**DU Simulator (DUSIM) for Standalone (SA) and Non-Standalone (NSA) Mode, CU Tester: Setup and Installation Guide**

**Prepare the Hardware Platform for KVM Host:**

Keysight’s “X100-5G” hardware platform is the validated platform that supports DU Simulator for both SA and NSA mode. Please follow below steps to prepare the KVM Host:

1. Unbox your X100-5G, then connect the Keyboard, monitor, and mouse.
2. Login into the system using user id **catapult** with password **catapult** and do the following command.
3. Isolate host CPU and Enable PCI Passthrough using below steps-

sudo vi /etc/default/grub (Edit existing line to add new parameters below)

GRUB\_CMDLINE\_LINUX\_DEFAULT="quiet splash video=vesafb:mtrr:3 isolcpus=1-21 nohz\_full=1-21 rcu\_nocbs=1-21 intel\_iommu=on iommu=pt"

sudo update-grub

1. Reboot the system
2. X100-5G has Ubuntu OS installed from factory. If you re-installed a new OS, please type in the following command:

sudo /etc/catapult/configure\_node.sh (change hostname if desired, enter number of 1G, 10G and 25G cards present on the PCI bus; the machine will reboot automatically)

**Note**: Supported NIC types are Intel Corporation 82599ES 10-Gigabit SFI/SFP*+* and 25G Mellanox Technologies MT27710 Family [ConnectX-4 Lx].

**Download VM Image Files and DUSIM SA/NSA Packages Installer:**

The next step is to download and install the required packages from the IxLoad software download portal to your X100-5G (to any directory):

List of required files for DUSIM solution where CP and UP runs inside a single VM:

1. IxVM Image (IxVM Image for IxLoad 5G (KVM))
2. DUSim VM Image (VM Image for IxLoad 5G DUSim (KVM))
3. DUSim SA Package Installer
4. DUSim NSA Package Installer
5. This document

List of required files for DUSIM solution with CP/UP split:

1. IxVM Image (IxVM Image for IxLoad 5G (KVM))
2. DUSIM CP VM Image (VM Image for IxLoad 5G DUSim CP (KVM))
3. DUSIM UP VM Image (VM Image for IxLoad 5G DUSim UP (KVM))
4. DUSim SA CP Package Installer
5. DUSim NSA UP Package Installer
6. This document

**Deploy Virtual Machines (VM) on KVM host:**

DUSIM uses two VMs when both CP and UP runs inside a single VM called DUSIM HLS-VM (High level Split-VM) and the other one is UE-VM. Follow below sections on how to deploy HLS-VM, UE-VM and EPC or 5GCore VM and later DUSIM SA Package installation instruction for HLS-VM.

DUSIM CP/UP Split Solution uses at least three VMs - UE-VM, DUSIM-CP and DUSIM-UP. The solution can scale number of UE-VM and DUSIM-UP VMs based on scaling and throughput requirement. Follow below section on how to deploy DUSIM-CP, DUSIM-UP and later DUSIM SA-CP and DUSIM SA-UP Package installation instruction.

**Deploy HLS-VM:**

Copy compressed disk image file to KVM images directory and extract ‘HLS-VM.qcow2’ image file using below steps-

sudo cp DUSim\_Virtual\_Appliance\_KVM.qcow2.tar.bz2 /var/lib/libvirt/images/

cd /var/lib/libvirt/images/

sudo su

tar xvf DUSim\_Virtual\_Appliance\_KVM.qcow2.tar.bz2

Above step will extract below 4 files -

HLS-VM.qcow2

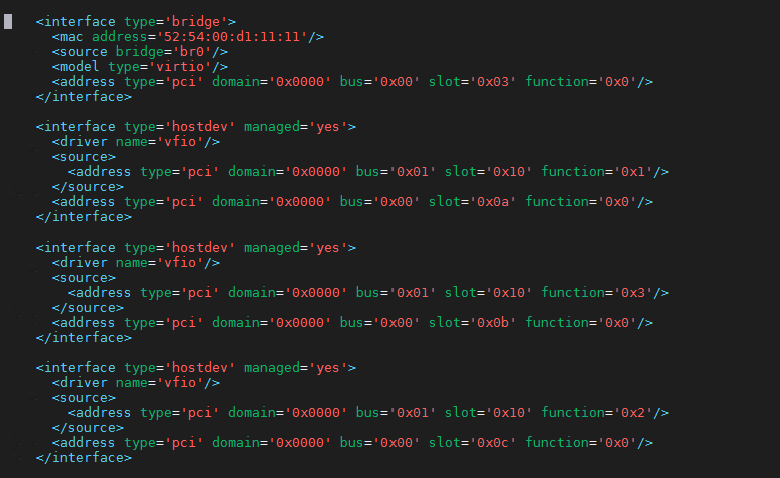
sample\_domain\_xml\_HLS-VM.xml

sample\_domain\_xml\_UE-VM.xml

sample\_domain\_xml\_CoreSim.xml

The XML domain file for HLS-VM-

A sample XML domain file ‘sample\_domain\_xml\_HLS-VM.xml’ is provided along with disk image file. The sample XML config assigns 16GB of memory, 19 CPUs and 4 network interfaces shown in picture below. Three of the network interfaces slot=0xa, slot=0xb and slot=0xc are SRIOV type interfaces. It is recommended to use SRIOV interface. The \***last three slots must have fixed slot id mapping**\* i.e. F1-C port has slot=0xa, F1-U port has slot=0xb and slot=0xc to assign to a port that goes to same switch or PF(physical function) as UE-VM (that we’ll deploy next).



