
David MICHEL
Adista
Opérateur de
Services Hébergés
COURS SÉCURITÉ POLYTECH NANCY

Adista

Métiers multiples :

- **Intégration de Systèmes**
- **Opérateur de télécommunications**
- **Hébergement informatique et infogérance**
- **Ingénierie de projet web**

David MICHEL

Architecte SD-WAN

Expert IT Réseau et OpenSource

CYBERSÉCURITÉ & CRYPTOGRAPHIE

- INTRODUCTION
- SÉCURITÉ FIREWALL
- SÉCURITÉ DES COMMUNICATIONS (HTTPS, SSH, VPN, ...)
- SÉCURITÉ DES DONNÉES (STOCKER/UTILISER UNE INFORMATION EN TOUTE SÉCURITÉ)

Adista
Opérateur de Services Hébergés

Cybersécurité & cryptographie

Sécurité d'un Service
Ex: Firewall

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

INTRODUCTION

- Comprendre l'Internet
  - Les Applications
  - Les sites
  - Les messages
  - Les packets
  - Les entêtes
  - Les IP
  - …

Adista
Opérateur de
Services Hébergés

Layer 7: Application Layer

- Defines interface to user processes for communication and data transfer in network
- Provides standardized services such as virtual terminal, file and job transfer and operation

Layer 6: Presentation Layer

- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logical links between users
- Reports upper layer errors

Layer 4: Transport Layer

- Manages end-to-end message delivery in network
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
- Provides connectionless oriented packet delivery

Layer 3: Network Layer

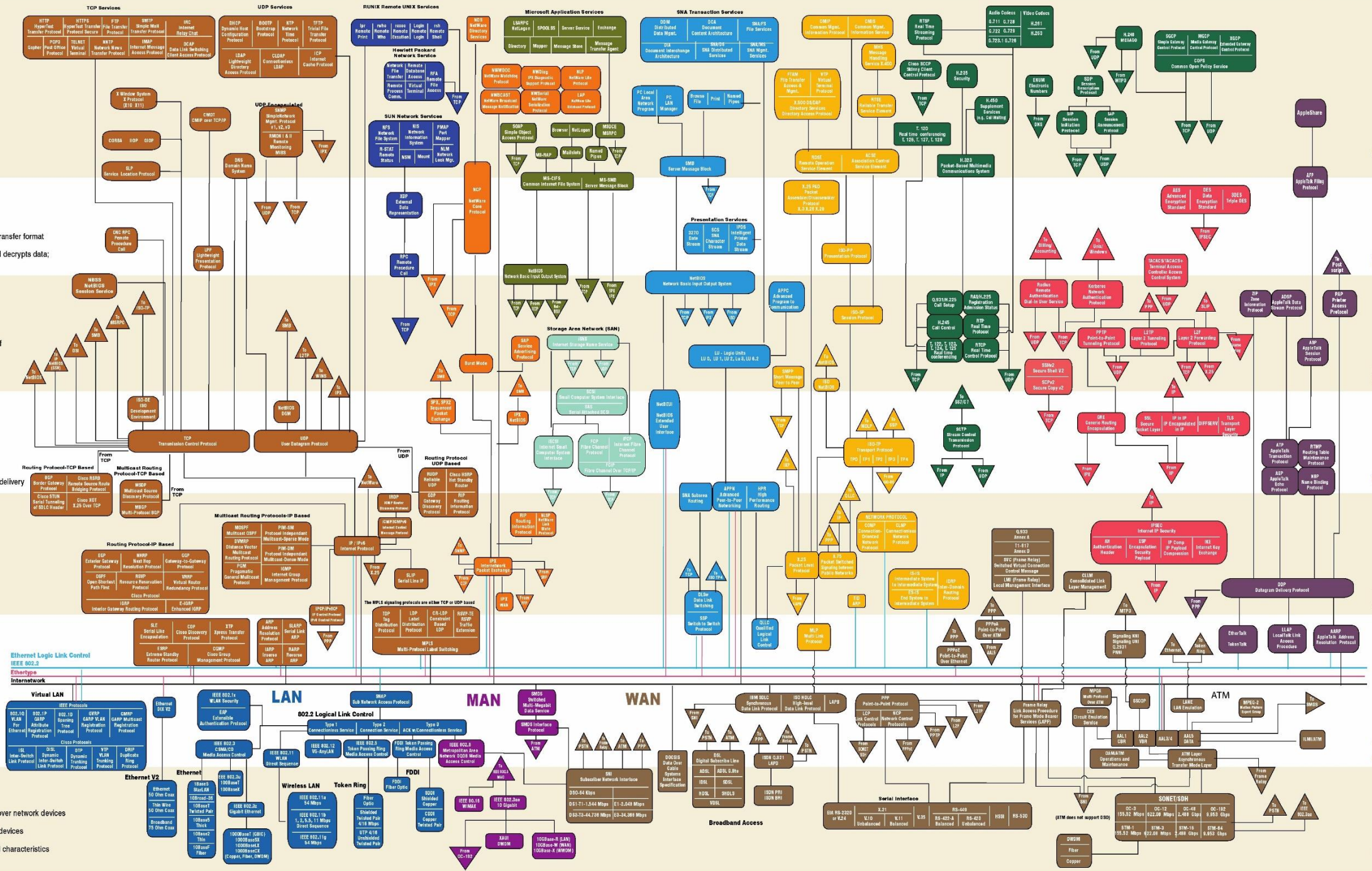
- Determines how data are transferred among network devices
- Routes packets according to unique network addresses
- Provides flow and congestion control to prevent network resource depletion

Layer 2: Data Link Layer

- Defines procedures for operating the communication link
- Provides framing and sequencing
- Detects and corrects received frame errors

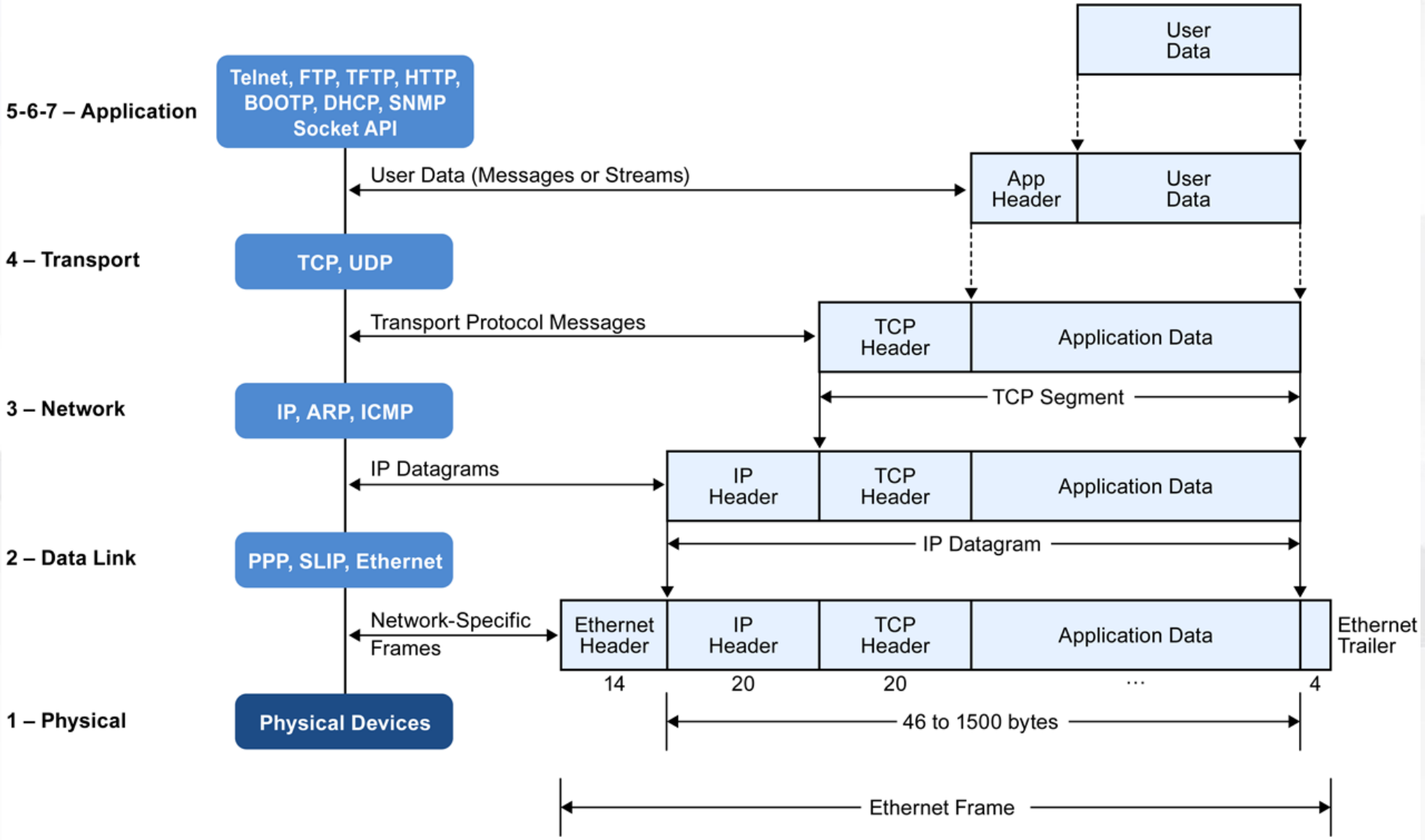
Layer 1: Physical Layer

- Defines physical means of sending data over network devices
- Interfaces between network medium and devices
- Defines optical, electrical and mechanical characteristics



SÉCURITÉ FIREWALL

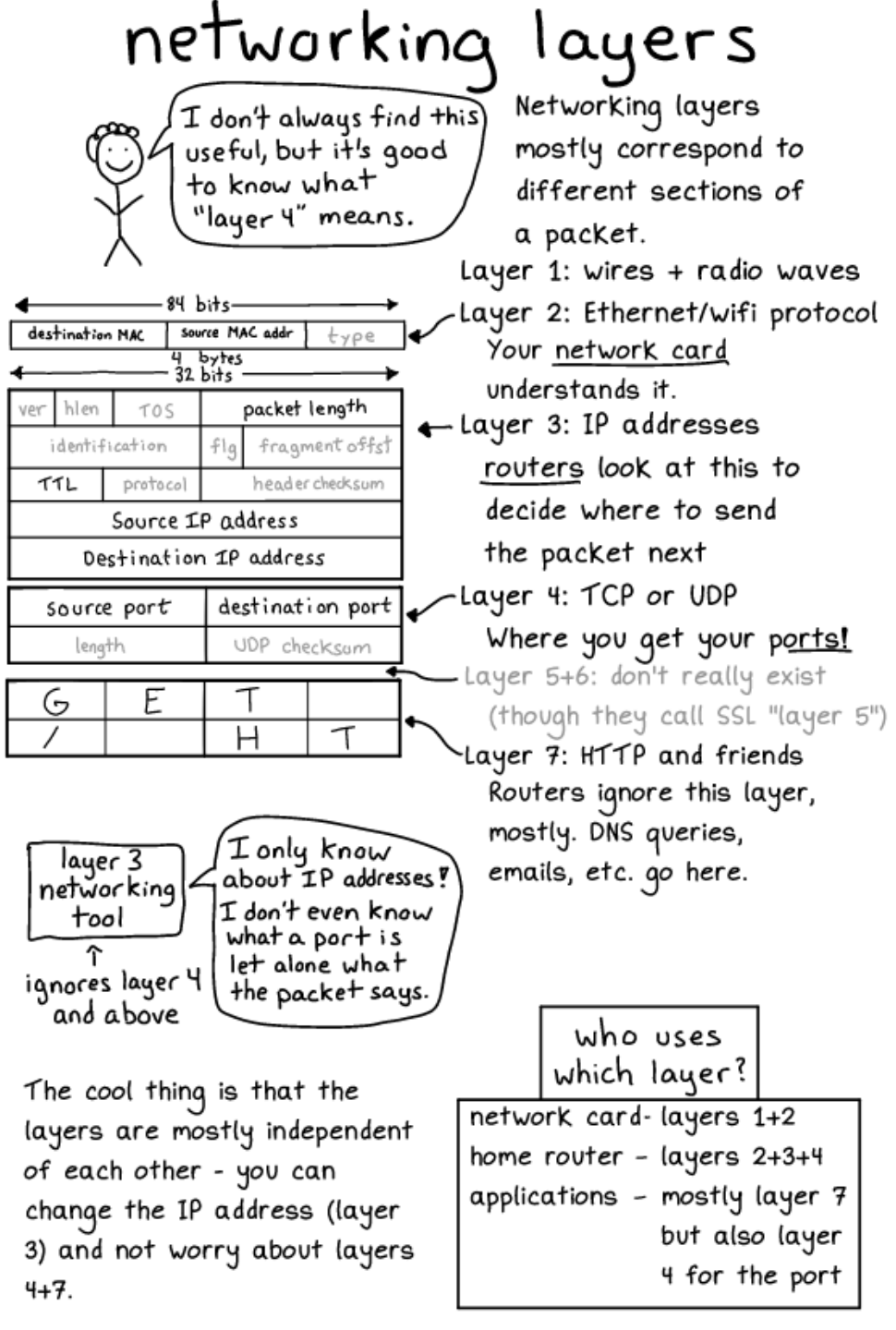
INTRODUCTION



Adista
Opérateur de Services Hébergés

SÉCURITÉ FIREWALL

INTRODUCTION



Adista
Opérateur de Services Hébergés

SÉCURITÉ FIREWALL

INTRODUCTION

- Qui fait
- Source et destination
- Séparations des droits
- Firewall externe != Firewall local
- Quel type de Firewall ?
  - L2
  - L3
  - L7 (ex : WAF pour http)

