Application Note

Vocality Gateway IPSec Application Note

Software From
V3.2.3

Revision
v1.1

Publish Date
December 2017

CUBIC vocality

SET UP IPSEC

1 Overview

This Applications Note discusses the configuration of Internet Protocol Security (IPSec) on systems running the Vocality Gateway Suite, using the Secure module.

IPSec is a protocol suite for ensuring private, secure communications over IP networks. It supports data integrity, data confidentiality, data origin authentication and peer authentication (among other features) using a range of services and technologies.

The Secure module provides the facility to set up IPSec tunnels to other Vocality Gateway Nodes and Vocality VOS-based devices as well as a range of third-party devices. The module also provides an IPSec transport mode for securing standard IP tunnels such as GRE. For authentication and data encryption, both pre-shared key (PSK) and Public Key Infrastructure (PKI) methods are supported.

2 Pre-requisites

The use of IPSec requires the system to be running Node Manager 2.0.0 or above, Node UI 2.0.0 or above, and Secure 1.0.0 or above.

3 Outline

The Secure module supports a very wide range of options for implementing IPSec communications. Other sections provide help with implementing the most common scenarios.

CAUTION: IPSec can be used in many ways and is no guarantee of network security. Your selections will determine the degree to which your data will be protected using IPSec. Vocality recommend that you take advice from a network security professional on the most appropriate way to secure your data before beginning configuration.

The example scenarios described in other Applications Notes are:

- **Set up IPSec tunnels - using Pre-Shared Keys (PSK)**
- **Set up IPSec tunnels - using Public Key Infrastructure (PKI)**, including how to **Generate self-signed certificates for IPSec using PKI**
- **Set up IPSec tunnels - Authentication Header (AH) only**
- **Set up IPSec transport - to secure traffic in GRE tunnel**

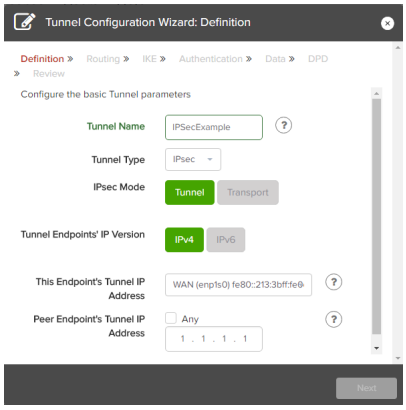
IPSec connections are created between two IPSec-enabled devices. In these examples, the two devices are referred to as the 'local' machine, on which IPSec configuration is taking place, and the 'peer' machine, to which an IPSec connection will be made. Both machines need to be correctly configured for the IPSec connection to be established. A successfully established and installed IPSec connection is called a Security Association (SA).

If you are new to IPSec, another section provides **IPSec terminology** for easy reference.

4 Set up IPSec tunnels - using Pre-Shared Keys (PSK)

Select the Secure menu.

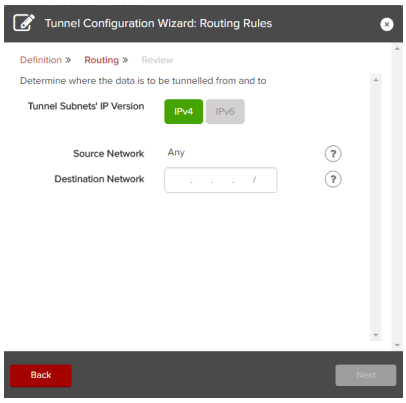
On the Summary submenu choose the **<Add Tunnel>** button to start the Tunnel Configuration wizard.



Give your tunnel a name and choose the tunnel type 'IPSec'. Select the IP address for the local endpoint of the tunnel, at this Vocality Gateway Node, from the dropdown menu. Enter an appropriate IP address for the peer endpoint of the tunnel.

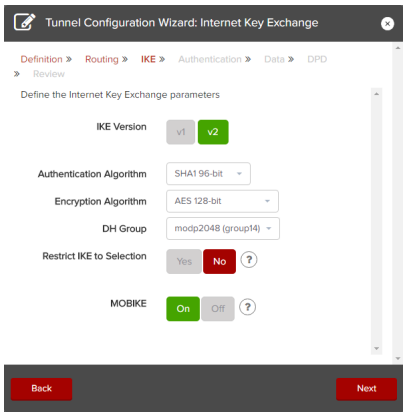
(Note: For ELITE Access or ELITE Fusion multi-bearer applications the option 'Floating' is available. This allows the address to be dynamically switched to the currently active bearer.)

