Router Framework for Secured Network Virtualization in Data Center of IaaS Cloud

Anant V. Nimkar and Soumya K. Ghosh

Abstract Data center exploits network virtualization to fully utilize physical network resources by collocating tenants' virtual networks. The virtual networks consist of sets of virtual routers connected by virtual links. The network virtualization must efficiently embed virtual networks on a physical network of the data center to balance load among physical resources to fully utilize the physical network. The virtual networks must also be securely managed so that they are not compromised by collocated users or a data center network administrator who has direct access to the physical network. In this paper, we propose a router framework in which virtual routers and links can be securely placed on physical router by adding a virtual plane on top of data and control planes, two abstract protocols and an enforcement of Federation Access Control Model (FACM). The two abstract protocols, viz. Secure Virtual Topology Embedding Protocol (SVTEP) and Node-and-Path Label Distribution Protocol (NPLDP) are presented along with a theoretical evaluation of the proposed router framework to fulfill all the aforesaid requirements.

Keywords Router framework · Access control model · Network virtualization · Virtual network embedding · IaaS · Cloud · Data center

1 Introduction

Network Virtualization Environment (NVE) supports virtual networks on top of physical network [1]. Virtual networks consist of virtual nodes and virtual links which are placed on physical routers and physical paths respectively. The virtual

A.V. Nimkar (✉) · S.K. Ghosh
School of Information Technology, Indian Institute of Technology,
Kharagpur 721 302, India
e-mail: anantn@sit.iitkgp.ernet.in

S.K. Ghosh
e-mail: skg@iitkgp.ac.in

A. Nagar et al. (eds.), *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Smart Innovation, Systems and Technologies 44, DOI 10.1007/978-81-322-2529-4_50

resources (i.e. virtual nodes and links) are collectively managed by stakeholders in network virtualization [2]. Network virtualization also needs node and link mapping algorithms so that the loads among physical routers and links are balanced [3]. The main challenge for deploying network virtualization is weaknesses in router virtualization for topology-aware applications [4] and IaaS Cloud Federation [2]. The weaknesses are minimal security provision for management of virtual resources, no load balancing on physical resources and no transparent mapping between physical and virtual resources. Recent router architectures [5–7] install control and data planes, in both centrally or distributively, using container or hypervisor based virtualization. None of the recent architectures e.g. Microsoft SoftRouter [8], OpenVRoute [9] and FIBIUM [10] concentrate on secure management of virtual resources except AVR [11] which allow secure creation and deletion of virtual routers but no secure configuration of virtual routers. Thus, router architectures face three major issues, namely (i) Secure and transparent management of collocated virtual resources, (ii) Load balancing for efficient and secure placement of virtual routers and links on physical router and links respectively, and (iii) Secure mapping between physical and virtual networks.

In this paper, we propose a layered router framework to address the aforementioned issues. The proposed router framework does not significantly change the standard router architecture and it only adds another *virtual plane* on top of control and data plane of existing standard router architecture. The proposed router framework augments a deploy-able unit of Federation Access Control Model (FACM) [12], network embedding algorithm and signaling protocol to provide secure load balancing, management of virtual resources and secure mapping between physical and virtual networks.

The main contributions of the paper has two parts: (i) Router framework for secured multi-tenant network collocation using a security component *Access Control Enforcement Engine* and (ii) Two abstract protocols, viz. *Node-and-Path Label Distribution Protocol* and *Secured Virtual Topology Embedding Protocol*. *Access Control Enforcement Engine* (ACEE) enforces FACM to address the issue of secure management of virtual resources in network virtualization. The abstract *Node-and-Path Label Distribution Protocol* (NPLDP) addresses the issue of mapping tenants' virtual networks to the physical network. The abstract *Secured Virtual Topology Embedding Protocol* (SVTEP) addresses the issue of uniformly distributing virtual nodes and links over the physical network.

