



Architectures, Composants et Sécurité

Yann Arzel LE VILLIO^{1,2*}

📌 Résumé

Ce document présente les architectures, Composants de cybersécurité.

Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information, de la cybersécurité, et de la cyberdéfense. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.

Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

📌 Mots clefs

Architectures, composants sécurité, SSI

¹Enseignant Sécurité ESIR

²Directeur Technique et Scientifique Orange CyberSchool

*email : yann-arzel.levillio@orange.com – umaila

Éléments de cours

Vérifiez la disponibilité d'une version plus récente de

L-Orange-Cyberdef101-M3-Architectures.doc.pdf sur GITHUB CYBERDEF [🔗](#)¹



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



1. <https://github.com/edufaction/CYBERDEF/raw/master/Builder/L-Orange-Cyberdef101-M3-Architectures.doc.pdf>



Table des matières

1	Introduction Architecture	3
2	De l'analyse de risques aux fonctions de sécurité	3
2.1	Filtrage	3
2.2	Accès	3
2.2.1	IAM	
2.3	Cryptographie	3
2.3.1	Définitions	
2.3.2	Concepts	
3	Architecture et composants de système d'information	8
3.1	Architecture logicielles	8
3.2	Middleware	9
3.3	Endpoints	9
3.4	Réseau	9
4	Modèles de sécurité et technologies de sécurité protectrices	9
4.1	Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié	9
4.1.1	Château fort	
4.1.2	pare-feu	
4.1.3	Proxy et Reverse Proxy	
4.2	Sondes de détection (IDS/IDP)	12
4.3	ZeroTrust, Bastion, VPN	13
4.3.1	ZeroTrust	
4.3.2	Bastion	
4.3.3	VPN	
4.4	Cloud	14
4.4.1	MultiCloud - Cloud Hybride	
4.4.2	Cloud Access Security Broker - CASB	
4.4.3	Secure access service edge (SASE)	
5	Sécurité Endpoints	15
5.1	composants Endpoints	15
5.2	FW local	15
5.3	Antivirus	15
5.4	EDS/EDR	15
5.5	Exemple	16
5.6	Network Access Control : NAC	16

Table des figures

1	Exemple d'une encapsulation asymétrique pour un chiffrement de fichier	5
2	Les briques à vérifier dans la chaîne de confiance	6
3	Château fort	10
4	Proxy	11
5	ReverseProxy	12
6	IDS/IDP	12
7	Bastion	13
8	VPN IPSec vs VPN SSL	14



1. Introduction Architecture

Nous allons dans ce chapitre aborder les sujets d'architectures sécurisées afin d'appréhender la complexité de l'environnement technique du client. L'analyse des menaces et des risques sur un périmètre défini permet d'identifier les fonctions de sécurité qui réduiront les impacts et qui doivent être inscrites dans la politique de sécurité et mises en oeuvre au sein de l'architecture conçue. L'ensemble de ces fonctions ainsi que les composants de l'architecture doivent être sécurisés à l'aide de contrôle, le filtrage des accès, cloisonnement et l'utilisation d'algorithmes cryptographiques. Nous identifierons ensuite les composants services, terminaux et réseaux du Système d'information afin de les intégrer dans la politique de sécurité protectrice. Puis nous découvrirons l'évolution des architectures de sécurité périmétrique depuis le modèle du château fort jusqu'au ZeroTrust et les services assurant les fonctions de sécurité comme le pare feu, les proxy, les bastions et les solutions utilisées sur les architectures CLOUD. Enfin, nous étudierons dans la dernière partie de ce chapitre la sécurité du poste de travail avec les solutions déployées pour assurer la sécurité des données de l'entreprise et de l'utilisateur.

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

Via exemples de traitement des risques

2.1 Filtrage

besoin de cloisonner entre clients (notion de multitenant), au sein du SI, entre différentes sections besoin de séparer production & pré-production ;

besoin de séparer les services

2.2 Accès

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

2.2.1 IAM

Déf IAM, process ET procédures

2.3 Cryptographie

A une époque où chaque jour la presse se fait régulièrement écho de pertes ou de vols de données, où l'on continue à investir dans la protection des données personnelles, certains s'interrogent encore sur les moyens de protéger et de partager de manière sûre son patrimoine informationnel. La cryptographie est une des disciplines de la cryptologie qui s'attache à protéger ces patrimoines en confidentialité, intégrité ou en authenticité. Il me paraissait intéressant de proposer en quelques mots, le vocabulaire et les concepts. Si la cryptographie est un outil pour déployer des mesures de sécurité, c'est aussi un ensemble de techniques utilisées par les attaquants. Au-delà des aspects mathématiques passionnants que nous ne traiterons pas ici, seuls quelques usages et arcanes techniques sont présentés.

2.3.1 Définitions

La cryptologie est par étymologie la science du secret. Elle regroupe la cryptographie, qui porte sur les moyens de coder et décoder les messages, et la cryptanalyse, qui permet de les déchiffrer (de manière non coopérative !). Ces techniques remontent à la nuit des temps. Historiquement militaires et diplomatiques, elles sont devenues civiles avec l'avènement de technologies de l'information, dont la carte à puce² et l'Internet.

Elles ont envahi à grande vitesse toutes les technologies numériques. « Signer, protéger, imputer, authentifier... » sont devenus des termes courants de cette vie numérique. On est toutefois surpris de l'usage, quelque fois un peu « dévoyé », de certaines expressions. « Crypter » s'oppose à « décrypter », mais si décrypter,

2. téléphonie mobile (SIM) et carte bancaire.



c'est « décoder » sans connaître les secrets, crypter est humoristiquement enterrer mettre en « crypte » ! Si les expressions « coder » et « décoder » sont régulièrement utilisées, celles préconisées sont « chiffrer » et « déchiffrer ». En France, au sein des armées, les acteurs du domaine se nomment d'ailleurs des spécialistes du chiffre³. Face à un spécialiste, du mathématicien cryptologue au commercial de services numériques de confiance, de nombreux termes se bousculent dans les discussions : algorithmes robustes de niveau militaire, clefs très longues, protocoles sûrs, certificats de confiance...

