REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et Télécommunications

Par :

OBANDAS Michelle Hardie
NGOYI NZIELE Posthurine

Sur le thème

Proposition et mise en œuvre d'une stratégie de sécurité

Soutenu publiquement le .. / .. / 2021 à Tiaret devant le jury composé de :

Mr AID Lahcen	Grade Université MCB	Président
Mr MOSTEFAOI Sid Ahmed Mokhtar	Grade Université MCB	Encadreur
Mr DAOUD Mohamed Amine	Grade Université MAA	Examinateur

2020-2021

REMERCIEMENT

Un grand merci à notre DIEU qui nous a permis de finir nos études et de prendre courage malgré les obstacles durant notre cursus mais encore de finaliser ce mémoire qui est le fruit de nos efforts et aussi l'accomplissement d'un travail de longue haleine.

Nous sommes reconnaissant envers notre encadreur Mr MOUSTEFAOUI Sidi Amed Mokhtar, pour sa compétence et son encadrement qui ont toujours suscité notre profond respect, nous le remercions pour son accueil et ses conseils.

Nous adressons nous remerciement aux membre du jury Mr AID Lahcen et Mr DAOUD Mohamed Amine qui nous ont l'honneur d'accepter d'évaluer ce travail.

Nous tenons à exprimer notre gratitude à TEFO Loïc d'avoir sacrifié de son temps et de nous avoir prodigué ses précieux conseils pour aboutir à ce projet.

Nous tenons également à remercier nos familles et nos ami(es) pour leur assistance morale et physique.

DEDICACE

À ma très chère tendre et douce mère, NGONDO VALERIE qui m'a doté d'une éducation digne, son amour inconditionnel a fait de moi ce que je suis aujourd'hui. Oui plus particulièrement à toi maman pour le goût à l'effort que tu as suscité en moi de par ta rigueur, conseils, ceci est ma profonde gratitude pour ton éternel amour. Que ce mémoire soit le meilleur des cadeaux que je puisse t'offrir.

À toi ma grand-mère LOPOUNDA VALENTINE pour tes prières, conseils et encouragements qui ont bercé mon enfance.

À toi ma sœur DABOUDARD ATTA ALPHONSINA OLIVIA celle à qui je souhaite un avenir radieux.

À vous mes tantes, oncles, cousins, cousines et ami(es) qui m'aviez toujours soutenu et encouragé durant ces années d'études.

OBANDAS Michelle Hardie

DEDICACE

À ma mère LOUHANGOU MELANIE RACHEL que j'ai nommé « my wonder-women », celle qui n'a pas cessé de m'aimer, de m'encourager d'aller plus loin dans mes études. Celle qui me pousse à lancer les nouveaux défis.

À mon feu père NGOYI NZIELE JEAN que je n'ai pas eu cette chance de connaitre, de là où tu es je peux ressentir la fierté que tu ressens à mon égard.

À ma sœur NGOYI NZIELE MARINA et mon frère NGOYI NZIELE BERANGER qui m'ont toujours soutenu et encouragé durant ces années d'études.

À mes ami(es) et à tous ceux qui me sont chers.

NGOYI NZIELE Posthurine

RESUME

La sécurité des réseaux informatique c'est l'ensemble des moyens technique, organisationnels juridique et humain mise en œuvre pour minimiser la vulnérabilité d'un système de réseau informatique contre des menaces accidentels ou intensionnels. Ce mémoire intitulé « proposition et mise en œuvre d'une stratégie de sécurité » introduit les différents services de sécurités et les mécanismes cryptographiques permettant de les réalisé en utilisant les outils nécessaires à la pointe de la technologie. Ce mémoire est scindé en un ensemble d'unité d'apprentissage qui permettent de vous sensibiliser aux risques liées aux attaques sur les réseaux d'entreprise, vous familiariser avec les concepts de la sécurité des réseaux informatique et d'acquérir ces compétences en matière d'utilisation des mécanismes cryptographique pour garantir différents services de sécurité et d'analyser l'environnement des sécurités réseaux informatique.

نبذة مختصرة

أمان شبكة الكمبيوتر هو جميع الموارد التقنية والتنظيمية والقانونية والبشرية التي يتم تنفيذها لتقليل ضعف نظام شبكة الكمبيوتر ضد التهديدات العرضية أو المكثفة. هذه الرسالة بعنوان "اقتراح وتنفيذ استراتيجية أمنية" تقدم خدمات الأمن المختلفة وآليات التشفير التي تسمح بتنفيذها باستخدام الأدوات اللازمة في طليعة التكنولوجيا. تنقسم هذه الرسالة إلى مجموعة من وحدات التعلم التي تسمح لك بالتعرف على المخاطر المرتبطة بالهجمات على شبكات الشركات، وتعرفك بمفاهيم أمان شبكات الكمبيوتر واكتساب هذه المهارات في 'استخدام آليات التشفير لضمان خدمات أمنية متنوعة ولتحليل بيئة أمان شبكة الكمبيوتر.

ABSTRACT

Computer network security is all the technical, organizational, legal and human resources implemented to minimize the vulnerability of a computer network system against accidental or intensive threats. This thesis entitled "proposal and implementation of a security strategy" introduces the various security services and the cryptographic mechanisms allowing them to be carried out using the necessary tools at the cutting edge of technology. This thesis is divided into a set of learning units that allow you to become aware of the risks associated with attacks on corporate networks, familiarize you with the concepts of computer network security and acquire these skills in 'use of cryptographic mechanisms to guarantee various security services and to analyze the computer network security environment.

Liste des tableaux

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des abréviations

ISO : Organisation Internationale de la Normalisation
DES : Data Encryption Standard
AES : Advanced Encryption Standard
SSL : Secure Sockets Layer
TLS : Transport Layer Security
ACL : Access control List
TCP : Transmission Control Protocol
IP : Internet Protocol
Http : Hypertext Transfer Protocol
FTP : File Transfer Protocol
SSH : Protocole Secure Shell
PAP : Password Authentication Protocol
CHAP : Challenge Handshake Authentiction Protocol
IPSEC : Internet Protocol Security
VLAN : Virtual Local Area Network
AAA : Authorization, Accounting/Auditing
SPD : Security Policy Database
ICV : Integrity Check Value
SPI : Security Parameter Index
AH : Authentification Hearder
ESP : Encasulated Security Payload
SA : Security Association
IKE : Internet Key Exchange
VPN : virtual private network
SNMP : Simple Network Management Protocol
BGP : Border Gateway Protocol
TTL : Time-to-Live
HTTPS : HyperText Transport Protocol Secure
IRDP : ICMP Router Discovery Protocol
OSPF Open Shortest Path First

CHAPITRE III : LES PRINCIPALES ATTAQUES RÉSEAU

CHAPITRE IV : MISE EN PLACE D'UN RESEAU D'ENTREPRISE SECURISÉ PAR LE PARE-FEU ASA

INTRODUCTION GÉNERALE

De nos jours avec le développement exponentiel de réseaux et télécommunication, chaque ordinateur connecté à internet (ou à un réseau) est susceptible d'être victime d'une intrusion (risque d'altérer l'intégrité du système et des données). Les pirates informatiques ayant l'intention de s'introduire dans les systèmes recherchent des failles dans les protocoles, les systèmes d'exploitations et les applications. Alors ils examinent donc le réseau avec soin dans le cadre de la recherche d'une machine connectée puis ils cherchent une faille de sécurité afin d'exploiter et d'accéder aux données.

Voilà pourquoi les ingénieurs de réseaux informatiques (ou administrateurs réseaux) ne cessent de puiser dans leurs connaissances pour contrecarrer les attaques réseaux et mettre en place un système de sécurité surélevée afin de renforcer les administrations mais surtout retrouver la fiabilité. Dans ce mémoire, nous évoquerons ces points et nous proposerons une meilleure stratégie pour avoir une fiabilité dans les réseaux d'entreprise.

CHAPITRE I
OBJECTIFS ET MÉCANISMES DE LA SÉCURITE INFORMATIQUE

I. INTRODUCTION

Internet est une jungle, remplie de dangers, la moindre erreur commise entraine la perte de vos Données confidentielles et peuvent être à la portée des hackers, de nos jours, avec l'arrivée du « big data », nous avons besoin de protéger ces données moyennant en sécurité informatique. La sécurité informatique est pour beaucoup d'entreprises un élément capital en sécurité informatique. Les exigences au milieu des organisations ont mené à plusieurs changements majeurs au cours de ces dernières années, ayant pour but de protéger nos données, elle se doit de s'appuyer sur différents objectifs pour garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cas prévu et ce grâce aux mécanismes mis en place qui évitent les intrusions pour assurer sa fiabilité. Dans un premier temps nous allons aborder les objectifs émis par ce système et ensuite nous découvrirons ces mécanismes.

II. LES OBJECTIFS

Dans la sécurité informatique l'objectif est défini comme un but à atteindre pour protéger les informations contre toute attaque réseau, et assurer en quelque sorte une protection totale du réseau (bien qu'en informatique la sécurité totale n'existe pas) et surtout avoir un contrôle sécurisé sur la ressource informatique.

Les objectifs que nous évoquons ici permettent d'identifier les vulnérabilités et prendre toutes les précautions adaptées pour assurer la sécurité des données. Ces principaux objectifs définis par l'Organisation Internationale de la Normalisation (ISO) sont :

- La confidentialité des données
- L'intégrité des donnés
- La disponibilité
- L'authentification
- Contrôles d'accès
- Non répudiation
- Protection contre l'analyse de trafic

Nous allons nous baser sur ces trois principaux objectifs :

1. La confidentialité

Elle garantit le secret d'information dans un système informatisé. Protège toutes les données qui ne peuvent pas être consultées par des entités tierces. (Seules les personnes autorisées qui ont accès aux ressources échangées) Elle est l'une des causes de l'existences

des cryptosystèmes. Un échange d'information ne sera pas divulgué aux personnes non autorisées nous allons prendre comme exemple le réseau social Facebook le plus populaire au monde qui compte près de 1,7millards de membres il adopte la politique de confidentialité qui se situe dans une section intitulé privacy basics qui permet de contrôler par exemple qui a le droit de voir vos publications. Alors Il est donc essentiel dans des entreprises informatiques et surtout de nos jours les entreprises qui utilisent les technologies web comme par exemples des entreprises d'ingénieries des connaissances sont dans l'obligation de certifier que des telles règles sont prises en considération.

2. Intégrité

De nos jours avec le « big data » comme système de traitement et de stockage de données, il est crucial de préserver l'intégrité des données collectées. Dans l'intégrité, les données ne peuvent pas être changées. Tout comme la confidentialité, l'intégrité s'applique à un flux de messages. Sa meilleure approche est une protection totale du flux et garantir la réception des messages aussitôt envoyés sans pourtant être modifiés, dupliqués etc. L'intégrité se base à la fiabilité ou encore à la crédibilité des données durant leurs cycles de vie.
L'intégrité des données préservent vos données au force extérieur, elle applique la conformité des données transmises lors d'une transmission d'information. Comme par exemple lors d'une transmission d'un message entre deux utilisateurs le message ne subit aucune alternation, le récepteur reçoit le message émis par l'émetteur en tout intégralité.

3. Disponibilité

La disponibilité permet de protéger ou défendre la bonne coordination des applications. Le principe de la disponibilité est d'assurer le bon fonctionnement d'un service sans irruption à l'instant où la requête est faite. Plusieurs attaques peuvent provenir(naitre) d'une réduction de la disponibilité d'une entreprise ou d'un service. En d'autre termes nous pouvons dire qu'elle garantit l'accès à un service ou à des Ressource.

III. LES MECANISME

La sécurité informatique s'attache aux mécanismes car ils permettent d'échapper aux intrusions. Avec l'échange de message dans le système de réseau nous déployons des mécanismes pour éviter un mélange de messages redondants (duplication) et non redondants et de pourvoir protéger les informations. Par définition un mécanisme est conçu pour prévenir

et détecter une attaque réseau. La progression de la technologie ramène une panoplie de mécanisme de sécurité il s'agit : des techniques cryptographiques (écriture chiffrée ou le chiffrement), signature numérique, technique d'utilisation d'identificateurs et de mot de passe, de bourrages et de notarisation ou d'autre transformation semblable à l'information est le biais le plus commun pour fournir une sécurité. Ainsi dans quelques lignes, nous allons mettre l'accent sur l'utilisation, le développement et la gestion de ces techniques.

1. LE CHIFREMENT

Le chiffrement consiste à transformer vos données afin de les rendre illisibles et intelligibles grâce à un algorithme de chiffrement et une clé de chiffrement.

La clé de chiffrement est utilisée par l'algorithme pour chiffrer et déchiffrer les données. Il faut noter que la clé de chiffrement peut être une suite de bits ou encore une donnée (comme une série de chiffre, une phrase…). Qu'on peut voir comme un mot de passe. En d'autre terme Le chiffrement est un procédé de la cryptographie qui consiste à protéger les informations vis-à-vis des personnes n'ayant pas la clé pour rendre le message incompréhensible.

Par exemple, lorsque vous vous connectez sur le site de votre banque, la connexion se fait toujours en https pour des raisons de sécurité parce que si la connexion se fait en http alors toutes les informations échangées transiteraient en claire. Ce qui veut dire qu'une personne malveillante peut intercepter les échanges entre vous et votre banque et donc avoir toutes les informations qui y transitent, d'où la nécessité du chiffrement. Il existe deux méthodes de chiffrement : symétrique et asymétrique.

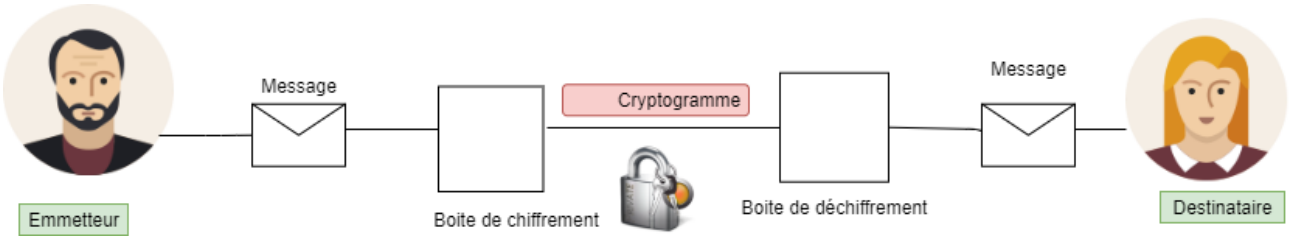


figure 1 : chiffrement

Description

Cet exemple nous illustre que l'émetteur envoie un message chiffré (cryptogramme) par une boite de chiffrement qui est un algorithme de chiffrement, le destinataire à son tour détient la

clé pour pouvoir déchiffrer le message émit par l'émetteur, le cadenas avec une clé représente le message chiffré.

- **CHIFFREMENT SYMÉTRIQUE**

Le chiffrement symétrique est la plus ancienne méthode de chiffrement, ici une seule clé nous permet de chiffrer et déchiffrer le message.

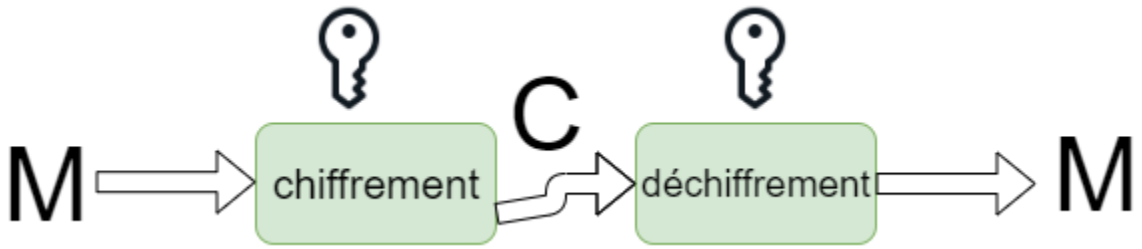


figure 2 : chiffrement symetrique

DESCRIPTION

Ici nous avons M comme message en claire, K est défini comme la clé secrète entre deux utilisateurs, comme nous venons de le dire précédemment, dans cet algorithme nous utilisons la même clé, une fois le message est chiffré, il est nommé C et avec la même clé nous pouvons le déchiffrer, le fonctionnement du chiffrement symétrique est irréversible.

Inconvénients et avantages du chiffrement symétrique

Le seul problème du chiffrement symétrique c'est l'échange de ces clés. Le fait d'avoir une même clé impose à avoir un canal sécurisé pour échanger la clé. Car si une personne tierce arrive à s'emparer de la clé elle sera dans la capacité de lire les messages échangés et une fois l'algorithme découvert tous les messages chiffrés deviennent lisibles par cette dernière.
Son avantage est qu'il est facile à réaliser, sa mise en œuvre est rapide et peut être utilisé dans divers milieux.

On distingue plusieurs types d'algorithmes de chiffrement symétrique. Les plus utilisés : DES, CHIFFRE DE VERNAM, 3DES, AES, RC5, RC5, MISFY1 et bien d'autres.

En effet le chiffrement symétrique s'appuie sur deux catégories

LE CHIFFREMENT PAR BLOC (BLOC CIPHER) : supposons qu'on a un messages M et une clé k, alors le chiffrement par bloc consiste à découper le message M en morceaux de taille constante qu'on appelle les blocs et ensuite on utilise la clé pour chiffrer chacun de ces blocs et les combiner. Il faut noter que la taille du bloc varie de 32 à 512bits, vers les années 1990 le standard était 64bits mais depuis 2000 AES standard est à 128 bits ce qui nous mène à citer deux méthodes principales de chiffrement par bloc :

- DES(data encryption standard) : conçu en 1977 par IBM et utilise une technique qui consiste à diviser les messages par blocs de 64 bits et utilise aussi une clé de 64 bits. Ici avec une clé de 64 bits il y'a deux puissances 64 différentes clés possibles environ 16 milliards de milliards de clés possibles à tester. Mais en réalité si on regarde l'implémention de l'algorithme c'est seulement une clé de 56 bits car il y'a 8 bits qui ne servent absolument à rien.

  Au fait lors du design NSA (le programme de surveillance électronique) l'algorithme fait pression pour qu'on utilise seulement 56 bits car à l'époque, craquer une clé de 64 bits était impossible. Mais au fil du temps les ordinateurs ont énormément évolué et les experts ont trouvé les attaques dans iOS qui permettent de craquer sans faire une recherche complète de toutes les clés. D'où le chiffrement DES n'est plus fiable. Mais il a été utilisé dans le chiffrement de mot de passe unix.
- AES(advanced encryption standard) : il a été crée par Joan DAEMAN et Vincent RIJMEN de nationalité belge, il a été conçu pour corriger les inconvénients de l'algorithme DES, AES est constitué de clés de 128 bits, 192 bits et 256 bits cela est important dans le monde de la sécurité informatique pour les données sensibles.
  Par exemple AES peut chiffrer un fichier, un disque dure et le fichier zip.
  AES utilise le principe de substitution et de permutation ; il possède une grande clé secrète comparativement plus sécurisée et à une vitesse plus rapide.

Tableau comparatif de DES et AES

RELATION	DES	AES
Base	Bloc de données divisé en deux	Bloc de données comme une matrice unique
Principe	Les travaux de DES sur la structure de Feistel Cipher	Substitution et permutation
Nombre de bits par clé	64 bits	128,192,256bits
Taille de la clé	Plus petite	Plus grande

Le nom de ronde	Permutation d'expansion,XOR ,S-BOX ,P-BOX,XOR et SWAP	Subbytes, Shiftrows,Colonnes Mix,Addroundkeys
Rondes	16tours	10tours pour 128 bits 12tours pour 192 bits 14 tours pour 256 bits
Sécurité	Moins sécurisé	Plus sécurisé
Vitesse	Plus lent	Plus rapide

En définitive DES est l'ancien Algorithme et AES est l'algorithme avancé, plus rapide, et plus sécurisé que DES.

En cryptographie, un mode d'opération est une façon de traiter les blocs de texte clairs et chiffrés au sein d'un algorithme de chiffrement par bloc. De nos jours il existe des modes d'opérations qui associent chiffrement et authentification de manière efficace.

Il existe plusieurs modes de chiffrement par bloc, certains sont plus vulnérables que d'autres:

- Le dictionnaire de code (Electronic Code Book, ECB)
- Enchainement des codes (Cipher Bloc Chaining, CBC)
- Chiffrement à rétroaction de sortie (Output FeedBack,OFB)
- Chiffrement rétroaction (Cipher FeedBack,CFB)
- Chiffrement avec vol de texte (CipherText Stealing ,CTS)
- Chiffrement basé sur un compteur(CounTeR,CTR)
- Compteur avec CBC-MAC
- EAX (inventé par David Wagner et al.)
- CWC

- **CHIFFREMENT PAR FLOT (STREAM CIPHER) :** il parvient à traiter les messages de taille quelconque et n'a pas besoin de les découper par blocs. Le chiffrement par flux utilise une clé symétrique et de nombres pseudo-aléatoire, à partir de ça on va pouvoir générer une ou plusieurs clés et chaque clé sera utilisée pour chiffrer un ou un petit groupe du bit du message. Cependant il existe quelques méthodes de chiffrement par flux à savoir RC4, A5 qui sont considérées comme non fiables car plusieurs attaques ont été retrouvées sur leurs algorithmes.

- **CHIFFREMENT ASYMÉTRIQUE** : c'est un chiffrement qui utilise deux clés différentes une pour chiffrer et l'autre pour déchiffrer. Il faut noter que chaque participant possède deux clés, l'une pour chiffrer appeler clé publique qui est connue de tout le monde et l'autre pour déchiffrer appeler clé privée qui doit être connue que par celui qui l'a possédé.

Ces clés sont des très grands nombres en général compris entre 2048 et 4096 bits ayant une certaine propriété mathématique. Par exemple si A et B veulent communiquer, A envoie un message à B et chiffre avec la clé publique de B on ne peut déchiffrer le message qu'avec clé privée de B et non avec celle de A et vice-versa.
Ce procédé assure la confidentialité de l'échange c'est-à-dire être sûr que A et B sont les seuls à échanger.
Et on ne peut pas retrouver la clé privée à partir de la clé publique. Le seul problème c'est au niveau de la transmission de la clé publique si une personne se positionne entre A et B se fait passer pour l'un d'eux et donne sa clé publique à la place. Cela inclus à l'attaque du « man in the middle » donc pour éviter l'attaque du « man in the middle », il faudrait pouvoir certifier l'identité du porteur de la clé qui est le rôle du certificat.
Comme par exemple dans un site web le client obtient la clé publique d'un site web à partir du certificat TLS ou SSL de ce site web et l'utilisera pour initier une communication sécurisée, le site web garde la clé privée secrète car le
https se repose aussi sur le chiffrement asymétrique.

Le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) est un protocole utilisé pour établir une connexion sécurisée entre la machine et le serveur, le certificat SSL ou TLS affiche les informations importantes pour vérifier le propriétaire d'un site web et chiffrer le trafic web avec SSL/TLS.

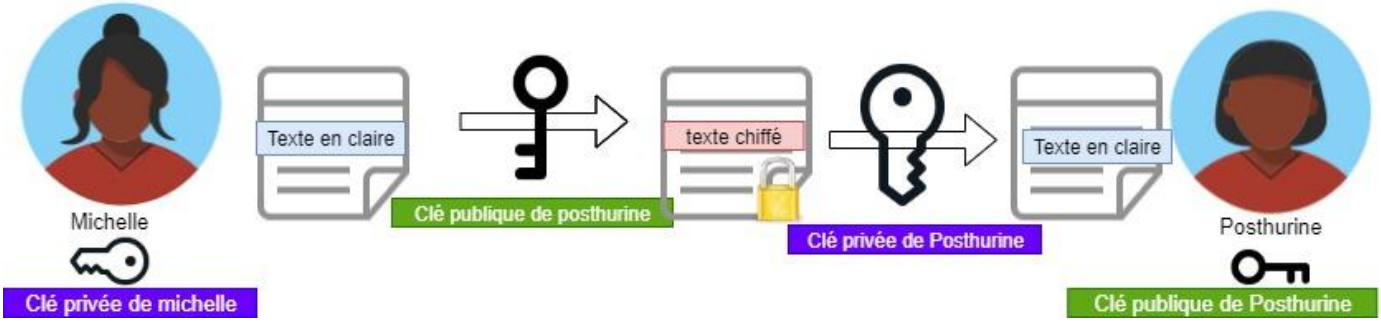


Figure 3 : chiffrement asymetrique

Description du schema

Michelle détient deux clés (privée et publique) elle chiffre le texte en claire avec la clé publique de Posthurine, une fois le message chiffré, Posthurine utilise sa clé privée pour pouvoir déchiffrer le message envoyé par Michelle et vice versa. Pour s'assurer que l'échange entre les deux est confidentiel, Michelle chiffre le message avec sa clé privée et envoi le message chiffré à Posthurine, puis Posthurine déchiffre avec la clé publique de Michelle.

- Le premier système de chiffrement asymétrique: le RSA est basé sur le problème de la factorisation.
  Cet algorithme a été décrit en 1977 par RONARD RIVEST, ADI SHAMIR ET LEONARD ADLEMAN d'où le nom de RSA est tiré.
  LE PRINCIPE DE RSA
  Chaque utilisateur utilise une clé publique (e,n), celle-ci peut être partagée par tout le monde, elle sert à chiffrer le message envoyé et chaque utilisateurs possède une clé privée (d,n) qui sert à déchiffrer le message reçu. Nous pouvons dire le prince RSA est similaire à celui du chiffrement asymétrique.
  Le déroulement du principe : choisir p et q deux nombre impairs distincts avec n=p*q appelé module de chiffrement, $\phi(n)=(p-1)(q-1)$ c'est la valeurs de l'indicatrice d'EULER en n. comme e est premier avec ϕ (n) d'après le théorème de Bachet-Bézout il existe deux entiers d et k tel que $e*d=1+k\ \phi(n)$ c'est-à-dire $e*d=1(\text{mod } \phi(n))$.
  Le chiffrement du message M est un entier, représente le message :
  $M^e=C \text{ (mod n)}$
  Le déchiffrement du message pour déchiffrer C en utilise d, l'inverse de e modulo (p-1) (q-1) et on retrouve le message en clair M, $M=C^d \text{ (mod n)}$.

