# FSx NFS IPSec Encryption with Libreswan on Linux client

#### Server Side - FSx for Netapp ONTAP Sample command:

::> security ipsec policy create -vserver ontap -name policy1 -local-ip-subnets 198.19.254.123/20 -remote-ip-subnets 172.31.19.109/20 -remote-ports 0 -ipsec-lifetime 86400 -ike-lifetime 604800

-local-ip-subnets >>>> IP address of NFS Share of the ontap fs.  
-remote-ip-subnets >>>> IP address of the NFS Client.  
  
Note that when using Libreswan, use of -local-identiy (represent FSxN) and -remote identity(client side) is also required.  
  
You can get subnet Information of ec2 instance using the command  
$ ip a s  
and for FSxN you can run  
::> network interface show  
  
Once you press enter it will ask you for a passphrase 18-30 digits in length as this method is pre shared secret (PSK). You can generate a random 20 digit code and use it as a passphrase on any linux machine.  
  
$ head -c 20 /dev/random |base64  
  
Enter the passphrase and IPsec policy would be created on ontap side. You can check the same on ontap cli using the command,

::> security ipsec policy show

::> security ipsec config modify -is-enabled true

Netapp mentions if you will be using more than one client then you need to use wildcard 0.0.0.0/0 on -remote-ip-subnets,  
and you must configure a specific local or remote port number to use. For example, NFS port 2049.  
  
<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/How_to_configure_multiple_clients_for_IPsec_for_ONTAP_9.8_and_higher>  
  
e.g.,

:> security ipsec policy create -vserver fsx -name tunnel\_1 -local-ip-subnets 198.19.255.202/32 -remote-ip-subnets 0.0.0.0/0 -local-identity @fsxn -remote-identity @dev -local-ports 2049 -ike-lifetime 604800 -ipsec-lifetime 86400

**Client-side configuration based on RHEL using Libreswan utility**

1. Install Libreswan on the Linux client (in this case it was RedHat)

sudo yum install libreswan

1. Add below parms to /etc/sysctl.conf

net.ipv4.ip\_forward=1  
net.ipv4.conf.all.accept\_redirects = 0  
net.ipv4.conf.all.secure\_redirects = 0  
net.ipv4.conf.all.send\_redirects = 0  
net.ipv4.conf.default.accept\_redirects = 0  
net.ipv4.conf.default.send\_redirects = 0  
net.ipv4.conf.lo.accept\_redirects = 0  
net.ipv4.conf.lo.send\_redirects = 0  
net.ipv4.conf.all.rp\_filter = 0  
net.ipv4.conf.default.rp\_filter = 0  
net.ipv4.conf.eth0.rp\_filter = 0

sysctl –system

1. Create a secrets file to store PSK (same as used when created ipsec policy in FSx for NetApp ONTAP), example below:

sudo nano /etc/ipsec.d/nfs.secrets  
  
%any : PSK 'edqtVhXvzHw2c0JpsMwWDMg4trOlNhU2hpH4CHpmWP5EP7Dh0SPrBt2zVwXm5gyu'

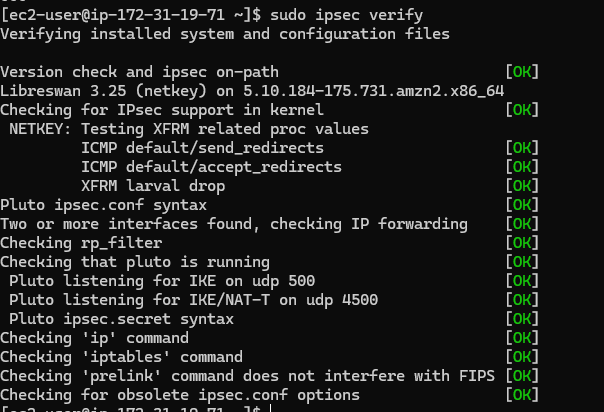
1. Create nfs.conf file, example below

sudo nano /etc/ipsec.d/nfs.conf  
  
conn fsxn  
authby=secret  
left=172.31.77.6 // client side ip address   
right=198.19.254.38 // server side IP address   
auto=start  
leftid=@dev  
rightid=@fsxn  
type=transport  
ikev2=insist  
keyexchange=ike  
ike=aes256-sha2\_384;dh20  
esp=aes\_gcm\_c256

