Actes de la conférence WACREN 2016

Etude du nomadisme dans un Cloud éducatif administré par la technologie SDN/OpenFlow

Traore Issa, Kouassi Brou Médard, Atta A. Ferdinand

Institut de recherches mathématique
Université Félix Houphouët-Boigny
08 BP 2035 Abidjan 08
issa.traore@univ-fhb.edu.ci

Résume. *Le Cloud Computing permet de partager, chez un fournisseur d'offres Cloud, une infrastructure réseau, une solution applicative ou une plateforme. Le recours au Cloud Computing pour les NRENs implique un renforcement de la sécurité, notamment en matière d'accès nomade via un service VPN. Dans ce contexte de haute virtualisation, il est possible de fournir une nouvelle architecture réseau dynamique fournissant la gestion contrôlée et efficiente de la transmission dans les nœuds du réseau.*
Dans cet article, nous décrivons une architecture SDN (Software-Defined Networking), qui permet à des postes nomades de s'authentifier puis accéder de manière sécurisée aux ressources génériques, sécurisées de l'intranet de son NREN.

Abstract. *Cloud Computing allows to share, in a provider Cloud provider, network infrastructure, application solution or platform. The use of cloud computing for NRENs involves strengthening security, particularly in terms of mobile access via a VPN service. In this context of high virtualization it is possible to provide a new dynamic network architecture providing controlled and efficient management of transmission in the network nodes.*
In this work, we describe an architecture SDN (Software-Defined Networking), which allows mobile workstations to authenticate and secure access to generic resources, secure intranet for its NREN.

Mots clés : *Cloud Computing, VPN, SDN, OpenFlow, IPSec, nomades.*
Keywords*: Cloud Computing, VPN, SDN, OpenFlow, IPSec, mobile.*

1. Introduction

Le Cloud Computing est un modèle Informatique qui permet un accès facile et à la demande par le réseau à un ensemble partagé de ressources informatiques configurables (serveurs, stockage, infrastructures réseaux, applications et services) voir [1] et [6]. Il fournit des services ou des applications informatiques en ligne, accessibles partout, à tout moment, et de n'importe quel terminal (smartphone, PC de bureau, ordinateur portable et tablette).
C'est ainsi que le Cloud Computing suscite beaucoup d'intérêt, car il apporte la réduction du matériel informatique, la haute disponibilité et le nomadisme.
Dans cet article, nous construisons une infrastructure Cloud Computing avec une architecture SDN (Software Defined Networking) traduit par

"réseau défini par le logiciel" voir [1], [3] et [4]. Le contrôleur de SDN embarque un certain nombre de directives grâce aux APIs voir [7] et [9]. Il contrôle le comportement des éléments du réseau sous-jacents via le protocole OpenFlow. Ainsi dans le SDN, Les routeurs effectuent essentiellement des fonctions de commutation, d'où la désignation de «switchs OpenFlow».
Nous proposons dans la deuxième partie de cet article de présenter la méthode SDN et le protocole OpenFlow. La troisième partie est consacrée au fonctionnement et à l'algorithme du tunnel SDN dans le contexte du nomadisme. Une analyse de notre proposition permet de conclure le travail.

2. Le modèle SDN

2.1. Le routage Classique des réseaux.

Dans les réseaux classiques, le routeur travail sur plusieurs plans décrit par la figure 1. Il contrôle le routage (recherche de la meilleure route), il contrôle le flux de données, gère la configuration et la transmission. L'ajout ou la modification d'équipements et l'implémentation d'une politique réseau est complexe, longue et peut être source d'interruption de service. Ce qui décourage les modifications et l'évolution du réseau.