Adista
Opérateur de
Services Hébergés

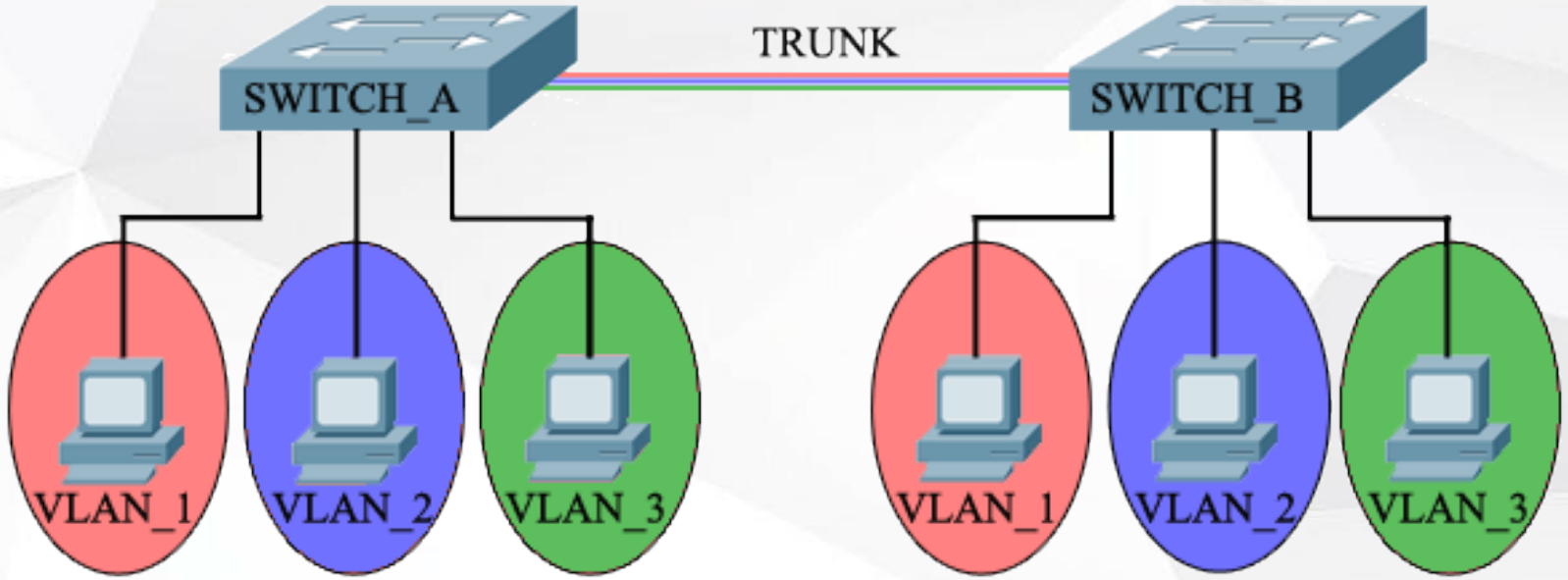
SÉCURITÉ FIREWALL

PROTOCOLES L1

- VLANs

802.1X avec EAP (Extensible Authentication Protocol)

- EAP-PSK



Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

PROTOCOLES L3

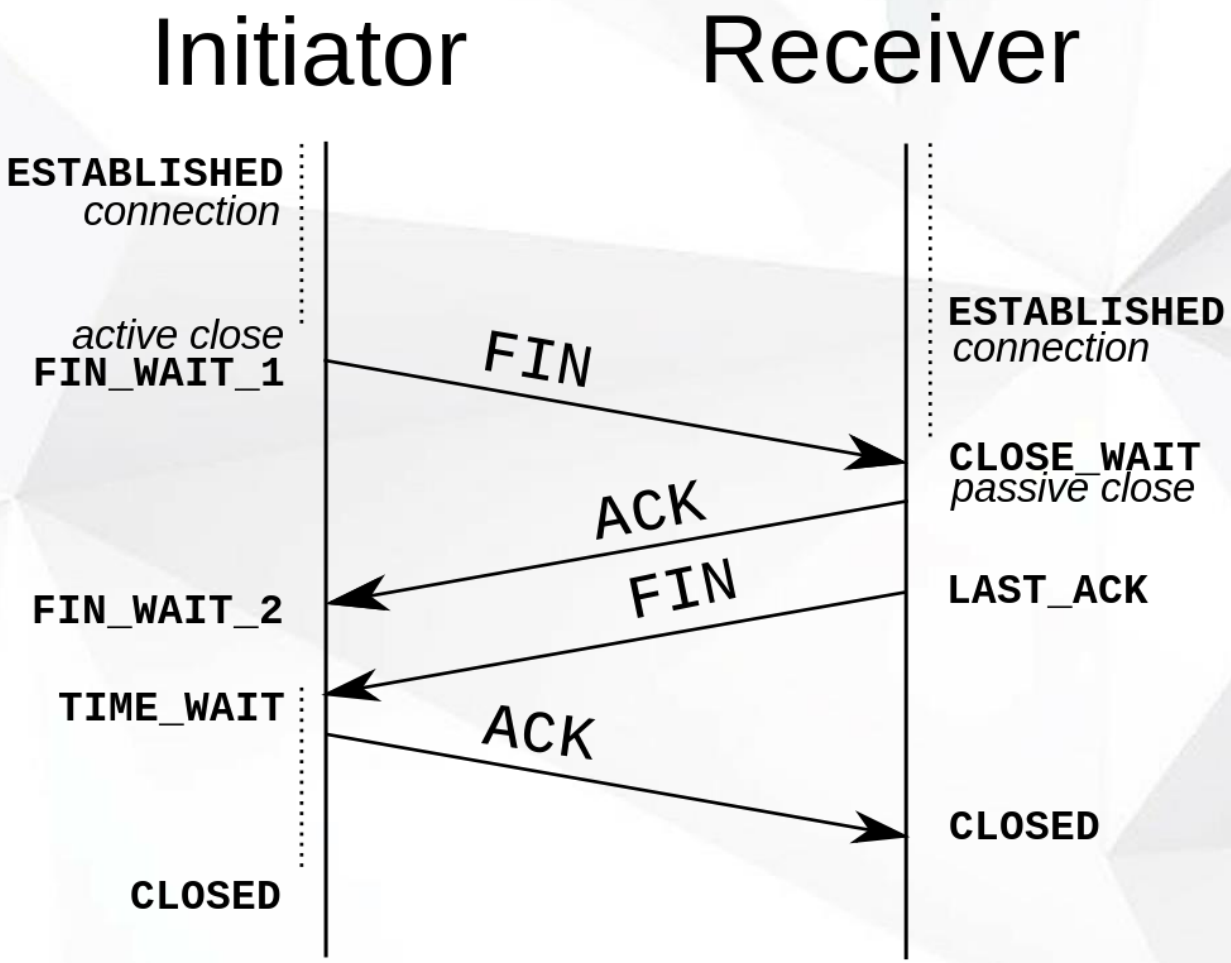
- UDP & TCP
- UDP est un protocole orienté « *stateless* ».
  - Le flux est unidirectionnel sans validation
- TCP est orienté « *statefull* »

- UDP plus rapide
- TCP plus fiable et sans IP Spoofing

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

PROTOCOL



Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

NFTABLES (IPTABLES)

NFTables , pour filtrer ses paquets, se base sur plusieurs propriétés du paquet :

- L'entête IP
- Le TCP ou UDP header

Pour l'entête IP :

- Aux flags, pour la fragmentation
- Aux Protocol (en général TCP, UDP ou ICMP)
- A l'adresse source et destination

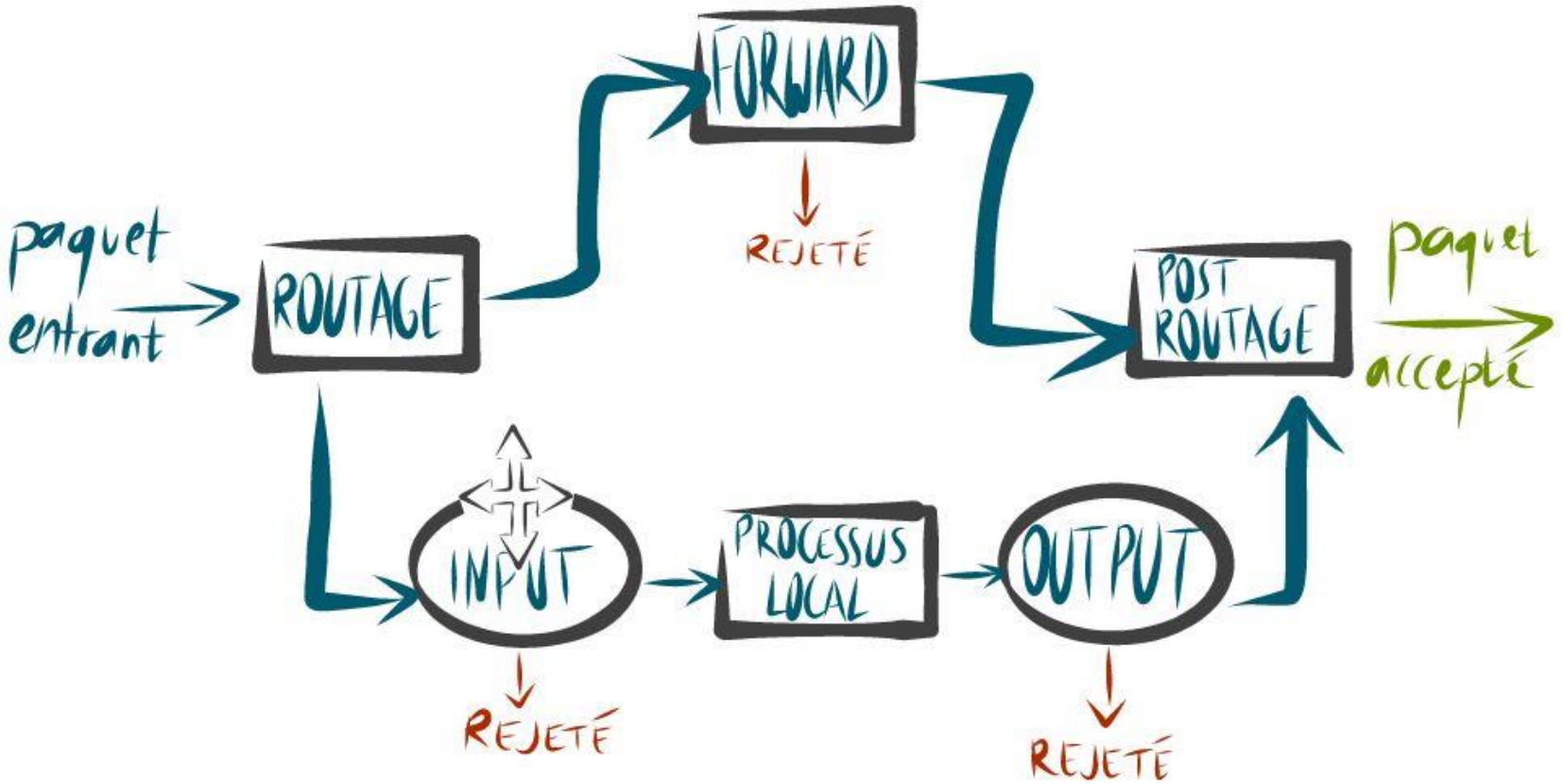
Pour l'entête source ou destination :

- Aux ports source et destination.
- Aux flags pour le protocole TCP

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

IPTABLES



Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

NFTABLES (IPTABLES)

Une règle de filtrage pourra donc par exemple être :

- Interdire les paquets avec adresses source X.X.X.X
- Interdire les paquets avec adresses destination X.X.X.X
- Interdire les paquets TCP si au-delà de 10 hits/secondes
- Interdire les paquets UDP
- Interdire les paquets avec port de destination 22 (pour la connexion SSH)

Toutes ces règles peuvent bien sûr aussi être autorisées et ajoutées les unes aux autres :

1. Autoriser les paquets TCP avec adresse destination X.X.X.X sur le port 22.
2. Interdire les paquets UDP avec adresse source X.X.X.X.

