Discussion 2

Initial Post

All companies need to pay some consideration to the security of their networked devices. The traditional approach has been to have a local area network (LAN) of trusted devices separated from the ‘Wild West’ of untrusted devices in the Internet by use of a firewall; this is known as ‘perimeterisation’.

There are many types of firewall (Schultz, 2021), and one of the most widely adopted is based on packet filtering which operates at the network at the network and transport layer of the OSI stack. For example, it is a major aspect of the ‘Great Firewall of China”. (Ensafi et al, 2015) A packet filtering firewall examines (usually only) incoming TCP/IP data packets and allows or denies entry to the LAN based on a set of access list rules. These rules are based solely on the source and destination protocol, IP address and port number. The advantages of this type of firewall are:

· They are very efficient i.e., consume few resources and are therefore cheap to deploy.

· Packet filtering is available on a wide range of devices with routing capacity.

The disadvantages include:

· They are susceptible to fragmentation attacks (Cohen, 1995)

· Continued maintenance of blacklisted IP addresses is challenging.

· Correct configuration and testing of filtering rules can be difficult.

· Due to the limitations of the information examined in a packet, some desirable rules are not possible to enforce.

To protect networks containing the most highly sensitive data such as those in the military, those controlling national utilities such as power grids or voting systems, air gapping is a popular technique. Air gapping involves completely isolating a network to prevent it establishing any external connections and since there is no connection to the Internet or to any network connected to the Internet, hacking these systems should be far more challenging (Sarkar, 2019). Whilst at first glance, air gapping would seem to be a very secure strategy, there have been several instances of air gapped networks being hacked. Since transfer of data between the Internet and an air gap network involves the use of a file transfer device such as a USB drive, this is a potential weakness and has indeed been the focus of several successful hacks on air gap networks e.g. Stuxnet (Kushner, 2013) and others (Dorais-Joncas Munõz, 2021).

References

Cohen, F., (1995). Internet holes—Part 2: Packet fragmentation attacks. *Network Security*, *1995*(9), pp.14-16.

Dorais-Joncas, A. and Munõz, F., (2021). *Jumping the Air Gap*.

Ensafi, R., Winter, P., Mueen, A. and Crandall, J.R., (2015). Analyzing the Great Firewall of China Over Space and Time. *Proc. Priv. Enhancing Technol.*, *2015*(1), pp.61-76.

Hinglaspure, R.P. and Burghate, B.R., (2014). Analysis of packet filtering technology in computer network security. *International Journal of Computer Science and Mobile Computing*, *3*(4), pp.1302-1927.

Kushner, D., (2013). The real story of stuxnet. *ieee Spectrum*, *50*(3), pp.48-53.

Sarkar, S., Chakraborty, A., Saha, A., Bannerjee, A. and Bose, A., (2019), August. Securing Air-Gapped Systems. In *International Ethical Hacking Conference* (pp. 229-238). Springer, Singapore.

Schultz, E.E., (2021). 83-10-41 Types of Firewalls. Available at : https://metacept.com/wp-content/uploads/2020/03/Types-of-Firewalls.pdf [Accessed: 31st October 2022].

Peer Responses

Steve, thanks for sharing an insight into packet-filtering firewalls.

One can agree that companies must implement cyber security solutions at the network's perimeter to separate the local area network from the internet of unwanted threats. As mentioned, the security of networked devices and the type of firewalls to implement are essential as the data and resources are protected.

Packet-filtering firewalls are known to be efficient, transparent, and affordable. They are also known to operate and work best where application security is not a concern. The focus is to block or accept data packet transmission entering and leaving the network based on protocols, and user define rules, ports and IP addresses (UNext Editorial Team Content Writer, 2020).

Depending on the user-defined packet-filtering rules, Static, Dynamic and Stateful are three types of rules assigned. Static packet filtering firewall rules set port connections between networks in the open or closed form by manual configuration. Dynamic packet filtering firewall rules open ports when a connection is established and closes when no link is available; otherwise, ports can remain closed by default. Stateful firewalls can identify UDP and TCP streams of traffic entering between points and distinguish between malicious and legitimate traffic flow (SecurityX, n.d.). One drawback with static and dynamic packet filtering firewall rules is their inability to offer address spoofing protection from hackers. Stateful packet filtering rules do eliminate some risk of address spoofing techniques.

After a small amount of research on air-gap techniques, the understanding is that Hackers used USB drives to breach computer networks by installing malware. To avoid these attacks, access to USB drives on air-gap systems should be disabled and only enabled for internal use by cyber security teams as a policy (Gillis, 2022).

References

Gillis, A. S., 2022. *Air Gap (Air Gapping).* [Online]
Available at: https://www.techtarget.com/whatis/definition/air-gapping
[Accessed 4 November 2022].

SecurityX, 2021. *Types of Firewall Packet Filtering Firewall.* [Online]
Available at: https://www.securityx.ca/blog/what-is-packet-filtering-its-types-benefits/
[Accessed 04 November 2022].

UNext Editorial Team Content Writer, 2020. *Packet Filtering Firewall.* [Online]
Available at: https://www.jigsawacademy.com/blogs/cyber-security/packet-filtering-firewall/
[Accessed 04 November 2022].

Summary Post

John rightly points out that there are different types of packet filtering firewall, and this led me to research the difference between stateless and stateful packet filtering. It's important to point out here that according to my research, dynamic packet filtering is another term for stateful inspection (Sheldon, 2021).

Stateless packet filtering filters traffic using rules based on source and destination protocol, IP address and port number only. Each packet is treated independently with no references to any other packet entering or leaving the network.

Stateful packet inspection filters traffic using state and context information.

State is defined by Fortinet, (N.D.) as:

"…the most recent or immediate status of a process or application"

In the case of the firewall, it examines the inside of a data packet and stores specific flags e.g., those used to initiate a three way handshake to establish a connection in a TCP in a TCP connection.

Context refers to other data gathered from inspecting the data packet such as IP addresses, port numbers and sequence numbers (Roeckl, 2004).

The key to stateful inspection is that storing state and context data in the state table, plus it's more powerful logging capabilities give it several advantages over stateless packet filtering. These are:

· Only inbound traffic which has a corresponding inbound entry in the state table is allowed.

· It is difficult for threat actors to spoof data stored in the state table.

· Ports only remain open whilst data exchange is taking place hence port sniffing, a major attack method of threat actors, cannot be used.

· Maintaining a state table prevents more types of denial of service attack than stateless inspection (Cisco Certified Expert, 2022).

The main disadvantage is that stateful inspection requires more resources.

My piece on air-gapping didn't prompt a great deal of response from either John or Jean-Pierre. In hindsight, perhaps this doesn't necessarily fall into the realm of a security technology but rather network design/topology. I included it as I found it interesting how even these types of networks, with no external data connections, have still been hacked.

References

Cisco Certified Expert. (2022). Advantages of Stateful Firewalls. Available from: https://www.ccexpert.us/firewall-security/advantages-of-stateful-firewalls.html [Accessed 13th November 2022].

Fortinet. (N.D.). Stateful Firewall. Available from: https://www.fortinet.com/resources/cyberglossary/stateful-firewall Accessed: 13th November 2022].

Sheldon, R. (2021). Stateful inspection. Available from: https://www.techtarget.com/searchnetworking/definition/stateful-inspection [Accessed 13th November 2022].

Van Rooij, G. (2001). Real stateful TCP packet filtering in IP filter. *White paper*.