ANNÉE PASSERELLE EN INGÉNIERIE

Chapitre 19 — Sécurité

Introduction à la Téléinformatique

Vincent Audergon · HEIA-FR

Année académique 2026-2027

Plan du chapitre

Objectifs du chapitre

HEIA-FR
HTA-FR

À l'issue de ce chapitre, vous saurez :

- **définir** les concepts de sécurité informatique et de cybersécurité ;
- **expliquer** les différents types de menaces et d'attaques informatiques courantes ;
- **lister** les éléments d'une infrastructure qui permettent d'augmenter la sécurité.

SECTION

01

Sécurité et authentification

Security vs Safety

HEIA-FR
HTA-FR

DÉFINITION · SÉCURITÉ DES SYSTÈMES D'INFORMATION

Ensemble des moyens techniques, organisationnels, juridiques et humains visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. (Wikipedia)

Security

Protection contre les menaces et attaques **externes** : cyberattaques, vol de données, intrusions.

Safety

Protection contre les risques **internes** : erreurs humaines, défaillances matérielles, accidents.

Les facteurs d'authentification

Cinq catégories de facteurs, combinables :

- **Connaissance** : mot de passe, code PIN, question secrète.
- **Possession** : carte à puce, clé USB, smartphone.
- **Inhérence** : empreinte digitale, scan de l'iris.
- **Localisation** : adresse IP, emplacement géographique.
- **Comportement** : schéma de frappe, rythme de marche.

> **REMARQUE**
> **MFA** (Multi-Factor Authentication) : au moins deux facteurs combinés. **SSO** (Single Sign-On) : une seule authentification pour plusieurs services.

? QUESTION 1

Pour accéder à un bâtiment sécurisé, vous présentez une carte d'accès et entrez un code PIN. Quels facteurs sont utilisés ?

> **RÉPONSE**
> **Possession** (la carte d'accès) et **connaissance** (le code PIN) : c'est de l'authentification **multi-facteurs**.

SECTION
02 —

Menaces et attaques

D'où viennent les menaces ?

- **Les utilisateurs** eux-mêmes, par négligence ou insouciance.
- **Une personne malveillante** : un hacker qui exploite des vulnérabilités.
- **Un groupe organisé** : cybercriminels, hacktivistes, espionnage industriel ou étatique.
- **Un malware** : virus, ver, cheval de Troie, ransomware...
- **Un sinistre** naturel, criminel ou accidentel : incendie, panne, vol.

REMARQUE
La sécurité vise à **mitiger** ces menaces : mises à jour, pare-feu, antivirus, sauvegardes, formation des utilisateurs, politiques de sécurité.

Familles d'attaques

- **Interceptions** :
  - **Spoofing** : usurpation d'identité
  - **Man-in-the-middle** : interception et modification de communications
- **Vol de session** (Session hijacking) : détournement d'une session active
- **Attaques physiques** : accès non autorisé, coupure de câbles, vol de matériel
- **Intrusions** :
  - **Vol de données** : accès non autorisé à des informations sensibles
  - **Destruction ou modification de données**

Familles d'attaques (suite)

- **Dénis de service** :
  - **DoS** (Denial of Service) : surcharge d'un service pour le rendre indisponible
  - **DDoS** (Distributed Denial of Service) : attaque DoS depuis plusieurs sources
  - **Attaque par paquet malformé** : envoi de paquets corrompus pour provoquer un crash
- **Social engineering** :
  - **Phishing** : hameçonnage par e-mail ou message
  - **Spear phishing** : phishing ciblé sur une personne ou un groupe
  - **SPAM** : envoi massif de messages non sollicités
  - **Désinformation** : diffusion de fausses informations pour tromper ou manipuler

Le phishing, en pratique

DÉFINITION · PHISHING

Faux e-mail ou message incitant la victime à divulguer des informations sensibles (mot de passe, numéro de carte). La **peur** est souvent utilisée pour pousser à agir sans réfléchir.

- **Spear phishing** : attaque **ciblée**, message personnalisé.
- **SPAM** : envoi **massif**, non ciblé.

ATTENTION
Les IA génératives facilitent aujourd'hui la création de désinformation crédible (faux articles, images, vidéos) : la vigilance et l'esprit critique restent essentiels.

? QUESTION 2

Un attaquant envoie un e-mail personnalisé au CFO d'une entreprise, imitant le PDG, pour lui demander un virement urgent. De quel type d'attaque s'agit-il ?

RÉPONSE
Du **spear phishing** : une attaque de phishing **ciblée**, personnalisée pour tromper une personne précise (par opposition au spam, massif et non ciblé).