UE-VM Traffic Port (slot=0xc)

F1-U Port (slot=0xb)

F1-C Port (slot=0xa)

Management

Create SRIOV VFs on X100-5G & Edit the sample XML file to update SRIOV VFs information for last 3 interfaces:

e.g. eth6 for F1-C, eth7 for F1-U and eth2 for UE-VM & HLS-VM Traffic port. To create 2 VFs on each NIC port, edit below files and write the number of VFs “2” in the file.

sudo vi /sys/class/net/eth6/device/sriov\_numvfs

sudo vi /sys/class/net/eth7/device/sriov\_numvfs

sudo vi /sys/class/net/eth2/device/sriov\_numvfs

List down PCI ID of VFs from eth6, eth7, and eth2.

sudo lspci | grep -i ethernet

Do assign a VF from eth6 to slot=0xa.

e.g. If VFs PCI-ID=[01:10.1](mailto:id@01:10.1), the XML section for this interface below.

<interface type='hostdev' managed='yes'>

<driver name='vfio'/>

<source>

<address type='pci' domain='0x0000' bus='0x01' slot='0x10' function='0x1'/>

</source>

<address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0'/>

</interface>

Same way assigns a VF from eth7 to slot=0xb & update sample XML file.

Also assign a VF from eth2 to slot=0xc and update sample XML file, the 2nd VFs from eth2 will be assigned to UE-VM.

Once the sample XML file is updated with the new interface information. We are ready to define and start the VM.

sudo virsh define sample\_domain\_xml\_HLS-VM.xml

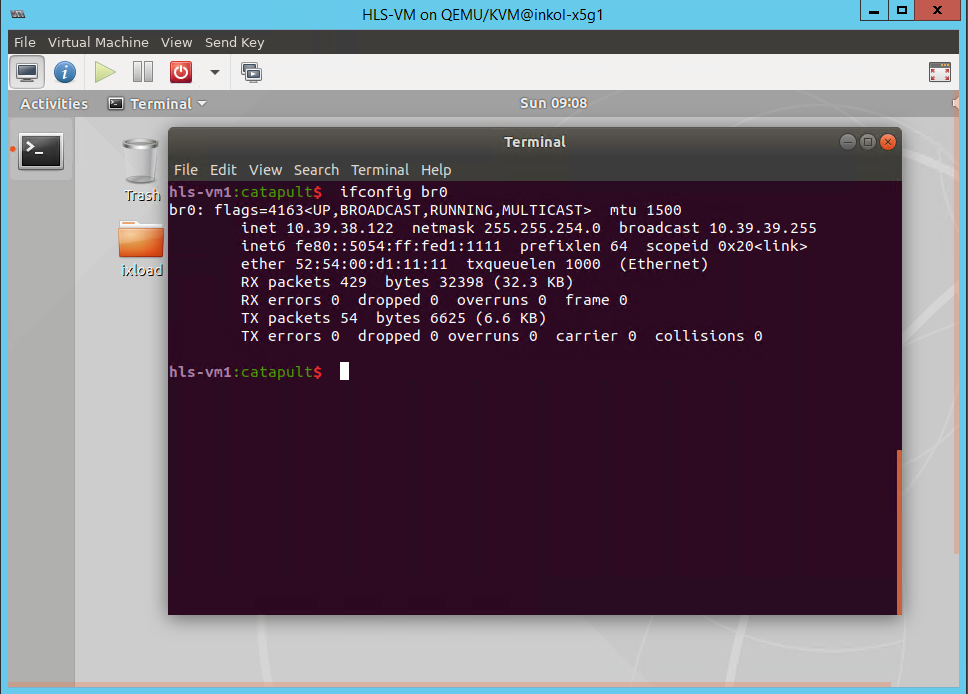
sudo virsh list --all

sudo virsh start HLS-VM

Open virt-manager tool & login to HLS-VM’s console with username **catapult**, password **catapult**

sudo virt-manager

Get IP address of br0 interface from Terminal

****

**Deploy DUSIM-CP VM:**

Copy compressed disk image file to KVM images directory and extract ‘DUSIM-CP.qcow2’ image file using below steps-

sudo cp DUSim\_CP\_Virtual\_Appliance\_KVM.qcow2.tar.bz2 /var/lib/libvirt/images/

cd /var/lib/libvirt/images/

sudo su

tar xvf DUSim\_CP\_Virtual\_Appliance\_KVM.qcow2.tar.bz2

Above step will extract below 2 files -

DUSIM-CP.qcow2

sample\_domain\_xml\_DUSIM-CP.xml

Edit the sample XML domain file ‘sample\_domain\_xml\_DUSIM-CP.xml’ to update the network interfaces associated with this VM. Edit the information between XML tag <interface> </interface>. This VM must have 2 network interfaces, first one is management interface that should be bound to a shared bridge e.g. br0 if that exist in host else macvtap type interface can be used. The other interface must have fixed target Slot address mapping to slot=0xa (F1-C interface). Source Bus, Slot & function needs to be filled up manually based on ‘lspci’ information on host system that physically connected to F1-C link towards gNB-CU.

Once the sample XML file is updated with the new interface information. We are ready to define and start the VM.

sudo virsh define sample\_domain\_xml\_DUSIM-CP.xml

sudo virsh list --all

sudo virsh start DUSIM-CP

Open virt-manager tool & login to VM’s console with username **catapult**, password **catapult**

sudo virt-manager

Get IP address of br0 interface from Terminal.

**Deploy DUSIM-UP VM:**

Copy compressed disk image file to KVM images directory and extract ‘DUSIM-CP.qcow2’ image file using below steps-

sudo cp DUSim\_UP\_Virtual\_Appliance\_KVM.qcow2.tar.bz2 /var/lib/libvirt/images/

cd /var/lib/libvirt/images/

sudo su

tar xvf DUSim\_UP\_Virtual\_Appliance\_KVM.qcow2.tar.bz2

Above step will extract below 2 files -

DUSIM-UP.qcow2

sample\_domain\_xml\_DUSIM-UP.xml

Edit the sample XML domain file ‘sample\_domain\_xml\_DUSIM-UP.xml’ to update the network interfaces associated with this VM. Edit the information between XML tag <interface> </interface>. This VM must have 3 network interfaces, first one is management interface that should be bound to a shared bridge e.g. br0 if that exist in host else macvtap type interface can be used. Last two interfaces must have fixed target Slot address mapping to slot=0xb (F1-U interface) and slot=0xc (UE traffic port). The source for address Bus, Slot, Function of slot=0xb needs to be manually filled up based on ‘lspci’ information on host system that physically connected to F1-U links towards gNB-CU.

