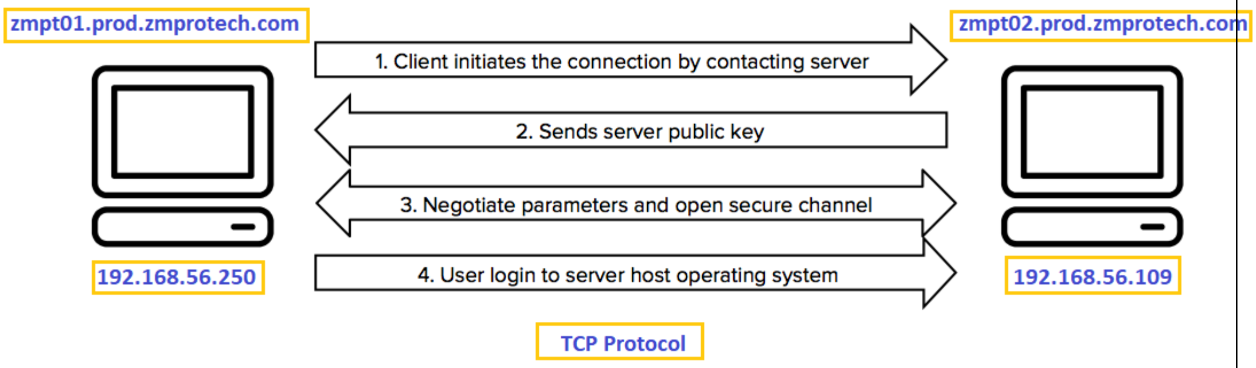
11-28-2020
https://youtu.be/fQlqwMi7JQQ

SSH – Secure Shell


zmpt01.prod.zmprotech.com
zmpt02.prod.zmprotech.com
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system
192.168.56.250
192.168.56.109
TCP Protocol

```
[root@zmpt01 ~]# ssh 192.168.56.109
The authenticity of host '192.168.56.109 (192.168.56.109)' can't be established.
ECDSA key fingerprint is SHA256:e3LN1URGQEPwXaMbDeo+aTYev2cOOWnP3WKmaRG9gRU.    < ---
#1
ECDSA key fingerprint is MD5:de:11:30:dd:ef:9e:ae:0a:ab:49:16:29:c9:08:36:8f.    < ---
#2
Are you sure you want to continue connecting (yes/no)? yes                       < ---
#3
Warning: Permanently added '192.168.56.109' (ECDSA) to the list of known hosts.
root@192.168.56.109's password:                                                  < ---
#4
```

11-29-2020
https://youtu.be/DVtalAskm3Y

Now logged into the remote server

```
Last login: Sun Nov 29 15:31:38 2020 from 192.168.56.250
[root@zmpt02 ~]# hostname
zmpt02.prod.zmprotech.com
```

Connecting as non-root user

```
[root@zmpt01 ~]# ssh zafar@71.57.95.5
The authenticity of host '71.57.95.5 (71.57.95.5)' can't be established.
ECDSA key fingerprint is SHA256:6C8O0slMqNbzLMaV2Lm4OrBh29qCtTHeoFi1bgRY6BQ.
ECDSA key fingerprint is MD5:bb:19:a3:ed:01:6d:8e:c5:6a:b7:3c:35:8b:ea:3f:97.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '71.57.95.5' (ECDSA) to the list of known hosts.
zafar@71.57.95.5's password:
```

```
[root@zmpt01 .ssh]# pwd
/root/.ssh

[root@zmpt01 .ssh]# cat known_hosts

192.168.56.109 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOPP3wf/x3cI2qcKmTcH4KPch
JHdTAHRnnO4ASznR9xZ06KCsbWyXQoj/5p+E85DH9cFmCKh+5rFED8bQZfKH2Q=

71.57.95.5 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNXZK5HP3F1AdNYJ5gKTio6z/
uJcDzAAdDPIcolYXUBd+r6Qv2PJqXiSq6OlMJrXUDxdTsfr4SofXL6bQWCX59Y=
```

