Architecture de sécurité et filtrage de paquets

Samuel Pélissier (samuel.pelissier@inria.fr)

2025

Planning

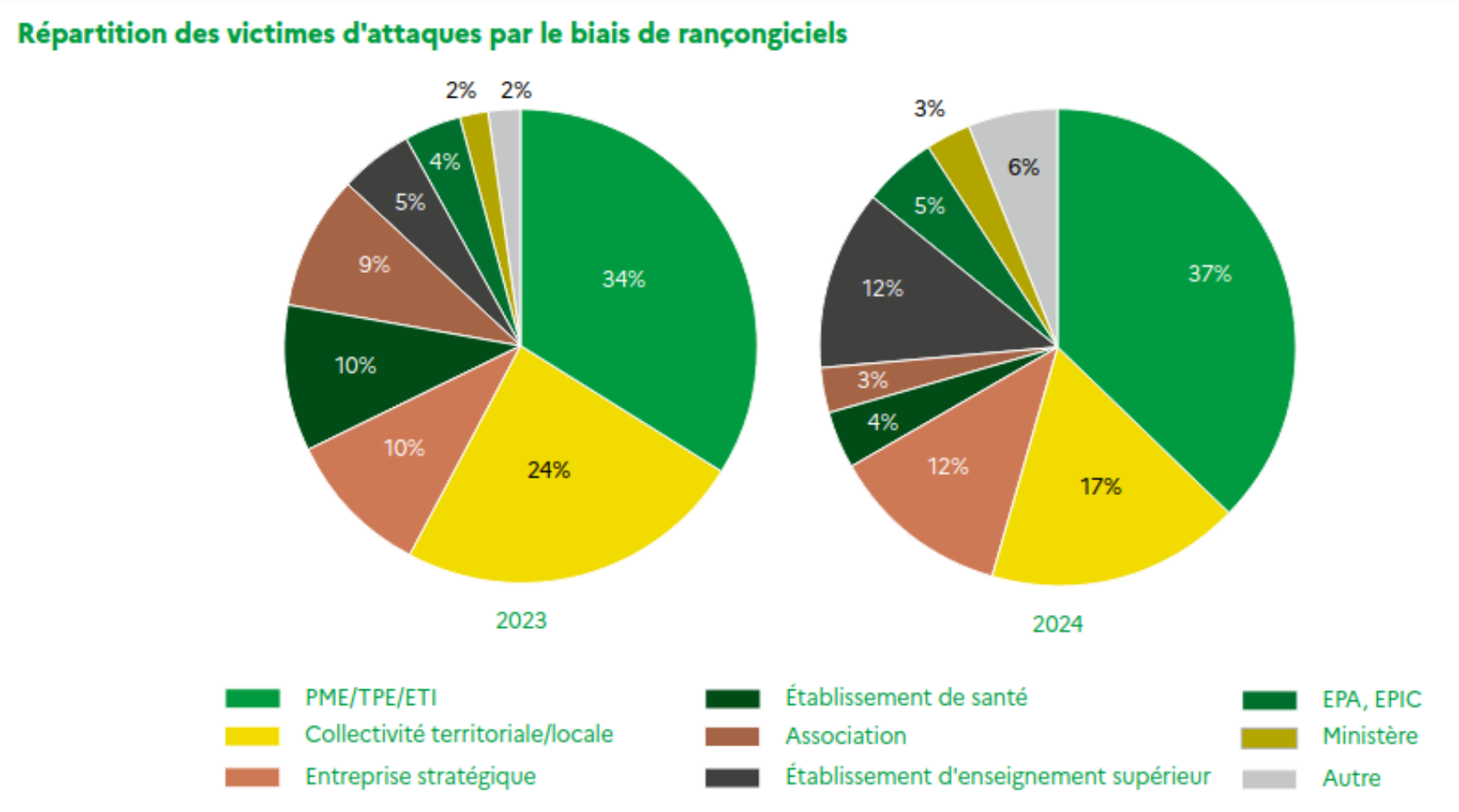
- CM1 : Sécurité des réseaux : cloisonnement vertical (Filtrage et Pare-feu)
- CM2 : Sécurité des réseaux : cloisonnement horizontal (VPN IPsec/TLS)
- CM3 : DNSSEC
- TD : Filtrage d'accès (matrice de flux)
- TP1 et 2 : Filtrage d'accès
- TP3 et 4 : VPN IPsec
- TP5 et 6 : DNSSEC

Modalités d'évaluation

- Rendus TP
- Evaluation de 1h sur table (ETA : 27 mai)

Les menaces

Tout le monde est à risque, avec des niveaux de menace différents.



Source : ANSSI, 2024 https://cyber.gouv.fr/le-panorama-de-la-cybermenace

Les menaces

Les solutions/équipement réseau sont particulièrement touchées.

CVE	SCORE CVSS3.x	ÉDITEUR	RISQUE	RÉFÉRENCE CERT-FR
CVE-2024-21887	9,1	IVANTI	Exécution de code arbitraire à distance, contournement d'authentification et de politique de sécurité, accès à des ressources restreintes sur différentes passerelles de sécurité et de VPN	CERTFR-2024-ALE-001 CERTFR-2024-AVI-0109 CERTFR-2024-AVI-0085
CVE-2023-46805	8,2			
CVE-2024-21893	8,2			
CVE-2024-3400	10,0	PALO ALTO NETWORKS	Exécution de code arbitraire à distance sur différents équipements de sécurité	CERTFR-2024-ALE-006 CERTFR-2024-AVI-0307
CVE-2022-42475	9,8	FORTINET	Exécution de code arbitraire à distance sur différentes passerelles VPN SSL	CERTFR-2022-ALE-012 CERTFR-2022-AVI-1090
CVE-2024-8963	9,4	IVANTI	Exécution de code arbitraire à distance et contournement de la politique de sécurité sur différentes passerelles de sécurité et de VPN	CERTFR-2024-ALE-013 CERTFR-2024-AVI-0796 CERTFR-2024-AVI-0917
CVE-2024-8190	7,2			
CVE-2024-47575	9,8	FORTINET	Exécution de code arbitraire à distance sur différents équipements de sécurité	CERTFR-2024-ALE-014 CERTFR-2024-AVI-0917
CVE-2024-21762	9,8	FORTINET	Exécution de code arbitraire à distance	CERTFR-2024-ALE-004

Les menaces

- Intrusion physique ou logique
- Phishing
- Social Engineering
- Virus, vers, chevaux de troie
- Déni de service (attaque sur la disponibilité)
- etc.

Ethique et responsabilité

Points-évidents-mais-nécessaires :

- Une bonne défense connaît et anticipe les attaques
- Connaître une attaque =/= l'utiliser sur ses petits camarades
- Ne JAMAIS lancer une attaque / un script sans comprendre / contre une machine non contrôlée / sans autorisation explicite

Méthodologie d'attaque

Dans une attaque sérieuse, rien n'est fait au hasard

- Reconnaissance
- Scanning
- Obtention d'accès
  - En attaquant une application
  - En attaquant un OS particulier
  - En attaquant le réseau
- Maintenir son accès
- Effacer ses traces

Méthodologie d'attaque

Dans une attaque sérieuse, rien n'est fait au hasard

- Reconnaissance
- Scanning
- Obtention d'accès
  - En attaquant une application
  - En attaquant un OS particulier
  - En attaquant le réseau
- Maintenir son accès
- Effacer ses traces

Chaque étape génère des traces potentiellement identifiables.

Pour détecter une attaque : le plus tôt est le mieux.

Pourquoi s'embêter ?

