CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 8: Anti-Virus, Anti-Spyware and Firewalls

Get the Right Software

- The right software is critical to protect your PC from malware.
- More than a single piece of software. You're going to need a suite of tools → often they won't come pre-equipped on your system.
- Two critical tools are Anti-Virus and Firewalls → we will look at these in this lecture.

Anti-Virus

Anti-Virus Software

- Start with the most basic protection: anti-virus software.
- This software will protect your system against some of the most common pests, including viruses, trojans, and worms.
- Your anti-virus software should run constantly and provide real-time protection to stop an infection before it happens.
- Your PC may have come with anti-virus software installed, probably either from McAfee or Norton.
- Don’t forget to renew.

Anti-Virus Software

- A variety of strategies are typically employed when it comes to virus detection.
- Anti-Virus (AV) Software is not guaranteed to detect threats → detection rates on the Zeus family of trojans can be as low as 40%
- As with other tools AV can have:
  - ➢ True positive → actual virus detected
  - ➢ False positive → benign file detected as virus
  - ➢ True negative → benign file detected as benign
  - ➢ False negative → virus missed!

Anti-Virus Detection

AV Software Detection

- There are several methods which antivirus software can use to identify malware.
- Three important ones are:
  1. Signature-based Detection
  2. Malicious Activity Detection
  3. Heuristic-based Detection

AV Signature Based Detection

Traditionally, antivirus software heavily relied upon signatures to identify malware.

- Cannot defend against malware unless samples have already been obtained and signatures created.
- AV scan → checks the contents of a file against a dictionary of virus signatures.

A virus signature is the viral code.

AV Signature Based Detection

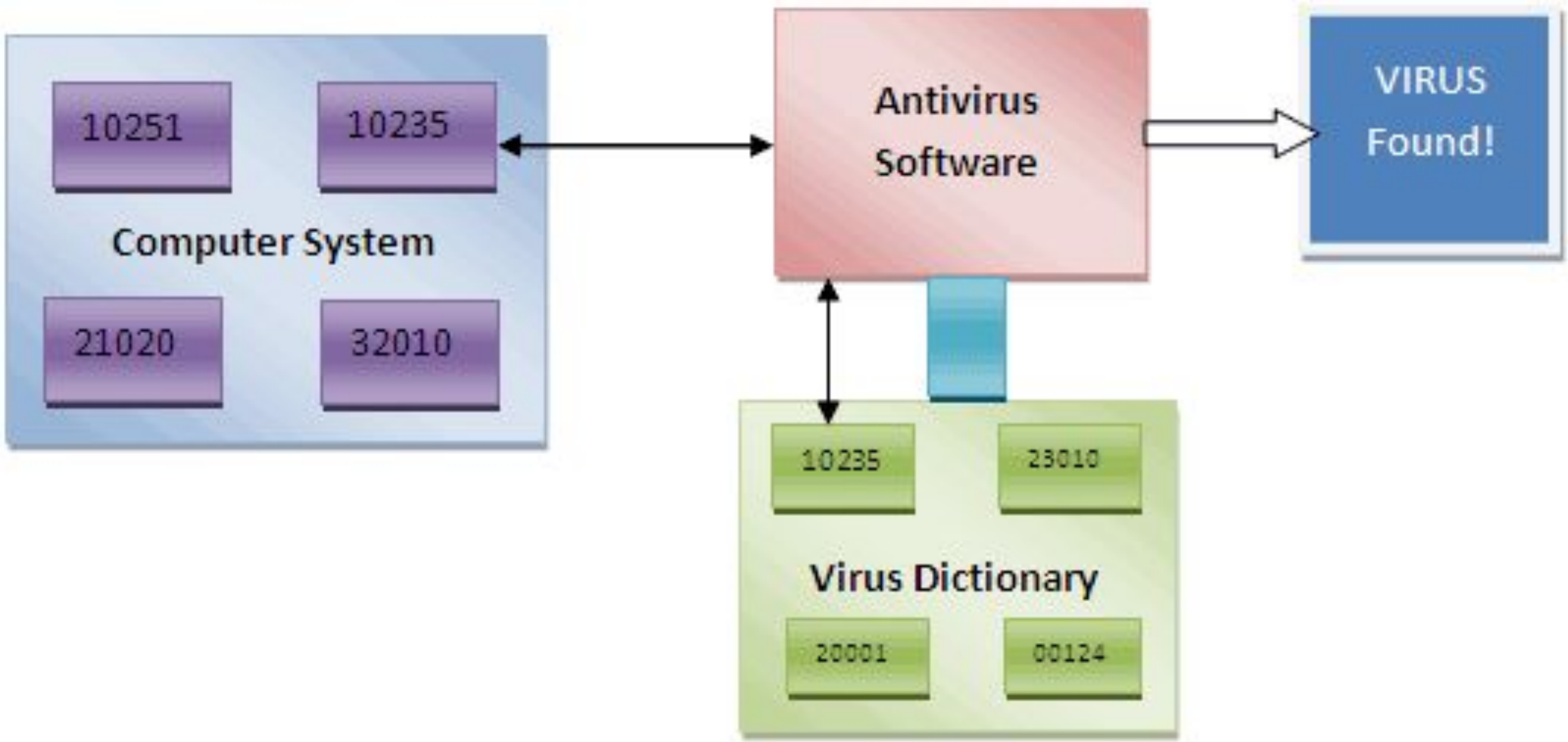
If a virus signature is found in a file the antivirus software can resort to some combination of quarantine, repair or deletion.