SECTION
03

Logiciels malveillants

Logiciel malveillant

- « malware » en anglais, contraction de **malicious software**.
- Logiciel conçu pour être nuisible envers un système informatique, ses utilisateurs ou ses données.
- Critères pour classer un malware :
  - **Mode de propagation** : comment il se propage (ex. par e-mail, réseau, clé USB).
  - **Mode de déclenchement** : comment il s'active (ex. à l'ouverture d'un fichier, à une date précise, à la connexion à Internet).
  - **Charge utile** : ce qu'il fait une fois installé (ex. vol de données, chiffrement, destruction, espionnage).

Les familles de malware

- **Virus** : infecte d'autres fichiers, nécessite une action de l'utilisateur.
- **Ver (worm)** : se propage seul à travers le réseau, sans intervention.
- **Cheval de Troie** : se fait passer pour un logiciel légitime.
- **Ransomware** : chiffre les fichiers, exige une rançon.
- **Keylogger** : enregistre les frappes clavier.
- **Rootkit** : prend le contrôle du système en restant caché.
- Bien d'autres encore : spyware, adware, etc.

? QUESTION 3

Quelle est la différence essentielle entre un **virus** et un **ver** ?

> **RÉPONSE**
> Le virus a besoin d'une **action de l'utilisateur** pour se propager (exécuter un fichier infecté). Le ver se propage **seul**, en exploitant des vulnérabilités réseau, sans intervention humaine.

Moyens de protection

- Mise à jour régulière des systèmes et logiciels
- Utilisation d'antivirus
- Pare-feu
- IDS/IPS (Intrusion Detection/Prevention System)
- VPN (Virtual Private Network)
- Chiffrement par SSL/TLS
- Formation des utilisateurs et sensibilisation à la sécurité
- Bien d'autres encore : sauvegarde, utilisation de mots de passe forts, authentification multi-facteurs, etc.

SECTION
04

Pare-feu et zones réseau

Trois types de pare-feu

Type	Principe	Couches OSI
Stateless	Filtre chaque paquet individuellement, sans contexte	3–4
Stateful	Tient compte de l'état de la connexion	3–4
Applicatif	Inspecte le contenu et les protocoles applicatifs	7

REMARQUE
Les pare-feu modernes combinent souvent plusieurs de ces approches.

Interne, DMZ, externe

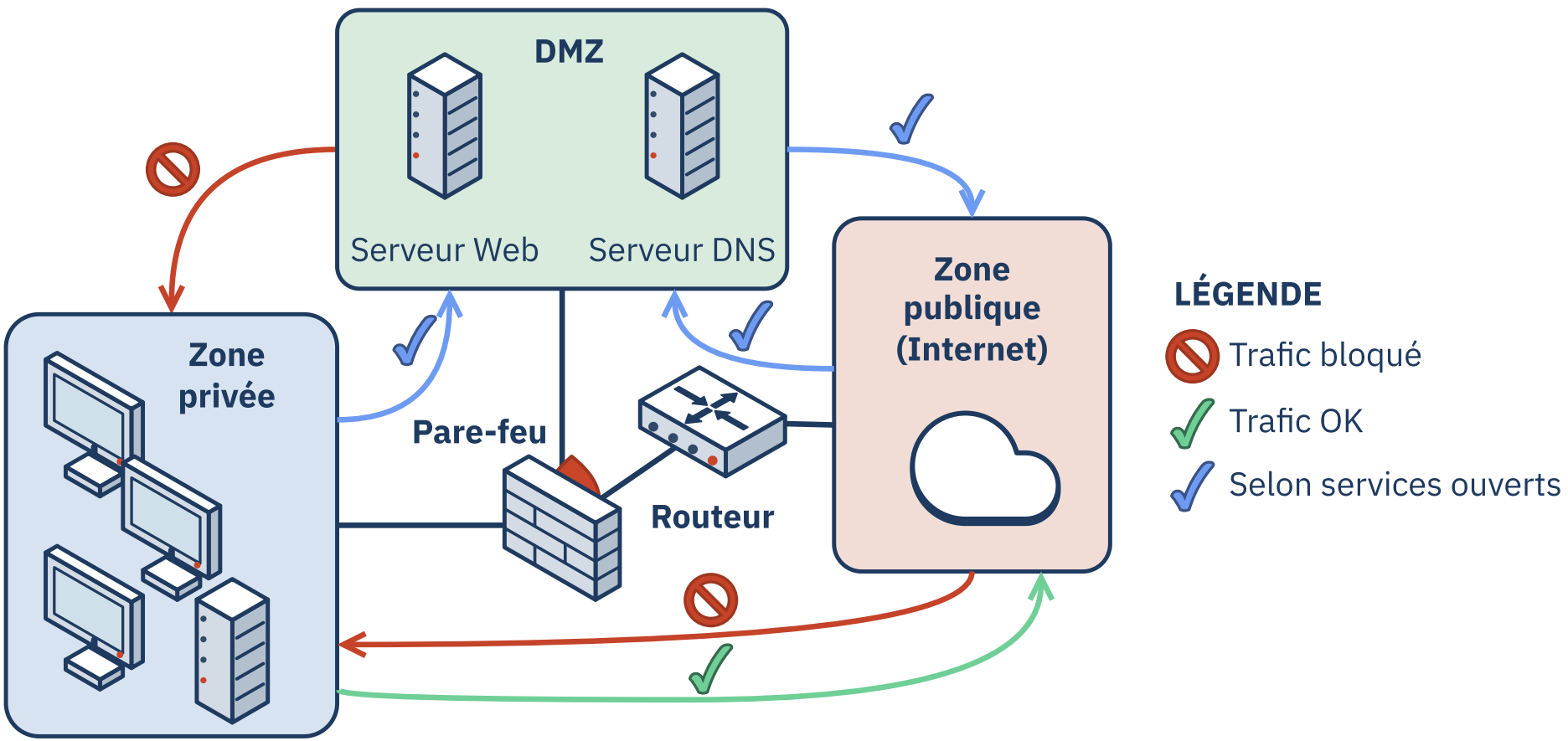
Un réseau est souvent segmenté en trois zones :