SÉCURITÉ FIREWALL

NFTABLES

- Ces règles sont **séquentielles**
  - Les plus globales doivent être placées à la fin
  - Permet les priorité
  - Permet de faire des actions plus précises
  - Plus rapide

Contre-exemple:

- Windows possède un firewall sans ordre de priorité entre ses règles

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

NFTABLES

Bonnes pratiques:

- On bloque l'entrant
- On laisse le sortant si maîtrisé
- Limitation par IP si possible
- Pas de RELATED (Conntrack+ IP helper)

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

IPTABLES

- Rate limit

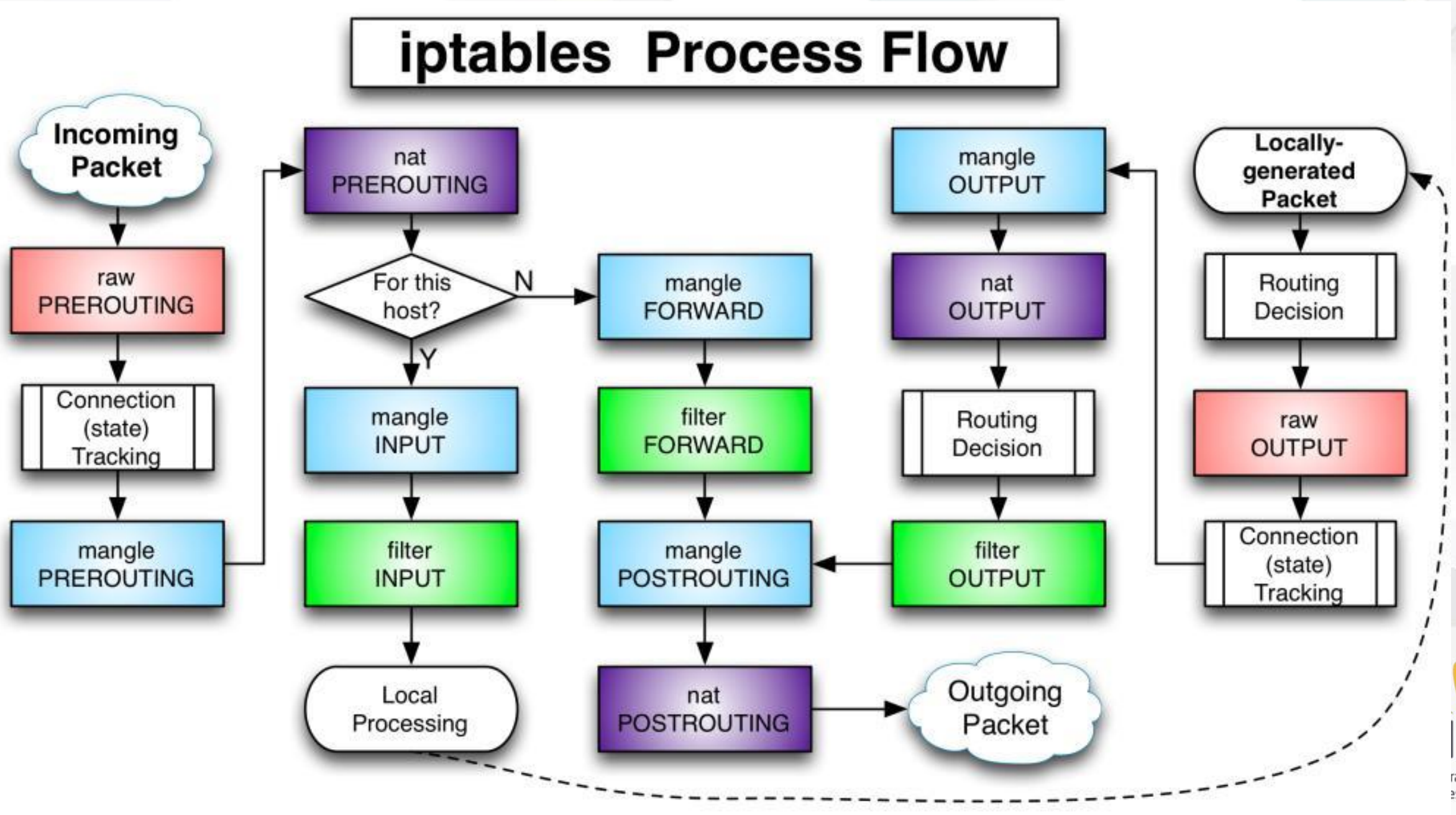
```
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --set
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent
        --update --seconds 60 --hitcount 4 -j DROP
```

NFTABLES

```
chain INPUT {
    type filter hook input priority 0;
    iif eth0  ip tcp dport 22 ct state new, untracked limit rate 4/minutes counter
accept
    counter drop
  }
```

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL



SÉCURITÉ FIREWALL

IPTABLES

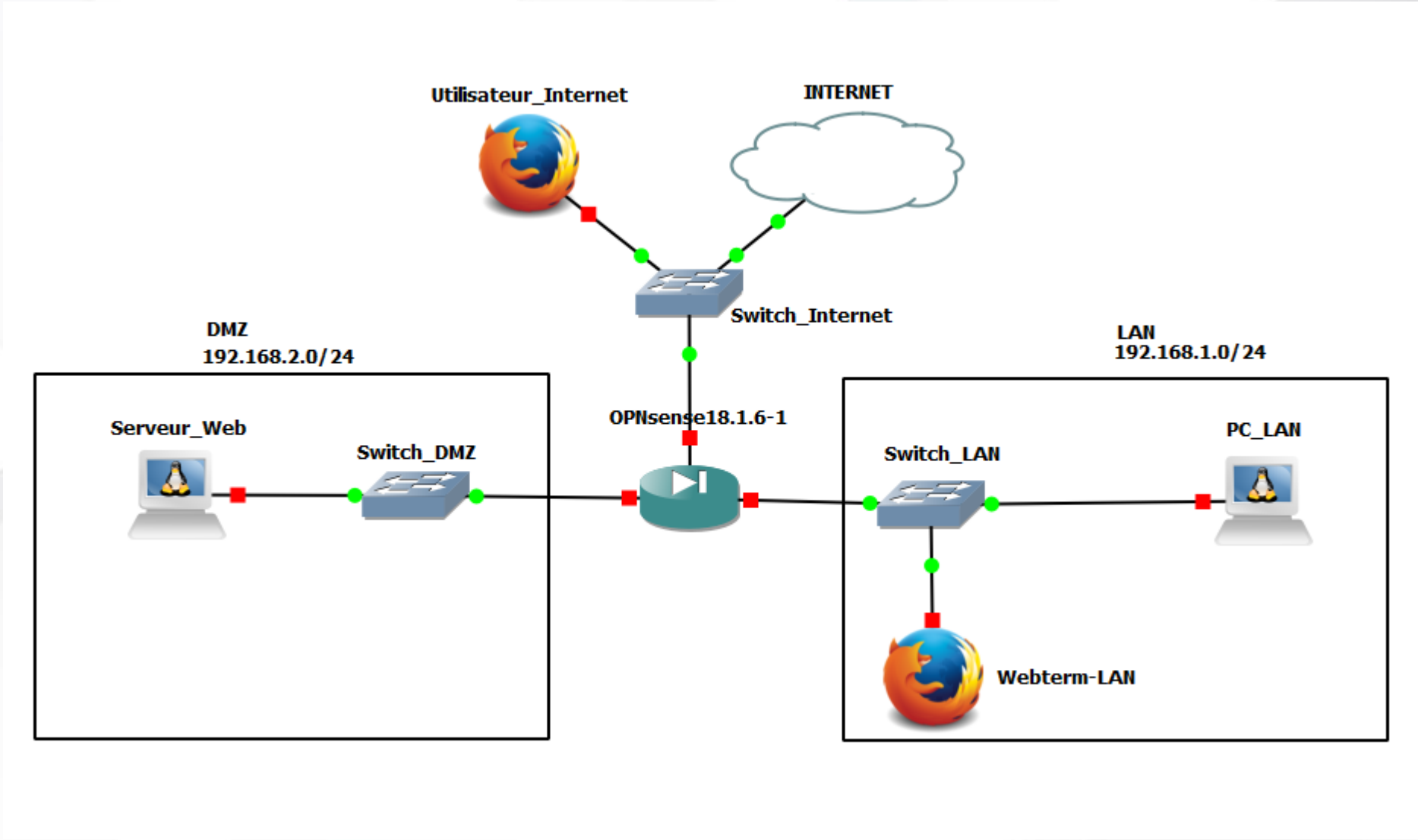
Pour du Niveau 7:

- DPI (Deep Packets Inspection)
  - gourmand en ressource, plus votre connexion Internet est rapide et votre utilisation du DPI grande, plus votre firewall devra être puissant (RAM, CPU, puce ASIC).
- Proxy
  - Cache DNS (dnsmasq, unbound,,,)
  - Cache APT (apt-cache-ng)
  - Squid
  - Olfeo

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

IPTABLES



Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

FAIL2BAN

- Basé sur les logs via des filtres
- Agit sur le Firewall via des actions

- Essentiel car dépend des logs et non du trafic -> Rétroaction

Adista
Opérateur de
Services Hébergés

SÉCURITÉ FIREWALL

NAT

- Translation d'adresse
- !!! Ce n'est pas une sécurité !!!

  - basic-nat-44 (static ipv4 – ipv4)
  - dnat-44 (translate la destination)
  - dynamic-nat-44 (translate la source vers un pool d'adresse)
  - mapt (ipv4 vers ipv6)
  - napt-44 (translate la source vers une ip externe)
  - twice-basic-nat-44 (translate la source et destination en statique)
  - twice-dynamic-nat-44 (translate la source vers un pool d'adresse + destination statique)
  - twice-napt-44 (translate un port vers une ip + destination statique)
  - npt-66 (translate la portion de gauche ipv6)

IPv6

IANA	RIR	LIR	Client	Sous-réseau	Hôte
3 bits	20 bits	9 bits	16 bits	16 bits	64 bits

Chaque utilisateur final se voit attribuer un bloc dont la taille varie de /64 (un seul sous-réseau) à /48 (65 536 sous-réseaux)

Adista
Opérateur de Services Hébergés

Sécurité des Communications

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - DÉFINITIONS

- Cryptologie

  Cette science englobe :

  - la cryptographie : l'écriture secrète
  - la cryptanalyse : l'analyse de cette dernière
  - la stéganographie : l'art de la dissimulation

- Cryptographie
  - La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité)
- Chiffrement
  - Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - DÉFINITIONS

- Chiffrer
  - L'action de procéder à un chiffrement.
- Déchiffrer
  - Consiste à retrouver le texte original (aussi appelé clair) d'un message chiffré dont on possède la clé de (dé)chiffrement.
- Décrypter
  - Décrypter consiste à retrouver le texte original à partir d'un message chiffré sans posséder la clé de (dé)chiffrement.

