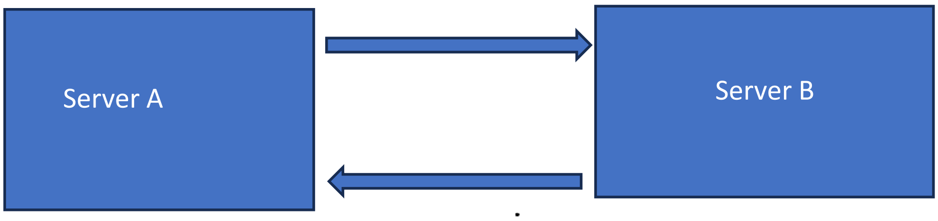
SSH -SECURE SHELL

OpenSSH is the premier connectivity tool for remote login with the **SSH** protocol. It encrypts all traffic to eliminate eavesdropping, connection hijacking, and other attacks.

A **protocol** is a set of rules that govern how data is transmitted and received in a network. set of rules used by the computer to communicate.

Transmission Control Protocol (TCP) - ensures reliable and efficient data transmission over the internet



What is SSH?

SSH, also known as Secure Shell or Secure Socket Shell, is a cryptographic network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.
it provides secure encrypted communications between two untrusted hosts over an insecure network.

Install OpenSSH Server Software Package

```
yum –y install openssh openssh-server openssh-clients
```

default port- 22

What is a port? A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service.

configuration files

```
/etc/ssh/sshd_config
/etc/ssh/ssh_config
```

service name

```
sshd
```

Starting SSH Service

```
sudo systemctl start sshd
```

Check sshd status

```
sudo systemctl status sshd
```

Enable OpenSSH Service

```
sudo systemctl enable sshd
```

To disable SSH after reboot enter:

```
sudo systemctl disable sshd
```

OpenSSH Server Configuration

```
vim /etc/ssh/sshd_config
PermitRootLogin no
Port 2222
AllowUsers user1
echo "DenyUsers user1" >> /etc/ssh/sshd_config
```

```
ssh user2@192.168.1.4
```

```
user2@192.168.1.4's password:
Permission denied, please try again.
```

<u>ssh client</u>

1. ssh <user_name>@ <server_IP> (or)<server_name>
   a. ssh user@192.168.1.44

<u>Command execution over SSH</u>

2. ssh user1@192.168.44.11 uname
3. ssh user1@vm-1.glotech.com "uname;hostname;date"
4. ssh user1@192.168.44.11 "uptime && free -m"
5. ssh user1@192.168.44.11 "top -bc | head -n 35" > /tmp/top-output.txt

   ```
   #!/bin/sh
   uname
   hostname
   ```
   chmod +x system-info.sh (create a script file system-info.sh)

6. ssh user1@vm-1.glotech.com ./system-info.sh (execute script)

<u>secure copy</u>

1. copy file to remote server
   a. scp /root/securefile root@192.168.44.11:/tmp

2. copy directory to remote server
   a. scp -r /tmp/dir1 user1@192.168.44.11:/home/user1

3. copy file from remote server to local server
   a. scp root@192.168.44.11:/tmp/file1 /media/file2

4. copy directory from remote server to local server
   a. scp -r root@192.168.44.11:/tmp/dir1 /mnt

Configure password-less SSH session (Key based authendication)

1. Generate public-private key pair
   a. ssh-keygen
   b. files - id_rsa , id_rsa.pub

2. Add public key to ~/.ssh/authorized_keys file on remote host
   a. Copy the pub key from id_rsa.pub and paste in ~/.ssh/authorized_keys file on remote host.
   b. ssh-copy-id -i ~/.ssh/id_rsa.pub username@192.168.44.11

      -i option indicates identity file
      ~/.ssh/id_rsa.pub is identity file
      remaining text is remote user and remote server IP

ssh directory for users

1. root - /root/.ssh
2. user1 - /home/user1/.ssh

SFTP

sftp root@192.168.1.10

share file windows -----> linux | linux -----> windows using sftp and scp

winscp ,filezilla