

ECOLE EL-BASMA

**Ecole Supérieure en Sciences
Appliquées de Tlemcen**



Sécurité des systèmes informatiques et de l'information

Réaliser par : Mr Bennanni Sid ahmed (CISO)

INTRODUCTION GÉNÉRALE

- Avec l'essor de la transformation numérique, les systèmes d'information sont devenus essentiels, mais aussi vulnérables face aux menaces croissantes comme les cyberattaques et les vols de données.
- Cette formation accélérée en **cybersécurité et en sécurité de l'information** est conçue pour fournir aux ingénieurs IT les bases nécessaires pour sécuriser les infrastructures, protéger les données et identifier les risques.

OBJECTIFS

Objectifs clés :

- Sensibilisation vis-à-vis de l'importance stratégique de la sécurité des systèmes informatiques et réseaux au sein de l'entreprise.
- Comprendre les fondamentaux de la sécurité informatique.
- Reconnaître et anticiper les menaces.
- Comprendre l'importance, le processus et les domaines de l'audit de la SSI.
- Maîtriser les outils et les techniques de sécurité (pare-feu, VPN, best practices, etc.).

Destinée aux professionnels IT, cette formation alterne théorie et pratique pour garantir une application concrète des acquis. Elle prépare les participants à devenir des acteurs clés dans la protection des systèmes critiques de leur organisation.

Bienvenue dans cette formation, où la sécurité devient un levier de progrès

PLAN

1. Sécurité informatique :

- **Définitions** : Concepts clés en cybersécurité.
- **Aspects fondamentaux de la sécurité CIA:**
 - Authentification.
 - Confidentialité.
 - Intégrité.
 - Disponibilité.
- **Concepts liés aux hackers et crackers :**
 - Différence entre hacker (éthique, malveillant) et cracker.
- **Historique :**
 - Exemple du ver d'Internet de 1988.
 - Exemples des années 2010

PLAN

2. Notions de base sur la cryptographie :

- **Introduction :**
 - Qu'est-ce que la cryptographie ?
 - Différence entre cryptographie et stéganographie.
- **Cryptographie ancienne :** Méthodes classiques (chiffre de César, Affine, Vigenère).
- **Cryptographie moderne :**
 - Cryptographie à clé symétrique.
 - Cryptographie à clé publique.
 - Cryptographie avec clé secrète partagée.
 - Cryptographie par clé de session.
 - RSA
 - Cryptographie par courbes elliptiques (ECC).
 - Algorithmes de hashage
 - Signature numérique.
 - Certificats électronique

PLAN

6. Gouvernance de la SSI :

- **La PSSi et l'Audit IT**
- **Gestion des risques**
- **Les 14 domaines de la SSI (ISO27002, RNSI)**

3. Types et exemples d'attaques :

- **Composantes à risque** : Systèmes, réseaux, utilisateurs.
- **Typologie des failles de sécurité** : Vulnérabilités courantes et erreurs humaines.
- **Classification des attaques** :
 - Attaques sur les serveurs (DoS/DDoS, injection SQL).
 - Attaques réseau (MITM, sniffing).
 - Attaques sur les postes de travail (phishing, malware).
- **Types des Malwares**
- **OWASP TOP 10**

PLAN

4. Technologies de sécurité avancées :

- Pare-feu (Firewall)
- Systèmes de détection d'intrusion (IDS/IPS)
- EDR (Endpoint Detection and Response)
- NDR (Network Detection and Response)
- XDR (Extended Detection and Response)
- Passerelles de messagerie sécurisées
- WAF (Web Application Firewall)
- SIEM & SOAR

PLAN

5. Focus sur :

- Réseaux locaux virtuels (VLAN)
- Réseaux privés virtuels (VPN) : IPSEC / SSL
- HTTPS
- WIFI Security
 - Principes de base.
 - Protocoles de sécurité (WPA, WPA2, WPA3).

6. La bonne pratique de la sécurité système et réseau

7. Tools :

- Outils de gestion des réseaux
- Outils d'administration système
- Outils cyber sec
- Liens des services cybersecurité en ligne

CONCEPTS CLÉS EN CYBERSÉCURITÉ.

La sécurité est un aspect important de la stratégie de toute entreprise qui se veut pérenne dans ses activités. Le risque d'incidents ou d'attaques étant plus important avec la digitalisation des processus, il faut adopter des solutions qui assurent la continuité des activités et la reprise après sinistre.

La triade CIA est un modèle de cybersécurité composé de trois principes indispensables à la protection de l'information : **confidentiality, integrity, availability**.

Elle est utilisée par la majorité des entreprises pour mettre en place des **contrôles et des politiques de sécurité efficaces**. Cela leur permet d'avoir les moyens de se défendre contre les différentes menaces comme la fuite de données, les cyberattaques, la compromission des accès, etc.

ASPECTS FONDAMENTAUX DE LA SÉCURITÉ CIA

La **triade CIA** désigne un modèle de sécurité de l'information qui permet d'assurer la sécurité des données d'une organisation ou d'une structure professionnelle. Ces trois principes que sont la **confidentialité**, **l'intégrité** et la **disponibilité** (Confidentiality, Integrity, Availability en anglais) constituent le socle d'une infrastructure protégée efficacement en matière de cybersécurité. En effet, leur application est essentielle à tous programmes de sécurité.

1. **Confidentialité** : ce principe garantit que les informations ne sont accessibles qu'aux personnes ou entités autorisées. Il implique de protéger les données sensibles contre tout accès, divulgation ou exposition non autorisés. Des mesures telles que le cryptage, les contrôles d'accès et l'authentification des utilisateurs sont utilisées pour maintenir la confidentialité.
2. **Intégrité** : l'intégrité se concentre sur l'exactitude et la fiabilité des données et des systèmes. Elle garantit que les données ne sont pas altérées, modifiées ou compromises de quelque manière que ce soit. Le maintien de l'intégrité des données est essentiel pour garantir que les informations restent fiables et exactes. Des techniques telles que le hachage des données, les signatures numériques et le contrôle des versions permettent de vérifier l'authenticité des données et de les protéger contre les modifications.

ASPECTS FONDAMENTAUX DE LA SÉCURITÉ CIA

3. Disponibilité : la disponibilité garantit que les systèmes et les données sont accessibles et fonctionnels lorsqu'ils sont nécessaires. Les efforts de cybersécurité visent à prévenir ou à atténuer les interruptions, les temps d'arrêt ou les attaques par déni de service qui pourraient rendre les systèmes inaccessibles. Des systèmes de redondance, de sauvegarde et des plans de reprise après sinistre sont mis en place pour assurer une disponibilité continue.



4. Authenticité : L'authenticité implique de vérifier l'identité des utilisateurs, des systèmes ou des sources de données pour s'assurer qu'ils sont authentiques et non usurpés. Des méthodes d'authentification telles que les mots de passe, la biométrie et l'authentification multifactorielle sont utilisées pour établir la confiance dans les interactions numériques. L'authenticité permet d'empêcher tout accès non autorisé et toute activité frauduleuse.

5. Non-répudiation : La non-répudiation garantit qu'une partie impliquée dans une transaction numérique ne peut pas nier son implication ou l'authenticité de ses actions. Les signatures numériques et les journaux d'audit jouent un rôle important dans la non-répudiation. Ce concept est particulièrement important dans les contextes juridiques et financiers, où la preuve des transactions et des accords est essentielle pour résoudre les litiges et établir la responsabilité.

HACKERS VS CRACKERS

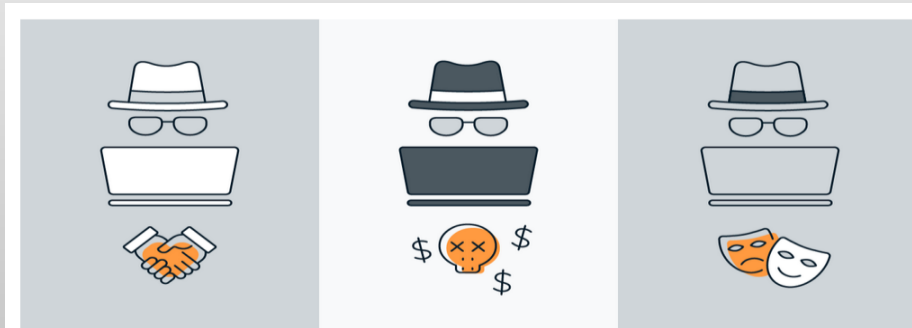
Pirates informatiques : les pirates informatiques légaux et éthiques protègent généralement les données et ne les volent ni ne les endommagent jamais . Leur seul but est d'obtenir des informations à partir des données et des informations pertinentes.

Crackers : d'un autre côté, les pirates informatiques volent, suppriment ou endommagent généralement les données qu'ils trouvent à partir des vulnérabilités du système.

HACKER	V/S	CRACKER
		
<ul style="list-style-type: none">• NEVER DAMAGE THE DATA.• THE ETHICAL PROFESSIONALS.• HACKERS HAVE LEGAL CERTIFICATES.• GOOD PEOPLE, HACK FOR KNOWLEDGE PURPOSES.		<ul style="list-style-type: none">• DELETE OR DAMAGE THE DATA.• UNETHICAL PERSON ,DO ILLEGAL TASKS.• MOTIVE IS TO STAY ANONYMOUS.• EVIL PERSON WHO BREAKS INTO A SYSTEM FOR BENEFITS.

HACKERS

- **Les hackers noirs** sont des cybercriminels qui cassent illégalement des systèmes à intention malveillante. Une fois qu'un hacker noir trouve une vulnérabilité de sécurité, ils essaient de l'exploiter, souvent en implantant un virus ou un autre type de logiciel malveillant tel qu'un cheval de Troie. Les attaques de ransomware sont un autre stratagème préféré que les pirates de chapeau noir utilisent pour extorquer des gains financiers ou des systèmes de données de violation.
- **Les hackers blancs**, également connus sous le nom de hackers de sécurité éthique, identifient et corrigent les vulnérabilités. Le piratage des systèmes avec l'autorisation des organisations dans lesquelles ils piratent, les pirates blancs tentent de découvrir les faiblesses du système afin de les résoudre et d'aider à renforcer la sécurité globale d'Internet.
- **Les pirates de la bonne humeur grise** peuvent ne pas avoir l'intention criminelle ou malveillante d'un pirate de chapeau noir, mais ils n'ont pas non plus la connaissance ou le consentement préalable de ceux dont ils piratent les systèmes. Néanmoins, lorsque les pirates du chapeau gris découvrent des faiblesses telles que les vulnérabilités zéro jour, ils les signalent plutôt que de les exploiter pleinement. Mais les pirates de chapeau gris peuvent exiger le paiement en échange de fournir des détails complets sur ce qu'ils ont découvert.



HISTORIQUE : VER INTERNET 1988

Le 2 novembre 1988, Robert Tappan Morris, étudiant en informatique, mit en circulation ce qui a été appelé plus tard le ver de Morris et qui causa le crash d'un très grand nombre d'ordinateurs sur Internet. Quant à Morris, il est la première personne condamnée en vertu de la loi américaine sur les fraudes et les abus (Computer Fraud and Abuse)

Le ver Morris ne fut pas écrit pour causer des dommages mais pour se propager. Des erreurs dans le code l'ont toutefois rendu plus dangereux : un ordinateur pouvait être infecté plus d'une fois et chaque processus additionnel ralentissait la machine au point de la rendre inutilisable.

Le ver Morris exploitait deux vulnérabilités connues dans sendmail, fingerd, et dans la faiblesse de mots de passe de certains utilisateurs. La faille de sendmail se situait dans la possibilité, en mode 'DEBUG', d'envoyer des fichiers sur une machine distante en utilisant un shell. Ce shell était utilisé pour compiler le code source envoyé. Ce programme une fois compilé était alors en mesure de tenter de se propager à d'autres machines.

La deuxième faille utilisée était un dépassement de tampon de l'utilitaire finger initialement conçu pour connaître à distance l'heure de connexion d'un utilisateur sur un poste. Ce bug permettait au ver de prendre le contrôle et d'utiliser les accès réseau de l'utilitaire pour se connecter à des machines distantes, et d'y migrer comme avec sendmail. Enfin, la troisième technique de propagation profitait des mots de passe faibles des utilisateurs des systèmes pour se copier sur des machines distantes avec les commandes rsh et rexec.

Une des **défenses** les plus simples contre ce ver était la création du répertoire /usr/tmp/sh. En effet, le ver utilisait le fichier sh du répertoire /usr/tmp/ pour se propager, et était bloqué lorsque ce chemin était déjà utilisé.

La faille de sendmail nécessitait de patcher l'application pour supprimer l'option 'DEBUG'.

HISTORIQUE

○ **Années 2000 : Montée en puissance**

- **2000 : Attaque DDoS de Mafiaboy**

- Un adolescent canadien a lancé des attaques DDoS contre des géants comme Amazon, eBay et CNN, rendant ces sites indisponibles pendant plusieurs heures.

- **2004 : Le virus MyDoom**

- L'un des vers les plus rapides à se propager, causant des milliards de dollars de dommages en ralentissant massivement Internet.

○ **Années 2010 : Professionnalisation des attaques**

- **2010 : Stuxnet**

- Un ver informatique sophistiqué conçu pour cibler les installations nucléaires iraniennes.
- Première cyberattaque connue liée à un sabotage industriel.

- **2013 : Piratage de Yahoo**

- Vol massif de données affectant 3 milliards de comptes.
- Considéré comme l'une des plus grandes violations de données de l'histoire.

- **2017 : WannaCry**

- Rançongiciel exploitant une vulnérabilité de Windows.
- A paralysé des organisations, notamment le NHS (service national de santé britannique).

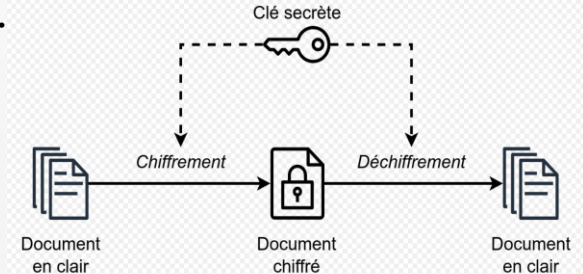
- **2017 : NotPetya**

- Rançongiciel déguisé en logiciel légitime, causant des pertes estimées à 10 milliards de dollars.
- Vise des entreprises internationales, notamment Maersk et FedEx.

CRYPTO

La **cryptographie** est la pratique de la protection des informations par l'utilisation d'algorithmes chiffrés, de hachages et de signatures.

La **cryptographie** est le processus qui consiste à cacher ou à coder des informations de manière à ce que seule la personne à laquelle un message est destiné puisse le lire. L'art de la cryptographie est utilisé pour chiffrer des messages depuis des milliers d'années et continue d'être utilisé dans les cartes bancaires, les mots de passe et le commerce électronique.



Alors que la **cryptographie** laisse le message visible mais le rend illisible à quiconque ne possède pas la clé de déchiffrement, la **stéganographie** consiste à rendre ce message quasi invisible aux yeux de tous.

La **stéganographie** est une étape supplémentaire qui peut être utilisée en conjonction avec le chiffrement afin de dissimuler ou de protéger des données. La **stéganographie** est un moyen de dissimuler des informations secrètes dans (ou même au-dessus) d'un document ou d'un autre support banal et non secret afin d'éviter toute détection.

CRYPTOGRAPHIE ANCIENNE : MÉTHODES CLASSIQUES

- Le **chiffre de César** est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une substitution mono-alphabétique. Chaque lettre est **remplacée**, c'est à dire **substituée**, par une seule et même lettre tout au long du texte.

CLAIR A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ici, il y a un décalage de trois lettres.

CODE D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

exemple : d'après cette méthode, "VIVE LES MATHS" devient donc "YLYH OHV PDWKV" !

- Le **chiffrement par substitution** est un chiffrement utilisé depuis bien longtemps, le chiffrement de César en fait partie. Cette méthode consiste à remplacer une lettre du texte, ou du message, à coder par une autre : exemple A par F. Sans clé particulière. (sans décalage de lettre définie, comme le code de César)

CRYPTOGRAPHIE ANCIENNE : MÉTHODES CLASSIQUES

- Le **chiffrement de Vigenère** est un système de chiffrement **polyalphabétique**. C'est un chiffrement par **substitution**, mais une même lettre du message clair peut être remplacée par des lettres différentes suivant sa position dans le texte.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Le **chiffrement affine** consiste à remplacer chaque lettre de l'alphabet A, B...Z par son rang entre 0 et 25 (A=0 jusqu'à Z=25) grâce à une fonction affine. On choisit deux nombres entiers **a** et **b** compris entre 0 et 25. On nomme **x** le rang de la lettre et **r(x)** le reste de la division euclidienne de **y=ax+b** par **26**. R(x) est alors le rang codé de la lettre. Chaque lettre est toujours codée par la même lettre ce qui signifie que c'est un chiffrement par substitution mono-alphabétique.

