

---

# Stopping the Nasties

---

---

# The Internet



---

# The Internet has many Layers

- Email
  - Web
  - FTP
  - VOIP
  - Your protection must cope with all traffic!!!
-

---

# Levels of Protection

## At the ISP

- Filters and other clever stuff

## At Home

- Modems -- NAT
  - Firewalls
  - Spam Filters
  - Virus Checkers
  - But overall “**Common Sense**”
-

---

# Testing your Protection

## Shields Up

<https://www.grc.com/x/ne.dll?bh0bkyd2>

---

---

# Shields Up



## Shields Up!

- When a star explodes or a Klingon death ray lances out of the darkness, the captain yells two words, "**Shields up!**", and all is well.
  - Spam and virus's are like a Klingon death Ray to your computer, you need protection
-

---

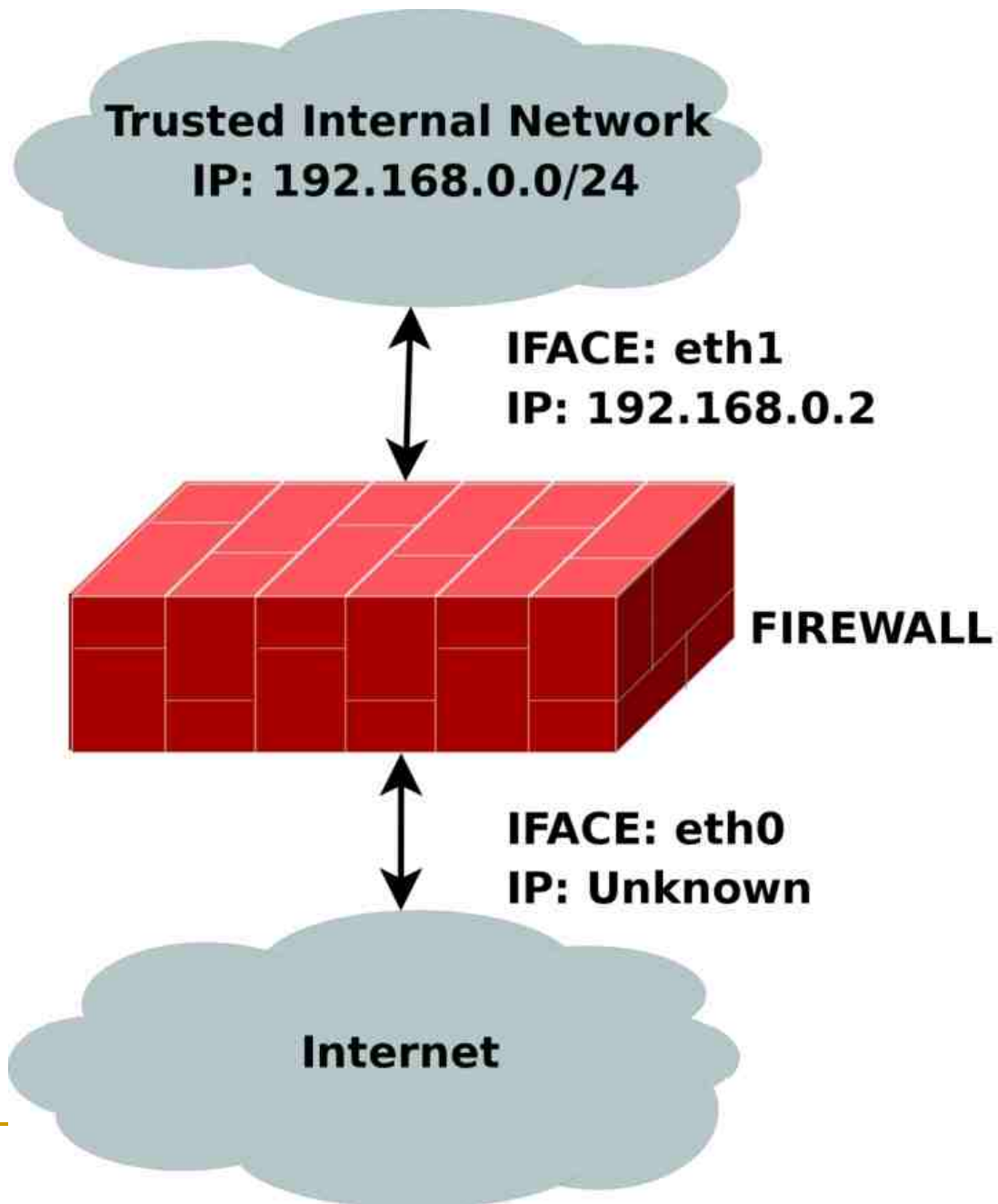
# Firewalls

- A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels.
  - Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust.
-

