EIT.swiss

Module 233

Protéger et assurer la maintenance d'un réseau

Rédaction et réalisation Nicolas Borowy

Version 1.0 - 30.05.2022

Traduction et relecture

Table des matières

Module 233 : Informaticien(ne) du bâtiment 2ème année

Thème qui sera traité : protéger et assurer la maintenance d'un réseau

Bienvenue dans ce module qui te permettra de découvrir plus en profondeur comment sécuriser un réseau informatique d'entreprise au moyen d'un firewall. La sécurité d'un réseau est primordiale et cet équipement en fait partie. Il n'est certes pas le seul à gérer cette thématique, plusieurs autres équipements ou solutions logicielles complètent l'ensemble afin d'assurer un haut niveau de sécurité du réseau informatique installé.

Prenons un exemple en nous plaçant dans un contexte fictif mais plausible d'un besoin de mise à niveau de la sécurité d'une entreprise. La société GI Technology SA, installée à Berne, est en pleine expansion. Au début de ses activités, seuls trois employés travaillaient sur le site et le routeur de leur connexion Internet, fourni par l'opérateur, suffisait à leurs besoins. Cette société s'agrandit et doit investir dans son matériel informatique. Elle veut notamment installer un nouveau serveur, gérer de manière plus efficace la sécurité de son réseau et le segmenter au niveau des différentes applications liées à leur fonctionnement interne. Dans un futur proche, elle aura également une succursale au Tessin. L'installation d'un lien sécurisé entre les deux sites sera alors nécessaire. Que peux-tu lui proposer en tant que spécialiste dans ce domaine ? Quels sont les thèmes que tu aborderas avec le client et quelles questions vas-tu lui poser afin de lui apporter une solution clé en main adaptée à ses différents besoins ?

Nous tâcherons de répondre à ces différentes questions durant ce module et proposerons une solution adaptée aux besoins de ce client.

Durant ce module, tu auras besoin du matériel requis suivant :

- Un firewall de type proxy (ou applicatif) fonctionnant au niveau des couches réseau et au niveau applicatif, comprenant un contrôleur Wi-Fi, des licences UTM ou équivalentes, proposant différents types de VPN
- Un environnement PC de laboratoire (machines virtuelles) avec :
    - Un serveur Windows de dernière génération (Win 2022 Standard) préconfiguré en contrôleur de domaine, sans autres rôles particuliers
    - Un ou deux PC client avec Windows de dernière génération (Win 11 Pro)
- 2 switches manageables via Web et/ou CLI (implémentation VLAN)
- Un point d'accès Wi-Fi pouvant être intégré dans le contrôleur du firewall ou un point d'accès Standalone ou intégré à une solution Cloud. La fonctionnalité de configuration de VLAN doit être disponible.
- Eventuellement, un dongle Wi-Fi USB
- Eventuellement un onduleur/alimentation secourue
- Eventuellement un serveur NAS (installation de paquets comme FTP, Radius, OpenVPN ou Wireguard, …)

Voici différents thèmes qui seront traitées dans ce module :

- Notions générales sur la sécurité
- Notions système
- Notions objets
- Notions réseau (zones et interfaces)
- Notions NAT/PAT
- Notions règles de sécurités (zones et interfaces), entrée et sortie
- Notions UTM et Cloud
- Notions spécifiques (Sandboxing, SSL Inspection, filtrage de contenu, …)
- Notions contrôleur Wi-Fi et CapWap
- Notions de VPN (IPSEC, Site to Site, Client to Site)
- Notions LDAP, RADIUS

Jour 1 : La sécurité informatique

Objectifs du jour 1

- Introduction sur la sécurité informatique
- Introduction sur les failles de sécurité
- Introduction sur l'évaluation des risques
- Introduction sur les lois et règles en vigueur
- Installation de la place de travail

Commençons ce module en parlant de sécurité informatique. La sécurité informatique est un terme générique qui s'applique aux réseaux, à Internet, aux points de terminaison, aux API, au cloud, aux applications, aux conteneurs, etc. Elle consiste à établir un ensemble de stratégies de sécurité qui fonctionnent conjointement pour nous aider à protéger nos données numériques. La sécurité devrait être intégrée dès la conception d'un projet ou au début d'un cycle de développement.

Qu'est-ce que la sécurité informatique ?

La sécurité informatique protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés. Pour préserver leur compétitivité dans le contexte de la transformation numérique, les entreprises doivent comprendre comment adopter des solutions de sécurité qui sont intégrées dès la phase de conception. En anglais, on utilise l'expression ''shift security left'', qui signifie littéralement ''placer la sécurité à gauche''. En d'autres termes, il faut veiller à intégrer au plus tôt la sécurité dans l'infrastructure et dans le cycle de vie des produits. Ainsi, elle sera à la fois proactive et réactive.

La sécurité continue repose sur un système régulier de feedback et d'adaptation qui est généralement géré au moyen de points de contrôle automatisés. Grâce à l'automatisation, le feedback est rapide et efficace. Il ne ralentit pas le cycle de vie du produit. Cette méthode d'intégration de la sécurité nous permet de mettre en œuvre les mises à jour et les réponses aux incidents rapidement et globalement dans un environnement en constante évolution.

La sécurité informatique demeure un investissement prioritaire pour les entreprises. La liste de contrôle détaille les principales fonctions de sécurité qu'une stratégie de modernisation doit proposer pour nous aider à libérer des ressources et réduire les risques en matière de sécurité et de conformité.

Pourquoi la sécurité informatique est-elle importante pour les entreprises ?

Traditionnellement, la sécurité informatique consistait avant tout à renforcer, maintenir et contrôler le périmètre des datacenters, mais aujourd'hui ce périmètre tend à disparaître. Les méthodes de développement, de déploiement, d'intégration et de gestion informatiques sont en pleine mutation. Avec l'arrivée des clouds publics et hybrides, les responsabilités en matière de sécurité et de conformité réglementaire sont désormais partagées entre différents fournisseurs. L'adoption massive des conteneurs a fait surgir le besoin d'instaurer de nouvelles méthodes d'analyse, de protection et de mise à jour de la distribution des applications. Les applications mobiles fonctionnent sur une multitude d'appareils différents et l'infrastructure repose de plus en plus sur des logiciels, plutôt que sur du matériel. Résultat : les méthodes traditionnelles de gestion de la sécurité sont dépassées. Pour suivre le rythme de la transformation numérique, les programmes de sécurité doivent être adaptés afin que celle-ci soit continue, intégrée et flexible.

Pour assurer la sécurité, certaines entreprises recrutent un responsable de la sécurité des informations métier. Ces responsables sont intégrés à l'équipe métier et sont impliqués dans le cycle de vie des produits, de leur conception à leur adoption. Sous la direction des responsables de la

sécurité des systèmes d'information, ils doivent s'assurer que les enjeux de sécurité sont pris en compte et gérés à toutes les phases, en trouvant le juste équilibre entre sécurité et risques pour l'entreprise afin que la distribution du produit soit à la fois rapide et sûre.

Les failles de sécurités et menaces informatique :

Pour commencer, prends le temps maintenant de dresser une liste la plus exhaustive possible des différentes failles de sécurités ou des menaces pouvant entraver le bon fonctionnement d'un réseau informatique.

Voici une liste non-exhaustive des failles de sécurités et/ou menaces à ce jour :

- Récolte d'informations utiles en questionnant les serveurs DNS ou les contrôleurs de domaines
- Mauvaise gestion des relations de confiance entre différents annuaires
- Mauvaise gestion des droits d'accès et des niveaux d'accès des utilisateurs
- Présence de protocoles d'administration non-sécurisés (SNMP, FTP, Telnet, …)
- Mauvaise gestion des partages de fichiers
- Equipements informatiques à l'abandon sans aucune mise à jour
- Mauvaise gestion des serveurs WEB et des failles de ceux-ci
- Mauvaise gestion des mots de passes, complexité faible, aucune rotation implémentée
- Mauvaise configuration de l'accès Internet
- Les ransomwares
- Le phishing, les spams
- Les fuites de données
- Les attaques DDoS
- L'usurpation d'identité
- Les chevaux de Troie (logiciels espion)
- Les malwares (logiciels malveillants)
- Les virus
- Les vers informatiques
- Le vol de matériel (PC portable, tablettes, smartphones, …)

Si tu en vois d'autres ou que tu en a rencontré d'autres dans ton travail quotidien, profite de mettre à jour cette liste.

Comment peut-on réaliser une évaluation des risques informatiques ?

Les risques dans le domaine de l'informatique sont très nombreux et peuvent découler d'une multitude de facteurs. Ce lien (Link_DE) te permettra de découvrir un document intéressant à ce sujet. Le document PDF est également disponible sur cette plateforme de formation.
Dans notre travail quotidien, nous devons être sensible à ce sujet et souvent trouver des solutions pour y remédier. Voici, en résumé, les différentes étapes qui permettent de définir ce qu'est le risque et comment le corriger d'une manière efficace :

1. Identifier et classer par ordre de priorité les actifs
2. Identifier les menaces
3. Identifier les vulnérabilités
4. Analyser les contrôles
5. Déterminer la probabilité d'un incident
6. Évaluer l'impact potentiel d'une menace
7. Classer par ordre de priorité les risques de sécurité informatique
8. Recommander des contrôles
9. Documenter les résultats

Les aspects juridiques sont également assez vastes et peuvent toucher différents domaines de l'informatique. Le lien (Link_DE) suivant traite de ce sujet.

Le contrôle du réseau est donc primordial et différentes procédures peuvent être mises en œuvre afin de détecter les différentes failles de sécurité.
Swisscom, par exemple, propose, à cet effet, un lien intéressant avec la possibilité d'effectuer un test de sécurité.

Ce lien permet également d'aborder le thème : Une journée de travail vue à travers les lunettes de la sécurité informatique. Le e-learning se trouve ici.

Ce lien permet de voir quelques trucs et astuces en lien avec la sécurité. Ce lien te permettra de faire un contrôle de sécurité en ligne.

Certaines évaluations et audits de sécurité sont réalisés selon certains labels de qualités. Nous pouvons citer ici le label suisse pour la cybersécurité Cyber-Safe. Certains outils, comme Nessus, permettent de faire quelques analyses intéressantes sur les vulnérabilités de nos systèmes informatiques.

Lois, ordonnances et divers liens régissant l'informatique et la sécurité

Une certaine quantité de documents divers et variés décrivent les bases légales de l'informatique et de la sécurité des données. Nous pouvons citer ici une liste non-exhaustive comme :

- La constitution fédérale (Cst ; RS 101)
- Le code civil (CC ; RS 210)
- Le code des obligations (CO ; RS 220)
- L'ordonnance concernant la tenue et la conservation des livres de comptes (Olico ; RS 221.431)
- La loi sur le droit d'auteur et les droits voisins (loi sur le droit d'auteur, LDA, RS 231.1)
- La loi sur les brevets d'invention (LBI ; RS 232.14)
- La loi fédérale sur la protection des données (LPD ; RS 235.1), en particulier l'article 7 et l'ordonnance relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11), en particulier les articles 8 à 11 et 20 à 21
- La loi fédérale contre la concurrence déloyale (LCD ; RS 241)
- Le code de procédure civile (CPC ; RS 272)
- Le code pénal (CP ; RS 311.0)
- La loi sur le travail dans l'industrie, l'artisanat et le commerce (LTr ; RS 822.11)
- L'ordonnance relative à la loi sur le travail (Hygiène) (OLT 3 ; RS 822.113)
- La loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique ; SCSE : RS 943.03)
- L'ordonnance sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique ; OSCSE)
- Le manuel de droit européen en matière de protection des données (la Suisse est également concernée du fait de son adhésion au conseil de l'Europe en 1963, ainsi que par d'autres aspects)
- L'ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (OSPT : RS 780.11), y compris notice explicative du 4 juillet 2018
- Guide relatif au traitement des données personnelles dans le domaine médical, traitement des données personnelles par des personnes privées et organes fédéraux de juillet 2002
- Etc.

Tous ces documents n'ont pas besoin d'être consultés mais permettent de voir que le domaine de l'informatique, bien que très vaste, doit être encadré, normalisé et s'appuyer sur des articles de lois ou des documents précis.

Buts de cette première journée de cours :

- Découvrir en quoi consiste la sécurité et utiliser les différents liens fournis ci-dessus pour réaliser différents tests de sécurité
- S'approprier le thème de la sécurité et rentrer dans le vif du sujet
- Monter l'infrastructure de lab dont tu auras besoin pour le reste du cours
    - Switch
    - Serveur
    - PC
    - AP Wi-Fi

Exercice

L'exercice 1 te donnera les indications nécessaires à la préparation de ton infrastructure.

Jour 2 : Premiers pas avec ton firewall :

Objectifs du jour 2

- Introduction au pare-feu
- Introduction aux ports, interfaces et trunks
- Introduction aux objets
- Configuration de base d'un pare-feu
- Introduction aux règles de sécurité et au NAT/PAT

Pourquoi un firewall ? Petit rappel sur les firewalls et les différents types :

De nos jours, la plupart des entreprises possèdent de nombreux postes informatiques qui sont en général reliés entre eux par un réseau informatique local. Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et ainsi de travailler en équipe sur des projets communs.

La possibilité de travail collaboratif apportée par un réseau informatique local constitue un premier pas. L'étape suivante concerne le besoin d'ouverture du réseau local vers le monde extérieur, c'est à dire internet.

En effet, une entreprise n'est jamais complètement fermée sur elle-même. Il est par exemple nécessaire de pouvoir partager des informations avec les clients de l'entreprise.

Ouvrir l'entreprise vers le monde extérieur signifie aussi laisser une porte ouverte à divers acteurs étrangers. Cette porte peut être utilisée pour des actions qui, si elles ne sont pas contrôlées, peuvent nuire à l'entreprise (piratage de données, destruction, ...). Les mobiles pour effectuer de tel actions sont nombreux et variés : attaque visant le vol de données, passe-temps, ...

Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire. L'architecture devant être mise en place doit comporter un composant essentiel qui est le firewall. Cet outil a pour but de sécuriser au maximum le réseau informatique local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut également permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, comme, par exemple, le partage de fichiers. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu. Tout ceci sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.

Cette vidéo en anglais ou cette vidéo en français expliquent également en quelques minutes ce qu'est un firewall.

Les différentes catégories de firewall

Depuis leur création, les firewalls ont grandement évolué. Ils sont effectivement la première solution technologique utilisé pour la sécurisation des réseaux. De ce fait, il existe maintenant différentes catégories de firewall. Chacune d'entre-elles disposent d'avantages et d'inconvénients qui lui sont propre. Le choix du type d'un type de firewall plutôt qu'un autre dépendra de l'utilisation que l'on souhaite en faire, mais aussi des différentes contraintes imposées par le réseau devant être protégé.

Firewall sans états (stateless)

Ce sont les firewalls les plus anciens mais surtout les plus basiques qui existent. Ils font un contrôle de chaque paquet indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL, Access Control Lists).
Ces firewalls interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquent alors par rapport à une d'adresses IP sources ou destination, mais aussi par rapport à un port source ou destination.

Firewall à états (stateful)

Les firewalls à états sont une évolution des firewalls sans états. La différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés. Les firewalls à états prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de stateful inspection. De ce fait, ils seront capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session :

- NEW : Un client envoie sa première requête.
- ESTABLISHED : Connexion déjà initiée. Elle suit une connexion NEW.
- RELATED : Peut éventuellement être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- INVALID : Correspond à un paquet qui n'est pas valide.

Les attributs gardés en mémoires sont les adresses IP, numéros de port et numéros de séquence des paquets qui ont traversé le firewall. Les firewalls à états sont alors capables de déceler une anomalie protocolaire de TCP. De plus, les connexions actives sont sauvegardées dans une table des états de Connexions. L'application des règles est alors possible sans lire les ACL à chaque fois, car l'ensemble des paquets appartenant à une connexion active seront acceptés.

Un autre avantage de ce type de firewall, se trouve au niveau de la protection contre certaines attaques DoS comme, par exemple, le Syn Flood. Cette attaque très courante consiste à envoyer en masse des paquets de demande de connexion (SYN) sans en attendre la réponse (c'est ce que l'on appel flood). Ceci provoque la surcharge de la table des connexions des serveurs ce qui les rend incapable d'accepter de nouvelles connexions. Les firewalls stateful étant capables de vérifier l'état des sessions, ils sont capables de détecter les tentatives excessives de demande de connexion. Il est possible, en autre, ne pas accepter plus d'une demande de connexion par seconde pour un client donné.

Un autre atout de ces firewalls est l'acceptation d'établissement de connexions à la demande. C'est à dire qu'il n'est plus nécessaire d'ouvrir l'ensemble des ports supérieurs à 1024. Pour cette fonctionnalité, il existe un comportement différent suivant si le protocole utilisé est de type orienté connexion ou non. Pour les protocoles sans connexion (comme, par exemple, UDP), les paquets de réponses légitimes aux paquets envoyés sont acceptés pendant un temps donné. Cependant, pour les protocoles fonctionnant de manière similaire à FTP, il faut gérer l'état de deux connexions (donnée et contrôle). Ceci implique donc que le firewall connaisse le fonctionnement du protocole FTP (et des protocoles analogues), afin qu'il laisse passer le flux de données établi par le serveur.

Firewall applicatif

Les firewall applicatif (aussi nommé pare-feu de type proxy ou passerelle applicative) fonctionne sur la couche 7 du modèle OSI. Cela suppose que le firewall connaisse l'ensemble des protocoles utilisés par chaque application. Chaque protocole dispose d'un module spécifique à celui-ci. C'est à dire que, par exemple, le protocole HTTP sera filtré par un processus proxy HTTP.

Ce type de firewall permet alors d'effectuer une analyse beaucoup plus fine des informations qu'ils font transiter. Ils peuvent ainsi rejeter toutes les requêtes non conformes aux spécifications du protocole. Ils sont alors capables de vérifier, par exemple, que seul le protocole HTTP transite à travers le port 80. Il est également possible d'interdire l'utilisation de tunnels TCP permettant de contourner le filtrage par ports. De ce fait, il est possible d'interdire, par exemple, aux utilisateurs d'utiliser certains services, même s'ils changeant le numéro de port d'utilisation du services (comme, par exemple, les protocoles de peer to peer).

Firewall authentifiant

Les firewalls authentifiant permettent de mettre en place des règles de filtrage suivant les utilisateurs et non plus uniquement suivant des machines à travers le filtre IP. Il est alors possible de suivre l'activité réseau par utilisateur.

Pour que le filtrage puisse être possible, il y a une association entre l'utilisateur connecté et l'adresse IP de la machine qu'il utilise. Il existe plusieurs méthodes d'association. Par exemple authpf, qui utilise SSH, ou encore NuFW qui effectue l'authentification par connexion.

Firewall personnel

Les firewalls personnels sont installés directement sur les postes de travail. Leur principal but est de contrer les virus informatiques et logiciels espions (spyware).

Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applications installés sur la machine. Ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisées à utiliser le réseau.

Première mise en service de ton firewall

La plupart des firewalls actuels possèdent un ‘’wizard’’ d’installation qui permet de réaliser la première configuration de ton équipement. Ce dernier étant très sensible et faisant la jonction entre le réseau WAN (Internet) et LAN (réseau privé), il doit être installé avec le plus grand soin. Son installation va avoir un impact sur toute l’infrastructure informatique de l’entreprise. Elle doit donc être bien planifiée et organisée en accord avec les besoins du client final. L’accès au firewall doit tout particulièrement être configuré en tenant compte de la sécurité et les protocoles par défaut qui ne sont pas utilisés doivent être désactivés. Un accès à la page Web de management doit également être sécurisé au moyen du protocole HTTPS.

Lors du premier ‘’wizard’’ d’installation, les fonctionnalités suivantes sont souvent configurées :

- Hostname
- Domaine
- Raccordement du firewall à un ISP (Ethernet, PPPoE, …)
- Serveur NTP
- Protocoles de gestion autorisés :
    - HTTP : 80 (ne doit plus être utilisé, un transfert vers un port sécurisé HTTPS doit être configuré)
    - HTTPS : 443 (év. 4443, 4444, 8443, …)
    - Telnet : 23 (ne doit plus être utilisé, une connexion SSH doit être privilégiée)
    - SSH : 22

    - FTP : 20 et 21
    - SNMP : 161 (162)
- Interface LAN avec adresse IP, masque de sous-réseau et serveur DHCP lié (pool d'adresses, bail, éventuellement réservation)
- Inscription chez le fournisseur du firewall et activation des licences UTM
- Eventuellement, configuration de la partie contrôleur Wi-Fi du firewall
- Eventuellement, premières règles de sécurité pour l'autorisation de trafic entre le LAN et le WAN
- Eventuellement restrictions d'accès pour le management du firewall et pour les accès VPN depuis la zone WAN
- Eventuellement changement des ports par défaut (management, VPN, …)

Les ports

Les ports physiques sont les connecteurs (RJ45) qui se trouvent sur la partie frontale ou arrière de ton firewall. Ils seront utilisés pour les connexions vers l'opérateur, vers le réseau local et, éventuellement, vers d'autres équipements. Un port peut être utilisé pour une ou plusieurs interfaces en fonction de la configuration effectuée sur le firewall.
Sur certains firewalls, il est possible de faire un regroupement de ports (LAG). Le Groupe d'Agrégation de Liaison (LAG) te permet de combiner plusieurs ports physiques ensemble pour créer un seul chemin de données à large bande passante, afin de mettre en œuvre le partage de la charge de trafic entre les ports membres du groupe et d'améliorer la fiabilité de la connexion. Le protocole utilisé pour ce genre de regroupement est le 802.3ad (LACP).

Les interfaces

Une interface est le point d'interaction logique entre le périphérique (port) et le logiciel du firewall. Dans la plupart des firewalls, il est possible d'attribuer une interface à un port disponible. Il peut y avoir plusieurs types d'interfaces :

- Interface interne (lan, dmz, opt, …), connectée à un réseau local. Le firewall ajoute les paramètres de routage et de NAT source correspondant par défaut.
- Interface externe (wan, ppp, …), connectée à un réseau externe (ISP). Le firewall ajoute les paramètres de routage et de NAT source correspondant par défaut
- Interface générale, connectée à un réseau local ou externe. Les règles de routages ne sont pas créées automatiquement et doivent être configurées manuellement.

Les caractéristiques des interfaces sont les suivantes :

- Entité logique qui effectue le routage L3 et se rapporte à toutes les interfaces
- Chaque interface a une et une seule adresse IP associée
- Les informations de routage sont automatiquement dérivées des paramètres IP de l'interface du firewall

Les fonctionnalités suivantes sont en général supportées :

- Les paramètres généraux comprennent une adresse IP statique, un client/serveur DHCP, etc.
- Un ou deux serveurs relais DHCP peuvent être pris en charge
- La bande passante ascendante et descendante est généralement configurable ainsi que la valeur MTU (Unité de Transmission Maximale)
- Une option de passerelle peut être disponible
- Un proxy IGMP peut être disponible
- Les options DHCP peuvent, en général, être configurées, notamment :
    - Serveurs DNS
    - Serveur WINS
    - Passerelle
    - Durée du bail
    - Réservation d'équipements

- Certaines options étendues peuvent, en général, également être configurées, notamment :
    - Code 2 : Décalage temporel (RFC 2132, mars 1997)
    - Code 4 : Serveur de temps (RFC 2132, mars 1997)
    - Code 42 : Serveurs NTP (protocole de temps de réseau) (RFC 2132, mars 1997)
    - Code 66 : nom du serveur TFTP (RFC 2132, mars 1997)
    - Code 67 : Nom du fichier de démarrage (RFC 2132, mars 1997)
    - Code 120 : serveur SIP (RFC 3361, août 2002)
    - Code 124 : Classe de vendeur identifiant le vendeur (RFC 3925, octobre 2004)
    - Code 125 : Informations spécifiques au vendeur permettant de l'identifier (RFC 3925, octobre 2004)
    - Code 138 : Contrôle et mise à disposition du contrôleur d'accès aux points d'accès sans fil (RFC 5417)
    - Code 150 : Option d'adresse de serveur TFTP (RFC 5859, juin 2010)

Les interfaces particulières

Les VLAN

Les VLANs permettent à un gestionnaire de réseau de segmenter un réseau local en différents domaines de diffusion (Broadcast domain). En général, les firewalls prennent en compte les VLAN standards de type IEEE 802.1q. Les VLANs sont basés sur des balises ou ID.
La balise VID dans l'entête de la trame MAC identifie l'appartenance à un VLAN spécifique (de 0 à 4095), les ID 0 et 4095 étant réservés et non attribuables. Une interface VLAN doit, en général, être configurée avec un VLAN-ID unique basé sur un port physique représentatif. Ce dernier peut avoir plusieurs interfaces VLAN.
En fonction du modèle de firewall, il peut y avoir un nombre maximum de VLAN configurables.