Accès sans technologie

- Ingénierie sociale
- Intrusion physique
- « On fouille les poubelles »

https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots

Reconnaissance

OSINT (Open Source INTelligence) : Internet, internet, internet

- Google est ton ami* : beaucoup (trop) de choses
- Site web de la cible : info utilisables

Reconnaissance

- Newsgroup, forum : les gens sont bavards pour trouver des solutions à leurs problèmes

https://knowyourmeme.com/memes/events/war-thunder-military-document-leaks

Reconnaissance : les bases RDAP

- **Registration Data Access Protocol (RDAP)**
- Précédemment : WHOIS
- Noms de domaine
- Autonomous System numbers
- Adresses IP (v4, v6)

https://about.rdap.org/

Reconnaissance : les bases RDAP

Nom de domaine : https://lookup.icann.org/en/lookup

Technical:

Handle: CTC4924105-FRNIC

Name: UNIVERSITE DE RENNES

Organization: UNIVERSITE DE RENNES

Email: domaines@listes.univ-rennes.fr

Status: associated

Whois Server: whois.nameshield.net

Mailing Address: 263 Avenue du GÃ©nÃ©ral Leclerc, RENNES, N/C, 35042, FR

Ou plus spécifique : https://get.gov/domains/whois/

Reconnaissance : les bases RDAP

Adresses IP : www.ripe.net

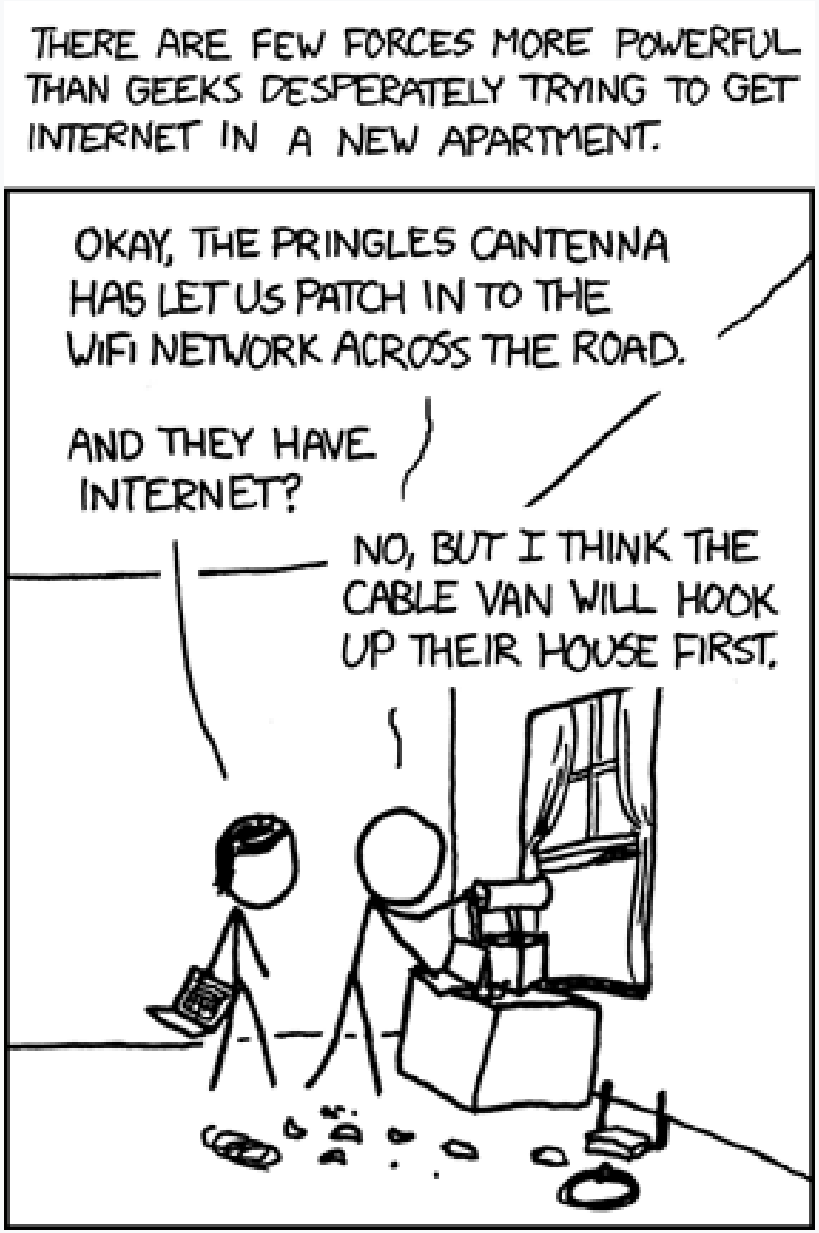
Mais aussi : search.arin.net, www.arin.net, www.apnic.net, lacnic.net…

```
inetnum:        148.60.0.0 - 148.60.255.255
netname:        FR-VERDUR-E
descr:          Universite de Rennes 1
descr:          Campus de Beaulieu, Avenue du General Leclerc
descr:          35042 Rennes Cedex
country:        FR
admin-c:        DU653-RIPE
tech-c:         HU477-RIPE
status:         LEGACY
mnt-by:         RENATER-MNT
remarks:        changed: ripe-dbm@ripe.net 19990706
remarks:        changed: rensvp@renater.fr 20020328
remarks:        changed: er-transfer@ripe.net 20031030
remarks:        changed: rensvp@renater.fr 20060405
remarks:        changed: rensvp@renater.fr 20150807
created:        2002-04-12T13:21:05Z
last-modified:  2019-12-04T13:02:04Z
source:         RIPE
```

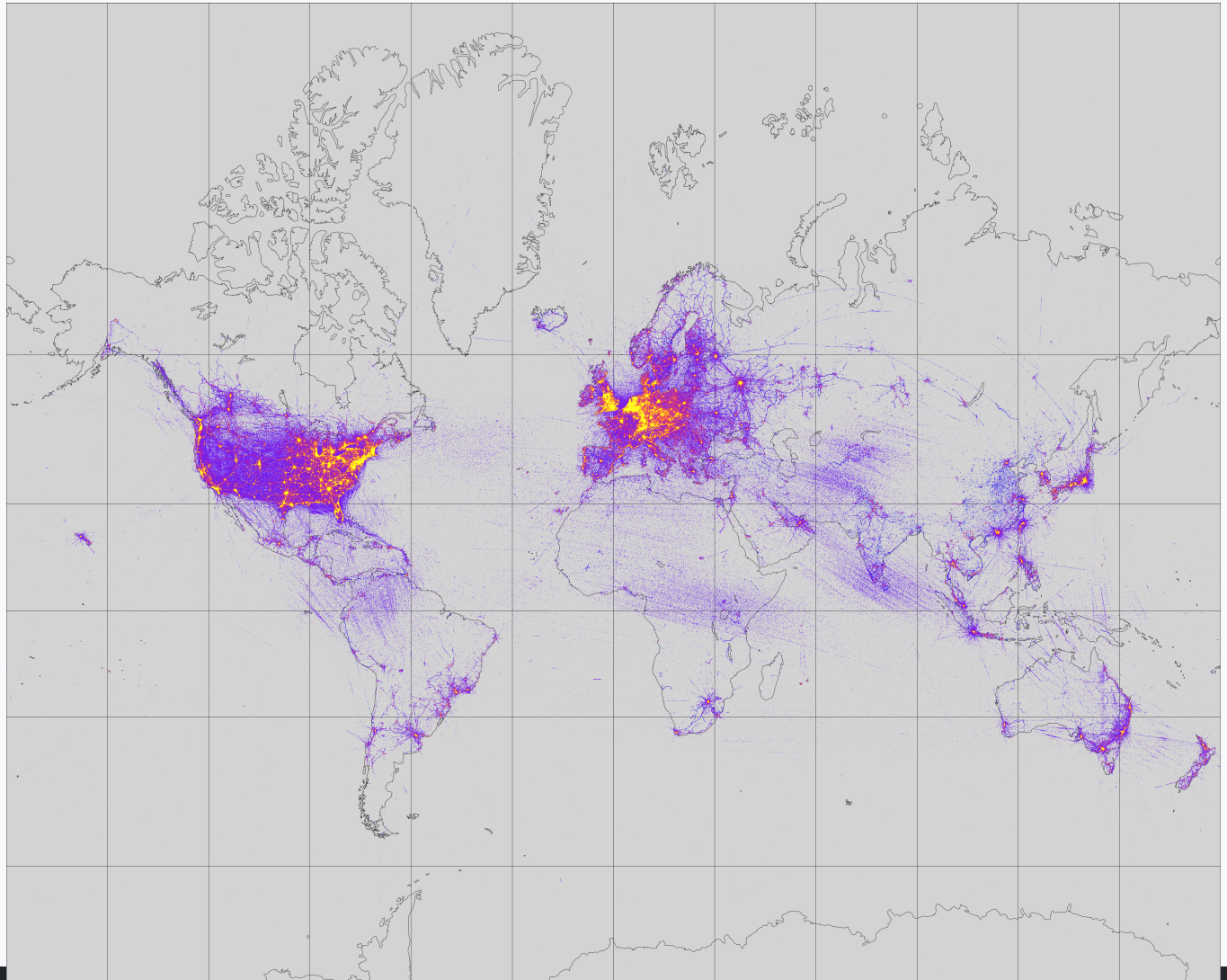
Scannez cette cible que je ne saurais voir

