International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 47 No. 1 Feb. 2020, pp. 1-10

http://www.ijisr.issr-journals.org/

UNE APPROCHE DE CONCEPTION D'UNE ARCHITECTURE HYBRIDE DE CONTROLE D'ACCES DE LA LIAISION INTERNET ET INTRANET PAR LA GESTION D'IDENTIFICATION MULTINIVEAUX

ENGOMBE WEDI Boniface[1], KIDIAMBOKO GUWA Simon[2], and OKIT'OLEKO ON'OKOKO Jean[3]

[1]Université Pédagogique Nationale de Kinshasa, RD Congo

[2]Institut Supérieur des Techniques Appliquées de Kinshasa, RD Congo

[3]Institut Supérieur des Statistiques de Kinshasa, RD Congo

ABSTRACT: In this article, we describe a hybrid architecture integrating firewalls, filtering routers, encryption algorithms and the proxy server as well as intrusion detection programs in an interface environment between Internet and Intranet. It is well known that the Cyber Security policy strategy has many advantages currently when it often intervenes in this environment chosen as a field of investigation for the identification of users who are not yet recognized to define a general policy of effective and efficient control. Indeed, the current approaches are based on a cyber security policy focused on a password not on which unfortunately is easily crackable using specialized programs used by hackers or pirates. However, our architecture is not based on architectures and therefore does not suffer from this limitation. On the other hand, it provides several levels of security thanks to the integration policy recommended respectively of filtering routers, proxy server and advanced encryption algorithms ensuring the security at several levels. Thus, this initiative taken, proves that our architecture makes it possible to compensate for the deficiencies of the previous in this article notably INTERNET and INTRANET.

KEYWORDS: design approach, hybrid architecture, access control, internet and intranet link, multi-level identification management.

RESUME: Dans cet article, nous décrivons une architecture hybride intégrant des firewalls, des routeurs filtrants , les algorithmes de cryptage et le serveur proxy ainsi que les programmes de détection d'intrusion dans un environnement d'interfaçage entre Internet et Intranet. Il est bien connu que la stratégie de la politique de la Cybersécurité multi niveaux procure beaucoup des avantages actuellement lorsqu'elle intervient souvent dans cet environnement choisi comme champ d'investigation pour l'identification des utilisateurs non reconnus enfin de définir une politique générale de contrôle efficace et performant. En effet, les approches actuelles sont basées sur une politique de Cybersécurité focalisée à un mot de passe non sûr qui, malheureusement est facilement crackable à l'aide des programmes spécialisés utilisés par des hackers ou pirates. Cependant, notre architecture ne se base pas sur des architectures antérieures et par conséquent ne souffre pas de cette limitation. En revanche, elle fournit plusieurs niveaux de sécurité grâce à la politique d'intégration préconisée respectivement des routeurs filtrants, serveur proxy et des algorithmes de chiffrement avancés assurant la sécurité à plusieurs niveaux. Ainsi, cette initiative prise, prouve que notre architecture permet de pallier aux insuffisances des générations antérieures de sécurisation d'interfaçage des réseaux les plus célèbres ciblés dans cet article notamment INTERNET et INTRANET.

MOTS-CLEFS: approche de conception, architecture hybride, contrôle d'accès, liaison internet et intranet, gestion d'identification multiniveaux.

Corresponding Author: OKIT'OLEKO ON'OKOKO Jean

1 INTRODUCTION

L'ouverture de l'**Intranet** vers l'extérieur plus précisément **l'Internet** au moyen des systèmes de sécurité rudimentaires existant non sûr comme le mot de passe par exemple, accroissent les risques d'intrusion aux systèmes d'information et les altérations des données par des hackers [1] qui ont comme objectifs visés de :

- Prendre connaissance des données stratégiques confidentielles, sans être habilité et autorisé d'y accéder ;
- Modifier (altérer) des données et identifier les correspondants par usurpation d'écoute ou crackage des mots de passe et nier l'existence d'une transaction (répudiation) et paralyser les systèmes d'information (demi de service)[2] ;

En contrepartie, une bonne politique de sécurité de contrôle d'accès à plusieurs niveaux dans une liaison de communication Internet et Intranet consiste à intégrer plusieurs niveaux des barrières de filtrage d'identification des personnes pour le contrôle d'accès aux informations.[3] Cela conduit en une approche de conception d'une architecture hybride Firewall, Proxy et VPN rationnelle de la sécurité en trois axes respectivement les routeurs filtrants, les serveurs proxy et l'usage des algorithmes de chiffrement à plusieurs clés pour assurer la confidentialité des informations. Cependant, il convient de distinguer deux approches de la sécurité.

La sûreté de fonctionnement, safety en anglais, concerne l'ensemble des mesures prises et des moyens utilisés pour se prémunir contre le temps de dysfonctionnement du système de sécurité informatique [4]. Ensuite **la sécurité,** Security en anglais, regroupe tous les moyens et les mesures pour mettre le système d'informations à l'abri de toute agression des agresseurs : HACKERS.[5] En ce qui concerne cet article, il sera question de concevoir une architecture mixte du type DMZ assurant l'interface de contrôle d'accès entre Internet et Intranet.

