# Network Security

Security can be achieved at two level

* Data at Rest
* Data in transition

1. Data at Rest

In means the data that are stored in the application or in memory

1. Data in transition

This means data send over the N/W

# TLS

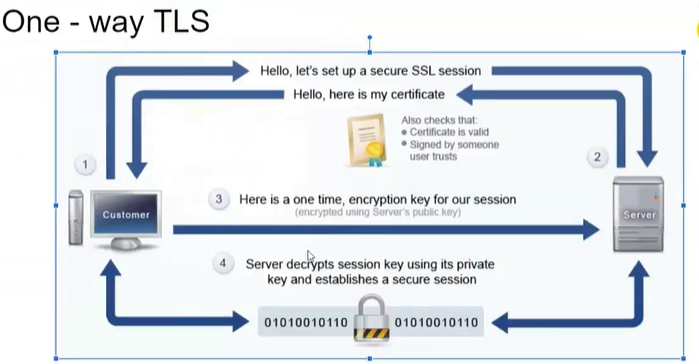
It is uses to implement network security

* It is used in combination with cryptography and digital signature
* Cryptography can use: symmetric, asymmetric or hybrid
* Two ways to implement TLS
  + One way TLS
  + Two way TLS

1. One way TLS

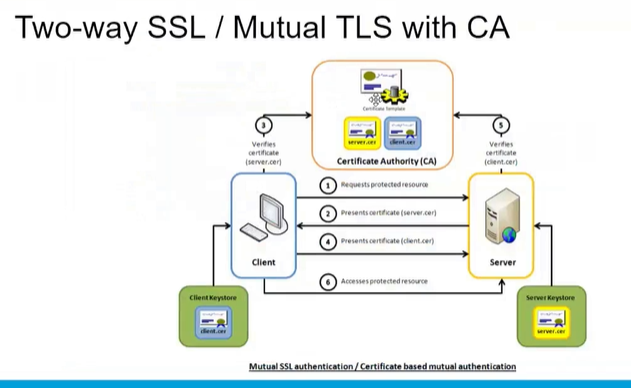
Eg. Request [www.google.com](http://www.google.com)

* In this method it is the responsibility of the clients to verify the server
* Steps:
  + Customer request for resources
  + Server gives the certificate
  + Customer uses the certificate and public key to generate symmetric key and send to the server
  + Server uses it to generate the secure key to start communication



1. Two way SSL

* Client and serve both need to verify each other
* Also called as **mutual HTTPS**
* It ensures that data is not tampered
* Prevents man in the middle attack
* Methods:
  + Client request for a resource
  + Server provides its certificates from its keystore to client
  + Client validates te certificate with CA. If client validates the certificate from its keystore then server validates clients certificate with CA  
    client and server will have their own key store to provide the certificate



# KeyStore and TrustStore

* Both uses **jks based concept**
* **KeyStore**: store public certificate and private key
  + **Provide** certificate
* **TrustStore**: store public key of the other party so that it can validate
  + **Validates** the certificate
* Create a key using JKS file
* In the command prompt run the following command
* - keyalg : RSA (default is DSA)
* - alias: give any name you want
* -keystore: give any name format <name>.jks file
* When the command executes it creates the \*.jks file. We have to copy that file in the anpoint studio inside main/resource folder

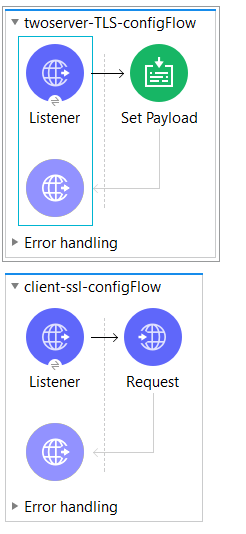




Create key

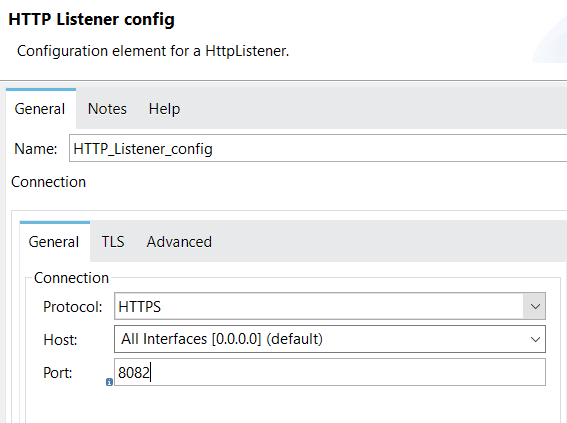
<https://docs.mulesoft.com/mule-runtime/4.3/tls-configuration#generate-a-keystore>