- Wardialing
- Wardriving passif ou actif

https://xkcd.com/466/

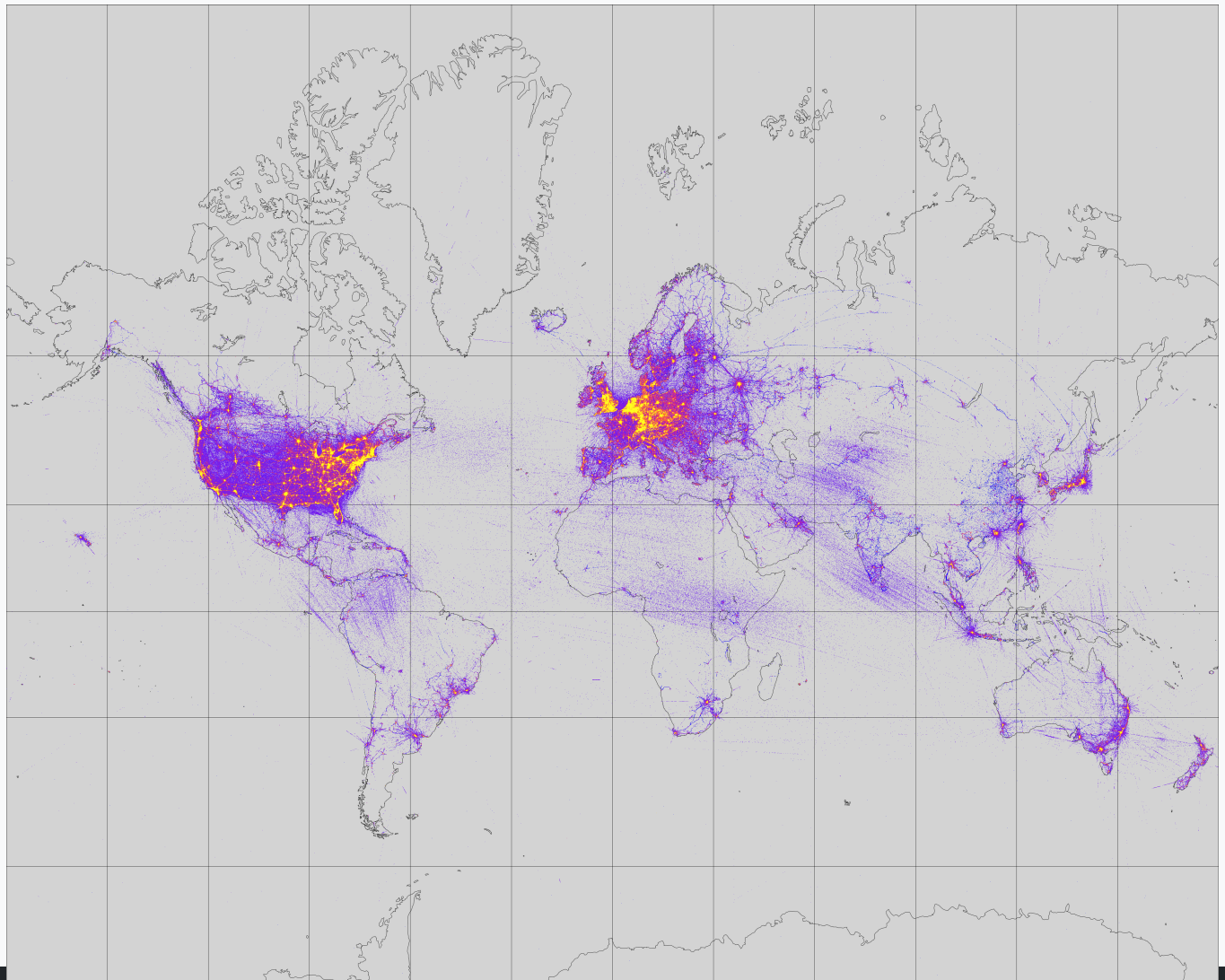


Scannez cette cible que je ne saurais voir



Scannez cette cible que je ne saurais voir

551 millions de réseaux Wi-Fi publics scannés par les utilisateurs du WiGLE project, 2019 https://wigle.net/



Scannez cette cible que je ne saurais voir

Cartographie du réseau?

Scannez cette cible que je ne saurais voir

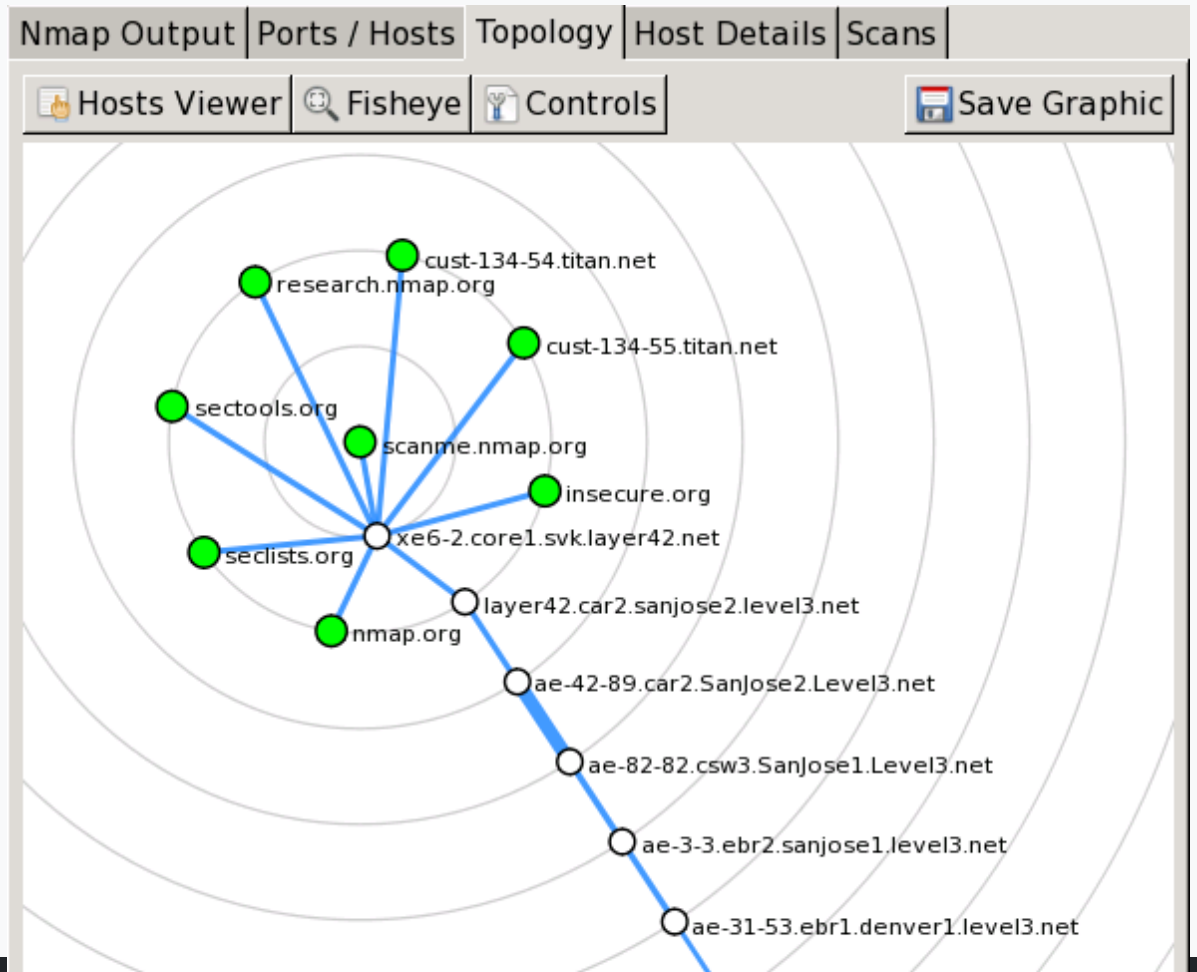
Cartographie du réseau?

