

Securing Networks

AP Cybersecurity ■ Unit 3

AP Cybersecurity



Securing Networks

What we will cover

- 1 Network attacks
- 2 Policies & wireless security
- 3 Segmentation & the DMZ
- 4 Firewalls
- 5 Access control lists
- 6 Detecting attacks

1 Network attacks

The classic network attacks

ARP poisoning 地址解析投毒
fake ARP messages divert traffic – an **on-path attack** 中间人攻击

DNS poisoning 域名投毒
a fake record redirects users – **credential harvesting** 凭据收集

MAC flooding 物理地址泛洪
floods a **switch** 交换机 into broadcast mode – **eavesdropping** 窃听

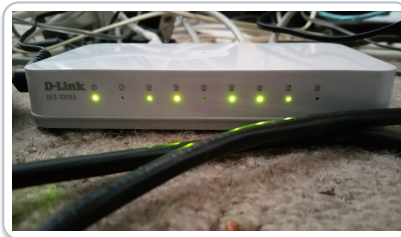
Smurf attack
ICMP to the broadcast address – a **DoS** 拒绝服务; many at once = **DDoS** 分布式拒绝服务

Pair each attack with its tell-tale sign: ARP poisoning = one IP with two MACs; MAC flooding = a surge of new MACs; DNS poisoning = an unexplained drop in web traffic.

Why weak networks fall

Adversaries exploit weak networks to flood, map, or spoof devices.

- a physical data port with no port security lets an attacker plug in
- an open port lets them install a **rogue access point** 非法接入点 that bypasses the firewall entirely



Network switches

2

Policies & wireless

Policies come first

Written policies set a minimum standard:

- router & switch policies – ban local accounts, require port security
- a VPN policy – authentication rules, and no **split tunneling** 分离隧道
- a wireless policy – strong encryption, authenticated access

disable beacon frames – harder to find

control signal strength
– no leak outside

WPA3 无线加密协议
– the current strongest

MAC filtering – known devices only

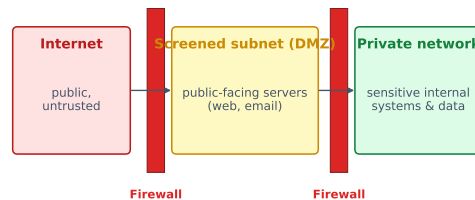
WPA3 is strong; WEP and the original WPA are broken – never accept them in an answer.

3 Segmentation

Segmentation and the screened subnet

Network segmentation 网络分段 divides one network into isolated **subnets** 子网. If one is breached, the damage is contained.

Build segments by subnetting (IP) or with **VLANs** 虚拟局域网 (logically, on one switch). Each gets its own policy.



public servers between two firewalls

Name the **screened subnet** 屏蔽子网 (DMZ) whenever a question separates public services from internal data.

4 Firewalls

Securing Networks

Firewalls

Three kinds of firewall

Stateless 无状态
filters on headers alone
– IP, port, protocol

Stateful 有状态
also tracks each
connection's state
– finer control

Next-generation
adds intrusion pre-
vention, deep
packet inspection

Firewalls belong at every point where data crosses between zones – each segment, and every gateway to the internet.

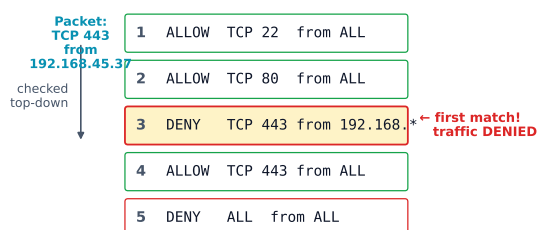
Securing Networks

Firewalls

The access control list – first match wins

A firewall follows an **ACL** 访问控制列表 – an ordered set of rules. Each names a direction, a filter (IP, port, service) and an action.

Rules are checked in order, and the first match wins – so rule order, not just rule content, decides what gets through.



checked top to bottom

Worked example – why the ALLOW rule fails

Rule 3: DENY TCP 443 from 192.168.*
Rule 7: ALLOW TCP 443 from ALL

A user at 192.168.45.37 cannot reach port 443 – even though Rule 7 would allow them – because Rule 3 matches first. The fix: move the ALLOW rule above the DENY.

Read ACLs top-to-bottom and stop at the first match. A Deny above an Allow blocks the traffic, however many Allows sit below it.

5 Detection

When prevention fails – detection takes over

Automated tools read the **log files** 日志文件 that record network activity:

NIDS 网络入侵检测系统
– alerts, does not block

NIPS 网络入侵防御系统
– can also stop an attack

SIEM 安全信息与事件管理 –
gathers many sources to spot patterns

The D in NIDS is detect; the P in NIPS is prevent.

Two detection methods – memorise the trade-off

Signature-based 基于特征

matches known attack signatures

- ✓ fast, few false positives
- ✗ blind to brand-new attacks

Anomaly-based 基于异常

compares to a normal **baseline** 基线

- ✓ catches novel attacks
- ✗ costs more, more false positives

A hybrid approach combines both – and is the safe answer when a question asks for the best of each.

6

Recap

Unit 3 – key takeaways

1 The tells

ARP = one IP two MACs; MAC flood = a surge of MACs

2 DMZ

public servers between the internet and the private network

3 ACL order

first match wins – a Deny above an Allow blocks

4 Detection

signature is fast but blind; anomaly catches new, cries wolf

Check yourself

- 1 A DENY sits above an ALLOW for the same traffic. What happens?
- 2 Which detection method misses brand-new attacks?
- 3 Which wireless encryption is currently strongest?
- 4 NIDS or NIPS: which can block an attack?

Answers 1. it is denied – first match wins 2. signature-based 3. WPA3 4. NIPS