- **Privé** : réseau interne de l'entreprise, protégé par le pare-feu.
- **DMZ** (Demilitarized Zone) : zone intermédiaire pour les services accessibles depuis Internet (ex. serveur web, serveur mail).
- **Public** : Internet, zone non sécurisée, accessible à tous.

DÉFINITION · DMZ (DEMILITARIZED ZONE)

Zone intermédiaire entre le réseau interne et Internet, où sont placées les ressources accessibles depuis l'extérieur (serveurs web, mail, FTP), isolées du réseau interne.

Interne, DMZ, externe



Les règles de flux entre zones

Flux	Autorisé ?
Privé → Public	Oui
Privé → DMZ	Oui, limité aux services nécessaires
DMZ → Public	Oui, limité (DNS, mises à jour…)
DMZ → Privé	Non
Public → DMZ	Oui, limité aux services exposés
Public → Privé	Non

REMARQUE

Principe du **moindre privilège** : seules les communications nécessaires sont autorisées, tout le reste est bloqué par défaut (dernière règle de la liste).

? QUESTION 4

Vous installez un serveur web accessible depuis Internet (HTTP/HTTPS), et administrable en SSH depuis le réseau interne. Où le placer, et quelles règles de pare-feu prévoir ?

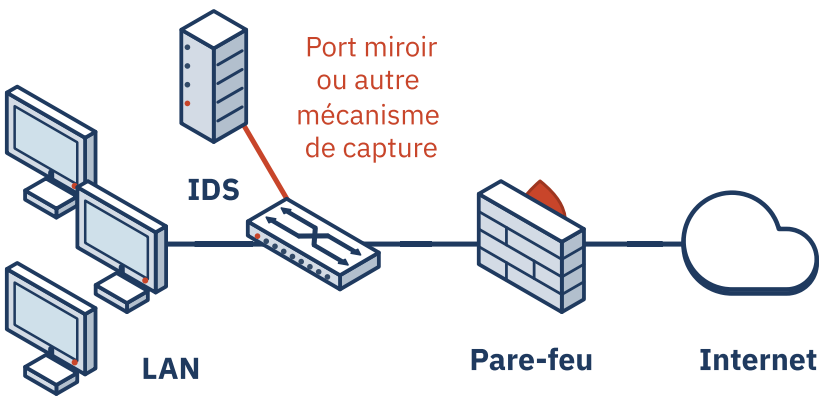
RÉPONSE

Dans la **DMZ**. Autoriser Public → DMZ sur les ports **80/443**, et Privé → DMZ sur le port **22** (SSH) ; bloquer tout le reste, notamment DMZ → Privé.

