COMPTE-RENDU D'ACTIVITES

Pendant mon stage, j'ai pu participer à divers :

Rencontres avec :

- Les membres de l'équipe Network Security.
- Les membres de l'équipe Browsing and Hosting.
- Les membres de l'équipe SDM (Service Delivery Management) ou bien Production.

Réunions :

J'ai participé à des réunions en Visio-conférences sur les thématiques suivantes :

- **Webinar :** une présentation sur le Zero-trust, qui est une nouvelle stratégie de sécurité. Elle adresse essentiellement les entreprises afin d'améliorer leur sécurité en changeant le rapport de confiance qu'elles ont en leur réseau et en y ajoutant/renforçant des points de contrôle d'accès.
- **Service Browsing :** C'est un service de navigation internet / intranet géré par du filtrage proxy (authentification, URL Filtering, Déchiffrement SSL, analyse anti-malware et DLP) pour assurer la sécurisation des flux Web utilisateurs et serveurs.
- **Formations :** J'ai participé aux formations ci-dessous qui sont obligatoire pour tous les employés :
    - **Sensibilisation sur la cybersécurité**
    - **Sécurisation des bureaux**

Les Firewalls : Un Firewall est un appareil de sécurité réseau qui analysent soigneusement le trafic entrant en fonction de règles préétablies et filtrent le trafic provenant de sources non sécurisées ou suspectes pour empêcher les attaques. Les firewalls contrôlent le trafic au point d'entrée d'un ordinateur, appelé port, qui est l'endroit où les informations sont échangées avec des appareils externes.

Le Browsing : C'est un service de navigation internet / intranet géré par du filtrage proxy (authentification, URL Filtering, Déchiffrement SSL, analyse anti-malware et DLP) pour assurer la sécurisation des flux Web utilisateurs et serveurs.

Le Lab virtuelle : c'est un laboratoire virtuel qui permet d'installer, configurer et tester des équipements.

La monétique : c'est le chemin parcouru par la monnaie virtuelle.

La Chaine de la production : C'est le cycle de la création d'une application par un métier (métier celui qui connait bien son travail).

ETUDES DE CAS

Les entreprises subissent de plus en plus d'attaques et les menaces viennent aussi bien de l'intérieur que de l'extérieur. Les acteurs malveillants utilisent les accès existants et piratent les périmètres. Une fois à l'intérieur, ils sont capables d'augmenter les niveaux des privilèges, d'effectuer des repérages et de se déplacer latéralement à l'intérieur du réseau, de perturber les activités et d'extraire des données. Le contexte actuel montre les limites du modèle traditionnel du château fort consistant à protéger le Système d'Information (SI) interne de l'entreprise.

En 2004, au Jericho Forum, sont élaborés les 'Network Access Control', initiant les débuts du Zero Trust. Puis en 2010, John KINDERVAG, ancien collaborateur de Forrester élabore le terme du Zero Trust qui veut dire : « *Ne jamais faire confiance, toujours vérifier* ». C'est un changement de vision qui passe d'un accès traditionnel basé sur le périmètre à un modèle axé sur l'utilisateur.

Le Zero Trust est une approche de sécurité intégrée pour les utilisateurs, les applications, les données et les réseaux qui nécessite des principes d'authentification forte et renforcée et l'utilisation de politiques d'accès.

Chaque tentative d'accès aux systèmes est controlée comme si elle provenait d'un réseau non fiable, hostile. Ce modèle encourage l'utilisation des analyses avancées pour mieux détecter les menaces et les violations. Pour atteindre son efficacité maximale, les entreprises doivent commencer par l'identité de l'utilisateur. Il faut mettre en place une stratégie forte de gouvernance et d'administrions des identités. Lorsqu'elle sera correctement mise en œuvre, la solution offrira une visibilité permettant de **vérifier : qui accède à quoi, pourquoi, comment et d'où ?**

Qui : utilisateurs et services (plus tard des ressources)

