Firewalls

https://education.nationalgeographic.org/resource/great-wall-china/

Agenda

- Types of Firewalls
  - Host-Based
  - Network-Based
  - Stateless
  - Stateful
- Reading Firewall Logs

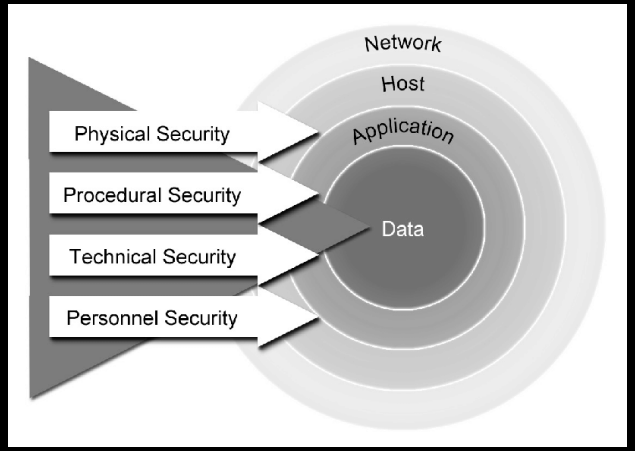
Host-Based Firewall

- Last line of defense in the world of Firewalls
- Software running on your host machines
- Sometimes packaged with OS
  - Windows Defender
  - iptables / UFW

https://answers.microsoft.com/en-us/windows/forum/all/i-love-windows-defender/3add2f03-5e9f-45a2-95e1-15bd97e2b1d8

Host-Based Firewall

- Controls traffic only on the individual host machine.
- Should be considered an additional layer of security to work with Network-Based Firewalls
- Security is all about layers



researchgate.net/figure/Classic-IT-Security-Onion_fig2_265675938

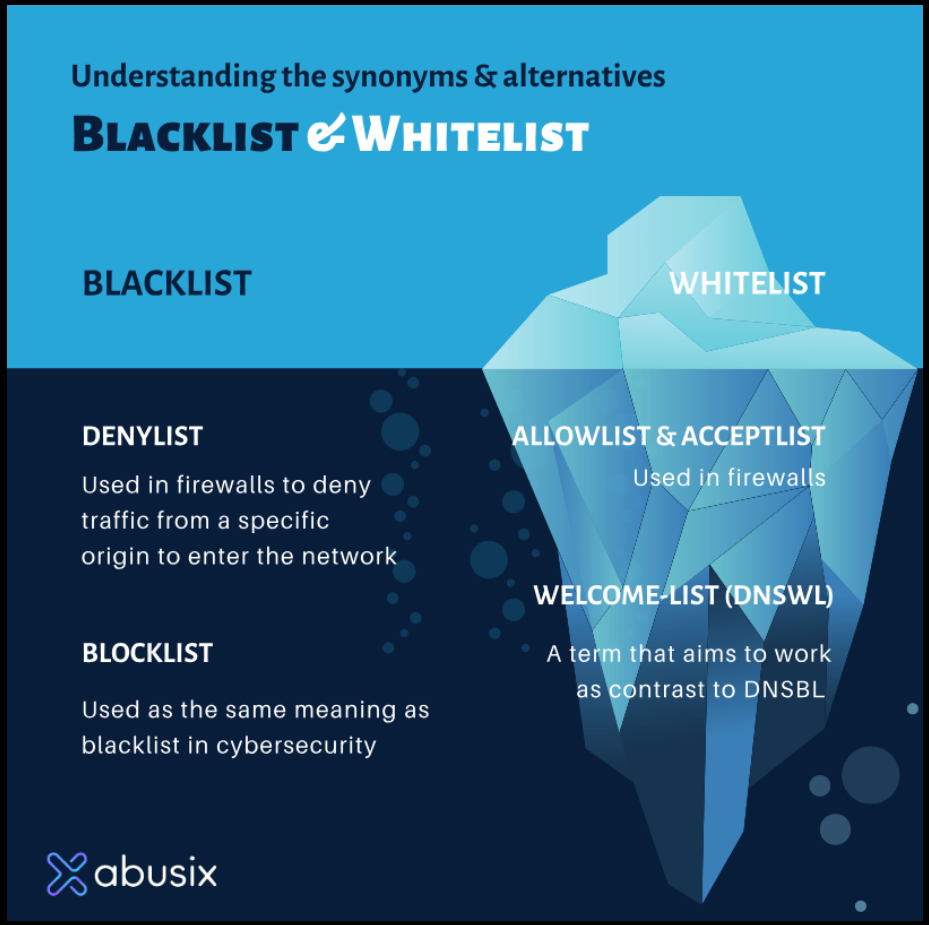
Network-Based Firewalls

- Often standalone “boxes” in your server racks. Sometimes referred to as “Hardware Firewalls”
- Can get **VERY** expensive depending on features.
- You want to place these at as many points on your network as possible and you want a mix of vendors if possible to support technology diversity

