Hardware Firewalls

DSCI 519

Sean Trujillo

USC Viterbi
School of Engineering

University of Southern California

Concept

- Physical hardware that enforces network facets of security policies
- Standalone unit
- Single “door” to internal network
- Congregation of all network traffic
- Active effort towards true isolation for strengthened security

Advantages

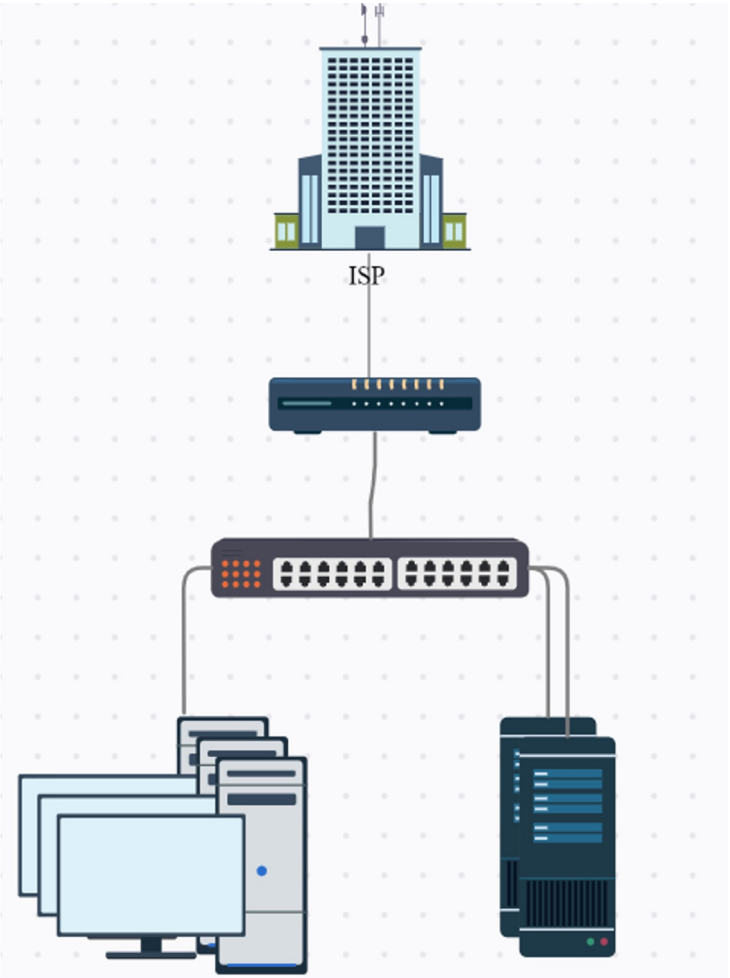
- Firewall enforcement is consistent and uniform
  - No risk of single host system having outdated configuration
- Separation of client from firewall hardware protects from immediate threat
- Single point of management of network-related security policy
- All data flow goes through firewall; everything subject to scrutiny
- Improved performance of client systems through freeing up resources
- Allows for a security-first kernel to be implemented wholly

