Firewalls and Network Defense

2.6 Firewalls and Network Defense

- There are many different appliances on the market that a system administrator can use to protect the network.

- These devices use **different techniques** and work on **different layers** to perform **access control, attack detection and prevention**.

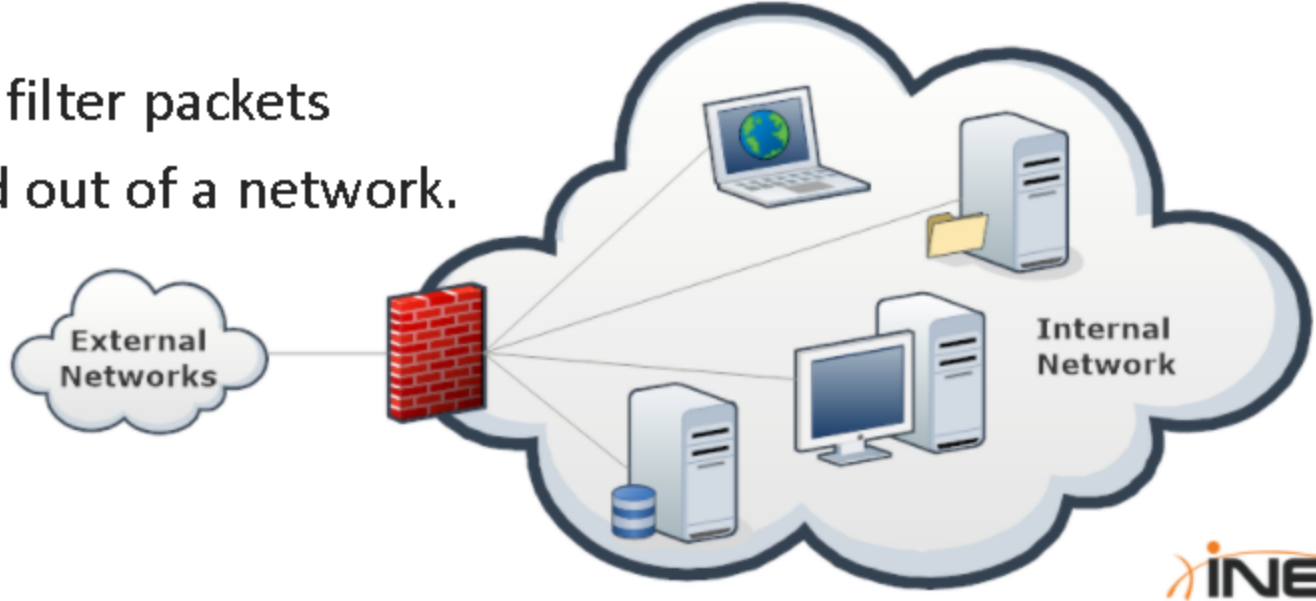
2.6 Firewalls and Network Defense

+ **How does this support my pentesting career?**

  - Evading firewalls
  - Advanced stealth scanning
  - Filtering evasion

2.6.1 Firewalls

- Firewalls are specialized software modules running on a computer or a dedicated network device.
- They serve to filter packets coming in and out of a network.



2.6.1 Firewalls

- Firewalls help system administrators and desktop users to control the access to network resources and services.
- A firewall can **work on different layers** of the OSI model, thus providing different features and protections.
- It is imperative that you understand how firewalls work and what kind of threats they prevent.
- Many people believe that firewalls and antiviruses are all they need to stay secure, in the following slides you will see why this idea is wrong.

2.6.2 Packet Filtering Firewalls

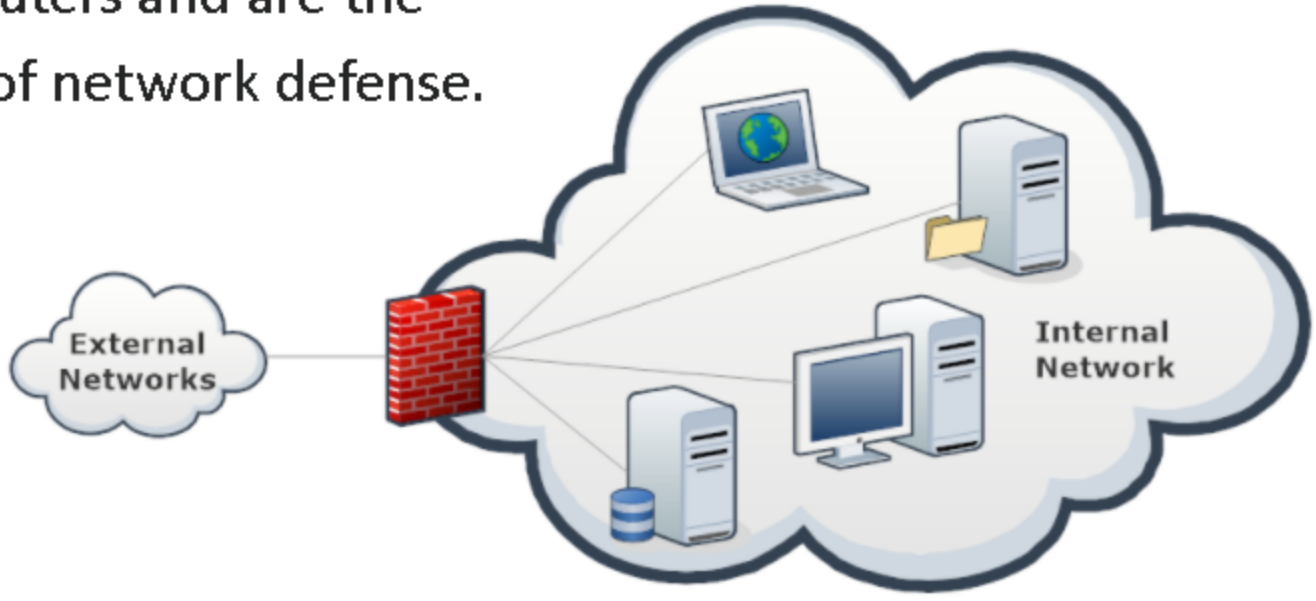
+ The most basic feature of a firewall is **packet filtering**.

+ With packet filtering, an administrator can create rules which will filter packets according to certain characteristics like:

  - Source IP address
  - Destination IP address
  - Protocol
  - Source port
  - Destination Port

2.6.2 Packet Filtering Firewalls

+ Packet filters run on home DSL routers as well as high-end enterprise routers and are the cornerstone of network defense.