Quoi : applications, qu'elles soient dans le cloud ou non

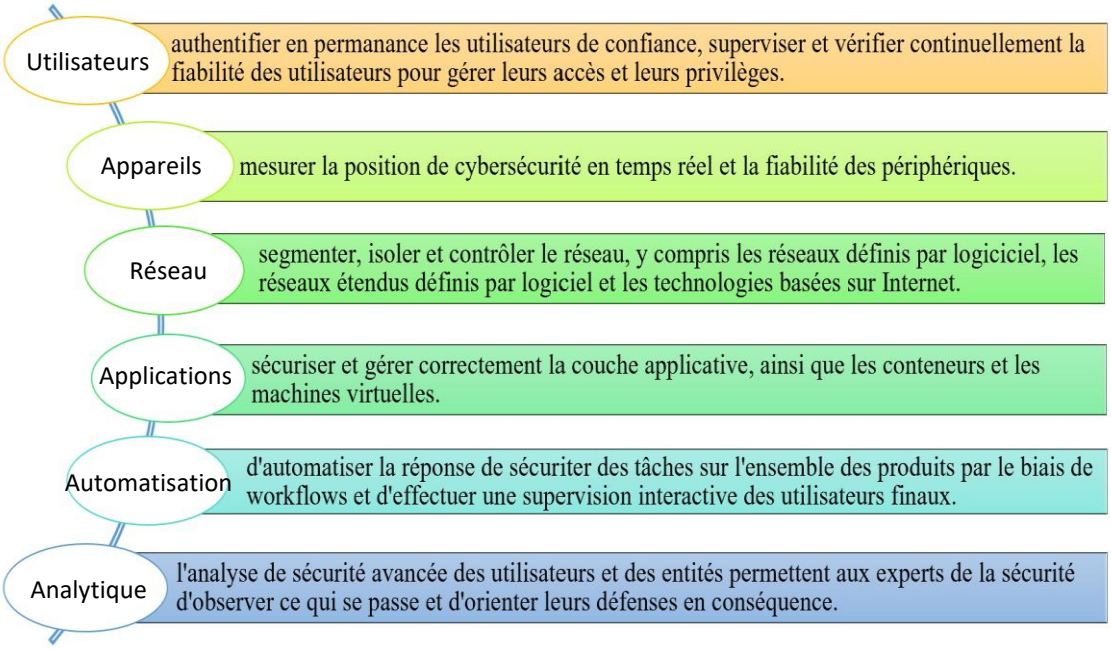
Pourquoi : raison de l'accès, basée sur des règles spécifiées

Comment : réseaux d'entreprise, et de plus en plus le réseau Internet

D'où : équipement et sa localisation.

La gestion des accès est essentielle dans le modèle Zero trust. L'évaluation du contexte de l'identité au cours du processus d'authentification et d'autorisation permet de s'assurer qu'un utilisateur est bien celui qui prétend être, qu'il utilise l'appareil qu'il devrait utiliser et qu'il accède au réseau depuis un lieu autorisé. L'identité définit et accorde l'accès que l'utilisateur devrait avoir et supprime tout accès qui n'est pas adapté, approprié ou dont il n'a plus besoin.

L'American Council for Technology and Industry Advisory Council (ACT-IAC), un partenariat public-privé à but non lucrative voué à l'amélioration du gouvernement par le biais des technologies de l'information, établit les six piliers du modèle Zero Trust. Ils se résument de la façon suivante :



Le confinement décrété en raison de la crise du Covid-19 par plusieurs gouvernements nationaux a obligé les entreprises à donner accès à leurs applications en dehors du réseau interne ou via des VPN. Les utilisateurs pouvaient se situer n'importe où, sans l'environnement sécuritaire requis. Ce bouleversement brutal, dont la date, le 17 mars 2020, restera dans toutes les mémoires, a obligé la plupart des entreprises à changer de paradigme pour la protection de leurs systèmes d'information et la sécurisation des accès.

Cette situation de travail à distance a généré des problèmes de sécurité, notamment pour accéder à des applications qui n'étaient pas forcément conçues pour être accessibles de l'extérieur du réseau de l'entreprise. Certaines entreprises ont atteint, voire dépassé, les limites de leur VPN, en particulier la limitation de la bande passante.