Nous pouvons dire que le chiffrement symétrique utilise une même clé pour chiffrer et déchiffrer les messages mais malheureusement il n'est pas fiable et risque de divulguer et compromettre potentiellement les messages chiffrés tandis que le chiffrement asymétrique s'appuie sur deux clés (privée et publique) pour chiffrer et déchiffrer les messages, il est fiable.

- Le deuxième système de chiffrement asymétrique : EL GAMAL est basé sur le problème du logarithme discret.

2. SIGNATURE NUMERIQUE :

C'est un processus sécurisé généralement via la cryptologie. Pour ce faire, on a besoin du mécanisme supplémentaire du fonction d'hachage c'est une fonction mathématique à sens unique qui permet à partir d'un message en clair de générer un haché. il existe plusieurs principales fonctions de hachage mais les plus utilisées sont MD5 et SHA.

En général, la signature manuscrite permet de prouver l'identité de l'auteur et d'être en accord avec le contenu du document, le problème est que la signature doit être unique sur tous les documents à signer et est moins fiable tandis que la signature numérique diffère car elle est authentique, aussi elle n'est pas réutilisable, est inaltérable, elle ne peut être falsifiée et reniée(non -répudiation). Elle ressemble à une suite de nombre associés à un fichier et à la personne à l'origine de la signature. La signature avec ses codes et ses cryptages n'est d'ailleurs pas nécessairement visible sur le document.

La signature numérique présente de nombreux avantages pour les entreprises qui sont : la suppression de l'archivage papier, les documents peuvent être conservés au format numérique, chaque document peut être envoyé par mail, moins de déplacements et gains de temps.

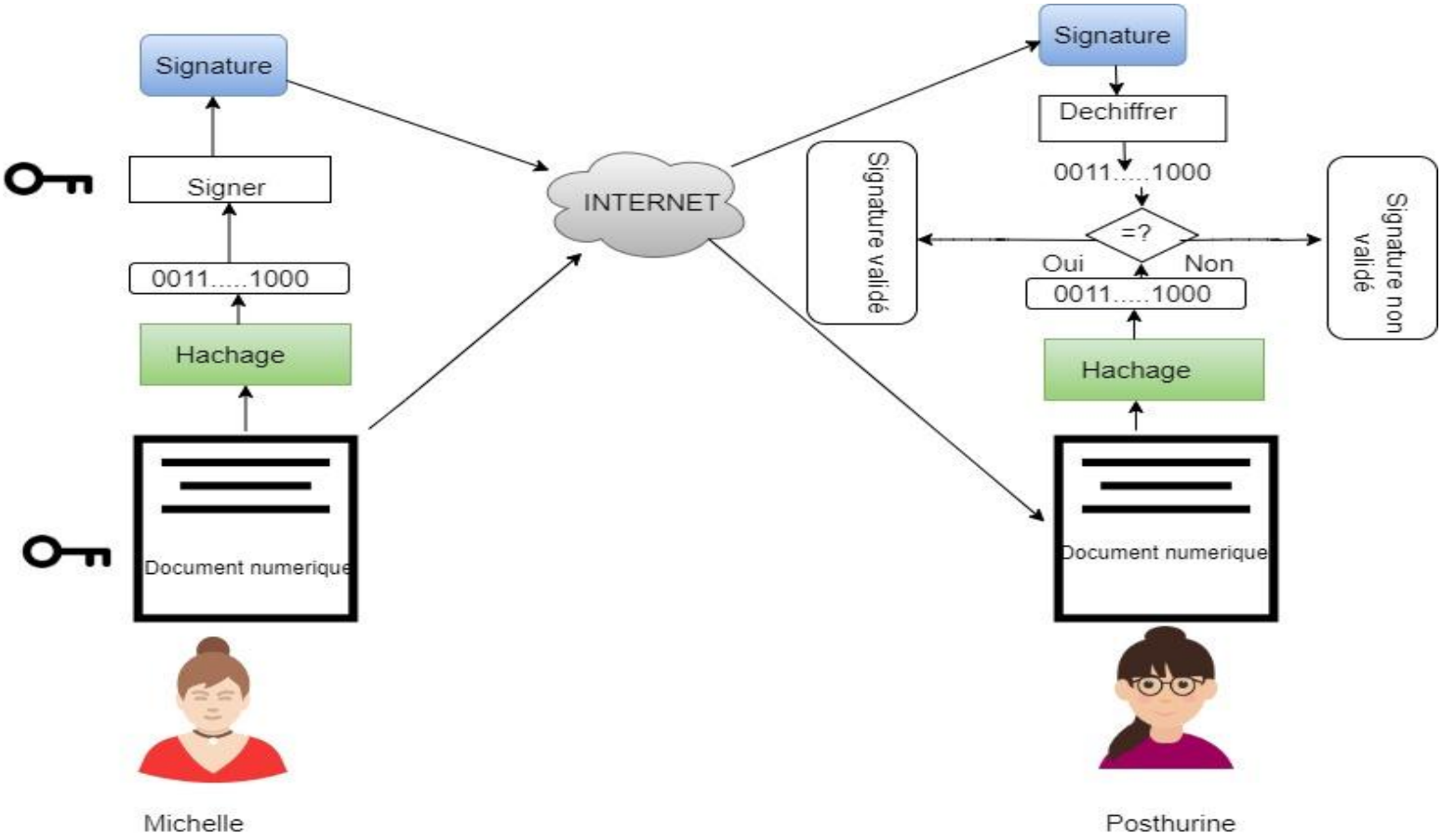
On peut dire que la signature numérique nous permet : d'approuver les documents ou l'authentification, de garantir l'identité du signataire, et de garantir l'intégrité des documents.

Comme par exemple, les échanges entre Michelle et Posthurine nous permettront de chiffrer et de signer un message à l'aide de l'algorithme de RSA :

- Avec une paire de clés (privée/publique), Michelle peut créer une signature numérique de son message certifiant que c'est bien elle qui a créé le message. Pour ce faire, Michelle passe le message à transmettre dans une fonction de hachage afin de créer une empreinte unique du message.
- Michelle chiffre cette empreinte avec sa clé privée afin d'obtenir la signature numérique de Michelle pour le message à transmettre. La clé privée de Michelle étant unique et non diffusée, elle est la seule à pouvoir obtenir cette signature.
- Une fois le message signé, Michelle envoie ce message et la signature à Posthurine. Michelle peut aussi chiffrer le message avec la clé publique de Posthurine afin d'assurer la confidentialité du message.
- Pour vérifier la signature numérique de Michelle, Posthurine fait passer le message reçu dans la même fonction de hachage que Michelle.

- En parallèle, elle déchiffre la signature de Michelle avec la clé publique de Michelle.
- Les deux actions précédentes lui permettent d'obtenir deux empreintes, celle du message reçu et celle du message envoyé par Michelle. Si les deux empreintes sont égales alors c'est le message original écrit par Michelle. Sinon, il y'a problème.

Figure 4 : signature numerique



3. MOT DE PASSE

Le mot de passe est la seule protection qui existe entre les hackers et nos informations sensibles (compte bancaire, fichier privé, etc.). Certains utilisent les ordinateurs capables de générer les millions de mots de passe jusqu'à ce qu'ils trouvent le bon et si l'on possède déjà les informations vous concernant, leur tâche est simplifiée pour pouvoir pirater votre mot de passe. L'utilisation d'un mot de passe s'effectue lorsque l'utilisateur d'un compte bancaire par exemple ou celui des réseaux sociaux souhaite se à un compte donné, l'entité passe par un identificateur d'utilisateur (login) et un mot de passe pour pouvoir accéder à son compte, la sécurité réseau ne peut pas se limiter par un identificateur, il faut protéger ses données à travers un mot de passe. Une enquête du centre de cyber sécurité nationale de royaume unis (NCSC) nous montre que 23,2 millions de personnes utilisent ce mot de passe *123456*, plusieurs internautes négligent

l'importance du mot de passe. La gestion du mot de passe doit être accompagnée de la gestion stricte des accès. Choisir un mot de passe solide reste indispensable lorsqu'il s'agit de protéger ses données.

En tant que responsable de sécurité informatique nous devrons porter une attention particulière sur le protocole qui transporte les mots de passe et les fichiers qui les sauvegarde, car ce système d'identification sur les réseaux n'est pas fiable, les mots de passe circulent en clair sur les réseaux. Pour y remédier, il faut ajouter le mécanisme de chiffrement.

4. LISTE DE CONTROLE D'ACCES

Une liste de contrôle d'accès (ACL) c'est un filtre qui sert à autoriser ou refuser l'accès d'un réseau. Ces listes de contrôle assurent :

- La limite du trafic réseau pour accroitre les performance réseau.
- Contrôle les flux du trafic
- Fournissent un niveau de sécurité de base pour l'accès réseau
- Filtre les hosts pour autoriser ou refuser l'accès au service sur le réseau, le filtrage des paquets se fait au niveau de la couche réseau et transparent du model TCP /IP.

Le fonctionnement de ces listes de contrôle s'applique sur le trafic entrant et sortant, ce fonctionnement est similaire au pare-feu. Le trafic entrant filtre les paquets entrant dans une interface spécifique avant qu'ils ne soient acheminés vers le chemin de la sortie. Le trafic sortant filtre les paquets après qu'ils aient été routés et ce quelle que soit la sortie.

Il est possible de pouvoir détecter les programmes automatique en essayant tous les mots de passe, ces informations utilisées sont : jeton des droits d'accès, les mots de passe, liste de droit d'accès etc.

5. LE BOURRAGE (STUFFING)

C'est une technique de transmission constantes des données inutiles pour masquer celles qui sont importantes. Autrement dit c'est un flot d'informations ajoutées pour garantir la confidentialité, surtout au niveau du volume de trafic.

Lorsqu' il y'a une attaque de bourrage d'adresse, les ensembles d'adresses de connexions volées d'une entreprise sont nécessaires pour tenter de s'infiltrer aux comptes de diverses autres entreprises. Le bourrage est utilisé à des fins diverses, tel que le remplissage des mémoires tampons ou des trames.

Prenant l'exemples d'un hacker qui pirate une liste de noms d'utilisateurs et leurs mots de passe lors d'une intrusion dans une entreprise et se sert des identifiants pour se connecter au site d'une banque de la place. Il espère qu'une partie des employés de cette entreprise de marque ont également un compte dans cette banque de la place et qu'ils réutilisent les mêmes coordonnées pour les deux services. Pour pouvoir vider leurs comptes bancaires.

6. LA NOTARISATION

La notarisation a pour but d'enregistrer et garder les éléments échangés auprès d'un tiers de confiance et qui peut ultérieurement en garantir et prouver l'exactitude. En outre, avoir les documents notariés signifie qu'on a délégué une personne spécialement autorisée appelée notaire publique disant un témoin pour témoigner la signature d'un document. On parle de l'objet de la notarisation si le contenu, l'origine, la date et la destination d'un message constituent les éléments essentiels, donc dans le Domaine informatique elle atteste l'intégrité et l'originalité des données. De nos jours, la protection contre les faux certificats et les tentatives de répudiation sont des mesures qui font partie de la notarisation et la signature numérique.

IV. CONCLUSION :

En définitive, la sécurité informatique permet la fiabilité et la sureté lors de la communication des informations d'un système à un autre, elle sert à garantir la sécurité des accès des utilisateurs dans des équipements informatiques ainsi que du système lui-même en se protégeant contre d'éventuelles attaques, en identifiant les vulnérabilités et en appliquant des systèmes de cryptage. La sécurité informatique consiste à garantir que les ressources logicielles et matérielles d'une entreprise sont uniquement utilisées comme prévu, grâce à ces objectifs et mécanismes bien établis, car le système informatique représente un patrimoine essentiel de l'entreprise qu'elle convient à protéger. Par exemple, l'usage de la mauvaise sécurisation d'autres appareils connectés au réseau (clé USB, les ordinateurs personnels etc..) sont des points de fragilité du système informatique qui est à la portée des virus.

Malgré tous ces objectifs et mécanismes mis en place le système informatique reste toujours exposé face aux nombreuses menaces qui naissent chaque jour à cause de l'évolution de l'informatique qui est remarquable.

CHAPITRE II
SECURITÉ DES RÉSEAUX INFORMATIQUES

I. INTRODUCTION

Autrefois, les transactions s'effectuaient en présence d'un contact physique pour établir une confiance, dès l'arrivée du cybermonde, cette relation de proximité est rompue, alors, la question qui se pose est : comment établir cette relation de confiance indispensable à la réalisation des transactions à distance entre les personnes qui ne se connaissent pas ? La sécurité des réseaux informatiques a des pratiques, mais aussi les politiques plus adaptées pour surveiller et empêcher l'accès non autorisé à des utilisations abusives. Il faut noter que la sécurité informatique est très importante, car elle permet au personnel d'un entreprise ALPHA la réalisation des différentes taches en faisant intervenir plusieurs composants qui assurent la communication et l'échange de données en toute confiance.
Car depuis plus de 30 ans, internet s'accroit à un rythme immodérée, face à tout cela l'internet se retrouve confronté à des problèmes d'accès aux données, de confidentialité et sans oublier des hackers.
De nos jours ce besoin de sécurité s'applique à des nombreux cas tels que le commerce électronique, le transfert d'un fichier, l'accès à distance, l'accès à certaines parties d'un site contenant des données confidentielles.

II. LA SÉCURITÉ AU NIVEAU DE LA COUCHE DEUX (INTERNET)

La sécurité des réseaux est un concept aussi vieux que la notion même de réseau, mais elle s'est accentuée avec l'apparition d'internet. De nombreuses entreprises se focalisent sur la sécurité en interne tout en oubliant la sécurité en externe, ignorant que celle-ci est très importante.

Vers les année 70, les réseaux informatiques prenaient leur essor, deux modèles distincts ont été fusionnées en 1984 et publiés la même année pour créer le modèle OSI, étant un modèle générique, indépendant du protocole, mais la plupart des protocoles y adhèrent. Quelques années après il y' a eu apparition de model TCP/IP, qui est basé sur les protocoles standards que l'internet a développés. La couche internet permet aux entités paires de soutenir une conversation.

1. DEFINITION D'AUTHENTIFICATION

L'authentification consiste à vérifier l'identité d'un utilisateur, en d'autres termes il consiste à apporter une preuve de notre identité pour que le service auquel il veut accéder puisse lui accorder l'Accès. Dans un serveur, un processus de contrôle valide l'identité et après authentification, il donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé**.** La combinaison de plusieurs de ces méthodes Permet de renforcer le processus d'authentification, on parle alors d'authentification forte qui est censée d'être plus sécurisée. De nos jours quand vous effectuez des commandes en ligne sur un site de E-commerce vous recevrez un code de confirmation par sms ou par mail que vous devrez renseigner sur la page de paiement du site. Les protocoles d'authentification ont chacun leur propre manière d'authentifier un utilisateur ou une machine. Appliquer l'authentification sur internet et bien d'autres outils informatiques n'est pas synonyme d'être à l'abri des hackers. Pour cela, d'autres principes d'authentification ont été appliqués :

Un élément d'information que l'utilisateur connaît (mot de passe, passphrase, etc.)

Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat)

Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (fond de rétine, empreinte digitale, ADN, etc.)

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle internet :

Au niveau applicatif : HTTP, FTP

Au niveau transport : SSL, SSH

Au niveau réseau : IPSEC

Au niveau transmission : PAP, CHAP

2. Différence entre l'authentification et l'identification

L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet répondre à la question : "Qui êtes-vous ?". L'utilisateur utilise un identifiant (que l'on nomme "Compte d'accès", "Nom d'utilisateur" ou "Login" en anglais) qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique. Par contre l'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait. [Référence google]

3. L'authentification sur un réseau

La question que nous allons nous poser est de savoir pourquoi faire une authentification sur un réseau ? le problème majeur sur le réseau c'est le fait d'être exposé aux attaques externes, le réseau est fragile donc il faut sécuriser le réseau par le cryptage et l'authentification, ces deux méthodes devraient être simples pour les personnes connectées et très difficiles à casser. Les mesures adoptées pour protéger le réseau doivent être protégées contre le vol et les incidents divers. Elles doivent être physiquement et logiquement inaccessibles : Pour interdire les postes inconnus, pour placer les postes connus à des endroits spécifiques du réseau (Vlan) de façon dynamique, Pour savoir quelle machine est connectée et où elle est connectée.

4. Les principaux protocoles d'authentification

a) Le fonctionnement de RADIUS

C'est un protocole client-serveur dont le navigateur Firefox est client et le serveur est RADIUS serveur, le protocole RADIUS est conçu pour authentifier les utilisateurs distants d'un serveur avec accès par modem et son importance de nos jours à un large éventail de scénarios d'authentification.
Il est important de noter qui le serveur RADIUS peut faire office de proxy, pour être clair et transmettre les requêtes du client à d'autres serveurs RADIUS.

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- L'utilisateur essaie de s'authentifier soit par une connexion https du navigateur au périphérique via le port 443, soit par le biais d'une connexion utilisant un VPN avec un IPsec. Le périphérique, le mot de passe et le nom d'utilisateur.
- Il Envoie au serveur RADIUS un message crée appelé message de demande d'accès et l'envoie au serveur RADIUS. Le périphérique envoie le secret partagé de RADIUS dans le message. Le mot de passe est toujours chiffré dans le message de demande d'accès
- Le serveur RADIUS s'assure que la demande d'accès provient d'un client reconnu (Firefox). Si le serveur RADIUS n'est pas configuré pour accepter le périphérique comme le client, il ignore le message d'accès et ne réponds pas.
- Si le périphérique est un serveur reconnu par le serveur RADIUS et que le secret partagé est correct, le serveur étudie la méthode d'authentification demandée dans le message.
- Si la demande d'accès utilise une méthode d'authentification autorisée.
- Le serveur RADIUS trouve les informations d'identification dans le message et recherche une correspondance dans la base de données des utilisateurs. Si le nom d'utilisateur et le mot de passe correspondent à une entrée de la base de données, le serveur peut obtenir les informations supplémentaires sur utilisateur dans la base de données (autorisation d'accès distant, appartenance à des groupes, heures de connexion, etc)
- Le serveur RADIUS vérifie si sa configuration comporte une stratégie d'accès ou un profil correspondant à toutes les informations dont il dispose sur l'utilisateur. Si cette stratégie existe, le serveur envoie une réponse
- S'il manque une seule condition ou si le serveur ne trouve pas de stratégie correspondante, il envoie un message de refus d'accès indiquant l'échec de l'authentification. La transaction avec RADIUS s'achève. L'accès est refusé à l'utilisateur.
- Si le message d'accès répond à toutes les conditions précitées, RADIUS envoie un message d'autorisation d'accès aux périphériques
- Le serveur RADIUS utilise le secret partagé à chaque réponse qu'il envoie. Si le secret partagé ne correspond pas. Le périphérique rejette la réponse RADIUS
- Le périphérique lit la valeur de l'attribution « filtrer ID » du message. Il connecte le nom d'utilisateur ayant cette attribut « filtrer ID » pour mettre l'utilisateur dans un groupe RADIUS.
- Le serveur RADIUS peut inclure une grande quantité d'informations supplémentaires dans le message d'autorisation d'accès. Le périphérique ignore la plupart de ces informations, comme le protocole que l'utilisateur est autoriser à utiliser (ppp ou slip par exemple), les ports auxquels il peut accéder, les délais d'inactivité et d'autre attributs.
- Ils s'intéressent uniquement à l'attribut « filtrer ID » (attributs RADIUS 11). « FiltrerID » c'est une chaine de texte que vous configurez pour que le serveur RADIUS l'intègre dans le message d'autorisation d'accès. Le périphérique a besoin de cet attribut pour associer l'utilisateur à un groupe RADIUS. Néanmoins il peut prendre en charge d'autre attributs RADIUS, comme les délais d'expiration de session (attributs RADIUS 27) et d'inactivité (attributs RADIUS 28).

« 2 »

b) Concernant l'utilisation et la pratique des groupes RADIUS

A retenir que RADIUS compte 63 attributs dans sa liste d'attributs et chaque attribut à son code et sa spécification.
Dans votre Firebox, lorsque vous configurez l'authentification RADIUS, vous pouvez définir le numéro d'attribut dans le groupe. Les groupes RADIUS que vous utilisez dans la configuration Firebox sont différents des groupes Windows définis dans votre contrôleur de domaine, ou de tous les groupes pouvant exister dans votre base de données des utilisateurs du domaine.

Un groupe RADIUS est uniquement un groupe d'utilisateurs logique que le Firebox utilise. Assurez-vous de bien sélectionner la chaîne de texte FilterID. Vous pouvez faire en sorte que la valeur de FilterID corresponde au nom d'un groupe local ou d'un groupe de domaine de votre organisation, mais ce n'est pas indispensable. Nous vous recommandons d'utiliser un nom représentatif qui vous permette de vous rappeler comment vous avez défini les groupes d'utilisateurs. Si votre organisation comporte beaucoup d'utilisateurs à authentifier, vous pouvez simplifier la gestion des stratégies de votre Firebox en configurant RADIUS pour qu'il envoie la même valeur FilterID pour un grand nombre d'utilisateurs. Le Firebox rassemble ces utilisateurs dans un même groupe logique afin que vous puissiez administrer facilement l'accès des utilisateurs. Lorsque vous établissez une stratégie qui autorise uniquement les utilisateurs authentifiés à accéder à une ressource du réseau, utilisez le nom de groupe RADIUS au lieu d'ajouter une liste de plusieurs utilisateurs.

Par exemple, quand Michelle s'authentifie, la chaîne FilterID qu'envoie RADIUS est ventes. Le Firebox met donc Michelle dans le groupe RADIUS ventes aussi longtemps qu'elle reste authentifiée. Si les utilisateurs Posthutine et Hardie s'authentifient par la suite, et que RADIUS donne la même valeur ventes FilterID dans les messages d'autorisation d'accès de Posthurine et Hardie, alors Michelle, Posthurine et Hardie font tous partie du groupe ventes. Vous pouvez établir une stratégie qui permet au groupe ventes d'accéder à une ressource.

Vous pouvez configurer RADIUS pour qu'il renvoie une autre valeur de FilterID, pour les membres de votre organisation de support interne. Vous pouvez ensuite ajouter une autre stratégie qui permet aux utilisateurs de support informatique d'accéder à des ressources.

Par exemple, vous pouvez autoriser le groupe ventes à accéder à Internet via une stratégie HTTP filtrée. Ensuite, vous pouvez filtrer leur accès au Web avec WebBlocker.

Une stratégie différente dans Policy Manager peut autoriser les utilisateurs de support informatique à accéder à Internet via une stratégie HTTP non filtrée, afin qu'ils puissent accéder au Web sans le filtrage de WebBlocker. Utilisez le nom de groupe RADIUS (ou les noms des utilisateurs) dans la liste d'une stratégie pour indiquer le groupe (ou les utilisateurs) auxquels cette stratégie s'applique.

« 3 »

c) Kerberos

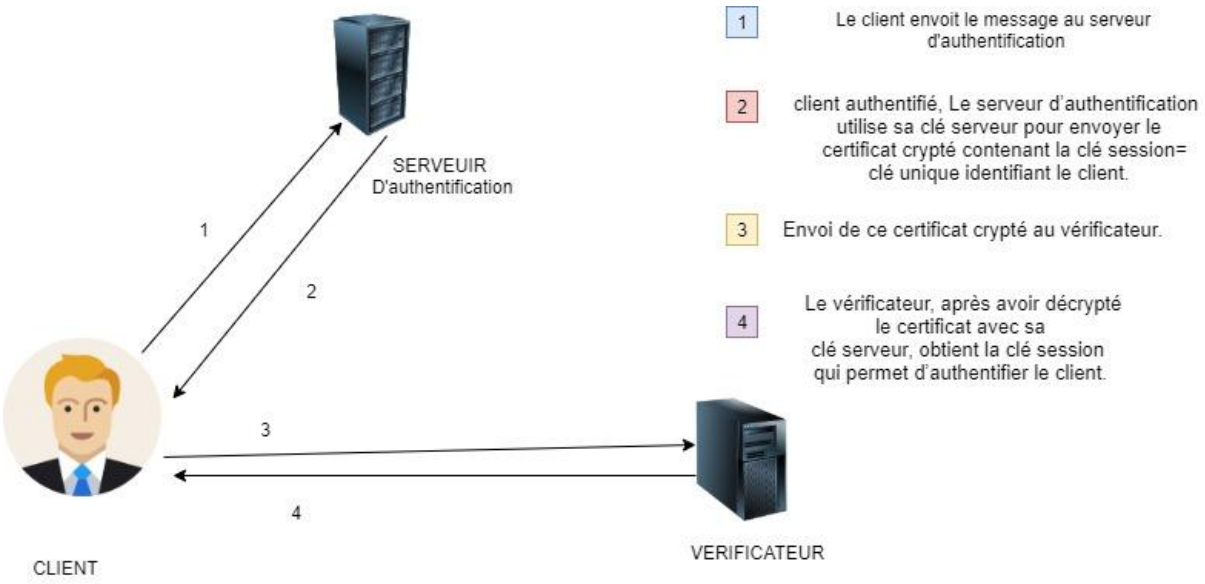
Kerberos est un service distribué d'authentification qui permet à un procédé (un client) à prouver son identité à un vérificateur (un serveur d'application, ou serveur simplement) sans envoyer des données à travers le réseau qui pourrait permettre à un agresseur de les imiter postérieurement.
Kerberos fournit intégrité et confidentialité pour des données envoyées entre le client et le serveur.

« 4 »

- **Fonctionnement de KERBEROS**

Un client veut envoyer un message au serveur d'authentification, le serveur pour s'assurer de l'identité du client, lui demande de s'authentifier. Une fois authentifié, Le client et le serveur possèdent une même clé d'authentification =clé client. Cette clé pour le client est équivalente à un mot de passe, ensuite il pourra envoyer un message d'authentification crypté avec la clé au niveau du serveur et il utilise la clé pour vérifier l'identité du client et si le message est décrypté le client est authentifié ; en d'autres termes pour pouvoir communiquer avec le serveur d'authentification il faut posséder la même clé que lui mais en s'identifiant premièrement.

