Quick Note 061

Main Mode IPsec IKEv1 VPN from TransPort to StrongSwan using Preshared key

22 August 2017

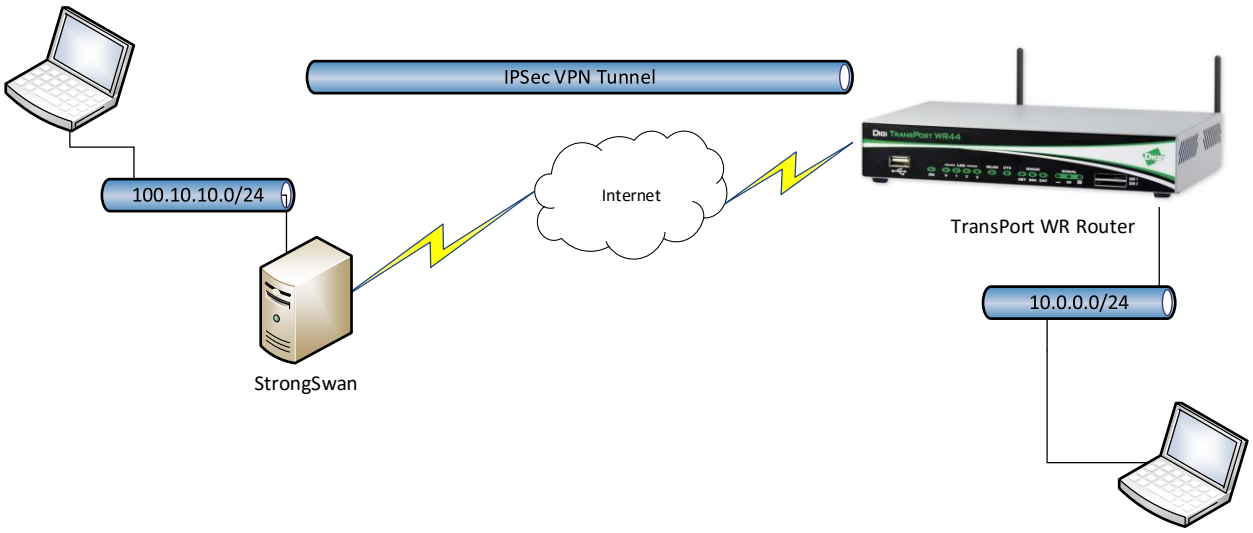
Contents

1 INTRODUCTION

1.1 Introduction

This document describes how to configure a VPN IPsec tunnel between a Digi TransPort WR to and a StrongSwan server using Main Mode, IKEv1 and pre-shared key authentication.

1.2 Network Diagram



1.3 Outline

This guide details the steps involved in configuring a Digi TransPort router to act as an IPsec VPN client to a StrongSwan appliance configured as an IPsec VPN server using Main Mode, IKEv1 and pre-shared key authentication. This example assumes that both equipment's are not behind a NAT box.

1.4 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router and configure it with basic routing functions

This application note applies to:

Model: Digi TransPort WR11/21/31/41/44

Firmware versions:
WR21: 5.2.17.10 and later

Configuration: This document assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

Please note: This application note has been specifically rewritten for the specified firmware versions and later but will work on earlier versions of firmware. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort WR routers.

1.5 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com Requests for new application notes can be sent to the same address.

