R5.B.09 – CYBERSÉCURITÉ

PARTIE II

Edward Staddon

Edward.Staddon@univ-ubs.fr

Université Bretagne Sud, IUT de Vannes, Département Informatique

PLAN DU COURS

- Introduction à la cybersécurité
- Les risques de la cyber espace
- Les cyberattaques
- Protection préventive
- Protection active et anticipative
- Architectures de sécurité et architectures sécurisés
- Introduction à l'analyse de risque

PLAN DU COURS

- Introduction à la cybersécurité
- Les risques de la cyber espace
- Les cyberattaques
- Protection préventive
- Protection active et anticipative
- Architectures de sécurité et architectures sécurisés

PARTIE II

- Introduction à l'analyse de risque

PROTECTION PRÉVENTIVE

LA PROTECTION

Sécuriser un système d'information contre des attaques

- Plusieurs approches possibles
  - Chacun possède une utilisation spécifique
- Trois grands types de protection
  - **Préventive**
  - **Active**
  - **Anticipative**

PRÉVENIR LES ATTAQUES

Réduire la probabilité et l'impact des attaques

- Pas toujours suffisant
- Utilisé en conjonction avec d'autres méthodes
- Plusieurs méthodologies

- Exemple : Sécurisation d'une porte avec clé
  - Controller les personnes ayant accès
  - Réduire la probabilité que quelqu'un entre

CONTROL D'ACCÈS

Physique

- Gestion de clés d'accès aux locaux / bureaux
  - Permet d'identifier les personnes
- Mise en place d'accès régulés
  - Utilisation de badges
  - Permet d'identifier QUI et QUAND

Numérique

- Mise en place de comptes nominatifs
  - Seul l'utilisateur désigné à accès
  - Sécurisation par mot de passe
    - Renforcement possible avec MFA
- Limiter les accès qu'aux personnes nécessaires
  - N'accéder QUE ce dont on a BESOIN

AUTHENTIFICATION MULTI FACTEUR

Mesure de sécurité nécessitant deux ou plusieurs preuves d'identité

- Utilisation de combinassions d'éléments de l'utilisateur
  - **Connaissances** → code PIN, question secrète, etc…
  - **Possessions** → Carte, token, etc…
  - **Physique** → empruntes, yeux, etc…
- Ajoute une couche de protection puissante
  - Possible de voler un mot de passe
  - Mais ont également besoin d'autres éléments pour avec accès

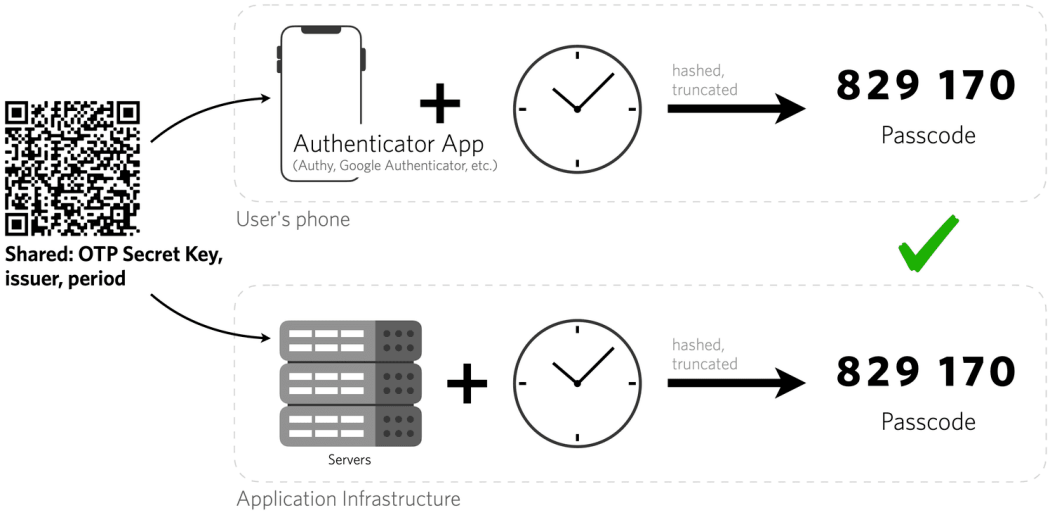
Plusieurs Méthodes

Token physique
Biométriques
Application
Mail
SMS
Etc…

OTP – « ONE-TIME PASSWORD »

Méthode couramment utilisé en MFA

- Création d'un nouveau code à chaque accès
  - Protégé contre les attaques replay
  - Couramment utilisé par mail ou SMS
- Méthode basée sur la synchronisation temporel – TOTP
  - Protection renforcée car seulement valide un temps limité
  - Couramment utilisé dans les Applications d'Authentification
  - Standardisé par l'IETF → RFC 6238



Twilo – What is a Time-based One-time Password (TOTP) - https://www.twilio.com/docs/glossary/totp

CHIFFREMENT

Méthode cryptographique très commun

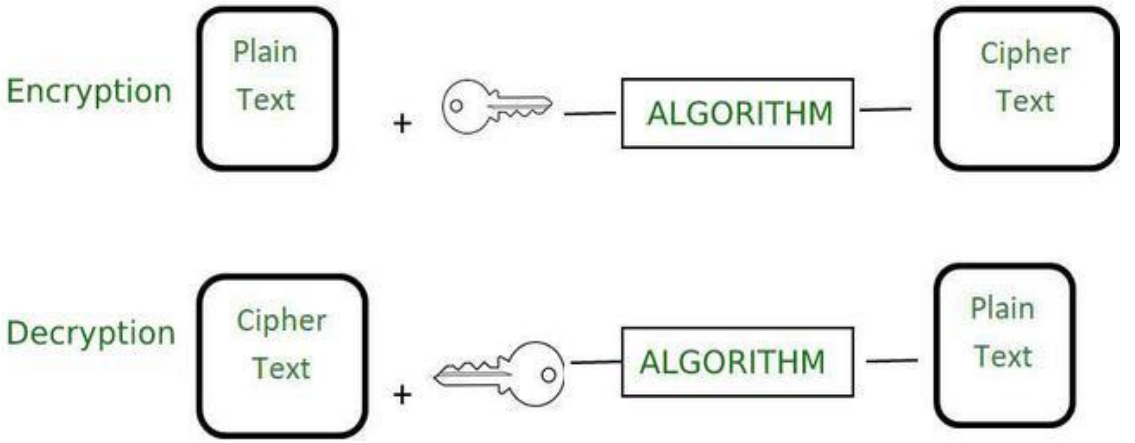
- Protection des données ou des communications
- Utilisé dans plusieurs protocoles
  - HTTPS, SSH, etc…
- Sans la clé, impossible (presque) de craquer
  - Les clés sont longues, en moyenne 2048 octets
- Plusieurs approches possibles
  - **Symétrique**
  - **Asymétrique**

Plusieurs Algorithmes

AES
RSA
Diffie-Hellman
FPE
DES
Etc…

CHIFFREMENT SYMÉTRIQUE

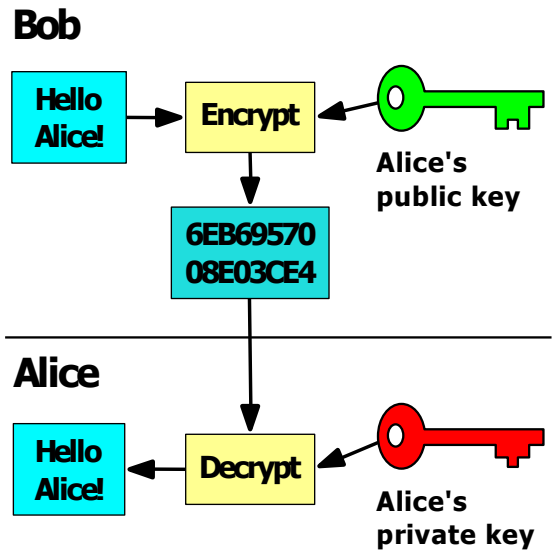
- Utilisation d'une même clé
  - Facilite le partage de clés
  - Permet d'ajouter de nouveaux utilisateurs facilement
- Pas très sécurisé
  - Il suffit de voler la clé partagée
  - Accès à toutes les communications

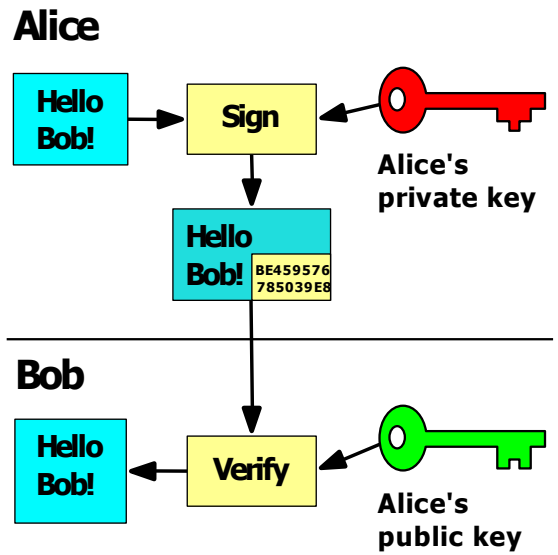


Source: Geeks for Geeks, "*Différence entre le cryotage et le codage*"

CHIFFREMENT ASYMÉTRIQUE

- Utilisation de deux clés
  - Clé **Privée** pour l'utilisateur seulement
  - Clé **Publique** pour les autres participants
- Est utilisé pour envoyer des données
  - Chiffrement clé publique → déchiffrement clé privé
- Peut également servir pour signer des documents ou des mails
  - Signer avec clé privé → validation avec clé publique



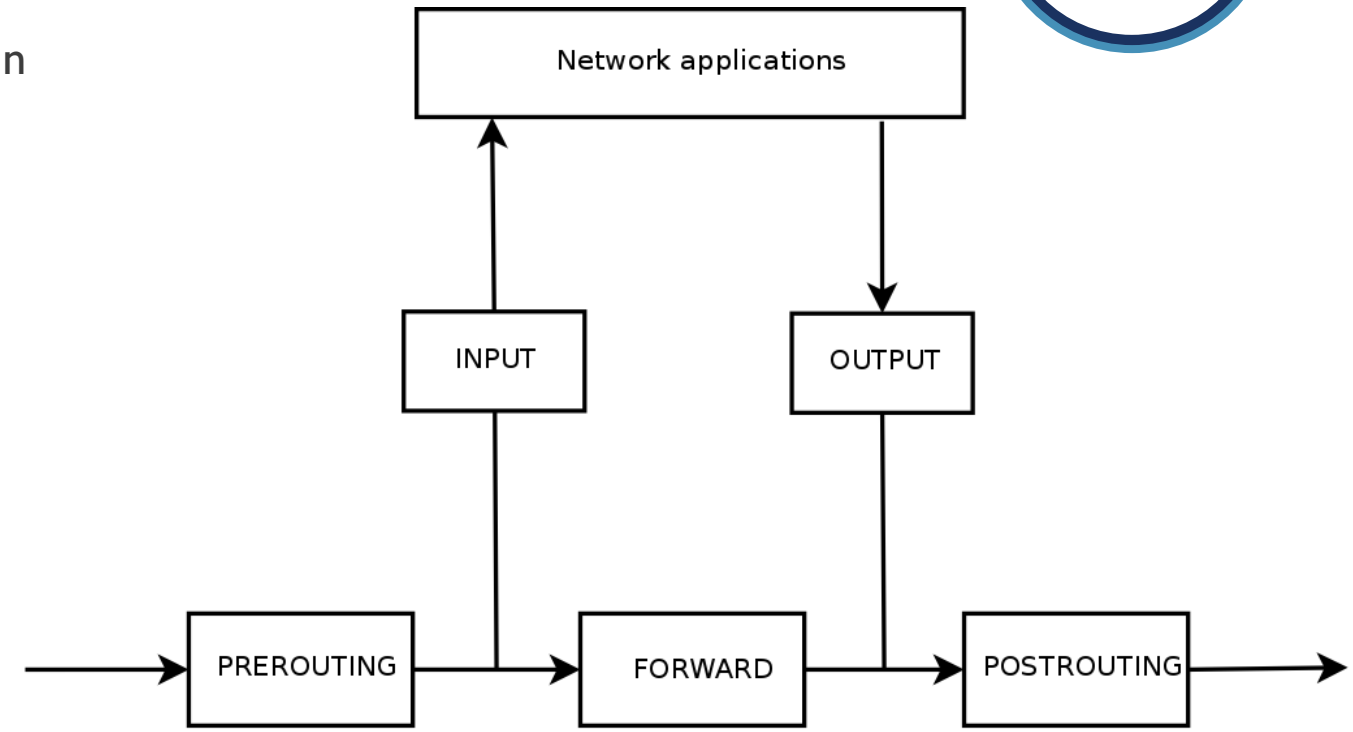


Source: Wikipedia, "*Public-key cryptography*"

PARE-FEU

Système de gestion de Traffic entrant et sortant d'un équipement réseau

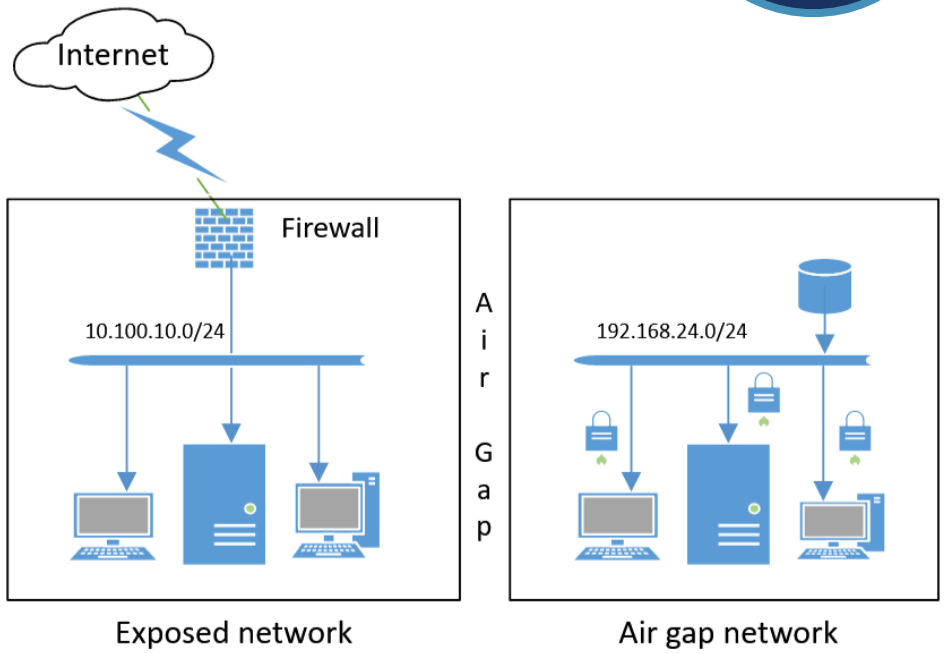
- Constitue une barrière entre un réseau « de confiance » et un réseau « non-confiant »
- Permet d'appliquer une politique d'accès aux ressources
- Permet également le filtrage détaillé des flux
- Plusieurs niveaux de filtrage possible
  - Statique ou dynamique



CLOISONNEMENT

Séparation des différents « niveaux » d'un réseau informatique

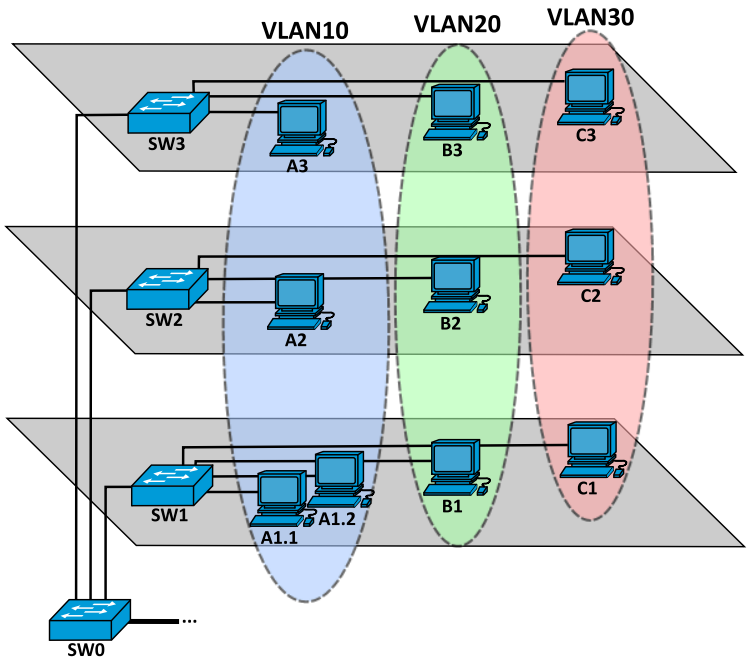
- Certaines utilisations n'ont pas besoin de se mélanger
  - Séparation physique ou logique
- Isolation physique d'un réseau informatique → « Air Gap »
  - Aucun contact entre le réseau interne et le réseau externe
  - Utilisé dans les systèmes de sécurité de haut niveau
- Couramment utilisé dans les entreprises pour la ségrégation des utilsations
  - Utilisation des **VLAN**



SÉGRÉGATION VLAN

Réseau local virtuel → *Virtual LAN*

- Permet la coexistence de deux réseaux sur le même équipement
- L'objectif des VLAN
  - Séparation des flux
  - Segmentation réseau (réduction du domaine de collision)
  - Amélioration de la sécurité
    - Passage par un routeur / passerelle obligatoire pour communiquer entre deux VLAN

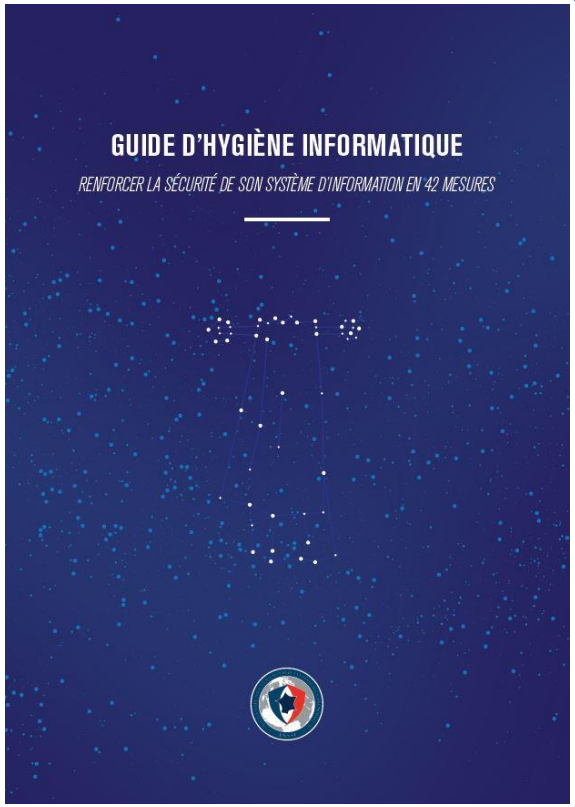


HYGIÈNE ET SÉCURITÉ

Sensibilisation et formation des utilisateurs informatique

- Mise en place dans toutes les entreprises (normalement)
  - Généralement nouveaux arrivants
  - Parfois inclus dans la « charte informatique »
- Pas toujours pris au sérieux par les utilisateurs

