vocality
Efficient Networks

Configuring IPSec with IP Aggregates

Application Note AN140
Revision v1.2
August 2015

AN140 Configuring IPSec with IP aggregates

**IPSec requires the Security software (RTUSEC)
at VOS07_44.01 or later
and a Feature Key on all products.**

1 Overview

This Application Note explains how you can configure IPSec tunnels, by setting up the menus below the **IP > IPSec menu**, for an IPSec tunnel with pre-shared keys or an IPSec tunnel with IKE.

Overview: IPSec

IPSec has been implemented to allow encryption and/or authentication of two different types of traffic in the Vocality Operating System (VOS). Security Associations (SAs) can be configured to provide an IPSec path to a peer device.

- Transport security associations are available to secure IP application data originating and terminating on the local unit – initially these are available for use by IP aggregates only.
- Tunnel security associations are available to secure streams of IP traffic that are routed through the integrated IP router.

For both transport and tunnel security associations, it is possible to select whether encryption, authentication or both mechanisms are used, as well as selecting the algorithms used for encryption and/or authentication. The keys used for these algorithms may be fixed pre-shared keys that must match those on the peer unit of the SA, or may be exchanged with the peer using the IKEv1 or IKEv2 protocols. The IKE implementation provides a pre-shared key mechanism for peer authentication.

2 Protocols and algorithms

Security associations (both tunnelled and transport) may be configured with a range of protocols/combination of protocols:

AH – authentication header only

ESP – encapsulating security protocol only

ESP-AH – combination of ESP & AH protocols

ESP-AUTH – encapsulating security protocol with authentication

Any of the following encryption algorithms:

3DES

AES128

AES192

AES256

Any of the following hash algorithms:

SHA1

MD5

AES128

SHA2-256

SHA2-384

SHA2-512

From VOS08_42.01 software onwards, if any of the permissible protocols are unsuitable for your applications, you are able to allow/disallow the use of certain protocols using the **IPSec > IKE Crypto Algorithms menu**, **IPSec > IKE Hash Algorithms menu**, **IPSec > IKE DH Groups menu** and **IPSec > IKE Auth Algorithms menu**

3 Securing IPAggs

Secure VPNs can now be created between Vocality units through the application of IPSec transport security associations on IP aggregate traffic. Any IP aggregate on the unit can be configured to use an IPSec transport SA to encrypt and or authenticate data over the IP aggregate. The IP aggregate peer must also be configured for IPSec use. IPAggs can be specifically configured to operate over an IPSec transport stream. Alternatively, it is possible to use IPSec tunnels (with their larger header overhead) by securing the IPAgg data as part of the standard embedded IP router tunnelling policy (refer to Application Note AN141 Configuring IPSec tunnels).

The use of an IPSec transport increases the data overhead of the IPAgg, and therefore the overall bandwidth used to multiplex data across the aggregate. The size of the IPSec transport header added to each packet depends on the IPSec protocol and algorithms chosen.

At this time the use of IPSec transport requires the IPAgg peer address to be known. This makes it incompatible with the existing IPAgg feature of accepting an authenticated connection from a peer configured as 'ANY'. If an IPAgg is configured with an IPSec transport, then the peer address must not be configured as 'ANY'.

It is possible to select IKE for key management on the IPSec transport SA used by an IPAgg and have the IKE configuration require re-keying (either periodically or after a certain amount of traffic has used the SA). In this case, it should be noted that constant bit rate tributary services carried across the IPAgg may suffer a brief interruption whenever the re-keying occurs.

4 Securing an IPAgg with pre-shared keys

Step 1

First, go to the **IP > IPSec > Keys menu** and select <ADD KEY>. Assign a name to the description field and then enter a pre-shared key. (In the M&C interface you must use the **<Enter>** key to submit each entry. In the web interface you will need to use the buttons to **<Validate>** your entries and **<Save Validated Changes>**.)

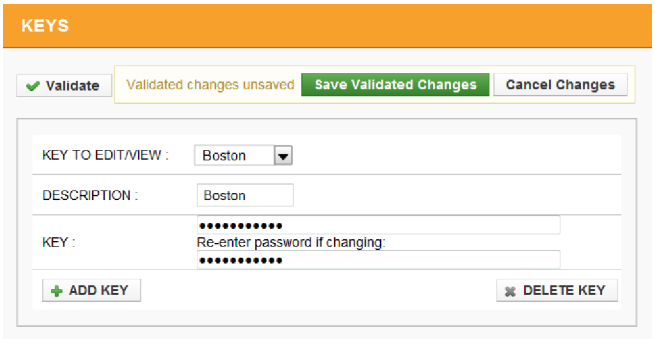

Figure 1 IPSEC Keys menu

Step 2

Then go to the **IP > IPSec > Transport Security Associations menu** and select <ADD SA>. Assign a name to the description field and change 'MODE' to 'MANUAL'. For all 'KEY' fields select the

named key created in Step 1 .

