COGICEO

Sending backdoors to the edge of the world for fun but mostly profit

LeHack2024

$ whoami

- Joytide | Clovis Carlier
  - @j0y71d3
- Auditeur en cybersécurité chez @Cogiceo
  - Sécurité offensive
  - ~25 pentesters et devs à Paris et Lyon
  - On recrute !

Contexte

Solution

Profit

Fun

Contraintes

Contexte

Redteams et intrusions physiques

Redteams et **intrusions physiques**

- S’introduire dans les bâtiments de la cible

Contexte

Redteams et intrusions physiques

Redteams et **intrusions physiques**

- S’introduire dans les bâtiments de la cible
- Récupérer des informations sensibles (fiches de payes, contrats, etc.)

Contexte

Redteams et intrusions physiques

Redteams et **intrusions physiques**

- S’introduire dans les bâtiments de la cible
- Récupérer des informations sensibles (fiches de payes, contrats, etc.)
- Accéder aux différents réseaux informatiques de l’entreprise
  - Intrusion de réseau **interne**

Contexte

RSE késako ?

« Intrusion interne » (Réseau Microsoft Active Directory, Samba, industriel… + serveurs + postes de travail)

→ Présentiel ou VPN

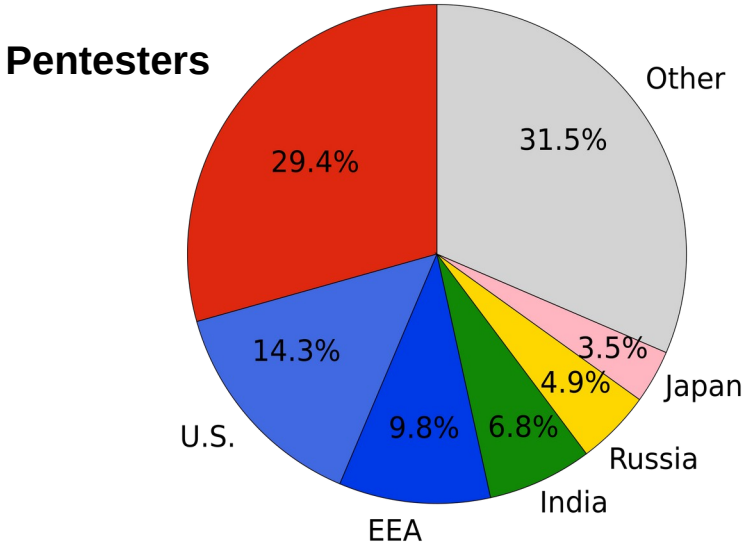
Contexte

RSE késako ?

« Intrusion interne » (Réseau Microsoft Active Directory, Samba, industriel… + serveurs + postes de travail)

→ Présentiel ou VPN

- **Responsabilité sociétale des entreprises** (RSE)
  - Limiter l'impact environnemental d'une société d'audit en cybersécurité
  - Nécessité commerciale (valorisée dans les appels d'offres)



Émissions de CO2 mondiales (source : estimation)

Contexte

Contrainte logistiques

Usine dans la Creuse

- Enchaînement des modes de transports
- Temps de transport perdu (voire facturé)
- Difficulté de logement
- Difficulté de restauration
- Ressources et compétences IT locales restreintes

Starter-pack du pentester en interne :

Contexte

VPN : une solution avec son lot de problèmes

g) la disponibilité de technologies de l'information et de la communication (par exemple les ressources techniques requises pour mettre en place un audit à distance à l'aide de technologies venant à l'appui d'une collaboration à distance);

Source : ISO19011, « 5.4.4 Détermination des ressources du programme d'audit »

Contexte

VPN : une solution avec son lot de problèmes

« Prérequis » d’audit ou de connexion

Contexte

VPN : une solution avec son lot de problèmes

« Prérequis » d’audit ou de connexion

- « Un VPN ? Oui pas problème on va ouvrir un ticket Jira dans le backlog »
- « Ah désolé la personne qui s’occupe des VPN est en vacances… Ah c’est aujourd’hui l’audit ? »
- « C’est normal que ca fonctionne pas, il faut du MFA avec un téléphone enrollé dans notre MDM, on ne vous l’avait pas dit ? »
- « Ouvrir des flux depuis la zone VPN ? Y en a pour 3 semaines minimum là… »

Contexte

Solution

Profit

Fun

Contraintes

Solution

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)
- Silencieux ! (La blueteam en sueur)

Solution

Implant réseau

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)
- Silencieux ! (La blueteam en sueur)
- Sécurisé ! (La douane postale en sueur)

Solution

#not an ad

Solution

#not an ad

- Routeur 4G-LTE commercial : Glinet-XE300
  - OpenWRT sur une architecture MIPS
  - Plein d’interfaces réseaux !
  - Batterie
  - <150€ (+SIM)

Solution

Checklist

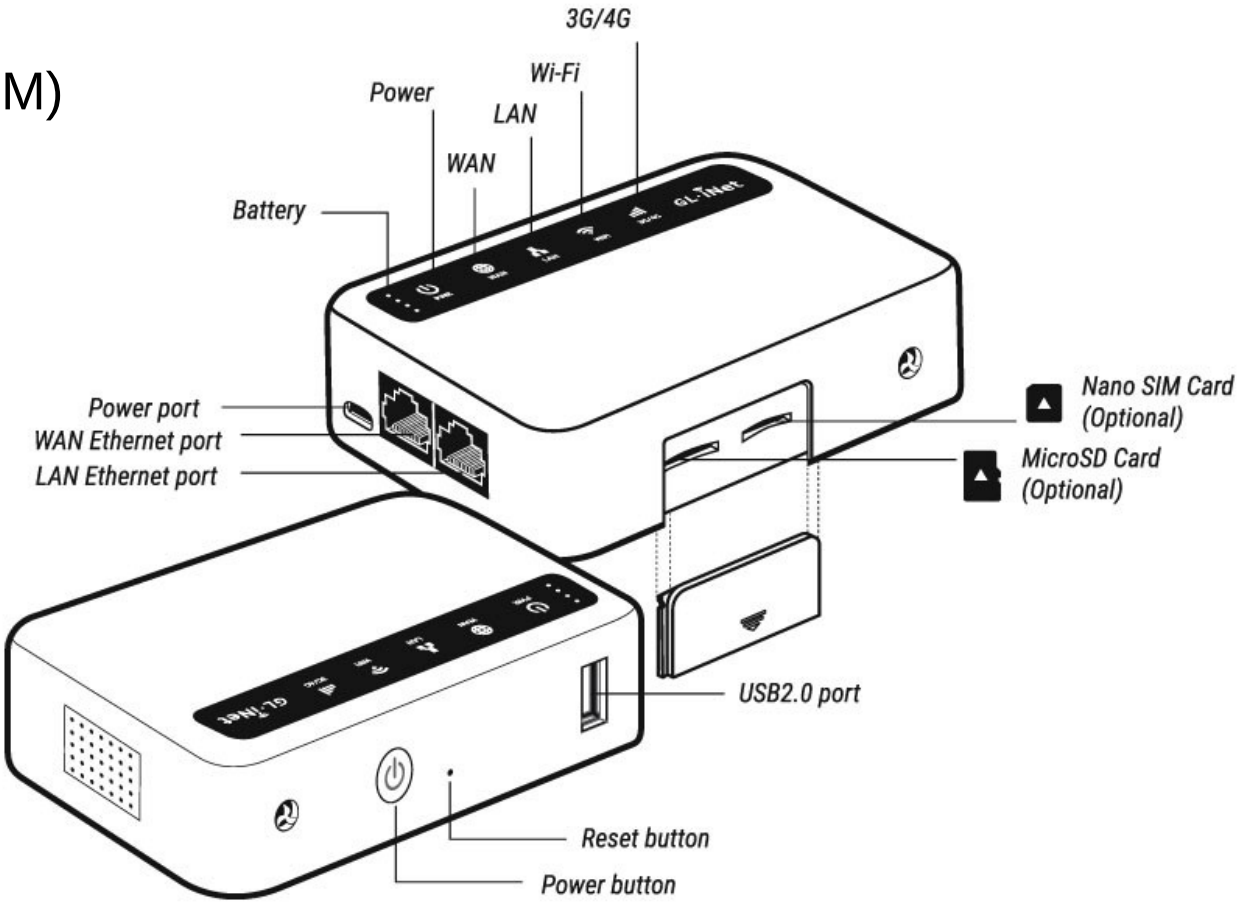
Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)
- Silencieux ! (La blueteam en sueur)
- Sécurisé ! (La douane postale en sueur)

Solution

#not an ad

- Routeur 4G-LTE commercial : Glinet-XE300
  - OpenWRT sur une architecture MIPS
  - Plein d’interfaces réseaux !
  - Batterie
  - <150€ (+SIM)