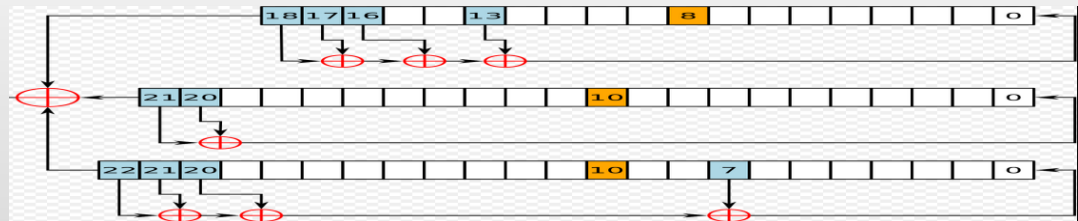
Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

CRYPTOGRAPHIE MODERNE : CHIFFREMENT PAR FLUX

La cryptographie entre dans son ère **moderne** avec l'utilisation intensive des ordinateurs. Dans la cryptographie moderne, on utilise aussi des **problèmes mathématiques** que l'on ne sait pas (encore) résoudre, par exemple **factoriser des grands nombres** (chiffre RSA)

○ **Le chiffrement de flux**, chiffrement par flot ou chiffrement en continu (en anglais stream cipher) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique, l'autre étant le chiffrement par bloc. Un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper. Une liste non exhaustive de chiffrements par flot :

- E0 utilisé par le protocole Bluetooth.
- RC4, le plus répandu, conçu en 1987 par Ronald Rivest, utilisé notamment par le protocole WEP du Wi-Fi ;Py, un algorithme récent de Eli Biham.
- A5/1, algorithme publié en 1994, utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche.



Un chiffrement par flux se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données.

CRYPTOGRAPHIE MODERNE : PAR BLOC / ASYMÉTRIQUE

○ Le chiffrement par Bloc :

Les algorithmes de chiffrement par bloc, pour la plupart basés sur des réseaux fiestel, sont actuellement les algorithmes à clef secrète les plus courants. Cependant, depuis l'invention du DES en 1977, la puissance de calcul des ordinateurs a incroyablement progressé, si bien que la longueur des clefs est maintenant insuffisante. L'AES (Advanced Encryption Standard) est destiné à prendre la relève du DES, réputé peu sûr depuis quelques années.

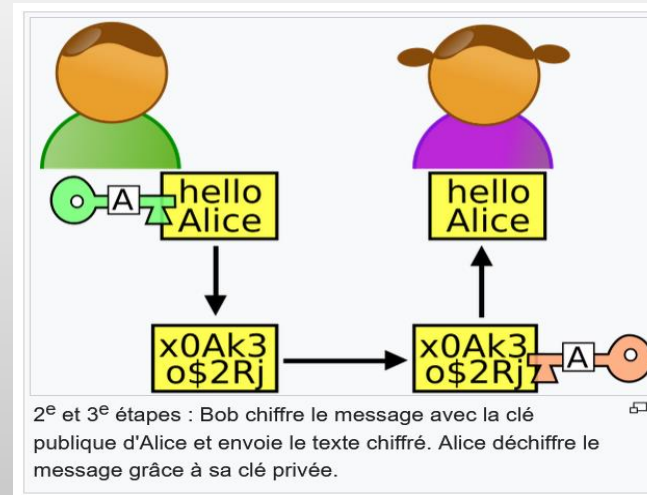
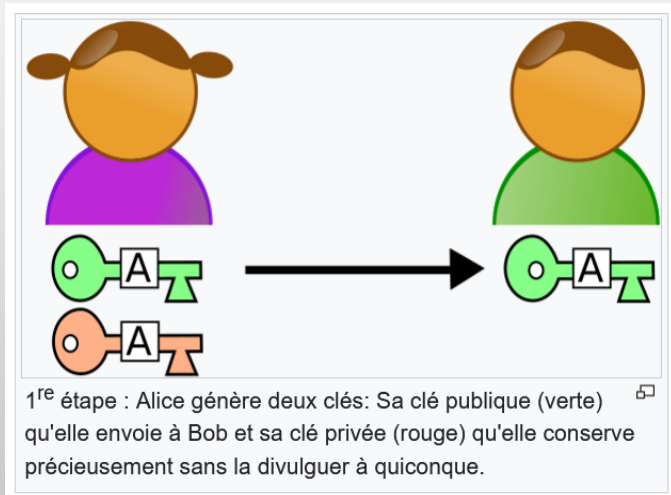
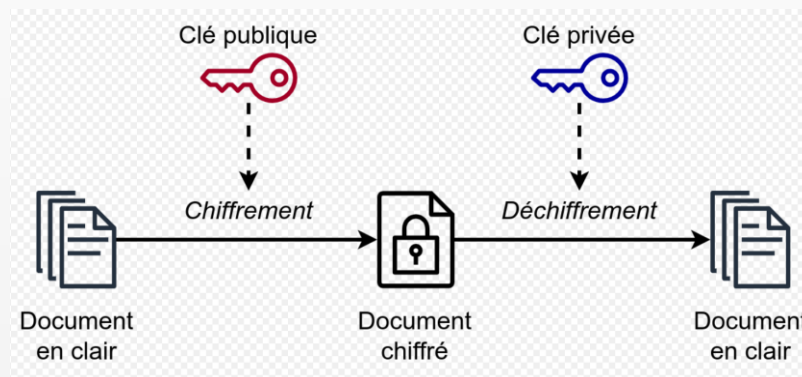
- Data Encryption Standard (DES), l'ancêtre conçu dans les années 1970
- Advanced Encryption Standard (AES), ou algorithme Rijndael (terme construit à partir d'une partie du nom de chacun de ses créateurs belges, Vincent Rijmen et Joan Daemen)
- Blowfish, Serpent et Twofish, sont des alternatives à AES

○ Les systèmes à clefs publiques

Depuis les origines de la cryptographie, et jusqu'à récemment, tous les procédés étaient basés sur une même notion fondamentale: chaque correspondant était en possession d'une **clef secrète**, qu'il utilisait pour chiffrer et déchiffrer. Cela a un inconvénient majeur: **comment communiquer la clef au correspondant?**

CRYPTOGRAPHIE MODERNE : CHIFFREMENT ASYMÉTRIQUE

La **cryptographie asymétrique**, ou cryptographie à clé publique elle permet d'assurer la confidentialité d'une communication, ou d'authentifier les participants, sans que cela repose sur une donnée secrète partagée entre ceux-ci, contrairement à la cryptographie symétrique qui nécessite ce secret partagé préalable.



CRYPTOGRAPHIE AVEC CLÉ SECRÈTE PARTAGÉE

La **cryptographie avec clé secrète partagée** repose sur l'utilisation d'une même clé (symétrique) pour chiffrer et déchiffrer les données. Elle appartient à la cryptographie **symétrique**, où la clé est connue uniquement par les deux parties communicantes.

○ **Caractéristiques :**

- **Rapidité** : Très efficace en termes de performances, adaptée aux grandes quantités de données.
- **Simplicité** : L'algorithme est généralement moins complexe que dans la cryptographie asymétrique.
- **Risque principal** : La sécurisation et l'échange de la clé secrète entre les parties sont critiques.

○ **Exemples d'algorithmes :**

- **AES (Advanced Encryption Standard)** :
 - Longueur de clé : 128, 192 ou 256 bits.
 - Utilisé pour des applications modernes (HTTPS, VPN, chiffrement de fichiers).
- **3DES (Triple Data Encryption Standard)** :
 - Version renforcée de DES.
 - Utilisation déclinante à cause de sa lenteur et de sa sécurité inférieure à AES.

○ **Protocole d'échange sécurisé de clé :**

Les clés doivent être échangées via un canal sécurisé ou à l'aide d'un protocole comme **Diffie-Hellman (DH)** ou **Elliptic Curve Diffie-Hellman (ECDH)**.

CRYPTOGRAPHIE PAR CLÉ DE SESSION

Une **clé de session** est une clé symétrique temporaire générée pour sécuriser une session de communication spécifique. Elle est utilisée uniquement pendant la durée de la session.

- **Utilisation principale :** La clé de session est couramment utilisée dans les protocoles de chiffrement hybrides comme **TLS/SSL** :
 - La clé de session est échangée à l'aide de cryptographie asymétrique (ex. RSA).
 - Les données de la session sont ensuite chiffrées avec la clé symétrique pour des raisons de performance.
- **Exemple dans TLS :**
 - **Handshake initial :**
Le client génère une clé de session et l'envoie au serveur après chiffrement via RSA ou Diffie-Hellman.
 - **Chiffrement symétrique :**
La clé de session est utilisée pour le chiffrement symétrique (AES).
 - **Destruction après la session :**
Une fois la session terminée, la clé est supprimée pour éviter tout risque de réutilisation ou de compromission.
- **Avantages :**
 - **Sécurité accrue :** Même si une clé de session est compromise, cela n'impacte que la session en cours.
 - **Performance optimisée :** Permet de combiner les avantages de la cryptographie asymétrique et symétrique.

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

- RSA est un algorithme de cryptographie asymétrique largement utilisé pour le chiffrement, la signature numérique et l'échange sécurisé de clés. Il repose sur la difficulté de factoriser de grands nombres premiers, ce qui garantit sa sécurité.
- Développé en 1977 par **Ron Rivest, Adi Shamir et Leonard Adleman**.
- RSA est basé sur la cryptographie asymétrique, utilisant une paire de clés :
 - Une **clé publique** pour chiffrer les messages ou vérifier les signatures.
 - Une **clé privée** pour déchiffrer les messages ou générer des signatures.

2. Principe de fonctionnement :

RSA repose sur trois concepts fondamentaux :

- **Génération de clés** (Clé publique et privée).
- **Chiffrement** (avec la clé publique).
- **Déchiffrement** (avec la clé privée).

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

3. Étapes Techniques :

a. Génération des clés

- **Choix de deux grands nombres premiers :**
p et q, chacun très grand (au moins 1024 bits aujourd'hui).
- **Calcul du produit n :**
 $n = p \times q$
n est utilisé comme **modulo** pour les opérations de chiffrement/déchiffrement.
n doit être suffisamment grand pour garantir la sécurité.
- **Calcul de $\phi(n)$:**
 $\phi(n) = (p-1) \times (q-1)$ (fonction indicatrice d'Euler).
- **Choix d'un exposant public e :**
e doit être un entier tel que $1 < e < \phi(n)$ et copremier avec $\phi(n)$.
Par convention, on utilise souvent $e=65537$, car il est efficace pour les calculs et garantit une bonne sécurité.
- **Calcul de l'exposant privé d :**
d est l'inverse modulaire de e modulo $\phi(n)$, soit : $e \times d \bmod \phi(n) = 1$
- **Clés générées :**
Clé publique : (e,n)
Clé privée : (d,n).

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

b. Chiffrement

Le message M (converti en entier, $M < n$) est chiffré avec la clé publique (e, n) : $C = M^e \bmod n$ où :

C est le **texte chiffré**.

c. Déchiffrement

Le texte chiffré C est déchiffré avec la clé privée (d, n) : $M = C^d \bmod n$ où :

M est le **message en clair** récupéré.

d. Signature numérique

Génération de la signature :

L'expéditeur utilise sa **clé privée** pour signer un message M .

Signature S : $S = M^d \bmod n$

Vérification de la signature :

Le destinataire utilise la **clé publique** de l'expéditeur pour vérifier la signature S .

Vérification : $M' = S^e \bmod n$ Si $M' = M$, la signature est valide.

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

Exemple :

- Prenons $p=5$ et $q=11$ donc $n=pq=55$ et $(p-1)(q-1)=40$
- Prenons $e=7$, on s'assure (Euclide) que e est premier avec 40

$$\begin{array}{lll} 40=5*7+5 & \text{On détermine alors} & 5-2*2=1 \\ 7=1*5+25=2*2+1 & \text{l'inverse mod (p-1)} & 5-2*(7-1*5)=3*5-2*7=1 \\ & (q-1) \text{ (Euclide étendu)} & 3*(40-5*7)-2*7=3*40-17*7=1 \\ & & \mathbf{7^{-1} \bmod 40 = -17 \bmod 40 = 23} \end{array}$$

- La clé publique vaut ($e=7$, $n=55$), la clé privée vaut $d=23$, les nombres $p=5$ et $q=11$ sont détruits
- Soit à coder un fragment de message représenté par la valeur $m=2$, le calcul de c est simplement
 $c=2^7 \bmod 55 = 128 \bmod 55 = 18$

Déchiffrement : le destinataire calcule de $c^d \bmod n = 18^{23} \bmod 55$ (on utilise ici l'exponentiation rapide qui permet de ne manipuler que des nombres relativement petits alors que 18^{23} est de l'ordre de 10^{29})

NB : $23_2 = 10111$

$18^1 \bmod 55 = 18$	1	18
$18^2 \bmod 55 = 324 \bmod 55 = 49$	1	$18*49 \bmod 55 = 2$
$18^4 \bmod 55 = 49^2 \bmod 55 = 2401 \bmod 55 = 36$	1	$2*36 \bmod 55 = 17$
$18^8 \bmod 55 = 36^2 \bmod 55 = 1296 \bmod 55 = 31$	0	17
$18^{16} \bmod 55 = 31^2 \bmod 55 = 961 \bmod 55 = 26$	1	$17*26 \bmod 55 = 2$

$$\mathbf{18^{23} \bmod 55 = 2}$$

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

4. Propriétés mathématiques garantissant la sécurité

○ Difficulté de factorisation :

- La sécurité de RSA repose sur la difficulté de factoriser n en p et q .
- Pour des clés de 2048 bits, cela est quasi impossible avec les technologies actuelles.

○ Modulo exponentiation :

- Les opérations RSA utilisent l'arithmétique modulaire, rendant le déchiffrement sans la clé privée inefficace.

6. Utilisations principales

○ Chiffrement hybride :

- RSA est utilisé pour échanger une **clé symétrique** (par exemple, dans TLS). La clé symétrique sert ensuite à chiffrer les données de manière rapide.

○ Signature numérique :

- Garantit l'authenticité des documents (exemple : certificats SSL/TLS ou certificat ID).

○ Certificats numériques :

- RSA est utilisé pour générer des certificats (X.509) dans des protocoles comme HTTPS.

○ Authentification :

- RSA est utilisé dans des systèmes comme SSH pour authentifier les utilisateurs.

Taille de clé (bits)	Niveau de sécurité
1024	Non sécurisé (faible)
2048	Standard actuel
3072	Plus sécurisé
4096	Sécurité renforcée

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

7. Avantages et inconvénients

○ Avantages :

- **Sécurité robuste** (si bien configuré).
- **Chiffrement asymétrique** éliminant le besoin d'un canal sécurisé pour l'échange de clé.
- **Applications polyvalentes** (chiffrement, signature, échange de clé).

○ Inconvénients :

- **Lent** par rapport à la cryptographie symétrique (comme AES).
- **Clés volumineuses** nécessitant un stockage et une transmission plus complexes.
- **Vulnérable** si des nombres premiers faibles ou mal générés sont utilisés.

8. Vulnérabilités possibles

○ Facteurs faibles dans n :

Si p ou q sont trop petits ou proches, cela facilite la factorisation.

○ Attaques par oracle :

Dans certains scénarios, des erreurs lors du déchiffrement peuvent révéler des informations sensibles.

○ Avancées en informatique quantique :

L'algorithme de Shor permettrait de factoriser n efficacement sur un ordinateur quantique. C'est pourquoi RSA pourrait devenir obsolète dans l'avenir post-quantique.

RSA : RIVEST-SHAMIR-ADLEMAN (CRYPTOGRAPHIE ASYMÉTRIQUE)

Critère	RSA	ECC (Courbes Elliptiques)	AES (Symétrique)
Type	Asymétrique	Asymétrique	Symétrique
Taille de clé	Grande (2048+)	Petite (256 bits suffisent)	Très petite
Performance	Lent	Plus rapide	Très rapide
Applications	Signatures, chiffrement hybride	Signatures, échange de clé	Chiffrement des données

CRYPTOGRAPHIE PAR COURBES ELLIPTIQUES (ECC - ELLIPTIC CURVE CRYPTOGRAPHY)

La cryptographie par courbes elliptiques utilise les propriétés mathématiques des courbes elliptiques pour offrir un chiffrement asymétrique robuste avec des clés plus petites.

○ Avantages de l'ECC :

- **Efficacité :**

- Pour un niveau de sécurité équivalent, ECC utilise des clés beaucoup plus courtes que RSA. Exemple :
 - ECC 256 bits \approx RSA 3072 bits en termes de sécurité.
- Moins gourmand en ressources, idéal pour les appareils avec des capacités limitées (IoT, mobiles).

- **Sécurité avancée :**

Basée sur le problème mathématique du **Logarithme Discret** sur les courbes elliptiques, considéré comme difficile à résoudre.

○ Applications courantes :

- **ECDH (Elliptic Curve Diffie-Hellman) :**

Utilisé pour l'échange sécurisé de clés.

