



Configuring a Virtual Private Network (VPN) on KlasRouter

KB article reference no. Q10615

Version: 1.0

Keywords: KlasRouter, VPN, IPSec, GRE

The information in this article applies to:

- o KlasRouter v.2.0

Table of Contents

1.0 Introduction.....	3
2.0 Configuration of KlasRouter.....	3
2.1 Cable Connections	3
2.2 Establishing a HyperTerminal Session	3
2.3 Configuring the Ethernet LAN	3
2.4 Configuring the WAN Interface	3
2.5 Configuring IPSec.....	4
2.5.1 Creating a VPN Policy.....	4
2.5.1.1 Gateway-to-Gateway/Mobile-to-Gateway Policy	5
2.5.1.2 Gateway-to-Mobile Policy.....	7
2.5.2 Deleting a VPN Policy.....	10
2.5.3 Starting IPSec.....	10
2.5.4 Stopping IPSec.....	11
2.5.5 Activating an IPSec Policy	11
2.5.6 Deactivating an IPSec Policy.....	11
2.5.7 Viewing the Status of an IPSec Policy	12
2.5.8 Editing an IPSec Policy	13
2.5.9 Advanced IPSec Options	13
2.6 Configuring GRE.....	14
2.6.1 Add a GRE Tunnel.....	14
2.6.2 Edit a GRE Tunnel.....	15
2.6.3 Delete a GRE Tunnel.....	16

Table of Figures

Figure 1. IPSec Configuration Menu	4
Figure 2. Create a Gateway-to-Gateway/Mobile-to-Gateway VPN Policy	6
Figure 3. Advanced VPN Policy Options	7
Figure 4. Create a Gateway-to-Mobile VPN Policy	9
Figure 5. Deleting an IPSec Policy	10
Figure 6. Starting IPSec	10
Figure 7. Activating an IPSec Policy	11
Figure 8. Deactivating an IPSec Policy	12
Figure 9. Viewing an IPSec Policy	12
Figure 10. Editing an IPSec Policy	13
Figure 11. Advanced IPSec Options	14
Figure 12. GRE Configuration Menu	14
Figure 13. Add a GRE Tunnel	15
Figure 14. Edit a GRE Tunnel	16
Figure 15. Delete a GRE Tunnel.....	17

1.0 Introduction

This document describes how to configure Virtual Private Network (VPN) settings with KlasRouter. A VPN is a logical connection between two routers that have agreed to certain security parameters enabling them to exchange encrypted data. Once the data has passed through the VPN interface on the receive side, the router unencrypts the data and routes it to its final destination. KlasRouter supports two methods of establishing a VPN connection by using either the IP Security Protocol (IPSec) or the Generic Routing Encapsulation Protocol (GRE). IPSec uses stronger encryption algorithms and is the preferred method for establishing a VPN. GRE is a good method for encapsulating non-IP traffic and transporting it across an IP-based network. The following sections outline the steps needed to configure IPSec and GRE VPN tunnels with KlasRouter.

2.0 Configuration of KlasRouter

2.1 Cable Connections

Prior to beginning, ensure the following cable connections have been properly secured:

1. Power cord is plugged in and KlasRouter is on.
2. Control Port Cable is connected to the PCs serial port.
3. Control Port Cable is connected to the 'Control' port on the front of the KlasRouter.

2.2 Establishing a HyperTerminal Session

To configure the KlasRouter, you must establish a HyperTerminal Session between a PC and the KlasRouter. Follow the instructions in KlasRouter Application Note Q10601 to successfully establish a HyperTerminal Session and open the KlasRouter Main Configuration Menu.

2.3 Configuring the Ethernet LAN

The Ethernet LAN is generally the source of the traffic that will be encrypted and sent over the VPN link. Therefore, prior to configuring the VPN parameters, it is important to know the exact network IP addresses that you will want to send over the link. Data coming from networks that are not identified as being sources of VPN traffic will not be encrypted. For more information on how to configure the Ethernet LAN, refer to KlasRouter Application Note Q10605.

