Communication Machine to Machine sécurisée appliquée aux workflows

Présenté par : Constantin DIVRIOTIS

Encadré par : Andréas GUILLOT

Equipe réseaux - UFR Mathématique et Informatique - Université de Strasbourg

constantin.divriotis@etu.unistra.fr

15 Mai 2019

Overview

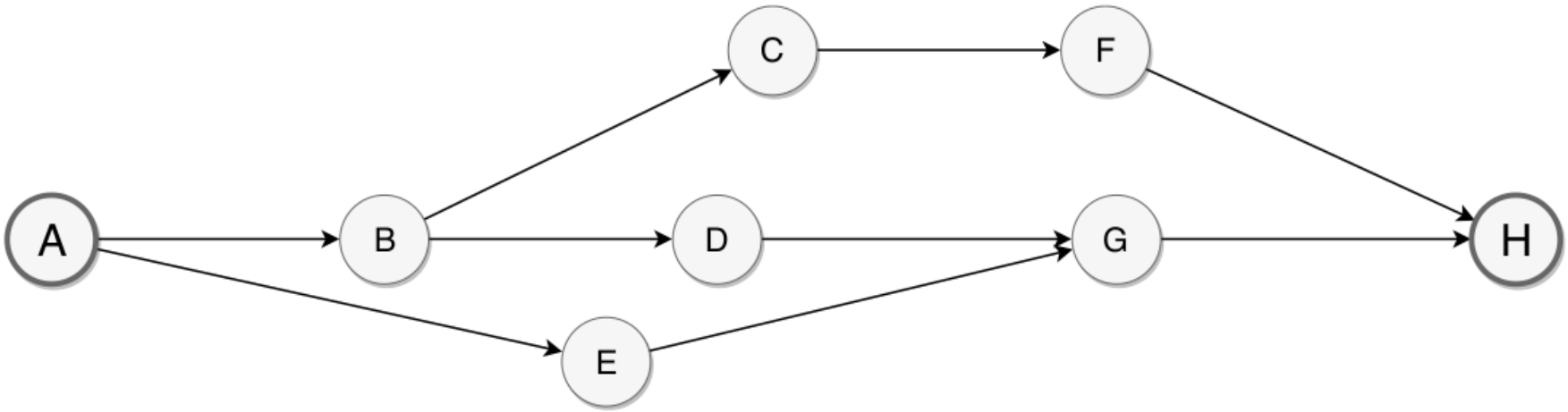

Figure 1: Exemple de workflow contenant un ensemble de communications entre différents acteurs

Qu'est que le cloud computing ?

Définition du NIST

Modèle établissant un accès à distance via le réseau, à la demande et en libre-service, à des ressources informatiques partagées configurables