Le serveur d'authentification envoi au client un certificat crypté (contenant une clé unique permettant d'identifier le client=clé session, et une date d'expiration au-delà de laquelle il ne pourra plus s'identifier) cette clé est connue par le serveur d'authentification et le vérificateur = clé serveur donc le client ne peut pas modifier le certificat puisqu'il ne connait pas cette clé. Alors Le vérificateur, après avoir décrypté le certificat avec sa clé serveur, obtient la clé session qui permet d'authentifier le client.



III. IPSEC

Ipsec (Internet Protocol Security) c'est un protocole de la couche 3 du modèle de OSI développée par un groupe de travail à l'IETF (Internet Engineering Task Force) depuis 1992 pour pouvoir sécuriser le protocole IP (internet Protocol). Conçu à l'origine pour les ipv6. Ipsec offre l'ensemble des services de sécurité attendus sur un VPN :

- Le tunneling : encore appelé transfert de port est un protocole de communication qui permet le transfert de donnée d'un réseau à un autre. La communication s'effectue

d'un réseau privé à travers réseau public appelé l'encapsulation dans ce processus d'encapsulation les paquets de données apparaissent comme s'ils étaient de nature public.

- L'authentification : réside en standard, être sûr de l'adresse origine du paquet grâce au calcul d'intégrité qui est par ailleurs effectué. On peut en outre ajouter à IPSEC des mécanismes de clé partagées voire de certificats ou signature numérique, le certificat et la signature numérique sera davantage dans des réseaux sensibles ou des réseaux constitués d'un grand nombre de sites.
- Le contrôle d'accès : la Security Policy Database (SPD) donne une variété importante de contrôle d'accès grâce aux sélecteurs IP (ceux-ci peuvent contenir en plus des adresses sources et destination le numéro de port du service demandé et autres informations permettant d'étendre le contrôle d'accès).
- Le cryptage des données : la confidentialité est assurée par un chiffrement des données (le chiffrement symétrique ou asymétrique).

IPSEC offre :

- Un contrôle d'intégrité : elle est ajoutée dans chaque paquet IP le résultat d'un calcul de hachage (SHA1 ou MD5) portant sur tout ou une partie de datagramme. Ce calcul est effectué par la source pur être contrôler par le destinataire, le résultat du calcul d'intégrité s'appelle ICV (Integrity Check Value).
- Une protection contre le rejet : le non rejet est attesté par la numérotation des paquets IP et la vérification de la séquence d'arrivée des paquets .la réémission des paquets est automatiquement détectée car son numéro apparait deux fois.

1) Le fonctionnement de IPSEC

Les différents modes de fonctionnement

Le fonctionnement de IPSEC se fait en deux modes

- **Le mode tunnel**

IPSEC ajoute un nouvel entête à un paquet IP (les adresses source et destination sont celles du tunnel et non plus les adresses réelles, ajoute un entête de sécurité spécifique (où figurent le SPI (Security Parameter Index) ainsi que le calcul d'intégrité des données et le séquencement) lorsqu'on utilise un chiffrement des données les adresses sources et destination réelles sont ainsi cachées.

C'est un mode obligatoire dès que le tunnel IPSEC comprend sur ses deux extrémités au moins une gateway (équipement ayant une fonction de routage : routeur ou firewall). C'est le mode utilisé aujourd'hui par IPSEC en attendant l'émergence de la version d'IPSRA (IPSEC Remote Access), qui sécurisera notamment les accès nomades.

2) Le mode transport

Dans ce mode l'entête est également ajouté au paquet IP .la nuance réside dans le fait que dans le mode transport l'entête IP d'origine est utilisée tout le long du canal de transmission même lorsqu'on utilise un chiffrement. Les données sont protégées c'est le mode privilégié

pour le tunneling de bout en bout offert aujourd'hui par des protocoles comme L2TP (protocole de niveau2).

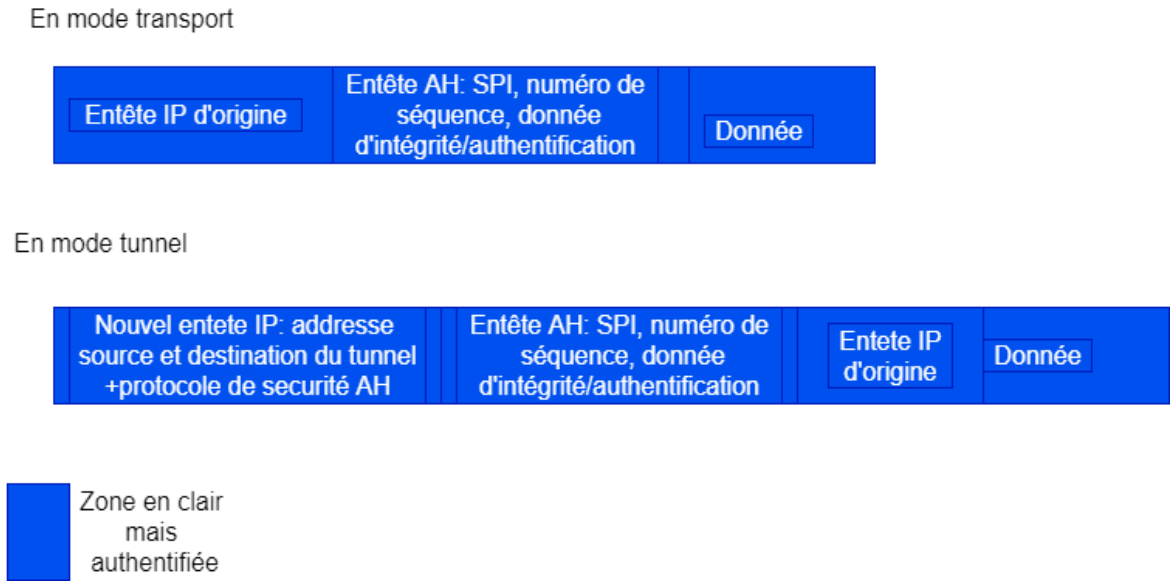
Ces deux modes ont deux protocoles de sécurités

AH (Authentification Hearder) assure l'authentification et l'intégrité des datagrammes IP mais sans cryptage des données. (Pas de confidentialité).

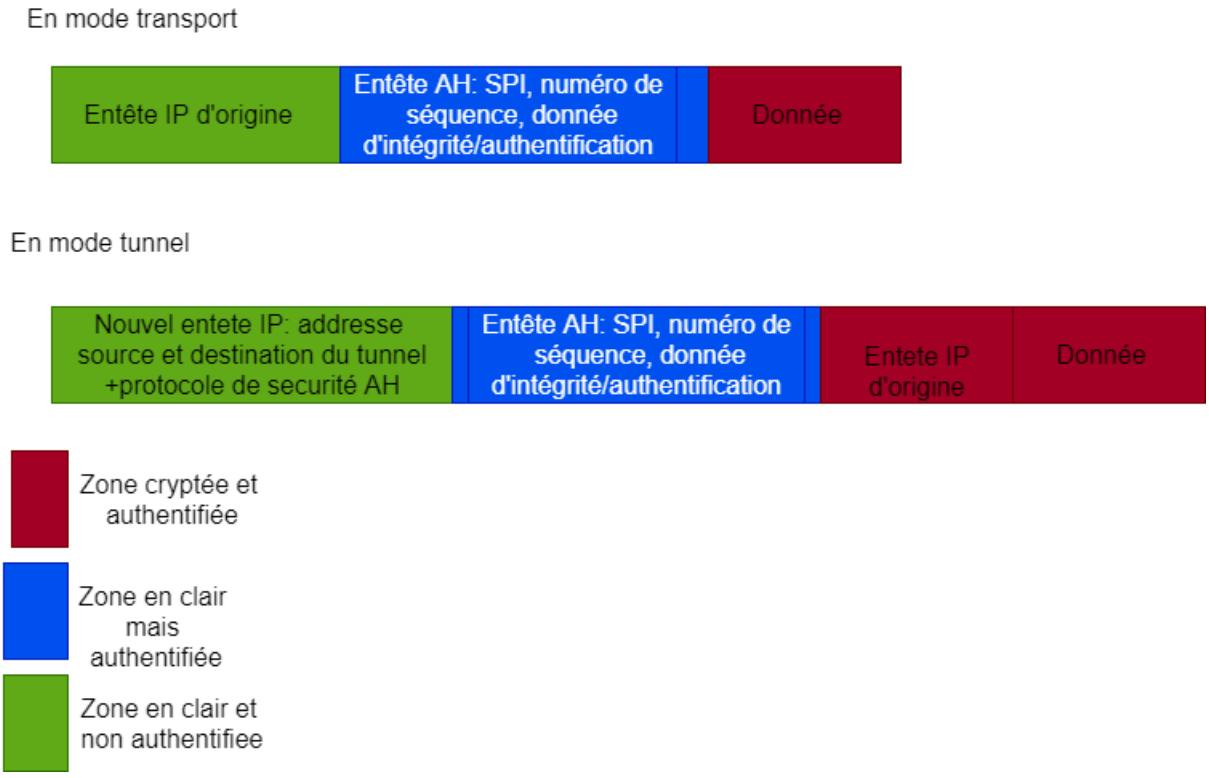
ESP (Encasulated Security Payload) permet le cryptage des données y compris des adresses réelles (mode tunnel)

En générale en mode tunnel on utilise les entêtes AH et ESP (ESP n'authentifie pas de nouvel entête).

AH (Authentification Hearder)



ESP (Encasulated Security Payload)



En combinant le mode d'utilisation et de type de protocole, IPSEC peut couvrir des besoins très variés, comme exemple au niveau d'un pare-feu en mode AH +ESP tunnel pour assurer un réseau privé virtuel entre plusieurs entités ; en mode AH +transport au niveau d'un commutateur d'accès pour avoir une garantie sur l'origine des données reçues d'un utilisateur nomade (cf. IPSRA) « 5 »

Le SAD ,SPD ,IKE

Cf.RFC 20401 pour plus de précisions.

Le protocole IPSEC est basé sur la notion de :

SA (Security Association) qui enferme les paramètres de sécurité (en mode unidirectionnel) propre à une session d'échange de données entre deux extrémités d'un tunnel. La SA comprend le choix en matière de protocole de sécurité (Ahou ESP), cryptage (si mode ESP) authentification hachage, mode tunnel ou transport. Elle contient aussi un champ d'une durée de vie

Une base SPD (Security Policy Database) est présente dans chacune des passerelles de sécurité permettant de traiter d'une part le Traffic entrant dans le tunnel (provenant du client) et d'autre part, le trafic sortant du tunnel (allant vers le client). Cette base est implémentée manuellement par le gestionnaire du réseau. Sur chaque paquet entrant sur une passerelle de sécurité, a la façon d'un firewall ou d'un routeur filtrant on interroge les sélecteurs du paquet (adresse source et destination, protocole de niveau 4, ports utilisés, user ID). Ces sélecteurs pointent sur un enregistrement de la base SPD : celui-ci contient la politique de sécurité à associer au paquet (protocole de sécurité, technique de cryptage, authentification, hachage …).

Ensuite on examine dans la base de SA (SAD) pour savoir si elle peut être configurée automatiquement et si un enregistrement peut être désigné par ces sélecteurs .si ce n'est pas le cas la création de la SA est décidée et est retransmise au travers du protocole IKE vers l'extrémité distant du tunnel.de plus, la SA contiendra un certain nombre de compteurs qui lui son propres : compteur d'antirejet, séquencement et de durée de vie.

Chaque SA possède un identifiant qui lui est propre. Entre deux extrémités, la négociation de la SAA (numéros de SA, définition des clés etc..) s'effectue grâce au protocole IKE " internet Key Exchange "

(RFC 2409) et son dérivé ISAKMP : Internet automatise le rafraîchissement de la clé commune (dans le cas de l'authentification par clé partagée). On peut combiner plusieurs SA : typiquement on peut combiner les modes AH et ASP : on parle alors de « paquet de SA »

Une fois la SA ou le paquet de SA négocié, les échanges de données peuvent s'effectuer : chaque paquet partant de l'origine du tunnel contiendra dans le SPI associé à chaque entête de sécurité (Ahou ASP) le numéro de SA permettant au destinataire (celui dont l'adresse destination du tunnel) d'appliquer la bonne SA ou paquet de SA (authentification, décryptage). Après ces opérations, on vérifie dans la base SAD que les sélecteurs présents dans le paquet IP après décryptage et authentification sont bien en phase avec la SA ou le paquet de SA appliqué pour terminer la vérification, on vérifie que l'enregistrement de la SPD correspondant aux sélecteurs trouvés désigne aussi la SA ou le paquet de SA trouvé.

3) La mise en œuvre d'IPSEC dans VPN

Avec le VPN (Virtual Private Network) il est plus facile et plus efficace de protéger le Traffic internet et de masquer l'identité en ligne. Quand on se connecte avec un serveur VPN sécurisé, le Traffic internet passe à travers un tunnel chiffré dans lequel personne ne peut vous voir.

La construction du VPN doit garantir l'étanchéité du réseau privé virtuel (aucun paquet ne peut passer d'un site client à un autre sans que ces mêmes sites appartiennent au même VPN).

Le VPN à base de tunneling de type LAN to LAN c'est le cas le plus fréquent, pour que deux sites A et B appartenant au même VPN puissent communiquer entre eux, il faudra créer un tunnel entre les routeurs d'accès au backbone (gateway) de ces deux sites.

L'étanchéité des VPN est garantie par Les tables VRF (VPN Routing and Forwarding Instance) implantées dans les routeurs d'accès. Le mécanisme se déroule comme suit:

(Cf. draft-Declercq-bgp-ipsec sur WWW.urec.fr) quand un paquet IP est reçu par le routeur d'accès d'un site donné, le routeur déduit la sous-interface empruntée par le paquet entrant, l'unique table de routage VRF. Cette table de routage ne contient que les routages vers les sites ayant un VPN en commun avec le site entrant. Ceci permet donc d'éviter toute communication entre sites n'appartenant pas au même VPN. Il est important de noter que implémenter l'IPSEC dans le VPN est consommatrice de ressource (la bande passante et le temps de transit dans le gateway IPSEC) notamment lors du calcul des clés IKE.

En conclusion IPSEC est plus sécurisant que les protocoles de niveau2. Il gère facilement une sécurité inter-backbone puisque seules les gateway d'extrémité sont impactées par la sécurisation. IPSEC est flexible et modulaire (administre comme on a vu au niveau de cryptage, et l'authentification plus ou moins élevée) par contre les traitements au niveau des paquets IP (ajout d'information dans le datagramme ; masquage des entêtes en mode tunnel) peuvent s'avérer incompatibles avec les fonctions de translations d'adresses IP¨(NAT)ou d'adressage dynamique

[6]

IV. FILTRAGE ACL

1) Définition

Une liste de contrôle d'accès (ACL) c'est un filtre qui sert à autoriser ou refuser l'accès aux réseaux ou encore une ACL sur un pare-feu ou un routeur filtrant. Une ACL est une liste d'adresses ou des ports autorisés ou interdits par le dispositif de filtrage.
En général Les ACL assurent les tâches suivantes :
Elles limitent les trafics réseaux pour accroître les performances réseaux, elle contrôle les flux de trafic, elles fournissent un niveau de sécurité de base pour l'accès de réseau, elles filtrent les hôtes pour autoriser ou refuser l'accès au service sur le réseau.

2) Le fonctionnement des listes de contrôles d'accès

En générale L'ordre des instructions ACL est important. Cisco IOS teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin. Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées.

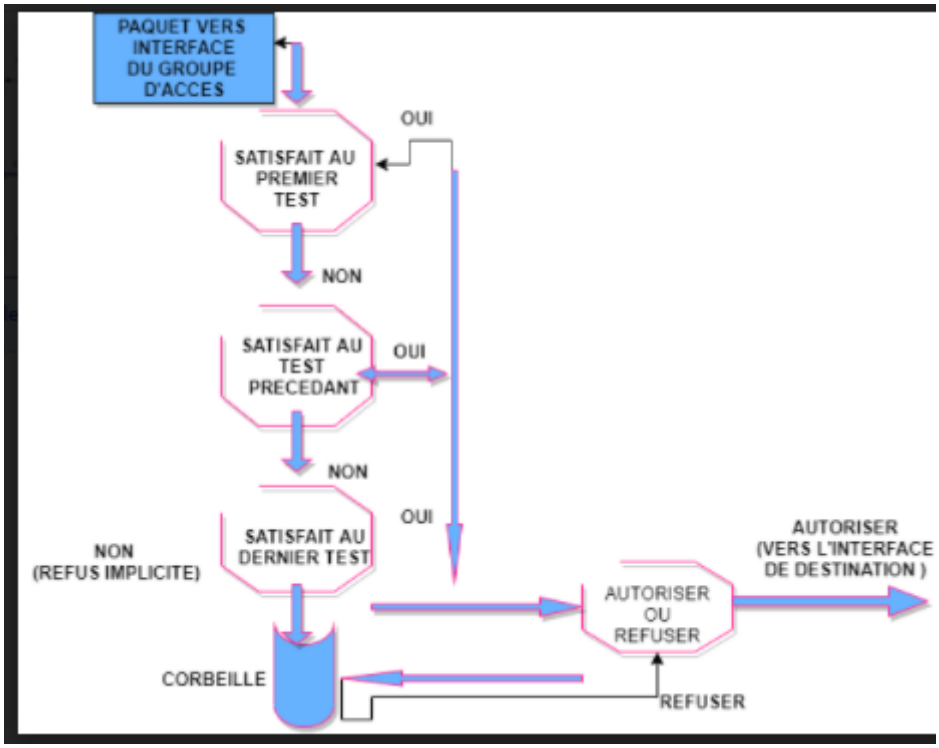
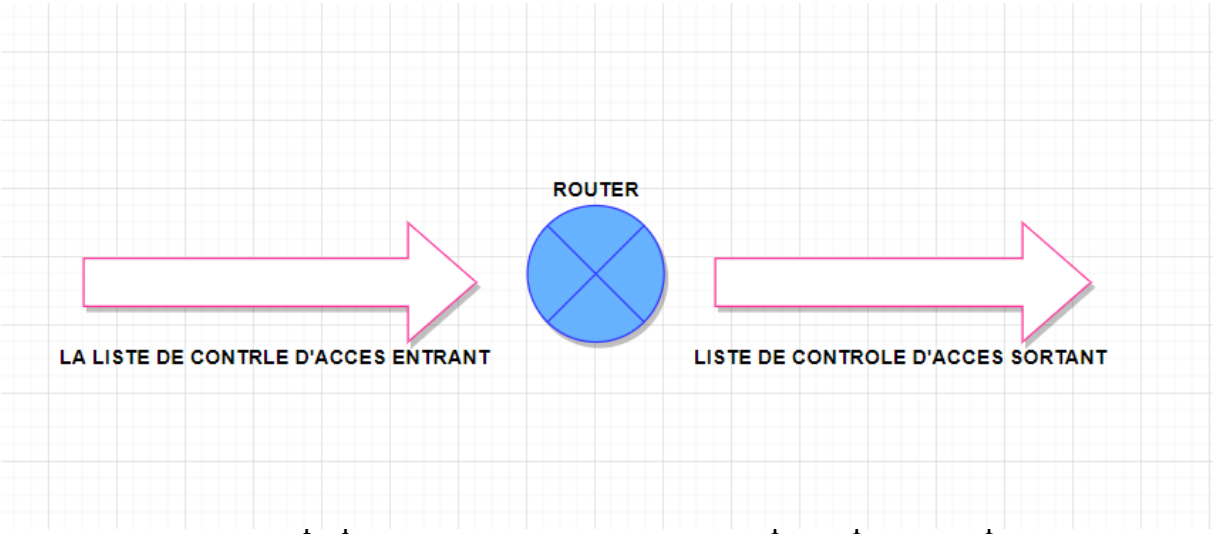


Figure 5 : fonctionnement des listes de contrôles

3) Filtrage des paquets et fonctionnement des listes de contrôles

Le filtrage des paquets se fait au niveau de la couche 3 (réseau) et la couche 4 (transport). Les listes de contrôles d'accès sont configurées pour s'appliquer au trafic entrant et sortant comme le montre la figure suivante :



acheminés vers l'interface de sortie tandis que les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils aient été routés et ce, quel que soit l'interface.

Figure 6 : filtrage des paquets dans ACL

Les principales raisons pour créer les listes de contrôles d'accès sont :

1. De limiter les trafic réseaux, d'augmenter les performances et contrôler le flux de trafic.

2. De fournir un niveau de sécurité d'accès réseau de base, les liste de contrôle d'accès permettent à un hôte d'accéder à une section de réseau tout en empêchant un autre hôte d'avoir accès à la même section.
3. De déterminer le type de trafic qui sera acheminé ou bloquer au niveau des interfaces routeur.
4. D'autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

4) Type de liste de contrôle d'accès IPV4 Cisco

Les ACL IPV4 sont divisées en trois grandes catégories : les liste standard et étendues.

- ACL standard, ne contrôle que deux ensembles : l'adresse IP source et une partie de l'adresse IP de destination au moyen de masque générique. Autrement dit les listes de contrôle standard peuvent d'être utilisées pour autoriser ou refuser le trafic uniquement depuis les adresses IPV4 source. Par exemples l'attribution d'un numéro en fonction du protocole à traiter de liste de contrôle d'accès IP standard est de la plage 1 à 99 et 1300 à 1900. Généralement les liste de contrôle d'accès Standard sont placées près de la destination.
- ACL étendu contrôle l'adresse IP de destination, la partie de l'adresse de destination (masque générique), le type de protocole (TCP, UP, ICMP, IGRP, IGMP, etc.), le port source et de destination, les flux TCP, IP TOS (type of service) ainsi que les priorités IP. L'attribution d'un numéro en fonction du protocole à traiter de liste de contrôle d'accès IP étendu est la plages 100 à 199 et 2000 à 2699. Généralement les liste de contrôle d'accès étendu sont placées près de la source.
- ACL la nommée-étendue est une ACL étendue à laquelle on a affecté un nom.

Les liste de contrôle d'accès standard et étendues et leurs listes d'instructions peuvent être identifiées par un numéro ou par un nom.

V. SSL /TLS

SSL (Secure Socket Layer) c'est un protocole de sécurité internet, il est basé sur le chiffrement, développé pour la première fois par Netscape en 1995 pour pouvoir garantir la confidentialité l'authentification et l'intégrité des données sur internet. SSL a été renommé par TLS (Transport Layer Security) suite à des discussions entre Netscape et IETF (Internet Engineering Task Force) ils ont eu un point d'entente de remplacer SSL par TLS.

En effet lorsque nous nous connecterons sur le site de notre banque par exemple, la connexion se fera toujours en https pour des raisons de sécurité. Que se passera-t-il si la communication est en http ? toutes les informations échangées transiteraient en clair (mot de passe, informations personnelles), toute personne malveillante pourrait voir vos conversations et pourrait les intercepter. Le https est une connexion http (HyperText Transfer Protocole) dans un tunnel chiffré SSL/TLS ce tunnel sert à sécuriser vos échanges, même si cette personne malveillante pouvait intercepter vos informations qui sont chiffrées, donc incompréhensibles pour elle.

- **Fonction du chiffrement SSL/TLS**

Le chiffrement consiste à rendre les informations illisibles sur internet par un algorithme de chiffrement et une clé de chiffrement, la clé de chiffrement c'est une donnée en gros, c'est comme une suite de bits qu'on peut voir comme un mot de passe. Cette clé est utilisée par l'algorithme pour chiffrer et déchiffrer les données. Comme nous avons vu précédemment au

chapitre1 où on parle du chiffrement symétrique et asymétrique qui est bien détaillé la redondance nous fera défaut.

SSL/TLS offre une protection point à point pour assurer la sécurité des données pendant le transport.

Un autre avantage clé est l'authentification. Une connexion SSL/TLS en bon état de fonctionnement garantit que les données sont envoyées et reçues par le bon serveur, plutôt que par un « Homme » malveillant. En d'autres termes, il aide à empêcher les acteurs malveillants de se faire passer pour un site à tort.

Parmi les autres avantages de SSL/TLS on y trouve : l'intégrité des données, les connexions SSL/TLS assurent qu'il n'y a aucune perte ou altération de données pendant le transport en incluant un code d'authentification de message, ou MAC. Ceci garantit que les données qui sont envoyées sont reçues sans aucune modification ou altération malveillante.

L'image ci-dessous nous montre comment savoir qu'un site web utilise le SSL/TLS, le Secure veut dire que ce site web est sécurisé. Nous le voyons avec les navigateurs Google, Firefox, Chrome le cadenas vert et le message Secure pour vérifier le certificat, il suffit de cliquer sur le symbole cadenas, l'acronyme HTTPS (HyperText Transfer Protocol Secure) montre que c'est un site web sécurisé.

Un certificat électronique SSL/TLS sert à authentifier l'identité du site web et une connexion sécurisée. Ce protocole de sécurité crée un lien chiffré entre un serveur web et une navigateur web.

Les entreprises doivent ajouter des certificats SSL à leur site Web pour sécuriser les transactions en ligne et sécuriser la confidentialité des informations client.

En résumé Le SSL sécurise les connexions Internet et empêche les criminels de consulter ou de modifier les informations échangées entre deux systèmes. Lorsque vous voyez un petit cadenas à côté de l'URL dans la barre d'adresse, cela veut dire que le SSL protège le site Web que vous visitez.

- **Le fonctionnement du certificat SSL**

Le SSL s'assure que les données transférées entre les utilisateurs et les sites Web, ou entre deux systèmes, sont impossibles à déchiffrer. Il utilise des algorithmes de chiffrement pour brouiller les données pendant le transit, ce qui empêche les cybercriminels de les lire pendant leur envoi. Ces données incluent des informations potentiellement sensibles comme des noms, des adresses, des numéros de carte de crédit ou d'autres informations financières.