- **ECDSA (Elliptic Curve Digital Signature Algorithm) :**

Utilisé pour les signatures numériques.

○ Exemples de courbes elliptiques standard :

- **secp256k1** : Utilisée par Bitcoin.
- **P-256 (NIST)** : Standard pour les applications web et réseaux.

ECC - ELLIPTIC CURVE CRYPTOGRAPHY

1. Principes fondamentaux

L'ECC repose sur des équations mathématiques de courbes elliptiques, qui ont la forme générale suivante :

$$y^2 = x^3 + ax + b \pmod{p} \text{ où :}$$

a et b sont des constantes choisies pour définir la courbe elliptique.

p est un nombre premier définissant le champ fini.

Pour que la courbe elliptique soit sécurisée, elle doit satisfaire la condition :

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}$$

2. Points sur une courbe elliptique

Un point P sur une courbe elliptique est une paire (x,y) qui satisfait l'équation de la courbe. Une "addition" spéciale entre deux points est définie pour créer un groupe abélien.

Opérations de base :

Addition de points : Si $P=(x_1,y_1)$ et $Q=(x_2,y_2)$, la somme $R=P+Q$ est un autre point sur la courbe. Les formules exactes dépendent des coordonnées (affines ou projectives).

Multiplication de point : Calculer kP (où k est un entier et P un point) est une opération fondamentale utilisée dans ECC.

3. Problème du logarithme discret (ECDLP)

La sécurité d'ECC repose sur la difficulté de résoudre le **problème du logarithme discret sur les courbes elliptiques** :

$Q=kP$ est un point connu, k est un entier privé, et Q est le point résultant. Trouver k à partir de P et Q est considéré comme extrêmement difficile.

ECC - ELLIPTIC CURVE CRYPTOGRAPHY

4. Fonctionnement de l'ECC dans le chiffrement

a) Génération de clé

Clé privée : Un entier d choisi aléatoirement ($1 \leq d \leq n-1$ ou n est l'ordre de la courbe).

Clé publique : $Q = d \cdot G$, où G est un point générateur défini par les paramètres de la courbe.

b) Échange de clés (ECDH - Elliptic Curve Diffie-Hellman)

Les deux parties choisissent des clés privées (d_A, d_B) et calculent leurs clés publiques ($Q_A = d_A G, Q_B = d_B G$).

Chaque partie calcule une clé partagée : $K = d_A Q_B = d_B Q_A$.

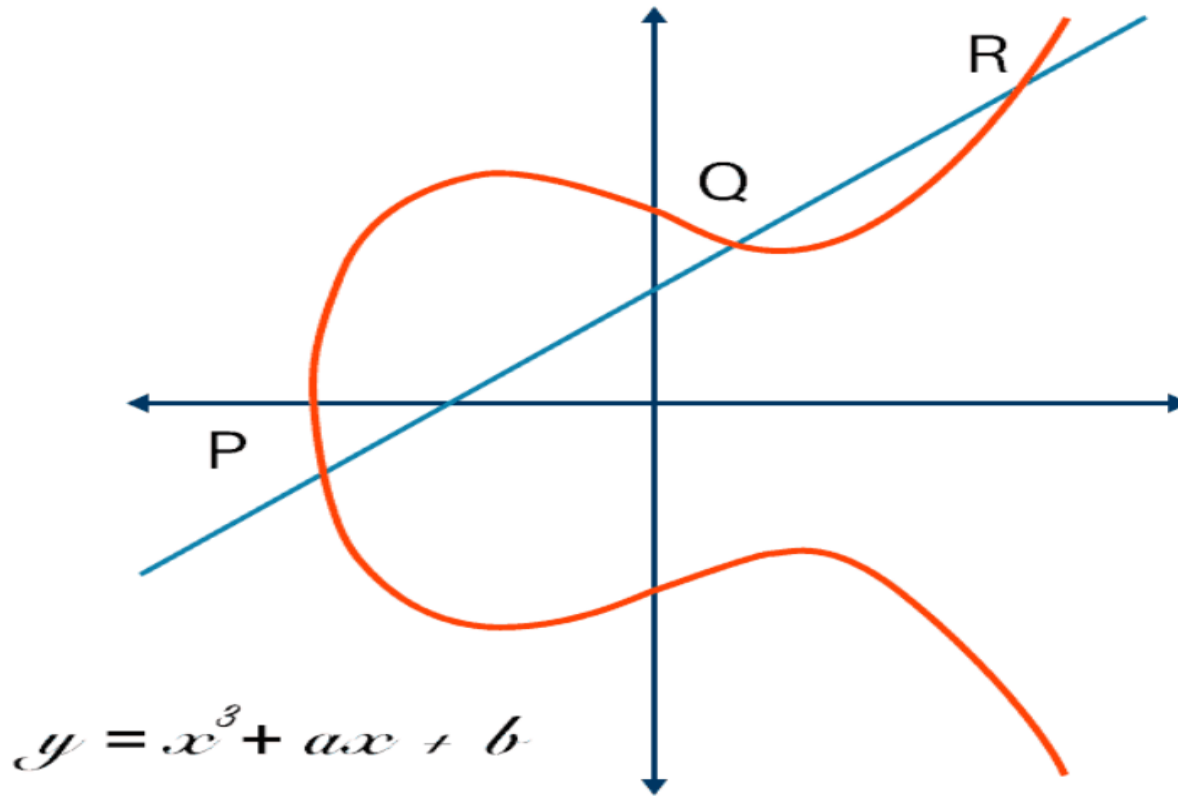
Grâce aux propriétés des courbes elliptiques : $d_A \cdot d_B \cdot G = d_B \cdot d_A \cdot G$.

c) Signature numérique (ECDSA - Elliptic Curve Digital Signature Algorithm)

Un message est signé en utilisant la clé privée (d) pour générer une signature (r, s) .

La vérification utilise la clé publique (Q) pour valider que la signature correspond au message.

ECC - ELLIPTIC CURVE CRYPTOGRAPHY



Caractéristique	ECC	RSA
Taille des clés	Plus petite (256 bits)	Plus grande (2048+ bits)
Performance	Plus rapide	Plus lente
Consommation	Moins de ressources	Gourmand en ressources

ALGORITHMES DE HASHAGE

Les algorithmes de hachage sont des fonctions cryptographiques utilisées pour transformer des données de taille variable en une empreinte numérique (ou hash) de taille fixe. Ces algorithmes sont fondamentaux pour la sécurité informatique, car ils sont utilisés dans de nombreux domaines, tels que l'intégrité des données, les signatures numériques, et l'authentification. Voici un aperçu détaillé des principaux algorithmes de hachage

1. Propriétés essentielles d'un bon algorithme de hachage

Un algorithme de hachage doit respecter certaines propriétés fondamentales :

- **Unidirectionnalité** : Il doit être pratiquement impossible de retrouver les données d'origine à partir de leur empreinte.
- **Diffusion (Avalanche)** : Un petit changement dans les données d'entrée doit entraîner un changement significatif dans l'empreinte.
- **Résistance aux collisions** : Il doit être difficile de trouver deux entrées différentes produisant la même empreinte.
- **Résistance aux attaques de préimage** :
 - **Préimage simple** : Difficile de trouver une entrée correspondant à un hash donné.
 - **Deuxième préimage** : Difficile de trouver une autre entrée ayant le même hash qu'une entrée donnée.

ALGORITHMES DE HASHAGE

2. Principaux algorithmes de hachage

2.1 MD5 (Message Digest 5)

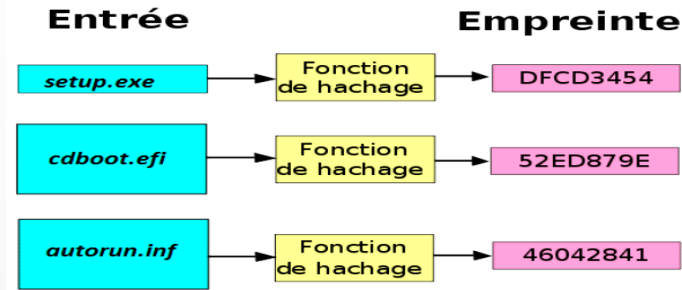
Longueur de l'empreinte : 128 bits.

Caractéristiques :

Créé en 1991, rapide et efficace à l'époque.

Actuellement considéré comme **inadapté** pour la sécurité cryptographique en raison de la découverte de nombreuses collisions.

Utilisation : Vérification de l'intégrité des fichiers (hors contexte cryptographique).



2.2 SHA (Secure Hash Algorithm)

Les algorithmes de la famille SHA sont développés par la **NSA** et standardisés par le **NIST**.

SHA-1

Longueur de l'empreinte : 160 bits.

Problèmes :

Des attaques de collision efficaces ont été découvertes.

N'est plus recommandé pour des applications de sécurité.

Utilisation : Certaines anciennes applications, mais progressivement abandonné.

SHA-2

- **Famille d'algorithmes** : SHA-224, SHA-256, SHA-384, SHA-512.
- **Longueur de l'empreinte** :
 - SHA-224 : 224 bits.
 - SHA-256 : 256 bits (le plus courant).
 - SHA-384 : 384 bits.
 - SHA-512 : 512 bits.
- **Sécurité** : Considéré comme sûr pour la plupart des applications modernes.
- **Utilisation** : Chiffrement, signatures numériques, certificats SSL/TLS.

SHA-3 (Keccak)

- Développé via un concours international et standardisé en 2015.
- Utilise un concept différent basé sur une "fonction éponge".
- **Sécurité améliorée** : Résiste aux attaques connues contre SHA-2.
- **Longueur de l'empreinte** : 224, 256, 384 ou 512 bits.

SIGNATURE NUMÉRIQUE

Une **signature numérique** est un mécanisme cryptographique qui permet de garantir :

- **Authenticité** : Le document ou le message provient bien de l'expéditeur.
- **Intégrité** : Le contenu n'a pas été altéré.
- **Non-répudiation** : L'expéditeur ne peut pas nier avoir envoyé le message.

○ Fonctionnement technique :

1. Création de la signature :

- L'émetteur calcule un **hachage** (empreinte) du message avec une fonction comme SHA-256.
- Ce hachage est chiffré avec la **clé privée** de l'émetteur (cryptographie asymétrique).

2. Vérification de la signature :

- Le destinataire déchiffre la signature avec la **clé publique** de l'émetteur.
- Il compare ensuite le hachage obtenu au hachage recalculé du message.

○ Exemple d'algorithmes :

- **RSA** : Utilisé pour les signatures numériques dans TLS.
- **ECDSA** : Version ECC des signatures numériques, plus rapide et plus légère.

SIGNATURE NUMÉRIQUE

L'Authentification par cryptographie :

1. Authentification basée sur la cryptographie asymétrique :

Utilisation de paires de clés publique/privée pour authentifier un utilisateur ou un serveur.

Exemple : Authentification dans SSH.

2. Authentification basée sur certificats :

Les certificats numériques (ex. X.509) permettent de valider l'identité d'une entité.

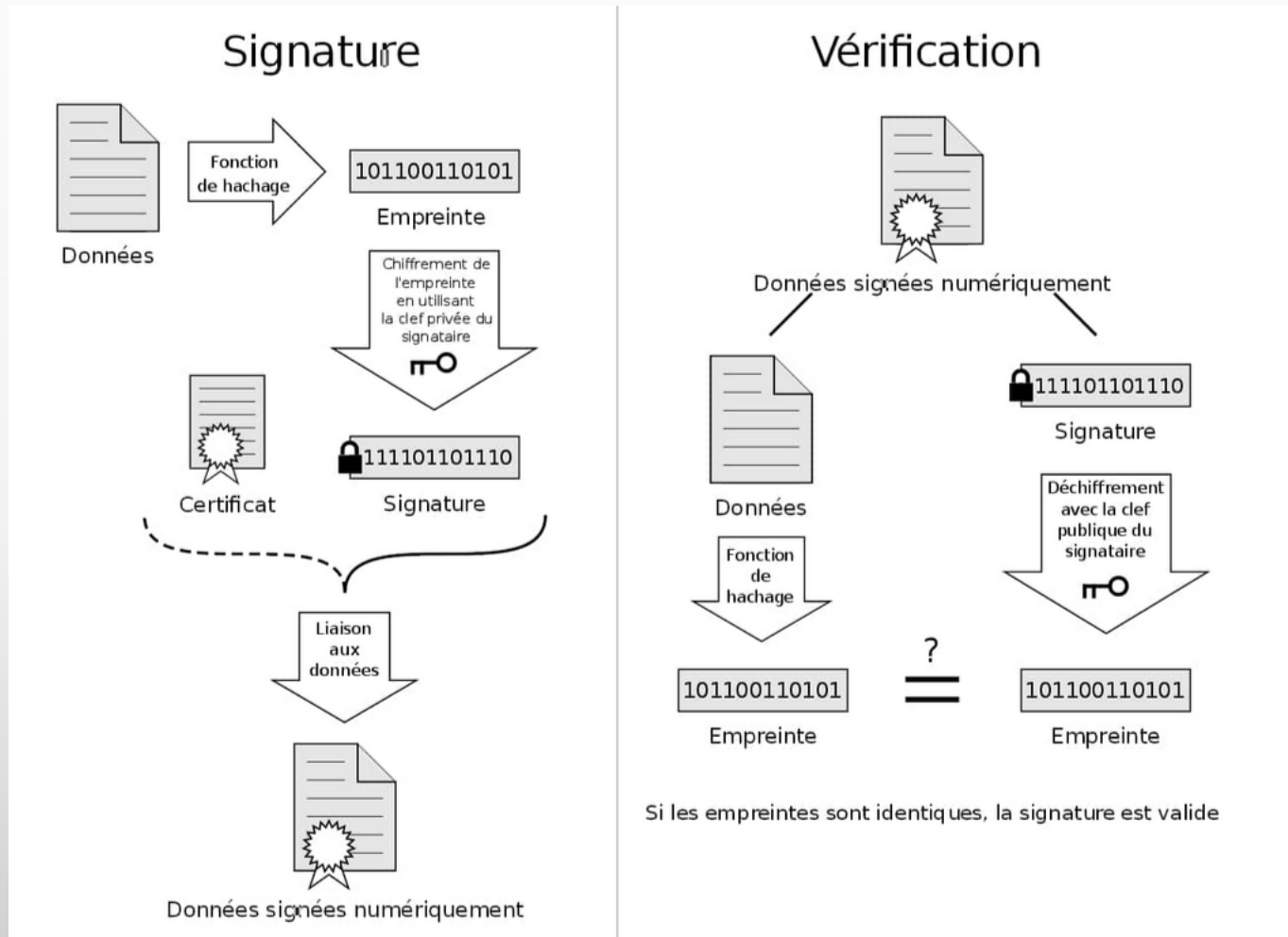
Utilisés dans **HTTPS** pour authentifier les serveurs.

3. Authentification mutuelle :

Implémentée dans TLS pour permettre au client et au serveur de prouver leur identité.

Technique	Type	Exemple	Avantage principal
Clé secrète partagée	Symétrique	AES, 3DES	Rapidité et simplicité
Clé de session	Symétrique (temporaire)	TLS (chiffrement hybride)	Sécurité temporaire
Courbes elliptiques (ECC)	Asymétrique	ECDSA, ECDH	Sécurité avec des clés plus courtes
Signature numérique	Asymétrique	RSA, ECDSA	Authentification et non-répudiation

SIGNATURE NUMÉRIQUE : CERTIFICAT



POLITIQUE DE SÉCURITÉ AU SEIN DE L'ÉTABLISSEMENT ET AUDIT INFORMATIQUE

La politique de sécurité informatique (PSI) est un ensemble de règles, de pratiques et de procédures définies pour protéger les actifs informationnels d'une organisation contre les menaces internes et externes.

1. Objectifs principaux :

1. **Assurer la confidentialité** : Protéger les données sensibles contre tout accès non autorisé.
2. **Garantir l'intégrité** : Préserver l'exactitude et la complétude des données.
3. **Assurer la disponibilité** : Garantir l'accès aux ressources informatiques en temps opportun.
4. **Encadrer l'utilisation des ressources** : Définir des règles pour l'usage des systèmes et réseaux.
5. **Réduire les risques** : Minimiser les menaces liées aux cyberattaques, erreurs humaines, et incidents matériels.

2. Composantes d'une politique de sécurité

a. Organisation de la sécurité :

Rôles et responsabilités :

- RSSI (Responsable de la Sécurité des Systèmes d'Information).
- Administrateurs réseau et système.
- Utilisateurs finaux.

Définir des procédures de gestion des accès, des incidents, et des mises à jour.

b. Charte d'utilisation des systèmes :

Documentation des règles d'utilisation pour les employés.