IN anypoint studio create two flows



1. HTTP listener config – for server

Set to https and port as 8082



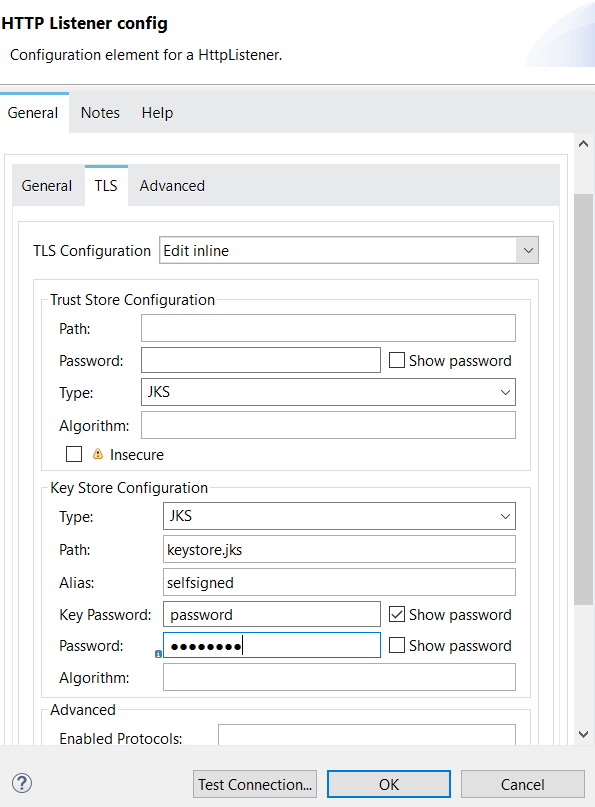


Figure : Configure only the keystore in one way SSL password: password

1. Configure listener for the client

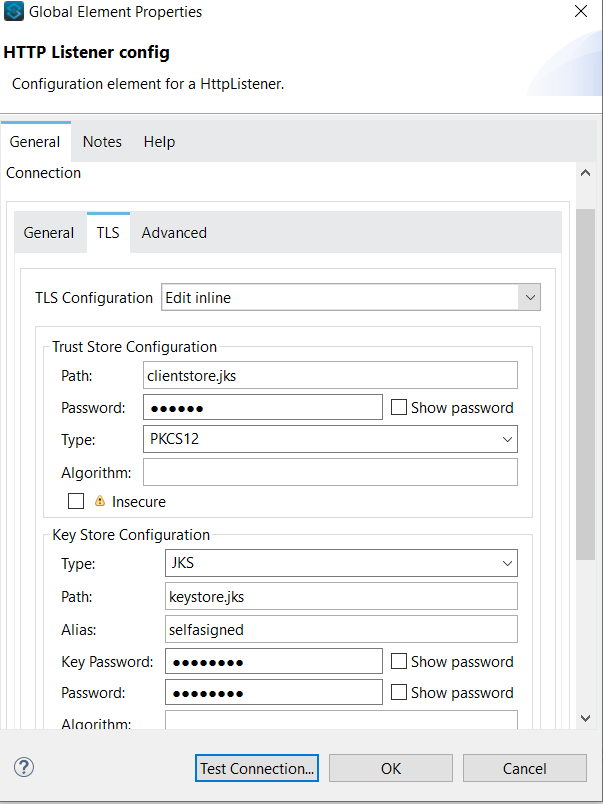
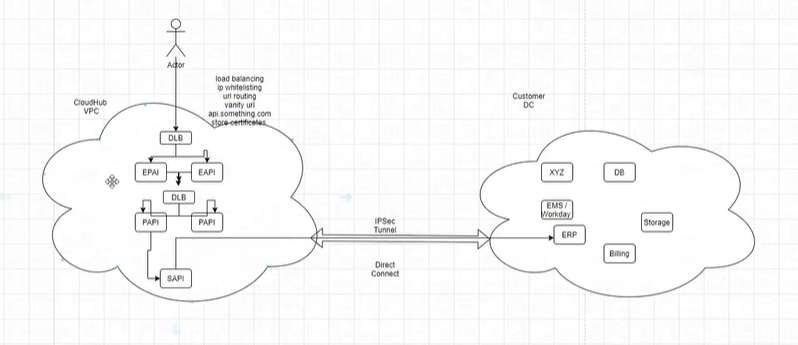