Les interfaces PPPoE

Les interfaces PPPoE sont souvent utilisées en lien avec un ISP. Elles prennent donc en charge le protocole PPP sur Ethernet. Ce protocole est largement utilisé pour les connexions de type DSL fournies par les ISP. Ce type de connexion nécessite d'avoir les paramètres de compte fournis par l'ISP.

Les Trunks

Les interfaces Trunk sont souvent liées aux interfaces WAN. Il s'agit, dans la majeure partie des cas, du regroupement de toutes les interfaces WAN (wan1, wan2, sfp, opt, cellulaire, …) qui permettent d'avoir des accès Internet redondant auprès de plusieurs ISP.
Trois algorithmes d'équilibrages de chargent sont souvent disponibles :

- WRR (Wighted Round Robin), les requêtes sont réparties sur les différents accès Internet. Le firewall divisera le trafic par numéro d'interface WAN et transmettra le trafic par poids d'interface WAN.
- LLF (Least Load First), les requêtes sont envoyées vers l'accès Internet le moins chargé. Le firewall calculera l'utilisation de l'interface WAN et transmettra le trafic par l'interface la moins chargée.
- Spillover, les requêtes sont envoyées d'abord sur le premier accès Internet jusqu'à ce que celui-ci soit utilisé à un certain pourcentage avant de basculer les requêtes suivantes sur le deuxième accès Internet

Chaque interface dans un Trunk peut être configurée comme active ou passive. Cette fonctionnalité est souvent utilisée pour du basculement de Trunk en cas d'indisponibilité d'une connexion Internet (Failover)
Le SNAT met en correspondance l'adresse source du trafic interne avec l'adresse de l'interface de sortie dans le Trunk WAN.

Les interfaces cellulaires

Il s'agit d'une connectivité réseau à haut débit mobile supplémentaire ou une liaison redondante pour une fiabilité maximale. Sur certains firewalls, il est possible de connecter une clé USB avec une carte SIM fournie par l'ISP.

Les objets

Les Firewalls utilisent l'une des innovations les plus sophistiquées en matière de programmation - la programmation référencée par objet ! Cela garantit une performance et une flexibilité optimales dans la programmation des fonctions de ton firewall.

Les zones de sécurité

Les zones de sécurités sont un élément essentiel d'un firewall de type proxy. Elles font souvent partie des objets configurables sur un firewall. Elles peuvent soit être définies et préconfigurées par le fournisseur, soit configurables par l'utilisateur, soit les deux.

- Quelles sont les caractéristiques d'une zone de sécurité :
- Permet une application flexible de la politique de sécurité à plusieurs interfaces
- Une zone est un regroupement logique d'interfaces (physiques ou virtuelles) ou de connexion IPSec
- Une interface existe dans une seule zone
- Le trafic de zone à zone est routé
- Définition de zones pour partitionner un réseau
- Appliquer des politiques de sécurité à une zone

Quels sont les types de zones de sécurité que tu peux rencontrer ?

- WAN
- OPT
- LAN (1, 2, …)
- DMZ
- WLAN
- SSL-VPN
- IPSEC-VPN
- VLAN
- …

Quels sont les différents types de trafic que tu peux rencontrer ?

- Trafic intra-zone : entre les interfaces ou les tunnels VPN dans la même zone
- Trafic inter-zones : entre les interfaces ou les tunnels VPN dans différentes zones
- Trafic extra-zone : vers ou depuis toute interface ou tunnel VPN qui n'est pas attribué à une zone

Il est fort probable que certaines interfaces par défaut soient directement attribuées à des zones particulières et qu'il n'est pas possible de modifier cette attribution dans ton firewall.

Comme nous l'avons déjà vu ci-dessus, les ports physiques de ton firewall peuvent être attribués de différentes manière aux interfaces. Chaque port peut être lié à une interface particulière. Il peut également arriver que plusieurs ports soient liés à la même interface ou qu'un port serve à plusieurs interfaces (VLAN).

Les utilisateurs et groupes

Le firewall intègre toujours des utilisateurs et des groupes locaux. Différents privilèges peuvent être attribués aux utilisateurs et aux groupes. Il peut, par exemple, y avoir des administrateurs, des utilisateurs, des invités, des utilisateurs externes, … Les groupes permettent simplement de

regrouper plusieurs utilisateurs en fonction de leurs droits d'accès ou des disponibilités des fonctionnalités du firewall.

Wi-Fi ou AP

Ces objets permettent en général de configurer différents profils d'utilisation des canaux et des fréquences Wi-Fi en 2.4 et 5 GHz, éventuellement 6GHz. Ils permettent aussi de configurer des identifiants définis de service (SSID, service set identifier) y compris les paramètres de sécurité (clé WPA2/3, liste de filtrage d'adresses MAC, …).
Le protocole CAPWAP est régulièrement utilisé pour faire un pairage (pairing) des points d'accès Wi-Fi avec le contrôleur intégré au firewall. CAPWAP est défini dans la RFC 5415, principalement. CAPWAP (Control And Provisioning of Wireless Access Points) est une protocole Couche 2 (Layer 2) utilisé pour connecter les Bornes Wi-Fi (Access Points) au contrôleur WLAN avec un tunnel. Le tunnel permet d'avoir une seule connexion Couche 3 (Layer 3) entre la borne et le contrôleur, et mettre tout le trafic (contrôle et donnés de plusieurs WLANs) dans cette connexion unique.

Applications

Certaines applications peuvent être configurées et traitées comme des objets par le firewall. Elles peuvent parfois être classées par catégories. Voici une liste non exhaustive de certaines applications :

- Messagerie instantanée
- P2P
- Transfert de fichier
- Streaming
- Base de données
- Terminaux d'accès à distance
- Mise à jour de sécurité
- Entreprise
- Protocole privé
- Courrier et Collaboration
- Jeux
- Contournement des proxy et tunnels
- MI Web
- Protocoles de réseau
- Réseaux sociaux
- Voix sur IP (VoIP)
- Gestion de réseaux
- Internet
- Trafic TCP/IP
- Mobile
- …

Adresse et groupe d'adresses

Les objets adresses regroupent toutes les adresses de type IP v4 et v6. Il peut s'agir des types suivants :

- Hôte ou Host
- Plage d'adresses ou Range
- Sous-réseau ou Subnet
- Interface
- FQDN (Fully Qualified Domain Name)
- Géographique

Il est également possible de créer des groupes d'adresses en fonction des besoins et des configurations du firewall.

Services

Les services permettent de définir tous les types de protocoles nécessaires aux différentes transmissions qui passent au travers du firewall. Il peut s'agir d'applications spécifiques utilisant TCP, UDP et ICMP (HTTPS, HTTP, SMTP, POP, FTP, …) par exemple ou de services définis par l'utilisateur.
Il est également possible de créer des groupes de services en fonction des besoins et des configurations du firewall.

Calendrier (planning ou scheduling)

Ce type d'objet permet de prendre en charge des plannings ponctuels ou récurrents au niveau du système. Ils peuvent être utilisés pour des politiques de routage, des politiques de sécurité, des services UTM (contrôle applicatif), du filtrage de contenu, de l'activation et/ou désactivation de diffusion de réseaux Wi-Fi, …
Il est également possible de créer des groupes de calendriers en fonction des besoins et des configurations du firewall.

Certificats

Ce type d'objet permet de créer un certificat auto-signé par le système, de générer une demande de certification ou d'utiliser un certificat établi par une société de certification (Verisign, GoDaddy, …). Il permet également d'échanger la clé publique pour l'authentification. Les firewalls enregistrent normalement les certificats CA et les certificats d'hôte distant autorisés sur les appareils.

Comptes ISP

Les comptes ISP sont également considérés comme des objets. Ils seront ensuite utilisés dans la configuration des interfaces WAN (PPPoE).

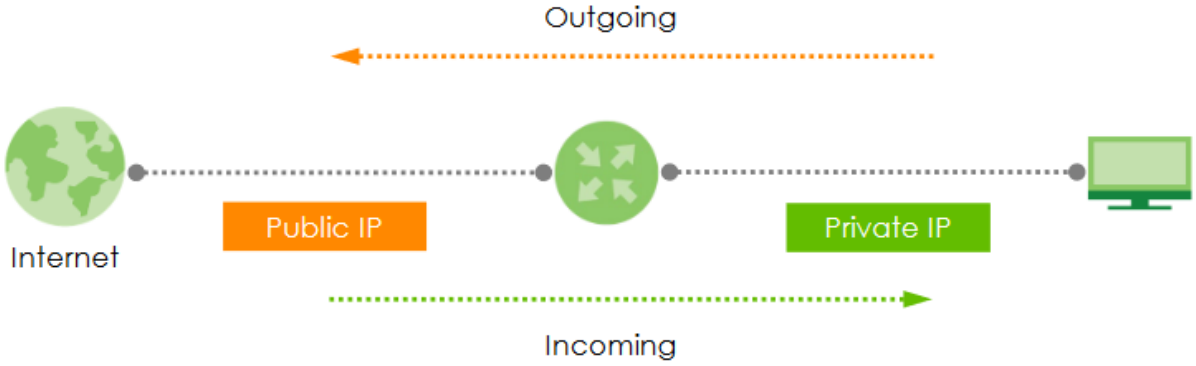
D'autres types d'objets peuvent également exister en fonction du modèle et de la marque du firewall choisi. Cette liste n'est donc pas exhaustive.

L'exercice 2 te permettra de mettre en service ton firewall et de configurer les paramètres essentiels à son bon fonctionnement. Il te permettra également de voir et de configurer les différents objets nécessaires lors des prochains jours.

Le NAT

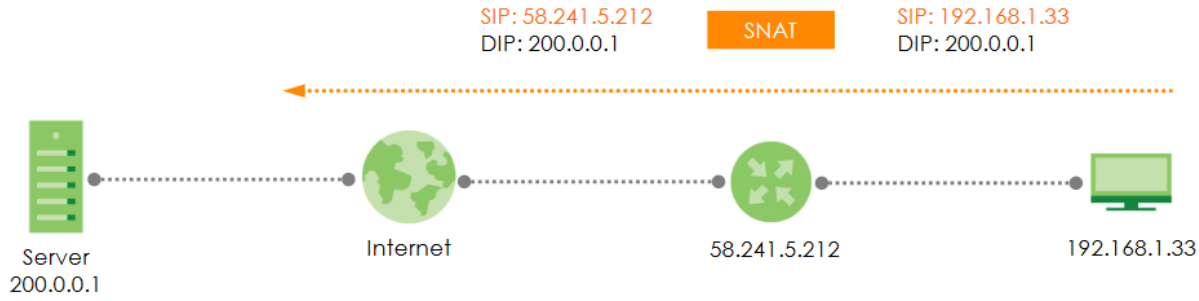
Qu'est-ce que le NAT et à quoi peut-il servir ?

Le NAT signifie Network Address Translation (traduction d'adresse réseau). Le NAT se charge de traduire l'adresse IP privé (LAN) en adresse IP publique (WAN), il s'agit donc d'un mappage NAT. Cette fonctionnalité sert notamment à sécuriser les hôtes qui se trouvent dans la partie privée (LAN) ainsi que les différentes ressources de l'entreprise. Elle permet également de palier à la pénurie d'adresses IP v4 au niveau mondial. Il est alors possible de faire correspondre une seule adresse IP externe publique et visible sur Internet à une ou plusieurs adresses IP d'un réseau privé.



SNAT

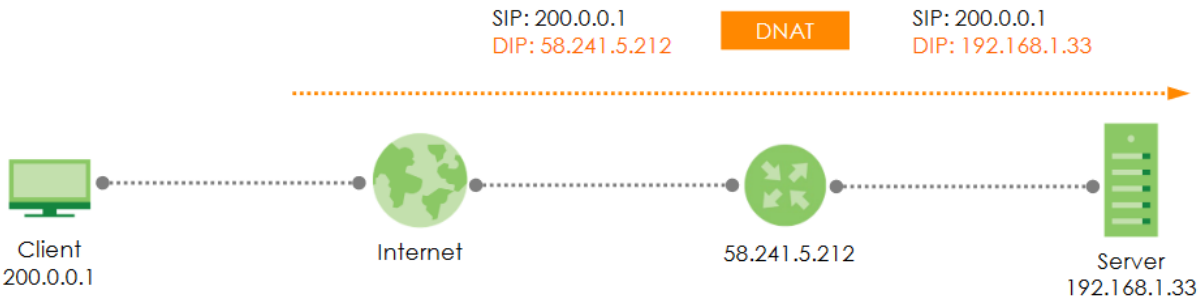
Le SNAT traduit l'adresse IP de la source du trafic



Note:
SIP: Source IP address
DIP: Destination IP address

Le DNAT

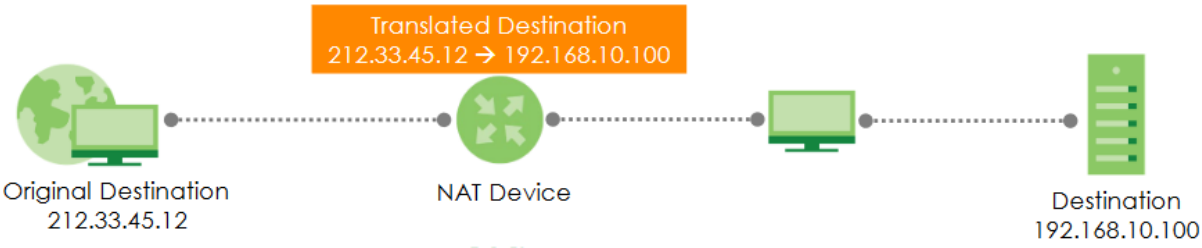
Le DNAT traduit l'adresse IP de la destination du trafic



Les types de NAT

- Serveur virtuel
- NAT 1:1
- Multi NAT 1:1

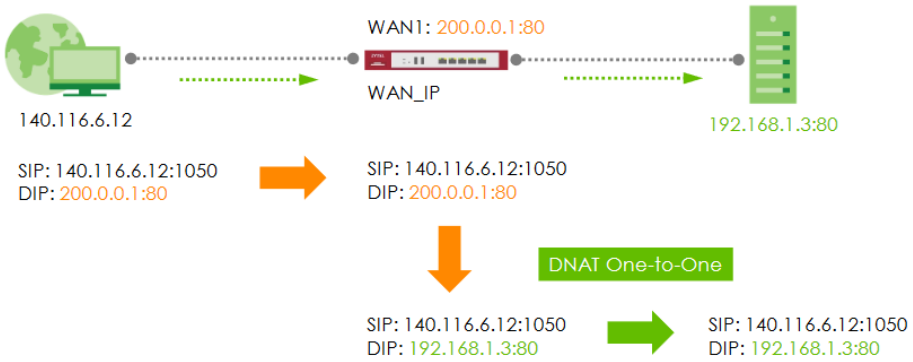
Serveur Virtuel



Il peut être configuré de 2 manières différentes :

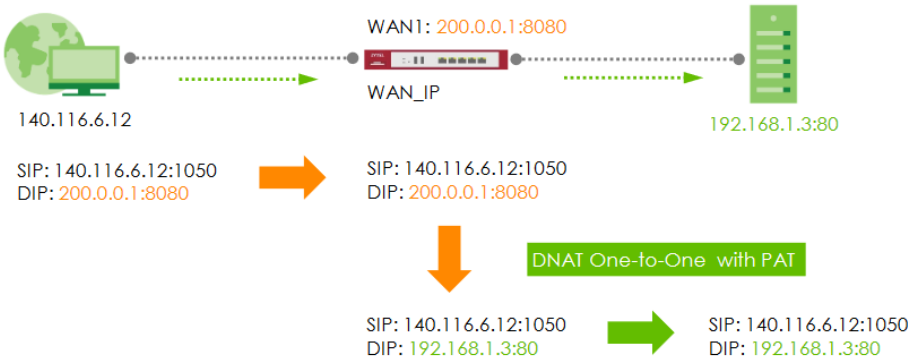
- DNAT un à un
- DNAT un à un avec PAT

Name	Interface	Original IP	Mapped IP	Mapping Type	Protocol Type	Original Port	Mapped Port
HTTP_SERVER	wan1	200.0.0.1	192.168.1.3	Port	TCP	80	80



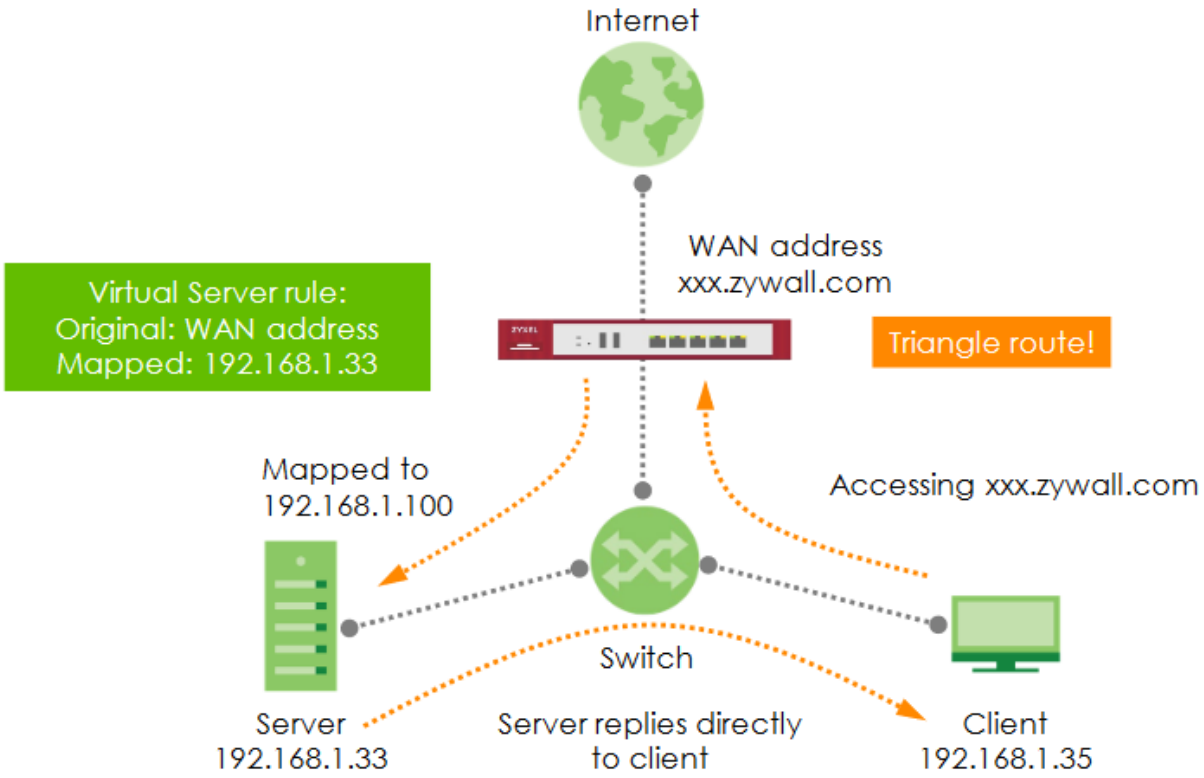
DNAT un à un

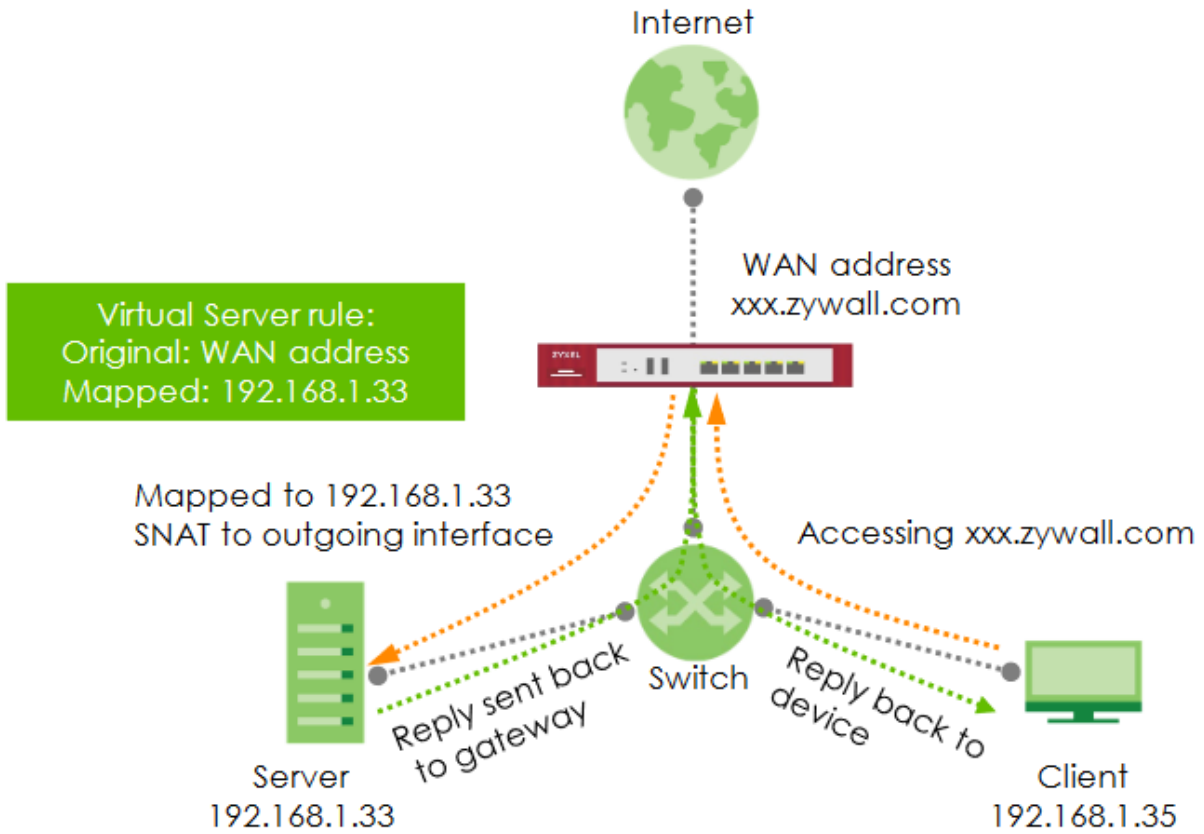
Name	Interface	Original IP	Mapped IP	Mapping Type	Protocol Type	Original Port	Mapped Port
HTTP_SERVER	wan1	200.0.0.1	192.168.1.3	Port	TCP	8080	80



DNAT un à un avec PAT

Dans ces deux scénarios, il sera peut-être nécessaire d'activer la fonction de Loopback si la destination à atteindre se trouve dans le même réseau interne (LAN) que le PC qui fait la requête.