Only when valid parameters have been entered in all of the boxes will the **<Next>** button become red and available to press.



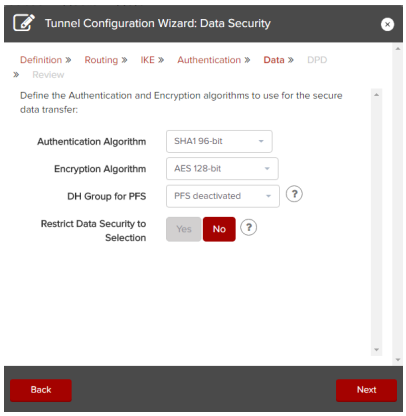
Complete the form to define the destination network for which tunneling will apply. Only when valid parameters have been entered in all of the boxes will the **<Next>** button become red and available to press.

Select the required Internet Key Exchange (IKE) version and authentication and encryption algorithms. These are the algorithms that will apply while the IPSec connection between the local and peer machines is being established, not those that will be used to authenticate or encrypt IP traffic once the connection is established and installed.



After selecting **<Next>**, select **<PSK>**, and enter a password into the 'Node Secret Key' field. (This key must consist of between eight and sixty-four characters. No symbols are allowed.) The box surrounding the field will show green when a key is entered that meets the rules. Enter the same password in the 'Repeat Node Secret Key' field. The same password will also need to be entered in the same fields when configuring the IPSec tunnel on the peer machine. Enter the Node ID for the peer machine. (If it is another Vocality Gateway Node this can be found in the **Platform > Status** menu.) If the field is left blank the peer's endpoint is used.

Choose **<Next>**, then select the authentication and encryption algorithms that will be used on IP traffic once the IPSec connection is installed.

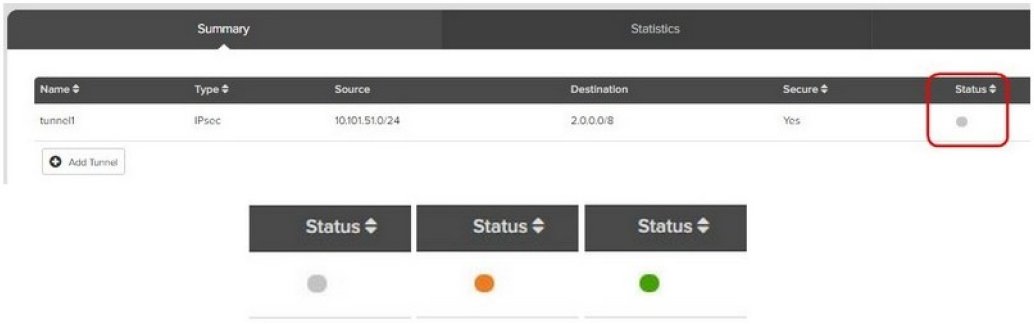


Choose **<Next>**, then select the required option for Dead Peer Detection. This feature allows the specification of an action to perform when the remote machine is no longer available.

Choose **<Next>** and review the IPSec tunnel settings. All of the information entered so far is presented back to you. If there are any errors use the **<Back>** button to go to the right page to make a correction. When you press **<Finish>** this new tunnel will be added to the list on the **Secure > Summary menu**, but will not be active. From there you can choose any one of the icons, when needed, to:

- edit it ;
- delete it;

- enable/disable it (new tunnels are initially disabled by default); or
- view statistics regarding the use of that tunnel.



Note: Before an IPSec tunnel can be established you must ensure that a matching IPSec tunnel has been configured on the peer machine. 'Matching' tunnel definitions means that, for instance, the authentication and encryption algorithms chosen are the same on both the local and peer machines.

Once local and peer machines have a matching IPSec tunnel configuration, select the drop-down box marked 'Disabled' next to your configured tunnel on the **Secure > Summary menu**, and select 'Enabled'.