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - DÉFINITIONS

- Chaînes dites “cryptées”
  - Dans le cadre de la télévision à péage, on parle quasi-exclusivement de chaînes « cryptées », ce que l’Académie Française accepte : « En résumé on chiffre les messages et on crypte les chaînes ».
- Crypter / Cryptage
  - Décrypter n’as pas d’antonyme car il est impossible de créer un message chiffré sans posséder de clé de chiffrement.
- Encrypter / Déencrypter
  - Le terme « encrypter » et ses dérivés sont des anglicismes
- Chiffrage
  - Le chiffrage, c’est évaluer le coût de quelque chose

https://chiffrer.info/

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

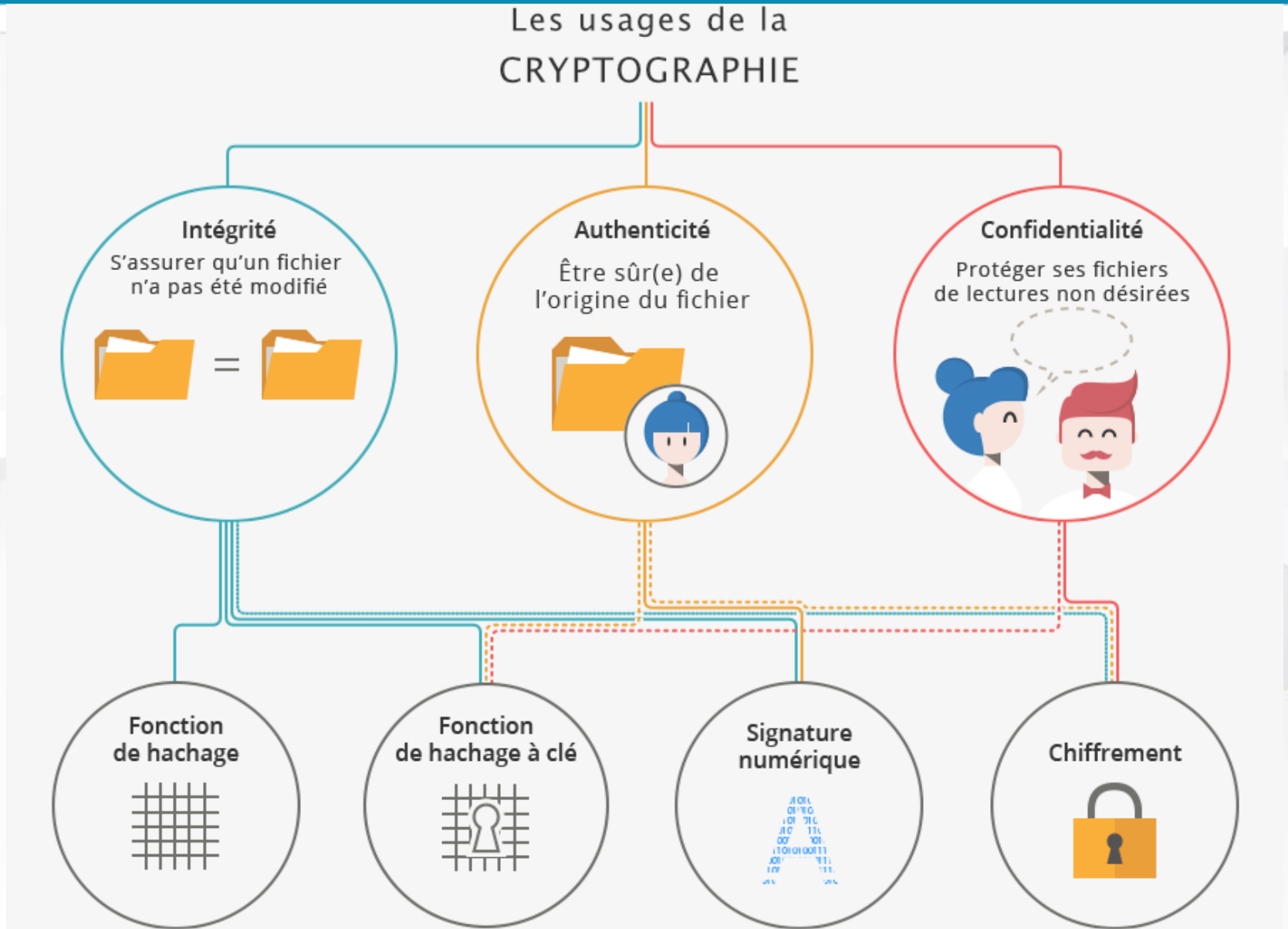
MÉTHODES DE CHIFFREMENT - DÉFINITIONS

- Digital
  - ! Anglissime !
  - On dit « Numérique » !!!!!

https://chiffrer.info/

Adista
Opérateur de Services Hébergés

Introduction



SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT

Objectifs:

- Confidentialité (Chiffrement)
  - Il est impossible d'espionner les informations échangées
- Authentification
  - Il permet de s'assurer de l'identité du programme, de la personne ou de l'entreprise avec laquelle on communique
- Intégrité
  - Il permet de s ’assurer que l’information échangé n’as pas été altéré

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - CONFIDENTIALITÉ

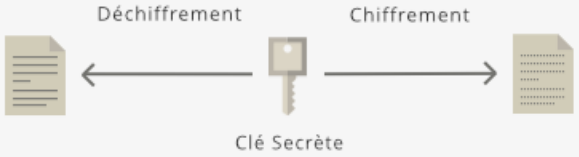
- Le chiffrement d'un message permet justement de garantir que seul l'émetteur et le destinataire légitime d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique.

Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - CONFIDENTIALITÉ



CHIFFREMENT SYMÉTRIQUE

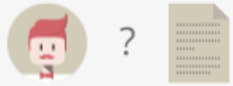
Le chiffrement symétrique permet de chiffrer et déchiffrer un fichier avec la même clé, dite secrète. Pour s'échanger un message il faut donc que les deux parties partagent la même clé.

MISE EN PRATIQUE

Alice vient d'enregistrer la liste des cadeaux de Noël de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accèder.

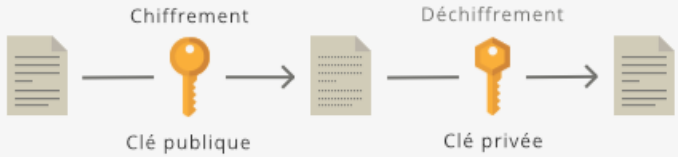
1. Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.

2. Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.



3. Malheureusement pour lui, Bob est incapable de lire la liste car il ne possède pas la clé secrète.

4. La liste est donc bien protégée. Seule Alice peut réussir à la déchiffrer et la lire !



CHIFFREMENT ASYMÉTRIQUE

Le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée.

La clé publique, accessible à tous, est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers, celle-ci étant connue que d'un seul individu.

MISE EN PRATIQUE

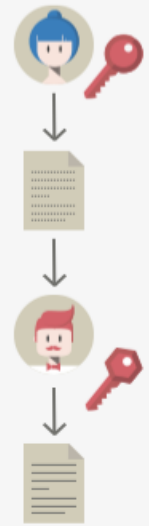
Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1. Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.

2. Elle l'envoie à Bob.

3. Bob reçoit le document et le déchiffre à l'aide de sa clé privée.

4. Une fois le document déchiffré, il rédige un article puis le publie dans son journal.



Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - AUTHENTIFICATION

- Le mécanisme de la **signature** numérique permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ».

Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - AUTHENTIFICATION

SIGNATURE NUMÉRIQUE

Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

Le procédé repose sur un couple de clés : l'une est privée et connue uniquement de son détenteur, l'autre est publique et accessible à tous.

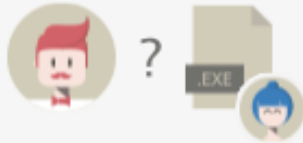
La signature est générée en utilisant la clé privée. La clé publique est utilisée pour vérifier cette signature. Cette vérification peut donc être effectuée par n'importe quelle personne ayant accès à la clé publique.

MISE EN PRATIQUE

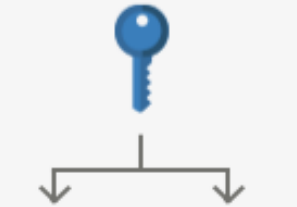
Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

1. Avant de publier librement son logiciel, Alice prend soin de le signer.

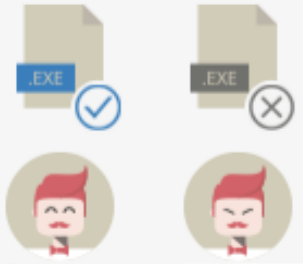
2. Bob vient de télécharger une copie du logiciel mais il veut s'assurer que cette copie provient bien d'Alice.



3. Bob utilise la clé publique d'Alice pour vérifier la signature de la copie.



4. Si la clé reconnait la signature, alors c'est une bonne copie !
Dans le cas contraire, Bob préfère ne pas prendre de risques. Il supprimera la copie.



Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - INTÉGRITÉ

- La cryptologie permet de détecter si le message, ou l'information, a été involontairement modifié.

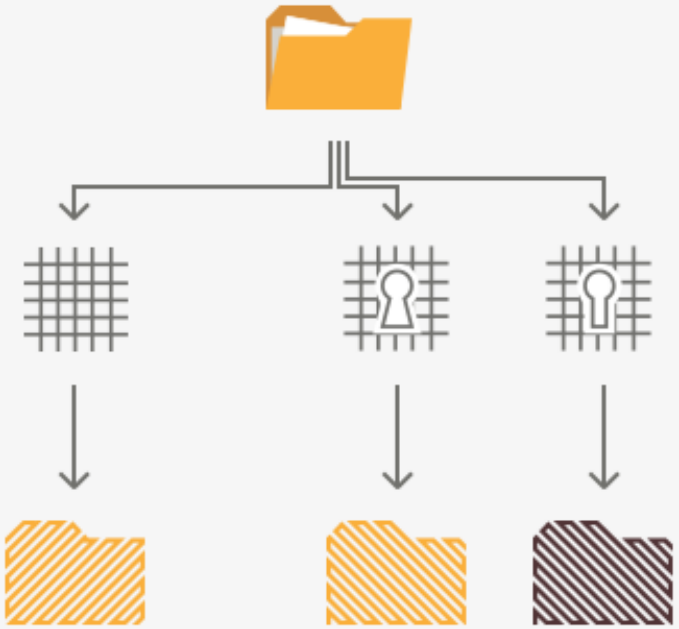
Une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous.

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

Source : https://cnil.fr

MÉTHODES DE CHIFFREMENT - INTÉGRITÉ



FONCTION DE HACHAGE

Une fonction de hachage calcule l'empreinte du document (message, fichier, répertoire) qui lui est passé.

Cette empreinte est une sorte d'identifiant unique du document généré à un moment précis.

FONCTION DE HACHAGE À CLÉ

Les fonctions de hachage à clé sont similaires aux fonctions de hachage, à l'exception du fait qu'une clé secrète est utilisée pour calculer l'empreinte du document.

Un même document peut donc avoir plusieurs empreintes différentes en fonction de la clé secrète utilisée pour les calculer.

MISE EN PRATIQUE

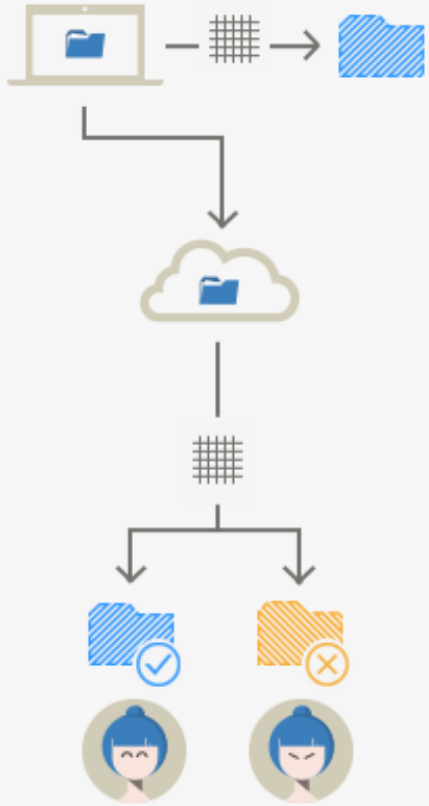
Alice veut charger un de ses fichiers sur le cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.