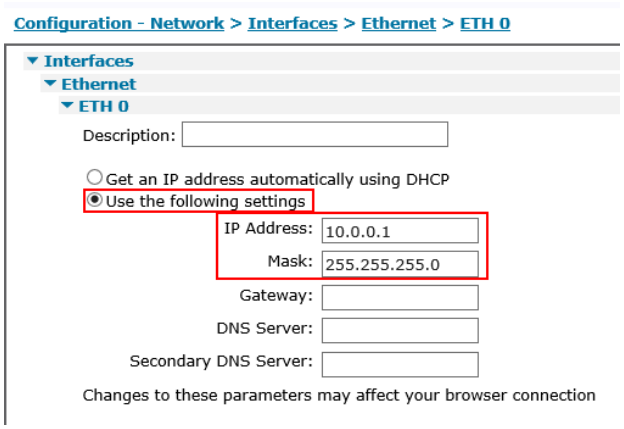
1.6 Version

Version Number	Status
1.0	Completed 14.08.2017

2 TRANSPORT CONFIGURATION

2.1 Local Ethernet Interface Configuration

Navigate to **Configuration – Network > Interfaces > Ethernet > Ethernet 0**



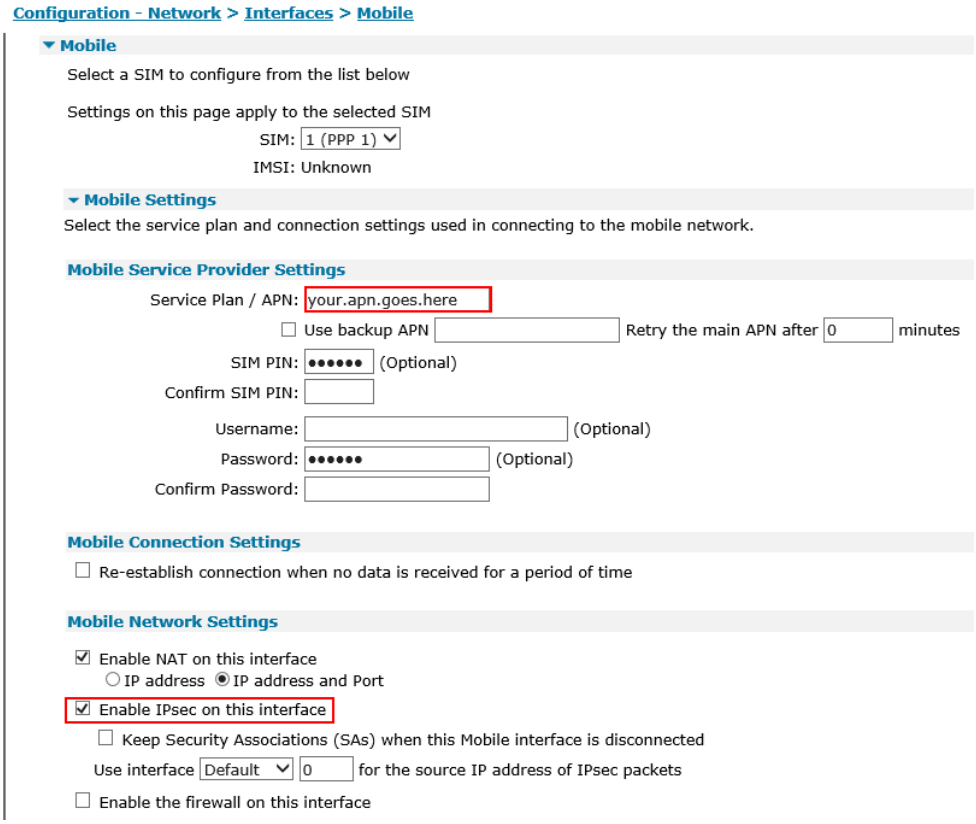
Parameter	Setting	Description
Use the following settings	Checked	A static IP Address will be used in this example
IP Address	10.0.0.1	IP Address of the TransPort WR21 Ethernet Interface. In this example, this IP Address is in the subnet range used for the Tunnel (useful for testing)
Mask	255.255.255.0	Subnet mask

2.1 WAN interface configuration

In this example, the mobile interface will be used as the WAN interface on which the IPsec tunnel will be established.

Navigate to:

Configuration – Network > Interfaces > Mobile



Parameter	Setting	Description
Service Plan / APN	Your.APN.goes.here	Enther the APN of your mobile provider
Enable IPsec on this interface	Checked	Enable IPsec to be built on this WAN interface

Please note: If required, enter a SIM PIN and Username/Password for this SIM card and APN.