1.1 PROBLÉMATIQUE

Dans le contexte de cet article, la sécurité de la liaison INTERNET ET Intranet est certainement le problème le plus épineux dans cet environnement ciblé.

En effet, une fois passé l'enthousiasme original pour la construction de l'autoroute de l'information notamment l'Internet, on s'aperçoit que celle-ci ne permet pas seulement de naviguer mais qu'elle permet également à un nombre considérable des malveillants externes à l'entreprise d'entrer dans votre réseau, vous visiter dont certains d'entre eux ne sont pas forcément les bienvenus. Ainsi, il se pose un problème sérieux d'insécurité.

Cependant, en termes de référence, notre préoccupation essentielle repose sur trois questions.

- Qu'est-ce qu'un Firewall intégrant des routeurs filtrants ?
- Ce type de Firewall peut-i-il contribuer efficacement au contrôle d'accès aux informations de la jonction Internet-Intranet ?
- Qu'apporte de nouveau une architecture hybride de Firewall Intégrant à la fois proxy, serveurs proxy, les algorithmes de chiffrement et des programmes de détection d'intrusion ?

1.2 MÉTHODOLOGIE

Premièrement, notre démarche a consisté à présenter d'abord, la problématique à l'échange des informations stratégiques dans la jonction d'interfaçage entre Internet et Intranet.

Secundo, la démarche tourne autour de l'étude de l'état des lieux des architectures existantes en vue de proposer une architecture hybride pour pallier aux insuffisances des architectures précédentes.

Pour répondre à ces différentes préoccupations, notre exposé aborde trois points suivants.

- Survol des quelques concepts de base.
- Etat des lieux des approches de conception des architectures de Firewall existantes.
- Une nouvelle approche de conception de Firewall hybride avancée.

2 SURVOL DES QUELQUES CONCEPTS DE BASE

Dans cette section, notre intervention scientifique s'effectue à la description des concepts clés suivants employés pour faciliter la bonne compréhension de cet article.

2.1 INTERNET

C'est l'acronyme d'interconnected qui signifie interconnexion et net, l'appellation anglaise du réseau.[6] Il désigne un ensemble de réseaux interconnectés utilisant tous les mêmes protocoles de transport et routage TCP/IP en vue d'accéder à des services dont les plus répandus sont respectivement E-mail, FTP, serveurs web, discussion en ligne (IRC), etc. C'est en 1957 que le réseau des réseaux a été imaginé par les militaires aux Etats Unis à partir d'une petite boule dite **SPOUTNIK** hérissée d'antennes russes affolait l'occident en effectuant, à partir du ciel, plusieurs rotations autour de la terre [7]. En ce qui concerne son organisation [8], on distingue :

- Les opérateurs de câblage et de transport disposent de leur réseau pour assurer le transport des informations d'un point à un autre. Ils fournissent les points de connexion sur leur réseau aux entreprises ainsi que les prestataires des services qui ont obtenu des adresses IP d'un organisme agréé comme Internic ou INRIA pour la France par exemple ;
- Les prestataires des services dits **Fournisseurs d'accès (ISP),** connectés sur **Internet,** fournissent des adresses IP aux particuliers ou PME qui peuvent obtenir l'adresse auprès de l'Internic ; [9]
- Les services tels que la messagerie électronique, la connexion aux serveurs web, l'hébergement des pages web, etc ;
- Les outils ou protocoles entre autres TCP/IP, UDP, IPX/SPX, SMTP, FTP, Slip, PPP, etc.,

2.1.1 LES GRANDS CONCEPTS DE L'INTERNET

Une communication mondiale, une absence de monopole et le paiement est local.

