

3 - Architectures, Composants et Sécurité

Eléments de cybersécurité d'entreprise

Yann Arzel LE VILLIO

yann-arzel.levillio@orange.com

<http://campus.orange.com>

Orange CyberSchool
Direction technique & scientifique

Publication Eléments de cours du
9 octobre 2023, 22 h 01 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





Construire une architecture sécurisée : politique, sécurité des solutions, identification des composants

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)

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

Cryptographie



- Cryptologie : science du secret
- Algorithmes
 - Chiffrement à clefs secrètes
 - Cryptographie à clefs publiques
 - Fonction de hachage
 - Clefs

Cryptographie



- Taille de clefs : 2048 bits
- Aléas et générateur d'aléas
- Protocoles et formats
- Certificats auto-signés
- IGC (infrastructure de gestion de clefs) ou PKI (public key infrastructure)



- pour les équipes réseaux : tunnels IPSEC, VPNSSL, chiffreurs réseaux
- pour les équipes des services informatiques : le déploiement, la mise à jour des certificats sur des terminaux et des serveurs concentrent une bonne partie des problèmes opérationnels
- pour la bureautique et le poste de travail : les produits et les services pour chiffrer les données et préserver la confidentialité dans les messageries ou sur les supports (smartdevice, disques, USB, serveur de fichiers) sont complexes à choisir pour l'interopérabilité ;
- pour les métiers de l'entreprise comme les achats ou l'archivage probant, les enjeux d'authenticité, d'imputabilité et d'intégrité ainsi que la signature électronique nécessitent des travaux transverses à l'entreprise souvent coûteux.



- Usure ou rupture cryptographique : la cryptographie quantique, quels sont les nouveautés et les risques ?
 - rupture de la sécurité de la cryptographie classique
 - compromission de la confidentialité des communications
- Blockchain, Crypto-monnaies, NFT (Non-Fungible Tokens)



1. Architectures logicielles - Monolithe vs microservices
 - FrontEnd : Web, applications mobiles, clientless
 - Backend
 - Bases de données
2. Middleware : Messagerie, ERP
3. Endpoints : PC, mobile, IoT
4. Réseau : traçabilité de tt accès, transactions et anomalies (bugs, erreurs, détection)

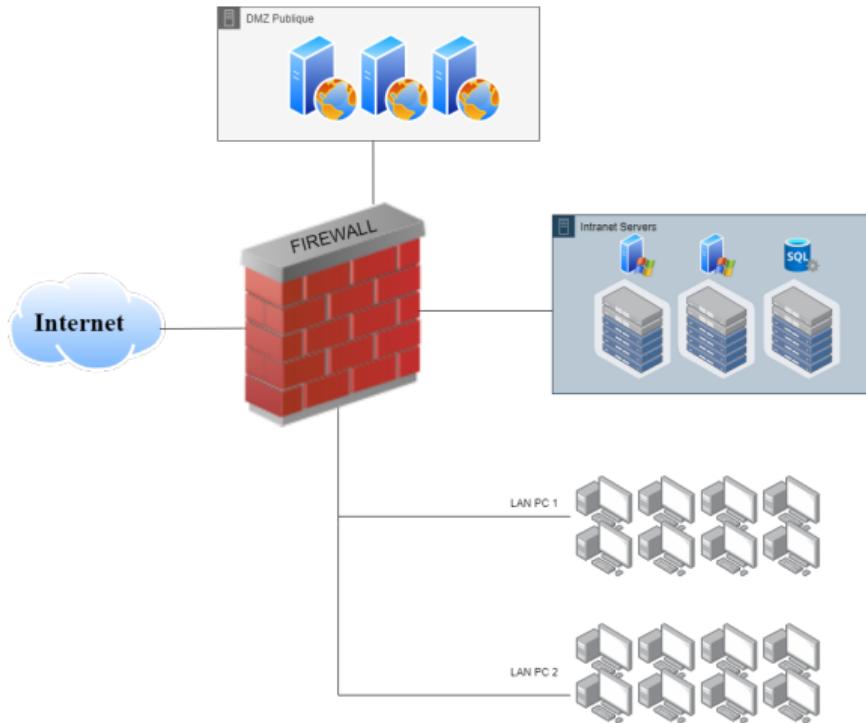
Modèles de sécurité et technologies de sécurité protectrices



