

Problem with IPSec tunnel, using IPv6 addresses, between Two FreeBSD systems.....

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2005-06/2916.html>

From: mohan chandra (*mohanchandra_01_at_yahoo.co.in*)

Date: 06/30/05

Date: Thu, 30 Jun 2005 08:17:06 +0100 (BST)

To: freebsd-questions@freebsd.org

Hi All,

I need to establish an IPSec tunnel between two FreeBSD systems using IPv6 addresses. The connection is host-to-host between two FreeBSD (RELEASE 4.11) systems with KAME IPSec implementation.

```
      |----->|
host1-[mohan] | host2-[ram]
      |<-----|
```

host1 IPv6 address : fe80::2b0:d0ff:fe6f:dfa0

host2 IPv6 address : fe80::2b0:d0ff:fe48:7ce7

The 'ipsec.conf' file at Host1 and Host2 are attached along with this email. (you can refer them)

IPsec is started with the following commands at both systems:

```
*****at Host1*****
```

```
mohan# /usr/local/etc/rc.d/setkey.sh start
```

```
Starting VPN tunnel encryption..Ok
```

```
mohan#
```

```
*****
```

```
*****at Host2*****
```

```
ram# /usr/local/etc/rc.d/setkey.sh start
```

```
Starting VPN tunnel encryption..Ok
```

```
ram#
```

```
*****
```

(File setkey.sh is also attached with the email below for ur reference)

After that I executed 'ping6' and 'tcpdump' commands to test the connection (on my system i.e., host1-mohan),

freebsd-questions: Problem with IPSec tunnel, using IPv6 addresses, between Two FreeBSD systems.....

but, it seems is not working properly...

```
##### ping6 command output at host1 #####
mohan# ping6 -I x10 fe80::2b0:d0ff:fe48:7ce7
PING6(56=40+8+8 bytes) fe80::2b0:d0ff:fe6f:dfa0%x10
--> fe80::2b0:d0ff:fe48:7ce7
^C
--- fe80::2b0:d0ff:fe48:7ce7 ping6 statistics ---
6 packets transmitted, 0 packets received, 100% packet
loss
mohan#
#####
```

But, with tcpdump command it seems like packets are moving from host1 to host2 without ESP(encryption) and reply packets from host2 to host1 with ESP(encryption) header. It is shown in the following output:

```
##### tcpdump at host1 #####

mohan# tcpdump -i x10 host fe80::2b0:d0ff:fe6f:dfa0
tcpdump: listening on x10

10:08:43.844723 fe80::2b0:d0ff:fe6f:dfa0[host1] >
ff02::1:ff48:7ce7[host2]: icmp6: neighbor sol: who has
fe80::2b0:d0ff:fe48:7ce7

10:08:43.845127 fe80::2b0:d0ff:fe48:7ce7 >
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0xf)

10:08:44.844736 fe80::2b0:d0ff:fe6f:dfa0 >
ff02::1:ff48:7ce7: icmp6: neighbor sol: who has
fe80::2b0:d0ff:fe48:7ce7

10:08:44.845109 fe80::2b0:d0ff:fe48:7ce7 >
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0x10)

10:08:48.844804 fe80::2b0:d0ff:fe6f:dfa0 >
ff02::1:ff48:7ce7: icmp6: neighbor sol: who has
fe80::2b0:d0ff:fe48:7ce7

10:08:48.845150 fe80::2b0:d0ff:fe48:7ce7 >
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0x13)

10:08:49.085694 fe80::2b0:d0ff:fe48:7ce7 >
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0x14)

10:08:49.844840 fe80::2b0:d0ff:fe6f:dfa0 >
ff02::1:ff48:7ce7: icmp6: neighbor sol: who has
fe80::2b0:d0ff:fe48:7ce7
```

freebsd-questions: Problem with IPsec tunnel, using IPv6 addresses, between Two FreeBSD systems.....

```
10:08:49.845232 fe80::2b0:d0ff:fe48:7ce7 >  
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0x15)
```

```
10:08:50.085696 fe80::2b0:d0ff:fe48:7ce7 >  
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0x16)
```

```
10:08:51.085741 fe80::2b0:d0ff:fe48:7ce7 >  
fe80::2b0:d0ff:fe6f:dfa0: ESP(spi=0x0000fead,seq=0x17)
```

```
#####
```

Please, reply me what is the problem with the connection setup. Inform me if there are any mistakes with the ipsec.conf file, policy setup..? Reply as soon as possible..

The connection works with IPv4 addresses without any problems. If you need any detail regarding the setup, I will send you the details..

Please, give me proper suggestions..any help will be greatly appreciated ..