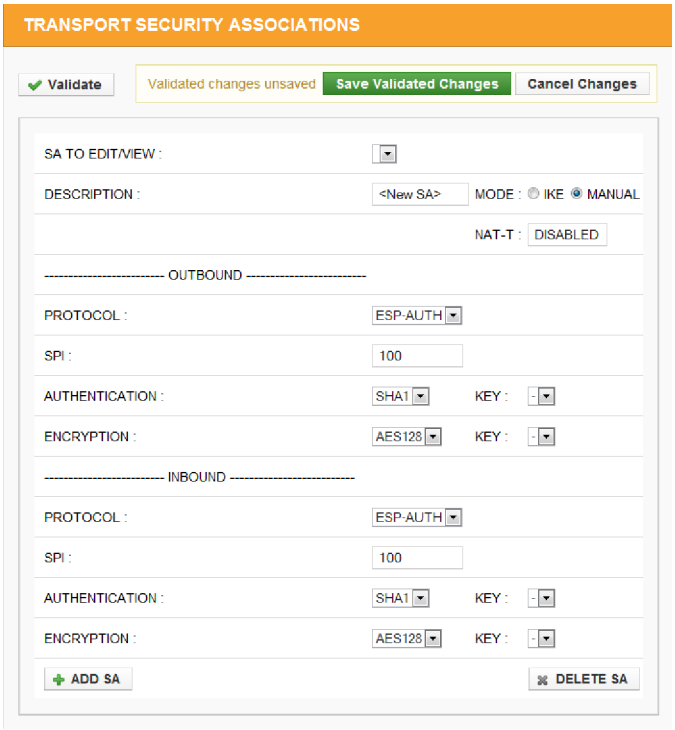

Figure 2 IPSec > Transport Security Associations menu - pre-shared keys

Refer to the **Menus** appendix for details of all the parameters that can be set.

Step 3

Finally, go to the **IP > IP Aggregates menu** and in the 'IPSEC' field select the named IPSec transport SA, which you created in Step 2 .

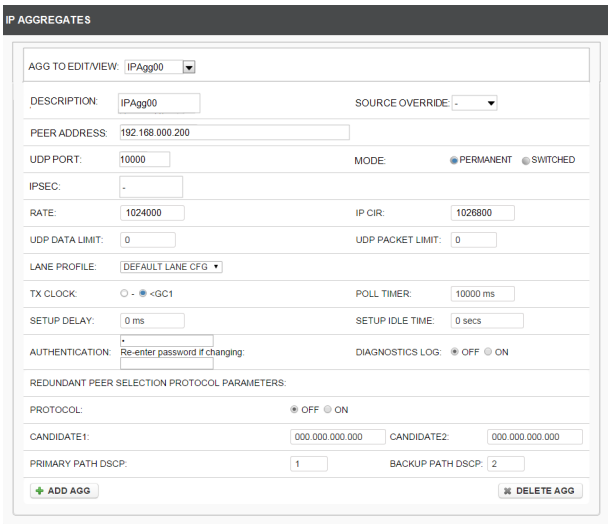

Figure 3 IP Aggregates menu

4.1 Securing an IPAgg with IKE

Step 1

First, go to the **IP > IPSec > IKE Server menu** and set the 'STATE' field to 'Enabled'. Set 'SOURCE INTERFACE' to the address used to identify the unit.

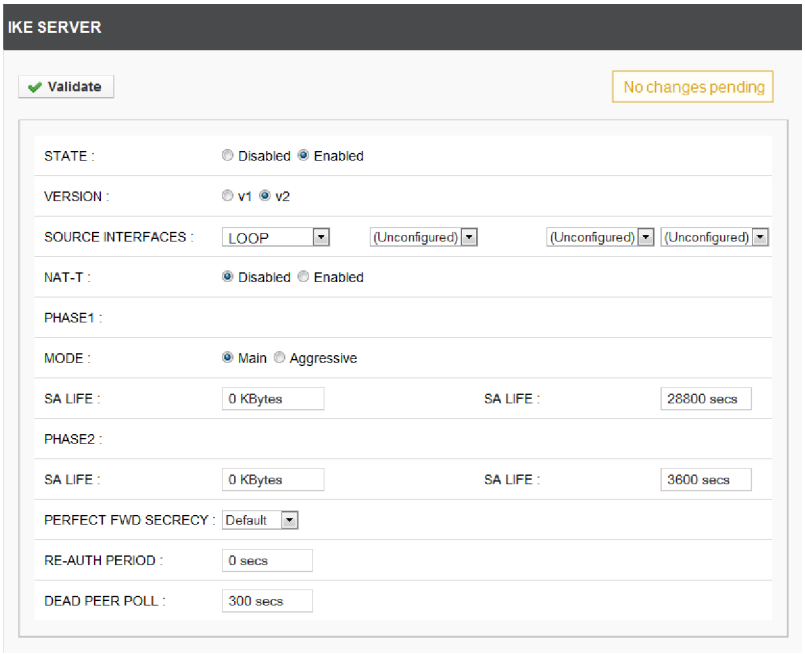

Figure 4 IPSec > IKE Server menu

Refer to the **Menus** appendix for details of all the parameters that can be set.

Step 2

Then, go to the **IP > IPSec > Keys menu** (see Figure 1) and select <ADD KEY>. Assign a name to the description field and then enter a pre-shared key.

Step 3

Next, go to **IP > IPSec > Transport Security Associations** and select <ADD SA>. Assign a name to the description field and change 'MODE' to 'IKE'. In the 'IKE PRE-SHARED KEY' field select the named key which you entered in Step 2 .

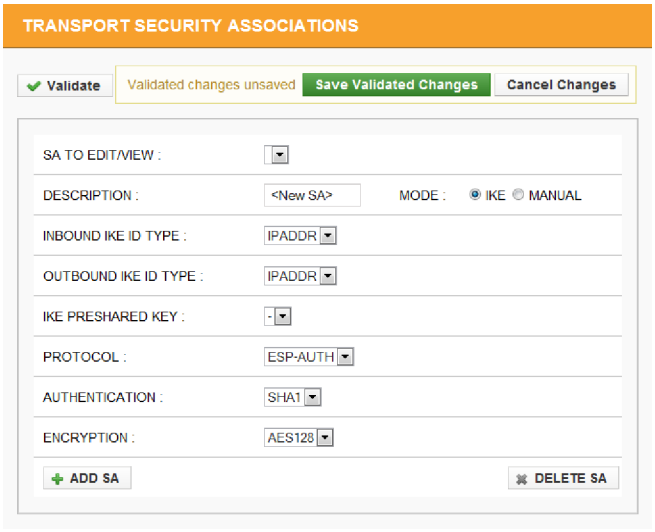

Figure 5 IPSec > Transport Security Associations menu - IKE

Refer to the **Menus** appendix for details of all the parameters that can be set.