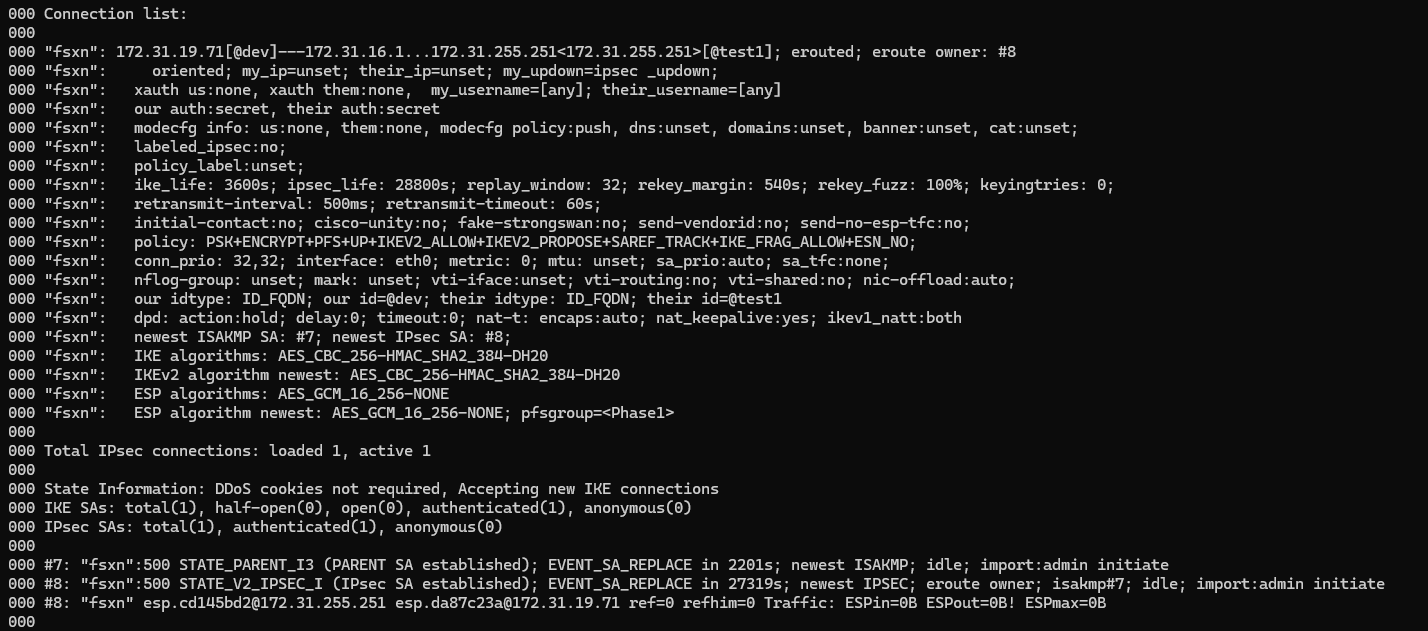
1. Run below commands to verify config and then start and check status

sudo ipsec verify  
sudo ipsec start  
sudo ipsec status

sudo ipsec verify – result



sudo ipsec status – result

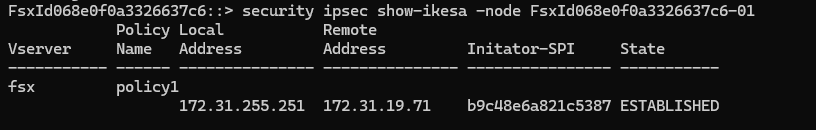


1. Now mount the fileshare on the client, example

sudo mount -t nfs svm-0214d5d9f14f2a0dc.fs-08a3a554752345f92.fsx.ca-central-1.amazonaws.com:/vol2 /fsxnvol2

1. Once mounted you can verify connection is established by running below command on FSx for NetApp ONTAP

security ipsec show-ikesa -node <fsxn node ID>



**Prerequisite –**

**End user should create a policy from FSx side, and he should provide following inputs to connector**

* 1. **PSK (pre shared key)**
  2. **Leftid and rightId ( to identify the server and client)**