When this has been done on both the local and remote machines, you should expect the 'Status' indicator to change to orange to show that a tunnel is being established, then green to show that the tunnel has been correctly installed. Now all IP traffic matching the source and destination networks, which you entered in the IPSec tunnel configuration, will be encapsulated and encrypted before being sent to the remote machine.

5 Set up IPSec tunnels - using Public Key Infrastructure (PKI)

When creating an IPSec Security Association using Public Key Infrastructure (PKI), a combination of public/private key pairs and certificate files are used to authenticate the peer machines and encrypt IP traffic.

Note: Take steps to obtain or identify the certificates to be used before you start to define the tunnel.

Private keys and certificate files, known as 'self-signed' certificates, can be created using a machine configured as a Certificate Authority (see **Generate self-signed certificates for IPSec using PKI**). Alternatively, certificate files may be obtained from a trusted third-party Certificate Authority. There is no difference in operation when 'self-signed' certificates are used, but additional infrastructure is required to create the Certificate Authority and to provide support for services such as the Online Certificate Status Protocol (OCSP).

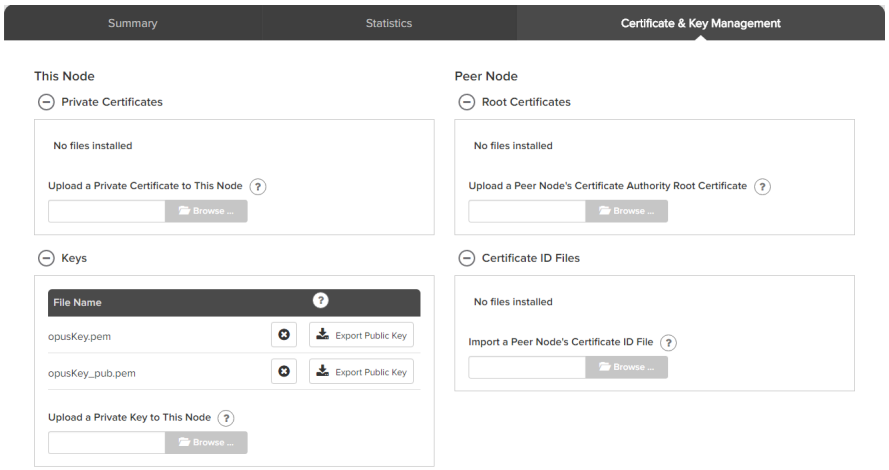
The following files must be generated or obtained before configuring an IPSec Security Association using PKI:

• A private key file for the local machine

• A certificate file for the local machine

• A root certificate file from the Certificate Authority

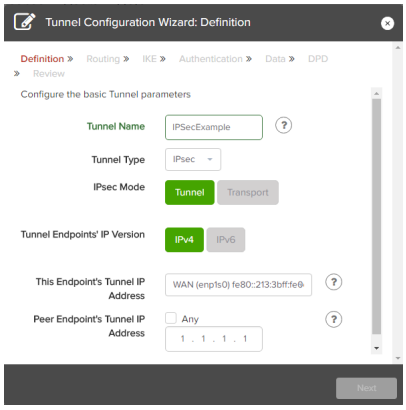
These should be uploaded to the Vocality Gateway Node using the appropriate fields on the **Secure > Certificate & Key Management submenu**. Use the **<Browse>** button beside each field to locate the appropriate file and then **<Open>**. Then, to upload the file to the correct place on the Vocality Gateway Node, press **<Upload>**:



The local and remote machines must also produce and exchange 'certificate ID' files.

Select the Secure menu.

On the Summary submenu choose the **<Add Tunnel>** button to start the Tunnel Configuration wizard.

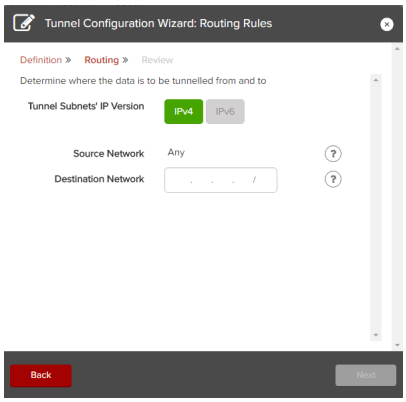


Give your tunnel a name and choose the tunnel type 'IPSec'. Select the IP address for the local endpoint of the tunnel, at this Vocality Gateway Node, from the dropdown menu. Enter an appropriate IP address for the peer endpoint of the tunnel.

