

**KPLABS Course**

**Splunk 2021 - Beginner to Architect**

**Domain 1**

## **ISSUED BY**

Zeal

## **REPRESENTATIVE**

[instructors@kplabs.in](mailto:instructors@kplabs.in)

# 

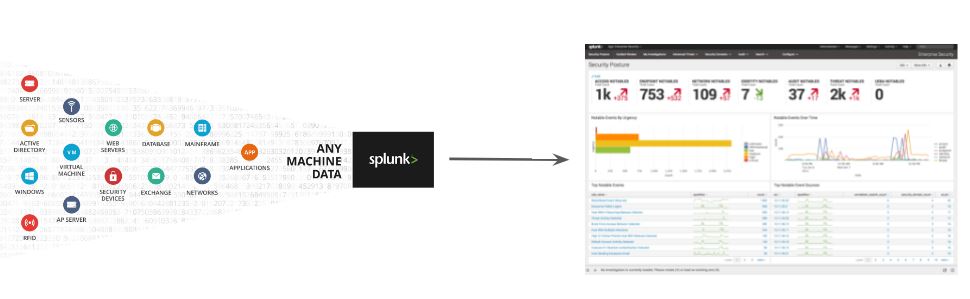
# **Domain 1 - Introduction to Splunk & Setting Up Labs**

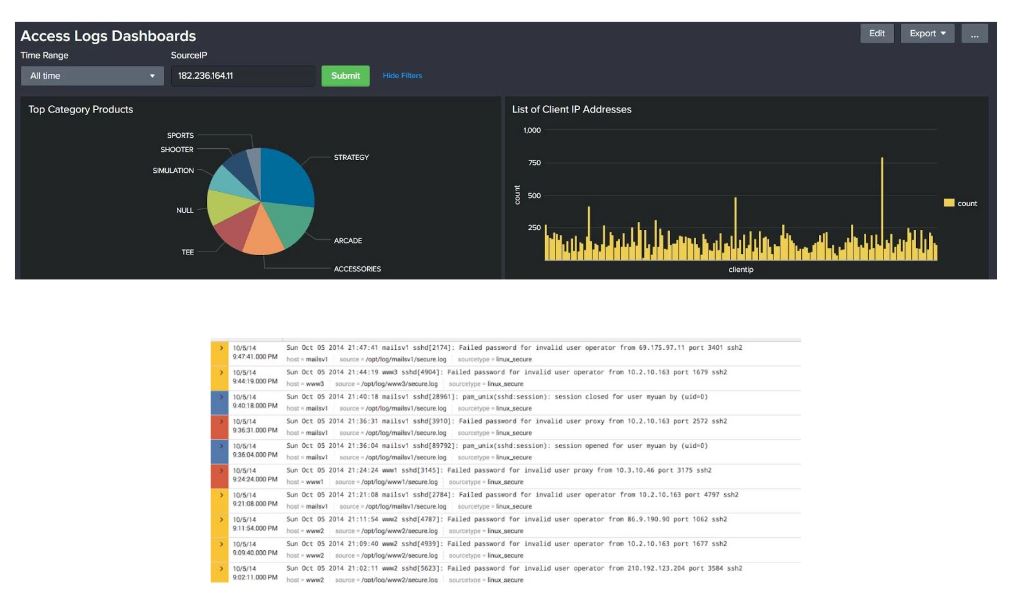
## **Module 1: Introduction to Splunk**

1.1 Overview of Splunk

Splunk is one of the most popular log analyzing and monitoring tools.

Splunk is a software platform to search, analyze and visualize the machine-generated data gathered from a wide variety of devices.





1.2 Powerful Marketplace

Splunk has its own marketplace referred to as splunkbase where people can submit their apps and add-ons.

This allows customers to use out-of-box solutions for a wide variety of use-cases.

