NAME

if_ipsec - IPsec virtual tunneling interface

SYNOPSIS

The **if_ipsec** network interface is a part of the FreeBSD IPsec implementation. To compile it into the kernel, place this line in the kernel configuration file:

options IPSEC

It can also be loaded as part of the **ipsec** kernel module if the kernel was compiled with

options IPSEC_SUPPORT

DESCRIPTION

The **if_ipsec** network interface is targeted for creating route-based VPNs. It can tunnel IPv4 and IPv6 traffic over either IPv4 or IPv6 and secure it with ESP.

if_ipsec interfaces are dynamically created and destroyed with the ifconfig(8) **create** and **destroy** subcommands. The administrator must configure IPsec **tunnel** endpoint addresses. These addresses will be used for the outer IP header of ESP packets. The administrator can also configure the protocol and addresses for the inner IP header with ifconfig(8), and modify the routing table to route the packets through the **if_ipsec** interface.

When the **if_ipsec** interface is configured, it automatically creates special security policies. These policies can be used to acquire security associations from the IKE daemon, which are needed for establishing an IPsec tunnel. It is also possible to create needed security associations manually with the setkey(8) utility.

Each **if_ipsec** interface has an additional numeric configuration option **reqid** *id*. This *id* is used to distinguish traffic and security policies between several **if_ipsec** interfaces. The **reqid** can be specified on interface creation and changed later. If not specified, it is automatically assigned. Note that changing **reqid** will lead to generation of new security policies, and this may require creating new security associations.

EXAMPLES

The example below shows manual configuration of an IPsec tunnel between two FreeBSD hosts. Host A has the IP address 192.168.0.3, and host B has the IP address 192.168.0.5.

On host A:

```
ifconfig ipsec0 create reqid 100
ifconfig ipsec0 inet tunnel 192.168.0.3 192.168.0.5
ifconfig ipsec0 inet 172.16.0.3/16 172.16.0.5
setkey -c
add 192.168.0.3 192.168.0.5 esp 10000 -m tunnel -u 100 -E rijndael-cbc "VerySecureKey!!1";
add 192.168.0.5 192.168.0.3 esp 10001 -m tunnel -u 100 -E rijndael-cbc "VerySecureKey!!2";
^D
```

On host B:

```
ifconfig ipsec0 create reqid 200
ifconfig ipsec0 inet tunnel 192.168.0.5 192.168.0.3
ifconfig ipsec0 inet 172.16.0.5/16 172.16.0.3
setkey -c
add 192.168.0.3 192.168.0.5 esp 10000 -m tunnel -u 200 -E rijndael-cbc "VerySecureKey!!1";
add 192.168.0.5 192.168.0.3 esp 10001 -m tunnel -u 200 -E rijndael-cbc "VerySecureKey!!2";
^D
```

Note the value 100 on host A and value 200 on host B are used as reqid. The same value must be used as identifier of the policy entry in the setkey(8) command.

SEE ALSO

gif(4), gre(4), ipsec(4), ifconfig(8), setkey(8)

AUTHORS

Andrey V. Elsukov <*ae@FreeBSD.org*>