Step 4

Finally, go to the **IP > IP Aggregates menu** (see Figure 3) and in the 'IPSEC' field select the named IPSec transport SA, which you created in Step 3 .

Repeat this for the other the Vocality unit at the other end of the link.

5 Logs

Messages are generated in the **Diagnostics > Slot n > Logs > IP Log** when IKE security associations are created, deleted or fail to establish.

6 Diagnostics

There is a **Diagnostics > Slot n > IP > IPSec SAs menu**. This presents a summary of each security association currently in use on the unit. Each line on the menu represents a separate SA.

Note: SAs are connectionless entities. Their presence in this table and indeed statistics showing data usage on outgoing SAs are not an indication that the SA has been successfully established, particularly for manually-keyed SAs. However, the presence of IKE SAs in the table is an indication that the SA has been successfully negotiated with the IKE peer.

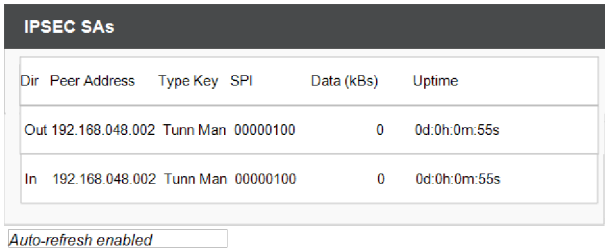

Figure 6 IPSec SAs diagnostics menu

Refer to the **Menus** appendix for details of all the parameters that can be set.

7 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 Menus

A.1 IP > IPSec menu

The feature is only available in the secure variant of software.

The IPSec menu provides access to menus for the configuration of security associations, tunnelling policies and the IKE (IPSec Key Exchange) server. There are then four menus which allow you to restrict which crypto, hash, Diffie-Hellman (DH) or authorisation algorithm types are allowable for your applications if you are using software VOS08_42.01 or later.

Tunnel menu entries are only shown on BASICS voice if the Router Feature Key is enabled.

A.1.1 IPSec > Keys menu

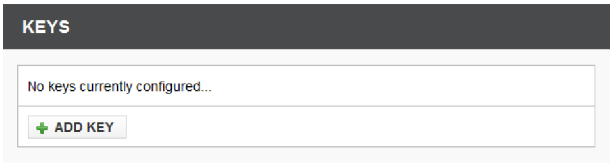

Figure 7 IPSec > Keys menu - blank

The keys menu is where any key used in IPSec or IKE is configured. As keys can be lengthy and cumbersome strings they are all separately configured in this menu where they are assigned a name. This name is used to reference the key in the security association and IKE menus. The keys can be referenced in the following locations:

- the pre-shared key for encryption for manually keyed transport or tunnel security associations (SAs)
- the pre-shared key for authentication for manually keyed transport or tunnel SAs
- the pre-shared key for IKE authentication for IKE keyed transport or tunnel SAs

Note: The keys used in the security association configuration must have been previously created in this menu, before the SA can be successfully configured.

By default there are no keys present.

Use the <ADD KEY> button to create a new named key. The following menu is presented:

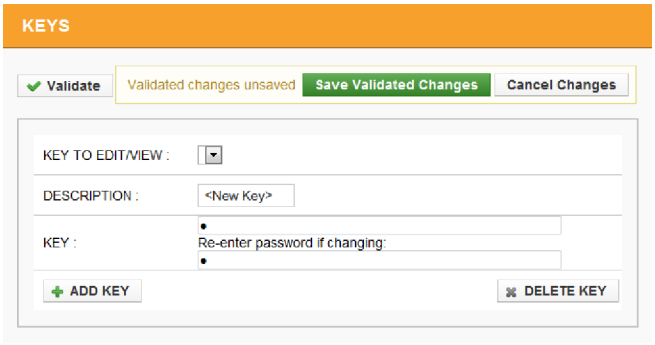

Figure 8 IPSec > Keys menu - new key

Enter the full case sensitive key information in the KEY field and then assign a unique key name to this key in the DESCRIPTION field.

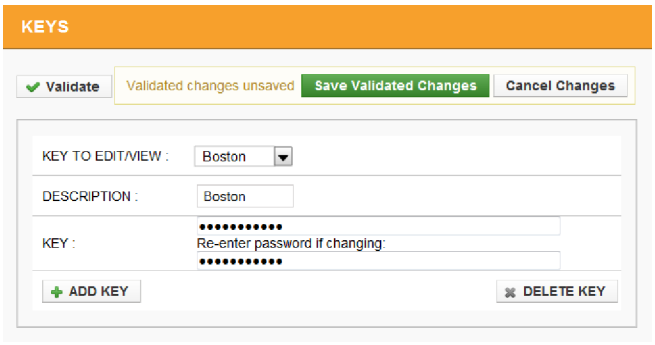

Figure 9 IPSec > Keys menu - adding key

The key name assigned in the DESCRIPTION field does not form part of the key data. It is only used to reference the entered key data in the security association menus. The KEY TO EDIT/VIEW field can be used to select which key to display/enter data for when more than one key is present in the configuration.

A.1.2 IPSec > Transport Security Associations menu

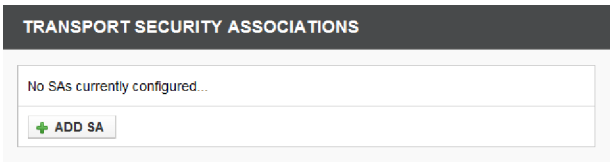

Figure 10 IPSec > Transport Security Associations menu - blank

The Transport Security Associations (SAs) menu provides configuration templates for transport security associations to be used by this unit. These are just named templates of parameters and do not include addressing information for the transport protocols that use these SAs. This addressing information comes from the application (for example GRE tunnel) that references these named transport SA templates.