Exemples :

- Utilisation des mots de passe robustes.
- Restrictions sur l'installation de logiciels non approuvés.
- Interdiction d'utiliser des supports amovibles sans autorisation.

c. Politique de gestion des accès :

- Principe du **moindre privilège** : Les utilisateurs ont uniquement les permissions nécessaires.
- Gestion des comptes administratifs et utilisateurs.
- Authentification renforcée (ex. MFA - Authentification multifacteur).

d. Protection des données :

- **Chiffrement** des données sensibles (en transit et au repos).
- **Sauvegardes** régulières (locales et hors site).
- Mise en œuvre de solutions de prévention des pertes de données (**DLP**).

e. Sécurisation du réseau :

- Utilisation de **pare-feu**, **IDS/IPS**, et segmentation des réseaux (**VLANs**).
- Surveillance et filtrage des flux réseau.

f. Gestion des incidents :

- Plan de réponse aux incidents (PRI).
- Identification, analyse, confinement, et restauration.
- Reporting aux autorités compétentes si nécessaire.

g. Sensibilisation des utilisateurs :

- Formation régulière sur les bonnes pratiques en cybersécurité (exemple : détection de phishing).

h. Conformité réglementaire :

- Respect des normes et réglementations, telles que le **ANPDP**, la norme **ISO/IEC 27001**, ou **PCI DSS**.

3. Audit informatique : Définition et objectifs:

Un audit informatique est une évaluation systématique des systèmes d'information, des processus et des pratiques de sécurité afin de garantir leur conformité, leur efficacité, et leur sécurité.

Objectifs principaux :

- Identifier les vulnérabilités dans les systèmes et réseaux.
- Vérifier la conformité aux normes et réglementations.
- Évaluer l'efficacité des politiques de sécurité et des contrôles en place.
- Recommander des améliorations pour renforcer la sécurité.

4. Types d'audits informatiques

a. Audit de conformité :

- Vérifie si les politiques, procédures et systèmes respectent les normes (ISO 27001, RGPD, etc.).

Exemple : Respect de la confidentialité des données personnelles selon le RGPD.

b. Audit de sécurité :

- Évalue les mesures de sécurité pour détecter les failles.

Exemples :

Tests d'intrusion (Pentest).

Vérification des configurations réseau.

c. Audit technique :

- Analyse approfondie des infrastructures informatiques :
 - Configuration des pare-feu, serveurs, et systèmes.
 - Analyse des journaux d'événements (**logs**).

d. Audit opérationnel :

- Évaluation des processus et des pratiques opérationnelles.
- Vérification des plans de reprise après sinistre (PRA) et de continuité d'activité (PCA).

e. Audit de gouvernance IT :

- Vérifie la gestion stratégique des ressources informatiques.
- Évalue si les objectifs de l'IT sont alignés avec les objectifs de l'entreprise.

5. Étapes d'un audit informatique

a. Planification :

- Définir le périmètre de l'audit : systèmes, processus, données.
- Identifier les parties prenantes.

b. Collecte des informations :

- Examen des documents (politiques, procédures).
- Interviews avec les responsables IT.
- Analyse des configurations systèmes et réseaux.

c. Évaluation et tests :

- **Tests de vulnérabilité** pour identifier les failles.
- Simulations d'attaques (pentests) pour tester les défenses.

d. Analyse des résultats :

- Comparaison des pratiques actuelles avec les normes.
- Classement des risques selon leur criticité.

e. Rapport et recommandations :

- Rapport détaillé avec :
 - Résumé exécutif.
 - Résultats techniques.
 - Recommandations pour corriger les failles.

6. Méthodes et outils pour l'audit

a. Méthodologies :

- **ISO 27001** : Pour les audits de sécurité.
- **COBIT (Control Objectives for Information and Related Technologies)** : Gestion et audit IT.
- **ITIL** : Optimisation des services IT.

b. Outils :

- **Scanner de vulnérabilités** :
 - Exemples : Nessus, OpenVAS, Qualys.
- **SIEM** :
 - Surveillance en temps réel et analyse des logs.
 - Exemple : Splunk, ELK.
- **Outils de Pentest** :
 - Exemple : Metasploit, Nmap, Burp Suite.
- **Outils de gestion des configurations** :
 - Exemple : CIS-CAT pour vérifier la conformité des configurations.

7. PSI & audit :

- La **politique de sécurité** établit les règles et les bonnes pratiques à suivre.
- L'**audit informatique** évalue l'application effective de cette politique et propose des améliorations.
- **Exemple :**
 - Politique : Exiger des mots de passe robustes.
 - Audit : Vérification si les mots de passe respectent les critères établis.

Aspect	Politique de sécurité	Audit informatique
Objectif	Prévenir les incidents, définir les règles de sécurité.	Détecter les vulnérabilités et évaluer l'efficacité.
Nature	Document stratégique, directives internes.	Processus d'évaluation et de tests techniques.
Résultat	Amélioration des pratiques quotidiennes en cybersécurité.	Rapport d'audit avec recommandations détaillées.

DOMAINES DE LA GOUVERNANCE SI

1. PSSI

2. Organisation de la sécurité de l'information

Mise en place de structures de gouvernance pour gérer la sécurité.

Définition des rôles et responsabilités, y compris avec des tiers.

3. Sécurité des ressources humaines

Sécurisation avant, pendant et après l'emploi.

Sensibilisation, formation et gestion des violations des politiques de sécurité.

4. Gestion des actifs

Inventaire et classification des actifs.

Protection des informations en fonction de leur criticité.

5. Contrôle d'accès

Gestion des droits d'accès basés sur les besoins (principe du moindre privilège).

Authentification forte et gestion des comptes utilisateur.

6. Cryptographie

Utilisation de techniques cryptographiques pour la confidentialité, l'intégrité et l'authenticité.

Gestion sécurisée des clés de chiffrement.

7. Sécurité physique et environnementale

Contrôle d'accès physique aux locaux.

Protection contre les menaces environnementales comme les incendies et inondations.

DOMAINES DE GOUVERNANCE LA SI

8. Sécurité des opérations

- Gestion des configurations, des journaux et des capacités.
- Protection contre les logiciels malveillants.
- Sauvegardes régulières des données.

9. Sécurité des communications

- Protection des informations échangées (chiffrement, VPN).
- Gestion des réseaux internes et externes.

10. Acquisition, développement et maintenance des systèmes

- Sécurité intégrée dès la conception (Security by Design).
- Gestion des vulnérabilités des logiciels et systèmes.

11. Relations avec les fournisseurs

- Évaluation des risques liés aux tiers.
- Inclusion des exigences de sécurité dans les contrats.

12. Gestion des incidents de sécurité de l'information

- Détection, signalement et réponse aux incidents.
- Analyse post-incident pour éviter leur récurrence.

13. Aspects de la sécurité de l'information liés à la continuité des activités

- Planification et tests des plans de reprise après sinistre (PRA).
- Résilience organisationnelle en cas de crise.

14. Conformité

- Respect des exigences légales, réglementaires et contractuelles.
- Audits réguliers pour vérifier la conformité des pratiques.

Chacun de ces domaines contient des objectifs spécifiques et des mesures de sécurité associées, permettant de répondre aux menaces et risques en fonction des besoins de l'organisation.

TYPES ET EXEMPLES D'ATTAQUES

1. Composantes à risque :

Les composantes à risque dans un système d'information sont celles susceptibles d'être exploitées pour compromettre la sécurité. On identifie trois grandes catégories :

a. Systèmes :

- **Serveurs** : hébergent des applications et des données sensibles, souvent ciblés pour des attaques par déni de service (DoS) ou des injections SQL.
- **Postes de travail** : vulnérables aux malwares, ransomwares et aux erreurs humaines (ex. ouverture de liens malveillants).
- **Périphériques IoT** : souvent mal sécurisés, pouvant devenir des points d'entrée pour les attaquants.

b. Réseaux :

- **Infrastructure réseau** : routeurs, pare-feu et commutateurs peuvent être ciblés par des attaques pour intercepter ou rediriger du trafic.
- **Wi-Fi** : plus exposé aux attaques de type man-in-the-middle (MITM) et au piratage si mal configuré.
- **Protocole de communication** : des vulnérabilités dans les protocoles (ex. TCP/IP) peuvent être exploitées pour déni de service ou interception.

c. Utilisateurs :

- **Comportement humain** : l'utilisateur est souvent le maillon faible, avec des pratiques risquées comme l'utilisation de mots de passe faibles ou le clic sur des liens phishing.
- **Comptes privilégiés** : les administrateurs système et réseau sont des cibles prioritaires pour les attaquants.

TYPLOGIE DES FAILLES DE SÉCURITÉ

Les failles peuvent être regroupées en deux grandes catégories : techniques et humaines.

a. Vulnérabilités courantes :

- **Logiciels obsolètes** : systèmes d'exploitation ou applications non mis à jour.
- **Mauvaises configurations** : par exemple, des permissions trop larges sur des bases de données ou des fichiers sensibles.
- **Failles zero-day** : exploitées avant qu'un correctif ne soit publié.

b. Erreurs humaines :

- **Partage de mots de passe** : qui favorise les intrusions.
- **Phishing** : tromperies visant à obtenir des informations sensibles.
- **Omissions** : oubli de configurer des protections comme le chiffrement des données.

CLASSIFICATION DES ATTAQUES

a. Attaques sur les serveurs :

- **Déni de service (DoS/DDoS)** : saturent un serveur en le submergeant de requêtes pour le rendre indisponible.
- **Injection SQL** : vise à manipuler une base de données via des entrées non sécurisées pour exfiltrer ou modifier des informations.

b. Attaques réseau :

- **Man-in-the-middle (MITM)** : un attaquant intercepte les communications entre deux parties pour les lire ou les modifier.
- **Sniffing** : capture du trafic réseau non chiffré pour en extraire des données sensibles (ex. mots de passe).

c. Attaques sur les postes de travail :

- **Phishing** : courriels ou sites frauduleux imitant des entités légitimes pour tromper l'utilisateur.
- **Malwares** : logiciels malveillants (ex. chevaux de Troie, ransomwares) installés sur les machines pour espionner ou chiffrer les données.

TYPES DE MALWARES

Un malware (ou logiciel malveillant) est conçu pour endommager, perturber ou accéder illégalement à des systèmes :

- **Virus :**

- Programme qui se propage en s'attachant à d'autres fichiers ou applications.
- Nécessite une action de l'utilisateur pour se propager (ex. ouverture d'un fichier infecté).

- **Cheval de Troie (Trojan) :**

- Se présente comme un programme légitime, mais exécute des actions malveillantes en arrière-plan.
- Souvent utilisé pour installer d'autres malwares ou voler des données.

- **Ransomware :**

- Chiffre les données d'une victime et exige une rançon pour fournir la clé de déchiffrement.
- Exemples célèbres : WannaCry, LockBit.

- **Spyware :**

- Logiciel espion qui collecte des informations (ex. mots de passe, activités en ligne) à l'insu de l'utilisateur.
- Souvent utilisé pour des campagnes de surveillance ou du vol d'identité.

- **Adware :**

- Affiche des publicités intrusives sur le système infecté.
- Peut collecter des données sur l'utilisateur pour cibler les publicités.

- **Rootkit :**

- Conçu pour fournir un accès administrateur non autorisé à un système tout en restant caché.
- Difficile à détecter et souvent utilisé pour des attaques persistantes.

- **Worms (vers informatiques) :**

- Se propage automatiquement d'une machine à une autre via des réseaux ou des périphériques.
- Contrairement aux virus, n'a pas besoin d'un fichier hôte pour se propager.

- **Keylogger :**

- Enregistre les frappes au clavier pour voler des informations sensibles (ex. mots de passe, numéros de carte bancaire).

- **Botnets :**

- Réseau de machines compromises (bots) contrôlées par un attaquant pour lancer des attaques massives, comme des DDoS.

OWASP TOP10

L'OWASP (Open Web Application Security Project) propose une liste des 10 principales vulnérabilités des applications web. Voici les attaques associées :

- **A01:2021 - Broken Access Control :**
 - Exploitation de failles dans les contrôles d'accès pour accéder à des données ou fonctionnalités non autorisées.
 - Exemples : escalade de privilèges, modification des URL ou des requêtes.
- **A02:2021 - Cryptographic Failures :**
 - Mauvaises pratiques dans la gestion du chiffrement (ex. absence de TLS, algorithmes obsolètes).
 - Permet l'interception ou la modification de données sensibles.
- **A03:2021 - Injection :**
 - L'attaquant injecte des commandes malveillantes (SQL, NoSQL, OS command) via des champs utilisateur.
 - Exemples : SQL Injection, Command Injection.
- **A04:2021 - Insecure Design :**
 - Défauts dans l'architecture de sécurité dès la conception.
 - Absence de protection contre des attaques prévisibles.
- **A05:2021 - Security Misconfiguration :**
 - Mauvaise configuration de serveurs ou d'applications (ex. interfaces d'administration accessibles).
 - Exemples : divulgation d'informations via des messages d'erreur.
- **A06:2021 - Vulnerable and Outdated Components :**
 - Utilisation de bibliothèques, frameworks ou modules obsolètes avec des vulnérabilités connues.
- **A07:2021 - Identification and Authentication Failures :**
 - Faiblesses dans la gestion des sessions et de l'authentification.
 - Exemples : attaques par force brute, session hijacking.
- **A08:2021 - Software and Data Integrity Failures :**
 - Absence de vérifications pour s'assurer que les mises à jour ou les données proviennent de sources fiables.
 - Exemples : dépendances compromises, pipelines CI/CD corrompus.
- **A09:2021 - Security Logging and Monitoring Failures :**
 - Insuffisance des journaux ou absence de surveillance des activités.
 - Conséquences : détection tardive ou impossible d'attaques.

FIREWALLS

Un **firewall** (pare-feu en français) est un dispositif matériel ou logiciel utilisé pour sécuriser un réseau ou un système informatique en filtrant le trafic entrant et sortant selon des règles préétablies. Son objectif principal est de protéger les systèmes contre les accès non autorisés, les cyberattaques et les communications malveillantes.

Types de Firewalls :

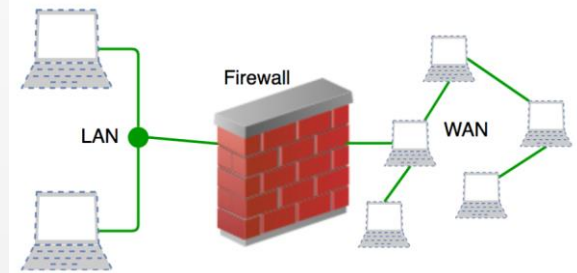
Les firewalls se déclinent en plusieurs catégories selon leur fonctionnement et leur emplacement dans l'infrastructure réseau.

a. Firewalls Matériels :

Appareils dédiés positionnés entre le réseau interne et Internet.

Exemples : Cisco ASA, Palo Alto, Fortinet.

Avantages : performances élevées, indépendance par rapport aux systèmes.



b. Firewalls Logiciels :

Programmes installés sur des systèmes (serveurs ou postes de travail).

Exemples : Firewall Windows, iptables (Linux).

Avantages : coût réduit, facilement adaptable aux besoins.

FIREWALLS

c. Firewalls Basés sur les Hôtes (HFW - Host-based Firewall) :

- Protège individuellement chaque machine en contrôlant le trafic réseau local.
- Utilisé pour les postes de travail ou serveurs spécifiques.

d. Firewalls Basés sur le Réseau (NFW - Network Firewall) :

- Protège l'ensemble du réseau.
- Filtre le trafic à l'entrée et à la sortie en fonction de règles appliquées globalement.

e. Firewalls de Nouvelle Génération (NGFW - Next-Generation Firewall) :

- Combine les fonctions classiques de firewall avec des fonctionnalités avancées comme l'inspection profonde des paquets (DPI), la prévention des intrusions (IPS) et le contrôle des applications.

Avantages : meilleure détection des menaces modernes comme les malwares et attaques avancées.

f. Firewalls Cloud :

- Solution virtuelle hébergée dans le cloud pour protéger les infrastructures cloud (ex. AWS, Azure).
- Adapté aux environnements virtualisés et infrastructures hybrides.

FIREWALLS

Different Types Of Firewalls Explained

1 Software Firewalls

A software firewall is installed on the host device. Since it is attached to a specific device, it has to utilize its resources to work. Therefore, it is inevitable for it to use up some of the system's RAM and CPU.

2 Packet-Filtering Firewalls

Packet-Filtering Firewalls serves as an inline security checkpoint attached to a router or switch. As the name suggests, it monitors network traffic by filtering incoming packets according to the information they carry.

Secureb4.io

3 Cloud Firewalls

A cloud firewall or firewall-as-a-service (FaaS) is a cloud solution for network protection. Like other cloud solutions, it is maintained and run on the Internet by third-party vendors.

Secureb4.io

4 Proxy Firewalls

It serves as an intermediate device between internal and external systems communicating over the Internet. It protects a network by forwarding requests from the original client and masking it as its own.

1

2

3

4

5

5 Hardware Firewalls

Hardware firewalls are security devices that represent a separate piece of hardware placed between an internal and external network (the Internet). This type is also known as an Appliance Firewall.

Secureb4.io

6

6 Next-Generation Firewalls

The next-generation firewall is a security device that combines a number of functions of other firewalls. It incorporates packet, stateful, and deep packet inspection.