2.1.2 FONCTIONNEMENT DE L'INTERNET[10]

2.1.2.1 SCHÉMA DE PRINCIPE FIREWALL BASTION

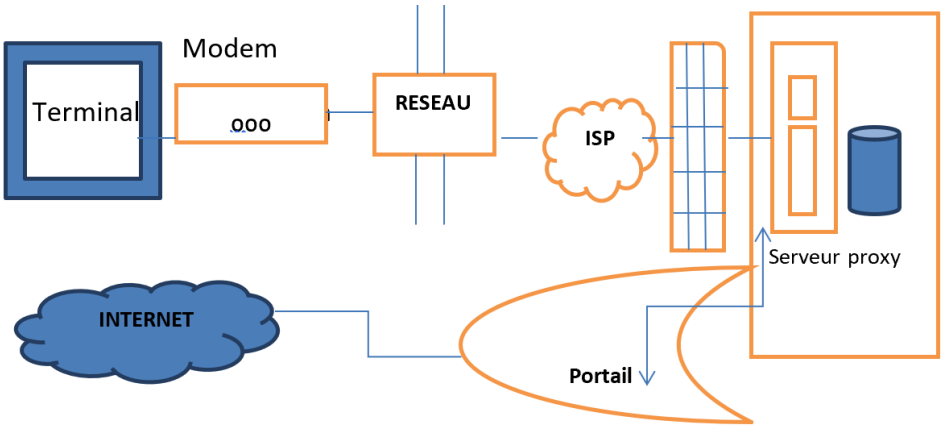

Fig. 1.Schéma de fonctionnement de l'Internet

2.1.2.2 DESCRIPTION

- Un terminal est un ordinateur client utilisé par un Internaute pour explorer l'Internet grâce au logiciel browser qui assure l'interface entre celui-ci et le monde Internet.[11]
- L'acronyme de modulation et démodulation qui sert d'adaptateur du signal entre deux machines distantes via un réseau de télécommunication ;
- Réseaux : ce sont les fameuses autoroutes de l'information utilisant comme supports les paires torsadées, câbles coaxiaux, fibres optiques et faisceaux hertziens ; services comme par exemple la connexion ;
- Portail : Gateway est une passerelle ;

- Firewall : c'est un ensemble de matériels et logiciels servant à contrôler l'accès entre Internet et Intranet ;
- Serveur proxy : est une machine cache assurant l'interface entre les terminaux des réseaux locaux et le web.
- Modem : est un adaptateur du signa2l de communication entre machines distantes ;
- ISP : Internet Service Proxy est un prestataire de services comme la connexion par exemple.

2.2 INTRANET

C'est un modèle réduit de l'Internet qui utilise les mêmes services offerts par ce dernier mais applicable dans environnement d'entreprise privée en vue d'assurer la confidentialité, l'intégrité de données, la disponibilité et la non répudiation des informations.[12]

2.2.1 NOTICE HISTORIQUE [13]

Le développement de l'informatique et des télécommunications ouvre des nouvelles perspectives de sécurisation des entreprises privées contre les menaces et les attaques des malveillants, pirates, des hackers à partir du réseau public Internet pour constituer une révolution invisible de celui-ci vers la mutation d'un réseau interne d'entreprise. De plus, le système d'information des entreprises à l'heure actuelle des technologies Internet ne permet pas de tisser des liens sécurisés forts des collaborations dans une entreprise avec les clients et les partenaires. Ainsi, pour pallier à ses inconvénients est né l'intranet. Les avantages de l'intranet sont respectivement l'utilisation des technologies et des infrastructures de l'internet au sein même d'une entreprise, la simplification considérable des problèmes de sécurité souvent redoutés lorsqu'on parle de l'internet, l'économie sur la facture téléphonique, les solutions non pariétaires car toute entreprise qui met en place un intranet n'est pas liée à un constructeur ou à un diffuseur des logiciels parce que les normes de l'Intranet sont mondialement adoptées et approuvées par l'ISO. Comme inconvénients de l'intranet nous pouvons citer notamment les couts internes sont à prendre en compte car sa réussite est fonction de la formation et du suivi des personnes qui seront amenées à l'utiliser, la nécessité de crypter des informations pour assurer la confidentialité et l'Intranet sans connexion à internet, peut amener une légitime frustration des utilisateurs qui voudront communiquer.

2.3 ROUTEURS FILTRANTS

Ce sont des équipements programmables intelligents installés dans le firewall pour examiner chaque datagramme par filtrage en comparant l'adresse IP source et de destination à des adresses placées dans table de filtrage. Si une adresse IP ne correspond pas à une adresse approuvée par la table, le datagramme est éliminé du réseau voilà le principe de filtrage des paquets. [14]

2.4 PROXY

C'est un logiciel sentinelle dans le réseau qui gère tout trafic entre l'Internet et l'Intranet par exemple. Un serveur proxy examine, dans le plus petit détail, jusqu'à l'appui sur chaque touche si nécessaire, le trafic entre les serveurs de l'internet et l'intranet. Mais l'hôte bastion est un intrus quincaillerie utilisé pour protéger le serveur proxy et empêcher les agressions sophistiquées des hackers.[15] Il sert comme intermédiaire entre les réseaux interconnectés Internet et intranet tout en offrant un passage contrôlé par le pare-feu. Ensuite, il offre également une possibilité de mise en cach c'est à dire sauvegarder une copie de fichiers auxquels les utilisateurs ont récemment accédé pour une consultation ultérieure si l'internet a des problèmes de communication.

2.5 CYBER SÉCURITÉ

C'est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques notamment matériels et immatériels connectés directement ou indirectement sur le réseau pour assurer la disponibilité, l'intégrité, authenticité, confidentialité, preuve et la non répudiation. [16]

3 ETAT DES LIEUX DES APPROCHES DE CONCEPTION DES ARCHITECTURES DE FIREWALL EXISTANTES

Etant un générique contrôlant les trafics réseaux entre Internet et Intranet, le firewall a connu plusieurs générations de construction des architectures jusqu'à cohabiter avec le proxy que nous allons analyser ensemble par la suite dans cet article.