pfsense offers a free version of their firewall server you can download and tinker with!
https://www.pfsense.org/download/

https://www.pfsense.org/

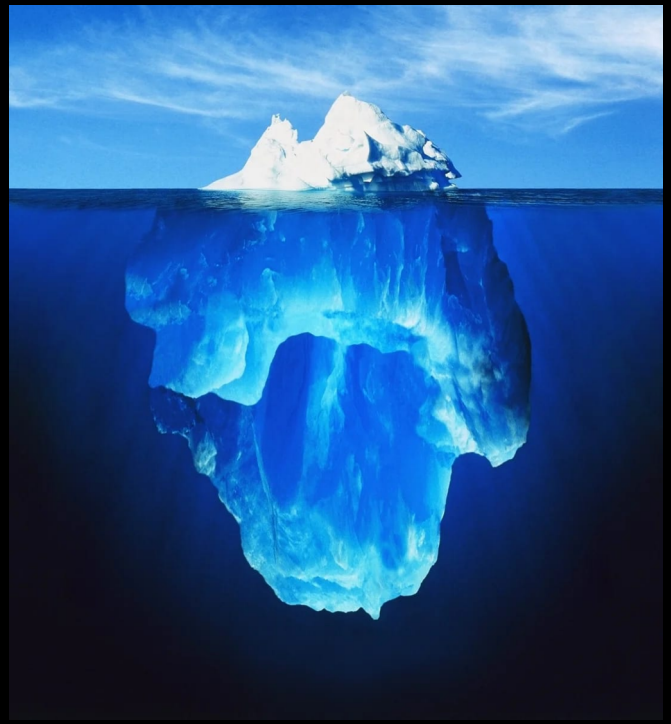
You’re Not on the List



https://abusix.com/resources/blocklists/why-changing-the-terms-blacklist-and-whitelist-isnt-as-easy-as-it-might-seem/

Iceberg Image is NOT real

It’s actually two different icebergs Photoshopped together.



https://www.youtube.com/watch?v=J4WUz7xY3rA

iptables

- The default firewall on Linux distributions
- Allows for very tight control of network traffic by allowing the user to define rules that determine how packets are handled
- Filters packets, Network Address Translation, and packet manipulation
- With great control comes great difficulty

UFW

- Uncomplicated Firewall
- A wrapper for iptables that makes managing them well… Uncomplicated.
- Provides a simplified interface for iptables
- The best Firewall configuration is the one you actually configure.
- UFW is a command-line tool GUFW provides a GUI wrapped for UFW

Stateless Vs Stateful

- Stateless
  - A stateless firewall uses the stateless protocol, and therefore doesn’t remember any previous state of data packets. Stateless firewalls filters the packet that’s passing through the firewall in real-time according to a rule list, held client-side. Each data communication is effectively in a silo.
- Stateful
  - Remembers the state of the data that’s passing through the firewall, and can filter according to deeper information than its stateless friend. It will monitor all the parts of a traffic stream, including TCP connection stages, status updates, and previous packet activity.
    After a type of traffic has been approved, it will be added to a kind of database (known as a state table or a connection table) so that the stateful firewall works to make intelligent decisions about these kinds of packets in the future. This type of firewall is also called a dynamic packet filtering firewall, and an example is the Microsoft Defender Firewall, often the default choice for PC users.

https://www.atera.com/blog/stateful-vs-stateless-firewall-whats-the-difference-and-why-does-it-matter/

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

Sep 26 18:45:47

Timestamp

When the traffic has handled. This also how the log is sorted.

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

telstar kernel:

Hostname

The hostname of the server running this firewall is **telstar**. The firewall is running as a **kernel** process.

Netfilter is the Linux kernel level process that is actually running the firewall and is controlled by iptables/UFW

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

FINAL_REJECT:

Type of Rule

This line is for a "reject" rule. You can also see DROP, INBOUND, or OUTBOUND.