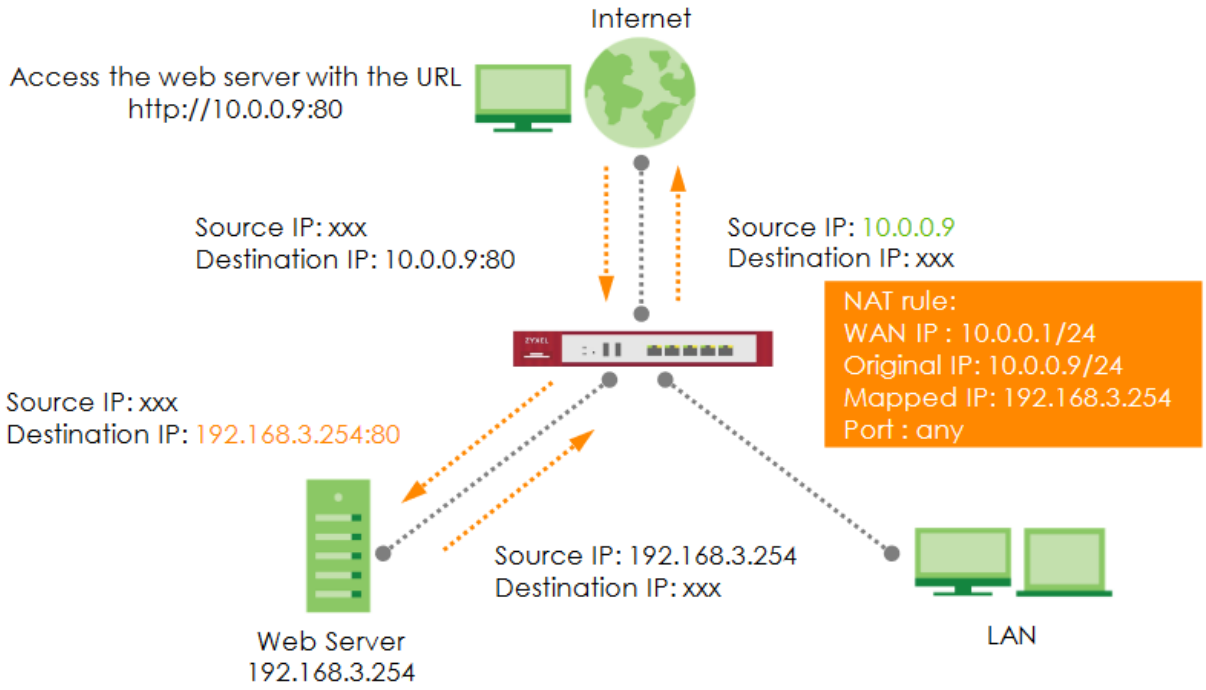




Loopback actif

NAT 1:1

Toutes les demandes adressées à l'adresse IP publique seront directement transmises au client interne sélectionné, peu importe le port utilisé.



Multi NAT 1:1

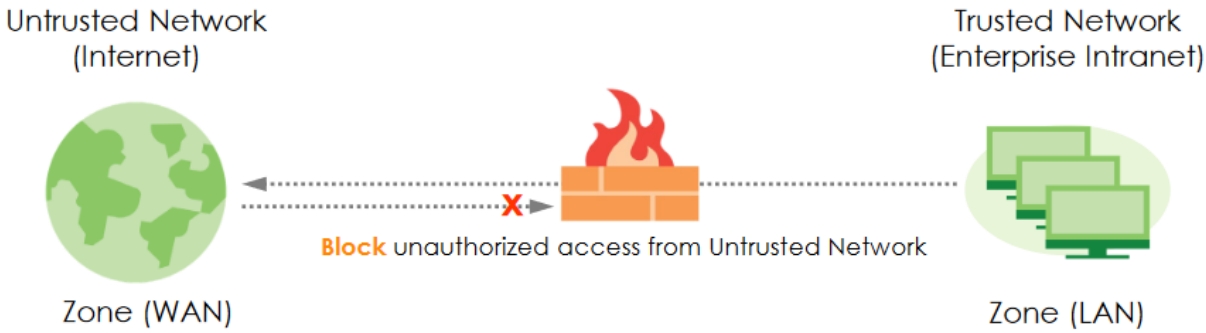
Il est semblable au NAT 1:1 :

- Le système acheminera le trafic et effectuera le SNAT automatiquement
- Plusieurs types de groupes sont disponibles :
  - Sous-réseau
  - Plage d'adresses
- Les sous-réseaux ou les plages d'adresses privées et publics doivent avoir le même nombre d'adresses IP

Les règles de sécurité (ou politique de sécurité)

Les règles de sécurité sont une des principales caractéristiques d'un pare-feu. Elles peuvent, dans certains cas, être liées à une règle NAT.

Cet outil de cybersécurité est utilisé pour filtrer le trafic sur le réseau informatique. Il établit généralement une barrière entre une réseau interne fiable et un réseau externe non fiable tel que l'Internet.



Comme nous l'avons déjà vu précédemment, il existe plusieurs types de pare-feu dont voici un résumer des principaux :

Pare-feu à filtrage de paquets (couche 3)

Il examine les paquets sur la base d'information contenues dans les entêtes, notamment les adresses sources et destinations

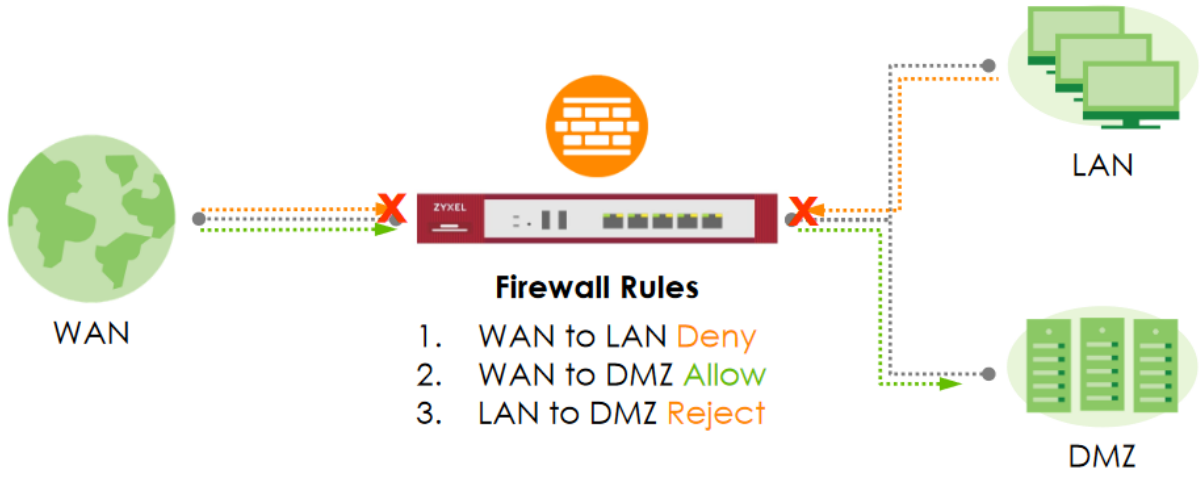
Pare-feu à inspection d'état (couche 4)

Il examine non seulement les informations contenues dans les entêtes mais également le contenu des paquets jusqu'à la couche application. Les adresses sources et destinations ainsi que l'état des sessions TCP et les numéros de séquences TCP seront analysés.

Pare-feu proxy complet (couche 7)

Il examine les différentes informations de façon similaire aux autres pares-feux mais il analysera également en profondeur toutes les applications générant les différents paquets ainsi que la raison d'être des différents protocoles utilisés.

Voici un exemple de protections de zones de sécurité :



Certains pares-feux ne possèdent aucune règle de sécurité lors de leur mise en service alors que d'autres en ont par défaut. Ces dernières permettent, en général, au trafic venant du réseau interne du client à sortir sur le réseau externe (Internet). Certains pares-feux possèdent également une règle par défaut refusant tout type de trafic qui n'aurait pu être traité par d'autres règles de sécurité en amont de cette dernière. Nous parlons souvent d'une politique de sécurité directionnelle dont voici un exemple :

Les règles de sécurités sont constituées des objets suivants :

- Zones de sécurité
- IP Source et IP de destination (Host, Range, Subnet, …)
- Service(s)
- Eventuellement, utilisateurs
- Eventuellement planification de temps (scheduling)
- Action du pare-feu (accepter/autoriser, rejeter, refuser, …)

Exercice

L'exercice 2 te donnera les indications nécessaires pour la configuration des règles NAT/PAT et des règles de sécurités de ton pare-feu. Il te permettra également de te familiariser avec toute la partie objets de ton pare-feu.

Jour 3

Objectifs du jour 3

- Configuration des services UTM
- Configuration des différents types de VPN

Nous poursuivons la configuration de notre pare-feu et continuons sur les règles de sécurité étudiées et pratiquées durant le jour 2.
Nous allons traiter des solutions de gestion unifiée des menaces ou Unified Threat Management (UTM) et les ajouter aux règles de sécurité déjà en place dans notre pare-feu. Ces différentes fonctionnalités ne se retrouvent que dans certains pares-feux et ne sont pas disponibles dans les routeurs d'accès Internet fournis par nos opérateurs. Certaines de ces solutions peuvent, en revanche, être fournies par l'opérateur par le biais de services additionnels (par ex. Swisscom BNS avec pare-feu avancé, filtrage de contenu, …).

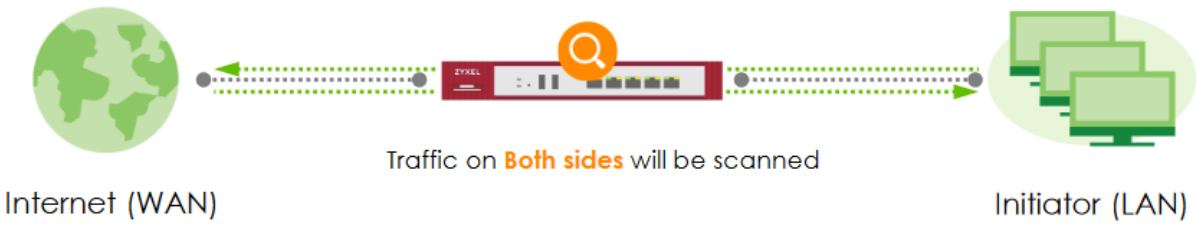
Politique de sécurité unifiée

Une politique de sécurité unifiée permet d'intégrer au pare-feu toutes les fonctionnalités UTM dans un flux de configuration unique. Aux règles de bases (zones, IP source et destination, ports, plannings, utilisateurs) s'ajoutent les différents profils UTM disposant des fonctionnalités suivantes :

- Monitoring des applications (Application Patrol)
- Filtrage du contenu (CF) WEB et DNS
- Détection et prévention des intrusion (IDP ou IPS)
- Anti-Virus
- Anti-Spam
- Anti-Malware
- Inspection SSL
- Filtre de réputation (IP, DNS, URL)
- Bac à sable (Sandboxing)
- Détection et prévention des anomalies (ADP)
- Détection et réponse collaborative (CDR)

En fonction des pares-feux, il peut y avoir éventuellement d'autres options disponibles.

Une politique de sécurité unifiée nécessite de configurer la direction en fonction de la direction initiale de la session, ceci pour chaque profils UTM. Par exemple, est-ce que la session et ouverte depuis le LAN vers le WAN ou inversement. Normalement, tout le trafic sera scanné automatique dans les deux sens.



La création d'une politique de sécurité peut se résumer en 3 étapes :

1. Création d'un objet en lien avec l'analyse désirée (par exemple, contrôle d'une application particulière comme Facebook)
2. Création d'un profil UTM en choisissant l'objet créé précédemment et appliquer une action spécifique comme transmettre, abandonner ou rejeter le paquet

3. Création d'une politique de sécurité et d'une règle de sécurité au niveau du pare-feu en définissant le trafic de la zone source vers la zone de destination et en y appliquant le profil UTM créé précédemment

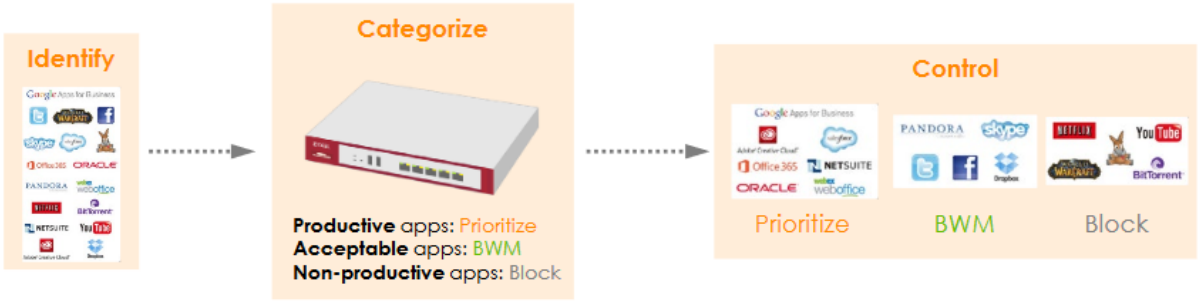
Services UTM

Patrouille d'applications (Application Patrol ou AP)

Un dilemme se pose entre le contrôle absolu des applications et leur vulnérabilité potentielle. L'Internet et les applications de réseaux sociaux sont une des principales sources d'attaque et de vulnérabilités. Ce sont toutefois des outils de communication modernes qui améliorent la productivité. Le défi qui se pose alors en informatique est de gérer cet ensemble d'applications sans entraver la productivité des collaborateurs.
La patrouille d'applications permet un contrôle granulaire, précis et flexible :

- Identifier, catégoriser et contrôler plus de 3000 applications et comportement sur le WEB
- Configurer divers modes de contrôle : prioriser, gestion de la bande passante (BWM), blocage
- Mise en œuvre efficace de la politique sur les médias sociaux, les jeux, le Peer to Peer (P2P) et d'autres applications WEB.

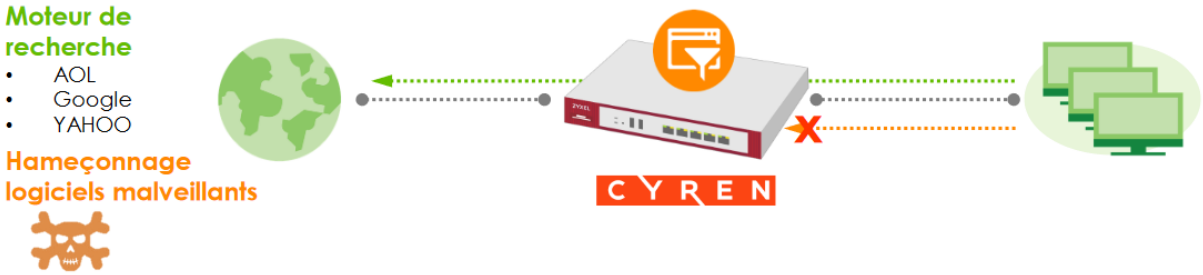
Le développement des signatures de ces différentes applications à la pointe de l'industrie permet une mise à jour régulière (journalière, hebdomadaire ou mensuelle) des pares-feux.



Exemple de configuration : blocage du trafic lié à Facebook :

Filtrage du contenu (CF)

Le filtrage de contenu permet d'empêcher les utilisateurs d'accéder à des sites WEB dangereux ou non autorisés. Il identifie les sites WEB et les classifie en fonction de leur contenu afin de gérer l'accès des utilisateurs. Il agit (autorise, bloque, averti ou restreint la fonction WEB) en fonction des profils configurés par le gestionnaire du pare-feu.



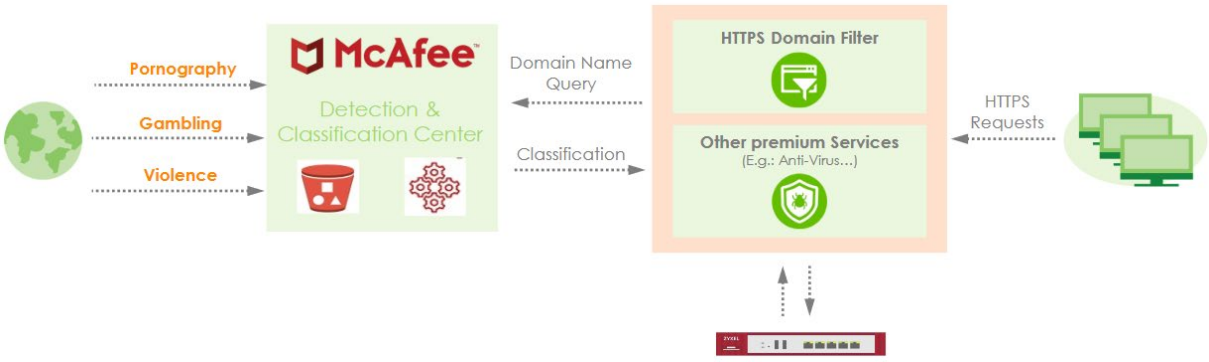
Certains pares-feux intègrent une fonction de tests des pages WEB afin de définir de quel contenu il s'agit. Il est également possible de créer ses propres listes de sites WEB autorisés (White List ou Trusted) ou non autorisés (Black List ou Forbidden). Lorsqu'un utilisateur essaie d'accéder vers un site WEB non autorisé, il peut être redirigé vers une page WEB lui indiquant que l'accès à ce dernier n'est pas autorisé par le gestionnaire du pare-feu.
Certains fournisseurs de matériel permettent également de leur signaler un site WEB dangereux afin qu'ils l'intègrent dans une future base de données et qu'il soit disponible pour d'autres utilisateurs des mêmes pares-feux.

Voici un exemple de filtrage qui permet de bloquer le site WEB IGN et les sites WEB du même type. Un utilisateur qui essaie d'y accéder verra une page lui indiquant que l'accès au site est interdit.

Certains pares-feux intègrent également des fonctionnalités complémentaires :

- Contrôle du contenu de sites WEB sécurisés avec SSL (HTTPS)
- Contrôle du nom de domaine utilisé plutôt que l'adresse WEB entière (URL)

Voici un exemple de filtrage de domaine HTTPS :

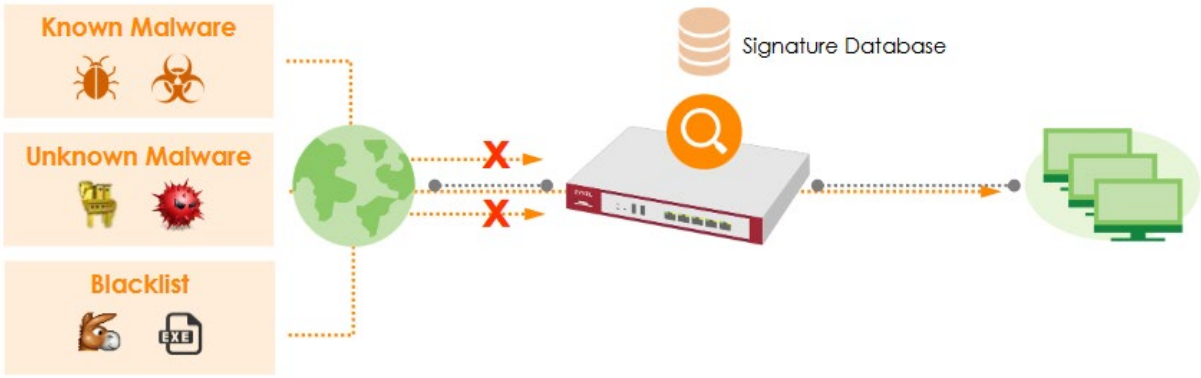


Certains pares-feux intègrent également des fonctionnalités de blocage de trafic en provenance ou à destination d'un pays ou d'un continent particulier.

L'IP géographique permet d'identifier la localisation des utilisateurs d'Internet. La base de données ''MaxMind'' fournit une précision de presque 100% pour les adresses IP des pays et est mise à jour chaque semaine. Le gestionnaire du pare-feu peut également ajouter une adresse ou une liste d'adresses en fonction des besoins.

Anti-Virus (AV)

La fonction anti-virus permet de sécuriser l'environnement local. Lorsqu'un utilisateur télécharge un fichier sur Internet, le moteur anti-virus l'analyse et applique une stratégie particulière (continue le téléchargement, suppression du fichier, …) en fonction de sa dangerosité. Le pare-feu constitue une base de données ou liste noire de fichiers ou de logiciels malveillants.



Anti-Spam (AS)

La fonction anti-spam assure une protection éprouvée et performante avec une stricte confidentialité des contenus.
Les objectifs principaux sont :

- D'identifier les nouveaux spams, logiciels malveillants et attaques de type phishing dès leur apparition sur le WEB. Les caractéristiques les plus fondamentales qui sont analysées sont la distribution en masse de mails et les motifs répétitifs.
- Bénéficier d'une détection globale à partir d'une solution brevetée, agnostique en termes de contenu et de langue
- Prise en charge des protocoles POP, IMAP et SMTP

En fonction du modèle de pare-feu, la fonction anti-spam utilise la mémoire de l'équipement pour charger et vérifier le courrier électronique. Il faut vérifier les spécifications de l'équipement pour savoir le nombre de requêtes qui peuvent être traitées simultanément et connaître le comportement de celui-ci si la mémoire est saturée. Certains pares-feux, dans cette situation, suppriment ou transfèrent le courrier à la destination finale.

Détection et prévention des anomalies et des intrusions (ADP et IDP)

La prévention des menaces et le blocage des trafics malveillants constituent la première étape pour assurer la sécurité des entreprises. Ces dernières peuvent exploiter davantage le ''lissage de trafic'' ou la régulation de flux et le contrôle d'application pour gérer entièrement leur réseau et donner la priorité à des trafics importants comme les appels vocaux ou les téléconférences.

La détection et la prévention d'anomalies (ADP) protège contre des violations de protocoles et des flux anormaux tels que les scans de ports. Elle permet de contrôler les anomalies liées à la circulation et aux protocoles. Elle est en général basée sur un microprogramme et analyse les anomalies suivantes.

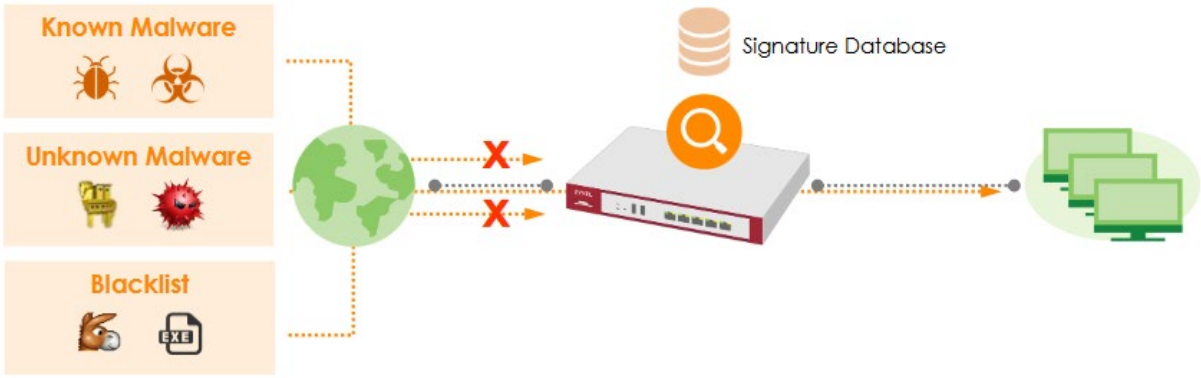
- Anomalie de trafic : balayage des ports, inondation des réseaux
- Anomalie basée sur des violation de normes et de protocoles : décodeur TCP, UDP, ICMP

La détection et la prévention d'intrusions (IDP) permet de détecter les paquets malveillants ou suspects et d'y répondre instantanément. Elle permet de contrôler et d'inspecter les signatures des paquets. Elle est en général basée sur une signature en lien avec les attaques connues provenant de l'Internet. Il s'agit d'une couverture complète des domaines suivants :

- DoS/DDoS
- Buffer Overflow
- Trojan et Backdoor
- Virus et Worm
- Contrôle d'accès
- Scan
- Attaque WEB
- Autres

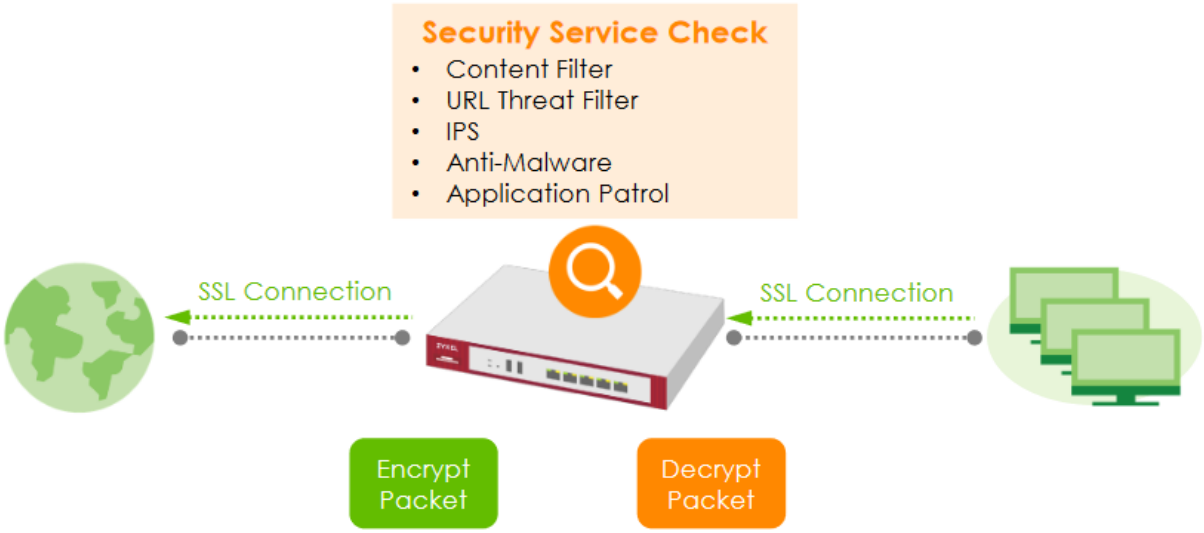
Les fonctionnalités suivantes sont en général mises en œuvre :

- Analyse de la menace en fonction du contexte des couches 4 à 7 du modèle OSI
- Analyse du comportement des menaces et des applications cryptées
- Protection contre les vulnérabilités côté client et côté serveur
- Fournir une protection contre les menaces fondées sur les anomalies et les vulnérabilités
- Moteur primé (certifié par différents organismes réputés comme NSS et ICSA)
- Soutenir la protection fondée sur l'exploitation et la vulnérabilité
- Soutenir les attaques WEB comme le XSS (Cross-site scripting ou injection de code malicieux)
- Système de gestion et de rapports



Inspection SSL

Le protocole SSL (Secure Socket Layer) est de plus en plus répandu. Le cryptage du trafic met les données privées à l'abri des regards indiscrets. Toutefois, son utilisation comporte des risques car le trafic crypté peut être utilisé pour contourner les défenses habituelles. Les logiciels malveillants peuvent malheureusement être transmis par le protocole SSL. L'inspection SSL déverrouille les sessions cryptées et les transmets aux fonctions UTM pour une vérification avancée du contenu. Ceci permet de protéger le réseau informatique contre les menaces.