SECUREB4
The Stronger Your Security

7

7 Circuit-Level Gateways

Circuit-level gateways are a type of firewall that work at the session layer of the OSI model, observing TCP (Transmission Control Protocol) connections and sessions.

8

8 Stateful Inspection Firewalls

A stateful inspection firewall keeps track of the state of a connection by monitoring the TCP 3-way handshake.



FIREWALLS

Fonctionnalités principales :

a. Filtrage de Paquets (Packet Filtering) :

- Vérifie chaque paquet de données en fonction des règles (adresse IP, port, protocole).
- Bloque ou autorise les paquets en fonction des critères définis.

b. Inspection Stateful :

- Analyse les connexions réseau et garde en mémoire l'état des sessions (ex. TCP/UDP).
- Permet de distinguer le trafic légitime du trafic malveillant.

c. Traduction d'Adresse Réseau (NAT - Network Address Translation) :

- Masque les adresses IP internes pour empêcher leur exposition à Internet.
- Protège contre les attaques ciblant directement les hôtes internes.

FIREWALLS

d. Contrôle des Applications :

- Identifie et bloque des applications spécifiques (ex. réseaux sociaux, torrents).
- Fonctionnalité souvent présente dans les NGFW.

e. Prévention des Intrusions (IPS - Intrusion Prevention System) :

- Identifie et bloque activement les menaces connues ou suspectes.
- Complément idéal des firewalls de nouvelle génération.

f. VPN (Virtual Private Network) :

- Fonction intégrée permettant de sécuriser les connexions à distance via le chiffrement.

g. Détection et Prévention des Menaces Avancées :

- Analyse des fichiers en temps réel pour détecter des malwares ou menaces (sandboxing, antivirus intégré).

FIREWALLS

Avantages des Firewalls :

- Protègent contre les accès non autorisés et les intrusions.
- Empêchent la propagation des malwares.
- Aident à sécuriser les communications entre différents réseaux.
- Facilitent le contrôle des applications et des utilisateurs.

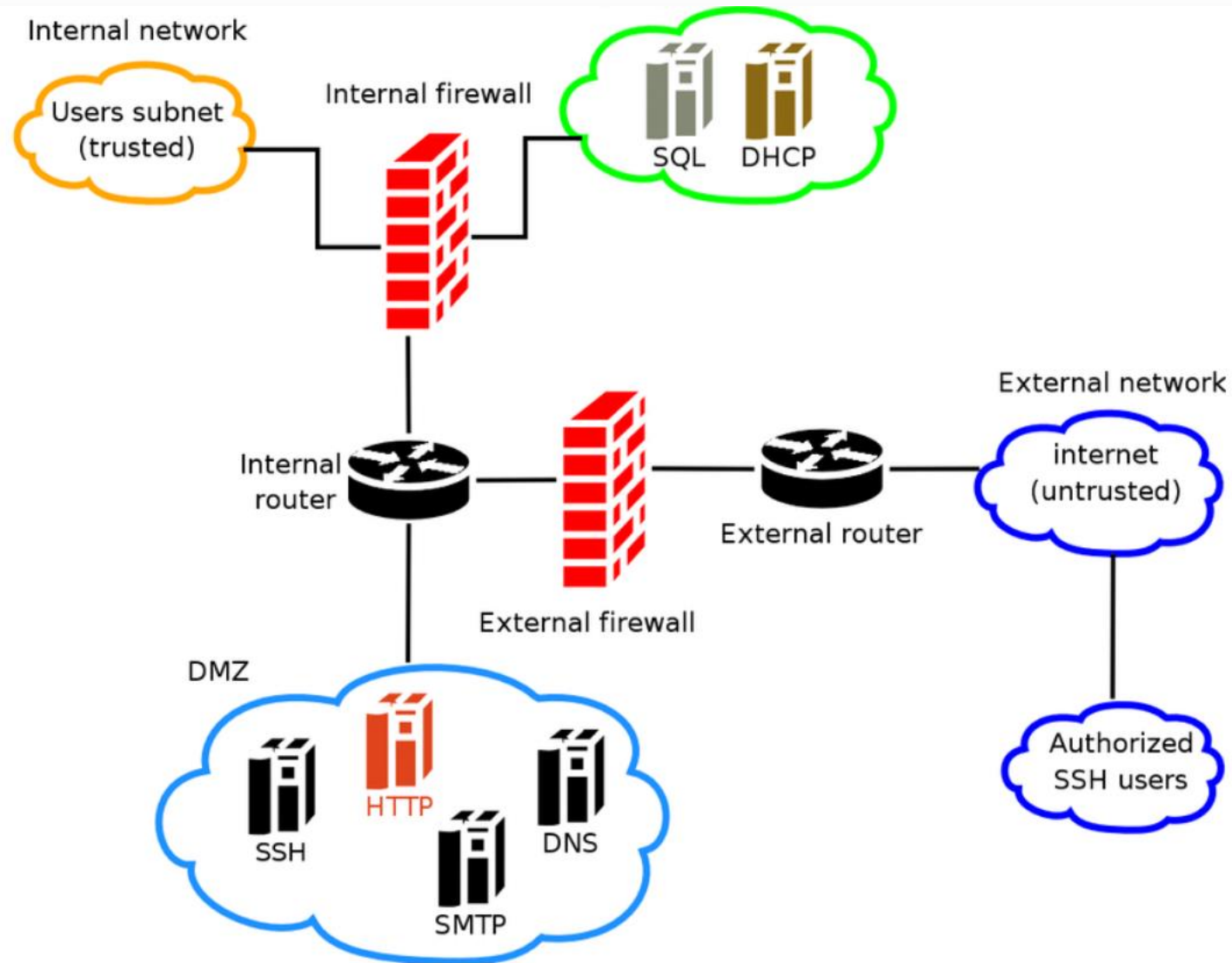
Limites des Firewalls :

- Inefficaces contre les menaces internes (si les règles ne couvrent pas ce cas).
- Peuvent être contournés par des menaces avancées (ex. malwares fileless).
- Nécessitent une configuration et une maintenance rigoureuses pour éviter des failles.

Meilleures Pratiques pour Utiliser un Firewall :

- Définir des règles de filtrage basées sur le principe du "moindre privilège" : tout ce qui n'est pas explicitement autorisé est bloqué.
- Mettre régulièrement à jour le firmware ou les signatures de menaces.
- Surveiller et analyser les journaux de trafic pour détecter les comportements suspects.
- Coupler le firewall avec d'autres solutions de sécurité (antivirus, IPS, WAF, etc.).

FIREWALLS



L'IDS

Un **système de détection des intrusions** détecte et alerte sur les activités suspectes dans le réseau ou sur un hôte, sans intervenir activement pour bloquer ces menaces.

- **Types d'IDS :**

- **HIDS (Host-based IDS)** : Surveille les activités sur un poste de travail ou un serveur.
- **NIDS (Network-based IDS)** : Analyse le trafic réseau pour identifier des attaques potentielles.

- **Fonctionnalités principales :**

- **Détection basée sur les signatures** : Repère des menaces connues à partir de modèles préenregistrés.
- **Détection comportementale (anomalies)** : Identifie des activités inhabituelles ou suspectes.
- **Alertes en temps réel** : Notifie les administrateurs en cas de menace.

Limite :

Ne bloque pas les attaques. Il nécessite un couplage avec d'autres outils (comme un IPS ou un pare-feu).

L'IPS

Un **système de prévention des intrusions** est un dispositif de sécurité qui analyse activement le trafic réseau et empêche automatiquement les activités malveillantes. Contrairement à un IDS (qui se limite à la détection), un IPS agit en temps réel pour bloquer les menaces.

- **Fonctionnalités principales :**

- **Inspection profonde des paquets (DPI) :** Analyse chaque paquet pour détecter des signatures ou comportements malveillants.
- **Blocage automatisé :** Interrompt les connexions suspectes avant qu'elles n'atteignent leur cible.
- **Protection contre les attaques connues :** Bloque les attaques comme les scans de ports, exploits, injections SQL.
- **Mises à jour régulières :** Intègre des bases de signatures pour répondre aux nouvelles menaces.

- **Cas d'usage :**

- Prévention des attaques par déni de service (DoS/DDoS).
- Blocage des intrusions via des failles connues.
- Surveillance et blocage des communications avec des serveurs malveillants.

L'EDR

EDR (Endpoint Detection and Response)

Une solution **EDR** est conçue pour surveiller, détecter et répondre aux menaces qui ciblent les **postes de travail, serveurs ou appareils connectés** (endpoints).

Fonctionnalités principales :

- **Surveillance continue** : Analyse en temps réel les activités sur les terminaux.
- **Détection avancée des menaces** : Identifie les attaques ciblées (ex. ransomware, malwares).
- **Réponse automatisée** : Isolations des endpoints infectés, suppression des fichiers malveillants.
- **Forensics et remédiation** : Enregistre les données d'attaque pour comprendre l'incident et y répondre.

Avantages :

- Protéger les terminaux mobiles, serveurs et ordinateurs dans un contexte de télétravail.
- Utile contre les menaces avancées qui échappent aux antivirus traditionnels.

Exemples d'outils EDR :

CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne.

NDR

Les solutions **NDR** se concentrent sur la détection et la réponse aux menaces au niveau du **réseau**. Elles analysent le trafic en temps réel pour repérer des comportements anormaux ou malveillants.

Fonctionnalités principales :

- **Analyse comportementale** : Identifie les anomalies dans le trafic réseau en utilisant des techniques comme le machine learning.
- **Détection des menaces internes** : Repère les activités malveillantes provenant de l'intérieur du réseau.
- **Corrélation des événements** : Combine les données réseau avec d'autres sources pour une vision globale.
- **Visibilité réseau accrue** : Analyse tous les segments, y compris les communications latérales (East-West traffic).

Cas d'usage :

- Détection des mouvements latéraux d'un attaquant dans le réseau.
- Surveillance des communications avec des serveurs de commande et de contrôle (C2).

Exemples de solutions NDR :

Darktrace, Cisco Stealthwatch, Vectra AI.

XDR

XDR (Extended Detection and Response)

L'**XDR** est une solution unifiée qui regroupe les capacités d'EDR, NDR et d'autres outils de sécurité (comme les SIEM et SOAR) pour fournir une **détection et réponse étendues** à l'échelle de l'organisation.

Fonctionnalités principales :

- **Corrélation multi-couches** : Analyse des données provenant des endpoints, réseaux, serveurs, cloud, et applications.
- **Automatisation des réponses** : Réagit automatiquement aux menaces détectées en appliquant des politiques prédéfinies.
- **Gestion centralisée** : Interface unique pour surveiller et répondre aux incidents à travers tous les environnements.
- **Détection des menaces avancées** : Protection contre les attaques complexes, telles que les menaces persistantes avancées (APT).

Avantages :

- Fournit une vision globale et centralisée des menaces.
- Simplifie les opérations de sécurité en réduisant la charge des équipes SOC.
- Améliore la capacité de réponse grâce à l'automatisation.

Exemples de solutions XDR :

Palo Alto Cortex XDR, Trend Micro Vision One, Microsoft Sentinel.

RÉSUMÉ IPS IDS EDR NDR XDR

Technologie	Focus	Niveau	Action principale
IPS	Prévention des intrusions	Réseau	Analyse et bloque les attaques
IDS	Détection des intrusions	Réseau/Host	Alerte sans intervention
EDR	Protection des terminaux	Endpoint	Détecte et répond sur les postes
NDR	Détection sur le réseau	Réseau	Analyse et corrige les anomalies
XDR	Protection unifiée étendue	Réseau + Endpoint	Corrélation multi-sources

WAF

WAF (Web Application Firewall)

Un **Web Application Firewall (WAF)** est une solution de sécurité qui protège les **applications web** contre les cyberattaques. Il agit comme une barrière entre l'application web et Internet, analysant et filtrant les requêtes HTTP/S pour détecter et bloquer les menaces. **Fonctionnalités principales :**

Protection contre les attaques OWASP Top 10 :

Empêche les attaques web courantes, comme :

Injection SQL

Cross-Site Scripting (XSS)

Falsification de requêtes côté serveur (SSRF)

Exposition de données sensibles

Inspection des requêtes HTTP/S :

Analyse les en-têtes, les cookies, les paramètres, et le corps des requêtes pour détecter des activités malveillantes.

Filtrage basé sur des règles :

Fonctionne avec des règles prédéfinies ou personnalisables, telles que celles proposées par l'OWASP ModSecurity.

Protection contre les bots et DoS :

Bloque les bots malveillants et atténue les attaques de type DoS/DDoS en limitant les requêtes excessives.

Contrôle des accès :

Restreint l'accès aux utilisateurs ou adresses IP suspectes.

Intègre des fonctionnalités de géorestriction ou de blocage des proxys/Tor.

Apprentissage automatique (ML) :

Les WAF avancés utilisent des algorithmes de machine learning pour détecter des modèles d'attaque inconnus.

WAF

Types de WAF :

- **WAF basé sur le réseau :**
Matériel ou solution physique déployée sur le réseau.
Exemple : F5 Networks.
- **WAF basé sur le cloud :**
Protection offerte via des services cloud.
Exemple : Cloudflare, AWS WAF, Akamai.
- **WAF logiciel :**
Déployé sur des serveurs applicatifs, intégré à l'application.
Exemple : ModSecurity.

Avantages :

- **Protection proactive** contre les vulnérabilités des applications.
- Réduit la surface d'attaque des applications web exposées à Internet.
- **Conformité réglementaire** : aide à respecter les normes comme PCI-DSS en protégeant les données sensibles.

Limites :

- Inefficace contre les attaques côté client (ex. phishing).
- Nécessite une configuration fine pour éviter les faux positifs.
- Coût élevé pour les solutions avancées.

MAIL GATEWAY

Une **Mail Gateway** est une solution qui sécurise et contrôle le flux des emails entrants et sortants d'une organisation. Elle agit comme une barrière pour analyser les messages et protéger les utilisateurs contre les cybermenaces.

Fonctionnalités principales :

Protection contre les spams :

Filtrage avancé des courriers indésirables en fonction de signatures, heuristiques ou listes noires.

Détection des malwares :

Analyse les pièces jointes et les liens pour détecter les fichiers malveillants et les URL dangereuses.

Blocage des attaques par phishing :

Identifie les emails frauduleux imitant des entreprises ou personnes légitimes.

Chiffrement des emails :

Garantit la confidentialité des communications sensibles via des protocoles comme S/MIME ou PGP.

Contrôle des politiques de contenu :

Analyse les emails pour s'assurer qu'ils respectent les règles de l'organisation (ex. blocage de fichiers types .exe ou données sensibles).

Prévention de la perte de données (DLP) :

Surveille les emails sortants pour empêcher la fuite d'informations confidentielles.

Sandboxing :

Exécute les pièces jointes suspectes dans un environnement isolé pour détecter les comportements malveillants.

MAIL GATEWAY

Authentification des emails :

Implémente des protocoles tels que :

DKIM (DomainKeys Identified Mail)

SPF (Sender Policy Framework)

DMARC (Domain-based Message Authentication, Reporting & Conformance)

Avantages :

- Protège les utilisateurs contre les **campagnes de phishing et ransomwares**.
- Réduit les risques de fuites de données.
- Centralise le contrôle et la surveillance des emails.

Exemples de Mail Gateways :

- **Solutions Cloud :**
 - Microsoft Defender for Office 365.
 - Google Workspace Email Security.
- **Solutions On-Premise :**
 - Symantec Email Security.
 - Barracuda Email Gateway.

Différences principales entre WAF et Mail Gateway :

Critère	WAF	Mail Gateway
Objectif principal	Protéger les applications web	Sécuriser les emails
Type de trafic	HTTP/S	SMTP (emails)
Menaces ciblées	Attaques web (SQLi, XSS, DDoS)	Phishing, spam, malwares par email
Déploiement typique	Devant les serveurs web	Entre le serveur mail et Internet

SIEM & SOAR

Les solutions **SIEM** et **SOAR** jouent un rôle clé dans les opérations de sécurité des entreprises, notamment dans les centres opérationnels de sécurité (SOC). Elles permettent de **détecter, analyser et répondre** aux cybermenaces.

SIEM (Security Information and Event Management)

Le **SIEM** est une solution qui collecte, centralise et analyse les **journaux (logs)** et événements de sécurité provenant de diverses sources dans un réseau. Il permet de **détecter des incidents de sécurité, générer des alertes et assurer la conformité réglementaire**.

Fonctionnalités principales :

Collecte et agrégation des données :

- Collecte des logs provenant de multiples sources : firewalls, serveurs, endpoints, applications, etc.
- Centralisation des données dans une interface unique.

Corrélation des événements :

- Analyse les événements pour détecter des **patterns d'attaques** ou des comportements anormaux.
- Par exemple : un utilisateur effectue plusieurs tentatives de connexion échouées suivies d'un accès depuis une IP étrangère.

Gestion des alertes :

- Génère des alertes en temps réel en cas de détection de menace.
- Classe les alertes par priorité (critique, moyenne, faible).