2.3.2 Concepts

Derrière ces arguments qui pourraient, au premier abord, paraître convaincants, il convient rapidement d'opposer une petite analyse terminologique et conceptuelle.

Algorithmes Le nombre d'algorithmes mathématiques (fonctions mathématiques) en cryptographie est presque aussi grand que le nombre de mathématiciens qui travaillent dans le domaine. Il faut y ajouter le nombre d'implémentations informatiques de chaque algorithme, sans compter les différents langages utilisés pour la même implémentation. Quelques grandes révolutions ont eu lieu depuis le chiffre de César, mécanisme de chiffrement par décalage « alphabétique » utilisé dans notre enfance, et celui de la machine allemande Enigma de la dernière guerre, avec des mécanismes de substitution dits polyalphabétiques. Ces évolutions et révolutions ont lieu chaque fois que ces fameux cryptanalystes trouvent ou entrevoient une solution pour casser ce chiffre... Une longue tradition dans cette course entre la cuirasse et le canon.

Chiffrement à clefs secrètes Ces premiers algorithmes dits symétriques ou à clefs secrètes ont été et restent centraux, car ils se révèlent très rapides. Le principe est que pour déchiffrer, il faut simplement la clef qui a servi à chiffrer, d'où le terme « symétrique ». Une des grandes difficultés dans ces algorithmes est la combinatoire pour partager le secret. Si partager de manière sûre un secret entre deux ou trois correspondants est maîtrisable, le faire pour mille ne permet plus vraiment de parler d'une clef secrète ! L'histoire des célébrités technologiques retient des algorithmes comme DES, 3DES, IDEA, RC4 et le dernier réputé inviolé et issu d'un appel à projet du NIST⁴ et paru dans les années 2000 : AES256.

Cryptographie à clefs publiques Le chiffrement asymétrique résout ce problème de la combinatoire, mais reste bien plus lent. Rendu célèbre par Alice et Bob, deux personnages illustrant les cours de cryptologie asymétrique, ce mécanisme utilise une paire de clés liées dites asymétriques : une clé publique et une clé privée. La clé publique est rendue publique et distribuée librement. La clé privée n'est jamais distribuée et doit être gardée secrète. Pour cette une paire de clés, les données chiffrées à l'aide de la clé publique ne peuvent être déchiffrées qu'avec la clé privée correspondante (donc si vous avez la clef publique de votre correspondant, vous pouvez chiffrer une information pour lui). Inversement, les données chiffrées à l'aide de la clé privée ne peuvent être déchiffrées qu'avec la clé publique correspondante. Cette caractéristique est utilisée pour mettre en œuvre la signature numérique.

Fonction de hachage Les fonctions de hachage cryptographique (de l'anglais « hash ») sont présentes dans tous nos systèmes numériques. Ce sont des fonctions rapides à sens unique qui permettent de transformer tout bloc d'information de taille quelconque et une donnée de taille fixe souvent courte. Ce mécanisme, qui permet de prendre une « empreinte » des données, est à la base des mécanismes de signature, de contrôle d'intégrité et de stockage de mots de passe. Les algorithmes les plus connus sont md5, sha1 et maintenant sha256, sha512 nécessaires par les fragilités découvertes sur les premiers, car ces algorithmes sont aussi sujets aux attaques !

Clefs Au cœur de la cryptographie, les clefs restent l'objet de toutes les attentions. Il est conseillé la lecture des quelques documents de référence de l'Anssi⁵ sur les « mécanismes cryptographiques »⁶ qui illustrent de manière pragmatique et concrète cette indispensable vigilance.

3. ARCSI : Association des réservistes du chiffre et de la sécurité de l'information - www.arcsi.fr

4. National institute of standards and technology.

5. Anssi : Agence nationale pour la sécurité des systèmes d'information, services du Premier ministre.

6. Annexe B1 et B2 du RGSV2 (Anssi : référentiel général de sécurité) : Mécanismes cryptographiques et gestion des clefs.



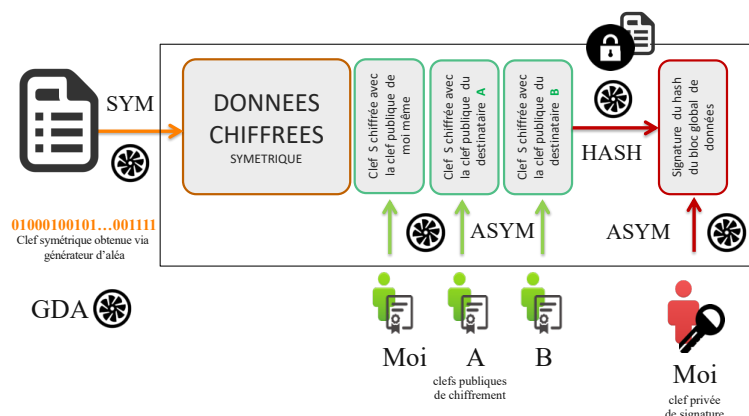


Figure 1. Exemple d'une encapsulation asymétrique pour un chiffrement de fichier

Taille de clefs Un des débats dans l'usage de la cryptographie concerne la taille optimale des clefs. Ce sujet fait l'objet de nombreuses publications. Pour les algorithmes symétriques, 1 280 bits est la taille de référence (soient 2 puissance 128 possibilités). La notion de taille de clefs pour les algorithmes asymétriques est moins simple. Cela dépend des problèmes mathématiques sous-jacents. Pour le plus célèbre RSA⁷ (6), qui aura bientôt 40 ans, les experts considèrent qu'une taille de 2 048 est à l'état de l'art jusqu'en 2030. RSA est utilisé pour les transactions pour la carte bleue, les achats sur internet, les courriels sécurisés. Pour ceux basés sur le logarithme discret, la taille préconisée est de 200 bits, pour les courbes elliptiques de 256 bits. Il est donc important de spécifier les algorithmes pour comparer des tailles de clefs.

