



PPTP VPN
USER GUIDE

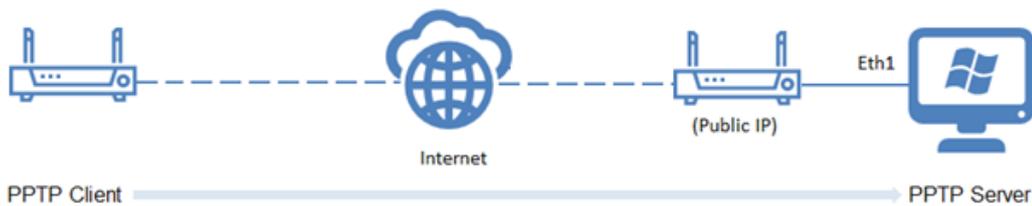
eSAM



INTRODUCTION

A VPN (Virtual Private Network) is a method for securely connecting two devices together on a single network across the internet. Packets from one device are encrypted and then sent over the network to the second device, where the packets are decrypted and read. As a result, both devices appear to be on the same network with each other and can communicate as if they were both plugged into the same router.

This guide will explain how to configure a Windows-based PPTP Host, using an eSAM Modem as the internet gateway. It will also explain how to configure a separate eSAM to act as a client for the Windows PPTP Host.



While this is specifically geared towards a Windows PPTP VPN, many other VPN configurations are possible using the eSAM. This guide can be thought of as an introduction to VPN's on the eSAM generally.

HOST CONFIGURATION

First, we will configure the eSAM Modem we will use to connect the PPTP Host to the internet.

1. Connect the Windows PPTP Server to your modem, and then use your web browser to open the Modem's web interface. Out of the box, this is accessible on port 192.168.1.1

Insert your SIM, and check that your ISP has provided you with a public IP Address. A Public IP Address is an IP Address that is visible from the internet. It is necessary for your PPTP Server to have a public IP Address, so Clients will be able to find it over the Internet.

Public IP Addresses are any addresses that are not in any of the following ranges:

10.x.x.x
192.x.x.x

It is not required for clients to have a Public IP Address, only the Host needs to have one.

Status	modem	
Basic Information	Modem Select	0
LAN	Up Time	2466 seconds
WAN	Modem Status	connected
WLAN	Network Type	LTE
Modem	Signal	 (31)
Routing Table	IP Address	120.157.100.168 
Network	DNS	10.4.130.164
Applications	SIM Status	ready
VPN	SIM ICCID	89610185001917598063
Forward	SIM IMSI	505013506992663
	LAC	12447
	CELL ID	135911169
	Refresh	

If your eSAM Modem does not have a public IP Address, or if it is unable to connect to the ISP please ensure you have entered the correct APN under the Network > Modem window.

2. Once you have confirmed that your eSAM is accessible over the internet, you must now configure the port forwarding. Port Forwarding specifies to the Modem where it should send packets when they arrive from the Internet. In this case, we want to route packets related to hosting VPN's to your Windows Machine, as it will be responsible for running the PPTP Host.

To configure port forwarding, select the Forward > NAT Screen

Status	MASQ
Network	Interface: modem Operation: Delete
Applications	
VPN	SNAT
Forward	Protocol Original Address Original Port Mapping Address Mapping Port Operation
NAT	DNAT
Routing	Protocol Original Address Original Port Mapping Address Mapping Port Operation
RIP	all modem --- 192.168.2.147 --- Del
OSPF	Add Refresh

Press 'Add' to enter a new Port Forwarding rule.

Basic Settings

NAT Type: DNAT SNAT MASQ

Protocol: all ▼

Original Address Type: interface ▼

Interface: modem ▼

Original Port: 1-65535 or [1-65535]

Mapping Address: * eg. 192.168.0.1

Mapping Port: 1-65535 or [1-65535]

Save | Return

We need to add a new port forwarding rule for each Port we wish to forward. For PPTP, there are two ports we need to forward:

Port Number	Protocol
1723	TCP
47	UDP

For both rules, we want to leave the other options set as follows:

Field Name	Value
Original Address Type	Interface
Interface	Modem
Mapping Address	IP Address of the PPTP Host Computer

Please note the IP Address of your computer using the ipconfig command, or similar.