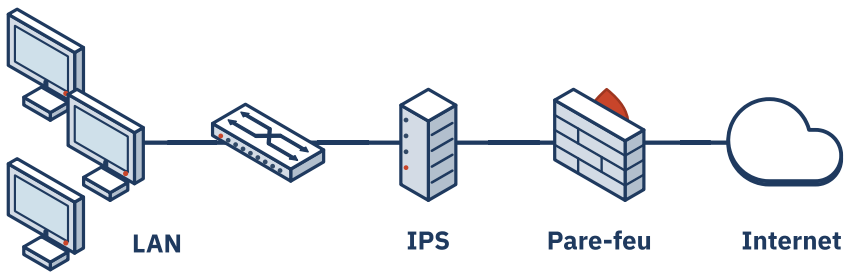
IDS et IPS

- Système de détection d'intrusion (IDS) : surveille le trafic réseau et alerte en cas d'activité suspecte.
- Système de prévention d'intrusion (IPS) : surveille le trafic réseau et bloque activement les attaques détectées.
- IDS/IPS peuvent être basés sur des signatures (reconnaissance de motifs connus) ou sur des anomalies (détection de comportements inhabituels).

IDS vs IPS



IDS, reçoit une **copie** du trafic (out-of-band), **détecte** et alerte.



IPS, placé **in-line**, **bloque** activement le trafic suspect en temps réel.

> **REMARQUE**
> Un IDS/IPS ne remplace pas un pare-feu : c'est un **complément** qui renforce la détection et la prévention des intrusions.

SECTION

05 —

VPN

Le VPN, un tunnel chiffré

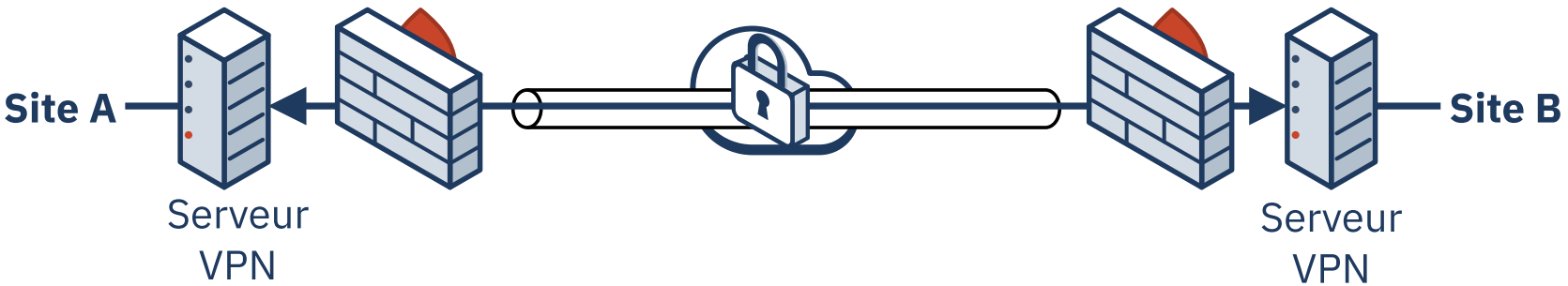
DÉFINITION · VPN (VIRTUAL PRIVATE NETWORK)

Réseau privé virtuel chiffré qui relie deux réseaux sûrs à travers un réseau public, en garantissant **confidentialité**, **intégrité** et **authenticité**.

ATTENTION
VPN ≠ sécurité absolue : il chiffre le trafic entre deux points, et c'est tout.