3.1 ARCHITECTURE DE CONFIGURATION FIREWALL DE FILTRAGE PAQUETS

Dans cette première génération, grâce aux routeurs filtrants intégrés, le firewall analyse chaque paquet et ne laisse passer que celui autorisé tout en bloquant le reste sur base des règles pré configurés comme le montre la figure 2 ci-après.

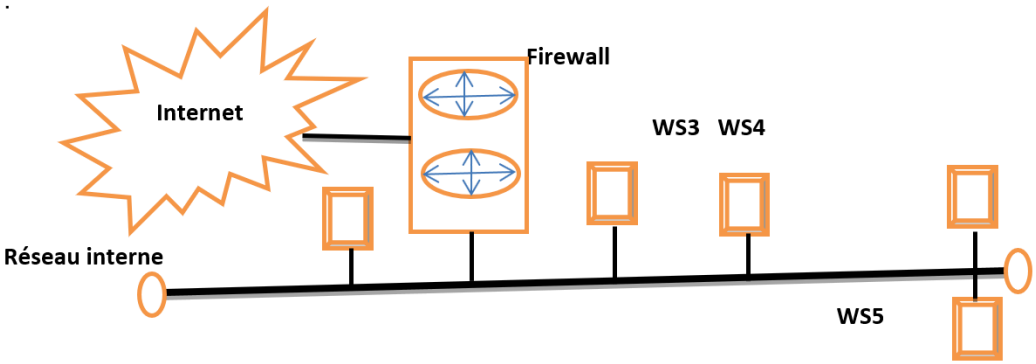

Fig. 2.Schéma de principe [17]

Comme interfaçage de filtrage, un firewall exerce un contrôle d'accès de haut à bas et vice versa par filtrage des paquets. En outre, il peut identifier et bloquer les paquets avec adresse IP « **Spoofed »** pour un paquet ayant une adresse source autre que son adresse source réelle mais sa configuration peut être difficile à réaliser, si bien que souvent on met en jeu certaines règles importantes et par conséquent on risque de désactiver des règles existantes.

3.2 ARCHITECTURE DE CONFIGURATION FIREWALL ET PROXY A DEUX SERVEURS SEPARES

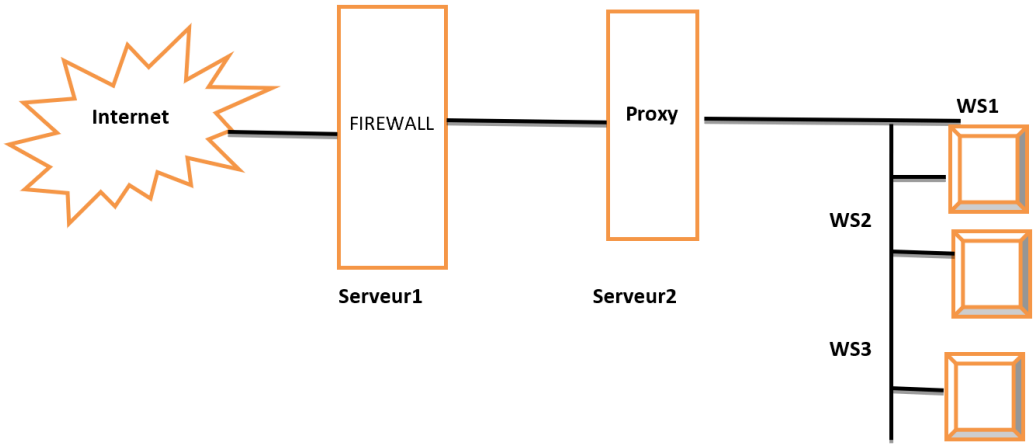

Fig. 3.Architecture Firewall et Proxy à des serveurs distincts[18]

Il existe deux types de serveur proxy : ceux qui fonctionnent au niveau des applications sur serveur, inspectent sont assez lents car ils doivent examiner chaque paquet réseau tandis que ceux qui fonctionnent au niveau des circuits ou des réseaux en utilisant une méthode de connexion réseau par socket restent plus sécurisant.

3.3 ARCHITECTURE FIREWALL ET PROXY INTEGRES DANS UN MEME SERVEUR

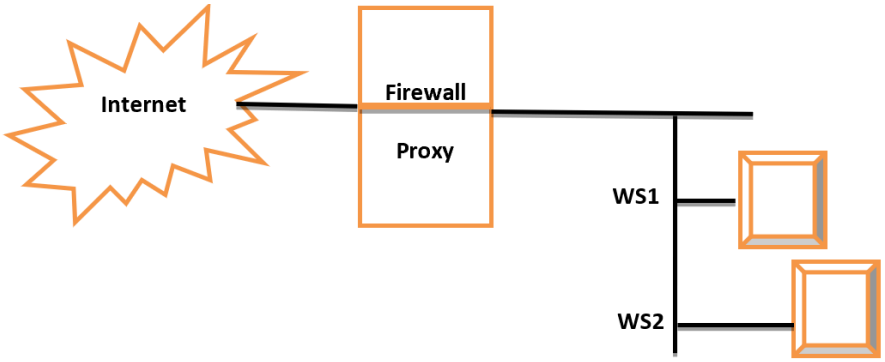

Fig. 4.Architecture Firewall et Proxy à des serveurs distincts [19]

