DUMP

|

N1 SGW1 | N2

[192.168.0.3] -------[192.168.0.2][10.0.0.1]--------[10.0.0.2]

default route for 192.168.0.3 is 192.168.0.2

default route for 10.0.0.2 is 10.0.0.1

We define the following policies with the setkey syntax :

<SA1>

########## For 192.168.0.2 (SGW1)

spdadd 192.168.0.3 10.0.0.2 any -P out ipsec

esp/tunnel/10.0.0.1-10.0.0.2/use;

add 10.0.0.1 10.0.0.2 esp 10

-m tunnel

-E aes-cbc "aescbcencryption"

-A hmac-sha1 "hmacsha1authenticati";

<SA2>

########## For 192.168.0.3 (N1)

spdadd 192.168.0.3 10.0.0.2 any -P out ipsec esp/transport//require;

add 192.168.0.3 10.0.0.2 esp 15

-E des-cbc "descbte"

-A hmac-sha1 "hmacsha1authenticati";

It means that packets coming from N1 to N2 will be encrypted with des-cbc and tunneled from SGW1 with ESP encryption aes-cbc to N2. If we have a look at the DUMP host, we have only two SAs to decrypt the entire packet. If we have a look at the different Layers it will be :

[IP1][ESP1][ENCRYPTION1]

with [ENCRYPTION1]=[IP2][ESP2][ENCRYPTION2]

and [ENCRYPTION2]=ICMP

IP1 is IP header from SGW1 to N2

ENCRYPTION2 is aes-cbc

IP2 is IP header from N1 to N2

ENCRYPTION2 is des-cbc



