**Network**

**Security**

**Class 9**

**Lab 25**

|  |
| --- |
| Lab Objectives:  * Network Security Basic |

# What is Network Security?

## Network security is the practice of preventing and protecting against unauthorized intrusion into corporate networks.



## Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure,

## IMG_256thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

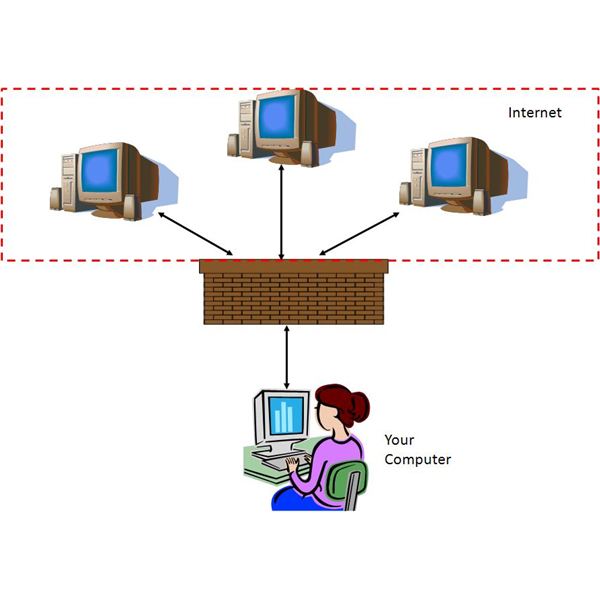
# Network Security Basics

## Network security consists of:

## **Protection**: You should configure your systems and networks as correctly as possible

## **Detection**: You must be able to identify when the configuration has changed or when some network traffic indicates a problem

## **Reaction**: After identifying problems quickly, you must respond to them and return to a safe state as rapidly as possible



# Network security methods

## To implement this kind of defense in depth, there are a variety of specialized techniques and types of network security you will want to roll out. Cisco, a networking infrastructure company, uses [the following schema to break down the different types of network security](https://www.cisco.com/c/en/us/products/security/what-is-network-security.html), and while some of it is informed by their product categories, it's a useful way to think about the different ways to secure a network

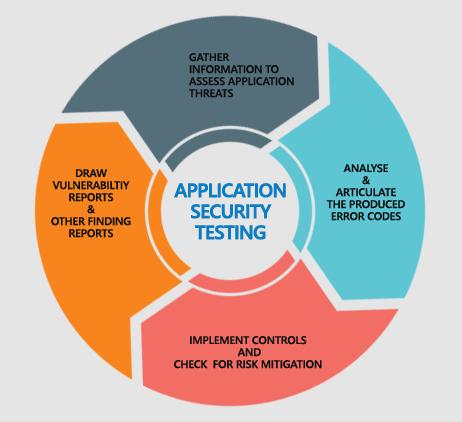
## **Access control:** You should be able to block unauthorized users and devices from accessing your network. Users that are permitted network access should only be able to work with the limited set of resources for which they've been authorized.



## **Anti-malware:** Viruses, worms, and trojans by definition attempt to spread across a network, and can lurk dormant on infected machines for days or weeks. Your security effort should do its best to prevent initial infection and also root out malware that does make its way onto your network.



## **Application security**: Insecure applications are often the vectors by which attackers get access to your network. You need to employ hardware, software, and security processes to lock those apps down.



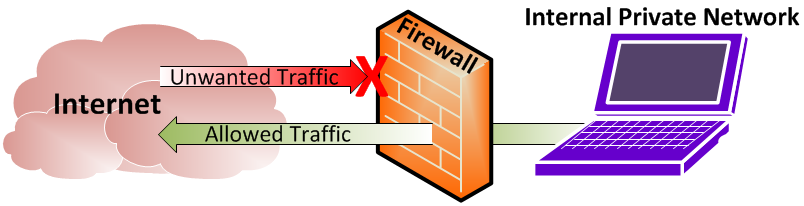
## IMG_256**Behavioral analytics:** You should know what normal network behavior looks like so that you can spot anomalies or breaches as they happen.

## IMG_256**Data loss prevention**: Human beings are inevitably the weakest security link. You need to implement technologies and processes to ensure that staffers don't deliberately or inadvertently send sensitive data outside the network.

## **Email security:** [Phishing](https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html) is one of the most common ways attackers gain access to a network. Email security tools can block both incoming attacks and outbound messages with sensitive data.



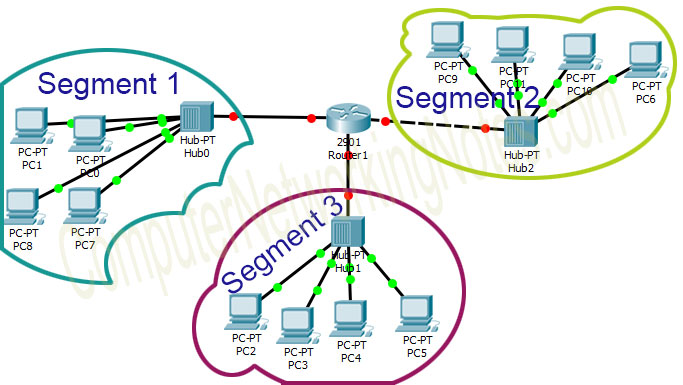
## **Firewalls**: Perhaps the granddaddy of the network security world, they follow the rules you define to permit or deny traffic at the border between your network and the internet, establishing a barrier between your trusted zone and the wild west outside. They don't preclude the need for a defense-in-depth strategy, but they're still a must-have.