2.4 Configuring the WAN Interface

KlasRouter has two WAN interfaces that are available as the VPN gateway interfaces, the Serial WAN and Ethernet WAN interfaces. Traffic arriving at these interfaces from the Ethernet LAN or VoIP ports will be encrypted and forwarded to the peer router on the

opposite side of the VPN logical connection. For more information on how to configure the KlasRouter WAN interfaces, refer to the following KlasRouter Application Notes:

- Configuring the KlasRouter Serial WAN Port: App Note Q10603
- Configuring the KlasRouter Ethernet WAN Port: App Note Q10604

2.5 Configuring IPSec

IPSec is a series of exchanges that involve a variety of different protocols and security algorithms. The specific combination of protocols and algorithms you choose to exchange and encrypt information make up a VPN Policy. When negotiating an IPSec connection, routers compare VPN Policies to ensure they are an exact match. If everything matches, the routers are able to authenticate each other and agree upon how they will encrypt the VPN traffic. This negotiation takes place in two phases. Phase I is known as the Internet Key Exchange (IKE) and is how routers authenticate each other in order to move on to Phase II. Phase II negotiates the actual IPSec parameters using the security parameters from Phase I. Once Phase II is complete and everything has matched up properly, the two routers officially accept the policies and establish the VPN connection or “tunnel”. Follow the steps below to reach the IPSec Configuration Menu.

1. Enter ‘7’ from the Main Configuration Menu to enter the Advanced Configuration Menu.
2. Enter ‘5’ from the Advanced Configuration Menu to enter the VPN Configuration Menu.
3. Enter ‘1’ on the VPN Configuration Menu to enter the IPSec Configuration Menu, shown below in Figure 1.

```

IPSec Confi gurati on
-----
1) IPSec Start/Stop/Restart
2) Vi ew IPSEc Poli ci es
3) Create IPSEc Poli cy
4) Del ete IPSEc Poli cy
5) Acti vate IPSEc Poli cy
6) Deacti vate IPSEc Poli cy
7) Edi t IPSEc Poli cy
8) IPSEc Debuggi ng
9) Advanced IPSEc Opti ons
Press 'x' to Return

Enter Opti on>

```

Figure 1. IPSec Configuration Menu

The following sections describe how to configure, activate, edit and view VPN policies using KlasRouter.

2.5.1 Creating a VPN Policy

There are two types of VPN Policies KlasRouter supports based on two possible scenarios involving the IP address of the peer VPN router. The first scenario assumes that

KlasRouter knows the actual IP address of the peer router and has a route to it. If you are creating a VPN tunnel over the Internet, the peer router must have a public IP address in order for KlasRouter to communicate with it and begin the negotiations. This scenario is called a Gateway-to-Gateway or Mobile-to-Gateway. However, another situation exists where the peer router may be connected to a private LAN and, therefore, does not have a public IP address. In this scenario, called Gateway-to-Mobile, KlasRouter recognizes that NAT Traversal is being used. NAT Traversal is a standard that takes the VPN packet from a private IP address and encapsulates it into a packet with a public IP address in order to route it over the Internet.

2.5.1.1 Gateway-to-Gateway/Mobile-to-Gateway Policy

1. Enter '3' on the VPN Configuration Menu to enter the Create IPsec Connection Configuration Menu.
2. Enter '1' on the Create IPsec Connection Configuration Menu to create a Gateway-to-Gateway/Mobile-to-Gateway Policy.
3. Enter a name to describe the policy you are creating. Figure 2 below, shows a sample policy being created. The policy name in this example is 'KlasVPN'.
4. You will now configure the IKE security parameters for Phase I in Steps 4-8. Enter the IKE encryption algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is AES-256.
5. Enter the IKE hash algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is the Secure Hash Algorithm (SHA).
6. Enter the IKE lifetime in seconds or press 'Enter' to accept the default, which is 86,400 seconds or 24 hours.
7. Enter the pre-shared key for authentication purposes. This key must match the key from the peer router exactly. In Figure 2, the pre-shared key is 'klas'.
8. Enter the peer router IP address. There are two options for entering the peer router address information. If you know the physical address, enter it in decimal form, as shown in Figure 2. The other option is to enter it as a fully-qualified domain hostname which can then be resolved using a DNS or Dynamic DNS Server. If you want to use a hostname, enter 'h' and then type in the fully-qualified domain hostname.
9. You will now configure the IPsec security parameters in Steps 9-12. Enter the IPsec hash algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is SHA-ESP.
10. Enter the IPsec encryption algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is AES-256.
11. Enter the IPsec mode you would like to use. KlasRouter supports both transport and tunnel mode. Type in 'transport' to use transport mode or press 'Enter' to accept the default, which is tunnel mode.
12. In Steps 12 and 13 you will configure a local and remote network pair. You can configure as many pairs as you like, but once configured, KlasRouter will only accept traffic where the source or destination IP addresses match the local or remote networks. All other packets will be dropped. Enter the IP Address and subnet mask