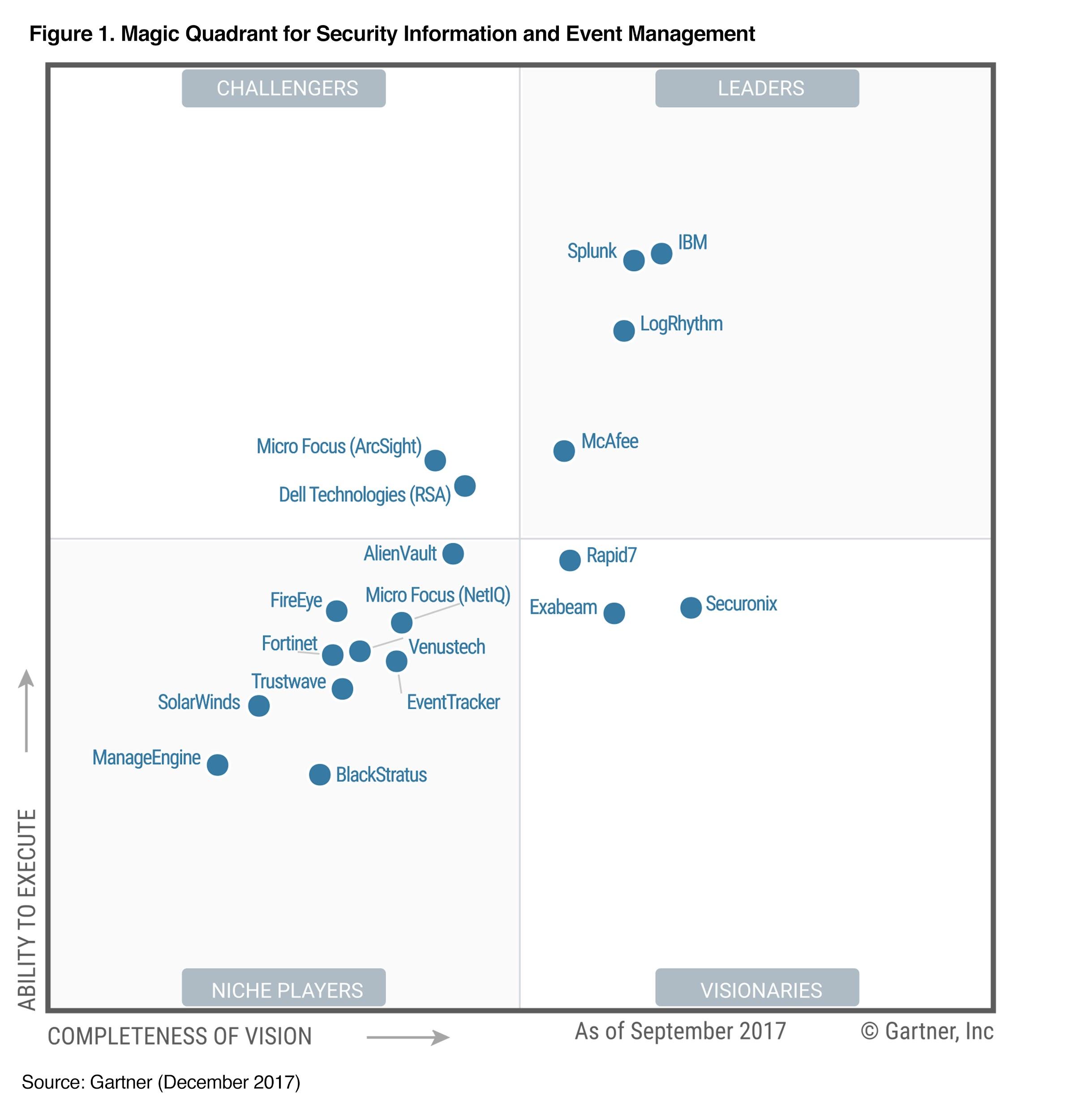


1.3 Splunk is More than Log Monitoring Solution

When a software platform is powerful in searching, analyzing, and visualizing, it can be used for much wider areas.