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

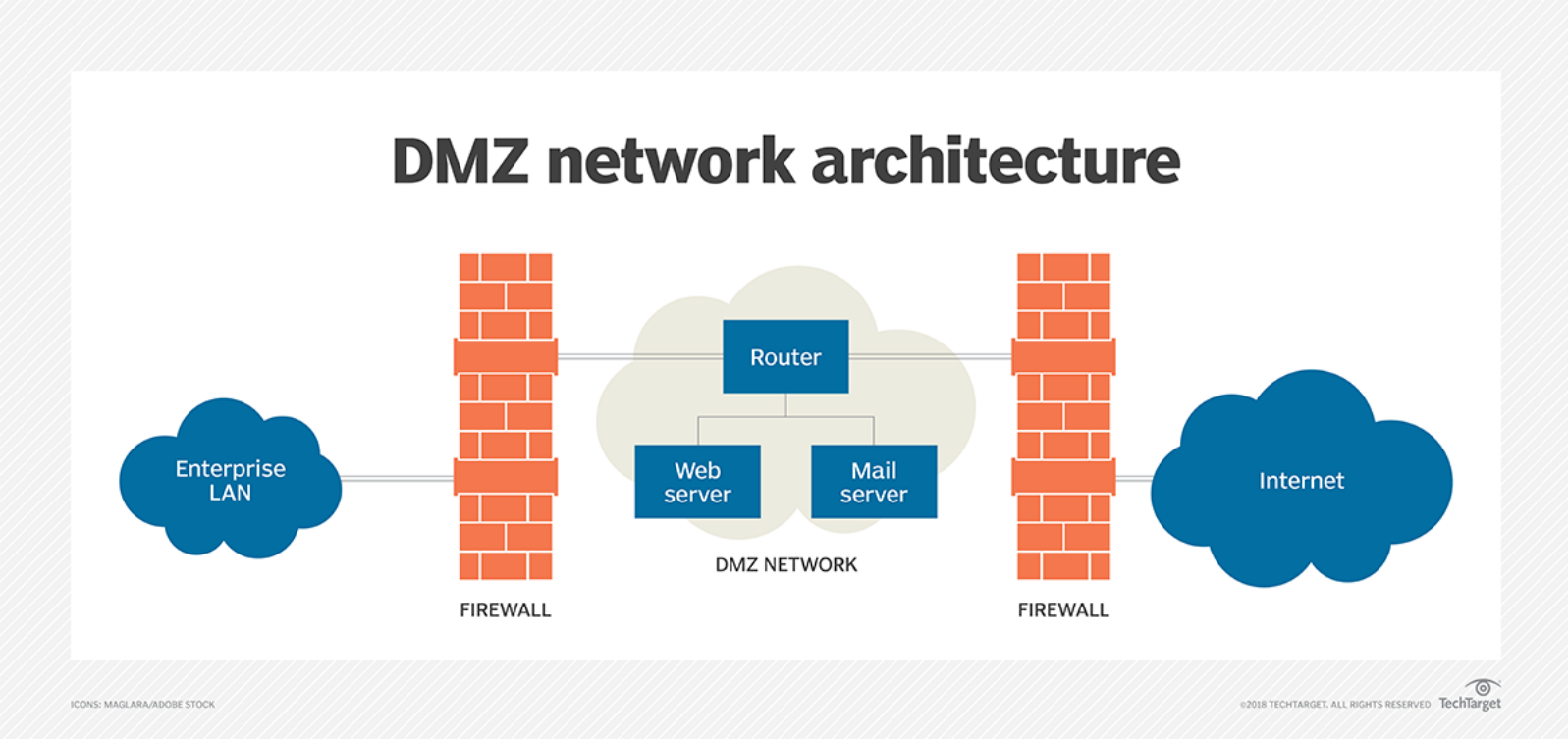
Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

IN=eth0 OUT=

Interface(s)

This packet came in on **eth0** and was rejected. If it were outbound, then it would have OUT=<interface>. If you have a rule redirecting traffic (like one that sends HTTP traffic to the DMZ) then you might see an IN= and an OUT=.

What is the DMZ?!?!



https://www.techtarget.com/searchsecurity/definition/DMZ

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

SRC=16.227.58.39 DST=4.195.210.97

Source & Destination

This packet came from 16.227.58.39 and was intended for 4.195.210.97

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 DF	PROTO=TCP	SPT=61953 DPT=9800

LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 DF

Extra Packet Info

Some more info from the packet. This data represents Length, Type of Service, Precedence bit, Time To Live, ID number, Don't Fragment (you can also see CE for Congestion)

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

PROTO=TCP

Protocol

Protocol being used. This is a TCP packet. You will also commonly see UDP and ICMP packets in firewall logs.

Firewall Logs

Sep 26 18:45:47 telstar kernel: FINAL_REJECT: IN=eth0 OUT= SRC=165.227.158.39 DST=194.195.210.97 LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023 PROTO=TCP SPT=61953 DPT=9800

Sep 26 11:45:11	telstar kernel	FINAL_ REJECT	IN=eth0 OUT=	SRC=16.227.58.39 DST=4.195.210.97	LEN=40 TOS=0x00 PREC=0x00 TTL=242 ID=9023	PROTO=TCP	SPT=61953 DPT=9800

SPT=61953 DPT=9800

Source and Destination Port

This packet originated on port 61953 and was bound for 9800.

Helpful CLI Tools for Parsing Logs

- grep – Search inside of files or STDIN for a pattern
- awk – Useful for formatting and manipulating data
- sort – Arrange data from a file in various ways
- uniq – Filter only unique lines from a sorted input
- wc – Useful for counting words, lines, characters, bytes, etc. from a file of STDIN