Dans cette architecture, au lieu de montrer les adresses IP de chaque utilisateur , le fichier journal ou l'annuaire LDAP standard dont la vocation est de créer des liens vers l'Internet en vue d'effectuer des recheches n'affichera qu'une seule,celle du pare-feu . ce mode de fonctionnement risque de masquer certains problèmes et par conséquent rend la surveillance des activités de plus en plus difficile malheusement l'ouverture d'un port sur le pare-feu pour faciliter le dialogue avec des correpondants de confiance en ligne par le biais d'un programme revient à ouvrir parfois la porte aux pirates.. En outre, du fait que le serveur proxy doit examiner chaque paquet réseau, il devient lent. Il est conseillé d'utiliser un pare-feu avec sous-réseaux protégés à cause de son aptitude à diviser le reseau en zones ayant leurs propres param-tres de sécurité pour y rémédier.

3.4 ARCHITECTURE DE CONFIGURATION FIREWALL ET PROXY A DEUX SERVEURS SEPARES

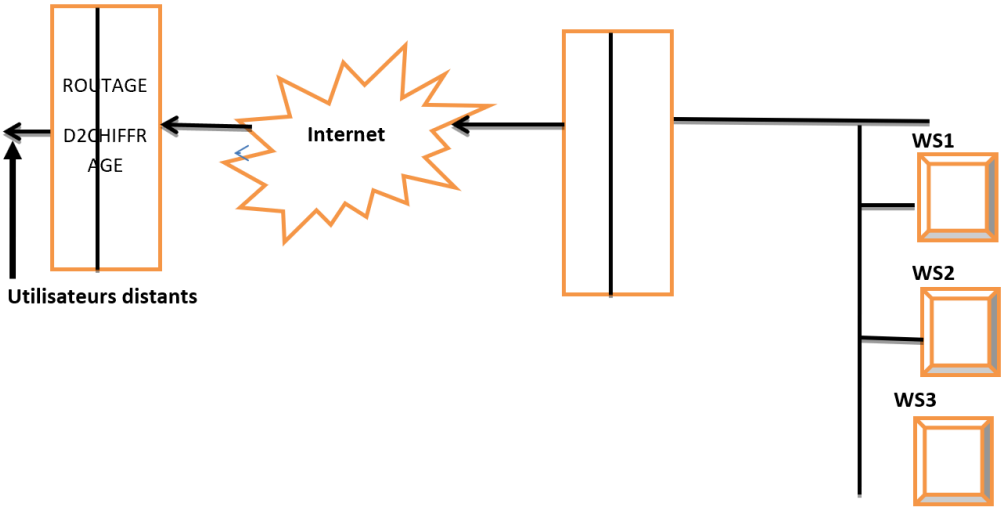

Fig. 5.Illustration d'une architecture d'usage des VPN personnalisés [20]

3.5 SÉCURISATION D'UNE DEFENSE FORTE

3.5.1 MODELE DE CLASSIFICATION DES RISQUES EN MATIERE DE SECURITE

Le modèle ci-après permet de classer les risques et de déterminer comment réagir face à chaque type de menace.

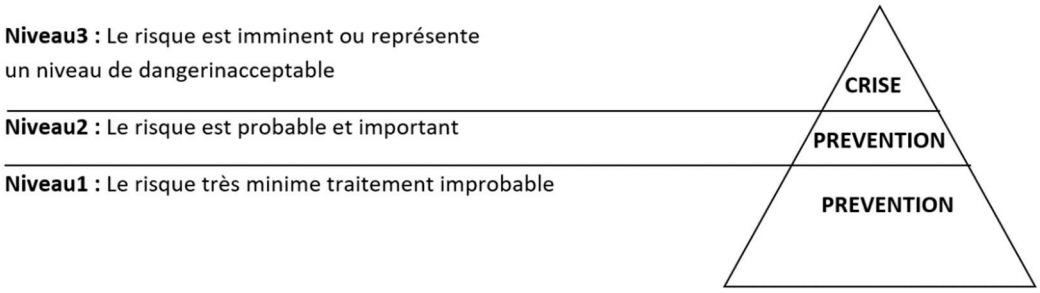

Fig. 6.Classement pour les risques[21]

3.5.2 DESCRIPTION

Les trois niveaux de gauche montrent le degré de risque. Lorsque l'on essaye d'évaluer un risque, on tente de déterminer respectivement la probabilité du risque et l'importance des dommages qu'il est susceptible de causer.