- of the local network that you want to encrypt traffic from in order to pass through the VPN tunnel.
13. Enter the IP Address and subnet mask of the remote network that you want to unencrypt coming from the VPN tunnel.
 14. KlasRouter will ask if you wish to configure another local/remote network pair. These additional local/remote network pairs will have the same IKE and IPsec security parameters as the original local/remote network pair. Enter 'y' to configure another pair or 'n' to move to the next step.
 15. If necessary, enter the next-hop router for this policy. Next-hop routing can be used when KlasRouter is acting as the Mobile VPN Router and must first forward IPsec packets on to another router that will have a route to the Internet. Enter the IP address of the next-hop router or press 'Enter' to accept the default, which is none.

```

Create Gateway-to-Gateway/Mobile-to-Gateway Policy
-----
Description:
- This option should be used if you are configuring the KlasRouter as an IPsec gateway in
a site-to-site configuration OR if the KlasRouter is a mobile unit using a dynamic IP
address.

Enter a name for this IPsec Connection ('?' for help|'q' to quit)>KlasVPN
CONFIGURE IKE
-----
Default IKE encryption algorithm: aes256
Enter IKE encryption algorithm ('?' for help|'q' to quit|<RET> for default)>aes256
Using Default IKE encryption algorithm: aes256

Default IKE hash algorithm: sha
Enter IKE hash algorithm ('?' for help|'q' to quit|<RET> for default)>sha
Using Default IKE hash algorithm: sha

Default IKE Lifetime: 86400 seconds
Enter IKE SA Lifetime seconds (1081-86400|'q' to quit|<RET> for default)>86400
Using Default IKE Lifetime: 86400 seconds

Enter pre-shared key ('q' to quit)>klas

Remote peer address options:
* Addr in IPv4 format | '?' for help | 'h' for hostname | 'q' to quit *
Enter remote peer address>192.168.3.1

CONFIGURE IPSEC
-----
Default IPsec hash algorithm: esp-sha
Enter IPsec hash algorithm ('?' for help|'q' to quit|<RET> for default)>esp-sha
Using Default hash algorithm: esp-sha

Default IPsec encryption algorithm: aes256
Enter IPsec encryption algorithm ('?' for help|'q' to quit|<RET> for default)>aes256
Using Default IPsec encryption algorithm: aes256

Default IPsec Mode: tunnel
Enter IPsec mode ('?' for help|'q' to quit|<RET> for default)>tunnel
Using Default IPsec mode: tunnel

Enter Local Network/Mask ('?' for help|'q' to quit)>192.168.1.0/24
Enter Remote Network/Mask ('?' for help|'q' to quit)>192.168.4.0/24
Enter another local/remote network/host pair? (y|n|'? ' for help|'q' to quit)>n
Enter nexthop router ('?' for help|'q' to quit|<RET> for none)>

```

Figure 2. Create a Gateway-to-Gateway/Mobile-to-Gateway VPN Policy

16. KlasRouter will ask if you wish to configure advanced options for this VPN Policy. Advanced options include IP Compression, Perfect Forward Secrecy and Dead Peer Detection. Enter 'y' to configure advanced option or 'n' to move to the configuration summary in Step 20. Figure 3, shown below, displays the IPsec Advanced Configuration Options.

```

Policy Advanced Options
-----
1) Perfect Forward Secrecy
2) Security Association Lifetime
3) Security Association Rekey
4) Keyingtries
5) Dead Peer Detection
6) Compression
7) Local/Remote Identity
Press 'x' to Return

Enter Option>6

Default Compression setting: no
Enable IPComp compression? (y|n|'q' to quit)>y
IPComp Compression enabled.

Press Enter to Return