Aléas et générateur d'aléas De nos jours, une bonne clé secrète est très rarement issue de notre cerveau (même un bon mot passe mémorisable est totalement perfectible sur le pur plan cryptographique)⁸. Pour générer des clefs d'un bon niveau cryptographique, c'est-à-dire non sujettes à des biais de prédiction possibles, il est nécessaire d'utiliser un générateur de nombres aléatoires (GDA ou RNG : « random number generator ») de qualité cryptographique. Il est fondamentalement complexe de générer de véritables nombres aléatoires. Le processus de génération d'aléas doit comporter des sources fondamentalement aléatoires (bruit électronique, thermique dans des composants) combinées à des sources multiples (hash d'une zone mémoire...), le tout passé à la moulinette d'algorithmes de pseudo-aléas suffisamment imprévisibles. Ce fondamental de la cryptologie est un domaine de recherche à part entière. C'est aussi une activité industrielle autour des HSM (hardware security module) pour la génération rapide, le stockage et la protection des clefs primordiales pour les transactions numériques bancaires en particulier.

Protocoles et formats De bons algorithmes, de bonnes clefs ne suffisent pas. Il est indispensable de s'assurer de l'ensemble des mécanismes qui vont permettre de garantir que « les secrets échangés » restent bien secrets. On parle de protocole d'authentification, de signature, d'échange de clefs (Kerberos, Diffie Elmann, RSA...). C'est souvent au cœur de ces protocoles qui nécessitent une attention particulière en termes de robustesse et de preuve formelle que l'on trouve des vulnérabilités. Le format des données chiffrées (cf Fig. 1) est aussi une source de fragilité (cacher une partie de la clé en piégeant l'ordinateur, exploiter une vulnérabilité logicielle). Les solutions technologiques de chiffrement combinent pour des raisons de performance des mécanismes de chiffrement symétrique et asymétrique.

Certificats Le terme « certificat électronique » est entré dans le langage courant du numérique : « certificat machine, serveur », « certificat utilisateur ». à la base des usages des systèmes à clefs publiques, ce certificat contient la (les) clé(s) publique(s), des informations d'identification, des dates de validité, et un mécanisme

7. 1978, apparition de l'algorithme à clé publique de Rivest, Shamir et Adelman (RSA).

8. Un mot de passe de qualité « cryptographique » devrait être d'au moins 20 caractères dans un alphabet de 90 symboles.



de signature garantissant l'origine. Informatiquement ce « paquet » de données nécessite des standards de formats structurés interopérables comme le codage X.509 ou le stockage PKCS12⁹.

Certificats auto-signés ! Une clef publique « valide » dans un système cryptographique de confiance, doit être signée par une autorité de confiance pour être vérifiée par la suite par son « usager ». Disposer d'une PKI (public key infrastructure) ou faire certifier sa chaîne de confiance est complexe et coûteux. Le monde informatique fait donc largement usage de l'auto-signature, c'est-à-dire de la génération des clefs, sans chaîne de confiance partagée. Lorsque les logiciels sont permissifs sur ces usages, l'ensemble du système est fragilisé.

IGC ou PKI Utiliser des mécanismes à clefs publiques nécessite donc l'utilisation d'un ensemble interopérable de confiance (algorithmes, protocoles, formats) permettant de générer les clefs (couple privée/publique), de les attribuer, de les signer (les certifier), de les distribuer, et de les révoquer (les supprimer de l'environnement de confiance). L'ensemble de ces mécanismes s'appelle une IGC (infrastructure de gestion de clefs) ou PKI (public key infrastructure). Ces outils logiciels et l'organisation globale sont indispensables à un usage structuré de confiance. Sans cette maîtrise des clefs, un système à clef publique peut s'effondrer. En effet, si des clefs de certification, ou des clefs privées d'utilisateurs sont compromises à la source, la résistance mathématique des algorithmes ou des protocoles ne vous garantira plus grand-chose... C'est dans cet esprit que sont nés les tiers de confiance, qui vous assurent que toutes les précautions sont prises pour protéger cette chaîne.

De la confiance aux usages en entreprise Comme vous l'avez noté, un système cryptographique est un ensemble de briques (fig. 2) qu'il est nécessaire de contrôler pour définir un niveau de confiance de la chaîne. Si disposer d'outils à clefs publiques sans un IGC (PKI) se révèle fragile, disposer d'une IGC sans disposer d'une maîtrise des usages l'est autant... En France, le terme de moyen (9) cryptologique est défini par loi sur la confiance numérique, mais il est à remarquer que, dans l'entreprise, il se conjugue différemment en fonction des interlocuteurs :

- ▶ pour les équipes réseaux : la cryptographie est enfouie dans les méandres des protocoles des technologies des canaux sécurisés VPN, IPSEC, VPN, 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.