Les étapes du certificat

- Un navigateur ou un serveur tente de se connecter à un site Web (par ex. un serveur Web) sécurisé par le SSL.
- Le navigateur ou le serveur demande au serveur Web de s'identifier.
- Le serveur Web envoie alors au navigateur ou au serveur une copie de son certificat SSL.
- Le navigateur ou le serveur vérifie qu'il peut faire confiance au certificat SSL. Si c'est le cas, il le signale au serveur Web.
- Le serveur Web renvoie alors un accord signé électroniquement pour commencer une session SSL chiffrée.
- Les données chiffrées sont partagées entre le navigateur ou le serveur et le serveur Web.

Ce processus est parfois appelé « SSL handshake » ou « négociation SSL ». Cette procédure peut sembler compliquée, mais elle se fait en quelques millisecondes.

Nous déduisons que pour avoir un site web sécurisé, il faut avoir un certificat électronique SSL/TLS, une URL HTTPS, et un cadenas qui marque la sécurité des sites.

VI. CONCLUSION

Aujourd'hui la sécurité est considérée comme la première des libertés. En dépit de ce qui vient d'être évoqué, nous pouvons dire qu'appliquer la politique de sécurité permet une amélioration de la gestion du système informatique dans les entreprises, car elle contribue à l'instauration d'un environnement propice, à la naissance d'un monde sécurisé et confiant parce que mettre en place une stratégie de protection contre les intrusions ou avoir une défense proactive sont des points importants vers la sécurisation d'une entreprise, il est nécessaire de protéger d'une manière exhaustive (complète, totale) une entreprise face aux multiples menaces qui empoisonnent nos systèmes et rendent défaillants nos réseaux entreprises.

CHAPITRE III
LES PRINCIPALES ATTAQUES RÉSEAU

I. INTRODUCTION

« En terme de sécurité, les ordinateurs sont un problème, les réseaux une horreur et les utilisateurs une catastrophe » Bruce SCHNEIER (Secrets and lies)

Tout ordinateur connecté à un réseau est potentiellement vulnérable à une attaque. Dans ce chapitre, nous allons découvrir un panorama sur les attaques pouvant affecter un réseau. Les fuites de données, cyberattaques, les logiciels malveillants... Les risques liés à l'exposition ou la divulgation des données sont devenus les principales préoccupations, car les conséquences peuvent être drastiques.

Ces attaques visent souvent les trois composantes les plus importantes d'un système. La couche réseau permettant de lier le système au réseau, le système d'exploitation permettant d'assurer le fonctionnement d'un système informatique et la couche applicative permettant de fournir des services choisis par l'utilisateur. Avec la vulgarisation de l'internet, tous les réseaux ainsi que leurs composants sont donc exposés à des risques d'attaque.

Nous allons au courant de ce chapitre vous présenter les faiblesses les plus courantes et étayer (appuyer) les mécanismes de ces attaques dans le but d'élucider les dangers qui menacent les réseaux.

II. LES ATTAQUES RESEAU

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait impossible de toute les décrire. Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, erreur de configuration, etc.) à des fins non connues par l'exploitant du système et généralement préjudiciables.
Celles-ci sont plus permanentes sur internet, à raison de plusieurs attaques par minute sur chaque machine connectée. Elles sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire.

On peut communément définir deux grands types d'attaque sur les réseaux : les attaques sur les protocoles de communications, d'une part, et les attaques sur les applications standards, d'une autre.

Les attaques sur les protocoles de communications consistent à profiter des failles des protocoles de communications (IP, ICMP, TCP et UDP pour l'essentiel) ou encore des protocoles utilisés dans un réseau, tels SNMP (Simple Network Management Protocol) pour la supervision ou BGP (Border Gateway Protocol) pour le routage. N'étant pas conçus pour la gestion des problèmes de sécurité, les protocoles réseau n'ont prévu aucun mécanisme d'authentification véritable et subissent des attaques qui s'appuient sur ces faiblesses d'authentification, comme les attaques par fragmentation déni de service, spoofing, main-in-the-middle, etc.

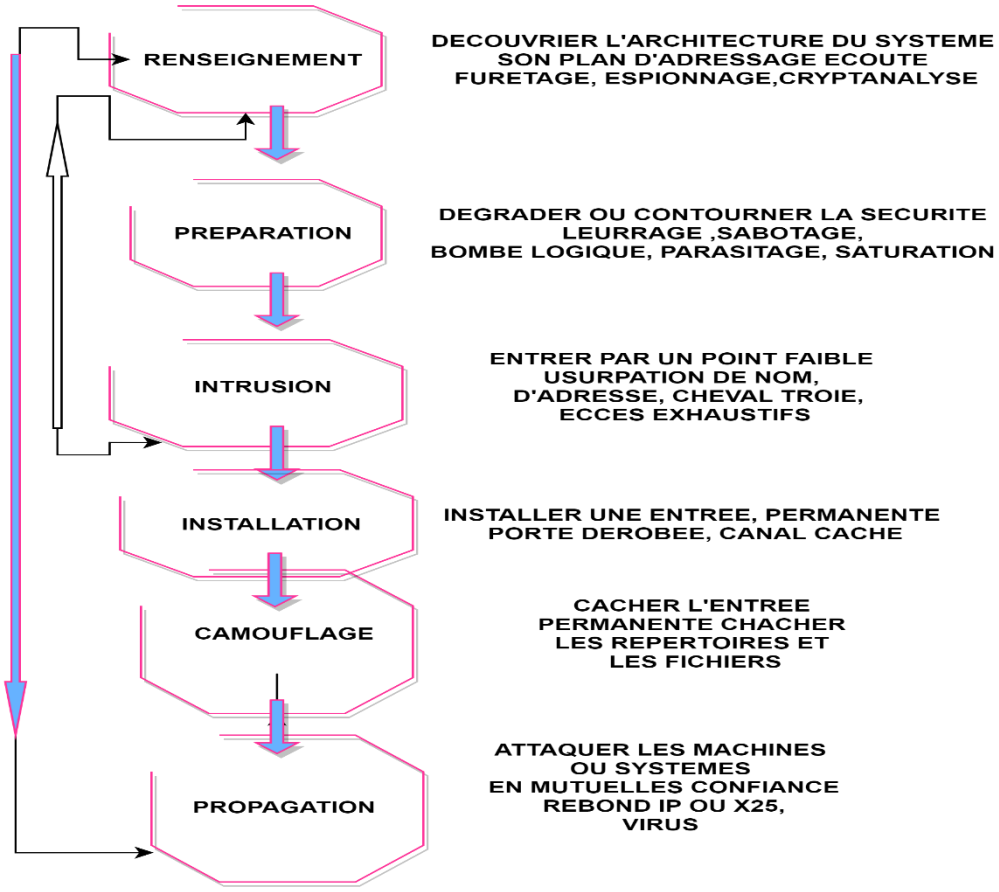


Figure 7: Scénario d'une intrusion

L'autre volet profite des vulnérabilités des applications classiques mises en œuvre dans les Intranets et les Extranets (HTTP, SMTP, FTP…).
On peut également distinguer les attaques sur l'information elle-même des attaques sur les systèmes d'informations.
Alors que dans le premier cas on s'attache atteindre en intégrité / disponibilité / confidentialité aux données traitées par les systèmes (par le biais de virus, d'écoute réseau, de modifications de données…), le second cas de figure vise à se ménager une porte d'entrée dans les systèmes traitant les données (vols de mots de passe, exécution de processus non autorisés, accès illicites aux composants du système d'exploitation…).

1. Les faiblesses des réseaux

Il est impossible de mentionner les attaques sans pourtant évoquer les faiblesses qui les occasionnent. Les faiblesses des réseaux proviennent essentiellement du fait que les protocoles réseaux n'aient pas été conçus avec prise en compte des problèmes sécuritaires dès le départ. À cela se rajoutent les faiblesses issues de l'erreur humaine. Ainsi, on peut classifier les faiblesses réseaux comme suit :

- Faiblesses des protocoles : les protocoles réseaux n'ont pas été conçus pour contrecarrer les attaques de sécurité potentielles, ainsi les protocoles réseaux ne s'appuient pas sur une couche "sécurité" et offrent donc plusieurs vulnérabilités
- Faiblesses d'authentification : la majorité des protocoles ne s'appuient sur aucun mécanisme d'authentification. Ceci facilite les attaques se basant sur l'usurpation d'identité comme IP Spoofing.
- Faiblesses d'implémentation : certains protocoles sont mal implémentés ou mal programmés ce qui offre certaines vulnérabilités exploitables comme TCP SYN ou Ping-of-the-death
- Faiblesses de configuration : beaucoup d'attaques sont dues à l'erreur humaine qui se manifeste par exemple par une mauvaise configuration, comme une mauvaise configuration d'un pare-feu qui laisse passer un flux non autorisé.

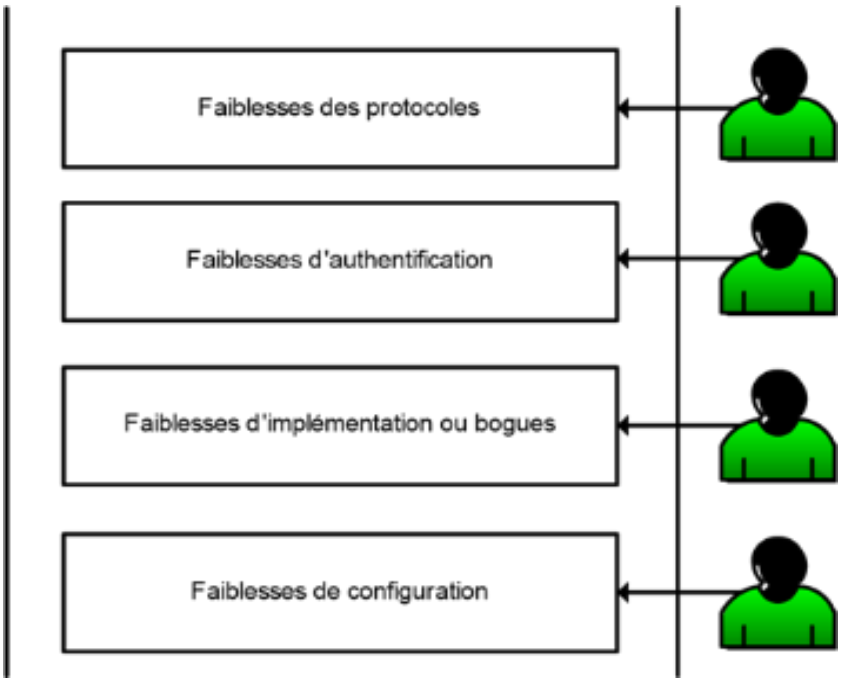


Figure8 : Typologie des faiblesses de sécurité

Nous allons toutefois dresser une classification des faiblesses de sécurité les plus courantes afin de mieux gérer et appréhender ces attaques.

2. Attaques permettant de dévoiler le réseau

a. Attaque par cartographie du réseau

Elles permettent de découvrir les artères de communication d'un futur système cible, en utilisant des outils de diagnostic tels que traceroute (ou Tracert sur Windows). Traceroute utilise l'option TTL (Time-to-Live) du paquet IP pour émettre un message ICMP time_exceeded pour chaque routeur qu'il traverse afin de visualiser le chemin suivi par un paquet IP d'un hôte à un autre.

La découverte des routes est une des premières étapes vers une attaque élaborée sur le système cible.

Traceroute envoie des petits paquets de données vers un port cible via un paramètre Time-to-Live (TTL, temps de vie en français). TTL ne traite pas d'unité de temps mais des nombres de sauts (hops) qu'un paquet IP peut couvrir sur Internet. Chaque routeur emprunté décrémente le TTL automatiquement de 1. Afin d'obtenir une réponse de la part de la machine cible, Tracert va envoyer des Pings automatiques (ICMP) tandis que Traceroute envoie lui des paquets UDP (User Datagram Protocol).

Le premier routeur atteint reçoit un paquet avec un paramètre TTL de 1. Lorsque le TTL atteint 0, le routeur ne fait pas suivre le paquet de données mais émet la réponse Time to live exceeded in transit vers la source (sa propre adresse IP). Tracert enregistre ces informations avec toute la durée de transmission et répète le processus avec un TTL incrémenté de 1. Ce mécanisme est répété jusqu'à ce que la destination ou le maximum de sauts (le TTL défini) soit atteint. Le port déterminé envoie le message Port unreachable et termine le protocole de IP Traceroute. En tout, trois paquets sont envoyés à chaque port, ce qui explique pourquoi Traceroute affiche pour chaque routeur aussi trois données de temps de réponse.

Traceroute et Tracert peuvent être très utiles pour résoudre les problèmes de réseau. Ces outils de commande peuvent par exemple donner des informations sur les paquets de données envoyés et voir si ceux-ci empruntent la bonne route. La défaillance d'un routeur peut souvent être entraînée par des chemins de données compliqués ou par la non-arrivée de paquet. Grâce à Tracert, les utilisateurs peuvent déterminer la localisation d'une station lente. Des tables de routage défaillantes peuvent entraîner des cycles de routage. Le protocole Traceroute peut découvrir ce genre de problème si ce même routeur apparaît plusieurs fois.

En utilisant Traceroute ou Tracert, il faut faire attention à ce que certains facteurs tels que les pare-feu ou les chemins d'accès modifiés n'entraînent pas de surcharge du réseau. En effet, ceux-ci peuvent influencer le résultat de la traque des paquets de données. Ainsi, le chemin réel sera affiché et le résultat sera faussé.

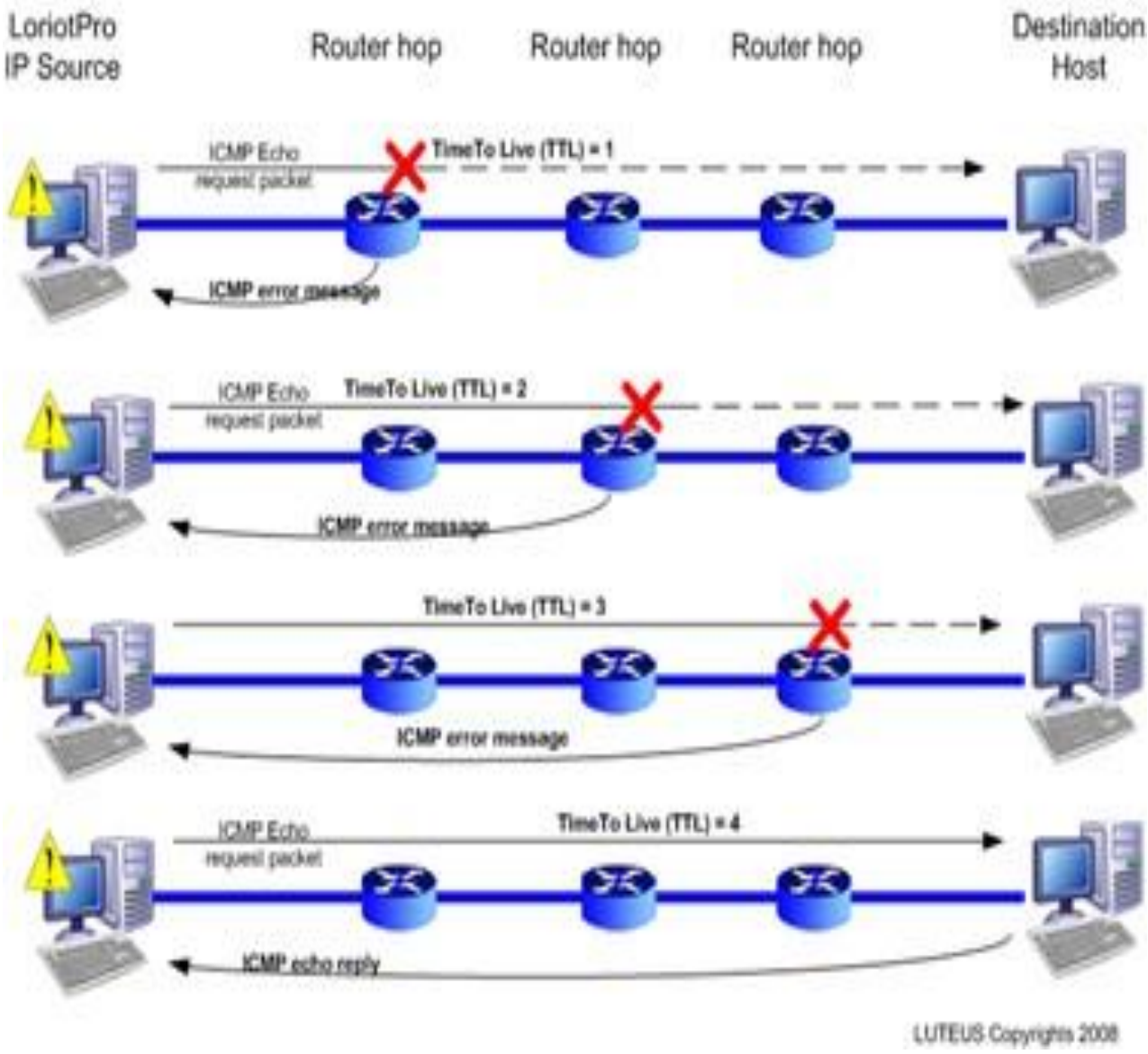


Figure 9 : Dévoilement du routage en utilisant trace-route

b. Attaques par identification des systèmes réseau

Ce type d'attaques vise à identifier tous les systèmes d'un réseau afin de dresser les futurs moyens de pénétration du réseau ou des systèmes qui le composent, Les outils qui ont fait leurs preuves dans le suivi des ports déverrouillés sont appelés balayeurs de ports. Il existe pour cela différentes technique de balayage des systèmes :

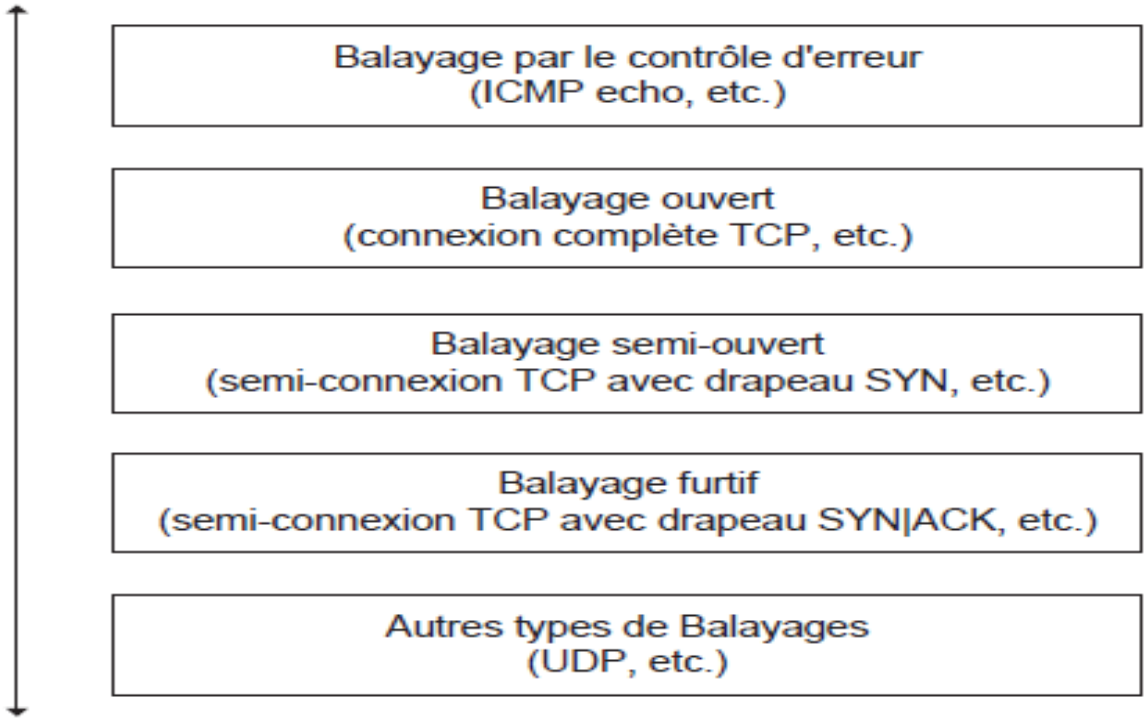


Figure 10 : Les différents types de balayages

- **Attaque par balayage ICMP**

L'utilisation de ICMP echo-request (ping) est la méthode de balayage la plus simple pour avoir la réponse du serveur cible (echo-reply). Elle consiste à utiliser le protocole ICMP et sa fonction request, plus connue sous le nom de ping Pour balayer tous les serveurs dans un réseau. Celle-ci est applicable sur toutes les machines ayant une adresse IP.

- **Attaque par balayage TCP**

Le client envoie une requête TCP SYN vers une adresse IP et Num POrt, s'il reçoit une réponse SYN/ACK alors une application écoute sur le port S'il reçoit RST, ceci signifie qu'aucune application n'utilise ce port. Cette méthode rapide et rusée est similaire au balayage ICMP et elle tente de trouver d'éventuels ports ouverts sur l'ordinateur cible. Ce balayage est rapide car il ne va jamais au bout du handshake TCP en 3 temps. Le scanner envoie un message SYN et note simplement les réponses SYN-ACK. Le scanner n'établit jamais la communication en envoyant le ACK final : la cible est laissée en suspens.

Toute réponse SYN-ACK correspond à des connexions possibles : une réponse RST (reset) signifie que le port est fermé mais que l'ordinateur est actif. L'absence de réponse signifie que SYN est filtré sur le réseau. Toute réponse SYN-ACK offre un moyen rapide aux hackers de trouver leur prochaine cible potentielle.

Si aucune réponse n'est reçue en retour, c'est qu'il existe un équipement filtrant entre le serveur et le client ou qu'il n'y a aucune machine derrière l'adresse IP visée.

Cette technique est cependant si peu discrète, que des variantes ont été élaborées pour améliorer le balayage en jouant sur le principe de fonctionnement de la pile TCP/IP.

c. Attaque par identification des routeurs

On peut dire que L'analyse des trames permet d'échanger, de capturer les mises à jour des tables de routage et d'identifier les routeurs participant au routage du réseau. Elle s'effectue par exemple à travers l'écoute d'un réseau.

Un pirate peut envoyer des requêtes IRDP *(ICMP Router Discovery Protocol*), également appelées sollicitations de routeur (*router solicitations*), vers l'adresse de broadcast afin de connaître la route par défaut du réseau. Il est également possible de lancer des requêtes spécifiques afin de forcer ces mêmes routeurs à répondre. Par exemple, des requêtes peuvent s'appuyer sur une demande *ICMP* de découverte de routeur (*ICMP router discovery*) ou des requêtes de routage (*OSPF, BGP*, etc).

- **Attaques DDOS**

Les pirates ont une manière facile et efficace d'utiliser nos appareils. Ils se servent des botnets (réseau de machine zombies) pour réaliser des attaques DDOS sur les sites web. Nous savons que les routeurs sont des concentrateurs qui gèrent directement le trafic internet d'un réseau, pour une telle attaque, ils constituent la faille idéale pour accéder aux appareils nécessaires. Cette dernière consistant à saturer un serveur de requêtes jusqu'à le rendre indisponible.

d. Attaques par traversée des équipements filtrants

Quand un pirate désire établir la cartographie d'un réseau, généralement il rencontre sur son chemin un équipement filtrant. On y trouve donc des attaques comme :

- **Attaque par modification du port source**

Lorsqu'un pare-feu n'est qu'un simple routeur utilisant des listes de contrôle d'accès (ACL) ou un pare-feu qui ne peut détecter qu'un flux correspond au trafic retour d'une session sortante déjà initiée (le pare-feu est alors dit « *stateful* »), il est possible de passer outre les règles de filtrage appliquées en usurpant (*spoofing*) le port source du paquet émis (*source porting*).

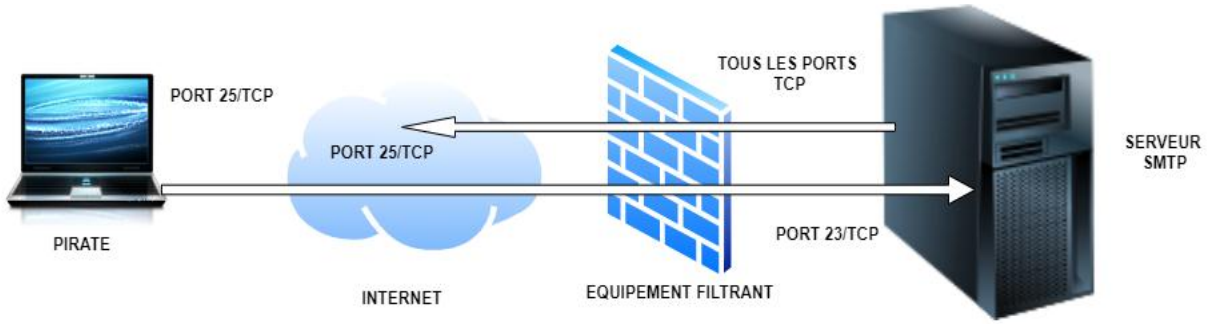


Figure 11 : Traversée d'un pare-feu en fixant le port source

- **Attaques par fragmentation des paquets IP**

Deux techniques permettent de jouer sur la fragmentation des paquets : celle dite par *Tiny Fragments* et celle par *Fragment Overlapping*.

✓ **Attaque par Tiny Fragments**

L'attaque par Tiny Fragments consiste à fragmenter sur deux paquets IP une demande de connexion TCP ou d'autres demandes sur une machine cible tout en traversant et en déjouant (par le mécanisme de fragmentation) un filtrage IP.

Le premier paquet IP contient des données telles que les huit premiers octets de l'en-tête TCP, c'est-à-dire les ports source et destination et le numéro de séquence.

Le second paquet contient la demande de connexion TCP effective (flag SYN à 1 et flag ACK à 0).