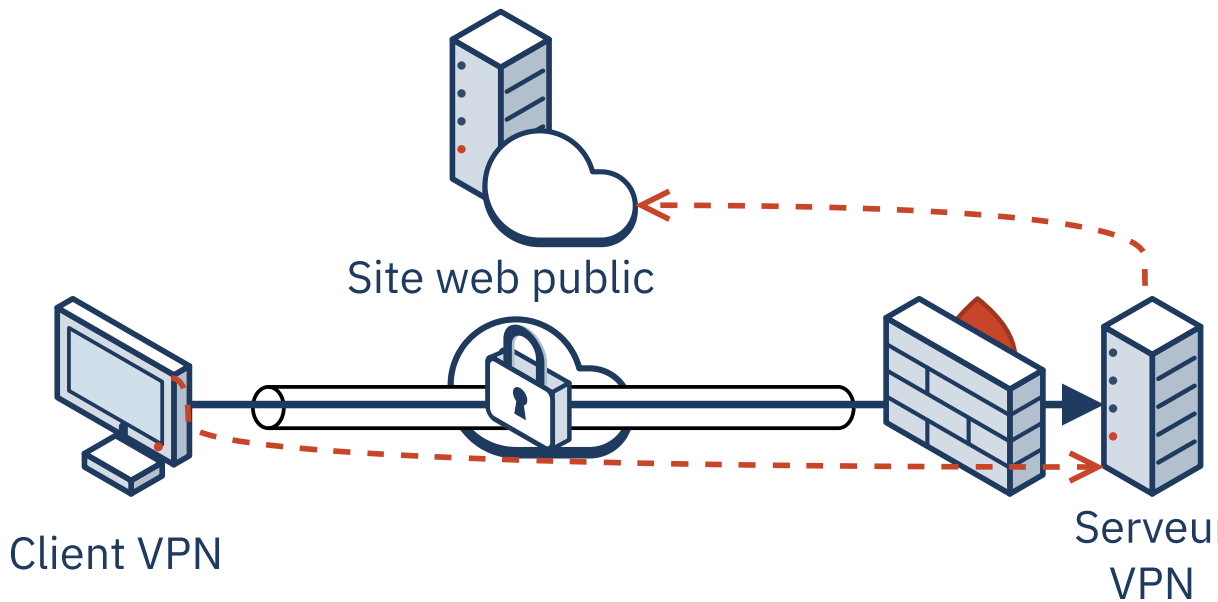
- Deux types de connexions VPN :
  - **Site-à-site** : deux sites d'entreprise reliés via Internet, de façon transparente pour les utilisateurs.
  - **Client-à-site** : un particulier protège son trafic et masque son IP derrière celle du serveur VPN.

VPN site-à-site vs client-à-site



Site-à-site : deux sites d'entreprise reliés via Internet, de façon transparente pour les utilisateurs.

VPN site-à-site vs client-à-site



Client-à-site : un particulier protège son trafic et masque son IP derrière celle du serveur VPN.

SECTION

06 —

Chiffrement par SSL/TLS

SSL/TLS, c’est quoi ?

- **SSL** (Secure Sockets Layer), renommé **TLS** (Transport Layer Security)
- Protocole de chiffrement des communications sur Internet, notamment pour le web (HTTPS).
- Garantit **confidentialité**, **intégrité** et **authenticité** des données échangées.
- Système de certificats et de clés publiques/privées.
- Le certificat est émis par une autorité de certification (CA) de confiance, qui vérifie l’identité du serveur.

ATTENTION
HTTPS (et TLS en général) garantit **confidentialité**, **intégrité** et **authenticité** des données échangées entre le client et le serveur. Il ne garantit pas que le site est sûr ou digne de confiance.

SSL/TLS, en quatre étapes

1. **Négociation** de la version et des algorithmes de chiffrement.
2. **Authentification** du serveur (certificat numérique).
3. **Établissement** d'une clé de session partagée.
4. **Chiffrement** et transmission des données.

? QUESTION 5

Un cadenas s’affiche dans la barre d’adresse de votre navigateur. Que garantit-il exactement, et que ne garantit-il **pas** ?

RÉPONSE

Il garantit que la communication est **chiffrée** et que l’identité du serveur a été **vérifiée** par une autorité de certification. Il ne garantit **pas** que le site est sûr ou dépourvu de contenu malveillant.

Synthèse

HEIA-FR
HTA-FR

CE QU'IL FAUT RETENIR

- La sécurité repose sur **confidentialité**, **intégrité**, **authenticité**, la sécurité **n'est jamais absolue** et a un **coût**.
- Menaces (utilisateurs, attaquants, malware, sinistres) vs attaques (interception, intrusion, DoS, ingénierie sociale).
- Types de malwares : virus, ver, cheval de Troie, etc.
- Le pare-feu segmente le réseau en zones **privée / DMZ / publique** selon le **moindre privilège**.
- **IDS** détecte, **IPS** bloque ; **VPN** chiffre un tunnel ; **TLS** sécurise une session applicative.

Synthèse (suite)

CE QU'IL FAUT RETENIR

- L’authentification repose sur cinq facteurs : connaissance, possession, inhérence, localisation, comportement.
- **MFA** : authentification multi-facteurs ; **SSO** : authentification unique.
- Le phishing est une attaque d’ingénierie sociale visant à obtenir des informations sensibles.
- Le chiffrement SSL/TLS sécurise les communications sur Internet, notamment pour le web (HTTPS).

Des questions ?

Sources

Les sources utilisées pour ce cours (normes, documentation officielle, articles, ouvrages de référence) sont citées et listées intégralement dans la **bibliographie du support de cours écrit**, disponible sur le site du cours :

https://api-teleinfo.isc.heia-fr.ch