Kaitlin Hoffmann

Office Hours:

SH 243 Monday 1:15 - 3:15PM. Tuesday 2:45 - 4:45 PM

Email: hoffmank4@newpaltz.edu

FIREWALLS

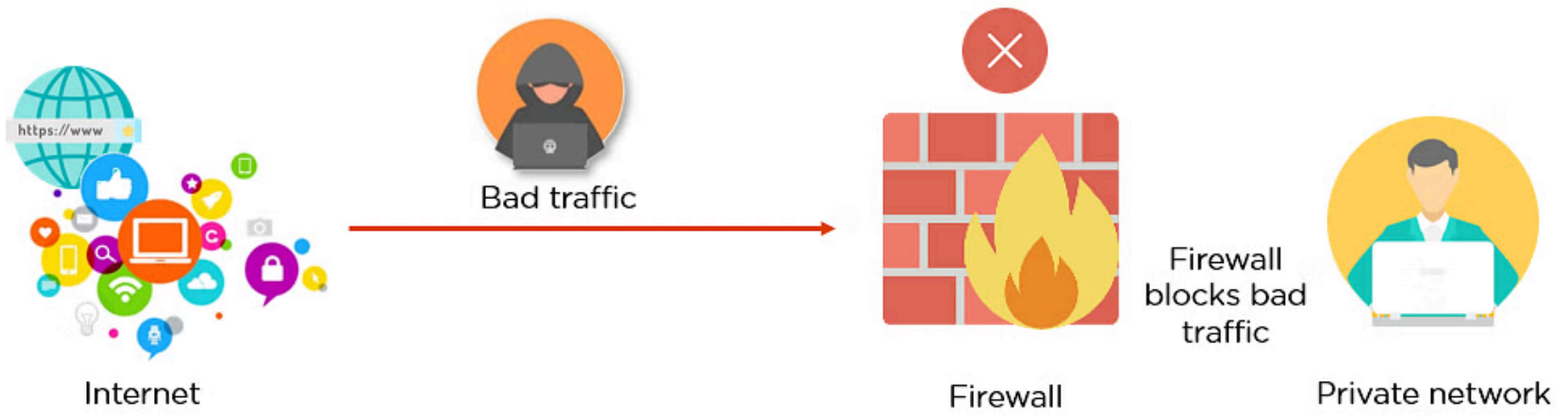
NETWORK SECURITY

OBJECTIVES

- Overview
- Blacklist Whitelist Greylist
- MAC address Filtering
- Access Control List
- Types of Firewalls
- Configuring Firewalls