Solution

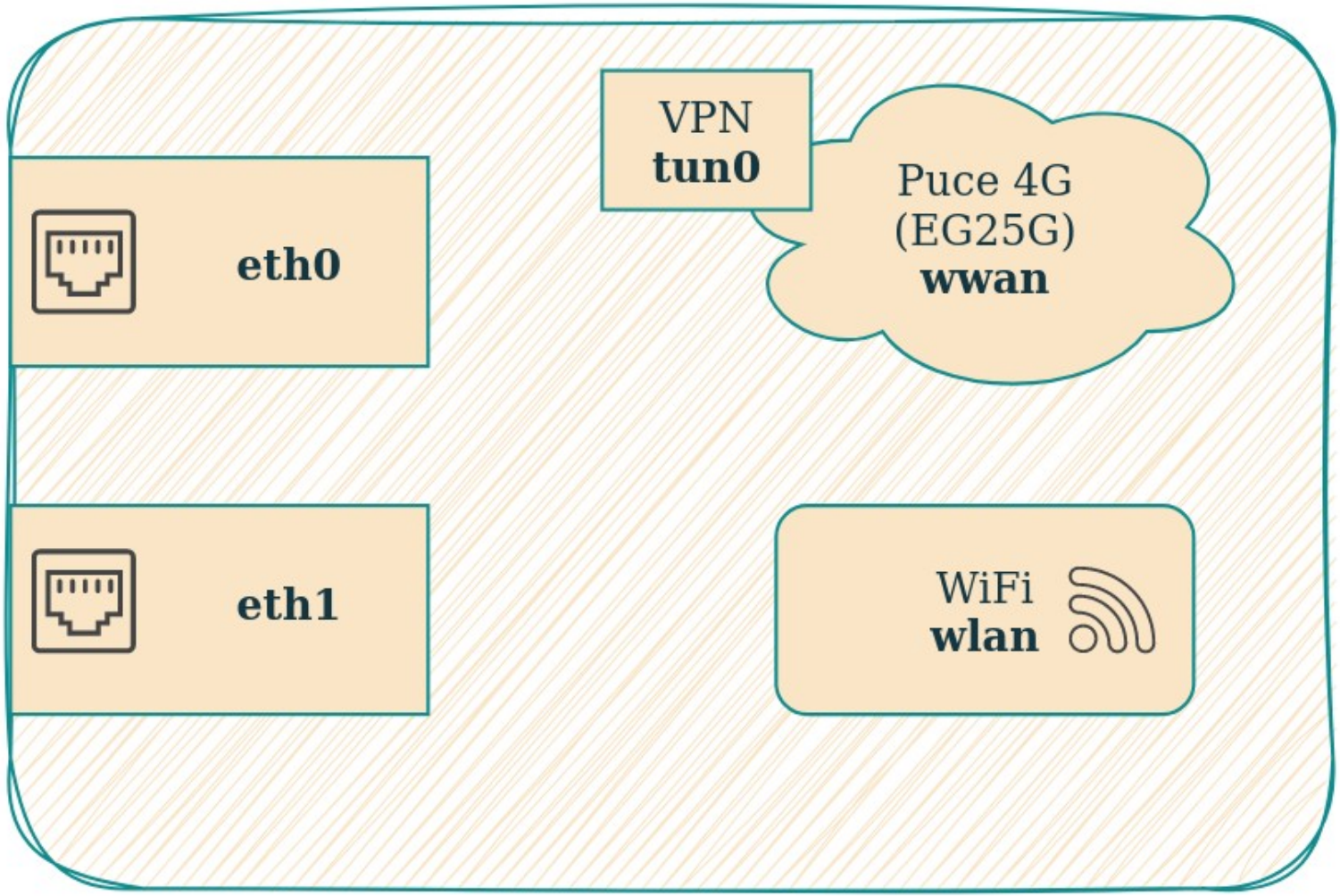
Checklist

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)
- Silencieux ! (La blueteam en sueur)
- Sécurisé ! (La douane postale en sueur)

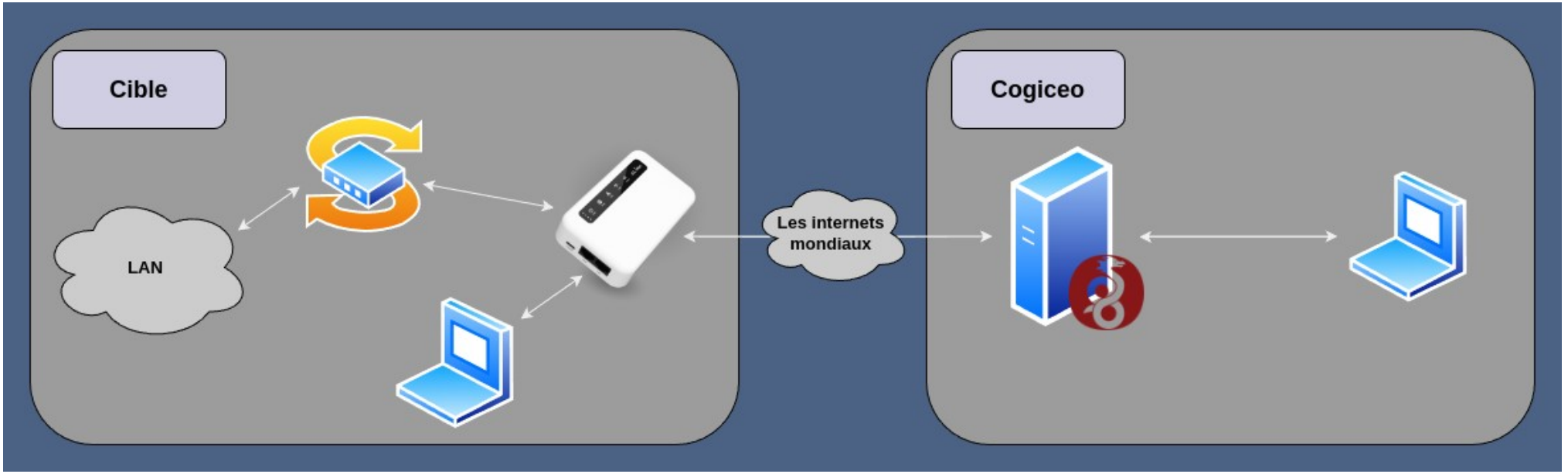
Solution

Interfaces réseau



Solution

VPNOver4G



Solution

Checklist

Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)
- Silencieux ! (La blueteam en sueur)
- Sécurisé ! (La douane postale en sueur)

Contexte

Solution

Profit

Fun

Contraintes

Profit

Firmware customisé

> Contraintes : ca reste un grille pain
>
> 128MB RAM, 128+16MB FLASH NAND/NOR

- Ports d’administration (HTTPS, SSH, Wireguard)

Profit

Firmware customisé

> Contraintes : ca reste un grille pain
>
> 128MB RAM, 128+16MB FLASH NAND/NOR

- Ports d’administration (HTTPS, SSH, Wireguard)
- Paquets classiques (bash, curl, screen)

Profit

Firmware customisé

> Contraintes : ca reste un grille pain
>
> 128MB RAM, 128+16MB FLASH NAND/NOR

- Ports d’administration (HTTPS, SSH, Wireguard)
- Paquets classiques (bash, curl, screen)
- Paquets pour les audits
  - python3, scapy
  - Tcpdump
  - Nmap + NSE scripts (offloader la bande passante)

Profit

Firmware customisé

> Contraintes : ca reste un grille pain
>
> 128MB RAM, 128+16MB FLASH NAND/NOR

- Ports d’administration (HTTPS, SSH, Wireguard)
- Paquets classiques (bash, curl, screen)
- Paquets pour les audits
  - python3, scapy
  - Tcpdump
  - Nmap + NSE scripts (offloader la bande passante)
- Outils !
  - Responder.py et mitm6 (python3-netifaces)
  - Impacket
  - Bypass NAC ?

Profit

Firmware customisé

> Contraintes : ca reste un grille pain
>
> 128MB RAM, 128+16MB FLASH NAND/NOR

- Hardening
  - Système de fichiers chiffré sur une carte SD
  - Firewall entre les différents réseau (LAN, WAN, WLAN, LTE) pour les accès
  - SerialTTY sécurisé
  - Superglue UART, ROM...
  - Hardening linux du serveurs et des dockers

Profit

Firmware customisé

Contraintes : ca reste un grille pain

128MB RAM, 128+16MB FLASH NAND/NOR

Profit

Firmware customisé

> Contraintes : ca reste un grille pain
>
> 128MB RAM, 128+16MB FLASH NAND/NOR

- Hardening
  - Système de fichiers chiffré sur une carte SD
  - Firewall entre les différents réseau (LAN, WAN, WLAN, LTE) pour les accès
  - SerialTTY sécurisé
  - Superglue UART, ROM...
  - Hardening linux du serveurs et des dockers
- Stealth
  - ICMP ? DHCPv6 ? C’est ciao
  - Wi-Fi caché
  - Pont transparent entre les interfaces au boot

Profit

Checklist

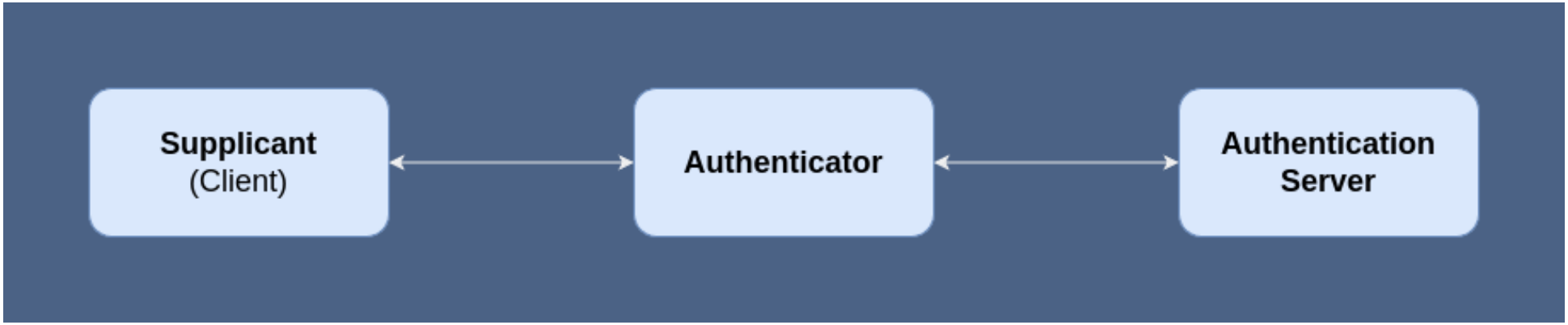
Construisons notre implant réseau pour les missions VPN **et** Redteam !