```

Figure 3. Advanced VPN Policy Options

17. The Policy Advanced Options shown above in Figure 3 list the 7 options you can choose to configure in addition to the mandatory IPsec parameters. Figure 3 shows the IP Compression option being enabled.
18. Press 'Enter' to return to the Policy Advanced Options.
19. Once finished configuring advanced options, press 'x' to move to the configuration summary.
20. The configuration summary will list all of the mandatory and advanced parameters chosen for this VPN policy. At the end of the list, you will be prompted to accept or deny the configuration. Enter 'y' to accept the configuration or 'n' to reject the parameters the way they are shown and edit one or more to a different value.
21. Once you have accepted the configuration, you will be asked whether or not you want to activate the policy. By activating the policy, you will be initiating the Phase I IKE exchange between two VPN routers. Enter 'y' to activate the IPsec policy immediately or enter 'n' to save the policy and activate it later.
22. Press 'Enter' to return to the Create IPsec Configuration Menu
23. Press 'x' to return to the IPsec Configuration Menu.

2.5.1.2 Gateway-to-Mobile Policy

1. Enter '3' on the VPN Configuration Menu to enter the Create IPsec Connection Configuration Menu.
2. Enter '2' on the Create IPsec Connection Configuration Menu to create a Gateway-to-Mobile Policy.

3. Enter a name to describe the policy you are creating. Figure 4 below, shows a sample policy being created. The policy name in this example is 'KlasMobile'.
4. You will now configure the IKE security parameters for Phase I in Steps 4-8. Enter the IKE encryption algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is AES-256.
5. Enter the IKE hash algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is the Secure Hash Algorithm (SHA).
6. Enter the IKE lifetime in seconds or press 'Enter' to accept the default, which is 86,400 seconds or 24 hours.
7. Enter the pre-shared key for authentication purposes. This key must match the key from the peer router exactly. In Figure 4, the pre-shared key is 'klas'.
8. You will now configure the IPSec security parameters in Steps 9-12. Enter the IPSec hash algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is SHA-ESP.
9. Enter the IPSec encryption algorithm you would like to use. Press '?' to list the algorithms available or press 'Enter' to accept the default, which is AES-256.
10. Enter the IPSec mode you would like to use. KlasRouter supports both transport and tunnel mode. Type in 'transport' to use transport mode or press 'Enter' to accept the default, which is tunnel mode.
11. In Steps 12 and 13 you will configure a local and remote network pair. You can configure as many pairs as you like, but once configured, KlasRouter will only accept traffic where the source or destination IP addresses match the local or remote networks. All other packets will be dropped. Enter the IP Address and subnet mask of the local network that you want to encrypt traffic from in order to pass through the VPN tunnel.
12. Enter the IP Address and subnet mask of the remote network that you want to unencrypt coming from the VPN tunnel.
13. KlasRouter will ask if you wish to configure another local/remote network pair. These additional local/remote network pairs will have the same IKE and IPSec security parameters as the original local/remote network pair. Enter 'y' to configure another pair or 'n' to move to the next step.
14. If necessary, enter the next-hop router for this policy. Next-hop routing can be used when KlasRouter is acting as the Mobile VPN Router and must first forward IPSec packets on to another router that will have a route to the Internet. Enter the IP address of the next-hop router or press 'Enter' to accept the default, which is none.

```

Create Gateway-Mobile Policy
-----
Description:
- This option should be used if you are configuring the KlasRouter as an IPSec
  gateway to allow mobile units to have secure access to your network
  NOTE: If creating more than 1 of this kind of policy, they must all be
  configured with the same pre-shared key!

Enter a name for this IPSec Connection ('?' for help|'q' to quit)>Klas_Mobile

CONFIGURE IKE
-----

Default IKE encryption algorithm: aes256
Enter IKE encryption algorithm ('?' for help|'q' to quit|<RET> for default)>
Using Default IKE encryption algorithm: aes256

Default IKE hash algorithm: sha
Enter IKE hash algorithm ('?' for help|'q' to quit|<RET> for default)>
Using Default IKE hash algorithm: sha

Default IKE Lifetime: 86400 seconds
Enter IKE SA Lifetime seconds (1081-86400|'q' to quit|<RET> for default)>
Using Default IKE Lifetime: 86400 seconds

Enter pre-shared key ('q' to quit)>klas

CONFIGURE IPSEC
-----

Default IPSec hash algorithm: esp-sha
Enter IPSec hash algorithm ('?' for help|'q' to quit|<RET> for default)>
Using Default hash algorithm: esp-sha

Default IPSec encryption algorithm: aes256
Enter IPSec encryption algorithm ('?' for help|'q' to quit|<RET> for default)>
Using Default IPSec encryption algorithm: aes256

Default IPSec Mode: tunnel
Enter IPSec mode ('?' for help|'q' to quit|<RET> for default)>
Using Default IPSec mode: tunnel

Enter Local Network/Mask ('?' for help|'q' to quit)>192.168.1.0/24

Enter Remote Network/Mask ('?' for help|'q' to quit)>192.168.4.0/24

Enter another local/remote network/host pair? (y|n|'? for help|'q' to quit)>n

Enter nexthop router ('?' for help|'q' to quit|<RET> for none)>

Configure advanced options for this policy? (y|n|'q' to quit)>y