The rest of the paper is organized as follows. The related work on architectures of router virtualization is given in Sect. 2. Section 3 presents background works on *Network Virtualization*, *IaaS Cloud Federation* and *Federation Access Control Model*. Section 4 proposes a router framework by adding *Node-and-Path Label Distribution Protocol* (Sect. 4.1), *Secured Virtual Topology Embedding Protocol* (Sect. 4.2), *Access Control Enforcement Engine* (Sect. 4.3) and the Information Bases (Sect. 4.4) to standard router architecture. Section 4.5 presents the working principle and theoretical evaluation of the proposed router framework. Finally, Sect. 5 concludes this work and gives the future works.

2 Related Work

The router framework for secure network virtualization needs investigation of recent router architectures and virtualization techniques to address the aforesaid three issues. Mattos et al. [7] evaluate three virtualization techniques, namely OpenVZ, Xen and VMware through four metrics namely memory, processor, network and disk performance of virtual routers. The evaluation shows that OpenVZ and Xen return a small performance overhead in terms of memory, processor and disk performance while OpenVZ and Xen return moderate and good network performance respectively. VMware offers fully virtualized solution but introduces significant overhead in handling virtual resources. Autonomic Virtual Routers (AVR) [11] provides automatic virtual router provisioning which serves as a recommendation for the separation of data and control planes in virtual routers. In SoftRouter architecture [8], control planes are far away from data planes. This separation provides easier scalability. SoftRouter does not securely manage virtual resources. FIBIUM [10] is hardware accelerated software router using virtualization on commodity PC and the separation of control and data planes on OpenFlow-based switches. Open Router Virtualization [13] allows data plane and control planes of virtual routers on server and OpenFlow switches respectively. It provides programming interfaces for forwarding plane. OpenVRoute [9] distributes data plane and control plane of virtual routers on server and OpenFlow switches respectively and uses Flow Management Proxy (FMP) to establish communication between data and control planes. Virtual Router as Service (VRS) [14] is a distributed service of forwarding planes of virtual routers and it optimally places forwarding plane and virtual links using some embedding algorithm. VROOM (Virtual ROuters On the Move) [15] provides network-management primitives to freely move virtual routers from one physical router to another physical router.

3 Background

The proposed router framework extends standard router architecture and uses Federation Access Control Model. This section provides fundamentals of Network Virtualization, IaaS Cloud federation and Federation Access Control Model.

3.1 Network Virtualization and IaaS Cloud Federation

Network virtualization environment facilitates collocation of multiple virtual networks on top of physical networks. Virtual network consists of virtual routers and links created on physical nodes and paths respectively. Figure 1 shows two virtual networks collocated on the same physical network. The black plain line polygon

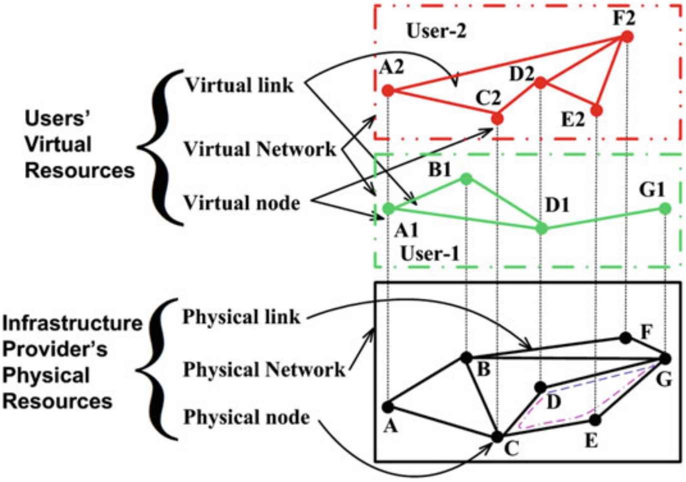

Fig. 1 Network virtualization

shows the physical network infrastructure of cloud provider. The virtual networks of User-1 and User-2 are represented in green dot-dash and red double-dot-dash polygons respectively. The node allocation algorithm map virtual nodes to physical node. Each virtual link is mapped to a physical path using some link allocation algorithm. The virtual nodes A1 and A2 are mapped onto physical node A. Similarly, the virtual link, (D1,G1) can be mapped to the direct edge, D-G or path, D-C-E-G.

