

SECURITY QUICK FACTS

Concept	Meaning
 Threat	Potential Cause of Harm
 Vulnerability	Weakness That Can Be Exploited
 Exploit	Method Used to Abuse a Vulnerability
 Risk	Potential Impact of a Threat
 Mitigation	Action That Reduces Risk



A threat can exploit a vulnerability, which can lead to a security incident and potential impact. Mitigation reduces the risk.

COMMON NETWORK THREATS

Threat	Main Goal / Effect
 DoS / DDoS	Disrupt Availability
 Spoofing	Impersonate a Trusted Source
 MITM	Intercept / Manipulate Communication
 Reconnaissance	Discover Systems & Services
 Password Attack	Gain Unauthorized Access
 Social Engineering	Manipulate Users



Attack techniques can target users, endpoints, network infrastructure or applications.

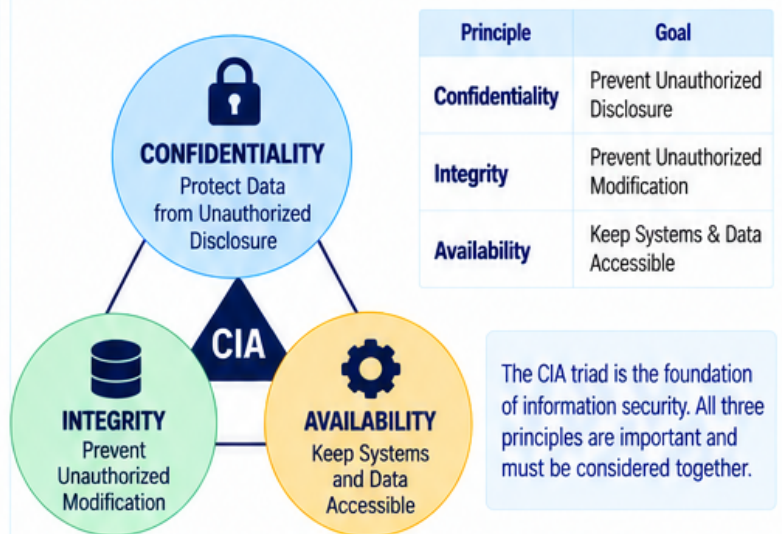
SOCIAL ENGINEERING

Technique	Description
 Phishing	Fraudulent Messages (Email)
 Spear Phishing	Targeted Phishing (Specific Individuals)
 Vishing	Voice-Based Social Engineering
 Smishing	SMS-Based Social Engineering
 Pretexting	Fabricated Scenario to Gain Trust

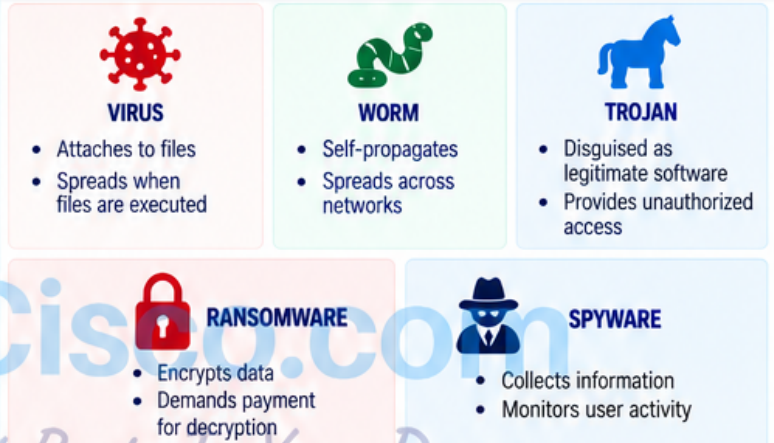


Social engineering targets people rather than relying only on technical vulnerabilities.

CIA TRIAD

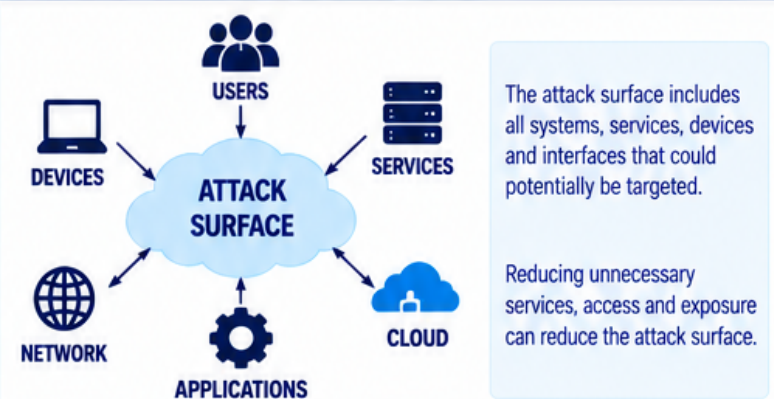


COMMON MALWARE



Malware behavior and delivery methods can overlap. Many modern attacks use a combination of techniques.

ATTACK SURFACE



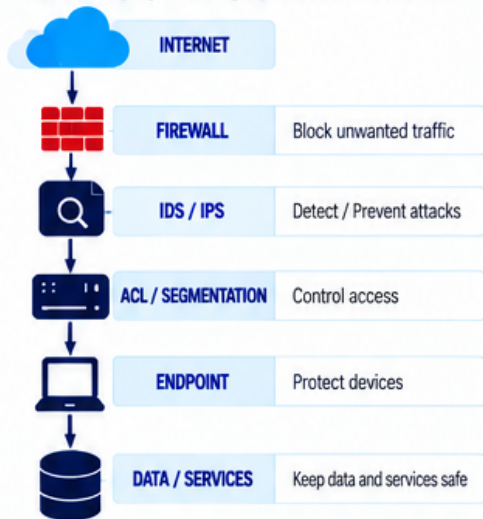
CORE SECURITY PRINCIPLES



 Always verify and test security configurations in a lab environment before applying them to a production network.