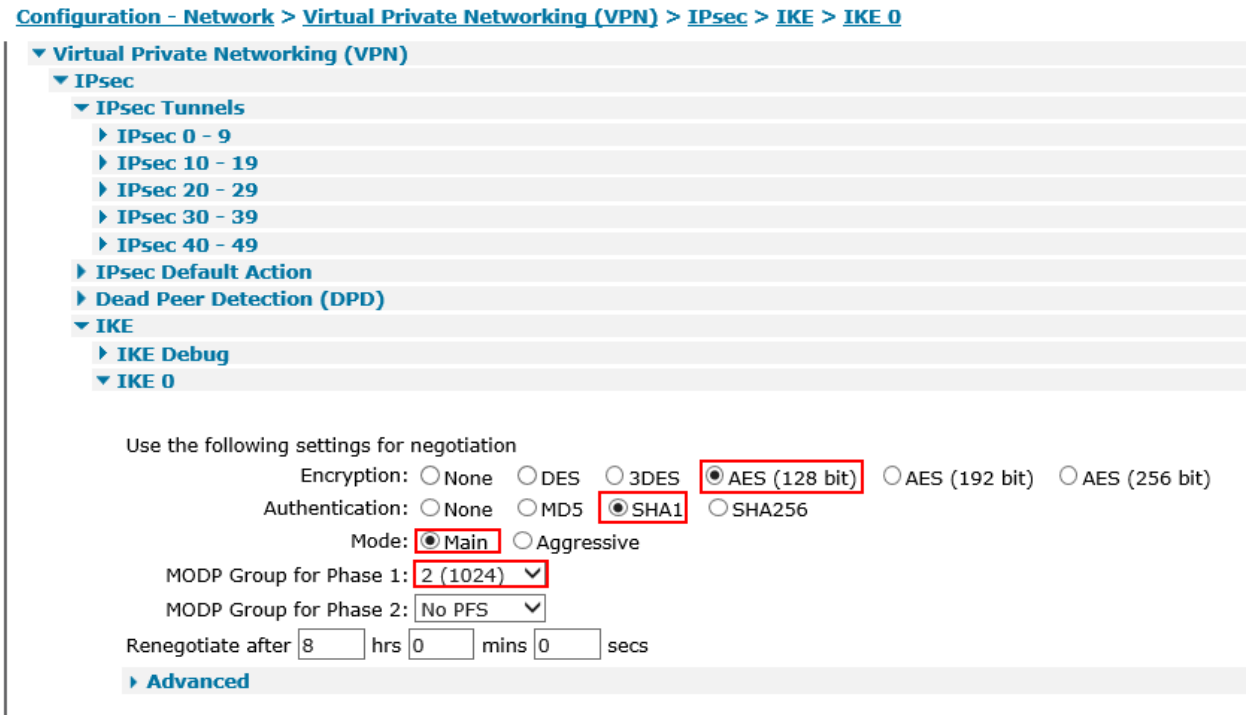
2.1 Tunnel Configuration

Open a web browser to the IP address of the TransPort WR21 router.