By default there are no transport security associations present.

Use <ADD SA> to create a new transport security association template:

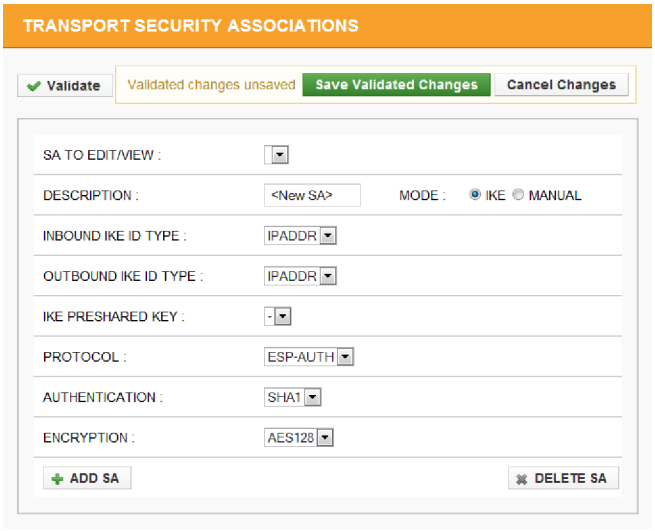

Figure 11 IPSec > Transport SAs menu - adding new

If a MANUAL mode is selected for this transport security association template, then the menu presentation changes to the following:

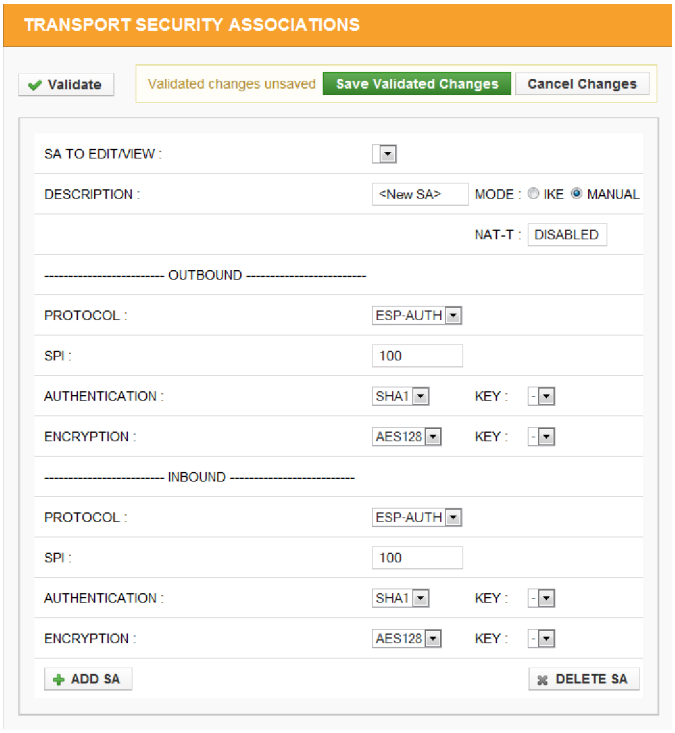

Figure 12 IPSec > Transport SAs menu - manual mode

The following fields are present for all Transport SAs:

Parameter	Use
SA TO EDIT/VIEW	Selection field used to select which of the named security associations to display/edit on this page. Used only when more than one transport security association is present in the configuration.
DESCRIPTION	Enter a unique name for this transport security association template. This name is used in the IPAgg configuration to reference an IPSec transport template to enable the securing of the IPSec transport.
MODE	IKE – use IKE for key management. MANUAL – use manual pre-shared keys for encryption and/or authentication.
NAT-T	Either DISABLED or the UDP port number to use for NAT translation if this SA traverses a NAT gateway.

Table A-1 Parameters applied to all Transport SAs

The following set of parameters are configurable separately for the inbound and outbound SAs associated with the IPSec transport:

Parameter	Use
INBOUND IKE ID TYPE	The type of identifier to use to identify inbound IKE peers: IPADDR – the IP address of the peer FQDN – a fully qualified domain name RFC822 – an RFC822 email-type address
INBOUND IKE ID	Only shown when the INBOUND IKE ID TYPE is FQDN or RFC822. This is the identifier to look for on IKE inbound traffic.
OUTBOUND IKE ID TYPE	The type of identifier to send to identify this SA to IKE peers. IPADDR – the IP address of the peer FQDN – a fully qualified domain name RFC822 – an RFC822 email-type address
OUTBOUND IKE ID	Only shown when the OUTBOUND IKE ID TYPE is FQDN or RFC822. This is the identifier to send on outbound IKE traffic.
IKE PRESHARED KEY	The pre-shared key used to authenticate the IKE peer. This is the name of a key configured in the **IPSec > Keys menu**.
PROTOCOL	The IPSec protocols to use on this SA. AH – authentication header only ESP – encapsulating security protocol only ESP-AH – combination of ESP & AH protocols ESP-AUTH – encapsulating security protocol with authentication
SPI	The security parameter index to use for this SA – entered as a 32 bit hex value. This must match with the value used on the peer.
AUTHENTICATION	The message authentication algorithm to use if a message authentication protocol has been selected: SHA1 AES MD5 SHA1-96 MD5-96 AES-XCBC-96 SHA2-256 SHA2-384 SHA2-512
KEY	The pre-shared key used to authenticate the message. This is the name of a key configured in the **IPSec > Keys menu**.
ENCRYPTION	The message encryption algorithm to use if a message encryption protocol has been selected: 3DES AES128 AES192 AES256 Several AES algorithms are presented with different key lengths. For manual SAs the actual algorithm used depends on the key length of the specified pre-shared key.
KEY	The pre-shared key used to encrypt the message. This is the name of a key configured in the **IPSec > Keys menu**.