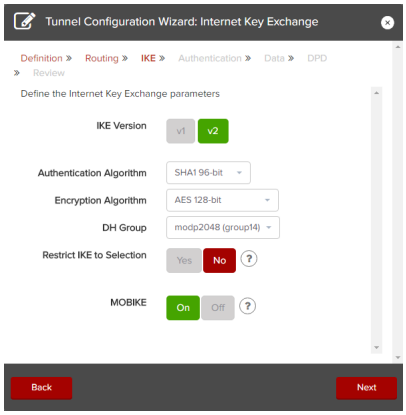
(Note: For ELITE Access or ELITE Fusion multi-bearer applications the option 'Floating' is available. This allows the address to be dynamically switched to the currently active bearer.)

Only when valid parameters have been entered in all of the boxes will the **<Next>** button become red and available to press.

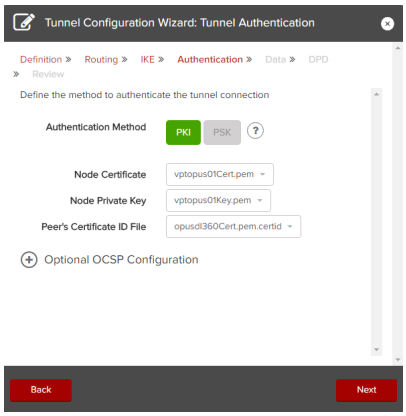
Select the required Internet Key Exchange (IKE) version and authentication and encryption algorithms. These are the algorithms that will apply while the IPSec connection between the local and peer machines is being established, not those that will be used to authenticate or encrypt IP traffic once the connection is established and installed.



Complete the form to define the destination network for which tunneling will apply. Only when valid parameters have been entered in all of the boxes will the **<Next>** button become red and available to press.



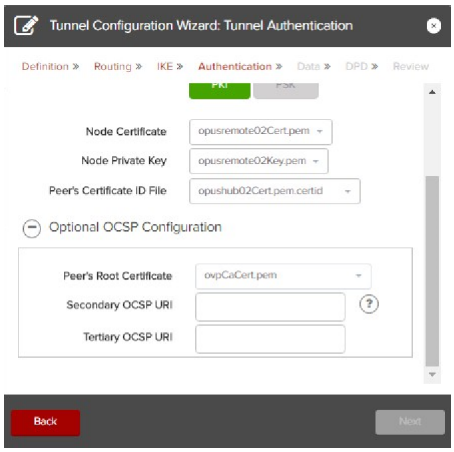
After selecting **<Next>**, select **<PKI>**, and use the drop-down boxes to select the appropriate key and certificate files for each field. Only files that have previously been uploaded via the **Secure > Certificate & Key Management submenu** (see above) will appear in the drop-down boxes:



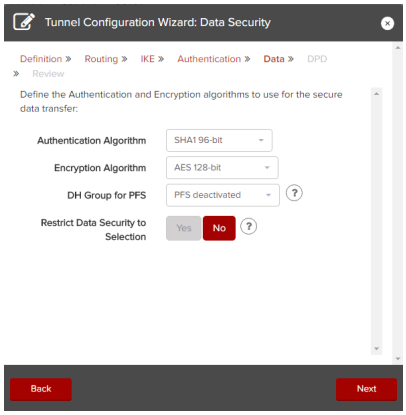
If using the Online Certificate Status Protocol (OCSP) to manage certificates, click the '+' symbol next to 'Optional OCSP Configuration'. Here, the root certificate file from the remote machine can be specified. If this root certificate was obtained from a third-party Certificate Authority, it may contain a URI for

exchanging OCSP information. The Tunnel Configuration Wizard has fields allowing secondary and tertiary URIs to be specified, if available, in the event that the primary URI cannot be reached.

If the root certificate does not contain an OCSP URI, one can be added manually by filling in the 'Secondary OCSP URI' field, with the 'Tertiary OCSP URI' used as a backup.