Splunk has been promoting new apps in various niche-specific areas like:

* Security information and event management (SIEM)
* Splunk IT Service Intelligence
* Splunk User Behavior Analytics

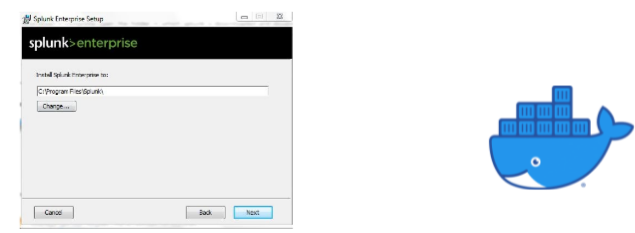


## **Module 2: Installation Methods for Splunk**

2.1 Installation Options

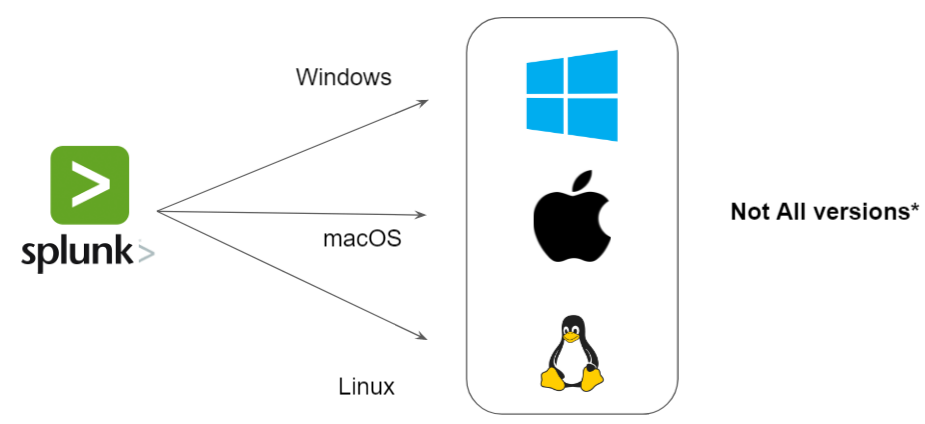
There are two primary ways for installing Splunk:

* Download and install a Splunk Enterprise installation package
* Download the Splunk Enterprise Docker image



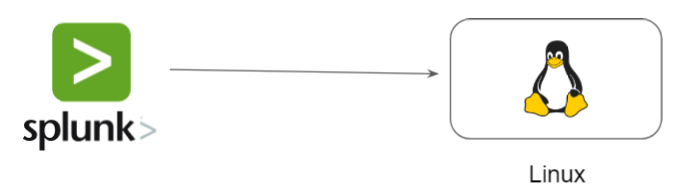
2.2 Installing Splunk via Installation Package

Splunk can be installed in a wide variety of operating systems.



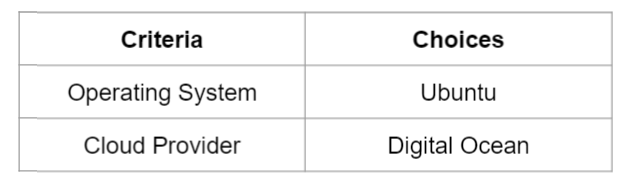
2.3 Preferred Choice for Splunk Installation Method

The preferred OS for Splunk installation would be Linux.



2.4 Revising the Choices

Following diagram illustrates the architecture that we will be following in this course:



2.5 Why Digital Ocean?

Digital Ocean allows developers to quickly deploy, manage and scale cloud infrastructure without much complexity at an affordable cost.

They provide multiple coupon codes which gives great amount of credits ranging from $50-100 USD for new users.