```

Figure 4. Create a Gateway-to-Mobile VPN Policy

15. KlasRouter will ask if you wish to configure advanced options for this VPN Policy. Advanced options include IP Compression, Perfect Forward Secrecy and Dead Peer Detection. Enter 'y' to configure advanced option or 'n' to move to the configuration summary in Step 16.
16. The configuration summary will list all of the mandatory and advanced parameters chosen for this VPN policy. At the end of the list, you will be prompted to accept or deny the configuration. Enter 'y' to accept the configuration or 'n' to reject the parameters the way they are shown and edit one or more to a different value.
17. Once you have accepted the configuration, you will be asked whether or not you want to activate the policy. By activating the policy, you will be initiating the Phase I IKE exchange between two VPN routers. Enter 'y' to activate the IPSec policy immediately or enter 'n' to save the policy and activate it later.

18. Press 'Enter' to return to the Create IPSec Configuration Menu
19. Press 'x' to return to the IPSec Configuration Menu.

2.5.2 Deleting a VPN Policy

1. Enter '4' on the IPSec Configuration Menu to enter the Delete IPSec Policy Configuration Menu.
2. As shown below in Figure 5, the currently configured VPN Policies are listed. Enter the number of the IPSec Policy you would like to delete. Figure 5 shows the 'Klas_Mobile' policy being deleted.

```

Delete an IPSec Policy
-----
Idx Name                Int   Networks to Tunnel                Status
-----
1  Klas_Mobile           Int   192.168.1.0/24   192.168.4.0/24   DOWN
2  KlasVPN                Int   192.168.1.0/24   192.168.4.0/24   DOWN

The 'Int' column refers to the interface on which the policy is activated.
The policy is not activated if this field is blank.

Select IPSec Policy to delete ('q' to quit)>1
Are you sure you want to delete the policy "Klas_Mobile"? (y|n)>y

```

Figure 5. Deleting an IPSec Policy

3. Enter 'q' to return to the IPSec Configuration Menu.

2.5.3 Starting IPSec

1. Enter '1' on the IPSec Configuration Menu to enter the IPSec Control Menu.
2. Enter '1' to Start IPSec, as shown below in Figure 6.

```

IPSec Control
-----
1) Start IPSec
2) Stop IPSec
3) Restart IPSec
4) IPSec Status
Press 'x' to Return

Enter Option>
Starting IPSec ... OK.

Press Enter to Return

```

Figure 6. Starting IPSec

3. Press 'Enter' to return to the IPSec Control Menu.
4. Press 'x' to return to the IPSec Configuration Menu.

2.5.4 Stopping IPsec

1. Enter '1' on the IPsec Configuration Menu to enter the IPsec Control Menu.
2. Enter '2' to Stop IPsec
3. Press 'Enter' to return to the IPsec Control Menu.
4. Press 'x' to return to the IPsec Configuration Menu.