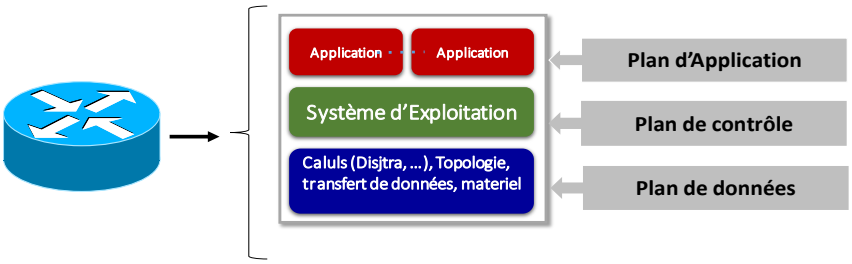

Figure 1. *Routage Classique*

La gestion de la topologie s'accompagne souvent d'une charge de calcul significative voir [9]. Par exemple, le protocole de routage OSPF exige de chaque routeur un travail important chaque fois qu'une modification topologique du réseau lui est signalée. Ce calcul est en effet nécessaire pour appliquer l'algorithme de Dijkstra, qui permet de déterminer les routes optimales vers les hôtes distants.

2.2. L'architecture SDN

Le SDN présente une architecture réseau où le plan de contrôle est totalement découplé du plan de données, cela est illustré par la figure 2. Selon [1] ce découplage est une approche de la gestion des réseaux dans

laquelle le contrôle est dissocié du matériel et transféré à une application logicielle appelée contrôleur.
Le plan de contrôle est relié aux équipements réseaux par le protocole OpenFlow décrit dans la figure 3.

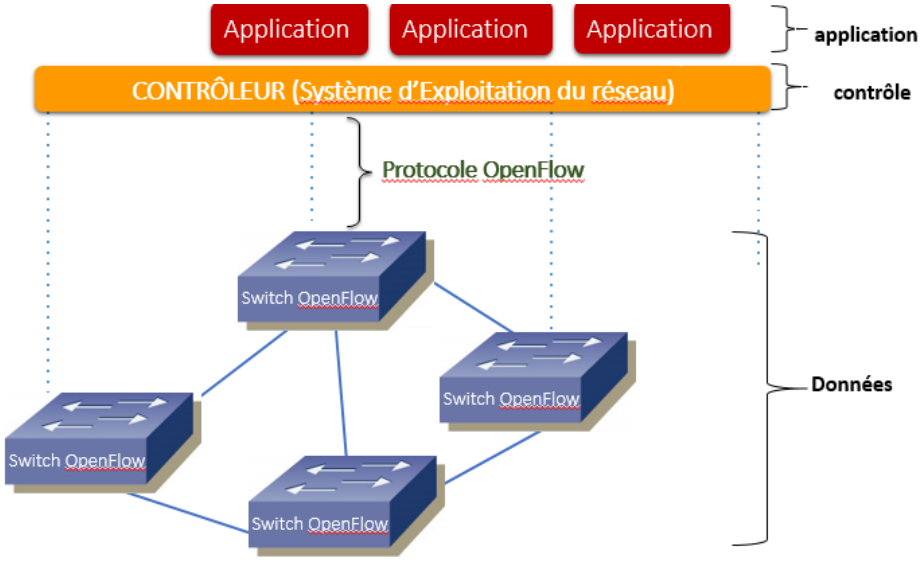

Figure 2. *Architecture SDN*

Ainsi, dans une approche SDN, la charge de calcul associée au contrôleur est en grande partie retirée des routeurs. Le contrôleur, est donc chargé du calcul et de la mise à jour des tables de routage,
D'après [8] et [9] OpenFlow est une interface de communication entre le plan de contrôle et le plan de données d'une architecture SDN. C'est un protocole développé pour permettre la communication entre contrôleurs et switchs OpenFlow.