- Guide disponible par l'ANSSI
  - Présente 42 mesures pour « renforcer la sécurité de son système d'information »



PRÉVENTION ACTIVE ET ANTICIPATIVE

LA PROTECTION … COMPLÉMENTAIRE

Protection Préventive très important pour la sécurité des systèmes d'information

- N'est pas infaillible

- Apport complémentaire à la protection
  - Permet d'apporter une sécurité en plus
  - Couramment utilisé pour protéger contre des attaques
- Apport de protection
  - **Active**
  - **Anticipative**

PROTECTION ACTIVE

Analyser et agir sur les systèmes et réseaux

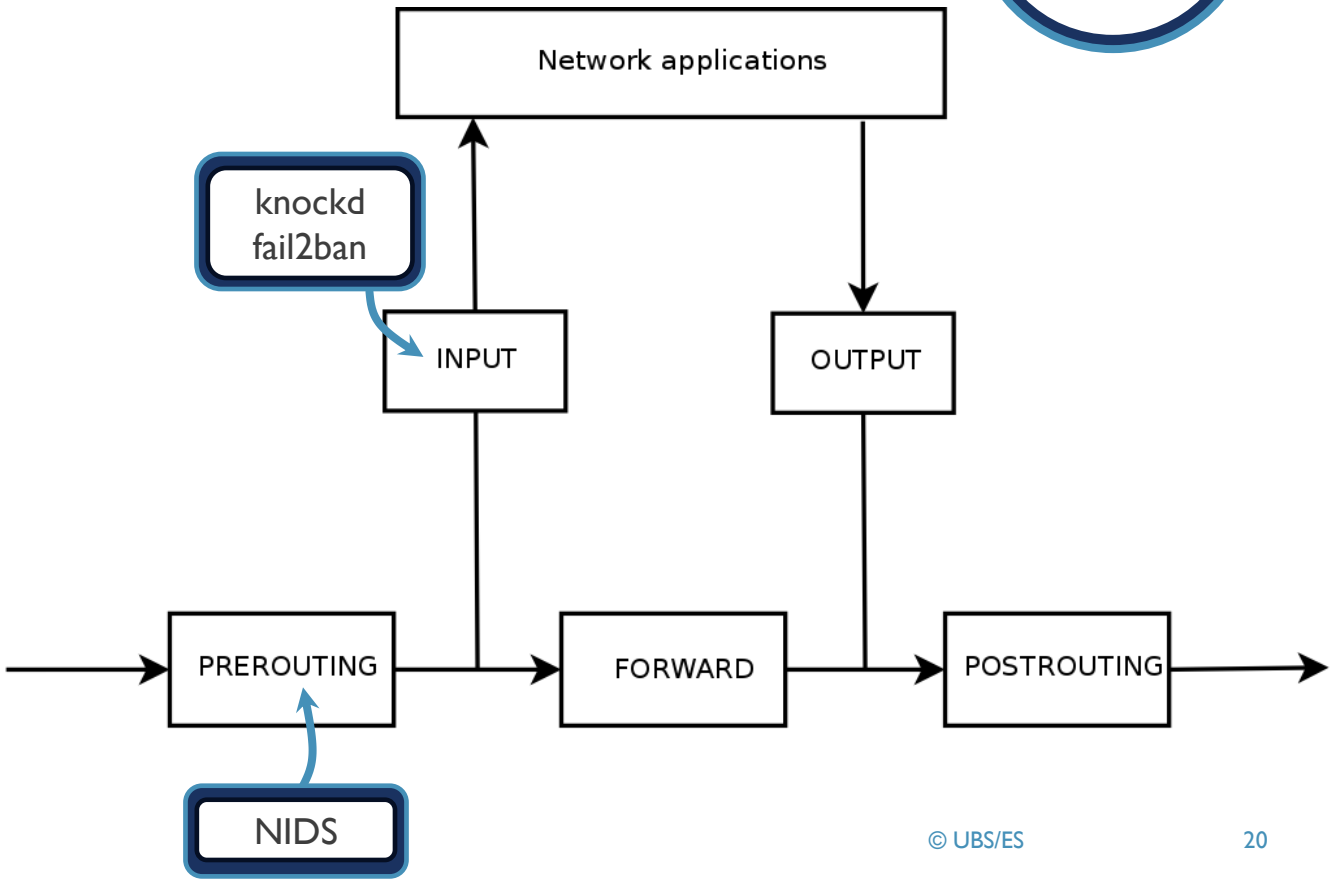
- Apport une protection supplémentaire en cas d'attaque
- Permet de détecter et d'agir pour renforcer la sécurité
- Plusieurs méthodologies

- Exemple : Surveillance d'une porte d'entrée avec une camera
  - Identifier les accès
  - Détecter des tentatives d'effraction

PARE-FEU DYNAMIQUE

Fonctionnement « étoffé » d'un pare-feu statique

- Deux grandes méthodologies
  - Dynamique adapté au cloud
    - Basés sur un jeu de données et logs locales
  - Règles d'adaptation pour fonctionnement local
    - Adapter accès selon conditions
- Capacité à s'adapter et évoluer
- Peuvent suivre les évolutions des systèmes



PARE-FEU DYNAMIQUE TERMINOLOGIE

Firewall-as-a-Service
FWaaS

Pare-feu intégré au cloud
Élimination du besoin de pare-feu sur place

Zero Trust Network Access
ZTNA

Besoin de vérification pour tout accès sur un réseau privé
Fonctionne qu'importe la localisation de la personne (interne/externe)

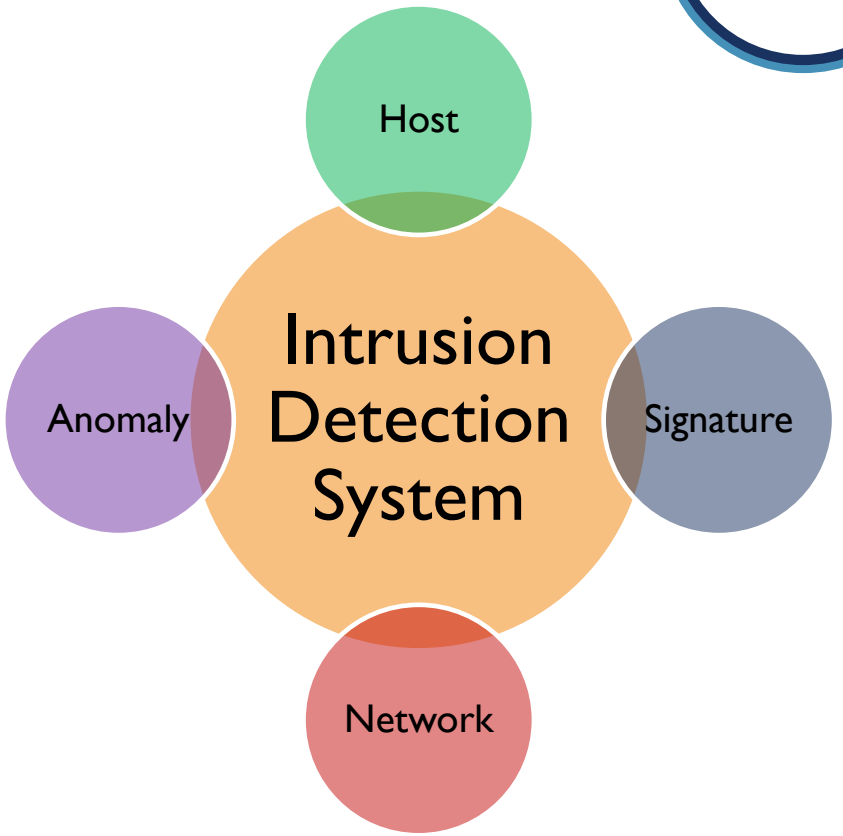
Secure Access Service Edge
SASE

Framework combinant plusieurs aspects de sécurité
Fonctionnement basé cloud
Intégration des pare-feu dynamiques pour renforcer la sécurité réseau avec d'autres outils (CASB, SWG, ZTNA, etc…)

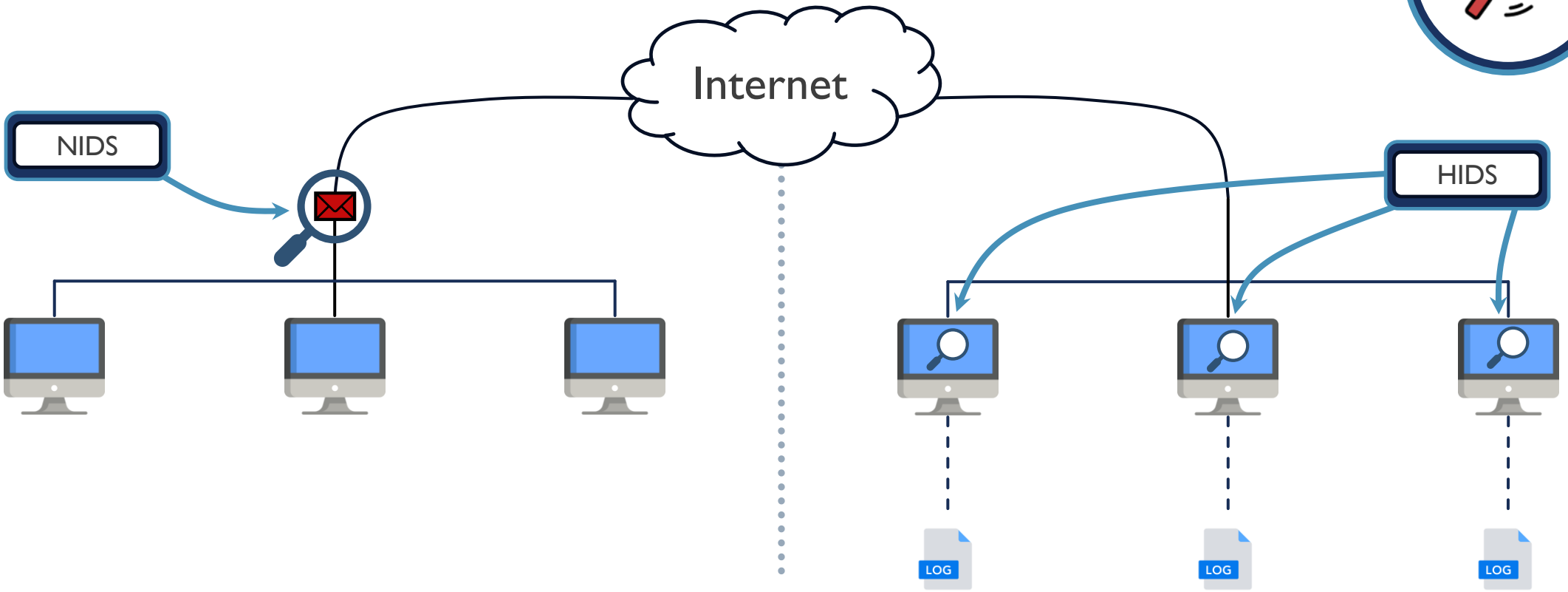
SYSTÈME DE DÉTECTION D'INTRUSION

Mécanisme destiné à identifier des activités suspectes ou anormales

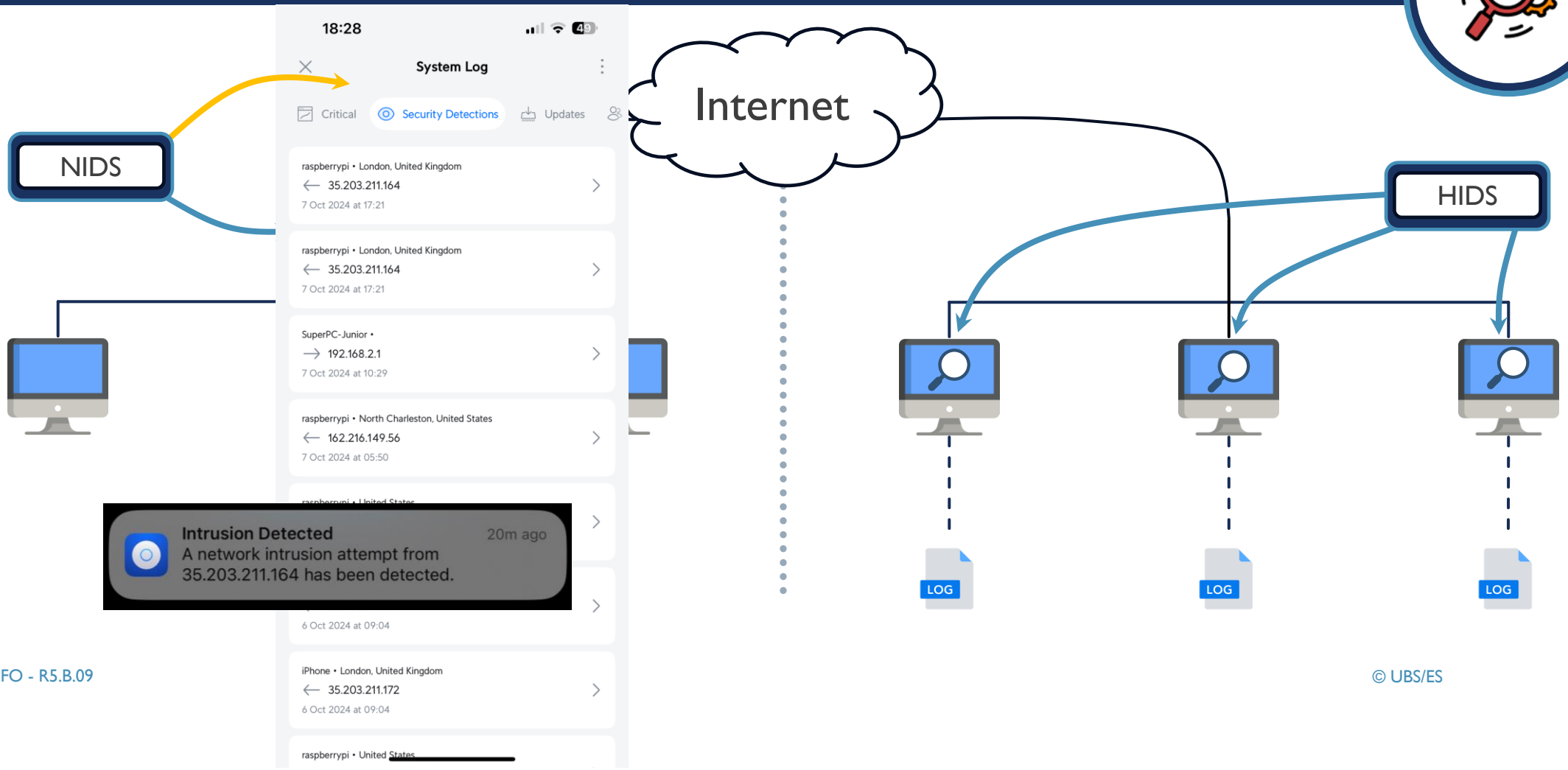
- Deux familles d'IDS
  - **Réseau** – NIDS (Snort, Suricata, Bro, …)
  - Machine **Hôte** – HIDS (OSSEC, Fail2ban, CrowdSec, …)
  - D'autres voient le jour (Collaboratifs – CIDS, Sans-fil – WIDS, Hybrides – APHIDS/HAMA-IDS)
- Deux catégories d'IDS
  - **Signatures** – SIDS
  - **Anomalies** -- AIDS



