

# Exploration: Networking Security Introduction

## Introduction

---



In this exploration we will talk about Network Security. It is another of those huge topics, which would take an entire career to master. In this brief introduction we will look at some of the problems, some of the policies that companies use, and some of the mechanisms that can give us some level of security.

The internet has enabled new types of crime. Since the beginning there has been explosive growth in the problem. Part of the issue is that defensive measures are mostly reactive instead of proactive. There are always new types of threats. So new, in fact, that many of the “crimes” aren’t even illegal yet. Also, many crimes are virtually untraceable, or are untouchable (as they originate in other countries).

Finally, there are all kinds of perpetrators. Criminal hackers, terrorists, sure. But perhaps your co-worker is about to click on an email link and unleash a virus on your company? Maybe a foreign government has been engaging in espionage to get business secrets? As pervasive, and expensive, as the problem seems to be, what can be done?

## Security Policies

---

Trying to make a website or organization secure is a never-ending task. It is imperative to work with a comprehensive security policy. A security policy for an organization will include stored information, transmitted info, email and contact lists, infrastructure, and more.

The costs and benefits of securing stored info should be part of the policy. A spectrum of sensitivity exists for information. The most critical and important documents should be encrypted and access should be limited. Less sensitive information may be accessible by all the members of the organization.

A security policy should recognize that Individuals play an enormous role in security. They must be educated about the dangers of email schemes, websites, browsers, computer updates, virus scans, and more. It is also important for individuals to understand the risks and procedures for taking information and computing devices outside the organization and using them to communicate.

The main components of Data Security include:

- Data integrity
  - Data should be transmitted unchanged
  - Stored data should be "safe"
- Data availability
  - Authorized users should have access
  - Access should not be interrupted
- Data confidentiality
  - Only authorized users should have access
  - No snooping, wiretapping, etc.
- Privacy
  - User identity is protected
  - Private transactions are protected

There are many different types of security mechanisms. We will look at perimeter security and encryption, VPN's, and a few others. There are others, including digital signatures, message authentication codes, hashing, and more. Your text has more examples.

## Virtual Private Networks (VPN's)

---

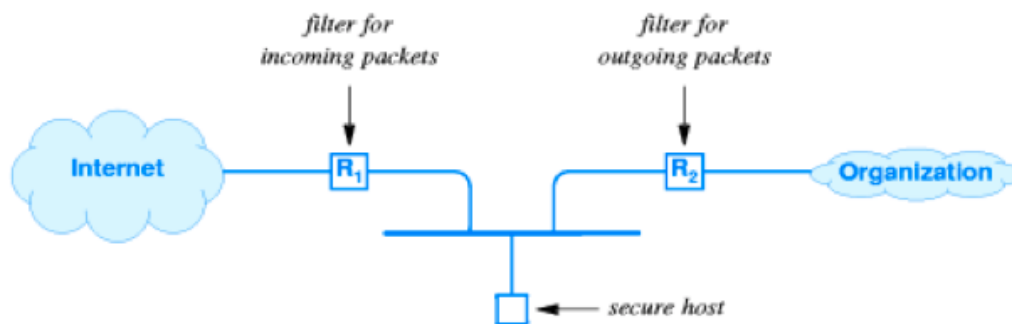
VPN's work by routing your internet traffic through a VPN server. The link between your computing device and the VPN server is encrypted, so that no usable information is available to any intermediary (such as a firewall or internet filter). A business or organization may employ a VPN to secure information from mobile workers to their servers.

Commercial VPN services offer a secure link from your computing device to their servers. From there, the data is unencrypted and passed on to the internet and the final destination. The destination server will see your requests as coming from the VPN network, thus hiding your own IP address and network info.

VPN's have enjoyed a rise in popularity recently, both in business and for personal use. Many companies exist that offer free VPN access. It should be said that any company that will receive the bulk of your internet traffic should be trustworthy to an extraordinary level.

## Perimeter Security

---



Perimeter Security is the most common scheme for protecting data in an institution. Typically firewalls are employed at internet access points. These firewalls use packet filtering techniques to intercept packets that do not conform to security policies. They may filter out packets from known malicious sites, packets that contain malicious code, or even benign packets that are trying to do things that aren't allowed.

If the filters intercept packets that do not conform to known policies, they can send these packets to a secure host for analysis. If the packets cannot be matched to a known policy, then the firewall can tell the secure host to update its policies, or the packet can be quarantined for further analysis, or dropped. This kind of system can check both incoming and outgoing packets for attachments or other malware.

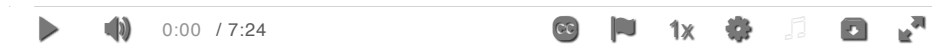
Firewalls can't protect against internal threats including malware delivered through USB keys or through malicious actors. Protection from active internal threats is an area of ongoing research. Efforts focus on ways to detect unusual activity, and isolate the hosts involved before malware can spread.


This concludes our brief introduction to Network Security. Be sure to watch the video lecture below for more details, including a discussion about the economic impact of cyber crime. Then head to the included Self-Check exercises to test your knowledge.

## Video Lecture


---

## Security Part 1



([PDF \(https://oregonstate.instructure.com/courses/1798856/files/83165096/download?wrap=1\)](https://oregonstate.instructure.com/courses/1798856/files/83165096/download?wrap=1).) 

(<https://oregonstate.instructure.com/courses/1798856/files/83165096/download?wrap=1>).|[PPT](#)


(<https://oregonstate.instructure.com/courses/1798856/files/83165076/download?wrap=1>). 

(<https://oregonstate.instructure.com/courses/1798856/files/83165076/download?wrap=1>).)

## Self-Check Exercises

---

What are some considerations which might be made before instituting a security policy at a company?

 Turn

Card 1 of 3



Drag the words into the correct boxes

What are some of the major components of networking security?

Availability

Intruders should not be able to understand the contents of a message.

Authentication

Intruders should not be able to change the contents of a message, without the end users being aware of it.

Confidentiality

Integrity

End users should be able to verify they are actually speaking to whom they think they are speaking to.

Services should be accessible, and not interrupted by attacks (resilience to DDoS, etc...)