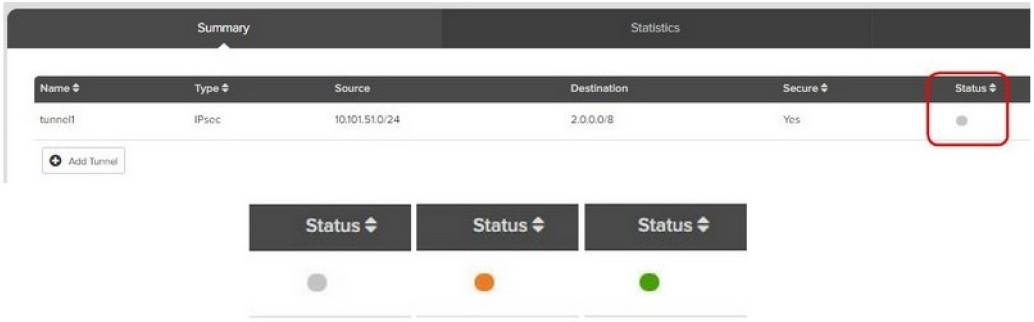
Choose **<Next>**, then select the authentication and encryption algorithms that will be used on IP traffic once the IPSec connection is installed.



Choose **<Next>**, then select the required option for Dead Peer Detection. This feature allows the specification of an action to perform when the remote machine is no longer available.

Choose **<Next>** and review the IPSec tunnel settings. All of the information entered so far is presented back to you. If there are any errors use the **<Back>** button to go to the right page to make a correction. When you press **<Finish>** this new tunnel will be added to the list on the **Secure > Summary menu**, but will not be active. From there you can choose any one of the icons, when needed, to:

- edit it ;
- delete it;
- enable/disable it (new tunnels are initially disabled by default); or
- view statistics regarding the use of that tunnel.



Note: Before an IPSec tunnel can be established you must ensure that a matching IPSec tunnel has been configured on the peer machine. 'Matching' tunnel definitions means that, for instance, the authentication and encryption algorithms chosen are the same on both the local and peer machines.

Once local and peer machines have a matching IPSec tunnel configuration, select the drop-down box marked 'Disabled' next to your configured tunnel on the **Secure > Summary menu**, and select 'Enabled'.

When this has been done on both the local and remote machines, you should expect the 'Status' indicator to change to orange to show that a tunnel is being established, then green to show that the tunnel has been correctly installed. Now all IP traffic matching the source and destination networks, which you entered in the IPSec tunnel configuration, will be encapsulated and encrypted before being sent to the remote machine.

5.1 Generate self-signed certificates for IPSec using PKI

To use Public Key Infrastructure (PKI) when configuring IPSec connections, certificates can either be obtained from a trusted third-party Certificate Authority, or a local Certificate Authority can be created and used to generate self-signed certificates. This section describes how to create a Certificate Authority using the *strongswan* application on a Linux machine, then how to use this to generate keys and certificates for use on Vocality Gateway Nodes or other IPSec-enabled devices. (There are other methods for creating self-signed certificates but these are not covered here.)

The Certificate Authority should be created on a separate machine that is not running the Vocality Gateway Suite (referred to as the 'CA machine'). This machine should be fully secured according to the organization's IT security policy. A secure method of moving files from the Certificate Authority machine to the IPSec devices will also be required. The machine should be running a Linux distribution with the *strongswan* package installed.

On the CA machine, create a 'master private key file'. The file can have any name, but in this example is called **`caKey.pem`**:

```
strongswan pki --gen --outform pem > caKey.pem
```

The command can take a number of parameters to tailor the key generation, but the default settings produce a 2048-bit RSA key in the specified file.

Use this key to self-sign a Certificate Authority X.509 certificate, known as the 'root certificate'. Again, any name will do, but this example uses **`caCert.pem`**:

```
strongswan pki --self --in caKey.pem --dn "C=GB, O=Vocality,
                    CN=VocalityGateway CA"
                --ca --outform pem > caCert.pem
```

In this command, the quoted string (C=GB, O=Vocality, CN=<ca-hostname> CA) is called the 'Distinguished Name' (DN). This can be made up of several components; here Country, Organization and Common Name (CN) are specified.