General Firewall Functionality

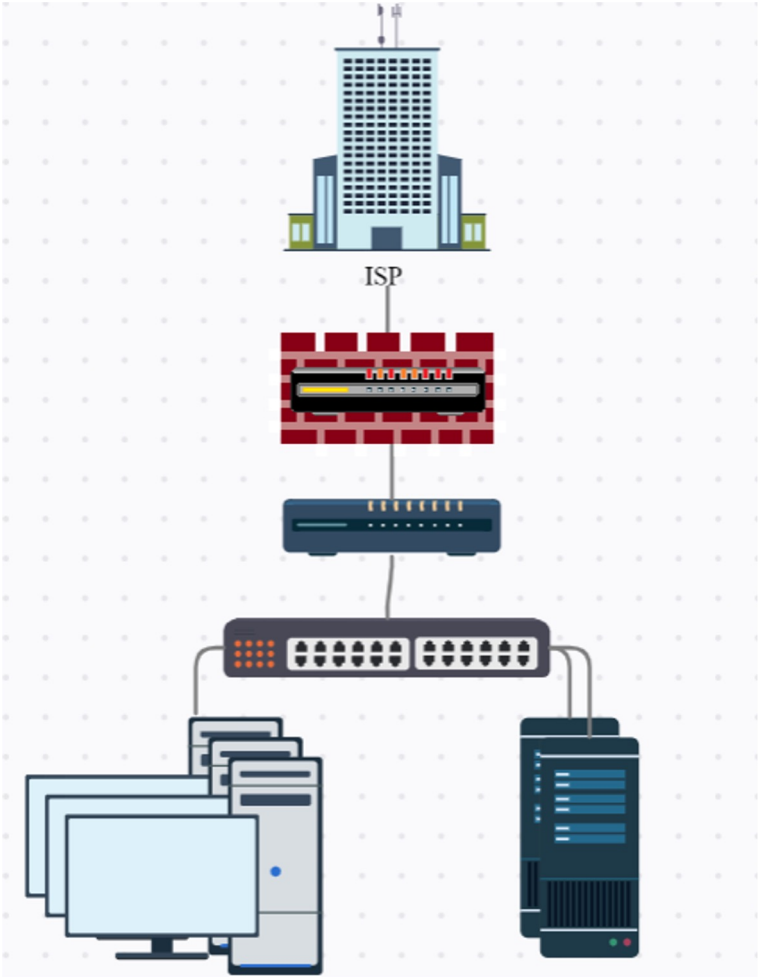
- First-in-line in a local network when building access to external networks
- All data packets to/from internal systems pass through the hardware
  - All packets logged, scrutinized according to security policy
- Packets are filtered according to accepted parameters set by security staff (IPs, domain names, protocols, ports, keywords, etc.)
- Approved packets are allowed through

What About Software Firewalls?

- Software firewalls are configured and operate within each system in need of protection
- Commercial OS' have firewall capabilities, making cost minimal
- Perform the same basic functionality as hardware firewalls on client hardware instead
- No isolation of firewall; subversion of firewall means immediate subversion of system and vice versa
- Flawed due to its "good enough", add-on approach



VS



Software Firewall Incident

COLUMBIA — S.C. Department of Revenue Director James Etter's office phone rang late in the morning on Oct. 10, 2012, with a call that would change the course of how South Carolina approached cybersecurity over the next decade.

On the line were U.S. Secret Service agents from Atlanta, who said someone had hacked his agency, responsible for all personal and business tax records in the state.

"How could this happen?" Etter thought.

Using an email with a link encrypted with malware, cyber criminals made off with the income tax returns of 6.4 million South Carolina residents and businesses — exposing 3.6 million Social Security numbers, impacting more than three-quarters of the state's population at the time — and 387,000 credit and debit card numbers.

vs Reference Monitor

- Hardware firewalls blur the line between subjects and objects
  - Subject because each packet is sent as act of intent to append, access, modify data
  - Object because packets themselves contain data
- Hardware firewalls wholly support audit trails
- Also uses an authorization database (comparing packet characteristics against those deemed acceptable)
  - ACL that explicitly lists which IPs and ports are accessible

vs Reference Monitor cont.

- Hardware firewalls are built specifically with security in mind, rendering them tamper-proof by software
- All network data in/out of internal network must pass through, thus it is non-bypassable and always active
- Verifiability is difficult if not impossible; hardware cannot be dissected the same as software. No two units can be guaranteed identical

Disadvantages

- Expensive
- Does not offer easy verifiability
- Requires expertise/training for proper configuration
  - Harms productivity and/or weakens network if improper
- Offers means of trap door implementation
- Only one aspect of protecting an internal network
- Upgrading may mean repurchasing
- Takes up physical space and power

Why not both?

- Combination of hardware and software firewalls
  - Diverse internal networks
- Extra effort needed to coordinate security policy enforcement
- Allows robust general security with a per-system basis customization

Sources

https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-hardware-firewall/

https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work

https://www.postandcourier.com/columbia/news/scs-massive-data-breach-10-years-later-questions-linger-as-investigation-remains-open/article_29dd8164-4025-11ed-9433-73cafd23fadb.html

https://www.anandsoft.com/networking/advantages-of-hardware-firewalls.html

https://www.youtube.com/watch?v=kDEX1HXybrU&ab_channel=PowerCertAnimatedVideos