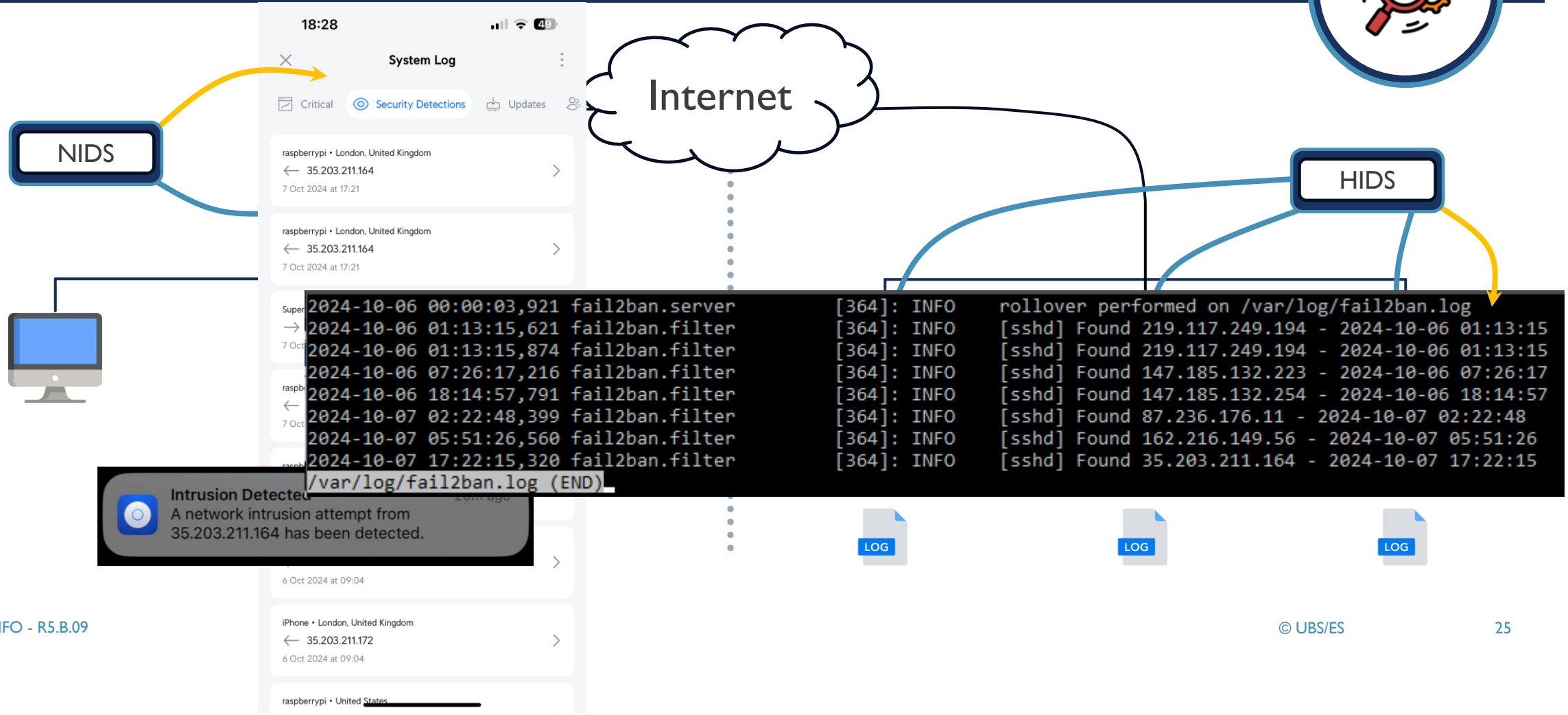
NIDS VS HIDS



NIDS VS HIDS



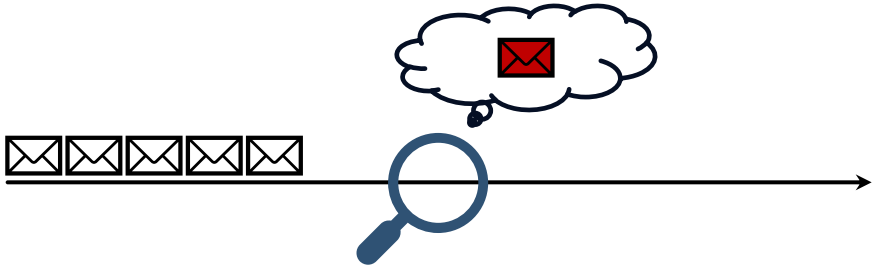
NIDS VS HIDS



SIDS VS AIDS

Signature

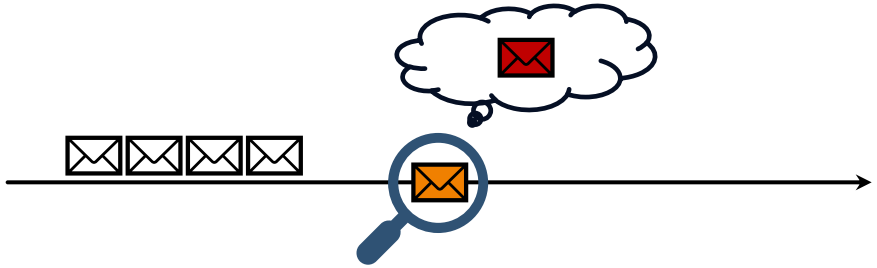
- Comparaison avec un pattern connue



SIDS VS AIDS

Signature

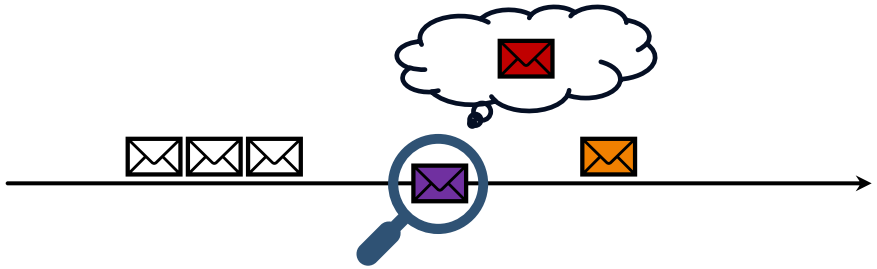
- Comparaison avec un pattern connue



SIDS VS AIDS

Signature

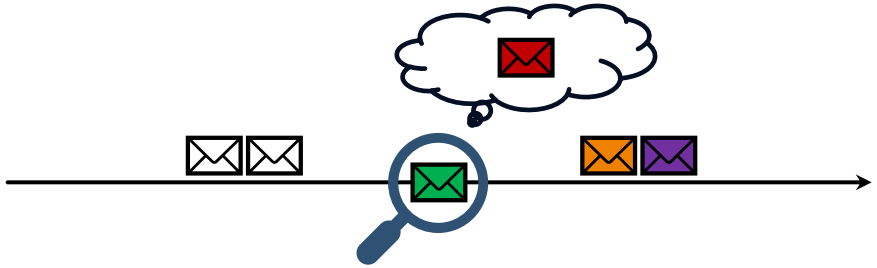
- Comparaison avec un pattern connue



SIDS VS AIDS

Signature

- Comparaison avec un pattern connue



SIDS VS AIDS

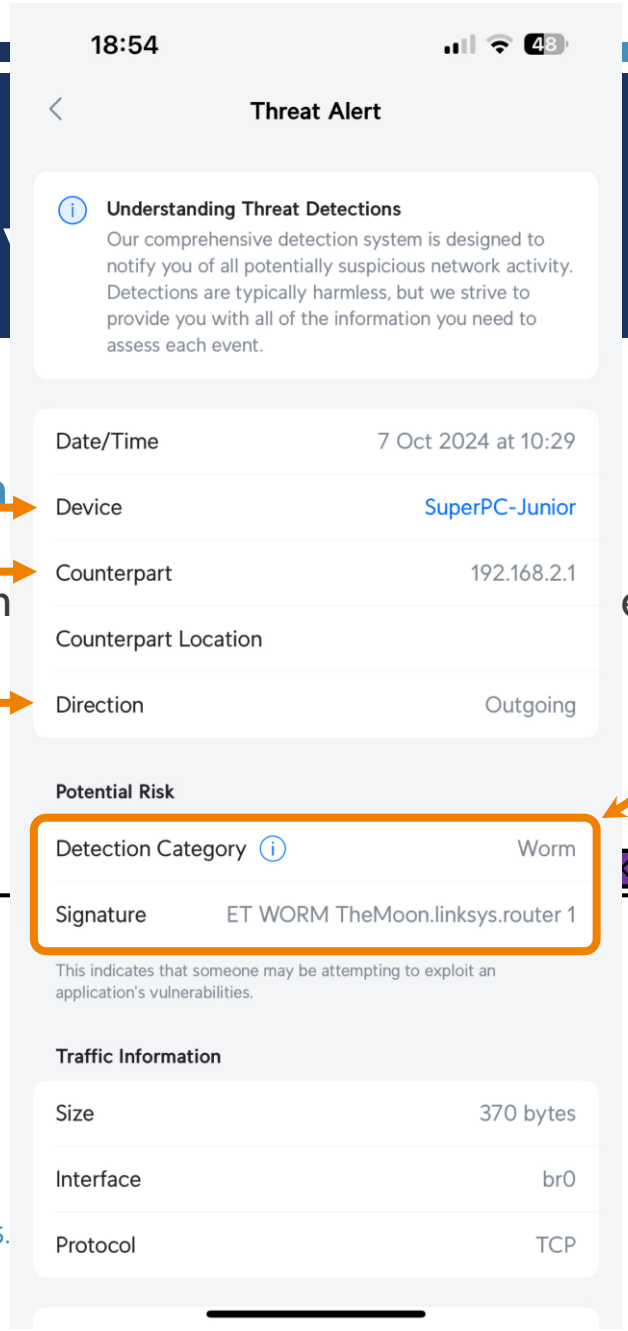
Signature

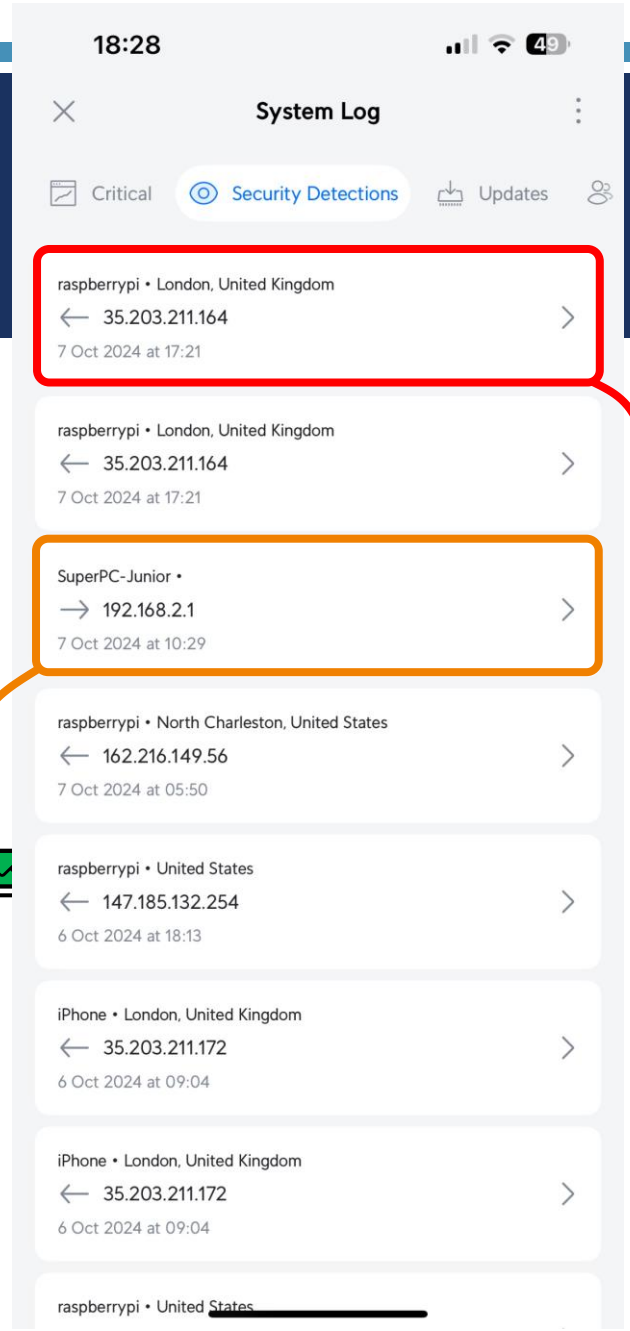
- Comparaison avec un pattern connue

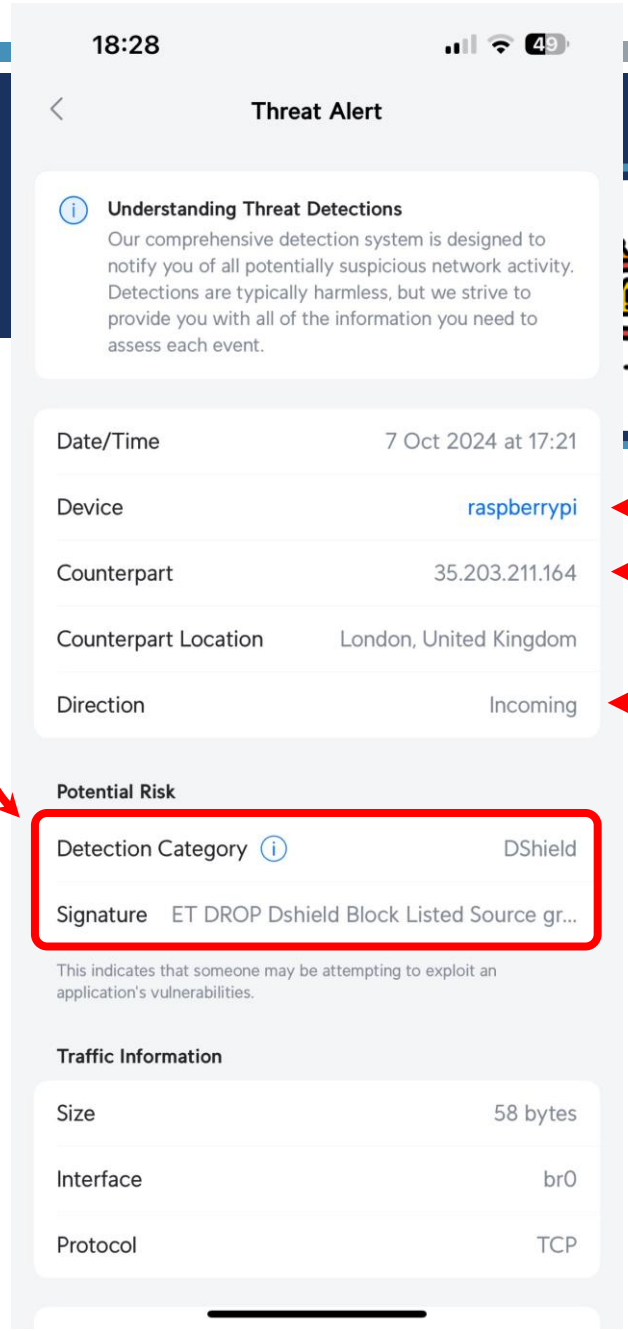
SIDS

Sign

- Com e







SIDS VS AIDS

Signature

- Comparaison avec un pattern connue

Anomalie

- Déviation de la « norme »

SIDS VS AIDS

Signature

- Comparaison avec un pattern connue

Anomalie

- Déviation de la « norme »

SIDS VS AIDS

Signature

- Comparaison avec un pattern connue

Anomalie

- Déviation de la « norme »

SIDS VS AIDS

Signature

- Comparaison avec un pattern connue

Anomalie

- Déviation de la « norme »

SIDS VS AIDS

Signature

- Comparaison avec un pattern connue

Anomalie

- Déviation de la « norme »

SI

/var/log/auth.log

```
Oct  7 02:09:01 raspberrypi CRON[12819]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct  7 02:09:01 raspberrypi CRON[12819]: pam_unix(cron:session): session closed for user root
Oct  7 02:17:01 raspberrypi CRON[12900]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct  7 02:17:02 raspberrypi CRON[12900]: pam_unix(cron:session): session closed for user root
Oct  7 02:22:47 raspberrypi sshd[12935]: error: kex_exchange_identification: Connection closed by remote host
Oct  7 02:22:47 raspberrypi sshd[12935]: Connection closed by 87.236.176.11 port 43939
Oct  7 02:22:48 raspberrypi sshd[12936]: Connection closed by 87.236.176.11 port 58113 [preauth]
Oct  7 02:39:01 raspberrypi CRON[13023]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct  7 02:39:01 raspberrypi CRON[13023]: pam_unix(cron:session): session closed for user root
Oct  7 03:06:01 raspberrypi CRON[13193]: pam_unix(cron:session): session opened for user staddon(uid=1002) by (uid=0)
Oct  7 03:06:01 raspberrypi CRON[13193]: pam_unix(cron:session): session closed for user staddon
...
Oct  7 05:17:01 raspberrypi CRON[14103]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct  7 05:17:01 raspberrypi CRON[14103]: pam_unix(cron:session): session closed for user root
Oct  7 05:39:01 raspberrypi CRON[14218]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct  7 05:39:01 raspberrypi CRON[14218]: pam_unix(cron:session): session closed for user root
Oct  7 05:51:26 raspberrypi sshd[14320]: Connection reset by 162.216.149.56 port 59646 [preauth]
Oct  7 06:06:01 raspberrypi CRON[14398]: pam_unix(cron:session): session opened for user staddon(uid=1002) by (uid=0)
Oct  7 06:06:01 raspberrypi CRON[14398]: pam_unix(cron:session): session closed for user staddon
Oct  7 06:07:01 raspberrypi CRON[14408]: pam_unix(cron:session): session opened for user staddon(uid=1002) by (uid=0)
Oct  7 06:07:01 raspberrypi CRON[14408]: pam_unix(cron:session): session closed for user staddon
```

/var/log/fail2ban.log

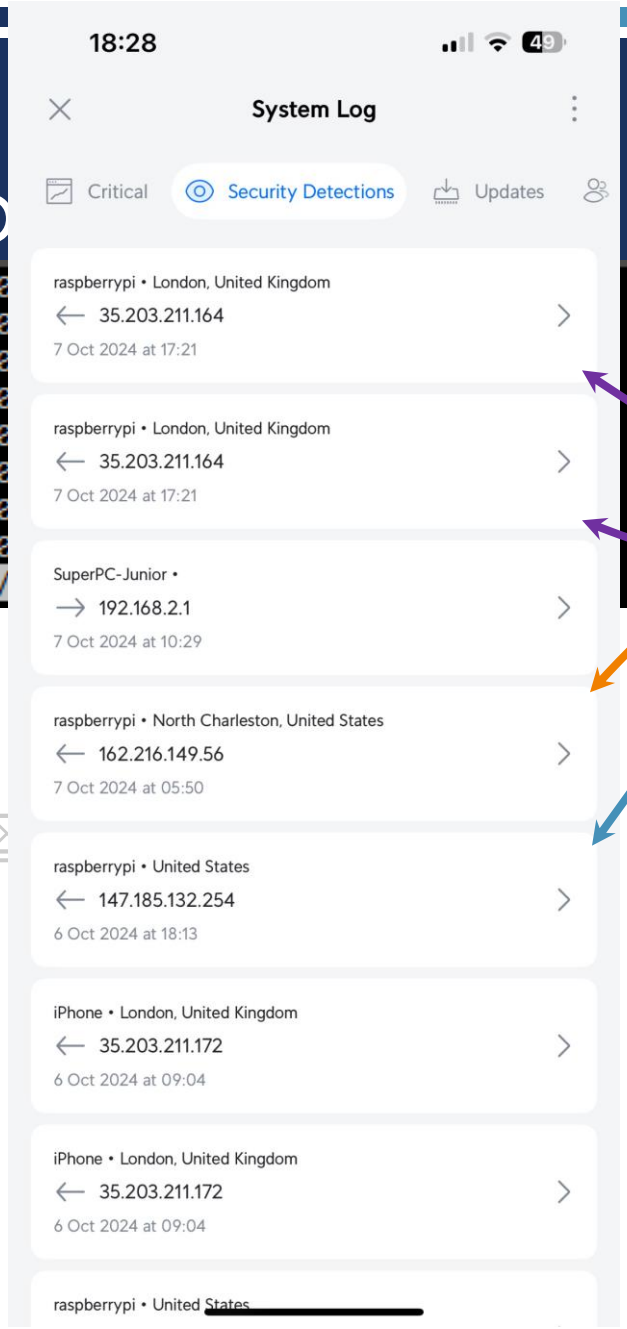
```
2024-10-06 00:00:03,921 fail2ban.server        [364]: INFO    rollover performed on /var/log/fail2ban.log
2024-10-06 01:13:15,621 fail2ban.filter        [364]: INFO    [sshd] Found 219.117.249.194 - 2024-10-06 01:13:15
2024-10-06 01:13:15,874 fail2ban.filter        [364]: INFO    [sshd] Found 219.117.249.194 - 2024-10-06 01:13:15
2024-10-06 07:26:17,216 fail2ban.filter        [364]: INFO    [sshd] Found 147.185.132.223 - 2024-10-06 07:26:17
2024-10-06 18:14:57,791 fail2ban.filter        [364]: INFO    [sshd] Found 147.185.132.254 - 2024-10-06 18:14:57
2024-10-07 02:22:48,399 fail2ban.filter        [364]: INFO    [sshd] Found 87.236.176.11 - 2024-10-07 02:22:48
2024-10-07 05:51:26,560 fail2ban.filter        [364]: INFO    [sshd] Found 162.216.149.56 - 2024-10-07 05:51:26
2024-10-07 17:22:15,320 fail2ban.filter        [364]: INFO    [sshd] Found 35.203.211.164 - 2024-10-07 17:22:15
/var/log/fail2ban.log (END)
```

SIDS VS AID

Signat

- Compa

```
2024-10-0
2024-10-0
2024-10-0
2024-10-0
2024-10-0
2024-10-0
2024-10-0
2024-10-0
/var/log/
```



/var/log/auth.loh

```
[364]: INFO    rollover performed on /var/log/fail2ban.log
[364]: INFO    [sshd] Found 219.117.249.194 - 2024-10-06 01:13:15
[364]: INFO    [sshd] Found 219.117.249.194 - 2024-10-06 01:13:15
[364]: INFO    [sshd] Found 147.185.132.223 - 2024-10-06 07:26:17
[364]: INFO    [sshd] Found 147.185.132.254 - 2024-10-06 18:14:57
[364]: INFO    [sshd] Found 87.236.176.11 - 2024-10-07 02:22:48
[364]: INFO    [sshd] Found 162.216.149.56 - 2024-10-07 05:51:26
[364]: INFO    [sshd] Found 35.203.211.164 - 2024-10-07 17:22:15
```

