Network

- bgp
- dependencies
- dns
- pivoting
- tools

Fundamentals

Network Security Fundamentals

Secure the Network. Protect Everything.

1 What Is Network Security?

Network security protects the confidentiality, integrity, and availability of systems and data as they move across networks. It combines people, processes, and technologies to prevent unauthorized access, misuse, disruption, or theft.

2 Primary Goals

- Confidentiality — keep data private
- Integrity — prevent unauthorized changes
- Availability — keep services accessible
- Authenticity — verify identities and sources
- Accountability / Non-repudiation — ensure actions can be traced

3 Core Principles

- Least Privilege
- Segmentation
- Secure Configuration
- Continuous Monitoring
- Resilience

4 Common Threats

- Eavesdropping / Sniffing
- Malware / Ransomware
- Man-in-the-Middle (MITM)
- Unauthorized Access
- DDoS
- Misconfiguration
- Spoofing

5 Network Security Architecture

Internet → Edge Router → NGFW / Firewall → IDS/IPS → DMZ / Public Services → Core Switch → Internal Network / Servers → End Users

Logs, alerts, and telemetry feed into monitoring and response.

6 Defense in Depth

- Layer 5 — Data & Identity Security
- Layer 4 — Application Security
- Layer 3 — Network Security
- Layer 2 — Endpoint / Host Security
- Layer 1 — Physical Security

If one layer fails, others still reduce risk.

7 Key Security Controls

- Firewalls — filter and enforce policy
- IDS/IPS — detect and block attacks
- Network Access Control (NAC)
- VPN / ZTNA — secure remote access
- Segmentation / VLANs
- Encryption in transit
- Patch & firmware management
- Logging / SIEM visibility

8 Common Network Attacks

Attack	Description
Packet Sniffing	capturing traffic in transit
ARP Spoofing	intercepting local network traffic
DNS Poisoning	redirecting users to malicious sites
TCP SYN Flood	exhausting connection resources
IP Spoofing	faking a source address
DDoS	overwhelming a service or network

9 Secure Network Design Best Practices

- ✓ Apply least privilege access
- ✓ Use MFA for remote and admin access
- ✓ Encrypt sensitive communications
- ✓ Patch network devices and firmware
- ✓ Segment users, servers, and critical assets
- ✓ Disable unused ports and services
- ✓ Use secure baselines and hardening
- ✓ Monitor continuously and test regularly

10 OSI Model & Security

7	Application	→ WAF, API security
6	Presentation	→ encryption / certificates
5	Session	→ session management
4	Transport	→ TLS, port controls
3	Network	→ routing security, ACLs, firewalls
2	Data Link	→ VLANs, 802.1X, MAC controls
1	Physical	→ cable, device, facility protection

11 VPN / ZTNA — How It Works

User Device → Encrypted Tunnel / Broker → Gateway / ZTNA or VPN Server → Internal Apps

Benefits

- ✓ Secure remote connectivity
- ✓ Protects data in transit
- ✓ Supports identity-aware access
- ✓ Limits exposure of internal services

12 Firewall Types

- Packet Filtering Firewall — filters by IP, port, protocol
- Stateful Inspection Firewall — tracks connection state
- Application / Proxy Firewall — inspects higher-layer traffic
- Web Application Firewall (WAF) — protects web apps and APIs
- Next-Generation Firewall (NGFW) — adds awareness, IPS, and app control

13 Useful Tools

- Wireshark → packet analysis
- Nmap → network discovery and scanning
- Zeek → network security monitoring
- Suricata / Snort → IDS/IPS
- pfSense / OPNsense → firewall platforms
- NetFlow / sFlow → traffic visibility

14 Key Takeaway

A secure network is built with layered defenses, strong identity controls, visibility, and continuous improvement.

Network security is not a product — it is an ongoing process.

15 Quick Checklist

- ✓ Firewalls configured and reviewed
- ✓ IDS/IPS enabled and tuned
- ✓ MFA enforced
- ✓ Patches applied regularly
- ✓ Logs collected and monitored
- ✓ Network segmented appropriately
- ✓ Admin access secured
- ✓ Config backups maintained
- ✓ Security testing performed

Daily Red Team — Learn. Defend. Outthink. — dailyredteam.io

From:
https://fortier-family.com/wiki/ - **Warnaud's Wiki**

Permanent link:
https://fortier-family.com/wiki/cybersecurity/network

Last update: **2026/09/21 09:47**