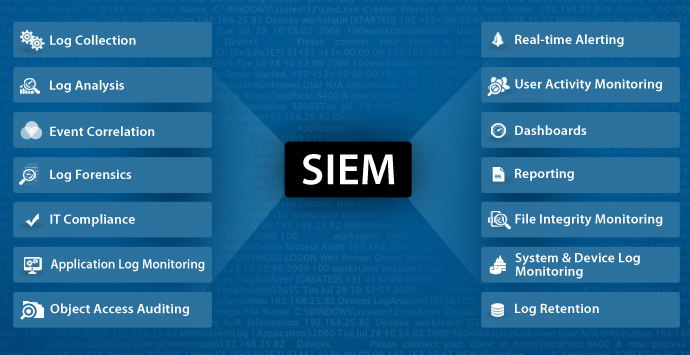
## IMG_256**Intrusion detection and prevention**: These systems scan network traffic to identify and block attacks, often by correlating network activity signatures with databases of known attack techniques.

## IMG_256**Mobile device and wireless security:** Wireless devices have all the potential security flaws of any other networked gadget — but also can connect to just about any wireless network anywhere, requiring extra scrutiny.

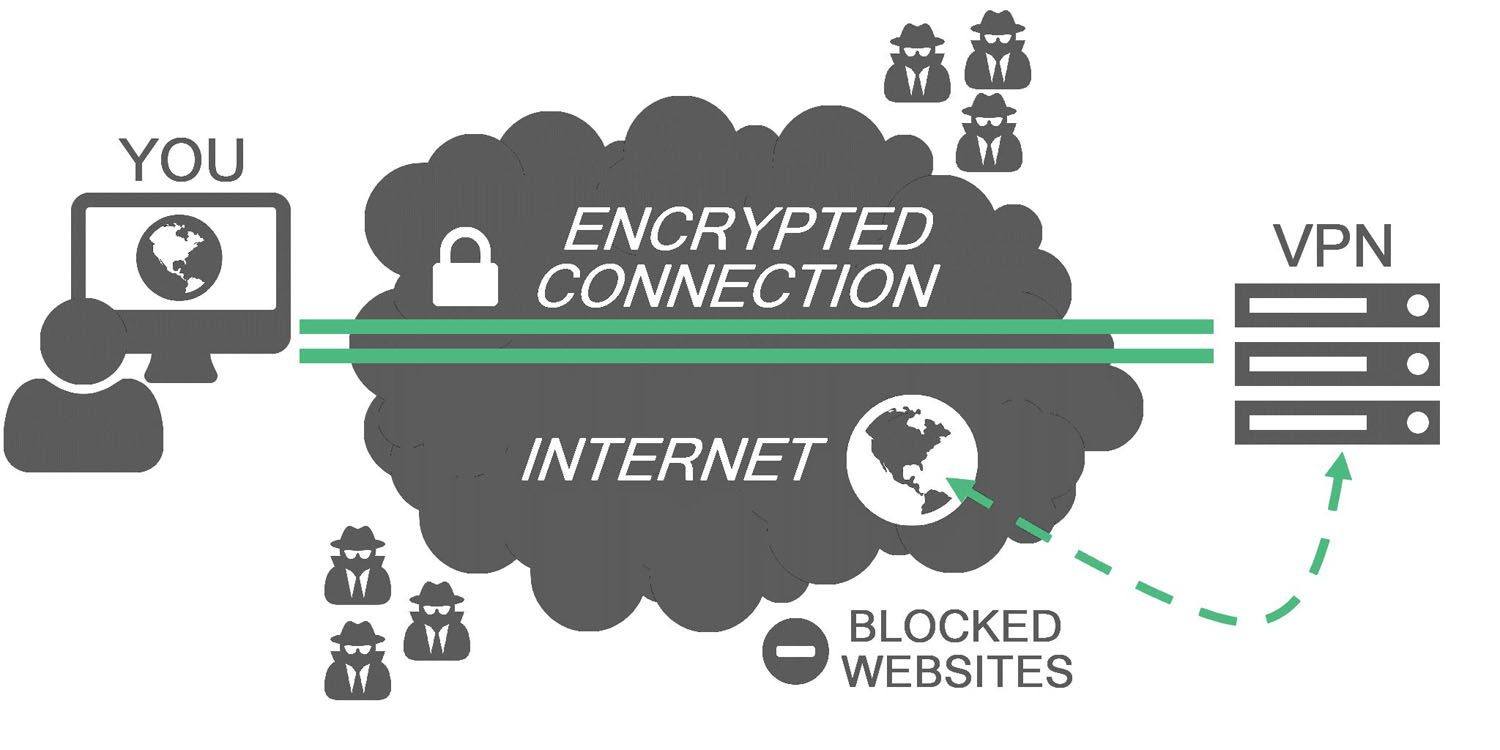
## **Network segmentation:** Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier.



## **[Security information and event management](https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html)** [(SIEM)](https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html): These products aim to automatically pull together information from a variety of network tools to provide data you need to identify and respond to threats.



## **VPN**: A tool (typically based on IPsec or SSL) that authenticates the communication between a device and a secure network, creating a secure, encrypted "tunnel" across the open internet.



## **Web security**: You need to be able to control internal staff's web use in order to block web-based threats from using browsers as a vector to infect your network.



## To know more about Network Security you have to know the basic of Cyber Security and Ethical Hacking concepts first. From next Lab we will learn the basic of ethical hacking.