1. Elle va d'abord calculer l'empreinte du fichier sur son ordinateur.

2. Une fois cela fait, elle charge son fichier sur le cloud.

3. Le fichier chargé, elle calcule alors l'empreinte du fichier transféré.

4. Alice compare les deux fichiers pour savoir si une modification involontaire a eu lieu ou non.



Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT

2 modes de protection :

- Point-à-point (TLS…)

- End-to-End (GPG, OTR…)

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - DÉFINITIONS

- Les algorithmes symétriques:
  - on utilise la même clé C pour encrypter et décrypter.

- Les algorithmes asymétriques (algorithmes à clé publique) :
  - On n'utilise pas la même clé pour chiffrer et déchiffrer

  - Il est impossible de trouver D à partir de E.

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

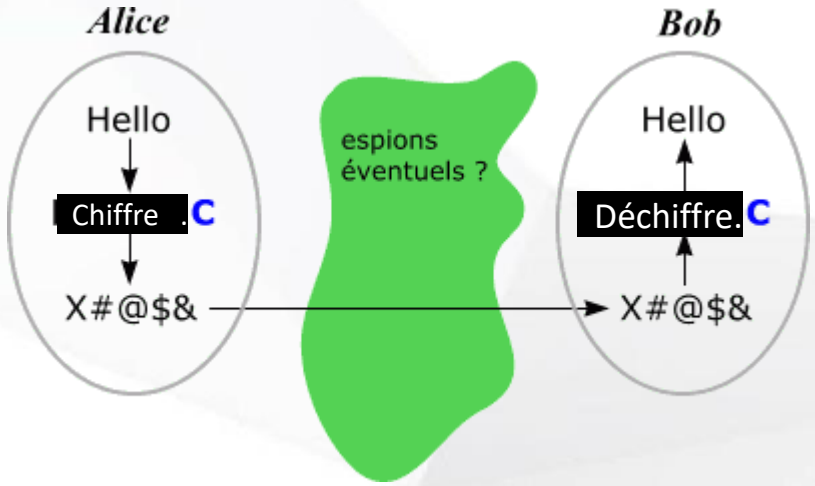
MÉTHODES DE CHIFFREMENT

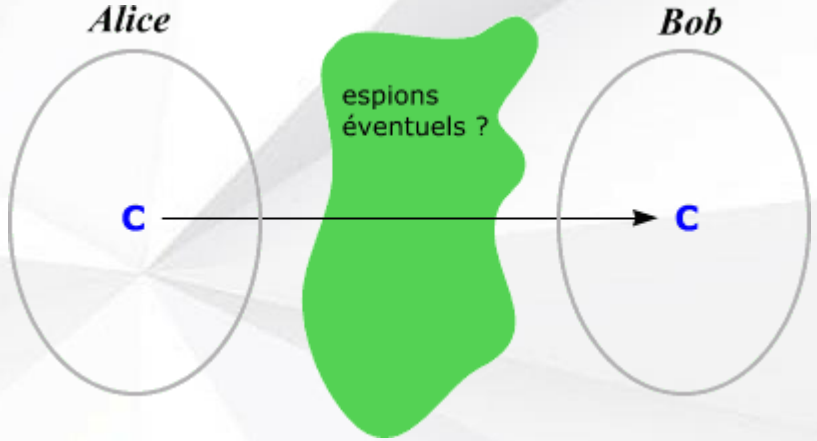
- Les chiffrements symétriques (AES, RC4, DES) sont rapides et supportent les flux mais reposent sur un partage de secret
- Les chiffrements asymétriques (RSA, DSS, ECDSA) sont lents et ne supportent pas les flux mais ne supposent pas une ligne sécurisée

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - SYMÉTRIQUE





Mais comment faire puisque tout le monde peut épier leurs communications et donc connaître aussi **C** ?

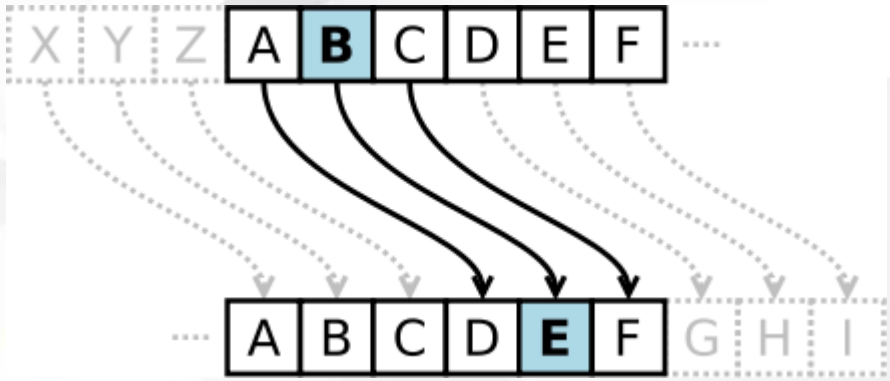
Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT

Examples:

- Chiffrement par décalage (chiffre de César)
  - Décalage des lettres de l'alphabet
  - Rapide
  - Inconvénient:
    - Brut-force
    - Analyse de fréquence



Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT

Exemple:

- Chiffre de substitution par mot-clé
  - Décalage des lettres de l'alphabet
  - Rapide
  - Inconvénient:
    - Analyse de fréquence

ABCDEFGHIJKLMNOPQRSTUVWXYZ
AZERTYUIOPQSDFGHJKLMWXCVBN

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT

Exemple:

- AES (*Advanced Encryption Standard)*

Fondé sur des entrées permutés selon une table définie au préalable, l'algorithme offre des tailles de blocs et de clés qui sont des multiples de 32 (compris entre 128 et 256 bits).

Notion de tour: les différentes opérations peuvent être répétées plusieurs fois. A chaque tour, une clé unique est calculée à partir de la clé de cryptage et incorporée dans les calculs.

- Les entrées permutées empêchent les analyses statistiques
- Les tours empêchent le brut-force rapide

Pour une clé de 128 bits, 2^{128} possibilités

Inconvénient : chaque bloc est toujours chiffré de la même manière

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - SYMÉTRIQUE

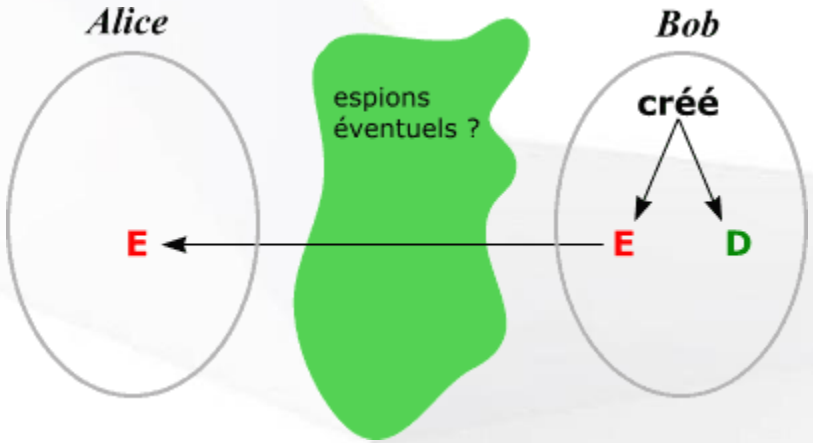
- Avantages:
  - Une clé forte dès le début
  - Une seule méthode de calcul
  - Rapidité des calculs

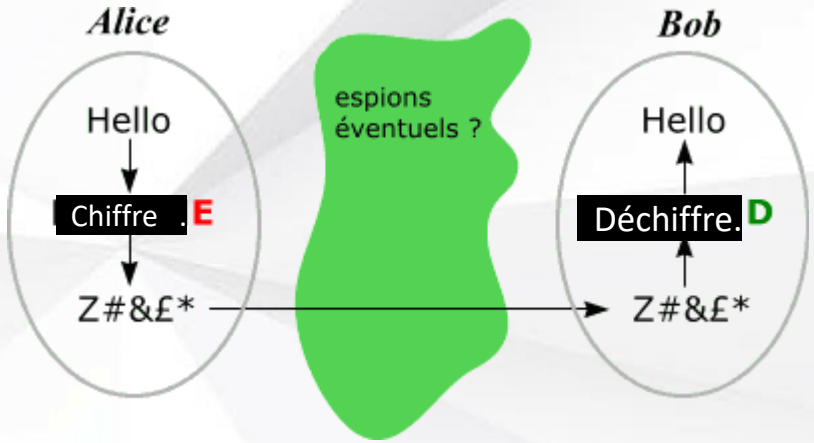
- Inconvénient:
  - Comment se partage-t-on la clé ?

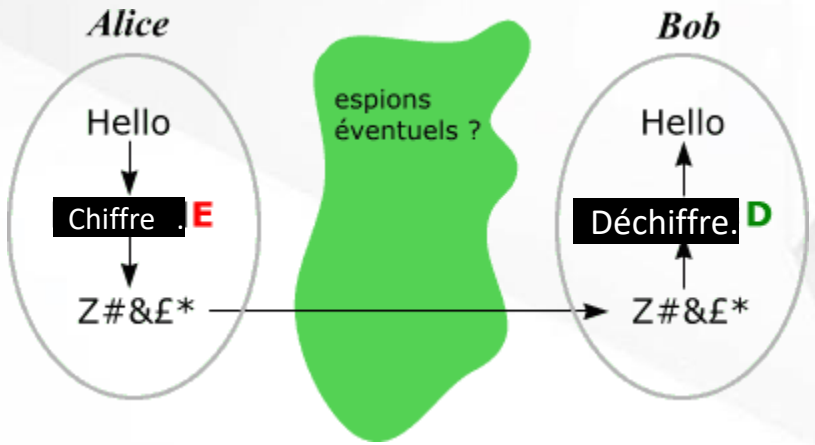
Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE







Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE

- La cryptographie asymétrique à clef publique est fondée sur l'existence des fonctions à sens unique et à brèche secrète.

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE - DIFFIE HELLMAN

Rouge - Privé
Vert - Public

Chez Alice	Publique (internet)	Chez Bob
	p = nombre premier arbitraire **g** = nombre aléatoire inférieur à p	
Ax = nombre aléatoire (privé)		**Bx** = nombre aléatoire (privé)
Ay = g^{Ax} modulo **p**		**By** = g^{Bx} modulo **p**
Ay →		**Ay**
By ←		**By**
s = By^{Ax} modulo **p**		**s** = Ay^{Bx} modulo **p**
	échange de données chiffrées avec **s** ↔	

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE

- Modulo : reste de la division entière.
- **s** est le secret commun d'Alice et Bob.
- Un espion sera incapable de calculer **s** à partir de **p** et **g**, car il ne connait ni le nombre aléatoire **Ax** choisi par Alice, ni le nombre aléatoire **Bx** choisi par Bob. **Ay** et **By** échangés entre Alice et Bob ne l'aideront pas non plus à calculer **s**.

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE - DIFFIE HELLMAN

Exemple Diffie-Hellman

Rouge - Privé
Vert - Public

Chez Alice	Publique (internet)	Chez Bob
	p = 419, nombre premier arbitraire **g** = 7, nombre aléatoire inférieur à p	
Ax = 178, nombre aléatoire (privé)		**Bx** = 344, nombre aléatoire (privé)
Ay = g^{Ax} modulo **p** **Ay** = 7^{178} modulo 419 = 208		**By** = g^{Bx} modulo **p** **By** = 7^{344} modulo 419 = 49
Ay = 208 →		**Ay** = 208
By = 49 ←		**By** = 49
s = By^{Ax} modulo **p** **s** = 49^{178} modulo 419 = 107		**s** = Ay^{Bx} modulo **p** **s** = 208^{344} modulo 419 = 107
	↔ échange de données chiffrées avec **s**	

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE

Diffie-Hellman seul ne suffit pas

Diffie-Hellman permet de créer un secret commun (Confidentialité), il ne permet pas de signer des documents.

Diffie-Hellman est souvent associé à DSS (Digital Signature Standard, un autre algorithme). DSS permet de signer les documents (Intégrité + Authenticité)

On voit donc souvent le sigle DH associé à DSS: DH/DSS.