Once all are entered, your NAT Screen should have the following rules:

MASQ

Interface	Operation
modem	Delete

SNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
----------	------------------	---------------	-----------------	--------------	-----------

DNAT

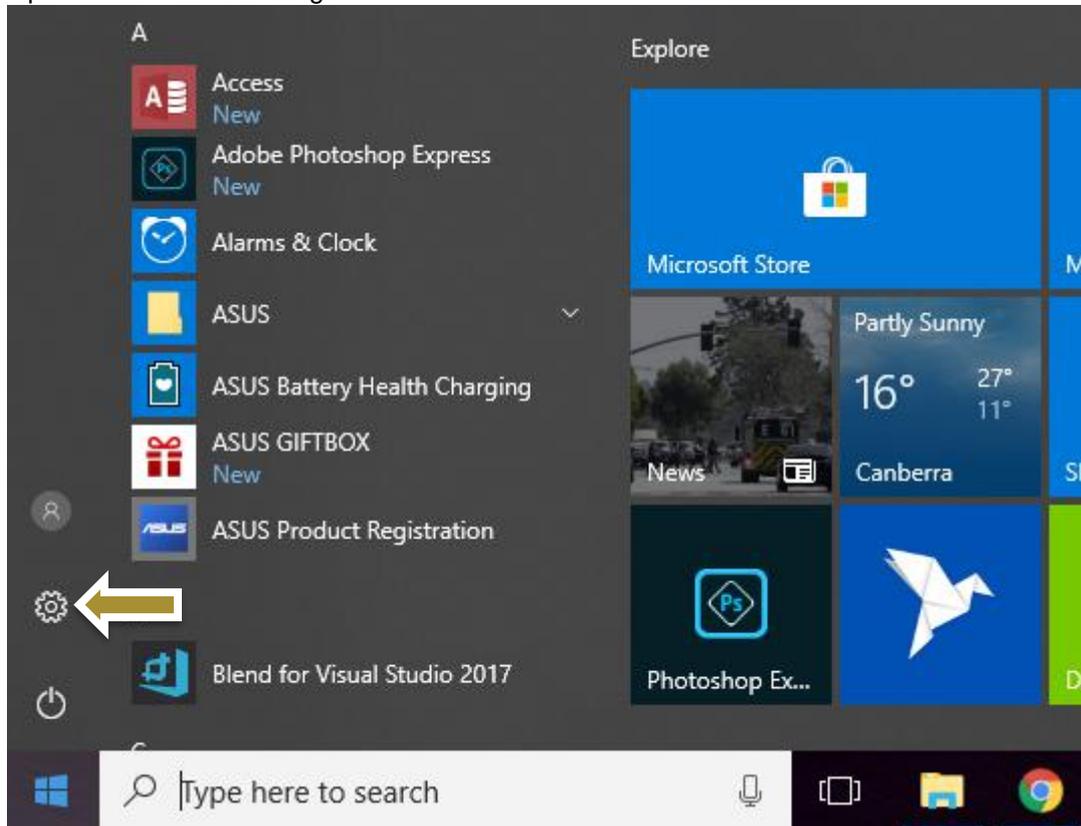
Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
tcp	modem	47	192.168.2.147	47	Del
udp	modem	1723	192.168.2.147	1723	Del

[Add](#) [Refresh](#)