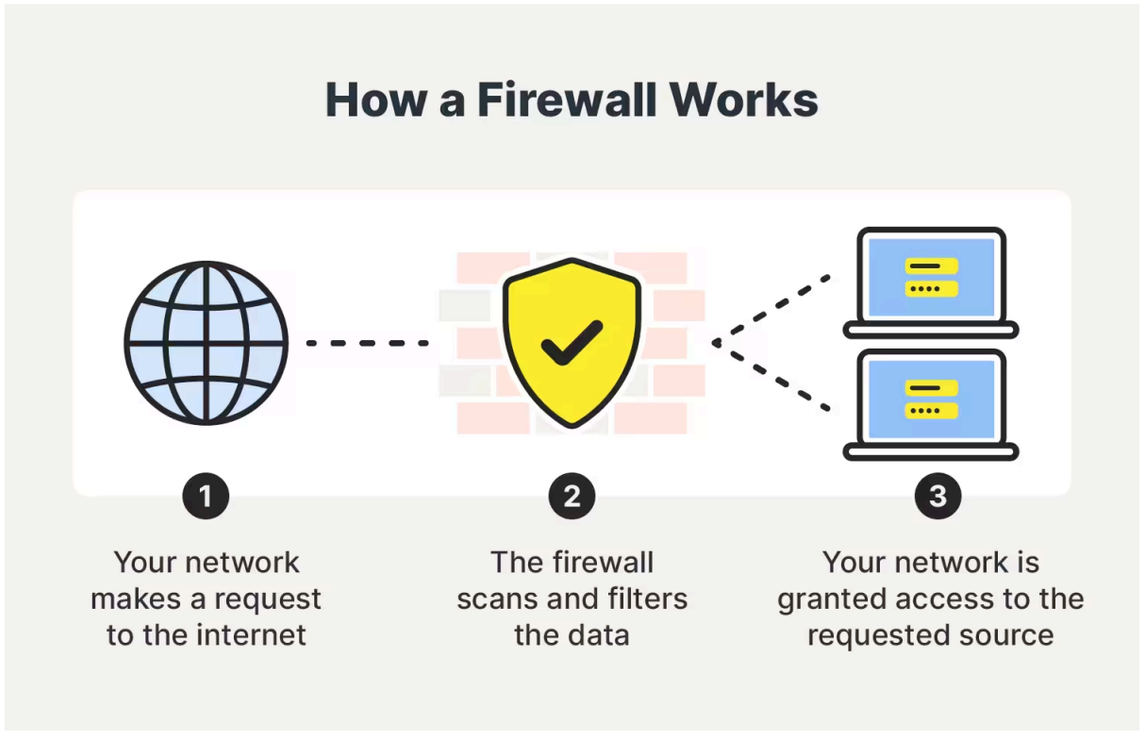
WHAT IS A FIREWALL

- A **firewall** is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Establishes a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be **hardware**, **software**, **software-as-a service** (SaaS), **public cloud**, or **private cloud**.



WHAT IS A FIREWALL

- Simply put, firewalls filter traffic that flows through its **ports**.
- The most basic job of the firewall is to look at each **packet** and decide based on a set of rules whether to block or allow the traffic.
- This traffic can be either **inbound** traffic (packets coming from **outside** the network) or **outbound** traffic (packets **leaving** the network).



HARDWARE VS SOFTWARE FIREWALLS

- The **network-based firewall** is often implemented in some sort of **hardware appliance** or is built into the router that is installed between the LAN and the the Internet.
- A common network-based firewall is the **SOHO (Small Office Home Office) firewall** which is built in to most consumer-grade routers. Best for home and small offices.
  - Can't provide any help if the malicious traffic is originating from inside the network itself.