Dans ce contexte, de nombreuses organisations commencent à adapter leur fonctionnement au travail à distance et leur intérêt pour le concept de Zero Trust a progressé afin d'établir un lien de confiance entre l'utilisateur et la machine. Ce n'est pas parce que l'on a confiance à un collaborateur qu'on a confiance envers sa machine.

➔ Problématique :

Que se passe-t-il lorsqu'on a volé ma carte bancaire ?

Etape 1 : Le voleur va surement utiliser le moyen de paiement SANS CONTACT.

Etape 2 : Au bout de 3 transactions, la carte ne pourra plus fonctionner en sans contact.

Etape 3 : Le voleur devra insérer la carte dans le terminal de paiement.

Etape 4 : Taper le code.

Etape 5 : Au bout de 3 essais, la carte sera bloquée et le porteur recevra un mail/SMS.

Cette problématique est liée avec le Zero Trust. Le paiement sans contact permet de passer la carte sans contact physique, c'est-à-dire sans taper le code confidentiel sur le terminal de commande. Le plafond de paiement sans contact par carte bancaire est relevé à 50€. Les établissements bancaires peuvent fixer un nombre maximum de transactions par jour. Une fois l'un de ces seuils atteints, pour réinitialiser vos plafonds, il faut effectuer une opération avec saisie du code confidentiel (un retrait ou un paiement). Ce code est la preuve pour que la carte puisse identifier et confirmer qu'il s'agit bien du porteur.

Lors de 3 essai, la carte sera bloqué bar une autre stratégie de sécurité, car il ne va pas identifier le vrai porteur de la carte.

➔ **La protection de l'information**

L'information est au cœur des interactions humaines. Elle s'échange à l'oral, à l'écrit, ou via des systèmes plus complexes, comme l'informatique. L'ensemble des ressources, des processus et des outils d'échange d'information (le personnel, le matériel, les logiciels, les procédures…) organisés pour collecter, stocker, traiter et communiquer les informations, constituent le système d'information.

L'information est un des actifs ayant le plus de valeur pour les entreprises (brevets, base de données clients, processus, savoir-faire…). Afin de sécuriser cet actif, il est essentiel de pouvoir garantir les critères suivants :

Confidentialité : il faut protéger les données confidentielles de toute divulgation non autorisée et réserver leur accès aux seules personnes strictement habilités,

Intégrité : il faut s'assurer que les données sont inaltérables dans le temps et dans l'espace,

Disponibilité : il faut garantir l'exécution des traitements et l'accès aux données dans des conditions horaires et de délais prédéfinis,

Traçabilité : il faut fournir des preuves correspondant aux actions effectuées.

➔ **Système d'information et sécurité**

La cybersécurité constitue l'ensemble des disciplines, technologies, organisations, procédures, processus et pratiques permettant de protéger le Systèmes s'Information (SI) contre les menaces internes et externes, notamment la cybercriminalité. **La cybersécurité fait appel à des techniques de sécurisation des systèmes d'information et à la mise en place d'une cyberdéfense.**

Les menaces sont multiples :

Fuites de données (accidentelle ou malveillante),

Attaques cybercriminelles,

Erreurs humaines,

Dégâts matériels…

Une brèche de sécurité au sein d'un Système d'Information peut avoir de lourdes conséquences :

Indisponibilité,

Vols ou corruptions de données,

Altération de la réputation de l'entreprise,

Sanctions légales, réglementaires et financières (exemple : amendes, pertes de licence bancaire)

Les exemples d'entreprises piratées ne manquent pas. Les données volées des entreprises peuvent être diffusées à grande échelle sur Internet ou revendues auprès de concurrents ou d'organisation criminelles.

Aucun secteur n'est épargné par la cybercriminalité. Les brèches de sécurité ont augmenté de 67% au cours des 5 dernières années, le secteur bancaire étant le plus affecté. De l'anticipation des dirigeants à la solidité des processus et des procédures, en passant par l'expertise et la solidité technologique, sans oublier la vigilance de toute personne ayant accès au système d'information (internes ou externes), **la cybersécurité est l'affaire de TOUS.**

➔ **Qui sont les hackers ?**

Aujourd'hui, les cyberattaques sont rarement le fruit d'une seule personne, mais plutôt d'organisations criminelles structurées et complexes. On parle aujourd'hui de CaaS (Cybercrime as a Service).

