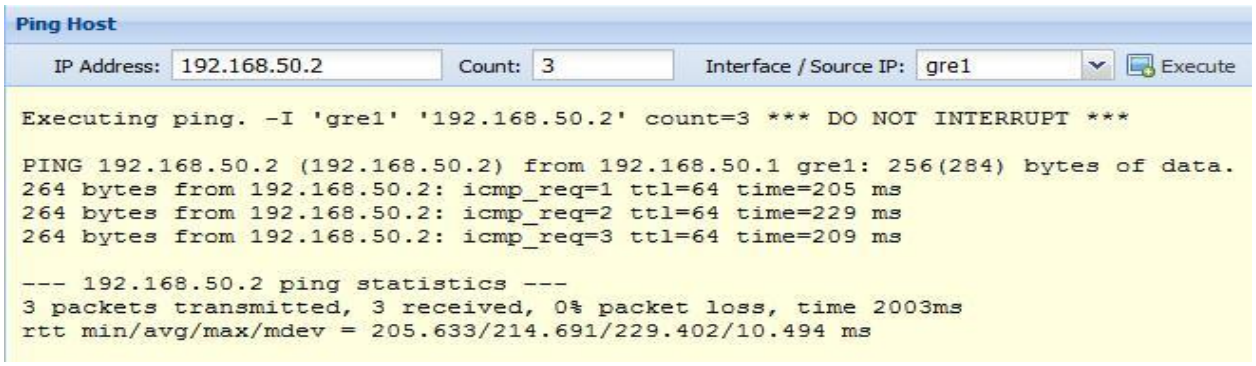
```
16: gre1: *POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP* mtu 1420
    link/gre 20.20.20.10 peer 20.22.24.12
    inet 192.168.50.1 peer 192.168.50.2/32 scope global gre1

Routing Table:
==============
Destination     Gateway     Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0     255.255.255.0   U     0      0        0 gre1
192.168.50.2    0.0.0.0     255.255.255.255 UH    0      0        0 gre1
```

- The same can be verified through Status / Troubleshoot / System Command / Routing Table

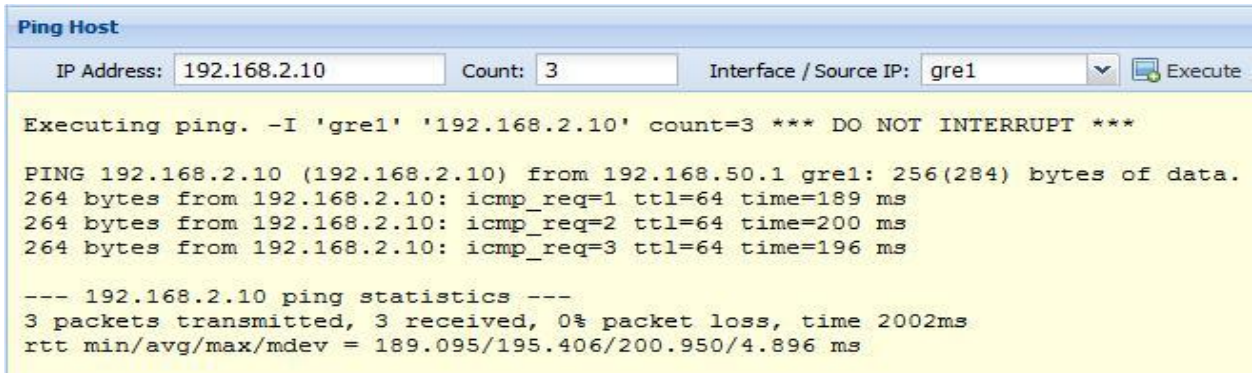
```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         20.20.20.10     0.0.0.0         UG    0      0        0 wan1
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 gre1
192.168.5.0     0.0.0.0         255.255.255.0   U     0      0        0 lan1
192.168.50.2    0.0.0.0         255.255.255.255 UH    0      0        0 gre1
192.168.254.252 0.0.0.0         255.255.255.252 U     0      0        0 lan1
```

Step3: Verifying established tunnels are reachable through ping command from both ends (USG-1 & USG-2)

- Choose Status / Troubleshoot / System Command / Ping Host command in the USG-1 appliance
- Type “192.168.50.2” in choose the interface as “gre1” and press execute
- This command should able to give ping response from USG-2 as shown below to ensure the GRE tunnel is established between USG-1 and USG-2



- Next is to check whether the Remote LAN subnet is reachable from USG-1
- In the ping host command of USG-1 type “192.168.2.10” and choose the interface as “gre1” and press execute.
- This command should able to give ping response from USG-2 LAN subnet as shown below



Note: Execute the same commands from USG-2 to ensure USG-1 LAN clients are reachable.