SIDS VS AIDS

Signature

- Comparaison avec un pattern connue

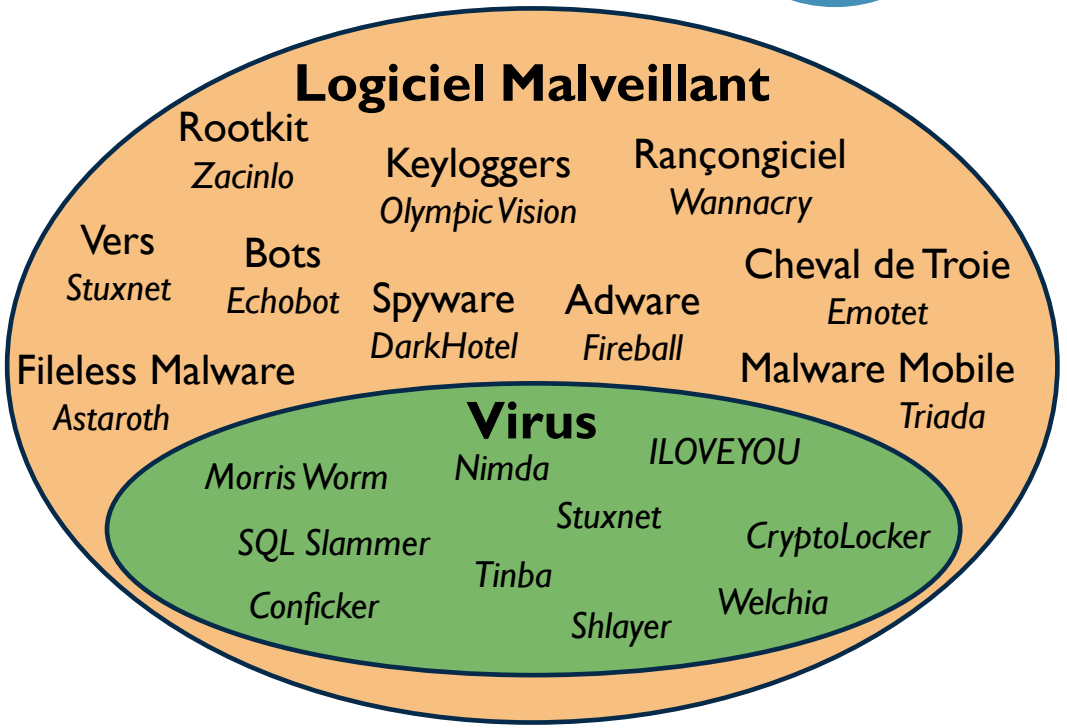
Anomalie

- Déviation de la norme

ANTI-VIRUS ET ANTI-MALWARE

Logiciel pour protéger un système informatique contre les menaces

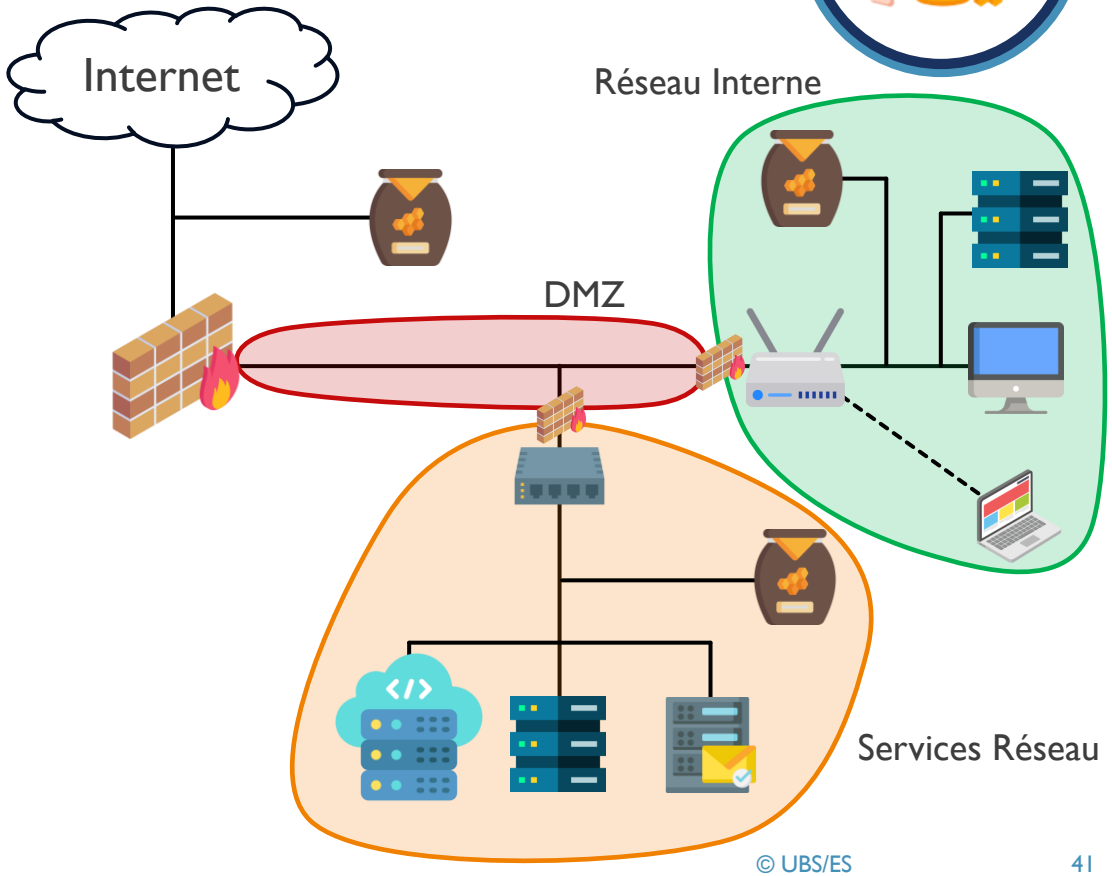
- Terminologie souvent mélangée
  - **Anti-Virus** → Prévenir, Détecter et Retirer des virus informatiques
  - **Anti-Malware** → Terme générique, protection contre des logiciels malveillants
- Cyberattaquants s'éloignent des virus
  - Préfèrent les malwares
- Terme « Anti-Virus » toujours utilisé principalement
  - Question de marketing
  - beaucoup d'investissement dans les années 1990 → naissance du terme



HONEYPOT

Mécanisme pour attirer des personnes malveillantes pour les identifier, voire neutraliser

- Mise en place de ressources cibles (physiques ou virtuels)
  - Serveurs, Programmes, Services, …
- Faire croire à l'attaquant qu'il peut prendre control de la cible
  - Permet l'observation et l'analyse de l'admin
- Utilisation de trois problématiques
  - **Surveillance** → Observation du trafic, analyse préattaque, journalisation des événements
  - **Collecte d'Information** → Utilisation de sniffing, analyseurs de trames
  - **Analyse d'Information** → Analyse des traces, identifier les vulnerabilités, comprendre les motivations de l'attaquant



TYPES D'HONEYPOT

Faible Interaction

Interaction système partiel
Emulation limité de services
Aucun interaction OS

Facile à détecter
Généralement utilisé pour détection en amont (Prod)

Moyenne Interaction

Interaction système amélioré
Emulation d'une couche applicative
Pas d'OS propre

Utilisé pour retarder les attaquants
Permet un temps de réponse plus grande

Forte Interaction

Interaction système quasi-complète
Utilisation de vraies services et OS

Complexe à déployer
Permet un retour détaillé d'une attaque
Susceptible aux infections

Honeypot Pure

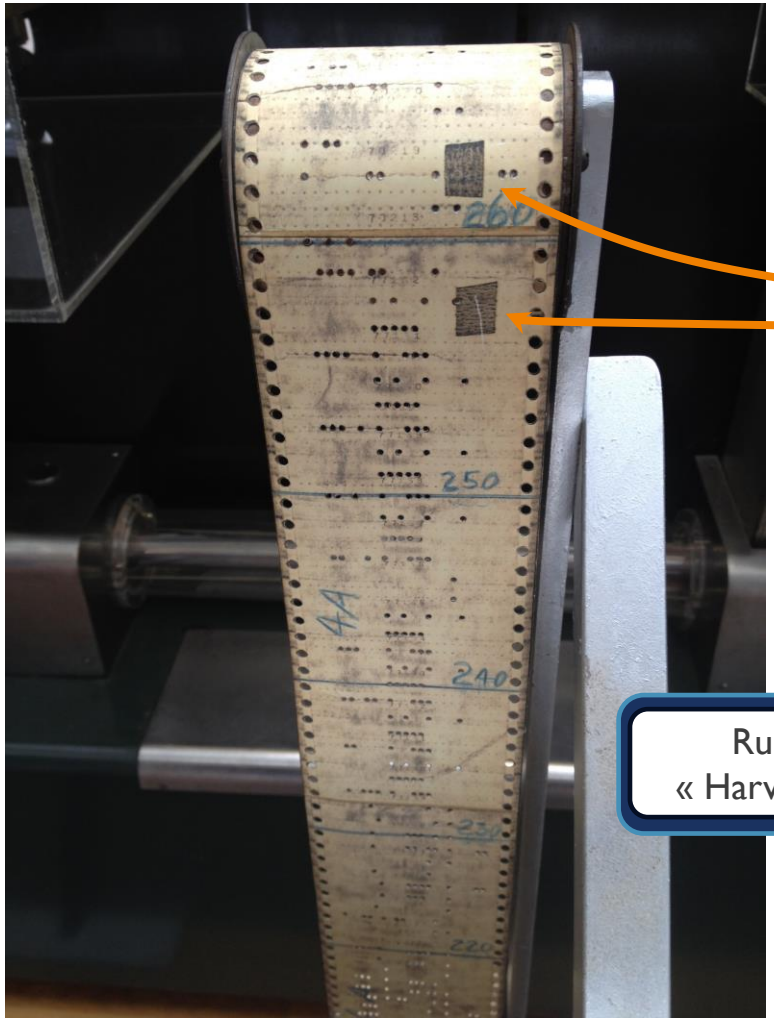
Système dédié

Difficile à détecter
Très efficace

PATCH DE SÉCURITÉ

Apport d'une correction de code sur un logiciel ou OS

- Généralement utilisé pour corriger une erreur
  - Bug, vulnérabilité, traduction, crack, …
- Très important dans le domaine de la sécurité
  - Utilisé pour renforcer une faille dans un système / réseau
  - Devrait être fait **DES QUE POSSIBLE**
- Origines autour des rubans perforés
  - Découpe des parties erronés
  - Collage de « patches correctifs » pour réparer



PROTECTION ANTICIPATIVE

Mettre en place des systèmes en cas d'attaque

- Préparer toujours au pire
- Peut apporter une sécurité en plus
  - Généralement très utile lors d'une attaque
- Plusieurs méthodologies

- Exemple :Vigil de sécurité à l'intérieur de la porte pour attraper les cambrioleurs
  - Protéger les accès
  - Combattre les attaquants

FORMATION CONTINUE

Continuation des sensibilisations « hygiène et sécurité »

- Rappels bonnes pratiques et consignes
  - Souvent oubliés avec le temps
- Très important pour les responsables informatiques
  - Aussi pour tous les utilisateurs
- Souvent oublié car manque d'implication
  - Mais manque de formation régulièrement la cause d'erreurs humaines
  - Fortement utile avec les relations clients (ingénierie sociale, etc…)

> *« Il est par ailleurs nécessaire de faire mention de clauses spécifiques dans les contrats de prestation pour garantir une formation régulière à la sécurité des systèmes d'information du personnel externe et notamment les infogérants. »*
>
> - Guide hygiene et sécurité -- ANSSI

SAUVEGARDE

Création d'une copie des données importants

- Permet de réduire l'impact d'une attaque
  - Ne permet pas de tout récupérer
  - Remise en état à la date de la dernière sauvegarde
- Ne pas se limiter aux sauvegardes sur site
  - Facile et rapide à mettre en œuvre
  - Dans le même domaine d'attaque → vulnérable
    - Incendie OVH → Backup dans le même datacenter …

Nécessaire pour la *continuité des services*

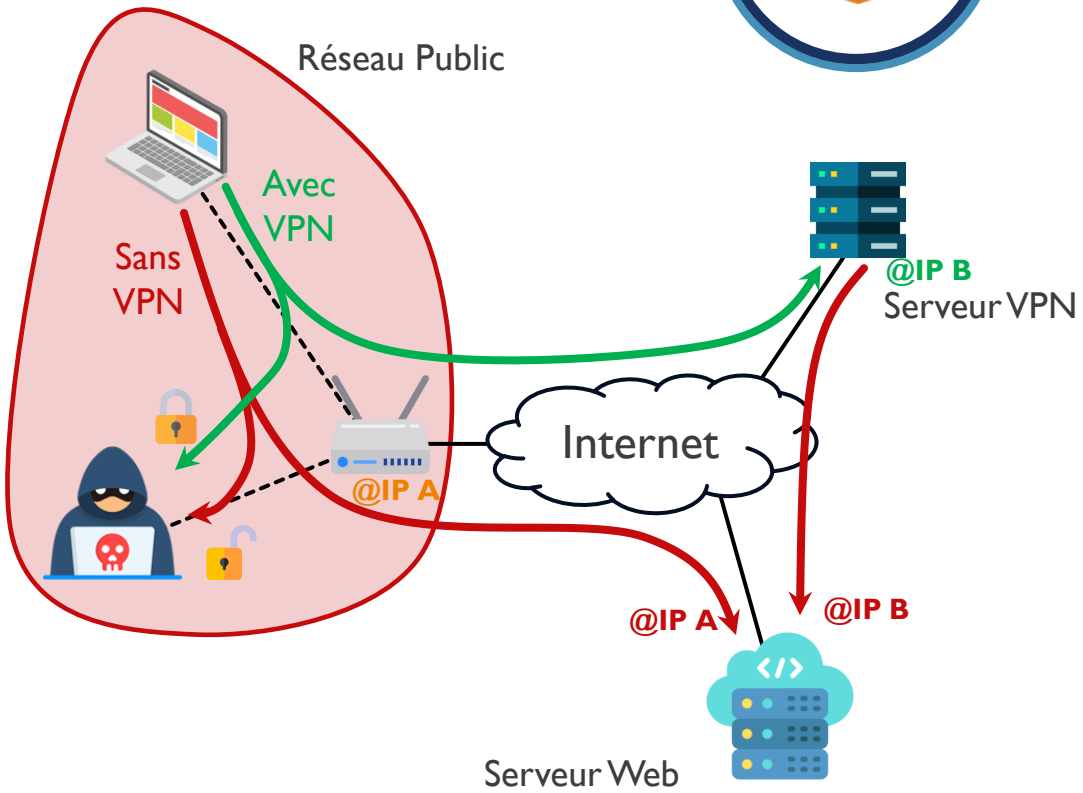
→ Combattre les erreurs système
→ Combattre les attaques

→ Permet de reprendre l'activité après un incident → **R6.B.07**

VPN

Connexion sécurisée avec un réseau privée distant

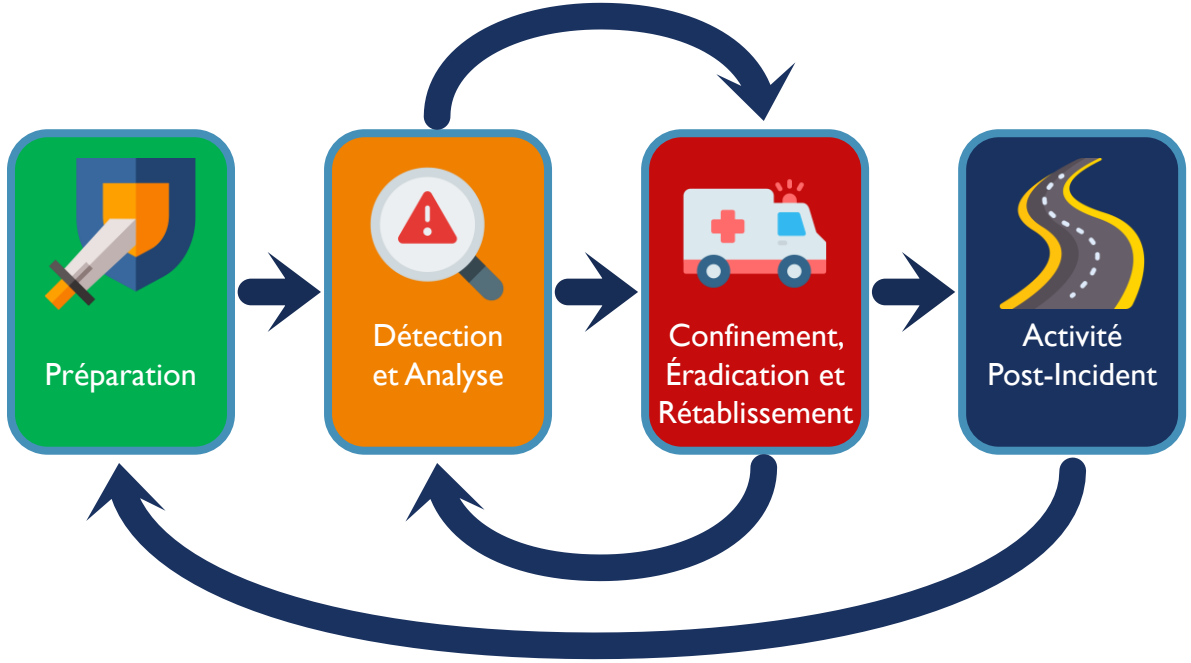
- Utilisation principale pour se connecter sur un réseau privé
  - Faire le pont entre plusieurs sites (UBS Vannes – IUT Vannes – UBS Lorient)
  - Utilisé pour se connecter à un réseau d'entreprise
- Sécurisation des communications
  - Utilisation de méthodes cryptographiques pour chiffrer les exchanges
  - Très utilisé sur les réseaux Wi-Fi publics
- Tendance marketing pour contourner le geolocking (ex: streaming)
  - Ne cache pas toutes les communications !!