Les attaques les plus connus :

L'ingénierie sociale

L'usurpation d'identité

Le phishing

Le déni de service pour une entreprise

La propagation d'un virus

L'espionnage …

Les motivations des hackers :

L'argent

L'activisme politique et religieux (hacktivisme)

L'espionnage et la déstabilisation

Sécurité de l'information et des données

Les données stockées et traitées par l'entreprise représentent des actifs extrêmes importants, qu'il convient de protéger de manière appropriée. Avant de communiquer une information, il faut s'assurer de connaître son niveau de classification :

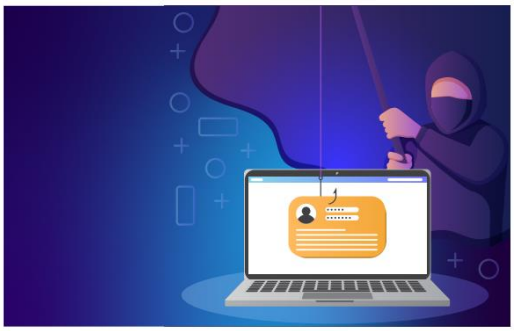
Public : informations qui peuvent être divulguée à quiconque sans briser les règles

Interne : information généralement consulté et utilisé par les employés de l'entreprise

Confidentiel : informations sensibles dont la divulgation non autorisée pourrait directement ou indirectement avoir un impact négatif sur les intérêts de l'entreprise.

Secret : informations hautement sensibles dont la divulgation non autorisée pourrait entraîner un préjudice grave.

➔ **Sécurité des mails**



Le phishing est une technique utilisée, via un email, par les cybercriminels pour obtenir des informations confidentielles ou pour infecter directement votre ordinateur, smartphone ou tablette. Les attaquants se font souvent passer pour un organisme ou une personne de confiance (par exemple : la banque).

Que faire en cas de doute ?

Ne pas ouvrir et ne pas répondre aux emails de provenance inconnue ou dont le contenu est suspect (fautes d'orthographes, mauvaises formulations, incohérences, ...)

Ne pas cliquer sur les liens Internet et ne pas ouvrir ou télécharger les fichiers jointe

En cas de doute, vérifier l'identité de l'expéditeur du message en affichant les détails de l'adresse d'expédition

Personne n'est censé vous demander vos coordonnées personnelles

Si vous constatez que votre ordinateur est infecté, couper immédiatement votre réseau.

Ingénierie sociale

L'ingénierie sociale est une forme de manipulation psychologique, qui permet d'obtenir des informations en exploitant la confiance de la victime. C'est aussi une forme d'usurpation d'identité. Les attaques sont souvent précédées d'une recherche d'informations pour connaître les procédures des entreprises ciblés.

➔ **Firewalls**

Qu'est-ce qu'un Firewall ?

Un Firewall est un appareil de sécurité réseau qui analysent soigneusement le trafic entrant en fonction de règles préétablies et filtrent le trafic provenant de sources non sécurisées ou suspectes pour empêcher les attaques. Les firewalls contrôlent le trafic au point d'entrée d'un ordinateur, appelé port, qui est l'endroit où les informations sont échangées avec des appareils externes.

Comment fonctionne un Firewall ?

Par exemple : « l'adresse source 172.18.1.1 est autorisé à atteindre la destination 172.18.2.1, par le port 22 ». Considérez les adresses IP comme des maisons, et les numéros de port comme des pièces de cette maison. Seules les personnes de confiance (adresses sources) sont autorisées à entrer dans la maison (adresse de destination). Il y a ensuite un filtrage ultérieur, afin que les personnes présentes dans la maison ne puissent accéder qu'à certaines pièces (ports de destination), selon qu'il s'agit du propriétaire, d'un enfant ou d'un invité. Le propriétaire est autorisé à accéder à n'importe quelle pièce (n'importe quel port), tandis que les enfants et les invités sont autorisés à accéder à un certain ensemble de pièces (ports spécifiques).