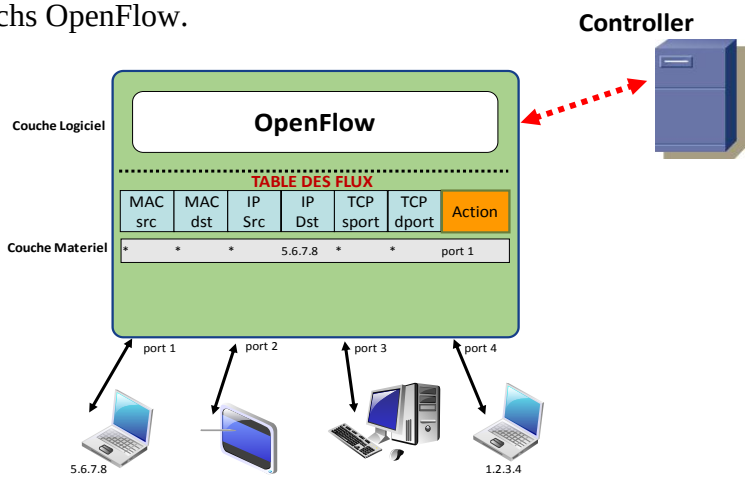

Figure 3. *Fonctionnement du protocole OpenFlow.*

Il permet d'accéder directement à la gestion et la configuration du plan d'acheminement des périphériques réseau tels que les switch OpenFlow, à la fois physiques et virtuels. Lorsqu'un switch reçoit un packet pour la première fois, il ne sait pas qu'elle action effectuée. C'est le contrôleur qui lui donne les directives de transmissions. Dans la section suivante, nous expliquons le fonctionnement de ce processus.

2.3. Fonctionnement du protocole OpenFlox

OpenFlow sert de lien entre le plan de contrôle et le plan de données. L'échange de messages se fait au cours d'une session TCP établie via le port 6653 du serveur contrôleur voir [4]. Le comportement d'un switch OpenFlow est alors déterminé par une ou plusieurs tables de flux (flow table) illustré par la figure 3. Chaque table s'assimile à un ensemble de flux, qui consistent chacune en une liste de discriminants relatifs au contenu d'une trame, associée à des actions de traitement à appliquer aux trames correspondantes.

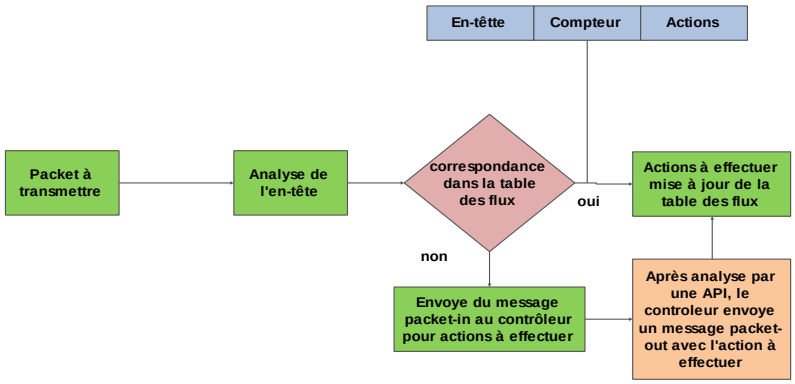

Figure 4. *Base d'échange entre Switch et le contrôle via OpenFlow.*

Lorsqu'un paquet parvient au switch, les valeurs contenues dans ses en-têtes sont comparées aux différents jeux de valeurs enregistrés dans la première table de flux du switch illustré à la figure 4. Les actions qui peuvent suivre sont de diverses natures : transfert de la trame par une interface, suppression, modification de champs d'en-têtes, et/ou transmission du traitement à une table de flux ultérieure, demande de directive au contrôleur.
Lorsque le contrôleur reçoit un message packet-in du switch, lui demandant l'action à effectuer, le contrôleur analyse le packet par l'intermédiaire des APIs du plan de contrôle. Ensuite, il donne les directives au switch grâce au message packet-out.