- Réseau
  - **VPN** jusqu'à chez nous sans faire 10 tunnels TLS
  - **4G/LTE** mondiale pour ne pas être dépendant du réseau du client
  - 2 ports ethernet pour le **contournement de NAC**
- Format
  - Petit : doit tenir dans une poche et être facilement **dissimulable**
  - Envoi postal à moindre coût
  - Doit être autonome électriquement : **batterie** (>4h)
- Moteur **linux**
  - Facilement **modulable**
  - Administration réseau et système
  - Portage des **outils** non-utilisables en VPN (Responder, mitm6…)
- Coût réduit (tests de cloisonnement)
- Silencieux ! (La blueteam en sueur)
- Sécurisé ! (La douane postale en sueur)

Profit

NAC : Network Access Control

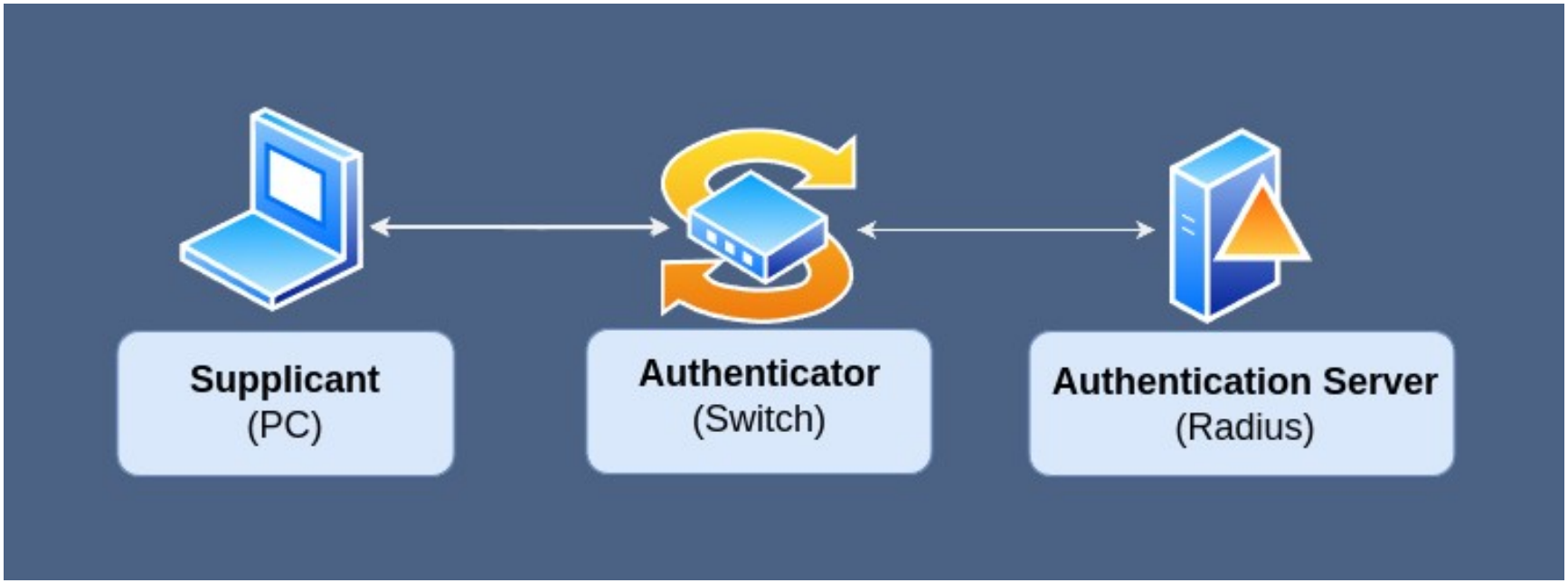
- Restriction des accès au réseau (Wi-Fi et filaire)
  - **Identification** de la machine
  - **Authentification** de la machine et/ou de l'utilisateur



Profit

NAC : Network Access Control

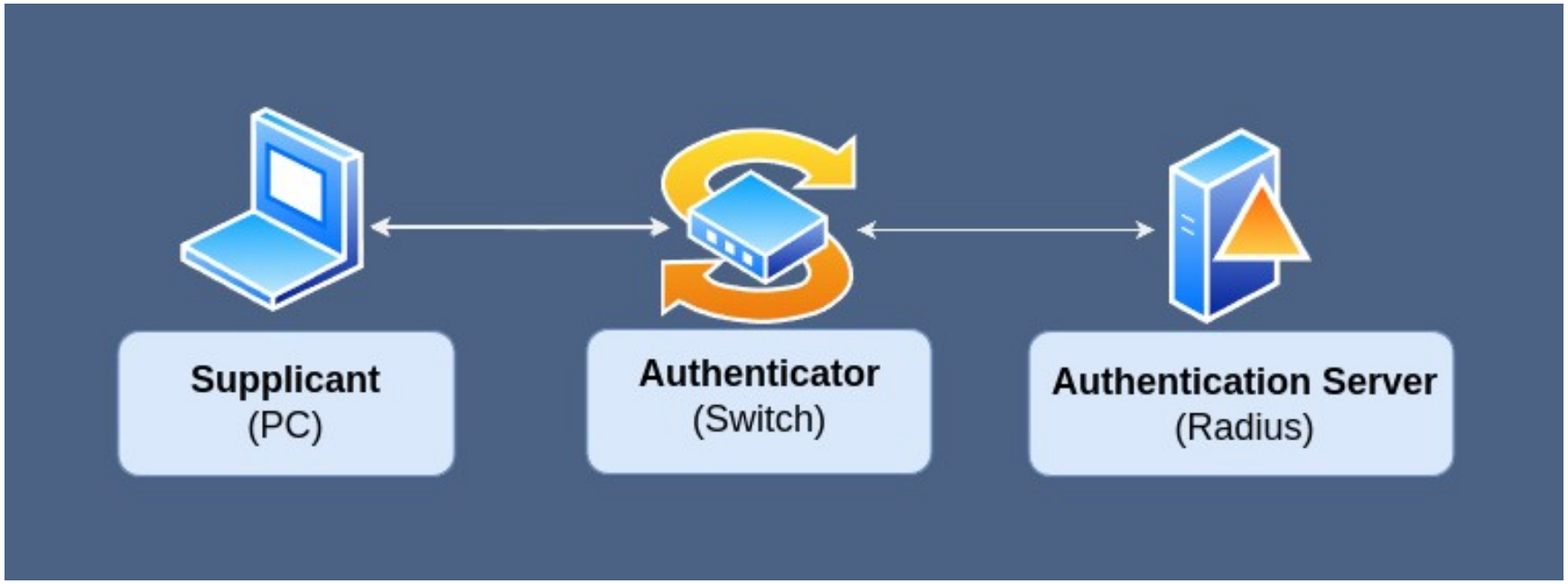
- Restriction des accès au réseau (Wi-Fi et filaire)
  - **Identification** de la machine
  - **Authentification** de la machine et/ou de l'utilisateur



RADIUS : « Remote Authentication Dial-In User Service »

Profit

NAC : Network Access Control

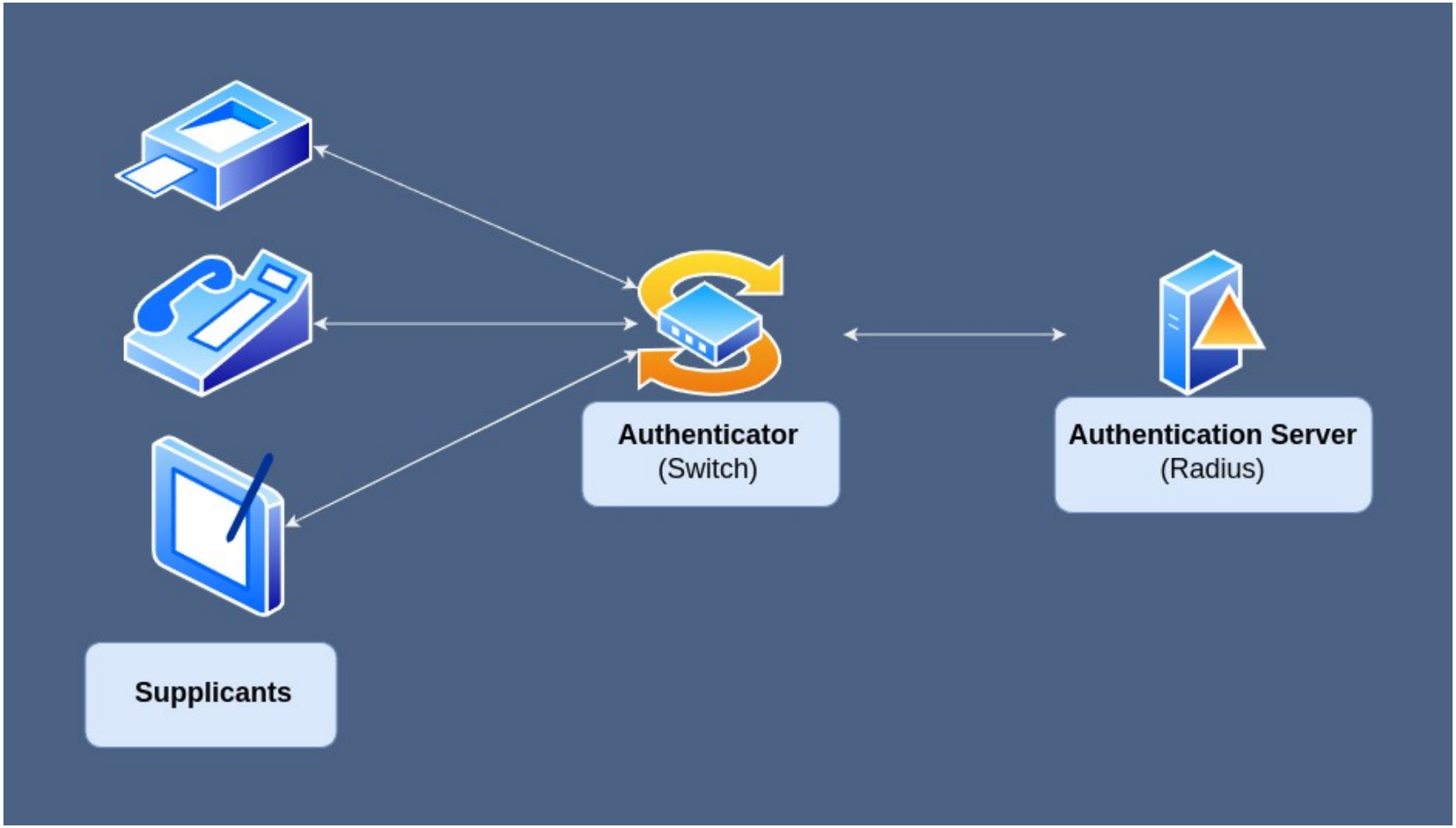


- **Uncontrolled** port
- **Controlled** port
  - **Authorized** state: trafic autorisé dans les 2 sens après l'authentification du client
  - **Unauthorized** state: le trafic est filtré en ingress et egress car le client est soit non-connecté, soit a échoué l'étape d'authentification. Les types de paquets autorisés seront **EAPoL, CDP et STP**