2.6.2 Packet Filtering Firewalls

+ Packet filters inspect the header of every packet to choose how to treat the packet. The more common actions are:
  - **Allow**: allow the packet to pass
  - **Drop**: drops the packet without any diagnostic message to the packet source host
  - **Deny**: do not let the packet pass, but notify the source host

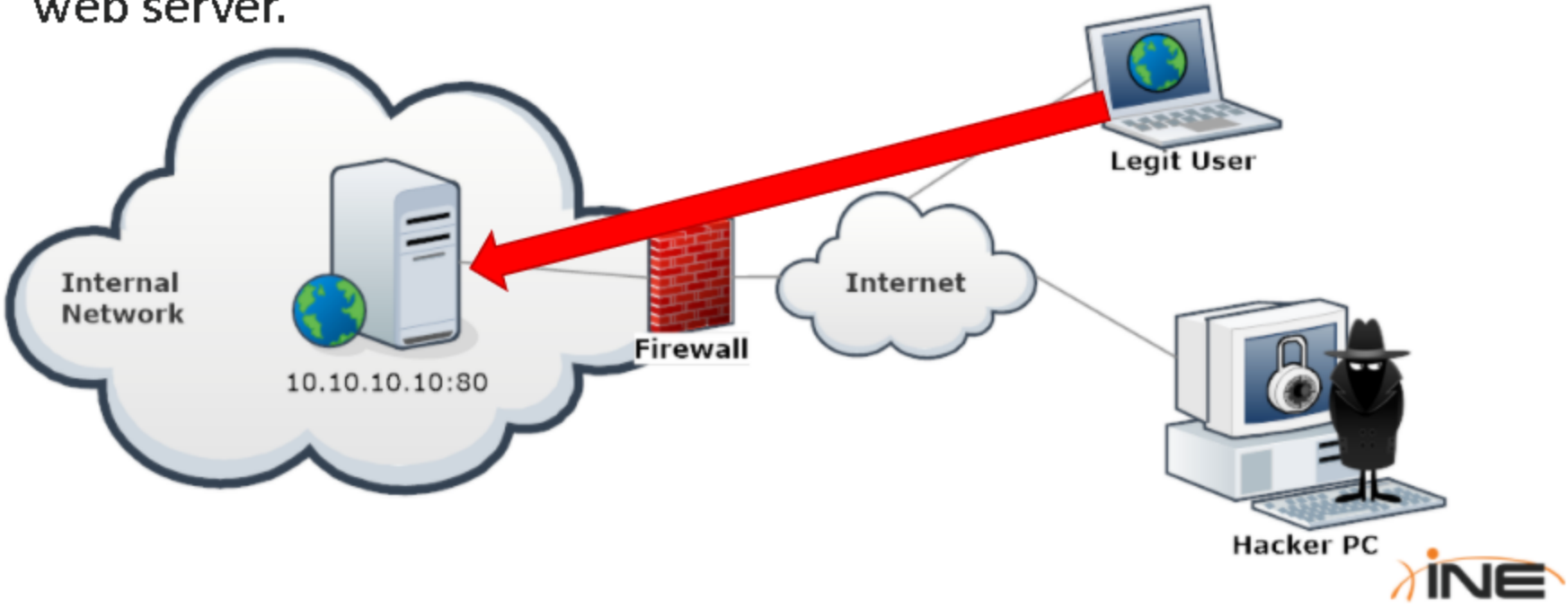
2.6.2 Packet Filtering Firewalls

EXAMPLE: Inspecting the header of a packet does not give you any information on the **actual packet content**

+ In a company, network administrators configure a corporate firewall to allow web browsing from the internal network. They do that by allowing TCP traffic to have 80 or 443 as destination ports. What happens if an internal machine tries to connect via SSH to a server listening on port 80?

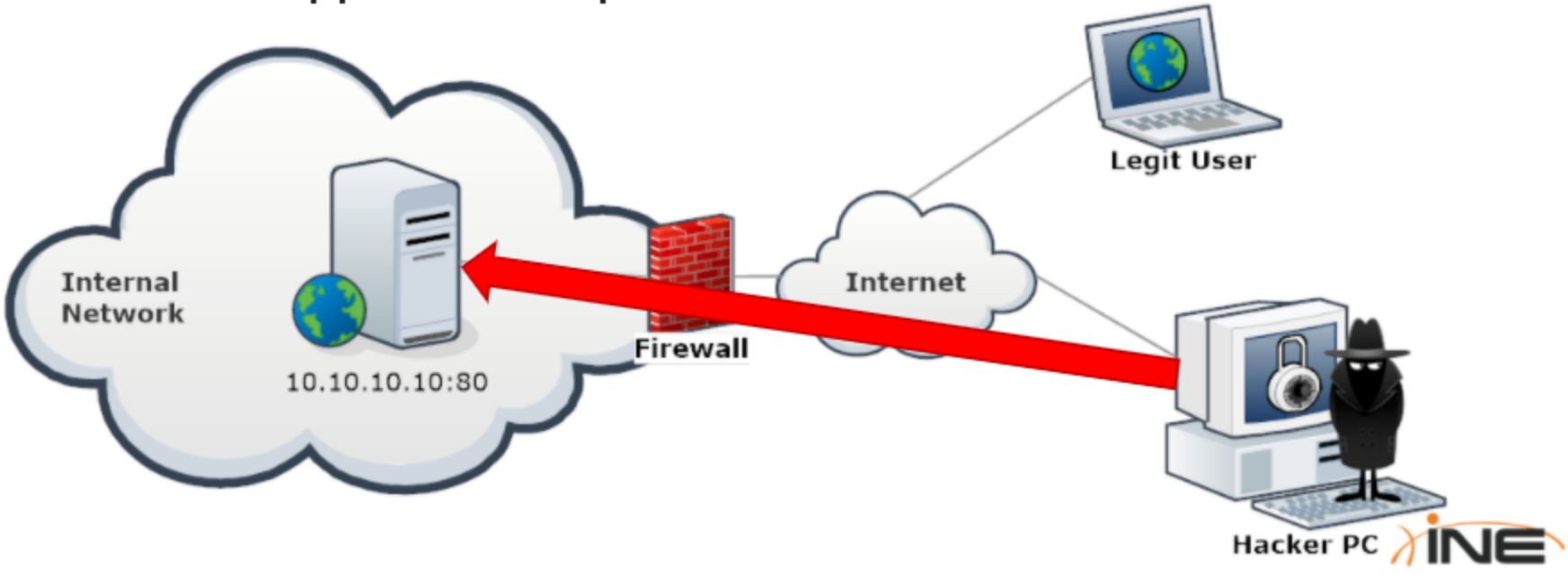
2.6.2.1 Packet Filtering vs. Application Attacks

- A company hosts a web server. The firewall will allow all incoming traffic from the Internet and direct it to port 80 of the web server.