3. Principe et fonctionnement des clients VPN nomades

3.1. Authentification des nomades

L'accès nomade par la technologie VPN IPSec est la solution la plus intégrée voir [1]. Elle permet aux utilisateurs nomades d'arriver directement dans le sous-réseau de leur NREN.
Le fonctionnement d'IPsec repose sur la négociation et la création de SA (Associations de Sécurité). Ces SA sont gérées par le protocole IKE qui se charge de la phase d'authentification. Dans notre cas, l'authentification des utilisateurs se fait par la méthode SSO (Single Sign-On) sur la base d'annuaire LDAP via un, serveur Radius alimenté par les annuaires des NRENs. Cette méthode d'authentification permet à un utilisateur d'accéder à plusieurs applications informatiques ou services en ne procédant qu'à une seule authentification.
Outre les attributs standards (login/mot de passe pour l'authentification), le schéma de l'annuaire contient les définitions nécessaires pour la configuration du client. Dès que le tunnel est créé, l'utilisateur nomade bénéficie de la protection et de la politique de sécurité locale définies dans son NREN.

3.2. Contexte des NRENs et du WACREN

Les réseaux et Datacenter des NRENs étant virtualisés et existant sous forme de Cloud. Dans ce contexte de haute virtualisation, la technologie SDN est orientée vers la transmission de données dans le réseau virtuel du NREN. Chaque NREN à sa politique de gestion du réseau. Cependant, certaines données des NRENs pourront être mutualisées ou des travaux collaboratifs seront initiés entre des laboratoires des NRENs différents.
Dans ce contexte, la position du réseau WACREN (interconnexion des NRENs) est celle d'un opérateur réseau. Il s'agit simplement de fournir un accès réseau de niveau 2 (couche liaison) ou de niveau 3 (couche réseau). Le réseau WACREN doit posséder l'annuaire de tous les NRENS pour faciliter le nomadisme dans ce vaste réseau.
Dans la section suivante, nous exposons le processus d'accès aux ressources d'un nomade qui n'est pas dans son NREN.

3.3. Fonctionnement des services nomades

Un utilisateur nomade ne se trouvant pas dans le réseau local de son NREN n'a pas accès aux ressources jugées sensibles donc sécurisées par l'administrateur du réseau. Seule une connexion VPN / IPSec pourra lui conférer la possibilité de consulter ces ressources.

Le client nomade envoie une requête pour avoir accès aux ressources de son NREN, cela est décrit dans figure 5. Le switch vérifie dans la table des flux. S'il y a correspondance avec une table, alors il effectue l'action de création d'un tunnel SDN (cela signifie que le client nomade s'est déjà connecté à son NREN en situation de nomade). S'il n'y a pas de correspondance dans la table des flux, le switch envoie un message packet-in au contrôleur. Celui-ci vérifie analyse l'en-tête du message puis demande au switch à travers le message packet-out de demander au client de s'authentifier.
Si l'authentification du client est correcte, le tunnel SDN est créé. Sinon, la requête la création du tunnel est rejetée. Après ce processus, le client obtient une adresse IP virtuelle de son NREN. La figure 6 illustre l'algorithme d'authentification et de création du tunnel SDN.
Le nomade ayant désormais une adresse IP de son NREN, pourra avoir accès aux ressources sécurisé dont il a le profil d'utilisation.
La figure 3 décrit l'algorithme d'un utilisateur se trouvant dans le réseau local. Les différents switchs auront la possibilité d'envoyer les données d'un point du réseau jusqu'à la ferme serveur illustré sur la figure 6.
Il est important de préciser que le nomade aura droit aux ressources en fonction de son niveau de privilège décrit dans son NREN.