Once the sample XML file is updated with the new interface information. We are ready to define and start the VM.

sudo virsh define sample\_domain\_xml\_DUSIM-UP.xml

sudo virsh list --all

sudo virsh start DUSIM-UP

Open virt-manager tool & login to VM’s console with username **catapult**, password **catapult**

sudo virt-manager

Get IP address of br0 interface from Terminal.

Note 1: Please login to DUSIM-UP VM and edit the /etc/dusim-service/dusim-service.conf and update the parameter “ip” field with DUSIM-CP VM’s management IP address. Run command ‘sudo systemctl restart dusim-service’ to apply the change.

Note 2: If DUSIM-CP VM is rebooted, you need to restart the DUSIM-UP VM (or dusim-service running inside the VM) to re-register it with DUSIM-CP VM.

**Deploy UE-VM:**

Copy compressed disk image file to KVM images directory

sudo cp Ixia\_Virtual\_Test\_Appliance\_9.20\_KVM.qcow2.tar.bz2 /var/lib/libvirt/images/

cd /var/lib/libvirt/images/

sudo su

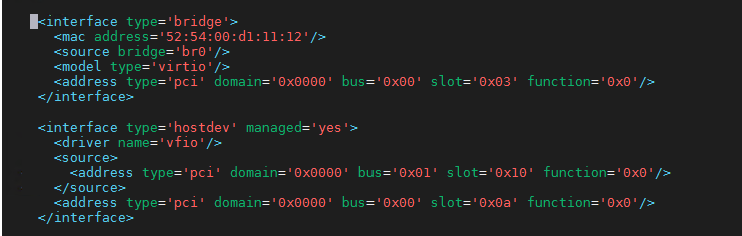
tar xvf Ixia\_Virtual\_Test\_Appliance\_9.20\_KVM.qcow2.tar.bz2

Ixia\_Virtual\_Test\_Appliance\_9.20\_KVM.qcow2

sudo cp Ixia\_Virtual\_Test\_Appliance\_9.20\_KVM.qcow2 UE-VM.qcow2

Open the sample XML domain file ‘sample\_domain\_xml\_UE-VM.xml’ extracted earlier. Edit this XML file’s 2nd interface to add SRIOV interface e.g. from above HLS-VM example eth2’s (traffic port) other VF interface should be assigned here.

e.g. If the eth2’s other VF PCI-ID=01:10:0 then the interface section of XML is as below picture.



Traffic Port (towards HLS-VM or DUSIM-UP)

Once the sample XML file is updated with the new interface information. We are ready to define and start the VM.

sudo virsh define sample\_domain\_xml\_UE-VM.xml

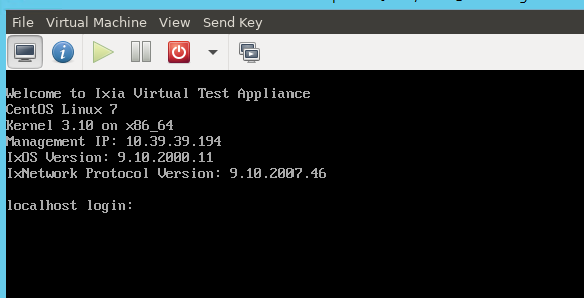
sudo virsh list --all

sudo virsh start UE-VM

Open virt-manager tool to open console

sudo virt-manager

Get the Management IP address.

****

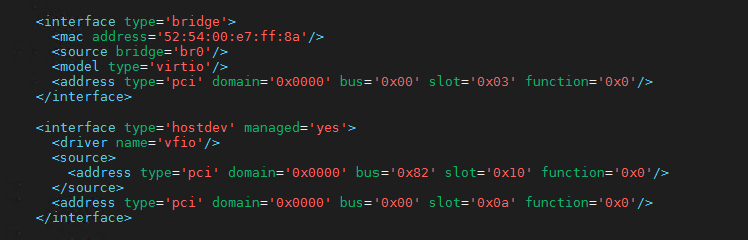
**Deploy EPC or 5G Core Simulator VM:**

**Note:** This is needed for the users who needs EPC Core or 5G Core (N1/N2/N3) needs to be simulated to test gNB-CU.

sudo cp Ixia\_Virtual\_Test\_Appliance\_9.20\_KVM.qcow2 CoreSim.qcow2

Open the sample XML domain file ‘sample\_domain\_xml\_CoreSim.xml’ extracted earlier. Edit this XML file’s 2nd interface to add SRIOV interface. It is recommended to use dedicated NIC port for this VM. So, use a different NIC than what were used for other VMs so far. The NIC can be a SRIOV VF NIC and assign the VF same way as UE-VM.

e.g. If the SRIOV VFs PCI-ID=82:10:0, then the XML’s interface section is below.



S1-C/S1-U

OR

N1/N2/N3

Once the sample XML file is updated with the new interface information. We are ready to define and start the VM.

sudo virsh define sample\_domain\_xml\_CoreSim.xml

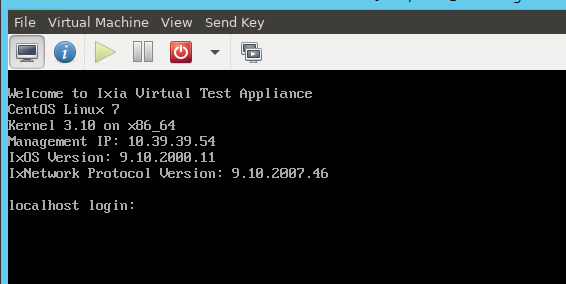
sudo virsh list --all

sudo virsh start CoreSim

Open virt-manager tool to open console

sudo virt-manager

Get the Management IP address.