Passwordless SSH

```
[root@zmpt01 .ssh]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):      < --- Hit Enter
Enter passphrase (empty for no passphrase):                   < --- Hit Enter
Enter same passphrase again:                                  < --- Hit Enter
Your identification has been saved in /root/.ssh/id_rsa.      < --- Generates Private Key
Your public key has been saved in /root/.ssh/id_rsa.pub.      < --- Gererates Public Key
The key fingerprint is:
SHA256:PFH7mLOaE/vac1SEZ867YhYKusl1PwNJ7UpSzHI3RSE root@zmpt01.prod.zmprotech.com
The key's randomart image is:
+---[RSA 2048]----+
|         . Eoo. |
|        . ...=  |
|       .o.. B   |
|      ...*++ +  |
|       S=++.o . |
|       +.+o+ .  |
|      ..*o= . . |
|    ..oo=+.B .  |
|      +.++o=.+   |
+----[SHA256]-----+
[root@zmpt01 .ssh]#
```

```
[root@zmpt01 .ssh]# pwd
/root/.ssh
[root@zmpt01 .ssh]# ls -la
total 12
drwx------. 2 root root   57 Nov 29 16:02 .
dr-xr-x---. 3 root root  123 Nov 28 17:46 ..
-rw-------. 1 root root 1675 Nov 29 16:02 id_rsa         < --- Private Key
-rw-r--r--. 1 root root  412 Nov 29 16:02 id_rsa.pub     < --- Public Key
-rw-r--r--. 1 root root  348 Nov 29 15:52 known_hosts  < --- Saves Public key of previously connected hosts
```

```
[root@zmpt01 .ssh]# ssh-copy-id 192.168.56.109
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.109 (192.168.56.109)' can't be established.
ECDSA key fingerprint is SHA256:e3LN1URGQEPwXaMbDeo+aTYev2cOOWnP3WKmaRG9gRU.
ECDSA key fingerprint is MD5:de:11:30:dd:ef:9e:ae:0a:ab:49:16:29:c9:08:36:8f.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.56.109's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '192.168.56.109'"
and check to make sure that only the key(s) you wanted were added.
```

```
[root@zmpt01 ~]# ssh 192.168.56.109
Last login: Sun Nov 29 16:49:50 2020 from 192.168.56.250

[root@zmpt02 ~]# hostname
zmpt02.prod.zmprotech.com
```