Les premiers filtres IP appliquaient la même règle de filtrage à tous les fragments d'un paquet. Le premier fragment n'indiquant aucune demande de connexion explicite, le filtrage le laissait passer, de même que tous les fragments associés, sans davantage de contrôle sur les autres fragments. Lors de la défragmentation au niveau IP de la machine cible, le paquet de demande de connexion était reconstitué et passé à la couche TCP. La connexion s'établissait alors malgré le filtre IP,

✓ Attaque par Fragment Overlapping

L'attaque par Fragment Overlapping consiste à fragmenter deux paquets IP au moyen de l'option Overlapping pour faire une demande de connexion TCP ou une autre demande sur une machine cible tout en traversant un filtrage IP.

Le premier paquet IP contient les données de l'en-tête TCP avec les indicateurs à 0. Le second paquet contient les données de l'en-tête TCP avec la demande de connexion TCP (flag SYN à 1 et flag ACK à 0).[google]

[7]

e. Attaques permettant d'écouter le trafic réseau

- **Attaque par sniffing**

Il est important de savoir qu'un sniffer est un magnifique outil permettant d'étudier le trafic d'un réseau quelconque. De nos jours Malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations confidentielles.

- **Attaque par commutateur**

Compte tenu de nombreux types d'attaques VLAN dans les réseaux commutés modernes. Grace à la simplification des architectures, VLAN permet d'améliorer les performances, elle peut également ouvrir la voie aux excès. Il est primordial de comprendre la méthodologie générale sous-tendant ces attaques et les principales approches permettant de les limiter.

Pour voir le trafic en prévenance d'un autre VLAN, le saut de VLAN permet à un VLAN de le voir, par exemple, l'usurpation de commutateur qui tire parti d'un port trunk configuré de

manière incorrecte. Les ports trunk par défaut ont accès à tous les VLAN et acheminent le trafic de plusieurs VLAN sur une même liaison physique, c'est généralement entre des commutateurs.

En fait, le pirate tire parti du fait que la configuration par défaut du port du commutateur est dynamique dans une attaque de base d'usurpation de commutateur. Il configure un système afin de se faire passer pour un commutateur. Cette usurpation exige que le pirate soit capable d'émuler 802.1Q et les messages DTP. En amenant un commutateur à penser qu'un autre commutateur tente de former un trunk, un pirate peut accéder à tous les VLAN autorisés sur le port trunk.

Désactiver le trunking sur tous les ports, est le meilleur moyen d'éviter une attaque de base d'usurpation de commutateur, sauf ceux qui le requièrent spécifiquement sur les ports de trunking requis, désactivez DTP, puis activez manuellement trunk.

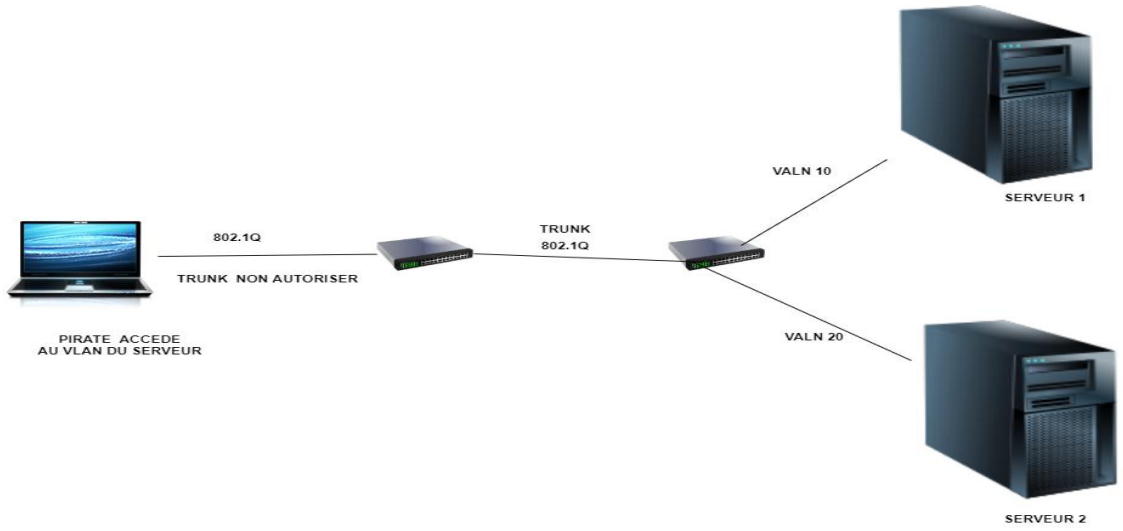


Figure 12 : ATTAQUE VLAN

f. Attaques permettant d'interférer avec une session réseau

Les attaques d'interférence avec sessions réseaux servent à interférer avec des sessions ouvertes par des entités légitimes puis voler leur session. Nous pouvons citer : attaque ARP spoofing qui s'appuie sur le protocole ARP (adress resolution protocol), qui implémente le mécanisme de résolution d'une adresse IP (32 bits) en une MAC (48bits) pour rediriger le trafic réseau d'un ou plusieurs systèmes vers le système pirate.

L'attaque IP spoofing qui a pour fonctionnement de se faire passer pour un autre système en falsifiant son addresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible.

L'attaque de l'homme du milieu ou man-in-the-middle attack (MITM) parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque « homme du milieu » est particulièrement applicable dans la méthode d'échange de clés Diffie-Hellman, quand cet échange est utilisé sans authentification. Avec authentification, Diffie-Hellman est en revanche invulnérable aux écoutes du canal, et est d'ailleurs conçu pour cela.

Attaque ip spoofing

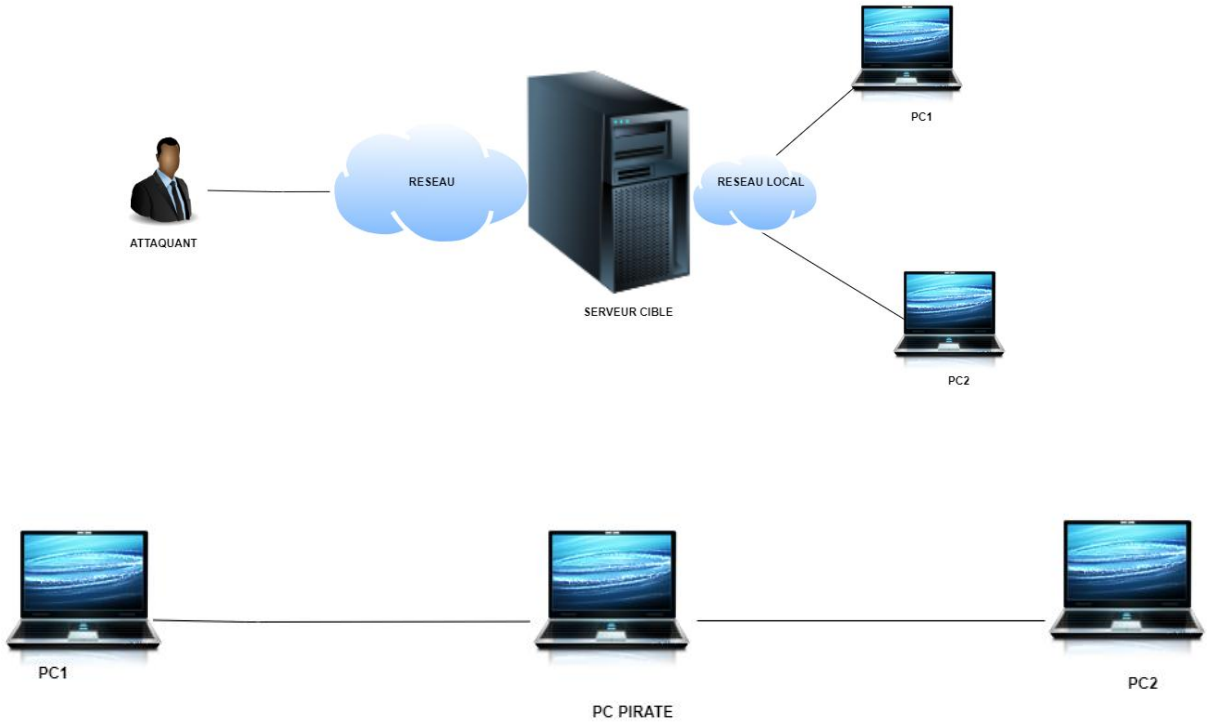


Figure 13 : Attaque man-in-the-middle

g. Attaques permettant de modifier le routage réseau

Dans les premiers grands réseaux, les tables de routage étaient statiques et donc maintenues à jour par des techniciens de bout en bout. De nos jours, les mises à jour des tables de routage et le calcul du meilleur chemin sont automatiquement propagés sur le réseau par les protocoles de routage.

IGP (Interior Gateway Protocol) et EGP (Exterior Gateway Protocol) sont les deux grandes familles de protocoles de routage dans les réseaux IP. Un réseau de routage est découpé généralement en systèmes autonomes, dits AS (Autonomous System). Dans un système autonome, le protocole de routage utilisé est de type IGP. Pour les échanges de routage entre systèmes autonomes différents, le protocole de routage utilisé est de type EGP.

Sachant que toute attaque ou perturbation du routage peut impacter directement la disponibilité du réseau et de ses services, il est primordial de considérer les protocoles de routage comme des éléments-clés de la sécurité d'un réseau. D'autant qu'il est aussi possible de détourner du trafic par le routage à des fins de vol d'information. Par exemple l'Attaques par OSPF (Open Shortest Path First) Le protocole OSPF (Open Shortest Path First) est un protocole de routage de type IGP permettant de gérer les routes internes à un AS. [8]

h. Les attaques des systèmes réseau

Entre le moment où le pirate peut examiner un système cible et celui où il réussit à le pénétrer, un certain nombre d'étapes doivent être franchies. Le pirate doit d'abord découvrir les services réseau offerts par le système, puis estimer l'attrait de chacun d'eux en terme de possibilités de pénétration (risque intrinsèque du service, vulnérabilités, etc.) et enfin faire le choix de ceux qui présentent la meilleure chance de pénétrer le système le plus discrètement possible.

i. Attaques permettant d'identifier les services réseau

Pour y arriver, le pirate doit d'abord déterminer la liste des services disponibles sur le système cible. Il dispose de plusieurs techniques, telles que le balayage de ports, la prise d'empreintes TCP/UDP/ ICMP/IP et l'interrogation de services particuliers.

- ✓ **Attaques par balayage TCP**

Le balayage de ports TCP (ou liste des services) consiste à contacter tous les ports d'un système cible afin de déterminer les services accessibles.

j. Attaque par balayage SYN/ACK

Dans cette attaque, le client envoie directement au serveur un paquet avec les drapeaux SYN/ACK, comme s'il répondait à une demande de session en provenance de cette même machine.

Le serveur répond par un paquet avec le drapeau RST si le port visé n'est pas en écoute. Sinon, le paquet est simplement jeté (dropped) sans qu'une réponse soit renvoyée.

- ✓ **Attaques permettant de prendre l'empreinte réseau du système**

Parmi les informations que doit récolter un pirate, celles concernant le système d'exploitation du serveur visé sont primordiales. Diverses techniques d'attaques d'une efficacité variable permettent d'y parvenir. Grâce aux spécificités des implémentations de la pile TCP/IP de chaque constructeur, il est possible de déterminer avec une bonne précision le système d'exploitation d'un système.

L'empreinte TCP : Lors de l'échange de paquets TCP pour l'ouverture d'une session entre deux ordinateurs, des attributs sont définis par la pile TCP/IP de chaque système d'exploitation. Sachant que chaque implémentation d'une pile IP/TCP est généralement spécifique du système d'exploitation considéré, il est possible de détecter ce dernier par un court échange de paquets TCP.

Exemple : Sondage par les drapeaux TCP. Parce que chaque système d'exploitation a une implémentation unique de la pile TCP/IP, l'échange de messages en faisant varier les drapeaux

TCP permet de constituer une source d'information solide sur le système d'exploitation du système visé.

k. Attaques permettant de pénétrer le système

Les attaques précédentes ne visent qu'à obtenir des informations. Avec ces données, le pirate dispose d'une liste des points d'entrée du système visé, qu'il peut ensuite exploiter pour tenter de le pénétrer.

Les attaques système s'appuient sur divers types de faiblesses, telles que les Faiblesses d'authentification, les Faiblesses de configuration, les Faiblesses des langages…etc.

- ✓ **Ouverture de session**

==> SYN=1 - ACK=0 - SeqNum=100 - AckNum=xxx
<== SYN=1 - ACK=1 - SeqNum=300 - AckNum=101
==> SYN=0 - ACK=1 - SeqNum=101 - AckNum=301

- ✓ **Transfert des données**

==> ACK=1 - SeqNum=101 - AckNum=301 - Data=30 octets
<== ACK=1 - SeqNum=301 - AckNum=131 - Data=10 octets
==> ACK=1 - SeqNum=131 - AckNum=311 - Data=5 octets
<== ACK=1 - SeqNum=311 - AckNum=136 - Data=10 octets

- ✓ **Fermeture de session**

<== ACK=1 - FIN=1 - SeqNum=321 - AckNum=136
==> ACK=1 - FIN=0 - SeqNum=136 - AckNum=321

[10]

III. Comment centrer les attaques

Avec cette crise sanitaire du Covid, de nombreux travailleurs travaillent à distance et oblige chaque salarié à travailler avec des outils personnels (ordinateur, tablette, smartphone…etc.) cela implique qu'ils sont exposés à des nombreuses attaques, nous allons montrer comment centrer ces attaques ou en d'autres termes comment mettre des barrières pour éviter ses attaques.

1) Firewalls

Le pare-feu est une solution pour limiter les attaques provenant d'un réseau public. Il s'active automatiquement lors d'une attaque DDOS.
Le firewall est un élément du réseau informatique il peut être logiciel, matériel ou une combinaison des deux et permet de sécuriser le réseau en définissant les communications autorisées ou interdites. Il permet d'interconnecter deux réseaux ou plus de niveaux de sécurité différents. Par exemple entre un réseau d'entreprise de la zone interne (une zone de confiance fort) et la zone internet (une zone de confiance faible), il sécurise les communications de la zone interne vers la zone internet. Il joue aussi un rôle de sécurité en contrôlant les flux de données qui les traversent que ce soit en entrée ou en sortie, il filtre les

communications et les analyse afin de les autoriser ou les rejeter selon les règles de sécurité en vigueur. Pour bien configurer le pare-feu, il suffit de respecter ces règles :

- Essayez de limiter l'accès à votre réseau à des utilisateurs connus utilisant une adresse IP statique. Vous pourrez ainsi rejeter toutes les autres requêtes venant d'utilisateurs utilisant une adresse IP non autorisée. Vous effectuez de la sorte un filtrage au niveau IP.
- Fermez tous les ports en écoute sur les différents serveurs et ouvrez seulement ceux dont vous avez besoin.
- Filtrez ces ports, c'est à dire rejetez toutes les autres requêtes sur les autres ports que ceux en écoutent.
- Empêchez toutes les connexions sortantes sur des services non autorisés. Pour cela, il suffit de définir un nombre limité de services auxquels les serveurs et les clients peuvent accéder (mail, ftp, web...). Ensuite, il faut configurer le firewall pour rejeter les connexions depuis l'intérieur vers l'extérieur sur des services différents de ceux définis.

2) Antivirus

En informatique l'anti-virus est un programme qui détecte un virus comme son nom l'indique. Tous les fichiers stockés sur un appareil passent en crible, il contrôle l'accès en temps réel, les activités au sein d'un système afin de détecter une menace potentielle. Cette surveillance se fait en trois étapes :
Spécifique, générique, heuristique

La surveillance spécifique repose sur la comparaison des programmes présents dans la machine avec une base de données qui renferme les signatures des logiciels malveillants les plus connus. Si la signature d'un malware est localisée, le dispositif de défense s'active. Ce procédé est aussi appelé scan ou scanning. La signature d'un logiciel correspond à une chaîne de caractères qui le rendent identifiable.

La surveillance générique s'apparente à la surveillance spécifique, mais se concentre sur les variantes des malwares les plus connus. Les meilleurs antivirus intègrent un système de surveillance heuristique, qui offre à la machine une protection contre les virus méconnus. Les virus informatiques étant en constante évolution, la mise à jour régulière des bases de données des antivirus est nécessaire pour conserver une protection efficace.

L'antivirus a pour mission la protection d'un système informatique contre toutes les menaces extérieures. Un logiciel malveillant qui pénètre dans un système non protégé peut avoir de lourdes conséquences comme :

- Une navigation web ralentie
- Une perte totale ou partielle des données, en particulier pour les entreprises qui manipulent des informations confidentielles qui attirent les hackers ;
  - des fichiers corrompus ;
  - des dysfonctionnements divers qui empêchent une utilisation normale et complète de l'appareil ;
  - un risque de propagation du logiciel malveillant vers d'autres machines avec lesquelles interagit la machine de l'utilisateur.

Les menaces proviennent parfois de l'extérieur, des périphériques comme les clés USB. Tous les antivirus n'offrent pas la même protection. Les entreprises utilisent en général des logiciels payants plus aboutis que les programmes gratuits, qui disposent d'un plus grand nombre de fonctionnalités pour une sécurité renforcée. Le recours à plusieurs antivirus pour protéger une machine est déconseillé. Les packages installés se détecteront mutuellement et seront confondus avec des programmes malveillants, une confusion qui réduira le degré de protection de l'ordinateur. [11]

3) Le Nessus

Nessus est un outil de sécurité permettant de scanner une ou plusieurs machines. Il permet aussi de tester différentes attaques pour savoir si une ou plusieurs machines sont vulnérables. Il est très utile lors de tests de pénétration (Pen test) et fait gagner un temps incroyable. Nessus se compose d'une partie serveur (qui contient une base de données regroupant différents types de vulnérabilités) et une partie client. L'utilisateur se connecte sur le serveur grâce au client et après authentification, il ordonne au serveur de procéder aux tests d'une ou plusieurs machines. Le client reçoit ensuite les résultats du test.
Nessus est disponible sous Linux et Windows, et il est entièrement gratuit.

4) Tunneling

Nous allons décrire dans cette section différentes méthodes pour sécuriser vos transactions, c'est-à-dire créer un VPN (Virtual Private Network). Un réseau privé virtuel (VPN) est utilisé pour établir des communications sécurisées en s'appuyant sur un réseau existant non sécurisé. Le principal outil utilisé pour la création de VPN est IPsec.
IPsec est facultatif sur IPv4 mais est obligatoire sur IPv6. IPsec a d'autres avantages que la sécurisation du trafic, il permet par exemple d'économiser la bande passante grâce à la compression des en-têtes des paquets.
IPsec fonctionne sous deux modes différents : le mode transport et le mode tunnel.
IPsec est composé de plusieurs protocoles différents : AH, ESP, IPcomp et IKE. Cette partie de tunneling est bien détaillée au chapitre2.

5) Système de détection d'intrusion réseau, (Network Intrusion Detection System), NID

Il peut détecter en temps réel une attaque s'effectuant sur l'une de vos machines. Il contient une base de données avec tous les codes malicieux et peut détecter leurs envois sur une des machines. Le NIDS travaille comme un *sniffer* sauf qu'il analyse automatiquement les flux de données pour détecter une attaque. Nous avons deux sortes de NIDS :

- **Prelude Hybrid IDS**

C'est l'un des détecteurs d'intrusions les plus connus. Prélude est disponible et libre sur les plateformes Linux, FreeBSD et Windows.
Prélude possède une architecture modulaire et distribuée. Modulaire, car ses composants sont indépendants, et peuvent être facilement mis à jour. Distribuée, car ces composants

indépendants interagissent les uns avec les autres. Cela permet d'avoir divers composants installés sur différentes machines et de réduire ainsi la surcharge d'applications.

Ces différents composants sont les sondes et les managers. Les sondes peuvent être de deux types : réseau ou local. Une sonde réseau analyse tout le trafic, pour y détecter d'éventuelles signatures d'attaques. La sonde locale assure la surveillance d'une seule machine, elle analyse le comportement du système pour y détecter des tentatives d'exploitation de vulnérabilités internes. Les sondes signalent les tentatives d'attaques par des alertes. Ces alertes sont reçues par le manager qui les interprète et les stocke.
Pour une description complète de Prélude (installation, configuration et utilisation) consultez ce document :
[12]

http://lehmann.free.fr/PreludeInstall/InstallPrelude.html

- ✓ ***Snort***

Téléchargeable librement sur www.snort.org, Snort est un NIDS lui aussi. Il n'est pas structuré comme Prélude. C'est un programme "monolithique", il ne comporte pas de module comme Prélude, ce qui peut rendre son implémentation dans un réseau un peu moins souple que Prélude. Snort fonctionne en trois modes (Sniffer, PacketLogger et NIDS). Les deux premiers modes ne sont pas intéressants pour la détection d'intrusions. Le troisième mode permet lui d'analyser le trafic réseau pour y détecter d'éventuelles attaques.
Pour une description complète de Snort (installation, configuration et utilisation) consultez ce site :
http://www.snort.org/docs/ (en anglais). [14]

Ces différentes barrières d'attaques que nous venons de voir nous permettent de détecter les attaques.

IV. CONCLUSION

Pour organiser une bonne défense, il faut connaître les attaques. Cet article a passé en revue les 10 cyberattaques les plus courantes, que les pirates utilisent pour perturber et compromettre les systèmes informatiques. Comme vous avez pu le constater, les attaquants disposent d'un vaste éventail d'options, telles que les attaques DDoS, les infections malveillantes, les interceptions par l'homme du milieu et les cassages de mot de passe par force brute, pour tenter d'obtenir un accès non autorisé aux infrastructures critiques et aux données sensibles.

Les mesures pour atténuer ces menaces varient, mais les principes de base de sécurité restent les mêmes : Mettez à jour vos systèmes et vos bases de données antivirus.

CHAPITRE IV
MISE EN PLACE D'UN RÉSEAU D'ENTREPRISE SECURISÉ PAR LE PAR-FEU ASA

I. INTRODUCTION

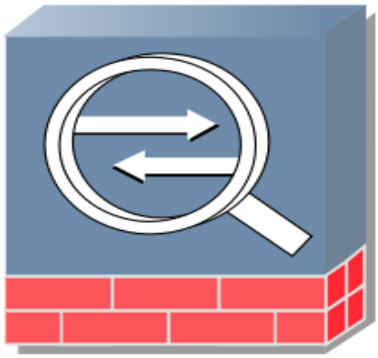
Cisco ASA est l'acronyme de Adaptive Security Appliance, c'est une gamme de pare feu produite par Cisco.
Par définition des dispositifs de sécurité Cisco ASA protègent et filtrent les entrées et sorties des réseaux d'entreprise de toutes tailles. Elle fournit aux utilisateurs un accès très sécurisé aux données où qu'ils soient, en tout temps et avec n'importe quel appareil. Ces dispositifs sont le reflet de plusieurs années de leadership en matière de pare-feu et de sécurité, plus de 1 millions de dispositifs de sécurité déployés dans le monde le démontrent bien.

II. OPTIONS ET FONCTIONNALITES DE ASA

Cisco Adaptive Security Appliance (ASA) Software est le système d'exploitation au cœur de la puissance de la famille de produits Cisco ASA. Ce logiciel procure des fonctionnalités de pare-feu de classe entreprise aux dispositifs ASA dans une variété de dimensions dispositifs autonomes, lames et virtuels. Le logiciel ASA s'intègre aussi à d'autres technologies de sécurité essentielles pour offrir des solutions complètes répondant à une demande de sécurité en constante évolution.
Voici quelques-uns des avantages de Cisco ASA Software :

- Offre des fonctionnalités intégrées en matière de système IPS, de RPV et de communications unifiées.
- Aide les organisations en vue d'accroître leur capacité et leur performance grâce à la mise en grappe
- Procure une haute disponibilité aux applications à haute résilience
- Reconnaît le contexte à l'aide des balises associées au regroupement de sécurité Cisco Trustés et d'un pare-feu fondé sur l'identité.
- Facilite le routage dynamique et le RPV de site à site selon le contexte
- En plus de la fonctionnalité principale de pare-feu ASA, d'autres fonctionnalité sont aussi offertes selon la version du pare-feu utilisée et Les licences adéquates acquise et installée au niveau du pare-feu ASA.
- Un service VPN sécurisé avec équilibrage de charges
- Des service ipsec
- Des interfaces VLAN (100-200)

Le logiciel Cisco ASA prend en charge les normes de cryptage de nouvelles générations, y compris l'ensemble d'algorithmes cryptographiques Suite B. De plus, il s'intègre à Cisco Cloud Web Security pour assurer la protection contre les menaces informatiques provenant du Web.



III. LES OUTILS REQUIS POUR METTRE EN PLACE UN FIREWALL CISCO ASA

Pour mettre en place un réseau virtuel comportant un pare-feu tel que Cisco ASA, il vous faut les éléments suivants :

- Un ordinateur fonctionnant de préférence sous un système 64 bits (en effet la virtualisation est plus facile avec ce type d'architecture
- Un paquet tracer, le logiciel GNS3, le VMware, etc.

En fait pour l'utilisation de ASA dans gns3 il est important d'avoir le fichier de boot d'ASA appelé < initrd.gz>, une image d'un IOS d'un Firewall ASA appelé <wmlinuz>, la configuration de Qemu.

1. PAQUET TRACER

Cisco Packet Tracer est un produit Cisco officiel pour les étudiants de la Cisco Academy qui simule les réseaux Cisco. Il n'émule pas le matériel Cisco et ne prend pas en charge les images réelles de Cisco ou d'autres fournisseurs.

Avantages :

- Facile à mettre en place
- Prend en charge les simulations de routeur, de commutateur et de PC Cisco
- Suffisant pour les études CCNA
- Simule plusieurs appareils et protocoles (routeurs, commutateurs, sans fil, RADIUS, etc...)
- Gratuit (nécessite une inscription sur le site Web NetAcad de Cisco)

Désavantages :

- Code propriétaire - pas open source
- Simule uniquement les appareils Cisco (n'exécute pas de vraies images Cisco)
- Pas de support multifournisseur
- Impossible de s'intégrer avec de vrais appareils physiques

Vous ne pouvez utiliser que les commandes IOS implémentées par les développeurs. Toutes les commandes imaginables disponibles sur une plate-forme simulée dans Packet Tracer ne seront pas présentes pour une utilisation.