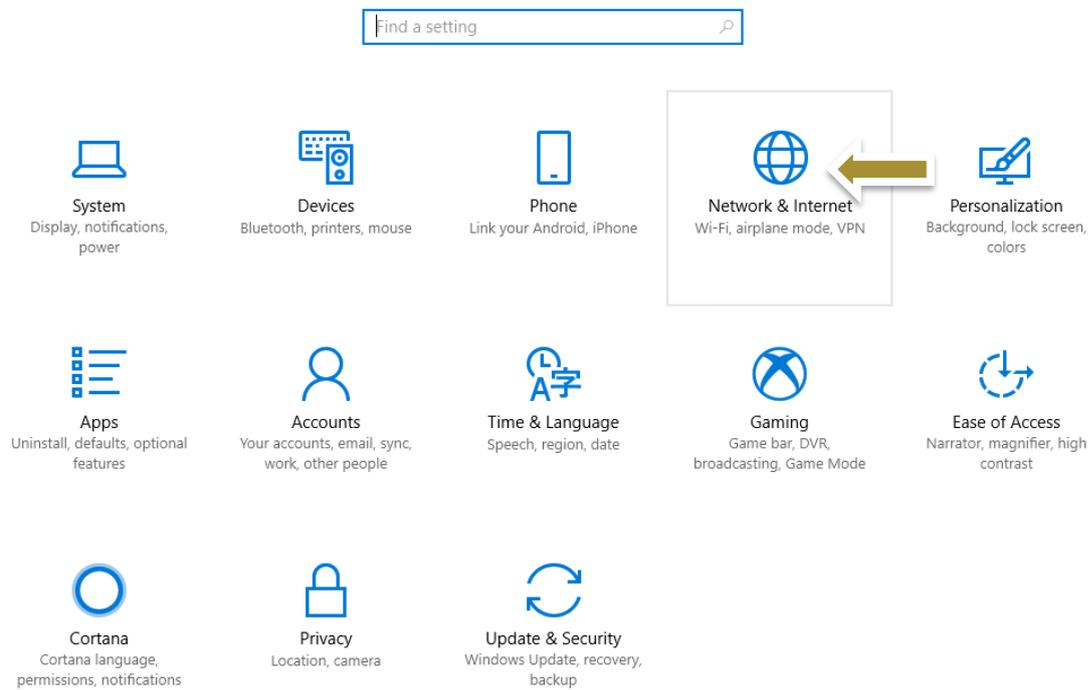
Note: Mapping Address will be set to the PPTP Host's LAN IP Address. For troubleshooting purposes, it may sometimes be useful to forward all ports. In this case, leave the Original and Mapping Port options blank.

- Now that the PPTP host is visible from the internet, we can enable the PPTP Host functionality within windows.

Open the Windows Settings Window



Under settings, select the *'Network & Internet'* Option
Windows Settings



From the Network and Internet Screen, select *'Change adapter options'*

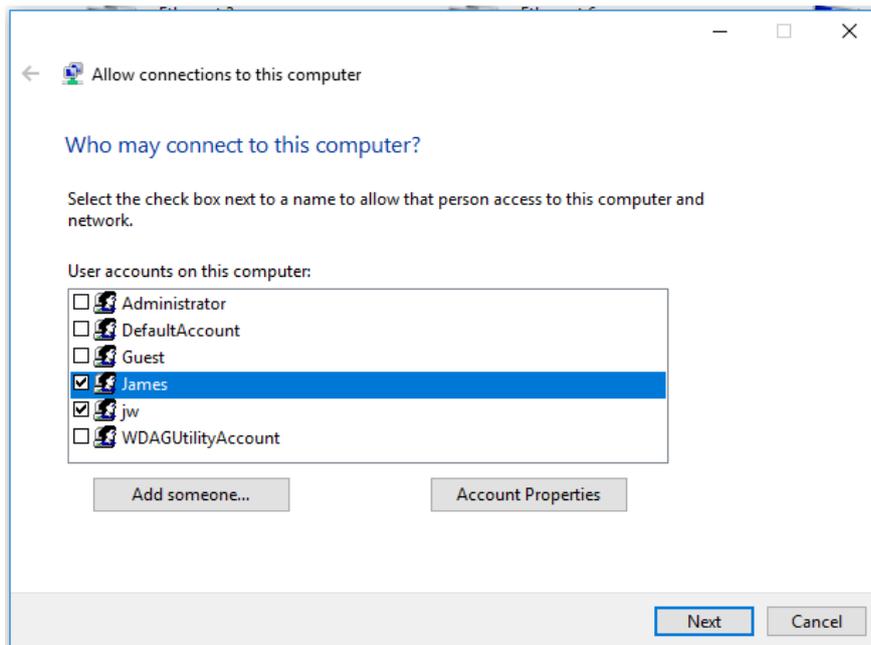
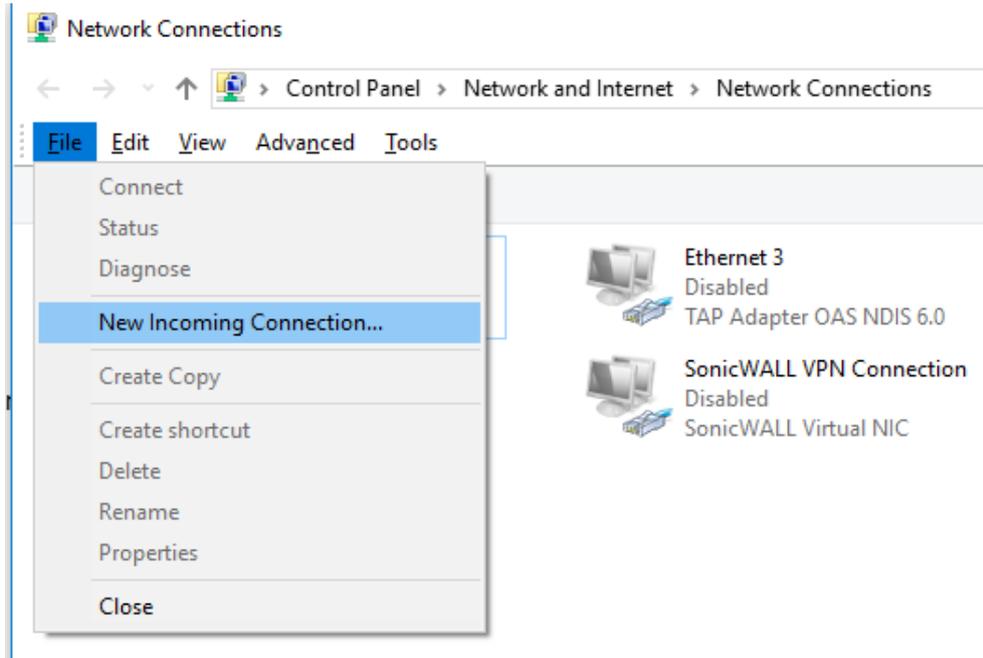
Change your network settings



