ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) **BREVET D'INVENTION**

(11) N° de publication :
MA 54776 B1

(51) Cl. internationale :
H04L 63/00; G06F 17/00

(43) Date de publication :
27.09.2023

(21) N° Dépôt :
54776

(22) Date de Dépôt :
29.10.2021

(71) Demandeur(s) :
Université Internationale de Rabat, Parc Technopolis Rabat-Shore, Campus universitaire UIR, Rocade Rabat-Salé, 11100 Sala El Jadida (MA)

(72) Inventeur(s) :
KARTIT ALI ; TAHIRI MOHAMMED

(74) Mandataire :
Bouya Mohsine

(54) Titre : **Méthode de déploiement d'une nouvelle politique de sécurité de Pare-feu dans un réseau informatique.**

(57) Abrégé : La présente invention concerne une méthode de déploiement de nouvelle politique de sécurité de pare-feu pour des réseaux informatique et afin palier aux différents risques d'une politique courante. Il s'agit d'une démarche de mise à jour d'une politique de sécurité initiale (I) basée sur un algorithme qui automatise cette démarche et minimise les risques de sécurité inhérents au moment de déploiement d'une nouvelle politique de sécurité (T). Ceci par la création d'une politique intermédiaire (R) qui reçoit progressivement les nouvelles règles de (T) à implémenter et selon un ordre bien précis. La démarche de déploiement selon l'invention s'achève lorsque la politique (R) est égale la politique cible (T).

MA 54776B1

Méthode de déploiement d'une nouvelle politique de sécurité de Pare-feu dans un réseau informatique.

ABREGE

La présente invention concerne une méthode de déploiement de nouvelle politique de sécurité de pare-feu pour des réseaux informatique et afin palier aux différents risques d'une politique courante. Il s'agit d'une démarche de mise à jour d'une politique de sécurité initiale (I) basée sur un algorithme qui automatise cette démarche et minimise les risques de sécurité inhérents au moment de déploiement d'une nouvelle politique de sécurité (T). Ceci par la création d'une politique intermédiaire (R) qui reçoit progressivement les nouvelles règles de (T) à implémenter et selon un ordre bien précis. La démarche de déploiement selon l'invention s'achève lorsque la politique (R) est égale la politique cible (T).

Contexte de l'invention

En raison de l'insécurité de l'internet et de l'intranet, l'utilisation de pare-feu est une solution très prisée afin de surmonter les problèmes d'accès illégal à l'information.

Actuellement, les politiques de pare-feu peuvent contenir de milliers de règles et ce à cause de la taille énorme et la structure complexe des réseaux modernes. Cela rend la configuration manuelle de ces politiques une mission impossible, même pour les administrateurs réseau expérimentés.

De ce fait, ces politiques nécessitent des outils automatiques fournissant un environnement convivial pour spécifier, configurer et déployer en sûreté une politique cible. C'est pour toutes ces raisons que nous avons pensés à élaborer une nouvelle stratégie sûre et efficace qui va nous permettre de mettre à jour ces politiques. En effet, le fruit de notre invention est une application client/serveur qui répond à toutes ces exigences puisqu'elle est basée sur un algorithme sans équivalent dans le monde technologique. En plus, notre solution contribue à l'amélioration de la capacité à surveiller les menaces de sécurité sur chaque site par le biais des audits périodiques.

Description

La présente invention se rapporte à la conception de nouvelles stratégies sûres et efficaces pour la mise à jour automatique des politiques de sécurité de pare-feu à distance. Il s'agit de créer une application sûre évitant à l'administrateur réseau de perdre trop de temps et d'énergie lors de déploiement manuel des politiques de sécurité. Cet outil convertira l'algorithme qu'on a conçu et qui est présenté dans la figure1 afin de faire le déploiement de politiques de grandes tailles automatiquement, efficacement et rapidement. Ce logiciel est installé et testé sur le serveur au niveau de siège de l'entreprise tandis que les clients sont au niveau des sites. En effet, notre application est capable de mettre à jour les politiques de sécurité de plusieurs pare feux en même temps. En d'autres termes, le déploiement peut se faire, selon le besoin, en unicast, multicast et broadcast.