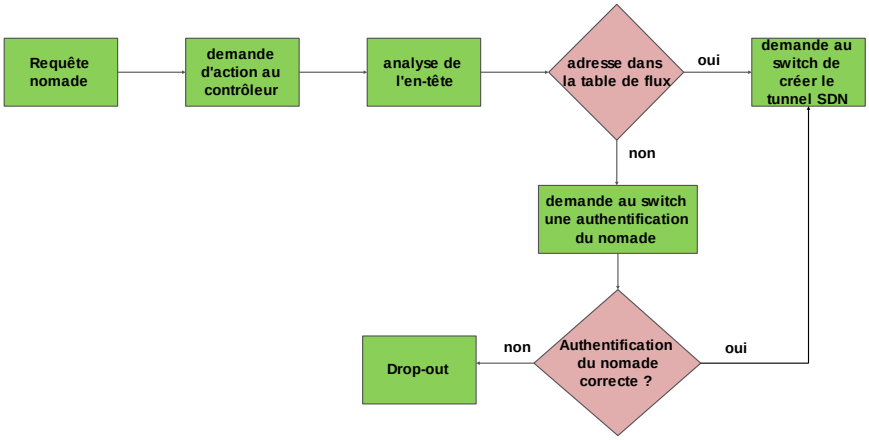

Figure 5. *Etape de création du tunnel SDN.*

Le processus inverse message packet-in des switchs et le message packet-out permet l'échange de la ferme serveur vers le nomade voir [2] et [8].

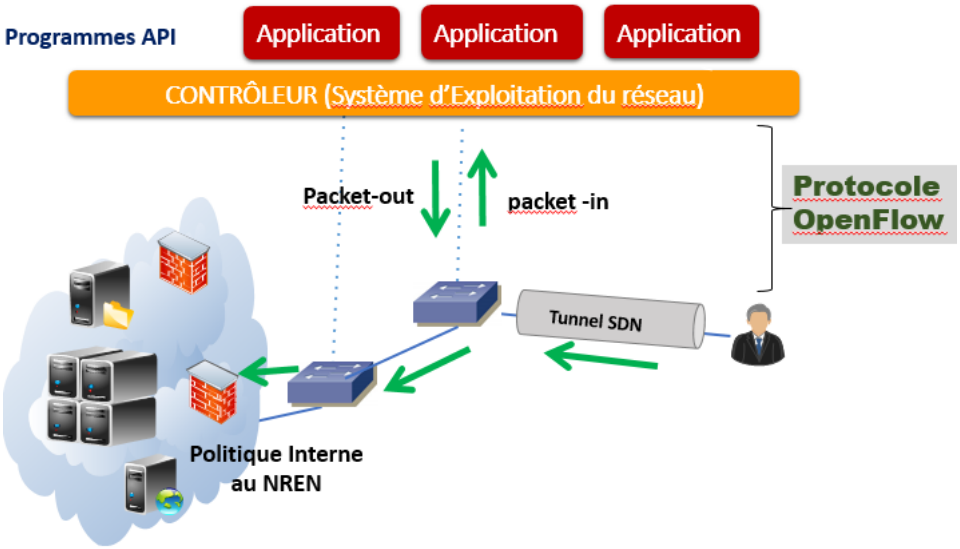

Figure 6. *Accès aux ressources du Cloud par un tunnel SDN*

Les applications sont des APIs (Application Programmable Interface), ce sont des programmes pour indiquer des actions au contrôleur voir [5]. Ce dernier agit comme un Système d'exploitation, il est l'interface entre les switch OpenFlow et les APIs tournant sous NOX (écrit en C++/ Python).

4. Analyse de la solution du tunnel SDN dans le Cloud

Le contrôleur gère les switchs via le protocole OpenFlow. En utilisant ce protocole, le contrôleur peut ajouter, modifier et supprimer des entrées de flux, à la fois d'une façon réactive (en réponse à des paquets) et de façon proactive. Ainsi, le contrôleur est l'élément central du réseau qui peut communiquer avec tous les nœuds afin de configurer leurs tables de transfert. Dans l'architecture SDN, lorsque le contrôleur gère plusieurs réseaux ayant des switchs OpenFlow compatibles, il est nécessaire qu'il soit de type FlowVisor. En effet, FlowVisor est un contrôleur OpenFlow spécial qui se comporte comme un proxy transparent entre les swithes OpenFlow et plusieurs contrôleurs OpenFlow. FlowVisor permet de créer des tranches de réseau et d'en déléguer le controle à différents contrôleurs.