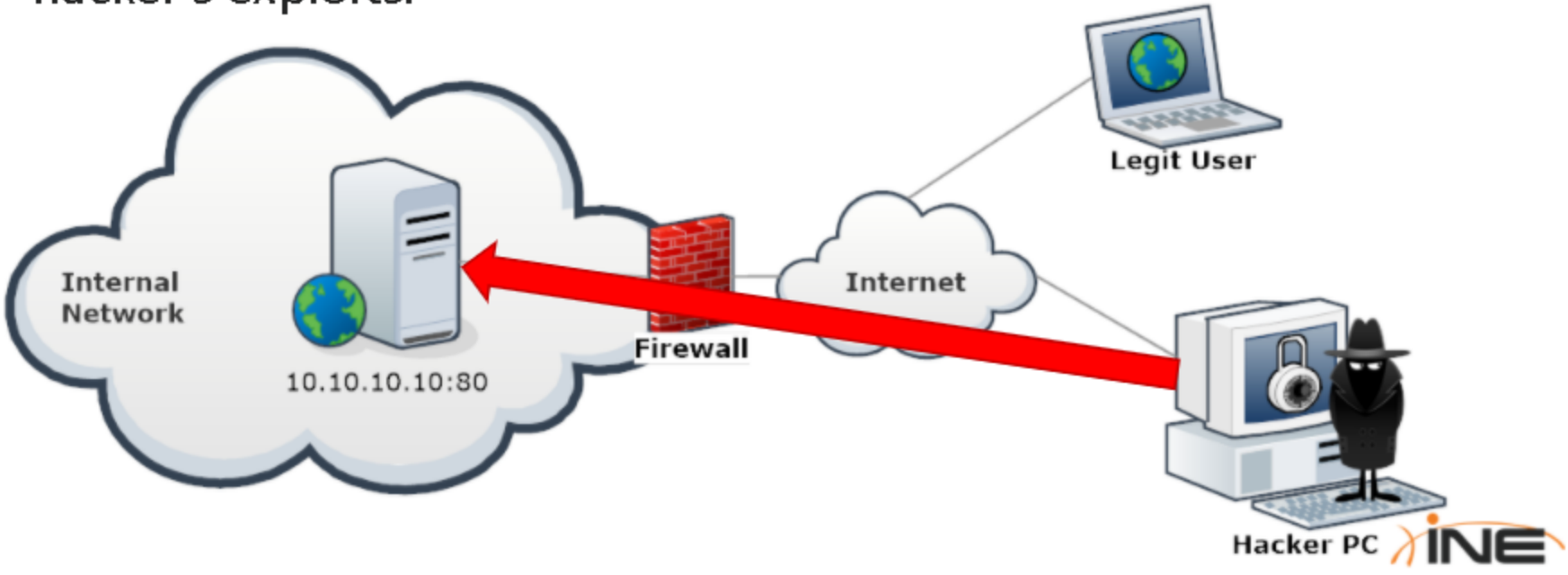
2.6.2.1 Packet Filtering vs. Application Attacks

- In the same way, application exploits will go through, because the firewall cannot see the difference between web browsing and a web application exploit.



2.6.2.1 Packet Filtering vs. Application Attacks

- The firewall can only filter traffic by using IP addresses, ports, and protocols. **Any** kind of application layer traffic will pass, even hacker's exploits.



2.6.2.1 Packet Filtering vs. Application Attacks

- An application layer exploit could be an XSS, a buffer overflow, a SQL injection and much, much more.
- Packet filtering is not enough to stop layer 7 attacks.
- Let's take a look at another scenario.

2.6.2.2 Packet Filtering vs. Trojan Horse

EXAMPLE

+ A hacker manages to exploit a workstation in a company network and wants to install a Trojan horse to remotely manage that machine.

+ The Trojan, by default, can be configured to **accept** connections on port 123 TCP or UDP or to **connect back** to the hacker's machine on port 123 TCP or UDP.

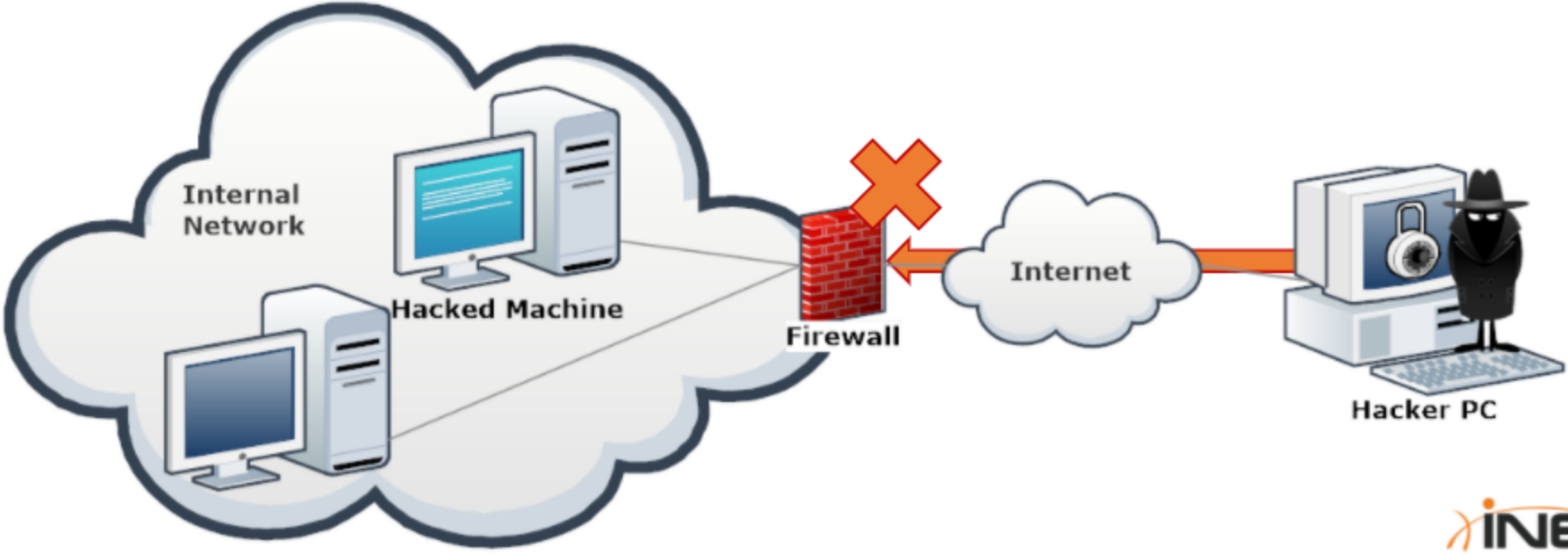
2.6.2.2 Packet Filtering vs. Trojan Horse

- A typical firewall configuration rule is to let HTTP traffic (TCP.dst = 80) pass, so internal workstations can browse the Internet. The remaining traffic is dropped.