- **Quarantining** a file will make it inaccessible. Encrypting the file is a good quarantining technique because it renders the file useless without the encryption key.
- **Repair** is when the AV will try to delete the pest and repair the file.
- **Deletion** → This is the best solution if the pest doesn't live inside one of your programs or data files.

AV Signature Based Detection

- With new viruses each day, the signature-based detection approach requires frequent updates of the virus signature dictionary → often a background process allowing the virus to be analysed and the signature added to the dictionary.
- Signature-based AV typically examines files when the computer's operating system creates, opens, closes, or e-mails them so it can detect a known virus immediately.

AV – Signature Based Detection



AV Signature Based Detection

- Polymorphic and metamorphic viruses → defeat simple signature based detection

- A solution to this is **whitelisting** → Rather than looking for only known bad software, prevent execution of all computer code except that which has been previously identified as trustworthy by the system administrator.

AV Malicious Activity Detection

- The suspicious behavior approach does not attempt to identify known viruses, but instead monitors the behavior of all programs.
- If one program tries to write data to an executable program, for example, the antivirus software can flag this suspicious behavior, alert a user and ask what to do.
- The suspicious behavior approach provides protection against zero day viruses that are not yet in the dictionary.
- However, it can also sound a large number of false positives and users may become de-sensitized to the warnings.