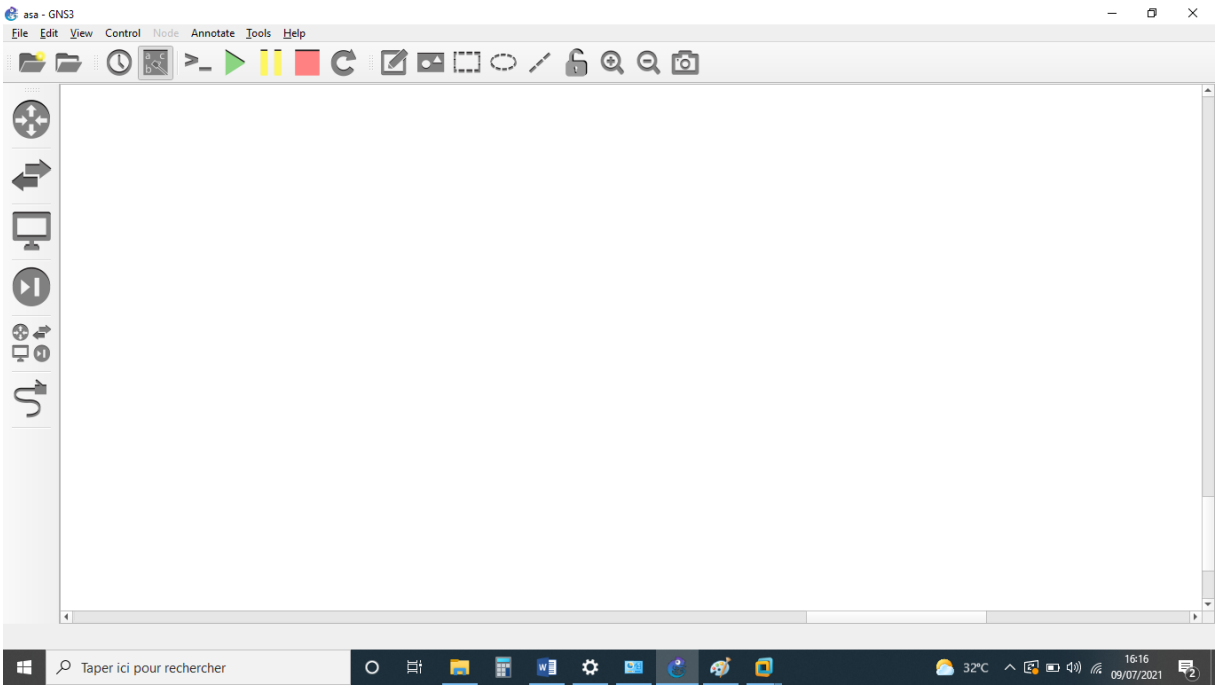
2. GNS3

GNS3 (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. Vous connaissez peut-être avec VMWare ou Virtual Box qui sont utilisées pour émuler les différents systèmes d'exploitation dans un environnement virtuel. Ces programmes vous permettent d'exécuter plusieurs systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type de d'émulation à l'aide de Cisco Internet work Operating Systems. Il vous permet d'exécute run IOS Cisco dans un environnement virtuel sur votre ordinateur. GNS3 est une interface graphique pour un produit appelé Dynagen. Dynamips est le programme de base qui permet l'émulation d'IOS. Dynagen s'exécute au-dessus de Dynamips pour créer un environnement plus convivial, basé sur le texte environnement. [13]

GNS3 est un logiciel libre et gratuit que vous pouvez télécharger à partir de http://gns3.com, il est utilisé par des centaines de milliers d'ingénieurs réseau dans le monde pour émuler, configurer, tester et dépanner des réseaux virtuels et réels. GNS3 vous permet d'exécuter une petite topologie composée de seulement quelques appareils sur votre ordinateur portable, à ceux qui ont de nombreux appareils hébergés sur plusieurs serveurs ou même hébergés dans le cloud.

Il est activement développé et soutenu et compte une communauté croissante de plus de 800 000 membres. En rejoignant la communauté GNS3, vous rejoindrez d'autres étudiants, ingénieurs réseau, architectes et autres qui ont téléchargé GNS3 plus de 10 millions de fois à ce jour. GNS3 est utilisé dans des entreprises du monde entier, y compris des entreprises Fortune 500.
GNS3 peut vous aider à vous préparer aux examens de certification tels que le Cisco CCNA, mais également vous aider à tester et à vérifier les déploiements dans le monde réel. Jeremy Grossman, le développeur original de GNS3 a créé à l'origine le logiciel pour l'aider à étudier pour ses certifications CCNP. En raison de ce travail original, vous pouvez aujourd'hui utiliser pour vous aider à faire de même sans payer pour du matériel coûteux.
GNS3 permet aux ingénieurs réseau de virtualiser de vrais périphériques matériels depuis plus de 10 ans. À l'origine, n'émulant que les appareils Cisco à l'aide d'un logiciel appelé Dynamips, GNS3 a maintenant évolué et prend en charge de nombreux appareils de plusieurs fournisseurs de réseaux, notamment les commutateurs virtuels Cisco, les Cisco ASA, les vRouters Brocade, les commutateurs Cumulus Linux, les instances Docker, les HPE VSR, plusieurs appliances Linux et bien d'autres.
GNS3 existe depuis plus de 10 ans. Certaines informations que vous trouverez sur Internet sont obsolètes ou malheureusement totalement erronées. Ce document vous aidera, espérons-le, à répondre aux questions et vous aidera à démarrer votre voyage avec GNS3.

GNS3 ne prend pas seulement en charge les appareils Cisco. Cisco est souvent évoqué car c'est ce que la plupart des ingénieurs réseau souhaitent découvrir. Cependant, de nombreux autres fournisseurs commerciaux et open source sont aujourd'hui pris en charge dans GNS3. Vous êtes désormais en mesure de tester l'interopérabilité entre de nombreux fournisseurs et même d'essayer des configurations ésotériques utilisant des technologies de réseau avec SDN, NFV, Linux et Docker.



ARCHITECTURE GNS3

GNS3 se compose de deux composants logiciels :
Le logiciel tout-en-un GNS3 (GUI)
La machine virtuelle (VM) GNS3

- **GNS3-tout-en-un :**

Il s'agit de la partie client de GNS3 et de l'interface utilisateur graphique (GUI). Vous installez le logiciel tout-en-un sur votre PC local (Windows, MAC, Linux) et créez vos topologies à l'aide de ce logiciel.
Lorsque vous créez des topologies dans GNS3 à l'aide du client GUI logiciel tout-en-un, les périphériques créés doivent être hébergés et exécutés par un processus serveur. Vous avez quelques options pour la partie serveur du logiciel:
Serveur GNS3 local, VM GNS3 locale, VM GNS3 distante
Le serveur GNS3 local s'exécute localement sur le même PC où vous avez installé le logiciel tout-en-un GNS3. Si, par exemple, vous utilisez un PC Windows, l'interface graphique GNS3 et le serveur GNS3 local s'exécutent en tant que processus sous Windows. Des processus supplémentaires tels que Dynamips seront également exécutés sur votre PC :
Si vous décidez d'utiliser la VM GNS3 (recommandé), vous pouvez soit exécuter la VM GNS3 localement sur votre PC à l'aide d'un logiciel de virtualisation tel que VMware Workstation, Virtualbox ou Hyper-V ; ou vous pouvez exécuter la VM GNS3 à distance sur un serveur utilisant VMware ESXi ou même dans le cloud.
Vous pouvez utiliser GNS3 sans utiliser la VM GNS3. C'est un bon moyen de commencer initialement, mais cette configuration est limitée et n'offre pas autant de choix en ce qui concerne la taille de la topologie et les périphériques pris en charge. Si vous souhaitez créer des topologies GNS3 plus avancées ou inclure des périphériques tels que les périphériques Cisco VIRL (IOSvL2, IOSvL3, ASAv) ou d'autres périphériques nécessitant Qemu, la machine virtuelle GNS3 est recommandée (et est souvent requise).

- **ROLE GNS3**

GNS3 prend en charge les appareils émulés et simulés.
Émulation : GNS3 imite ou émule le matériel d'un appareil et vous exécutez des images réelles sur l'appareil virtuel. Par exemple, vous pouvez copier Cisco IOS à partir d'un routeur Cisco physique réel et l'exécuter sur un routeur Cisco virtuel émulé dans GNS3.
Simulation : GNS3 simule les caractéristiques et fonctionnalités d'un appareil tel qu'un commutateur. Vous n'exécutez pas de systèmes d'exploitation réels (tels que Cisco IOS), mais plutôt un périphérique simulé développé par GNS3, comme le commutateur de couche 2 intégré.
REMARQUE
Les frontières entre simulation et émulation sont un peu floues de nos jours. Vous pouvez désormais exécuter des images Cisco VIRL qui sont des images d'images réelles du système d'exploitation Cisco qui s'exécutent sur du matériel virtuel standardisé. GNS3 émule le matériel dont les images VIRL ont besoin pour fonctionner.
Dynamips est une technologie plus ancienne qui émule le matériel Cisco. Il utilise de vraies images Cisco IOS. Il convient aux topologies de base de type CCNA, mais présente un certain nombre de limitations telles que la prise en charge uniquement des anciennes versions de Cisco IOS (12.X) qui ne sont pas non plus prises en charge ou mises à jour activement par Cisco.
Les images Cisco recommandées à utiliser avec GNS3 sont celles de Cisco VIRL (IOSv, IOSvL2, IOS-XRv, ASAv). Ces images sont prises en charge et mises à jour activement par Cisco. Les images prennent en charge les versions actuelles de Cisco IOS (15.X) et offrent la meilleure échelle et la meilleure expérience utilisateur.

- **AVANTAGE GNS3**

- Logiciel gratuit
- Logiciels open source
- Pas de frais de licence mensuels ou annuels
- Aucune limitation sur le nombre d'appareils pris en charge (la seule limitation est votre matériel : CPU et mémoire)
- Prend en charge plusieurs options de commutation (module Etherswitch NM-ESW16, images IOU/IOL Layer 2, VIRL IOSvL2) :
- Prend en charge toutes les images VIRL (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASAv)
- Prend en charge les environnements multifournisseurs
- Peut être exécuté avec ou sans hyperviseurs
- Prend en charge les hyperviseurs gratuits et payants (Virtualbox, poste de travail VMware, lecteur VMware, ESXi, Fusion)
- Appliance téléchargeables, gratuites, préconfigurées et optimisées disponibles pour simplifier le déploiement
- Prise en charge native de Linux sans avoir besoin d'un logiciel de virtualisation supplémentaire
- Logiciels de plusieurs fournisseurs disponibles gratuitement

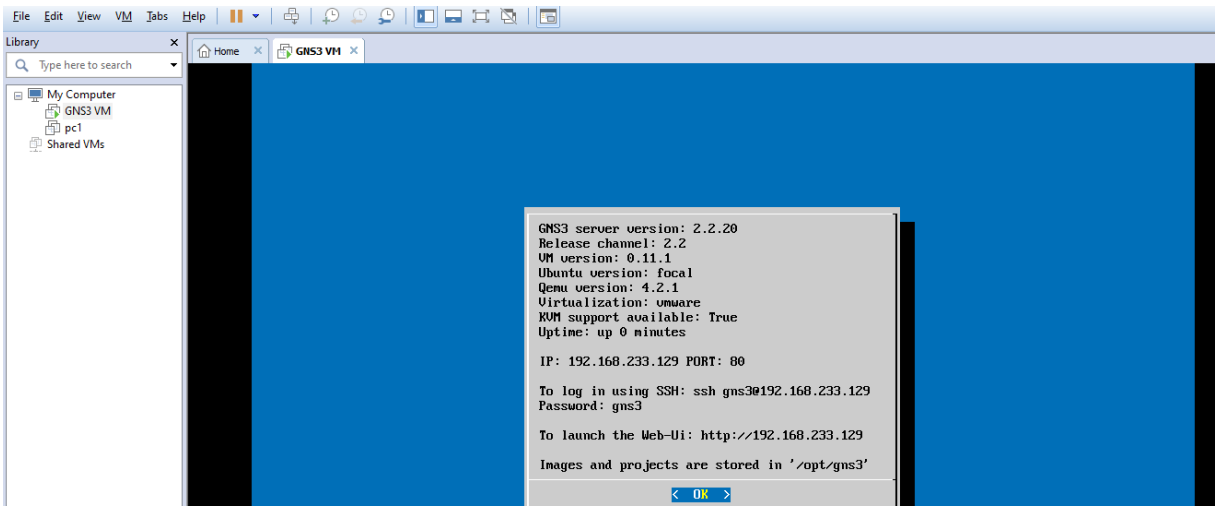
Grande communauté active (plus de 800 000 membres)

- **DESAVANTAGES GNS3**

Les images Cisco doivent être fournies par l'utilisateur (téléchargement depuis Cisco.com, ou achat d'une licence VIRL, ou copie depuis un périphérique physique).
Pas un package autonome, mais nécessite une installation locale de logiciel (GUI).
GNS3 peut être affecté par la configuration et les limitations de votre PC en raison de l'installation locale (paramètres de pare-feu et de sécurité, politiques d'ordinateur portable de l'entreprise, etc.). [15]

3. VMWARE WORKSTATION PRO

VMware Workstation Pro est la norme de l'industrie pour l'exécution de plusieurs systèmes d'exploitation en tant que machines virtuelles (VM) sur un seul PC Linux ou Windows pour créer, tester ou démontrer des logiciels.
La VM GNS3 est recommandée pour la plupart des situations lorsque vous utilisez Windows ou Mac OS. L'équipe de développement GNS3 a travaillé dur pour créer un moyen léger et robuste de créer des topologies GNS3 qui évite les multiples problèmes courants rencontrés lors de l'utilisation d'une installation locale de GNS3. Cela inclut le manque de prise en charge appropriée de Qemu lors de l'exécution native de VIRL sous Windows (non recommandé). Cependant, si vous souhaitez uniquement créer des topologies GNS3 de base à l'aide de routeurs Cisco IOS, une installation locale (Dynamips) suffira. Cela signifie que vous n'installez que l'interface graphique GNS3 (tout-en-un) et n'utilisez pas la machine virtuelle GNS3.
C'est plus simple à mettre en place à certains égards, mais a des limites et doit être considéré comme le point de départ de votre voyage GNS3. Dès que vous êtes à l'aise avec GNS3, il est recommandé de passer à une configuration de machine virtuelle GNS3 pour tirer le meilleur parti des options et de l'optimisation de GNS3.[GNS3.COM]



IV. INTEGRATION DE ASA SOUS GNS3

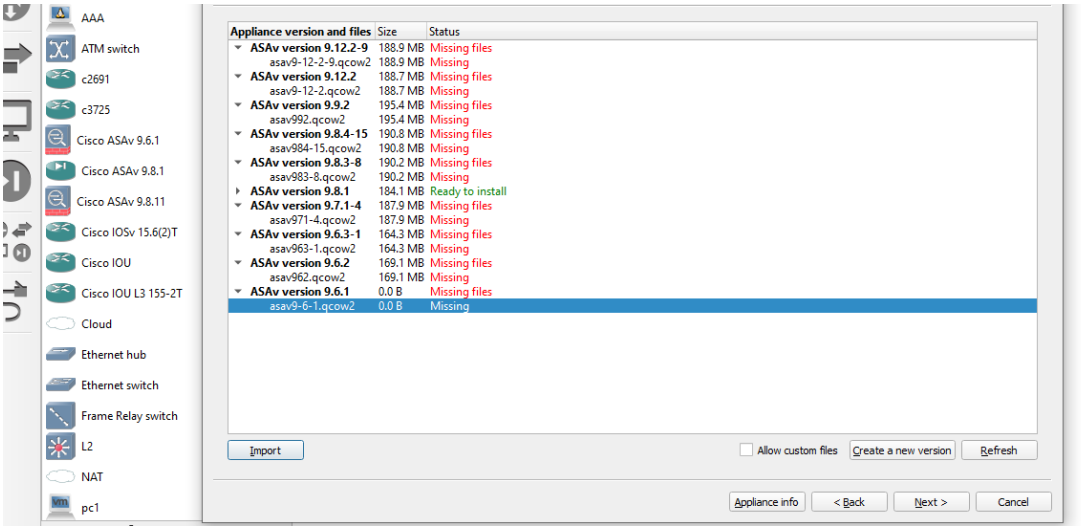
L'émulation de ASA sous GNS3 s'effectue à travers une image QEMU.
Comme nous l'avons dit précédemment que trois fichiers doivent être présents pour rendre possible l'émulation de ASA sous GNS3:

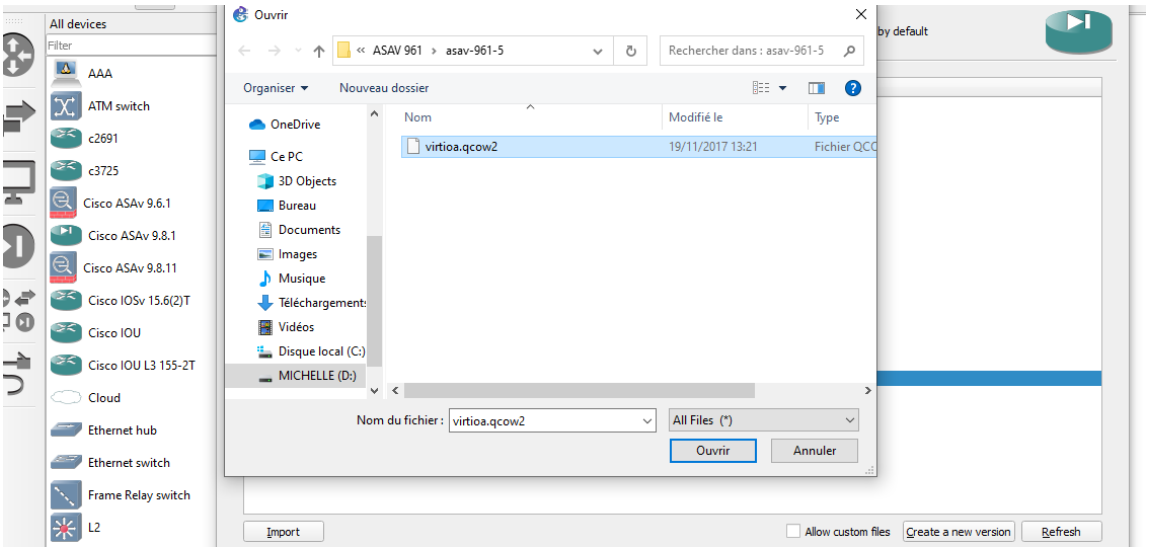
- Le fichier d'initialisation de la RAM dont le nom est sous la forme <initrd.gz> pour notre cas nous n'avons pas utilisé car notre ASA c'est le ASA961

- Le fichier image du noyau ASA dont le nom est sous la forme <vmlinuz> pour notre cas nous n'avons pas utilisé car notre ASA c'est le ASA961
- Le fichier image de ASDM (Adatative Security Device Manager) dont le nom est sous la forme asdm*** bin, ce fichier est optionnel, sa principale fonction est d'offrir un environnement graphique qui facilité les taches de configuration ASA complexes en mode commande.

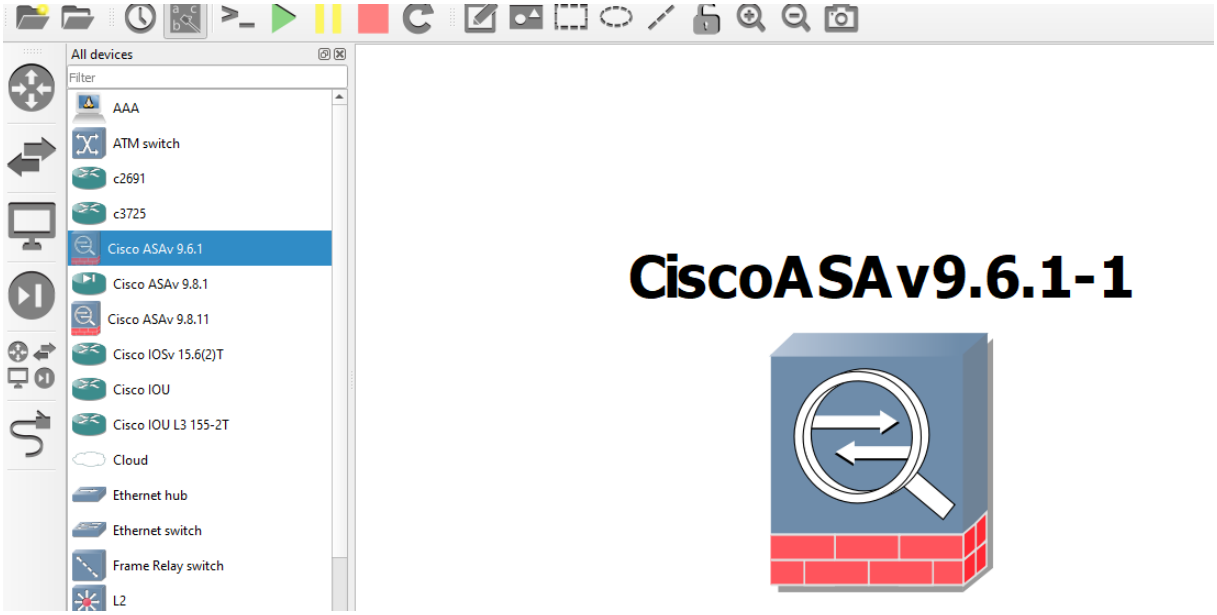
Pour configurer ASA dans GNS3, voici comment faire: il faut tout simplement aller dans **file**, sélectionner **import Appliance** sélectionner le fichier < cisco-asav.gns3a.gns3a> enregistrer dans fichier de votre ordination et suive les instructions ci-dessous sous forme d'images.

A cette étape c'est à vous de choisir la version que vous souhaitez utiliser dans notre cas nous avons utilisez la version de ASA961 et importer le fichier < virtioa.qcow2> que nous avons télécharger.

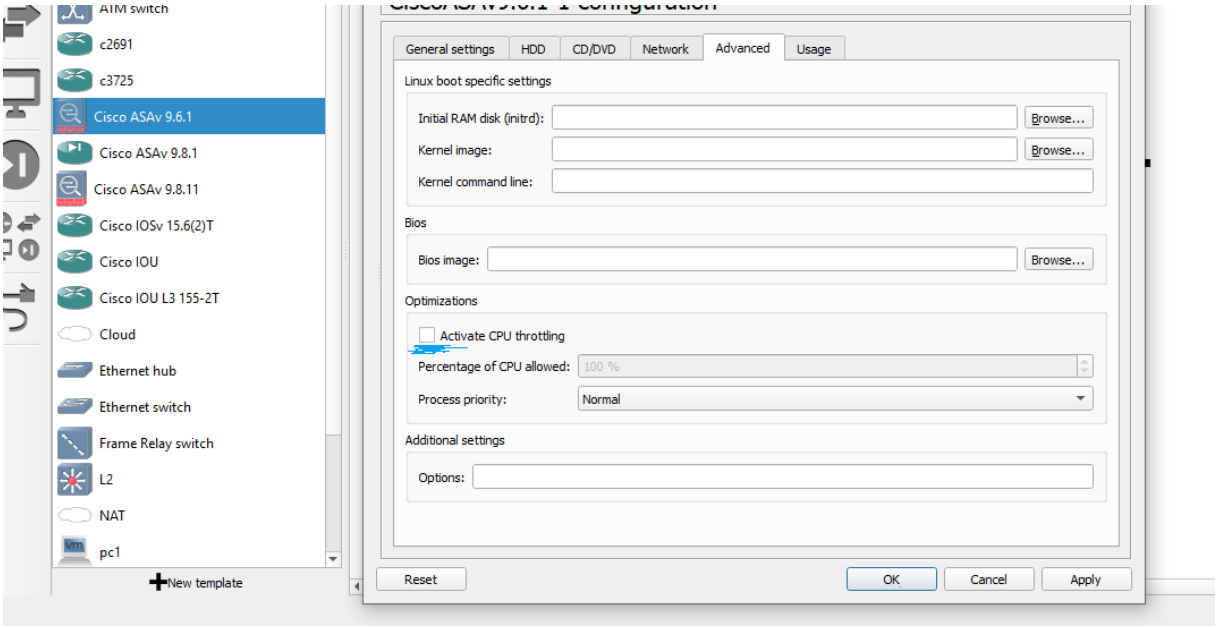




Une foi l'installation terminer voici comment notre ASA se présente sur l'interface GNS3



En suite pour finaliser la configuration faite un clic droit en suite cliquez sur configuration aller dans **Advanced** puis cliquez sur la case suivante



Voilà le ASA961 est parfaitement configurer.

