

---

# SOC LEVEL 1 ESSENTIALS

## – PART A: NETWORKING FUNDAMENTALS (POSTS 1–10)

---

A practical series for junior SOC analysts to master core networking concepts essential for detection and incident triage.



MAY 30, 2025

INAAM KABBARA

Security Analyst | Cybersecurity Content Creator | EPITA MSc Graduate

## Table of Contents

1- TCP vs UDP – What's the Difference?.....	2
2- OSI vs TCP/IP – How They Map and Why It Matters? .....	4
3- Top 10 Ports & Protocols Every Analyst Should Know .....	8
4- What Is a 3-Way Handshake — and Why Does It Matter in a SOC?.....	10
5- ICMP and Ping – How They're Used and Abused.....	12
6- NAT and Firewall Basics – What Every SOC Analyst Should Know .....	14
7- DNS – How It Works & Why It's Abused.....	16
8- VPN vs Proxy vs Firewall – What's the Difference?.....	18
9- What Is Packet Capture – and Why Should SOC Analysts Use Wireshark?.....	20
10- IDS vs IPS – What's the Difference?.....	22

# 1- TCP vs UDP – What's the Difference?

As a SOC Analyst, understanding how data travels across networks is essential. One of the most basic — yet critical — distinctions is between TCP and UDP, two core transport layer protocols.

- ◆ TCP (Transmission Control Protocol)
  - Connection-oriented
  - Ensures reliable delivery (3-way handshake, retransmissions)
  - Slower, but guarantees order and completeness
  - Common use cases: HTTP(S), SSH, FTP, SMTP
  
- ◆ UDP (User Datagram Protocol)
  - Connectionless
  - No guarantee of delivery or order
  - Faster, lightweight
  - Common use cases: DNS, VoIP, video streaming, SNMP

 In a SOC context:

Understanding whether a service uses TCP or UDP helps in triaging alerts, interpreting packet captures, and detecting anomalies. For example, a brute-force SSH attack will typically appear over TCP port 22, whereas DNS tunneling exploits often use UDP port 53.

 Question for you:

Which protocol have you seen more often in your environment — and what kinds of threats did it involve?

---

## TCP vs UDP – Quelle est la différence ?

En tant qu'analyste SOC, il est essentiel de comprendre comment les données circulent sur le réseau. Une distinction fondamentale à maîtriser : les protocoles TCP et UDP, tous deux utilisés au niveau transport.

- ◆ TCP (Transmission Control Protocol)
  - Orienté connexion
  - Garantit la livraison fiable (handshake, retransmissions)
  - Plus lent mais assure l'ordre et l'intégrité
  - Cas d'usage : HTTP(S), SSH, FTP, SMTP
  
- ◆ UDP (User Datagram Protocol)
  - Sans connexion
  - Pas de garantie de livraison ou d'ordre
  - Plus rapide et léger

– Cas d'usage : DNS, VoIP, streaming vidéo, SNMP

 Dans un contexte SOC :

Connaître le protocole utilisé aide à qualifier les alertes, analyser les paquets réseau, et détecter des comportements anormaux. Exemple : une attaque brute-force SSH passe par TCP (port 22), tandis que le tunneling DNS s'appuie souvent sur UDP (port 53).

 Et vous ?

Quel protocole voyez-vous le plus souvent dans vos investigations ? Quels types de menaces y sont liés ?

## 2- OSI vs TCP/IP – How They Map and Why It Matters?

Understanding how the OSI and TCP/IP models relate to each other is fundamental for any SOC analyst. These models provide a framework to analyze how data travels across networks — and more importantly, where vulnerabilities and logs occur.

- ◆ OSI Model (7 Layers)

Application  
Presentation  
Session  
Transport  
Network  
Data Link  
Physical

- ◆ TCP/IP Model (4 Layers)

Application  
Transport  
Internet  
Network Access

💡 Mapping Overview:

OSI layers 5–7 → TCP/IP Application  
OSI layer 4 → TCP/IP Transport  
OSI layer 3 → TCP/IP Internet  
OSI layers 1–2 → TCP/IP Network Access

💡 Why it matters in SOC work:

Logs from different tools (e.g., Wireshark, Zeek) often correspond to specific layers  
Helps pinpoint where an attack occurs (ex: DDoS at layer 3, malware at layer 7)  
Essential for interpreting alerts and correlating events across network flows

📌 Mastering this mapping allows analysts to understand attack surfaces, read logs with precision, and communicate findings clearly across technical teams.

🧠 Question for you:

At which layer have you most often seen attacks or anomalies in your investigations?

---

OSI vs TCP/IP – Comment ils se correspondent et pourquoi c'est important?

Comprendre la relation entre les modèles OSI et TCP/IP est essentiel pour tout analyste SOC. Ces modèles structurent la manière dont les données circulent sur le réseau — et permettent de localiser les attaques, les anomalies et les journaux.