Suivant les fournisseurs de pares-feux, il est nécessaire de contrôler les paramètres suivants :

- Chiffrements pris en charge par l'inspection SSL : RC4, DES, 3DES, AES
- Versions SSL prises en charge par l'inspection SSL : TLSv1, TLSv1.1, TLSv1.2, SSLv2, SSLv3

Suivant les fournisseurs de pares-feux, il peut être nécessaire d'importer le certificat généré par le pare-feu sur les ordinateurs. Pour se faire, la commande certmgr.msc peut être lancée en mode administrateur de la machine et le certificat peut être importé dans ''Trusted Root Certificate Authorities > Certificates''.

Les moteurs de recherche affichent des résultats qui correspondent à vos mots-clés. Toutefois, les sites Web illicites apparaissent parfois dans les résultats de recherche (images et/ou vidéos inappropriées ou explicites). SafeSearch est une caractéristique des moteurs de recherche qui permet de filtrer les résultats de recherche illicites. La plupart des grands moteurs de recherche viennent avec la fonctionnalité SafeSearch, ce qui permet aux utilisateurs d'ajuster la rigueur de la fonctionnalité SafeSearch.

Lorsque SafeSearch est activé, le pare-feu ajoute un paramètre de spécification à l'URL de recherche.

Exemple : https://www.google.com/search?q=Red+crowned+crane&safe=active

Anti-Malware

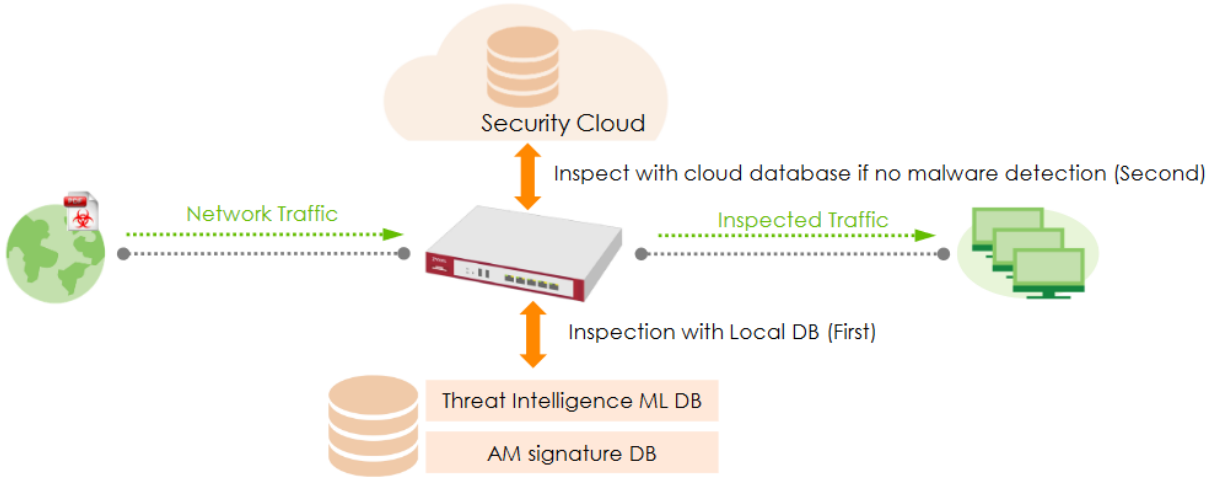
La fonction anti-programmes malveillants (anti-malware) peut être utilisée de différentes manières en fonction du matériel informatique fourni. Les modes de scans suivants peuvent être disponibles :

- Scan local (mode streaming) : le moteur d'analyse anti-malware s'appuie sur les bases de données locales de signatures de virus pour déterminer si le fichier est infecté et prend des mesures. Les protocoles suivants peuvent être analysés : HTTP, HTTPS, FTP, FTPS, POP3, POP3S, SMTP, SMTPS, autres protocoles. De manière générale, tous les types de fichiers sont analysés, peu importe la taille du fichier.
- Scan Cloud : le moteur d'analyse anti-malware inspecte le fichier en envoyant la valeur de hachage MD5 au service Cloud. Ce dernier consulte sa base de données puis répond au pare-feu dans un laps de temps relativement court. La mise à jour des signatures est souvent

beaucoup plus rapide dans ce mode. Les protocoles analysés sont en général les mêmes que pour le scan local. En fonction du service Cloud, il n'est pas certains que tous les types de fichiers puissent y être analysés, en revanche, la taille du fichier n'a pas de limite spécifique. Il faut également configurer une action spécifique si le service Cloud ne répond pas, afin que le pare-feu sache que faire des paquets (faire suivre le trafic, suppression, …).

- Scan hybride regroupant les deux premiers. Dans ce mode, le moteur d'analyse anti-malware s'appuie premièrement sur sa base de données locale. S'il ne trouve pas de signature particulière, il fera une requête au service Cloud pour identifier le programme malveillant.

Exemple d'un scan hybride :



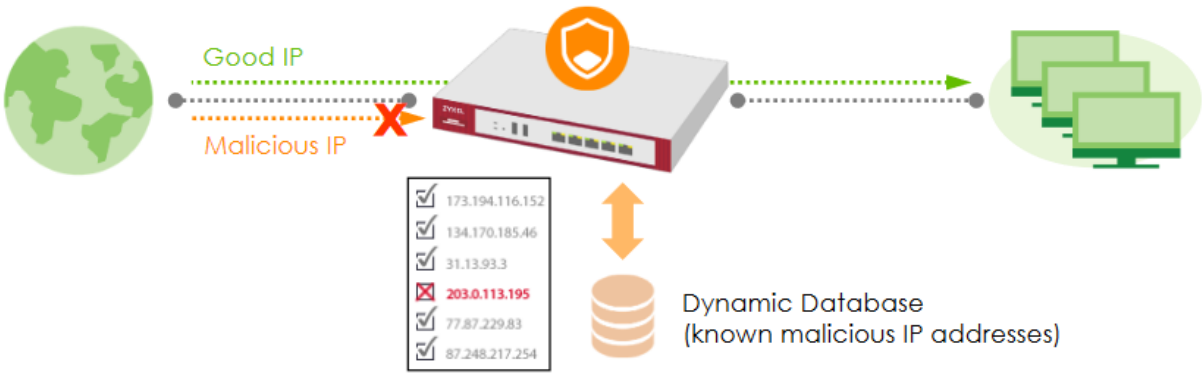
Filtre de réputation

Le filtre de réputation est une combinaison des services de filtrage de réputation IP et de la menace URL. La réputation IP filtre le trafic sur la base de l'adresse IP. Le filtre de menace d'URL filtre le trafic en fonction de la catégorie d'URL.

Le blocage du trafic à destination ou en provenance d'adresses IP malveillantes connues est le moyen efficace d'améliorer la sécurité du réseau et les performances de la passerelle. Il permet de filtrer très rapidement le trafic crypté et non crypté. Il permet également de réduire le nombre de paquets devant être scannés par d'autres services de sécurité tels que l'IDP, l'Anti-Malware.

Le service de réputation IP fournit une base de données des adresses IP publiques réputées comme malveillantes, ce qui permet au pare-feu d'agir lorsqu'il reçoit du trafic de et vers une adresse IP figurant sur la liste. La base de données est régulièrement mise à jour.

Exemple de filtrage :



Les adresses IP publiques malveillantes figurant dans la base de données sont classées selon un certain nombre de menaces et selon plusieurs niveaux (faible, moyen, élevé, …) :

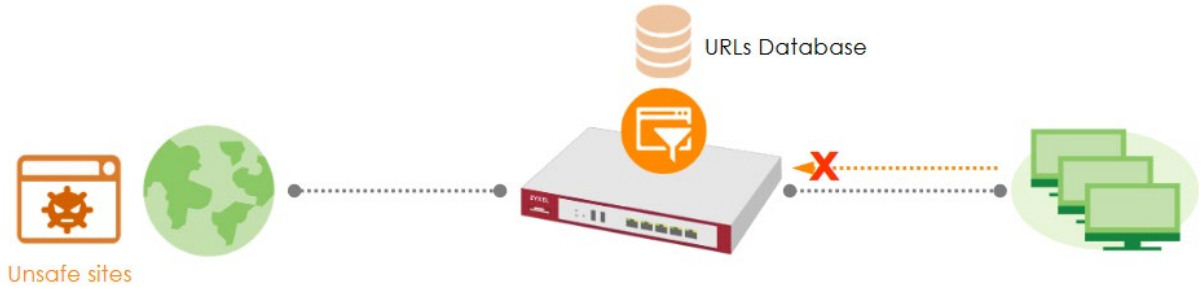
- Proxys anonymes
- Déni de service (DoS)
- Exploits
- Réputation négative
- Scanners
- Sources de spam
- Proxy TOR
- Attaques WEB
- Botnets
- Phishing (hameçonnage)

Un défi persiste malheureusement avec les services Cloud. De nos jours, les prestataires tels que les hébergeurs partagent l'adresse IP publique avec de nombreux locataires, ce qui conduit à ce que leur adresse IP publique soit parfois répertoriée comme malveillante ce qui peut perturber plusieurs services de locataires pourtant fiables.

En fonction du matériel, il est possible de sélectionner les catégories ou les niveaux d'analyses afin d'autoriser certains accès à l'adresse IP de destination.

Il faut également contrôler quels types d'adresses IP sont prise en charge par le fournisseur du pare-feu.

Le filtre de menaces d'URL compare l'accès à des URL spécifiques à une base de données de sites bloqués ou autorisés.

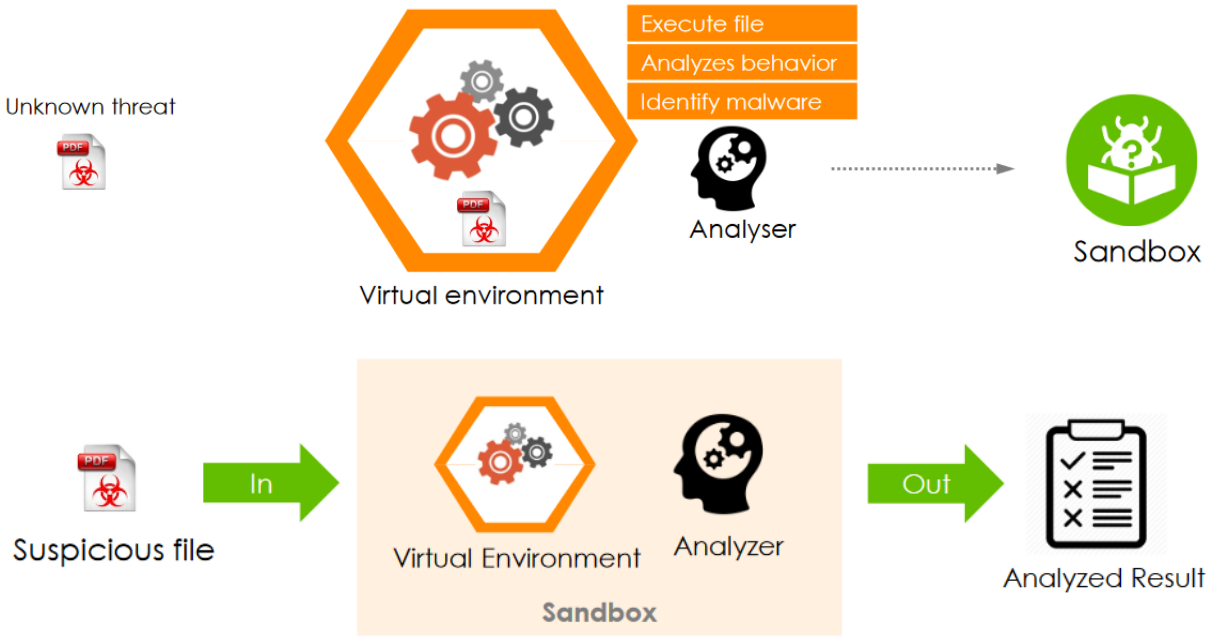


Selon le pare-feu et la configuration effectuée, l'utilisateur qui tente d'accéder à un site bloqué ou dangereux peut recevoir un message d'alerte ou d'avertissement.

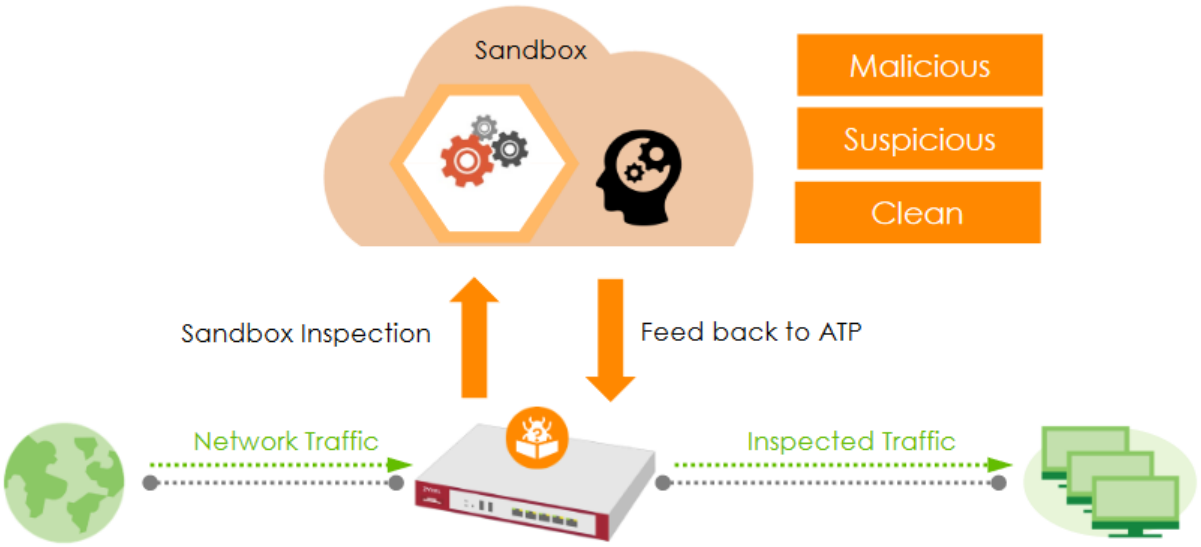
Bac à sable (Sandbox)

Malheureusement, les anti-virus et les IDP basés sur les signatures n'ont bien évidemment aucune chance de détecter les menaces inconnues et qui ne se trouvent pas dans leurs bases de données.

La meilleure façon d'identifier les menaces inconnues est de permettre aux fichiers dans lesquels elles résident de s'exécuter dans un environnement sûr. Un bac à sable (Sandbox) est un environnement isolé qui reproduit l'environnement d'exploitation d'un utilisateur final où le fichier suspect peut être exécuté, surveillé et classé en fonction de son comportement.



Le bac à sable (Sandbox) est souvent un service basé sur le Cloud qui peut détecter les nouveaux logiciels malveillants inconnus trouvés dans les fichiers téléchargés ou les pièces jointes qui se trouvent dans les e-mails. Les logiciels peuvent être triés et catégorisés (malveillant, susceptible, propre, …).

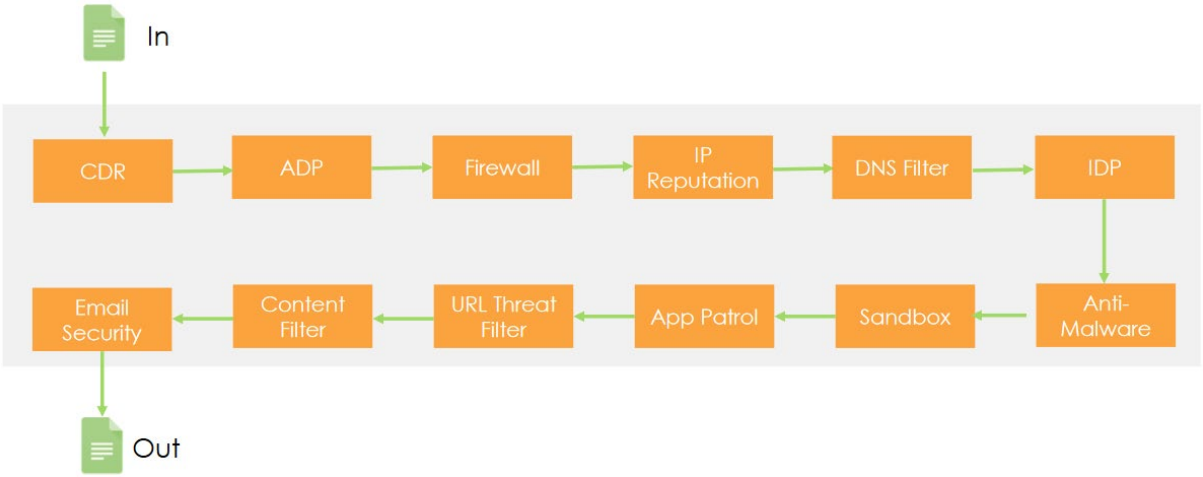


En fonction du pare-feu, plusieurs types de systèmes d'exploitation et de protocoles peuvent être supportés :
Systèmes d'exploitation : Windows, Linux, MacOS
Protocoles : HTTP, HTTPS, FTP, FTPS, POP3, POP3S, SMTP, SMTPS, autres protocoles

Le bac à sable (Sandbox) est généralement couplé à d'autres services comme le filtrage d'extensions de fichiers, l'anti-malware.

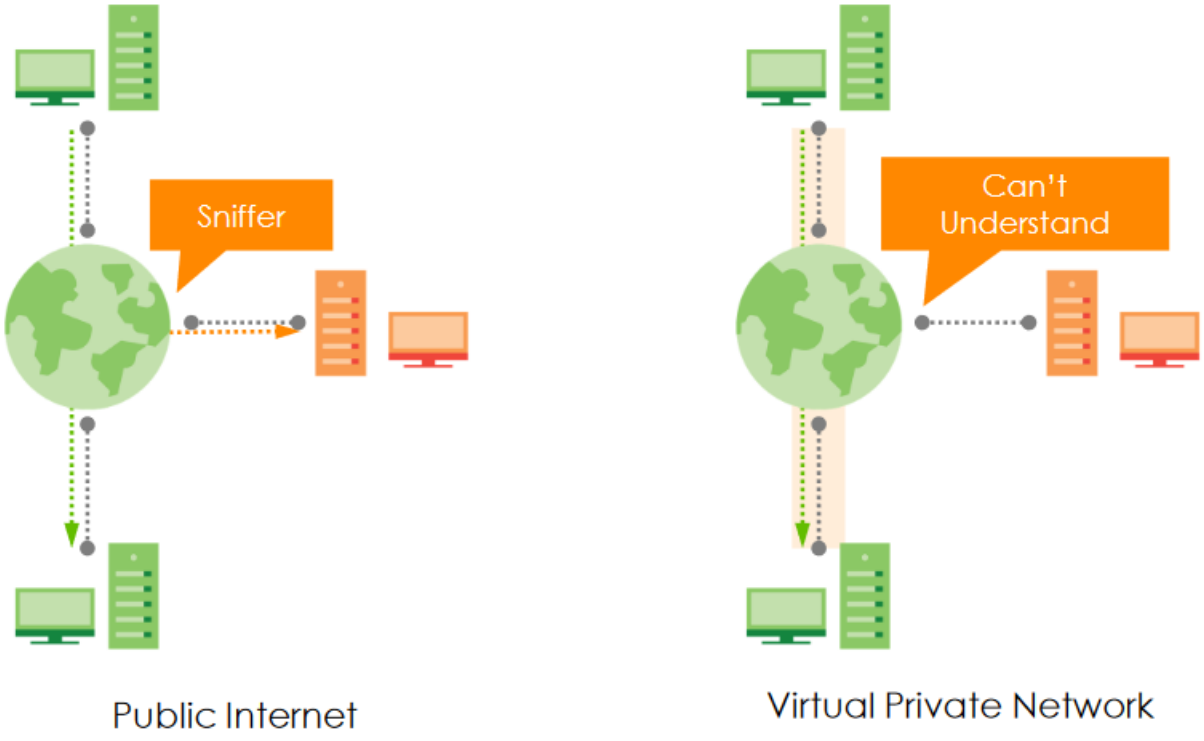
Un flux des paquets est configuré par le constructeur du pare-feu afin de faire transiter ceux-ci par les différents services UTM installés et configurés.

Exemple d'un flux dans un pare-feu :



Réseau privé virtuel (VPN)

Un réseau privé virtuel ou Virtual Private Network (VPN) est une connexion sécurisée et chiffrée entre deux réseaux ou entre un utilisateur individuel et un réseau. Les VPN permettent à un utilisateur de se cacher lorsqu'il surfe sur le Web. Son rôle premier est de protéger la confidentialité en ligne et surtout sur le Web. Il repose sur la création d'un tunnel (via un protocole d'encapsulation) entre deux réseaux qui pourront alors se ''voir'' au travers d'un réseau publique.



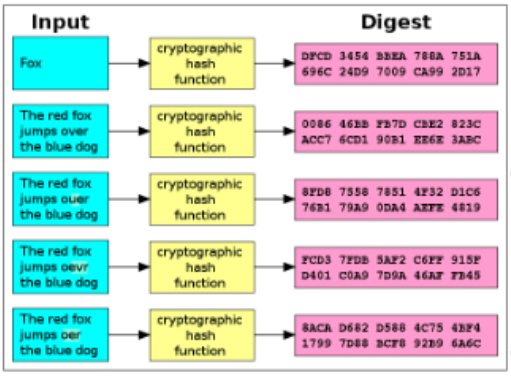
Les entreprises utilisent ce moyen pour :

- Etablir des connexions étendues sur plusieurs sites géographiques sans utiliser de ligne louée
- Renforcer la sécurité pour l'échange de données
- Donner la possibilité pour les bureaux et les employés distants d'utiliser l'intranet de l'entreprise via une connexion Internet existante comme s'ils étaient directement connectés à ce réseau

Le problème d'un réseau public est qu'il n'y a aucune confidentialité par rapport aux données qui y transitent. Un réseau privé est sous contrôle et permet de rendre confidentiel les données qui y transitent.

Il est donc question de fiabilité (authentification) et de sécurité (chiffrement).

