

## Frequently Asked Questions

### Question

DI-804HV IPSec B C = = 5 ; L @ C B 5 @ - @ C B 5 @ 8 FreeBSD

### Answer

```
564C A0<8<8 @CB5@0<8 BC==5;L >?8AK205BAO ?@>AB>,  
A;54CO A;54CNI8<:0@B8=:0<2?>@O4:5>G5@54=>AB8.  
0AB@>9:8<5=ONBAO2A>>B25BAB288A;>:0;L=K<8A5BO<88  
2=5H=8<8?C40;5==>9B>G:8. 0>4=><4;8=:5AB028BAO  
30;;003@5AA88(8=8F80B>@A>548=5=8O),=04@C3><=5B.
```

A5. 'B>:0A05BAO @01>BK AFreeBSD, =5>4E>48<>2rc.conf 4>1028BL:

s

```
tatic_routes="Pvpn"  
route_Pvpn="192.168.6.0/24 192.168.4.1" # C B L :  
C 4 0 ; 5 = = > 9 A 5 B 8 G 5 @ 5 7 ; > : 0 ; L = K 9 8 ?  
D @ 5 2 > 3 > @ C B 5 @ 0
```

```
ipsec_enable="YES"  
ipsec_file="/etc/ipsec.conf"  
racoon_enable="YES"
```

\$09;/etc/ipsec.conf A>45@68B2A5152>BMB>:

```
# more /etc/ipsec.conf  
flush;  
spdf flush;  
spdadd 192.168.4.0/24 192.168.6.0/24 any -P out ipsec  
esp/tunnel/91.123.123.116-80.80.123.111/require;  
spdadd 192.168.6.0/24 192.168.4.0/24 any -P in ipsec  
esp/tunnel/80.80.123.111-91.123.123.116/require;
```

345?5@20Ospdadd A>45@68B2A515;>:0;L=0O?>4A5BL-

C 4 0 ; 5 = = 0 0 ; > : 0 ; L = 0 0 ? > 4 A 5 B L 2 = 5 H = 8 9 8 ? - C 4 0 ; 5 = = K 9  
2 = 5 H = 8 9 8 ? , 2 B > @ 0 0 - = 0 > 1 > @ > B . - B > > ? 8 A 0 = 8 5 G B > < 5 6 4 C  
G 5 < H 8 D @ > 2 0 B L 8 2 : 0 : > < = 0 ? @ 0 2 ; 5 = 8 8 .

; O B > 3 > G B > 1 K 8 ? A 5 : 7 0 @ 0 1 > B 0 ; ? @ 8 4 5 B A O  
> B : > < ? 8 ; 8 @ > 2 0 B L O 4 @ > , 4 > 1 0 2 8 2 2 > B B 0 : 8 5 ? 0 @ 0 < 5 B @ K :

```
> 4:
options          IPSEC
options          IPSEC_ESP
options          IPSEC_DEBUG
```

```
device          crypto
```

0 G B > 1 K 7 0 ? C A B 8 B L A 0 < B C = = 5 ; L , ? @ 8 = O B L C 4 0 ; 5 = = K 5  
7 0 ? @ > A K 8 8 = 8 F 8 8 @ > 2 0 B L A 0 < > < C , A B 0 2 8 B A O 8 7 ? > @ B > 2  
security/ipsec-tools ( B > B A 0 < K 9 racoon ), 2 : 0 B 0 ; > 3 5 /usr/local/etc/racoon A > 7 4 0 B L D 0 9 ;  
psk.txt D > @ @ < 0 B 0

123.123.123.123 ? 0 @ > ; L

4 0 B L 5 < C ? @ 0 2 0 6 0 0 root:wheel, 7 0 B 5 < = 0 @ 8 A > 2 0 B L D 0 9 ; racoon.conf  
? @ 8 < 5 @ = > 2 > B B 0 ::

```
path pre_shared_key "/usr/local/etc/racoon/psk.txt" ;
path backupsa "/usr/local/etc/racoon/back.tmp" ;                                     #
  5 A ; 8 M B > 3 > D 0 9 ; 0 = 5 B 5 3 > B > 6 5 ? @ 8 4 5 B A O
  A > 7 4 0 B L
#path certificate "/usr/local/etc/cert" ;
```

```
padding
{
    maximum_length 20;          # maximum padding length.
    randomize off;              # enable randomize length.
    strict_check off;           # enable strict check.
    exclusive_tail off;         # extract last one octet.
}
```

```
listen
{
    #isakmp :::1 [7000];
    isakmp 91.123.123.116 [500];
    #admin [7002];              # administrative's port by kmpstat.
    #strict_address;            # required all addresses must be bound.
```

```
}

timer
{
    # These value can be changed per remote node.
    counter 5;                # maximum trying count to send.
    interval 20 sec;          # maximum interval to resend.
    persend 1;                # the number of packets per a send.
    # timer for waiting to complete each phase.
    phasel 30 sec;
    phase2 15 sec;
}

remote 80.80.123.111
{
    #   exchange_mode main,aggressive;
    exchange_mode aggressive,main;
    doi ipsec_doi;
    situation identity_only;
#   my_identifier address 123.123.123.123;
#   peers_identifier address 195.131.123.123;
#   my_identifier user_fqdn "user@domain.ru";
#   peers_identifier user_fqdn "user@domain.ru";
#certificate_type x509 "mycert" "mypriv";
nonce_size 16;
lifetime time 3600 sec;      # sec,min,hour
initial_contact on;
support_mip6 on;
proposal_check obey;        # obey, strict or claim
proposal
    {
        encryption_algorithm 3des;
        hash_algorithm sha1;
        authentication_method pre_shared_key ;
        dh_group 2 ;
    }
}

sainfo anonymous
{
    pfs_group 2;
    lifetime time 3600 sec;
    encryption_algorithm 3des ;
    authentication_algorithm hmac_sha1;
#   authentication_algorithm non_auth;
    compression_algorithm deflate ;
}
```

1 @ 0 B 8 B 5 2 = 8 < 0 = 8 5 = 0 B > G B > ? 0 @ 0 < 5 B @ K 2 : > = D 8 3 5 8 C  
4 ; 8 = : 0 dh\_group encryption\_algorithm authentication\_algorithm(hash\_algorithm) 4 > ; 6 = K A > 2 ? 0 4 0 B L.  
0 ? C A : 0 5 B 5 8 ? A 5 ; , 7 0 ? C A : 0 5 B 5 @ 0 : > = , A < > B @ 8 B 5 G B >  
? > ; C G 8 B A O . 5 8 I 8 B 5 8 = B 5 @ D 5 9 A > 2 8 ; 8 : 0 : 8 E - ; 8 1 > 4 @ C 3 8 E  
" 2 = 5 H = 8 E " ? @ > O 2 ; 5 = 8 9 B C = = 5 ; O . > C B 8 = 3 A ? 5 F 8 0 ; L = >  
A B 0 2 8 B A O = 0 ; > : 0 ; L = K 9 8 ? @ C B 5 @ 0 , = 8 : 0 : 8 E 8 = B 5 @ D 5 9 A > 2 = 5  
A > 7 4 0 5 B A O , > ? > @ = K < A B 0 = > 2 8 B A O ; > : 0 ; L = K 9 8 ? 0 4 @ 5 A.

---

## Details

Info Sunday 14 March 2010 - 17:13:00 by

---

Vampyr`s House!