En plus, notre solution garantit la confidentialité des politiques car l'administrateur central (au niveau de siège) sera le seul qui saura le contenu des différentes politiques qui seront envoyées aux firewalls distants (au niveau des sites).

Etat de l'art antérieur

La demande de brevet **CN108650222A** divulgue une méthode de mise à jour des politiques de sécurité de pare-feu par la mise à jour de règle de pare-feu basé sur un filtrage étendu.

La demande de brevet d'invention **US2006010491A1** concerne un Système de pare-feu protégeant une communauté d'appareils et procédé de mise à jour des règles de pare-feu au sein du système. Ce procédé est constitué d'un filtre des messages à destination et en provenance du réseau auquel est connecté l'appareil mettant en œuvre le procédé. Cette méthode comporte au moins les étapes suivantes : - la détection de l'ajout, du retrait et du bannissement d'un appareil de la communauté ; - la détection des changements d'adresse réseau d'un appareil de la communauté ; - le déclenchement d'un nouveau calcul des règles en réponse au changement de la politique locale de sécurité.

Le brevet de Microsoft **US2008148380A1** divulgue une méthode de mise à jour dynamique des paramètres du pare-feu. Selon son mode de réalisation, la méthode comprend la réception d'une règle de politique qui comprend une référence à un conteneur prédéfini qui spécifie une plage de valeurs autorisée d'au moins un paramètre de pare-feu autorisé en vertu de la règle de politique, la réception d'une valeur de paramètre de pare-feu et le remplissage du conteneur prédéfini avec la valeur de paramètre de pare-feu si la valeur du paramètre de pare-feu se situe dans la plage de valeurs autorisée, mettant ainsi à jour la règle de politique.

Mode de réalisation de l'invention

Selon un mode particulier de réalisation de l'invention, l'administrateur doit s'authentifier avec un identifiant et un mot de passe via une fenêtre d'authentification comme le montre la figure 2. Il doit préciser le chemin du fichier contenant les deux politiques initiale et cible en cliquant sur la commande « Browse » comme le montre la figure 3. Ensuite, il clique sur le bouton "Deploy" pour lancer l'algorithme qui prend en charge le processus de mise à jour.

Selon un mode particulier de réalisation de l'invention, une vérification de la réussite du déploiement de la mise à jour est effectuée (le bouton "Check"). Pour cela, une des deux infobulles s'affiche comme le montre la figure 4. Tout d'abord, nous spécifions le chemin réseau d'un fichier contenant la "Politique actuelle" au niveau du site 1. Et ensuite, nous fournissons le chemin réseau d'un fichier contenant la "Politique cible" au niveau du siège social. Après avoir choisi les deux fichiers que nous voulons, nous les comparons. Ces deux fichiers qui doivent être à la base non identiques afin de changer la politique en cours d'exécution "Politique en cours".

Selon un mode particulier de réalisation de l'invention, il est possible de comparer les performances de notre solution avec la solution de référence "SanitizeIT" (Le bouton "Plot"). En effet, en cliquant sur le bouton "Plot" dans l'interface graphique de l'application, un graphique s'affiche comparant la variation des performances des politiques de sécurité à l'aide des deux algorithmes : Enhanced-Greedy-2-Phase Deployment et SanitizeIT comme le montre la figure 5.

À partir de la courbe affichée, on peut conclure que Enhanced-Greedy-2-PhaseDeployment est plus efficace que SANITIZEIT et que le temps d'exécution est presque linéaire. De plus, SANITIZEIT semble avoir un temps d'exécution polynomial.

Pour renforcer la sécurité, un audit est lancé périodiquement afin de trouver les nouvelles failles au niveau de réseau de chaque site. Suite à cette opération, l'administrateur est amené à concevoir puis déployer une nouvelle politique de sécurité qui répond aux besoins de l'audit de site concerné. On peut conclure que la sécurité des réseaux est un processus continu comme le montre la figure 6.