IaaS Cloud federation provides virtual nodes, virtual machines and virtual links to get the economies of scale through federation among cloud providers. Figure 2 shows an example of a cloud federation among three IaaS cloud providers for two users. The green dot-dash and red double-dot-dash polygons show the virtual infrastructures of User-1 and User-2 respectively. The virtual nodes e.g. E1, E2, M1 etc. are cooperatively managed by users and corresponding IaaS cloud providers. Similarly, virtual links are managed by user and one/two IaaS cloud provider(s) e.g. the virtual link (H2,Q2) is cooperatively managed by User-2, Cloud Provider-2 and Cloud Provider-3 while the virtual link (L2,Q2) is cooperatively managed by User-2 and Cloud Provider-3. Management of all federated virtual resources among IaaS cloud providers needs a special kind of access control mechanism FACM which handles federated resources.

3.2 Federation Access Control Model

Federation Access Control Model [12] is MAC-and-DAC based access control model to access virtual resources by subjects which are sets of participants from

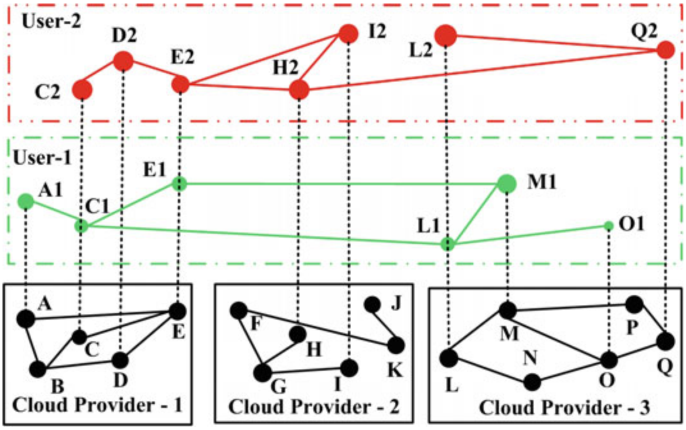

Fig. 2 IaaS Cloud federation

federated infrastructure providers (InPs) and users. Each InP $j \in E$ maintains a part of FACM as $F_j = (S_j, O_j, P_j, F_j, L_j)$ where E is set of all InPs in federated system. S_j is a set of subjects which are collective subset of federating participants. O_j is a set of virtual links, virtual routers and virtual machines. The subjects $s \in S_j$ can perform P_j basic operations (i.e. access rights) on the objects O_j. The set F_j maps security labels of subjects to security labels of objects at particular time instance. L_j is a partially ordered set of security classes of the federations in the system.

FACM employs a different notion of security label which is an ordered tuple. The security label has a form of $\langle SeP_{SL}, U_{SL}, InP_{SL} \rangle$ and; SeP_{SL}, U_{SL} and InP_{SL} are the security labels of service provider, the user from the service provider and a set of federated infrastructure providers respectively. FACM uses two operators namely, the Cartesian equal (i.e. $\equiv$) and Cartesian subset (i.e. $\subseteqq$) to check relation between the security class of subjects and objects. FACM also uses Cartesian union (i.e. $\Cup$) to dynamically create the security labels of federated subjects and objects.

4 Router Framework for Secured Network Virtualization

The proposed router framework adds a virtual plane on top of data and control planes of standard router architecture, an deploy-able unit of FACM, a set of information bases to address three aforementioned issues as shown in Fig. 3. The two abstract protocols are *Node-and-Path Label Distribution Protocol* (NPLDP) and *Secured Virtual Topology Embedding Protocol* (SVTEP). The deploy-able unit includes *Access Control Enforcement Engine* (ACEE) and the information bases are *Label Information Base* (LIB), *Forwarding Security Label Information Base* (FSLIB) and *Forwarding Virtual Label Information Base* (FVLIB).