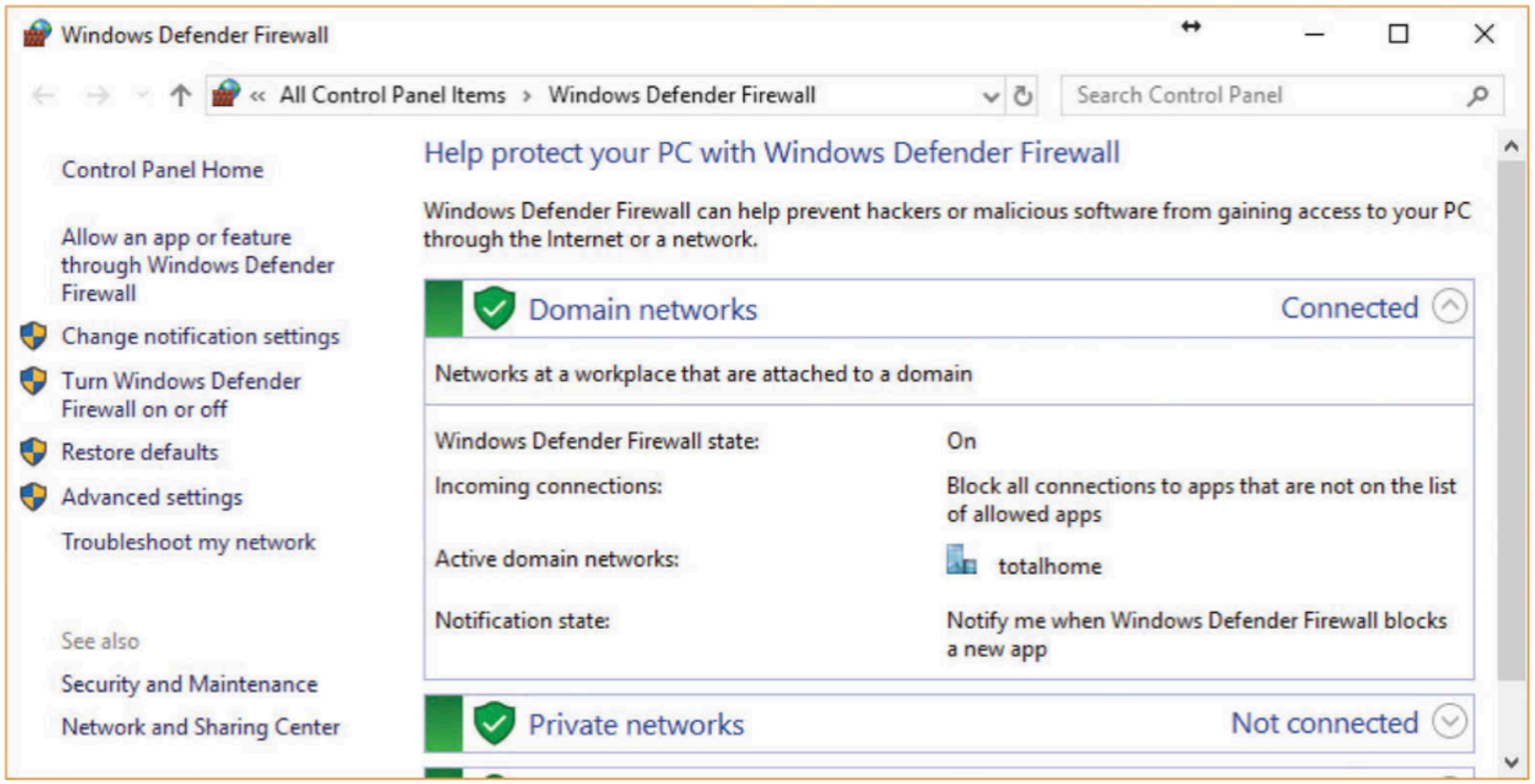
SOHO Network Security Firewall

These affordable firewalls let small businesses and home offices take full advantage of high-speed broadband, without compromising the highly effective protection needed to stop cyberattacks.

https://www.youtube.com/@professormesser/playlists

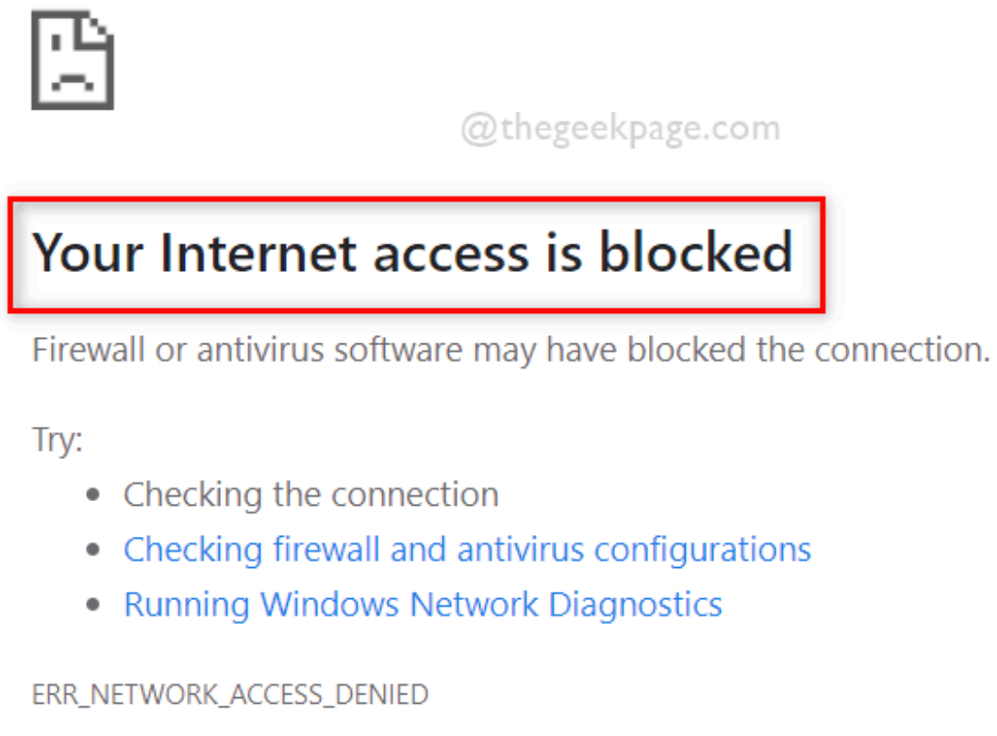
SOFTWARE VS HARDWARE FIREWALLS

- A **host-based firewall** is a software firewall installed on a "host" that provides firewall services for just that machine.
- A great example of this type of firewall is the Windows Firewall/ Windows Defender Firewall that has shipped with every version of Windows since XP.