- Trouver les machines allumées : nmap
- Trouver le chemin d'accès : traceroute

Scannez cette cible que je ne saurais voir

Capture d'écran d'une topologie réseau obtenue avec zenmap, GUI de nmap

https://nmap.org/book/zenmap-results.html



Scannez cette cible que je ne saurais voir

- Trouver les ports ouverts
- Trouver les services
- Trouver les OS (fingerprinting)

Sortie de nmap -O :

```
~ ❯ sudo nmap -O localhost                                          15:38:28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 15:38 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000042s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
631/tcp open  ipp
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

Scannez cette cible que je ne saurais voir

Chercher les vulnérabilités présentes : utilisation d'un scanner de vulnérabilités

- Des dizaines d'outils https://owasp.org/www-community/Vulnerability_Scanning_Tools
- Qualité à géométrie variable
- Ne pas avoir de vulnérabilité remontée automatiquement == déjà un bon début

Attaque sur une appli ou un OS

- Attaque par buffer overflow (voir https://fr.wikipedia.org/wiki/D%C3%A9passement_de_tampon)
- Attaque d'appli web : ex script CGI vulnérable
- Vol de session
- Injection SQL
- www.owasp.org

Pourquoi s'embêter ? (2)

- Mots de passe par défaut (admin:admin)
- Mots de passe faibles
  - Dans des listes connues : rockyou.txt
  - Dans des leaks connus : https://haveibeenpwned.com/
  - Via des outils *rapides* : hashcat

Attaques sur le réseau

- Sniffing
- Address Spoofing
- Interception et modification de paquet
- Vol de session

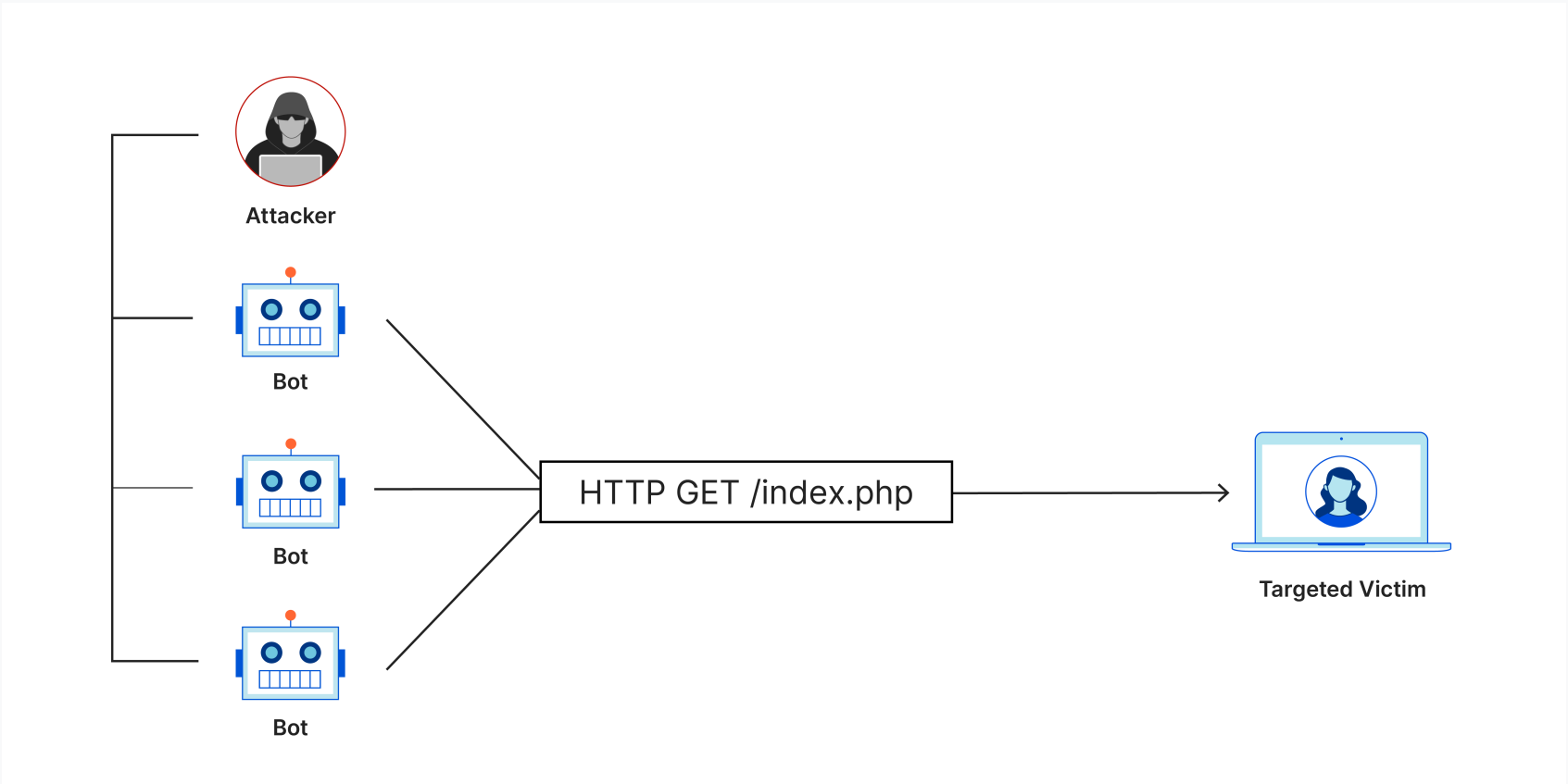
Déni de service

Multiples moyens, multiples applications du (D)DOS:

- Arrêt de services en local
- Monopolisation des ressources d'une machine en local
- Arrêt de service à distance
- Monopolisation des ressources d'une machine à distance : SYN flooding, DdoS, etc.

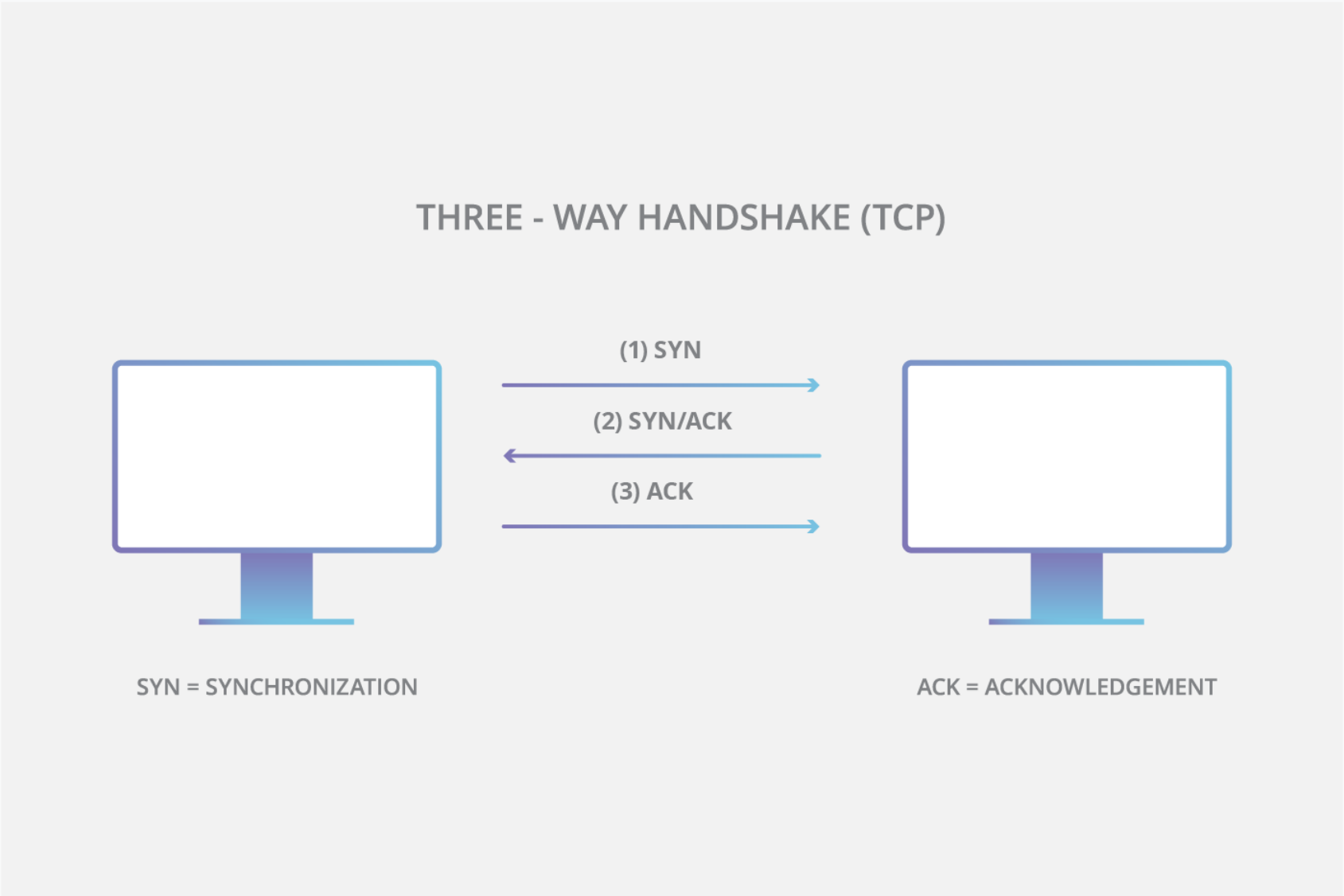
DDOS : principes de base

https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/



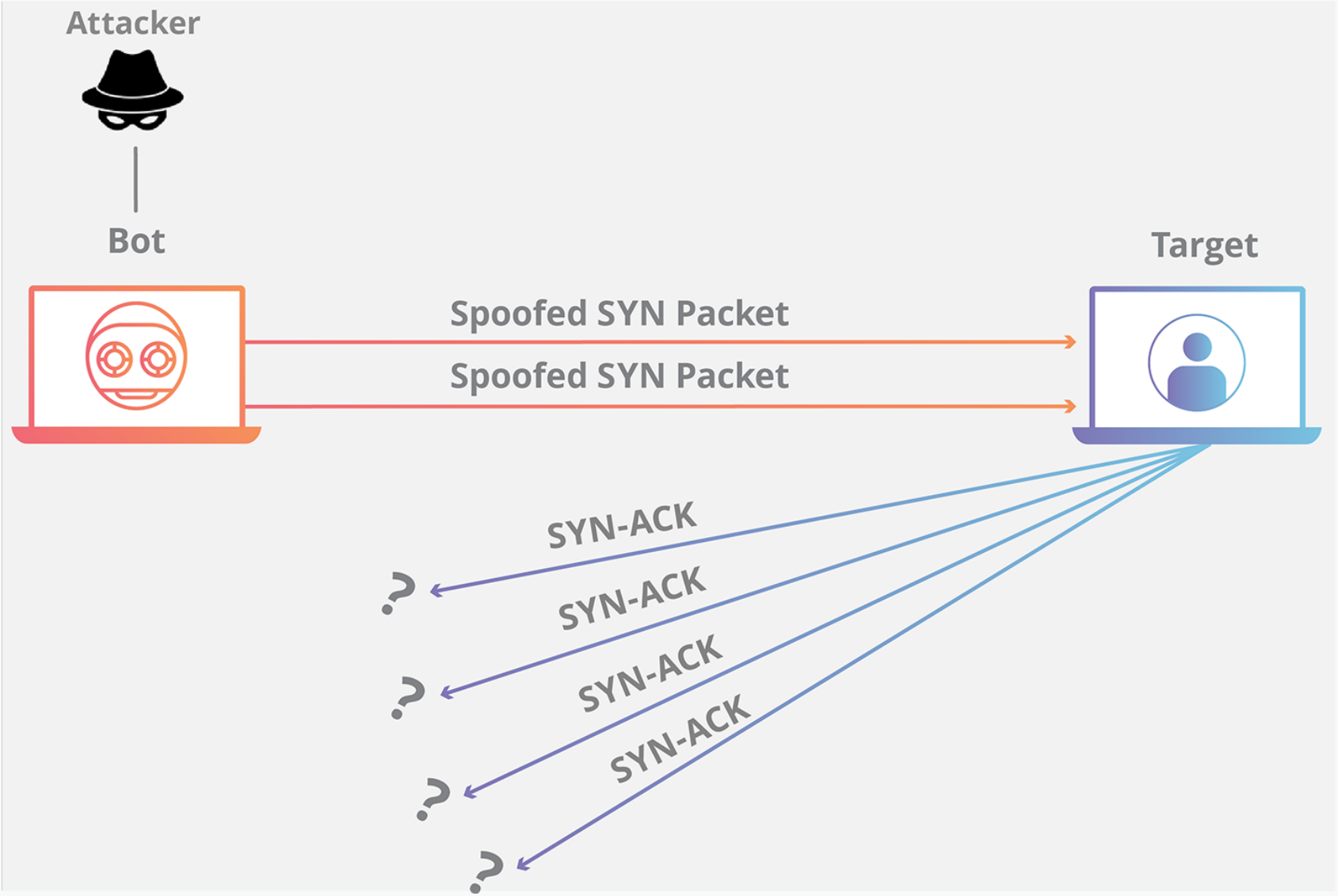
SYN flooding