---

# A Firewall

- A firewall's function within a network is similar to firewalls with fire doors in building construction.
  - In the former case, it is used to prevent network intrusion to the private network. In the latter case, it is intended to contain and delay structural fire from spreading to adjacent structures.
-



---

# Firewalls First Generation - packet filters

- The first paper published on firewall technology was in 1988, when engineers from Digital Equipment Corporation (DEC) developed filter systems known as **packet filter** firewalls.
  - Packet filters act by inspecting the "packets" which represent the basic unit of data transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).
-

---

## Second Generation - "stateful" filters

- Second Generation firewalls do not simply examine the contents of each packet on an individual basis without regard to their placement within the packet series as their predecessors had done, rather they compare some key parts of the trusted database packets.
-

---

# Third Generation - application layer

- The key benefit of is that it can "understand" certain applications and protocols (such as File Transfer Protocol, DNS, or web browsing), and it can detect whether an unwanted protocol is being sneaked through on a non-standard port or whether a protocol is being abused in a known harmful way.
-

---

# Network Address Translation

- NAT adds to security as it disguises the internal network's structure: all traffic appears to outside parties as if it originates from the gateway machine.
  - NAT is built in to most modem routers
-

---

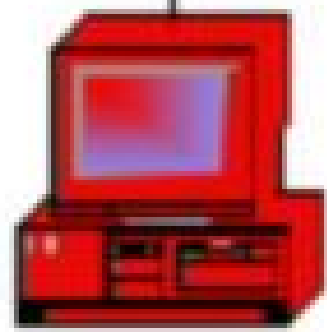
# Network Address Translation

## Benefits

- It prevents malicious activity initiated by outside hosts from reaching those local hosts. This can enhance the reliability of local systems by stopping worms and enhance privacy by discouraging scans. Many NAT-enabled firewalls use this as the core of the protection they provide.
-