Depuis le modèle du château fort jusqu'aux solutions de sécurité utilisées dans les déploiements CLOUD

#Firewall #Proxy #ReverseProxy #IDS/IDP #ZeroTrust #Bastion #VPN #CASB #SASE

Château fort

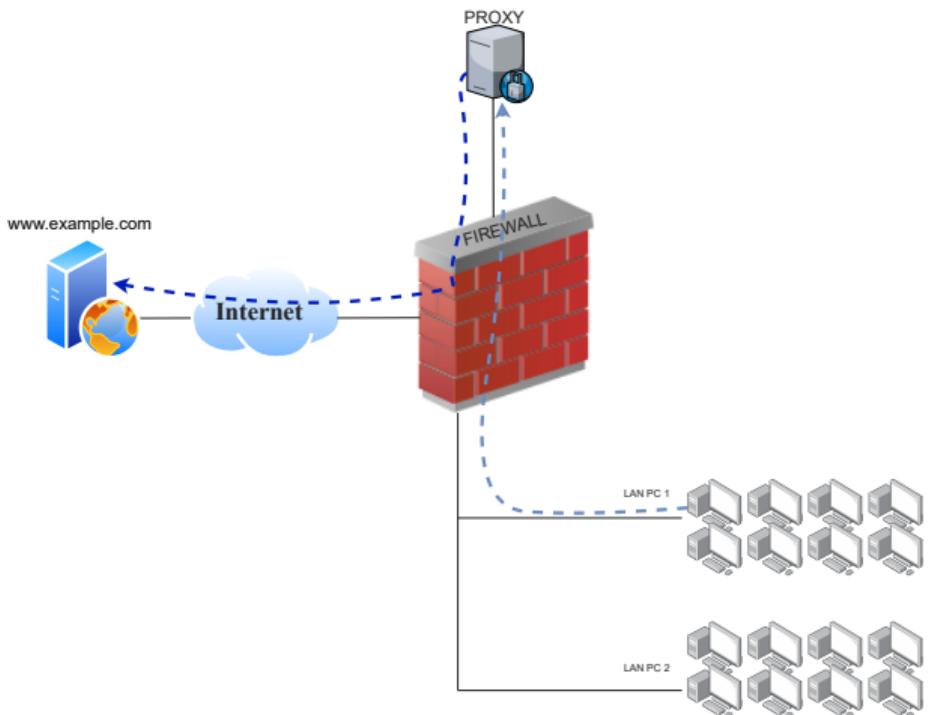


Firewall

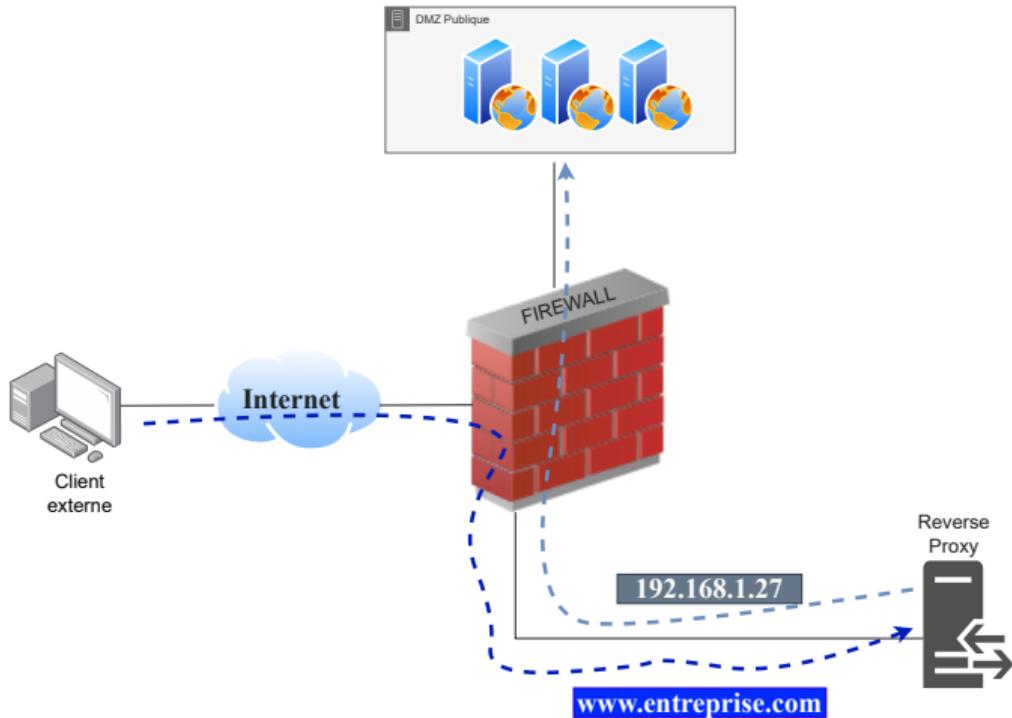


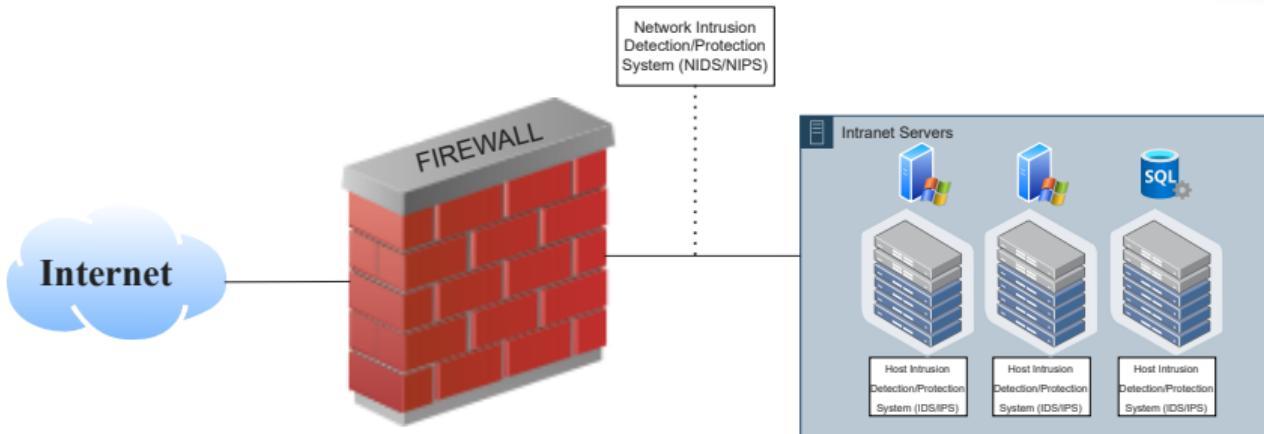
- Fonctions sécurité : filtrage et cloisonnement
- Le pare feu empêche et jette les flux illégitimes
- Seuls ceux autorisés sont routés vers les destinations

Proxy



ReverseProxy







- Limites du modèle de sécurité périmétrique : télétravail, Cloud, BYOD -> réduction du contrôle VS augmentation de la menace
- Le modèle impose :
 - une réduction de la confiance implicite aux utilisateurs
 - ajout de contrôles et de politique d'accès aux ressources



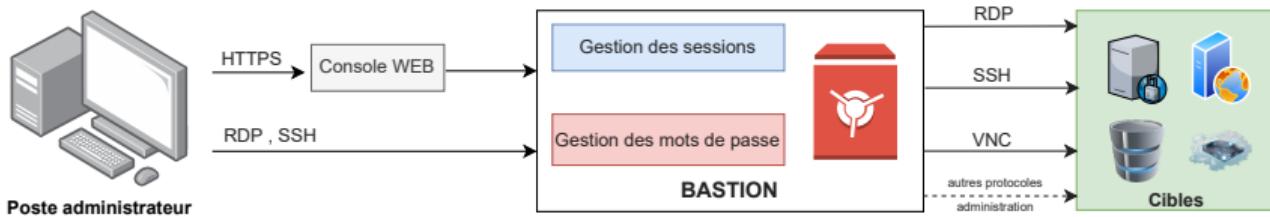
Les actions d'administration imposent entre autres des exigences de traçabilité et de confidentialité. La figure ci-dessous présente la mise en œuvre de rebonds dans une zone d'administration permettant d'appliquer un certain nombre de traitements tels

le filtrage des connexions, l'authentification des administrateurs sur un portail frontal, un contrôle d'accès ou encore la journalisation des actions effectuées et des commandes exécutées par les administrateurs. le bastion constitue une ressource d'administration critique dans la mesure où il concentre potentiellement à un instant des secrets d'authentification des comptes d'administration ou des journaux liés aux actions d'administration. Il ne doit donc pas être exposé sur un SI de faible niveau de confiance, un SI bureautique par exemple.