- What happens to the Trojan horse?

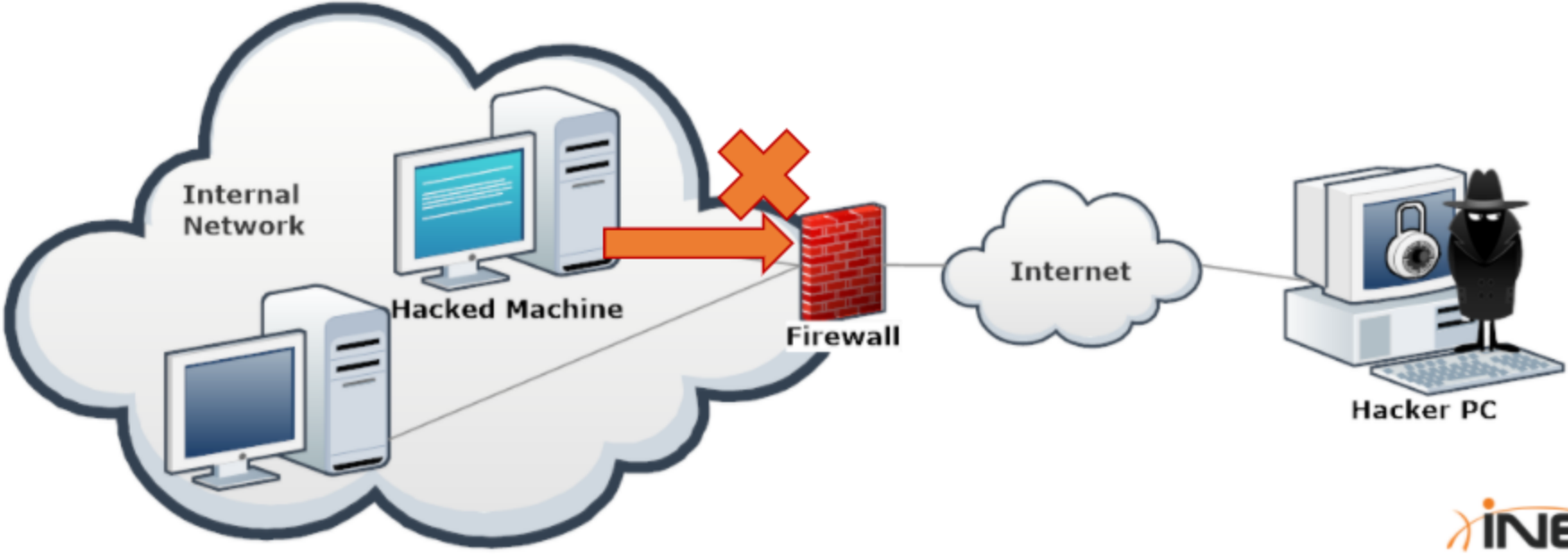
2.6.2.2 Packet Filtering vs. Trojan Horse

+ The hacker cannot connect to the infected machine, as there are no rules to allow traffic coming to port 123.



2.6.2.2 Packet Filtering vs. Trojan Horse

+ Similarly, the firewall will deny the traffic from the infected machine to the hacker's PC.

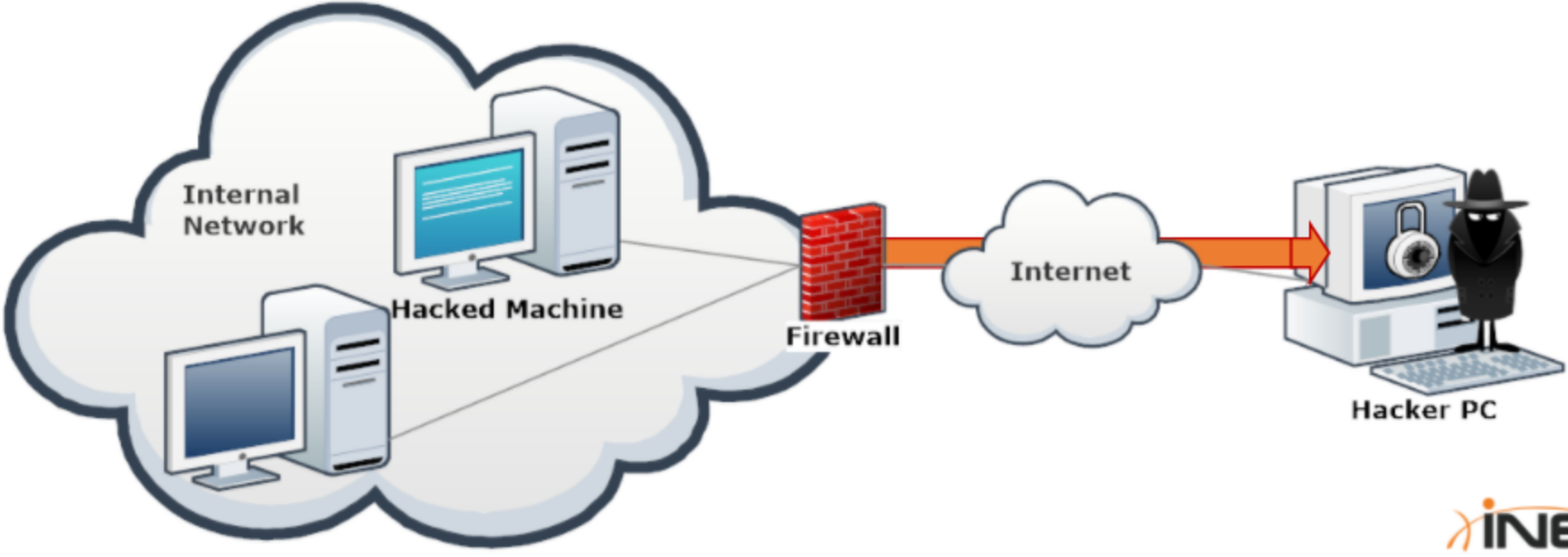


2.6.2.2 Packet Filtering vs. Trojan Horse

- What happens if the hacker, who is smart and knows all the well-known ports by heart, configures the Trojan to **connect back** to his or her machine on port 80?

2.6.2.2 Packet Filtering vs. Trojan Horse

+ The firewall will **allow** the connection!