L'authentification est le processus d'assurer l'identité d'une personne ou d'une chose. Ce processus se réalise au moyen d'une fonction de hachage qu'il est pratiquement impossible à inverser. La fonction de hachage est conçue pour prendre une chaîne de caractère du message original en entrée et de produire une valeur de hachage de longueur fixe.



A cryptographic hash function (specifically, SHA-1) at work. Note that even small changes in the source input (here in the word "over") drastically change the resulting output, by the so-called avalanche effect.

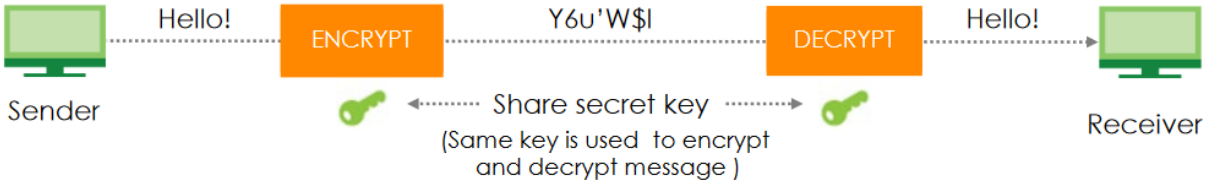
Voici un tableau avec les algorithmes de hachage habituels :

Name	Publish	Max Input Size	Digest	Description & Note
MD5	1991	$(2^{64}-1)$ bits	128 bits	• Designed by Ron Rivest
SHA-0	1993	$(2^{64}-1)$ bits	160 bits	• Withdrawn shortly after publication
SHA-1	1995	$(2^{64}-1)$ bits	160 bits	• The standard was no longer approved for most cryptographic uses after 2010. • Designed by the NSA.
SHA-2	2001	$(2^{64}-1)$ bits	256 bits(SHA-256)	• Designed by the NSA.
		$(2^{128}-1)$ bits	512 bits(SHA-512)	
SHA-3	2012	__	224 bits (SHA3-224) 256 bits (SHA3-256) 384 bits (SHA3-384) 512 bits (SHA3-512)	• Its internal structure differs significantly from the rest of the SHA family.

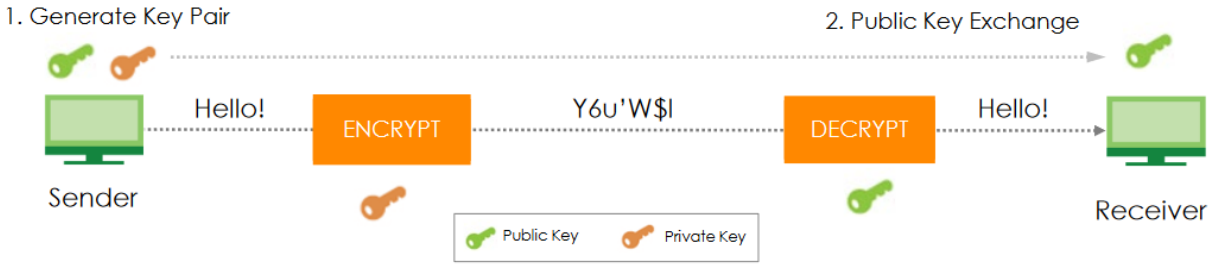
Le chiffrement est le processus d'encodage de messages ou d'informations que seules les parties autorisées peuvent lire.

Le chiffrement est réalisé en utilisant des clés symétriques ou asymétriques.

Chiffrement à clé symétrique : les clés de chiffrement et de déchiffrement sont les mêmes. Ainsi les parties qui communiquent doivent avoir la même clé avant de pouvoir établir une communication secrète (DES, 3DES, AES).



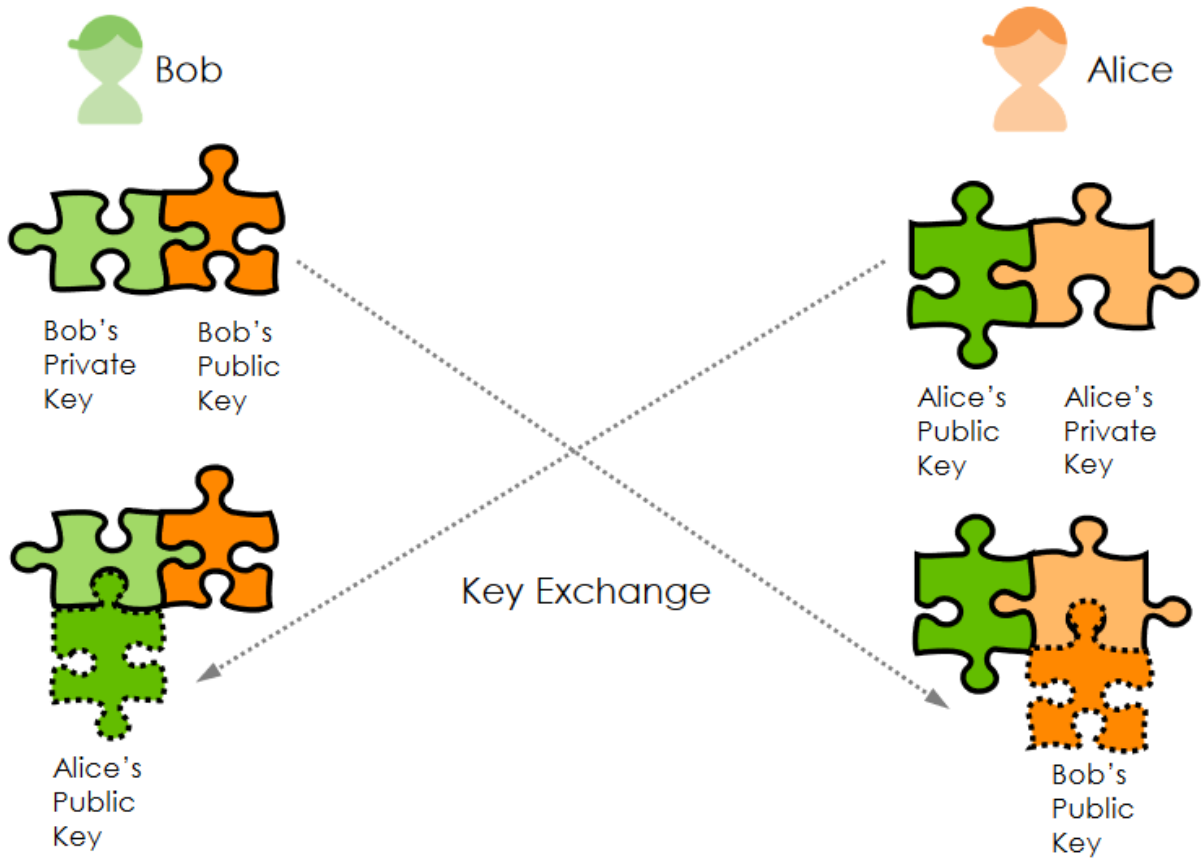
Chiffrement à clé asymétrique : la clé de chiffrement est publiée à la portée de tous pour crypter les messages. Cependant, seul le destinataire a accès à la clé de déchiffrement qui permet de lire les messages (RSA, DSA).

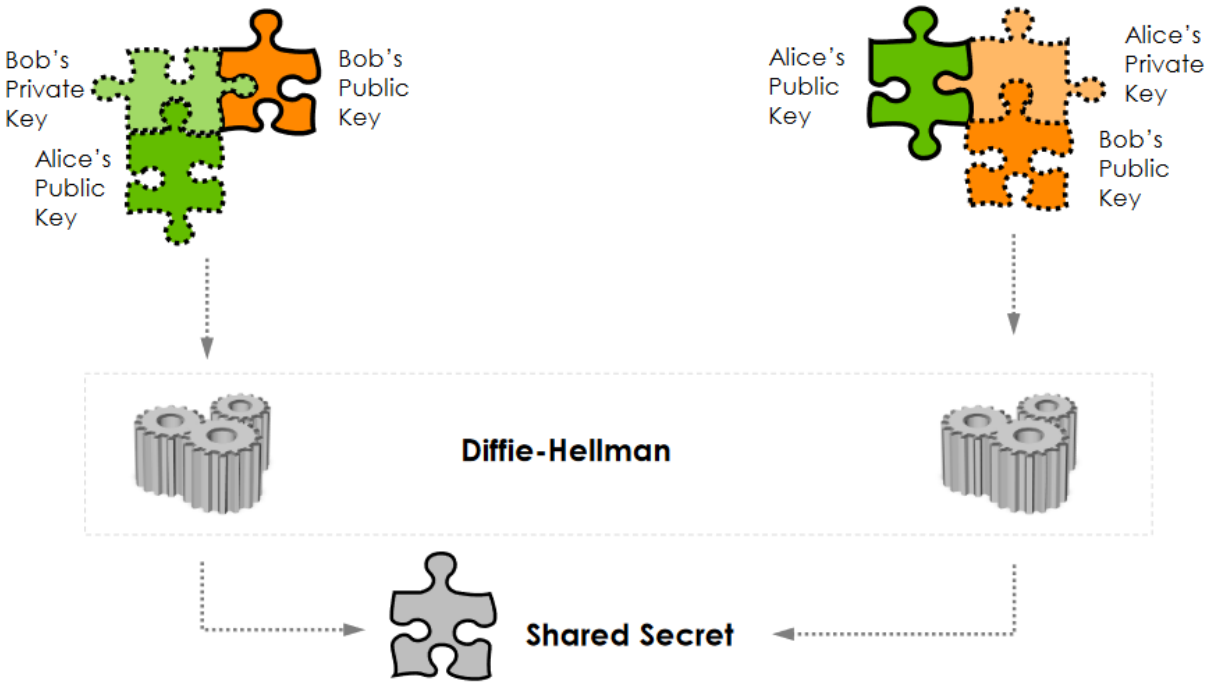


Voici un tableau avec les algorithmes de chiffrement habituels :

Name	Published	Key Size	Description & Note
DES	1977	56 bits	• Developed by IBM • DES is now considered to be insecure due to the 56-bit key size being too small
3DES	1998	168 bits	• Applies the DES cipher algorithm three Senderes to each data block
AES	2001	128 bits (AES128) 192 bits (AES192) 256 bits (AES256)	• AES has been adopted by the U.S. government and is now used worldwide

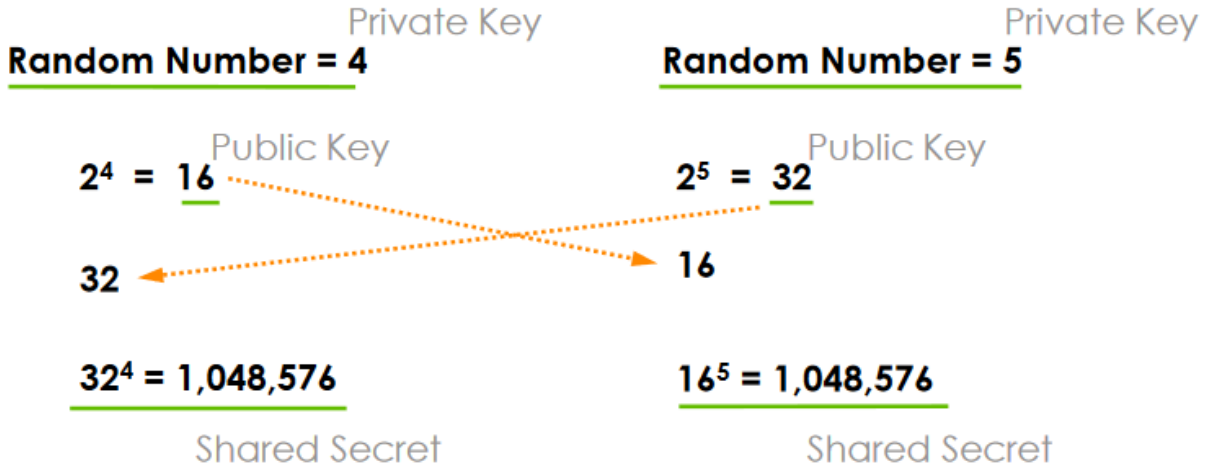
Le procédé d'échange de clés Diffie-Hellman est certainement disponible sur ton pare-feu. Il fonctionne de la façon suivante :





Dans la pratique, voici le procédé qui est appliqué :

Un numéro commun est défini, par exemple le chiffre 2.
Le secret partagé est alors calculé de la sorte :
Secret partagé = (Numéro commun $^{\text{Clé privée 1}}$) $^{\text{Clé privée 2}}$



Les types de VPN actuels peuvent être soit d'accès à distance (connexion d'un ordinateur à un réseau), soit de site à site (connexion de deux réseaux).
Les VPN les plus couramment utilisés sont :

- VPN IPSec (accès site à site et client à site)
- VPN L2TP/IPSec (client à site)
- VPN SSL (client à site)
- OpenVPN (client à site)
- Wireguard (client à site)

Schémas de types de VPN :

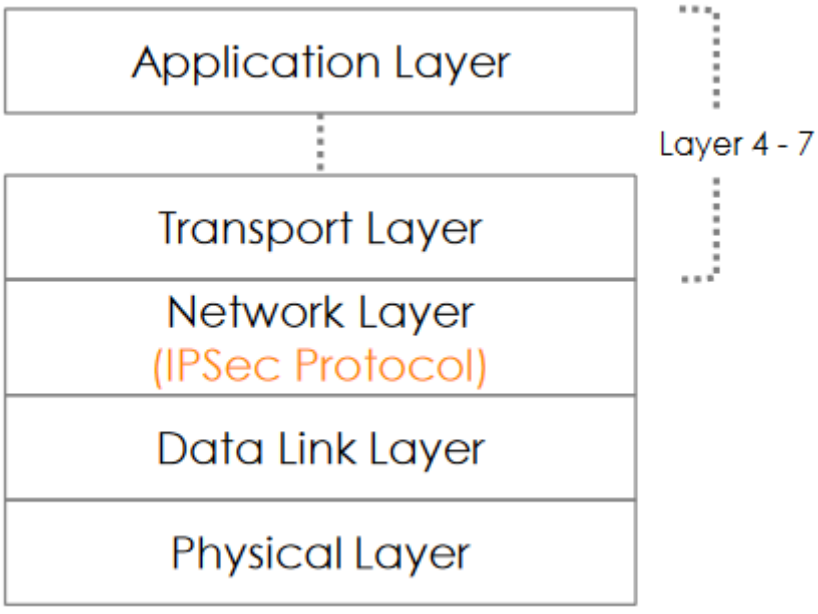
- **Remote Access VPN**

- **Site to Site VPN**

VPN IPSec

Le VPN IPSec est certainement le plus répandu des types de VPN de nos jours. Il permet de relier plusieurs succursales entre elles ou de relier un client vers le site principal de l'entreprise.

Le protocole IPSec (Internet Protocol Security) est un VPN basé sur des normes qui offre des solutions flexibles pour la communication sécurisée de données sur un réseau public, type Internet. Le protocole IPSec se trouvent dans la couche 3, soit la couche réseau.



Le fonctionnement du protocole IPSec peut être décomposé en 5 étapes principales :

- Etape 1 : Initiation du processus IPSec
- Etape 2 : Phase 1 avec le protocole IKE (Internet Key Exchange)
- Etape 3 : Phase 2 avec le protocole IKE
- Etape 4 : Transfert de données
- Etape 5 : Terminaison du tunnel IPSec

Etape 1 : Initiation du protocole IPSec

Qu'est-ce que le protocole IKE ?

- IKE est un protocole qui va initier un échange de clés par le biais d'Internet
- IKE est le protocole utilisé pour implémenter une Association de Sécurité (SA, Security Association) dans la suite du protocole IPSec

- Une SA est un groupe logique de paramètres de sécurité tels que :
    - Algorithme de cryptographie
    - Mode de fonctionnement
    - Clé de chiffrement du trafic
    - Paramètres de transmission de données réseau sur la connexion Internet
- Une SA est un canal à sens unique
- Le protocole IKE utilise le port UDP 500
- Le protocole IKE est constitué de deux phases : Phase 1 et Phase 2
- Le protocole IKE existe en deux versions : IKEv1 et IKEv2

Le protocole IPSec va donc utiliser le protocole IKE pour authentifier un homologue et pour générer une clé de chiffrement. Le protocole IKE va négocier et créer une association de sécurité (SA IKE). Il va également créer et gérer les SA enfants (SA IPSec).

IKEv2 a tendance à remplacer IKEv1 car ce dernier est souvent plus complexe et peut conduire à des problèmes d'interopérabilité. De plus, il engendre une certaine latence dans la construction du tunnel IPSec et possède une faible protection contre les attaques de type DoS.

IKEv2 (RFC 5996) a été créé pour surmonter les différentes limitations de IKEv1.
IKEv2 est donc beaucoup plus efficace, notamment dans les spécifications suivantes :

- Négociation plus rapide
- Création plus rapide de nouvelles clés
- Moins de problèmes liés aux protocoles Internet (IOP, Internet of Protocols)
- Meilleure mécanisme de détection de perte de leur pair distant (DPD, Dead Peer Detection, RFC 3706) au moyen de mécanisme de type Keepalive
- Possibilité d'utiliser NAT-T (NAT Traversal) dans le protocole. Le protocole IPSec peut donc passer au travers d'un réseau en réalisant de la translation d'adresses dynamique)
- Il est également supporter en natif dans les dernières versions de Windows (7/8/10/11).

IKEv2 est également beaucoup plus sécurisé, notamment dans les spécifications suivantes :

- Protection contre les attaques de type DoS (usurpation d'adresse IP)
- Prise en charge de l'authentification EAP (intégration plus flexible avec un serveur d'authentification de l'entreprise)

IKEv2 possède quelques limitations :

- Il n'est pas compatible avec IKEv1
- Il ne permet une authentification EAP avec MS-CHAPv2 uniquement
- Le client natif de Windows ne supporte pas la segmentation de tunnel
- Si le protocole AAA (Authentification, autorisation et traçabilité ou Authentication, Accounting et Auditing) utilise la fonction RADIUS, la méthode d'authentification ne peut inclure qu'une seule méthode
- Une règle existante en IKEv1 ne peut pas être modifiée en IKEv2. Il faut donc recréer la règle.

Etape 2 : Phase 1 avec le protocole IKE

La construction de la phase 1 s'établi selon le processus suivant :

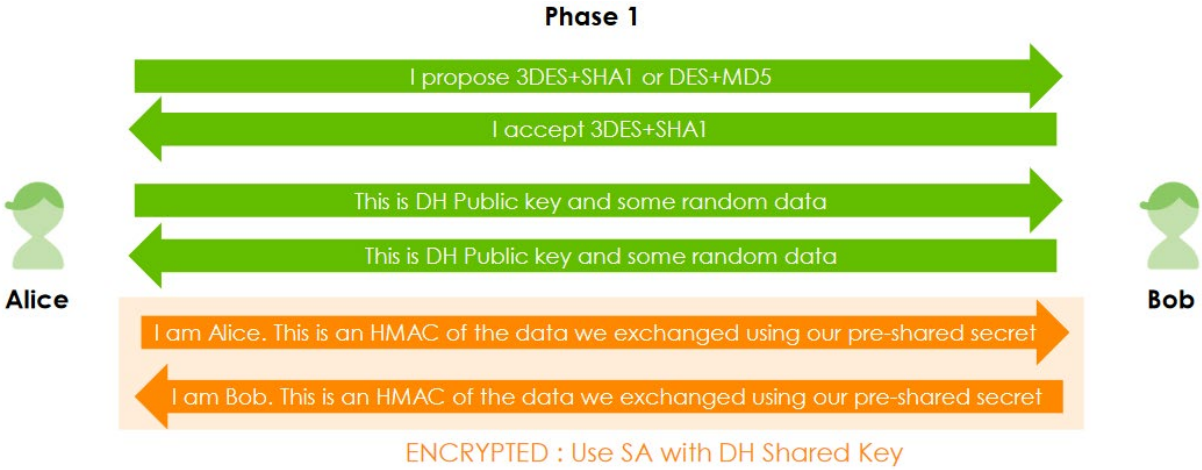
- Négociation d'une politique IKE SA correspondante entre pairs pour protéger l'échange IKE
- Echange authentifié de clé Diffie-Hellman afin d'obtenir une correspondance des clés secrètes partagées
- Authentification et protection de l'identité des pairs avec IPSec
- Construction du tunnel sécurisé pour négocier ensuite les paramètres de la phase 2 de IKE

Deux modes existent pour cette première phase :

- Mode principal
- Mode Agressif

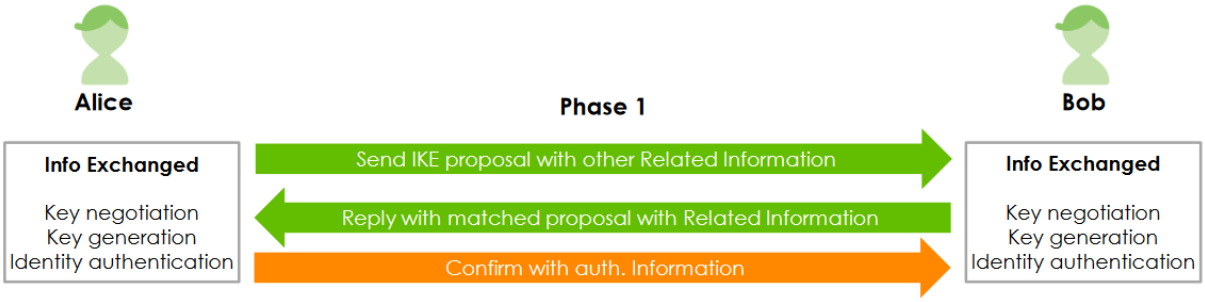
Le mode principal comporte 6 étapes d'échange entre l'initiateur et le récepteur :

- Echange de propositions (algorithme d'authentification, algorithme de chiffrement, groupe de clés Diffie-Hellmann)
- Echange de clés Diffie-Hellmann
- Echange d'identité (crypté avec la clé Diffie-Hellmann)



Le mode agressif comporte 3 étapes d'échange entre l'initiateur et le récepteur. Il y aura donc moins d'échanges et moins de paquets.

- Envoi d'une proposition IKE locale, d'informations relatives à la clé et d'informations d'identité
- Recherche d'une proposition IKE correspondante. Envoi de la proposition IKE correspondante avec les informations relatives à la clé, les informations d'identification et les informations d'authentification locale
- Réponse avec les informations d'authentification locale pour implémenter l'authentification.