DEFENSE IN DEPTH

Defense in depth uses multiple security controls instead of relying on a single protection mechanism.



AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)

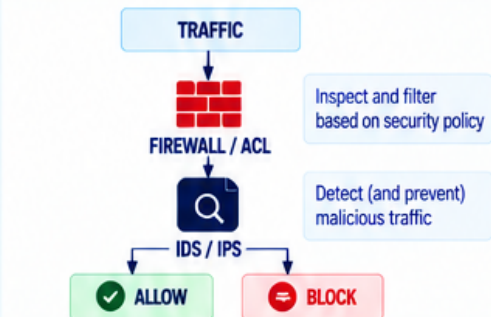
AAA provides a framework for controlling and tracking access to network resources.



AAA can be implemented using local or centralized servers or TACACS+.

FIREWALL vs ACL vs IDS/IPS

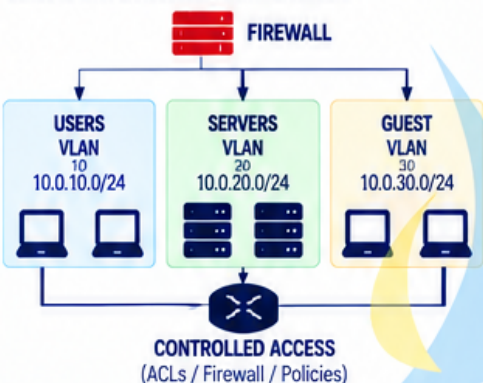
Technology	Primary Role
ACL	Permit / Deny Traffic (IP, Port, etc.)
Firewall	Enforce Security Policy (Stateful Inspection, Filtering)
IDS	Detect Suspicious Activity (Monitor and Alert)
IPS	Detect & Act on Suspicious Traffic (Monitor and Block)



Firewalls and ACLs filter traffic, while IDS centralizes and alerts. An inline IPS can actively block malicious traffic.

NETWORK SEGMENTATION

Segmentation separates networks into smaller security zones to limit unnecessary communication.



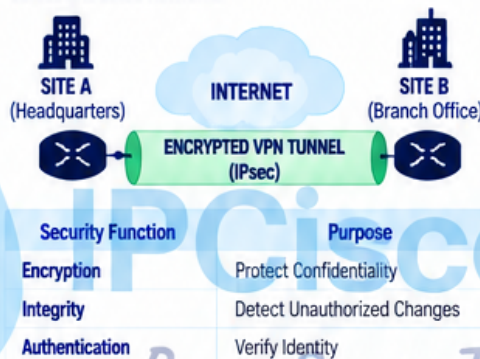
Common Segmentation Methods

VLANs, ACLs, Firewalls, VRFs, Security Zones

Segmentation can reduce the attack surface and limit the spread of an attack.

VPN & ENCRYPTION

VPNs can protect traffic between remote sites or users across untrusted networks.



Common VPN Technologies

IPsec: Site-to-Site VPN, Remote Access VPN, Widely Used. **SSL VPN**: Remote Access, Browser / Client, Application Access.

IPsec is commonly used to secure IP communications and VPN connectivity.

LAYER 2 SECURITY

Layer 2 security helps protect the network from common attacks in the local network.

Feature	Helps Protect Against
Port Security	Unauthorized MAC / Device Access
DHCP Snooping	Rogue DHCP Servers
Dynamic ARP Inspection	ARP Spoofing / Poisoning
BPDU Guard	Unwanted STP Devices
802.1X	Unauthorized Network Access



These features help prevent common Layer 2 attacks and improve local network security.

SECURE DEVICE MANAGEMENT

Network devices should be managed securely and only by authorized users.



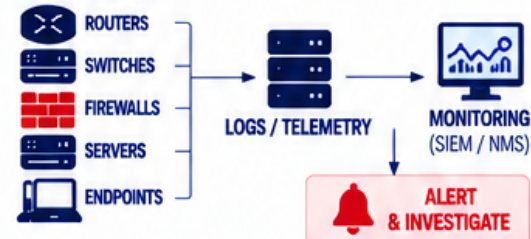
Best Practices

- Use SSH instead of Telnet
- Use HTTPS instead of HTTP
- Strong authentication (local or AAA)
- Least privilege access
- Disable unused services
- Restrict management access (ACLs)

Management traffic should be limited to authorized systems and secured with encryption and strong authentication.

MONITORING & LOGGING

Monitoring helps detect abnormal behavior and supports incident investigation.

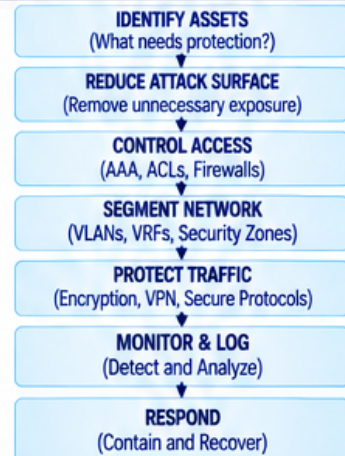


Common Monitoring Sources

Syslog Logs, SNMP Traps / Polling, Flow Data (NetFlow, IPFIX), Authentication Logs (AAA), IDS/IPS Alerts

Centralized logging and monitoring provide visibility and help identify potential security incidents.

NETWORK SECURITY FLOW



Always verify and test security configurations in a lab environment before applying them to a production network.