- ◆ Modèle OSI (7 couches)

Application

Présentation

Session

Transport

Réseau

Liaison de données

Physique

- ◆ Modèle TCP/IP (4 couches)

Application

Transport

Internet

Accès Réseau

💡 Correspondance des couches :

Couches OSI 5–7 → TCP/IP Application

Couche OSI 4 → TCP/IP Transport

Couche OSI 3 → TCP/IP Internet

Couches OSI 1–2 → TCP/IP Accès Réseau

💡 Pourquoi c'est utile dans un SOC :

Les journaux (logs) des outils comme Wireshark ou Zeek ciblent des couches précises

Permet d'identifier où se situe l'attaque (ex : DDoS en couche 3, malware en couche 7)

Facilite l'analyse des alertes et la corrélation entre les événements réseau

📌 Maîtriser cette correspondance permet aux analystes de visualiser la surface d'attaque, interpréter les logs avec précision et collaborer efficacement avec les équipes réseau.

🧠 Et vous ?

À quelle couche avez-vous détecté le plus d'anomalies dans vos analyses ?

# OSI MODEL

Application	email, web, FTP,..	
Presentation Layer	encoding, encryption,..	
Session	sockets	{ 01 01 }
Transport	TCP, UDP	
Network	IP, routing	
Data Link	MAC, switch	
Physical	bits on wire	

# TCP/IP MODEL

Application Layer



HTTP, FTP  
SMTP

Transport Layer



TCP UDP

Internet Layer



IP, ICMP, IPsec

Network Access Layer



Ethernet & Wifi

## 3- Top 10 Ports & Protocols Every Analyst Should Know

⚠️ Brute-force attacks, phishing, ransomware... they all often start the same way: an open port. If you're a junior SOC analyst, knowing which ports map to which protocols is not optional — it's essential for detection, triage, and escalation.

- ◆ FTP (20/21) – Unencrypted file transfer. Often exploited.
- ◆ SSH (22) – Secure remote access. Bruteforce target.
- ◆ Telnet (23) – Legacy remote login. Insecure.
- ◆ SMTP (25) – Email sending. Used in phishing.
- ◆ DNS (53) – Name resolution. Risk of tunneling.
- ◆ HTTP (80) – Web traffic. Visible, often scanned.
- ◆ POP3 (110) – Legacy email retrieval.
- ◆ IMAP (143) – Modern email access.
- ◆ HTTPS (443) – Encrypted traffic. May hide C2.
- ◆ RDP (3389) – Remote desktop. Ransomware target.

💡 Why it matters in a SOC:

- Port 22 is a vector for bruteforce.
- Port 3389 is tied to lateral movement.
- Anomalies on ports 80/443 may indicate phishing or exfiltration.

🧠 Pro tip: Don't just memorize ports. Learn how they're used in real attacks — that's how you become detection-ready.

❓ Which port have you seen abused most often — and how did you detect it?

---

### Top 10 ports & protocoles à connaître absolument

⚠️ Attaque bruteforce, phishing, ransomware... tout commence souvent par un port ouvert. Pour un analyste SOC débutant, maîtriser les ports et protocoles critiques est indispensable.

- ◆ FTP (20/21) – Transfert non chiffré. Souvent ciblé.
- ◆ SSH (22) – Accès distant sécurisé. Cible de bruteforce.
- ◆ Telnet (23) – Connexion obsolète. Insecure.
- ◆ SMTP (25) – Envoi d'e-mails. Utilisé en phishing.
- ◆ DNS (53) – Résolution de noms. Risque de tunneling.
- ◆ HTTP (80) – Trafic web non sécurisé.
- ◆ POP3 (110) – Ancien protocole email.

- ◆ IMAP (143) – Accès aux mails.
- ◆ HTTPS (443) – Trafic chiffré. Peut masquer du C2.
- ◆ RDP (3389) – Bureau à distance. Vecteur ransomware.

 Pourquoi c'est important dans un SOC :

- Port 22 → bruteforce.
- Port 3389 → mouvement latéral.
- Ports 80/443 → phishing ou exfiltration.

 Conseil : Apprenez comment ces ports sont exploités dans les vraies attaques — c'est ça, être analyste SOC.

 Et vous ? Quel port avez-vous vu le plus souvent dans une attaque ?

1		<b>FTP</b> (20/21) – File transfers. Unencrypted and often exploited
2		<b>SSH</b> (22) – Secure shell access. A top brute-force target
3		<b>Telnet</b> (23) – Legacy remote login. Insecure but still found in production
4		<b>SMTP</b> (25) – Email sending. Abused in spam and phishing
5		<b>DNS</b> (53) – Domain resolution. Watch for tunneling and data leaks
6		<b>HTTP</b> (80) – Web traffic. Unencrypted, often scanned
7		<b>POP3</b> (110) – Legacy email retrieval. Rare, but still seen
8		<b>IMAP</b> (143) – Modern email access. Used in credential compromise
9		<b>HTTPS</b> (443) – Encrypted web traffic. Can mask command-and-control
10		<b>RDP</b> (3389) – Remote desktop. Common in ransomware and lateral movement

## 4- What Is a 3-Way Handshake — and Why Does It Matter in a SOC?

Before two systems can exchange data over TCP, they need to establish a reliable connection. That's where the 3-way handshake comes in — it's the foundation of every TCP session.