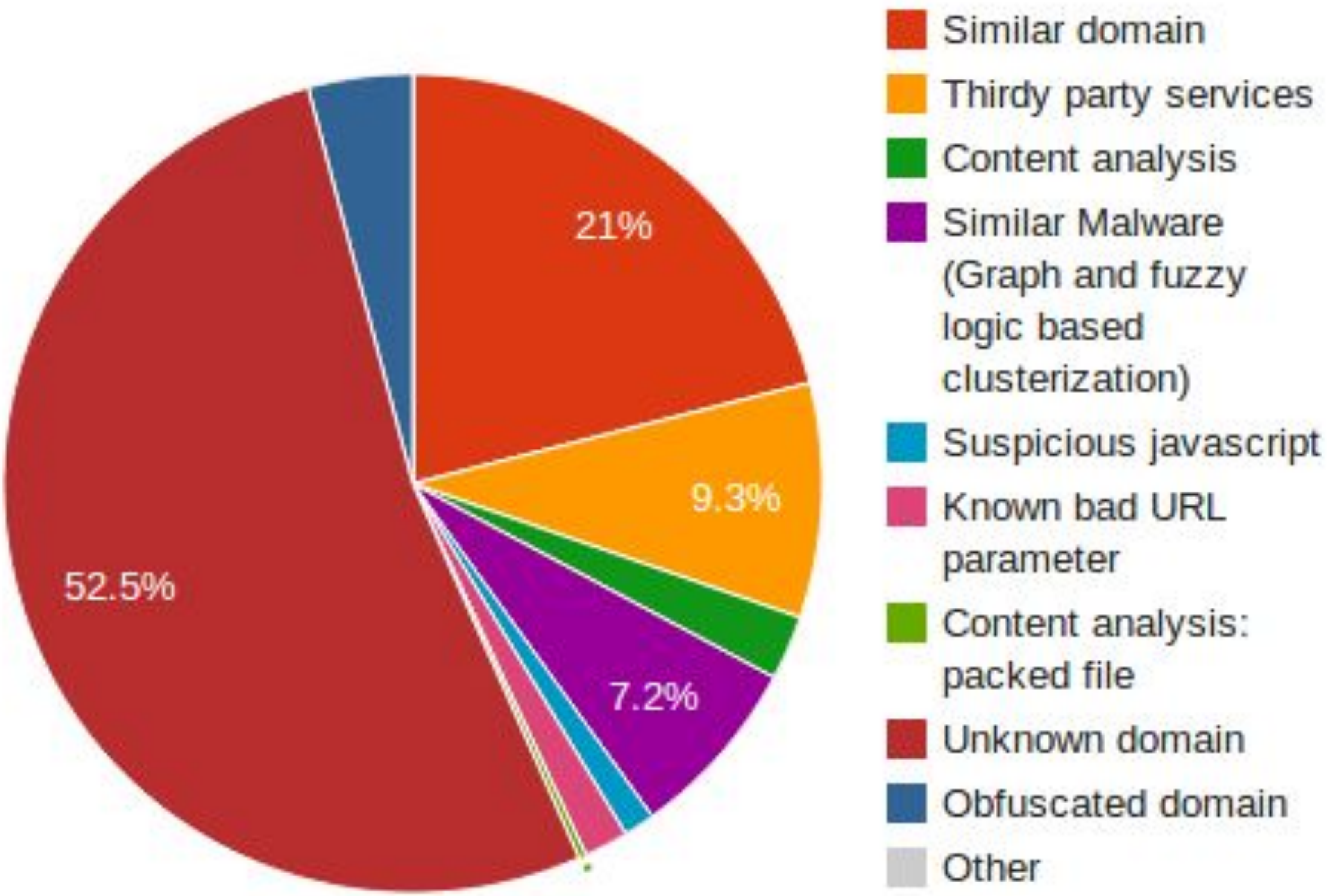
AV – Heuristic Detection

Some more sophisticated antivirus software uses heuristic analysis to identify new malware or variants of known malware.

Three methods are used:

- File Analysis
- File Emulation
- Generic Signatures

AV – Heuristic Detection



AV – Heuristic Detection

File Analysis

- File analysis is the process by which antivirus software will analyze the instructions of a program.
- Based on the instructions, the software can determine whether or not the program is malicious.
- For example, if the file contains instructions to delete important system files, the file might be flagged as a virus.
- Can trigger many false positives.

AV – Heuristic Detection

File Emulation

- This runs the target file in a virtual system environment, separate from the real system environment.
- The antivirus software would then log what actions the file takes in the virtual environment.
- If the actions are found to be damaging or malicious, the file may be marked a virus.

Sandboxing is a form of software virtualization that lets programs and processes run in its isolated virtual environment thus protecting the OS from unexpected or malicious activity.

AV – Heuristic Detection

Generic Signatures

- Signature-based detection → it is possible for a user to be infected with new malware for which no signature exists yet.
- Generic signatures → can identify new viruses or variants of existing viruses by looking for known malicious code (or slight variations of such code) in files.
- Entire families of viruses can be protected against!