3.6 ARCHITECTURE DE CONFIGURATION ROUTEURS FILTRANTS ET FIREWALLS PAR SEGMENTATION A DES SOUS RESEAUX

Cette solution architecturale est utilisée lorsqu'on a besoin de protéger plusieurs Serveurs ou Workstation (ws) sous système réseau contenant des données sensibles aux intrusions des points stratégiques et en particulier si vous ne souhaitez pas autoriser **Telnet** sur votre réseau. Cependant, il peut y avoir certains utilisateurs qui préfère à des informations du réseau dit segment1 via Telnet sur d'autres serveurs sous Linux des sites distants alors la solution consiste à segmenter le réseau à des sous réseaux dit segment.

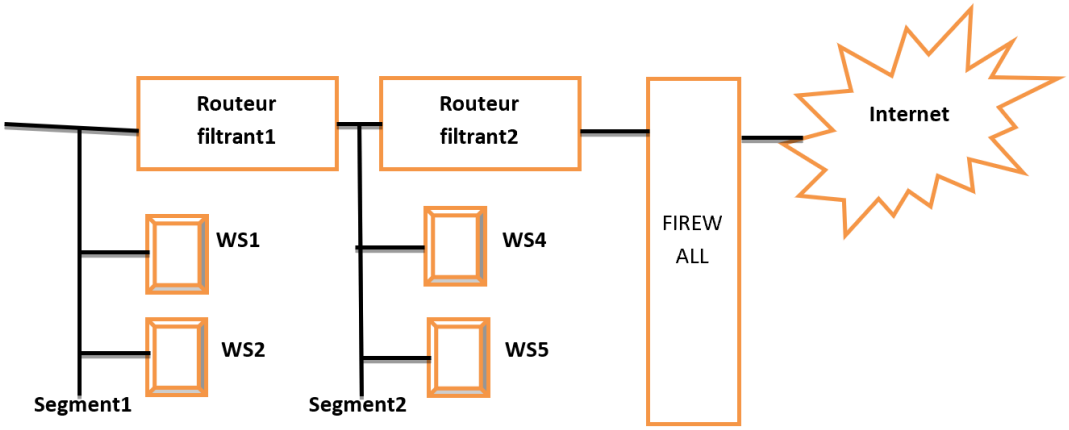

Fig. 7.Architecture de segmentation réseau en sous/réseaux[22]

3.7 UNE ARCHITECTURE PAR APPROCHE ENTREE AXEE SUR UNE MACHINE A 3 CARTES RESEAUX[23]

Les trois cartes sont reparties de la manière suivante :

- Une carte attachée au réseau public (Internet) ;
- Une carte attachée au réseau Intranet ;
- Une carte attachée au réseau périphérique (DMZ).

3.7.1 SCHÉMA ARCHITECTURAL DE PRINCIPE

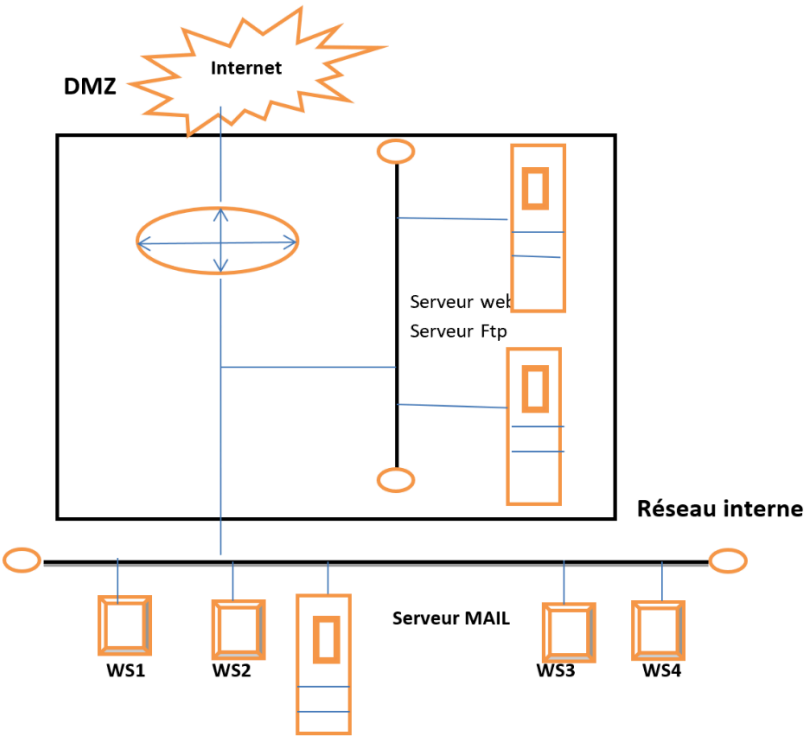

Fig. 8.Architecture d'intégration DMZ utilisant routeur à 3 cartes réseaux[24]

Dans cette architecture, comme les serveurs publics sont dans leur propre réseau périphérique, il sera très difficile pour les pirates informatiques de les utiliser comme point de lancement d'attaque contre les autres systèmes du réseau interne[6]. En utilisant cette architecture, on peut limiter sévèrement l'accès aux services du réseau DMZ en activant les ports 80 et 443 par exemple.