💡 Here's how it works:

- 1 SYN → The client sends a synchronize (SYN) request to the server to initiate a connection.
- 2 SYN-ACK → The server responds with a synchronize-acknowledge (SYN-ACK).
- 3 ACK → The client replies with an acknowledge (ACK) — and the connection is established.  
⚠ After this exchange, data can flow securely and in order. If any step fails, the connection doesn't proceed.

💡 Why it matters in a SOC:

- It helps analysts detect scanning behavior (SYN floods, half-open connections).
- It's used in TCP state analysis and firewall logs to validate sessions.
- Understanding it is crucial for packet inspection and anomaly detection (e.g., missing ACKs = possible spoofing).
- It forms the basis of alert rules in Zeek, Suricata, Wireshark, and SIEM systems.

🧠 Pro Tip: When investigating network logs, incomplete handshakes often signal reconnaissance or an attack in progress.

❓ Question for you: Have you ever caught malicious activity just by observing handshake patterns?

---

## Qu'est-ce que le 3-Way Handshake — et pourquoi c'est crucial en SOC ?

Avant d'échanger des données via TCP, deux machines doivent établir une connexion fiable. C'est là que le 3-Way Handshake intervient : c'est la base de toute communication TCP.

💡 Comment ça fonctionne :

- 1- SYN → Le client envoie une requête synchronize au serveur.
- 2- SYN-ACK → Le serveur répond par un synchronize-acknowledge.
- 3- ACK → Le client répond avec un acknowledge — la connexion est établie.  
⚠ Si l'un de ces échanges échoue, la session TCP ne peut pas commencer.

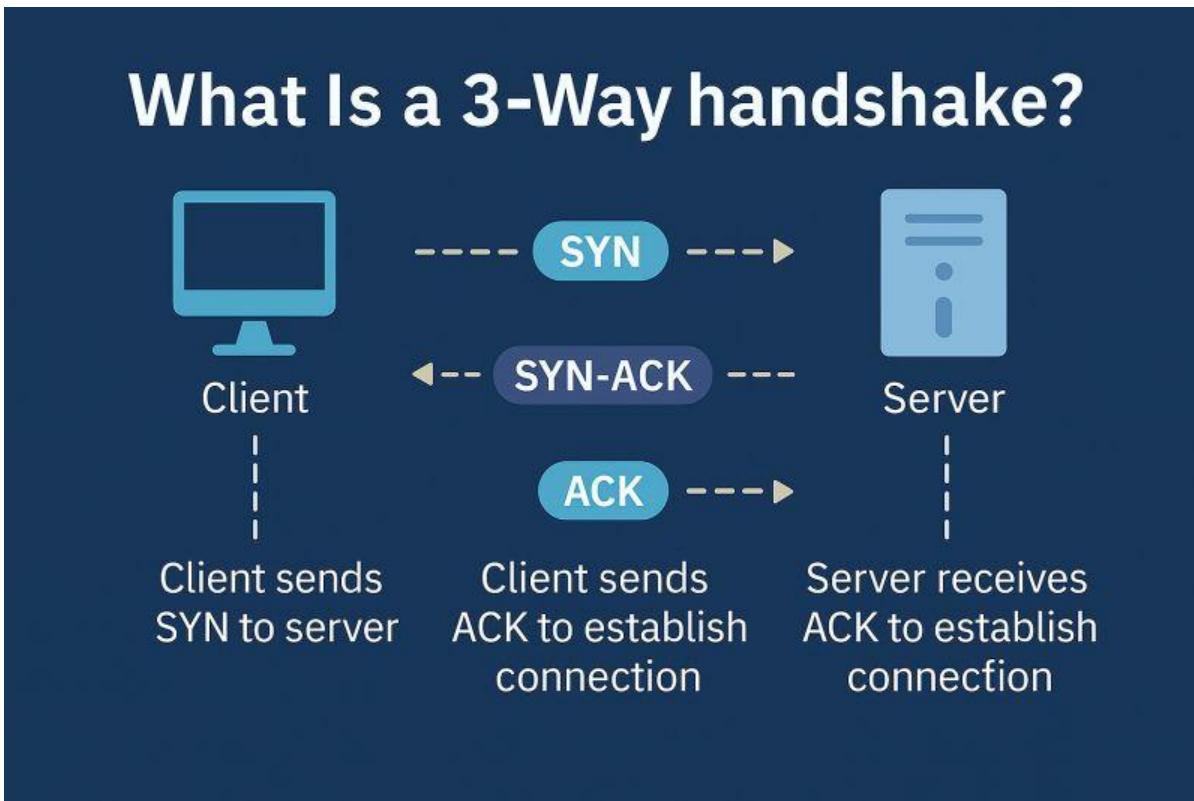
💡 Pourquoi c'est important dans un SOC :

- Il permet de détecter les scans réseau (SYN flood, connexions incomplètes).
- Il est utilisé dans l'analyse d'état TCP et les logs de pare-feu.