https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/



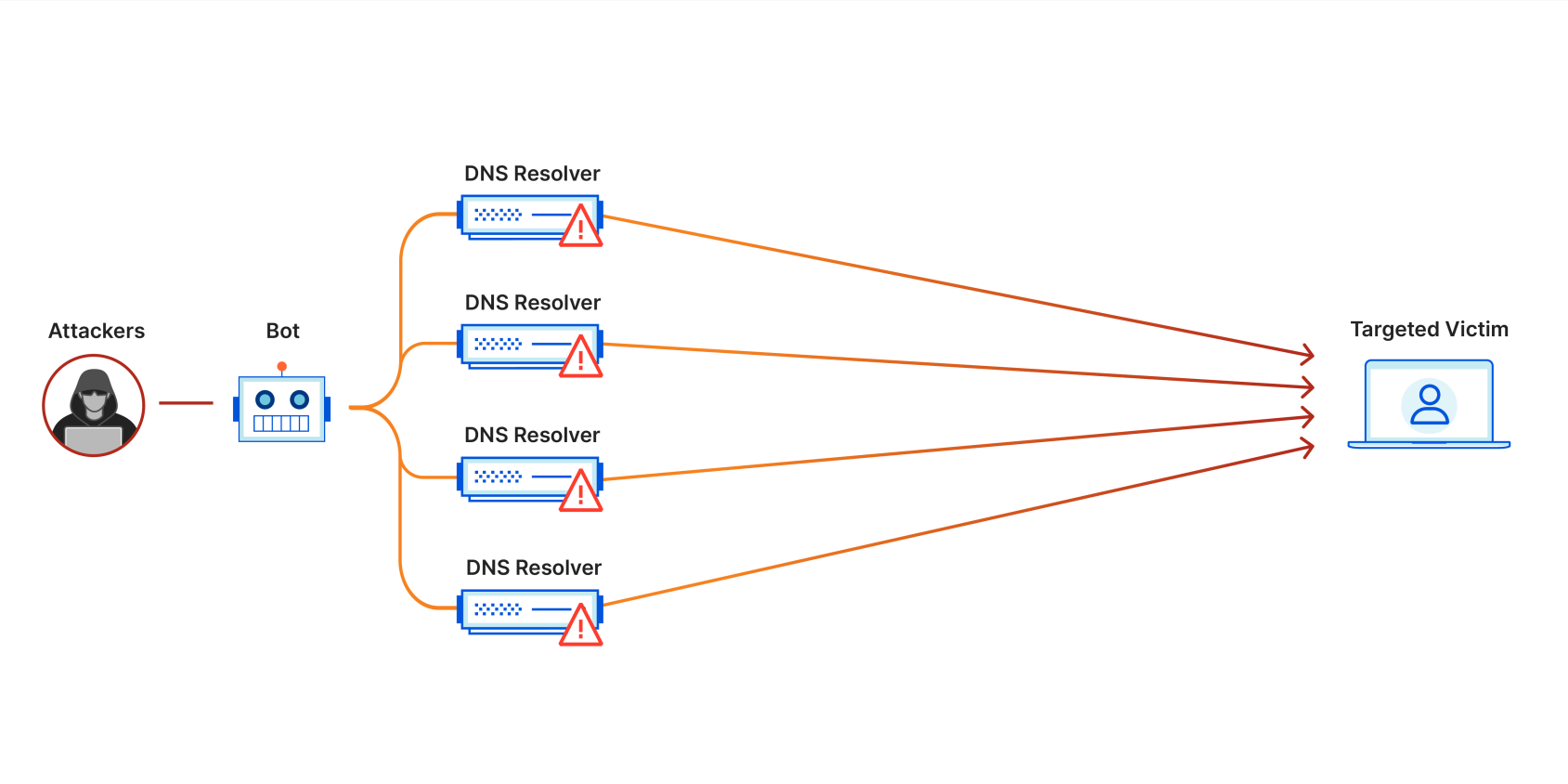
SYN flooding

https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/



DDoS par amplification

https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/



Maintenir son accès

- Mise en place de chevaux de Troie (*trojan horse*)
- Mise en place de backdoors
- Mise en place de rootkits

Effacer ses traces...

- Nécessite une bonne connaissance de ce qu'on fait, du réseau et des systèmes d'exploitation
- Effacer les logs
- Créer des fichiers cachés
- Effacer ses accès réseaux

Un poste est compromis : quelle confiance ?

Voir : analyse forensique
https://fr.wikipedia.org/wiki/Analyse_forensique

ou pas...

Défacement web :

Défensif et offensif ?

Le reste du cours est à but *défensif*. Pour l'offensif, voir :

- https://www.root-me.org/
- https://www.hackthebox.com/
- CTF (ex: BreizhCTF)
- ...

Défénse & pare-feu

Quelques outils de défense

Meta :

- La veille technologique
- Les formations

Technique :

- L'authentification
- Les anti-virus

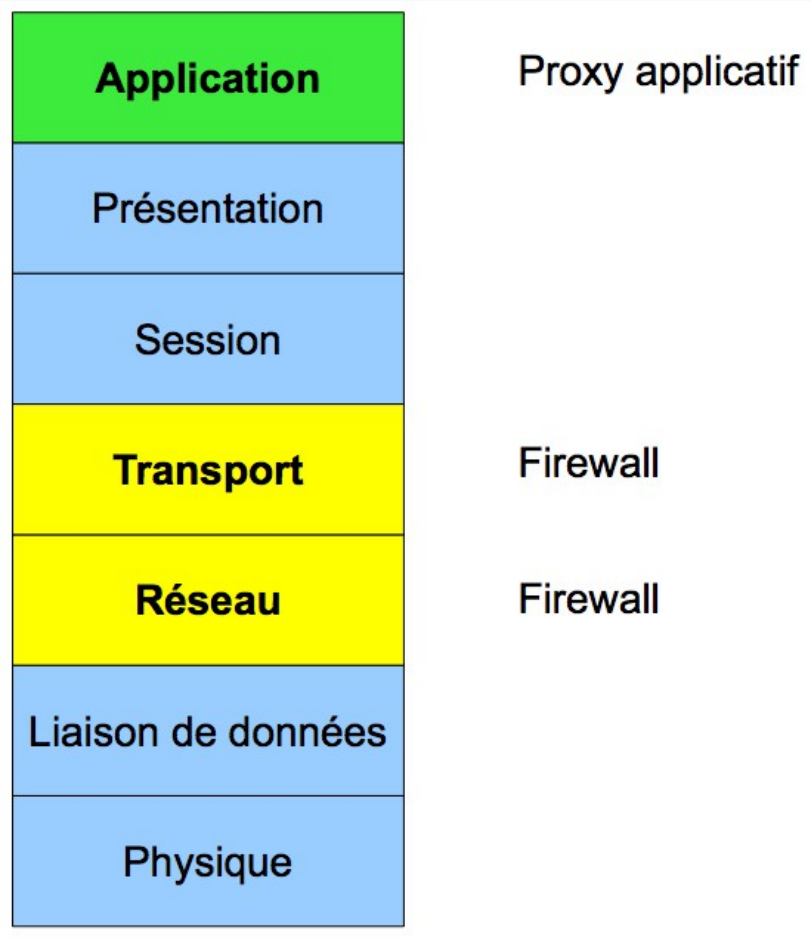
Quelques mots sur les anti-virus

- Ils ne protègent que contre les virus connus
- Ils ne sont utiles que si ils sont à jour
- Ils ne protègent pas des utilisateurs « non-avertis »

Différents filtres, différents niveaux

De nombreuses attaques informatique passent par le réseau à un moment ou un autre.

On peut les voir passer à plusieurs niveaux.



Les pare-feu : principes de base

On filtre au niveau réseau, sur un équipement dédié

- Pour créer un point d'accès unique
- Pour appliquer les règles d'une politique de sécurité
- Pour créer une frontière physique entre votre réseau interne et le grand méchant Internet

Les pare-feu : principes de base

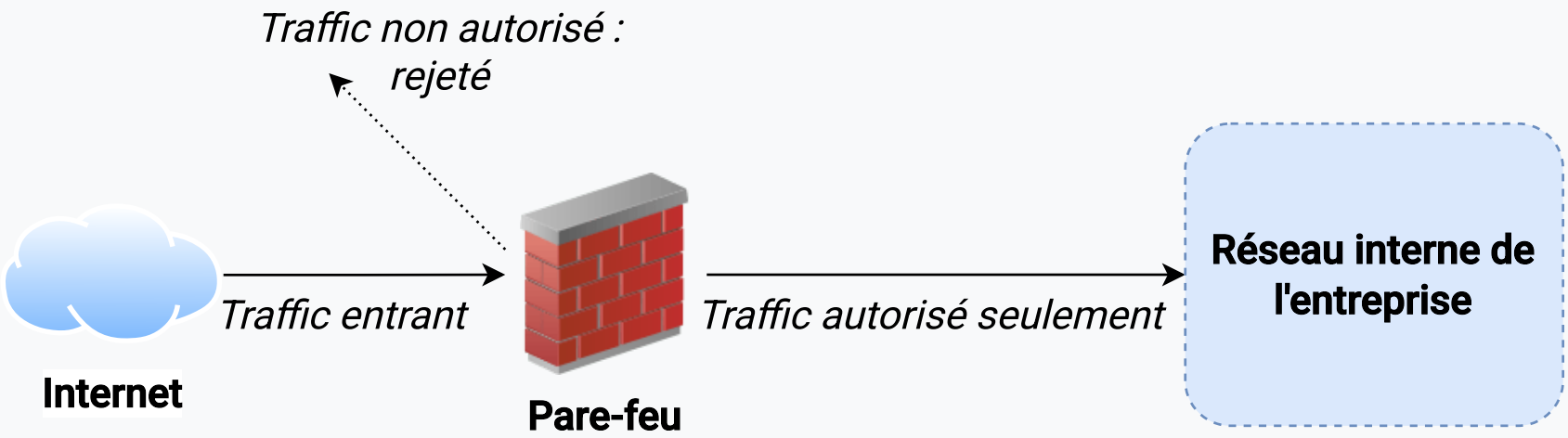
Il est difficile d'avoir une vue globale de toutes les machines de votre réseau et de leurs configurations

> Ca évite d'avoir à installer, mettre à jour et faire de la veille technologique sur 36 logiciels de filtrage souvent dépendant des OS

Les pare-feu : principes de base

- L'équipement dédié est sous VOTRE contrôle