Change adapter options

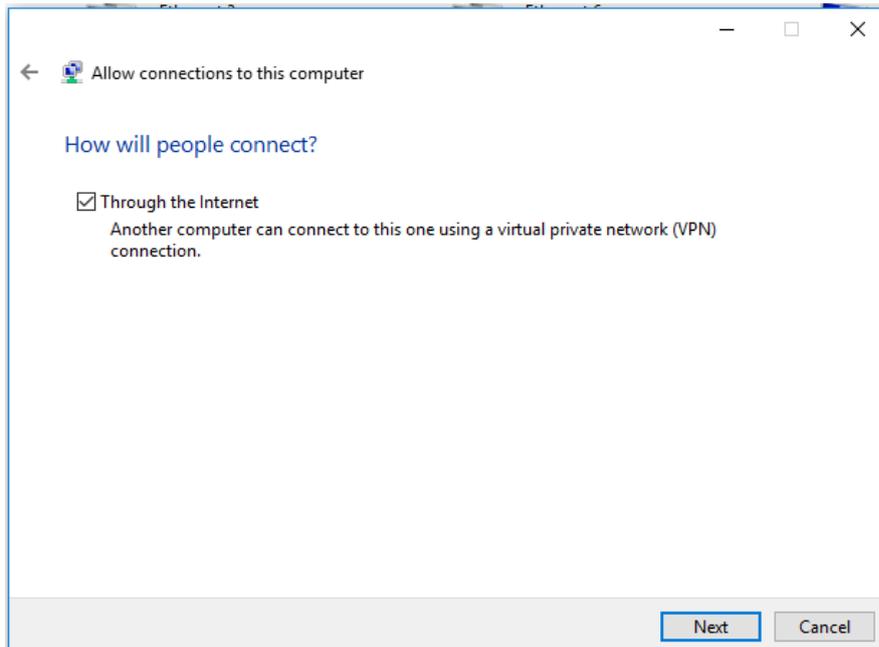
View network adapters and change connection settings.

Press the 'Alt' key to open the file menu, then select File > New Incoming Connection