- Comprendre le handshake est essentiel pour lire les paquets réseau.
- Il sert de base aux règles d'alerte dans Zeek, Suricata, Wireshark et les SIEM.

💡 Conseil : Si vous voyez beaucoup de SYN sans ACK, pensez à une phase de reconnaissance ou à une attaque potentielle.

❓ Et vous ? Avez-vous déjà détecté une activité suspecte en observant uniquement les handshakes ?



## 5- ICMP and Ping – How They're Used and Abused

One of the first tools you learn in networking is ping — and behind it is a protocol every SOC analyst should know: ICMP (Internet Control Message Protocol).

### 💡 What is ICMP?

It's a network-layer protocol used for sending diagnostic and error messages. It's not used to transfer data but to report conditions like "host unreachable" or "TTL expired."

📡 Ping, one of its most common tools, sends ICMP Echo Request packets to a target, and expects Echo Reply packets in return. It's widely used to test connectivity and latency.

### 🌐 In a SOC context:

#### ✓ Used for:

- Connectivity testing (host up/down)
- Network troubleshooting (latency, packet loss)
- Path analysis (with tools like traceroute, which uses ICMP or UDP)

#### ⚠️ Abused for:

- Ping floods (ICMP flood attacks): DoS by overwhelming the target with echo requests.
- ICMP tunneling: Attackers encapsulate data in ICMP packets to bypass firewalls.
- Network scanning: Attackers use ICMP to map hosts and detect live systems.
- Covert channels: Malware may use ICMP to exfiltrate data or communicate with C2 servers.

🧠 Pro Tip: Just because it's "diagnostic" doesn't mean it's harmless. Watch for unexpected ICMP activity, especially large payloads, spikes, or communication with unknown external IPs.

❓ Have you ever seen ICMP used in a real attack — or blocked it in your firewall rules?

---

## ICMP et Ping – Leur utilisation... et leur détournement

Parmi les premiers outils que l'on apprend, il y a ping — derrière lui se cache un protocole essentiel à connaître : ICMP (Internet Control Message Protocol).

### 💡 Qu'est-ce que ICMP?

C'est un protocole de couche réseau utilisé pour envoyer des messages d'erreur ou de diagnostic. Il ne transfère pas de données, mais signale des états comme "hôte injoignable" ou "TTL expiré".

📡 Ping utilise ICMP pour envoyer des Echo Request à une cible, et recevoir une Echo Reply. Cela permet de tester la connectivité et la latence.

### 🌐 Dans un SOC :

#### ✓ Utilisation légitime :

- Vérification de connectivité (hôte disponible ou non)
- Diagnostic réseau (latence, perte de paquets)
- Analyse de chemin (traceroute)

⚠ Utilisation malveillante :

- Ping flood : DoS par saturation avec des requêtes ICMP.
- Tunneling ICMP : Contournement de pare-feu en encapsulant des données dans ICMP.
- Scan réseau : Détection d'hôtes actifs via ICMP.
- Canaux cachés : Exfiltration de données ou commandes de malware.

🧠 Conseil : Ce n'est pas parce qu'il est "diagnostique" qu'il est inoffensif. Surveillez les pics ICMP suspects, les payloads volumineux, ou les destinations inconnues.

❓ Avez-vous déjà vu ICMP utilisé dans une attaque réelle ou bloqué dans vos règles firewall ?



# 6- NAT and Firewall Basics – What Every SOC Analyst Should Know

When analyzing alerts, you'll often encounter NAT and firewalls. Both are essential to understand for accurate triage.

## ⌚ What is NAT?

Network Address Translation allows multiple internal devices to access the internet using a single public IP by translating private addresses.

- ◆ Example:

192.168.1.10 → NAT → 203.0.113.5

## 🔍 Why it matters in a SOC:

- Multiple users may appear under one public IP.
- Logs need NAT mapping to trace internal users.
- NAT also hides internal systems from scans.

## 🔥 What is a Firewall?

A firewall filters traffic between trusted and untrusted networks, based on rules.

## 🧱 Types:

- Packet-filtering
- Stateful inspection
- Application-layer
- NGFW (with IDS/IPS)

## 🔍 Why it matters in a SOC:

- Alerts often originate from firewall logs.
- Blocked ports, dropped sessions, or suspicious outbound traffic may indicate attacks.
- Knowing firewall behavior helps filter false positives from real threats.