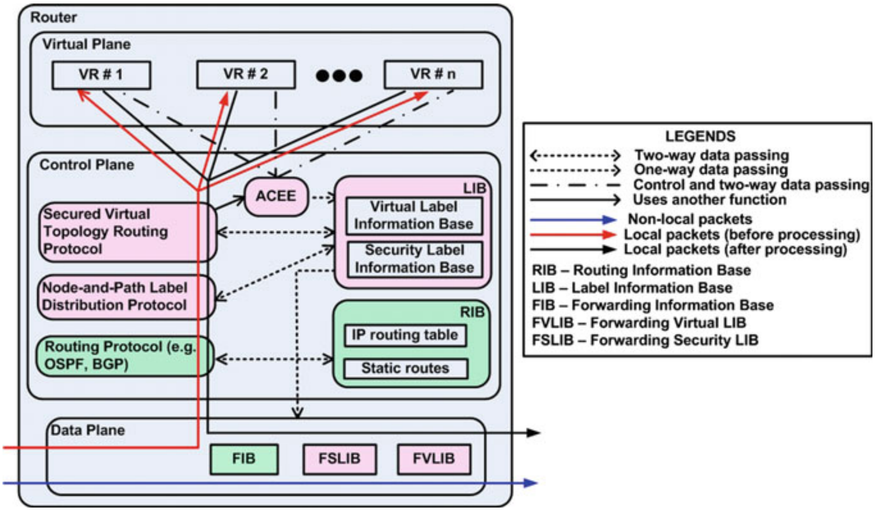
Router
Virtual Plane
VR # 1
VR # 2
VR # n
Control Plane
ACEE
LIB
Virtual Label Information Base
Security Label Information Base
Secured Virtual Topology Routing Protocol
Node-and-Path Label Distribution Protocol
Routing Protocol (e.g. OSPF, BGP)
RIB
IP routing table
Static routes
Data Plane
FIB
FSLIB
FVLIB
LEGENDS
Two-way data passing
One-way data passing
Control and two-way data passing
Uses another function
Non-local packets
Local packets (before processing)
Local packets (after processing)
RIB – Routing Information Base
LIB – Label Information Base
FIB – Forwarding Information Base
FVLIB – Forwarding Virtual LIB
FSLIB – Forwarding Security LIB

Fig. 3 Router framework for secured network collocation

SVTEP and NPLDP cooperatively run on top of existing routing protocol and provide security through ACEE. ACEE first authorizes the requests received from users/customers for the management of virtual router and links. Then, NPLDP signals physical routers for creation/deletion of virtual resources. NPLDP also distributes node and path labels to provide mapping between physical and virtual networks so that it securely multiplex and de-multiplex data-centric and network-centric traffic. SVTEP securely handles load balancing among physical nodes and links using some virtual node and link allocation algorithms.

LIB consists of (i) Virtual Label Information Base (VLIB) and (ii) Security Label Information Base (SLIB). NPLDP updates VLIB whenever virtual routers and links are created/deleted. ACEE automatically and synchronously updates SLIB to store the security labels of virtual resources whenever the access control services (e.g. create/delete virtual router/link) are executed through a sequence of primitives operations on *Access Control Matrix* (ACM) which is a data structure of FACM. The forwarding plane uses FVLIB and FSLIB which hold subset of virtual and security labels from VLIB and SLIB respectively.

4.1 Node-and-Path Label Distribution Protocol

Node-and-Path Label Distribution Protocol (NPLDP) distributes identities of virtual routers and virtual links as follows. The labels of virtual routers are entered in VLIB whenever FACM successfully executes create-node service. Similarly, the labels of virtual links are entered in VLIB whenever FACM successfully executes create-link service. In case of virtual labels of virtual links, NPLDP has a set of procedures to send virtual labels of source and destination virtual routers along the physical path selected by SVTEP. The deletion of virtual labels from VLIB is performed when delete-node and delete-link services are successfully executed by FACM. The mapping between physical and virtual networks is carried out by NPLDP and it allows multiplexing and de-multiplexing of all users' traffics.