Les échanges de règles IPSec doivent généralement correspondre entre les pairs. Les points suivants peuvent être identiques ou non :

- Mode de négociation (identique)
- Passerelle (identique ou non, statique ou dynamique)
- Proposition (Authentification chiffrement, Diffie-Hellmann) (au moins une correspondance)
- NAT-T (identique)
- XAUTH (identique)
- Echange de clés (identique)
- Mode d'authentification (identique, PSK, certificat, …)
- Les identifiants des pairs (Local ID, Peer ID : Type et Content) (identique ou non)

Etape 3 : Phase 2 avec le protocole IKE

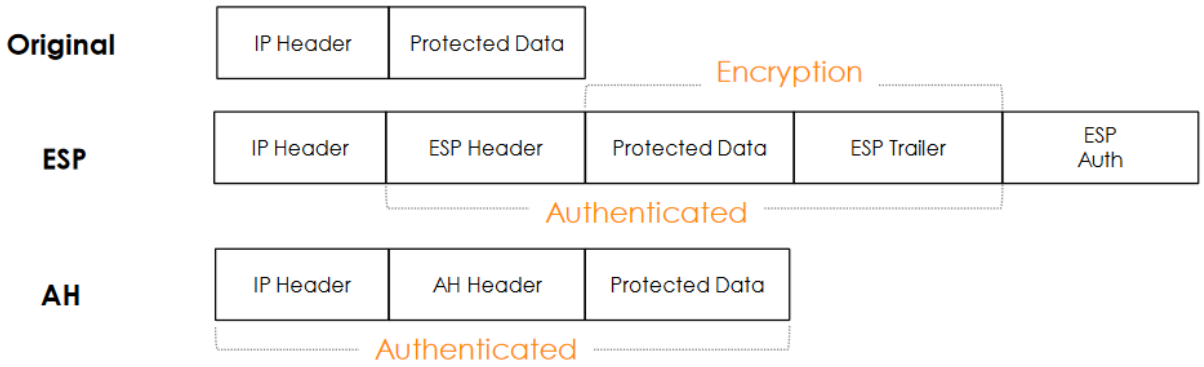
La construction de la phase 2 s'établi selon le processus suivant :

- Négociation des paramètres SA IPSec par un SA IKE existant, comme, par exemple :
  - AH ou ESP
  - Mode d'encapsulation (Tunnel ou Transport)
- Renégociation des SA IPSec pour assurer la sécurité
- Etablissement des SA IPSec définitif
- Périodicité du renouvellement des SA

Authentification et chiffrement (cryptage)

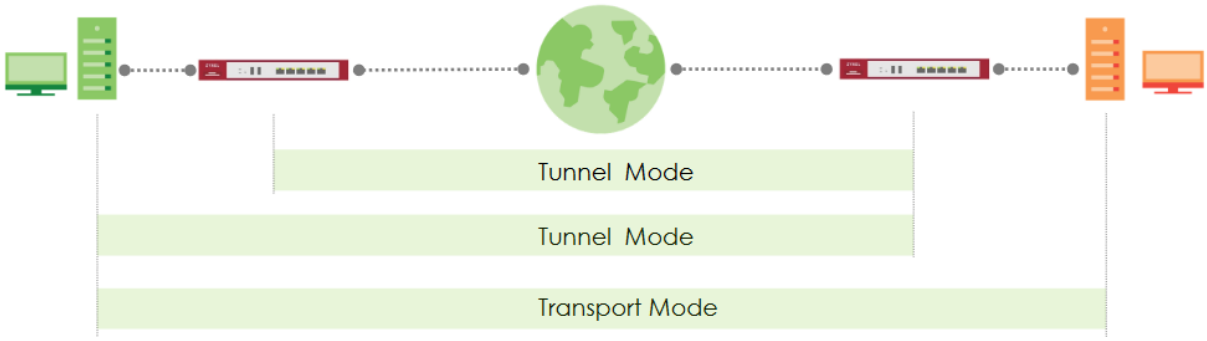
Ce processus utilise soit le protocole ESP soit le protocole AH

- ESP ou Encapsulation de la Charge Utile assure l'authentification et le chiffrement
- AH ou Entête d'Authentification assure uniquement l'authentification



Mode d'encapsulation :

Il existe le mode tunnel ou le mode transport.



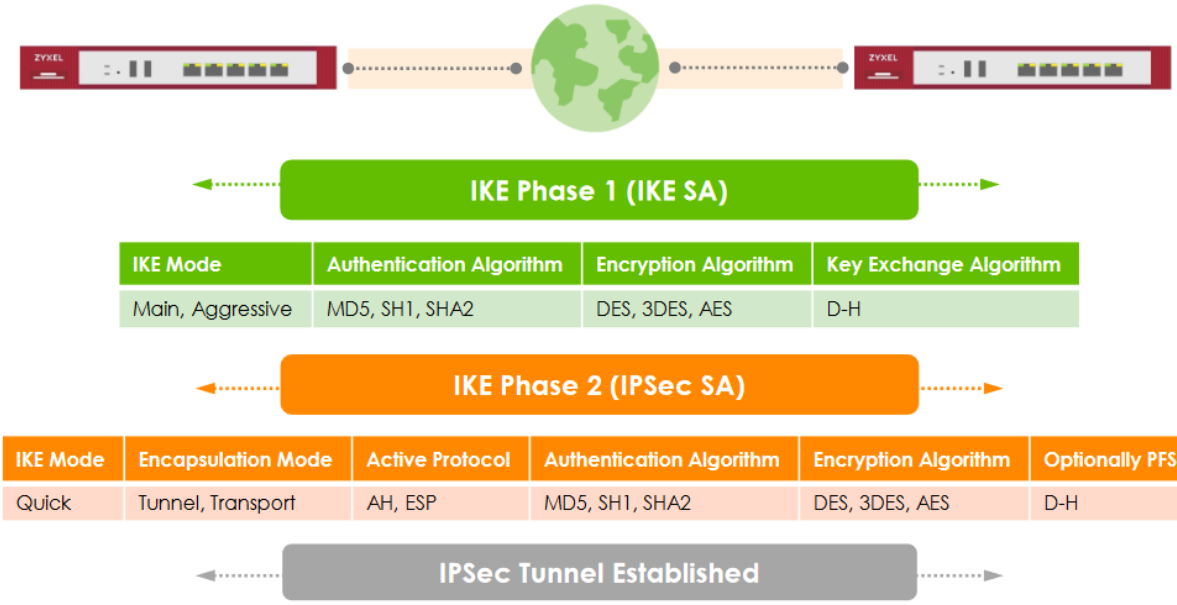
Etape 4 : Transfert de données

Les données peuvent ensuite être échangée de bout en bout au travers du tunnel VPN construit entre les pairs.

Etape 5 : Terminaison du tunnel IPSec

La terminaison du tunnel IPSec intervient :

- Lorsque les SA IPSec prennent fin par suppression ou par temporisation
- Lors les SA IPSec sont terminées, les clés sont également supprimées
- Lorsque des SA IPSec ultérieurs sont requis pour un flux, IKE effectue un nouveau processus de négociation
- Une nouvelle négociation réussie aboutit à de nouvelles SA IPSec et à de nouvelles clés.



3 scénarios d'application sont possibles :

- Site à site avec adresses IP statiques
- Site à site avec homologue avec adresse IP dynamique
- Accès à distance (client vers le site, Client to Site). Dans ce scénario, les clients ont généralement des adresses IP dynamiques. Ils sont aussi appelés utilisateurs ''dial-in'' ce qui veut dire que seuls les clients peuvent initier l'ouverture du tunnel VPN.

Pour réaliser des connexions client vers site (Client to Site), il est possible d'utiliser le logiciel gratuit Shrew VPN. Les solutions fournies par les fabricants sont souvent malheureusement payantes.

VPN L2TP/IPSec

L2TP signifie Layer 2 Tunneling Protocol, et il ne fournit aucun cryptage par lui-même. Le VPN L2TP utilise généralement un protocole d'authentification, IPSec (Internet Protocol Security), pour un cryptage et une authentification forte, ce qui lui donne un avantage ultime sur certains autres protocoles les plus utilisés comme PPTP. Le protocole L2TP utilise les ports UDP 1701.

Les données transmises via le protocole L2TP/IPSec sont généralement authentifiées deux fois. Chaque paquet de données transmis via le tunnel comprend des en-têtes L2TP. En conséquence, les données sont démultiplexées par le serveur. La double authentification des données ralentit les performances, mais elle offre la plus haute sécurité.

L'une des nombreuses raisons qui font de L2TP un protocole populaire est qu'il n'existe aucune vulnérabilité connue. De plus, le double cryptage offre aux utilisateurs une tranquillité d'esprit lorsqu'ils utilisent Internet. De plus, Mac et Windows OS prennent tous deux en charge le protocole.

Avantages :

- Contrairement au PPTP, il offre un excellent niveau de cryptage et de sécurité
- Le protocole encapsule les données deux fois, ce qui signifie une double vérification des données
- Le protocole est disponible non seulement sur les ordinateurs de bureau mais aussi sur les systèmes d'exploitation mobiles. Il n'y a donc pas besoin d'installer un logiciel supplémentaire.
- L2TP est assez facile à configurer sur tous les systèmes d'exploitation qu'il prend en charge
- Prise en charge du multithread pour des performances améliorées

Désavantages :

- Il offre des performances lentes en raison de la double authentification (encapsulation)
- Certains pares-feux peuvent bloquer les ports du protocole L2TP
- Le protocole est difficile à configurer sur les appareils qui s'exécutent sur des routeurs NAT
- La rumeur dit que L2TP/IPSec est délibérément affaibli par la National Security Agency (NSA)

Voici un scénario exemple avec une adresse IP publique :

Voici un scénario exemple avec un routeur et un NAT :

La plupart des pares-feux possèdent un wizard d'installation qui permet de configurer rapidement le L2TP-VPN.

Il suffit ensuite de paramétrer le VPN sur son équipement, par exemple, son PC Windows :

Selon les pare-feux, il sera nécessaire de suivre une documentation spécifique pour la configuration du client, afin de respecter les paramètres spécifiques de cette connexion.

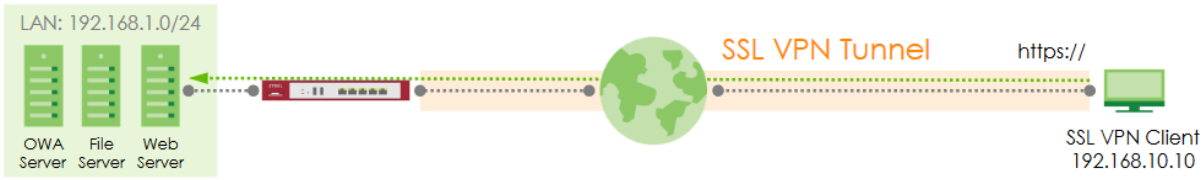
SSL VPN

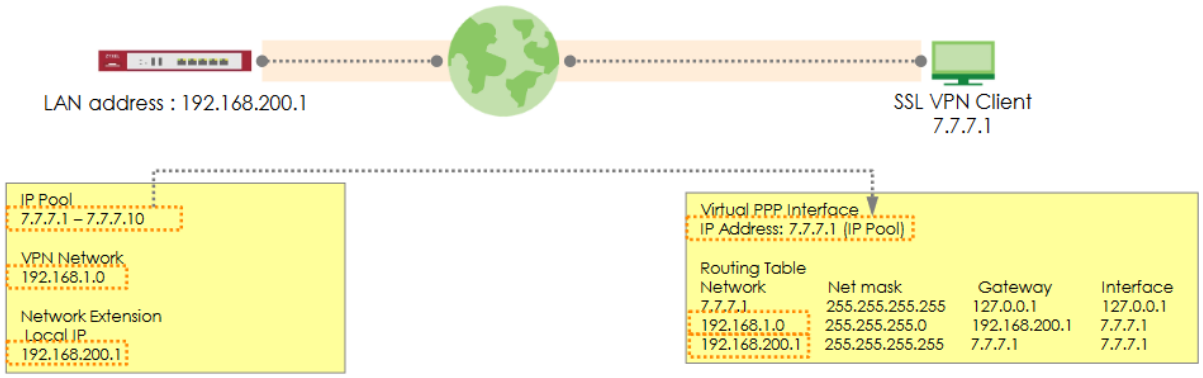
SSL signifie Secure Socket Layer (Couche de sockets sécurisés). Ce protocole utilise, entre autres, RC4, RSA et d'autres méthodes de chiffrement. Il est largement utilisé pour la navigation web sécurisée via le protocole HTTPS (port 443). SSL gère l'authentification et le chiffrement et assure la sécurité de la couche application (couche 7 du modèle OSI). Un de ses avantages est qu'il peut facilement contourner les NATs.

La configuration sur les postes clients est souvent relativement simple. Elle peut, cependant, nécessiter l'installation d'un logiciel client, souvent gratuit et fournit par le constructeur du pare-feu. Le SSL-VPN est également idéal pour l'accès mobile. Il permet de sécuriser la communication entre le client et le serveur au moyen du protocole SSL qui gérera l'authentification et le cryptage des données.

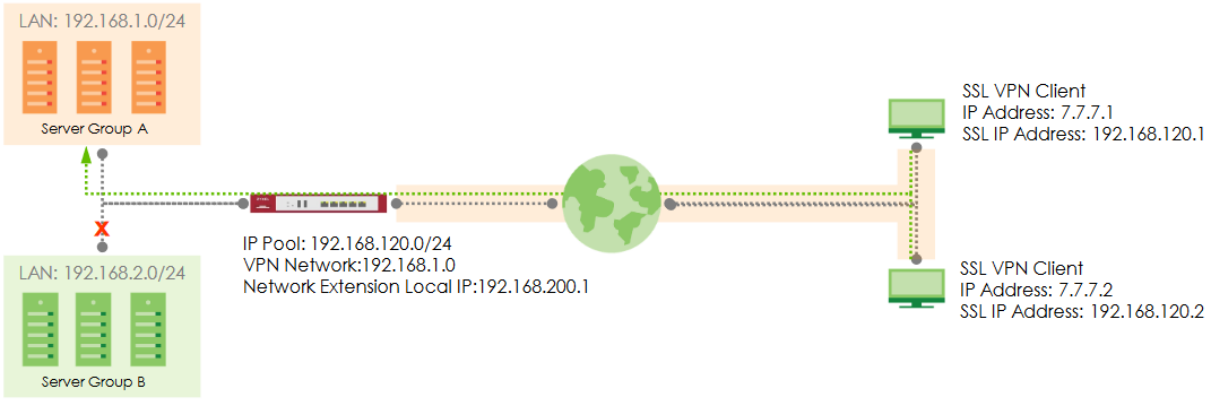
Comme conditions préalables, il faudra configurer au niveau du pare-feu une plage d'adresses IP spécifiques qui seront fournies aux client SSL-VPN. Ces adresses IP leur permettront d'accéder au réseau local du pare-feu. Il faudra également définir quels seront les objets auxquels les clients VPN-SSL auront accès (réseau entier, groupe de serveurs, …).

En général, le client VPN-SSL va utiliser le mode Tunnel complet (Full Tunnel) :





Exemple d'accès spécifique à un groupe de serveurs :



Le client aura généralement besoin de l'adresse IP publique du pare-feu ainsi que d'un nom d'utilisateur et d'un mot de passe pour se connecter en SSL-VPN.

L'exercice 3 te donnera les indications nécessaires pour la configuration des services UTM ainsi que pour l'installation des différentes solutions de VPN.

Autres solutions VPN

D'autres solutions VPN sont en train d'émerger sur le marché et remplace petit à petit les solutions traditionnelles.

Pour n'en citer que 2, voici une brève présentation de OpenVPN et Wireguard. En fonction du fabricant et du modèle de pare-feu, ces deux solutions peuvent éventuellement être mise en service si le pare-feu intègre un paquet spécifique nativement ou installable en complément.

WireGuard est un protocole VPN de nouvelle génération sous licence GPLv2 (ou MIT, BSD, Apache 2.0 ou GPL suivant le contexte) créé par Jason A. Donenfeld. Le site officiel étant accessible via ce lien.

WireGuard se veut être plus simple, rapide et sécurisé que les protocoles VPN communs que sont OpenVPN et IPsec.

- La simplicité de configuration se passant en une seule phase standardisée contrairement à IPsec où deux phases, souvent difficiles à appréhender pour des novices, sont nécessaires. De plus la non-utilisation de certificats, comme on la retrouve avec OpenVPN, simplifie la gestion à plus long terme et ne nécessite pas la création d'une PKI.
- La sécurité est assurée avec l'utilisation de primitives cryptographiques modernes mais aussi par la mise à disposition d'une seule combinaison de méthodes de chiffrements. De plus le

code complet de WireGuard tient sur environ 4 000 lignes ce qui facilite les audits de sécurité et réduit sa surface d'attaque.

- La rapidité tient en grande partie des points précédents mais aussi parce que WireGuard fonctionne au niveau du noyau (seulement sous Linux) et non au niveau de l'espace utilisateur. Les tests présents sur le site officiel démontrent un très fort avantage de WireGuard sur OpenVPN et un avantage un peu plus ténu sur IPsec, à la fois en débit maximal atteint et en temps de latence. A savoir que d'autres tests sont disponibles sur Internet et tendent à placer WireGuard comme le plus performant même si l'écart n'est pas toujours aussi important, notamment avec IPsec.

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Son développement a commencé le 13 mai 2001 grâce à James Yonan.

OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe. Il utilise de manière intensive la bibliothèque d'authentification OpenSSL ainsi que le protocole SSLv3/TLSv1. Disponible avec une multitude d'environnements tel que Solaris, OpenBSD, FreeBSD, NetBSD, Linux (Debian, Redhat, Ubuntu, etc.), Mac OS X, Windows 2000, XP, Vista, 7, 8 et 10, il offre de nombreuses fonctions de sécurité et de contrôle.

OpenVPN n'est pas compatible avec IPsec ou d'autres logiciels VPN. Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie.

Exercice

L'exercice 3 te donnera les indications nécessaires pour la configuration des différents types de VPN. Tu pourras expérimenter ces configurations et profiter de travailler en binôme. Tu pourras également de familiariser avec les services UTM et les tester en mettant en place des règles spécifiques sur ton pare-feu.

Jour 4

Objectif du jour 4

- Authentification des utilisateurs
- Configuration d'un accès Wi-Fi

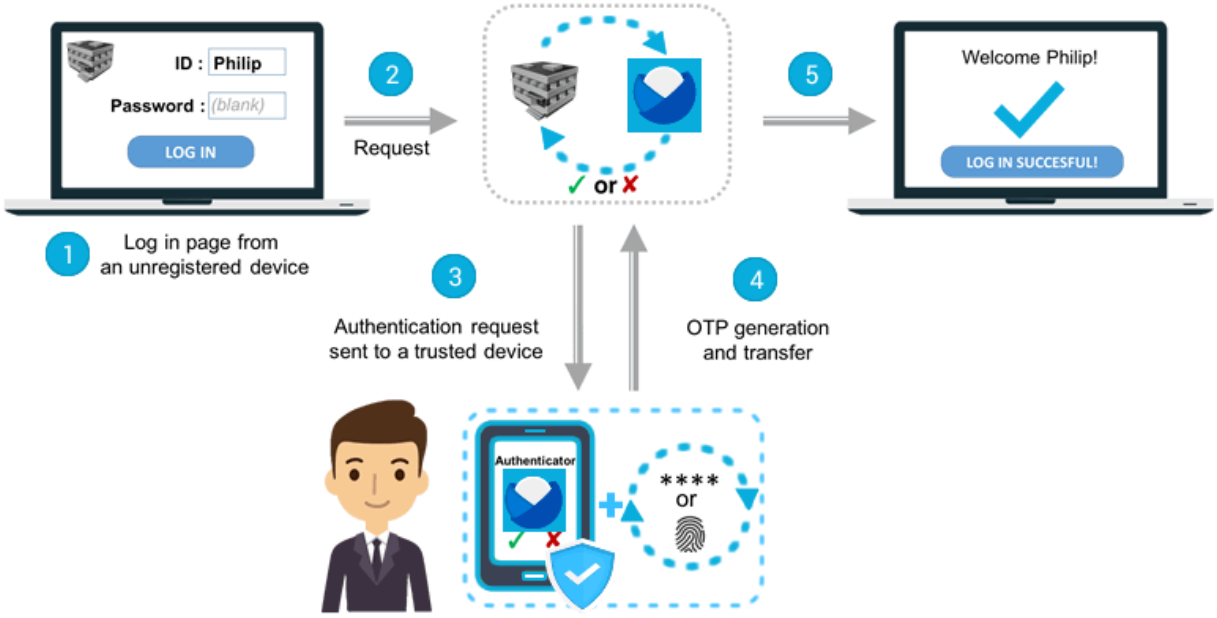
Ton pare-feu possède en général la fonctionnalité de configurer l'authentification des utilisateurs par le biais de serveurs de types LDAP, RADIUS, AD (Active Directory), voire encore par d'autres types de protocoles. De plus, la plupart des pare-feux propose une authentification à double-facteur de type MFA (Authentification multi-facteurs, ou multi-factor authentication).

Cette fonctionnalité d'authentification peut être implémentée pour différents services fournis par le pare-feu, notamment :

- Accès VPN Client-to-Site authentifié
- Accès à un réseau Wi-Fi particulier
- Accès au management du pare-feu
- Autorisation d'applications
- Autorisation de contenu

Prenons le temps de décrire certaines de ces fonctionnalités d'authentification.

Authentification multi-facteurs MFA



L'authentification multi-facteurs (MFA), ou authentification forte, est un processus de sécurité qui nécessite deux ou plusieurs facteurs de vérification pour prouver l'identité d'un utilisateur. Le plus souvent, cela implique de se connecter à un réseau, une application ou une autre ressource sans se contenter d'une simple combinaison nom d'utilisateur (ID) + mot de passe.

L'utilisation de l'authentification multi-facteurs présente de nombreux avantages compte tenu des problématiques actuelles liées à l'évolution des modes de travail, mais aussi au paysage de la cybersécurité et aux réglementations.

Diverses méthodes sont disponibles, notamment grâce aux SMS, aux e-mails, aux applications spécifiques (Google Auth, Authy, …), voire même avec les réseaux sociaux (Facebook, …).

Le MFA pour prévenir les cyberattaques

L'authentification multi-facteurs (MFA), ou authentification forte, est principalement réputée pour constituer une défense supplémentaire et rendre plus difficile l'accès d'une personne non autorisée à un réseau ou à une base de données. La mise en place d'une solution MFA robuste permet de sécuriser instantanément les données et les ressources informatiques contre le vol d'identité, l'usurpation de compte et le phishing.

Les entreprises recourent donc au MFA pour contrôler l'accès à leurs systèmes et solutions informatiques internes, mais aussi pour leurs applications B2C.

Le MFA pour s'adapter à l'évolution des modes de travail

Dans un contexte de transformation digitale, l'authentification forte multi-facteurs MFA est un excellent moyen de promouvoir la mobilité et la productivité des employés. En utilisant une solution MFA pour sécuriser l'accès aux applications de l'entreprise ou la connexion à distance au réseau via un VPN, sans dépendre d'un matériel spécifique ("device"), les organisations bénéficient d'une grande flexibilité.

Le MFA pour se conformer aux contraintes réglementaires

La réglementation en matière de sécurité des données est de plus en plus stricte, entraînant d'importants enjeux de conformité dans la gestion et la protection des données. Dans certains secteurs, le MFA est indispensable pour se conformer aux exigences réglementaires.

Le MFA pour simplifier l'expérience de connexion des utilisateurs

Dans le monde numérique, il est communément admis que renforcer la sécurité d'un système passe forcément par une dégradation de l'expérience utilisateur. Pourtant, en choisissant la bonne solution d'authentification multi-facteurs (MFA), vous pouvez simplifier l'expérience de connexion en permettant à vos utilisateurs de se connecter très rapidement et facilement, depuis n'importe quel appareil, et n'importe où.

Comment fonctionne le MFA ?

Au lieu de demander le traditionnel "nom d'utilisateur + mot de passe", l'authentification forte MFA demande à l'utilisateur de fournir des informations de vérification supplémentaires, appelées ''facteurs d'authentification'', pour s'assurer qu'il est bien la personne qu'il affirme être.

Le processus d'authentification nécessite ici la combinaison d'au moins deux facteurs provenant de deux catégories différentes parmi les suivantes :

- Quelque chose que je connais (facteur de connaissance), comme un mot de passe, une phrase de passe ou un code PIN
- Quelque chose que j'ai (facteur de possession), comme un appareil (smartphone, ordinateur, etc.), un token physique, une carte à puce
- Quelque chose qu'ils sont (facteur d'inhérence), soit une empreinte digitale, une reconnaissance vocale ou faciale, et tout autre type de biométrie

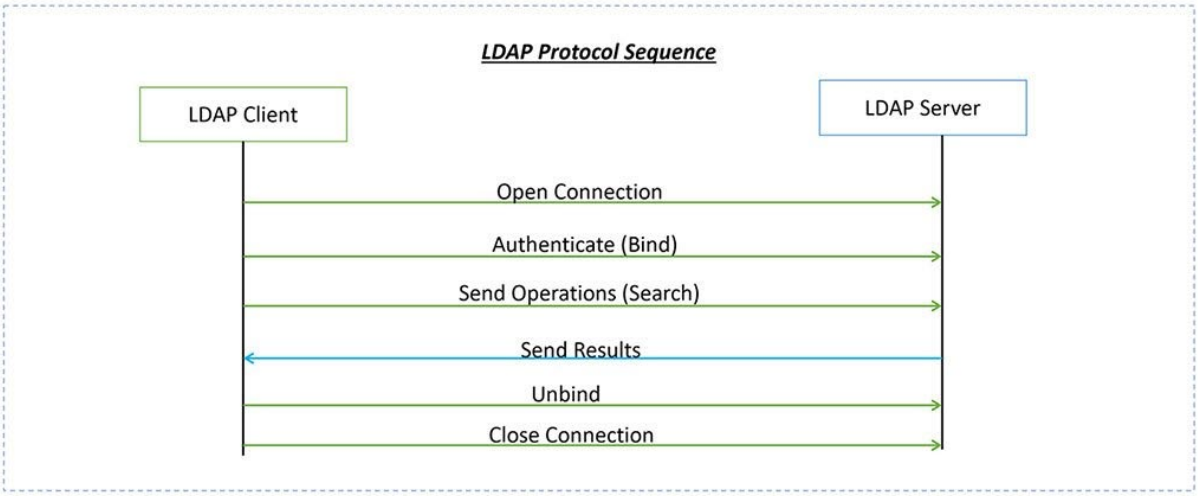
Tandis que le MFA intègre le machine learning et l'intelligence artificielle (IA), certains comptent de nouveaux facteurs d'authentification, notamment les facteurs d'authentification basés sur la localisation et le comportement. Toutefois, ces méthodes de vérification font partie de ce que nous appelons l'authentification ''MFA adaptative''.