Figure 2. Les briques à vérifier dans la chaîne de confiance

Il est à noter, le point particulier du recouvrement des données chiffrées et du séquestre des clefs. Indispensable pour les malchanceux qui perdent leur clef privée ou par nécessité (départ de l'entreprise, réquisition sur des

9. PKCS : Public-Key Cryptography Standards. (9) Moyen de cryptologie : Tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux)



données...), la confiance dans celui qui possède cette capacité de recouvrement est un enjeu fondamental. Acquérir et déployer un système cryptographique dans l'entreprise doit se baser sur un minimum de confiance dans l'implémentation des briques. Il est important que ces produits aient été analysés, vérifiés par des tiers (entre le constructeur ou éditeur et l'utilisateur ou acheteur). On parle ainsi de certifications de produits au titre de la norme de l'iso 15408 (critères communs), qualification de produits et de services par l'ANSSI. Perturbant un peu l'écosystème et les frontières de gouvernance des DSI, l'usage des services dans le cloud nécessite de nouvelles technologies de chiffrement pour maintenir la confidentialité totale, mais autoriser tout de même des traitements. Le chiffrement homomorphe permet justement à un système tiers d'opérer des calculs sur des données chiffrées sans les déchiffrer et ainsi récupérer les résultats exploitables. Des solutions matures arrivent sur le marché depuis peu.

De l'usure électronique au partage de confiance

Usure ou rupture cryptographique Si le temps n'est pas l'ami de l'archivage, il ne l'est pas non plus du chiffrement. Non par l'usure du support, mais simplement par la complexité d'une longue conservation des clefs, de l'érosion de la résistance des mécanismes. En outre, depuis des années, le terme « quantique » est apparu dans la littérature du domaine. Si la distribution quantique offre une transmission sûre de clef, l'ordinateur quantique pourrait apporter cette rupture que redoute l'industrie numérique, car capable de rompre la solidité des problèmes mathématiques sur lesquels repose une grande partie des mécanismes cryptographiques actuels.

La cryptographie quantique est un espace de recherche de cryptographie qui utilise les propriétés quantiques de la matière pour sécuriser les communications et protéger les données. Elle repose sur des phénomènes quantiques tels que l'intrication et la superposition, qui permettent de réaliser des calculs et des opérations de manière beaucoup plus rapide et plus efficace que les algorithmes classiques utilisés dans la cryptographie traditionnelle.

La cryptographie quantique est encore en développement et n'est pas encore largement utilisée dans les applications pratiques. Cependant, elle offre des avantages potentiels considérables en termes de sécurité et de vitesse de calcul. Par exemple, les algorithmes de cryptographie quantique pourraient être utilisés pour créer des clés de chiffrement plus sécurisées et pour effectuer des calculs complexes de manière beaucoup plus rapide que les algorithmes classiques.

Il est important de noter que la cryptographie quantique est également confrontée à des défis importants, notamment en ce qui concerne la stabilité des données quantiques et la difficulté à mettre en œuvre ces algorithmes de manière pratique. En outre, il existe des inquiétudes quant à la sécurité à long terme de la cryptographie quantique, car il est possible que de futurs progrès technologiques permettent de casser la confiance dans les chaînes de confiance basée sur les algorithmes actuels de manière plus efficace.

En effet, si ces technologies sont pleinement mises en œuvre et deviennent largement utilisées, cela pourrait remettre en question la sécurité de nombreux systèmes de sécurité actuellement en place qui reposent sur des algorithmes de cryptographie classiques.

On peut citer les risques suivants :

- ▶ rupture de la sécurité de la cryptographie classique : si les algorithmes de cryptographie quantique sont mis au point et deviennent largement utilisés, ils pourraient être utilisés pour cracker les codes de cryptographie classique, mettant ainsi en danger la sécurité de nombreux systèmes de sécurité actuels ;
- ▶ compromission de la confidentialité des communications : si les algorithmes de cryptographie quantique sont utilisés pour chiffrer les communications, ils pourraient être « crackés » par des parties malveillantes, compromettant ainsi la confidentialité de ces communications.

blockchain, Crypto-monnaies, NFT... Nous avons rapidement parcouru l'usage courant de la cryptographie en entreprise, mais de nouvelles révolutions des usages de la cryptographie sont déjà à nos portes. Après quelques années d'hésitation, la montée des « crypto-monnaie » comme Bitcoin donne une large expression



aux mécanismes de signature pour assurer intégrité, traçabilité, imputabilité et modifie le rapport à la confiance « centralisée ». Dans l'émergence rapide de cette « décentralisation de la confiance », quelques positions établies sont remises en cause. On notera en particulier une forme naissante « d'ubérisation » des chaînes de confiance, qui bouscule déjà le marché effervescent de la cybersécurité. Les chaînes de confiance sont de plus en plus utilisées dans les crypto-monnaies et NFT.

La cryptographie joue un rôle clé dans la sécurité et l'intégrité des Blockchains en permettant de protéger les données et les transactions contre la modification ou la falsification. Ces actifs numériques à caractère authentique sont basés sur ces Blockchains. Une blockchain est un registre, une base de données distribuée qui permet de stocker de manière sécurisée et transparente ces enregistrements de données. Elle est composée de blocs de données qui sont liés les uns aux autres de manière sécurisée grâce à l'utilisation de cryptographie.

Chaque bloc de la chaîne contient des informations sur les transactions qui ont été effectuées, ainsi que des données sur les blocs précédents. Lorsqu'un nouveau bloc est ajouté à la chaîne, il est vérifié et validé par plusieurs ordinateurs dans le réseau, ce qui rend la Blockchain très difficile à altérer ou à falsifier.

Les Blockchains sont principalement utilisées pour stocker et transférer des cryptomonnaies, mais elles peuvent également être utilisées pour d'autres applications, telles que la gestion de la chaîne d'approvisionnement, la gestion des actifs, la gestion de la santé, etc. Elles offrent un niveau élevé de transparence et de sécurité, ce qui les rend particulièrement utiles dans les situations où la confiance et l'intégrité des données sont importantes.