Table A-2 Parameters separately configurable for inbound and outbound Transport SAs

A <DELETE SA> button is provided to delete a previously configured SA.

Note: If an SA which is deleted is being referenced by an IPAgg, then the IPAgg will no longer be secured.

A.1.3 IPSec > Tunnel Security Associations menu

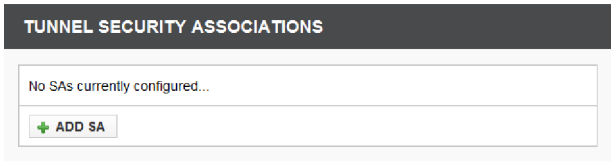

Figure 13 IPSec > Tunnel Security Associations menu - blank

The Tunnel Security Associations (SAs) menu provides configuration parameters for tunnel security associations to be used by this unit. Alternatively it is possible to use IP aggregates secured using IPSec transport encryption. Each tunnel is given a name – these named tunnels are referenced in **IPSec > Tunnelling Policies menu** to indicate which traffic is tunnelled through this SA.

By default there are no tunnel security associations present.

Use <ADD SA> to create a new tunnel security association:

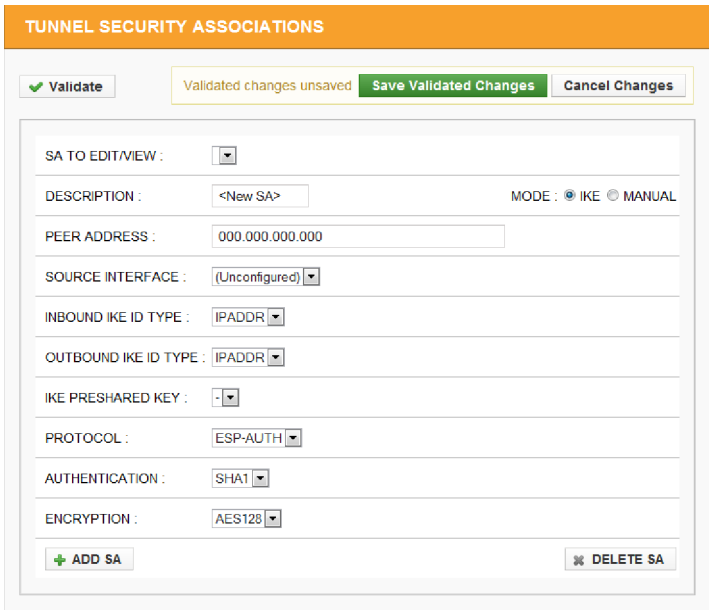

Figure 14 IPSec > Tunnel SAs menu - adding new

By default, IKE is selected as the mode, and the menu is presented as shown in Figure 14 If a MANUAL mode is selected for this tunnel security association template, then the menu presentation changes to the following:

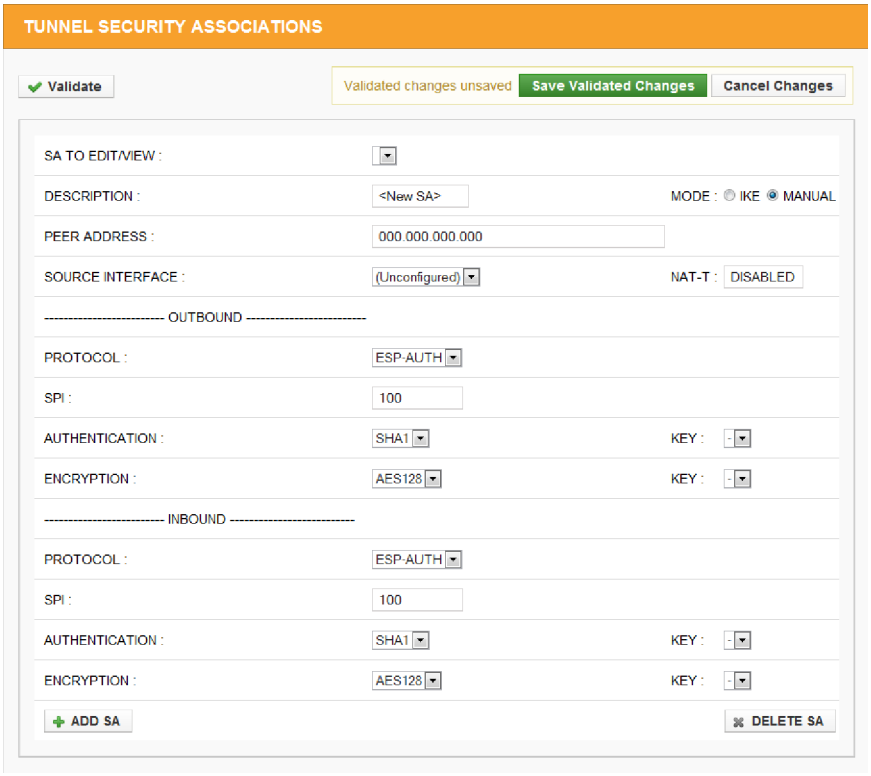

Figure 15 IPSec > Tunnel SAs menu - manual mode

The following fields are present for all Tunnel SAs:

Parameter	Use
SA TO EDIT/VIEW	Selection field used to select which of the named security associations to display/edit on this page. It is only of use when more than one tunnel security association is present in the configuration.
DESCRIPTION	Enter a unique name for this tunnel security association template. This name is used in the IPAgg configuration to reference an IPSec tunnel template to enable the securing of the IPSec tunnel.
MODE	IKE – use IKE for key management. MANUAL – use manual pre-shared keys for encryption and/or authentication.
PEER ADDRESS	The IP address of DNS resolvable name for the tunnel peer
SOURCE INTERFACE	Select the interface to use as the source address for this peer – this is not necessarily the interface on which data will be transmitted. It is only used to find the IP address to source packets. The peer unit may expect this to be fixed regardless of how traffic is routed to the peer.
NAT-T	Either DISABLED or the UDP port number to use for NAT translation if this SA traverses a NAT gateway.

