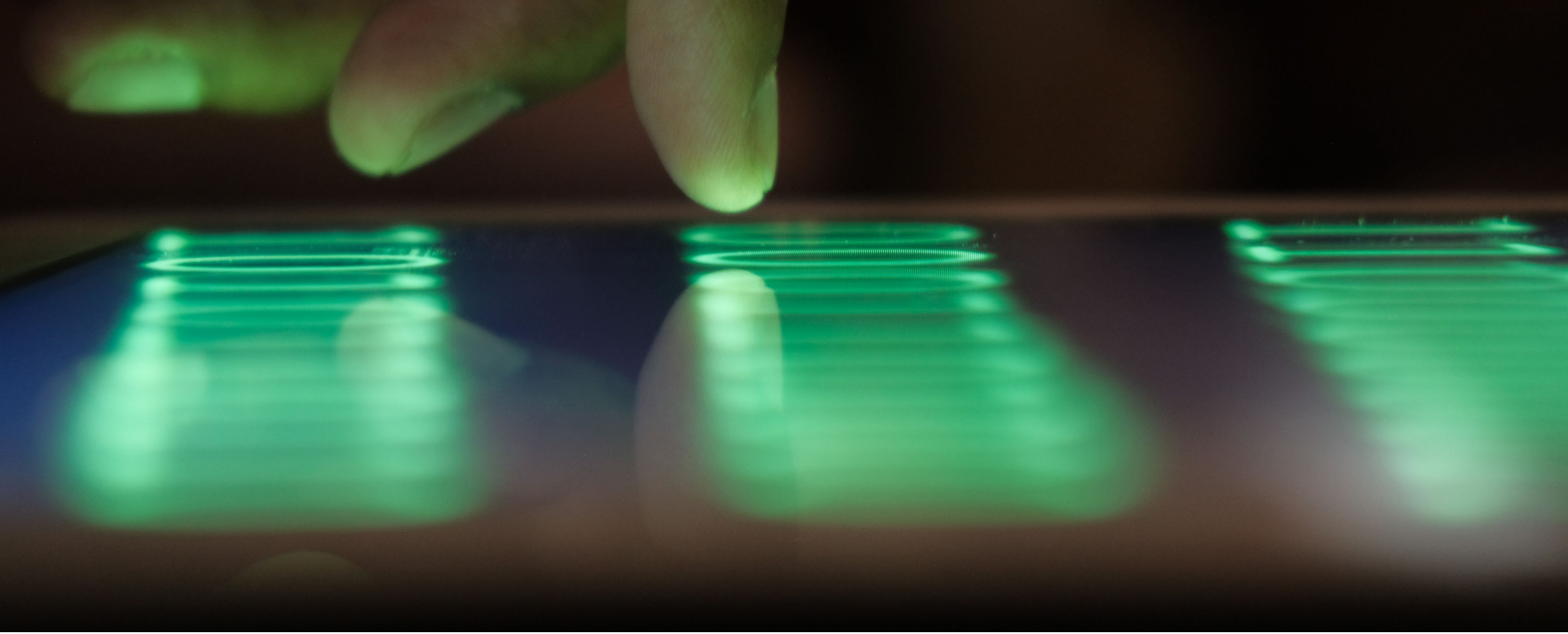

FIREWALL WHITELISTING

Lecturer: Mark Gillan

WHAT IS WHITELISTING?

- Whitelisting within a firewall is a security technique that allows only specific IP addresses or domains to access a network or system. This is in contrast to blacklisting, which blocks all IP addresses or domains except for those that are explicitly allowed.

WHAT IS IT USED FOR?

- Whitelisting is typically used to protect sensitive data or systems from unauthorised access.
- For example, a company might whitelist the IP addresses of its remote employees so that they can access the company's internal network
- A financial institution might whitelist the IP addresses of its ATM networks to prevent unauthorised withdrawals.
- Whitelisting can be implemented at the firewall level or at the application level.
- Firewall whitelisting allows or denies traffic based on the IP address of the sender or receiver.
- Application whitelisting allows or denies traffic based on the specific application or process that is trying to access the network or system.

COMPARED WITH BLACKLISTING

- Whitelisting can be a more effective security measure than blacklisting because it is more difficult for attackers to bypass.
- If an attacker is able to spoof their IP address to match a trusted IP address on the whitelist, they will still be able to access the network or system.
- However, it is much more difficult for an attacker to spoof their IP address to match a trusted application or process.

BENEFITS OF WHITELISTING IN A FIREWALL

- **Increased security:**
  Whitelisting can help to prevent unauthorised access to networks and systems. By only allowing traffic from approved IP addresses or domains, attackers are less likely to be able to gain access.
- **Reduced risk of malware infection:**
  Whitelisting can help to reduce the risk of malware infection by preventing unauthorised applications from running on the network or system.
- **Improved performance:**
  Whitelisting can improve the performance of the firewall by reducing the number of packets that need to be processed.
- **Simplified management:**
  Whitelisting can simplify the management of the firewall by reducing the number of rules that need to be configured.

DRAWBACKS

- **Complexity:**
  Whitelisting can be complex to implement and manage, especially for large networks with many different applications and systems.
- **Flexibility:**
  Whitelisting can reduce the flexibility of the network or system by limiting the number of applications and systems that can access it.
- **Support:**
  Whitelisting may require additional support from IT staff to manage and troubleshoot.

OVERALL POINTS

- Overall, whitelisting can be a valuable security measure for organizations that need to protect sensitive data or systems from unauthorised access.
- However, it is important to carefully consider the benefits and drawbacks of whitelisting before implementing it.