Cependant, une question de sécurité se pose. En effet, le contrôleur a tous les pouvoirs sur le réseau. Il faut être sûr que la communication entre le plan de contrôleur et les switchs OpenFlow physiques ou virtuels sont sécurisées. Hautement virtualisé, le SDN diffère des paradigmes réseaux classiques, ce qui introduit de nouveaux enjeux de sécurité dans le même registre que celui du Cloud Computing.

La protection d'un switch OpenFlow passe donc par le cloisonnement et l'intégrité des communications des réseaux d'administration et de production, ainsi que l'utilisation exclusive de TLS/SSL sur le réseau d'administration pour assurer une sécurité de la connexion.

5. Conclusion

Le Cloud Computing offre aujourd'hui un service mutualisé des connexions sécurisées par les serveurs VPN virtuels. Les NRENs ayant des difficultés de réaliser une infrastructure moderne de haute disponibilité pourront se tourner vers ce modèle.

Le SDN ou réseaux définis par logiciels et la virtualisation des fonctions réseau NFV (Network Function Virtualization) sont de nouvelles façons de concevoir, construire et exploiter les réseaux de manière efficiente. Le nomadisme implique l'authentification SSO du nomade par l'intermédiaire d'une annuaire LDAP. Tout chercheur d'une NREN est un nomade dans le NREN d'un autre pays du WACREN.

La mise en place d'un annuaire global de tous les nRENs du WACREN facilitera l'intégration de l'ensemble des enseignants, des chercheurs et des étudiants et de fédérer tous les services autour d'une authentification unique.

Cela permettra aux étudiants, enseignants et chercheurs d'être dans le réseau WACREN regroupant les pays de l'Afrique de l'ouest et central.

Nous travaillons actuellement à prototyper notre solution grâce à un émulateur très utilisé dans le domaine de la recherche sur les réseaux SDN nommé **Mininet**.

6. Bibliographie

[1] Guy Pujolle; *Les réseaux; Eyrolles* ; Edition 2014

[2] Pate!, A., Ji, P., and Wang, T. ; *Qos-aware optical burst switching in openflow based software-defined optical networks*. In Optical Network Design and Modeling (ONDM); 2013

[3] Pfaff, B., LANTZ, B., HELLER, B., et al. *Openflow switch specification, version 1.3.* 0; Open Networking Foundation; 2012

[4] Open Networking Foundation (OIF); *OpenFlow Switch Speification, version 1.5.1* (protocol version ox06) ; 26 mars 2016

[5] 17th International Conference on, pages 275-280. Sezer, S., Scott-Hayward, S., Chouhan, P., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M., and Rao, N. ; *Are we ready for sdn? implementation challenges for software-defined networks.* Communications Magazine, IEEE; 51(7) :36-43. 2013

[6] Sherwood, R., Gibb, G., Yap, K.-K., Appenzeller, G., Casado, M., McKeown, N., and Parulkar, G. Flowvisor : *A network virtualization layer*. *Technical Report OpenFlow Switch Consortium Openflow-tr*-2009-1; Stanford University; 2009
[7] Shin, M.-K., Nam, K.-H.; and Kim, H.-J. *Software-defined networking (sdn)* : A reference architecture and open apis; In IEEE International Conference on ICT Convergence, pages 360–361; 2012
[8]Xavier Jeannin , GIP RENATER; SDN / Open Flow dans le projet de recherche de GEANT (GN3+) ; JRES 2013
[9] Xenofontas Dimitropoulos et al ; *Software Defined Networks (SDN)*; Spring