Certaines caractéristiques des firewalls :

Identifier les applications, pas uniquement les ports : identification exacte de ce qu'est l'application sur tous les ports, indépendamment du protocole, du chiffrement (SSL ou SSH) ou de la technique d'évasion. L'identité d'application devient le fondement de toutes les stratégies de sécurité ;

Identifier les utilisateurs, pas uniquement les adresses IP : utilisation des informations de groupes ou d'utilisateurs stockées dans les annuaires d'entreprise pour la visibilité, la création de stratégies, la génération de rapports et l'investigation détaillée – quel que soit l'endroit où se trouve l'utilisateur ;

Inspecter le contenu en temps réel : protection du réseau contre les failles de sécurité et les logiciels malveillants incorporés dans le trafic d'application, quel que soit leur origine ;

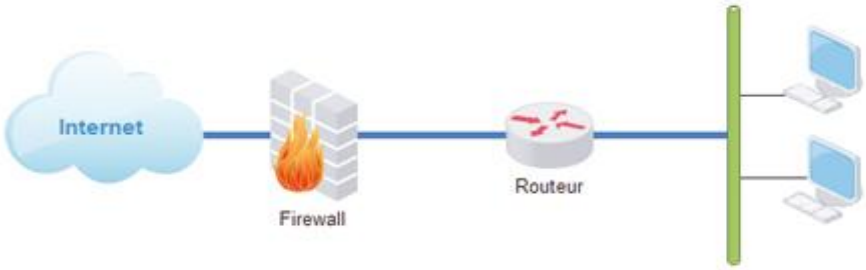
Simplifier la gestion des stratégies : activation sécurisée d'applications à l'aide d'outils graphiques simples d'utilisation qui les lient entre elles de manière unifiée ;

Activer un périmètre logique : sécurisation de tous les utilisateurs en déplacement ou en voyage, avec un niveau de sécurité cohérent qui s'étend du périmètre physique au périmètre logique ;

Fournir un débit multi-gigabits : combinaison de logiciels et de matériel créée dans le but d'offrir des performances à faible latence et à haut débit avec tous les services activés.

Types de Firewall

Les firewalls peuvent être des logiciels ou matériels, mais il est préférable d'avoir les deux. Un firewall est un programme installé sur chaque ordinateur, qui régule le trafic par liais de numéro de port et d'applications. Un firewall physique est un équipement installé entre votre réseau et la passerelle d'accès.



Les firewalls à filtrage de paquets, le type le plus courant, examinent les paquets et leur interdisent de passer s'ils ne correspondent pas à un ensemble de règles de sécurité établies. Ce type de firewalls vérifie les adresses IP source et destination du paquet. Si les paquets correspondent à ceux d'une règle « autorisé » sur le firewall, alors on lui fait confiance pour entrer sur le réseau.

Les firewalls à filtrage de paquets sont divisés en deux catégories : les stateful et les stateless (avec statut ou sans statut). Les firewalls stateless examinent les paquets indépendamment les uns des autres et manquent de contexte, ce qui en fait des cibles faciles pour les pirates informatiques. En revanche, les firewalls stateful (filtrage de paquets, inspection du trafic IPsec[1] et des VPN sous SSL, monitoring réseau ou encore les fonctions de mapping IP[2]) retiennent les informations sur les paquets précédemment transmis et sont considérés comme beaucoup plus sûrs.

Si les firewalls à filtrage de paquets peuvent être efficaces, ils fournissent en fin de compte une protection très élémentaire et peuvent être très limités - par exemple : ils ne peuvent pas déterminer si le contenu de la demande envoyée aura un effet négatif sur l'application qu'elle atteint. Si une requête malveillante autorisée à partir d'une adresse de source fiable entraînait, par exemple, la suppression d'une base de données, le firewall n'aurait aucun moyen de le savoir. Les firewalls de nouvelle génération et les firewalls à proxy sont mieux équipés pour détecter ces menaces.