Table A-3 Parameters applied to all Tunnel SAs

The following parameters are configurable separately for the inbound and outbound SAs associated with the IPSec tunnel:

Parameter	Use
INBOUND IKE ID TYPE	The type of identifier to use to identify inbound IKE peers: IPADDR – the IP address of the peer FQDN – a fully qualified domain name RFC822 – an RFC822 email-type address
INBOUND IKE ID	Only shown when the INBOUND IKE ID TYPE is FQDN or RFC822. This is the identifier to look for on IKE inbound traffic.
OUTBOUND IKE ID TYPE	The type of identifier to send to identify this SA to IKE peers. IPADDR – the IP address of the peer FQDN – a fully qualified domain name RFC822 – an RFC822 email-type address
OUTBOUND IKE ID	Only shown when the OUTBOUND IKE ID TYPE is FQDN or RFC822. This is the identifier to send on outbound IKE traffic.
IKE PRESHARED KEY	The pre-shared key used to authenticate the IKE peer. This is the name of a key configured in the **IPSec > Keys menu**.
PROTOCOL	The IPSec protocols to use on this SA. AH – authentication header only ESP – encapsulating security protocol only ESP-AH – combination of ESP & AH protocols ESP-AUTH – encapsulating security protocol with authentication
SPI	The security parameter index to use for this SA – entered as a 32 bit hex value. This must match with the value used on the peer.
AUTHENTICATION	The message authentication algorithm to use if a message authentication protocol has been selected: SHA1 AES MD5 SHA1-96 MD5-96 AES-XCBC-96 SHA2-256 SHA2-384 SHA2-512
KEY	The pre-shared key used to authenticate the message. This is the name of a key configured in the **IPSec > Keys menu**.
ENCRYPTION	The message encryption algorithm to use if a message encryption protocol has been selected: 3DES AES128 AES192 AES256 Several AES algorithms are presented with different key lengths. For manual SAs the actual algorithm used depends on the key length of the specified pre-shared key.
KEY	The pre-shared key used to encrypt the message. This is the name of a key configured in the **IPSec > Keys menu**.

Table A-4 Parameters separately configurable for inbound and outbound Tunnel SAs

A <DELETE SA> button is provided to delete a previously configured SA.

CAUTION: If a deleted SA is being referenced by a tunnel policy, then the referenced policy traffic will no longer be secured.

A.1.4 IPSec > Tunnelling Policies menu

An IPSec tunnelling policy menu is presented which provides access to menus for configuring which traffic that is routed through the embedded IP router should be sent via an IPSec tunnel.

A.1.4.1 ‡Tunnelling Policies > Address Definitions menu

This Address Definitions menu is identical to, but separate from, the **IP > Service Management > Address Definitions menu**. This ensures that IPSec tunnel policy can only be altered by Administrators.

Note: Only address definitions that use the MATCH operator may be used in the IPSec tunnel policy configuration.

A.1.4.2 ‡Tunnelling Policies > Protocol Definitions menu

This Protocol Definitions menu is identical to, but separate from, the **IP > Service Management > Protocol Definitions menu**. This ensures that IPSec tunnel policy can only be altered by Administrators.

A.1.4.3 ‡Tunnelling Policies > IPSec Tunnel Policy menu

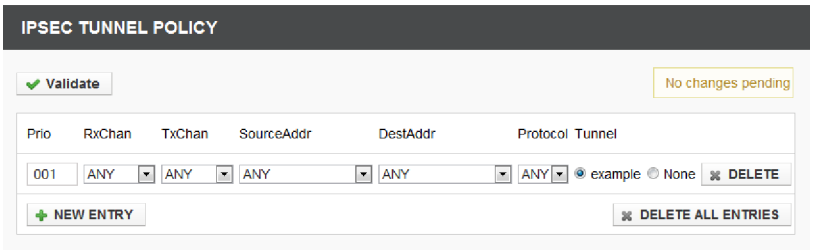

Figure 16 ‡Tunnelling Policies > IPSec Tunnel Policy menu - blank

The IPSec tunnel policy menu is where named address definitions and named protocol definitions are brought together in an ordered list to provide a selection mechanism for which traffic is to be tunnelled via IPSec and the security associations to use. The menu is similar to the Service Management menus for IP filtering and TCP gateway filtering. When traffic is IP routed, it is compared against each entry in the tunnel policy table in turn – if a match is found then the traffic is tunnelled via the specified IPSec tunnel SA. If no match is found, or the specified IPSec tunnel SA is 'None' then the traffic is not IPSec tunnelled and is routed unencrypted. To block specific traffic use the existing IP filter table.

By default, the IPSec tunnel policy table is empty (no packets will be IPSec tunnelled).

Use the <NEW ENTRY> button to add an entry to the policy table.

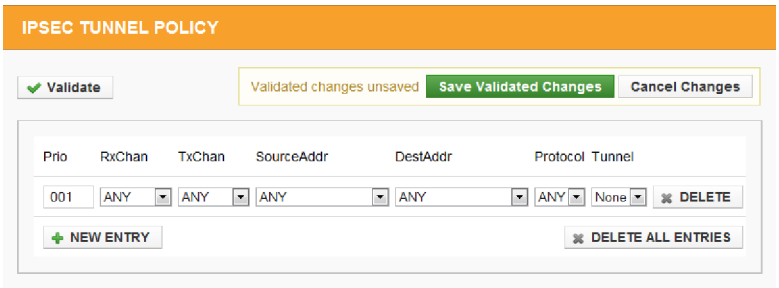

Figure 17 ‡Tunnelling Policies > IPSec Tunnel Policy menu - adding new

New entries are added to the end of the table. The order of the entries is important and this is the order that the comparisons are applied to routed traffic. When more than one entry is present the order can be altered via the Pri column.