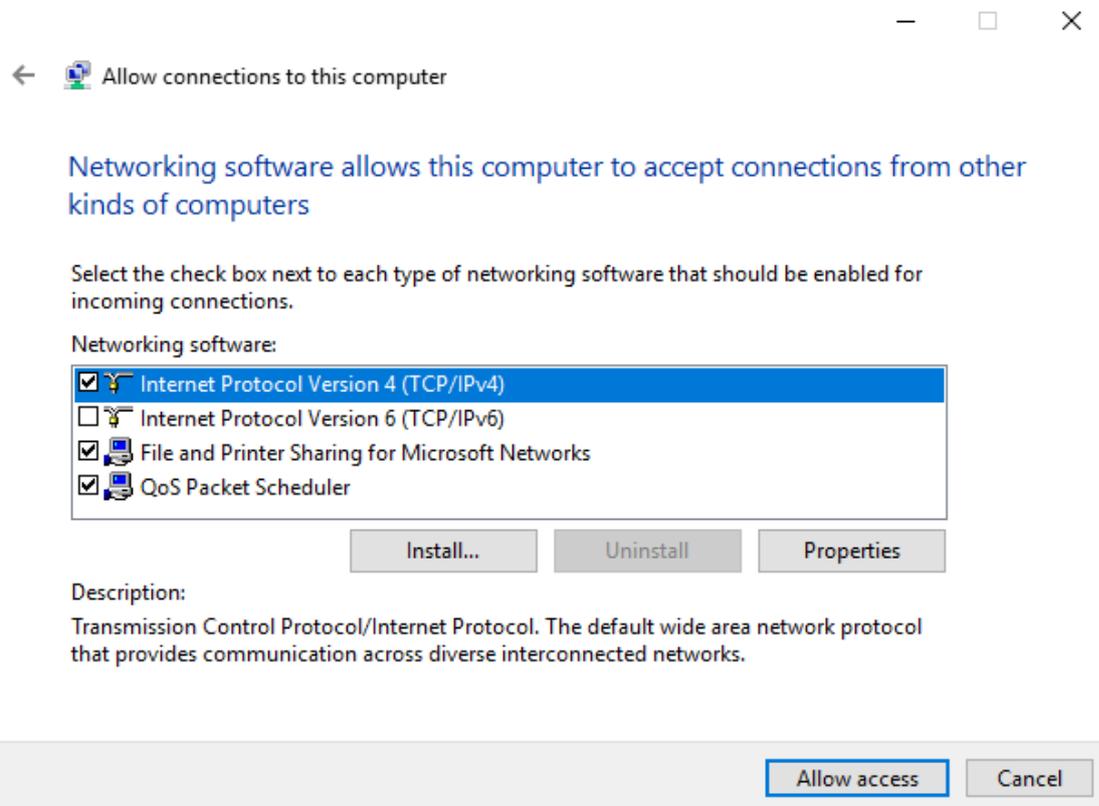


Select the users you wish to be able to connect to the VPN. Whenever an outside client connects to the VPN Host, it must use this users login details to connect to the Host Machine.

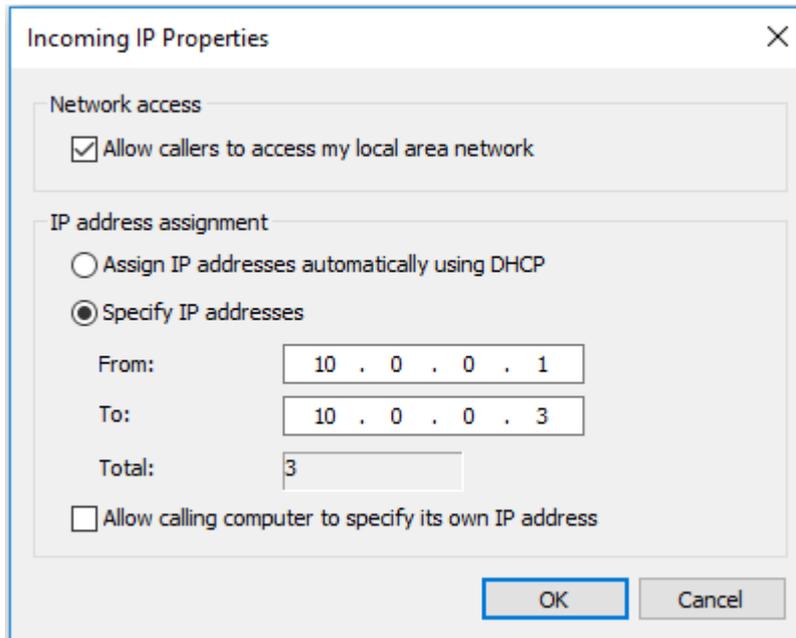
If you don't want to use a pre-existing login, you can add a new user using the 'Add someone' option.



Leave the 'Through the Internet' option enabled and press Next.



Select the '*Internet Protocol Version 4 (TCP/IPv4)*' option, and press properties



Choose '*Specify IP addresses*' and enter a suitable range of addresses. This will cause the Windows PPTP Host to assign an IP Address to each Client that connects to it.

Press OK once configured, then 'Allow Access'.