V. LA TOPOLOGIE D'UN RESEAU NON SECURITE PAR LE PARFEU ASA

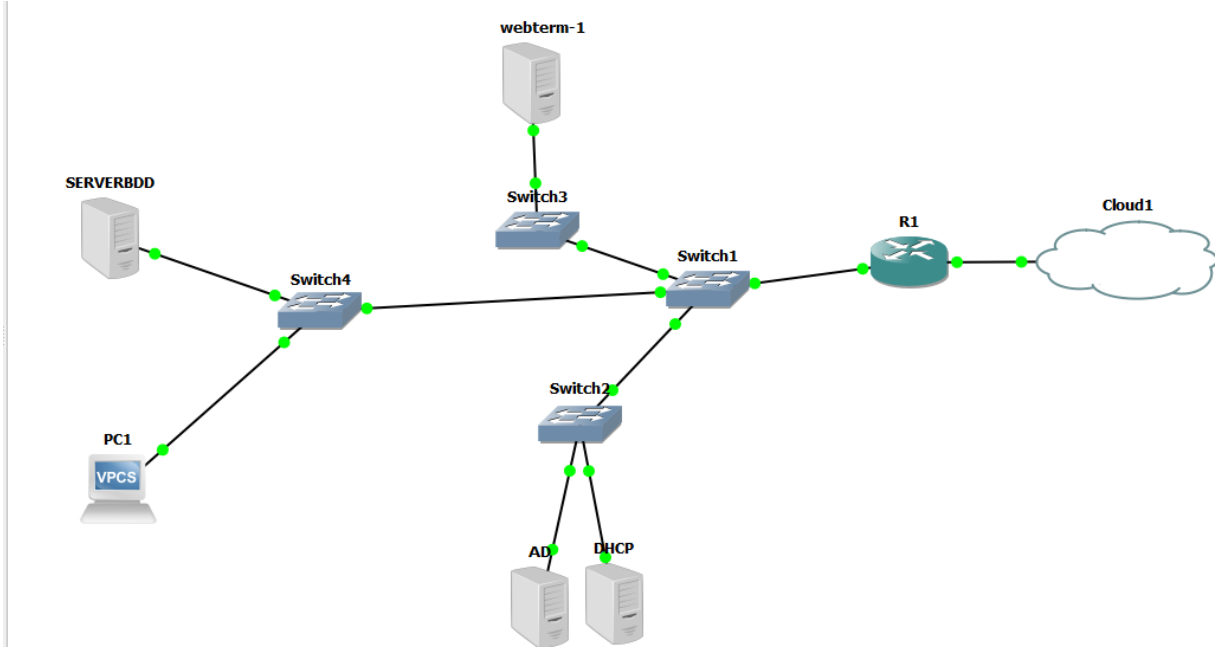


Figure 14 : proposition d'une architecture existante

LES CRITIQUES (Figure 14) :

- Le réseau est installé anarchiquement et non administré.
- Le réseau n'est pas sécurisé il est disposé au réseau externe (internet).
- Le réseau installé est non sécurisé contre les intrusions d'une façon faible.
- L'accès est permis de chaque unité émettrice vers n'importe quelle unité destinataire (accès non limité).
- L'absence de gestion réseaux centralisé « Domain »(tous les machines interconnectes elles sont dans le même groupe de travail.
- L'absence de VLAN (augmentation du trafic réseau).
- Le serveur DHCP n'est pas sécurisé (les attaques de « DHCP spoofing »)
- Manques firewall pour sécuriser l'accès (DMZ, ACL, zone base firewall)
- Manque de VPN pour les connexions nomades.
- Manque de politique de cryptage de données l'intégrité des données
- Manque de stratégie de gestion d'autorisation pour assure la disponibilité des données
- Manque de serveur radius pour l'authentification.
- Le manque de sécurité au niveau de port de Switch (les attaques par « mac flooding » et les attaques « man in the middle ».
- Manque d'un système de détection d'intrusion pour analyser le contenu des paquets (Données). [16]

VI. SOLUTION PROPOSEES

A l'issu d'un réseau existant nous avons opté à l'implémentation d'un plan de sécurité comme suite :

- Administration et ordonnancement du réseau local.
- Configuration d'un firewall(ASA9.6.1)
- Isolation des postes à l'aide de VLAN (pour segmenté les réseaux et minimisé le trafic réseau)
- Installation d'un serveur radius (pour l'authentification

Voici L'architecteur du réseau avec les solutions proposées dans ce plan de sécurité est par la figure

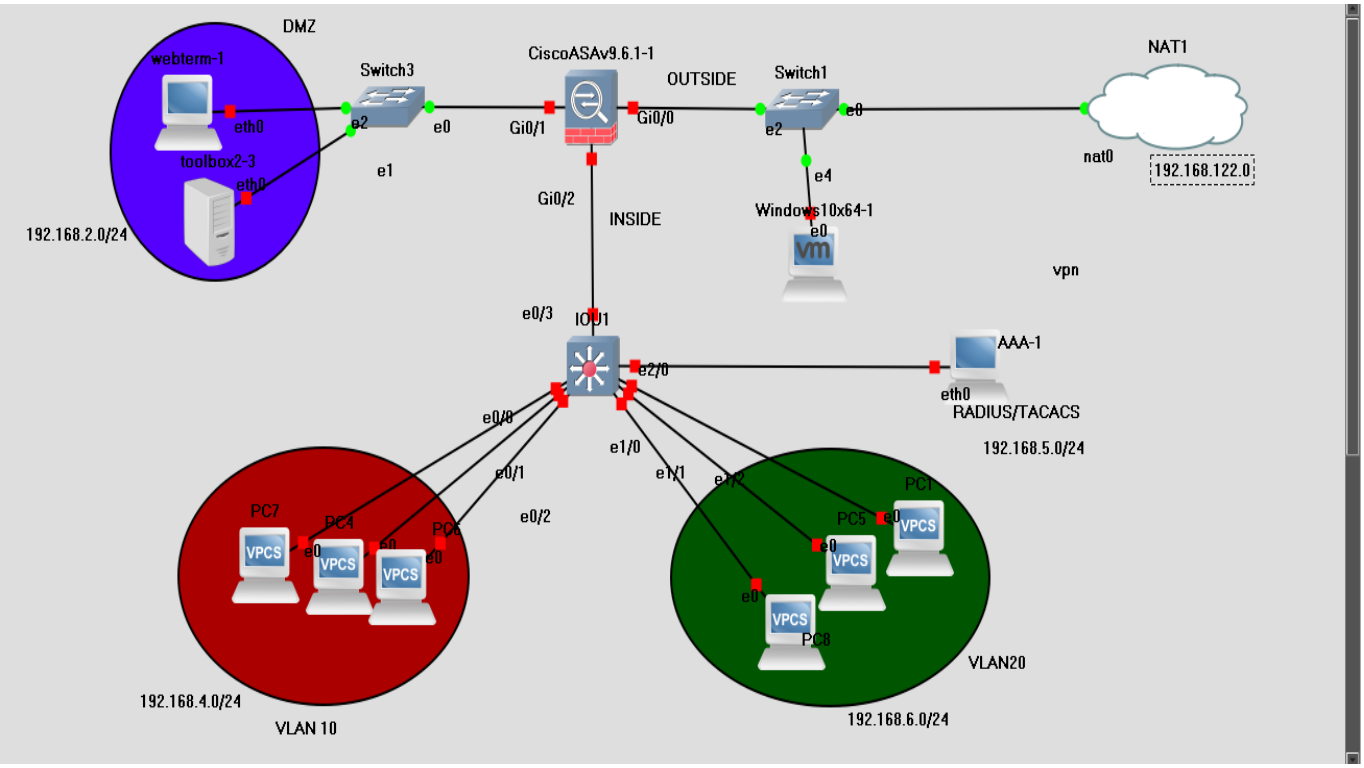
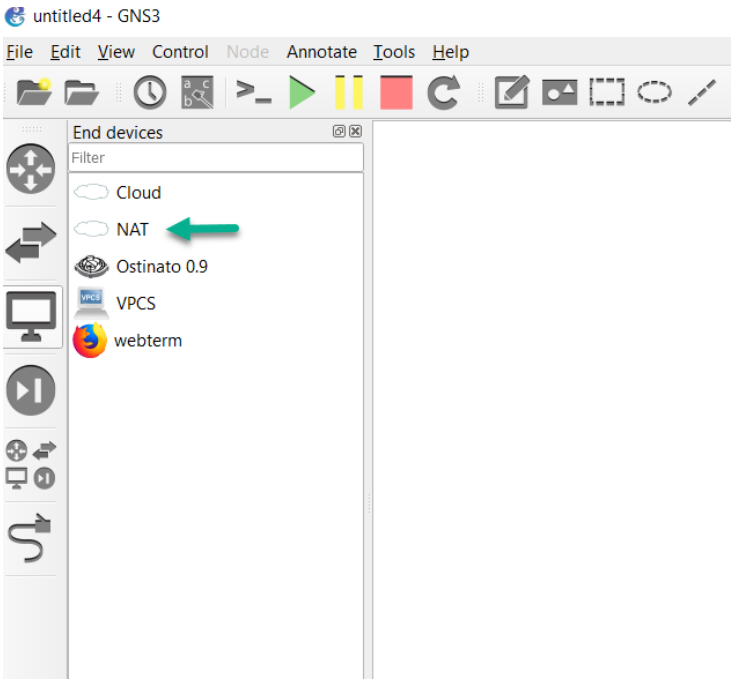


FIGURE 15 : ARCHITECTURE RESEAU PROPOSE

Ce modèle est constitué de cinq grandes parties qui sont les suivantes :

A. LE NŒUD NAT :

À partir de GNS3 2.0, le nœud NAT est devenu disponible. Ce nœud vous permet de connecter une topologie à Internet via NAT.
C'est utile lorsque vous devez télécharger des éléments depuis Internet, comme des packages, si les nœuds doivent effectuer une vérification de licence, etc.). Il est également beaucoup plus simple à utiliser que le nœud Cloud préexistant.
Le nœud NAT nécessite soit la machine virtuelle GNS3, soit un ordinateur Linux sur lequel libvirt est installé. Libvirt est nécessaire pour créer une interface virbr0 pour que ce nœud fonctionne.
Par défaut, le nœud NAT exécute un serveur DHCP avec un pool prédéfini dans la plage 192.168.122.0/24
La connectivité vers le google.com dans la zone interne et dmz et ASA marche par le ping du 8.8.8.8 cela signifie qu'avec le node NAT pour peut atteindre l'internet. Voici les images du ping



B. Configuration des noms des interfaces et leurs niveaux de sécurité

Le firewall ASA a trois interfaces connectées à trois segments du réseaux :

- Le segment de réseau connecté à l'interface GigabitEthernet 0/0 est la zone OUTSIDE avec un niveau de sécurité de 0

  Cette partie concerne toutes les entités qui sont à l'extérieur de l'entreprise. Ces entités peuvent être des commerciaux nomades qui transmettent leurs données, des employés qui veulent avoir accès à leurs comptes, des internautes voulant naviguer sur le site institutionnel de l'entreprise ou des partenaires commerciaux qui veulent faire des échanges à travers l'Extranet de l'entreprise.

- Le segment de réseaux connecté à l'interface GigabitEthernet 0/2 est la zone INSIDE avec un niveau de sécurité de 80 pour VLAN10 et 90 VLAN20

  Cette partie regroupera les différents utilisateurs de l'entreprise. Elle doit être la plus sécurisée des différentes autres parties. C'est pour cela qu'elle n'est pas accessible de l'extérieur.

  Lors de la conception de l'architecture réseau proposée nous avons utilisé plusieurs matériels afin d'aboutir à un bon résultat et voici la liste des matériels utilisés:

1. Serveur de certificats d'autorités.
2. Serveur d'authentification Tacacs+.
3. Serveur TFTP.
4. Serveur Web.
5. Des postes client
6. Des Switch Cisco
7. Un routeur
8. Un firewall ASA
9. Câbles de connexions
10. Les logiciels utiliser pour les serveur sont les dockers

- Le segment de réseaux connecté à l'interface GigabitEthernet 0/1 est la zone DMZ avec un niveau de sécurité de 50

Cette partie de l'architecture contiendra les serveurs et les services accessibles de l'extérieur et de l'intérieur. On trouvera par exemple le serveur Webterm, serveur toolbox, qui sont publiés (exposé) sur internet d'une façon sécurisée.

C. PRESENTATION DE CONFIGURATION DE NOTRE MAQUETTE

- **Configuration des interfaces dans ASA**

```
ciscoasa> en
Password:
ciscoasa# show int ip br
Interface                IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0       192.168.122.97  YES CONFIG up                    up
GigabitEthernet0/1       192.168.2.2     YES CONFIG up                    up
GigabitEthernet0/2       unassigned      YES unset  up                    up
GigabitEthernet0/2.1     192.168.4.1     YES CONFIG up                    up
GigabitEthernet0/2.2     192.168.6.1     YES CONFIG up                    up
GigabitEthernet0/3       unassigned      YES unset  down                  down
GigabitEthernet0/4       unassigned      YES unset  administratively down down
GigabitEthernet0/5       unassigned      YES unset  administratively down down
GigabitEthernet0/6       unassigned      YES unset  administratively down down
Management0/0            unassigned      YES unset  administratively down down
ciscoasa#
```

- **Configuration de NAT et ACL dans ASA**

```
object network vlan-inside
object network vlan10-inside
 subnet 192.168.4.0 255.255.255.0
object network vlan20-inside
 subnet 192.168.6.0 255.255.255.0
object network inside-subnet
 subnet 192.168.4.0 255.255.255.0
object network dmz-subnet
 subnet 192.168.2.0 255.255.255.0
object network webserver-external-ip
 host 192.168.122.12
object network webserver
 host 192.168.2.4
object network toolbox-external-ip
 host 192.168.122.11
object network toolbox
 host 192.168.2.5
object network inside-subnet1
 subnet 192.168.6.0 255.255.255.0
access-list inside-in extended permit tcp 192.168.4.0 255.255.255.0 host 192.168.2.4 eq www
access-list inside-in extended permit tcp 192.168.6.0 255.255.255.0 host 192.168.2.4 eq www
access-list inside-in extended permit ip any any
access-list inside-in extended permit icmp any any
access-list dmz-in extended permit ip any any
access-list dmz-in extended permit icmp any any
access-list outside-in extended permit tcp any host 192.168.2.4 eq www
access-list outside-in extended permit tcp any host 192.168.2.5 eq https
access-list outside-in extended permit ip any any
access-list outside-in extended permit icmp any any
pager lines 23
mtu outside 1500
mtu dmz 1500
mtu inside1 1500
mtu inside2 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-714.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
```

```
ciscoasa# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list inside-in; 4 elements; name hash: 0x53c2f06a
access-list inside-in line 1 extended permit tcp 192.168.4.0 255.255.255.0 host
192.168.2.4 eq www (hitcnt=0) 0xd5ec4c8d
access-list inside-in line 2 extended permit tcp 192.168.6.0 255.255.255.0 host
192.168.2.4 eq www (hitcnt=0) 0x946eae7f
access-list inside-in line 3 extended permit ip any any (hitcnt=0) 0x503914ad
access-list inside-in line 4 extended permit icmp any any (hitcnt=0) 0x5aa487b7
access-list dmz-in; 2 elements; name hash: 0x71043bca
access-list dmz-in line 1 extended permit ip any any (hitcnt=0) 0xef3ddf6a
access-list dmz-in line 2 extended permit icmp any any (hitcnt=0) 0x61816968
access-list outside-in; 4 elements; name hash: 0x4cd7d86a
access-list outside-in line 1 extended permit tcp any host 192.168.2.4 eq www (h
itcnt=0) 0x7778cf58
access-list outside-in line 2 extended permit tcp any host 192.168.2.5 eq https
(hitcnt=0) 0xec70b4d5
access-list outside-in line 3 extended permit ip any any (hitcnt=0) 0x02a82900
access-list outside-in line 4 extended permit icmp any any (hitcnt=0) 0xea400d9d

ciscoasa#
```

```
Management0/0              unassigned      YES unset  administratively down down
ciscoasa# show run nat
!
object network inside-subnet
 nat (inside1,outside) dynamic interface
object network dmz-subnet
 nat (dmz,outside) dynamic interface
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
object network toolbox
 nat (dmz,outside) static toolbox-external-ip service tcp https https
object network inside-subnet1
 nat (inside2,outside) dynamic interface
ciscoasa#
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

- **Configuration des vlans dans le switch dans INSIDE**

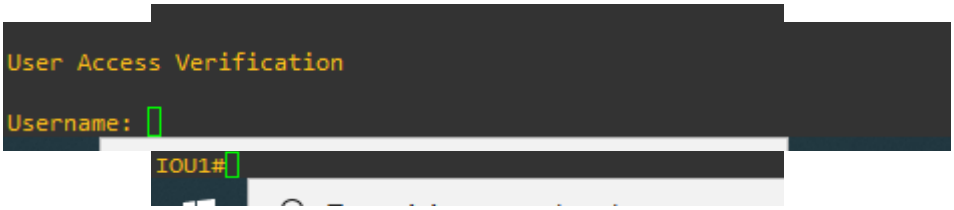
```
!
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport access vlan 20
 switchport mode access
!
interface Ethernet1/1
 switchport access vlan 20
 switchport mode access
!
interface Ethernet1/2
 switchport access vlan 20
 switchport mode access
!
interface Ethernet1/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
```

- **Configuration de TACACS+ dans le switch de INSIDE**

```
interface Vlan1
 ip address 192.168.5.1 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
tacacs server container
 address ipv4 192.168.5.2
 key gns3
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 transport input all
!
!
end
```