**Install DUSIM SA Package for HLS-VM:**

Copy the SA Package Installer (SA\_DUSim\_\*.tgz) downloaded earlier [ item (3)] to HLS-VM’s /home/catapult/ixload/install/ directory.

scp SA\_DUSim\_\*.tgz catapult@<HLS-VM’sIP>:/home/catapult/ixload/install/ (passwd: catapult)

Do SSH to HLS-VM using same credential as above and run below commands:

cd /home/catapult/ixload/install/

tar xvf SA\_DUSim\_\*.tgz (this will extract 3 files)

chmod u+x hlssa\_\*\_Installer.sh

./hlssa\_\*\_Installer.sh

At this point when SA package is successfully installed, user is ready to configure and run test using IxLoad User Interface.

**Install DUSIM NSA Package for HLS-VM:**

NSA Package installer needs more than 10GB of free space. User need to add a second Disk in the HLS-VM. Follow below steps –

Add a seconds HDD (e.g. of size 30GB) from virt-manager.

Reboot the VM.

sudo fdisk -l (find new added hdd Disk e.g. /dev/sdb: 30 GiB)

sudo vgdisplay

sudo lvdisplay

sudo pvcreate /dev/sdb

sudo vgextend lvm-vg1 /dev/sdb

sudo lvextend -l +100%FREE /dev/lvm-vg1/root

sudo resize2fs /dev/lvm-vg1/root

df -h (check available free space now)

Copy the NSA Package Installer (NSA\_DUSim\_\*.tgz) downloaded earlier [ item (4)] to HLS-VM’s /home/catapult/ixload/install/ directory.

scp NSA\_DUSim\_\*.tgz catapult@<HLS-VM’sIP>:/home/catapult/ixload/install/ (passwd: catapult)

Do SSH to HLS-VM using same credential as above and run below commands:

cd /home/catapult/ixload/install/

tar xvf NSA\_DUSim\_\*.tgz (this will extract 3 files)

chmod u+x ixloadInstaller\_\*.sh

./ixloadInstaller\_\*.sh

./dctInstall.sh

At this point when NSA package is successfully installed, user is ready to configure and run test using IxLoad User Interface.

**Install DUSIM SA-CP Package for DUSIM-CP VM:**

Copy the SA Package Installer for CP (SA\_CP\_DUSim\_\*.tgz) to this VM’s /home/catapult/ixload/install/ directory.

scp SA\_CP\_DUSim\_\*.tgz catapult@<DUSIM-CP’s IP>:/home/catapult/ixload/install/ (passwd: catapult)

Do SSH to DUSIM-CP VM using same credential as above and run below commands:

cd /home/catapult/ixload/install/

tar xvf SA\_CP\_DUSim\_\*.tgz (this will extract 4 files)

chmod u+x hlssa\_\*\_CP\_Installer.sh

./hlssa\_\*\_CP\_Installer.sh

At this point when SA package for CP is successfully installed.

User has to configure SA package for UP(s) and run test using IxLoad User Interface.

**Install DUSIM SA-UP Package for DUSIM-UP VM:**

Copy the SA Package Installer for UP (SA\_UP\_DUSim\_\*.tgz) to this VM’s /home/catapult/ixload/install/ directory.

scp SA\_UP\_DUSim\_\*.tgz catapult@<DUSIM-UP’s IP>:/home/catapult/ixload/install/ (passwd: catapult)

Do SSH to DUSIM-UP VM using same credential as above and run below commands:

cd /home/catapult/ixload/install/

tar xvf SA\_UP\_DUSim\_\*.tgz (this will extract 4 files)

chmod u+x hlssa\_\*\_UP\_Installer.sh

./hlssa\_\*\_UP\_Installer.sh

At this point when SA package for UP is successfully installed.

User has to configure SA package for CP(s) and run test using IxLoad User Interface.

IPSEC Configuration for DUSIM F1-C

Contents

[1 Overview 5](#_Toc64566063)

[2 Install and Configure Strongswan on Ubuntu VM 5](#_Toc64566064)

[2.1 Step 1: Enable Kernel Packet Forwarding 5](#_Toc64566065)

[2.2 Step 2: Install strongSwan - Needs to be included in VM image 5](#_Toc64566066)

[2.3 Step 3: Setting Up a Certificate Authority 5](#_Toc64566067)

[2.3.1 For Server - CU VM 5](#_Toc64566068)

[2.3.2 For Client - DUSim VM: 6](#_Toc64566069)

[2.4 Step 4: Configure Strongswan 6](#_Toc64566070)

[2.4.1 Rakuten IPSEC Profile 7](#_Toc64566071)

[2.4.2 Example 1: Static DU F1-C IP addresses 7](#_Toc64566072)

[2.4.3 Example 2: DU F1-C IP addresses dynamically assigned by CU 9](#_Toc64566073)

[2.5 Step 5: Configure Authentication 11](#_Toc64566075)

[2.5.1 Client/DU Side ipsec.secrets 11](#_Toc64566076)

[2.5.2 Server/CU Side ipsec.secrets 12](#_Toc64566077)

[2.6 Step 6: Enable and start Strongswan Service 12](#_Toc64566078)

[3 Validation and Debugging 12](#_Toc64566079)

[3.1 Strongswan Status 12](#_Toc64566080)

[3.2 IPSEC Status 12](#_Toc64566081)

[3.3 XFRM Policy and State 14](#_Toc64566082)

[3.4 Ping test from each direction: 15](#_Toc64566083)

[3.5 How to decode ESP packets at Wireshark 16](#_Toc64566084)

[4 Running with IxLoad HLS-SA 17](#_Toc64566085)

# Overview

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane. In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported and mandatory to implement on the gNB-DU per specification.

In this IPSEC solution, Strongswan, a free, open-source, widely used IP-SEC based VPN is adopted without impacting lizard based F1-C implementation.

