

3 - Architectures, Composants et Sécurité

Eléments de cybersécurité d'entreprise

Yann Arzel LE VILLIO

yann-arzel.levillio@orange.com [umaila](#)

<http://campus.orange.com>

Orange CyberSchool
Direction technique & scientifique

Publication Eléments de cours du
28 juillet 2023, 15 h 35 CEST



CYBERDEF 101
Eléments de cybersécurité
et de cyberdéfense
d'entreprise





Abstract

Hashtags : Architectures, composants sécurité, SSI

Ce document présente les architectures, Composants de cybersécurité.

Sommaire

1. Introduction Architecture

2. De l'analyse de risques aux fonctions de sécurité

3. Architecture et composants de système d'information

4. Modèles de sécurité et technologies de sécurité protectrices

5. Sécurité Endpoints

6. Contributions





Architectures, Composants et Sécurité

1. De l'analyse de risques aux fonctions de sécurité
2. Architecture et composants de système d'information
3. Modèles de sécurité et technologies de sécurité protectrices
4. Sécurité Endpoints



De l'analyse de risques aux fonctions de sécurité

1. Filtrage : cloisonnement, Multitenant
2. Accès : RBAC (Role Based Access Control), droit d'en connaître
3. Cryptographie : intégrité des données, protection des flux (IPSec, VPN SSL)



Architecture et composants de système d'information

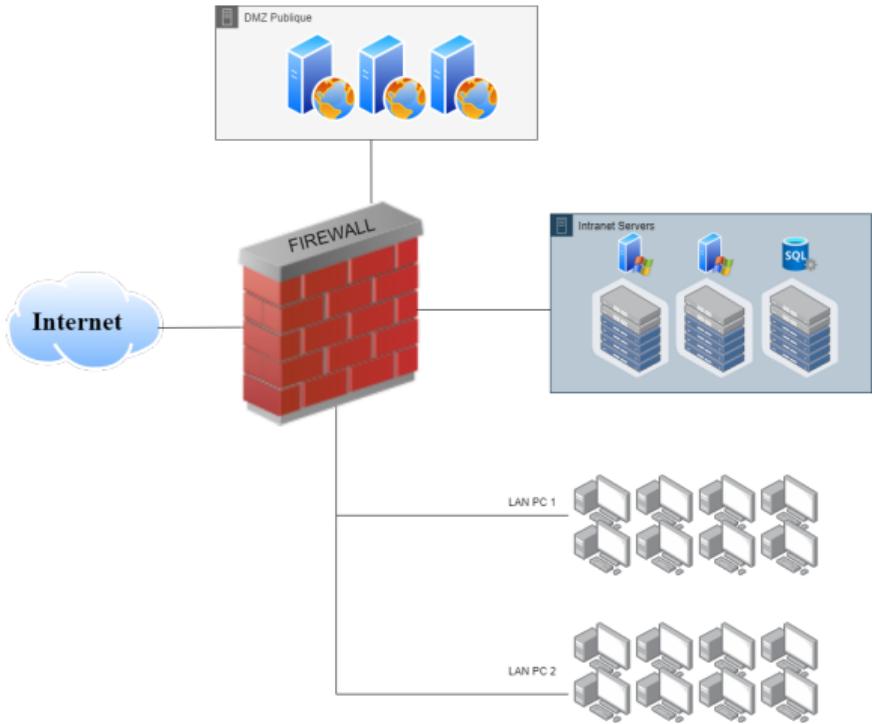
1. Front : Web, applications mobiles, clientless
2. Middle : BDD, Messagerie, ERP
3. Endpoints : PC, mobile, IoT
4. Réseau : traçabilité de tt accès, transactions et anomalies (bugs, erreurs, détection)

Modèles de sécurité et technologies de sécurité protectrices





Château fort





Modèles de sécurité et technologies de sécurité protectrices

- stateless (Access Control List : ACL)
- statefull
- Next generation



Modèles de sécurité et technologies de sécurité protectrices

Schéma Proxy

Modèles de sécurité et technologies de sécurité protectrices

Schéma Reverse Proxy





Modèles de sécurité et technologies de sécurité protectrices

Schéma sondes de détection (IDS/IDP)



Gestion des identités : IAM

- Définition
 - IAM (identity and access management)
 - IAG (identity access governance)
 - DAG (data access governance)
 - PAM (privileged access management)
- Process Gestion des identités - cycle de vie
- Procédures Contrôle des habilitations

Zerotrust



- Définition
- Exemples Schéma ?

Bastion

schéma



VPN SSL

schéma



NAC

- Définition
- Exemples Schéma ?



Multi Cloud - CASB



- Définition
- Exemples Schéma ?



des questions ?



Contributions



Les notes et les présentations sont réalisées sous \LaTeX .

Vous pouvez contribuer au projet du cours CYBERDEF101. Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. A chaque session des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de vos expertises dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace :

(edufaction/CYBERDEF101) ^a.

a. <https://github.com/edufaction/CYBERDEF101>

Mises à jour régulières

Vérifiez la disponibilité d'une version plus récente de

Orange-Cyberdef101-M3-Architectures.prz.pdf sur GITHUB CYBERDEF 



2023 eduf@ction - Publication en Creative Common BY-NC-ND



CYBERDEF 101
Eléments de cybersécurité
et de cyberdéfense
d'entreprise