Sécurité du cloud

Disponibilité : ressources toujours accessibles

Integrité : impossible de modifier ou supprimer sans autorisation un fichier

Confidentialité : données secrètes

Contrôle : gestion des ressources

Authentification : garantie l'identité d'un utilisateur

Non-répudiation : un utilisateur ne peut pas remettre ses actions en cause

Enjeux de la sécurité du cloud

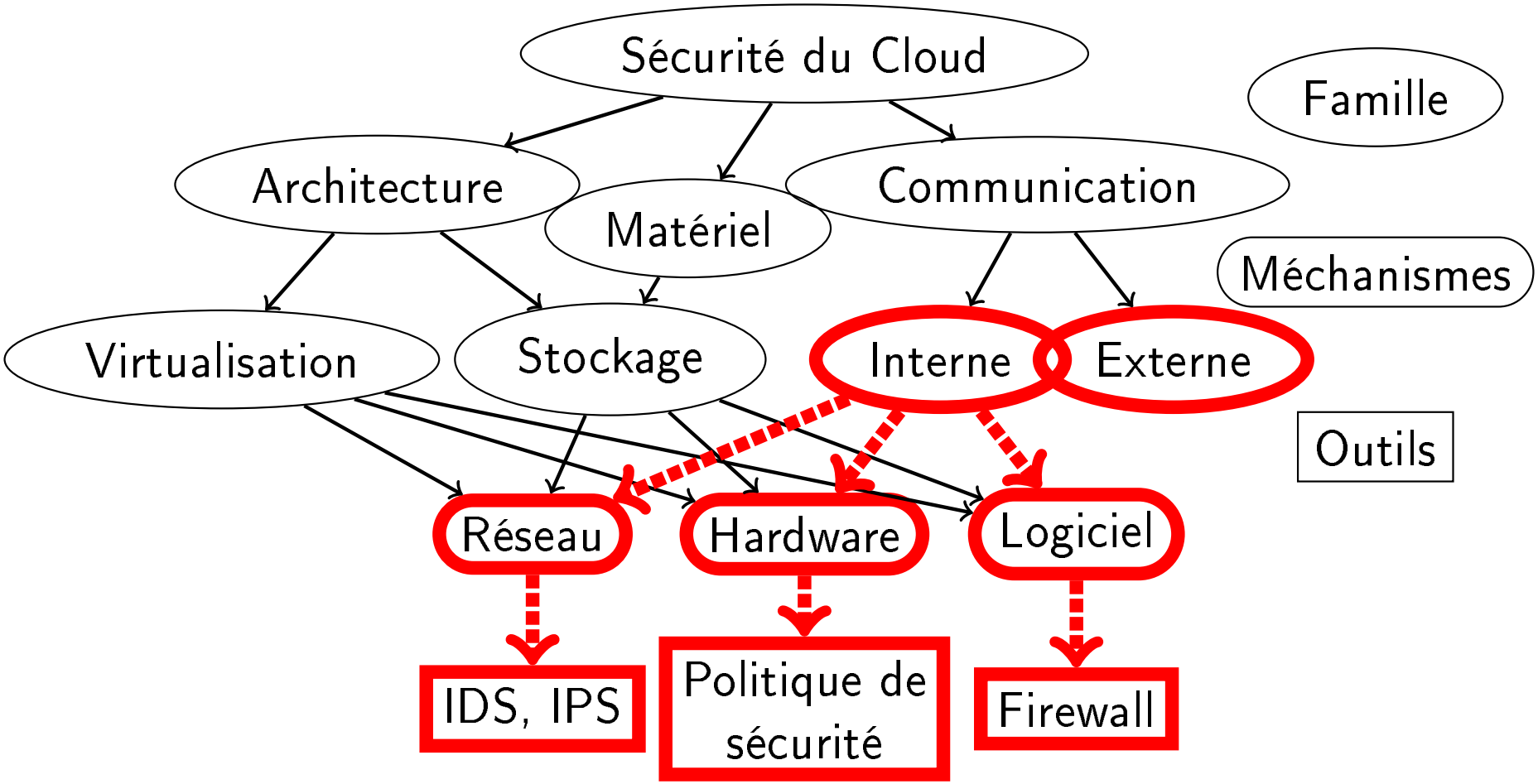

Figure 2: Challenges de la sécurité du cloud

Enjeux de la sécurité du cloud

Problématique

Comment obtenir un réseau sécurisé tout en garantissant un niveau de performance élevé et une confiance limitée à tous les niveaux ?

Cas d'étude : *Tree-Rule firewall*[1]

- Faire respecter la politique de sécurité du réseau
- Environnement cloud
- *Listed-Rule firewall* présente de gros inconvénients tels que :
  - Présence de *Shadowed Rule*
  - Changements de positions des règles problématiques
  - Règles redondantes possibles
  - Configuration difficile
  - Recherche séquentielle

[1] X. He, T. Chomsiri, P. Nanda, Z. Tan, Improving cloud network security using the tree-rule firewall,Future Gener. Comput. Syst. 30 (2014) 116–126

