The Role of Firewalls in National Security

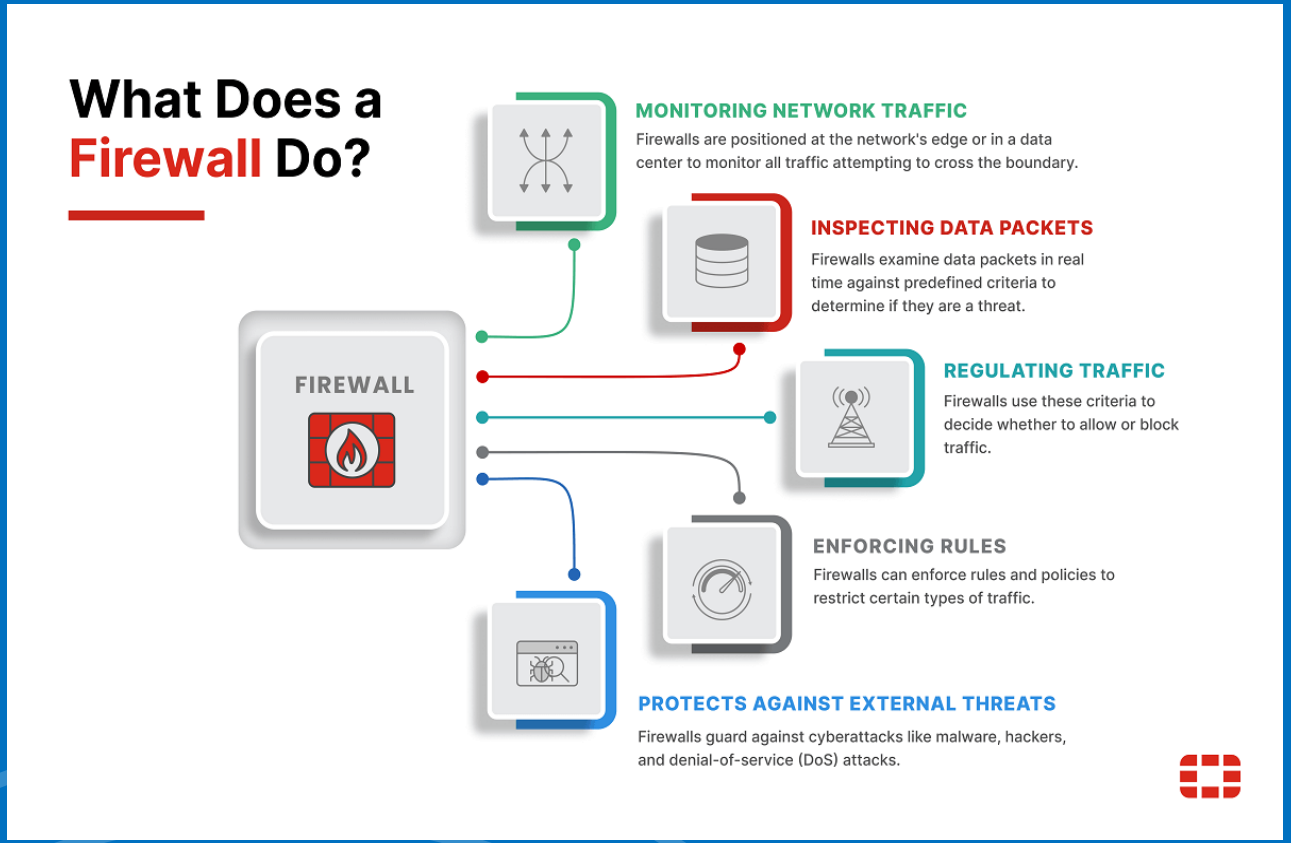
By Christopher Hernandez and Raquel Perez

What is National Security?

National security refers to the collective security and defense of a nation's citizens, infrastructure, and institutions, which is primarily the responsibility of the government to ensure their protection from internal and external threats.

What is a Firewall? Why are they important to have?

- A firewall is a security system that monitors and controls network traffic, acting as a barrier to prevent unauthorized access and protect sensitive data.
- Firewalls are essential as the first line of defense, safeguarding networks and devices by filtering harmful traffic and ensuring secure, efficient network performance.



https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use
https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

How does Cybersecurity tie into National Security?