Profit

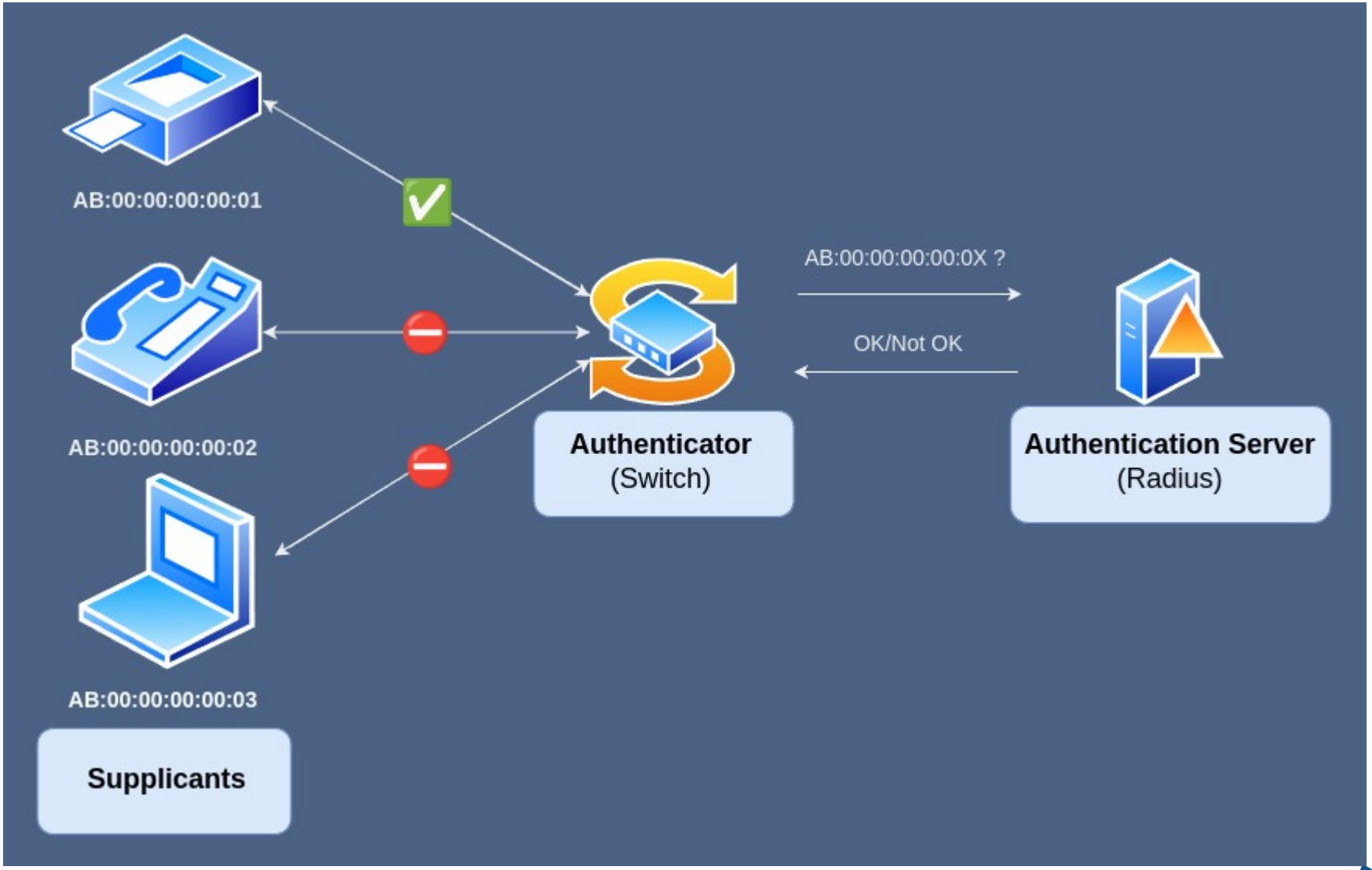
NAC : Network Access Control

- Le minimum syndical : le MAC Address Filtering



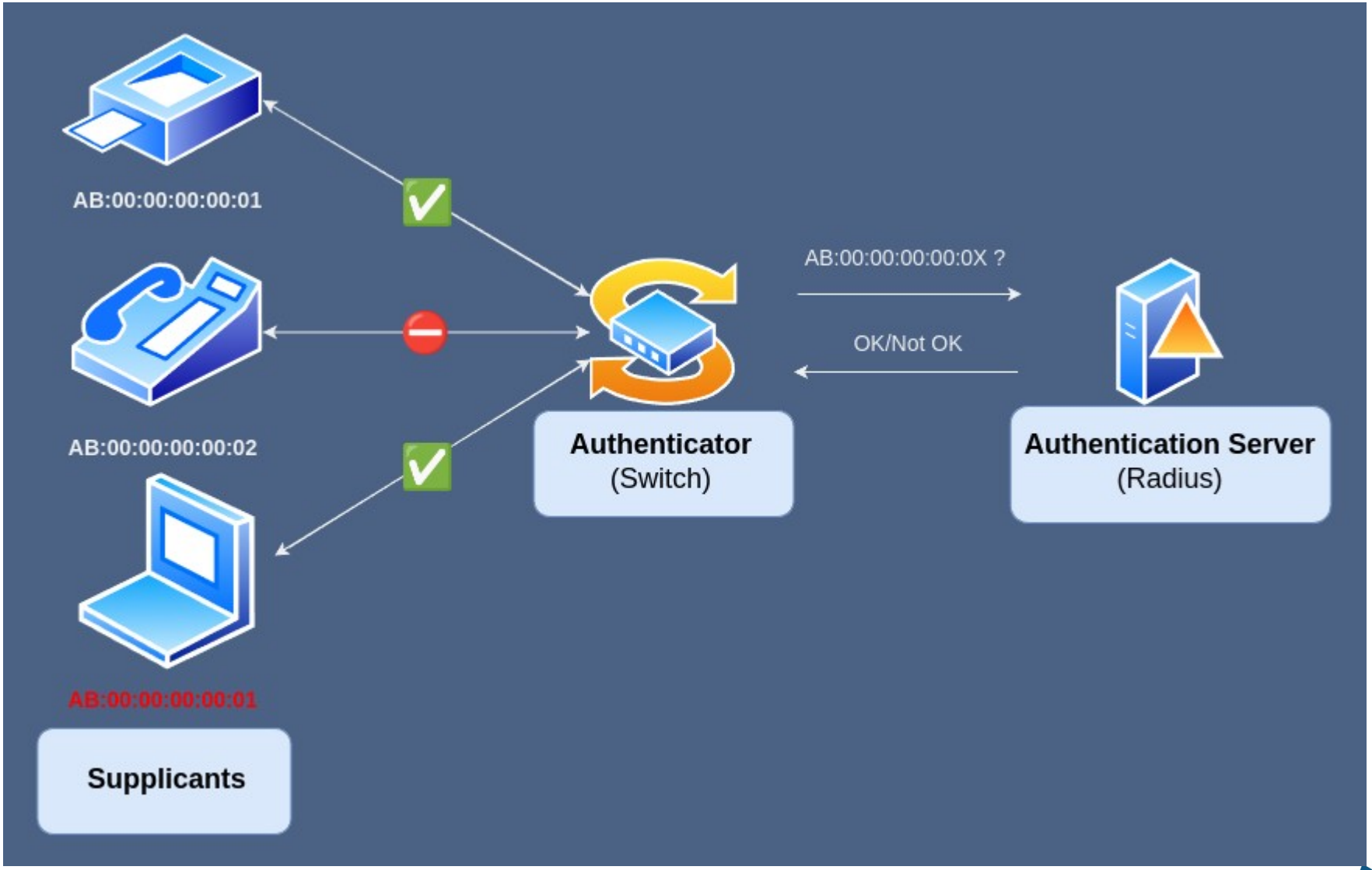
Profit

NAC : MAC Address Filtering



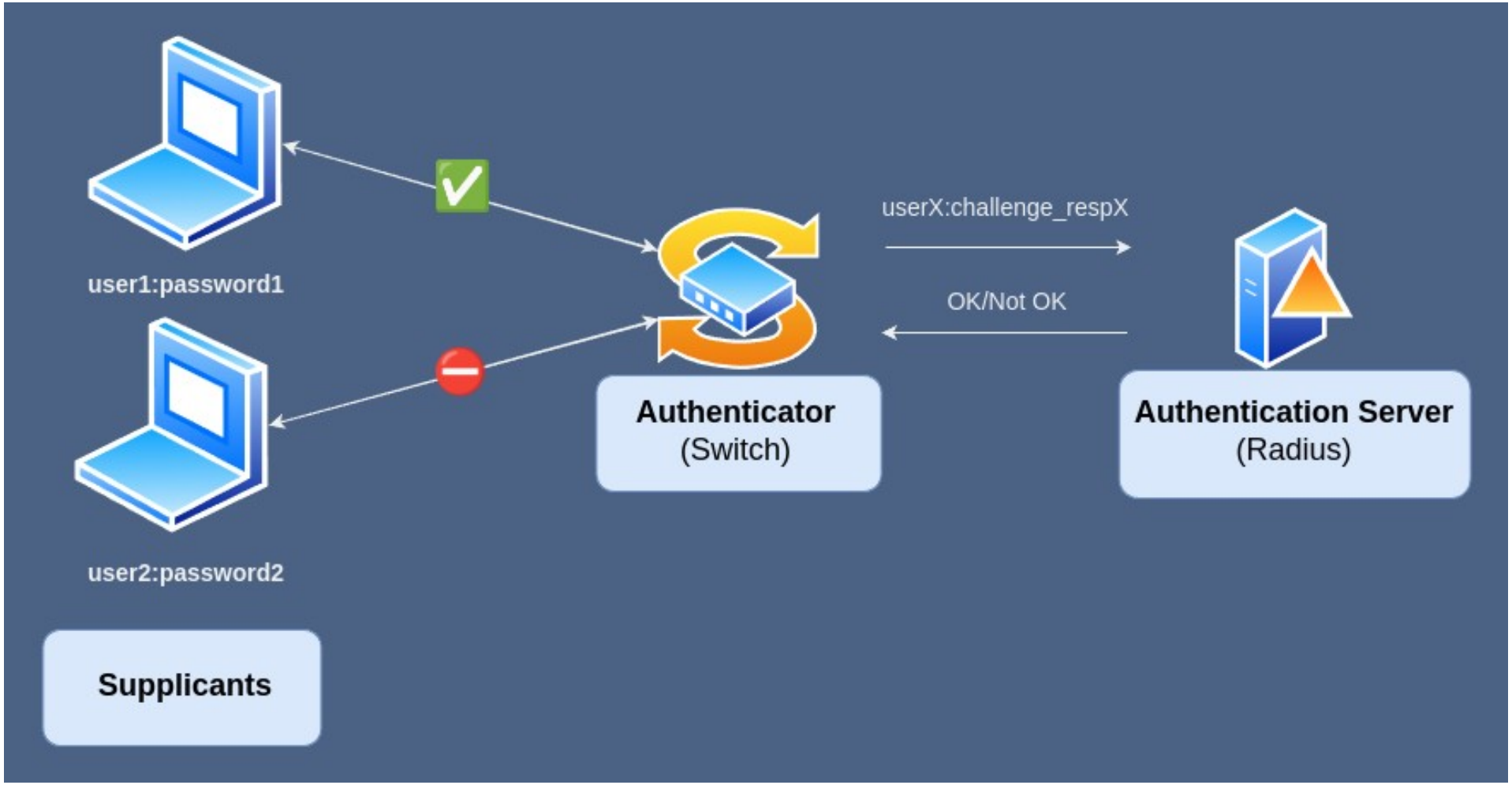
Profit

NAC : MAC Address Filtering

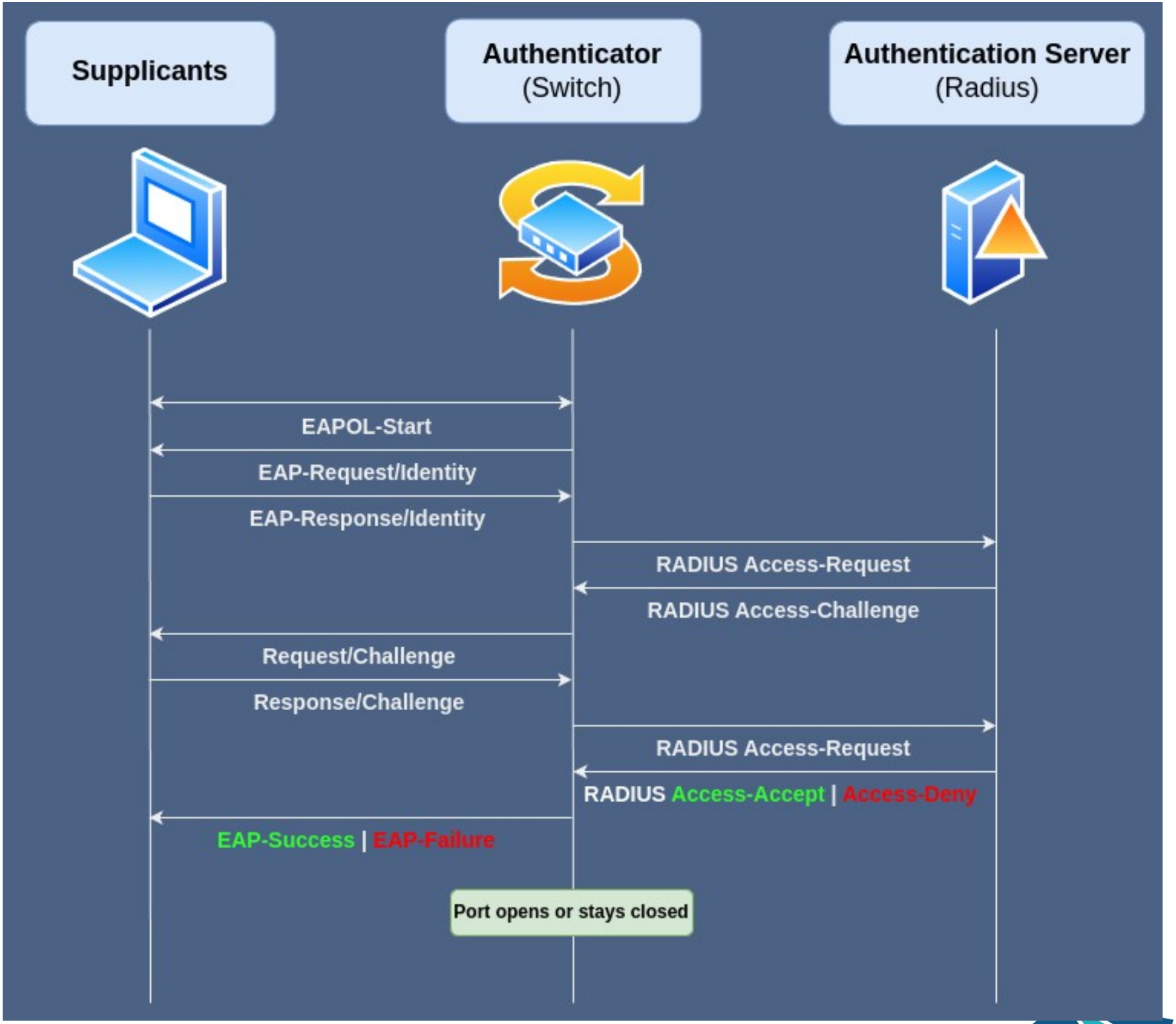


Profit

NAC : 802.1X



- EAP : Extensible Authentication Protocol
- EAPoL pour les paquets user – switch
- Radius ou EAPoR pours les paquets switch - Radius


Supplicants
Authenticator
(Switch)
Authentication Server
(Radius)
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request
RADIUS Access-Challenge
Request/Challenge
Response/Challenge
RADIUS Access-Request
RADIUS Access-Accept | Access-Deny
EAP-Success | EAP-Failure
Port opens or stays closed