2.1.1 Phase 1 Settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) >IKE > IKE 0

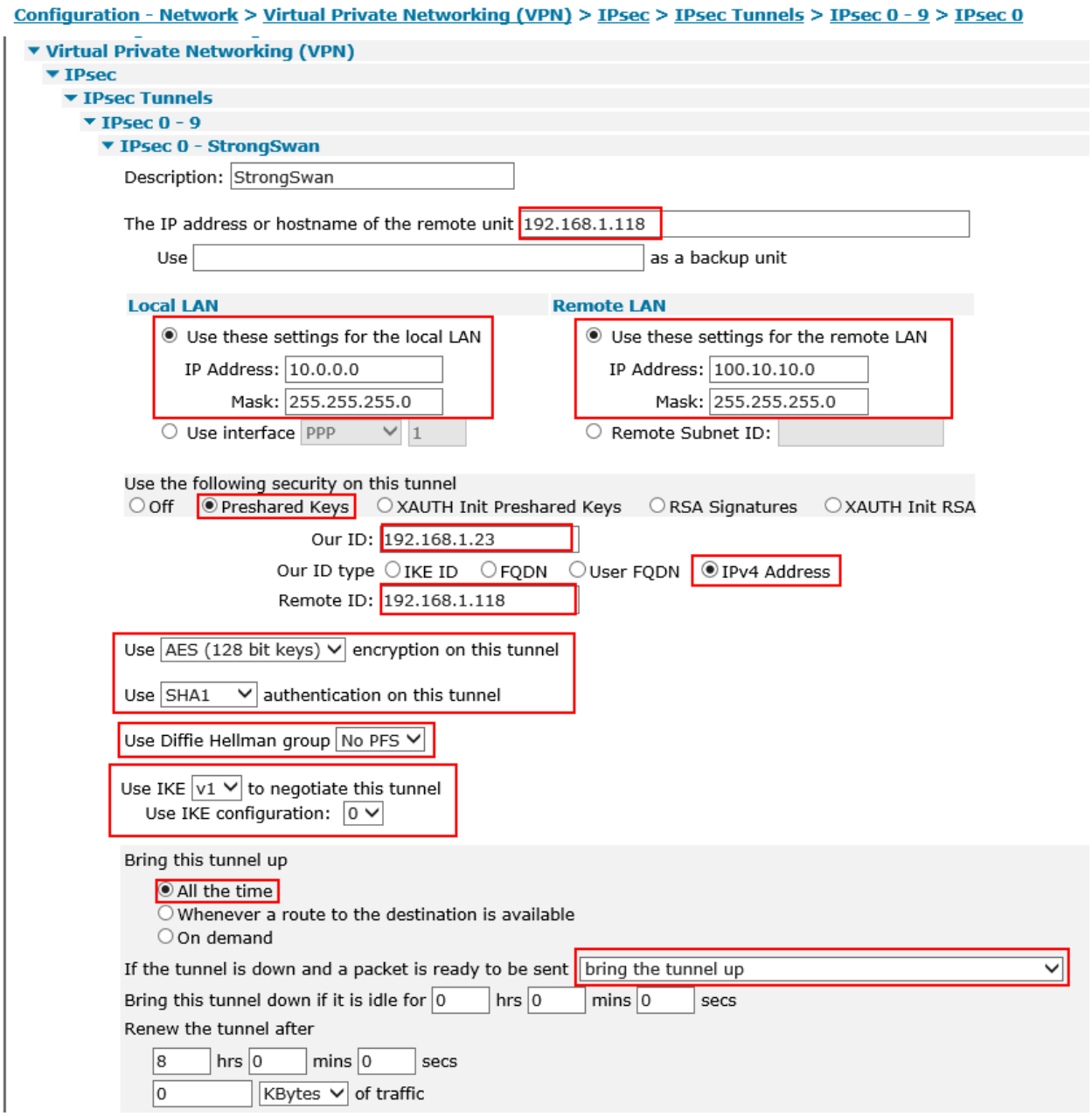


Parameter	Setting	Description
Encryption	AES (128 bit)	Encryption algorithm used in this tunnel
Authentication	SHA1	Authentication algorithm used in this tunnel
Mode	Main	IKE Mode used in this tunnel
MODP Group for Phase 1	2 (1024)	Key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	No PFS	Key length used in the ESP Diffie-Hellman exchange

