Chapitre 3

Yann Arzel

27 juillet 2023

1 Introduction Architecture

CONSTRUIRE vs Politique Architecture de sécurité vs Sécurité des architectures (Crypto, Sécurité Perimétrique). - PERIMETRE, CLOISENEMENT, ZERO TRUST, FILTRAGE, DETECTION, BASTION . . . CHÂTEAU FORT (Mur) / AEROPORT (Portique) - Contrôle d'accès à tout objets

Appréhender la complexité de l'environnement technique du client (Protection, Défense, Résilience) et identifier les composants services, terminaux et réseaux du SI afin de les intégrer dans la politique de sécurité protective. Découvrir les modèles d'architecture de sécurité périmétrique afin d'assurer le filtrage nécessaire et la détection des menaces sur le SI.

2 De l'analyse de risques aux fonctions de sécurité

Via exemples de traitement des risques

2.1 Filtrage

besoin de cloisonner entre client,

multitenant ; besoin de séparer prod & pré-prod ;

besoin de séparer les services

2.2 Accès

gérer les populations, les droits (RBAC, droit d'en connaître)

2.3 Cryptographie

gestion intégrité des données, protection des flux (IPSec, VPN SSL)

3 Architecture et composants de système d'information

Via exemples de traitement des risques

3.1 Middle

BDD, fonctions today dispatch (! Sécurité) versus centralisé historiquement ; archi serveurs messagerie historique VS cloud today

3.2 Front

fait tout mais attention, bcp de choses faites coté client now (!sécu) WEB, applis mobiles

3.3 Endpoints

(PC, mobile, IoT)

3.4 Réseau

accès et traçabilité de tt accès, transactions et anomalies (bugs, erreurs, détection)

4 Modèles de sécurité et technologies de sécurité protectrices

4.1 Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié

4.1.1 Château fort

• En s'appuyant sur un schéma global, notion de DMZ externe, DMZ interne, illustration des flux entrant et sortant, positionnement de composants clés : proxy, serveurs, middleware, sondes, etc. • Cloisonnement • Accès admin – réseau dédié • Accès partenaires (VPN), flux vers Cloud, etc.

4.1.2 pare-feu

Définition (source ANSSI) : Un pare-feu (firewall), est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

Le pare-feu apporte la notion de filtrage dans la sécurité des réseaux et est une pierre angulaire de l'architecture de la sécurité de l'entreprise. Il assure le cloisonnement et

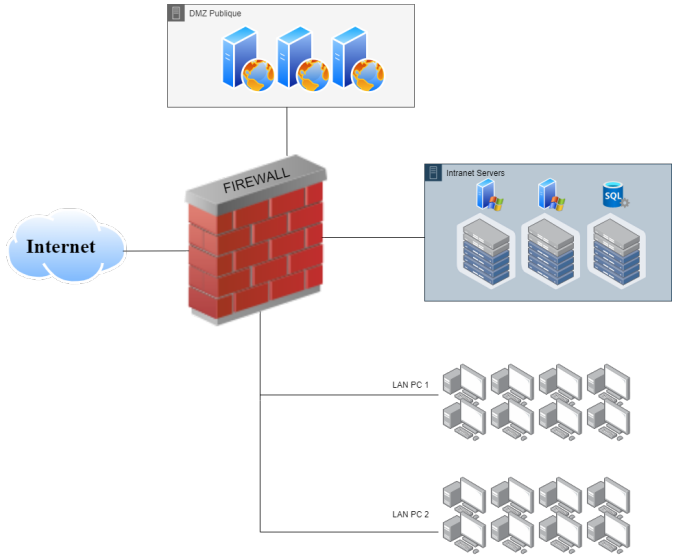

FIGURE 1 – Château fort

la segmentation entre les sous-réseaux (Local Area Network ou LAN). L'ensemble des flux, autorisés ou non, entre ces sous-réseaux et autres réseaux externes (INTERNET, VPN partenaires, etc.) sont inscrits dans la politique de sécurité du pare-feu.

Historique :

— stateless
— statefull
— Next generation

stateless (ACL CISCO), puis statefull, puis next Gen (jusqu'à la couche applicative) Stateless : exemple d'une ACL CISCO, associée à du NAT, i.e. définition du NAT avec le besoin (visibilité extérieure, gestion des adresses IP, pénurie, etc.) & le comment (Schéma) Statefull UDP/TCP mainly Next Gen (L7, déchiffrement, proxy, voire IDP, DLP, etc.)

4.1.3 Proxy et Reverse Proxy

Schéma Proxy (firewall applicatif), lié à de l'authentification, antivirus, URL Filtering Les équipements de type proxy permettent de sécuriser l'accès aux applicatifs. Ils sont en général utilisés pour accéder à Internet depuis le réseau de l'entreprise et donc applique un filtrage en sortie. L'autorisation des flux devra être aussi implémentée sur le pare-feu, par exemple :

A) règle accès au proxy Source : LAN bureautique Destination : Adresse IP du proxy sur le réseau local Protocoles : HTTP, HTTPs Décision : ACCEPT

b) règle de sortie du proxy Source : Proxy Destination : ANY Protocoles : HTTP, HTTPs Décision : ACCEPT

Seul le proxy sera donc autorisé à se connecter aux serveurs distants. Plusieurs briques de sécurité peuvent être ajoutées sur le proxy, comme l'authentification des utilisateurs (jusqu'à la gestion via un annuaire), le filtrage des URL demandées ou encore des protections contre les fuites de données (Data Leak Protection : DLP).

Schéma ReverseProxy, rupture protocolaire, protection serveur, réécriture, LB , WAF

4.2 sondes de détection (IDS/IDP)

Schéma sondes, positionnement dans l'architecture Rôle : détection ou coupure, quid des flux chiffrés ?

4.3 IAM , ZeroTrust, Bastion, VPN SSL, NAC

4.3.1 IAM

Déf IAM, process ET procédures

4.3.2 Zerotrust

: pkoi ? et comment ?

4.3.3 Bastion

: schema, fonctions

4.3.4 VPN SSL

: schema, functions

4.3.5 NAC

: schema, fonctions

4.4 Multi Cloud - CASB

Schémas , mix cloud pub et cloud privé, positionnement du CASB (fonction/pkoi)

5 Sécurité Endpoints

5.1 composants Endpoints

Schéma composants ENDPOINTS + éléments de supervision (réseau, logs)

5.2 FW local

- fonctions

5.3 Antivirus

- fonctions

5.4 EDS/EDR

– fonctions

5.5 Exemple

Exemple d'incident de sécu corrélé d'événement sur un endpoint ?