Les cryptomonnaies sont des formes de monnaies numériques qui utilisent la technologie de la Blockchain pour sécuriser les transactions et contrôler la création de nouvelles unités de monnaie. Elles sont décentralisées, ce qui signifie qu'elles ne sont pas émises ni gérées par une banque centrale ou tout autre organisme gouvernemental.

La cryptomonnaie la plus connue est probablement le Bitcoin, qui a été créée en 2009. Depuis, de nombreuses autres cryptomonnaies ont vu le jour, chacune avec ses propres caractéristiques et utilisations. Certaines sont conçues pour être utilisées comme moyen de paiement, tandis que d'autres sont plus axées sur l'investissement.

Les cryptomonnaies sont souvent utilisées comme moyen de paiement en ligne et sont acceptées par certaines entreprises et commerçants en tant que moyen de paiement. Cependant, elles restent controversées en raison de leur manque de réglementation et de leur volatilité, avec des fluctuations de prix importantes pouvant survenir en très peu de temps. En outre, leur utilisation a été associée à des activités illégales en raison de la confidentialité qu'elles offrent aux utilisateurs.

Les NFT (Non-Fungible Tokens) sont des tokens numériques qui représentent de manière unique des actifs numériques ou physiques. Ils sont stockés sur une chaîne de confiance basée sur des blockchains, comme la blockchain Ethereum, ce qui leur confère une certaine forme de rareté et de valeur.

Les NFT sont utilisés pour représenter des objets virtuels tels que des œuvres d'art numériques, des enregistrements de musique, des GIFs animés, des émoticônes, des personnages de jeux vidéo, etc. Ils permettent aux créateurs de ces actifs de monétiser leur travail de manière transparente et sécurisée, tout en offrant aux acheteurs la possibilité de devenir les propriétaires uniques de ces actifs.

Si les NFT sont de plus en plus populaires et suscitent beaucoup d'intérêt en raison de leur capacité à représenter de manière unique des actifs numériques, il est important de noter qu'il existe également des risques liés à l'achat et à la possession de ceux-ci. On note en particulier la confiance dans la sécurité globale dans ces blockchains ainsi que la stabilité et la liquidité du marché des NFT.

3. Architecture et composants de système d'information

Nous allons dans ce chapitre présenter les composants des architectures logicielles, postes de travail et réseaux.

3.1 Architecture logicielles

Les architectures logicielles ont fortement évolué ces dernières années et le classique architecture "trois tiers" se décompose de plusieurs types de solutions basées sur les dernières technologies d'intégration et de déploiement.



Les modèles dits « monolithes » existent toujours et restent utilisés dans beaucoup de cas d'applicatifs qui ont des besoins élevés en capacité de traitement ou de bande passante. L'apparition et l'utilisation des micro-services a apporté des solutions en scalabilité et résilience. Cependant, ce type d'architecture apporte aussi son lot de complexité dans le cadre de montée en version versus la solution monolithe où une seule mise à jour serait nécessaire. L'exemple de vulnérabilités impactant un fort ensemble de composants comme log4shell¹⁰ est illustratif de difficultés à patcher les applications vulnérables (plusieurs applications possibles, avec patch ou non disponible qui impose une montée en version préalable et donc ajoute des difficultés à la remédiation).

Les architectures logicielles sont généralement composées des composants suivants :

- ▶ Front ou FrontEnd qui sont les composants directement consultés par le client de l'applicatif. Ils peuvent être de type applications mobiles, pages web par exemple ;
- ▶ Backend ou moteur/serveur applicatif qui vont assurer la partie métier ;
- ▶ Bases de données qui assurent le rôle de stockage des données applicatives.

3.2 Middleware

Les composants dits middleware sont de type :

- ▶ Bases de données ;
- ▶ ERP ;
- ▶ Annuaire

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.

Par la suite, nous aborderons les fonctions de sécurité telles que le 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 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. Celle-ci se représente par une matrice des flux contenant l'ensemble des informations telles que :

- ▶ le nom de la règle ;

10. <https://www.ssi.gouv.fr/publication/lanssi-alerte-sur-la-faible-de-securite-log4shell/>



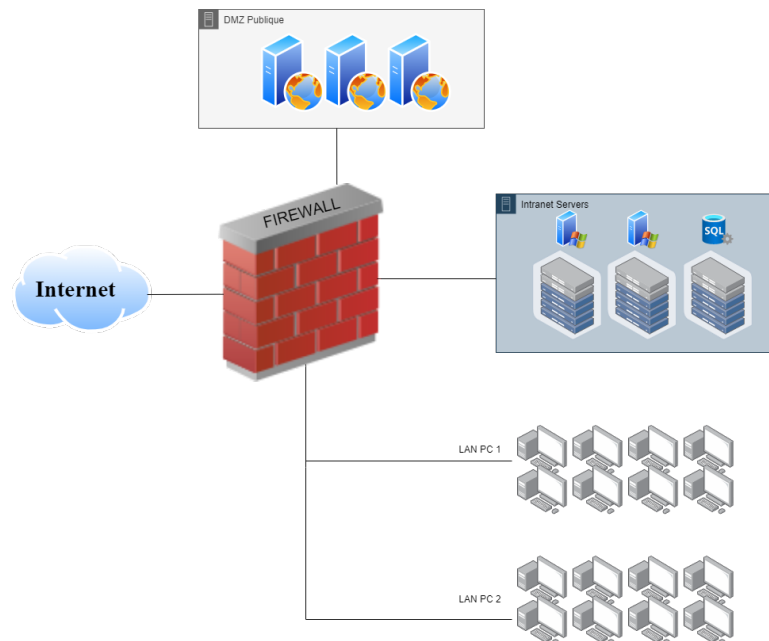


Figure 3. Château fort

- ▶ le ou les IP source(s) ;
- ▶ le ou les IP destination(s) ;
- ▶ le protocole concerné (HTTP, FTP, SMTP, etc.) ;
- ▶ l'option éventuelle (NAT, authentification, application d'une politique de sécurité supplémentaire, etc. ; cela dépend de la version du pare-feu utilisé) ;
- ▶ l'action : accept, drop, reject, etc.
- ▶ l'option de journalisation sélectionnée.
- ▶ etc.