🧠 Pro Tip: Check the NAT table and firewall rule hit — they often reveal what really happened.

❓ Ever seen an alert dismissed due to NAT or a misconfigured firewall?

---

## Notions de base sur le NAT et les pare-feux – À connaître pour les analystes SOC

En investigation réseau, on retrouve souvent le NAT et les pare-feux. Les comprendre est essentiel en SOC.

## ⌚ Qu'est-ce que le NAT ?

Il permet à plusieurs machines internes d'accéder à Internet via une même IP publique.

- ◆ Exemple :

192.168.1.10 → NAT → 203.0.113.5

- 💡 Pourquoi c'est important en SOC :

- Plusieurs utilisateurs internes partagent une même IP publique.
- Il faut corrélérer les logs avec les traductions NAT.
- NAT masque l'architecture interne.

- 🔥 Qu'est-ce qu'un pare-feu ?

Il filtre le trafic en appliquant des règles entre réseaux de confiance et extérieurs.

- 💻 Types :

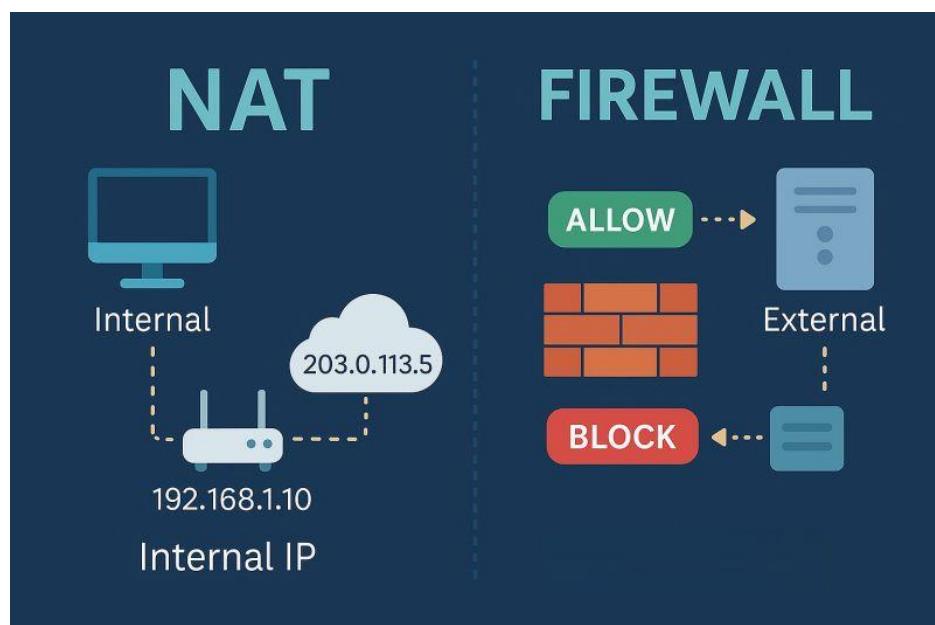
- Filtrage stateless
- Inspection avec état
- Pare-feu applicatif
- NGFW avec IDS/IPS

- 💡 Pourquoi c'est important en SOC :

- Source fréquente d'alertes : connexions bloquées, ports interdits.
- Aide à séparer le bruit des vraies menaces.

🧠 Conseil : Vérifiez la règle pare-feu et la traduction NAT : c'est souvent la clé d'un incident.

❓ Avez-vous déjà mal interprété une alerte à cause du NAT ou du pare-feu ?



## 7- DNS – How It Works & Why It's Abused

When you type [example.com](#), DNS translates it into an IP address so your browser can connect. It's the internet's phonebook — but attackers know how to exploit it.

💡 DNS Resolution (Simplified):

- 1 Client requests domain
- 2 Resolver checks cache or queries authoritative server
- 3 IP is returned → connection is made

🔍 SOC tools (Zeek, Suricata, SIEM) log DNS activity — critical for tracking phishing or malware callbacks.

⚠️ DNS Poisoning (aka Spoofing):

Injecting fake DNS replies to redirect users to malicious IPs.

Example: [bank.com](#) leads to a fake login page → stolen credentials.

💡 In the SOC:

- Watch for abnormal DNS traffic (C2, phishing, exfiltration)
- Fast-flux domains = high-risk
- Monitor TTLs and newly registered domains

🧠 Pro Tip: Short TTL + new domain + external DNS? Likely malicious.

❓ Ever caught threats by analyzing DNS logs alone?

---

## DNS – Fonctionnement & Exploitation

Quand vous tapez [example.com](#), le DNS traduit ce nom en adresse IP. C'est l'annuaire d'Internet — mais aussi une cible fréquente.