Keys and certificates can now be created for each IPSec-enabled device that will form the IPSec connection end-points. Generate a private key for each device:

```
strongswan pki --gen --outform pem > PrivateKeyLHS.pem

strongswan pki --gen --outform pem > PrivateKeyRHS.pem
```

The CA certificate can then be used to generate individual certificates for each device. First, a public key file for the device needs to be created from the private key:

```
strongswan pki --pub --in PrivateKeyLHS.pem --outform pem >
                    PublicKeyLHS.pem

strongswan pki --pub --in PrivateKeyRHS.pem --outform pem >
                    PublicKeyRHS.pem
```

The public key is then used, in conjunction with the CA certificate and master private key, to create a certificate for the device:

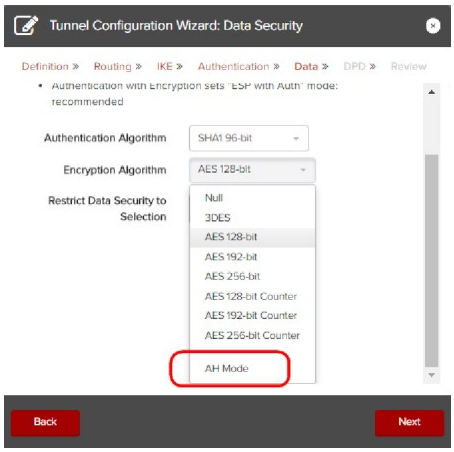
```
strongswan pki --issue --in PublicKeyLHS.pem --cacert caCert.pem
  --cakey caKey.pem --dn "C=GB, O=Vocality, CN=VocalityGateway"
           --san 12.1.1.2 --outform pem > CertLHS.pem

strongswan pki --issue --in PublicKeyRHS.pem --cacert caCert.pem
  --cakey caKey.pem --dn "C=GB, O=Vocality, CN=VocalityGateway"
           --san 13.1.1.2 --outform pem > CertRHS.pem
```

The device private key file (**`PrivateKeyLHS.pem`**), the device certificate (**`CertLHS.pem`**) and the Certificate Authority root certificate (**`caCert.pem`**) need to be available to the IPSec device. In the case of a machine running the Vocality Gateway Suite, these files can be uploaded via the **Secure > Certificate Management submenu** (see **Set up IPSec tunnels - using Public Key Infrastructure (PKI)**).

6 Set up IPSec tunnels - Authentication Header (AH) only

The IPSec Authentication Header provides authentication of IP traffic, but not encryption. This allows integrity and data origin to be confirmed, but does not provide data confidentiality.

To create an IPSec Security Association using only AH, follow all the steps to **Set up IPSec tunnels - using Pre-Shared Keys (PSK)** or **Set up IPSec tunnels - using Public Key Infrastructure (PKI)**. However, in the **Tunnel Configuration Wizard > Data Security** select 'AH Mode' in the 'Encryption Algorithm' drop-down box.



Once the IPSec tunnel has been correctly established and installed, IP traffic matching the source and destination networks entered in the IPSec tunnel configuration will be sent with an additional

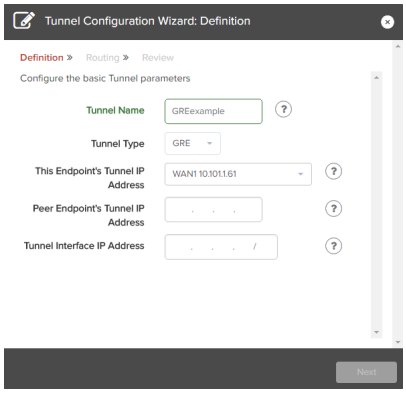
Authentication Header to the peer machine, but will not be encrypted.

7 Set up IPSec transport - to secure traffic in GRE tunnel

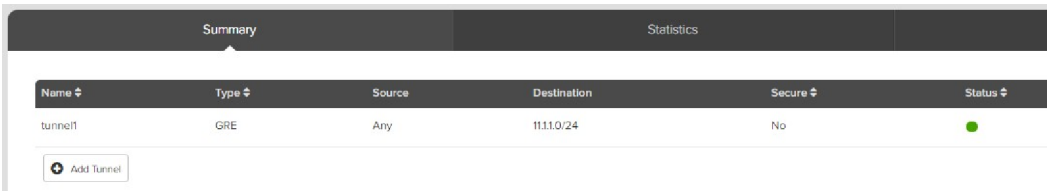
In some situations it is not appropriate to set up an IPSec tunnel directly. Particularly as IPSec does not support multicast or broadcast addressing. One of the most common ways to use those services in conjunction with IPSec is to establish a non-secure tunnel, and then use IPSec in transport mode to encrypt the IP traffic sent via the tunnel. In this example, IPSec is used in transport mode to secure the traffic sent over a GRE tunnel.