GESTION D'INCIDENT

Processus de gestion du cycle de vie de tous les incidents

- Permet de définir les gestes à effectuer en cas d'incident informatique
  - Rétablir rapidement les systèmes / services
  - Réduire au maximum l'impact sur l'entreprise
- Assurer un meilleur niveau de qualité de service et disponibilité
- Processus normalisé – ISO 20000 / ITIL



ARCHITECTURES DE SÉCURITÉ ET ARCHITECTURES SÉCURISÉS

SÉCURITÉ VS SÉCURISÉ

Nuance des deux terminologies

Architecture de Sécurité

- Conception stratégique pour protéger les systèmes d'information et les actifs
  - Systèmes / Politiques / Technologies
- Aligne la cybersécurité avec les objectifs commerciaux et le profil de gestion des risques
- Dicté et géré par des normes internationales

Architecture Sécurisé

- Architectures Informatiques renforçant la sécurité
  - Ségrégation
  - Détection / Mitigation
  - Authentification
- Systèmes déployés pour renforcer la protection

AVANTAGES DES ARCHITECTURES DE SÉCURITÉ

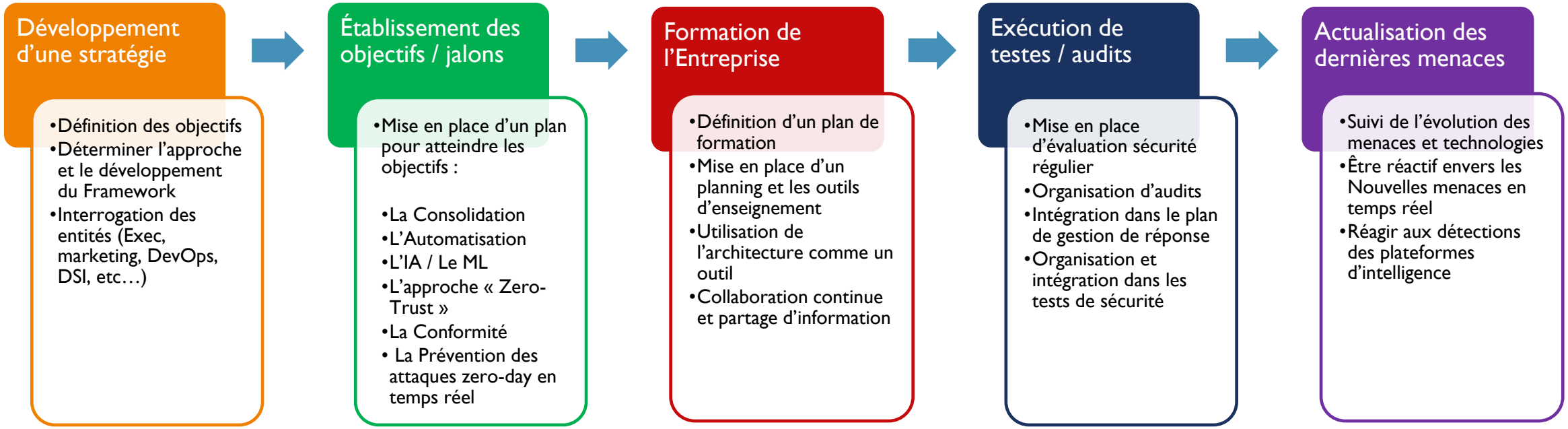
1. Réduire les failles de sécurité
   - Ne pas attendre une intrusion pour réagir
   - Permet de réduire le volume / sévérité des attaques
     - Peut même les empêcher
   - Objectivement créer un environnement « sans-risque »

2. Accélérer les temps de réponse
   - Majorité des intrusions résultent d'erreurs dans les processus de sécurité
   - Fermer lacunes et fournir des protocoles de réponse
     - Réaction rapide avant qu'ils progressent
     - Utilisation de l'automatisation

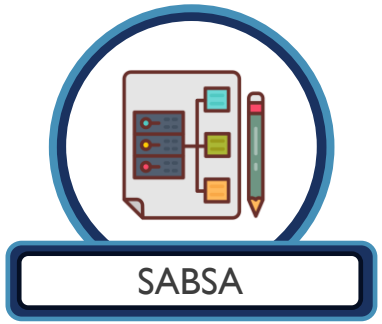
3. Améliorer l'efficacité opérationnelle
   - Utilisation de beaucoup d'outils (≈31,5 par entreprise)
   - Forte complexité des infrastructures
     - Réduction de la variété des produits / fabricants
   - Utilisation d'outils intégrés

4. Conformer aux réglementations de l'industrie
   - Obligation de suivi des réglementations de région / industrie
     - Santé US → HIPPA / EU → RGPD
   - Intégration de la sécurité dans chaque entité d'une organisation
     - Prévention / Maintien de conformité

MEILLEURES PRATIQUES DES ARCHITECTURES DE SÉCURITÉ



ARCHITECTURES DE SÉCURITÉ



COMPUTER EMERGENCY RESPONSE TEAM

Centre d'alerte et de réaction aux attaques informatiques

- Destiné aux entreprises / administrations
  - Accessibles à tous
- Europe → *Computer Security Incident Response Team* – **CSIRT**
- Plusieurs taches importantes
  - Centralisation des demandes d'assistance post-incident
  - Traitement des alertes et réactions aux attaques
  - Établissement et maintenance d'une BDD de vulnérabilités
  - Prévention par diffusion d'informations
  - Coordination éventuelle avec autres entités hors domaine action

Europe → CERT-EU

France → CERT-FR
→ CERT Santé
→ CERT-PJ
→ CERT-RENATER
→ CSIRT-BFC
→ …

COMPUTER EMERGENCY RESPONSE TEAM

27 septembre 2024	CERTFR-2024-ALE-012	[MàJ] Vulnérabilités affectant OpenPrinting CUPS	Alerte en cours
10 septembre 2024	CERTFR-2024-ALE-011	Vulnérabilité dans SonicWall	Alerte en cours
01 juillet 2024	CERTFR-2024-ALE-009	Vulnérabilité dans OpenSSH	Clôturée le 07/10/24
09 août 2024	CERTFR-2024-ALE-010	Multiples vulnérabilités dans Roundcube	Clôturée le 07/10/24
12 avril 2024	CERTFR-2024-ALE-006	[MàJ] Vulnérabilité dans Palo Alto Networks GlobalProtect	Clôturée le 01/07/24

CENTRE DES OPÉRATIONS DE SÉCURITÉ

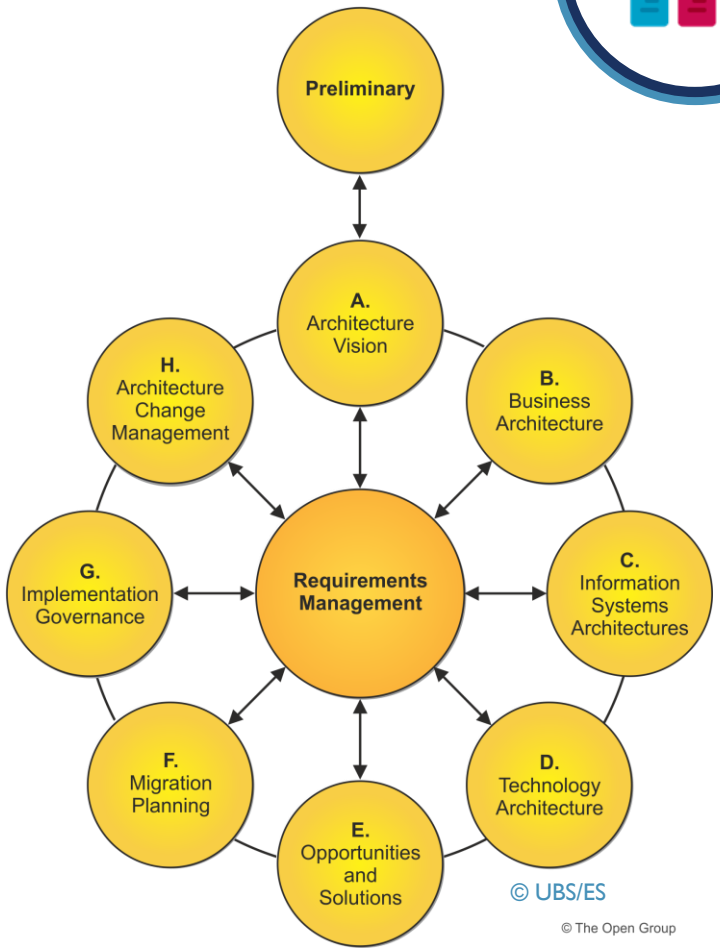
Division responsable de la sécurité informatique au sein d'une entreprise

- Un SoC
  - Supervise le site
  - Traite les données spécifiques
    - Gestion d'accès (badge, portes, barrières de parking, etc…)
    - Control des lumières / alarmes
- Pas très développé en France
  - Besoin de la mise en place d'une SoC pour les OIV
- Lié aux personnes / processus / technologies utilisés
- Assurer la connaissance de la situation des menaces
  - Détection
  - Confinement
  - Assainissement
- Gere également les incidents pour l'entreprise
- Surveillance des applications

THE OPEN GROUP ARCHITECTURE FRAMEWORK

Framework standardisé pour les architectures de sécurité

- Le standard TOGAF est utilisé par plusieurs entités (entreprises commerciales → gouvernement)
- Aide à déterminer quels problèmes ont besoin d'être traités
- Focus principal
  - Objectifs et portée de l'entreprise
  - Phases préliminaires de la définition de l'architecture
- Ne donne pas de guidage spécifique pour les problèmes de sécurité



SHERWOOD APPLIED BUSINESS SECURITY ARCHITECTURE

Framework axé autour des politiques de l'entreprise

- Aide a définir les questions critiques d'une architecture de sécurité
  - Quoi / Pourquoi / Quand / Qui ?
- Permet non seulement la planification des services
  - Concerne la livraison et l'intégration dans la gestion informatique
- Décrit comme une « méthode d'architecture de sécurité »
  - Ne contient pas d'information technique d'implémentation

Vue d'Entreprise	Architecture Contextuelle
Vue d'Architecte	Architecture Conceptuelle
Vue de Conception	Architecture Logique
Vue Constructeur	Architecture Physique
Vue de Commerçant	Architecture des Composants
Vue de Directeur	Architecture de Gestion

OPEN SECURITY ARCHITECTURE

Framework lié aux contrôles de sécurité techniques et fonctionnelles

- Idée générale → la sécurité est une partie intégrale de l'entreprise
  - Prise en compte au début → pas un ajout secondaire
- Conçu pour comprendre les menaces
- Permet la concevoir des systèmes de sécurité adaptés aux besoins
- Framework flexible et adaptable
  - Souvent utilisé en conjonction avec d'autres Frameworks → SABSA
- Quatre composants principaux
  - **Objectives** du système de sécurité
  - **Besoins** spécifiques pour le système
  - **Architecture** du système (Technologies / processus d'implémentation)
  - **Évaluation** de l'efficacité et modifications nécessaires

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Framework de sécurité commun pour les entreprises

- Permet de
  - Décrire l'infrastructure actuelle
  - Décrire l'état de sécurité ciblé
  - Identifier et prioriser les opportunités d'amélioration
  - Évaluer le progrès vers l'état ciblé
  - Communication sur les risques de sécurité entre les parties prenantes internes et externes
- Le « core » décrit cinq activités applicables aux secteurs des infrastructures critiques

ARCHITECTURES SÉCURISÉS

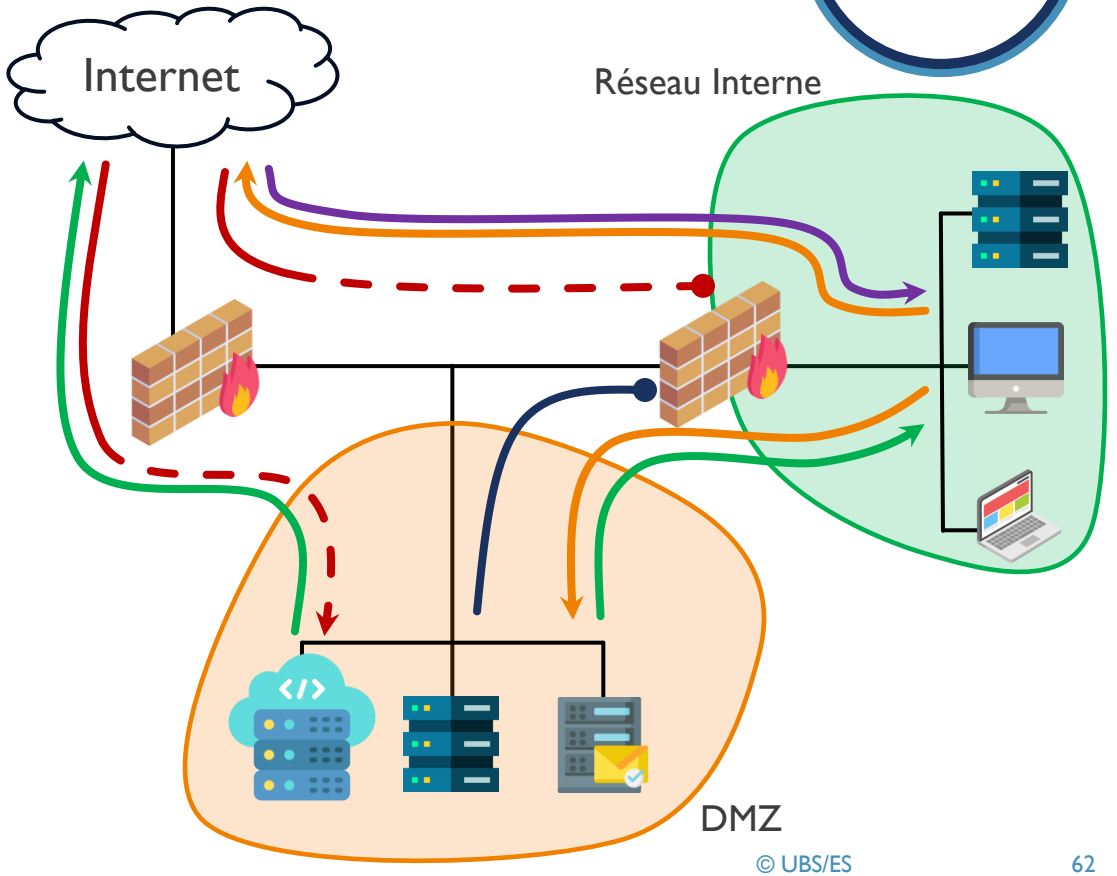
Renforcer la sécurité des systèmes d'information

- Influencé par l'architecture de sécurité mis en place
- Objectif de permettre l'accès à des ressources informatiques
  - Réduire les risques de sécurité
- Permet l'identification et le suivi des participants

ZONE DÉMILITARISÉE

Sous-réseau isolé et accessible depuis l'internet

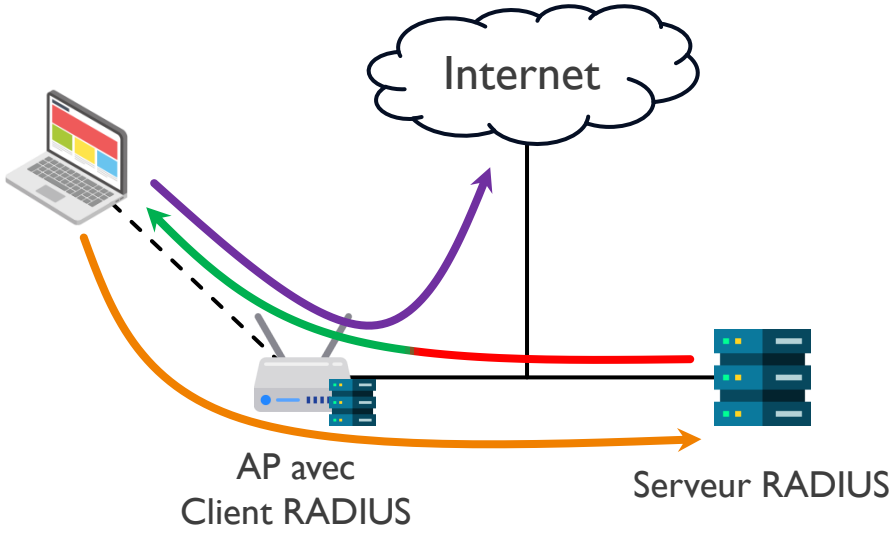
- Ségrégation des services réseau
  - DMZ accessible du réseau local et l'internet
  - Réseau local pas accessible du DMZ
- Réduction de la probabilité de compromission du réseau local
- Utilisation des règles de pare-feu



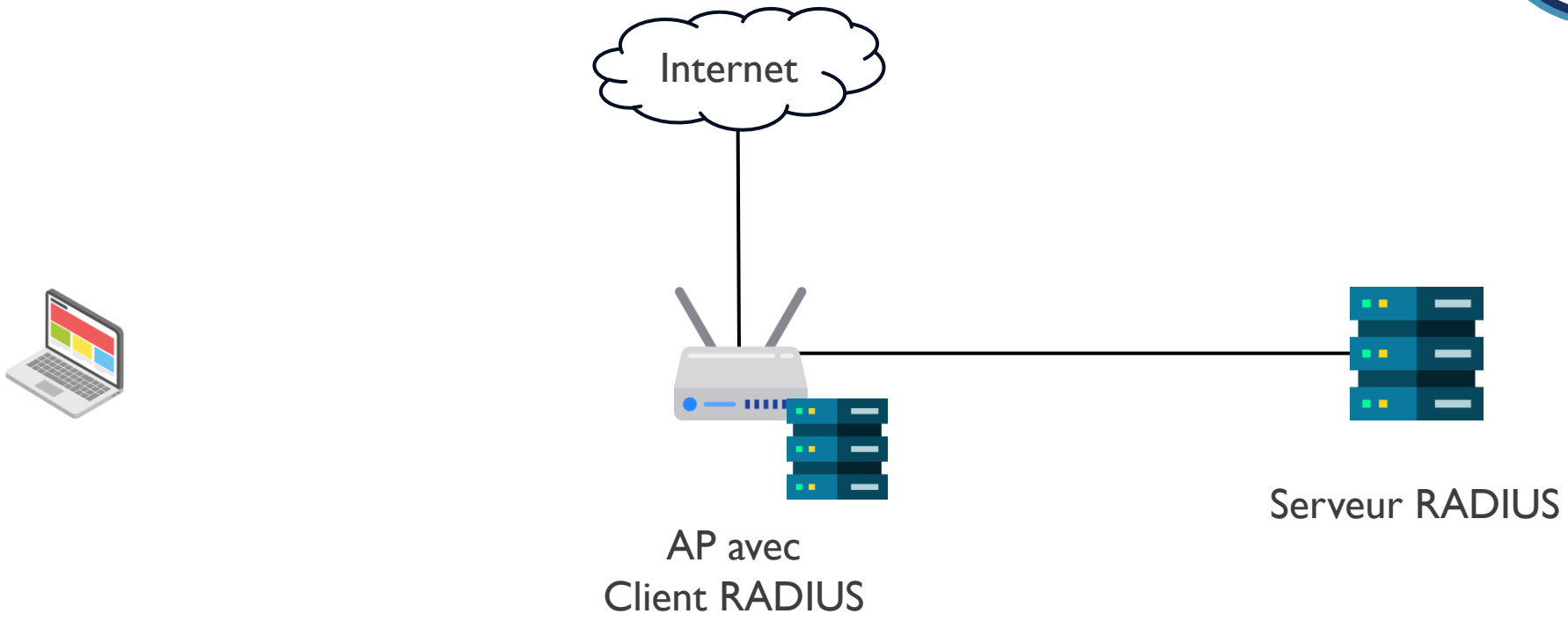
REMOTE AUTHENTICATION DIAL-IN USER SERVICE

Protocole de gestion d'authentification, autorisation et comptabilisation (AAA)