Figure two ways ssl password: client

# VPC



Things to consider when setting the VPC

* Size of the VPC
* How to configure connection between two VPC and between other networks (customer db, customer app or other cloud)
* Configure DLB

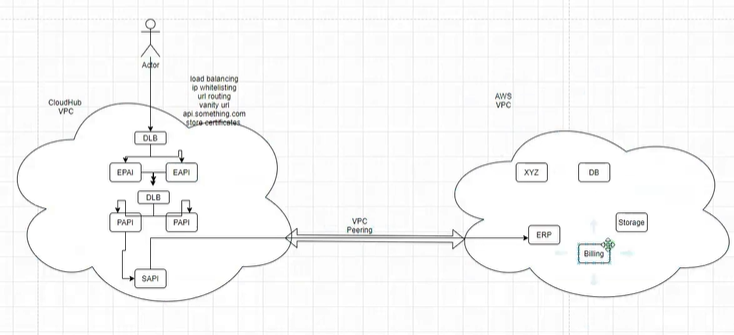
To create VPC

* Goto runtime manager -> VPC -> create VPC
* When VPC is subscribed two VPC are provided
* In production – one VPC is used for production and – another is used for DevOps, test
* It is always created at regional level
* It allows to add different environment, different business groups and sub groups, configure firewalls
* In order to deploy application out of the VPC you need to configure the IP address
* In VPC to access application from outside you have to used the configured port
* It allows to deploy application to multiple workers
* Allows to choose number of workers to deploy the application

TO get customer data to VPC  
- you have to create a secure network which is called VPN

* It is a secure n/w established over the internet
* To create VPN you can use IPSec or Direct connect
* DirectConnect is more espensive, and uses a separate pipe between customers and the aws
* All tha application are configured using port 8091 for security

Communicate two VPC we **use VPC peering**



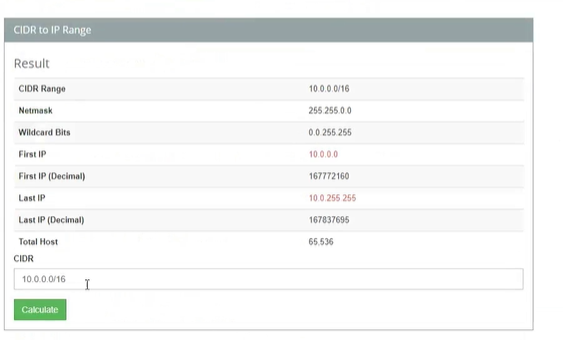
# DLB

* It allows the VPC to communicate with the application outside of VPC
* It is used to access the secure application in VPN  
  It has the public IP associated with it
* Since the associated IPs are public it can be accessed outside
* This public IP can be added to the DNS server. So you can get a vanity URL
* Eg: api.configuration.com
* Advantage
  + Can do IP whitelisting
  + Load balancing
  + Vanity url
  + You can store certificate in DLB so it automatically works as key store and truststore

## VPC size

* CIDR block is used to identify the VPC size
* The size should be between 16 – 24
* 16: 65000 IPs will be allocated
* 24: 256 IPs will be allocated
* Calculate the size of ip using the following apps

Use the link <https://www.ipaddressguide.com/>



## Relationship between Mule app and IP

For every application it should have an IP

* Zerodown time 2 IP
* 2 worker – 2 IP
* One IP per worker
* VLC size
  + Example for 100 apps
    - To achieve high availability – 2 \* 100 Ips
    - To achieve high zero downtime – 50% of IPs i.e 300 Ips

To find the size of IPS we need to know

* How many applications we have
* The number of non functional requirements