- Cybersecurity is crucial for national security because it protects critical infrastructure, data, and systems from cyberattacks that could lead to espionage, disruption of essential services, or even compromise military operations.
- A firewall is a cybersecurity solution that protects your network from unauthorized access to mitigate the risk from cyber attacks(national threat).

https://www.dhs.gov/topics/cybersecurity
https://www.fortinet.com/resources/cyberglossary/what-does-a-firewall-do#:~:text=Basically%2C%20a%20firewall%20is%20a,to%20a%20more%20secure%20environment.

What are some common types of Firewalls and how do they work?

Next-Generation Firewall (NGFW)

• NGFW defend the network perimeter by using deep packet inspection (DPI) and intrusion prevention systems (IPS) to detect sophisticated threats, including hidden attacks within applications and encrypted traffic (inbound/outbound traffic.).

Web Application Firewall (WAF)

- Firewall helps protect web applications by) filtering and monitoring HTTP traffic between a web application and the Internet. It acts as a reverse proxy between the web application and the internet.

Cloud Firewalls

- Filter traffic between cloud services, data centers, and remote users while enforcing security policies across hybrid and multi-cloud environments, often operating as Firewall-as-a-Service (FWaaS) to provide specialized cloud protection.

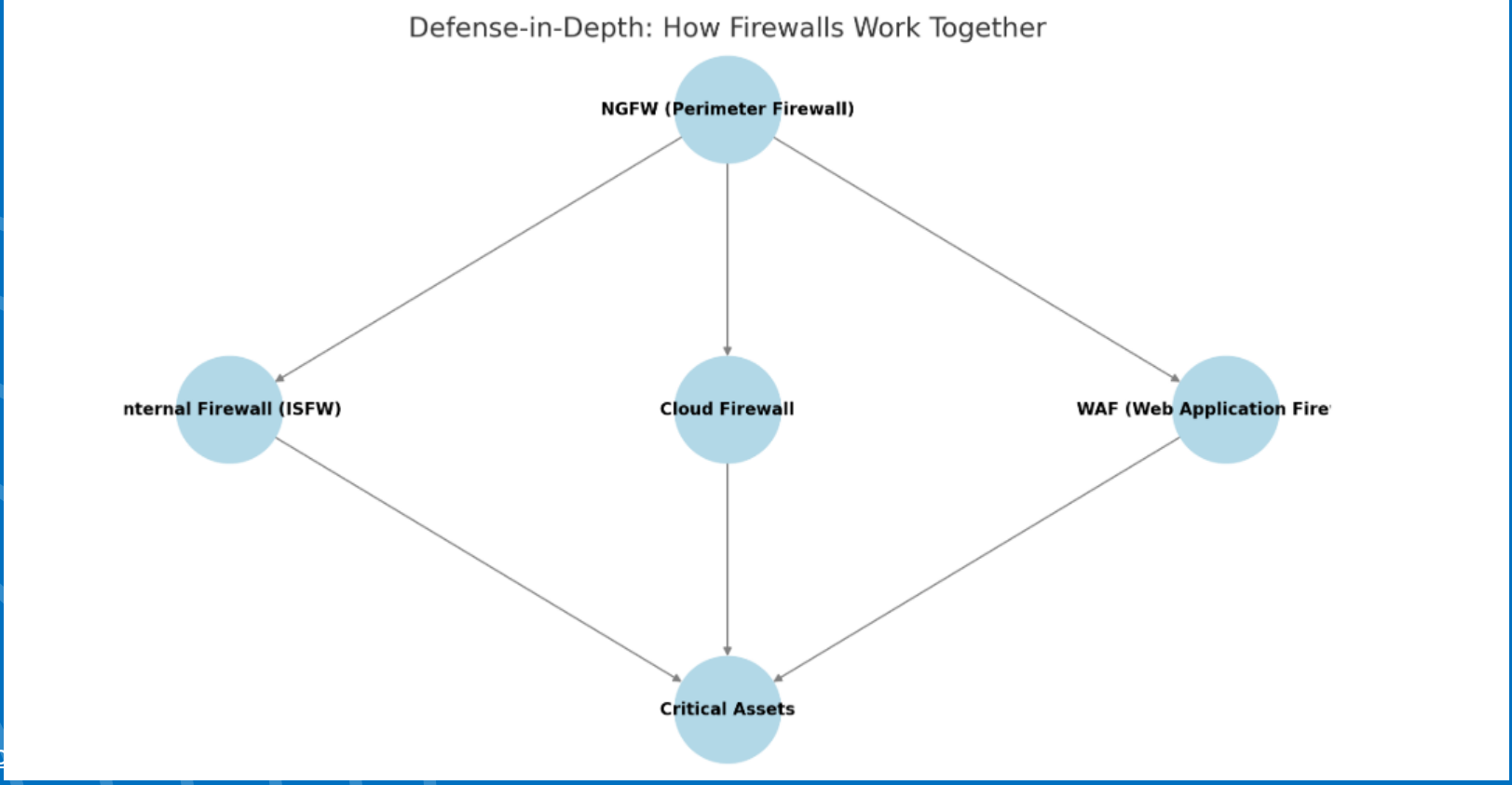
Internal Firewalls

- An internal firewall is a type of network firewall that operates by regulating the traffic within an organization's internal network based on security policies. Mitigates insider threats and stops the spread of breaches inside the network.

https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

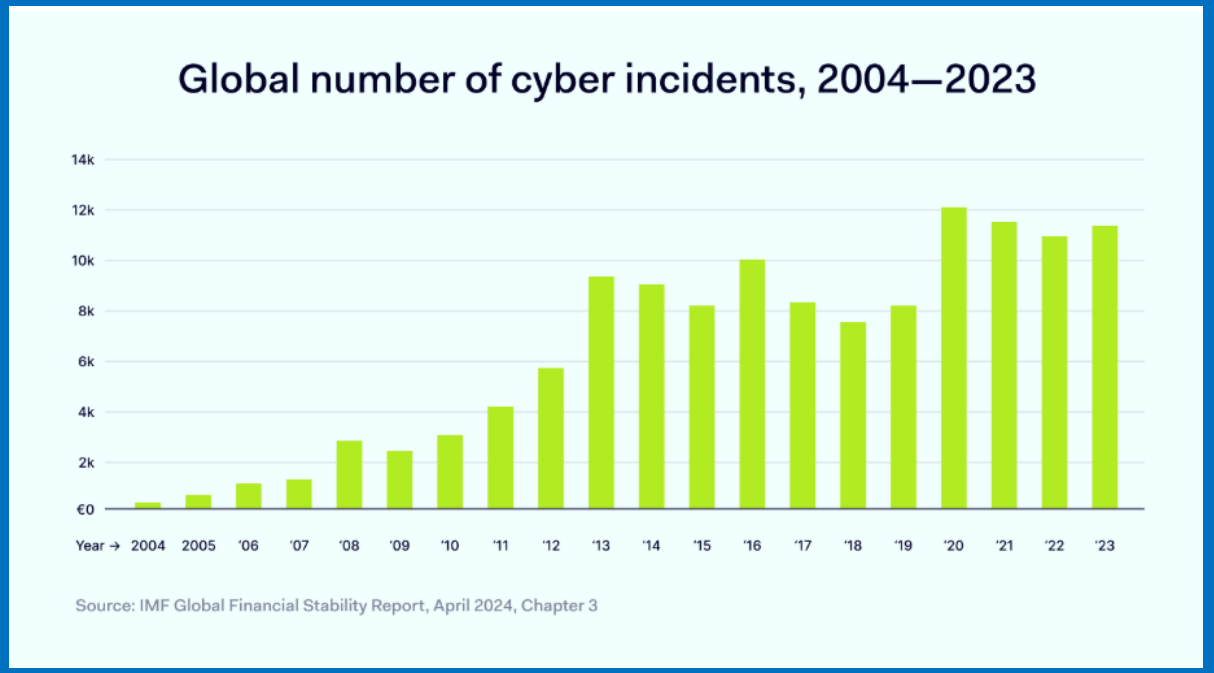
How They Work Together in National Security (DiD)