  - Sur une machine utilisateur, il y a un utilisateur…
- Le bon comportement pour un filtrage en entreprise :
  - Interdire par défaut
  - Limiter au minimum requis les privilèges
  - Attention : sur un réseau de cœur, on ne peut pas interdire par défaut
- Eviter la complexité

Un exemple simple



Les pare-feu

- Agit au niveau réseau
- Peut assurer la translation d'adresse
- Fonctions de filtrage avancées
  - Règles sur les flag TCP
  - Spécifications de plage horaire
  - Etc.
- Joue le rôle de point d'entrée unique

Les pare-feu : limites

Ce qu'ils ne font pas :

- Arrêter les virus
- Arrêter les spams
- Authentifier les utilisateurs

Les pare-feu : le mandataire/proxy

- Agit au niveau applicatif
- Reçoit les demandes de connexions des clients et les envoie à leur place
- Permet d'effectuer des traitements supplémentaires : mise en mémoire, lien avec l'anti-virus ou l'anti-spam, filtrage applicatif plus fin.
- Joue souvent le rôle de relais de connexion et de cache

Aussi, imputabilité et non-répudiation des connexions :

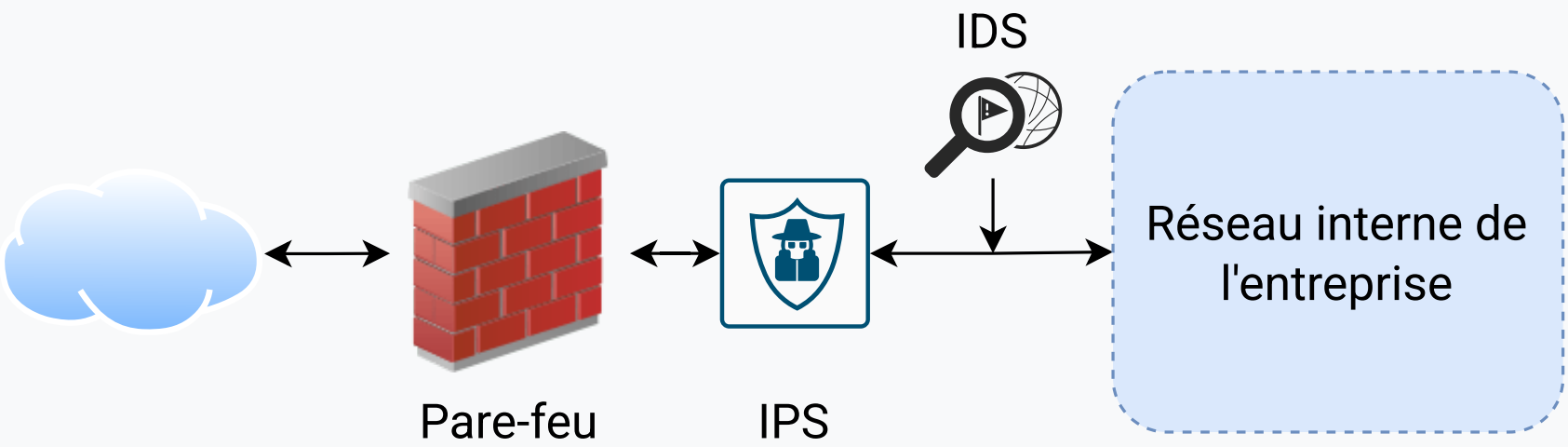
- Identification et authentification
- Journalisation (logs)

Pare-feu, IDS, IPS ?

Résumé grossier :

- Pare-feu
  - Filtre de paquets selon règles pré-définies
  - Mandataires (proxy)
- Intrusion Detection system (IDS)
  - Base de données de menaces (signatures)
  - N'importe quel layer
  - Alerte seulement
- Intrusion Prevention System (IPS)
  - Base de données de menaces
  - N'importe quel layer
  - Bloque les attaques

Pare-feu, IDS, IPS ?



Le filtrage de paquets: stateless

Le pare-feu intercepte les paquets entrant et sortant (couche 3)

Filtrage classique (stateless) basé sur :

- Les interfaces d'entrée et de sortie
- Les adresses IP source/destination
- Les numéros de ports

Vulnérable à

Le filtrage de paquets: stateless

Le pare-feu intercepte les paquets entrant et sortant (couche 3)

Filtrage classique (stateless) basé sur :

- Les interfaces d'entrée et de sortie
- Les adresses IP source/destination
- Les numéros de ports

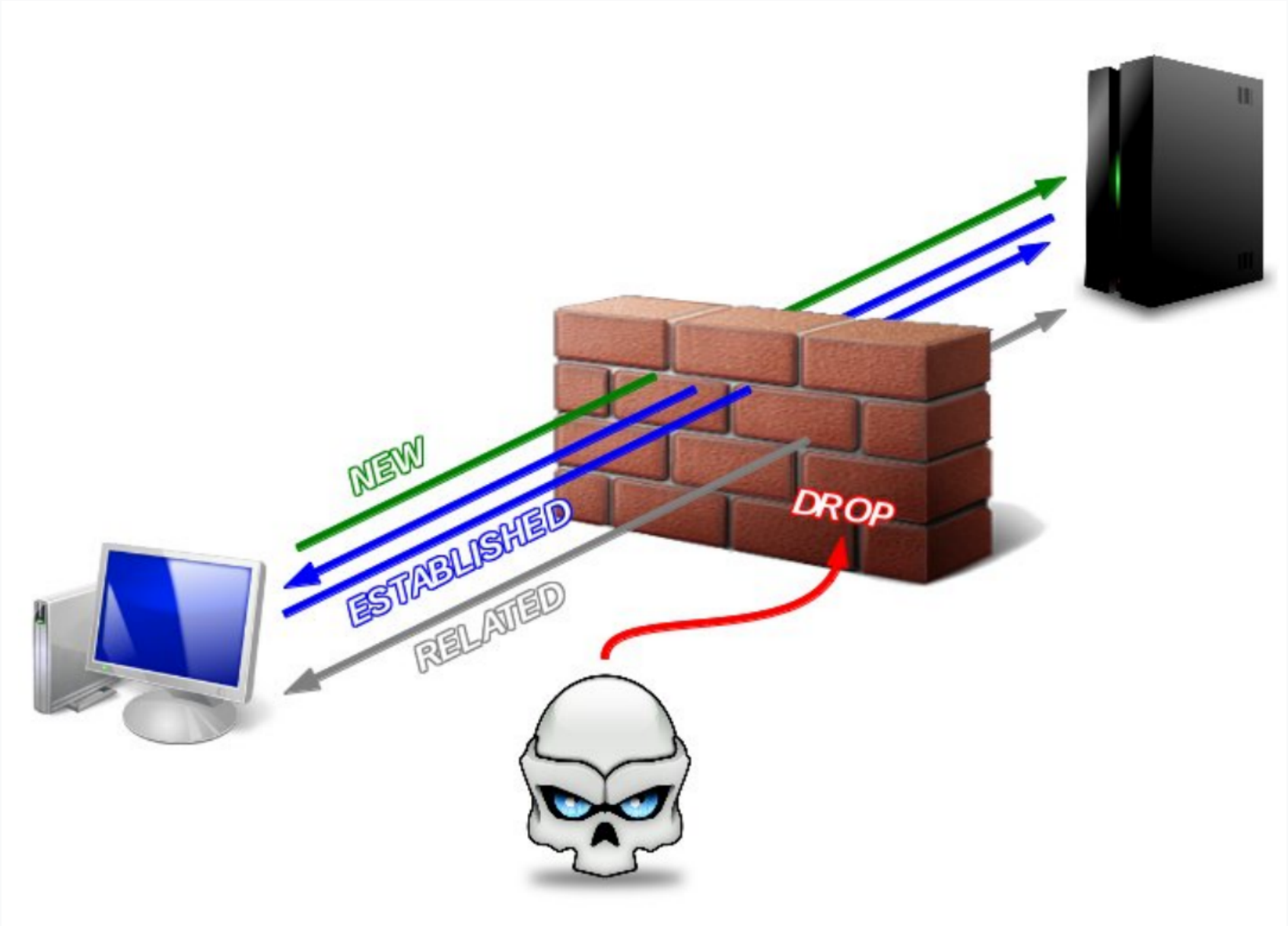
