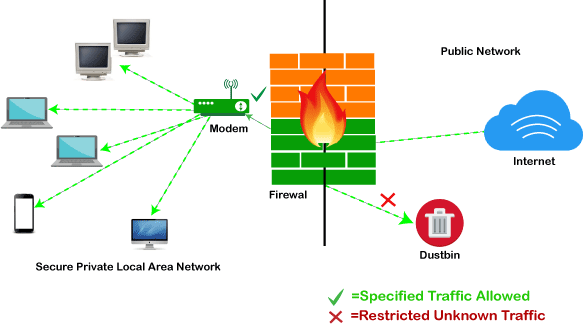
**7.Study of the features of firewall in providing security and to set Firewall Security inwindows.**

AIM:

### 1. Unified Security Management

Organizations must cope with rapidly increasing [network security](https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/) complexity. Most companies’ networks are growing larger and more complex as mobile devices, cloud deployments, and Internet of Things (IoT) devices join traditional user workstations and on-premises servers on the corporate network. At the same time, cyber threats are becoming more sophisticated and numerous. As a result, companies must deploy, monitor, and maintain a growing array of security solutions to manage their cyber risk.

An organization’s [next-generation firewall](https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/) should help to alleviate security complexity, not contribute to it. A firewall with integrated Unified Security Management (USM) functionality enables an organization’s security team to easily and efficiently manage and enforce security policies across their entire network environment. This allows the security team to keep up with the company’s expanding digital attack surface and minimize the organization’s cyber risk.



### #2. Threat Prevention

The longer that a cyber threat has access to an organization’s network, the more expensive it will be to remediate it. Cyberattacks can cause damage and additional expense in a number of different ways. Exfiltration of sensitive data can result in legal and regulatory penalties, ransomware can

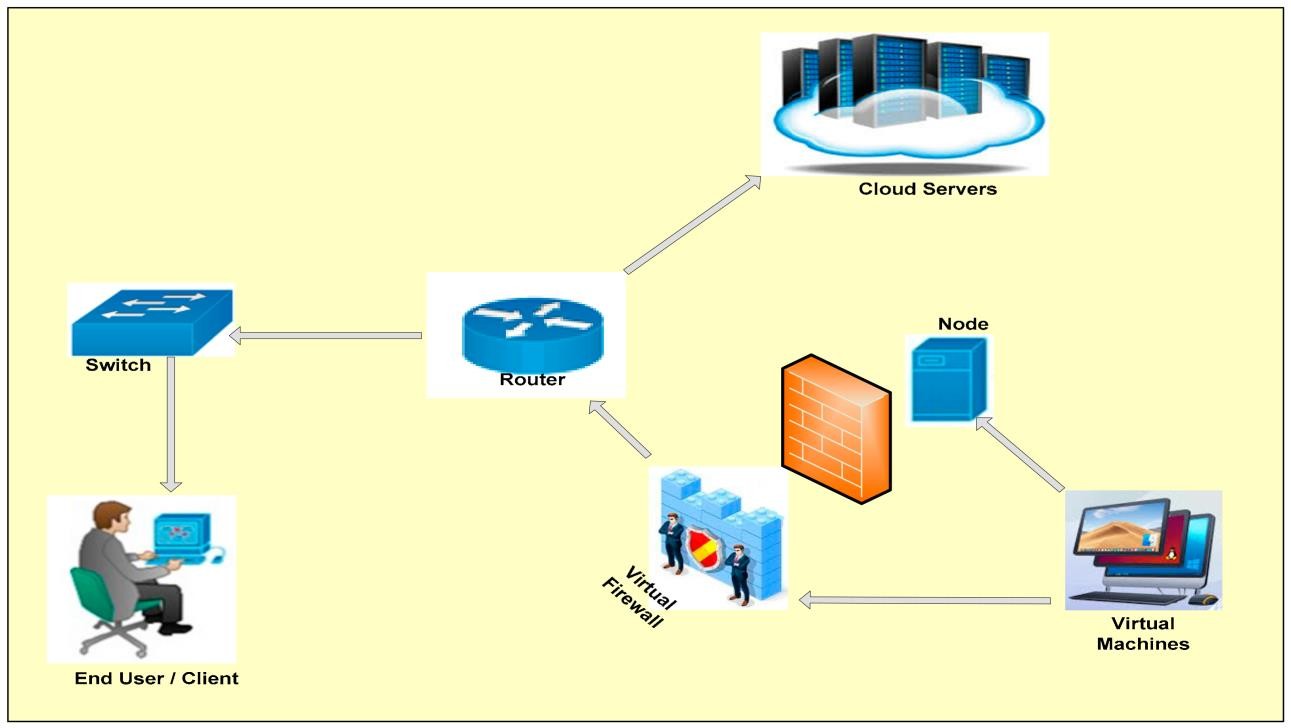
decrease productivity and cause a loss of profits, and even simple malware often has persistence mechanisms designed to make it difficult and time-consuming to remove from a system.

