Network Devices & Security Concepts

Critical Differences for Security+

Core Network Devices

Switch (Layer 2)

What it does: Connects devices within a network using MAC addresses

How it works:

- Learns which MAC addresses are on which ports
- Forwards traffic only to the intended recipient
- Reduces network congestion

Security Features:

- Port security (limit MAC addresses per port)
- VLANs (virtual network segmentation)
- Port mirroring (for monitoring)

Security Risks:

- MAC flooding attacks
- ARP spoofing
- CAM table overflow

Remember: Switch = Layer 2 = MAC addresses

Router (Layer 3)

What it does: Connects different networks using IP addresses

How it works:

- Examines destination IP address
- Determines best path to destination
- Forwards packets between networks

Security Features:

- Basic packet filtering (ACLs)
- NAT (Network Address Translation)
- Route filtering

Remember: Router = Layer 3 = IP addresses

Firewall (Layer 3/4 or Layer 7)

What it does: Controls traffic flow based on security rules

Types:

1. **Packet-Filtering Firewall** (Layer 3/4)
    - Examines IP addresses and port numbers
    - Simple allow/deny rules
    - Stateless (doesn't track connections)
2. **Stateful Firewall** (Layer 3/4)
    - Tracks connection state
    - Knows if traffic is part of established connection
    - More intelligent than packet-filtering
3. **Next-Gen Firewall (NGFW)** (Layer 7)
    - Deep packet inspection
    - Application awareness
    - Integrated IPS
    - Most advanced

Remember: Firewall = Traffic cop that decides what gets in/out

---

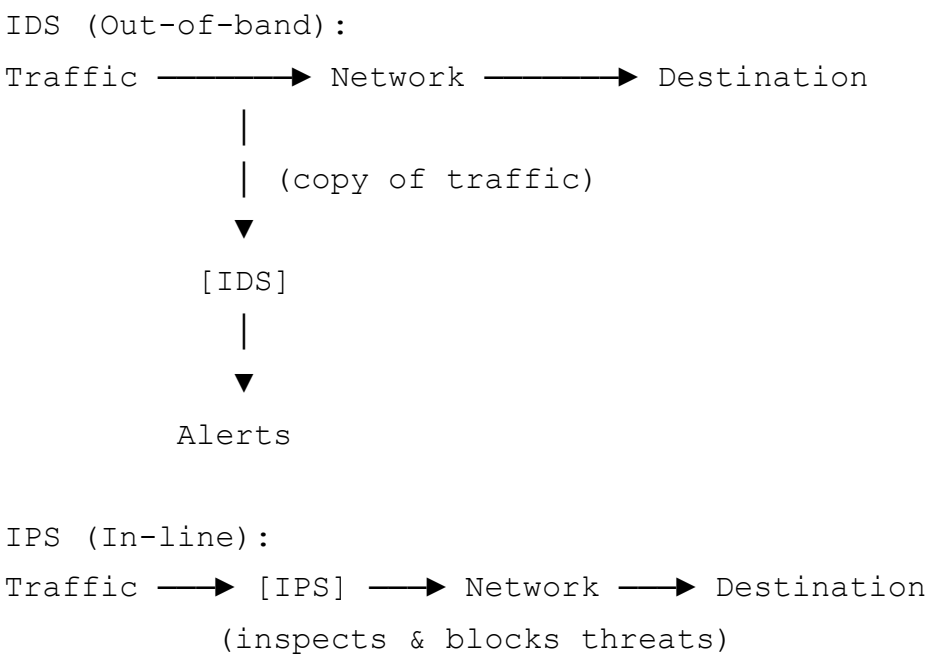
Security Devices - CRITICAL FOR SEC+!

IDS vs IPS ⭐⭐⭐ (KNOW THIS COLD!)

Feature	IDS (Detection)	IPS (Prevention)
Stands for	Intrusion Detection System	Intrusion Prevention System

Feature	IDS (Detection)	IPS (Prevention)
Position	Out-of-band (monitors copy of traffic)	In-line (traffic flows through it)
Action	**PASSIVE** - Detects & alerts only	**ACTIVE** - Detects & blocks
Analogy	Security camera	Security guard
Pro	Can't break network (false positives don't block)	Stops attacks automatically
Con	Doesn't stop attacks	False positives can block legitimate traffic
Response Time	After the fact	Real-time
Use Case	Monitoring, forensics, low risk	Active defense, high security needs

Visual Comparison



Exam Scenarios

Scenario 1: "You need to monitor for attacks but cannot risk blocking legitimate traffic"

- **Answer:** IDS (passive, alert-only)

Scenario 2: "You need to automatically stop attacks in real-time"

- **Answer:** IPS (active, in-line)

Scenario 3: "False positives from this device could disrupt business operations"

- **Answer:** IDS (can't block traffic)