2.5.5 Activating an IPsec Policy

1. Enter '5' on the IPsec Configuration Menu to enter the Activate IPsec Policy Menu.
2. As shown below in Figure 7, the currently configured IPsec policies will be listed. Enter the number of the IPsec policy you would like to activate. In Figure 7, the 'KlasVPN' policy is being activated
3. Enter the WAN interface you would like to apply the IPsec policy on. Press '?' to list the available WAN interfaces. If you are using a default route over a WAN interface and you wish to use that WAN interface, you must type in 'defroute' in order to activate the IPsec policy. In Figure 7, the IPsec policy is being activated on the Ethernet WAN interface, 'ixp1'. Once activated, KlasRouter will begin to exchange IPsec parameters with the VPN peer.

```

Activate IPsec Policy
-----
Idx Name                Int  Networks to Tunnel                Status
-----
1  KlasVPN                192.168.1.0/24  192.168.4.0/24  DOWN

The 'Int' column refers to the interface on which the policy is activated.
The policy is not activated if this field is blank.

Select IPsec Policy to activate ('q' to quit)>1
IPsec Policy to activate: KlasVPN
Select WAN interface ( <RET> for 'defroute' | '?' for help | 'q' to quit )>ixp1
Initiating IPsec connection ...
IPsec Policy "KlasVPN" mapped to ixp1.
Starting IPsec ... OK.

Press Enter to return to IPsec Menu

```

Figure 7. Activating an IPsec Policy

4. Press 'Enter' to return to the IPsec Control Menu.

2.5.6 Deactivating an IPsec Policy

1. Enter '6' on the IPsec Configuration Menu to enter the Deactivate IPsec Policy Menu.
2. As shown below in Figure 8, the currently configured IPsec policies will be listed. Enter the number of the IPsec policy you would like to deactivate. In Figure 8, the 'KlasVPN' policy is being deactivated.

```

Deactivate IPsec Policy
-----
Idx Name           Int   Networks to Tunnel           Status
-----
1   Kl asVPN        i xp1 192. 168. 1. 0/24           192. 168. 4. 0/24           DOWN

The 'Int' column refers to the interface on which the policy is activated.
The policy is not activated if this field is blank.

Select IPsec Policy to deactivate ('q' to quit)>1

Deactivating IPsec Policy: Kl asVPN. conn ...
Stopping IPsec ... OK.

```

Figure 8. Deactivating an IPsec Policy

3. You can now continue to deactivate more IPsec policies or enter 'q' to return to the IPsec Configuration Menu.

2.5.7 Viewing the Status of an IPsec Policy

1. Enter '2' on the IPsec Configuration Menu to view the currently configured IPsec policies.
2. As shown below in Figure 9, the currently configured IPsec policies will be listed. A description of the information provided in each column is provided below:
 - **Idx** – The policy list number.
 - **Name** – The configured name of the policy.
 - **Int** – The interface that the policy as been activated over. If the policy has not been activated, this column will be blank.
 - **Networks to Tunnel** – The configured local and remote network pair.
 - **Status** – The current status of the policy. 'Down' indicates that the policy has not been activated or has not found a proper policy match from the VPN peer. 'Up' indicates that the policy has found a matching policy from the VPN peer and is ready to exchange IPsec packets.

```

Current IPsec Policies
-----
Idx Name           Int   Networks to Tunnel           Status
-----
1   Kl asVPN        i xp1 192. 168. 1. 0/24           192. 168. 4. 0/24           DOWN

The 'Int' column refers to the interface on which the policy is activated.
The policy is not activated if this field is blank.

Press Enter to return to IPsec Menu

```

Figure 9. Viewing an IPsec Policy

3. Press 'Enter' to return to the IPsec Configuration Menu.

2.5.8 Editing an IPSec Policy

1. Enter '7' on the IPSec Configuration Menu to edit the currently configured IPSec policies.
2. The currently configured IPSec policies will be listed. Enter the number of the IPSec policy you would like to edit.
3. As shown in Figure 10, each parameter of the IPSec policy will be listed next to a letter. Enter the letter of the parameter you would like to edit. In Figure 10, the 'Next-Hop Router' parameter is being edited.

```

Edit IPSec Policy Configuration
-----
a) Name:                               KlasVPN
b) IKE encryption algorithm:           aes256
c) IKE hash algorithm:                 sha
d) IKE Lifetime:                       86400 seconds
e) Pre-shared secret:                  klas
f) Remote peer:                        192.168.2.1
g) IPSec hash algorithm:                esp-sha
h) IPSec encryption algorithm:         aes256
i) IPSec mode:                          tunnel
j) Local network:                      192.168.1.0/24
k) Remote network:                     192.168.4.0/24
l) Nexthop router:                     None

Advanced Settings:
m) Perfect Forward Secrecy:            No
n) SA Key Lifetime:                    28800 seconds
o) Rekey at expiry:                     Yes
p) Keyingtries:                         Always
r) Dead Peer Detection:                Active
   - DPD Delay:                         10 seconds
   - DPD Timeout:                       30 seconds
   - DPD Action:                         hold
s) IPComp Compression:                 Yes
t) Remote Identity:                     None
u) Local Identity:                      None

Select option to edit ('q' to quit)>l