Anti-Virus Tips

Anti-Virus Software

How to stay free of viruses

Use real-time protection

- You want to catch a virus before it infects you, not after it does its damage. You must enable real-time virus protection—in other words, have the anti-virus software running at all times so that when a virus attempts to infect your machine, the software automatically kills it.

Scan e-mail

- Many pieces of malware spread via infected email, so make sure your anti-virus software scans incoming email. For safety's sake, have it scan outgoing email as well.

Scan instant messenger attachments

- Increasingly, pests spread via instant messenger attachments. Make sure your anti-virus software scans instant messenger attachments.

Anti-Virus Software

Schedule virus scans

- Even with real-time protection, a virus may make it onto your system. So, you need to scan your system regularly for viruses.

Use Automatic Updates

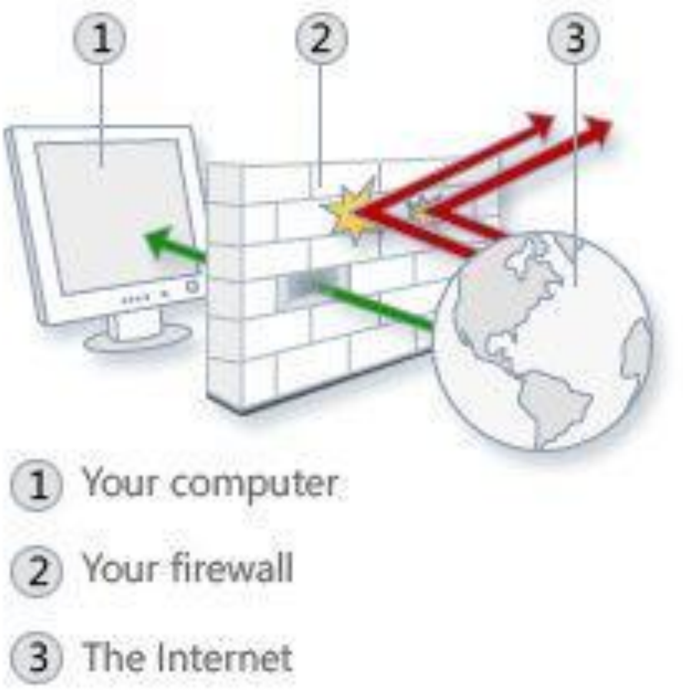
- You should set your anti-virus software to check for new definitions automatically. That way, you won't have to remember to do it yourself.
  - As soon as new definitions are released, your software will get a copy.
  - So, no matter which software you use, make sure it checks for virus definition updates automatically.

Kill Viruses

- When the anti-virus software finds a virus, it can either quarantine, repair or delete the virus

Firewalls

Firewalls



Just as a brick wall can create a physical barrier, a firewall creates a barrier between the Internet and your computer

Firewalls

- Firewalls can block unauthorised programs from getting onto your PC, and also stop them from making outbound connections without your knowledge.
- A Firewall is an important layer in your Defense in Depth approach to protecting your PC.
- Windows 7 onwards comes with a free firewall which has been recommended by security professionals as a much needed upgrade to previous versions.
- You can also download a third party Firewall such as McAfee Personal Firewall, Norton Personal Firewall or ZoneAlarm.