DH/DSS est l'algorithme par défaut de Gnu Privacy Guard (gpg).

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

MÉTHODES DE CHIFFREMENT - ASYMÉTRIQUE

Exemples:

RSA: factorisation

DSA: logarithme discret

ECDH/ECDSA: Cryptographie sur les courbes elliptiques

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

PROTOCOLES

Applications à des protocoles connus:

- TLS / SSL
- HTTPS
- OpenVPN
- IPSec
- SSH
- Signal Protocol (par Open Whisper Systems)
- GPG

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

PROTOCOLES - HTTPS

HTTP + SSL

- Le SSL utilise:

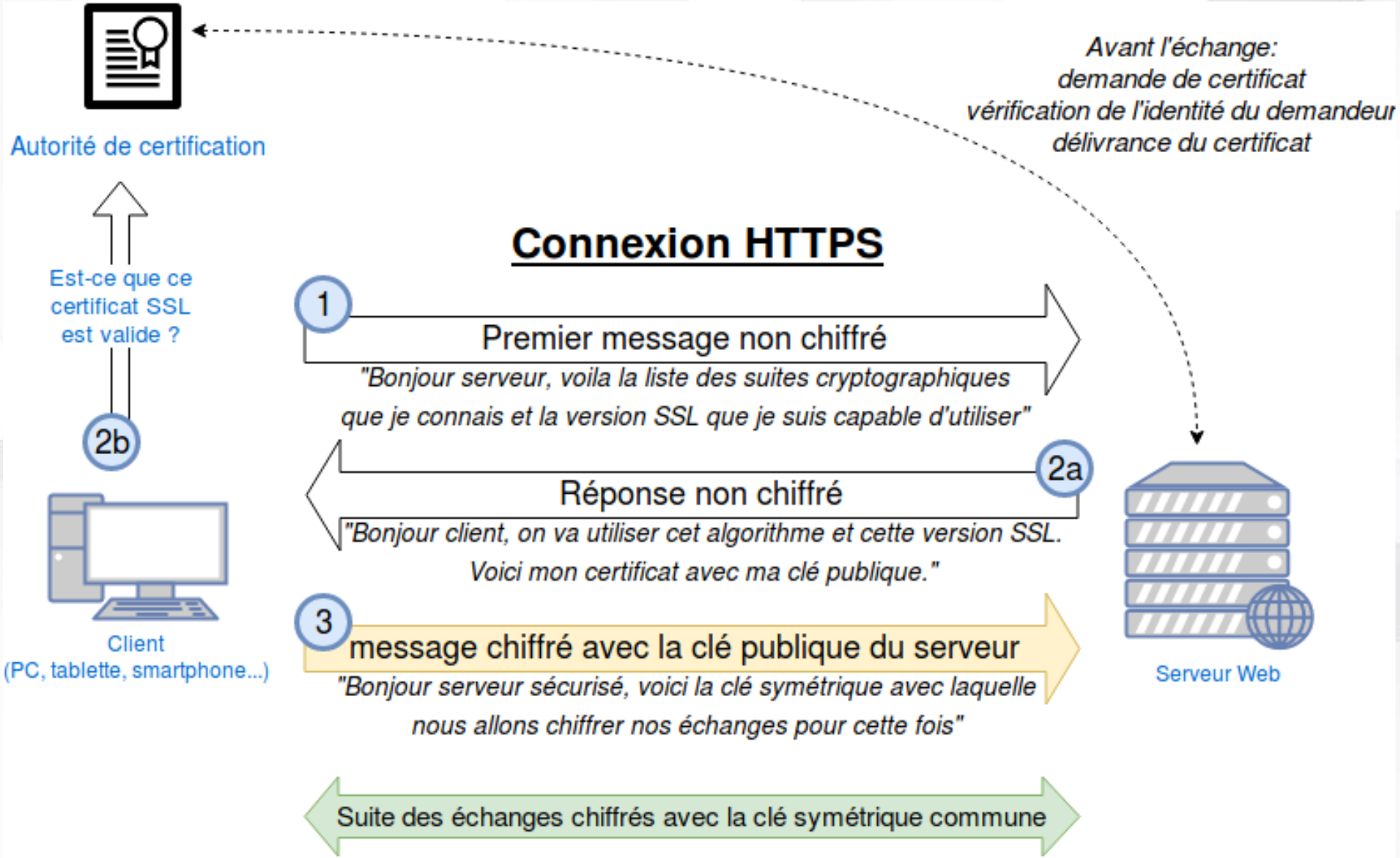
1. chiffrement asymétriques (comme RSA ou Diffie-Hellman). Il est utilisé pour générer la master key (clé principale) qui permettra de générer des clés de session.
2. chiffrement symétrique (AES, IDEA, RC4...) en utilisant les clés de session pour chiffrer les données.
3. signature cryptographique des messages (HMAC, basé sur SHA...) pour s'assurer que les messages ne sont pas corrompus.

C'est lors de la négociation SSL que le client et le serveur choisissent des systèmes communs (chiffrement asymétrique, symétrique, signature et longueur de clé).

Dans votre navigateur, vous pouvez voir la liste des systèmes utilisés en plaçant votre curseur sur le petit cadenas quand vous êtes dans une page en HTTPS.

SÉCURITÉ DES COMMUNICATIONS

PROTOCOLES - HTTPS



Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

PROTOCOLES - HTTPS

Faiblesses:

- TLS est basé sur une chaîne de confiance : Les amis de mes amis sont mes amis.

⇒ Embarqués « en dur » dans le navigateur, 181 dans Mozilla Firefox

- DNS

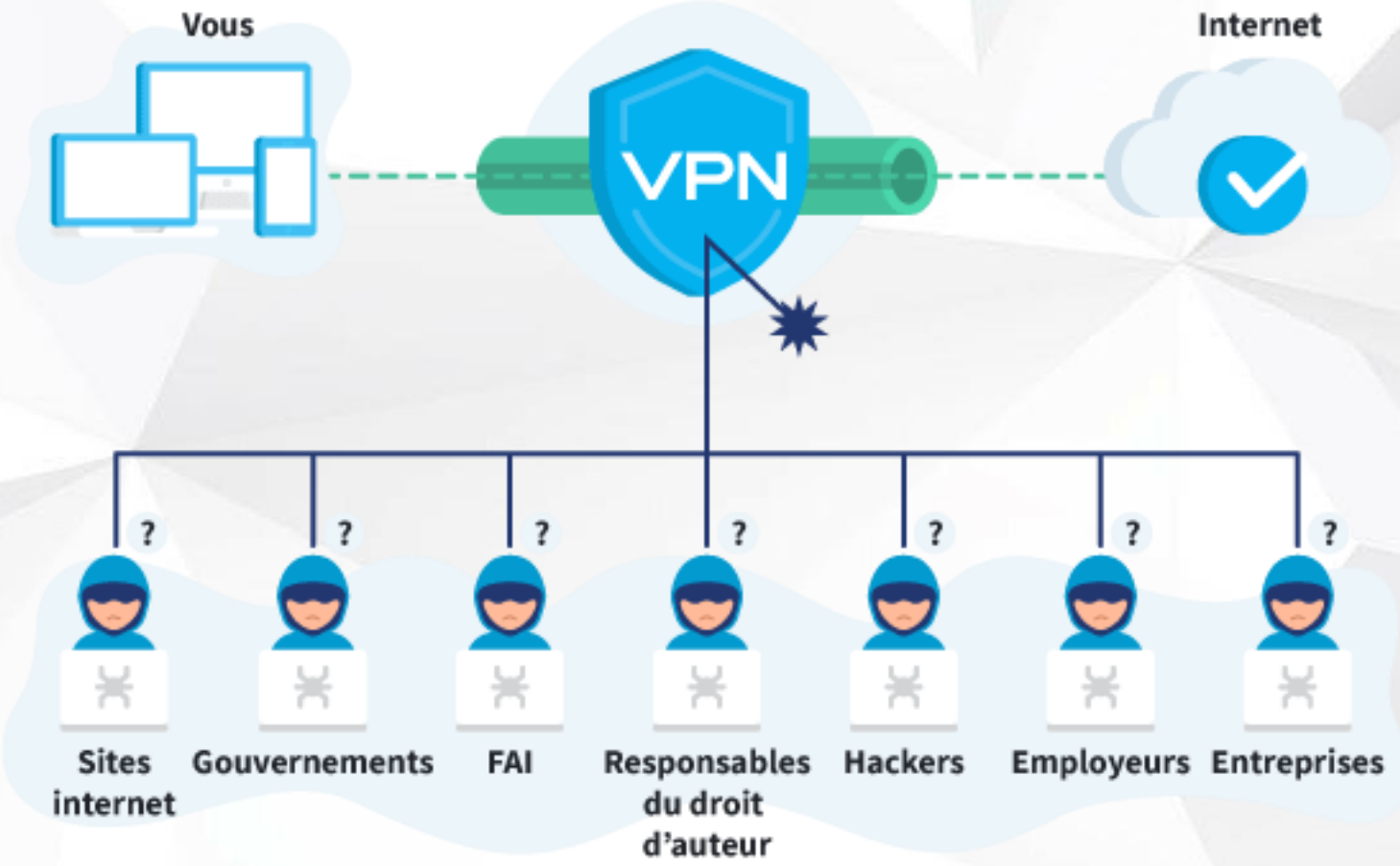
Adista
Opérateur de Services Hébergés

VPN

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

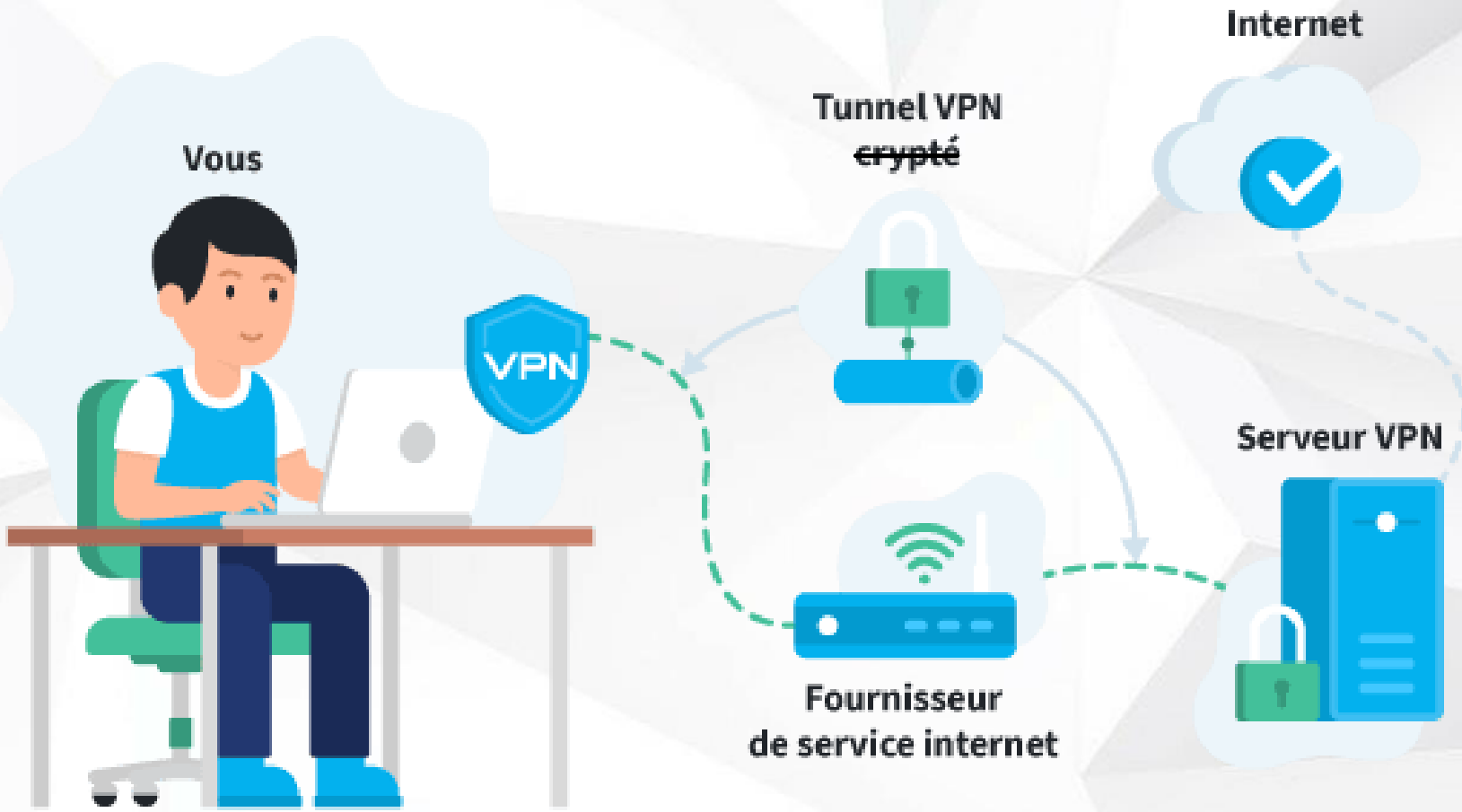
VPN



Adista
Opérateur de Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

VPN



Adista
Opérateur de
Services Hébergés

SSH

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES COMMUNICATIONS

PROTOCOLES - OUTILS

https://tls.imirhil.fr/

https://www.ssllabs.com/ssltest/

https://github.com/arthepsy/ssh-audit

https://ssl-config.mozilla.org/

https://www.cert.ssi.gouv.fr/

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

- N’écoutez que le minimum (ss –tupln)
- Firewall pour limiter les accès
  - NFTables
- Mot de Passe
- On ajoute une rétroaction pour éviter les brutforces

