

Frequently Asked Questions

Question

IPSec B C = = 5 ; L FreeBSD - FreeBSD 1 5 7 racoon

Answer

@ 8 3 8 = 0 ;: [Konstantin Nikonenko](#)

```
! : @ 8 ? B, 4 ; O ? > 4 = O B 8 O : @ 8 ? B > 2 0 = > 3 > B C = = 5 ; O G 5 @ 5 7
8 = B 5 @ = 5 B < 5 6 4 C 4 2 C < O
A 5 @ 2 5 @ 0 < 8. racoon = 5 8 A ? > ; L 7 C 5 B A O - A B 0 B 8 G 5 A : 8 5 ; ; N G 8. gif
= 0 < 4 5 ; 0 5 B
B C = = 5 ; L. IPsec : @ 8 ? B C 5 B ? @ > E > 4 O I 8 5 ? 0 : 5 B 8 : 8. setkey -D
? > : 0 7 K 2 0 5 B
H 8 D @ C 5 < 2 > > 1 I 5 8 ; 8 = 5 B - 7 4 > @ > 2 > ? > < > 3 0 5 B ? @ 8
> B ; 0 4 : 5. ipsec_gif.sh C
< 5 = O B 0 : 8 6 8 2 Q B 2 /usr/local/etc/rc.d

3 @ > < = > 5 A ? 0 A 8 1 > drook from IRC Rusnet channel #freebsd, : > B > @ K 9
? > ? @ 0 2 8 ; < 5 = O, C : 0 7 0 2, G B > ? @ 8 8 A ? > ; L 7 > 2 0 = 8 8 gif
? > ; C G 0 5 B A O B C = = 5 ; L 2
B C = = 5 ; 5 8 G B > < > 6 = > > 1 > 9 B 8 A L 1 5 7 = 5 3 >. B 0 : > < A ; C G 0 5
> 1 E > 4 O B A O 3 ; N : 8
NAT. traceroute A < > B @ 5 B L 8 7 - ? > 4 A 5 @ > 9 A 5 B 8.
```

ipsec_gif.sh

```
#!/bin/sh
```

```
#
```

```
INTERNAL_IP_SRC=192.168.2.1
```

```
INTERNAL_IP_DST=192.168.1.1
```

```
INTERNAL_IP_MASK=255.255.255.0
```

```
EXTERNAL_IP_SRC=X.X.X.X
```

```
EXTERNAL_IP_DST=Y.Y.Y.Y
```

```
# on remote side change SRC to DST
```

```
ARG_SRC=0x10004
```

```
ARG_DST=0x10003
```

```
# ----- #
```

```
ifconfig gif0 destroy
```

```
ifconfig gif0 create
```

```
gifconfig gif0 "&#036;EXTERNAL_IP_SRC" "&#036;EXTERNAL_IP_DST"
ifconfig gif0 inet "&#036;INTERNAL_IP_SRC" "&#036;INTERNAL_IP_DST" netmask "&#036;INTERNAL_IP_MASK"
```

```
setkey -F
setkey -PF
```

```
setkey -c
spdadd &#036;INTERNAL_IP_SRC/24 &#036;INTERNAL_IP_DST/24 any -P out ipsec
    esp/tunnel/&#036;{ EXTERNAL_IP_SRC }-&#036;{ EXTERNAL_IP_DST }/require;
```

```
spdadd &#036;INTERNAL_IP_DST/24 &#036;INTERNAL_IP_SRC/24 any -P in ipsec
    esp/tunnel/&#036;{ EXTERNAL_IP_DST }-&#036;{ EXTERNAL_IP_SRC }/require;
```

```
add &#036;EXTERNAL_IP_SRC &#036;EXTERNAL_IP_DST esp &#036;{ ARG_SRC } -m any
    -E 3des-cbc "XXXXXXXXXXXXXXXXXXXXXXXXXXXX";
```

```
add &#036;EXTERNAL_IP_DST &#036;EXTERNAL_IP_SRC esp &#036;{ ARG_DST } -m any
    -E 3des-cbc "XXXXXXXXXXXXXXXXXXXXXXXXXXXX";
```

EOF

```
/sbin/route add 192.168.1.0/24 192.168.1.1
```

ipsec.sh

```
#!/bin/sh
#
# Office, for another end point change only in <-> out
#
# Great thank's to drook on RusNet IRC, channel #freebsd
#
```

```
EXT1_IF=2.3.1.126
EXT2_IF=5.4.1.10
INT1_NET="192.168.1.0/24"
INT2_NET="192.168.2.0/24"
setkey -c <<-EOF
spdadd $EXT1_IF $INT2_NET any -P in ipsec
    esp/tunnel/$EXT1_IF-$EXT2_IF/require
    ah/transport/$EXT1_IF-$EXT2_IF/require;
spdadd $INT2_NET $EXT1_IF any -P out ipsec
    esp/tunnel/$EXT2_IF-$EXT1_IF/require
    ah/transport/$EXT2_IF-$EXT1_IF/require;
spdadd $EXT2_IF $INT1_NET any -P out ipsec
    esp/tunnel/$EXT2_IF-$EXT1_IF/require
```

```
ah/transport/$EXT2_IF-$EXT1_IF/require;
spdadd $INT1_NET $EXT2_IF any -P in ipsec
esp/tunnel/$EXT1_IF-$EXT2_IF/require
ah/transport/$EXT1_IF-$EXT2_IF/require;

#
# policies again
spdadd $INT2_NET $INT1_NET any -P out ipsec
esp/tunnel/$EXT2_IF-$EXT1_IF/require
ah/transport/$EXT2_IF-$EXT1_IF/require;
spdadd $INT1_NET $INT2_NET any -P in ipsec
esp/tunnel/$EXT1_IF-$EXT2_IF/require
ah/transport/$EXT1_IF-$EXT2_IF/require;

#
# sas again
add $EXT1_IF $EXT2_IF esp 0x10009 -m tunnel -E 3des-cbc
"XXXXXXXXXXXXXXXXXXXXXXXXXXXX" -A hmac-md5 "ZZZZZZZZZZZZZZZZZZ";
add $EXT1_IF $EXT2_IF ah 0x10010 -m transport -A keyed-md5
"YYYYYYYYYYYYYYYYYYYY";
add $EXT2_IF $EXT1_IF esp 0x10011 -m tunnel -E 3des-cbc
"WWWWWWWWWWWWWWWWWWWWWWWWWW" -A hmac-md5 "OOOOOOOOOOOOOOOOOO";
add $EXT2_IF $EXT1_IF ah 0x10012 -m transport -A keyed-md5
"BBBBBBBBBBBBBBBBBBBB";
EOF
```

Details

Info Sunday 14 March 2010 - 17:01:23 by