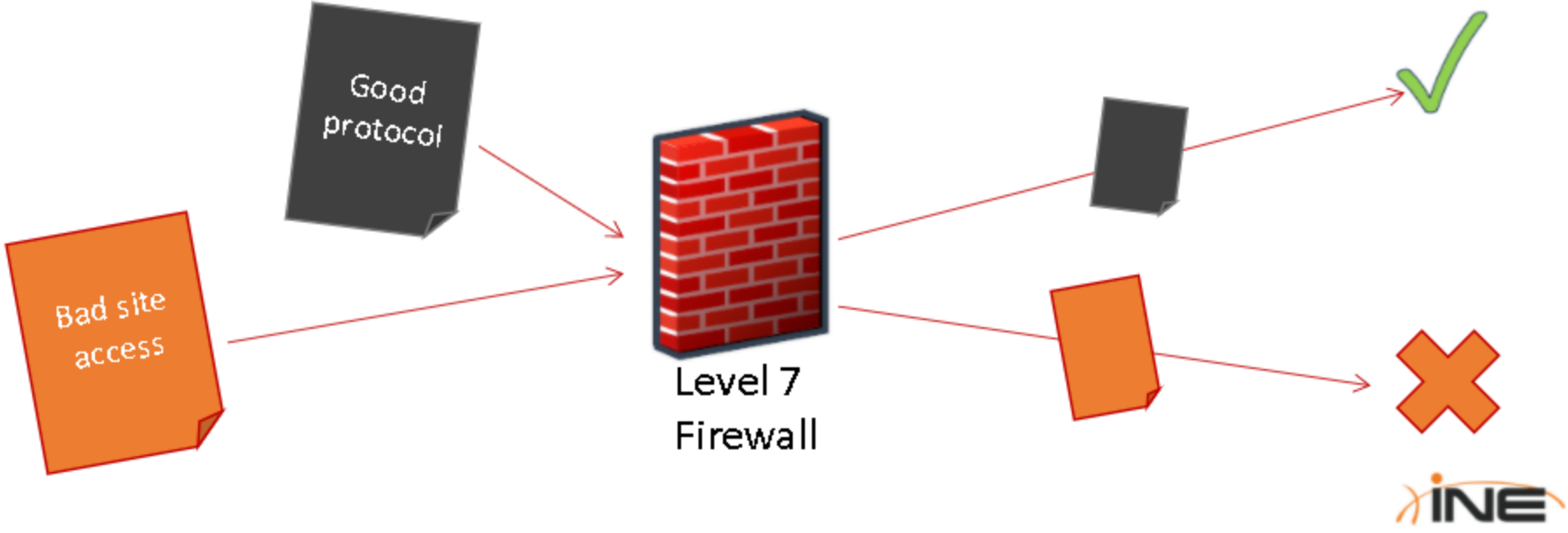


2.6.3 Application Layer Firewalls

- **Application level firewalls** work by checking all the OSI 7 layers.
- They provide a more comprehensive protection because they inspect the actual content of a packet, not just its headers. For example:
  - Drop any peer-to-peer application packet.
  - Prevent users from visiting a site.

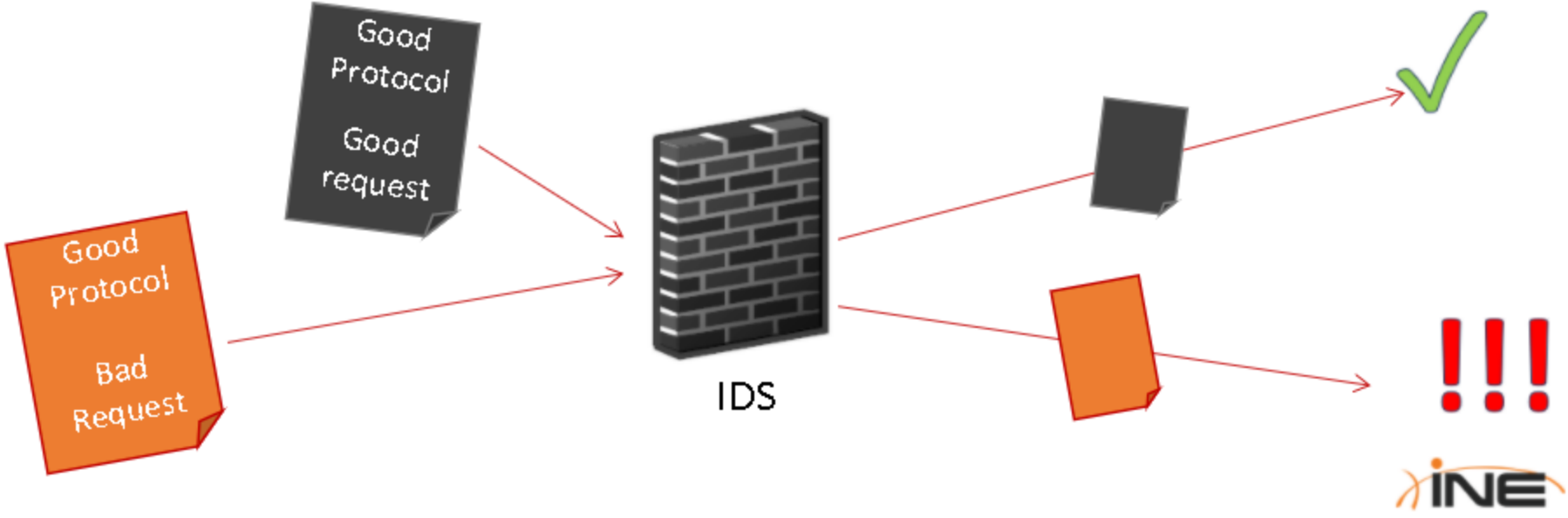
2.6.3 Application Layer Firewalls

+ Level 7 firewalls are indeed able to understand most of the application layer protocols in use nowadays. Organizations use them not only to protect their network from hackers but also to filter unwanted traffic.



2.6.4 IDS

- There is not just traffic detection, but intrusion detection! **Intrusion Detection Systems** (IDS) inspect the application payload trying to detect any potential attack.



2.6.4 IDS

- An IDS is specialized software used for **detecting ongoing intrusions**. It checks for attack vectors like ping sweeps, port scans, SQL injections, buffer overflows and so on.

- IDS can also **identify traffic** generated by a virus or a worm. Pretty much every kind of network threat can be detected by a well-configured IDS.

2.6.4 IDS

- An IDS, like an antivirus, detects risky traffic by means of **signatures**. The vendor provides frequent signature updates as soon as new attack vectors are found in the wild. Without the right signatures an IDS cannot detect and report an intrusion; the **IDS cannot detect something if it does not already know**.