Firewalls nouvelle génération (NGFW)

Les NGFW combinent la technologie traditionnelle, mais avec des fonctionnalités supplémentaires. Ils effectuent notamment une inspection approfondie des paquets DPI (Deep Packet Inspection). Alors que les firewalls de base n'examinent que les en-têtes de paquets, l'inspection approfondie examine les

[1] IPsec (Internet Protocol Security), regroupe un ensemble de protocoles, qui utilisent des algorithmes destinés à transporter des données sur un réseau IP de façon sécuriser.
[2] Localiser une adresse IP.

données contenues dans le paquet lui-même, ce qui permet aux utilisateurs d'identifier, de classer ou d'arrêter plus efficacement les paquets contenant des données malveillantes.

Firewalls à proxy

Les firewalls à proxy filtrent le trafic réseau au niveau de l'application. Contrairement aux firewalls de base, le proxy agit comme un intermédiaire entre deux terminaux. Le client doit envoyer une demande au firewall, où elle est ensuite évaluée en fonction d'un ensemble de règles de sécurité, puis autorisée ou bloquée. Plus particulièrement, les firewalls à proxy surveillent le trafic pour les protocoles de la couche 7 tels que HTTP et FTP, et utilisent à la fois l'inspection stateful et l'inspection approfondie des paquets pour détecter le trafic malveillant.

Firewalls NAT (Networks Address Translation)

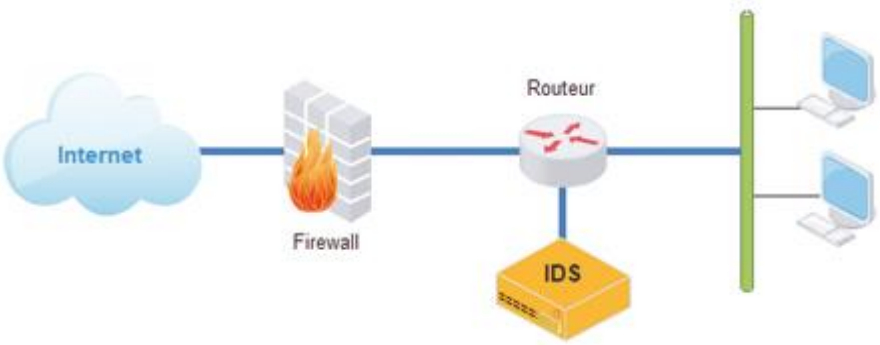
Les firewalls NAT permettent à plusieurs appareils avec des adresses réseau indépendantes à se connecter à l'Internet en utilisant une seule adresse IP, tout en dissimulant les adresses IP individuelles. Par conséquent, les attaquants qui scannent un réseau à la recherche d'adresses IP ne peuvent pas capturer de détails spécifiques, ce qui assure une plus grande sécurité contre les attaques. Les firewalls NAT sont similaires aux firewalls proxy en ce sens qu'ils servent d'intermédiaire entre un groupe d'ordinateurs et le trafic extérieur.

Firewalls SMLI (Stateful Multi-Layer Inspection)

Les firewalls d'inspection de statut multicouches filtrent les paquets au niveau des couches réseau, transport et application, en les comparant à des paquets dont la confiance est connue. Comme les firewalls nouvelle génération, les SMLI examinent également l'ensemble du paquet et ne leur permettent de passer que s'ils sont validés individuellement à chaque couche. Ces firewalls examinent les paquets pour déterminer le statut de la communication afin de s'assurer que toute communication initiée n'a lieu qu'avec des sources fiables.

➔ **IDS**

Un IDS (Système de détection d'intrusion) est un dispositif passif ou une application passive qui surveille et analyse des paquets entiers, en-tête et charge utile, traversant le réseau et les compare aux modèles de signatures connues. Les IDS détectent des événements sur le réseau ou sur un hôte pouvant être malveillant et les signalent. Il déclenche une alarme lorsqu'il détecte une activité suspecte. Les activités suspectes pouvant être par exemple des tentatives d'intrusion, des attaques virales, un débit trop important, un trafic suspect.



Avantages et inconvénients des IDS

Les définitions se trouvent à la page 12.