RTFM

Adista
Opérateur de
Services Hébergés

Cybersécurité & cryptographie

Sécurité des données

(Stocker/utiliser une information en toute sécurité)

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

La conservation des mots de passe et autres données sensibles

Définition :

Opinions, conviction, identification, intimité, ce qui peux te nuire, santé

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION - LA LOI

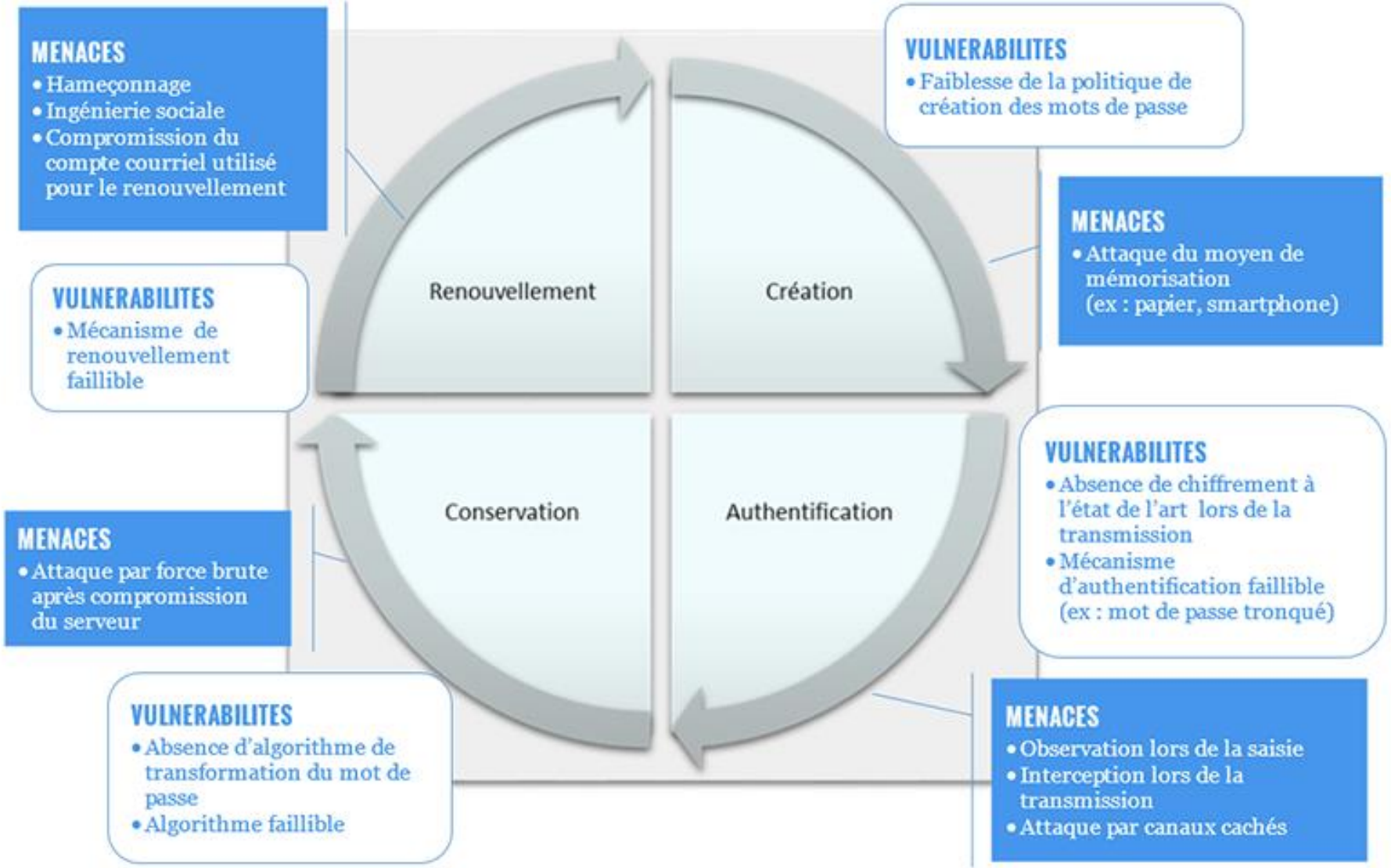
Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée)
- si les informations sont manifestement rendues publiques par la personne concernée
- si elles sont nécessaires à la sauvegarde de la vie humaine
- si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique ou syndicale.

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

UTILISATION PERSONNELLE



Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION - LA LOI

Délibération n° 2017-190 du 22 juin 2017 portant modification de la recommandation relative aux mots de passe :

« S'agissant des modalités de conservation, la commission considère que le mot de passe ne doit jamais être stocké en clair. Elle recommande que tout mot de passe utile à la vérification de l'authentification et devant être stocké sur un serveur soit préalablement transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé. »

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

Fonction cryptographique non réversible:

Le HASH

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION - LE HASH

Définition d'une fonction de hachage:

- il est très difficile de trouver le contenu du message à partir de la signature
- à partir d'un message donné, de sa signature et du code source de la fonction de hachage, il est très difficile de générer un autre message qui donne la même signature
- il est très difficile de trouver deux messages aléatoires qui donnent la même signature (résistance aux collisions).

« très difficile » = « techniquement impossible en pratique »

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

Exemples:

- Taille d'un fichier
- Pixeliser une image
- MD5 (algo sinus + rotation)
- SHA1 (algo vectoriel + addition en boucle)
- SHA256
- SHA512
- SHA3 (algo de Keccak, 2012)

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

Le Hash ne suffit pas:

- 2 mots identique donnent toujours le même résultat, rendant l'attaque par dictionnaire et brute-force accessible.

Ajoutons du SEL

- Ajout d'un mot supplémentaire / action supplémentaire pour brouiller les pistes

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

Résultat : **Fonction de dérivation de clé (**PBKDF2, Bcrypt(blowfish), Argon2)

Exemple : PBKDF2 (Password-Based Key Derivation Function 2)

Mot de passe : moncodetopsecret

Sel : CA7D6F872A1769FBC5F6AF531858287E

Itérations : 1000

Longueur : 32 bytes

Empreinte calculée :

- i3p48N0gGl/bFFtj1lp0HMx7ffRfdMlACHyNS1ugd+4=

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

Exemple:

PHP = password_hash (PASSWORD_DEFAULT)

- Blowfish, Argon2 …

Python = bcrypt.hashpw( )

Java = import javax.crypto.SecretKeyFactory;

import javax.crypto.spec.PBEKeySpec;

Bash = openssl

Adista
Opérateur de
Services Hébergés

SÉCURITÉ ET CRYPTO

UN MDP

Un mot de passe doit :

- Être unique par service
- Ne pas être en lien avec vous
- Ne pas être généré par un tiers
- Ne pas être celui par défaut
- Jamais en clair (bloc-note, post-it)
- Jamais en mail
- Au moins 12 caractères de types différents

Source : https://www.ssi.gouv.fr/administration/guide/mot-de-passe/

Adista
Opérateur de Services Hébergés

SÉCURITÉ ET CRYPTO

UN MDP

Deux méthodes pour choisir vos mots de passe :

- La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
- La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

Adista
Opérateur de
Services Hébergés

SÉCURITÉ ET CRYPTO

UN MDP

Les différentes attaques sur les mots de passe :

- Attaques par force brute
- Attaques par dictionnaires
- Attaques par compromis temps/mémoire (brute force logique avec fonction de réduction)
- Attaques indirecte (phishing…)

Adista
Opérateur de
Services Hébergés

SÉCURITÉ ET CRYPTO

UN MDP

Un gestionnaire de mot de passe:

- Sur tous les terminaux
- Mot de passe solide
- Gestion de droits (en entreprise)
- Accessible facilement + Backup
- ! Attention au Cloud !

Source : https://cnil.fr

Adista
Opérateur de Services Hébergés

SÉCURITÉ ET CRYPTO

UN MDP

KeePass (Kee, KeePass2Android, Keeweb …)

Bitwarden

Laspass (service)

Dashlane (service)

EnPass

Kaspersky Password Manager

Nextcloud, mais celui là, je pourrais le mettre partout

Source : https://cnil.fr

Adista
Opérateur de Services Hébergés

SÉCURITÉ ET CRYPTO

DÉPLOIEMENT ET MAJ

Parlons

- Dockers
- containers (LXC)
- VM
- Mise à jour
- CI/CD
- Versioning de code
- Responsabilité

Source : https://cnil.fr

Adista
Opérateur de Services Hébergés

SÉCURITÉ ET CRYPTO

BACKUP ET REDONDANCE

Raid

- Raid 0
- Raid 10
- Raid 5 - 6

Backup, chiffrement

Redondance de service (VRRP)

Adista
Opérateur de
Services Hébergés

SÉCURITÉ DES DONNÉES

UTILISATION PERSONNELLE

Il faut connaitre ce que l'on veux partager/récupérer comme information.

Choisir le minimum.

Ex: https://exodus-privacy.eu.org/en/

2FA : TOTP

Adista
Opérateur de Services Hébergés

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

La conservation des mots de passe et autre données sensibles

Définition : Les données sensibles forment une catégorie particulière des données personnelles.