Profit

NAC : 802.1X

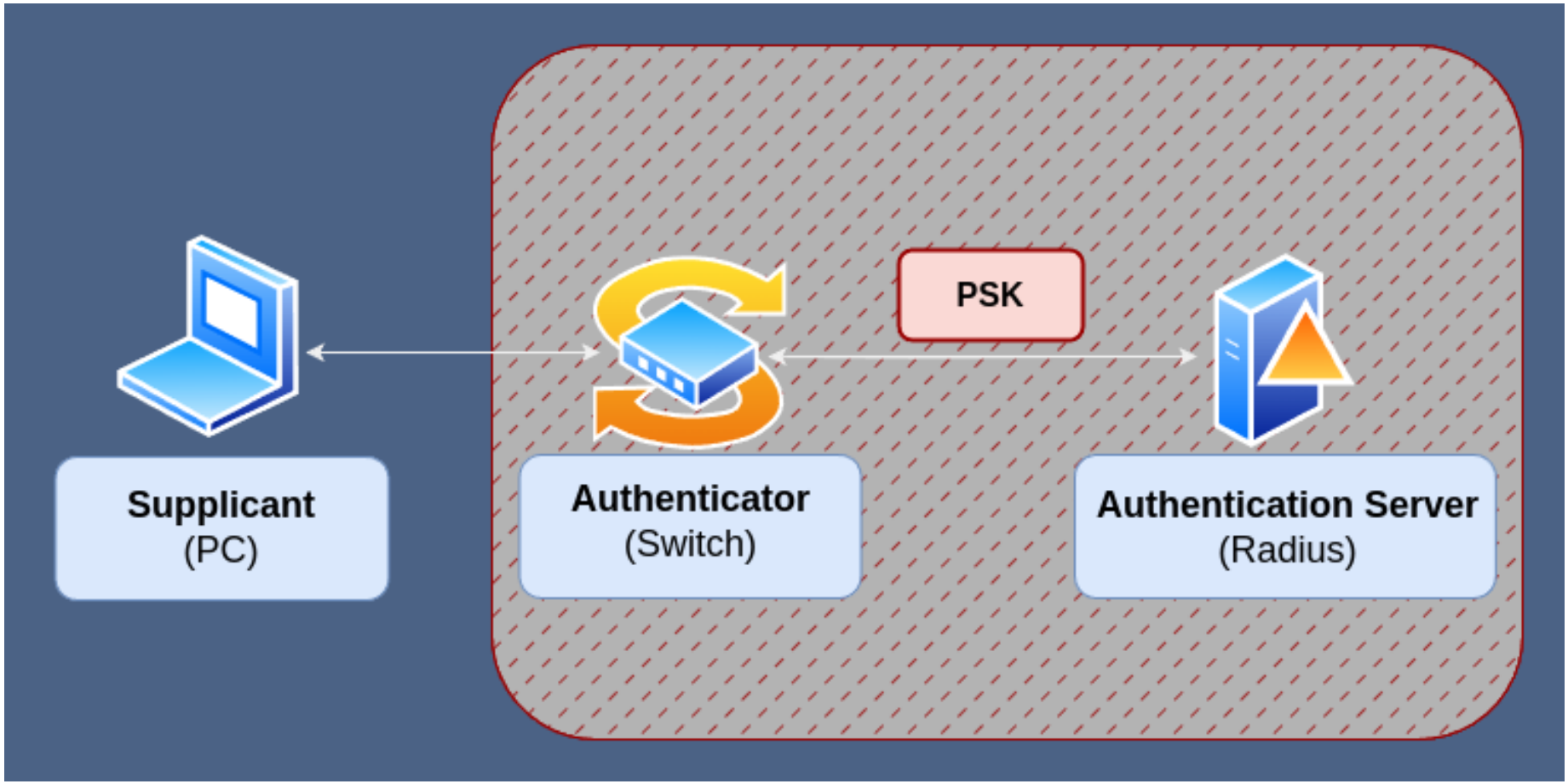
- Différentes méthodes EAP
  - EAP-MD5
  - PEAP (Certificat server-side) ou EAP-TTLS (Certificat server-side avec PKI)
    - « inner-EAP » avec PAP, CHAP ou **MSCHAPv2**
  - EAP-TLS (Certificat server-side et client-side avec PKI, authentification simultanée)
  - [...]

```
eap.md5.value = md5(hexa(request id | password | request challenge))
```

Profit

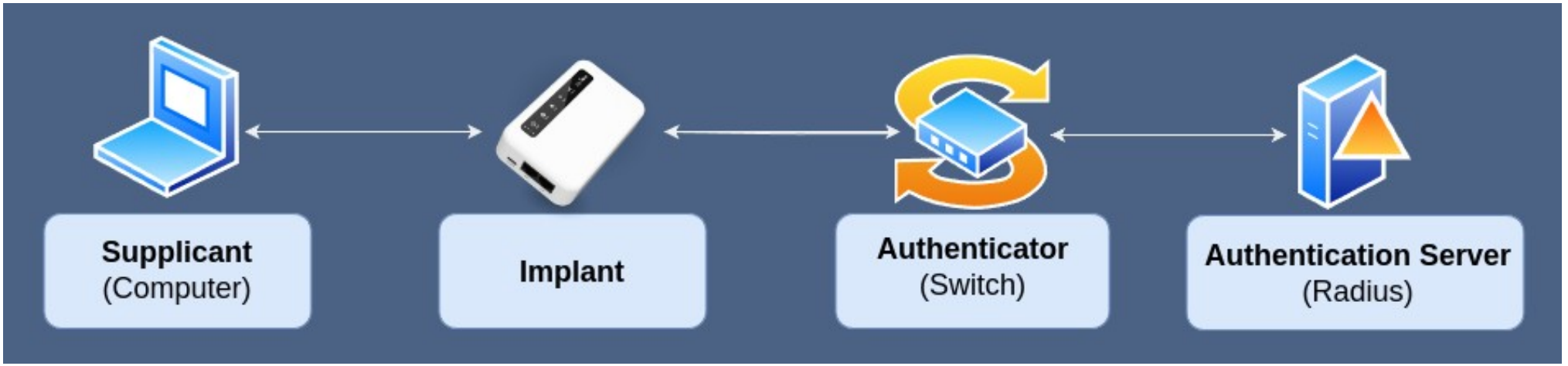
NAC : Pont transparent

- « Vulnerable-by-design »



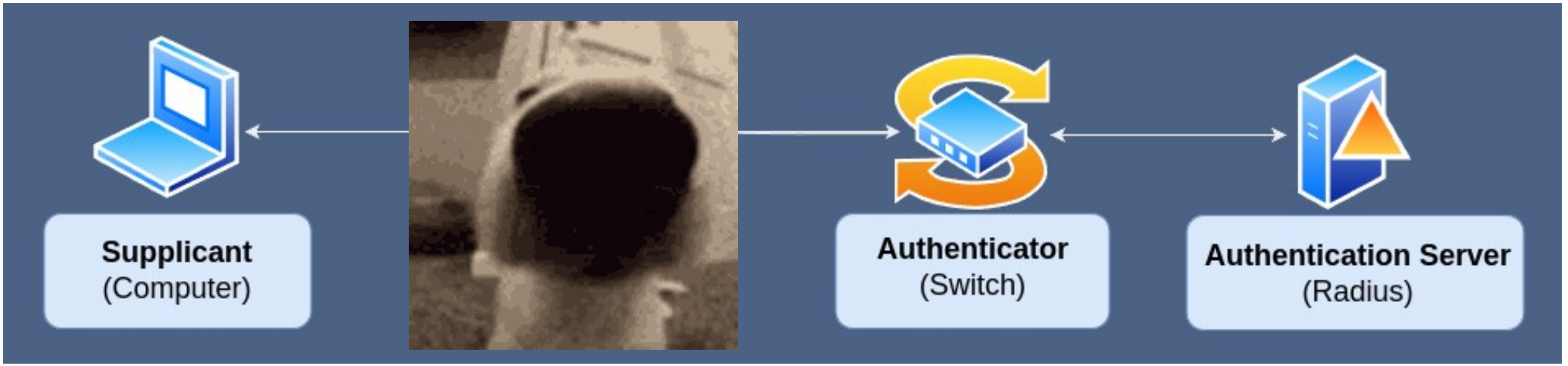
Profit

NAC : Pont transparent



Profit

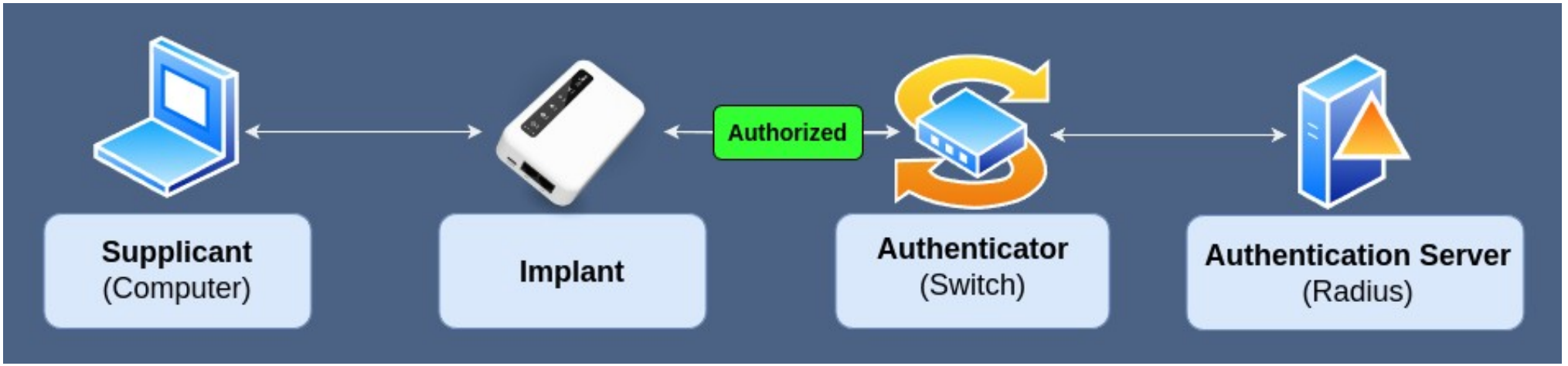
NAC : Pont transparent



Profit

NAC : Pont transparent

- « Vulnerable-by-design »



Contexte

Solution

Profit

Fun

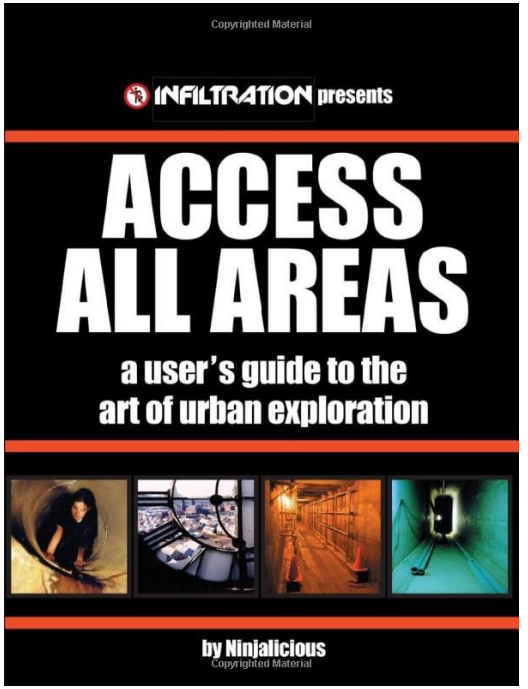
Contraintes

Fun

AAN : Access All Networks

- **Pont transparent** entre les 2 interfaces ethernet
- Monitoring réseau **passif** (IPs, MACs, targets)
- **Capture** du flux EAP
- Evil twin filaire avec **hostapd-wpe**