2.1.2 Phase 2 settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec 0 – 9 > IPsec 0

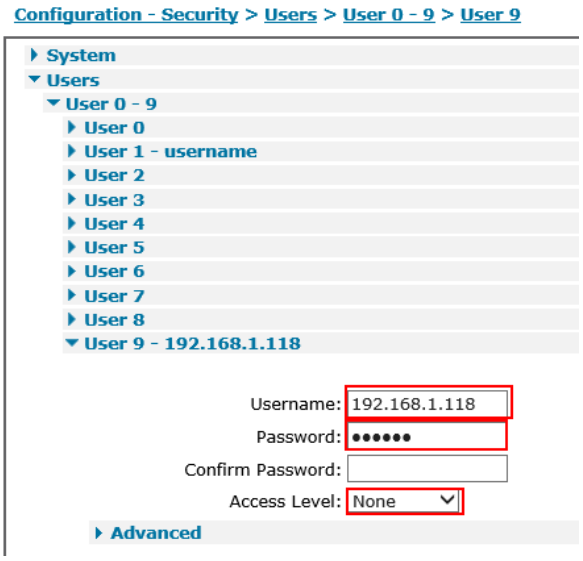


Parameter	Setting	Description
The IP address or hostname of the remote unit	192.168.1.118	WAN IP Address of the StrongSwan
Local LAN settings		
Use these settings for the local LAN	Checked	Local LAN subnet
IP Address	10.0.0.0	Local LAN subnet IP Address
Mask	255.255.255.0	Local LAN subnet mask
Remote LAN settings		
Use these settings for the local LAN	Checked	Remote LAN subnet
IP Address	100.10.10.0	Remote LAN subnet IP Address
Mask	255.255.255.0	Remote LAN subnet mask
Tunnel Security		
Preshared Keys	Checked	Use Preshared keys for authentication on this tunnel
Our ID	192.168.1.23	The ID of the VPN initiator router (this router). In our case, the WAN IP Address
Remote ID	192.168.1.118	The ID of the VPN responder router (remote router). In this case, the WAN IP Address
Our ID type	IPv4 Address	Use IPv4 as the type ID
Use () encryption on this tunnel	AES (128 bit keys)	The IPsec encryption algorithm to use is AES
Use () authentication on this tunnel	SHA1	The IPsec ESP authentication to use is SHA1
Tunnel creation		
Bring this tunnel up	On demand	Always on tunnel
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	

Click **Apply**

2.2 Configure users

Navigate to **Configuration - Security > Users > User 0-9 > User 9**



Here the pre-shared key is configured using the WAN IP address of the StrongSwan. The username value should therefore match the Peer ID set in the IPsec configuration above:

Parameter	Setting	Description
Username	192.168.1.118	Enter the IP Address of the StrongSwan (WAN)
Password	digidigi	Enter the Preshared Key
Access Level	None	As this user is only for the pre-shared key, no access will be granted to the router for this username

3 STRONGSWAN CONFIGURATION

3.1 Configure Ethernet Interfaces

3.1.1 WAN Interface

Configure the WAN interface for the StrongSwan Server. In this example, the Ethernet interface used for WAN is called ens33

```
root@ubuntu:/home/digi# ifconfig ens33 192.168.1.118
root@ubuntu:/home/digi# ifconfig ens33 netmask 255.255.255.0
root@ubuntu:/home/digi# route add default gw 192.168.1.254 ens33
```

3.1.2 Local Interface

Configure the Local interface for the StrongSwan Server. In this example, the Ethernet interface used for LAN is called enx00249b09ef56

```
root@ubuntu:/home/digi# ifconfig enx00249b09ef56 100.10.10.2
root@ubuntu:/home/digi# ifconfig enx00249b09ef56 netmask 255.255.255.0
```

3.2 Install StrongSwan

Depending on the Linux distribution, the installation of StrongSwan might defer. In this document, Ubuntu is used. Please refer to http://www.strongswan.org for further installation instructions.