The following table describes the parameters presented:

Parameter	Range	Use
Pri	1-216	The relative priority of this entry in the table. Change this to alter the order of the table row
Rx Chan	List of present IP router interfaces and ANY	The ingress interface to match for this policy entry
Tx Chan	List of present IP router interfaces and ANY	The egress interface to match for this policy entry
SourceAddr	List of configured MATCH address definitions and ANY, *DHCP Cli *portname*, *DHCP Net *portname*	The IP source address to match for this policy entry. *DHCP Cli portname identifies the IP address assigned to the port portname by DHCP. *DHCP Net portname identified the IP address/mask assigned to the port portname by DHCP. These can be selected for any port configured for DHCP operation.
DestAddr	List of configured MATCH address definitions and ANY, *DHCP Cli *portname*, *DHCP Net *portname*	The IP destination address to match for this policy entry *DHCP Cli portname identifies the IP address assigned to the port portname by DHCP. *DHCP Net portname identified the IP address/mask assigned to the port portname by DHCP. These can be selected for any port configured for DHCP operation.
Protocol	List of configured protocol definitions and ANY	The protocol to match for this policy entry
Tunnel	List of configured IPSec tunnel SAs and 'None'	The IPSec tunnel SA to use for traffic that matches this policy entry. If 'None' is specified then traffic that matches this policy entry is not IPSec tunnelled.

Table A-5 Parameters in the ‡Tunnelling Policies > IPSec Tunnel Policy menu

A.1.5 IPSec > IKE Server menu

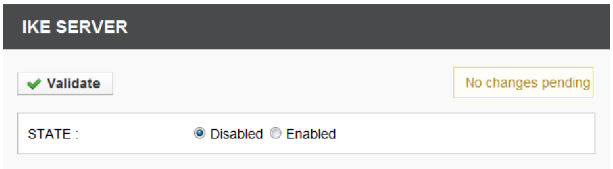

Figure 18 IPSec > IKE Server menu

Several parameters are available to tune operation of the IKE server. The IKE server must be configured if any IKE SAs are configured. IKE server configuration is presented in a single menu. By default, the IKE server is disabled.

When the STATE parameter is Enabled, the menu is updated to include all available IKE parameters:

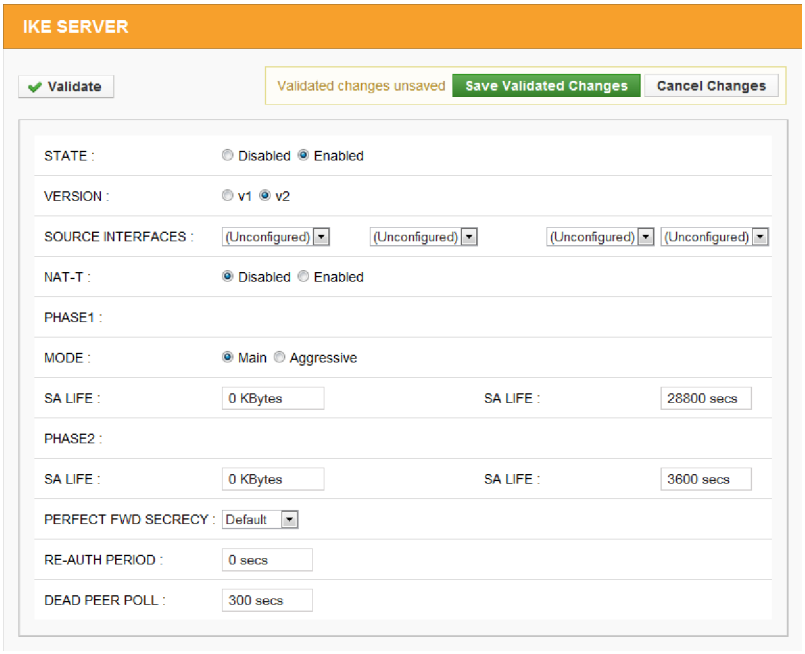

Figure 19 IPSec > IKE Server menu - State parameter enabled

The parameters available for configuration are:

Parameter	Range	Use
STATE	Disabled / Enabled	Enable/disable operation of the IKE server
VERSION	v1 / v2	Select the version of the IKE protocol to use
SOURCE INTERFACE	Range of present IP network interfaces	The source address to use for the IKE server. The address is selected from the specified interface.
NAT-T	Disabled / UDP port number	The port number to use for NAT traversal
PHASE 1		
DH GROUP	Any / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18	For IKEv1 this is the phase 1 Diffie-Hellman group to use. For IKEv2 this is the IKE SA initialisation default Diffie-Hellman group to use
MODE	NormalMain/Aggressive	Phase 1 negotiation mode
SA LIFE	kBytes – 0 for never	Proposed phase 1 number of kBytes to use the SA before re-keying
SA LIFE	secs – 0 for never	Propose phase 1 number of seconds to use the SA before re-keying
PHASE 2		
SA LIFE	kBytes – 0 for never	Proposed phase 2 number of kBytes to use the SA before re-keying
SA LIFE	secs – 0 for never	Propose phase 2 number of seconds to use the SA before re-keying
PERFECT FWD SECRECY	Default / Group1 / Group2 / Group5 / Group14 / Disabled	Perfect Forward Secrecy exchange mode
RE-AUTH PERIOD	secs – 0 for never	Time at which re -authentication is attempted (IKEv2 only)
DEAD PEER POLL	secs – 0 to 99999	The length of time no traffic is seen from the peer before it is considered to be dead and re-keying takes place.