BLACKLISTING

- Blacklisting is a method of controlling access to data or networks by identifying users or devices that are ***not allowed***.
- Usually done by keeping a list of known bad actors or dangerous IP addresses and blocking any traffic from those addresses.
- Blacklisting can be used to block specific websites, email addresses, or even entire countries. This approach is threat-centric and allows access as the default setting.



BENEFITS OF BLACKLISTING

- **Proactive approach to security –** You're not just waiting for someone to try and access your network, you're actively preventing them from doing so.
- **Can be very effective at blocking known bad actors –** If you have a list of addresses or devices that are known to be malicious, blacklisting them can be a very effective way to stop them from causing damage.
- **Easy to implement –** Blacklisting only requires a list of addresses or devices to be blocked. It doesn't require any extra hardware or software.

DISADVANTAGES OF BLACKLISTING

- **Not foolproof –** Just because an address or device is on a blacklist doesn't mean it's definitely malicious. It's possible for legitimate addresses or devices to be blacklisted.
- **Can be time-consuming to maintain –** If you want your blacklist to be effective, you need to keep it up-to-date with new threats. This can take a lot of time and effort.
- **Not very flexible –** Once an address or device is blacklisted, it can be difficult to unblock it if you need to.
- **Useless against unknown threats –** New attacks won't be stopped as they wouldn't be on your blacklist

WHITELISTING

- Whitelisting is the ***opposite*** of blacklisting. Instead of blocking specific addresses or devices, whitelisting **allows only specific addresses** or devices to access data or networks.
- Usually done by **keeping a list of trusted** users or devices and only allowing traffic from those addresses. Whitelisting can be used to allow specific websites, email addresses, or even IP addresses to a specific network.
- This approach is trust-centric and blocks access as the default setting.

BENEFITS OF WHITELISTING

- **Very secure approach to data security –** If you only allow trusted devices or users to access your data, it's much harder for someone to get in and cause damage.
- **Very effective at blocking untrusted sources –** If you have a list of addresses or devices that are known to be malicious, whitelisting them can be a very effective way to stop them from causing damage.

DISADVANTAGES OF WHITELISTING

- **Can be difficult to implement –** It requires a lot of specific information about each organization and when new tools or applications are installed, the whitelist needs to be updated.
- **Not very flexible –** Users are restricted with what they can do on their systems.
- **Not foolproof –** Even with a whitelist, it's possible for malicious devices or users to get through if they manage to spoof a trusted address or device.

GREYLISTING

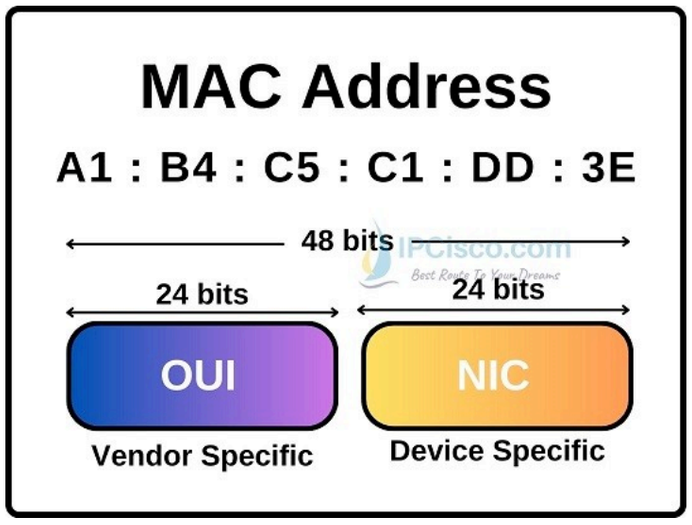
- **Greylisting** is similar to blacklisting, but it's not as aggressive.
- Items on a greylist have not yet been confirmed as either safe or harmful.
- These items are **temporarily blocked** from your system until it is further analyzed. Once it has been determined safe or not, it moves to either the blacklist or the whitelist.