The easiest way to install StrongSwan is via the "**apt-get install strongswan**" CLI command:

```
digi@ubuntu:~$ sudo apt-get install strongswan
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libstrongswan libstrongswan-standard-plugins strongswan-charon
  strongswan-libcharon strongswan-starter
Suggested packages:
  libstrongswan-extra-plugins libcharon-extra-plugins
The following NEW packages will be installed:
  libstrongswan libstrongswan-standard-plugins strongswan strongswan-charon
  strongswan-libcharon strongswan-starter
0 upgraded, 6 newly installed, 0 to remove and 59 not upgraded.
Need to get 3,731 kB of archives.
After this operation, 16.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64
libstrongswan amd64 5.3.5-1ubuntu3.4 [1,398 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64
strongswan-libcharon amd64 5.3.5-1ubuntu3.4 [1,241 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64
strongswan-starter amd64 5.3.5-1ubuntu3.4 [742 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64
strongswan-charon amd64 5.3.5-1ubuntu3.4 [55.6 kB]
```

```
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64
libstrongswan-standard-plugins amd64 5.3.5-1ubuntu3.4 [267 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64
strongswan all 5.3.5-1ubuntu3.4 [27.1 kB]
Fetched 3,731 kB in 12s (307 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libstrongswan.
(Reading database ... 175214 files and directories currently installed.)
Preparing to unpack .../libstrongswan_5.3.5-1ubuntu3.4_amd64.deb ...
Unpacking libstrongswan (5.3.5-1ubuntu3.4) ...
Selecting previously unselected package strongswan-libcharon.
Preparing to unpack .../strongswan-libcharon_5.3.5-1ubuntu3.4_amd64.deb ...
Unpacking strongswan-libcharon (5.3.5-1ubuntu3.4) ...
Selecting previously unselected package strongswan-starter.
Preparing to unpack .../strongswan-starter_5.3.5-1ubuntu3.4_amd64.deb ...
Unpacking strongswan-starter (5.3.5-1ubuntu3.4) ...
Selecting previously unselected package strongswan-charon.
Preparing to unpack .../strongswan-charon_5.3.5-1ubuntu3.4_amd64.deb ...
Unpacking strongswan-charon (5.3.5-1ubuntu3.4) ...
Selecting previously unselected package libstrongswan-standard-plugins.
Preparing to unpack .../libstrongswan-standard-plugins_5.3.5-
1ubuntu3.4_amd64.deb ...
Unpacking libstrongswan-standard-plugins (5.3.5-1ubuntu3.4) ...
Selecting previously unselected package strongswan.
Preparing to unpack .../strongswan_5.3.5-1ubuntu3.4_all.deb ...
Unpacking strongswan (5.3.5-1ubuntu3.4) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libstrongswan (5.3.5-1ubuntu3.4) ...
Setting up strongswan-libcharon (5.3.5-1ubuntu3.4) ...
Setting up strongswan-starter (5.3.5-1ubuntu3.4) ...
Setting up strongswan-charon (5.3.5-1ubuntu3.4) ...
Setting up libstrongswan-standard-plugins (5.3.5-1ubuntu3.4) ...
Setting up strongswan (5.3.5-1ubuntu3.4) ...
```

Please note: All commands have to be used in elevated or super user mode. For ease of configuration, this document will use the root user (not recommended). In most case, using “sudo” in front of each commands will provide the expected result.

3.3 Configure StrongSwan

3.3.1 IPsec VPN Configuration

The IPsec configuration of StrongsWan is done via 2 main files (when using pre-shared keys as in this example):

- ipsec.conf : Used for Phase 1 (IKE) and Phase 2 IPsec configuration
- ipsec.secrets : Used for pre-shared keys

In this example, the following Phase 1 settings will be used:

- AES (128 bit)
- SHA 1
- MODP Group 2
- Main Mode

In this example, the following Phase 2 settings will be used:

- AES (128 bit)
- SHA 1
- No PFS
- ID Types : IPv4
- Preshared Keys

3.3.1.1 ipsec.conf

Edit the ipsec.conf file using a text editor such as **vi**:

```
config setup

conn %default
  ikelifetime=60m
  keylife=20m
  rekeymargin=3m
  keyingtries=%forever
  keyexchange=ikev1
  authby=secret

conn peer1-peer2
  left=192.168.1.118
  leftsubnet=100.10.10.0/24
  leftfirewall=yes
  right=%any
  rightallowany=yes
  rightsubnet=10.0.0.0/24
  auto=start
  closeaction=restart
  ike=aes128-sha1-modp1024
  esp=aes128-sha1
  type=tunnel
  keyingtries=%forever
```

type **:wq** to save and close

conn %default		
ikelifetime	60m	IKE Lifetime
keylife	20m	IKE Key Lifetime
Rekeymargin	3m	Margin between IKE rekey
keyingtries	%forever	Amount of retries for rekey
keyexchange	Ikev1	Use IKEv1
authby	Secret	Use preshared keys authentication
conn peer1-peer2		
left	192.168.1.118	WAN Ip address (StrongSwan)
leftsubnet	100.10.10.0/24	Local Subnet (StrongSwan)
leftfirewall	yes	Automatically create firewall rules for the IPsec VPN tunnel
right	%any	Allow any remote IP Address to connect
rightsubnet	10.0.0.0/24	Remote subnet (TransPort WR)
auto	start	Establish tunnel automatically when deamon is started
closeaction	restart	Restart tunnel automatically when deamon is restarted/closed
ike	aes128-sha1-modp1024	IKE (Phase 1) Settings
esp	aes128-sha1	ESP (Phase 2) settings
type	tunnel	Type of IPsec tunnel
keyingtries	%forever	Amount of retries for rekey

3.3.1.2 ipsec.secrets

Edit the ipsec.secrets file using a text editor such as **vi**:

```
192.168.1.118 : PSK "digidigi"
192.168.1.23 : PSK "digidigi"
```

type **:wq** to save and close

Parameter	Description
192.168.1.118	IPv4 ID
192.168.1.23	IPv4 ID
“digidigi”	Preshared key

3.4 Start/Restart the StrongSwan IPsec daemon

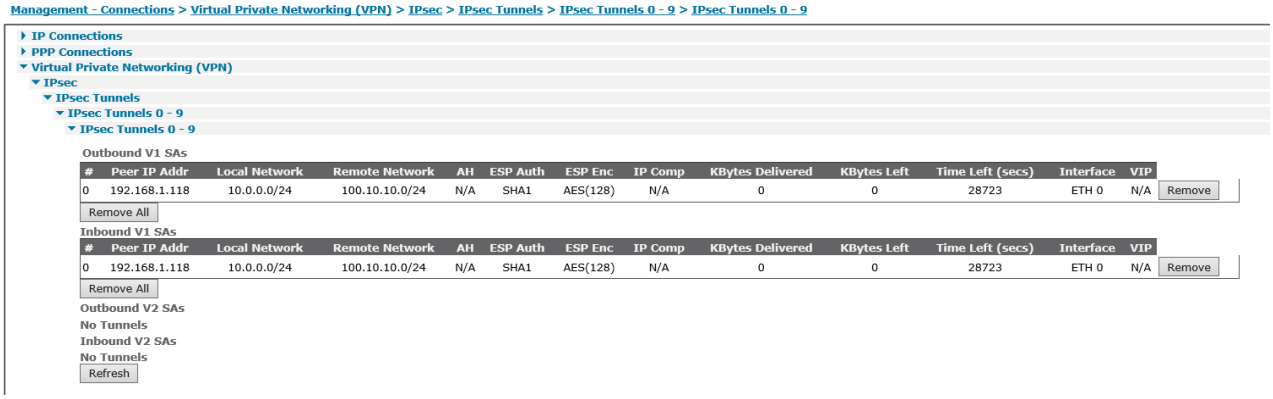
Once the files are modified, the changes will only take effect after reloading the StrongSwan daemon. To do so, issue the following command:

```
root@ubuntu:/home/digi# ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.3.5 IPsec [starter]...
```

4 CHECK TUNNEL STATUS

4.1 Digi TransPort

Navigate to **Management – Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 – 9 > IPsec Tunnels 0-9**