To configure a GRE tunnel with IPSec transport, first create the GRE tunnel. Start the Tunnel Configuration Wizard. Give your tunnel a name and choose the tunnel type 'GRE'. Select the IP address for the local endpoint of the tunnel, at this Vocality Gateway Node, from the dropdown menu or select 'Enter IP Address' to manually enter another address. Enter an appropriate IP address for the peer endpoint of the tunnel.

Only when valid parameters have been entered in all of the boxes will the **<Next>** button become red and available to press.



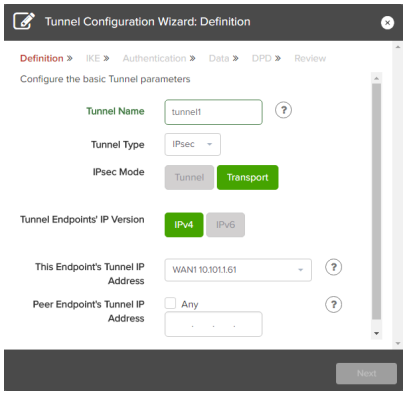
Repeat this procedure on the peer machine, then click the drop-down box marked 'Disabled' next to your configured tunnel on the **Secure > Summary menu**, and select 'Enabled'. When this has been done on both the local and peer machines, you should expect the 'Status' indicator will change to green to show that the tunnel has been correctly set up.



To configure an IPSec transport for the GRE tunnel, start the Tunnel Configuration Wizard again to add another tunnel.

Give your tunnel a name and choose the tunnel type 'IPSec'. Select IPSec Mode 'Transport'. Select the same IP address for the local endpoint of the tunnel, at this Vocality Gateway Node, from the dropdown menu as you have for your GRE tunnel. Enter an appropriate IP address for the peer endpoint of the tunnel, again matching your GRE tunnel.

Only when valid parameters have been entered in all of the boxes will the **<Next>** button become red and available to press.



Note: In transport mode, no source or destination networks are entered in the IPSec configuration. This is because in transport mode IPSec is only used to authenticate and encrypt IP traffic that has already been routed over the GRE tunnel.

Continue through the Tunnel Configuration Wizard, following all the steps to **Set up IPSec tunnels - using Pre-Shared Keys (PSK)** or **Set up IPSec tunnels - using Public Key Infrastructure (PKI)**.

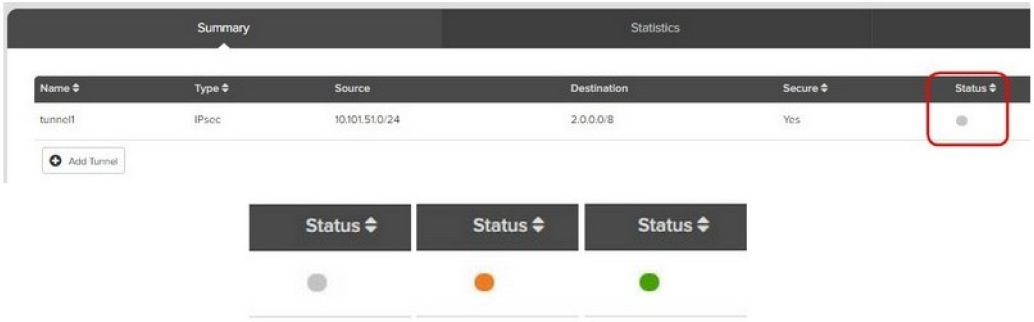
Once these have been completed, review the IPSec transport settings. All of the information entered so far is presented back to you. If there are any errors use the **<Back>** button to go to the right page to make a correction. When you press **<Finish>** this new tunnel will be added to the list on the **Secure > Summary menu**, but will not be active. From there you can choose any one of the icons, when needed, to:

- edit it ;
- delete it;
- enable/disable it (new tunnels are initially disabled by default); or
- view statistics regarding the use of that tunnel.