- There are also **false positives**. They happen when legit traffic is flagged as malicious.

2.6.4 IDS

- Detection is performed by a multitude of **sensors**, software components that inspect network traffic.

- Sensors passively intercept intrusions and communicate them to the **IDS manager**, software in charge of maintaining policies and which provides a management console to the system administrator.

2.6.4 IDS

- IDSs **do not substitute firewalls**.

- They support firewalls by providing a further layer of security protecting the network from mainstream and well-known attack vectors.

2.6.4 IDS

+ IDSs fall into two main categories:

Network Intrusion Detection Systems (NIDS)

Host Intrusion Detection Systems (HIDS)

2.6.4.1 NIDS

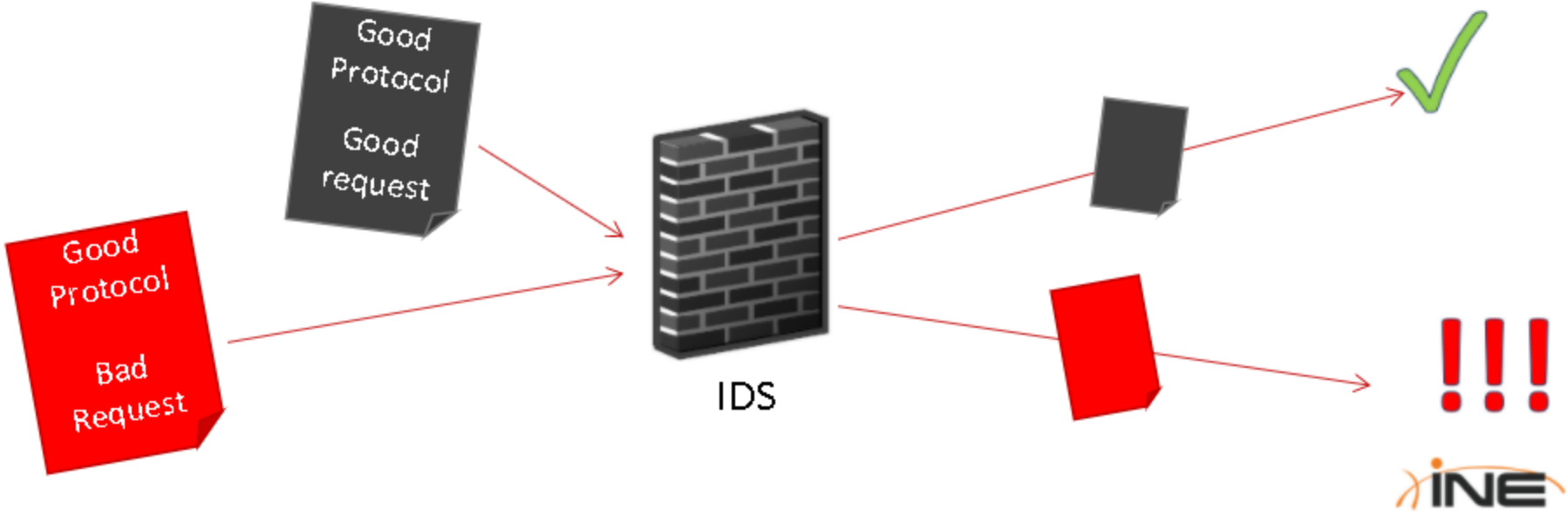
- Network intrusion detection systems inspect network traffic by means of sensors which are usually placed on a router or in a network with a high intrusion risk, like a DMZ.

2.6.4.2 HIDS

- On the other hand, host IDS sensors monitor application logs, file-system changes and changes to the operating system configuration.

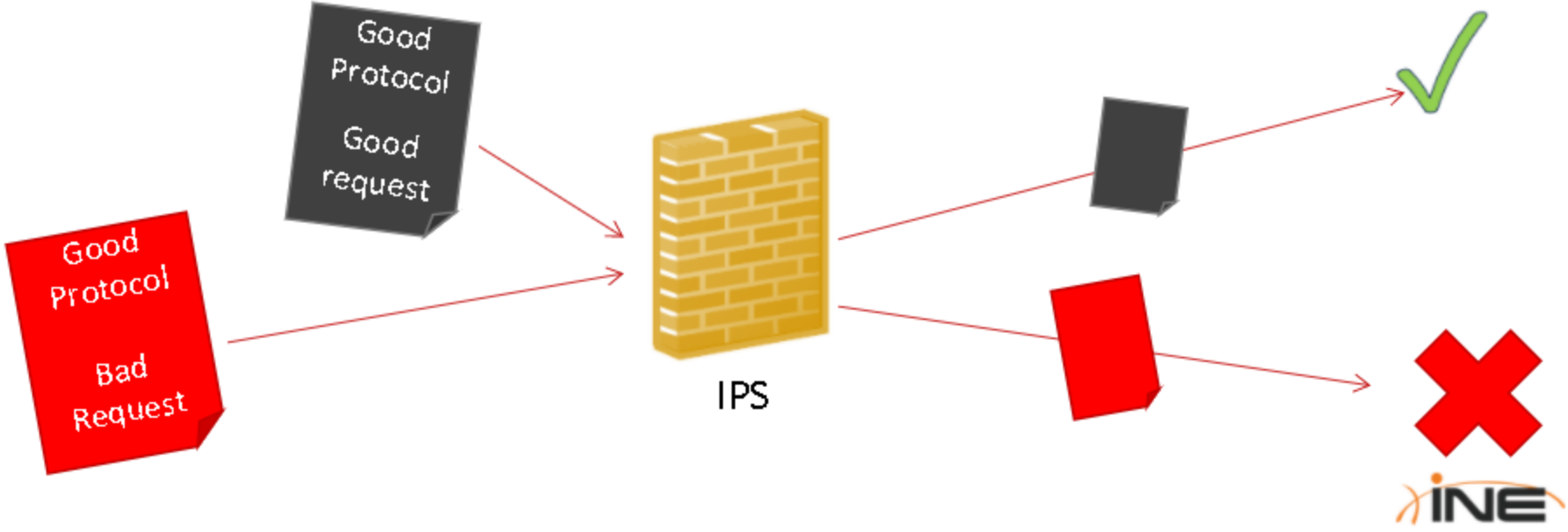
2.6.5 IPS

- IDSs, unlike firewalls, can detect suspicious activities and report them to the network administrator. Suspicious activity is logged for future analysis, but **it is not blocked**.