Sur le plan économique, notre projet contribuera au développement financier au niveau de chiffre d'affaire de toute entreprise possédant des pare-feu au niveau de ses succursales.

Le déploiement d'une politique de pare-feu devrait avoir les caractéristiques suivantes : l'exactitude, la confidentialité, la sureté et la vitesse :

- Exactitude : Un déploiement est exact s'il met en œuvre avec succès la politique de cible sur le pare-feu. Après un déploiement exact, la politique de cible devient la politique en cours d'exécution. L'Exactitude est une exigence essentielle pour tout déploiement.

- Confidentialité : La confidentialité fait référence à la sécurisation de la communication entre un outil de gestion et un pare-feu. En raison de la nature sensible de l'information transmise lors d'un déploiement, la communication entre l'outil de gestion et de pare-feu doit être confidentielle. La confidentialité peut être réalisée en utilisant les protocoles de communication cryptés tels que SSH ou SSL.
- Sureté : Un déploiement est sûr si aucun paquet légal n'est rejeté et aucun paquet illégal n'est accepté pendant le déploiement.
- Vitesse : Un déploiement devrait se faire dans les plus brefs délais, de sorte que l'état final souhaité est atteint le plus rapidement possible. Un algorithme de déploiement doit avoir un temps optimal de fonctionnement, de sorte qu'il soit applicable même pour les politiques de sécurité de taille très grande. Un lent déploiement est désagréable pour les utilisateurs et peut aller à l'encontre du but de déploiement.

L'algorithme présenté dans la figure 1 constitue le cœur de notre invention. Il est conçu pour faire le déploiement automatique d'une politique cible « T » à partir d'une politique initiale « I » en passant par une politique en cours « R ». En effet, notre application est basée entièrement sur set algorithme.

Le déploiement d'une politique est le processus par lequel les commandes d'édition de la politique sont mises sur le pare-feu, de sorte que la politique cible devient la politique en cours d'exécution
Un administrateur réseau ou un logiciel de gestion exécute des commandes sur le pare-feu afin de transformer la politique en cours d'exécution **R** (Running) en une politique cible **T** (Target). L'ensemble de commandes supportées par un pare-feu est appelé son langage d'édition de politiques. Habituellement, un pare-feu utilise le sous-ensemble de commandes d'édition suivantes :

(app r) ajoute la règle r à la fin de R.
(del r) supprime r de R.
(del i) supprime la règle à la position i de R.
(ins i r) insère r en position i.
(mov ij) déplace la règle i à la position j dans R.

Description des figures

La présente invention sera décrite par l'intermédiaire des figures détaillées du monde de réalisation préféré, en référence aux figures.

Fig.1 : représente notre propre algorithme qu'on a conçu et qui constitue le cœur de l'invention.

Fig.2 : illustre l'authentification de l'administrateur avec un identifiant et un mot de passe. Cette étape est très importante car le processus de mise à jour doit se faire uniquement par l'administrateur.

Fig.3 : représente l'interface de l'application permettant le déploiement de la politique. Pour cela, l'administrateur doit préciser le chemin du fichier contenant les deux politiques : initiale et cible.

Fig.4 : montre l'interface de vérification de mise à jour. Elle est chargée de vérifier les deux politiques avant et après le déploiement.

Fig.5 : affiche les performances de notre solution avec la solution de référence "SanitizeIT".

Fig.6 : résume le processus complet de mise à jour d'une politique de sécurité de pare feu. En effet, ce processus commence par la vérification de l'identité de la personne qui se chargera d'amener cette opération, passant par la découverte des failles au niveau de réseau et enfin, par la conception et le déploiement d'une nouvelle politique qui va corriger les défauts trouvés auparavant.