Vulnérable à l'usurpation d'IP (aucun moyen de savoir qu'un packet correspond à une connexion existante)

Le filtrage de paquets: stateful

Filtrage avancé (stateful)

- Regarde les flags TCP
- Garde en mémoire un état des connexions
- Rejette les paquets ne correspondant pas à l'état attendu (selon l'automate TCP)
- Rappel sur l'établissement d'une connexion TCP :
  - SYN
  - SYN+ACK
  - ACK

Le filtrage de paquets: stateful



Le filtrage de paquets

- Mise en place des règles en fonction de la politique de sécurité décidée
- Les règles définissent les paquets autorisés à entrer et à sortir
- Autorisation/refus en fonction des adresses/ports source/destination
- On termine toujours (dernière règle) par un refus d'accès de toutes les adresses et de tous les ports (blocage par défaut)

Le filtrage de paquets

La configuration suivante est-elle correcte ?

	src	port	dst	port	proto	action
1	any	any	any	any	any	deny
2	any	any	10.0.0.1	25	tcp	permit

Le filtrage de paquets

La configuration suivante est-elle correcte ?

	src	port	dst	port	proto	action
1	any	any	any	any	any	deny
2	any	any	10.0.0.1	25	tcp	permit

ATTENTION à l'ordre d'évaluation des règles

Correction :

	src	port	dst	port	proto	action
1	any	any	10.0.0.1	25	tcp	permit
2	any	any	any	any	any	deny

Le filtrage de paquets

La configuration suivante est-elle correcte ?

	src	port	dst	port	proto	action
1	any	any	10.0.0.1	25	tcp	permit
2	any	any	any	any	any	deny

Le filtrage de paquets

La configuration suivante est-elle correcte ?

	src	port	dst	port	proto	action
1	any	any	10.0.0.1	25	tcp	permit
2	any	any	any	any	any	deny

ATTENTION : si les requêtes sortent, les réponses doivent entrer !

Correction :

	src	port	dst	port	proto	action
1	any	any	10.0.0.1	25	tcp	permit
2	10.0.0.1	25	any	any	tcp	permit
3	any	any	any	any	any	deny

Le filtrage de paquets

ATTENTION aux règles cachées

- Cisco applique implicitement `deny all` à la fin.
- Ce n'est pas plus mal de l'expliciter.

https://cyber.gouv.fr/sites/default/files/IMG/pdf/NP_Politique_pare_feu_NoteTech.pdf

Les règles de filtrage : Cisco

Sur Cisco, on applique les règles soit en entrée soit en sortie sur une interface donnée :