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 utilisés pour assurer un filtrage des accès Internet depuis le réseau de l'entreprise. C'est une des fonctions primordiales de la sécurité du système d'information. En effet, il est indispensable de maîtriser les flux de sortie et d'assurer la sécurité des utilisateurs sur Internet en imposant le filtrage via des équipements réseaux de type Proxy. Ce filtrage pourra assurer des fonctions anti-malware, antivirus mais aussi sur le type de site consulté par exemple.

L'autorisation des flux devra être aussi implémentée sur le pare-feu. Voir ci-dessous en exemple un extrait simplifiée d'une matrice de flux implémentée sur un pare feu :



Source	Destination	Protocoles	Décision
LAN bureautique	Adresse IP du proxy sur le réseau local	HTTP, HTTPS	ACCEPT
Proxy	ANY	HTTP, HTTPS	ACCEPT
ANY	ANY	ANY	DENY

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).

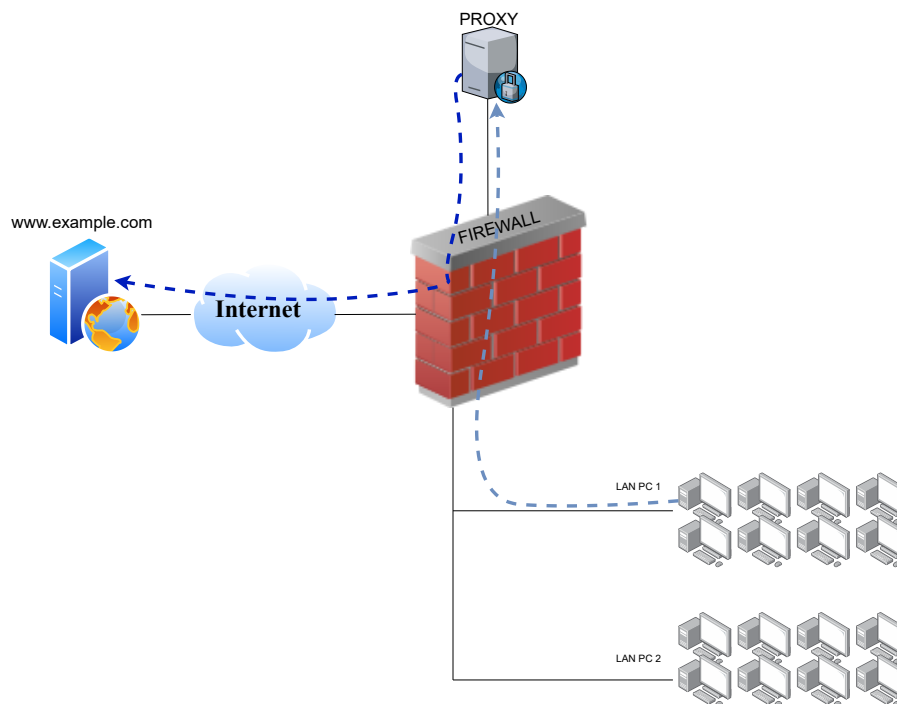


Figure 4. Proxy

Le Reverse Proxy aura lui le rôle de protéger les serveurs des accès utilisateurs, externes ou internes. Il peut assurer une **rupture protocolaire** et donc agir en tant que mandataire auprès du serveur. Plus précisément, la connexion TCP/HTTP par exemple entre le client A et le serveur Web **www.monexemple.com** peut s'effectuer de la manière suivante :

- ▶ le client effectue une requête DNS sur **www.monexemple.com** et le serveur DNS lui indique l'IP associée, cette IP est portée par le Reverse Proxy ;
- ▶ le client initie une connexion TCP/HTTP vers le Reverse Proxy ;
- ▶ le Reverse Proxy effectue éventuellement les contrôles configurés et ensuite initie à son tour une connexion TCP/HTTP vers le serveur.

Le Reverse Proxy est un équipement ou bien une fonction portée par un service qui permet donc d'interagir avec la connexion et assurer par exemple :

- ▶ de la répartition de charges (load balancing) ;
- ▶ de la réécriture d'URL ;
- ▶ des fonctions de sécurité et donc assurer un rôle de pare feu applicatif/Web (Web Application Firewall : WAF).