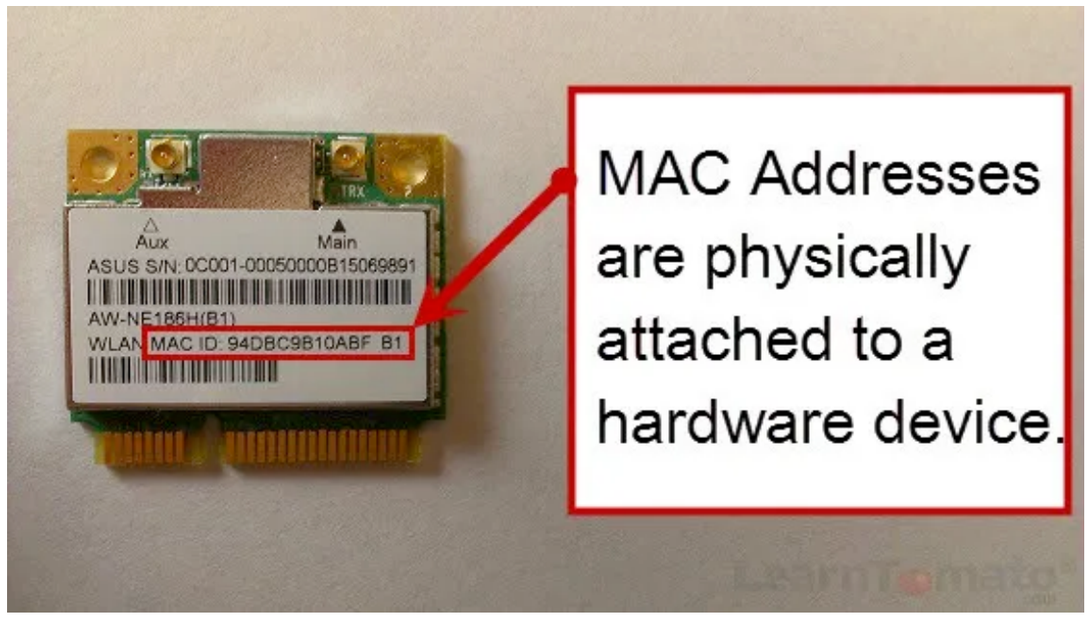
GREYLISTING – WHERE IT'S USED

- Most commonly greylisting is used in **email security**.
- Greylisting is used to **combat spam** by temporarily rejecting all email messages from sources that you don't recognize.
- By temporarily rejecting all emails, greylisting effectively filters out most spam messages while allowing legitimate emails to get through.

MEDIA ACCESS CONTROL FILTERING

- Every device that connects to your device has a MAC address (the physical address). You can limit access through the **physical hardware address**.
- Allows you to configure your firewall to allow or disallow access for particular MAC addresses on your network.
- This is a common filtering technique that allows your network administrator to control exactly what devices are able to communicate through your router.





RESTRICTING ACCESS VIA ACL

- At its core, configuring a firewall is about defining which traffic can flow and which traffic shall not pass.
- This rule often takes the form of an access control list (ACL), a rule applied to an interface that allows or denies traffic based on things like source or destination IP addresses.
- ACLs can restrict access to network resources.