## 

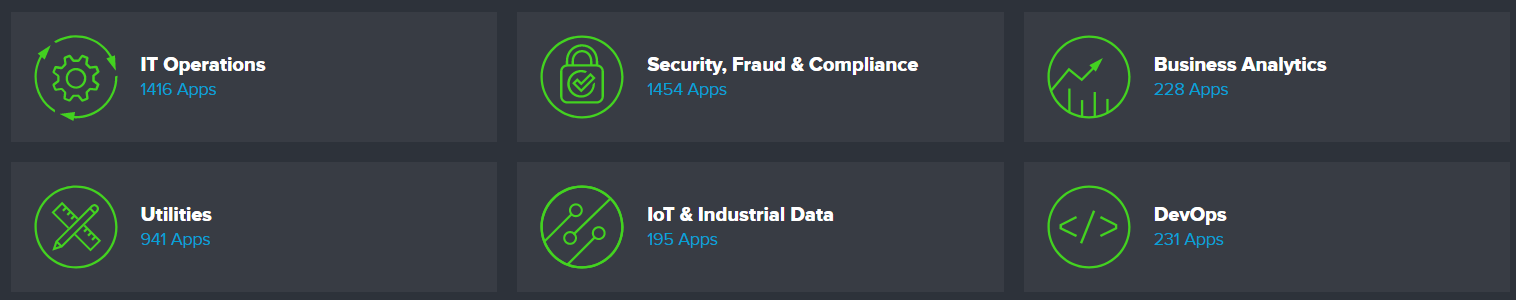
## **Module 3: Creating Splunk Account**

3.1 Overview of Splunk Account

Creating a Splunk account is an important first step and it allows users to perform various operations.

Some of these include:

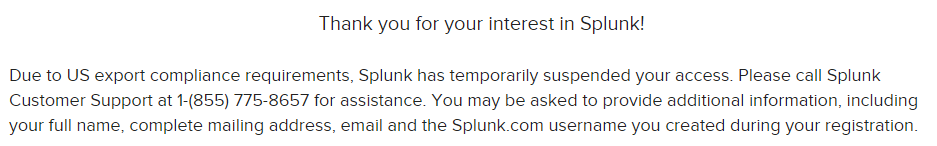
* Free Trials and Downloads
* Download Apps and Add-Ons from Splunk Marketplace.



3.2 Overview of Splunk Account

Sometimes, the Splunk signup process might fail due to restrictions based on name and countries part of a consolidated list.

The Consolidated List is a list of all persons and entities who are subject to targeted financial sanctions

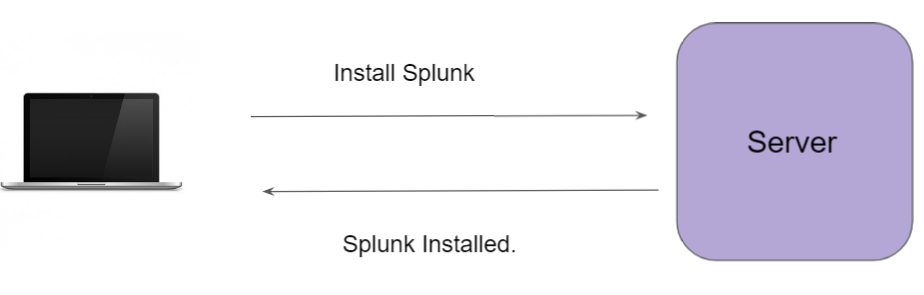


## 

## **Module 4: Infrastructure for Splunk**

4.1 Creating Infrastructure for Splunk

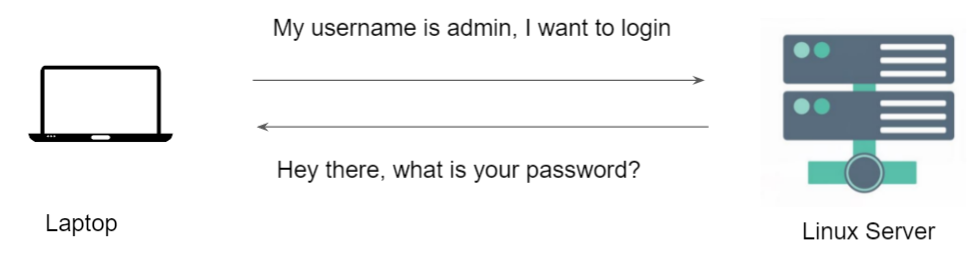
To begin with the Splunk installation process, we need one server hosting Ubuntu OS.