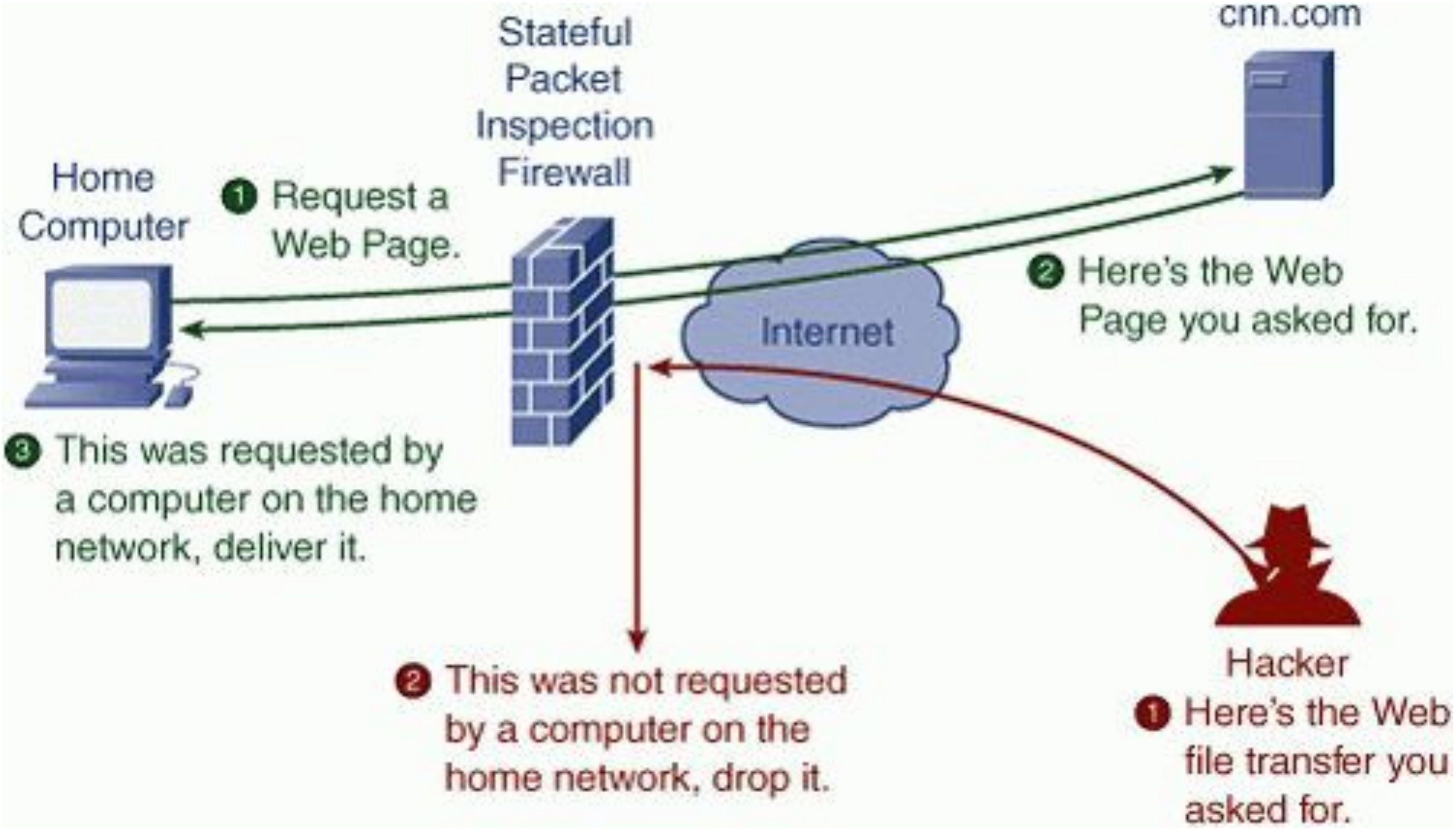
Firewalls

- All firewalls work in a similar manner. When a program tries to access the Internet, either outbound or inbound, you receive a warning.
- If the firewall recognises the program, it tells you whether it's safe or dangerous.
- You then tell the firewall to let the program access the Internet if it is safe.
- Firewalls remember your decisions for future operations if configured to do so.

Firewalls

- If the firewall fails to immediately recognise the program, you'll get a link to a site offering more information.
- As a general rule, if neither you nor the firewall recognises the program, don't let it access the Internet.
- You also need to "**train**" your firewall and tell it which programs you want to allow to access the Internet.