RESTRICTING ACCESS VIA ACL

- Below is a simple ACL that you may find on a router or firewall:

```
access-list 10 deny 10.11.12.0 0.0.0.255
access-list 10 permit any
```

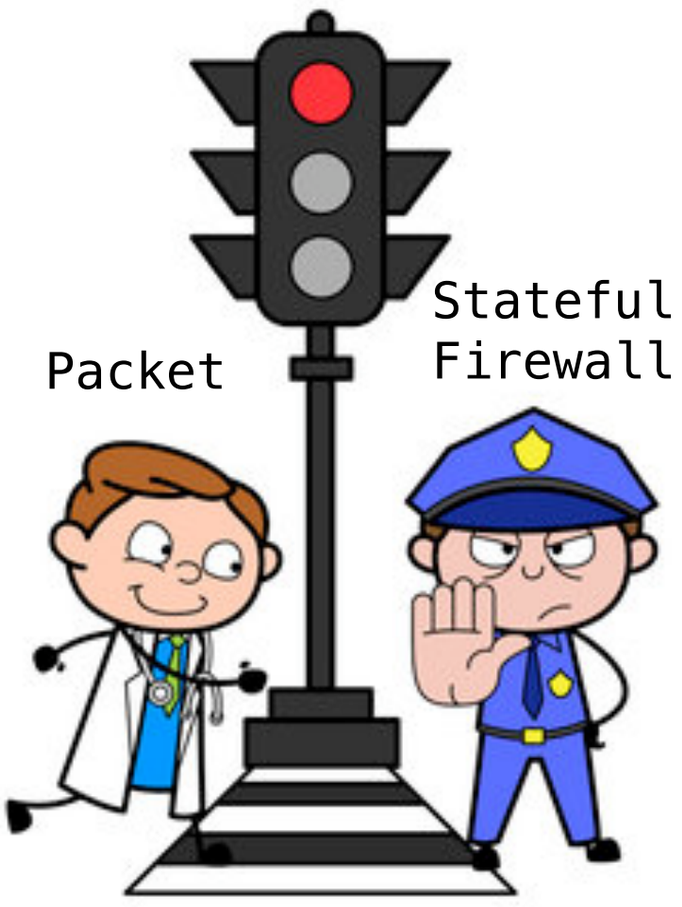
- The beginning of the first line, **access-list 10**, tells IOS that we want to create an ACL and its number is 10. The end of the first line, deny 10.11.12.0 0.0.0.255, is the actual rule we want the firewall to apply.
- If we stopped after the first line, no traffic would get through because we don't have a rule that explicitly permits it! So the last rule in this list will permit through ***any*** traffic that wasn't dropped by the first rule.

STATELESS FIREWALL

- ACLs are considered **stateless firewalls**. Stateless firewalls only focus on **individual packets** using preset rules to filter traffic.
- Although rules within ACLs look a little different depending on what hardware you're using, they generally include the following elements:
  - **Permission** - PERMIT/ALLOW or DENY traffic.
  - **Protocol** - TCP, UDP, etc.
  - **Source** - the source IP address (where packet is from)
  - **Destination** - the destination IP address (where packet is going)
  - **Port or Protocol** - Typically, you'll often see a well-known port such as port **443** for **HTTPS** in a rule. However, some devices support codes such as HTTPS for HTTPS traffic.

STATEFUL FIREWALL

- A **stateful firewall** inspects traffic and makes decisions based on the **traffic context or state**.
- It keeps track of established sessions, inspects traffic based on its state within a session, and it blocks traffic that isn't part of an established session.
- **Example**: A TCP session starts with a three-way handshake. If a stateful firewall detects TCP traffic without a corresponding three-way handshake, it recognizes this as suspicious traffic and can block it.

