Orange
CyberSchool

Architectures, Composants et Sécurité

CYBERDEF101

Yann Arzel LE VILLIO, Orange CyberSchool

1er septembre 2023

orange

Abstract

Hashtags : Architectures, composants sécurité, SSI

Ce document présente les architectures, Composants de cybersécurité.

Let’s go

Architectures, Composants et Sécurité

Sommaire

Architectures, Composants et Sécurité

Introduction

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

exemples de traitement des risques

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)

Cryptographie

Définitions et concepts

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

Cryptographie

Clefs

- 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)

Cryptographie

De la confiance aux usages en entreprise

- 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.

Cryptographie

De l'usure électronique au partage de confiance

- 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)

Architecture et composants de système d'information

exemples de traitement des risques

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)

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

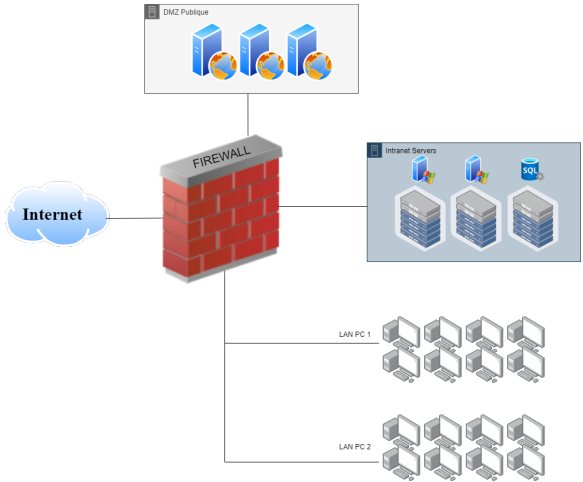
- Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié
- Sondes de détection (IDS/IDP)
- IAM , ZeroTrust, Bastion, VPN SSL, NAC
- Cloud

5 Sécurité Endpoints

Modèles de sécurité et technologies de sécurité protectrices

Château fort

Château fort



Yann Arzel LE VILLIO

1er septembre 2023

Modèles de sécurité et technologies de sécurité protectrices

Firewall

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

Modèles de sécurité et technologies de sécurité protectrices

Proxy

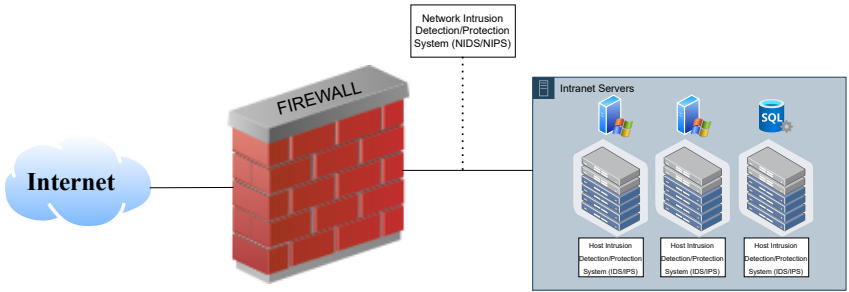
Schéma Proxy

Modèles de sécurité et technologies de sécurité protectrices

Reverse Proxy

Schéma Reverse Proxy

IDS/IDP



Modèles de sécurité et technologies de sécurité protectrices

sondes de détection (IDS/IDP)

Schéma sondes de détection (IDS/IDP)

Gestion des identités : IAM

Identity Access Management

- 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

- 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

Bastion

schéma

VPN SSL

schéma

NAC

- 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 ?

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 ;
- NGFW (firewalls de nouvelle génération) ;
- zero trust network access (ZTNA).

Cloud

- 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 : Authenfication, chiffrement, DLP, mapping des identifiants, etc.
- Schéma ?

Orange
CyberSchool

Des questions !

Eric Dupuis

eric.dupuis@orange.com

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

Eduf@ction yann-arzel.levillio@orange.com

Vérifiez la disponibilité d'une version plus récente de

L-Orange-Cyberdef101-M3-Architectures.prz.pdf sur GITHUB CYBERDEF [1]