2.6.5 IPS

- **Intrusion Prevention Systems** (IPS) can **drop** malicious requests when the threat has a risk classification above a pre-defined threshold.

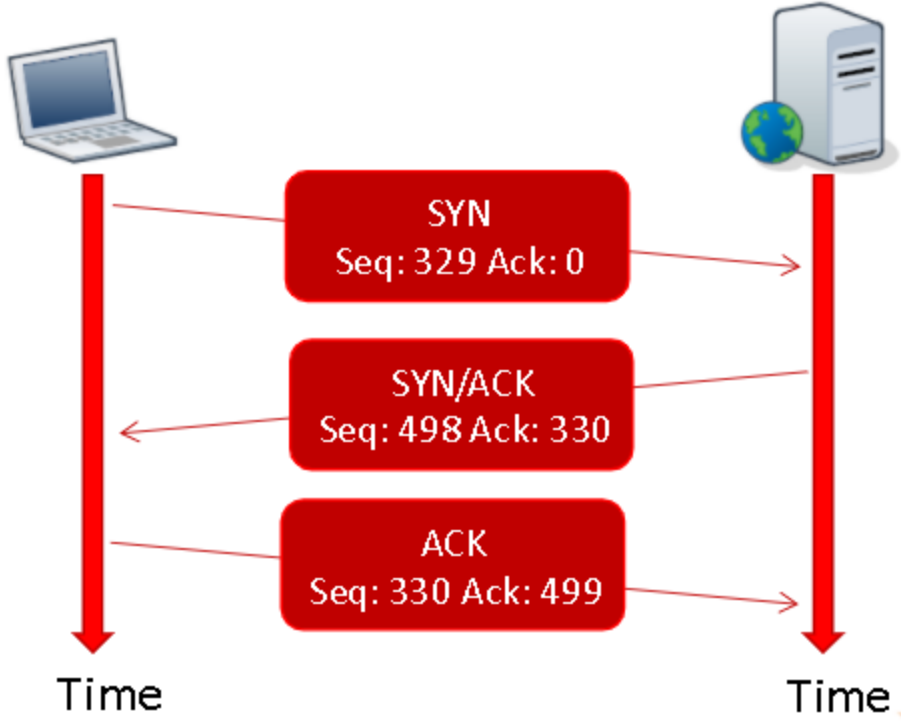


2.6.6 Spot an Obstacle

- During penetration testing activities, you might want to identify if a firewall-like mechanism is used in the environment.
- If you suspect presence of a firewall, you might want to check for anomalies in TCP Three-Way Handshake that was introduced previously in this module.

2.6.6 Spot an Obstacle

A proper Three-way handshake looks like:



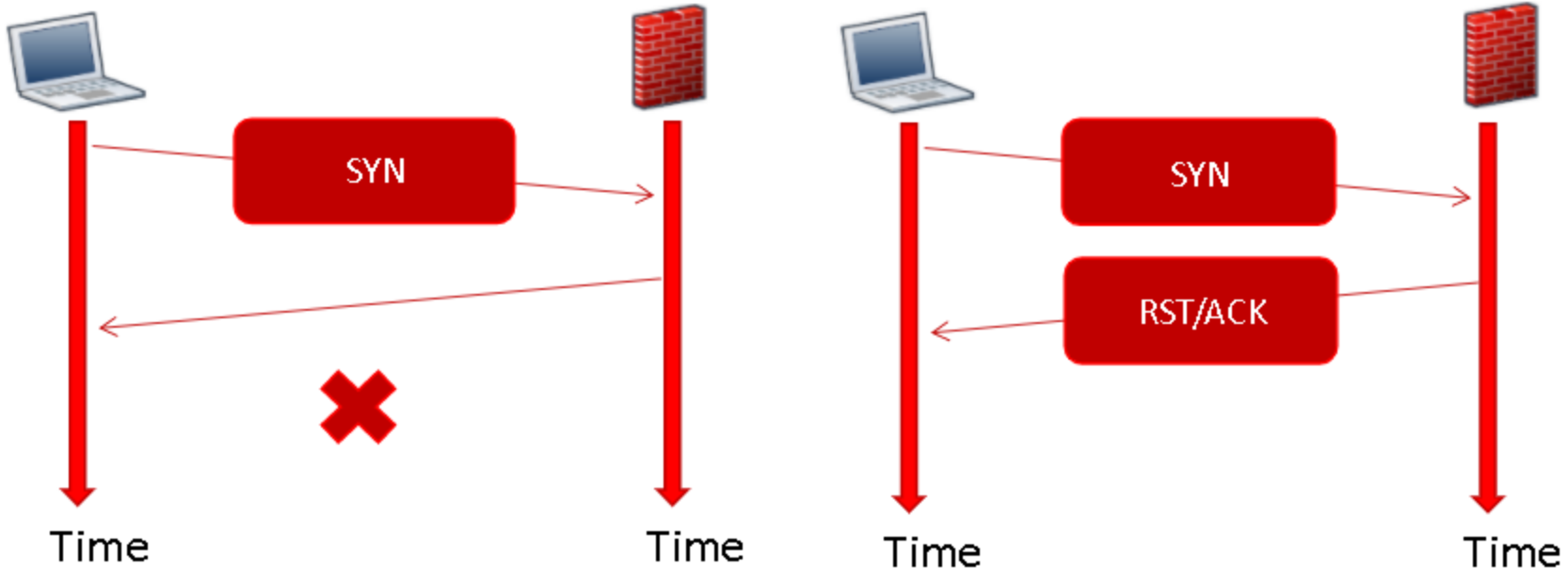
2.6.6 Spot an Obstacle

+ When a firewall is in place, the following behavior may be spotted:

  - **TCP SYN** are sent, but there no **TCP SYN/ACK** replies

  - **TCP SYN** packets are sent but a **TCP RST/ACK** reply is received

2.6.6 Spot an Obstacle



2.6.6 Spot an Obstacle

- Note, that this type of observation does not determine whether the detected obstacle is a **firewall**, an **IDS**, or **any other** device; this just helps you to identify **environmental constraints**.

2.6.7 NAT and Masquerading

+ Firewalls not only filter packets but can also be used to implement **Network Address Translation** or **NAT**.

+ *Note: Your home router is most probably running NAT protocol to connect all your home devices to the internet without having to have a public IP assigned for each of them.*

+ What is NAT and why is it needed?