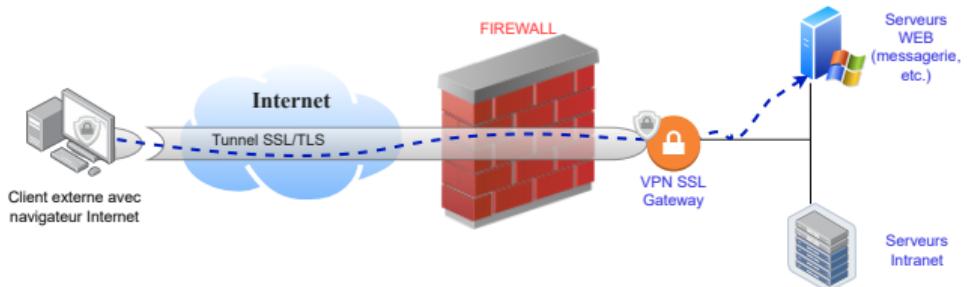
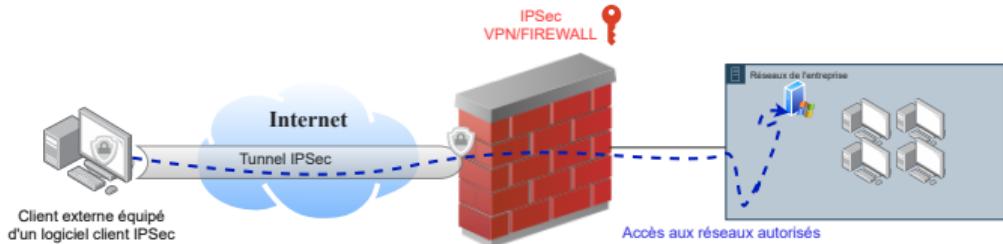
ANSSI (AGENCE NATIONALE SÉCURITÉ DES SYSTÈMES D'INFORMATION)

RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION v3-0

Bastion



VPN IPSec vs VPN SSL





- MultiCloud : double déploiement sur des CSP
- CloudHybride : Master sur Cloud Publique et Slave sur Cloud Privé

Cloud Access Security Broker - CASB



- But : protéger et surveiller les applications dans le CLOUD
- Fonctionnalités : Authentification, chiffrement, DLP, mapping des identifiants, etc.
- Schéma ?

Secure access service edge (SASE)



fonctionnalités réseau et sécurité, dans un environnement Cloud Natif incluant les technologies/services Cloud Based suivants :

- SD-WAN (Software Defined WAN)
- SWG (Proxy sortant sécurisé)
- CASB (Cloud Access Security Broker)
- NGFW (firewalls de nouvelle génération)
- zero trust network access (ZTNA)

Points à retenir



- Le modèle du château fort demeure mais évolue
- les technologies de protection et filtrage évoluent et restent indispensables à la SSI
-> #FirewallNextGeneration #ProxydansleCloud
- les contrôles d'accès administrateurs et utilisateurs sont de plus en plus fins et imposent une rigueur d'implémentation et de gestion dans le temps
-> #Bastion #ZeroTrust
- La sécurité périmétrique s'étend jusqu'au Cloud
-> #CASB #SASE



- inspecte et assure que les équipements connectés ont une configuration et un état conforme avec la politique de sécurité
- Le NAC peut vérifier qu'il y a un antivirus, un pare feu local Schéma ?



des questions ?

Contributions



Les notes et les présentations sont réalisées sous L^AT_EX.

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

[L-Orange-Cyberdef101-M3c-Architectures.prz.pdf sur GITHUB CYBERDEF ↗¹](#)



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



CYBERDEF 101
Eléments de cybersécurité
et de cyberdéfense
d'entreprise