How Personal Firewalls Operate



1 Request a Web Page.

2 Here's the Web Page you asked for.

3 This was requested by a computer on the home network, deliver it.

1 Here's the Web file transfer you asked for.

2 This was not requested by a computer on the home network, drop it.

Firewalls – Sorting Data

Firewalls employ a few different manners of sorting data including:

- **Packet filtering** - a simple method, packet filtering entails analysing small packets or chunks of data through a series of filters/rules. (Susceptible to IP Spoofing)
- **Proxy service** - all of the data entering or leaving the network is first sent to the Proxy server. It hides the true network addresses.
- **Stateful inspection** - this method looks at parts of packets to see if they match specific characteristics that are allowable. It tracks all of the network connections and distinguishes which are valid packets for different types of connections.

Firewall Analysis

Firewall analysis is based on four mechanism:

1. Address,
2. Port,
3. Protocol,
4. Application.

Firewall Analysis

- ***Address*** - Every computer or network gateway on the Internet has an IP (Internet Protocol) address, such as 126.1.228.4. They also have names corresponding to those addresses, known commonly as 'domain names,' like mail.yahoo.com. Firewalls can block particular sites from sending data through them based on their IP addresses. This can go as far as blocking certain subnets (126.1.228.x), meaning nothing from any computer in that realm of addresses will get through.

Firewall Analysis

- ***Protocol*** - Certain types of data conform to different communication standards or protocols. For example, the HTTP (Hyper Text Transfer Protocol)
- ***Port*** - Firewalls can block or restrict transmission based on a port or series of ports. More common ports closed off are Telnet(23) and FTP(21) ports since more secure methods of transmission are available
- ***Application*** - Is it an Instant Messenger client that's sending the data? An interactive game? Or is it attempted access by some unknown program, spyware you didn't know was installed, or some backdoor bot that wants to control your computer? Firewalls can observe the application level as well and warn you of attempted communications.

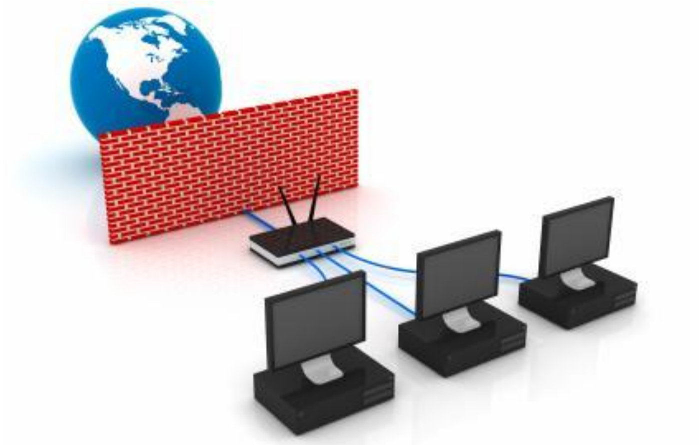
Firewalls – Additional Services

These days Firewalls also have a wide range of additional services to offer their clients:

- Data Encryption – encrypt all data being sent.
- Pop-up Ad Blocking
- Logging/Reporting – Modern firewalls can report in detail what packets came from where, when, and provide analysis as to their purposes.
- Hiding your Presence – Some Firewalls will try to hide your presence to the outside world.
- Email Virus Protection

Firewalls

- Firewall → always launch automatically on startup
- Broadband provides "always-on" connections therefore, most targeted connections → make sure to use a firewall
- Many home routers have firewall capability built in → activate and configure this!



Firewall/AV Examples

webroot
G DATA
K7 Computing
ウイルスセキュリティ
eset
KASPERSKY lab
bitdefender
Norton
from symantec
RISING
LION-STRONG SECURITY
McAfee
Microsoft
Security Essentials
ZONEALARM
by Check Point
VIPRE
from SUNBELT SOFTWARE
ca
Quick Heal
avast!
TREND MICRO
pctools
BULLGUARD
AhnLab
PANDA
SECURITY
AVG
F-Secure