# Install and Configure Strongswan on Ubuntu VM

## Step 1: Enable Kernel Packet Forwarding

Add the following lines at the end of the /etc/sysctl.conf

net.ipv4.ip\_forward = 1

net.ipv6.conf.all.forwarding = 1

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.all.send\_redirects = 0

Save and close the file. Then, run the following command to reload the settings:

sudo sysctl -p

## Step 2: Install strongSwan - Needs to be included in VM image

You can install it by simply running the following command:

sudo apt-get install strongswan libcharon-extra-plugins strongswan-pki -y

## Step 3: Setting Up a Certificate Authority

Server side generates the IPSEC server certificate and the key for the IPSEC client to verify the authenticity of the server. Client side, i.e. our DUSIM, only needs the private key.

### For Server - CU VM

First, generate a private key for self-signing the CA certificate using a PKI utility:

ipsec pki --gen --size 4096 --type rsa --outform pem > ca.key.pem

Next, create your root certificate authority and use the above key to sign the root certificate:

ipsec pki --self --in ca.key.pem --type rsa --dn "CN=RakutenCU" --ca --lifetime 3650 --outform pem > ca.cert.pem

Next, create a certificate and the key for the IPSEC server so that the client can verify the server’s authenticity using the CA certificate- just generated.

First, create a private key for the VPN server with the following command:

ipsec pki --gen --size 4096 --type rsa --outform pem > server.key.pem

Next, generate the server certificate by running the following command:

ipsec pki --pub --in server.key.pem --type rsa | ipsec pki --issue --lifetime 2750 --cacert ca.cert.pem --cakey ca.key.pem --dn "CN=172.172.172.100" --san="172.172.172.100" --flag serverAuth --flag ikeIntermediate --outform pem > server.cert.pem

Next, copy the above certificate in the respective IPSec certificates directories as shown below:

sudo mv ca.cert.pem /etc/ipsec.d/cacerts/

sudo mv server.cert.pem /etc/ipsec.d/certs/

sudo mv ca.key.pem /etc/ipsec.d/private/

sudo mv server.key.pem /etc/ipsec.d/private/

### For Client - DUSim VM:

We will get **ca.cert.pem** from customer or from our CU VM as generated above.

sudo mv ca.cert.pem /etc/ipsec.d/cacerts

## Step 4: Configure Strongswan

There are many type of IPSEC configuration and examples at strongswan website.

Please check possible configuration settings for connection setup from:

<https://wiki.strongswan.org/projects/strongswan/wiki/ConnSection>

IKEV2 supported algorithms from:

<https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2CipherSuites>

### Rakuten IPSEC Profile

Rakuten has provided the following IPSEC profile:

IPSEC Encapsulation Mode: Tunnel Mode

IKE Version: IKE v2

IKE Mode: Aggressive

Encryption Algorithm Phase 1 (preferred): AES-GCM with 16 octet ICV with 256 bit key length

Hash Algorithm Phase 1(preferred): SHA256.384 or SHA256.512

Pseudo-random function for IKE SA is PRF\_HMAC\_SHA2\_384

Encryption Algorithm Phase 2(preferred): ESP-AES-256

Hash Algorithm Phase 2(preferred): Could be SHA256

### Example 1: Static DU F1-C IP addresses

The following ipsec.conf files are created for Rakuten’s IPSEC profile with static client inner IP address (DU F1-C) configuration.

#### Client/DU Side Ipsec.conf

The following ipsec.conf file needs to be generated and copied to /etc/ipsec.conf at DU VM.

#ipsec.conf – strongSwan Ipsec configuration file.

config setup

# you can increase the log levels to 3 and 4 to get more information

       charondebug="ike 4, knl 2, cfg 2, chd 4, net 2, esp 2, dmn 2, mgr 2"

       strictcrlpolicy=no

       uniqueids=yes

       cachecrls=no

conn ipsec-ikev2-vpn-client

type=tunnel

aggressive=yes

# local ip address of outer IPSEC tunnel

left=172.172.172.3

# subnet for local DU F1-C addresses – static defined at DU.

**leftsubnet=1.1.1.0/16**

leftid=catapult

leftauth=eap-mschapv2

# remote ip address of outer IPSEC tunnel

right=172.172.172.100

rightid=172.172.172.100 # used while creating the certificates

# subnet for remote CU F1-C addresses

rightsubnet=1.1.1.0/16

     rightauth=pubkey

# defines the identity the client uses to reply to an EAP Identity request.

eap\_identity=%identity

     ike=aes256gcm16-sha384-prfsha384-ecp384! #Rakuten requirements

esp=aes256-sha256! #Rakuten requirements

auto=start

#### Server/CU Side Ipsec.conf

The following ipsec.conf file needs to be generated and copied to /etc/ipsec.conf at CU VM.

#ipsec.conf – strongSwan Ipsec configuration file.

config setup

# you can increase the log levels to 3 and 4 to get more information

       charondebug="ike 4, knl 2, cfg 2, chd 4, net 2, esp 2, dmn 2, mgr 2"

       strictcrlpolicy=no

       uniqueids=yes

       cachecrls=no

conn ipsec-ikev2-vpn

     auto=add

     compress=no

     type=tunnel # defines the type of connection, tunnel.