Avantages	Inconvénients
Pas d'impact sur le réseau (latence, gigue)	Nécessite un bon réglage pour une réaction rapide en cas d'attaque
Pas d'impact en cas de défaillance de la plus sonde	Nécessite une bonne politique de sécurité
Ne peut pas stopper des paquets d'initiation de connexion	Plus vulnérable aux attaques de type « flooding »
La sonde n'est pas visible pour un attaquant (en théorie)	

➔ Les NIDS

Les NIDS (Network Intrusion Detection System) surveillent l'état de la sécurité du réseau en analysant le trafic (les paquets). Si un NIDS détecte une menace, il lance une alerte (qui peut servir à entreprendre des actions de blocage). Il est entièrement passif et ne voit qu'une copie du trafic du réseau à surveiller, il ne peut donc pas communiquer avec ce dernier. Il est situé sur un réseau isolé.

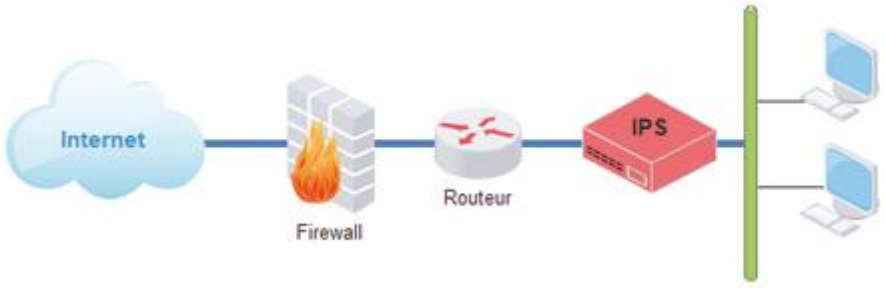
➔ Les HIDS

Les HIDS (Host Intrusion Detection System) surveillent l'état de sécurité sur une seule machine en se basant sur les journaux système et analyse l'activité de l'hôte (nombres de processus, d'utilisateurs ou de ressources consommées), l'activité de l'utilisateur lui-même (horaires, durée de connexion, commandes utilisées, programmes activités) et toutes activités suspectes (vers, virus, trojans).

Exemple de HIDS : Snort

Un NIDS Master récupère les informations des HIDS et les analyses.

➔ IPS



Un IPS (Système de Prévention d'Intrusion) est un dispositif actif ou une application active qui analyse des paquets entiers, en-tête et charge utile, à la recherche d'événements connus. Lorsqu'un événement connu est détecté, le paquet est rejeté

Ils sont positionnés en coupure, à l'inverse des IDS qui analysent une copie du trafic, les IPS sont directement positionnés sur le réseau et le trafic passe directement à travers eux. L'IPS va donc analyser et stopper en temps réel le trafic suspect.

5.1) Les NIPS

Les NIPS (Network Intrusion Prevention System) analysent le trafic réseau en s'appuyant sur une base de données de signatures d'attaques pour bloquer les flux malveillants.

5.2) Les HIPS

Les HIPS (Host Intrusion Prevention System) surveillent les différents éléments (Processus, divers, DLL, etc.) des machines hôtes et bloquent les activités suspectes.

Avantages	Inconvénients
Stoppe les paquets d'initiation de connexion	Une défaillance de la sonde[2] peut affecter le réseau
Peut stopper les attaques de type « flooding[1] »	La surcharge de trafic sur la sonde impactera le réseau
	Nécessite une bonne politique de sécurité
	Quelques impacts sur le réseau (latence[3], gigue[4])
	La sonde est visible et en première ligne pour un attaquant

Identités et des accès (IAM), la gestion des accès privilèges (PAM) et la segmentation du réseau, pour une défense exhaustive et en profondeur. L'accès Zero Trust valorise également les stratégies de gouvernance telles que le principe du moindre privilège.

[1] Action malveillante, en envoyant un grand nombre de requêtes pour provoquer un trafic important ce qui fera que le service sera dégradé pour les utilisateurs.
[2] Un équipement qui permet de gérer la qualité des flux réseau.
[3] une mesure de délai, définit le temps nécessaire pour que les données parviennent à leur destination puis, renvoyer à l'émetteur.
[4] la variation de latence, ou différence de délai de transmission, entre des paquets transmis entre deux systèmes d'un réseau informatique.

Projet monétique