💡 Résolution DNS :

- 1- Le client fait une requête
- 2- Le résolveur vérifie ou interroge un serveur autoritatif
- 3- Une IP est renvoyée → connexion établie

🔍 Les logs DNS (Zeek, Suricata, SIEM) aident à identifier phishing et malwares.

⚠️ Empoisonnement DNS :

Injection de fausses réponses DNS pour rediriger vers une IP malveillante.

Ex : [bank.com](#) renvoie vers un faux site → vol d'identifiants.

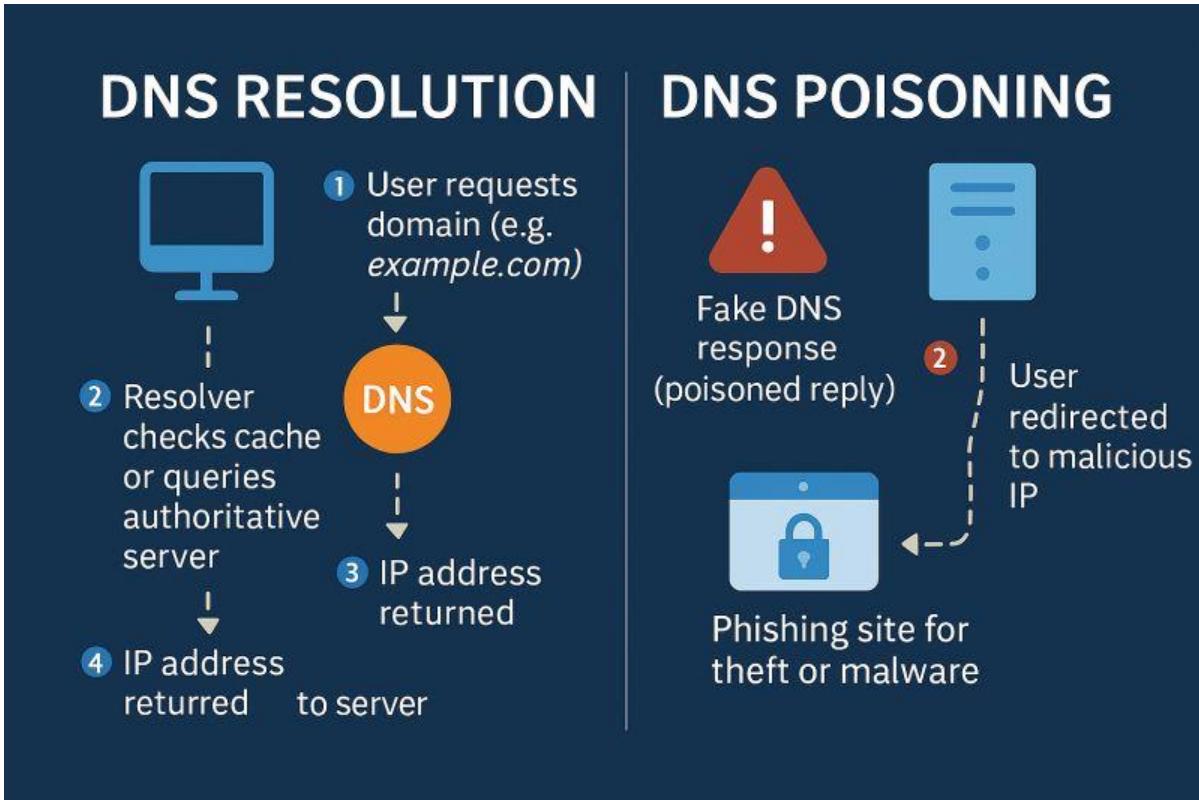
💡 Dans un SOC :

- Trafic DNS anormal = phishing, C2, exfiltration

- Domaines fast-flux = haut risque
- Surveiller les TTL courts + domaines récents

💡 Conseil : Domaine récent + TTL court + requête externe = ⚠️

❓ Avez-vous déjà détecté une attaque via les seuls logs DNS ?



## 8- VPN vs Proxy vs Firewall – What's the Difference?

These tools are often grouped together, but their functions are distinct. Every SOC analyst should know how they impact visibility, detection, and logs.

### VPN (Virtual Private Network)

Encrypts traffic and tunnels it through a secure server — hides IP and location.

#### Use cases:

- Public Wi-Fi security
- Remote access
- Privacy

#### SOC Relevance:

- May bypass local firewalls
- Can mask attacker origin
- Cross-check VPN logs with endpoint activity

### Firewall

Blocks or allows traffic based on rules (IP, port, protocol).

#### Use cases:

- Perimeter protection
- Block malicious traffic

#### SOC Relevance:

- Logs help trace blocked or dropped connections
- First line of defense against scans, brute-force, C2

### Proxy

Acts as a go-between for client requests — filters or logs web traffic.

