



# GRE over IPSec tunnel setup

## 6350-SR

# GRE over IPSec tunnel setup

Difficulty level: *advanced*

Minimum firmware: 18.10.225.15

## Goal

---

To setup a GRE tunnel through a secure IPSec tunnel

## Background

---

Digi ACL devices provide the option of setup up a GRE tunnel either as a standalone tunnel, or as an advertised set of routes through an IPSec tunnel. This allows users to leverage the dynamic route advertisement of GRE tunnels through a secured IPSec tunnel.

## Setup

---

You will need to configure the ACL device to establish an inbound or outbound IPSec tunnel. For details on configuring the IPSec tunnel, see the following link.

[VPN Access with IPSec tunnels](#)

## Sample Configuration

---

The following configuration setting show a sample setup of a GRE tunnel paired with an IPSec tunnel, where the IPSec tunnel setup is named *tunnel\_name* with a local tunnel network of 172.30.0.1/32 and a remote network of 172.30.0.2/32

1. VPN > IPsec > Tunnels > *tunnel name* > Policies  
Create or modify the IPSec tunnel to include a policy with specified remote and local network addresses.  
*Choosing 'Custom network' can be helpful here because you can see both IP addresses*
2. Network > Interfaces > Add Interface  
*Add a IPsec loopback endpoint.*
3. VPN > IP Tunnels > Add IP tunnel  
*The remote endpoint is the IPsec tunnel virtual IP at the other end and the local endpoint is the IPsec loopback endpoint interface we configured earlier.*
4. Network > Interfaces > Add Interface  
*Add an interface to the IP tunnel device. In this step we are creating a virtual IP address on the GRE tunnel.*

☰ Policies ▾

1. ☰ Policy ▾

☰ Local network ▾

Type	Custom network
Custom network	172.30.0.1/32
Remote network	172.30.0.2/32

Add Policy: Add

☰ ipsec\_endpoint ▾

Enable	<input checked="" type="checkbox"/>
Interface type	Ethernet
Zone	Internal
Device	Ethernet: Loopback

☰ IPv4 ▾

Enable	<input checked="" type="checkbox"/>
Type	Static IP address
Metric	0 <input type="text"/>
Weight	10 <input type="text"/>
Management priority	0 <input type="text"/>
MTU	1500 <input type="text"/>
Address	172.30.0.1/32
Default gateway	

☰ DNS servers ▾

☰ DHCP server ▾

☰ DHCP relay ▾

☰ Active recovery ▾

VPN ▾

IPsec ▾

OpenVPN ▾

IP Tunnels ▾

TUN0 ▾

Enable	▾	<input checked="" type="checkbox"/>
Mode	▾	GRE
Local endpoint	▾	Interface: ipsec_endpoint
Remote endpoint	▾	172.30.0.2
Key	▾	
Enable keepalive reply	▾	<input type="checkbox"/>

Add IP tunnel:

greiface ▾

Enable	▾	<input checked="" type="checkbox"/>
Interface type	▾	Ethernet
Zone	▾	Internal
Device	▾	IP tunnel: TUN0

IPv4 ▾

Enable	▾	<input checked="" type="checkbox"/>
Type	▾	Static IP address
Metric	▾	0 <input type="text"/>
Weight	▾	10 <input type="text"/>
Management priority	▾	0 <input type="text"/>
MTU	▾	1500 <input type="text"/>
Address	▾	172.31.0.1/30
Default gateway	▾	

DNS servers ▾

DHCP server ▾

DHCP relay ▾

Active recovery ▾

IPv6 ▾

MAC address blacklist ▾

MAC address whitelist ▾