Network

Remote login

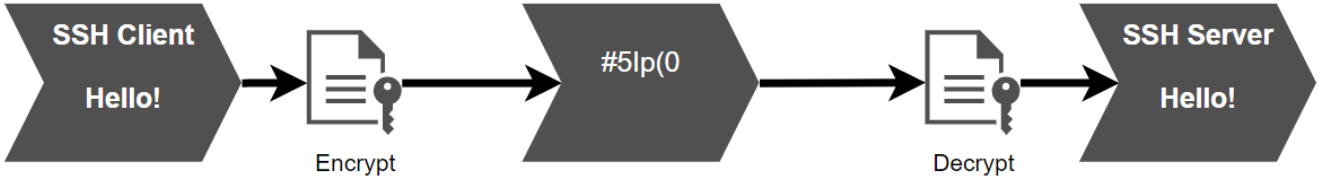
Remote login concepts and protocols

The Remote connection delimited to major groups : Remote recourses connection, Remote control, Remote login. In this course we talk about Remote login – this type of remote connection open login session on remote server and give user possibility run apps on remote server.

What is SSH

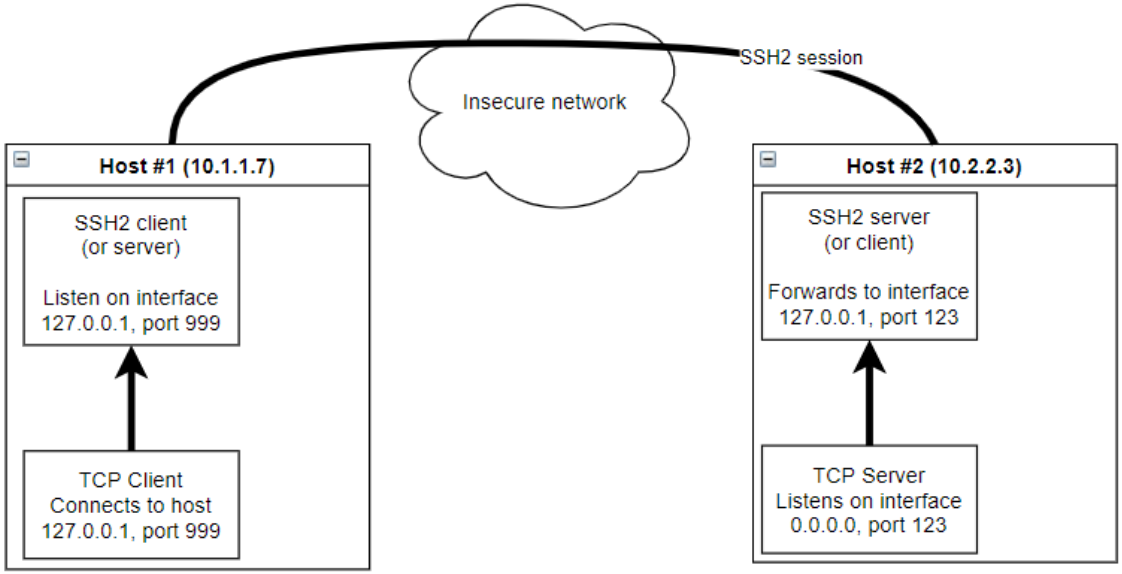
Secure Shell (**SSH**) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.
SSH provides a secure channel over an unsecured network by using a client–server architecture, connecting an SSH client application with an SSH server. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2. The standard TCP port for SSH is 22. SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows.

© Wikipedia



SSH Feature: port redirect

SSH port forwarding, or TCP/IP connection tunneling, is a process whereby a TCP/IP connection that would otherwise be insecure is tunneled through a secure SSH link, thus protecting the tunneled connection from network attacks.



* IP Addresses and ports is sample.

SSH feature: auth by keys

SSH keys enable the automation that makes modern cloud services and other computer-dependent services possible and cost-effective. They offer convenience and improved security when properly managed.
Functionally SSH keys resemble passwords. They grant access and control who can access what.

1) **Create the key pair**

```
ssh-keygen –t rsa
```

2) **Install the public key in remote server**

```
ssh-copy-id -i $HOME/.ssh/id_rsa.pub user@server
```

What is RDP

Remote Desktop Protocol (**RDP**) is a ***proprietary protocol*** developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.
Clients exist for most versions of Microsoft Windows (including Windows Mobile), Linux, Unix, macOS, iOS, Android, and other operating systems. RDP servers are built into Windows operating systems; an RDP server for Unix and OS X also exists. By default, the server listens on TCP port 3389 and UDP port 3389.