Minimizing the damage that a cyberattack can cause to a network requires threat prevention. By identifying and blocking an attack before it crosses the network boundary, an organization nullifies the threat it poses to the network. This is why a network firewall with integrated threat prevention functionality – including anti-phishing, anti-malware, anti-bot, and integration with high-quality threat intelligence feeds – is an essential component of an organization’s cybersecurity strategy.

### #3. Application and Identity-Based Inspection

Digital transformation efforts mean that an organization’s network landscape is constantly evolving. New applications are deployed on the corporate network to accomplish certain goals, and others are phased out when they become obsolete. Different applications require different policies. Some applications may be high-priority traffic, while others should be blocked, throttled, or otherwise managed on the network. An organization’s next-generation firewall should be capable of identifying the application that generates a particular stream of traffic and applying application-specific policies to that traffic.

Organizations are also composed of a number of individuals with different job roles and responsibilities. An organization’s security policies should also be configurable based upon the identity of the user. Employees within an organization should have access to different systems and be able to use varying sets of applications. A firewall should support policy creation and enforcement based upon user identity.



### #4. Hybrid Cloud Support

Almost all organizations are using cloud computing, and the vast majority are using a hybrid cloud deployment. Private and public cloud deployments have different security requirements, and it is necessary for an organization to be able to enforce consistent security policies across cloud-based environments hosted by multiple vendors.

For this reason, an organization’s next-generation firewall should incorporate hybrid cloud support. The firewall should be easily deployable and scalable in any major cloud environment and enable an organization’s security team to manage all of their security settings from a single console. According to Gartner, [99% of cloud security failures through 2025 will be the customer’s fault](https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/), a problem that the company’s firewall should help the organization to avoid.

### #5. Scalable Performance

Many organizations have transitioned to cloud-based infrastructure due to its increased scalability and flexibility. Ultimately, we want the benefits of the cloud, in the cloud and on-premises. In the cloud this simply means choosing a NGFW template. In regards to on-premises, this means looking beyond legacy HA clustering solutions.

Hyperscale is the ability of an architecture to scale appropriately as increased demand is added to the system. This involves the ability to seamlessly provision and add more resources to the system that make up a larger distributed computing environment. Hyperscale is necessary to build a robust and scalable distributed system. In other words, it is the tight integration of storage, compute, and virtualization layers of an infrastructure into a single solution architecture.

## Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome).

AIM:

## Google Chrome:

* **Enable phishing and malware protection:** Make sure that Chrome’s phishing and malware protection feature is enabled under the “Privacy” section. This feature will warn you if a site you’re trying to visit may be phishing or contain malware.
* **Turn off instant search:** The Instant search feature should be turned off for optimal security. While it offers some convenience in searching, having this feature enabled means that anything you type in the address bar is instantly sent to Google.
* **Don’t sync:** Disconnect your email account from your browser under the “Personal Stuff” tab. Syncing your email account with your Chrome browser means that personal information such as passwords, autofill data, preferences, and more is stored on Google’s servers. If you must use sync, select the “Encrypt all synced data” option and create a unique passphrase for encryption.
* **Configure content settings:** Click “Content settings” under the “Privacy” section and do the following:
* *Cookies:* Select “Keep local data only until I quit my browser” and “Block third-party cookies and site data.” These options ensure that your cookies will be deleted upon quitting Chrome and that advertisers will not be able to track you using third-party cookies.
* *JavaScript:* Select “Do not allow any site to run JavaScript.” It is widely recommended that JavaScript be disabled whenever possible to protect users from its security vulnerabilities.
* *Pop-ups:* Select “Do not allow any site to show pop-ups.
* *Location:* Select “Do not allow any site to track my physical location.”
* **Configure passwords and forms settings:** Disable Autofill and deselect “Offer to save passwords I enter on the web” under the “Passwords and forms” section. Doing so will prevent Chrome from saving your logins, passwords, and other sensitive information that you enter into forms.

## Mozilla Firefox:

* **Configure privacy settings:** Under the “Privacy” tab, complete the following steps. These measures ensure that Firefox is storing only as much of your information as it needs to function normally.
* Select “Use custom settings for history.”
* Deselect “Remember my browsing and download history.”
* Deselect “Remember search and form history.”
* Deselect “Accept third-party cookies.”
* Set cookie storage to “Keep until I close Firefox.”
* Select “Clear history when Firefox closes.”
* **Configure security settings:** Under the “Security” tab, choose the following settings. These steps prevent Firefox from saving your passwords and keep you from visiting potentially harmful sites.
* Verify that “Warn me when sites try to install add-ons,” “Block reported attack sites,” and “Block reported web forgeries” are all selected.
* Deselect “Remember passwords for sites.”
* **Disable javaScript:** Deselect “Enable JavaScript” under the “Content” tab. JavaScript is notorious for containing security vulnerabilities and it is recommended that users only enable it for trusted sites.
* **Enable pop-up blocking:** Verify that “Block pop-up windows” is selected under the “Content” tab. This feature should be turned on by default as it protects users from unwarranted advertisements and windows.
* **Don’t sync:** Avoid using Firefox Sync. By doing so you prevent Firefox from storing your logins, passwords, and other sensitive information.
* **Turn on automatic updates:** Verify that “Automatically install updates” is selected in the “Update” tab under “Advanced.” Doing so will ensure that your browser receives critical security updates. Verify that “Automatically update Search Engines” is selected as well.
* **Use secure protocols:** Verify that “Use SSL 3.0” and “Use TLS 1.0” are selected in the “Encryption” tab under “Advanced.”