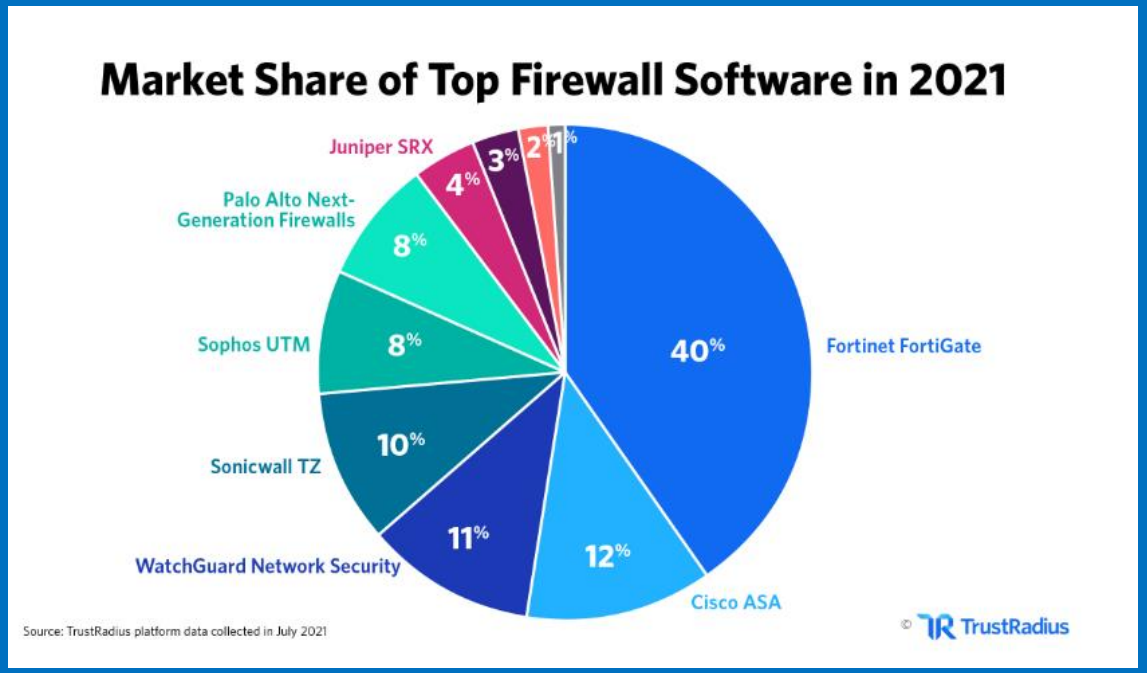
✓ NGFW blocks external cyberattacks at the perimeter.
✓ Internal Firewalls isolate sensitive systems and prevent lateral movement and isolating compromised segment if there is a breach.
✓ Cloud Firewalls protect hybrid environments and secure remote users.
✓ WAF defends web applications and APIs from targeted cyberattacks.



https://www.paloaltonetworks.co

Statistics regarding the use of Firewalls...





Examples & Final Points

U.S. Government Agencies – Protection Against Cyber Espionage

Agencies like the Department of Defense (DoD) and NSA use NGFWs and internal firewalls to prevent nation-state cyberattacks from adversaries like China, Russia, and Iran.

Example: In 2020, the SolarWinds cyberattack infiltrated U.S. government networks. Better internal firewall segmentation could have prevented lateral movement, limiting the breach's impact.

Power Grid Protection – Preventing Cyber Sabotage

Firewalls defend critical infrastructure, such as SCADA systems controlling power grids, water plants, and military bases.

Example: The 2015 Ukraine power grid attack—a Russian-linked cyberattack bypassed weak firewalls, causing a massive blackout. Stronger firewall policies could have stopped the attackers from gaining deeper access.

Election Security – Preventing Foreign Interference

Firewalls block unauthorized access to voting systems and databases.

Example: During the 2020 U.S. elections, agencies like CISA used NGFWs and WAFs to defend election infrastructure from cyberattacks aimed at disrupting voting systems.

- **Firewalls are a critical component of a layered security approach, blocking unauthorized access, ensuring safe traffic, and supporting compliance. When combined with other security measures like antivirus software, IDS/IPS, MFA, and encryption, they help create a robust defense strategy.**
- **Proper configuration, ongoing monitoring, and regular updates are essential to maintain firewall effectiveness and adapt to evolving threats.**

Thank you!

Any Questions?