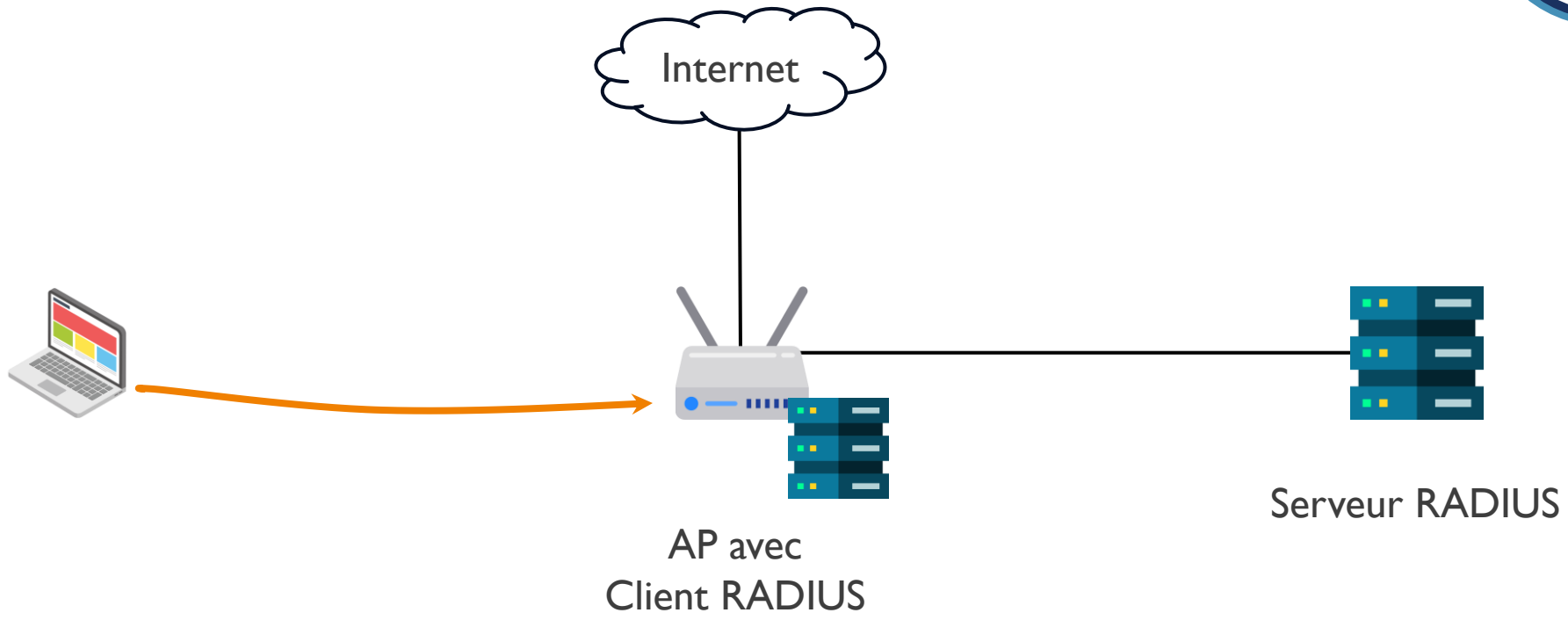
- Développé 1991 – Normalisé RFC 2865/6
- Protocole couche applicatif – TCP/UDP
- Fonctionnement client-serveur
  - **Client** → Gere l'authentification (NAS – Network Access Server)
  - **Serveur** → Gere une BDD de profiles utilisateurs (Annuaire, LDAP, etc…)
- Utilisé pour la gestion d'accès 802..1X (Wi-Fi Eduroam)
  - Couple login – mdp → Protocole LEAP



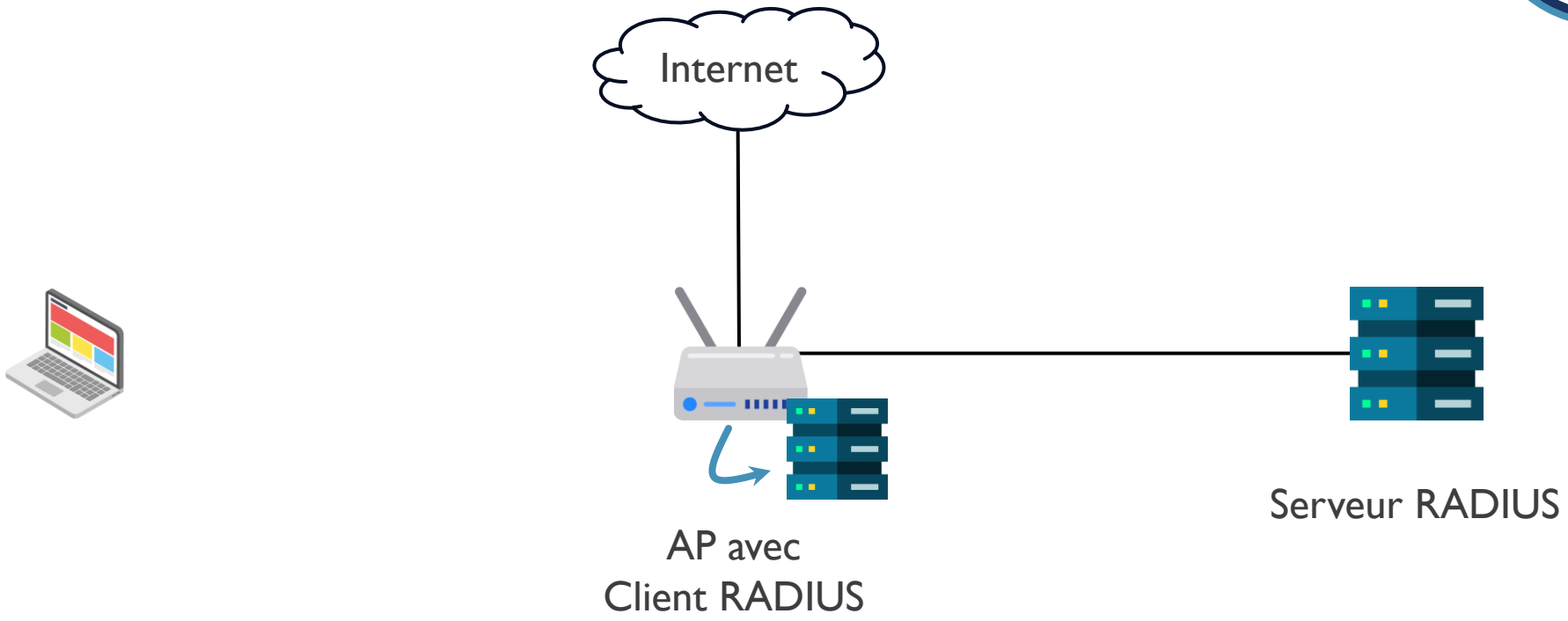
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



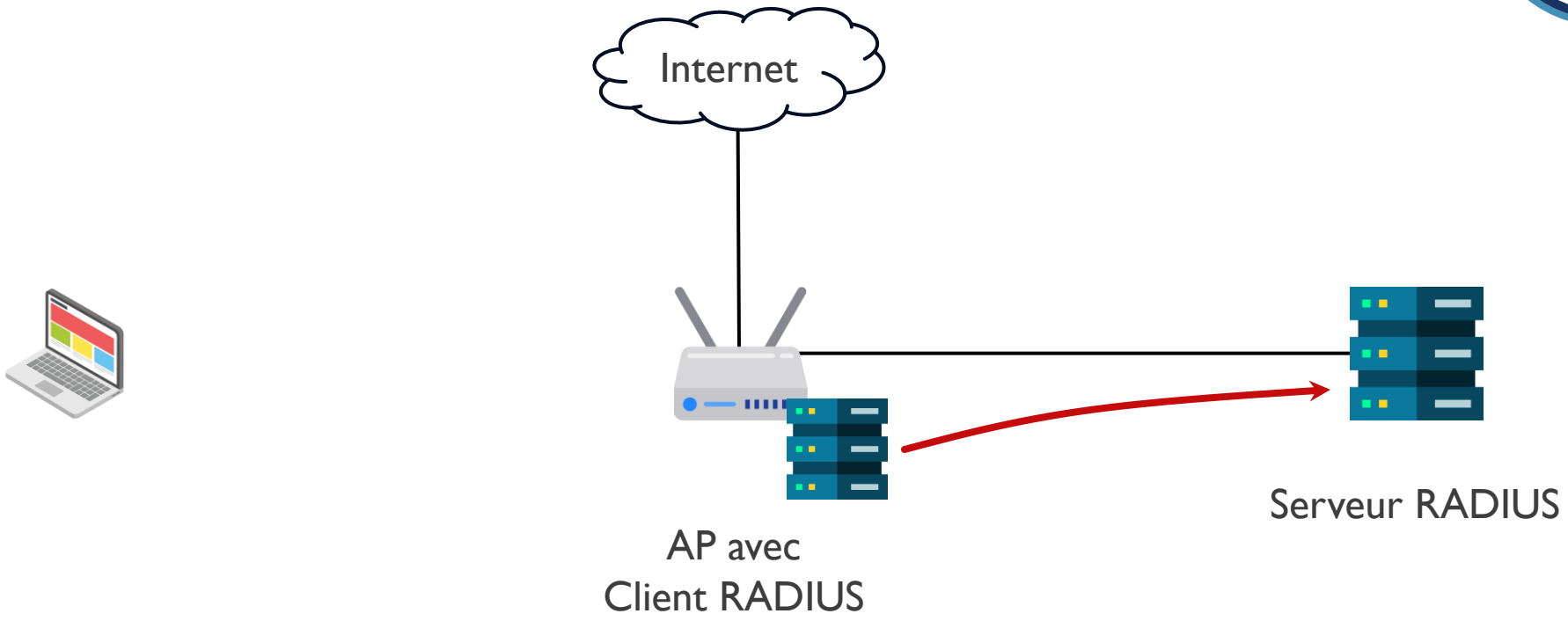
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



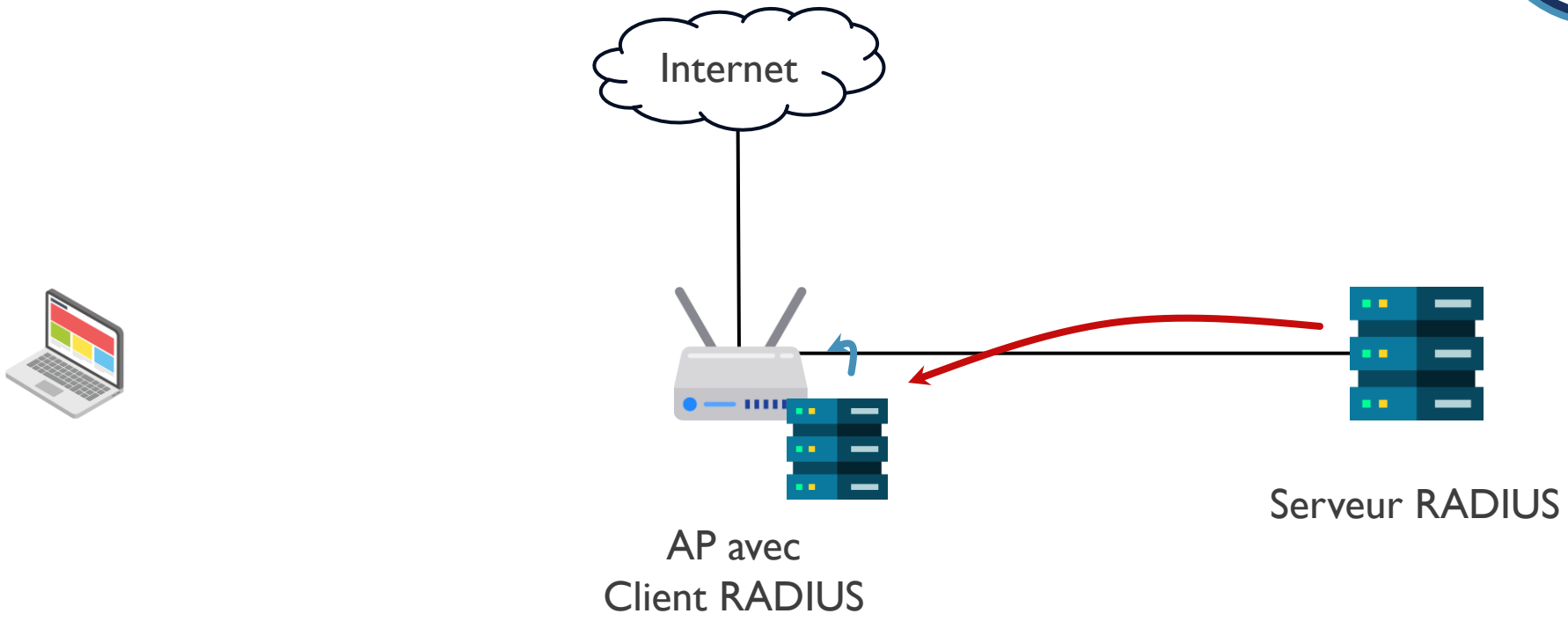
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



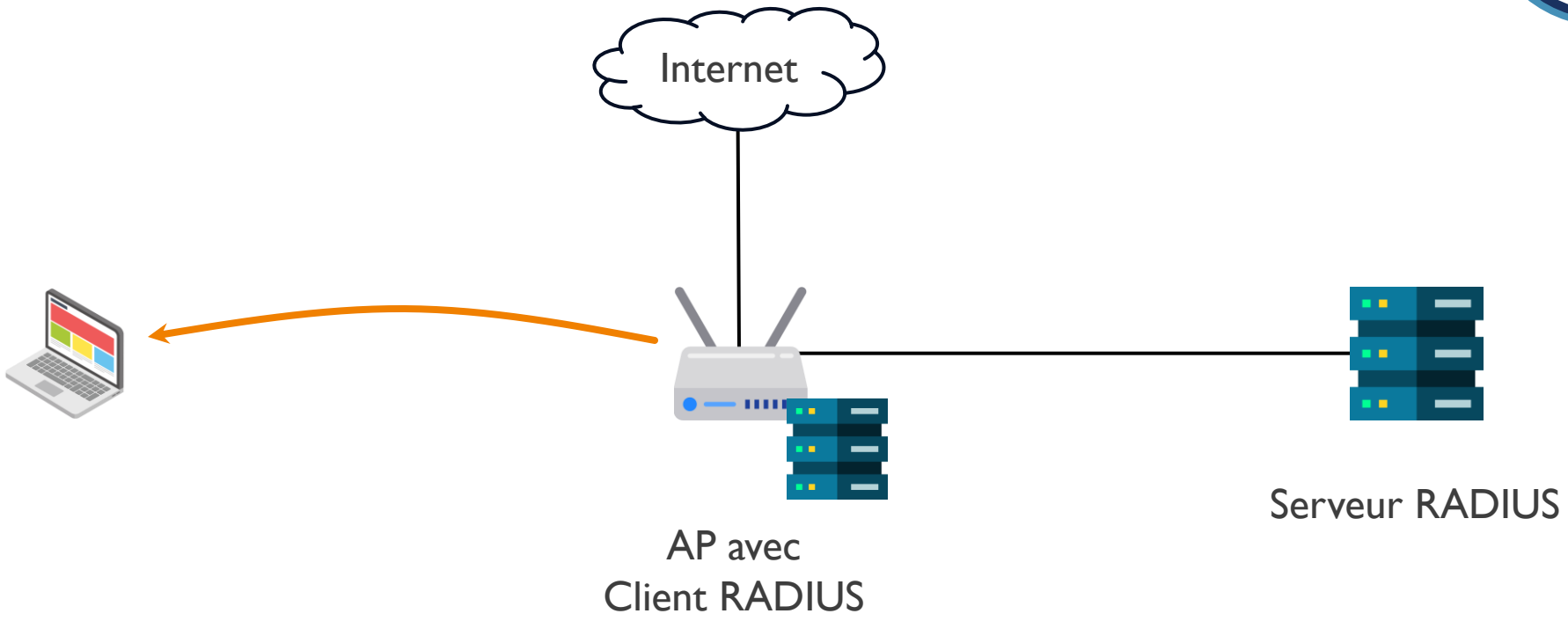
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



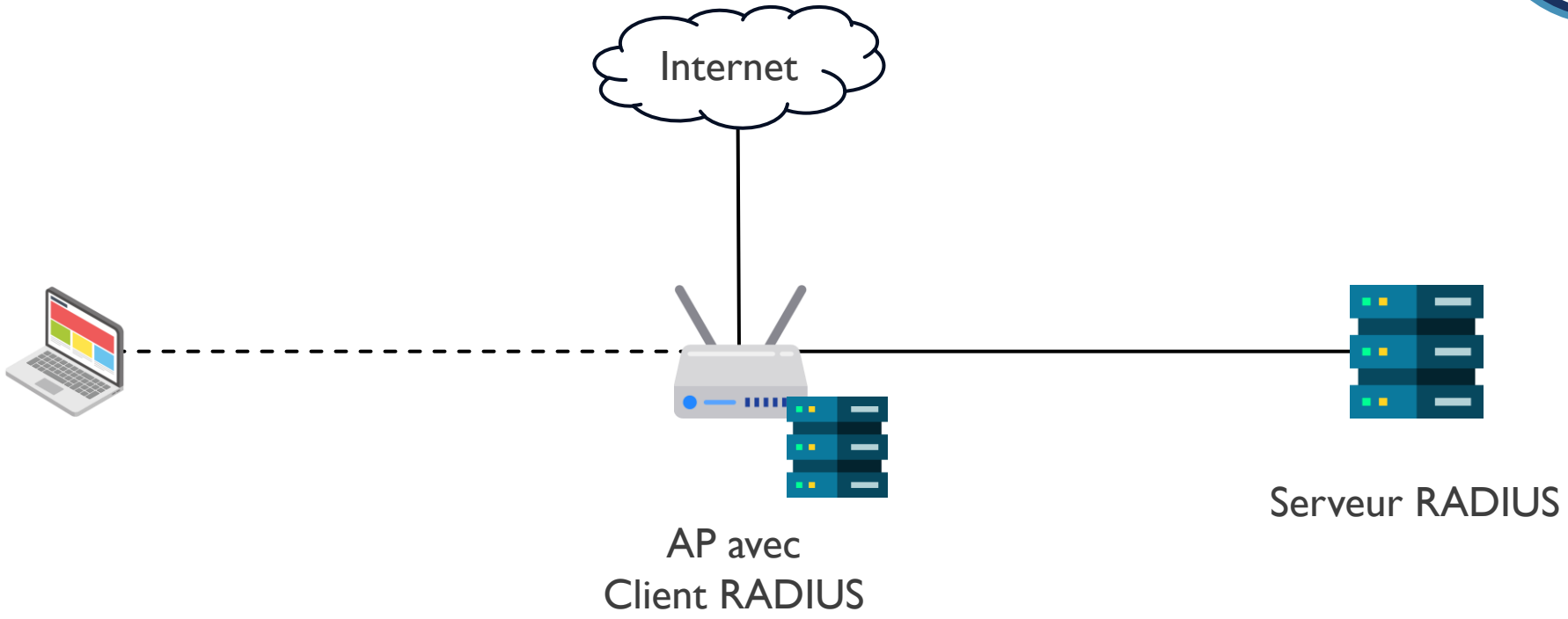
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