© Wikipedia

Microsoft RDP includes the following features and capabilities:

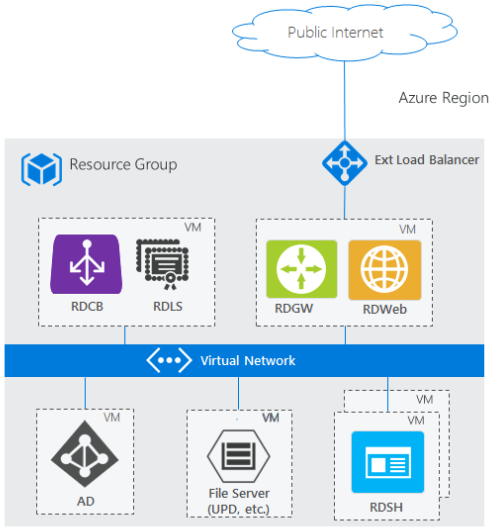
Encryption
Bandwidth reduction features
Roaming disconnect
Clipboard mapping
Print redirection
Virtual channels
Remote control
Network load balancing

In addition, RDP contains the following features:
•Support for 24-bit color.
•Improved performance over low-speed dial-up connections through reduced bandwidth.
•Smart Card authentication through Remote Desktop Services.
•Keyboard hooking. The ability to direct special Windows key combinations, in full-screen mode, to the local computer or to a remote computer.
•Sound, drive, port, and network printer redirection. Sounds that occur on the remote computer can be heard on the client computer running the RDC client, and local client drives will be visible to the remote desktop session.

RDP part of Terminal services :

Remote Desktop Services (**RDS**), known as **Terminal Services** in Windows Server 2008 and earlier,[1] is one of the components of Microsoft Windows that allow a user to take control of a remote computer or virtual machine over a network connection. RDS is Microsoft's implementation of thin client architecture, where Windows software, and the entire desktop of the computer running RDS, are made accessible to any remote client machine that supports Remote Desktop Protocol (RDP).

© Wikipedia



Remote Desktop Services roles:

Remote Desktop Session Host
Remote Desktop Connection Broker
Remote Desktop Gateway
Remote Desktop Web Access
Remote Desktop Licensing

Self study

GOAL:

Repat use case with configure key based SSH authentication on you own virtual environment

What to do:

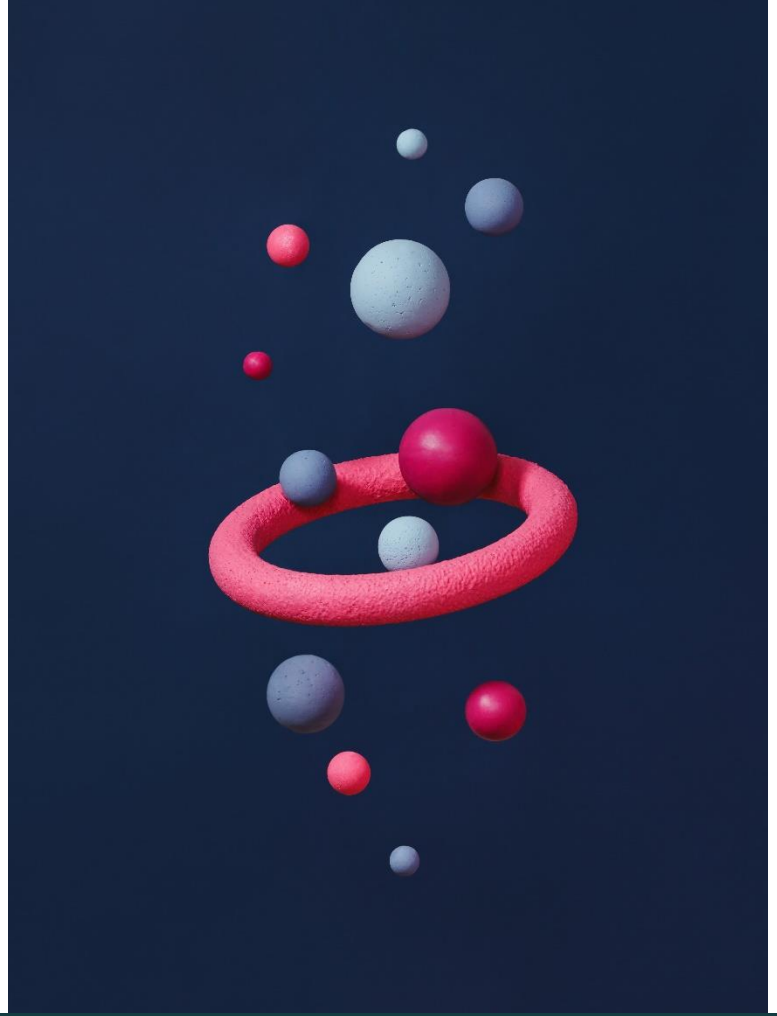
- install SSH packages
- Config SSH service
- Generate RSA keys
- Copy keys to server.

Environment:
2 Virtual Machines (VM) with ethernet adapters in same network.

Suggest use VirtualBox and CentOS 7 image.

How to check:
reboot client VM , and do
$ ssh user@server

Where *user* – your user on *server* from command, you may use IP address instead of DNS names.



THANK YOU