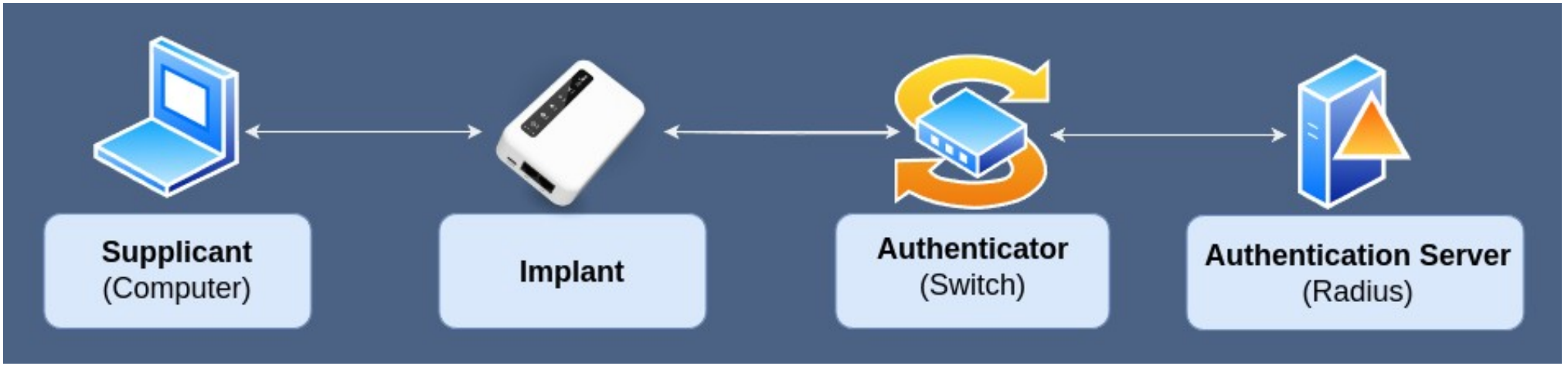
https://github.com/cogiceo/aan



Fun

AAN : Access All Networks

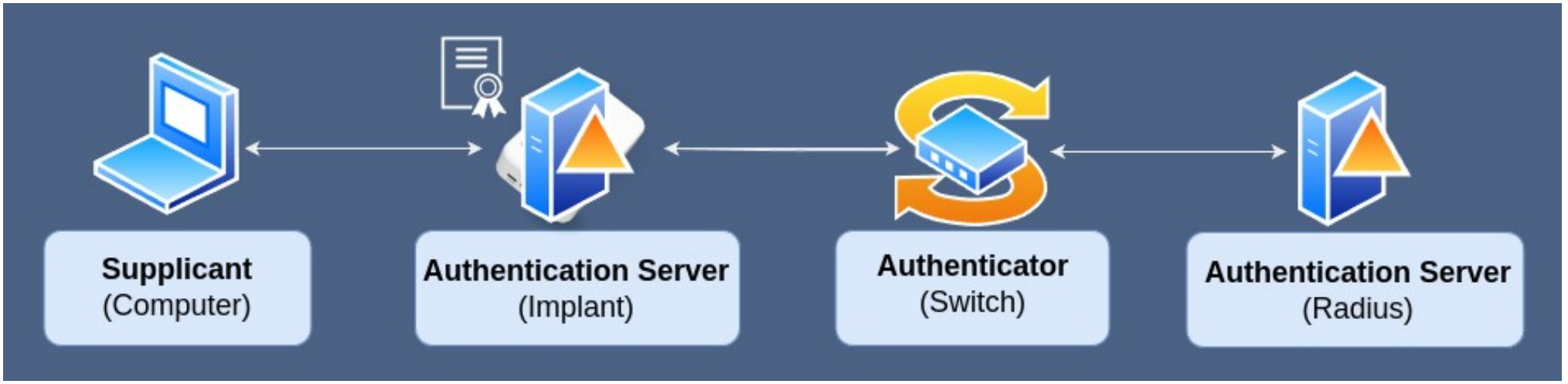
- Pont transparent + récupération des infos supplicant + spoof = win !
- Hostapd-wpe + Pont transparent = double win ! (On récupère potentiellement des identifiants AD)



Fun

AAN : Access All Networks

- Pont transparent + récupération des infos supplicant + spoof = win !
- Hostapd-wpe + Pont transparent = double win ! (On récupère potentiellement des identifiants AD)
  - Condition : le client ne vérifie pas le certificat serveur



Fun

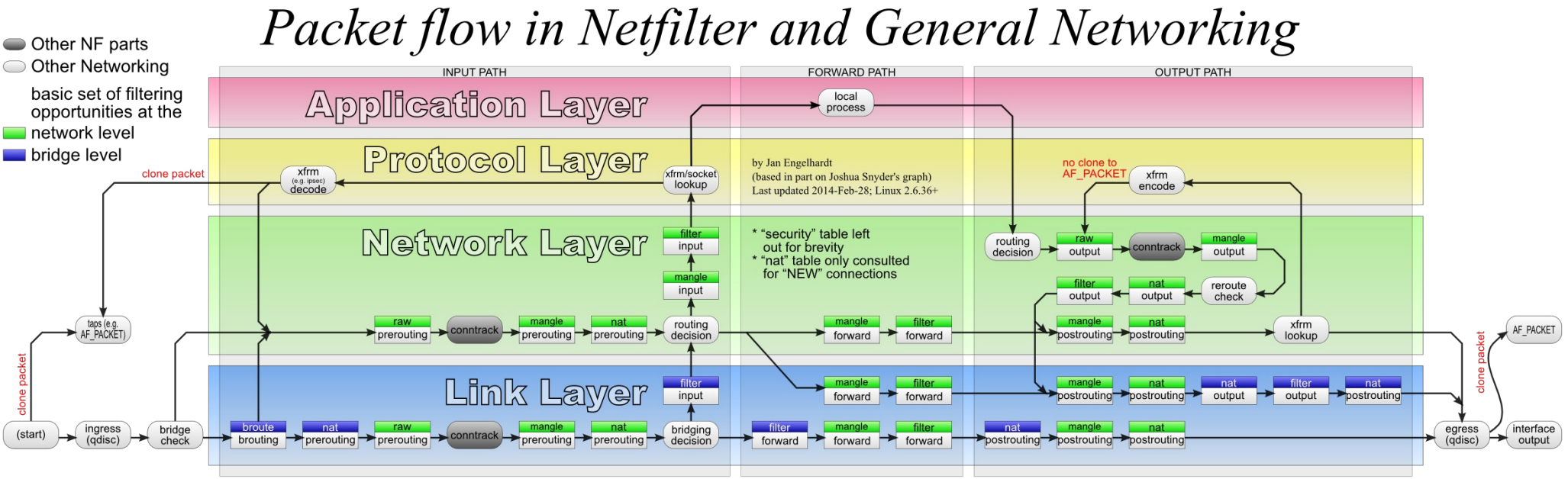
AAN on a toaster

- Comment on fait un pont transparent **avec** scapy ?
- Réponse quand on a 128mb de ram : **on ne fait pas**

Fun

AAN on a toaster

- Comment on fait un pont transparent **sans** scapy ?



Fun

Réplication de paquets

- Comment on fait un pont transparent **sans** scapy ?
- Netfilter avec iptables / nftables ? (tee / dup)

TEE

The **TEE** target will clone a packet and redirect this clone to another machine on the **local** network segment. In other words, the nexthop must be the target.

--gateway *ipaddr*
Send the cloned packet to the host reachable at the given IP address. Use of 0.0.0.0 (for IPv4 packets) or :: (IPv6) is invalid.

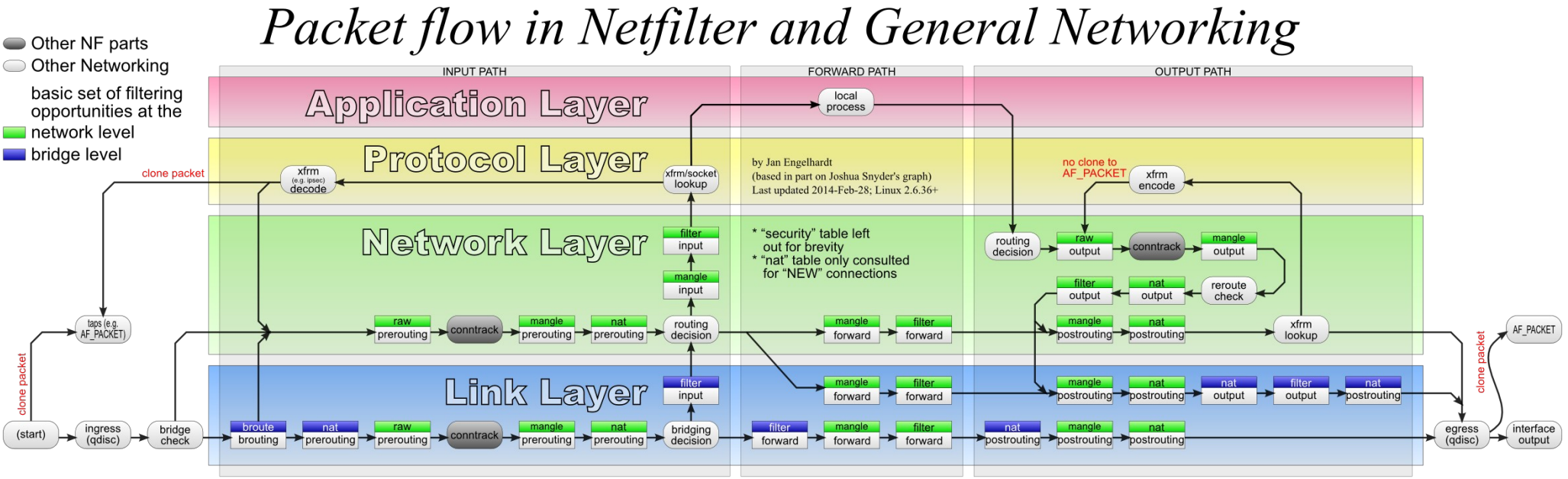
To forward all incoming traffic on eth0 to an Network Layer logging box:

-t mangle -A PREROUTING -i eth0 -j TEE --gateway 2001:db8::1

Fun

Réplication de paquets

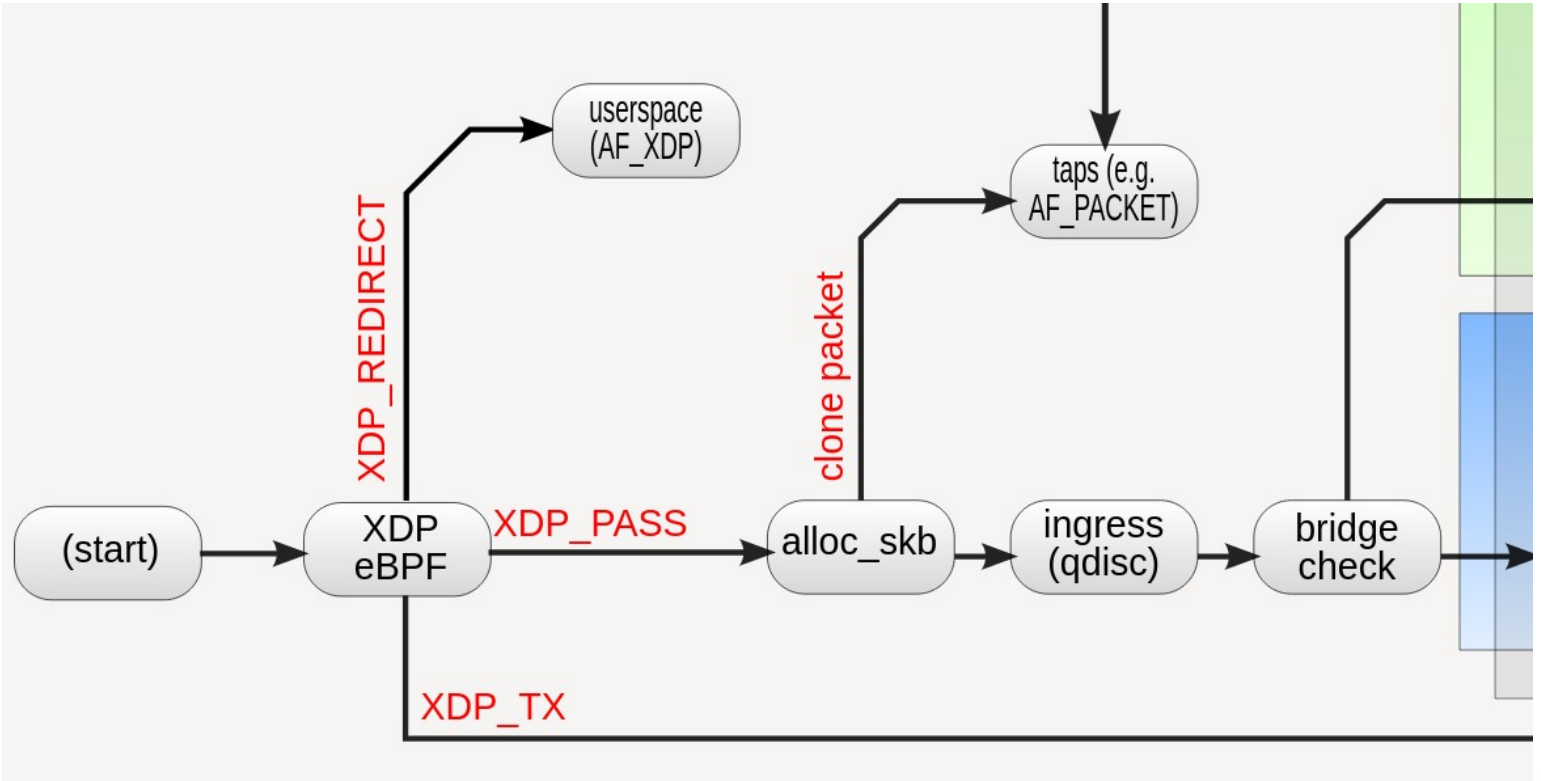
- Comment on fait un pont transparent **sans** scapy ?
- Netfilter avec iptables / nftables ? (tee / dup)
- Avec autre chose ?



Fun

Réplication de paquets

- Comment on fait un pont transparent **sans** scapy ?
- Netfilter avec iptables / nftables ? (tee / dup)
- Avec autre chose ?



Fun

Réplication de paquets

- Comment on fait un pont transparent **sans** scapy ?
- Netfilter avec iptables / nftables ? (tee / dup)
- Avec autre chose ?

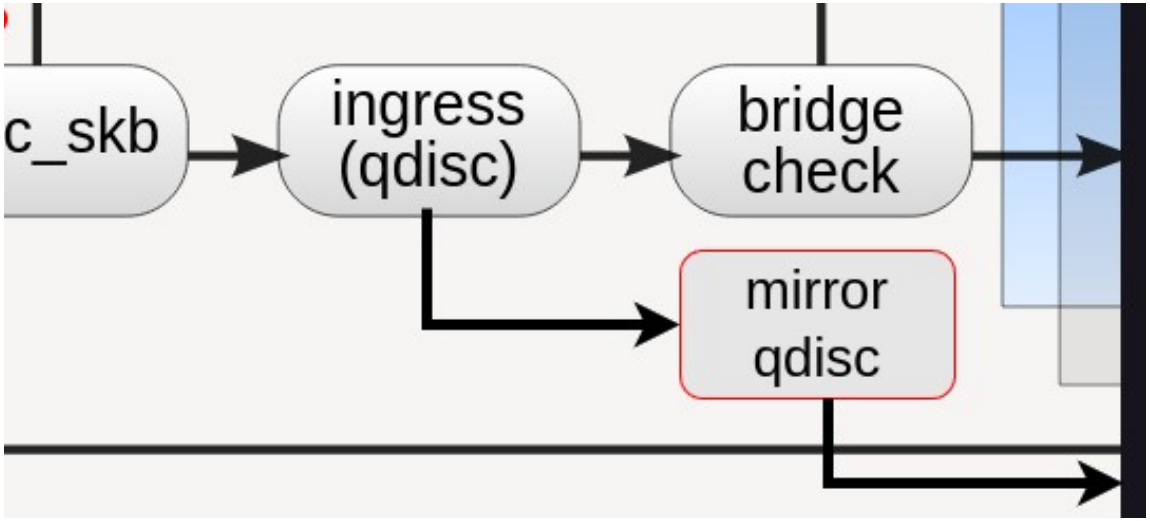
```
tc qdisc add dev eth0 ingress
tc qdisc add dev eth1 ingress

tc filter add dev eth0 parent ffff: protocol all u32 match u32 0 0 action mirred egress mirror dev eth1
tc filter add dev eth1 parent ffff: protocol all u32 match u32 0 0 action mirred egress mirror dev eth0
```

Fun

Réplication de paquets

- Comment on fait un pont transparent **sans** scapy ?
- Netfilter avec iptables / nftables ? (tee / dup)
- Avec autre chose ?



Fun

Démo # 1 : AAN

Fun

Démo # 1 : hostapd-wpe

Contexte

Solution

Profit

Fun

Contraintes

Contraintes

Story time

- Contrainte technique #1 : Dépendance au **réseau LTE**, de la **compatibilité géographique** de l'antenne ou de la **SIM.**
  - **« on va vous le mettre sur le rebord d’une fenêtre pas de soucis »**
  - Résolue en partie si on arrive à sortir sur internet
  - Force potentiellement le client à acheter une SIM locale

Contraintes

Story time

- Contrainte technique #1 : Dépendance au **réseau LTE**, de la **compatibilité géographique** de l'antenne ou de la **SIM.**
  - **« on va vous le mettre sur le rebord d'une fenêtre pas de soucis »**
  - Résolue en partie si on arrive à sortir sur internet
  - Force potentiellement le client à acheter une SIM locale

- Contrainte technique #2 : **Puissance de calcul faible** (limité dans les outils, les librairies)
  - On abandonne tout et on achète un NUC ? Mais comment on fait nos intrusions physiques ?
  - On se soumet aux incertitudes des prérequis réseaux ?

Contraintes

Story time

- Contrainte technique #3 : **Débit LTE** limité (CAT 4/6 **théorique**)
  - Solution : installation locale de certain outils utilisant beaucoup de bande passante

Contraintes

Story time

- Contrainte technique #3 : **Débit LTE** limité (CAT 4/6 **théorique**)
  - Solution : installation locale de certain outils utilisant beaucoup de bande passante

- Contrainte logistique #1 : dépendance avec les ressources sur place
  - Est-ce-qu'il y a du monde sur place ?
  - Est-ce-qu'il y a des compétences IT sur place ?
    - ➜ Latences lors des interventions

Contraintes

Story time

- Contrainte technique #3 : **Débit LTE** limité (CAT 4/6 **théorique**)
  - Solution : installation locale de certain outils utilisant beaucoup de bande passante

- Contrainte logistique #1 : dépendance avec les ressources sur place
  - Est-ce-qu'il y a du monde sur place ?
  - Est-ce-qu'il y a des compétences IT sur place ?
    - ➜ Latences lors des interventions

- Contrainte logistique #2 : **douane postale** plus ou moins clémente sur des outils informatiques rentrant sur le territoire

Remerciements

Cogiceo
Sylvain LECONTE
Louis DELAHAYE

Fin.

Questions ?

(Both french and english questions are welcomed!)

cogiceo.com
+33(0) 1 88 333 700
contact@cogiceo.com
twitter.com/cogiceo
linkedin.com/company/cogiceo