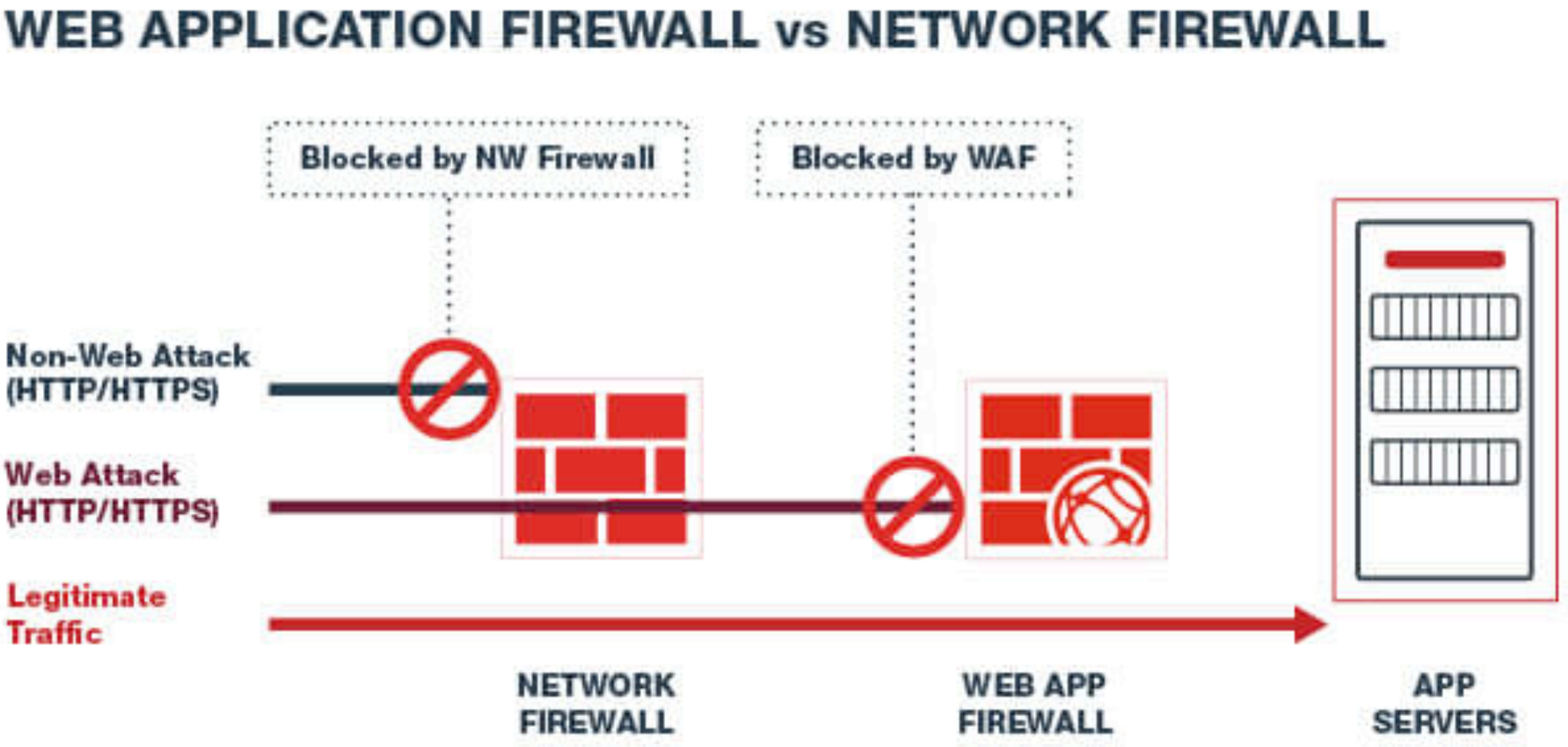


WEB APPLICATION FIREWALL

- A **web application firewall** (WAF) is a firewall specifically designed to protect a web application.
- A web server hosts the web application, and the WAF is placed ***between*** the web server and web server clients.
- The WAF can be a stand-alone appliance or software added to another device.
- Note that you wouldn't use a WAF in place of a network-based firewall. Instead, it provides **an added layer of protection** for the web application in addition to a network-based firewall.

WEB APPLICATION FIREWALL

- A WAF protects web applications by targeting Hypertext Transfer Protocol (HTTP) traffic. This differs from a network firewall, which provides a barrier between external and internal network traffic.