Conformité :

- Facilite la conformité avec des réglementations comme **GDPR, PCI-DSS, ISO 27001** en fournissant des rapports d'audit détaillés.

Visualisation et tableaux de bord :

- Offre une interface graphique pour surveiller les activités en temps réel et analyser les tendances historiques.

SIEM & SOAR

Avantages :

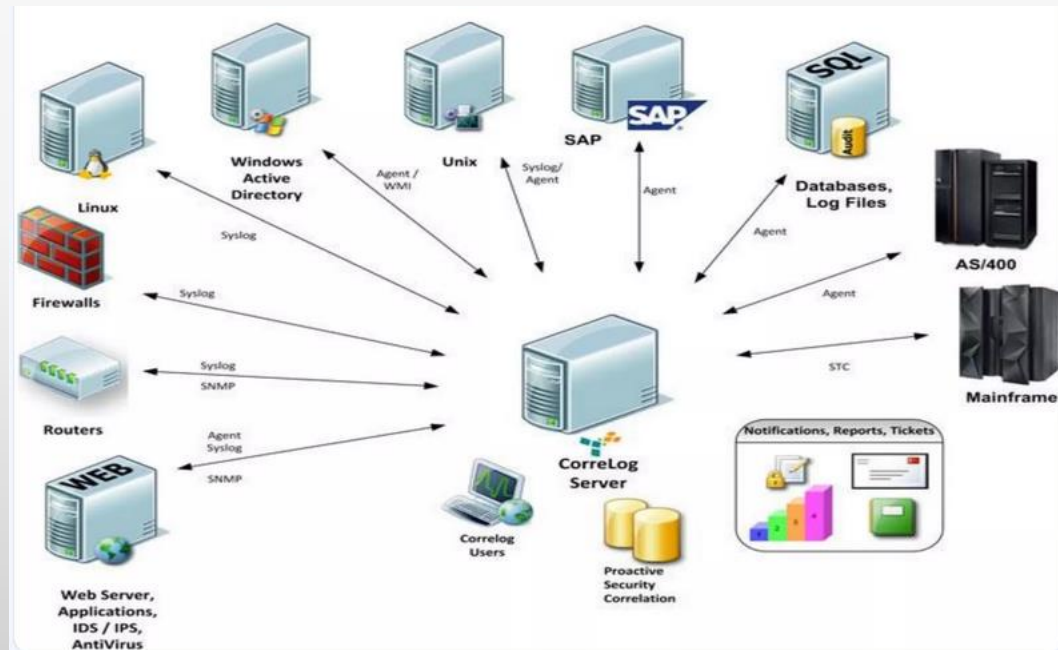
- **Détection centralisée** : Surveillance unifiée des infrastructures complexes.
- **Réduction des silos** : Combine les données de sécurité provenant de différents outils.
- **Conformité facilitée** : Automatise la génération de rapports pour les audits.

Limites :

- **Faux positifs fréquents** : Nécessite une configuration et une gestion continue.
- **Coût élevé** : Les solutions SIEM (et leur maintenance) peuvent être coûteuses.
- **Dépendance humaine** : Les analystes doivent interpréter les alertes et intervenir manuellement.

Exemples de solutions SIEM :

1. Splunk Enterprise Security
2. IBM QRadar
3. Microsoft Sentinel
4. Elastic Security (ELK Stack)



SIEM & SOAR

SOAR (Security Orchestration, Automation, and Response)

Le **SOAR** est une solution qui vise à automatiser et orchestrer les **processus de réponse aux incidents** dans un environnement de cybersécurité. Il est conçu pour augmenter l'efficacité et réduire le temps de réponse des équipes de sécurité.

Fonctionnalités principales :

Orchestration :

Intègre différents outils de sécurité (SIEM, EDR, firewalls, etc.) dans une seule plateforme.

Centralise les workflows pour une meilleure coordination.

Automatisation :

Automatise les réponses aux menaces, comme :

Isoler un endpoint infecté.

Bloquer une adresse IP malveillante sur un firewall.

Réduit la charge de travail des analystes.

SIEM & SOAR

Gestion des incidents :

Regroupe toutes les informations sur un incident (source, impact, logs associés).

Permet une collaboration entre les membres de l'équipe pour résoudre le problème.

Playbooks :

Définit des scénarios de réponse automatisés pour chaque type d'incident (ex. phishing, malware, ransomware).

Exemples :

Phishing : analyser automatiquement un email suspect, bloquer le domaine, notifier l'utilisateur.

Ransomware : isoler la machine touchée, analyser les fichiers, démarrer la restauration des sauvegardes.

Threat Intelligence :

Intègre des sources de renseignements sur les menaces pour enrichir la détection et la réponse.

Exemple : consulter une base de données de menaces pour valider si une adresse IP est malveillante.

SIEM & SOAR

Avantages :

- **Réduction du temps de réponse** : Automatise les tâches répétitives pour accélérer la résolution des incidents.
- **Amélioration de l'efficacité** : Libère les analystes pour qu'ils se concentrent sur des tâches critiques.
- **Meilleure coordination** : Standardise les processus et réduit les erreurs humaines.

Limites :

- **Complexité d'intégration** : Nécessite une configuration initiale pour s'adapter aux outils existants.
- **Dépendance aux playbooks** : Les scénarios mal définis peuvent limiter l'efficacité.

Exemples de solutions SOAR :

- Palo Alto Cortex XSOAR
- Splunk SOAR (anciennement Phantom)
- IBM Resilient
- Swimlane

Critère	SIEM	SOAR
Objectif principal	Collecte, analyse et corrélation des logs	Automatisation et orchestration des réponses
Focus	Détection et génération d'alertes	Réponse aux incidents
Automatisation	Limité (alertes automatisées)	Avancée (playbooks automatisés)
Utilisation principale	Surveillance et analyse des menaces	Gestion des incidents
Exemples d'outils	Splunk, QRadar, Microsoft Sentinel	Cortex XSOAR, Splunk SOAR, IBM Resilient

vLANs

VLAN (Virtual Local Area Network)

Un **VLAN** est une technologie de réseau qui permet de segmenter un réseau physique en plusieurs réseaux virtuels logiques indépendants. Chaque VLAN est traité comme un réseau distinct, bien qu'il partage la même infrastructure physique.

Fonctionnalités et Objectifs :

- **Segmentation des réseaux :**
 - Isoler logiquement les utilisateurs ou équipements selon des critères (ex. service, département, type d'équipement).
- **Amélioration de la sécurité :**
 - Les VLAN empêchent la communication directe entre segments (par exemple, entre le réseau des employés et le réseau des invités), sauf si elle est explicitement autorisée via des règles.
- **Gestion simplifiée :**
 - Facilite l'administration des réseaux en attribuant des ressources ou permissions spécifiques à chaque VLAN.
- **Optimisation de la bande passante :**
 - Réduit le trafic inutile sur le réseau en limitant les diffusions (broadcasts) à un VLAN spécifique.

Préambule	SFD	@ MAC destination	@ MAC source	TAG	Type donnée	Données	FCS (CRC)	Délai intertrame
7x 10101010	10101011	6 octets	6 octets	4 octets	2 octets	46-1500 octets	4 octets	12 octets

TPID	Priority	CFI	VID
16 bits	3 bits	1 bit	12 bits

vLANs

Types de VLAN :

- **VLAN par port :**
 - Les VLAN sont assignés selon les ports des switches.
- **VLAN par adresse MAC :**
 - Les VLAN sont attribués dynamiquement en fonction des adresses MAC des équipements connectés.
- **VLAN par protocole :**
 - Les VLAN sont définis en fonction des protocoles utilisés (ex. VLAN pour le trafic IP, un autre pour le trafic VoIP).
- **VLAN pour la Voix (Voice VLAN) :**
 - Spécifiquement dédié au trafic VoIP pour garantir la qualité du service (QoS).

Avantages :

- Améliore la **sécurité** interne du réseau.
- Réduit la complexité de gestion des réseaux physiques.
- Permet une meilleure **performance réseau** via une segmentation efficace.

Exemple d'utilisation :

Entreprise : Un VLAN pour les administrateurs, un pour les employés et un pour les invités.

Université : VLAN distincts pour le personnel, les étudiants et les chercheurs.

vLANs

Limites :

- Nécessite une configuration correcte (via les switches gérés).
- Peut être vulnérable aux attaques comme le **VLAN hopping** si mal sécurisé.

Technologie associée :

IEEE 802.1Q : Standard utilisé pour le marquage des trames VLAN (VLAN tagging). **Protocole associé : IEEE 802.1Q**

Tagging VLAN :

802.1Q est le standard utilisé pour insérer un **VLAN tag** dans la trame Ethernet. Ce tag permet de transporter plusieurs VLANs sur un même lien physique.

Structure du tag :

Tag Protocol Identifier (TPID) : Identifie la trame comme une trame VLAN (16 bits, valeur hexadécimale 0x8100).

Priority Code Point (PCP) : Permet de prioriser les trames (3 bits).

VLAN Identifier (VID) : Identifie le VLAN (12 bits, **plage de 1 à 4094**, VLAN 0 réservé pour trafic prioritaire).

Ports des switches dans un VLAN :

Access Ports :

Connectés aux équipements finaux (PC, imprimantes, caméras, etc.).

Transmettent uniquement les trames non taggées.

Trunk Ports :

Transmettent les trames taggées entre les switches ou vers des routeurs.

Permettent le transport de plusieurs VLANs sur une seule connexion.

vLANs

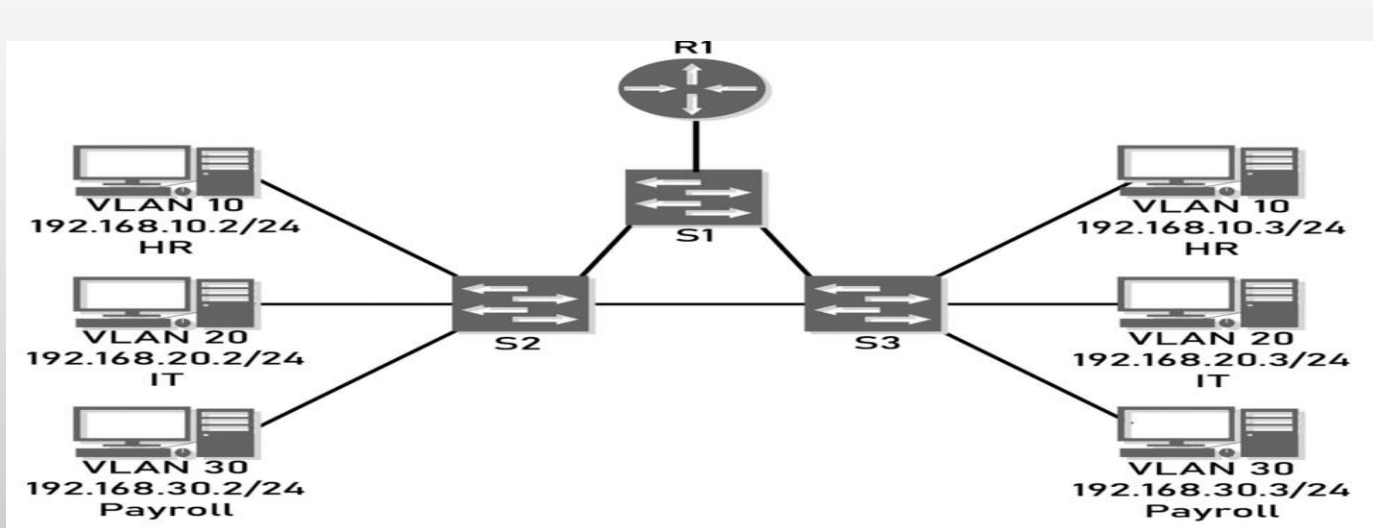
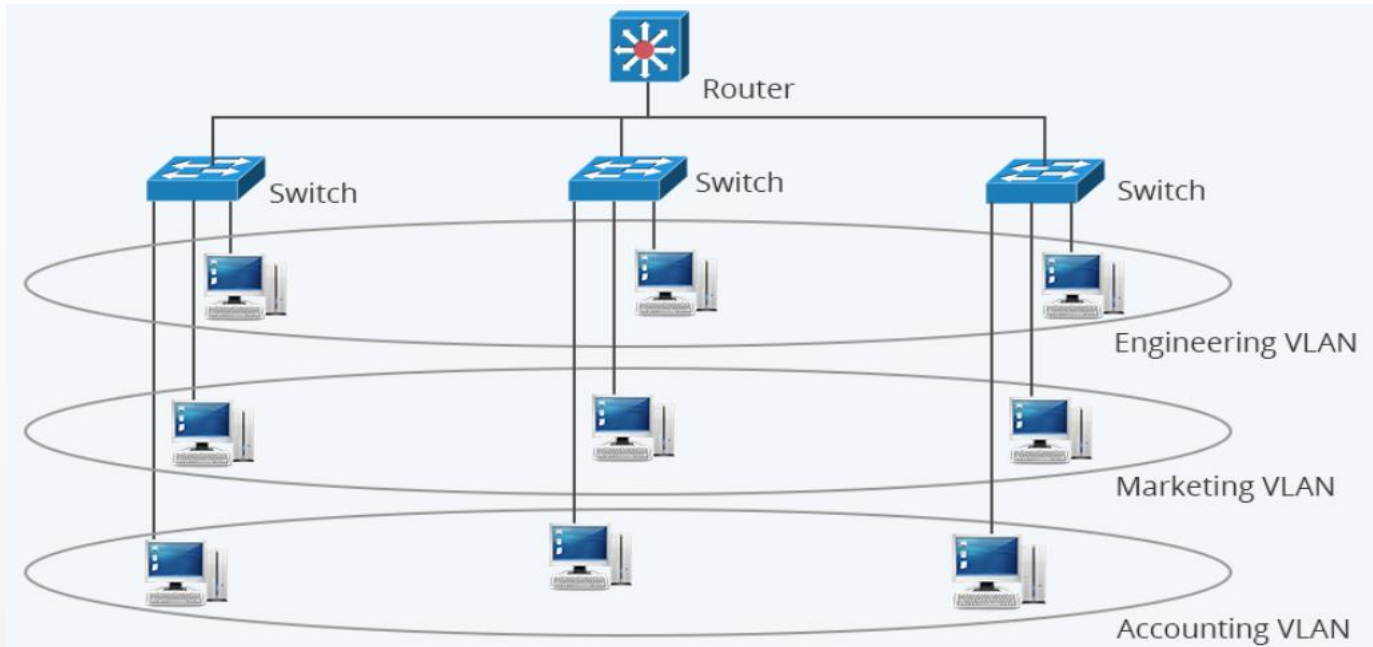
- **Protocole de gestion : VTP (VLAN Trunking Protocol) :**
 - Protocole propriétaire Cisco pour gérer les VLANs sur un réseau de switches.
 - Rôles des switches VTP :
 - **Server** : Crée, modifie ou supprime les VLANs.
 - **Client** : Applique les modifications reçues des serveurs.
 - **Transparent** : Transmet les mises à jour VTP sans les appliquer.
- **Inter-VLAN Routing :**
 - Les VLANs étant isolés, la communication entre eux nécessite un routeur ou un switch de niveau 3 (Layer 3 Switch).
 - Méthodes courantes :
 - **Router-on-a-Stick** : Utilisation d'un seul port routeur configuré en mode trunk.
 - **Layer 3 Switch** : Routage interne basé sur les VLANs.

```
# Création des VLANs
Switch(config)# vlan 10
Switch(config-vlan)# name Finance
Switch(config)# vlan 20
Switch(config-vlan)# name HR

# Configuration d'un port en mode access (pour le VLAN 10)
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10

# Configuration d'un port trunk
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20
```

vLANs



vLANs

Risques de sécurité associés aux VLANs :

1. VLAN Hopping

Principe : Un attaquant force son trafic à accéder à un VLAN non autorisé.

Méthodes courantes :

Switch Spoofing : Le pirate se fait passer pour un switch pour obtenir un accès au VLAN trunk.

Double Tagging : Envoi de paquets avec deux tags VLAN, exploitant la priorité du premier switch.

2. Propagation des tempêtes de diffusion

Une mauvaise configuration peut entraîner des tempêtes de diffusion affectant tous les VLANs.

3. Attaques Man-in-the-Middle (MITM)

Exploitation des failles dans la configuration des VLANs pour intercepter le trafic.

vLANs

Bonnes pratiques pour sécuriser les VLANs

1. Configuration des ports

Utiliser des ports d'accès uniquement pour les hôtes finaux :

Désactiver le mode trunk sur les ports inutilisés.

Associer chaque port à un VLAN spécifique (statique).

Configurer les ports inutilisés :

Désactiver ou associer les ports non utilisés à un VLAN isolé.

2. Sécurisation des trunks

Limiter les VLANs autorisés sur les trunks :

Éviter que tous les VLANs traversent un trunk par défaut.