Scenario 4: "This device must sit in-line with traffic"

- **Answer:** IPS

Other Security Devices

WAF (Web Application Firewall) ⭐⭐

Layer: 7 (Application)

What it protects: Web applications and websites

Blocks:

- SQL injection
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- File inclusion attacks

Difference from regular firewall:

- Regular firewall: Protects the network (Layers 3-4)
- WAF: Protects the web application (Layer 7)

Proxy Server ⭐

Types:

1. **Forward Proxy** (Outbound)
    - Users → Proxy → Internet
    - Content filtering
    - Caching
    - Hides user IPs
2. **Reverse Proxy** (Inbound)
    - Internet → Proxy → Internal Servers
    - Protects web servers
    - Load balancing
    - SSL offloading

Security Benefits:

- Content filtering
- Anonymity
- Caching (performance)
- Additional layer of protection

Load Balancer ⭐

What it does: Distributes traffic across multiple servers

Security Benefits:

- High availability (redundancy)
- Helps mitigate DDoS attacks
- Can perform health checks

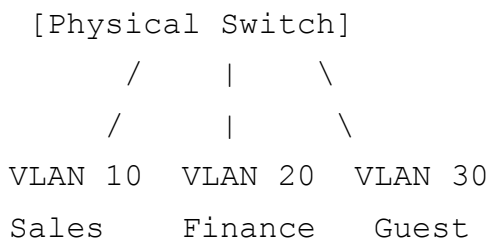
Not primarily a security device, but provides resilience

VLANs (Virtual LANs) ⭐⭐⭐

What Are VLANs?

Virtual networks created on a physical switch

Visual Example



How It Works

- Same physical switch
- Devices on different VLANs can't communicate directly
- Must go through router/firewall to cross VLANs

Security Benefits

Network Segmentation!

- Isolates departments (Sales can't access Finance)
- Contains malware (can't spread between VLANs)
- Separate security policies per VLAN
- Reduces broadcast domains

Common VLAN Setup

- VLAN 10: Internal employees
- VLAN 20: Servers/IT
- VLAN 30: Guest WiFi
- VLAN 99: Management traffic

Key Security Principle: Segmentation limits blast radius of attacks

---

Access Control Lists (ACLs) ⭐⭐

What They Are

Rules that permit or deny traffic based on:

- Source IP
- Destination IP
- Protocol
- Port number

Example ACL

```
PERMIT TCP from 192.168.1.0/24 to ANY port 443
DENY   TCP from ANY to ANY port 23
PERMIT ICMP from 10.0.0.0/8 to ANY
DENY   ALL from ANY to ANY
```

Where They're Used

- Routers (basic filtering)
- Firewalls (more advanced)
- Switches (port security)

Security Concept

Implicit Deny: If not explicitly allowed, it's blocked (best practice)

DMZ (Demilitarized Zone) ⭐⭐

What It Is

A buffer network between the internet and internal network

Visual Diagram

```
Internet ⟶ [Firewall] ⟶ [DMZ] ⟶ [Firewall] ⟶ Internal Network
                          (Web Server)
                          (Mail Server)
```

Purpose

- Public-facing servers go in DMZ
- Adds extra security layer
- If DMZ is compromised, internal network is still protected

What Goes in the DMZ

✅ Web servers
✅ Email servers
✅ FTP servers
✅ DNS servers (external-facing)

❌ Internal databases
❌ File servers
❌ Domain controllers

Quick Comparison Chart

Device	Layer	Function	Security Role
Switch	2	Connect devices in network	Port security, VLANs

Device	Layer	Function	Security Role
Router	3	Connect networks	Basic filtering, NAT
Firewall	3/4/7	Control traffic	Permit/deny rules
IDS	Various	Monitor traffic	Detect & alert
IPS	Various	Inspect traffic	Detect & block
WAF	7	Protect web apps	Block web attacks
Proxy	7	Intermediary	Filter, cache, hide IPs

Exam Tips – Common Questions

Q: Device monitors traffic and alerts but doesn't block?
→ IDS

Q: Device actively blocks malicious traffic in real-time?
→ IPS

Q: Protects against SQL injection on a website?
→ WAF (Web Application Firewall)

Q: Connects devices on same network using MAC addresses?
→ Switch

Q: Routes packets between different networks?
→ Router

Q: Prevents Sales VLAN from accessing Finance VLAN?
→ Network segmentation / VLANs

Q: Buffer zone between internet and internal network?
→ DMZ

Memory Aids

IDS = I Detect and Shout (but don't block)
IPS = I Prevent and Stop (blocks threats)

Layer 2 = Switch = MAC
Layer 3 = Router = IP

Layer 4 = Firewall = Ports

Layer 7 = WAF = Web Apps

VLAN = Virtual LAN = Segmentation = Security