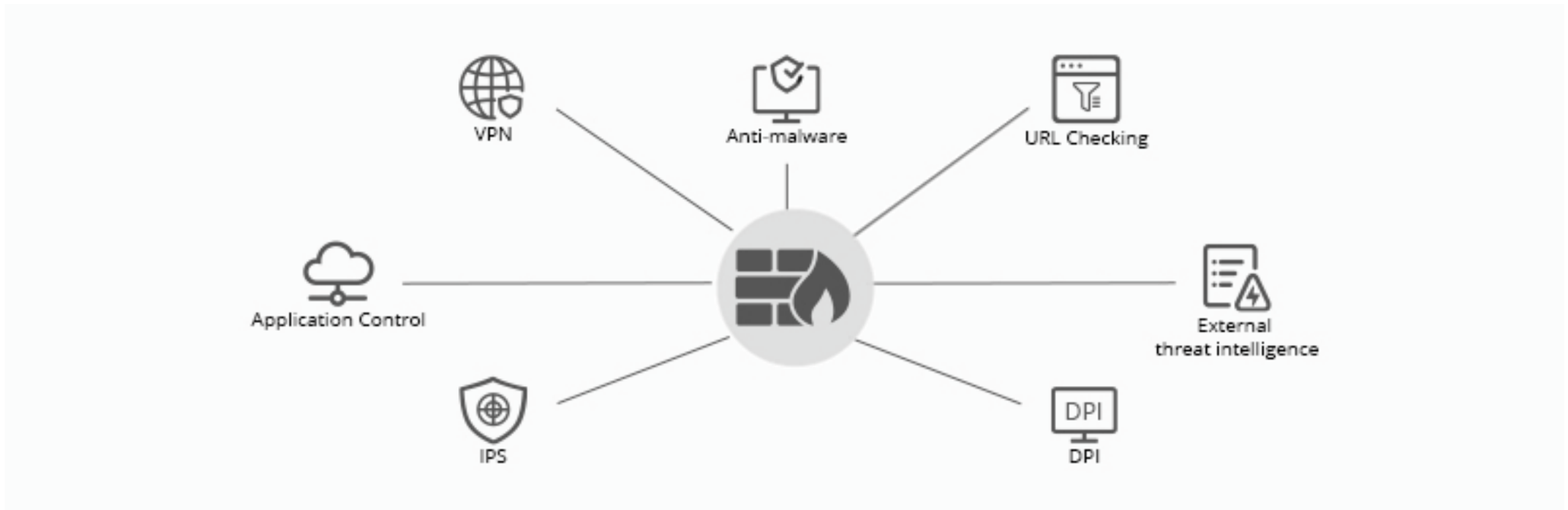


NEXT GENERATION FIREWALL

- A **next-generation firewall** (NGFW) is an advanced firewall that adds capabilities that aren't available in first-generation or second-generation firewalls.
- The first generation of firewalls were **packet-filtering** firewalls, using stateless firewall rules, and could only allow or block traffic after evaluating individual packets.
- The second generation of firewalls added in **stateful firewall** rules. This allows firewalls to evaluate traffic based on its session state.

NEXT GENERATION FIREWALL

- An NGFW performs **deep-packet inspection**, adding application-level inspection as a core feature.
- The NGFW is aware of common application protocols used on the Internet, such as FTP and HTTP.
- By using deep-packet inspection, the NGFW can identify application commands and detect potentially malicious traffic. This allows it to apply **content filtering** and **URL filtering**.



FIRST, SECOND AND NEXT GENERATION FIREWALLS

Capability	Traditional firewall	Next generation firewall	Advantages of next generation firewall
Inspection	Stateless	Stateful	Blocks traffic that deviates from expected norm compared to established connections
Visibility	Rudimentary, only lower TCP/IP layers	Deep, includes all TCP/IP layers	Enables more granular and robust analysis of traffic
Services	Basic	Comprehensive	Includes UTM services such as antivirus, content filtering, IDS/IPS, and logging in addition to packet filtering
Protection	Limited	Enhanced	Identifies, prevents, and reports a broader variety of attacks

CONFIGURE FIREWALL IN ROUTER

- If you want to configure firewall settings or check out the settings in your home router, you can!
- In browser URL, type the IP address of your router. Most routers use an address of 192.168.1.1, but that's not always the case.
- You should be taken to your ISP's login page. Enter your information.
- Once logged in, you should have access to various configuration settings, including Firewall rules.

CONFIGURE FIREWALL IN SOFTWARE

- The default firewall configuration tool for Ubuntu is **Uncomplicated Firewall (UFW)**. Developed to ease `iptables` firewall configuration, `ufw` provides a user friendly way to create an IPv4 or IPv6 host-based firewall.
- You will be configuring the UFW in your VM as part of your assignment. Please read the following article as well: https://www.baeldung.com/linux/uncomplicated-firewall
- Second part of your assignment will be completing a TryHackMe lab.