```
!
username master privilege 15 password 0 cisco
aaa new-model
!
!
aaa group server tacacs+ gns3group
 server name container
!
aaa authentication login default group gns3group local
aaa authentication enable default enable
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
```

- **Vérification d'accès dans le switch avec le serveur AAA (TACACS+)**

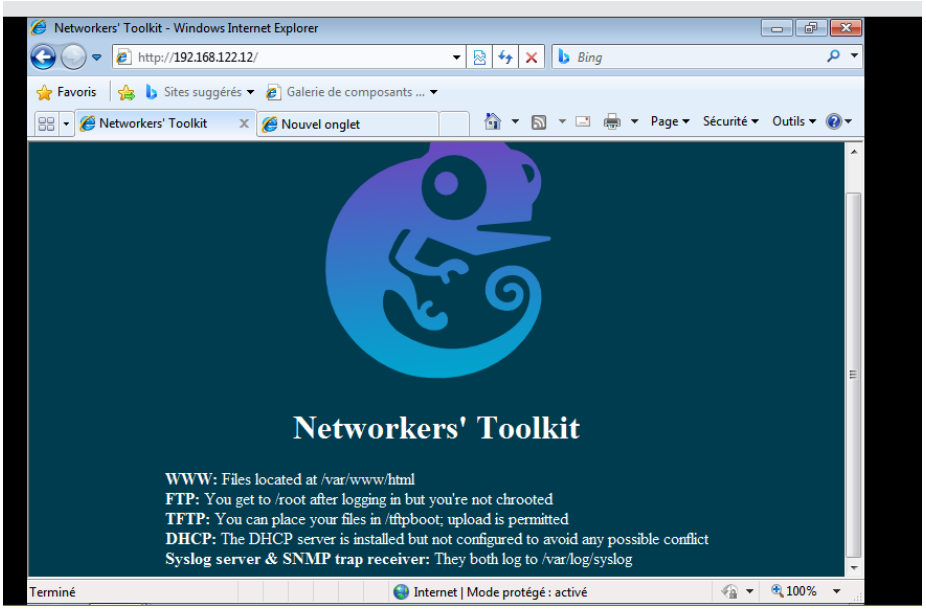


- Configuration dans ASA de packet-tracer route port 80 (OUTSIDE-DMZ)

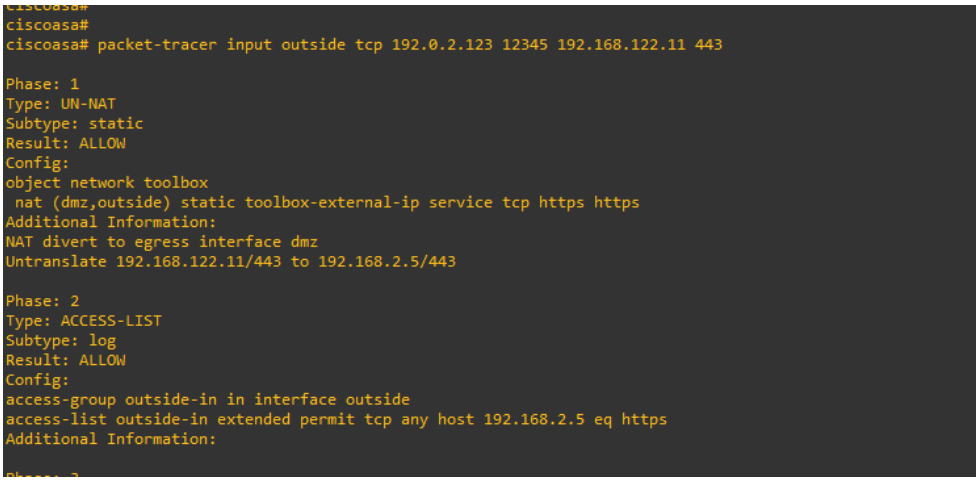
```
ciscoasa#
ciscoasa#
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 192.168.122.12 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
 nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 192.168.122.12/80 to 192.168.2.4/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 192.168.2.4 eq www
Additional Information:
```



- Configuration dans ASA de packet-tracer route port 443 (OUTSIDE-DMZ)



- **Configuration de serveur dockers**

Définition dockers

La technologie de conteneur Docker a été lancée en 2013 en tant que moteur Docker open source.

Il a tiré parti des concepts informatiques existants autour des conteneurs et en particulier dans le monde Linux, des primitives connues sous le nom de groupes de contrôle et d'espaces de noms. La technologie de Docker est unique car elle se concentre sur les exigences des développeurs et des opérateurs de systèmes pour séparer les dépendances des applications de l'infrastructure.
Le développement d'applications aujourd'hui nécessite bien plus que l'écriture de code. Plusieurs langages, frameworks, architectures et interfaces discontinues entre les outils pour chaque étape du cycle de vie créent une énorme complexité. Docker simplifie et accélère votre flux de travail, tout en donnant aux développeurs la liberté d'innover avec leur choix d'outils, de piles d'applications et d'environnements de déploiement pour chaque projet.[17]

Dans notre travail nous avons utilisé les docker comme serveurs :toolbox, AAA,webterm décrivons ces dockers en quelques ligne :

a. dockers Toolbox

Le docker toobox se trouve sur le site GNS3 dans la partie makeplace Appliance, dans gns3 il porte le nom de <Networkers Toolkit>qui signifie en français appareil de boite à outils réseau. Cette Appliance contient un logiciel côté serveur pour la gestion secondaire des périphériques réseau :
- www (nginx)
- ftp (vsftpd)
- tftp (tftpd)
- syslog (rsyslog)
- dhcp (isc-dhcpd)
- serveur snmp (snmpd + snmptrapd)

Le Mot de passe racine : gns3
Ce Toolbox nous a servi comme un serveur ftp pour le transfert du fichier vers la zone outside.

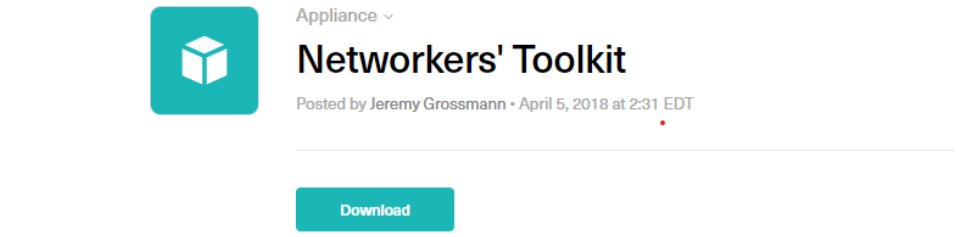


Figure de toolbox

b. Docker webtern

webterm est une boîte à outils réseau basée sur Debian. Il contient le navigateur web firefox ainsi que les utilitaires suivants : net-tools, iproute2, ping, traceroute, curl, host, iperf3, mtr, socat, ssh client, tcpdump, ab (apache benchmark) et les outils de test multicast msend / mreceive. Dans le webtern nous avons utilisé le https.

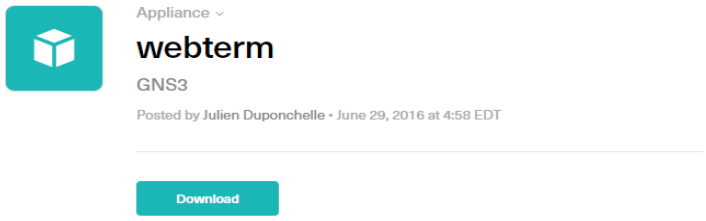
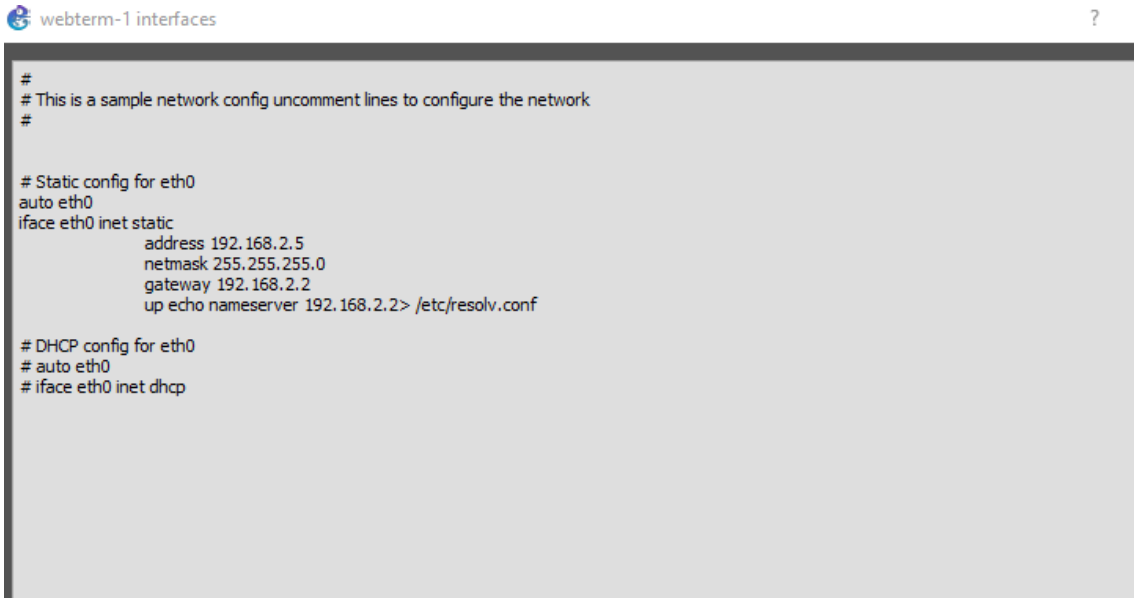
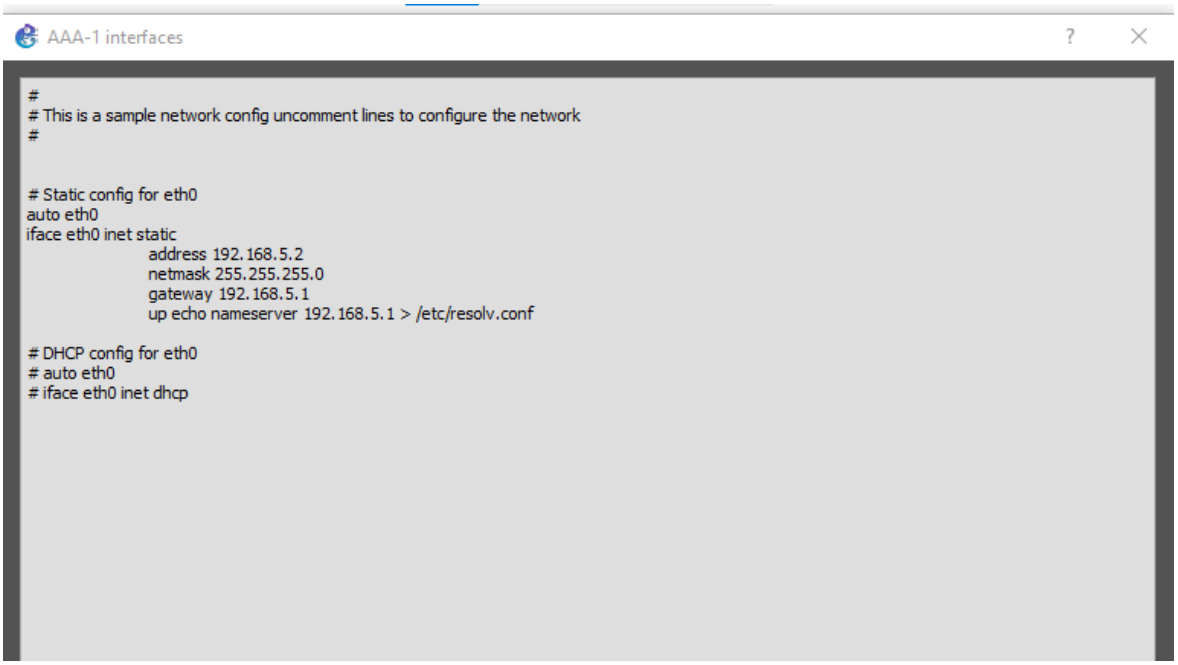


Figure du docker webtern



c. Docker AAA

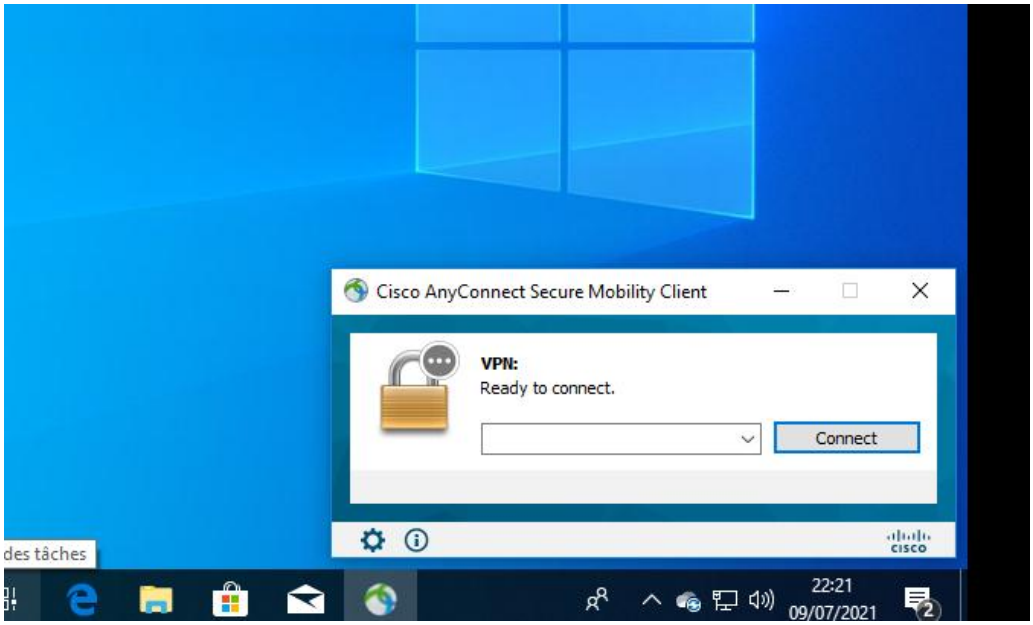
Cette appliance fournit des services RADIUS et TACACS + avec des utilisateurs et des groupes préconfigurés.
L'utilisation du docker
Utilisateurs RADIUS : - Alice - bob Utilisateurs TACACS+ : - gns3 (rôle : admin) - readonly Tous les utilisateurs, ainsi que les clients RADIUS/TACACS+ ont le mot de passe 'gns3' défini.
Cette Appliance fournit des services RADIUS et TACACS+ avec des utilisateurs et des groupes préconfigurés. Mais dans notre travail nous avons configurer le Tacacs dans l'utilisation du serveur AAA on a besoin de deux routeurs ou switch pour faire la configuration de radius et Tacacs vu que on ne peut pas mettre ses deux configurations dans un seul routeur.



- **Définition de Tacacs+**

TACACS+ est un protocole entièrement nouveau et n'est pas compatible avec ses prédécesseurs, TACACS et XTACACS. TACACS+ utilise TCP (alors que RADIUS fonctionne sur UDP).
Comme TCP est un protocole orienté connexion, TACACS+ doit implémenter le contrôle de transmission. RADIUS, cependant, n'a pas à détecter et à corriger les erreurs de transmission telles que la perte de paquets , le délai d'attente, etc., car il utilise UDP qui est sans connexion . RADIUS crypte uniquement le mot de passe des utilisateurs lorsqu'il se déplace du client RADIUS au serveur RADIUS. Toutes les autres informations telles que le nom d'utilisateur, l'autorisation, la comptabilité sont transmises en clair. Par conséquent, il est vulnérable à différents types d'attaques. TACACS+ crypte toutes les informations mentionnées ci-dessus et ne présente donc pas les vulnérabilités présentes dans le protocole RADIUS.
TACACS+ est une extension conçue par CISCO pour TACACS qui crypte le contenu complet de chaque paquet. De plus, il fournit un contrôle granulaire (commande par autorisation de commande).
Puisse dans notre configuration nous avons un seul switch relier dans la zone interne on a choisi de faire la configuration de Tacacs une fois quand on ouvre le switch il demande le mot

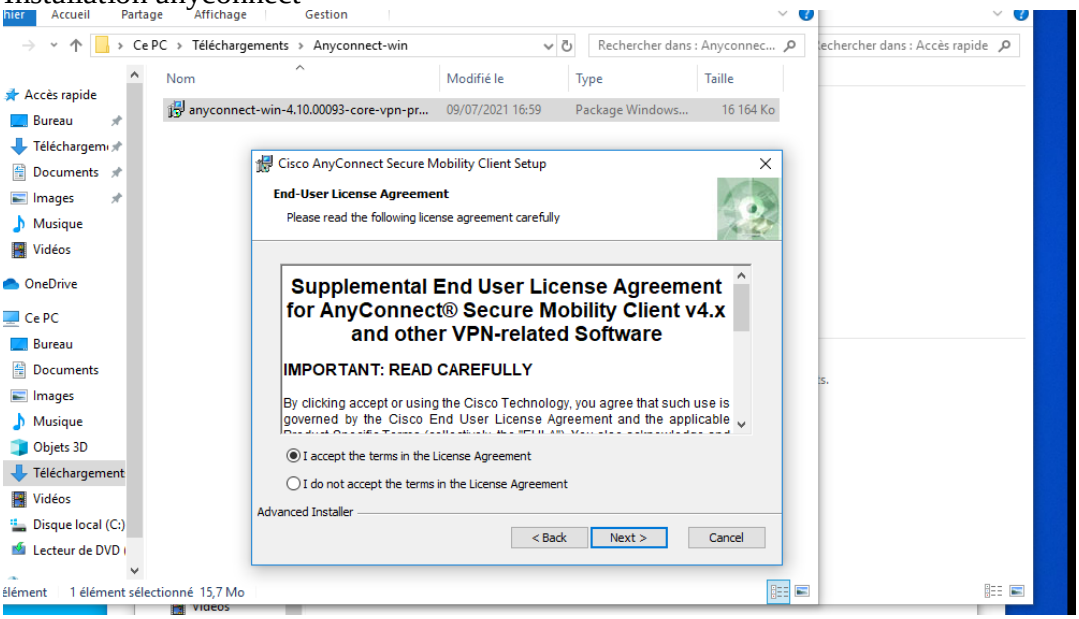
de



passe il faut s'authentifier pour accéder au switch.
Voici une image dans le switch.[18]

- **VPN ANYCONNECT**

Le vpn anyconnect remplacé par Cisco AnyConnect Secure Mobility Client permet aux travailleurs distants d'accéder sans friction(résistance) et hautement sécurisé au réseau de l'entreprise depuis n'importe quel appareil, à tout moment et en tout lieu, tout en protégeant l'entreprise.
AnyConnect Secure Mobility Client est un produit logiciel de point de terminaison modulaire. Il fournit non seulement un accès au réseau privé virtuel (VPN) via Secure Sockets Layer (SSL) et Internet Protocol Security (IPsec) Internet Key Exchange version2 (IKEv2), mais offre également une sécurité améliorée grâce à divers modules intégrés. Par rapport a la topologie de notre travail nous avons choisi vpn anyconnect.
Installation anyconnect



- **VLAN**

Vlan veut dire Virtual local area network … en d'autres mots : réseau local virtuel.

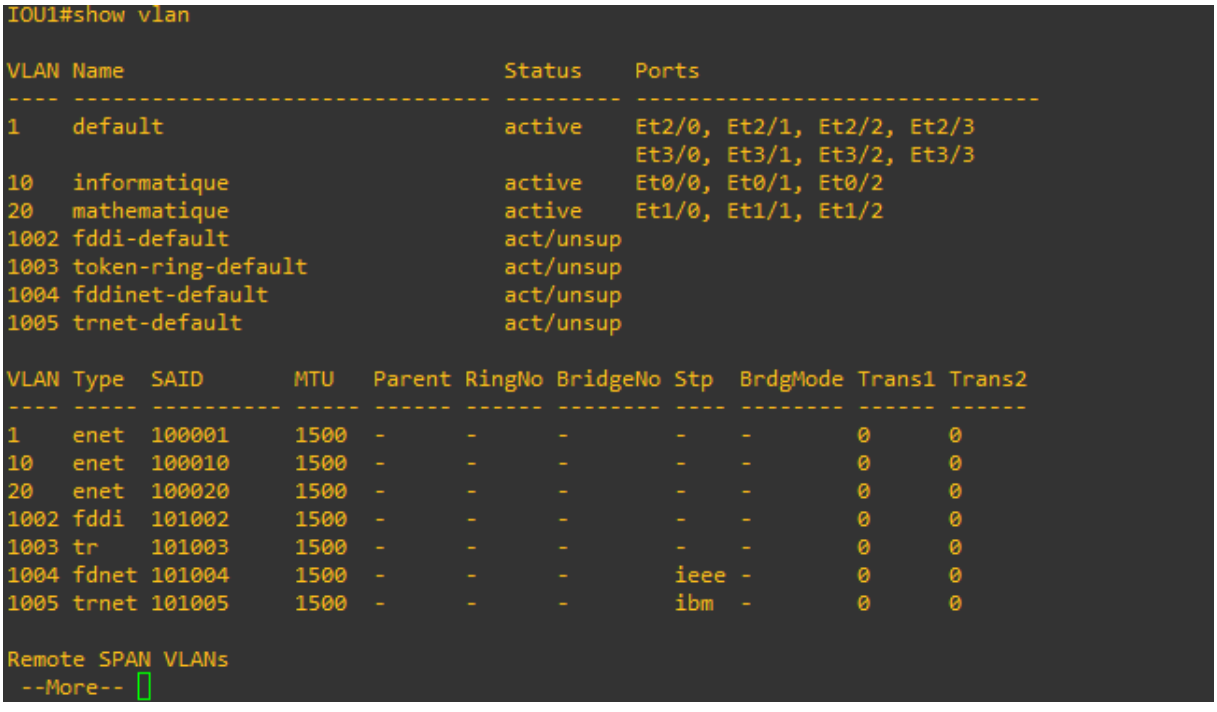
Il s'agit, sur un même switch de créer plusieurs réseaux indépendants ne pouvant pas, par défaut, communiquer entre eux.
Dans notre exemple, un switch est comme un grand immeuble avec plusieurs appartements. Chaque appartement créé correspond à un Vlan.
Donc si notre immeuble contient 2 appartements, cela correspond à 2 Vlans sur notre switch. Chaque occupant d'un appartement est indépendant de son voisin avec qui il ne communique pas.
Chacun peut faire ce qu'il veut dans son appartement sans que le voisin ne puisse le voir ou communiquer avec lui. En d'autres termes Un VLAN est donc un LAN logique fonctionnant sur une infrastructure LAN physique commutée.
Une infrastructure physique commune peut supporter plusieurs VLANs. Chaque LAN virtuel fonctionnera comme n'importe quel LAN distinct.

- **Trunking**

Les ports d'une liaison qui agrègent le trafic de plusieurs VLANs s'appellent un "Trunk" chez le constructeur Cisco Systems et "liaison d'agrégation" chez d'autres. Sur ce type de liaison, le commutateur ajoute des champs supplémentaires dans ou autour de la trame Ethernet. Ils servent notamment à distinguer le trafic de VLAN différents car ils contiennent entre autres le numéro d'identification du VLAN.
le trunk est un moyen du protocole dot1q. Il permet de faire communiquer deux appareils (des switches en général) et leurs VLAN respectifs. De cette façon, le VLAN 2 du switch 1 et du switch 2 peuvent communiquer ensemble.
Le VLAN 1 s'appelle le VLAN natif. En fait, sur un switch CISCO (même chez d'autres constructeurs) par défaut, tous les ports sont configurés sur le VLAN natif c'est-à-dire le VLAN 1 ici. Du coup, lorsque l'on branche un ordinateur sur un port dont le VLAN n'est pas configuré, cet ordinateur est en fait sur le VLAN 1.

Avantage d'un vlan

Indépendance de la couche physique
Contribue à la séparation des flux et la sécurité de l'infrastructure.
Flexibilité : allocation dynamique des utilisateurs dans un réseau indépendamment de l'emplacement
Facilité de gestion : QoS, classification, routage, filtrage
Performances : diminution de la taille des domaines de Broadcast
Coût abordable.
On a cree deux vlan :vlan 10 informatique et vlan 20 dans un switch l'image est ci-dessus



- **Configuration IP route ASA**

```
Gateway of last resort is 192.168.122.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.122.1, outside
C        192.168.2.0 255.255.255.0 is directly connected, dmz
L        192.168.2.2 255.255.255.255 is directly connected, dmz
C        192.168.4.0 255.255.255.0 is directly connected, inside1
L        192.168.4.1 255.255.255.255 is directly connected, inside1
C        192.168.6.0 255.255.255.0 is directly connected, inside2
L        192.168.6.1 255.255.255.255 is directly connected, inside2
C        192.168.122.0 255.255.255.0 is directly connected, outside
L        192.168.122.97 255.255.255.255 is directly connected, outside

ciscoasa#
```

VII. TEST DE LA CONFIGURATION DE NOTRE STRATEGIE

Après avoir bien configuré notre Firewall ASA, il est necessaire de tester celui-ci pour bien assurer la fiabilité de ce dernier.

✓ **Le ping de INSIDE vers DMZ**

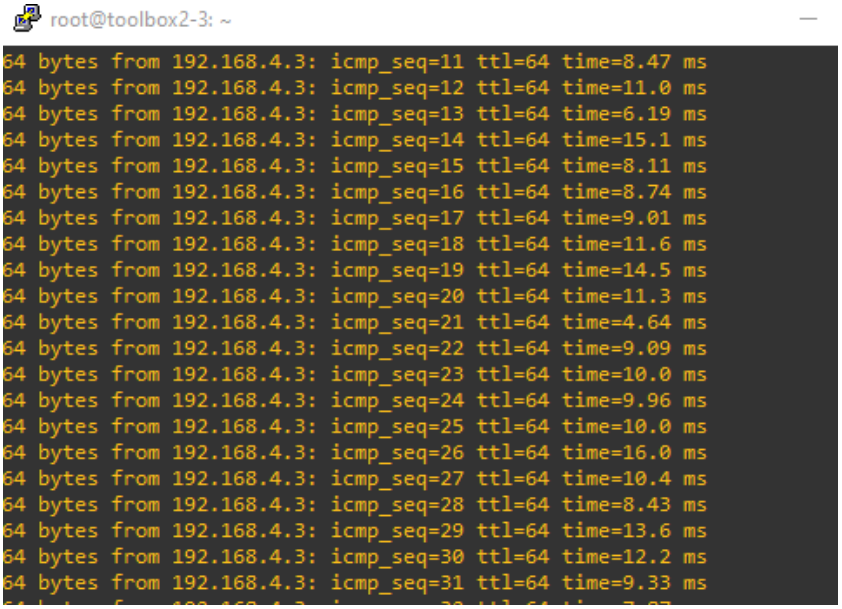
```
PC6> ping 192.168.2.4
84 bytes from 192.168.2.4 icmp_seq=1 ttl=64 time=8.195 ms
84 bytes from 192.168.2.4 icmp_seq=2 ttl=64 time=6.570 ms
84 bytes from 192.168.2.4 icmp_seq=3 ttl=64 time=6.344 ms
84 bytes from 192.168.2.4 icmp_seq=4 ttl=64 time=8.748 ms
84 bytes from 192.168.2.4 icmp_seq=5 ttl=64 time=8.253 ms

PC6>
```

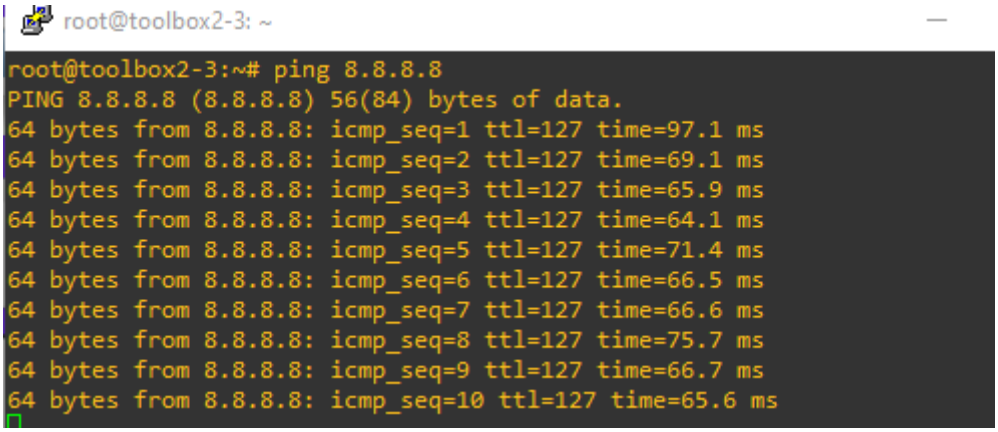
✓ **Le ping des VLANs (VLAN20 vers VLAN10)**

```
PC8> ping 192.168.4.3
84 bytes from 192.168.4.3 icmp_seq=1 ttl=64 time=45.095 ms
84 bytes from 192.168.4.3 icmp_seq=2 ttl=64 time=10.644 ms
84 bytes from 192.168.4.3 icmp_seq=3 ttl=64 time=9.458 ms
84 bytes from 192.168.4.3 icmp_seq=4 ttl=64 time=6.309 ms
84 bytes from 192.168.4.3 icmp_seq=5 ttl=64 time=5.997 ms
```

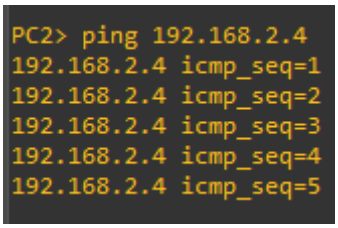
✓ **Le ping de DMZ vers INSIDE**



✓ **Le ping de DMZ vers OUTSIDE**



✓ **Le ping de OUTSIDE vers DMZ**



✓ **Le ping de INSIDE vers OUTSIDE**

```
PC6> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=75.127 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=73.923 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=71.481 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=64.221 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=127 time=67.689 ms
```

- ✓ **Le ping de OUTSIDE vers INSIDE**

```
PC2> ping 192.168.4.3
192.168.4.3 icmp_seq=1 timeout
192.168.4.3 icmp_seq=2 timeout
192.168.4.3 icmp_seq=3 timeout
192.168.4.3 icmp_seq=4 timeout
192.168.4.3 icmp_seq=5 timeout
```

Ici à partir de l'internet il est impossible de joindre l'intranet (INSIDE) à cause de notre Firewall qui bloque tous les accès. Les hôtes au niveau de l'internet peuvent plus joindre notre intranet. En testant de joindre le LAN nous avons comme résultat indiqué sur ce figure ci-dessous :

On a comme message « centre server de destination inaccessible »

- ✓ **Le Ping ASA vers GOOGLE**

```
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/68/80 ms
ciscoasa#
```

VIII. CONCLUSION

En définitive nous avons pu mettre en place une proposition et une mise en œuvre d'une stratégie de sécurité tout en se basant sur le pare-feu ASA.

Ceci nous a permis de nous familiariser avec l'environnement du GNS3. Notre recherche revêt d'une importance capitale car nous avons pu consolider nos connaissances sur des programmes qui interagissent avec la gestion de la sécurité d'une entreprise.

CONCLUSION GENERALE

A l'issu de notre travail, le message que nous avons voulu faire passer dans ce mémoire est que nous vivions dans un monde ou les systèmes d'information prennent une place chaque jour plus importante pour tirer profit de ces nouvelles technologies des entreprises mais aussi chacun d'entre nous doivent prendre conscience des risques associés à l'utilisation des ordinateurs.

La connaissance de ces risques constitue une première étape pour apprendre à les gérer. Nous avons vu que la plupart des menaces pouvais être combattu par des moyens techniques mais aussi par des recoures à des procédures. L'industrie informatique est encore relativement jeune ces premiers balbutiements remontent au milieu du XXème siècle. Elle a accompli depuis des progrès magnifiques et ne semble pas que l'imagination de concepteurs matériels et des logiciels soient sur le points de se tarir.

Ces évolutions constantes ont eux des inconvénients : la nécessité d'innover souvent n'a pas toujours laisser le temps de réfléchir au problèmes de sécurité et de fiabilité. Une vision court termes à souvent prévalu. Gageons qu'avec le temps l'industrie informatique gagnera en maturité les nouvelles applications informatiques en particuliers les entreprises réseaux ont besoin de systèmes sécurisées.

Dans notre mémoire nous avons appris le parti de ne pas nous concentrer sur les risques et les menaces présentés par certaines architectures mise en place. Au contraire nous avons essayé d'entreprendre une réflexion générale sur les problèmes de sécurité des réseaux informatiques, indépendamment de la technologie.

REFERENCES

[1] strasbourg.fr

Académie de Strasbourg - 6 rue de la Toussaint 67975 Strasbourg cedex 9

[2] Firewall help

© 2018 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo de WatchGuard, WatchGuard Dimension, Firebox, Core, Fireware et LiveSecurity sont des marques déposées ou des marques de commerce de WatchGuard Technologies aux Etats-Unis et/ou dans d'autres pays.

https://www.watchguard.com/help/docs/fireware/12/fr-FR/Content/fr-FR/authentication/radius_how_works_c.html

[3] Firewall help

© 2018 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo de WatchGuard, WatchGuard Dimension, Firebox, Core, Fireware et LiveSecurity sont des marques déposées ou des marques de commerce de WatchGuard Technologies aux Etats-Unis et/ou dans d'autres pays.

https://www.watchguard.com/help/docs/fireware/12/fr-FR/Content/fr-FR/authentication/radius_how_works_c.html

[4] S. Coze et S. Heldebaume de l'IUP du Littoral

http://jmainy.free.fr/guill.web-/Authentification.html

[5] Auteur inconnu

http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2000/angebertlevesque/exposeipsec.htm

[6] auteur iconnu

http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2000/angebertlevesque/exposeipsec.htm#3.%20La%20mise%20en%20oeuvre%20d'IPSEC%20dans%20les%20VPN

[7] © Groupe Eyrolles, 2003, 2006, 2010, ISBN : 978-2-212-12821-5
C é d r i c L l o r e n s L a u r e n t L e v i e r D e n i s V a l o i s B e n j a m i n M o r i n
A v e c l a c o n t r i b u t i o n d e O l i v i e r S a l v a t o r i
https://static.fnac-static.com/multimedia/editorial/pdf/9782212128215.pdf

[8] La dernière modification de cette page a été faite le 15 mai 2020 à 00:37.
Wikipedia® est une marque déposée de la Wikimedia Foundation, Inc., organisation de bienfaisance régie par le paragraphe 501(c)(3) du code fiscal des États-Unis.
https://fr.wikipedia.org/wiki/Interior_gateway_protocol

[9] **©2001-2021** Futura-Sciences, tous droits réservés - Groupe MadeInFutura
https://www.futura-sciences.com/tech/definitions/informatique-antivirus-10999/

[10] référence aux cours du Mr MOUSTEFAOUI sécurité web

[11] ©**2001-2021** Futura-Sciences, tous droits réservés - Groupe MadeInFutura

https://www.futura-sciences.com/tech/definitions/informatique-antivirus-10999/

[12]auteur inconnu Wikipédia

[13] Jérémy Grossman

Copyright © 2021 Galaxy Technologies LLC.

https://docs.gns3.com/docs/

[14]

2021 Cisco et/ou ses filiales. Snort, le logo Snort et Pig sont des marques déposées de Cisco. Tous les droits sont réservés.

http://www.snort.org/docs

[15] Jérémy Grossman

Copyright © 2021 Galaxy Technologies LLC.

https://docs.gns3.com/docs/

[16]mémoire de **F**ACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
Etude et sécurisation d'une infrastructure DMZ avec ASA
CISCO5510Promotion 2015

[17] https://www.docker.com/

[18] https://fr.wikipedia.org/wiki/Terminal_Access_Controller_Access-Control_System_Plus