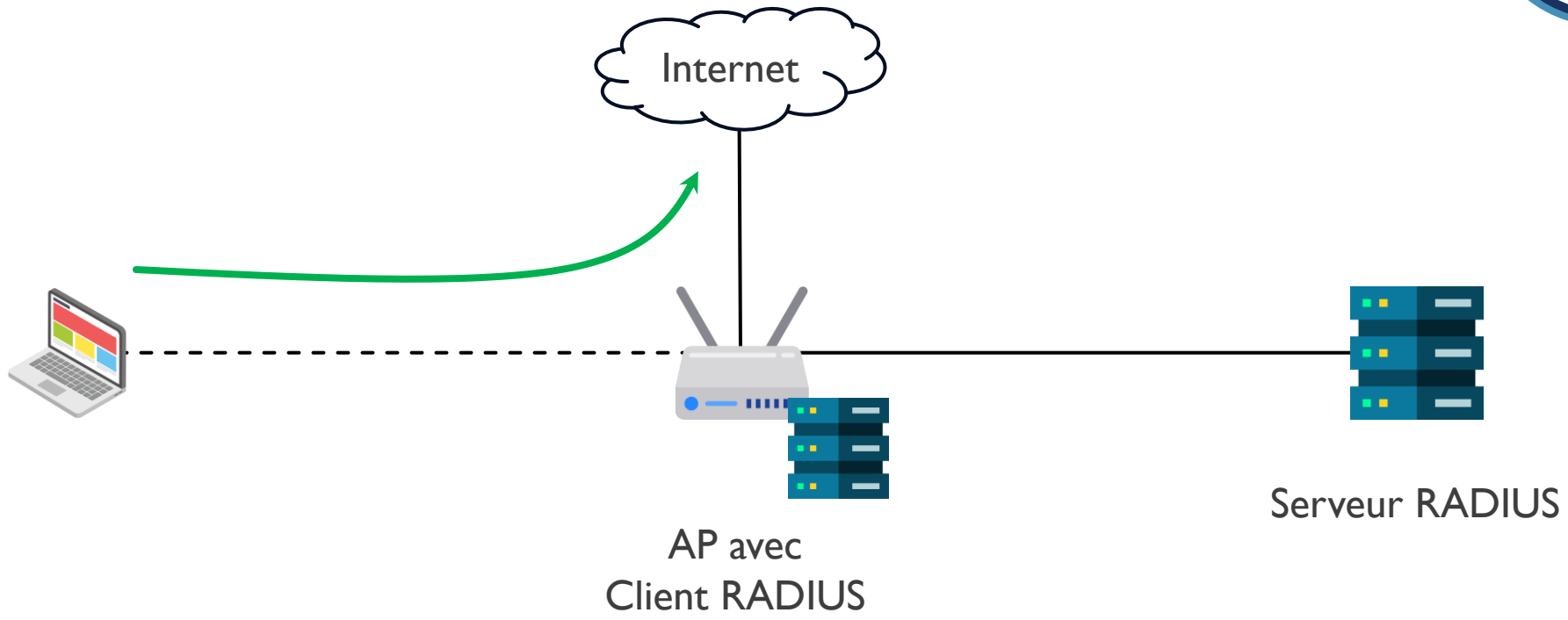
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



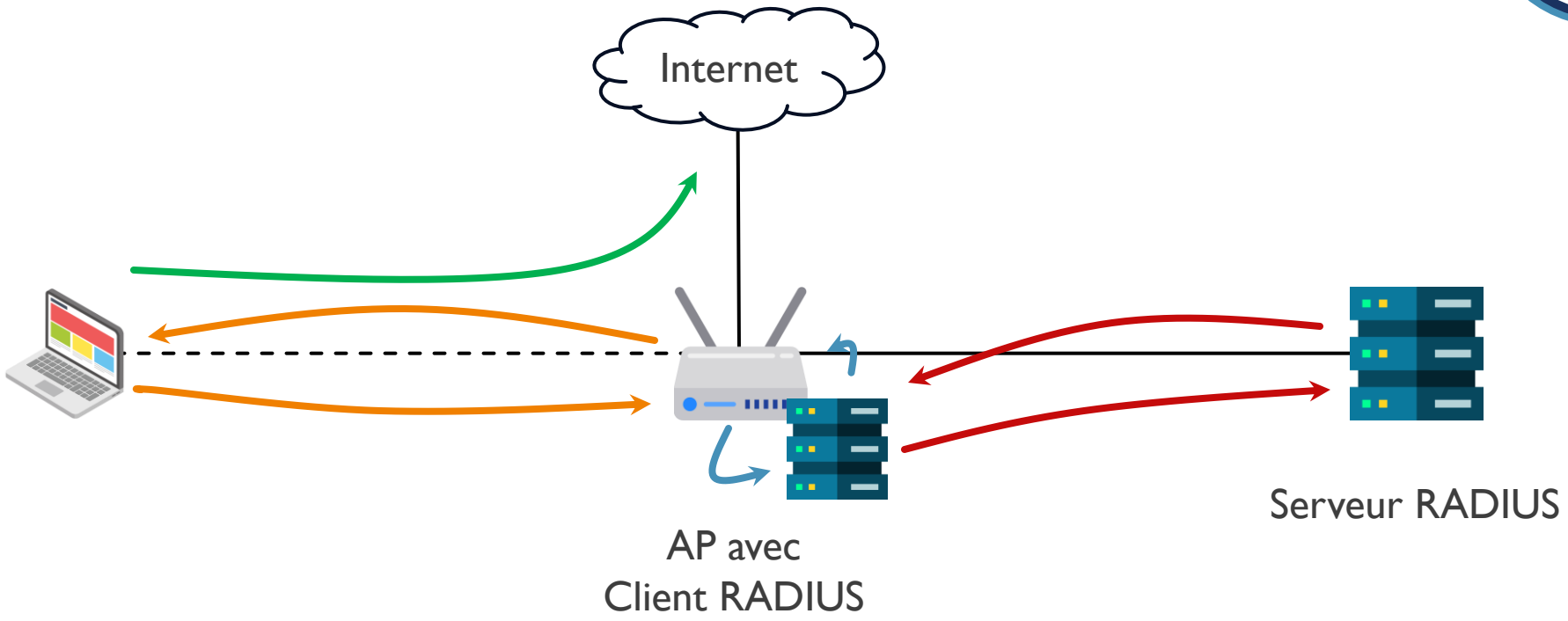
REMOTE AUTHENTICATION DIAL-IN USER SERVICE



REMOTE AUTHENTICATION DIAL-IN USER SERVICE



REMOTE AUTHENTICATION DIAL-IN USER SERVICE

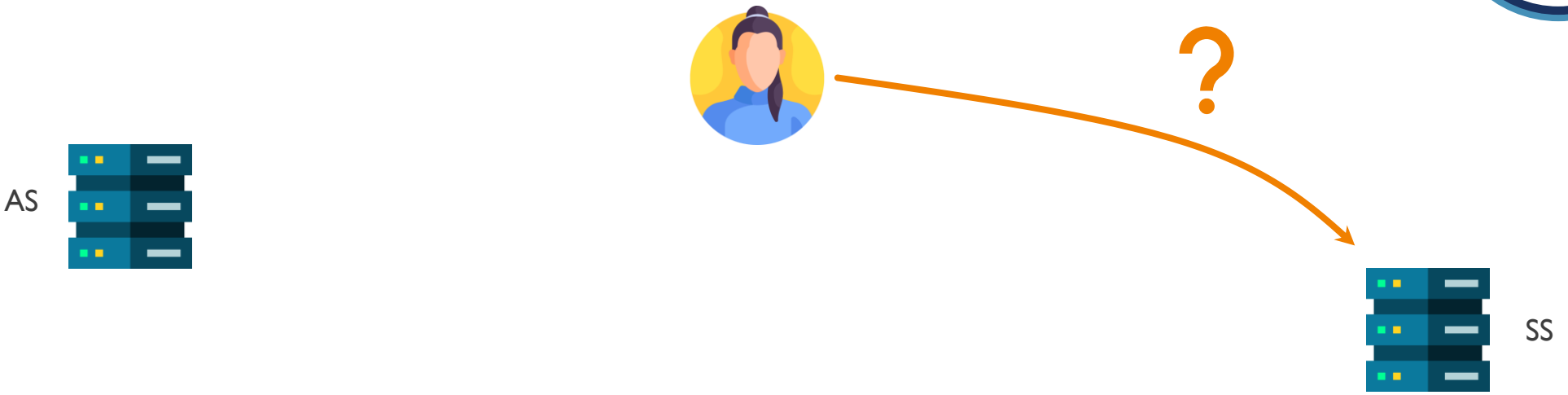


KERBEROS

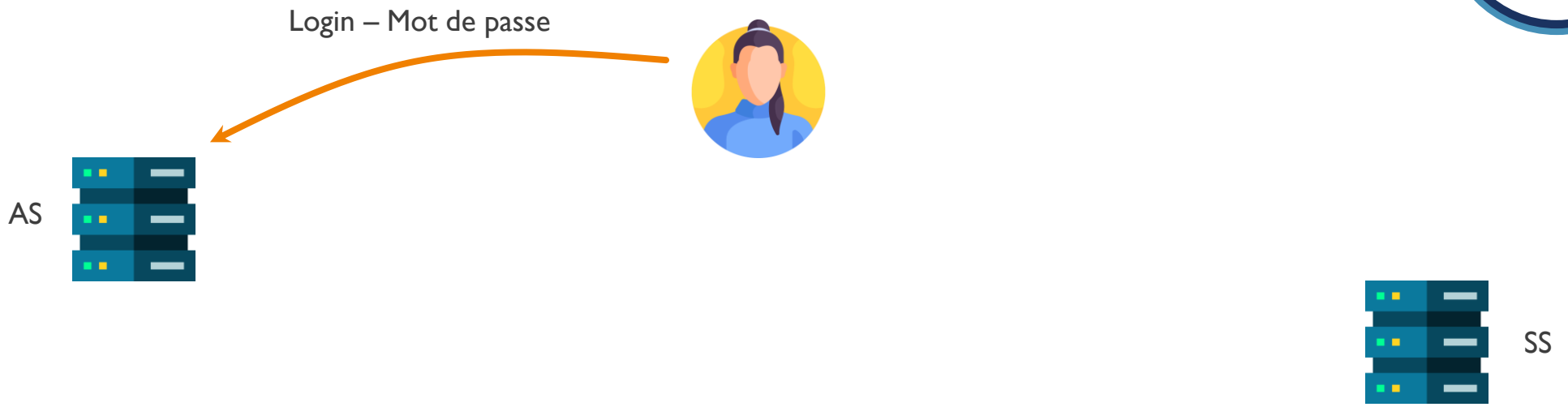
Protocol d'authentification réseau cryptographique

- Permet l'authentification sans envoi de mot de passe sur internet
- Protocole de référence pour les sites internet et Windows
- Utilisation de la cryptographie symétrique par clé
  - Empêcher le partage d'informations personnels sur internet
- Authentification et vérification d'identité par un *Centre de Distribution de Clés* (**KDC**)
- Implication de trois aspects
  - Un *Serveur d'Attribution de Tickets* (**TGS**) → connecter l'utilisateur au *Serveur de Service* (**SS**)
  - Une BDD stockant les mots de passe et l'identification des utilisateurs vérifiés
  - Un *Serveur d'Authentification* (**AS**) qui effectue l'authentification initiale
- Tickets stockés coté utilisateur
  - *Ticket d'Attribution de Billet* (**TGT**) utilisé pour authentifier sur les services
    - Appelé aussi jeton
  - Permet la réauthentification sans mot de passe