Note: Before an IPSec transport can be established you must ensure that a matching IPSec transport has been configured on the peer machine. 'Matching' transport definitions means that, for instance, the authentication and encryption algorithms chosen are the same on both the local and peer machines.

Once local and peer machines have a matching IPSec transport configuration, select the drop-down box marked 'Disabled' next to your configured tunnel on the **Secure > Summary menu**, and select 'Enabled'.

When this has been done on both the local and remote machines, you should expect the 'Status' indicator to change to green to show that the transport has been correctly installed. Now all IP traffic matching the source and destination networks, which you entered in the GRE tunnel configuration, will be encapsulated and encrypted before being sent to the remote machine.

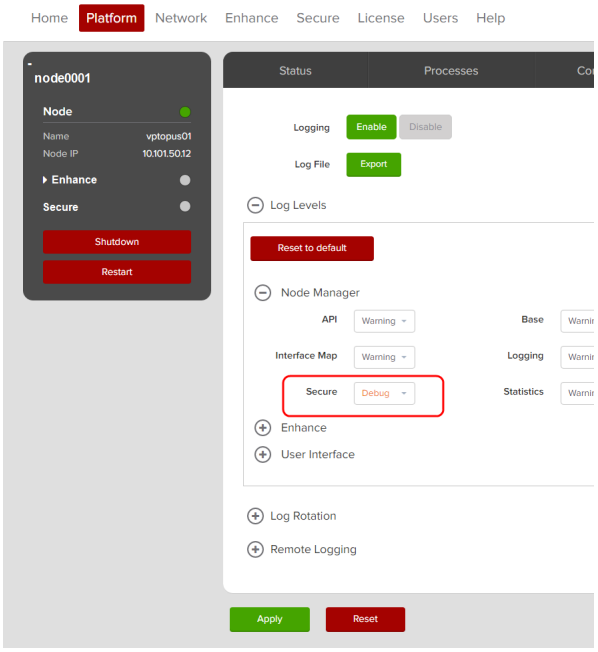


8 Debug IPSec tunnel problems

If you need more information about an IPSec tunnel which is failing to establish, you have the option to collect logs of the steps in the process.

The majority of operations required to create, establish and install an IPSec Security Association are carried out by the *strongswan* application. Log data from this application is controlled by the Vocality Gateway NodeManager logging system. At the default 'Warning' level of logging, none of the detail from *strongswan* is recorded; if you set the logging level for the 'Secure' module to 'Info' or higher the *strongswan* logs will be retained.

To set this log level, go to the **Platform > Status menu**. Expand the 'Log Levels' section using '+', and for Node Manager > Secure select a level of 'Info' or 'Debug'. It can also be useful to change the level of the User Interface > Secure to match.



Once the log levels have been updated, all output detail from *strongswan* will be captured in the log file **`/var/log/vocality/secure.log`**.

9 About Application Notes

Application Notes are intended as a supplement to, rather than a substitute for, your User Manual. Should you have queries which are not answered by our current documentation, your local Vocality support team would be happy to hear from you.
E-mail **support@vocality.com**.

A IPSEC TERMINOLOGY

Here are a few of the terms used in describing IPSec:

AH	Authentication Header	Member of the IPSec protocol suite; guarantees connectionless integrity and data origin authentication
CA	Certification Authority	Entity that issues digital certificates
DH	Diffie Hellman	Algorithm used to establish a shared secret between two parties
ESP	Encapsulating Security Payload	Member of the IPSec protocol suite; provides authentication, integrity and confidentiality
GRE	Generic Routing Encapsulation	Tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links
IKE	Internet Key Exchange	Protocol used to set up a Security Association in the IPSec protocol suite
IPSec	Internet Protocol Security	Protocol suite for secure IP communications
OCSP	Online Certificate Status Protocol	Internet protocol used for obtaining the revocation status of X.509 digital certificates
PKI	Public Key Infrastructure	Set of roles, policies and procedures needed to create, manage, distribute, store and revoke digital certificates and manage public-key encryption
PSK	Pre-Shared Key	A shared secret, distributed to two or more parties before it needs to be used
SA	Security Association	The establishment of shared security attributes between two network entities to support secure communication