This should add an 'Incoming Connections' Icon to the network adapter screen. This confirms that your PPTP Host is now enabled.



Incoming Connections
No clients connected

If you want to verify the host configuration before continuing, you can connect to the Windows PPTP Host using either an Android phone, iPhone or another Windows Computer.

CLIENT CONFIGURATION

Connect a second eSAM Module to the device you want available over the VPN. This eSAM does not need to have a public IP Address – as long as it has internet connectivity, it should suffice.

1. Log into the web interface for the Client eSAM. By default, this can be done through your web browser by connecting to IP 192.168.1.1

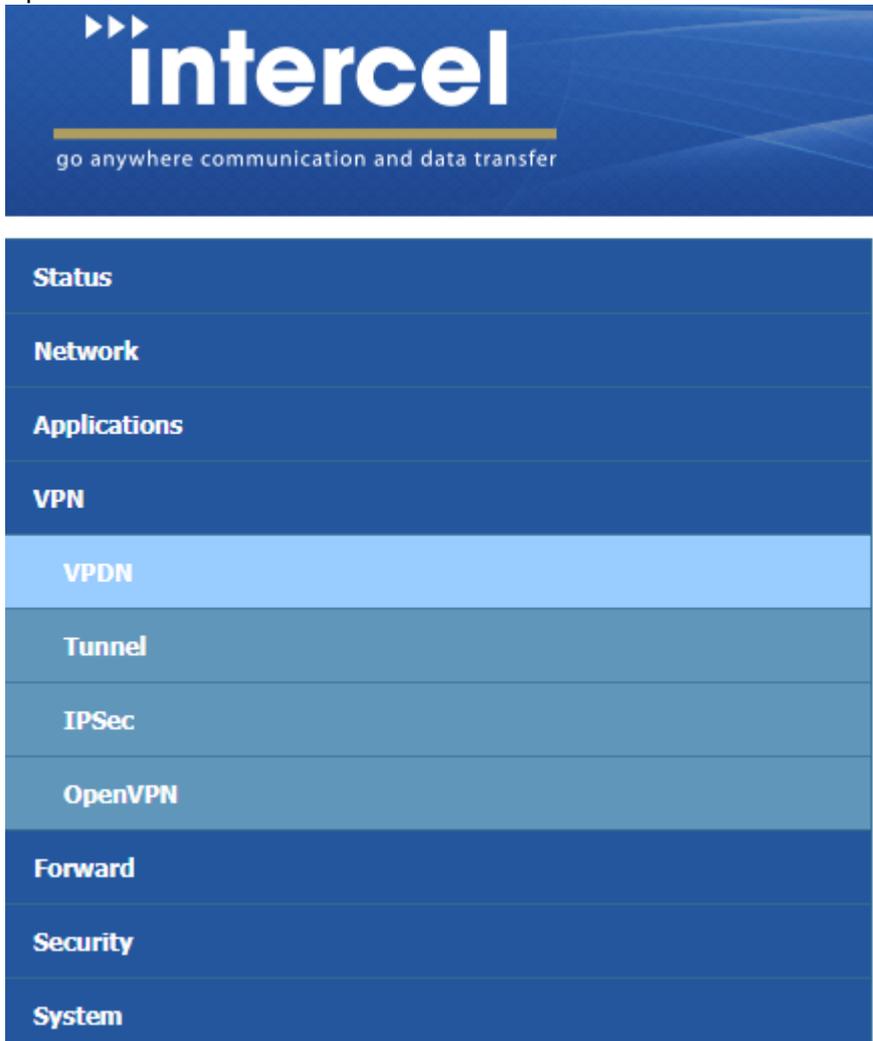


The screenshot shows the Intercel eSAM web interface. The header features the Intercel logo and the tagline "go anywhere communication and data transfer". The main content area is divided into a left sidebar and a main panel. The sidebar has a "Status" section with sub-items: "Basic Information", "LAN", "WAN", and "WLAN". The main panel displays a table with the following data:

Router SN	AU0HH00073
Hardware Version	V11
Software Version	V1.0.0_180208

At the bottom right of the main panel, there is a "Refresh" button.