Table A-6 Parameters in the IKE Server menu

A.1.6 IPSec > IKE Crypto Algorithms menu

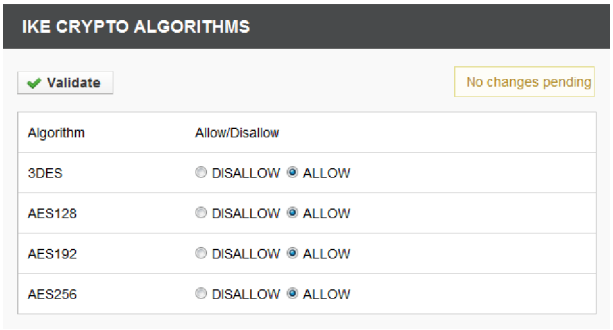

Figure 20 IPSec > IKE Crypto Algorithms menu

This menu allows you to restrict the encryption algorithms allowed. All of the algorithms listed are allowed on the unit by default, for maximum interoperability. You can use this menu to ALLOW or DISALLOW the use of particular algorithms from IKE.

When any changes are made to this menu the IKE server is restarted automatically.

A.1.7 IPSec > IKE Hash Algorithms menu

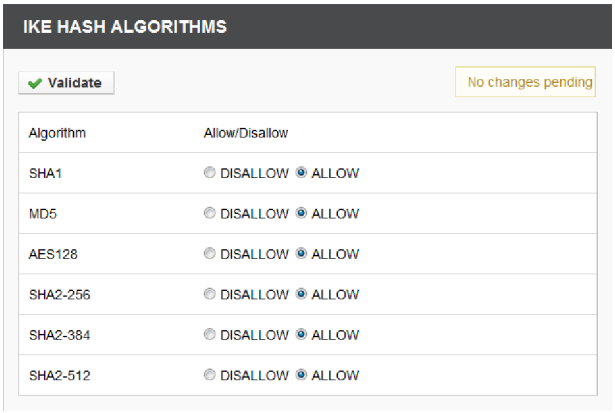

Figure 21 IPSec > IKE Hash Algorithms menu

This menu allows you to restrict which hash algorithms are allowed for pseudo-random functions. All of the algorithms listed are allowed on the unit by default, for maximum interoperability. You can use this menu to ALLOW or DISALLOW the use of particular algorithms from IKE.

When any changes are made to this menu the IKE server is restarted automatically.

A.1.8 IPSec > IKE DH Groups menu

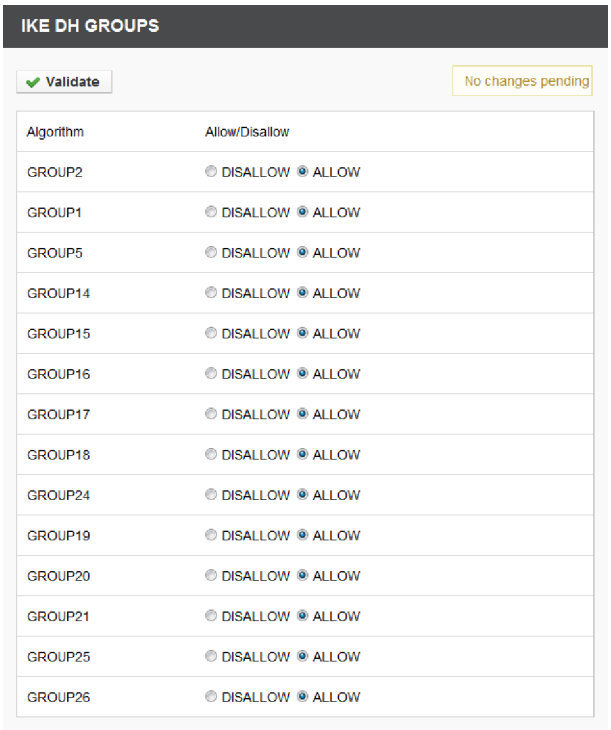

Figure 22 IPSec > IKE DH Groups menu

This menu allows you to restrict which Diffie-Hellman groups are allowed for key exchange. All of the algorithms listed are allowed on the unit by default, for maximum interoperability. You can use this menu to ALLOW or DISALLOW the use of particular algorithms from IKE.

When any changes are made to this menu the IKE server is restarted automatically.

A.1.9 IPSec > IKE Auth Algorithms menu

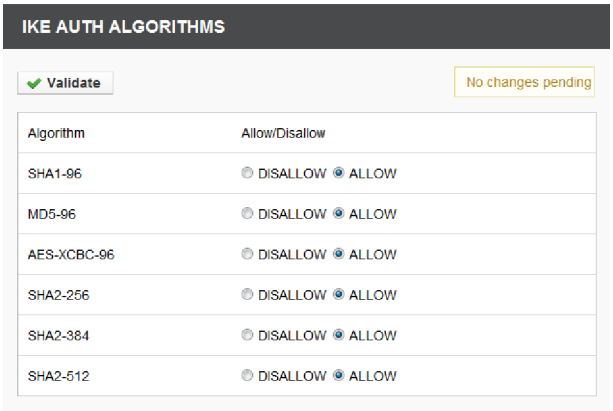

Figure 23 IPSec > IKE Auth Algorithms menu

This menu allows you to restrict which algorithms are allowed for message authentication. All of the algorithms listed are allowed on the unit by default, for maximum interoperability. You can use this menu to ALLOW or DISALLOW the use of particular algorithms from IKE.

When any changes are made to this menu the IKE server is restarted automatically.