Désactiver le mode DTP (Dynamic Trunking Protocol) :

Configurer manuellement les trunks pour éviter les attaques de switch spoofing.

3. Protection contre le VLAN Hopping

Double tagging : Configurer les switches pour supprimer les tags supplémentaires.

Switch spoofing : Activer le mode « access » sur tous les ports non trunks.

4. Utilisation de VLANs isolés

VLAN par défaut : Ne pas utiliser le VLAN 1 pour des opérations critiques.

VLAN pour invités : Séparer les invités sur un VLAN dédié et restreint.

vLANs

5. Renforcer l'accès administratif

VLAN management sécurisé :

Utiliser un VLAN dédié uniquement pour la gestion.

Configurer des ACLs pour limiter les IPs autorisées à gérer les switches.

Chiffrement : Activer HTTPS, SSH et SNMPv3 pour les communications d'administration.

Maintenir la Sécurité des vLANs :

Audits réguliers :

Vérifier les configurations des switches.

Analyser les ACLs et les VLANs utilisés.

Outils de supervision réseau :

SolarWinds, Nagios, ou Wireshark pour détecter les anomalies.

Mise à jour du firmware des switches :

Corriger les vulnérabilités connues.

VPN

Un **VPN** est une technologie qui établit une **connexion sécurisée et cryptée** entre deux points sur un réseau non sécurisé (ex. Internet). Cela permet aux utilisateurs ou systèmes de communiquer comme s'ils étaient dans le même réseau local.

Fonctionnalités et Objectifs :

- **Sécurisation des communications :**
 - Chiffrement des données pour garantir la confidentialité (protection contre l'espionnage).
- **Connexion distante sécurisée :**
 - Permet aux employés d'accéder aux ressources internes d'une entreprise depuis n'importe où dans le monde.
- **Masquage de l'adresse IP :**
 - Protège l'identité en masquant l'adresse IP réelle des utilisateurs.
- **Accès à des contenus restreints :**
 - Permet de contourner des restrictions géographiques ou des censures.

VPN

Types de VPN :

○ VPN Site-to-Site :

- Connecte deux réseaux distants (ex. le siège et une succursale).
- Utilisé principalement par les entreprises.

○ VPN Remote Access :

- Connecte un utilisateur individuel au réseau interne d'une organisation.
- Très utilisé pour le télétravail.

○ VPN SSL/TLS :

- Utilise les protocoles SSL ou TLS pour sécuriser les connexions au niveau des applications (ex. accès via un navigateur web).

○ VPN IPsec :

- Sécurise les connexions réseau au niveau de la couche réseau (modèle OSI).

○ VPN MPLS :

- Utilisé par les grandes entreprises pour une interconnexion privée et performante entre sites.

VPN

Avantages :

- Garantit la **confidentialité** et la **sécurité** des données en transit.
- Permet une **mobilité accrue** pour les employés.
- Facilite l'interconnexion sécurisée des réseaux distants.

Exemple d'utilisation :

- Un employé en télétravail utilise un VPN pour accéder au réseau interne de son entreprise.
- Une entreprise multinationale connecte ses filiales via un VPN site-to-site.

Limites :

- Dépendance à la **connexion Internet** : Une mauvaise connexion affecte les performances.
- Complexité de gestion pour les VPN à grande échelle.
- Vulnérabilité si le VPN n'est pas correctement configuré.

VPN vs VLAN

Critère	VLAN	VPN
Objectif principal	Segmentation logique des réseaux	Connexion sécurisée sur des réseaux distants
Portée	Réseau interne	Réseaux internes ou distants
Sécurité	Empêche l'accès non autorisé entre segments	Chiffre les données en transit
Utilisation typique	Isoler les départements au sein d'une entreprise	Accès distant ou connexion sécurisée sur Internet

Comparaison Techniques entre VLAN et VPN :

Aspect	VLAN	VPN
Niveau OSI	Couche 2/3 (données et réseau)	Couche 3 (réseau) ou 4 (transport)
Protocole standard	IEEE 802.1Q	IPsec, SSL/TLS, OpenVPN
Objectif	Segmentation interne du réseau	Connexion sécurisée sur des réseaux distants
Chiffrement	Aucun	Obligatoire pour sécuriser les données
Performance	Haute, dépend de l'équipement	Impactée par le chiffrement

VPN

Protocoles et Standards VPN :

○ IPsec (Internet Protocol Security) :

Protocole standard pour sécuriser les communications au niveau de la couche 3 (réseau).

Fonctionnalités principales :

Authentication : Vérifie l'identité des parties.

Chiffrement : Garantit la confidentialité des données.

Intégrité : Assure que les données ne sont pas altérées.

Modes :

Transport Mode : Chiffre uniquement les données utiles (payload).

Tunnel Mode : Chiffre l'intégralité du paquet IP.

Protocoles associés :

ESP (Encapsulating Security Payload) : Fournit le chiffrement et l'intégrité.

AH (Authentication Header) : Fournit uniquement l'intégrité et l'authentification.

VPN

○ SSL/TLS (Secure Sockets Layer / Transport Layer Security) :

- Utilisé pour les VPN d'accès distant (Remote Access VPN).
- Chiffrement au niveau de la couche 4 (transport).
- Avantage : Peut être utilisé via un navigateur web sans configuration complexe.

○ OpenVPN :

- Solution open-source basée sur SSL/TLS.
- Flexible et supporte une large gamme d'algorithmes de chiffrement.

○ IKEv2/IPsec (Internet Key Exchange Version 2) :

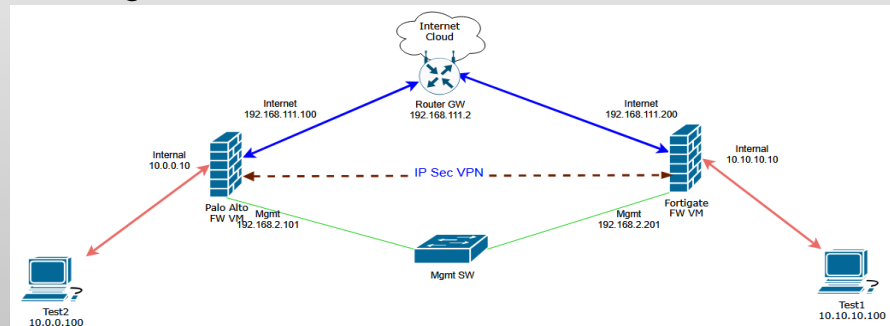
- Utilisé pour négocier et établir des connexions sécurisées.
- Offre une meilleure résilience en cas de changement de réseau (ex. basculement Wi-Fi → 4G).

○ PPTP (Point-to-Point Tunneling Protocol) :

- Protocole obsolète et peu sécurisé, bien que rapide.
- Remplacé par des alternatives comme IPsec ou OpenVPN.

○ WireGuard :

- VPN moderne et léger utilisant des algorithmes de chiffrement avancés.
- Rapide et facile à configurer.



VPN

Fonctionnalités VPN avancées :

- **Split Tunneling :**
 - Permet de définir quel trafic passe par le VPN et quel trafic accède directement à Internet.
- **Double VPN :**
 - Envoie le trafic via deux serveurs VPN pour améliorer la confidentialité.
- **Kill Switch :**
 - Coupe automatiquement la connexion Internet si le VPN est déconnecté.
- **Chiffrement :**
 - Protocoles populaires : AES-256, ChaCha20.

```
crypto isakmp policy 1
  encryption aes
  hash sha256
  authentication pre-share
  group 14
  lifetime 86400

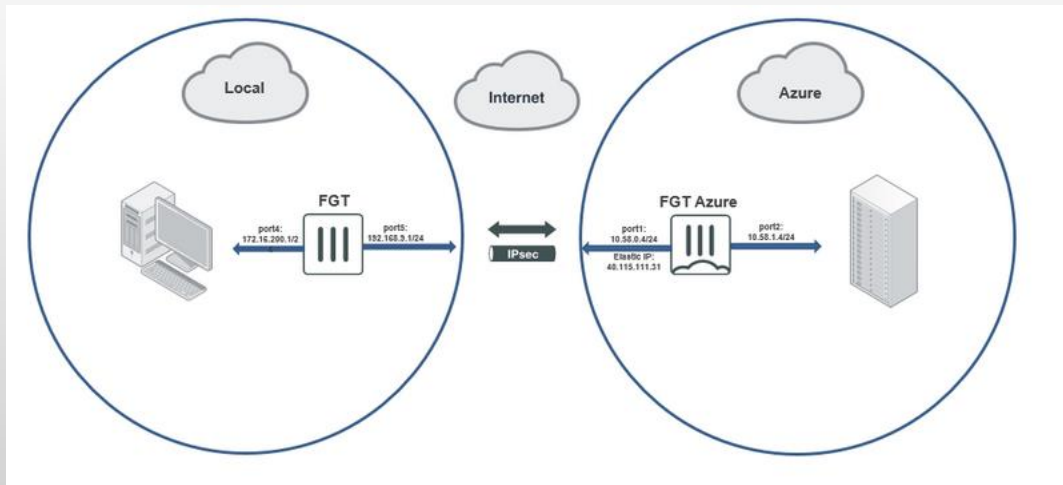
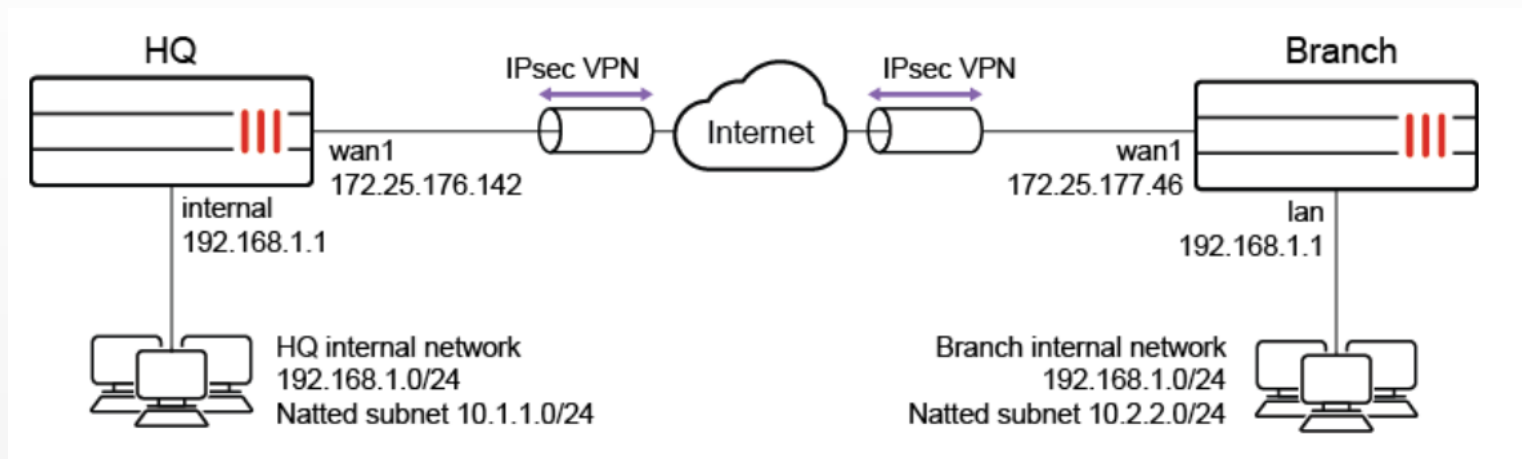
crypto isakmp key VPN_KEY address 192.168.1.1

crypto ipsec transform-set VPN_SET esp-aes esp-sha256-hmac

crypto map VPN_MAP 10 ipsec-isakmp
  set peer 192.168.1.1
  set transform-set VPN_SET
  match address 101

interface GigabitEthernet0/0
  crypto map VPN_MAP
```

VPN



HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE)

- **Qu'est-ce que HTTPS ?**

HTTPS (HyperText Transfer Protocol Secure) est une version sécurisée du protocole HTTP, utilisée pour la communication sur le World Wide Web. Il combine HTTP avec une couche de chiffrement assurée par le protocole TLS (**Transport Layer Security**) ou son prédécesseur SSL (**Secure Sockets Layer**).

- HTTPS est utilisé pour garantir :

Confidentialité :

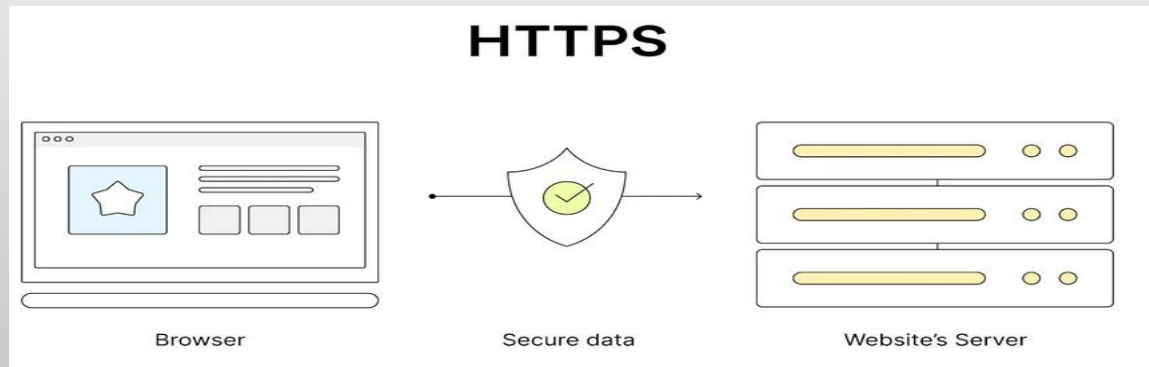
Les données échangées entre le client (navigateur) et le serveur sont chiffrées, rendant leur interception inutile.

Authentification :

Le serveur prouve son identité grâce à un certificat numérique émis par une autorité de certification (CA).

Intégrité :

Les données transmises ne peuvent pas être modifiées ou corrompues en transit sans être détectées.



HTTPS

Fonctionnement Technique du HTTPS

Étapes de la communication HTTPS :

a. Demande HTTPS (Initiation) :

Le client envoie une requête HTTPS (souvent via un navigateur) à un serveur.

b. Établissement du handshake TLS :

Le client et le serveur négocient les paramètres de sécurité via un processus appelé **handshake TLS** :

Le client envoie une liste de **chiffres cryptographiques** (algorithmes) qu'il supporte.

Le serveur sélectionne un chiffre cryptographique commun et envoie son **certificat SSL/TLS**.

Le client vérifie le certificat (authenticité et validité).

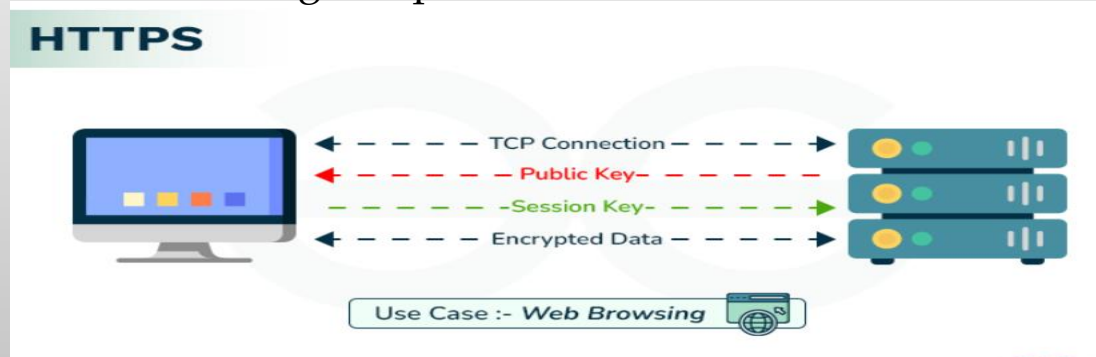
Les deux parties échangent une clé de session (généralement par un processus d'échange de clé RSA, Diffie-Hellman ou ECDHE).

c. Établissement de la clé de session :

Une clé symétrique est générée pour chiffrer les communications.

d. Échange de données sécurisées :

Toutes les données échangées après le handshake sont chiffrées avec la clé de session.



HTTPS

Protocole TLS/SSL :

HTTPS repose sur **TLS** (successeur de SSL), qui assure le chiffrement, l'intégrité et l'authentification.

Les versions courantes :

- **TLS 1.2** : Standard actuel largement utilisé.
- **TLS 1.3** : Plus rapide et plus sécurisé (supprime certains algorithmes obsolètes).

Chiffrement :

- **Symétrique** : Pour les données échangées après le handshake.
- **Asymétrique** : Pendant le handshake pour sécuriser l'échange de la clé de session.

Certificats SSL/TLS

1.Qu'est-ce qu'un certificat SSL/TLS ?

- Un certificat numérique émis par une autorité de certification (**CA**, Certificate Authority).
- Il contient :
 1. Le nom de domaine du site.
 2. La clé publique du serveur.
 3. Des informations sur l'entité propriétaire (organisation ou individu).
 4. La signature de l'autorité de certification.