#### Use cases:

- URL filtering
- Content caching
- IP masking (outbound)

#### SOC Relevance:

- Reveals web-based threats
- Useful for phishing detection & data leaks

### Pro Tip:

VPN = secure tunnel

Proxy = traffic controller

Firewall = network gatekeeper

 Which one plays the biggest role in your threat detection process?

---

## VPN vs Proxy vs Pare-feu – Quelle différence ?

Ces trois technologies sont souvent confondues, mais leurs rôles sont bien distincts. Pour un analyste SOC, cette distinction est essentielle.

### VPN (Réseau Privé Virtuel)

Chiffre le trafic et masque l'IP via un serveur distant.

#### Cas :

- Sécurité Wi-Fi public
  - Accès distant
  - Anonymat
-  En SOC :
- Contourne les pare-feux
  - Masque l'origine
  - Vérifier les connexions VPN

### Pare-feu

Filtre le trafic selon des règles IP/port.

#### Cas :

- Protection réseau
- Blocage du trafic malveillant

#### En SOC :

- Logs utiles pour analyser les connexions rejetées
- Défense contre les scans ou tentatives de C2

### Proxy

Intermédiaire réseau qui filtre ou journalise les requêtes.

#### Cas :

- Filtrage URL
- Cache
- Masquage IP (sortant)

#### En SOC :

- Détection phishing
- Analyse du trafic web

#### Conseil :

VPN = tunnel privé

Proxy = filtre

Pare-feu = mur de sécurité

 Lequel utilisez-vous le plus dans vos investigations ?

## 9- What Is Packet Capture – and Why Should SOC Analysts Use Wireshark?

In a Security Operations Center, there's no deeper visibility than what you get from packet captures.

💡 Packet capture (PCAP) is the process of recording raw network traffic — every packet that enters or exits an interface.

🛠️ Wireshark is the most widely used tool to analyze those packets. It provides deep insight into protocols, payloads, and traffic behavior.

🔍 Why it matters for SOC work:

- ✓ Inspect suspicious connections in real time
- ✓ Analyze malicious traffic (e.g., C2, DNS tunneling, data exfiltration)
- ✓ Reconstruct sessions (e.g., HTTP POST, login attempts)
- ✓ Validate firewall rules and detections
- ✓ Hunt anomalies in protocol behavior (e.g., malformed packets)
- ✓ Confirm or refute alerts raised by SIEM or EDR tools

🧠 Key Features to Know in Wireshark:

- Filters (e.g. ip.addr == 192.168.1.5 && tcp.port == 443)
- Follow TCP/HTTP streams to reconstruct conversations
- Protocol hierarchies to understand traffic distribution
- Coloring rules to highlight suspicious activity
- Export packets, files, or payloads for deeper analysis or reporting

💡 Pro Tip: Learning Wireshark is like learning a microscope — it reveals what other tools summarize. Don't rely only on SIEM alerts. Go to the packet level.

❓ Have you ever solved an alert by inspecting raw packets?

---

## Qu'est-ce que la capture de paquets – et pourquoi les analystes SOC doivent-ils utiliser Wireshark ?

En SOC, il n'y a pas de meilleure visibilité que l'analyse des paquets réseau bruts.

💡 La capture de paquets (PCAP) consiste à enregistrer le trafic réseau en temps réel — chaque paquet entrant ou sortant d'une interface.

🛠️ Wireshark est l'outil de référence pour lire ces paquets et analyser les communications en profondeur.

🔍 Pourquoi c'est utile en SOC :

- ✓ Inspecter une connexion suspecte
- ✓ Analyser le trafic malveillant (ex. : C2, tunneling DNS, exfiltration)