4 UNE NOUVELLE APPROCHE DE CONCEPTION D'UNE ARCHITECTURE INTEGREE HYBRIDE DES OUTILS DE SECURITE

C'est une architecture d'intégration des outils de sécurité dans une zone démilitarisée, **DMZ** en sigle **DMZ**[25].

4.1 SCHÉMA DE PRINCIPE

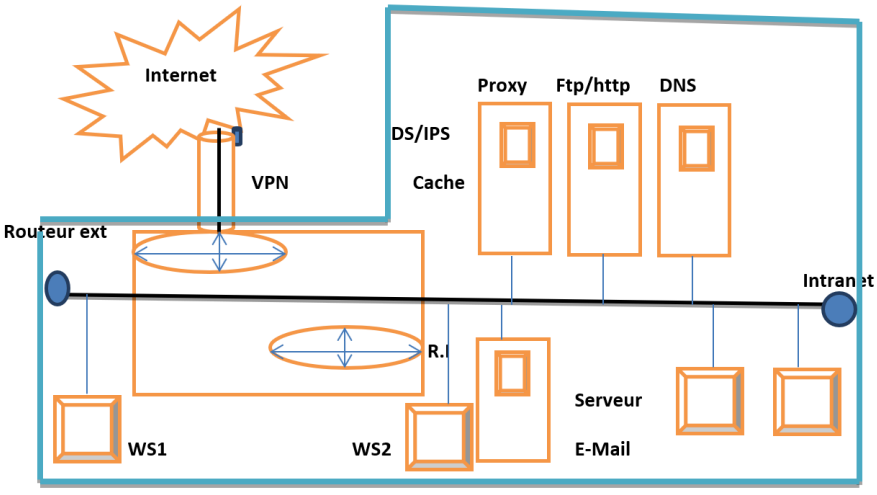

Fig. 9. Architecture hybride par approche DMZ

4.2 DESCRIPTION

- Ayant comme principe de base le tunneling, les VPN chiffrent les données avant de les envoyer et les déchiffre à l'arrivée. A cela s'ajoute, pour renfocer la capacité de sécurité .

Les adresses réseau de l'expéditeur et du destinataire sont également chiffrées grace aux protocoles spécialisés. Ses protocoles d'encapsulation tunneling sont les suivants[26] :

- Point to Point tunneling Protocol(PPTPC) crée des tunnels privés à travers l'Internet , ce qui permet à vos données d'atteindre leur destination en toute sécurité. Il s'agit d'un cousin de PPP qui permet de créer des tunnels PPP dans un réseau IP[27] ;
- Laye 2 Tunneling Protocol , L2TP en sigle, est un protocole qui a été conçu pour libérer les ISP des contraintes liées à l'utilisation des adresses IP enregistrées spécifiques.il permet un service de connexion distante virtuelle fac ilitant l'usage de façon privée des adresses IP non enregistrées et des supports pour des protocoles réseaux existants(IP, IPX, Apple talk, etc).
- Internet protocol security protocol, IPSEC en sigle ; est un protocole qui offre une sécurité au niveau du traitement des paquets plutôt que de l'application. Il offre deux modes de sécurité notamment le mode Authetification Header(AH) fournit une authetification de l'expéditeur, mais ne chiffre pas les données tandis que le mode Encapsulating Security Payload authetifie l'expéditeur et chiffre les données.[28].

En revanche, Telnet constitue une source potentielle de problèmes en matière de sécurité. D'ailleurs, les administrateurs sont d'accord pour dire le fait d'autoriser l'accès telnet à vos serveurs augmente considérablement les chances d'attaque des hackers. En utilisant Telnet , les pirates peuvent exécuter des programmes, apporter des changements au système , etc.

- **Zone démilitarisée, DMZ** en sigle, est un regroupement des outils intégrés de sécurité fiable en vue de constituer un réseau périphérique dit DMZ entre Internet et Intranet (un réseau d'entreprise) pour éviter que les intrus accèdent à leurs données et leurs machines stratégiques en créant plusieurs barrières d'identification.
- **DNS (Domain Name Service)** : est un serveur qui traduit les adresses IP à des noms des domaines et vice versa. Il constitue un protole standard sur Internet pour relayer les requêtes et les réponses entre les clients et les serveurs afin que ces derniers puissent agir à la demande des clients ou d'autres serveurs. [29].

Comme avantage principal, cette architecture est plus performante du point de vue fiabilité grâce à la présence sécurisation à plusieurs niveaux. Mais en revanche, elle est très complexe et coute chère pour son implantation.

5 CONCLUSION

La sécurité dans un environnement de développement intégré des outils d'identification, constitue une zone démilitarisée, DMZ en sigle, entre Internet et Intranet. Elle nous a aidé à exploiter de manière approfondie les différentes approches de conception des architectures existantes en vue de proposer une nouvelle approche hybride des outils intégrés d'identification et de contrôle d'accès à plusieurs niveaux de filtrage mais dont le cout d'implantation est couteux. En effet, les fonctions de sécurité intégrées sont efficaces lorsqu'elles s'insèrent dans un plan de cybesécurité. Cet article ainsi constitué énonce les concepts clés dans le domaine stratégique des réseaux notamment le contrôle d'accès, le Firewall, le serveur proxy, le chiffrement des informations et VPN. [30].