```
interface GigabitEthernet0/0
 ip access-group 100 in
 ip access-group 101 out
```

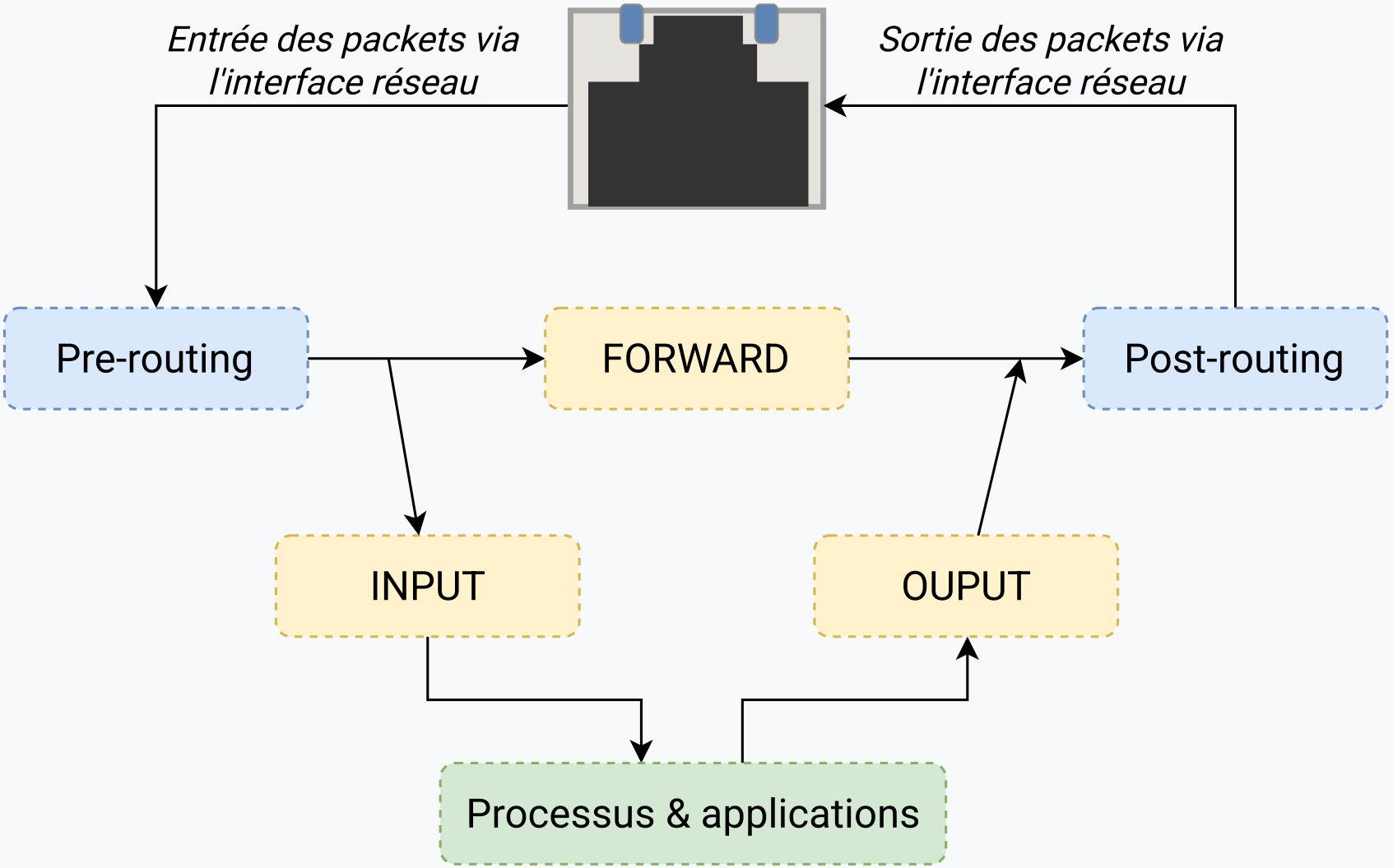
Les règles de filtrage : Netfilter

Sous Linux : Netfilter (commande : iptables)

La table `filter` comprend 3 chaînes :

- INPUT : ce qui entre
- OUTPUT : ce qui sort
- FORWARD : ce qui traverse

Les règles de filtrage : Netfilter



Les problèmes d'architecture

Le filtre de paquets travaille sur des adresses IP et des numéros de ports

- Êtes-vous en adressage public ou privé ?
- Avez-vous du NAT statique ?
- Avez-vous du NAT dynamique ?
- Votre pare-feu est placé avant ou après la translation ?

Rappel sur le NAT

- Adressage privé en interne
- Une seule adresse publique : celle du routeur d'accès
- Règle de réécriture :
  ```
  @client:port_X => @serveur:port_80 # devient
  @routeur:port_Y => @serveur:port_80
  ```
- Traitement inverse sur la réponse

Les problèmes de protocoles

Que savez vous des protocoles

- FTP ?
- IRC ?

Les problèmes de gestion

- Mon réseau est important
  - Beaucoup de machines => beaucoup de règles
- J'acquière un nouveau serveur
  - => nouvelle adresse IP (fixe et joignable de dehors)
- J'ai déjà 10 000 règles
- Où vont se positionner les nouvelles règles ?

Cloisonnement des réseaux

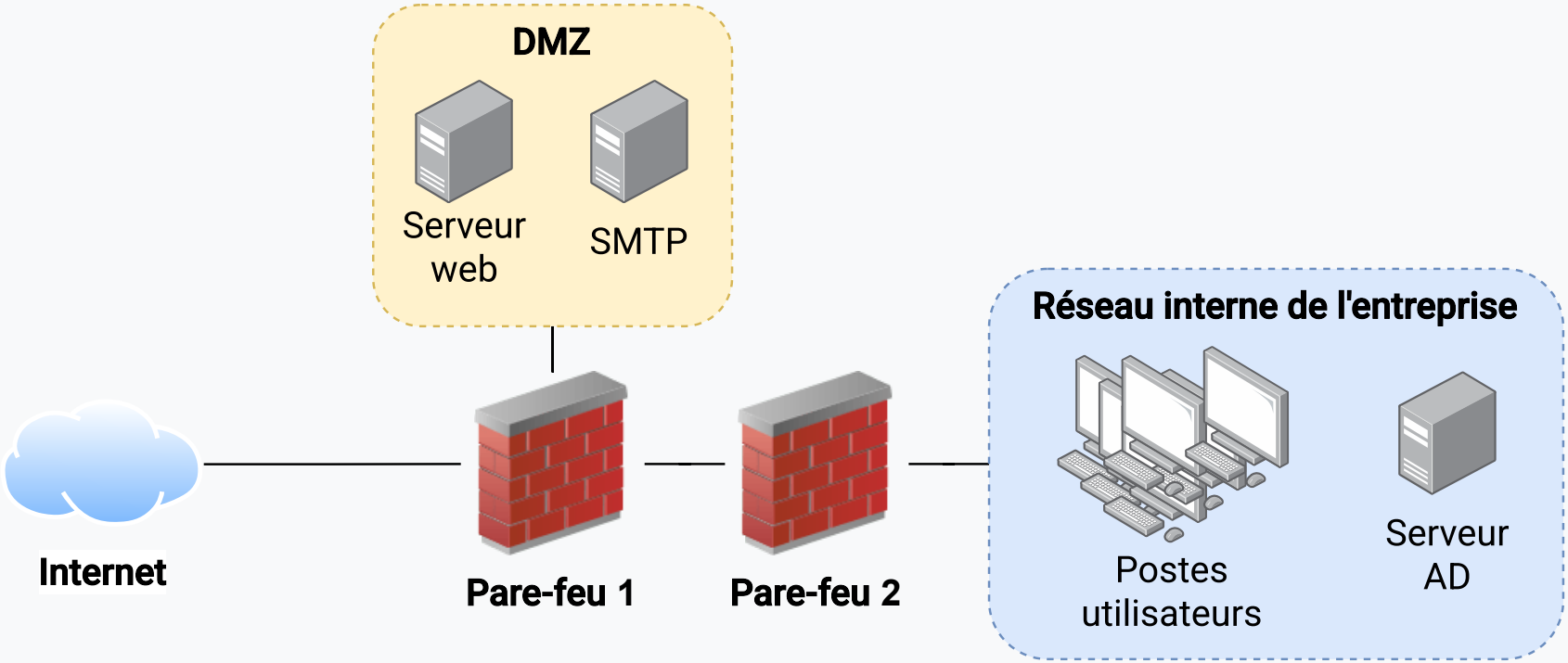
Différents sous-réseaux ont des besoin de sécurité différents :

- Réseau des employés
- Compta
- Réseaux de test
- Réseaux des serveurs
- Réseaux des serveurs publics
- Etc

Cloisonnement des réseaux

- Séparation de ces réseaux par différents pare- feu
- Le réseau le « plus interne » sera le « plus protégé »
- Tous les équipements de sécurité auront dû être traversés
- A condition que tout soit configuré correctement

Cloisonnement des réseaux



Cloisonnement des réseaux

- Avantages :
  - Contrôle des flux entrants et sortants
  - Contrôle aux niveau liaison de données, réseau, transport et application
  - Analyse de contenu
  - Hiérarchisation des besoins de sécurité
- Mais solution très lourdes et coûteuse

Conclusion

- Création d'un point d'entrée unique
  - Plus facile à gérer
  - Que faire si cet élément tombe ?
- Le cloisonnement des réseaux est un élément de base d'une architecture de sécurité
- Inséparable de la mise en place d'une politique de sécurité en amont
- Nécessite des moyens humains et financiers