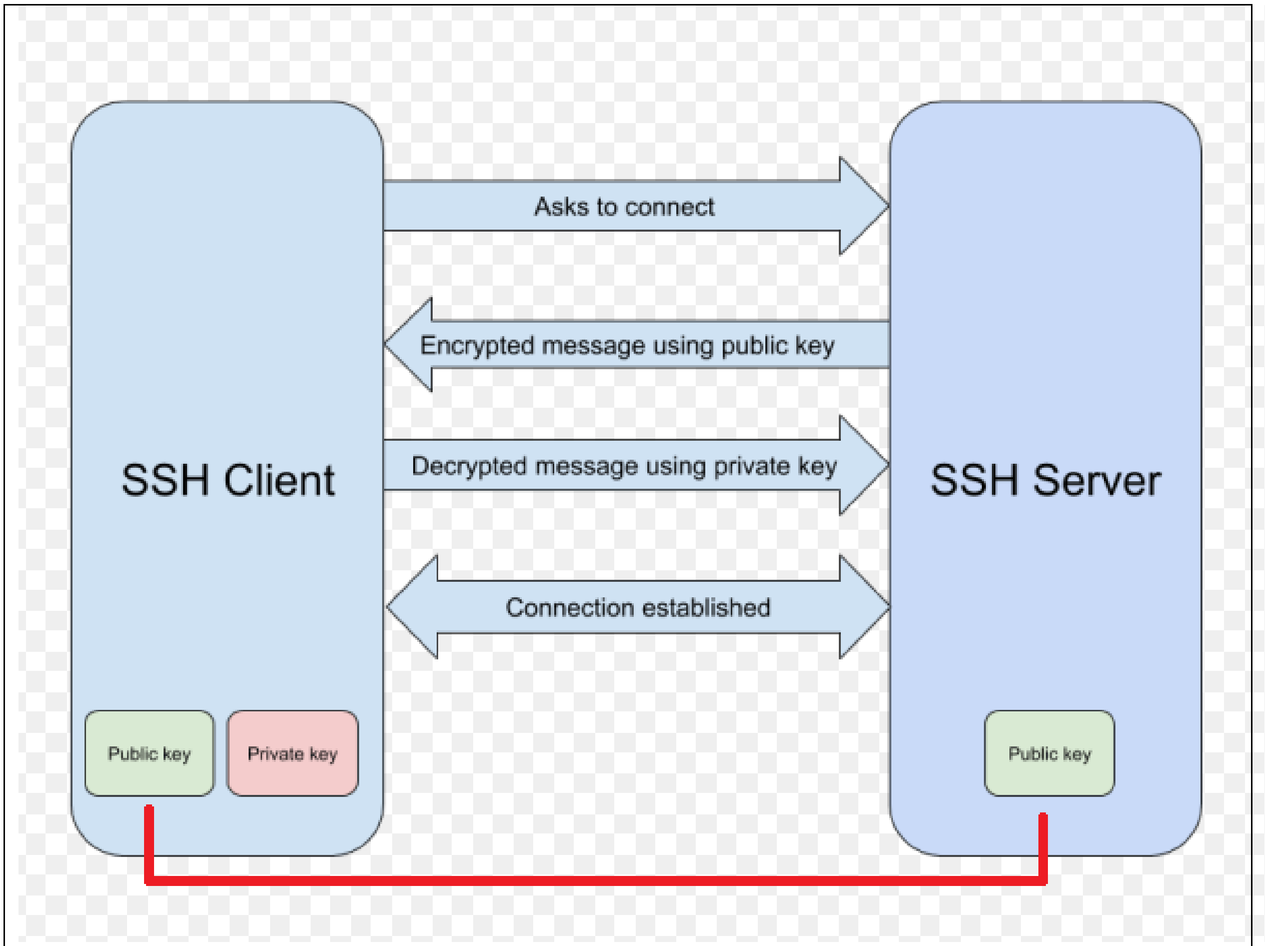
```
[root@zmpt02 ~]# cd .ssh/
```

```
[root@zmpt02 .ssh]# ls -la
total 4
drwx------. 2 root root  29 Nov 29 16:20 .
dr-xr-x---. 3 root root 123 Nov 29 16:20 ..
-rw-------. 1 root root 412 Nov 29 16:20 authorized_keys    < --- New file with authorized keys of
known hosts
```