Schéma ReverseProxy



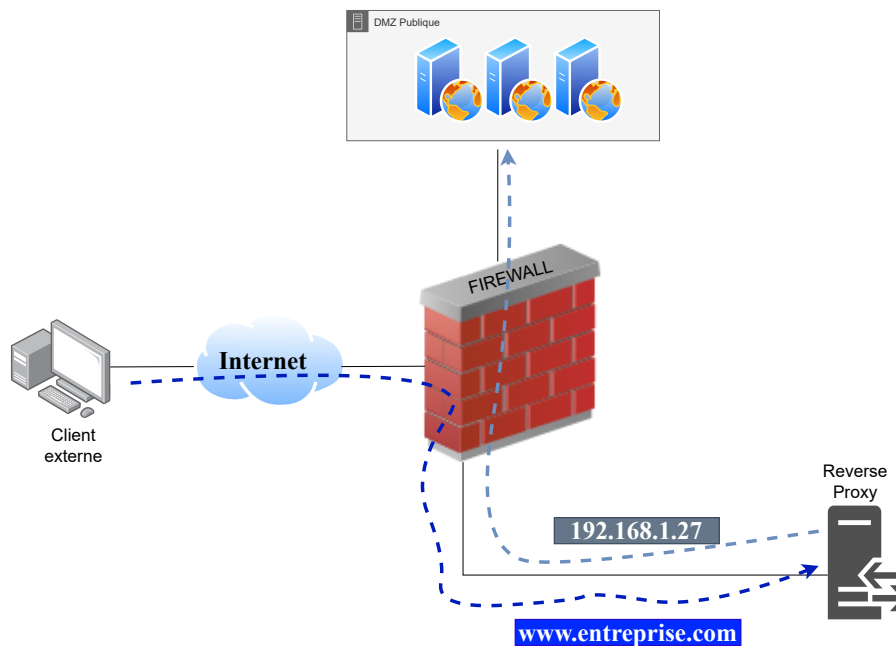


Figure 5. ReverseProxy

4.2 Sondes de détection (IDS/IDP)

Les sondes de détection d'intrusion sont utilisées pour surveiller et analyser le trafic réseau afin de détecter des actes malveillants tels que des tentatives d'exploitation de vulnérabilités qui peuvent entraîner l'ex-filtration de données confidentielles par exemple.

Plusieurs types de sondes peuvent être utilisées :

- ▶ Réseaux :
 - NIDS Network Intrusion Detection System (NIDS)
 - Network Intrusion Prevention System (NIPS)
- ▶ Sur les équipements :
 - Host Intrusion Detection System (HIDS)
 - Host Intrusion Prevention System (HIPS)

Exemple de schéma d'infrastructure avec positionnement des sondes :

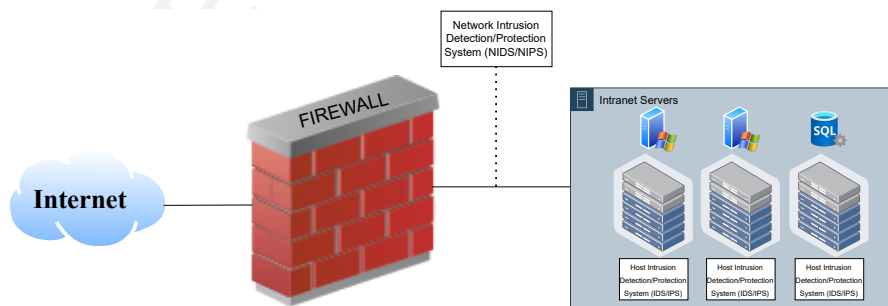


Figure 6. IDS/IDP

Il existe plusieurs méthodes de détection telles que :

- ▶ celle basée sur les signatures qui compare avec sa base de signatures les événements observés pour identifier des incidents potentiels ;



- ▶ celle basée sur les anomalies qui compare les définitions d'une activité considérée comme normale avec les événements observés afin d'identifier les écarts significatifs ;
- ▶ l'analyse dynamique qui compare les profils prédéterminés des protocoles, avec les événements observés, afin d'identifier les écarts. L'ensemble des résultats des sondes sont consignés dans des journaux et peuvent être utilisés dans les détections d'incidents de sécurité.

4.3 ZeroTrust, Bastion, VPN

4.3.1 Zerotrust

Les modèles actuels de sécurité périmétrique atteignent leurs limites face à l'augmentation du télétravail, de l'utilisation des infrastructures Cloud et l'utilisation de terminaux mobiles pour se connecter au SI d'entreprise. Le principe du ZeroTrust est de ne plus faire uniquement confiance aux contrôles et filtrage des équipements classiques tels que les pare-feux et proxies et d'ajouter un système de contrôle d'accès dynamique aux ressources supplémentaire.

4.3.2 Bastion

Le Bastion permet également de tracer les sessions administrateurs en offrant la possibilité de les visionner à posteriori dans le cadre d'audits, comme pour identifier des anomalies ou des actes malveillants. Le Bastion propose également des alertes en temps réels pour signaler les utilisateurs ne respectant pas les politiques de sécurité de la société.

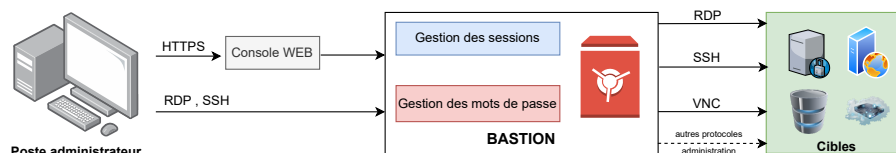


Figure 7. Bastion

4.3.3 VPN

L'utilisation d'un Virtual Private Network répond aux besoins :

- ▶ de connecter des utilisateurs nomades au système d'information de l'entreprise avec une technologie fiable et sécurisée ;
- ▶ d'interconnecter des partenaires au SI de l'entreprise en maîtrisant les flux autorisés ;
- ▶ de sécuriser les données en transit au travers d'un réseau en les chiffrant afin de se protéger des attaques de type 'Man in the middle'

L'utilisation de tunnels L2TP/IPSec (Layer Two Tunneling Protocol¹¹/Internet Protocol Security¹²) permet de raccorder des équipements réseaux (routeurs ou firewalls) point à point, et ainsi étendre les systèmes d'information à d'autres sites géographiques internes, externes ou partenaires.

La technologie TLS/SSL (Secure Socket Layer) est utilisée généralement avec un navigateur WEB et le protocole HTTPS et ne nécessite donc pas de client dédié (mais il en existe pour faciliter l'accès à certaines applications par exemple).