Par ailleurs, pour inciter tout chercheur intéressé à s'informer et se ressourcer sur les stratégies de conception des architectures hybride de contrôle à plusieurs niveaux ainsi que les connaissances réfléchies, le présent article représente un ouvrage de référence pouvant aider tout chercheur pour la politique sécuritaire d'interface entre internet et intranet.

REMERCIEMENTS

Nous adressons notre profonde gratitude de reconnaissance à l'Eternel Dieu tout puissant qui nous a accordé le souffle de vie jusqu'à nos jours. A cela s'ajoute, toutes les personnes qui ont contribué à l'élaboration de cet article de près ou de loin selon la sphère de leur contribution respective à la réussite de ce travail, notamment aux professeurs Engombe Wedi Boniface, Kidiamboko Guwa Simon pour leurs orientations respectives.

REFERENCES

[1] CLAUDE SERVIN, Réseaux et télécoms, 3ème éd. Dunod, Paris, 2009
[2] STEPHANE LOHIER et D., Internet: services et réseaux, Ed. Dunod, Paris, 2003.
[3] OKIT'OLEKO, Mémoire de fin d'études intitule: Sécurité sur le DNS cas d'Internet/Intranet, Deuxième ingénieur informatique appliquée, ISTA/Ndolo, 2000-2001.
[4] STEPHANE LOHIER et D., Transmissions et réseaux, 2ème Ed. Dunod, Paris, 2009.
[5] LEFEVRE, Intranet client/serveur universel, Ed. Collection, Info, Paris, 2006.
[6] B. CHESWIK, Firewalls and internet security, repelling the wily Hacker Wesley publishing company, 2004
[7] RANDALL A. TAMURA & DOMINO, Edition CAMPUS PRESS, 2003
[8] DANIELE DROMARD et FETAH, Réseaux informatiques : la sécurité dans les réseaux, cours et exercices, Ed. Dunod, Paris, 2003.
[9] STEPHANE LOHIER et D., Internet: services et réseaux, Ed. Dunod, Paris, 2003.
[10] STEPHANE LOHIER et D., Internet: services et réseaux, Ed. Dunod, Paris, 2003.
[11] BARRY RAVENDRAN GREENE et PHILIP SMITH, CISCO, ISP Essentiels cisco press, 2002
[12] Livre d'or de Microsoft: Mise en place d'un intranet, 2004
[13] CLAUDE SERVIN, Réseaux et télécoms, 3ème éd. Dunod, Paris, 2009
[14] KASENGEDIA, Cours de cryptographie et sécurité informatique, L1 info, Décembre 2019
[15] OKIT'OLEKO, Mémoire de fin d'études intitule: Sécurité sur le DNS cas d'Internet/Intranet, Deuxième ingénieur informatique appliquée, ISTA/Ndolo, 2000-2001.
[16] R. YUAN, virtual private Network: Technologie and solutions, Ed. Addison Wesley, Paris, 2001.
[17] B. CHESWIK, Firewalls and internet security, repelling the wily Hacker Wesley publishing company, 2004
[18] C. SCOTT, P. Wolfe et M., virtual private Network, 2ème Ed. O'Reilly, Paris, 2007.
[19] Andrew TANENBAUM, Réseaux Inter Editions, Paris, 2007.
[20] P. TOMSU, MPLS-BASED VPN Practice Hall, 0-13-028225-1.
[21] D. BRENT CHAPMAN et ELIZABETH D. ZWICKY, la sécurité sur l'internet/firewalls, éd. O'Reilly, Paris, 1996.
[22] G. PUJOLE et D. SERET, Réseaux et Télématique, Ed. Eyrolles, Paris, 2003.
[23] J. WILLIAM STALLINGS, Networking Standards, A guide to OSI, ISDN, LAN and MAN standards, Addison Wesley, 1994.
[24] KITSISA, Notes de cours des normes et protocoles, 1er Ir. Informatique appliqué, ISTA, 2000.
[25] KITSISA, Notes de cours des normes et protocoles, 1er Ir. Informatique appliqué, ISTA, 2000.
[26] PATRICE ROLIN: Cours de réseaux de la maitrise informatique, Université d'Angers, 2002.
[27] RAFAEL CORVALAN et Ernesto, Les VPN: Principes, conception et déploiement des réseaux privés virtuels, 2ème Ed. Dunod. Paris 2003.
[28] J. S. TILLER, A technical guide to IPsec virtual private network, Ed. Press, Paris, 2003.
[29] T. GAIDOSCH, C. KUNZIGER et M., A guide to virtual private Networks, practice Hall, 0-13-083964-7
[30] STRAUSS-KAHN, Management stratégique des PME/PMI: guide méthodologique, Ed. Economia, Paris, 2001.