Ce sont des informations qui révèlent :

- la prétendue origine raciale ou ethnique
- les opinions politiques
- les convictions religieuses ou philosophiques ou l'appartenance syndicale
- le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique
- des données concernant la santé
- des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

SÉCURITÉ DES DONNÉES

STOCKER UNE INFORMATION

La conservation des mots de passe et autre données sensibles

Définition :

Classification facebook

Adista
Opérateur de
Services Hébergés

800 POSSIBILITÉES DE CIBLAGE

RÉSUMÉ DE CE QUE FACEBOOK SAIT DE VOUS :

- Lieu de résidence
- Âge
- Génération
- Sexe
- Langue maternelle
- Niveau d'éducation
- Champ d'étude
- École
- Affinité ethnique
- Salaire
- Propriétaire ou locataire
- Valeur de la maison
- Taille de la propriété
- L'année de construction de la maison (ceci n'est pas une blague)
- Famille
- Utilisateurs qui ont leur anniversaire dans les 30 jours à venir
- Utilisateurs qui sont éloignés de leur famille ou de leur maison
- Utilisateurs qui ont parmi leurs amis des personnes dont leur anniversaire approche, qui viennent de se fiancer ou de se marier, qui ont déménagé récemment ou dont l'anniversaire est à venir
- Utilisateurs qui ont une relation longue-distance (de n'importe quel type)
- Utilisateurs qui viennent de se mettre en couple
- Utilisateurs qui viennent d'avoir un nouveau boulot
- Utilisateurs qui viennent de se fiancer
- Utilisateurs qui viennent de se marier
- Utilisateurs qui viennent de déménager
- Utilisateurs dont l'anniversaire approche
- Parents
- Futurs parents
- Utilisateurs qui vont probablement s'engager en politique
- Conservateurs et libéraux (US seulement)
- Statut relationnel
- Patron
- Entreprise
- Poste
- Type de travail
- Intérêts
- Utilisateurs qui dispose de motos
- Utilisateurs qui pensent à acheter une voiture (quand/quel type...)
- Utilisateurs qui ont acheté des accessoires de voiture
- Utilisateurs qui ont besoin d'accessoires de voiture
- Style et marque de voiture conduite
- Année d'achat de la voiture
- Âge de la voiture
- Combien d'argent l'utilisateur compte dépenser sur sa future voiture
- Où est-ce que l'utilisateur s'apprête à acheter sa voiture

Adista
Opérateur de Services Hébergés

TP

TP

HTTPS

https://badssl.com/

Pour le compte rendu :

- Certificat expiré
- Clé d’échange diffie-hellman trop petit.
- Mixed Content (avec et sans formulaire)
- Pas de chiffrement (cipher null)
- …

Adista
Opérateur de
Services Hébergés

TP

SSH

Pour le compte rendu :

- Expliquer le message lors d'un clé SSH changé
  - Mauvaise/nouvelle machine
  - Clé renouvelées

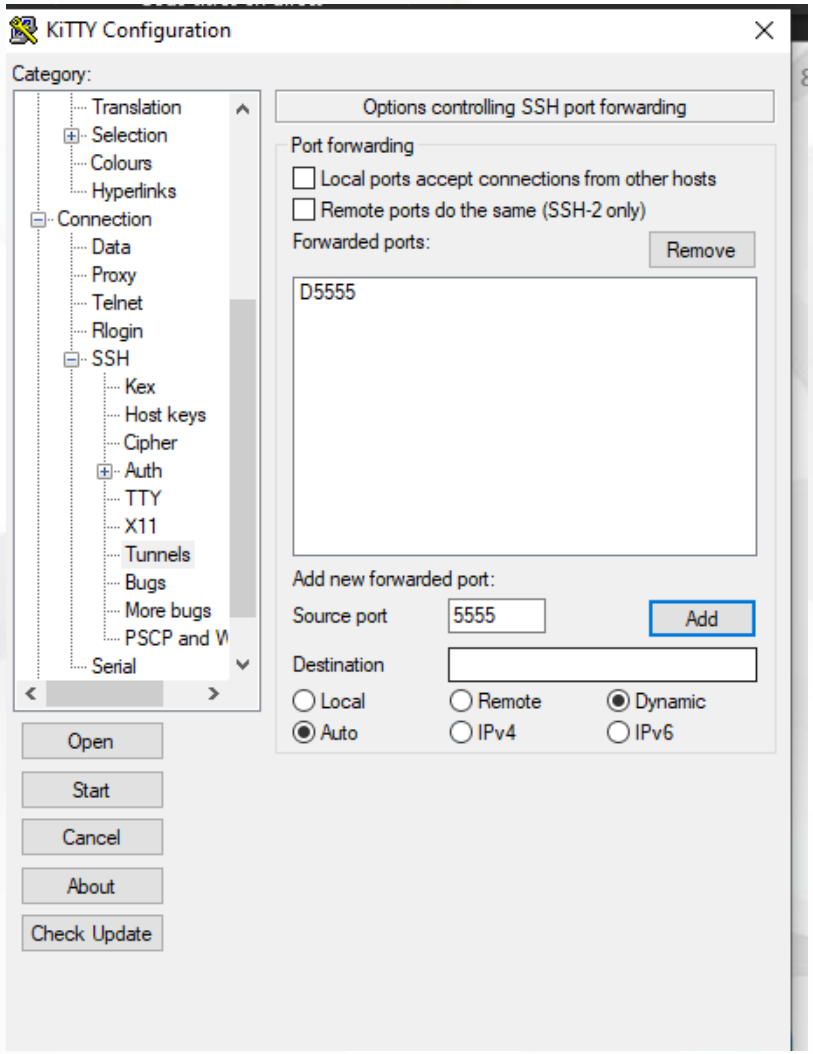
A faire:

- Utiliser votre navigateur via un Proxy socks5
- Configurer une défense face à une attaque (identification par clé/ fail2ban …)

Adista
Opérateur de
Services Hébergés

PROXY SOCKS VERS 192.168.1.46

- Windows



- Unix

Lire le manuell ssh:

ssh -D 5555 login@192.168.1.46 -p 8822

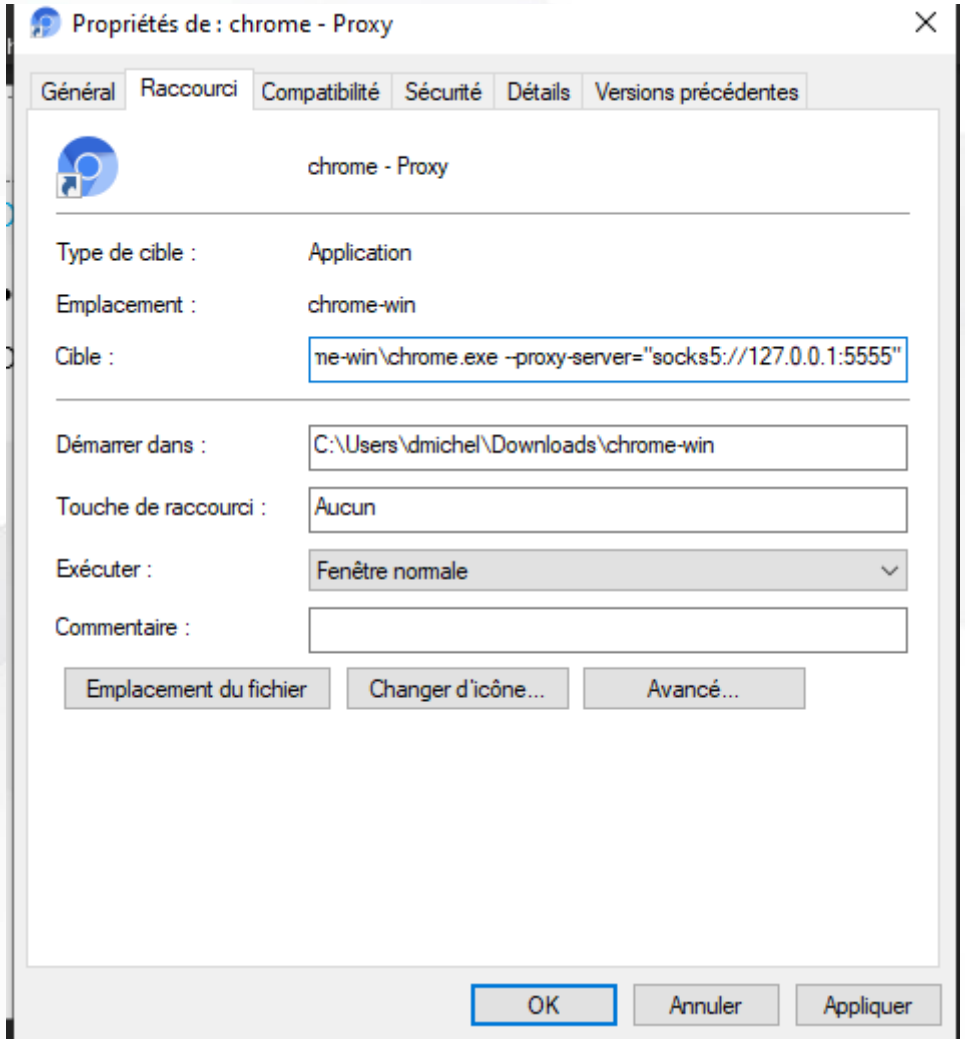
Adista
Opérateur de Services Hébergés

PROXY SOCKS VERS P1855460A.PROBES.ATLAS.RIPE.NET

- Chrom(ium)e

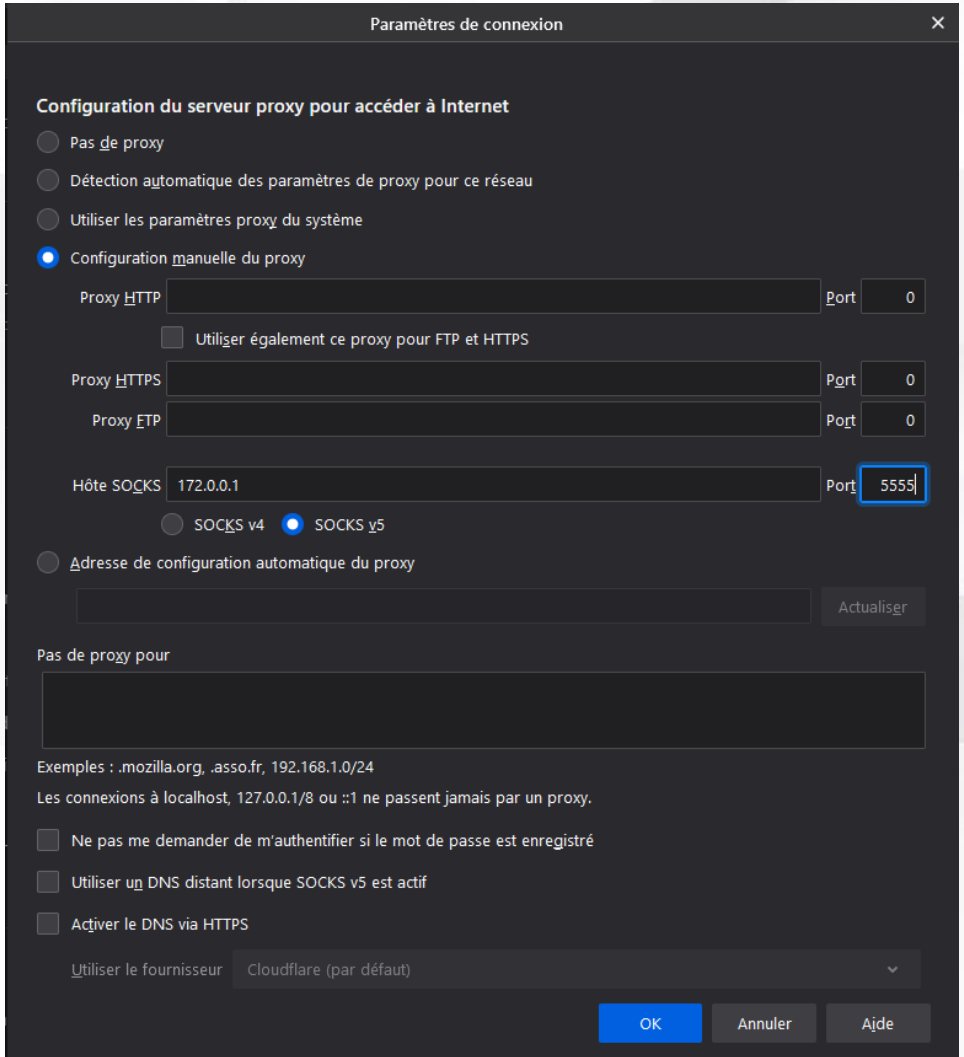
Se créer un raccourci en ajoutant à la cible

--proxy-server="socks5://127.0.0.1:5555"



- Firefox

Dans Général > Paramètres réseaux



Adista
Opérateur de Services Hébergés

TP

CLOUD

Mettre en place son propre Cloud (de type Nextcloud)

- Pas d'auto-intégration (docker)
- 2 machines
  - 1 serveur pour le service cloud + cache
    - Accès SSH + HTTPS depuis l'exterieur (ajouter sécurité)
    - Redirection HTTP vers HTTPS
    - IPTables
  - 1 serveur mutualisé pour la BDD
    - Accès limités + Sécu (script dans le /root)

- Compte rendu :
  - Indiquer la méthode pour prduire le serveur, et surtout, tout ce que vous mettez en place pour le sécuriser

Adista
Opérateur de Services Hébergés

TP

SSH

Optionnel (pour aller plus loin):

- Créer un HoneyPot SSH
  - Cowrie
- Attaque par dictionnaire sur serveur SSH (user:admin)

Adista
Opérateur de
Services Hébergés