Voir ci-dessous un schéma représentant les deux technologies. Dans le cas du tunnel IPSec, le point de terminaison peut être un pare feu sur lequel sera implémenté les règles permettant (ou non) l'accès depuis le poste externe aux différents réseaux privés de l'entreprise. Le deuxième cas représenté l'utilisation d'un tunnel SSL/TLS entre un client avec un navigateur Internet et une passerelle VPN SSL dédiée. Les règles et paramétrage des autorisations s'effectuent sur la passerelle qui peut supporter par exemple de l'authentification (SAML ou autres).

11. rfc2661 : <https://datatracker.ietf.org/doc/html/rfc2661>

12. rfc6071 : <https://datatracker.ietf.org/doc/html/rfc6071>



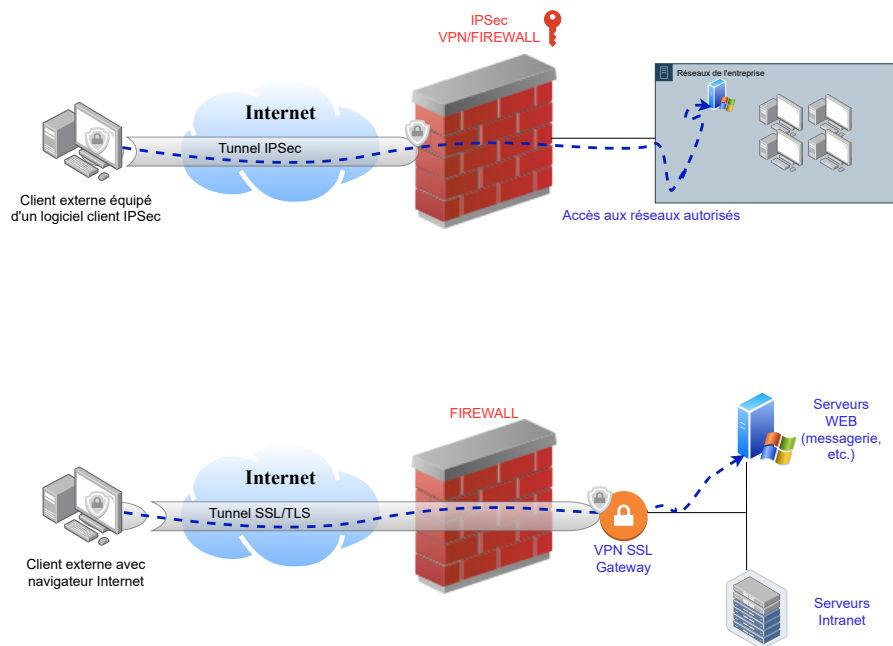


Figure 8. VPN IPSec vs VPN SSL

4.4 Cloud

4.4.1 MultiCloud - Cloud Hybride

Un des enjeux majeur pour les entreprises est la résilience de leurs services. Un grand distributeur et marchand en ligne ne peut pas se permettre d'être à l'arrêt complet lors de périodes fastes comme les fêtes de fin d'année. Il est arrivé que certains soient bloqués car ils avaient migrés l'entièreté de leurs applications dans un Cloud public qui malheureusement fut inaccessible pendant plusieurs heures. Le résultat commercial fut catastrophique pour le marchand (et leur fournisseur Cloud aussi). La disponibilité est aussi de la sécurité et doit être d'assurée en évitant de mettre « tous ses oeufs dans le même panier ».

MultiCloud En ce qui concerne l'hébergement dans le CLOUD, les entreprises prennent donc le choix du Multi-Cloud, i.e. de dupliquer leurs architectures sur des clouds providers (CSP) différents. Ce choix peut apporter son lot de complexité et des coûts associés non négligeables car il sera nécessaire d'adapter les déploiements/configurations par rapport aux spécifications du CSP utilisé.

Cloud Hybride Le MultiCloud ayant ses avantages mais aussi ses inconvénients, beaucoup d'entreprises décident de déployer leurs infrastructures dans un Cloud Public et dans un cloud privé. En effet, ils configurent le déploiement sur le cloud public comme le « maître ou master » et puis la partie sur l'infrastructure privée, dit « on premise » comme l'« esclave ou slave ».

4.4.2 Cloud Access Security Broker - CASB

Le Cloud computing a apporté un lot d'évolution technologique qui nous force à repenser les stratégies de sécurité nécessaires pour protéger et surveiller les applications et les données hébergées dans le Cloud. Les solutions de Cloud Access Security Broker agissent comme un pont entre les services et infrastructures « on premises » et les différents Cloud services utilisés par l'entreprise. Les CASB peuvent proposer les fonctionnalités suivantes :

- ▶ authentication
- ▶ single sign-on,
- ▶ authorization,
- ▶ credential mapping,



- ▶ device profiling,
- ▶ encryption,
- ▶ tokenization,
- ▶ logging,
- ▶ alerting,
- ▶ malware detection/prevention.

Les CASB peuvent être intégrés comme composants au sein d'architectures de type Secure access service edge (SASE).

4.4.3 Secure access service edge (SASE)

Les évolutions des méthodes de travail avec l'explosion de l'utilisation du télétravail, des accès professionnels via les terminaux mobiles et l'utilisation de plus en plus fréquente du edge computing (<https://www.red-hat.com/fr/topics/edge-computing/what-is-edge-computing>) nécessite une évolution des architectures de sécurité afin de faire face à de nouvelles menaces liées à ces changements.

Les architectures de type Secure access service edge (SASE) assurent des fonctionnalités réseau et sécurité, dans un environnement « Cloud Natif » incluant les technologies/services, dits « 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)

- ▶ 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

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 ?

5.6 Network Access Control : NAC

: schema, fonctions, 802.1X

Eléments de cours