Via CLI:

```
sastat
Command: sastat

Command result

IPsec SAs (total:1). Eroute 0 -> 49
Outbound V1 SAs
      SPI Eroute          Peer IP                  Rem. subnet
Loc. subnet     TTL      KBytes Left                 VIP
 c3b444ae       0   192.168.1.118               100.10.10.0/24
10.0.0.0/24  28648                0                  N/A
Inbound V1 SAs
      SPI Eroute          Peer IP                  Rem. subnet
Loc. subnet     TTL      KBytes Left                 VIP
 6eb46719       0   192.168.1.118               100.10.10.0/24
10.0.0.0/24  28648                0                  N/A
Outbound V2 SAs
      List Empty
Inbound V2 SAs
      List Empty
OK
```

4.2 StrongSwan

```
root@ubuntu:/home/digi# ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.10.0-28-generic,
x86_64):
  uptime: 29 seconds, since Aug 22 06:25:17 2017
  malloc: sbrk 1486848, mmap 0, used 344640, free 1142208
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0,
scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce
x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey
pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve
socket-default connmark stroke updown
Listening IP addresses:
  192.168.1.118
  100.10.10.2
Connections:
 peer1-peer2:  192.168.1.118...%any,0.0.0.0/0,::/0  IKEv1
 peer1-peer2:   local:  [192.168.1.118] uses pre-shared key authentication
 peer1-peer2:   remote: uses pre-shared key authentication
 peer1-peer2:   child:  100.10.10.0/24 === 10.0.0.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
 peer1-peer2[1]: ESTABLISHED 22 seconds ago,
192.168.1.118[192.168.1.118]...192.168.1.23[192.168.1.23]
 peer1-peer2[1]: IKEv1 SPIs: 6eb06982e84e8679_i 208d286522e19369_r*, pre-
shared key reauthentication in 54 minutes
 peer1-peer2[1]: IKE proposal:
AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
 peer1-peer2{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cc5e3c54_i 6eb4671a_o
 peer1-peer2{1}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in
15 minutes
 peer1-peer2{1}:   100.10.10.0/24 === 10.0.0.0/24
```

5 TESTING

To simply test the tunnel, generate a ping from each side of the tunnel and ping the remote end's ethernet interface.

5.1 TransPort side

```
Command: ping 100.10.10.2 -e0
Command result

Pinging Addr [100.10.10.2]

sent PING # 1
PING receipt # 1 : response time 0.00 seconds
Iface: PPP 1
Ping Statistics
Sent         : 1
Received     : 1
Success      : 100 %
Average RTT : 0.00 seconds

OK
```

5.2 StrongSwan side

```
root@ubuntu:/home/digi# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=250 time=2.30 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=250 time=1.30 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=250 time=1.56 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=250 time=1.28 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=250 time=1.35 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=250 time=1.38 ms
^C
--- 10.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 1.287/1.532/2.304/0.358 ms
```

6 TRANSPORT CONFIGURATION

```
eth 0 IPaddr "10.0.0.1"
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "StrongSwan"
eroute 0 peerip "192.168.1.118"
eroute 0 peerid "192.168.1.118"
eroute 0 ourid "192.168.1.23"
eroute 0 ouridtype 3
eroute 0 locip "10.0.0.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 locipifadd 1
eroute 0 remip "100.10.10.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 enckeybits 128
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.etherios.com"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 username "username"
ppp 1 epassword "KD5lSVJDVVg="
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 do_nat 2
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ike 0 encalg "AES"
ike 0 keybits 128
```

```
ike 0 authalg "SHA1"
ike 0 ikegroup 2
ike 0 noresp ON
ike 0 deblevel 4
ike 0 debug ON
ana 0 anon ON
ana 0 l2on OFF
ana 0 l3on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ikeon ON
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 name "192.168.1.118"
user 9 epassword "PDZxU0FFQFU="
user 9 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
cloud 0 clientconn ON
cloud 0 ssl ON

OK
```