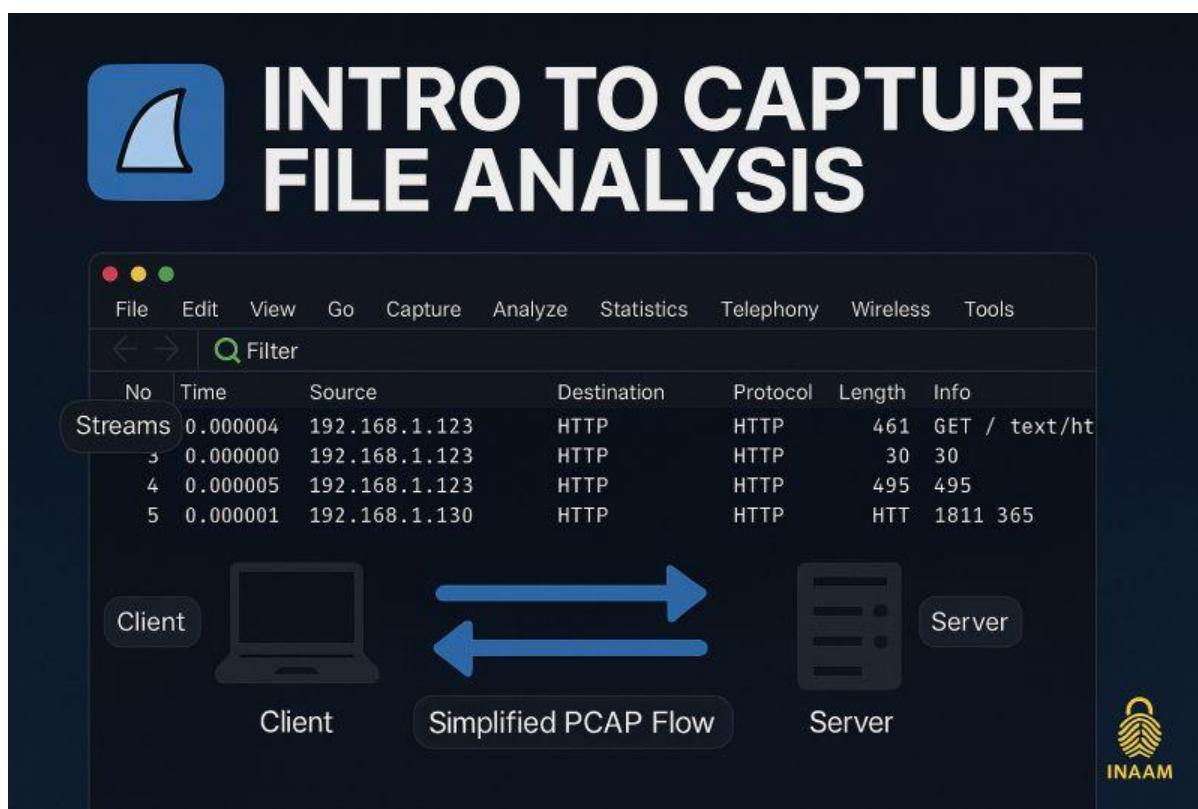
- Reconstruire une session HTTP ou SSH
- Vérifier les règles pare-feu et alertes
- Identifier des anomalies dans les protocoles (paquets corrompus, etc.)
- Confirmer ou infirmer une alerte levée par un SIEM ou un EDR

🧠 Fonctions clés de Wireshark :

- Filtres puissants (`ip.addr == 192.168.1.5 && tcp.port == 443`)
- Suivi des flux TCP/HTTP
- Vue hiérarchique des protocoles
- Règles de coloration personnalisées
- Export des paquets, fichiers ou charges utiles pour analyse approfondie

💡 Conseil : Wireshark, c'est comme un microscope. Il montre ce que les autres outils résument. N'attendez pas tout de vos alertes — analysez les paquets.

❓ Avez-vous déjà élucidé une alerte en inspectant directement les paquets ?



## 10- IDS vs IPS – What's the Difference?

They sound similar, but their roles in a SOC are very different. Knowing how they work helps analysts respond better.

### 🔍 Core difference:

- IDS = detects and alerts only (no blocking)
- IPS = detects and blocks threats in real time (inline)

### 💡 Think of it like this:

- IDS is a security camera: it watches and reports.
- IPS is a security guard: it takes action to stop threats.

### 🛠️ IDS Use Cases:

- Detect brute-force attempts or malware signatures
- Monitor sensitive segments
- Send alerts to SIEM for analysis

### 💡 IPS Use Cases:

- Block exploits automatically
- Stop zero-day attacks
- Prevent lateral movement

### 💡 Why it matters in a SOC:

- IDS gives visibility and context for investigations
- IPS adds prevention — but must be fine-tuned
- Both tools strengthen layered defense when used together

🧠 Pro Tip: IDS is great for alerting and threat hunting. IPS is ideal for automated blocking — just beware of false positives.

❓ Do you prefer detection first — or blocking threats as they happen?

---

## IDS vs IPS – Quelle est la différence ?

Ces deux solutions sont essentielles — mais leurs fonctions en SOC ne sont pas les mêmes.

### 🔍 Différence clé :

- IDS = détecte et alerte uniquement
- IPS = détecte et bloque en temps réel

### 💡 Une analogie simple :

- IDS = caméra de surveillance
- IPS = agent de sécurité qui intervient

🛠 Cas d'usage IDS :

- Identifier les attaques par force brute
- Surveiller des segments critiques
- Générer des alertes pour le SIEM

💡 Cas d'usage IPS :

- Bloquer les exploits
- Arrêter les attaques zero-day
- Empêcher les déplacements latéraux

💡 Pourquoi c'est utile en SOC :

- L'IDS offre visibilité et contexte
- L'IPS protège automatiquement
- Ensemble, ils forment une défense solide

🧠 Conseil : L'IDS est parfait pour la détection, l'IPS pour la réponse immédiate — à condition d'éviter les faux positifs.

❓ Et vous ? Vous misez d'abord sur la détection ou sur la prévention automatique ?