Open the VPN > VPDN Screen



The screenshot shows the Intercel eSAM web interface with the "VPN" menu item selected in the sidebar. The main panel displays a list of VPN-related options:

- Status
- Network
- Applications
- VPN
- VPDN** (highlighted)
- Tunnel
- IPSec
- OpenVPN
- Forward
- Security
- System

2. Press the 'add' button to configure a new VPN



Tunnel secrets Max length is 64 [Save](#)

Interface Name	Protocol	Server IP or Domain	User
test	pptp	192.168.2.147	interc

[Add](#) [Refresh](#)

3. On this screen, select '*pptp*' as protocol type and then enter your Publicly accessible PPTP Server IP Address in the 'Server IP or Domain' Field. Enter the username and password for a valid user on the PPTP Host.

VPDN Service [Enable](#) [Disable](#)

Basic Settings

Interface Name * Max length is 8

Protocol

Server IP or Domain * Max length is 64

Username Max length is 64

Password Max length is 64

Advanced Settings [Display](#)

Press '*Display*' for the Advanced Settings option and then enter the settings as shown below:

Authentication

CHAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
PAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
MS-CHAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
MS2-CHAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable
EAP	<input checked="" type="radio"/> Negotiation <input type="radio"/> Disable

Compress

Compression Control Protocol	<input checked="" type="radio"/> Require <input type="radio"/> Disable
Address/Control Compression	<input checked="" type="radio"/> Require <input type="radio"/> Disable
Protocol Field Compression	<input checked="" type="radio"/> Require <input type="radio"/> Disable
VJ TCP/IP Header Compress	<input checked="" type="radio"/> Require <input type="radio"/> Disable
Connection-ID Compression	<input checked="" type="radio"/> Require <input type="radio"/> Disable

More

Debug	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Peer's DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LCP Interval	<input type="text" value="30"/> 1-512 s
LCP Retry	<input type="text" value="5"/> 1-512 times
MTU	<input type="text"/> 128-16384 B
MRU	<input type="text"/> 128-16384 B
Local IP	<input type="text"/> eg. 192.168.8.1
Remote IP	<input type="text"/> eg. 192.168.8.254

Professional

nomppe: Disable Microsoft Point to Point Encryption.
mppe required: Enable Stateful Microsoft Point to Point Encryption.
mppe stateless: Enable Stateless Microsoft Point to Point Encryption.
nodeflate: Disable Deflate compression entirely.
nobsdcomp: Disables BSD-Compress compression.
default-asynccmap: Disable asynccmap negotiation.

mppe required
mppe stateless

Note: mmppe required and mppe stateless are both required for a Windows Host. Other hosts may have different settings requirements.

4. Save the settings for your PPTP Client and enable the VPN Service. You should now have a single VPN Connection on your VPDN Screen

Tunnel secrets Max length is 64 [Save](#)

Interface Name	Protocol	Server IP or Domain	Username	Operation				
test	pptp	192.168.2.147	intercelvpn2	Mod	Del	View	En	Dis

[Add](#) [Refresh](#)

Press 'View' to view the state of your VPN.

Operation				
Mod	Del	View	En	Dis



Provided everything is configured correctly, your VPN should show as connected and the VPN will now be available as an interface on the router.

Interface Name	test
Status	connected
Protocol	pptp
Local IP Address	192.168.10.49
Remote IP	192.168.10.10

Basic Settings

NAT Type	<input checked="" type="radio"/> DNAT <input type="radio"/> SNAT
Protocol	all ▼
Original Address Type	interface ▼
Interface	br0 ▼
Original Port	br0
Mapping Address	modem
Mapping Port	eth0
	eth1
	vpdnhdwh
	vpdntest

You can now forward traffic from this port as you can with any other network interface.

In this case, we wish to forward traffic arriving from the VPN to the relevant device on the client side of the network. Typically, this would be a PLC or other piece of industrial equipment.

Basic Settings

NAT Type	<input checked="" type="radio"/> DNAT <input type="radio"/> SNAT <input type="radio"/> MASQ
Protocol	all ▼
Original Address Type	interface ▼
Interface	vpdntest ▼
Original Port	80 1-65535 or [1-65535]
Mapping Address	192.168.8.120 * eg. 192.168.0.1
Mapping Port	80 1-65535 or [1-65535]



go anywhere communication and data transfer



www.facebook.com/Intercel-775004365883748



www.linkedin.com/company/intercel



www.intercel.com.au  33 Glenvale Crescent Mulgrave VIC 3170 Australia



intercel@intercel.com.au



+61 (0) 3 9239 2000