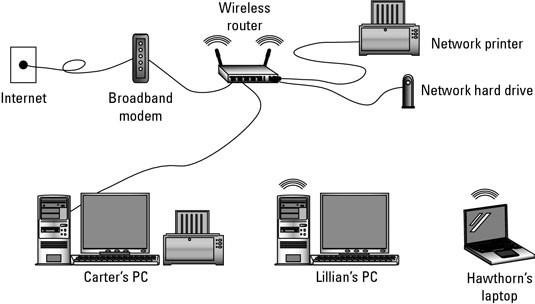


### Study of different wireless network components and features of any one of the Mobile Security Apps.

**AIM:**

### Introduction

As long as you have all the hardware, you can quickly set up any wireless network. Here is everything you need to know about the hardware you need to have in place before you use Windows to configure the wireless network. There are two types of wireless networks: infrastructure and ad hoc. The *infrastructure* network is most likely the type of wireless setup youhave in your home or office. It’s laid out similarly to a wired network, butwithout wires.



The basic wireless, peer-to-peer network consists of these components:

### Wireless Network Adapters

Wireless network adapters (also known as *wireless NICs* or *wirelessnetwork cards*) are required for each device on a wireless network. All

newer laptop computers incorporate wireless adapters as a built-in feature of the system.

No wireless hardware other than adapters is required to build a small local network. However, to increase the performance of network connections, accommodate more computers, and increase the network's range, additional types of hardware can be deployed.

### Wireless Routers

Wireless routers function comparably to traditional routers for wired Ethernet networks. One generally deploys wireless routers when building an all-wireless network from the ground up.

Similar to routers, access points allow wireless networks to join an existing wired network. One typically deploys access points when growing a network that already has routers installed. In home networking, a single access point (or router) possesses sufficient range to span most residential buildings. Businesses in office buildings often must deploy multiple access points and/or routers.

### Wireless Antennas

Access points and routers often utilize a Wi-Fi wireless antenna that significantly increase the communication range of the wireless radio signal. These antennas are optional and removable on most equipment. It's also possible to mount aftermarket add-on antennas on wireless clients to increase the range of wireless adapters.

### Wireless Repeaters

A wireless repeater connects to a router or access point. Often called signal boosters or *range expanders*, repeaters serve as a two-way relay station for wireless radio signals, helping clients otherwise unable to receive anetwork's wireless signal to join.

**Wire-based connections:** Almost every wireless router has one or more standard, wire-based Ethernet port. One port is used to connect the router toa broadband modem. Other Ethernet ports might be also available, allowing you to connect standard wire-based networking to the wireless hub.

**Wireless NIC:** Your computer needs a wireless Network Interface Card, or NIC, to talk with the wireless router. A laptop comes standard with a wireless NIC, but for a desktop PC you have to get a wireless NIC as an option. It’s installed internally as an expansion card, or you can use one of the various plug-in USB wireless NICs.

When evaluating mobile devices and apps for security, developers should ask themselves the following questions.

* How do users obtain a particular app?
* Should a firm create its own app store?
* How is an app vetted before it is offered for sale?
* How is an app protected against malware?
* How can users tell the difference between a legitimate app and a fake?
* How easily can automatic update features get hijacked?
* What measures exist to control the risk of device jail breaking?
* What kind of permissions should a particular app ask for?
* Can any other apps keep track of when, where, and how a certain appis used? Let us now discuss the features of a popular mobile security app called CM Security.

### 1.2.1 CM Security

CM security (Clean Master) is an all-singing, all-dancing option made by Cheetah Mobile that brings you a whole host of anti-virus and security features for free - as long as you don't mind a few ads.

### Features of CM security

Feature-wise it tries to offer everything - anti-virus, browsing protection, battery saving, privacy protection of apps, the whole lot. It takes pretty much the same simplified approach to each of those things too. CM security identifies what it describes as threats and then asks what you want to do about them in a straightforward way.

That might disappoint people who love spending time in settings menus, but you're not going to be doing that with CM Security. One potential drawback, however, is that it's relentless in nagging you about other aspects of your device and other apps made by Cheetah that can help you out. But again, it's free, so it's hard to complain too much.