```

Figure 10. Editing an IPSec Policy

4. Follow the instructions for that parameter to edit it to the value you would like.
5. You may now continue to edit additional parameters or enter 'q' to return to the Edit IPSec Policy Configuration Menu.
6. You may enter another number to edit additional policies or enter 'q' to return to the IPSec Configuration Menu.

2.5.9 Advanced IPSec Options

KlasRouter offers advanced IPSec options that a user may or may not wish to apply. If an advanced option is changed, the change will apply to all IPSec policies.

1. Enter '9' on the IPSec Configuration Menu to enter the Advanced IPSec Options Menu.
2. Figure 11 shows the two advanced options. Enter the number of the option you would like to configure and follow the directions to make the appropriate change.

```

IPSec Advanced Options
-----
NOTE: IPSec must be restarted if you change any of the
      following options!

1) Hide ToS field
2) Edit IPSec MTU (Default value: 16260)
Press 'x' to Return

Enter Option>

```

Figure 11. Advanced IPSec Options

3. Press 'x' to return to the IPSec Configuration Menu.

2.6 Configuring GRE

GRE is a form of VPN that is primarily used to encapsulate non-IP packets into a form that can be routed over an IP network. Since encryption is involved, GRE falls within the category of a VPN, but does not have the in-depth security features of IPSec. Follow the steps below to enter the GRE Configuration Menu.

1. Enter '7' from the Main Configuration Menu to enter the Advanced Configuration Menu.
2. Enter '5' from the Advanced Configuration Menu to enter the VPN Configuration Menu.
3. Enter '2' on the VPN Configuration Menu to enter the GRE Configuration Menu, shown below in Figure 12.

```

GRE Tunnel Configuration Menu
-----
1) Show Tunnels
2) Add Tunnel
3) Edit Tunnel
4) Delete Tunnel
Press 'x' to Return

Enter Option>

```

Figure 12. GRE Configuration Menu

The following sections describe how to add, edit and delete GRE tunnels with KlasRouter.

2.6.1 Add a GRE Tunnel

1. Enter '2' on the GRE Configuration Menu to add a GRE Tunnel. Steps 2-10 describe the steps needed to configure the parameters of a GRE Tunnel, as shown in Figure 13.
2. Enter a Tunnel Number from 0-9 to uniquely identify the GRE tunnel.

3. Enter the WAN Interface you would like to use for this tunnel. Figure 13 uses the Ethernet WAN interface.
4. Enter the destination IP address. This is the address of the peer router for this specific GRE Tunnel.
5. Enter the local tunnel IP address. This is the IP address you would like to assign the local end of the tunnel.
6. Enter the remote tunnel IP address. This is the IP address you would like to assign the remote end of the tunnel.
7. Enter the Time To Live (TTL) value for the tunnel. By pressing 'Enter' or entering '0', the TTL value will be taken from the tunneled packets. If you would like to specify a different TTL, enter a number from 1-255.
8. Indicate whether you would like to activate the tunnel checksum. The default is to not activate the checksum. To accept the default, press 'Enter' or enter 'n'. To activate the checksum, enter 'y'.
9. Enter the tunnel key. The tunnel key identifies specific traffic, which adds an element of security. The default is to not have a tunnel key. To add a tunnel key, enter a number from 0-4294967295. Figure 13 adds a tunnel key of 1000.
10. The configured parameters will be listed. You will be prompted to accept or reject the tunnel as shown. Enter 'y' to accept the tunnel configuration or 'n' to reject it.

```

Add Tunnel
-----
Enter Tunnel Number 0-9 ('q' to quit)>1
Enter Interface Name ('?' for help | 'q' to quit)>ixp1
Enter Destination IP Address ('?' for help | 'q' to quit)>192.168.2.2
Enter Local Tunnel IP Address ('?' for help | 'q' to quit)>192.168.1.1
Enter Remote Tunnel IP Address ('?' for help | 'q' to quit)>192.168.4.1
Enter Tunnel TTL value 0-255 (default:0 | '?' for help | 'q' to quit)>
Using default value 0.
Activate tunnel checksum (n=no,y=yes | default: no | '?' for help | 'q' to quit)>y
Enter tunnel key ("", 0-4294967295 | default: "" | '?' for help | 'q' to quit)>1000

Tunnel configuration:
Interface       : ixp1
Destination IP  : 192.168.2.2
Local Tunnel IP : 192.168.1.1
Remote Tunnel IP : 192.168.4.1
TTL             : 0
Checksum        : enabled
Tunnel Key      : 1000

Do you want to add the tunnel?(y/n)>y

Tunnel 1 added.

Press Enter to return to Tunnel Configuration