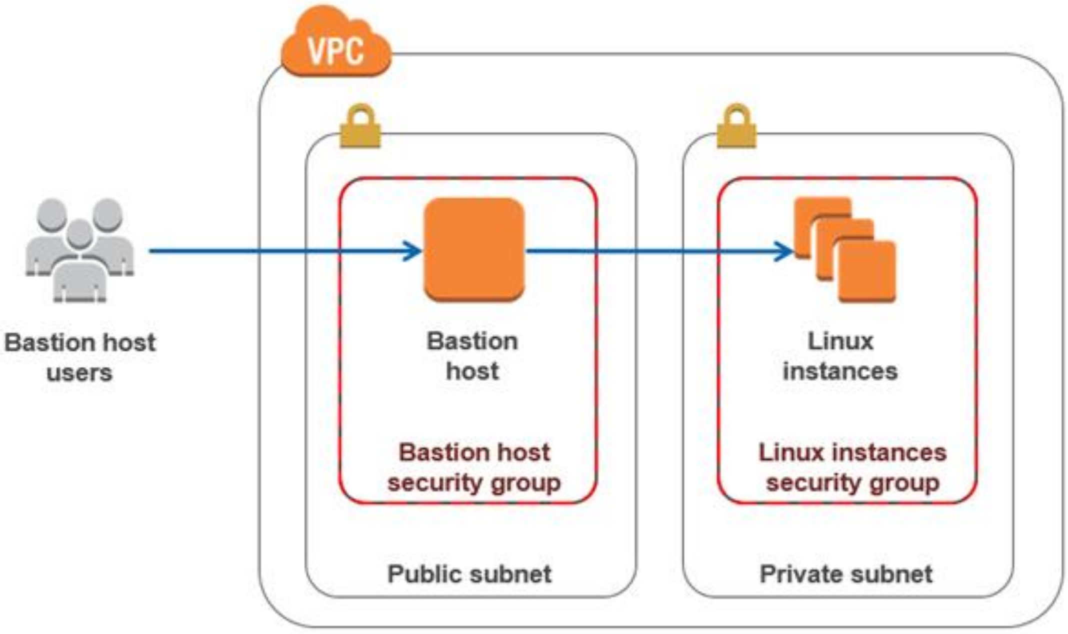
```
[root@zmpt01 .ssh]# cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC4xSOCeATZnKwEUTzSoKns4zEioGBP3uUq9bXVZ1CTIKtGMx
4snIq6q
+/q331sGFKZsEMdgxMaGLy3/mp6bl5Nv2D1LeqCVvkmoeW5+rEWn853ggV2Syjigo2UrXqnVUK05Ks6c
AmlqPYC3TWvmTH
nbSMKqbfQGKykxEkF0Xv/CRm3FSyVW7S1Aq5yPavAQa0+TFkaxBUO7Ooy+3QZ6Jolb8UiQROo7WdPAk
ITAOUJoYTVHujKBh
D9Pf21PutmdiKhqHUX2rlw1HJmUJQFYRBwlJ3INd+Q9qDjllQ1wiPyi/XpmoenGkHjqEXjsQzJGEAQtFd9ay
Mybdh+TNnb/
xCX root@zmpt01.prod.zmprotech.com
```

```
[root@zmpt02 .ssh]# cat authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC4xSOCeATZnKwEUTzSoKns4zEioGBP3uUq9bXVZ1CTIKtGMx
4snIq6q
+/q331sGFKZsEMdgxMaGLy3/mp6bl5Nv2D1LeqCVvkmoeW5+rEWn853ggV2Syjigo2UrXqnVUK05Ks6c
AmlqPYC3TWvmTH
nbSMKqbfQGKykxEkF0Xv/CRm3FSyVW7S1Aq5yPavAQa0+TFkaxBUO7Ooy+3QZ6Jolb8UiQROo7WdPAk
ITAOUJoYTVHujKBh
D9Pf21PutmdiKhqHUX2rlw1HJmUJQFYRBwlJ3INd+Q9qDjllQ1wiPyi/XpmoenGkHjqEXjsQzJGEAQtFd9ay
Mybdh+TNnb/
xCX root@zmpt01.prod.zmprotech.com
```

NOTE: This is good only for each specific user, you have to establish same connection for each user



Configure Host security – Deny direct root connection



Secure the server

zmpt02.prod.zmprotech.com

```
[root@zmpt02 ~]# vi /etc/ssh/sshd_config

PermitRootLogin no       < ---root login line is uncommented and changed to no from yes
```

Restart the service

```
[root@zmpt02 ~]# systemctl restart sshd   < --- Change will take affect after restart of service
```

```
[root@zmpt01 ~]# ssh 192.168.56.109
root@192.168.56.109's password:
Permission denied, please try again.
```

Deny access fro mspecific network

```
[root@zmpt02 ~]# vi /etc/ssh/sshd_config
```

```
ListenAddress 0.0.0.0
ListenAddress 192.168.56.0/24
```

```
[root@zmpt01 ~]# ssh 192.168.56.109
ssh: connect to host 192.168.56.109 port 22: Connection refused
```

Allow only specific users

```
[root@zmpt02 ~]# vi /etc/ssh/sshd_config    #< --- Add line at the end of file

AllowUsers terminator
```