AUTHENTIFICATION NORMALE

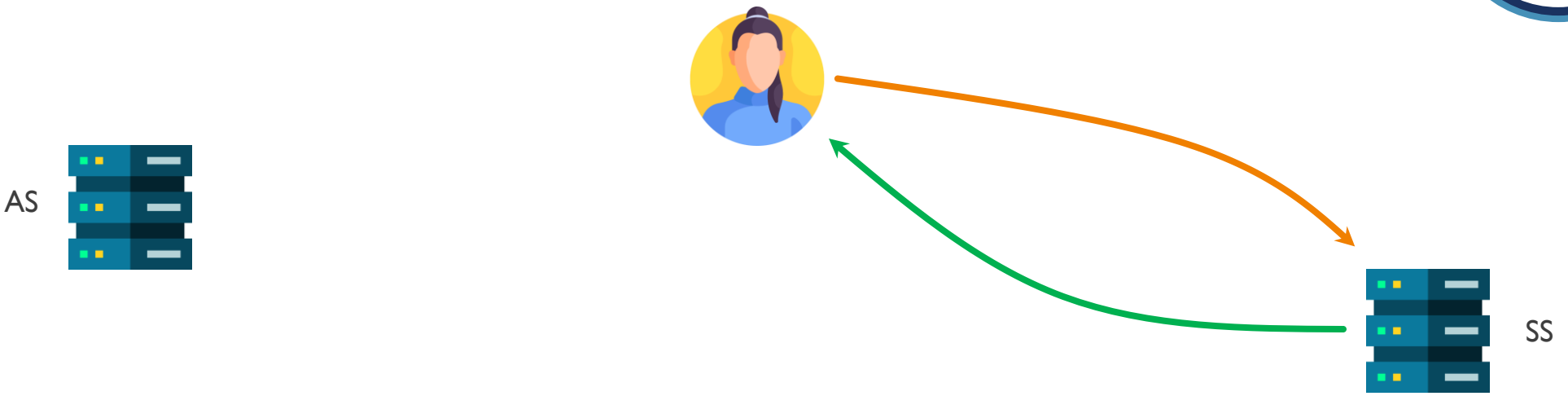


AUTHENTIFICATION NORMALE

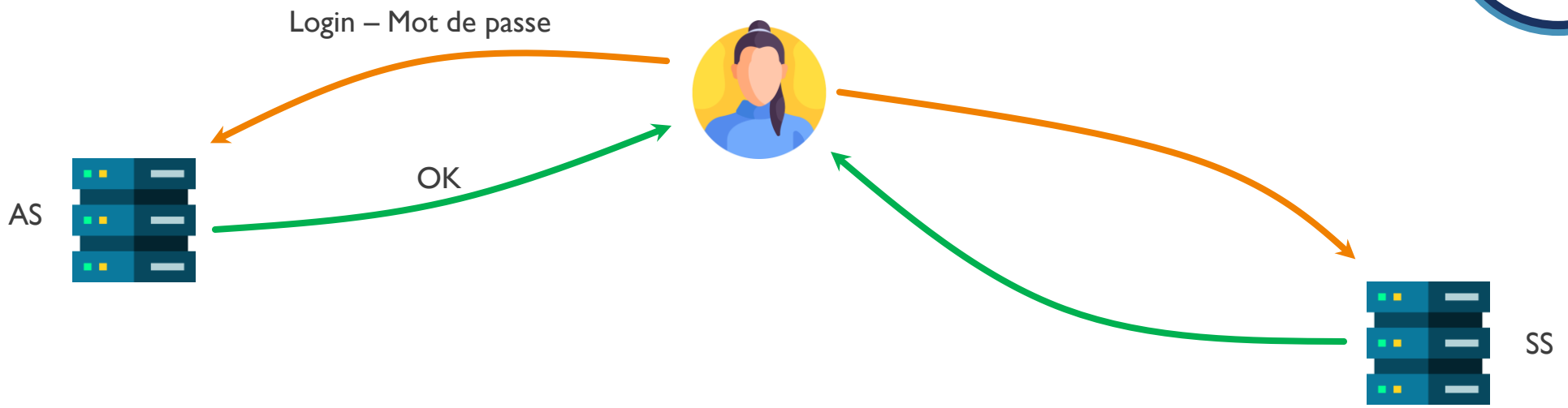


AUTHENTIFICATION NORMALE

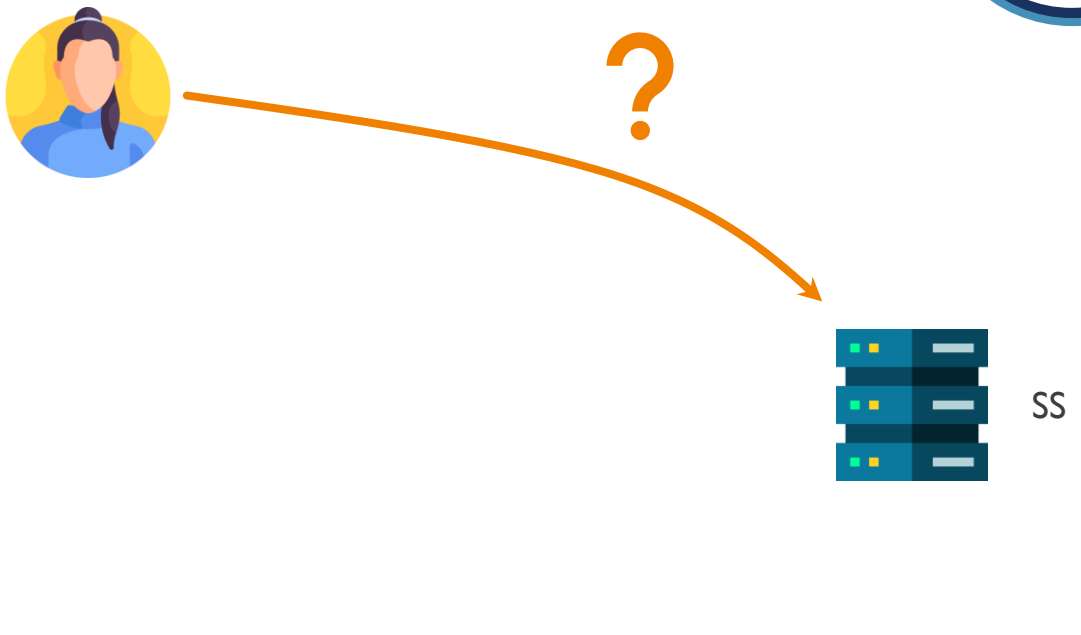
AUTHENTIFICATION NORMALE



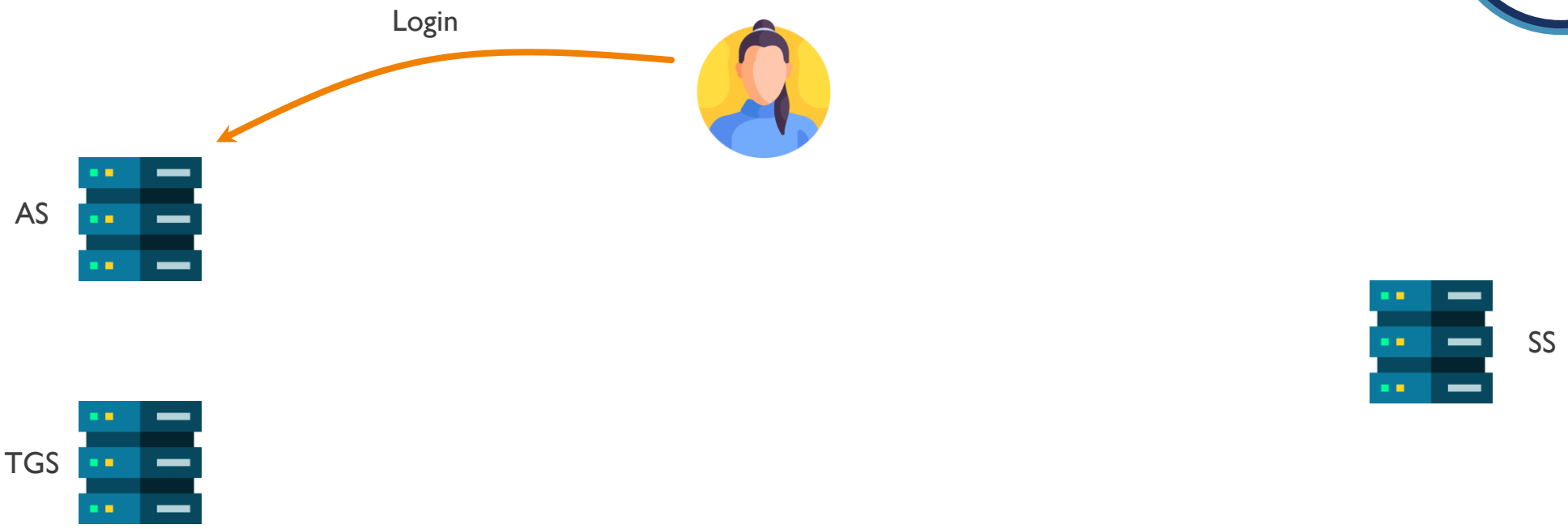
AUTHENTIFICATION NORMALE



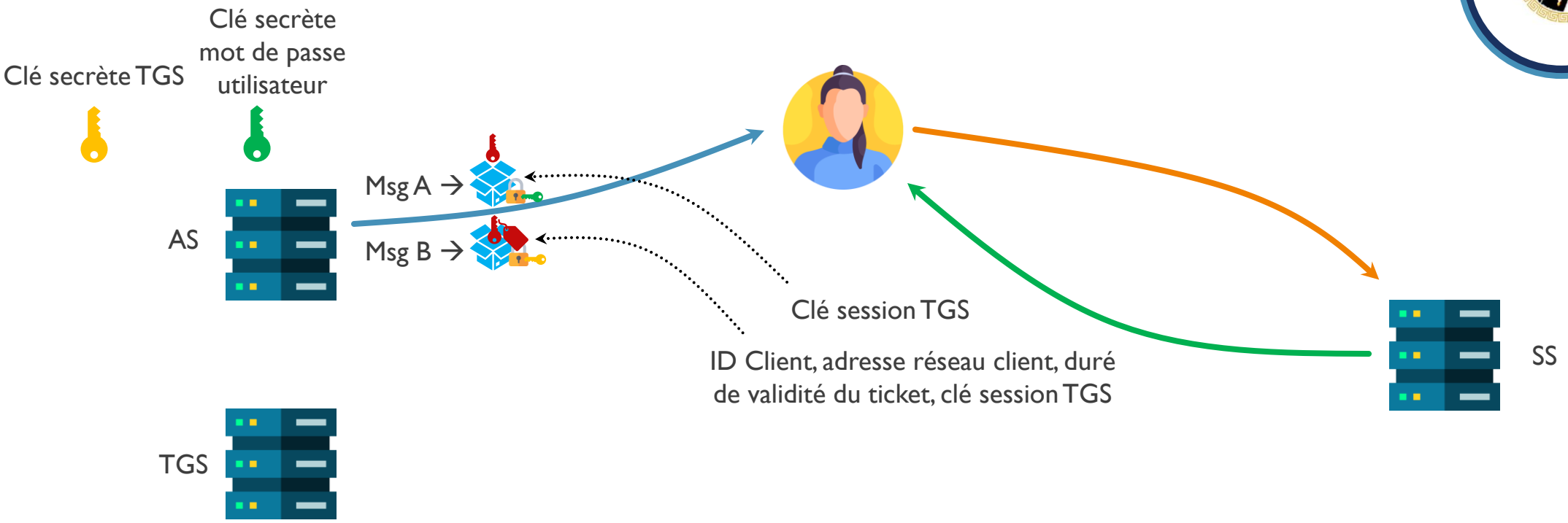
AUTHENTIFICATION KERBEROS



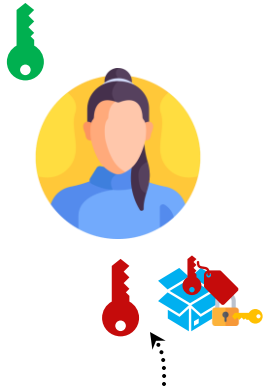
AUTHENTIFICATION KERBEROS



AUTHENTIFICATION KERBEROS



AUTHENTIFICATION KERBEROS

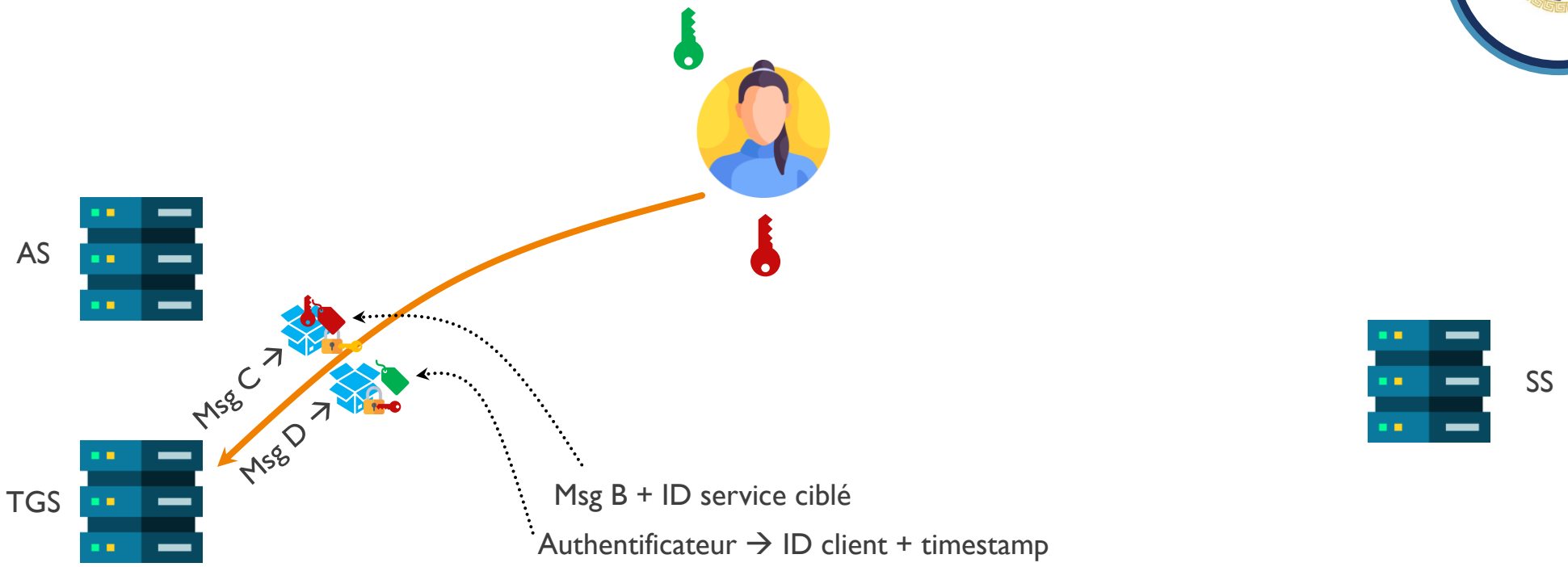


AS

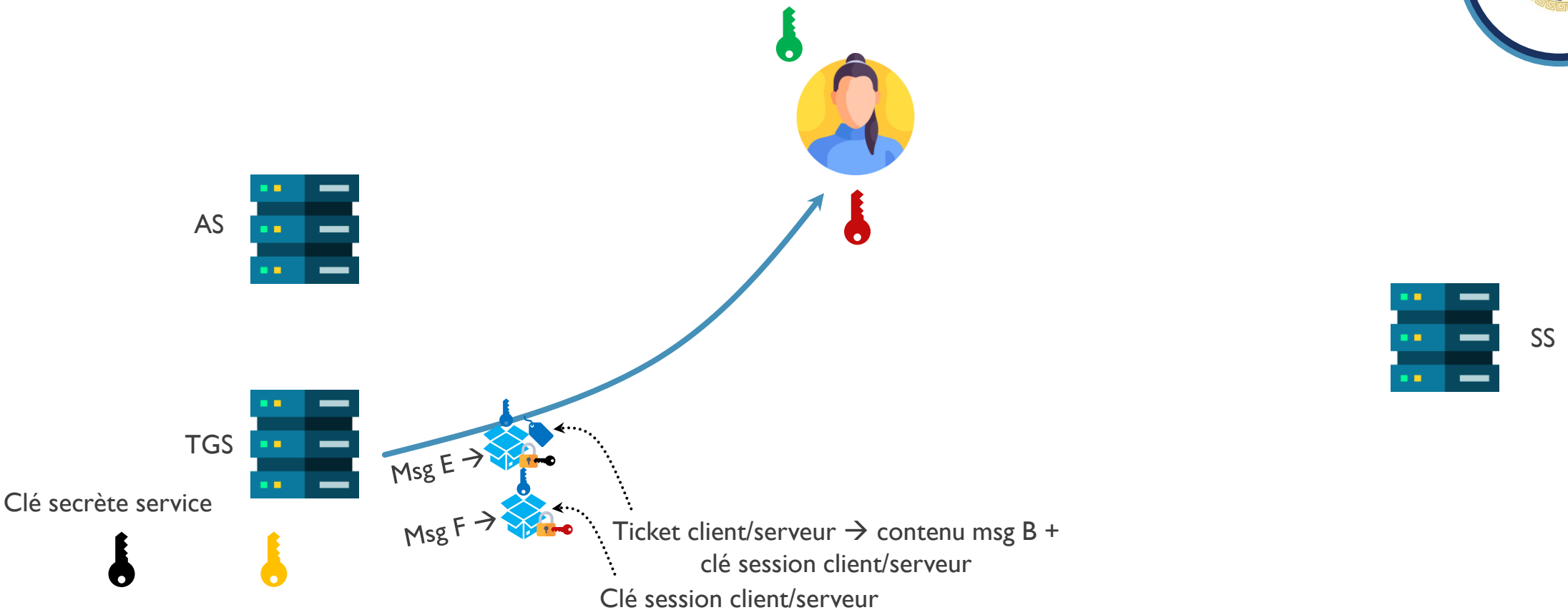
TGS

SS

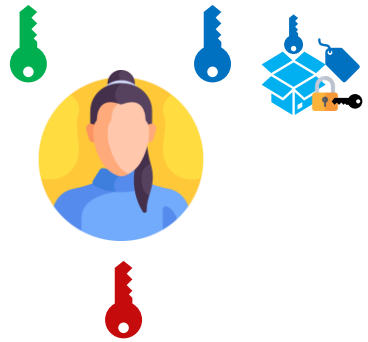
AUTHENTIFICATION KERBEROS



AUTHENTIFICATION KERBEROS



AUTHENTIFICATION KERBEROS



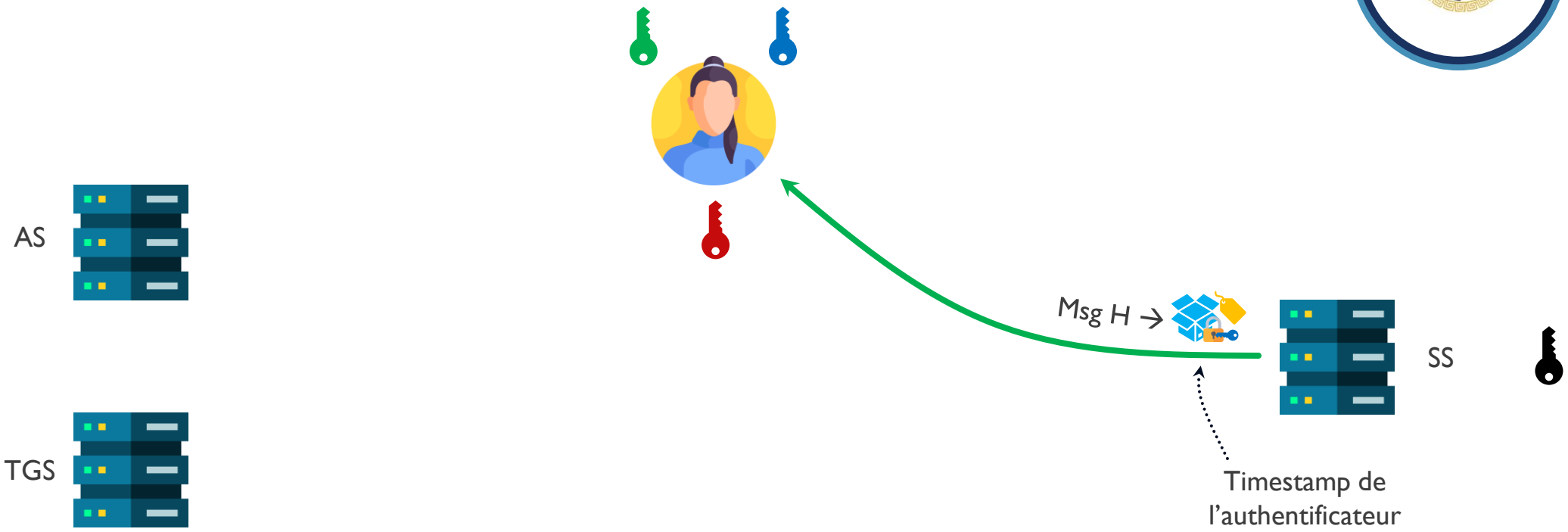
AS

TGS

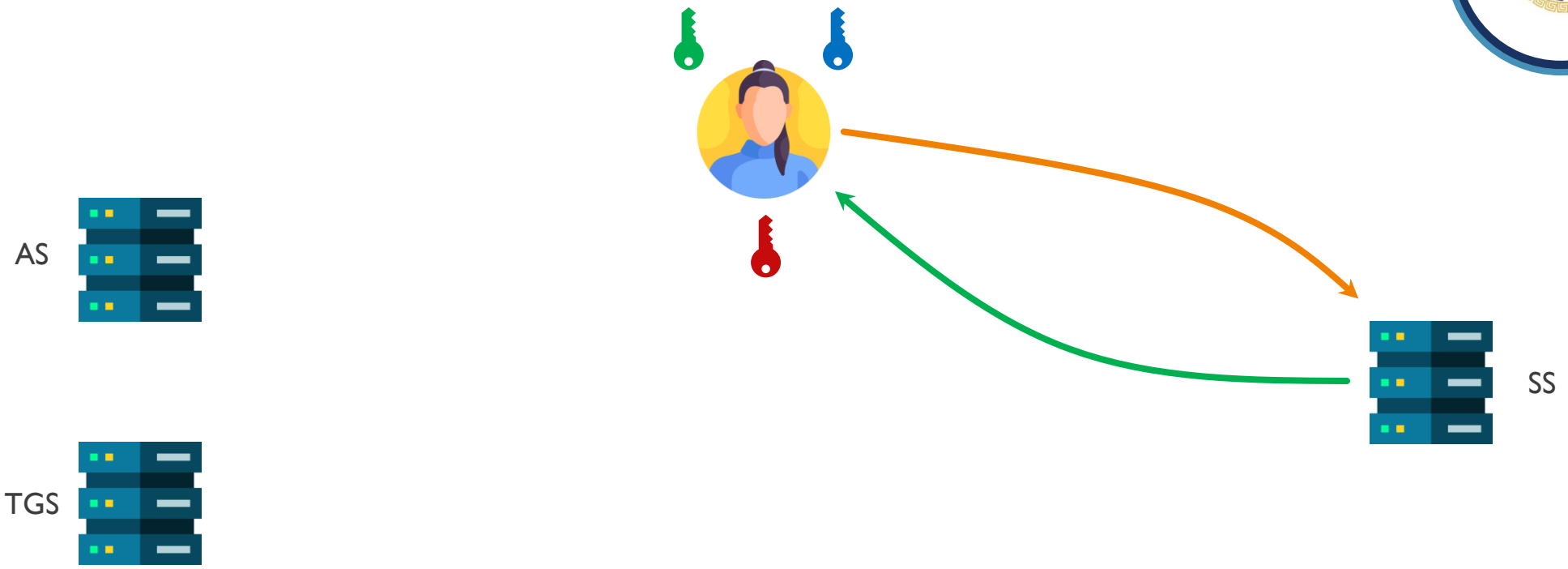
SS

AUTHENTIFICATION KERBEROS

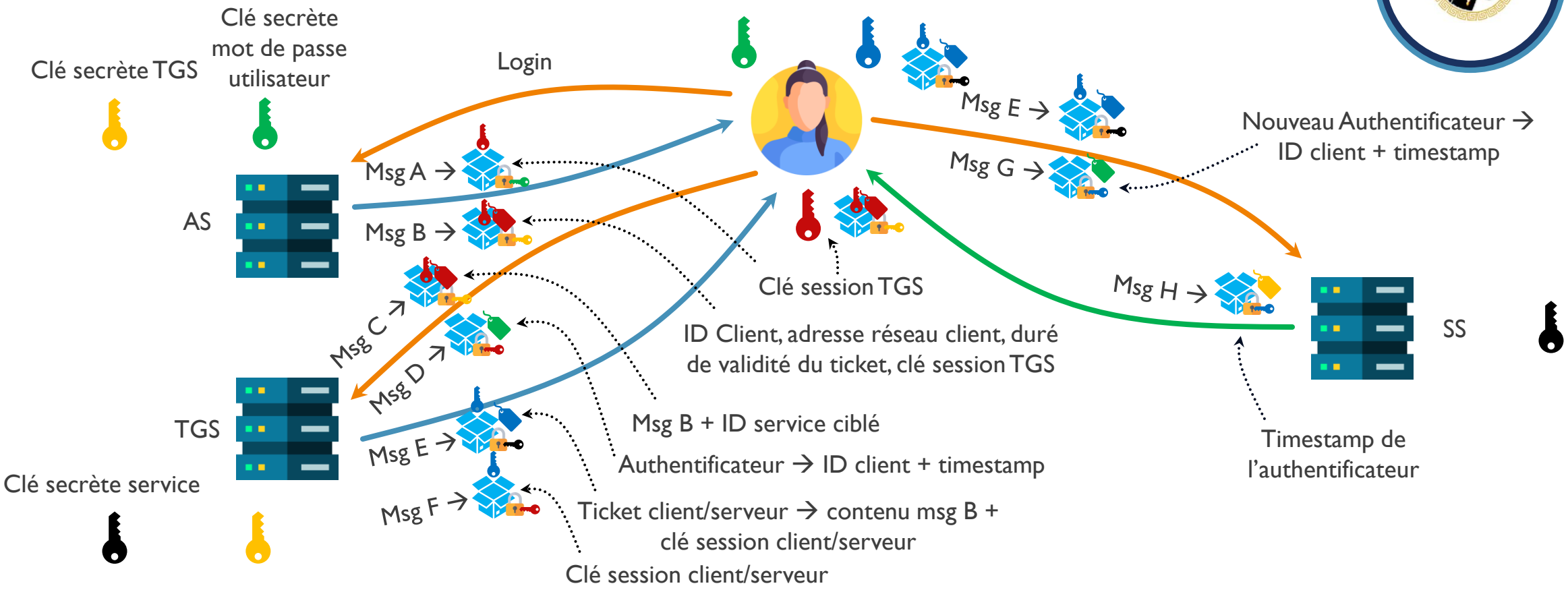
AUTHENTIFICATION KERBEROS



AUTHENTIFICATION KERBEROS



AUTHENTIFICATION KERBEROS



KERBEROS – AVANTAGES

Control d'accès

- Système efficace
- Point unique de suivi des connexions et des politiques

Authentification mutuelle

- Confirmation de l'identité des utilisateurs ET les systèmes de service

Durée de vie limitée

- horodatage des tickets avec une durée de vie d'authentification administrable

Authentification réutilisable

- Mécanisme durable avec une authentification unique
- Pas de renseignement d'informations personnelles pendant la durée du ticket

Sécurité

- Plusieurs clés cryptées
- Autorisation de tiers
- Pas d'envoi de mdp
- Maturité
- Solidité
- Intégration OS
- Correspond aux attentes modernes

KERBEROS – FAIBLESSES

Point de défaillance unique

- Système efficace
- Point unique de suivi des connexions et des politiques

Autant de clés que de services

- Une clé par service
- Défis d'hébergement en cluster / virtualisation

Exigences temporelles strictes

- Synchronisation obligatoire de date avec des limites prédéfinis
- Authentification echoue à cause de l'horodatage des tickets