aggressive=yes

     keyexchange=ikev2

     fragmentation=yes

     forceencaps=yes

     dpdaction=clear

     dpddelay=300s

     rekey=no

     left=172.172.172.100

     leftid=172.172.172.100

     leftcert=server.cert.pem # reads the VPN server cert in /etc/ipsec.d/certs

     leftsendcert=always

     leftsubnet=1.1.0.0/16

     right=172.172.172.3

     rightid=%any

**rightsubnet=1.1.0.0/16**

     rightauth=eap-mschapv2

     rightsendcert=never

     eap\_identity=%identity

     ike=aes256gcm16-sha384-prfsha384-ecp384! #Rakuten requirements

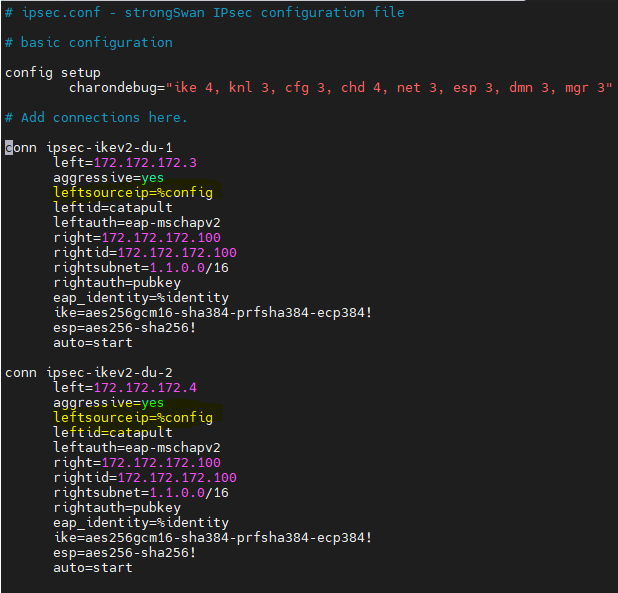
esp=aes256-sha256! #Rakuten requirements

### Example 2: DU F1-C IP addresses dynamically assigned by CU

In this example, multiple DU IPSEC tunnels are configured per DU and DU F1-C is assigned by CU during tunnel establishment. Please note that the inner IP is assigned to the same interface with outer IP address.

#### Client/DU Side Ipsec.conf

Notice **leftsourceip = %config** which indicates inner IP is assigned by CU.



#### Server/CU Side Ipsec.conf

Notice **rightsourceip = 1.1.0.0/16** indicates the IP pool where client IP addresses will be assigned from.

## 

## Step 5: Configure Authentication

### Client/DU Side ipsec.secrets

Configure IPSEC client authentication by editing the file /etc/ipsec.secrets:

sudo vi /etc/ipsec.secrets

Add the following line:

catapult : EAP "your-secure-password”

### Server/CU Side ipsec.secrets

Next, we will need to configure client-server authentication credentials to define the RSA private keys for authentication and set up the EAP user credentials.

sudo vi /etc/ipsec.secrets

Add the following lines:

: RSA "server.key.pem"

catapult : EAP "your-secure-password"

## Step 6: Enable and start Strongswan Service

On CU VM, restart the strongSwan service and enable it to start at reboot:

sudo systemctl restart strongswan

sudo systemctl enable strongswan

On DU VM restart the strongSwan.

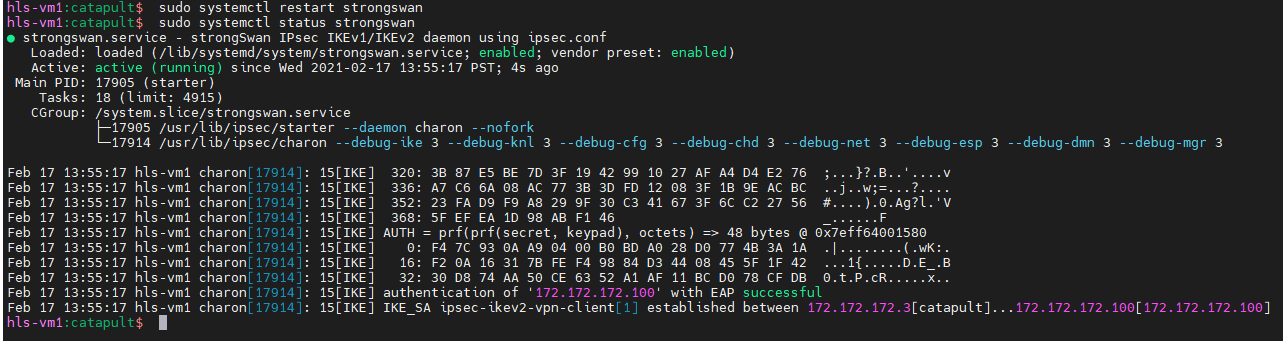
# Validation and Debugging

You can check the following at DU and CU VM.

## Strongswan Status

sudo systemctl status strongswan

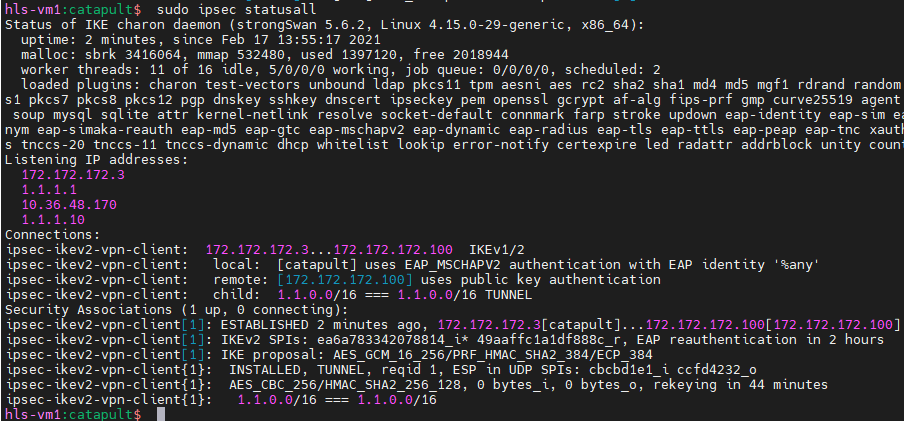
You should see:



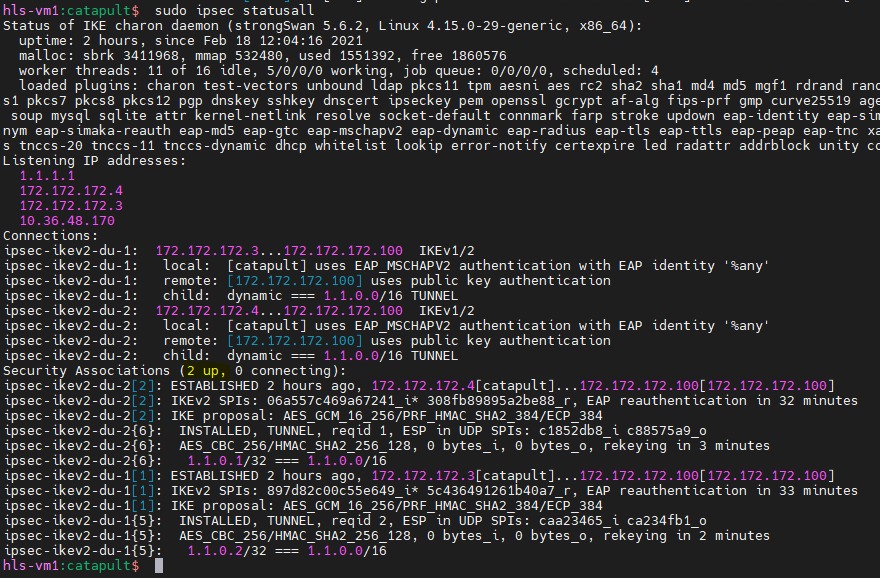
## IPSEC Status

sudo ipsec statusall

**For Example1:**



**For Example2:**



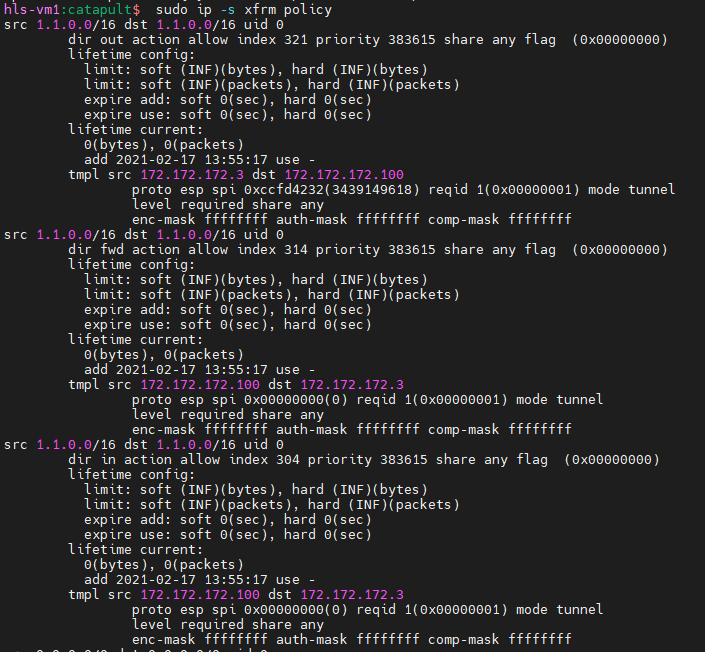
## XFRM Policy and State

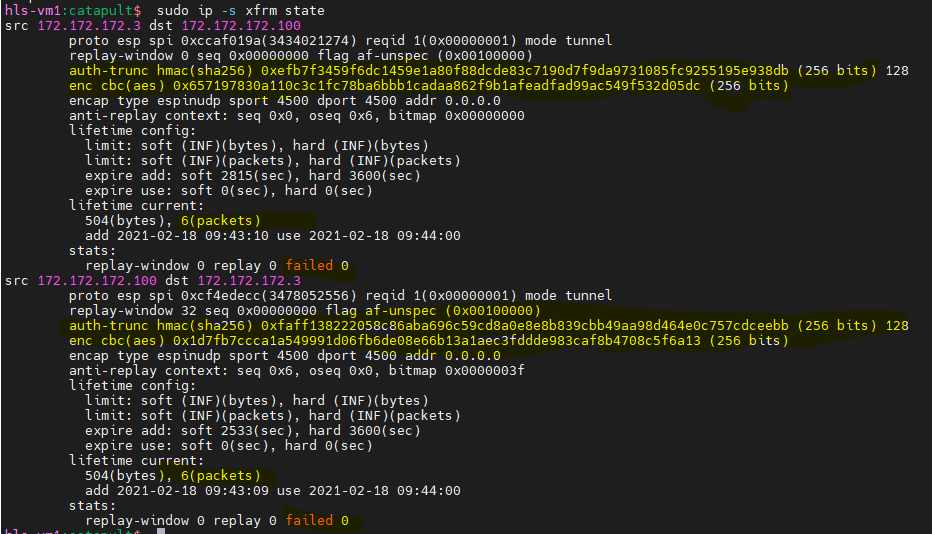
* Check if ipsec SA’s are installed successfully:

sudo ip -s xfrm policy

sudo ip -s xfrm state

You should see the policies are installed. If connection is established but IPSEC SA’s not created, it indicates some problem. If that happens, please check /var/log/syslog for more detailed logs.





**NOTE**: ESP keys can be extracted from this command as highlighted above. You can use

them to decode the ESP packets at Wireshark! Please see section 3.5 for more details.

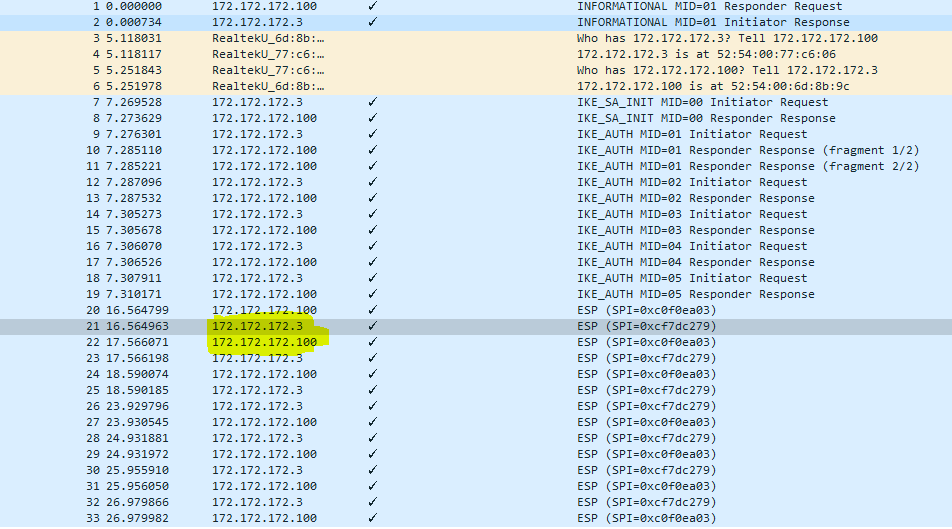
## Ping test from each direction:

Please capture the packets at the bridge – br-dusim interface.

ping -I 1.1.1.1 1.1.2.2 # On CU VM ping DU F1-C address

ping -I 1.1.2.2 1.1.1.1 # On DU VM ping CU F1-C address

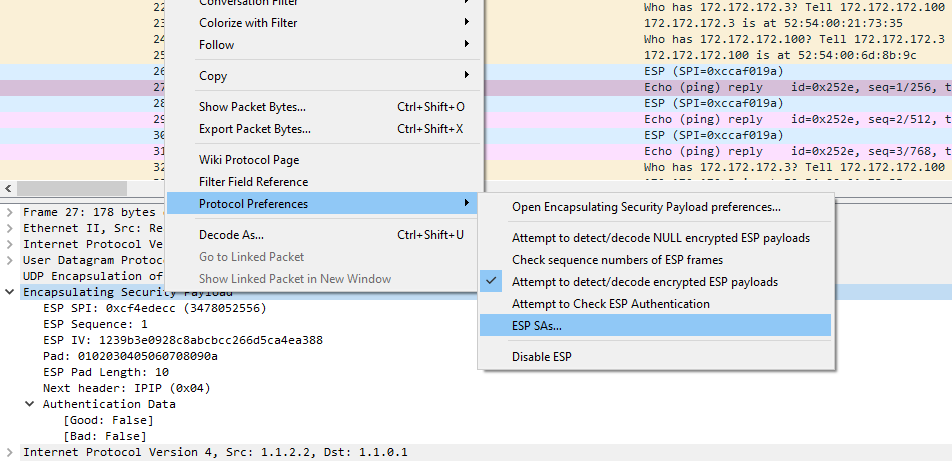
Ping should work and the capture should show ESP encrypted packets with IPSEC outer IP addresses configured at ipsec.conf



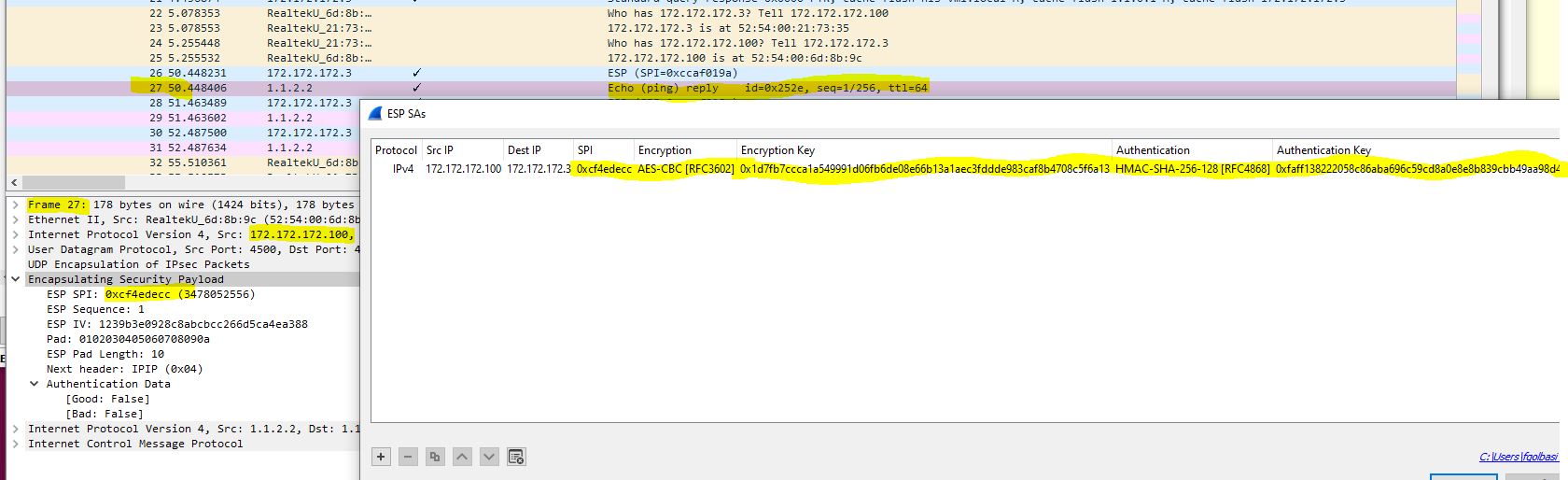
You can update esp=null at ipsec.conf and restart strongswan service on both VMs ( first on the server) to see the inner packets not encrypted.

## How to decode ESP packets at Wireshark

ESP keys can be extracted from “ip -s xfrm state” as shown in 3.3. You can configure wireshark as below to decode the inner packets.



Notice after configuring ESP SAs with the keys, the inner Echo Ping packet can be seen from wireshark.



# Running with IxLoad HLS-SA

## Before doing Apply Config, login to the HLS-VM, assign IPSEC outer and inner IP address to the same interface where F1-C control plane to be assigned after Apply Config (eth1)

sudo ip addr add 172.172.172.3/8 dev eth1 - outer IP address

Example 1: sudo ip addr add 1.1.2.2/16 dev eth1 - inner IP address

Example 2: No need for this, as ip address is added during tunnel setup.

Restart strongswan service on CU VM and HLS VM. After verifying IPSEC connection as described at Section 3, use 1.1.2.2 (or the dynamically assigned IP address) as F1-C DU address at IxLoad configuration and do apply config. After this point packets should go through IPSEC tunnel.