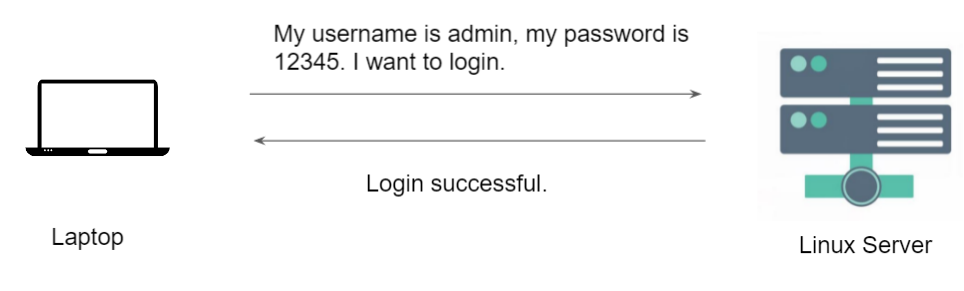


4.2 Creating Infrastructure for Splunk

There can be multiple methods for authentication against a system.

Password based authentication is the simplest form.





4.3 Challenges with Password Based Authentication

Password based authentication is generally considered to be less-secure.

Many users write down the passwords in notepad files or as part of sticky notes.

Most users would not create a complex password that is difficult to hack.

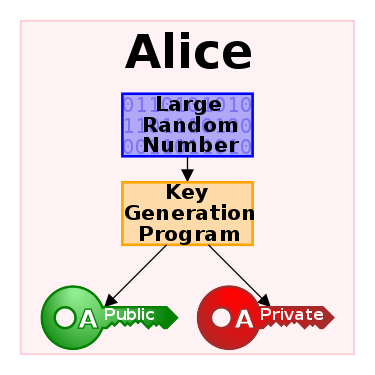


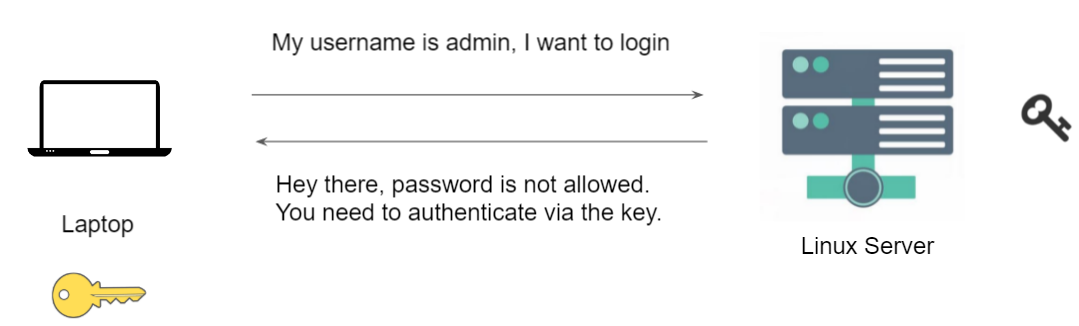
4.4 Key Based Authentication

In this type of authentication, there are two special keys that are generated.

One key is called a Public Key and the second key is called a Private key.

If the public key is stored in server and is used as authentication mechanism, only the corresponding private key can be used to successfully authenticate.

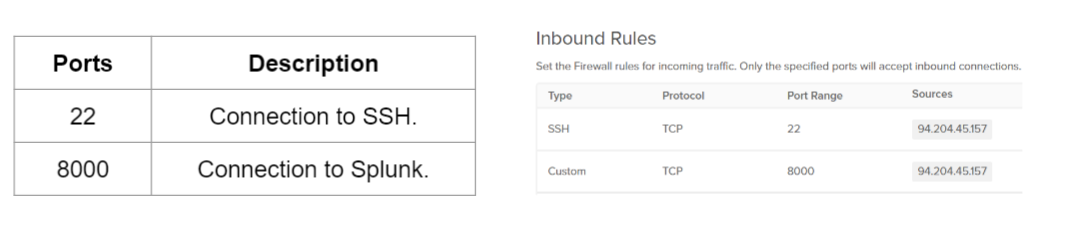




4.5 Firewall Rules

We do not want the entire internet to connect to our server.

With the help of Firewall, you can restrict the connection to your Splunk instance.



## 