```

Figure 13. Add a GRE Tunnel

11. Press 'Enter' to return to the GRE Tunnel Configuration Menu.

2.6.2 Edit a GRE Tunnel

1. Enter '3' on the GRE Configuration Menu to edit a GRE Tunnel.

2. As shown in Figure 14, the currently configured GRE Tunnels will be listed. Enter the number of Tunnel you would like to edit.
3. KlasRouter will now step you through each of the configured parameters. The current value for that Tunnel will be shown. You can either press 'Enter' to accept the current value or enter a new value to edit the Tunnel's parameters.
4. After all of the parameters have either been edited or changed, KlasRouter will again list the configured parameters. You will then be prompted to accept or reject the new parameters. Enter 'y' to accept them or 'n' to reject them.

```

Edit Tunnel
-----
#  IF      Destination IP   Local Tunnel IP   Remote Tunnel IP   Status   TTL   CSum   Key
-----
1  ixp1    192.168.2.2        192.168.1.1      192.168.4.1      active   0     no     1000

Enter Tunnel Number 0-9 ('q' to quit)>1

Interface Name: ixp1
Enter New Interface Name ('?' for help | 'q' to quit)>
...

New tunnel configuration:
Interface       : ixp1
Destination IP  : 192.168.2.2
Local Tunnel IP : 192.168.1.1
Remote Tunnel IP : 192.168.4.1
TTL             : 0
Checksum       : enabled
Tunnel Key     : 1000

Do you want to activate the tunnel changes?(y/n)>y
Attention! Check that existing routes for this tunnel are still correct!

Tunnel 1 changed.

Press Enter to return to Tunnel Configuration

```

Figure 14. Edit a GRE Tunnel

5. Press 'Enter' to return to the GRE Tunnel Configuration Menu.

2.6.3 Delete a GRE Tunnel

1. Enter '4' on the GRE Configuration Menu to delete a GRE Tunnel.
2. As shown in Figure 15, the currently configured GRE Tunnels will be listed. Enter the number of Tunnel you would like to delete.

```

Delete Tunnel
-----
#  IF      Destination IP   Local Tunnel IP   Remote Tunnel IP   Status
-----
1  i xp1    192.168.2.2         192.168.1.1       192.168.4.1       active
      TTL  CSum  Key
      0    yes  1000

Enter Tunnel Number 0-9 ('q' to quit)>1
Tunnel 1 deleted.
Press Enter to return to Tunnel Configuration

```

Figure 15. Delete a GRE Tunnel

3. Press 'Enter' to return to the GRE Tunnel Configuration Menu.

MORE INFORMATION

For more information about KlasRouter and other Klas products, visit the following Klas website:

<www.klasonline.com>

Copyright © 2005 Klas Ltd. All rights reserved. All company and brand names are trademarks or registered trademarks of their respective owners.

DISCLAIMER OF WARRANTY: THE DOCUMENT IS PROVIDED AS IS, WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WITH RESPECT TO THE DOCUMENT AND / OR ANY ASSOCIATED ON-LINE INFORMATION, KLAS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDED BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.