Thanx,

with Regards
Mohan.

```
#####The 'ipsec.conf' file at Host2 #####
```

```
# flush configs  
flush ;  
spdflush ;  
  
# add a SAD entry  
add fe80::2b0:d0ff:fe48:7ce7  
fe80::2b0:d0ff:fe6f:dfa0 esp 0xFEAD -m transport -E  
3des-cbc  
"ip6readylogo3descbcout1" -A hmac-sha1  
"ip6readylogsha1out1";  
add fe80::2b0:d0ff:fe6f:dfa0  
fe80::2b0:d0ff:fe48:7ce7 esp 0xFEED -m transport -E  
3des-cbc  
"ip6readylogo3descbcin01" -A hmac-sha1  
"ip6readylogsha1in01";  
  
# and specify what has to be encrypted  
spdadd fe80::2b0:d0ff:fe48:7ce7  
fe80::2b0:d0ff:fe6f:dfa0 any -P out ipsec
```

freebsd-questions: Problem with IPsec tunnel, using IPv6 addresses, between Two FreeBSD systems.....

```
esp/transport/fe80::2b0:d0ff:fe48:7ce7-fe80::2b0:d0ff:fe6f:dfa0/require  
;
```

```
spdadd fe80::2b0:d0ff:fe6f:dfa0  
fe80::2b0:d0ff:fe48:7ce7 any -P in ipsec
```

```
esp/transport/fe80::2b0:d0ff:fe6f:dfa0-fe80::2b0:d0ff:fe48:7ce7/require  
;
```

```
#####The 'ipsec.conf' file at Host2 #####
```

```
# flush configs
```

```
flush ;
```

```
spdflush ;
```

```
# add a SAD entry
```

```
add fe80::2b0:d0ff:fe48:7ce7
```

```
fe80::2b0:d0ff:fe6f:dfa0 esp 0xFEAD -m transport -E
```

```
3des-cbc
```

```
"ipv6readylogo3descbcout1" -A hmac-sha1
```

```
"ipv6readylogsha1out1";
```

```
add fe80::2b0:d0ff:fe6f:dfa0
```

```
fe80::2b0:d0ff:fe48:7ce7 esp 0xFEED -m transport -E
```

```
3des-cbc
```

```
"ipv6readylogo3descbcin01" -A hmac-sha1
```

```
"ipv6readylogsha1in01";
```

```
# and specify what has to be encrypted
```

```
spdadd fe80::2b0:d0ff:fe48:7ce7
```

```
fe80::2b0:d0ff:fe6f:dfa0 any -P out ipsec
```

```
esp/transport/fe80::2b0:d0ff:fe48:7ce7-fe80::2b0:d0ff:fe6f:dfa0/require  
;
```

```
spdadd fe80::2b0:d0ff:fe6f:dfa0
```

```
fe80::2b0:d0ff:fe48:7ce7 any -P in ipsec
```

```
esp/transport/fe80::2b0:d0ff:fe6f:dfa0-fe80::2b0:d0ff:fe48:7ce7/require  
;
```

How much free photo storage do you get? Store your friends 'n family snaps for FREE with Yahoo! Photos
<http://in.photos.yahoo.com>

```
#####The 'ipsec.conf' file at Host2 #####
```

freebsd-questions: Problem with IPSec tunnel, using IPv6 addresses, between Two FreeBSD systems.....

```
# flush configs
flush ;
spdflush ;

# add a SAD entry
add fe80::2b0:d0ff:fe48:7ce7 fe80::2b0:d0ff:fe6f:dfa0 esp 0xFEAD -m transport -E 3des-cbc
"ipv6readylogo3descbcout1" -A hmac-sha1 "ipv6readylogsha1out1";
add fe80::2b0:d0ff:fe6f:dfa0 fe80::2b0:d0ff:fe48:7ce7 esp 0xFEED -m transport -E 3des-cbc
"ipv6readylogo3descbcin01" -A hmac-sha1 "ipv6readylogsha1in01";

# and specify what has to be encrypted
spdadd fe80::2b0:d0ff:fe48:7ce7 fe80::2b0:d0ff:fe6f:dfa0 any -P out ipsec
esp/transport/fe80::2b0:d0ff:fe48:7ce7-fe80::2b0:d0ff:fe6f:dfa0/require ;

spdadd fe80::2b0:d0ff:fe6f:dfa0 fe80::2b0:d0ff:fe48:7ce7 any -P in ipsec
esp/transport/fe80::2b0:d0ff:fe6f:dfa0-fe80::2b0:d0ff:fe48:7ce7/require ;
```

#####The 'ipsec.conf' file at Host2 #####

```
# flush configs
flush ;
spdflush ;

# add a SAD entry
add fe80::2b0:d0ff:fe48:7ce7 fe80::2b0:d0ff:fe6f:dfa0 esp 0xFEAD -m transport -E 3des-cbc
"ipv6readylogo3descbcout1" -A hmac-sha1 "ipv6readylogsha1out1";
add fe80::2b0:d0ff:fe6f:dfa0 fe80::2b0:d0ff:fe48:7ce7 esp 0xFEED -m transport -E 3des-cbc
"ipv6readylogo3descbcin01" -A hmac-sha1 "ipv6readylogsha1in01";

# and specify what has to be encrypted
spdadd fe80::2b0:d0ff:fe48:7ce7 fe80::2b0:d0ff:fe6f:dfa0 any -P out ipsec
esp/transport/fe80::2b0:d0ff:fe48:7ce7-fe80::2b0:d0ff:fe6f:dfa0/require ;

spdadd fe80::2b0:d0ff:fe6f:dfa0 fe80::2b0:d0ff:fe48:7ce7 any -P in ipsec
esp/transport/fe80::2b0:d0ff:fe6f:dfa0-fe80::2b0:d0ff:fe48:7ce7/require ;
```

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"

freebsd-questions@freebsd.org mailing list

freebsd-questions: Problem with IPSec tunnel, using IPv6 addresses, between Two FreeBSD systems.....

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@freebsd.org"