Dans quelle mesure l'authentification multi-facteurs MFA est-elle efficace ?

Selon Microsoft, le MFA bloque plus de 99,9 % des attaques de compromission de compte. Vous entendrez souvent dire que le MFA est une composante essentielle de la sécurité de Zero Trust. En

effet, alors qu'il est relativement facile d'obtenir les informations d'identification d'un utilisateur par des attaques telles que le phishing ou credential stuffing, l'authentification forte multi-facteurs rend quasiment impossible pour les hackers d'obtenir le second facteur d'authentification.

Authentification LDAP



Qu'est-ce que l'authentification LDAP ?

Le LDAP a été introduit pour la première fois en 1993 par Tim Howes de l'Université du Michigan, Steve Kille d'Isode Limited et Wengyik Yeong de Performance Systems International. Selon M. Howes, ses co-inventeurs et lui-même ont travaillé sur le LDAP afin de remplacer le protocole d'accès aux annuaires (Directory Access Protocol, DAP), un type d'accès aux annuaires plus complexe et plus exigeant. En utilisant moins de code dans LDAP - d'où le "léger" - l'équipe espérait rendre le protocole plus accessible à ceux qui utilisent des systèmes informatiques de bureau communs.

Depuis lors, LDAP est devenu un programme extrêmement populaire. Par exemple, en 1997, LDAP.v3 a été adopté comme norme pour les services d'annuaire. Il a également servi de base à Microsoft pour la création d'Active Directory, et a joué un rôle essentiel dans le développement des annuaires actuels basés sur le cloud - également connus sous le nom de Directories-as-a-Service.

En termes simples, LDAP est le protocole ou le langage que les serveurs utilisent pour communiquer avec Active Directory et des services d'annuaire similaires. Version du protocole d'accès aux annuaires (DAP), LDAP fait partie de la norme X.500 pour les services d'annuaires dans les intranets organisationnels et sur l'internet. LDAP permet d'envoyer des messages entre les serveurs et les applications clientes - des messages qui peuvent inclure tout, des demandes des clients et des réponses des serveurs au formatage des données.

Sur le plan fonctionnel, LDAP fonctionne en liant un utilisateur LDAP à un serveur LDAP. Le client envoie une demande d'opération qui demande un ensemble particulier d'informations, telles que les identifiants de connexion de l'utilisateur ou d'autres données organisationnelles. Le serveur LDAP traite ensuite la requête en fonction de son langage interne, communique avec les services d'annuaire si nécessaire et fournit une réponse. Lorsque le client reçoit la réponse, il se détache du serveur et traite les données en conséquence.

Pourquoi avons-nous besoin de LDAP ?

Le LDAP a un sous-ensemble de cas d'utilisation divers, mais son objectif le plus populaire est d'agir comme un centre d'authentification central. Qu'est-ce que l'authentification LDAP ? Eh bien, LDAP est particulièrement utile pour aider les organisations à stocker et à accéder aux noms d'utilisateur et aux mots de passe au sein de leur réseau et entre les applications. Avec les extensions appropriées,

les organisations peuvent utiliser LDAP comme moyen de stocker et de vérifier les informations d'identification de base lorsque les utilisateurs tentent d'accéder à un annuaire LDAP ou à des systèmes et applications compatibles LDAP. Pour ce faire, les professionnels de l'informatique peuvent utiliser les serveurs Docker, Jenkins, Kubernetes, Open VPN et Linux Samba. L'authentification unique LDAP est également un choix populaire.

Toutefois, les identifiants LDAP ne se limitent pas aux noms d'utilisateur et aux mots de passe. Le protocole logiciel peut également être utile pour gérer d'autres attributs organisationnels auxquels les employés de votre entreprise peuvent avoir accès. Par exemple, LDAP peut aider à stocker des adresses, des numéros de téléphone, des données sur la structure organisationnelle, etc., ce qui fait de LDAP un outil utile pour la gestion et la protection des identités d'utilisateur essentielles dans toute une organisation. En outre, LDAP peut mettre les utilisateurs en contact avec des informations sur les actifs et les données connectés au réseau, tels que les imprimantes, les fichiers et autres ressources partagées.

Au-delà de ces cas d'utilisation de base, LDAP est un outil essentiel dans toute entreprise en raison de ses interactions avec les services d'annuaire - le plus souvent Active Directory de Microsoft. Comme nous le verrons plus tard, LDAP est un moyen de communiquer avec Active Directory et de connecter les clients aux informations dont ils ont besoin et que les services d'annuaire stockent réellement. En fournissant un langage efficace et partagé que les différents clients peuvent tous utiliser, LDAP permet aux différentes ressources de fournir plus facilement des réponses coordonnées et cohérentes aux demandes des clients.

Est-ce que LDAP est la même chose qu'Active Directory ?

Bien qu'ils soient intimement liés, LDAP et Active Directory ne sont pas la même chose. LDAP est une sorte de langage logiciel utilisé pour l'authentification des services d'annuaire - il fournit simplement le langage et les moyens d'échanger des messages correctement formatés entre différents clients. C'est une étape essentielle du processus d'authentification, mais il ne fournit pas l'infrastructure sous-jacente que les services d'annuaire tels qu'Active Directory fournissent.

En revanche, Active Directory de Microsoft fournit aux organisations des services d'annuaire essentiels. Ces services vont de l'authentification des identifiants des utilisateurs et des identités de base à la gestion des groupes et des utilisateurs. Pour l'essentiel, Active Directory stocke et gère des domaines, des informations sur les utilisateurs et d'autres ressources partagées dans un réseau organisationnel. C'est un must pour les organisations qui doivent pouvoir localiser des milliers d'objets dans leur infrastructure numérique et réglementer soigneusement qui a accès à quelles ressources.

En bref, Active Directory stocke les informations sur les utilisateurs et enregistre la politique numérique de l'organisation au niveau de l'utilisateur et du groupe. LDAP permet de formater des requêtes qui peuvent extraire les informations nécessaires et de communiquer les réponses à ces requêtes entre les clients. Ensemble, LDAP et Active Directory permettent aux clients de toutes les entreprises d'accéder aux informations dont ils ont besoin et d'utiliser les applications dont ils ont besoin pour s'acquitter de leurs responsabilités.

Qu'est-ce que la sécurité LDAP ?

Parce que LDAP facilite la communication entre les clients et Active Directory, il traite une quantité considérable d'informations sensibles. Des informations d'identification des employés aux identités des utilisateurs principaux, en passant par l'emplacement des fichiers critiques et des ressources de l'entreprise, les données transférées d'Active Directory aux clients via LDAP sont importantes pour se protéger des cybercriminels et autres mauvais acteurs. Il s'agit d'une opportunité unique pour les mauvais acteurs d'intercepter les messages entre Active Directory et les clients qui demandent des informations propriétaires de valeur.

Bien que le processus d'authentification LDAP puisse fournir un niveau de sécurité de base en mettant en œuvre une couche intégrée de gestion des accès, les mauvais acteurs peuvent toujours essayer d'écouter les informations passant d'Active Directory aux clients afin d'apprendre comment accéder à votre infrastructure numérique. En conséquence, les PSM devraient travailler avec leurs clients pour ajouter un cryptage amélioré au processus d'authentification LDAP. Ce faisant, l'authentification LDAP peut être plus sûre contre les menaces internes et externes auxquelles sont confrontées les entreprises d'aujourd'hui.

Par exemple, l'utilisation du cryptage SSL/TLS peut ajouter une protection bien nécessaire aux informations partagées via LDAP et apporter une sécurité supplémentaire aux canaux de communication. En outre, le port par défaut utilisé au cours du processus d'authentification LDAP, le port 389, n'est pas sûr en soi. Afin de créer une connexion sécurisée, les organisations devraient envisager des extensions de sécurité supplémentaires. L'extension LDAPv3 TLS peut offrir une plus grande sécurité de connexion, ou le mode StartTLS peut aider les informations à passer à une connexion TLS plus protégée après la connexion au port.

Authentification Active Directory

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, MacOs et encore Linux. Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Si les administrateurs ont indiqué les attributs convenables, il sera possible d'interroger l'annuaire pour obtenir, par exemple, « toutes les imprimantes couleur à cet étage du bâtiment ».

Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012 (voire hors Microsoft par Samba), Windows Server 2016, Windows Server 2019 et Windows Server 2022 il résulte de l'évolution de la base de compte plane SAM. Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ».

Active Directory stocke ses informations et paramètres dans une base de données distribuée sur un ou plusieurs contrôleurs de domaine, la réplication étant prise en charge nativement1. La taille d'une base Active Directory peut varier de quelques centaines d'objets, pour de petites installations, à plusieurs millions d'objets, pour des configurations volumineuses.

Structure

Active Directory est un service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine.

Une structure Active Directory (AD) est une organisation hiérarchisée d'objets. Les objets sont classés en trois grandes catégories : les ressources (par exemple les imprimantes), les services (par exemple le courrier électronique) et les utilisateurs (comptes utilisateurs et groupes). L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité.

Chaque objet représente une entité unique — utilisateur, ordinateur, imprimante ou groupe — ainsi que ses attributs. Certains objets peuvent également être des conteneurs pour d'autres objets. Un objet est identifié de manière unique dans l'AD par son nom et possède son propre jeu d'attributs — les caractéristiques et les informations que l'objet peut contenir — défini par un schéma, qui détermine également le type d'objets qui peuvent être stockés dans l'AD.

Chaque objet attribut peut être utilisé dans plusieurs classes d'objets de schéma différents. Ces objets de schéma existent pour permettre au schéma d'être étendu ou modifié si nécessaire. Cependant, comme chaque objet de schéma est intégral à la définition des objets de l'AD, la désactivation ou la modification de ces objets peut avoir de graves conséquences car elle entraîne des modifications fondamentales dans la structure de l'AD. Un objet de schéma, lorsqu'il est modifié, est automatiquement propagé dans Active Directory et une fois créé, il ne peut plus être supprimé (il peut seulement être désactivé). Pour cette raison, une modification du schéma doit être mûrement réfléchie et planifiée2.

Le nombre de types d'objets disponibles dans un Active Directory n'est pas limité, en voici quelques exemples :

- OU (Organisational Unit) : L'unité d'organisation
  Dans l'arborescence, ce sont des conteneurs qui permettent de créer une hiérarchie d'objets au sein d'un domaine. Ces OU sont principalement utilisées pour permettre la délégation de droits et pour l'application de GPO. Les OU sont parfois confondues avec les groupes, qui sont des objets et non des conteneurs.
- Ordinateur
- Utilisateur
- Groupe : il est principalement destiné à établir des listes d'utilisateurs pour leur attribuer des droits ou des services. On distingue trois types de groupes :
  - Le groupe local : il peut contenir des utilisateurs de son domaine et ne peut être placé que sur des ressources de son domaine.
  - Le groupe global : au sein d'un domaine, il est principalement utilisé pour affecter des droits à des ressources dans un domaine. Il peut comprendre des utilisateurs, des groupes globaux ou universels de tous les domaines de l'annuaire.
  - Le groupe universel : disponible depuis la version 2000, permet d'inclure des groupes et utilisateurs d'autres domaines.

Active Directory étant un annuaire objet, la notion de schéma définit les contraintes concernant la dérivation et l'héritage des objets, sensiblement de la même manière qu'en programmation objet. Cela introduit également la notion d'extension, permettant d'ouvrir l'annuaire à toutes sortes d'applications souhaitant stocker des objets personnalisés au niveau du ou des domaines constituant la forêt Active Directory.

Authentification RADIUS

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston enterprise (rachetée par Lucent Technologies), qui fabriquait des serveurs d'accès au réseau pour du matériel uniquement équipé d'interfaces série ; il a fait ultérieurement l'objet d'une normalisation par l'IETF.

Normalisation

La dernière version du protocole RADIUS est normalisée par l'IETF dans deux RFC : RFC 28651 (RADIUS authentication) et RFC 28662 (RADIUS accounting) de juin 2000. Le successeur du protocole RADIUS pourrait être le protocole Diameter (jeu de mots sur le double du rayon). Le protocole est souvent dénommé AAA (Authentication Authorization Accounting), la phase d'autorisation (définition des droits d'accès) étant accomplie lors de la réponse d'identification (ajout d'attributs au

paquet "Authentication Response"). Un autre exemple de protocole AAA aurait pu être TACACS de Cisco, mais il est propriétaire ; et depuis la publication de la norme 802.1X qui donne en annexe D comme seul exemple de mise en œuvre le protocole Radius, ce dernier est devenu un standard de fait du AAA.

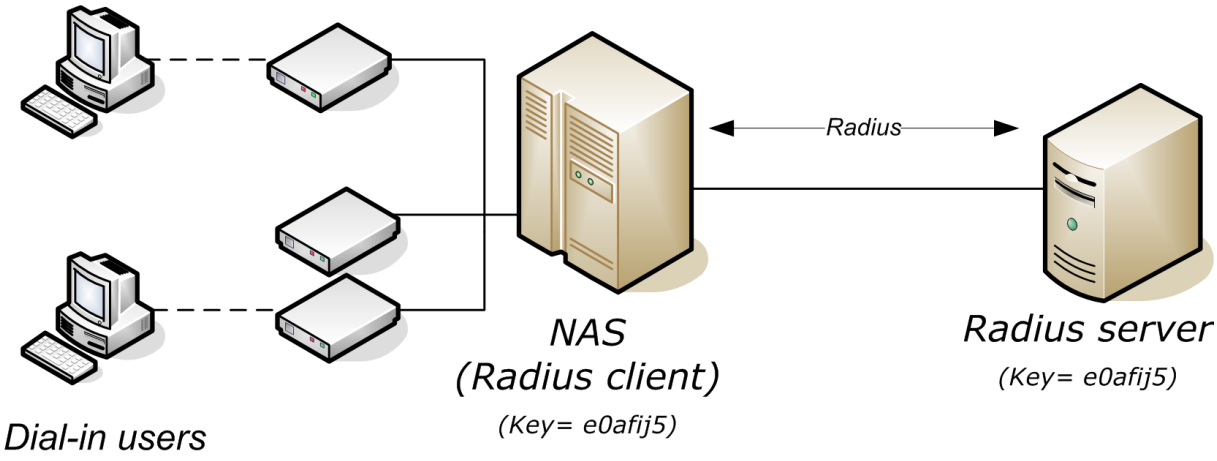
Utilité

Le but de RADIUS était à l'origine de permettre aux fournisseurs d'accès à Internet d'authentifier les utilisateurs distants utilisant les connexions par modem RTC à partir de multiples serveurs mais d'une seule base utilisateurs. Dans la situation précédente, les noms et mots de passe des utilisateurs devaient être dupliqués dans chaque appareil ayant besoin d'identifier des utilisateurs. De même, l'authentification POP (messagerie électronique) devait être gérée par ce biais. L'identification sur les sites Web par un nom et un mot de passe est aussi gérée en RADIUS, le serveur Apache est un des clients Radius les plus répandus. C'est toujours l'utilisation la plus courante du protocole RADIUS : nom et mot de passe de connexion à l'Internet, mais de plus en plus les réseaux sans fil ou filaires y ont aussi recours pour identifier les utilisateurs.

Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée. L'opération d'authentification est initiée par un client du service RADIUS, qui peut être un boîtier d'accès distant (NAS : Network Access Server), un point d'accès réseau sans fil, un pare-feu (firewall), un commutateur, un autre serveur. Le serveur la traite en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine ; un serveur Radius dispose pour cela d'un certain nombre d'interfaces ou méthodes.

Fonctionnement de l'identification

Schéma Client Radius entre les postes utilisateurs et le serveur Radius



Le poste utilisateur (supplicant dans les RFC) transmet une requête d'accès à un client RADIUS pour entrer sur le réseau. Ce client se charge de demander les informations identifiant l'utilisateur : le nom d'utilisateur (login) et le mot de passe par exemple.

Le client RADIUS génère selon le protocole une requête Access-Request contenant les informations d'authentification. Le serveur RADIUS peut traiter lui-même cette requête ou la transmettre à un autre serveur RADIUS par un mécanisme appelé Proxy Radius. Le serveur Radius chargé de l'identification finale (appelé Home Radius) peut traiter la demande s'il dispose de suffisamment d'éléments dans l'Access-Request ou demander des informations supplémentaires par un renvoi de paquet "Access Challenge", auquel le client répondra par un autre « Access-Request », et ainsi de suite. Les échanges sont retransmis par la chaîne de serveurs Radius proxy intermédiaires dans un sens et dans l'autre.

Quand le serveur Radius dispose de suffisamment d'éléments (jusqu'à une douzaine d'échanges pour les protocoles complexes de type EAP) le serveur RADIUS valide ou refuse l'identification en renvoyant un paquet de type : Access-Accept ou Access-Reject.

Protocoles de mot de passe

RADIUS connaît nativement deux protocoles de mot de passe : PAP (échange en clair du nom et du mot de passe), et CHAP (échange basé sur un hachage de part et d'autre avec échange seulement du « challenge »). Le protocole prévoit deux attributs séparés : User-Password et CHAP-Password.

Depuis, se sont greffées les variations Microsoft : MS-CHAP et MS-CHAP-V2 ; leur similitude avec CHAP permet de les transporter en RADIUS de la même façon, à l'initiative du serveur et sous réserve de possibilité de transport de bout en bout du supplicant au client Radius, du client au serveur Radius et enfin du serveur Radius à la base de données d'identification.

C'est sur cette dernière étape que souvent le bât blesse : rien n'est prévu par exemple en LDAP pour transporter le challenge ni les étapes spécifiques de MS-CHAP ou MS-CHAP-V2 qui, du coup, se terminent exclusivement sur des bases d'identification Microsoft locales pour le serveur Radius.

Exigences de connexion à un service d'authentification

Plusieurs paramètres sont nécessaires à l'établissement d'une connexion à un service d'authentification externe depuis un pare-feu. Ceux-ci peuvent bien sûr différés en fonction de la marque et du modèle de pare-feu.

Certains pare-feux possèdent des procédures simplifiées comme des Wizard de configuration par exemple. Pour d'autres, la configuration doit se faire manuellement.

Les paramètres suivants se retrouvent normalement pour chaque marque de pare-feu :

- Adresse IP du serveur d'authentification, éventuellement une adresse IP de backup d'un deuxième serveur d'authentification pour la redondance
- Ports et protocoles de connexion (389, 636, SSL, …)
- Base DN (La Base DN est le sommet d'un arbre DIT (Voir Directory Information Tree pour plus d'information). Il contient le nom unique de l'objet de base d'où commencera une recherche dans un annuaire. Un exemple de base DN est : DC=mycompany, DC=com)
- Intervalle et limite de temps de recherche
- Attributs de nom d'utilisateur, de groupe
- Authentification d'un utilisateur ayant les droits d'accès à l'annuaire, authentification avec MSChap
- Attribution d'un groupe spécifique de l'annuaire ayant les droits d'utiliser ce service d'authentification
- Création d'objets spécifiques dans le pare-feu (serveur AAA, …)
- …

Il est souvent possible de tester la liaison entre le pare-feu et le serveur d'authentification au moyen d'un petit outil sur le pare-feu qui permet d'entrer le nom d'un utilisateur et de voir si la connexion s'effectue correctement ou échoue. Si le dernière cas ce produit, il faudra alors contrôler les différents paramètres et les corriger en fonction.

Méthodes disponibles sur un pare-feu

Plusieurs méthodes d'authentification peuvent fonctionner simultanément sur un pare-feu, ceci en fonction des services ou des accès que l'on désire donner aux différents utilisateurs.

Quelles sont ces méthodes :

- Authentification locale : au moyen d'utilisateurs et de groupes locaux, propre au pare-feu
- Authentification AD : au moyen d'Active Directory de Microsoft
- Authentification LDAP : au moyen d'un serveur LDAP
- Authentification RADIUS : au moyen d'un serveur RADIUS (Microsoft, NAS, …)
- Autres méthodes aussi possibles

La première nécessite de tenir à jour une liste d'utilisateurs et de groupes ne se trouvant que sur le pare-feu.
Les trois suivantes permettent de tenir à jour une base de données centrales avec des utilisateurs et des groupes sans que ceux-ci soient configurés directement dans le pare-feu.

Exercice 1

L'exercice 4a te permettra d'utiliser ces différentes possibilités de services d'authentification, notamment avec l'accès VPN, l'accès à la page de management de ton pare-feu, l'accès à certains contenus ou à l'utilisation de certaines applications en lien avec les services Web. Reprends donc tes configurations existantes et complètes-les en ajoutant ces différentes fonctionnalités.

Sécurisation du réseau WLAN

La sécurité d'un réseau WLAN passe notamment par deux facteurs importants que nous allons parcourir dans ce cours. Il s'agit du cryptage et de l'authentification. D'autres méthodes existent mais elles feront partie d'un autre cours.

Cryptage d'un WLAN

Plusieurs normes de cryptage d'un WLAN existent et sont plus ou moins sécurisée. De nos jours, les normes conseillées sont WPA2 et WPA3. Faisons un petit tour d'horizon de ces deux normes.

La norme WPA

WPA est l'acronyme de Wi-Fi Protected Access.
Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), et Wi-Fi Protected Access 3 (WPA3) sont des mécanismes utilisés pour sécuriser les réseaux sans-fil de type Wi-Fi. La première version a été créée au début des années 2000 en réponse aux nombreuses et graves faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP.

En janvier 2018, la Wi-Fi Alliance annonce la dernière version en date (WPA3) avec des améliorations de sécurité notables par comparaison avec le WPA2.

WPA

WPA respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire pour remplacer le WEP en attendant que la norme 802.11i soit terminée. WPA a été conçu pour fonctionner, après mise à jour de leur micrologiciel, avec toutes les cartes Wi-Fi, mais pas nécessairement avec la première génération des points d'accès Wi-Fi.

WPA2

WPA2, le successeur de WPA, ratifié en 2004, comprend tous les éléments obligatoires de la norme 802.11i. C'est la version de la norme 802.11i certifiée par la Wi-Fi Alliance. En particulier, la norme WPA2 impose de prendre en charge le mécanisme CCMP, lequel s'appuie sur AES. Le protocole CCMP est considéré comme complètement sécurisé ; en mai 2004, le NIST l'a approuvé. Il est pris en charge depuis 2005 sur Windows XP2 et par tous les Macintosh comportant une carte Airport Extreme.

Les deux mécanismes fournissent une bonne sécurité, si l'on respecte deux points importants :

- L’utilisateur doit encore souvent faire le choix explicite d'activer WPA ou WPA2 en remplacement du WEP, car le WEP reste habituellement le choix de chiffrement par défaut sur la plupart des équipements ;
- Lorsque le mode ‘’WPA personnel’’ (WPA-Personal) est utilisé, ce qui est le choix le plus probable pour les particuliers et les PME, une phrase secrète plus longue que les classiques mots de passe de six à huit caractères utilisés par les utilisateurs est nécessaire pour assurer une sécurité complète.

WPA3

Wi-Fi Alliance a annoncé le protocole de sécurité WPA3 en 2018, qui fournit une méthode beaucoup plus sûre et fiable pour remplacer WPA2 et les anciens protocoles de sécurité. Les lacunes fondamentales de WPA2, comme une négociation à quatre voies imparfaite et l'utilisation d'une PSK (clé pré-partagée), exposent vos connexions Wi-Fi à un risque. WPA3 apporte d'autres améliorations de sécurité qui rendent plus difficile l'accès aux réseaux en devinant les mots de passe. Voici les considérations d'implémentation recommandées :

- Protection fiable par mot de passe
  La norme utilise une longueur de clé de 192 bits pour WPA3-Enterprise (AES-256 en mode GCM avec SHA-384 comme HMAC) et définit AES-128 comme exigence minimale pour le personnel WPA3 en mode CCM. Le but est d’améliorer la force du mot de passe. Il protège contre les mots de passe faibles qui peuvent être craqués relativement facilement par devinettes.