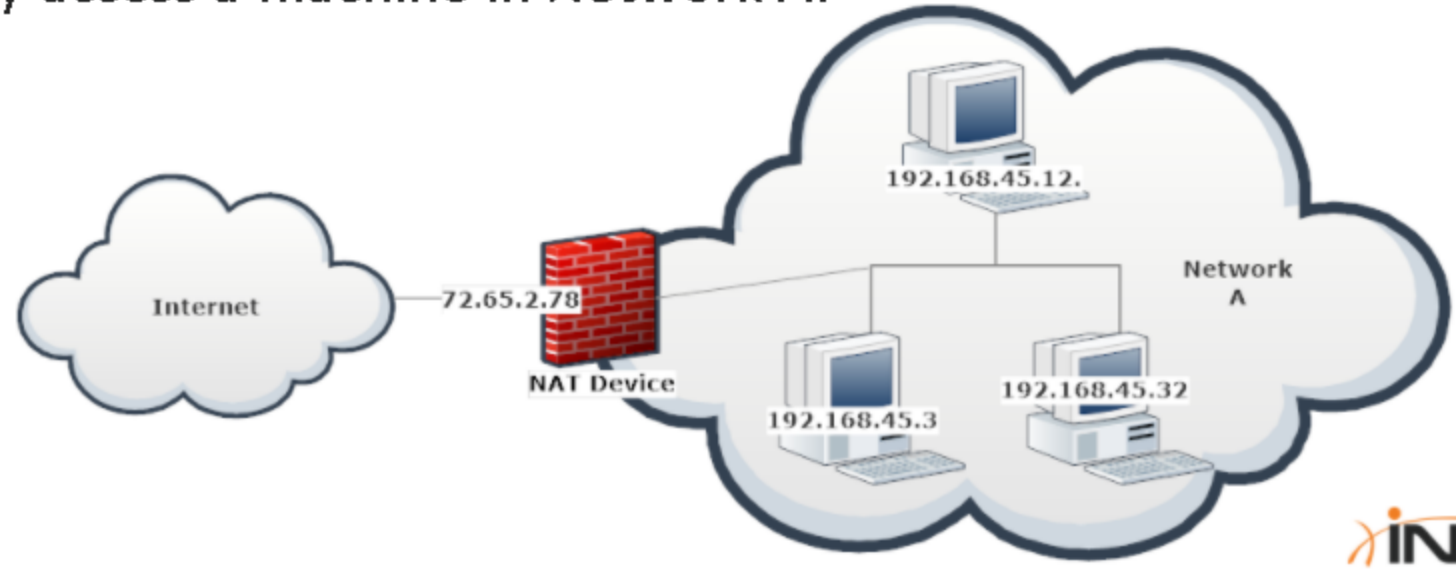
2.6.7 NAT and Masquerading

- As you know, every machine on the Internet must have a unique IP address. This does not mean that every device that can **access** the internet must have a unique **public** IP address.

- **Network Address Translation (NAT)** and **IP masquerading** are two techniques used to provide access to a network from another network.

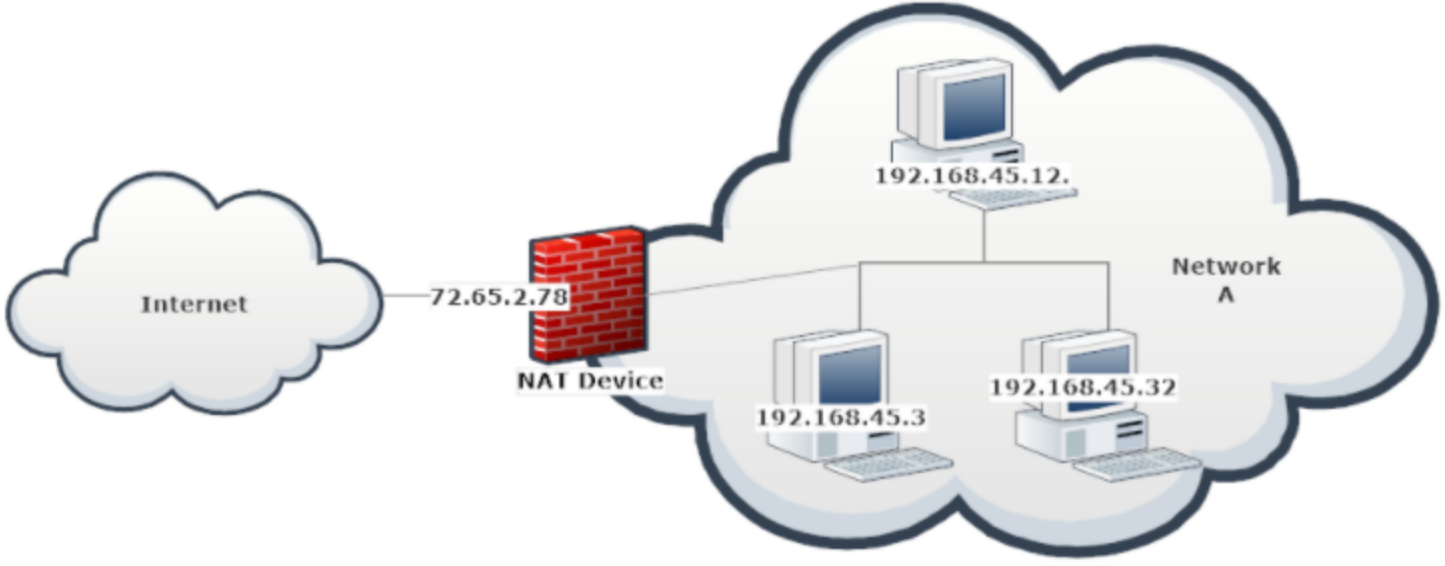
2.6.7 NAT and Masquerading

- **EXAMPLE:** *Network A* can be a private network using a NAT device to access the Internet. A machine on the internet cannot directly access a machine in *Network A*.



2.6.7 NAT and Masquerading

- But, a machine in *Network A* can access the Internet, if the NAT device allows the traffic to pass.



2.6.7 NAT and Masquerading

- Every machine inside *Network A* will use the NAT device as **its default gateway**, thus routing its Internet traffic through it. The NAT device then rewrites the **source IP address** of every packet setting it to `72.65.2.78` (in our example), thus masquerading the original client's IP address.

- A machine on the Internet will never know the original client's IP address.

2.6.8 Resources

- Netfilter the Linux kernel packet filtering framework.
- Book: Firewall Fundamentals the essential guide to understanding and using firewalls to protect personal computers and your network.
- OSSEC IDS an Open Source Host-based Intrusion Detection System.
- IDS FAQ answers to simple questions related to detecting intruders who attack systems through the network.

http://www.netfilter.org/
http://www.amazon.com/Firewall-Fundamentals-Wes-Noonan/dp/1587052210/ref=cm_cr_pr_sims_t
http://www.ossec.net/
http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html