Cas d'étude : *Tree-Rule firewall*

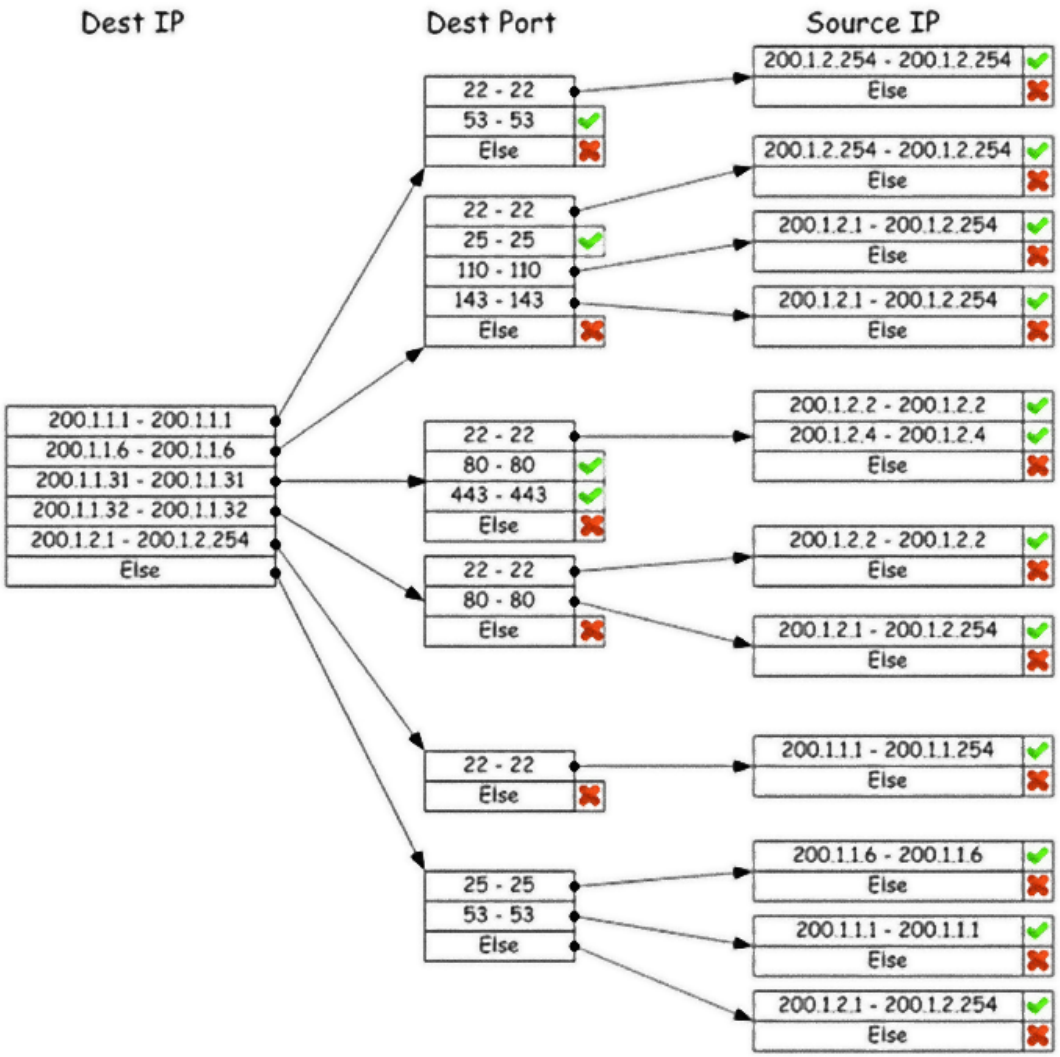

Figure 3: Structure d'un *Tree-Rule firewall*

Cas d'étude : *Tree-Rule firewall*

	ESXi firewall	5Nine vFirewall	IPTABLES	Tree-Rule firewall
Can protect hypervisor	Yes	Yes	Yes	Yes
Can protect internal VMs	No	Yes	Yes	Yes
Can prevent attacking between VMs	No	Yes	Yes	Yes
Stable	Yes	No	Yes	Yes
Fast packet decision	No	No	No	Yes
Support more than 5000 rules	No	No	No	Yes
No shadowed/redundant/confliction rules	No	No	No	Yes
No down time for adding new VMs	No	Yes (only on Hyper-V)	No	No

Figure 4: Comparaison des fonctionnalités de différents firewall dans un environnement cloud

Conclusion et perspectives

Conclusions

- Le cloud a généré de nouveaux problèmes
- Propositions de plusieurs pistes répondant à la problématique
- *Tree-Rule firewall* est un exemple

Perspectives

- Gestion d'IPv6, du NAT ou encore des VPNs dans le *Tree-Rule firewall*
- Décalage entre la sécurité mise en place et l'évolution des technologies actuelles, comment y remédier ?

References

Peter Mell and Timothy Grance (2011)
The NIST Definition of Cloud Computing
NIST Special Publication, 800-145.

Mazhar Ali, Samee U. Khan and Athanasios V. Vasilakos (2015)
Security in cloud computing: Opportunities and challenges
Elsevier : Information Sciences, 305, 357-383.

X. He, T. Chomsiri, P. Nanda and Z. Tan (2014)
Improving cloud network security using the tree-rule firewall
Elsevier : Future Generation Computer Systems, 30, 116-126.

Merci de votre attention