- Protégez vos périphériques réseau
  WPA3 remplace la clé pré-partagée WPA2 (PSK) par l'authentification simultanée d'égaux (SAE) pour éviter les attaques de réinstallation de clés comme le KRACK notoire. Il gardera vos périphériques réseau en sécurité lors de la connexion à un point d'accès sans fil. SAE est également une défense efficace contre les attaques par dictionnaire hors ligne.

- Connexion plus sûre dans l'espace public
  Même si les attaquants obtiennent des clés de chiffrement du trafic, il est difficile de calculer l'utilisation du trafic et les données transmises avec WPA3-Personal. SAE (Simultaneous Authentication of Equals), normalisée avec IEEE 802.11s, offre l'avantage de la confidentialité du transfert et beaucoup plus de sécurité des données sur un réseau ouvert. WPA3 fournit également des cadres de gestion protégés (PMF) pour éviter l'écoute clandestine et la falsification de la zone publique.

Les technologies WPA

On peut classer les technologies WPA selon trois axes : la version (dans l'ordre chronologique), le groupe d'utilisateurs visés (en termes de simplicité de la distribution de la clé d'authentification), ou le protocole de chiffrement (des données elles-mêmes) utilisé :

Selon la version :

- WPA : la version initiale de WPA, qui améliore la sécurité offerte par l'ancien protocole WEP. WPA utilise en général le protocole de chiffrement TKIP (voir plus loin).
- WPA2 : également connu sous le nom IEEE 802.11i-2004, ce successeur de WPA remplace le chiffrement TKIP par CCMP pour plus de sécurité. La compatibilité WPA2 est obligatoire pour les équipements certifiés Wi-Fi depuis 2006.

Selon le groupe d'utilisateurs visés :

- WPA personnel (WPA-Personal) : connu également sous le nom de mode à secret partagé ou WPA-PSK (Pre-shared key), WPA personnel est conçu pour les réseaux personnels ou de petites entreprises, car il n'y a pas besoin d'utiliser un serveur d'authentification. Chaque

équipement du réseau sans fil s'authentifie auprès du point d'accès en utilisant la même clé sur 256 bits.
- WPA entreprise (WPA-Enterprise) : connu également sous le nom de mode WPA-802.1X ou WPA-EAP, WPA entreprise est conçu pour les réseaux d'entreprise et demande que l'on installe un serveur d'authentification RADIUS. C'est plus compliqué à mettre en place, mais offre plus de sécurité, car cette méthode ne repose pas sur des phrases secrètes, vulnérables aux attaques par dictionnaire. Le protocole EAP (Extensible Authentication Protocol) est utilisé pour l'authentification. EAP existe en plusieurs variantes, dont EAP-TLS, EAP-TTLS et EAP-SIM.

Remarque : WPA personnel et WPA entreprise concernent à la fois WPA, WPA2 et WPA3.

Selon le protocole de chiffrement :
- TKIP (Temporal Key Integrity Protocol) : une clé de 128 bits est utilisée pour chaque paquet. On génère une nouvelle clé pour chaque paquet. TKIP est utilisé par WPA.
- CCMP : un mécanisme de chiffrement qui s'appuie sur AES et qui est plus fort que TKIP. On fait parfois référence à cette méthode de chiffrement sous le nom d'AES plutôt que sous le nom de CCMP. CCMP est utilisé par WPA2.

De nos jours, bon nombre de points d'accès Wi-Fi utilisés à titre personnel sont réglés par défaut soit en WPA en mode clé partagée (PSK) avec le chiffrement TKIP, soit en WPA2 en mode clé partagée avec chiffrement CCMP, et prennent également en charge le mode entreprise.

Méthodes d'authentification à un WLAN

Comme nous l'avons vu ci-dessus, deux méthodes existent. Il s'agit de Personal (PSK) et Enterprise (802.1X).

Personal

Cette méthode convient à la plupart des réseaux domestiques. Lorsqu'un mot de passe est défini sur un routeur sans fil ou un point d'accès, il doit être saisi par les utilisateurs lors de la connexion au réseau Wi-Fi.

En mode PSK, l'accès sans fil ne peut pas être géré individuellement ou de manière centralisée. Un mot de passe s'applique à tous les utilisateurs. Il doit être modifié manuellement sur tous les clients sans fil une fois qu'il a été modifié manuellement sur le routeur ou le point d'accès sans fil d'origine.

Le mot de passe est stocké sur les clients sans fil. Par conséquent, n'importe qui sur l'ordinateur peut se connecter au réseau et voir le mot de passe.

Le mode pre-shared key (PSK, aussi connu comme Personal mode) a été conçu pour les réseaux individuels ou de PME qui ne peuvent se permettre le coût et la complexité d'une solution utilisant un serveur d'identification 802.1X. Chaque utilisateur doit saisir une phrase secrète pour accéder au réseau. La phrase secrète peut contenir de 8 à 63 caractères ASCII ou 64 symboles hexadécimaux (256 bits). Si une phrase secrète sous forme de caractères ASCII est utilisée, elle sera, au préalable, convertie vers une clé de 256 bits que l'on nomme Pairwise Master Key ou PMK en appliquant une fonction de dérivation de clé PBKDF2 qui utilise le SSID comme sel (méthode de salage) et 4096 itérations de HMAC-SHA114.

Utiliser une suite aléatoire de caractères hexadécimaux reste plus sûr – une phrase secrète reste, toutes proportions gardées, sujette à une attaque par dictionnaire – mais la clé est alors plus difficile à écrire et à retenir. La plupart des systèmes d'exploitation permettent à l'utilisateur de stocker la phrase secrète sur l'ordinateur (en règle générale sous forme de PMK), afin de ne pas avoir à la saisir à nouveau. La phrase secrète doit rester stockée dans le point d'accès Wi-Fi.

Cependant, les phrases secrètes que les utilisateurs ont l'habitude d'utiliser rendent le système vulnérable aux attaques par force brute sur les mots de passe. Des programmes réalisant ce type d'attaque sur des systèmes WPA-PSK ou WPA2-PSK sont disponibles sur Internet, c'est le cas de WPA Cracker. De plus, le temps nécessaire pour réaliser une attaque peut être réduit par un facteur 20 et plus grâce à l'utilisation de technologies telles que CUDA ou OpenCL tirant parti de la puissance de traitement massivement parallèle des cartes graphiques actuelles, en utilisant par exemple l'outil pyrit.

Ces attaques peuvent être contrecarrées en utilisant conjointement à WPA et à WPA2 un secret d'au moins 5 mots générés par la méthode Diceware ou 14 caractères complètement aléatoires. Pour une sécurité maximum, 8 mots générés par la méthode Diceware ou 22 caractères aléatoires devraient être utilisés. Les phrases secrètes devraient, de plus, être changées dès qu'une personne ayant un accès au réseau n'est plus autorisée à l'utiliser ou bien dès qu'un équipement connecté au réseau est perdu ou compromis.

Enterprise

Cette méthode fournit la sécurité nécessaire pour les réseaux sans fil dans les environnements professionnels. Plus complexe à installer, il offre un contrôle individualisé et centralisé de l'accès au réseau Wi-Fi. Lorsque les utilisateurs essaient de se connecter au réseau, ils doivent présenter leurs identifiants de connexion.

Ce mode prend en charge l'authentification RADIUS 802.1x et convient dans les cas où un serveur RADIUS est déployé. WPA-Enterprise ne doit être utilisé que lorsqu'un serveur RADIUS est connecté pour l'authentification du client.

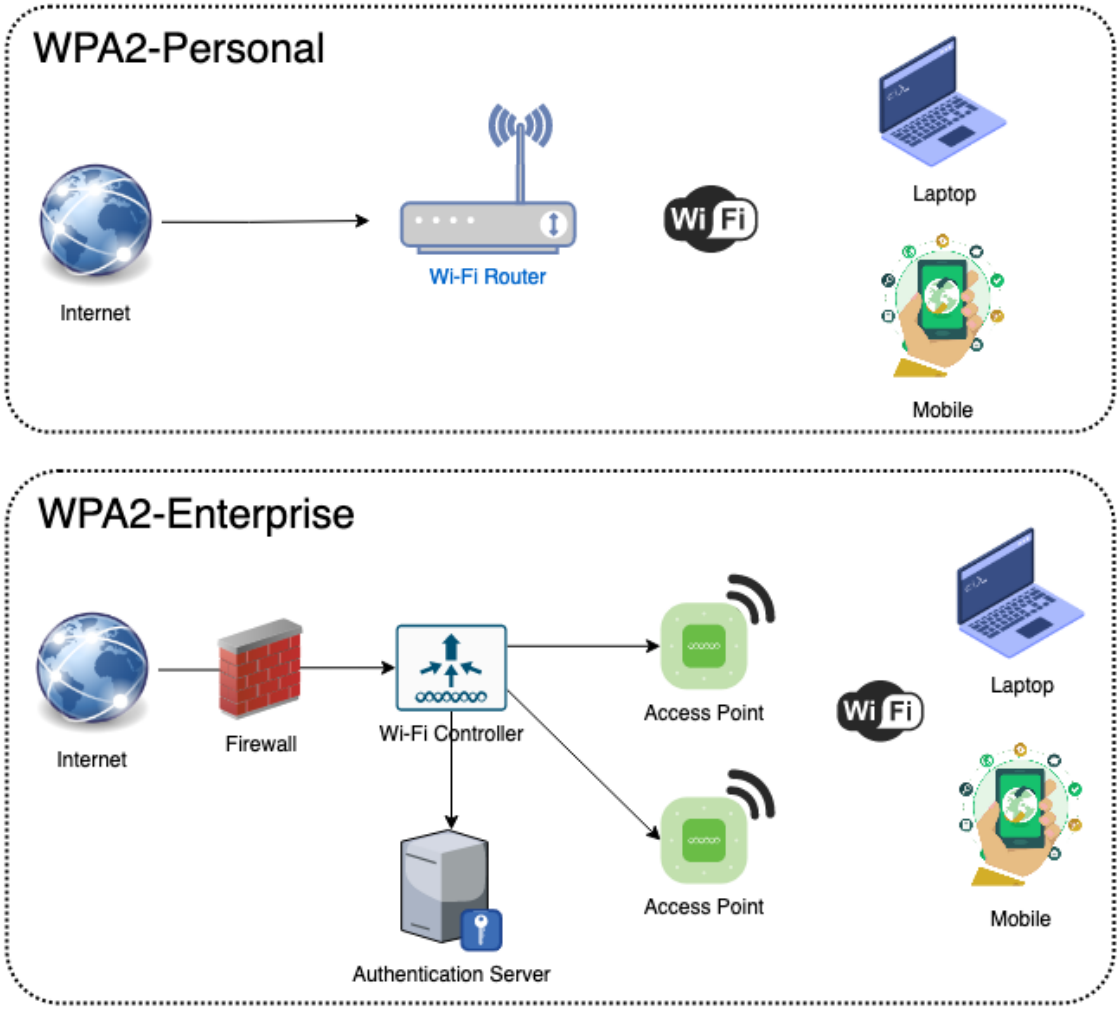
Les utilisateurs ne traitent jamais avec les clés de chiffrement réelles. Ils sont créés de manière sécurisée et attribués par session utilisateur en arrière-plan après qu'un utilisateur présente ses informations de connexion. Cela empêche les utilisateurs d'obtenir la clé réseau des ordinateurs.

La Wi-Fi Alliance a annoncé l'intégration de mécanismes EAP (Extensible Authentication Protocol) supplémentaires dans son programme de certification pour les modes WPA-Enterprise et WPA2-Enterprise. Ainsi, a-t-on la certitude que les produits certifiés WPA-Enterprise peuvent interopérer entre eux. Auparavant, seul le mécanisme EAP-TLS (Transport Layer Security) était certifié par la Wi-Fi Alliance.

Les différents mécanismes EAP inclus dans le programme de certification sont :

- EAP-TLS (précédemment testé)
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

D'autres mécanismes EAP peuvent être pris en charge par les clients et les serveurs 802.1X. Cette certification est une tentative pour faire interopérer les mécanismes EAP les plus courants. L'échec de la Wi-Fi Alliance à réaliser cette interopérabilité est actuellement un des problèmes majeurs empêchant le déploiement de solutions 802.1X au sein de réseaux hétérogènes.



Exercice 2

L'exercice 4b te permettra d'utiliser ces différentes possibilités de services d'authentification et d'encryption dans la gestion et la configuration de ton réseau WLAN. Reprends donc tes configurations existantes et complètes-les en ajoutant ces différentes fonctionnalités.

Jour 5

Objectifs du jour 5

- Sauvegarde du pare-feu
- Mise à jour du pare-feu
- Elaboration de la documentation
- Evaluation des compétences acquises
- Rangements de la place de travail

Ce dernier jour de cours permettra de valider tes différents acquis, entraînés durant cette semaine de cours inter-entreprises. Un test sur la configuration du pare-feu aura lieu et déterminera si tes compétences en matière de pare-feu sont atteintes. Il sera temps, pour terminer, de ranger ta place de travail et de remettre tous les équipements utilisés en configuration de base.

Mais avant cela, les points suivants doivent encore être traités :

- Sauvegarde du pare-feu
- Mise à jour du logiciel (firmware) du pare-feu
- Gestion de la documentation

Sauvegarde du pare-feu

La règle la plus importante, lors de la configuration et de la modification d'un pare-feu, est de s'occuper, avant toute chose, de la sauvegarde complète de la configuration.

Certains pare-feux intègrent un système de gestion pouvant gérer plusieurs fichiers de configurations simultanés, ce qui permet, en cas d'erreur de configuration, de revenir rapidement à une version fonctionnelle du pare-feu.

La bonne pratique veut que, lors d'une maintenance, une sauvegarde complète du système soit effectuée lors de la connexion sur le pare-feu. Ce fichier doit ensuite être téléchargé sur ton PC puis être stocké dans le dossier client. Une fois la maintenance terminée, une nouvelle sauvegarde complète du système doit être effectuée. Ce fichier doit également être téléchargé sur ton PC, puis être stocké dans le dossier client.

La nomenclature ou nommage des fichiers doit permettre d'identifier à quel moment ces derniers ont été créés. Voici un exemple :

EVO-FW001_20220525_0832 : Trigramme client – nom du pare-feu – date – heure

Certains fabricants proposent de réaliser des sauvegardes automatiques de la configuration du système. Celle-ci peut être envoyée par e-mail, par FTP, par SFTP, … Une solution d'envoi sécurisée doit être privilégiée afin d'empêcher des personnes malveillantes de récupérer le fichier de configuration et de pouvoir l'analyser. Cette situation pourrait être fort dommageable pour l'entreprise si l'accès au pare-feu tombait dans de mauvaises mains.

Mise à jour du logiciel

L'objectif d'une mise à jour logiciel d'un pare-feu est, souvent, de corriger différents bugs du système ainsi que d'apporter des nouvelles fonctionnalités. Certaines mises à jour sont liées au système d'exploitation du pare-feu, alors que d'autres sont liées aux différents paquets complémentaires comme les mises à jour des services UTM (mise à jour des bases de données). Ces dernières sont généralement installées automatiquement et régulièrement (tous les jours, toutes les semaines ou tous les mois). Les mises à jour du système d'exploitation sont moins régulières et doivent généralement être installées manuellement.

La majorité des pares-feux intègrent deux partitions et peuvent accueillir ainsi deux versions du système d'exploitation. Une partition sera en mode actif et l'autre en mode passif.

Lors d'une mise à jour du système d'exploitation, le nouveau logiciel doit être installé sur la partition en mode passif. En cas de problème de fonctionnement, un retour vers l'ancien logiciel peut être effectué très rapidement.

Il est évident qu'une procédure de sauvegarde (expliquée au point précédent) doit absolument être effectuée avant toute mise à jour du système d'exploitation du pare-feu.

Dans la mesure du possible, un test de mise à jour devrait être réalisé dans ton laboratoire, sur un pare-feu de tests afin de vérifier le bon fonctionnement du nouveau système d'exploitation. Cette étape te permet de te familiariser avec la nouvelle version, de tester et mettre en service les nouvelles fonctionnalités, d'identifier si de nouveaux bugs sont apparus et de contrôler si les bugs précédents ont été corrigés.

Généralement, les fabricants fournissent un document de mise à jour qui permet d'être averti des différentes modifications apportées et d'éventuelles restrictions ou suppression de fonctionnalités, ainsi que des nouvelles fonctionnalités disponibles. Il est important d'identifier les prérequis et les recommandations du fabricants avant toute mise à jour. Parfois, une mise à jour n'est pas conseillée.

La nomenclature des mises à jour a généralement un schéma bien particulier. Voici un exemple :

La numérotation de type X.Y.Z est utilisée par de nombreux fabricants.

La convention Semantic Versioning propose la signification suivante :

- X correspond à la version majeure : changements non rétrocompatibles. Les évolutions majeures apportent de nouvelles fonctionnalités, en changeant radicalement l'apparence ou l'architecture du produit.
- Y correspond à la version mineure : ajouts de fonctionnalités rétrocompatibles, principalement des corrections de bugs, ajouts de quelques fonctionnalités, …
- Z correspond au correctif : corrections d'anomalies rétrocompatibles, failles de sécurité, … On parle parfois de patch

Il existe parfois des versions qui ne sont pas encore finalisées. En voici deux exemples :

- Version alpha : généralement peu stable et comportant plusieurs bugs et fonctionnalités non finalisées
- Version beta : généralement assez stable et proche de la version finale. L'intégration de nouvelles fonctionnalités est proche de l'achèvement.
- Version ''weekly'' : certains fabricants proposent des versions à la semaine avec la correction des bugs principaux

Ces dernières mises à jour ne devraient être utilisées que dans un environnement de laboratoire pour différents tests et ne pas être installées dans un environnement de production, notamment chez le client.

Gestion de la documentation

La documentation d'une infrastructure est primordiale et doit être disponible en tout temps dans le dossier du client. Elle doit être mise à jour régulièrement, lors de chaque mise à jour ou modifications de l'installation. Elle doit pouvoir servir pour le support du client, ce qui favorisera un dépannage

rapide et efficace. Il faut toujours penser qu'un autre technicien doit pouvoir intervenir chez le client et avoir à sa disposition toutes les informations nécessaires au bon déroulement de son intervention.

Une bonne documentation devrait contenir au moins les éléments suivants :

- Photos de l'installation, des connexions et des équipements
- Fichier sécurisé avec les mots de passes et comptes utilisateurs
- Matrice des droits d'accès (infrastructure et/ou données)
- Journaux des modifications et configurations listant toutes les interventions effectuées
- Schémas de l'installation, plans d'étages
- Listing des licences actuelles et dates de renouvellement
- Backup du système avant et après l'intervention, éventuellement la gestion de backups automatisés
- Etiquetage des équipements avec une nomenclature propre à chaque client
- Procédures particulières en lien avec l'infrastructure du client final
- Plan d'adressage complet avec tous les réseaux (LAN, VLAN, …)

Il est évident que d'autres documents devraient encore faire partie d'une documentation complète d'un client. Voici un listing non-exhaustif qui peut être complété selon les besoins :

- Clauses de confidentialité en lien avec le client final
- Offres, devis, bulletins de livraison, offres complémentaires / plus-value, factures du matériel, demandes d'acomptes, facture finale
- Listing des intervenants dans le projet (chef de projet, technicien, référant du client, autres personnes impactées, …)
- PV de mise en service et de rendu de l'installation au client final
- Décharge de responsabilité
- Correspondances, mails importants
- Automatismes (GPO, …)
- Procédures de traitement des données (suppression, élimination, …)

Comment est géré cette partie documentation dans ta société ? Pourrais-tu ajouter des points aux listes ci-dessus ? Ou, au contraire, pourrais-tu mettre en place certains points dans les diverses procédures existantes dans ta société ?

Test de validation

Il est maintenant temps de passer à l'évaluation qui te permettra de valider tes acquis sur le pare-feu et de valider également ce module de cours inter-entreprise.

Ton formateur te donnera les détails et l'exercice à réaliser dans le temps imparti.

Nous te souhaitons beaucoup de réussite.

Fin du module et rangements

Tu viens de terminer ton évaluation et nous espérons qu'elle s'est bien déroulée et que tu as pu montrer à ton formateur le niveau acquis durant ce cours inter-entreprise.

Il est maintenant temps de ranger ta place de travail afin qu'elle soit opérationnelle pour un prochain cours.

Nous t'encourageons à sauvegarder tous les backups des différents équipements afin de reproduire, au besoin, cette infrastructure. Nous te conseillons vivement, par la suite, de refaire les différents exercices afin de t'entraîner un maximum sur ce genre d'équipements réseau.

Nous te souhaitons beaucoup de plaisir dans ta profession d'informaticien de bâtiments et beaucoup de satisfaction dans l'installation et la configuration d'équipements réseau.

Liens, bibliographies, sources, etc.

- https://www.redhat.com/fr/topics/security
- https://www.informatiquenews.fr/les-10-failles-securite-representent-99-cas-jean-nicolas-piotrowski-ittrust-19224
- https://www.sfrbusiness.fr/room/securite/differents-types-menaces-informatiques-entreprises.html
- https://www.telus.com/fr/business/blog/securite-information-menaces-courantes
- https://blog.netwrix.fr/2019/04/03/comment-realiser-une-evaluation-des-risques-informatiques/
- https://cours-de-droit.net/droit-et-informatique-a121603678/
- https://www.swisscom.ch/fr/b2bmag/securite/entreprise-securite-verifier/
- https://www.swisscom.ch/fr/business/pme/it-cloud/security-check.html#/start
- https://www.swisscom.ch/fr/b2bmag/securite/journee-travail-securite/
- https://www.swisscom.ch/fr/business/pme/downloads/elearning-security.html
- https://www.swisscom.ch/fr/b2bmag/topic/trucs-astuces/
- https://securitycheck.suissedigital.ch/
- http://www-igm.univ-mlv.fr/~duris/NTREZO/20052006/MasquelierMottierPronzato-Firewall-rapport.pdf
- https://www.frameip.com/firewall/
- https://www.frameip.com/wp-content/espace-multimedia-video/frameip.com-302-what-is-a-firewall.mp4
- https://www.frameip.com/wp-content/espace-multimedia-video/frameip.com-207-initiation-a-la-notion-de-firewall.mp4
- https://fr.tenable.com/products/nessus
- https://www.cyber-safe.ch/
- https://www.avast.com/fr-fr/c-what-is-a-vpn
- https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/l2tp
- https://wiki-tech.io/fr/S%C3%A9curit%C3%A9/WireGuard
- https://www.algofi.fr/communication/le-versionnage-des-logiciels.html
- https://semver.org/lang/fr/
- https://www.inwebo.com/mfa-authentification-multifacteurs/
- https://ibracilinks.com/blog/quest-ce-que-lauthentification-ldap
- https://docs.microsoft.com/fr-fr/windows-server/security/windows-authentication/windows-authentication-overview
- https://www.watchguard.com/help/docs/help-center/fr-FR/Content/en-US/Fireware/authentication/active_directory_about_c.html
- https://fr.wikipedia.org/wiki/Active_Directory
- https://www.watchguard.com/help/docs/fireware/12/fr-FR/Content/fr-FR/authentication/radius_how_works_c.html
- https://www.commentcamarche.net/contents/91-radius
- https://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
- https://www.visual-guard.com/FR/net-powerbuilder-application-securite-authentification-permission-controle-acces-rbac/authentification-multi-facteurs/strong-authentication-method-scenario.html
- https://www.beyondtrust.com/fr/docs/remote-support/getting-started/admin/security-providers.htm
- https://sysopstechnix.com/wpa2-enterprise-secure-your-organization-wi-fi-network/
- https://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access
- https://blog.netwrix.de/category/security/

- https://www.lehmanns.ch/shop/recht-steuern/25461-9783423055628-it-und-computerrecht-compr
-