2.Types de certificats :

1. **DV (Domain Validation)** : Valide uniquement le nom de domaine.
2. **OV (Organization Validation)** : Valide l'organisation propriétaire du site.
3. **EV (Extended Validation)** : Offre un niveau de vérification supérieur, visible dans le navigateur par un cadenas vert ou le nom de l'organisation.

3.Chaîne de confiance :

Le certificat doit être signé par une autorité de certification reconnue, qui elle-même peut être vérifiée par une autre autorité jusqu'à atteindre une autorité racine.

HTTPS

Algorithmes Utilisés dans HTTPS

- **Chiffrement symétrique** (pour le contenu) :
Algorithmes courants : **AES-256, ChaCha20**.
Avantage : Rapide et efficace pour chiffrer de grandes quantités de données.
- **Chiffrement asymétrique** (pour le handshake) :
Algorithmes courants : **RSA (2048/4096 bits), Elliptic Curve Cryptography (ECC)**.
Avantage : Sécurise l'échange de clé mais plus lent.
- **Fonctions de hachage** (pour l'intégrité des données) :
Algorithmes courants : **SHA-256, SHA-384**.
Avantage : Détecte toute modification des données en transit.
- **Échange de clé** :
Méthodes courantes : **Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH)**.

Caractéristique	HTTP	HTTPS
Port	80	443
Chiffrement	Aucun	Oui (via TLS/SSL)
Authentification	Non	Oui (via certificat)
Protection des données	Non (en clair)	Oui (chiffrement des données)
Vérification d'identité	Non	Oui

HTTPS

Avantages :

- **Sécurité accrue :**

Protège contre l'espionnage, le vol de données (ex. mots de passe), et les attaques de type **Man-in-the-Middle (MITM)**.

- **Confiance des utilisateurs :**

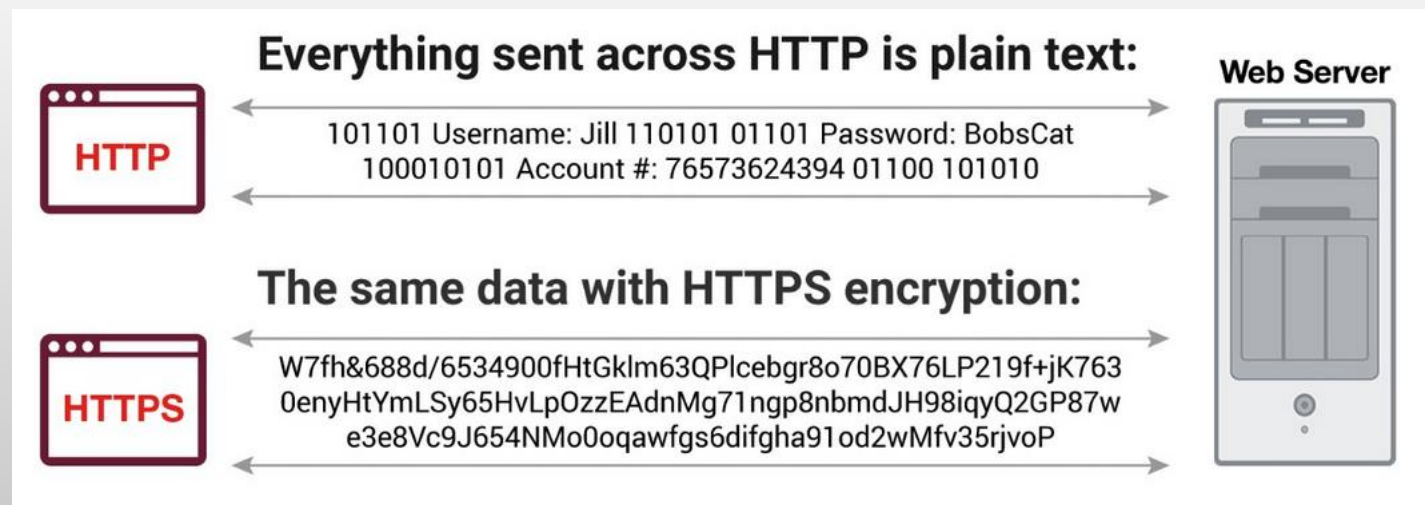
Un site HTTPS montre un cadenas dans la barre d'adresse, rassurant les utilisateurs.

- **SEO (Search Engine Optimization) :**

Google privilégie les sites HTTPS dans ses résultats de recherche.

- **Conformité réglementaire :**

Obligatoire pour certaines législations (ex. RGPD) en cas de traitement de données sensibles.



WI-FI

Le Wi-Fi (Wireless Fidelity) est une technologie de communication sans fil qui permet de connecter des appareils à Internet ou entre eux via un réseau local sans fil (WLAN).

Développé dans les années 1990, il est basé sur les normes IEEE 802.11.

Normes Wi-Fi :

Norme	Année	Fréquence(s)	Débit théorique	Portée (env.)
802.11a	1999	5 GHz	54 Mbps	35 m
802.11b	1999	2.4 GHz	11 Mbps	38 m
802.11g	2003	2.4 GHz	54 Mbps	38 m
802.11n	2009	2.4/5 GHz	600 Mbps	70 m
802.11ac	2014	5 GHz	1.3 Gbps	35 m
802.11ax (Wi-Fi 6)	2019	2.4/5 GHz	9.6 Gbps	70-80 m

WI-FI

Protocoles de sécurité Wi-Fi :

1. WEP (Wired Equivalent Privacy)

Apparu en : 1999

Caractéristiques :

Clé statique de 64 ou 128 bits.

Vulnérable aux attaques (obsolète depuis 2004).

Risques : Faiblesse dans la gestion des clés.

2. WPA (Wi-Fi Protected Access)

Apparu en : 2003

Caractéristiques :

Clé dynamique (TKIP).

Amélioration du WEP, mais toujours vulnérable.

3. WPA2

Apparu en : 2004

Caractéristiques :

Chiffrement AES-CCMP (fort).

Mode entreprise avec 802.1X.

Limite : Vulnérable aux attaques KRACK.

4. WPA3

Apparu en : 2018

Caractéristiques :

Chiffrement 192 bits pour les réseaux d'entreprise.

Simultaneous Authentication of Equals (SAE) : résistance aux attaques par dictionnaire.

WI-FI

Risques de sécurité Wi-Fi :

1. Attaques par déni de service (DoS) : Saturation du réseau avec des signaux parasites.
2. Attaques de type Evil Twin : Création d'un faux point d'accès pour intercepter des données.
3. Interception des communications : Attaques « Man-in-the-Middle » pour capturer les données.
4. Cracking de mots de passe : Via des attaques par dictionnaire ou de force brute.

Bonnes pratiques de sécurité Wi-Fi :

1. Configurer correctement les réseaux

Désactiver le SSID broadcast pour les réseaux sensibles.

Utiliser des noms de réseau non identifiables (éviter « entreprise_wifi »).

2. Renforcer l'authentification

Utiliser WPA3 dès que possible.

Activer 802.1X pour les entreprises.

3. Sécuriser les points d'accès

Modifier les identifiants par défaut.

Déployer un firmware à jour.

4. Segmenter les réseaux

Réseaux séparés pour invités et employés.

VLANs pour compartimenter les flux.

5. Surveiller le réseau

Outils d'analyse Wi-Fi pour détecter les anomalies.

Activer les logs pour identifier les accès non autorisés.

WI-FI

Outils utiles :

Wireshark : Analyse des paquets réseau.

Kismet : Surveillance et détection des intrusions Wi-Fi.

Aircrack-ng : Test de robustesse des clés Wi-Fi.

NetSpot : Cartographie des signaux Wi-Fi.

BONNE PRATIQUE

1.1. Sécurisation des équipements réseau

- **Changer les identifiants par défaut** : Modifiez immédiatement les noms d'utilisateur et mots de passe par défaut des routeurs, switches et autres équipements.
- **Limiter l'accès administratif** :
 - Restreindre l'accès par des ACL (Access Control Lists).
 - Activer l'accès uniquement depuis des IP spécifiques.
- **Désactiver les services inutilisés** : Désactivez les protocoles et services inutiles (par exemple, Telnet, SNMP non sécurisé).
- **Mise à jour régulière** : Appliquez les correctifs et mises à jour de firmware.

1.2. Segmenter le réseau

- Utilisez des **VLANs** pour isoler les différents types de trafic (invités, IoT, production).
- Implémentez un pare-feu interne pour restreindre les communications entre les segments.
- Employez des réseaux séparés pour les zones sensibles (ex. : DMZ pour les serveurs exposés).

BONNE PRATIQUE

1.3. Utilisation de technologies de sécurité réseau

- **VPN** : Chiffrez les connexions distantes avec des protocoles sécurisés comme IPSec ou OpenVPN.
- **Pare-feu** :
 - Implémentez des règles strictes sur les entrées et sorties.
 - Activez l'inspection approfondie des paquets (DPI).
- **IDS/IPS** : Déployez des systèmes de détection ou de prévention des intrusions pour surveiller et bloquer les activités suspectes.
- **WAF (Web Application Firewall)** : Protégez les applications web contre les attaques comme l'injection SQL ou le XSS.

1.4. Surveillance et journalisation

- Activez la journalisation sur tous les équipements réseau.
- Centralisez les journaux avec un SIEM (Security Information and Event Management).
- Configurez des alertes pour les événements critiques (tentatives d'accès non autorisées, attaques DoS).

BONNE PRATIQUE

2.1. Gestion des comptes utilisateur

- **Principe des moindres privilèges** : Les utilisateurs doivent avoir uniquement les droits nécessaires pour accomplir leurs tâches.
- **Authentification forte** :
 - Implémentez une authentification à deux facteurs (2FA) pour tous les accès critiques.
 - Utilisez des mots de passe complexes et renouvelez-les régulièrement.
- **Désactivation des comptes inactifs** : Supprimez ou désactivez les comptes d'utilisateurs qui ne sont plus actifs.

2.2. Mise à jour et gestion des correctifs

- **Mises à jour régulières** : Maintenez les systèmes d'exploitation et logiciels à jour.
- **Correction des vulnérabilités** : Appliquez rapidement les correctifs pour les vulnérabilités critiques identifiées (CVE).
- Utilisez des outils comme WSUS (Windows Server Update Services) pour automatiser les mises à jour.

BONNE PRATIQUE

2.3. Protection contre les logiciels malveillants

- Déployez des solutions antivirus et antimalware sur tous les systèmes.
- Activez les analyses régulières et en temps réel.
- Bloquez l'exécution des scripts et macros non autorisés (ex. : dans les documents Office).

2.4. Sauvegarde et reprise après sinistre

- **Plan de sauvegarde :**
 - Effectuez des sauvegardes régulières des données critiques (quotidiennes ou hebdomadaires).
 - Testez les sauvegardes pour garantir leur récupération.
- **Plan de reprise après sinistre (PRA) :** Élaborez un PRA documenté et testé pour minimiser les interruptions en cas de sinistre.

OUTILS DE GESTION DES RÉSEAUX

1. Surveillance et supervision

- **Nagios** : Supervision des équipements réseau, serveurs et applications.
- **Zabbix** : Solution complète de surveillance réseau et système avec visualisation.
- **PRTG Network Monitor** : Outil tout-en-un pour surveiller les réseaux et les applications.
- **SolarWinds Network Performance Monitor** : Suivi des performances des réseaux complexes.
- **Cacti** : Génère des graphiques pour surveiller les performances réseau.

2. Analyse du trafic réseau

- **Wireshark** : Analyseur de paquets réseau pour diagnostiquer les problèmes et détecter les anomalies.
- **Tcpdump** : Capture et analyse de paquets réseau en ligne de commande.
- **Nmap** : Scanner réseau pour identifier les ports ouverts, services et vulnérabilités.
- **NetFlow Analyzer** : Analyse et rapport du trafic réseau basé sur NetFlow.
- **Angry IP Scanner** : Scanner rapide pour trouver les appareils connectés sur un réseau.

3. Gestion et configuration

- **Cisco Packet Tracer** : Simulation de réseaux Cisco pour formation et tests.
- **Ansible** : Outil d'automatisation pour gérer la configuration réseau et système.
- **PuTTY** : Client SSH/Telnet pour gérer les équipements réseau.
- **WinSCP** : Transfert sécurisé de fichiers via SFTP ou SCP.

OUTILS D'ADMINISTRATION SYSTÈME

1. Gestion des serveurs

- **Cockpit** : Interface web pour gérer les serveurs Linux.
- **Webmin** : Gestionnaire web pour administrer les systèmes Unix/Linux.
- **Hyper-V Manager / VMware vSphere** : Gestion des environnements virtualisés.
- **Active Directory Users and Computers (ADUC)** : Gestion des utilisateurs et groupes sous Windows.
- **PowerShell** : Script pour l'automatisation et la gestion des environnements Windows.

2. Supervision des performances

- **Glances** : Outil de monitoring système multiplateforme (CPU, RAM, disques).
- **htop** : Gestionnaire de tâches interactif pour les systèmes Unix/Linux.
- **Nagios XI** : Supervision avancée des infrastructures systèmes.
- **Zabbix** (open source)

3. Sauvegarde et restauration

- **Veeam Backup & Replication** : Sauvegarde et restauration pour les environnements virtuels et physiques.
- **Clonezilla** : Sauvegarde et clonage de disques/partitions.
- **Rsnapshot** : Sauvegarde incrémentielle pour systèmes Unix/Linux.
- **Windows Server Backup** : Sauvegarde intégrée pour les serveurs Windows.

OUTILS CYBERSEC

1. Détection des vulnérabilités

- **Nessus** : Scanner de vulnérabilités pour les infrastructures réseau et système.
- **OpenVAS** : Solution open-source pour l'analyse des vulnérabilités.
- **Qualys** : Scanner SaaS pour les vulnérabilités et la conformité.
- **Burp Suite** : Analyse des failles des applications web.

2. Protection

- **Snort** : Système de détection/prévention d'intrusion (IDS/IPS).
- **Suricata** : Alternative à Snort, offrant des fonctionnalités similaires.
- **Fail2Ban** : Blocage des adresses IP en cas de tentatives répétées de connexion échouées.
- **Bitdefender GravityZone** : Solution EDR pour protéger les postes de travail et serveurs.

3. Audit et journalisation

- **Splunk** : Plateforme de gestion des journaux et des données machine.
- **Graylog** : Plateforme open-source pour l'analyse des logs.
- **ELK Stack (Elasticsearch, Logstash, Kibana)** : Collecte, analyse et visualisation des journaux.
- **Syslog-ng** : Collecte et gestion des journaux système.

TESTS ET DIAGNOSTICS

- **Iperf** : Mesure des performances réseau (débit, latence).
- **Ping/ Traceroute** : Diagnostic des problèmes de connectivité.
- **MTR (My Traceroute)** : Combinaison de ping et traceroute pour analyser les connexions réseau.
- **Speedtest CLI** : Mesure la vitesse Internet en ligne de commande.

LIENS DES SERVICES CYBERSEC UTILES

VirusTotal : Analyse de fichiers et d'URLs pour détecter les malwares à l'aide de multiples moteurs antivirus.

<https://www.virustotal.com/>

AlienVault Open Threat Exchange (OTX) : Plateforme communautaire de partage d'informations sur les menaces.

<https://otx.alienvault.com/>

Sucuri SiteCheck : Scanner en ligne pour détecter les malwares et vulnérabilités sur les sites web.

<https://sitecheck.sucuri.net/>

SSL Labs : Outil d'analyse de la configuration SSL/TLS des serveurs web pour évaluer leur sécurité.

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

Have I Been Pwned : Service permettant de vérifier si une adresse e-mail ou un domaine a été compromis dans une violation de données.

<https://haveibeenpwned.com/>

Wappalyzer : identifier les technologies Web

LIENS DES OUTILS CYBERSEC UTILES

1. Outils en ligne pour le diagnostic réseau

Pingdom : Test de disponibilité et de temps de réponse des serveurs web.

<https://www.pingdom.com/>

MTR Online (My Traceroute) : Analyseur combinant Ping et Traceroute pour diagnostiquer les problèmes de connectivité.

<https://mtr.sh/>

DNS Propagation Checker : Vérifiez la propagation des enregistrements DNS sur Internet.

<https://dnschecker.org/>

IntoDNS : Vérifiez la configuration DNS d'un domaine et obtenez des recommandations de correction.

<https://intodns.com/>

MXToolbox : Diagnostiquez les problèmes de messagerie (MX, SPF, DKIM, etc.) et DNS.

<https://mxtoolbox.com/>

2. Détection des problèmes de connectivité

Speedtest by Ookla : Mesure la latence, le débit descendant et montant pour tester les performances réseau.

<https://www.speedtest.net/>

Cloudflare Radar : Obtenez des insights globaux sur les performances Internet, les interruptions et les cybermenaces.

<https://radar.cloudflare.com/>

WhatIsMyIP : Identifiez rapidement l'adresse IP publique et vérifiez les informations associées.

<https://www.whatismyip.com/>