Revendications

1. Méthode de déploiement de politique de sécurité de pare-feu composée des étapes suivantes :
   - Authentification par un administrateur.
   - Audit pour identifier les failles de sécurité au niveau du réseau de chaque site.
   - Conception et création du fichier contenant la nouvelle politique de sécurité qui va répondre aux failles détectées.
   - Déploiement de la nouvelle politique de sécurité selon le procédé suivant (figure 1) :
     - Prendre comme paramètre la politique initiale (I) et la politique cible (T).
     - Création d'une politique intermédiaire (R) étant vide au démarrage du process et qui est rempli pendant l'exécution de la méthode.
     - Insérer progressivement les règles de la politique cible dans la politique intermédiaire appelée (R).
     - Achèvement du déploiement lorsque la politique intermédiaire (R) est égale à la politique cible (T).

2. Méthode de déploiement de politique de sécurité de pare-feu selon la revendication 1 caractérisé en ce que si une règle dans (T) existe déjà dans (I) celle-ci sera déplacée vers la position prédéfinie par (T) dans (R).
3. Méthode de déploiement de politique de sécurité de pare-feu selon la revendication 1 caractérisé en ce que si une règle dans (I) n'existant pas dans (T) celle-ci sera supprimé dans (R).
4. Méthode de déploiement de politique de sécurité de pare-feu selon la revendication 1 caractérisé en ce que si une règle dans (T) est redondante celle-ci sera supprimée.

5. Méthode de déploiement de politique de sécurité de pare-feu selon la revendication 1 caractérisée en ce que le déploiement automatique des politiques de sécurité de pare-feu de bout en bout càd du serveur se trouvant au niveau de siège qui constitue la source des mises à jour vers le pare feu se trouvant au niveau de site ou la filiale qui va recevoir les mises à jour provenant de la source.

MA 54776B1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 54776	Date de dépôt : 29/10/2021
Déposant : Université Internationale de Rabat	
Intitulé de l'invention : Méthode de déploiement d'une nouvelle politique de sécurité de Pare-feu dans un réseau informatique.	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de forme et de clarté
- ☐ Cadre 5 : Défaut d'unité d'invention
- ☐ Cadre 6 : Observations à propos de certaines revendications exclues de la brevetabilité
- ☒ Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 24/05/2022
Téléphone: **212 5 22 58 64 14/00**	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  5 Pages
- Revendications
  1-5
- Planches de dessin
  6 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : G 06F 17/00
CPC : H04L63/00

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, IEEE, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
A	CN112491822 ; ZHONGYING YOUCHUANG INF TECH CO LTD ; 12/03/2021	1-5
A	CN111786949 ; SHANDONG LUNENG SOFTWARE TECH CO LTD ; 16/10/2020	1-5

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté	Revendications 1-5 Revendications aucune	Oui Non
Activité inventive	Revendications 1-5 Revendications aucune	Oui Non
Application Industrielle	Revendications 1-5 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : CN112491822

1. Nouveauté

Aucun document ne divulgue l'objet des revendications 1-5 qui est donc nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. Activité inventive

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1 et divulgue (voir abrégé et description de D1):
Une méthode de déploiement de politique de sécurité de pare-feu composée des étapes suivantes :

- Authentification par un administrateur.
- Audit pour identifier les failles de sécurité au niveau du réseau de chaque site.
- Conception et création du fichier contenant la nouvelle politique de sécurité qui va répondre aux failles détectées.
- Déploiement de la nouvelle politique de sécurité.

L'objet de la revendication 1 diffère de D1 en ce que : le déploiement de la nouvelle politique de sécurité est réalisé selon le procédé suivant :

- Prendre comme paramètre la politique initiale et la politique cible ;
- Création d'une politique intermédiaire étant vide au démarrage du process et qui est remplie pendant l'exécution de la méthode ;
- Insérer progressivement les règles de la politique cible dans la politique intermédiaire.
- Achèvement du déploiement lorsque la politique intermédiaire est égale à la politique cible.

Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : Fournir une alternative au procédé de déploiement d'une politique de sécurité pare-feu.

Aucun document de l'état de la technique ne contient un enseignement ou une suggestion sur la solution proposée. Par conséquent, l'objet des revendications 1-5 implique une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

3. Application industrielle

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.