Cable/DSL Modem

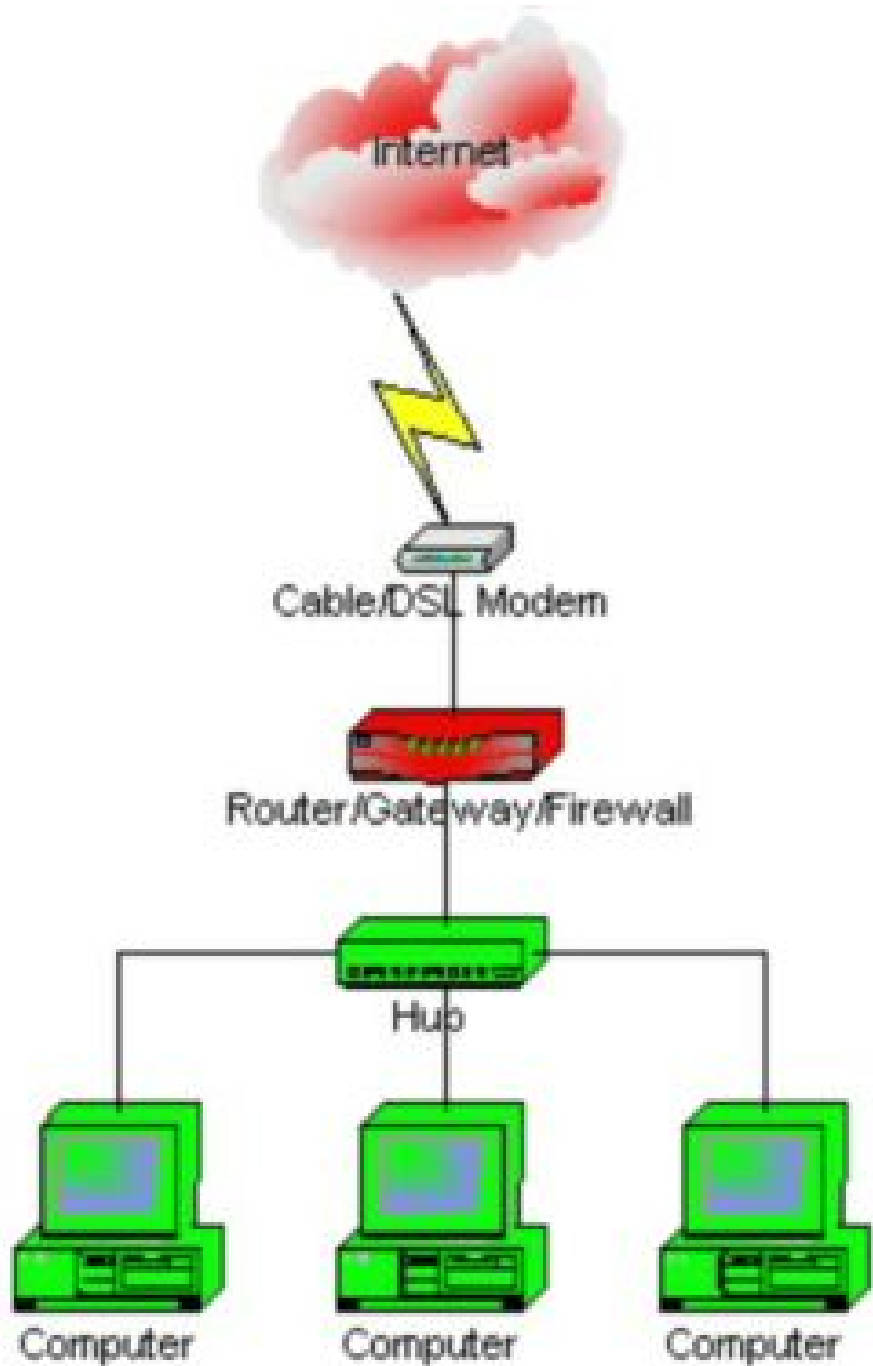


Computer

---

# Simple Setup

- Your cable/DSL modem plugs straight into the computer. The computer is exposed to the public Internet (indicated by the colour red).
  - There is no connection for more than one computer.
  - You only have one IP address from your ISP.
-



---

## **Advantages:**

- All PCs are protected by firewall (indicated by the colour green)
  - File sharing between PCs is safe
  - No additional ISP cost
  - Connect many PCs to home network without additional cost
  - Easy PC configuration due to DHCP server in gateway device
  - Optional additional functionality with gateway-integrated wireless access point, print server, DMZ, content filtering, and more
-

## What Windows Firewall Does and Does Not Do

It does	It does not
<p><b>Help block computer viruses and worms</b> from reaching your computer.</p>	<p><b>Detect or disable computer viruses and worms</b> if they are already on your computer. For that reason, you should also install antivirus software and keep it updated to help prevent viruses, worms, and other security threats from damaging your computer or using your computer to spread viruses to others. For more information, see <a href="#">Frequently Asked Questions About Antivirus Software</a>.</p>
<p><b>Ask for your permission</b> to block or unblock certain connection requests.</p>	<p><b>Stop you from opening e-mail with dangerous attachments.</b> Don't open e-mail attachments from senders that you don't know. Even if you know and trust the source of the e-mail you should still be cautious. If someone you know sends you an e-mail attachment, look at the subject line carefully before opening it. If the subject line is gibberish or does not make any sense to you, check with the sender before opening it.</p>
<p><b>Create a record (a security log)</b>, if you want one, that records successful and unsuccessful attempts to connect to your computer. This can be useful as a troubleshooting tool.</p>	<p><b>Block spam or unsolicited e-mail</b> from appearing in your inbox. However, some e-mail programs can help you do this. Check the documentation for your e-mail program or see <a href="#">Fighting Unwanted Spam</a> to learn more.</p>

# Software Firewalls

## To open Windows Firewall

1. Click **Start** and then click **Control Panel**.
2. In the control panel, click **Windows Security Center**.
3. Click **Windows Firewall**.



---

# How many Firewalls do you Need?

- It should be noted that firewalls **do not protect you from viruses**, so having a firewall does not mean that you don't need an anti-virus program.
  - Although the software-based firewall is different from the hardware-based firewall; they both will protect a computer and network if properly installed and updated.
-

---

# Software vs Hardware Firewalls

- The differences between a software and hardware firewall are vast, and the best protection for your computer and network is to use both, as each offers different but much-needed security features and benefits.
  - Updating your firewall and your operating system is essential to maintaining optimal protection, as is testing your firewall to ensure it is connected and working correctly.
-