A Brief History of the Firewall

Original term coined, meaning "A physical wall meant to prevent the spread of fire in a structure, from fire (n.) + wall (n.)". [1]

1851

The **Secure Computing Technology Center research group is formed** at Honeywell, working with the NSA to develop a high-assurance hardened operating system (Logical Coprocessing Kernel or LOCK) that is later featured in Secure Computing's Sidewinder firewall (1994).

1984

The Morris worm is unleashed, one of the first Internet viruses, compromising an estimated 6,000 systems (approximately 10% of the Internet at that time). This first set of viruses made clear the need for an increased focus on network security.

1988

The **first network firewalls** begin to appear, created to protect "private networks by securing gateway servers to external networks like the Internet." [2]

Late 1980s

The **first security firewalls** —IP routers with filtering rules—were put to use. "The first security policy was something like the following: allow anyone 'in here' to access 'out there.' Also, keep anyone (or anything I don't like) 'out there' from getting 'in here.'" [3]

Appearance of the **first commercial firewall**, the DEC SEAL, a hybrid firewall using application proxies and packet filters.

Early1990s

The **first of the "stateful" firewalls** appear. Check Point Software Technologies originates the term "stateful inspection."

1992

IDC coins the term UTM (unified threat management), and several security vendors follow suit, beginning to market their firewalls that run multiple security functions running on a single appliance as a UTM.

1994

2004

Results of first **widespread analysis of firewall management practices** are published, including statistics like: "93% [of supervisors of firewall administrators] felt their firewalls contained at least one category of error and 70% felt that it was likely their rulebases contain undetected errors." [5]

Gartner defines the Next-Generation Firewall as "a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks." [4]

2009

Gartner releases a forecast that says "Through 2018, more than 95 percent of firewall breaches will be caused by misconfigurations, not firewall flaws." [6]

2012

The key finding from Dark Reading's **Death of the Perimeter** poll is that "the classic view about what constitutes a network boundary has given way to a new metaphor. For 55% of respondents, the network perimeter has evolved to a seemingly boundless space "anywhere and everywhere data is located" that incorporates what is on the device, in a cloud, or on a server (51%) and how the data gets there and back (4%)." [7]

2014

illumio

Resources

[1] Online Etymology Dictionary.
[2] "Firewall Security," Veracode.com.
[3] Frederic Avolio, "Firewalls and Internet Security," The Internet Protocol Journal, Vol. 2, No. 2.
[4] John Pescatore and Greg Young, "Defining the Next-Generation Firewall," Gartner RAS Core Research Note G00171540, Oct. 12, 2009.
[5] Michael J. Chapple, John D'Arcy, and Aaron Striegel, "An Analysis of Firewall Rulebase (Mis)Management Practices," ISSA Journal, February 2009.
[6] "NetCitadel Unveils Industry's First Software Defined Security Solution for Centralized Security Intelligence in Cloud, Virtual and Physical Environments," NetCitadel press release, Jan. 29, 2013.
[7] Marilyn Cohodas, "Poll: The Perimeter Has Shattered!," DarkReading, Dec. 8, 2014.