4.2 Secured Virtual Topology Embedding Protocol

Secure Virtual Topology Embedding Protocol (SVTEP) uses a concept of node and link stresses which represent the loads on physical router and link respectively. The concept of node and link stresses is borrowed from a survey of virtual network embedding [3]. The node stresses are updated in local databases of physical routers when a virtual routers is placed/removed on/from physical router. Similarly, the link stresses are updated in local databases of physical routers when a virtual links are added/removed on/from physical link. SVTEP has two alternative scheme to update node and link stresses. First, SVTEP may use centralized algorithm to update the node and link stresses of physical routers and links. Second, it may use a distributed wave traversal algorithm which does the function of propagating node and link stress to all physical routers in the data center. Once the propagation of node and link stresses is finished, SVTEP can securely find the optimal physical router and path for the placement of virtual router and link respectively.

4.3 Access Control Enforcement Engine

Access Control Enforcement Engine (ACEE) carries out two functions. First, ACEE manages virtual resources through a combined enforcement of Mandatory Access Control (MAC) and Discretionary Access Control (DAC) policies. ACEE also updates security labels of federated subjects and virtual resources in SLIB of whenever management operations are executed. Second, ACEE uses VLIB and SLIB to multiplex and de-multiplex traffic of local virtual routers. The non-local traffic is forwarded using FVLIB and FSLIB.

4.4 Label Information Bases

Label Information Base (LIB) consists of two types of data structures for storing virtual labels and security labels of virtual routers and virtual links respectively. Virtual Label Information Base (VLIB) stores virtual labels of collocated virtual routers and links which have the forms of ⟨pnode,vnode⟩ and ⟨source pnode,source vnode, destination pnode,destination vnode⟩ respectively where pnode and vnode stand for local virtual and physical labels respectively. The formation of virtual labels is cooperatively carried out by SVTEP, NPLDP and ACEE. Security Label Information Base (SLIB) stores security labels of virtual resources and it is automatically updated by FACM. To perform fast forwarding of incoming non-local packets, the data plane uses FVLIB and FSLIB. FVLIB and FSLIB consist of subsets of VLIB and SLIB respectively. FVLIB is frequently updated at some regular interval.

4.5 Working Principle and Theoretical Evaluation

The design of proposed router framework for secure network virtualization must address the placement of ACEE, SVTEP and NPLDP at various locations. There are two alternatives for the placement, namely, distributed and centralized. The placement of ACEE must be distributed because the decision about packet forwarding must be very fast and on-line. The placement of SVTEP and NPLDP can either be centralized or distributed. The centralized placement may results into two dis-advantages (i) single point of failure and (ii) delay in load balancing and virtual network management. But it has two advantages (i) less computation and (ii) less message complexity which result into low network-centric traffic. The distributed placement results into least delay-time for network management with more message complexity as compared to centralized version.

All the recent virtual router architecture support security provision only for data-centric traffic and no provision for network-centric traffic except AVR. AVR concentrates on confidentiality of all types of traffic whereas the proposed router framework provides a full-fledged solution for secure management of collocated virtual resources, efficient load balancing among physical resources and transparent mapping between physical and virtual networks.

5 Conclusion

This paper proposes a router framework by adding a virtual plane without significantly changing the existing standard router architecture. The paper also proposes two abstract protocols namely *Secure Virtual Topology Embedding Protocol* (SVTEP) and *Node and Path Label Allocation Protocol* (NPLDP) to efficiently and securely manage the placement of virtual resources on physical network through *Access Control Enforcement Engine* (ACEE). Further, the proposed router framework is the first step towards the design of router which supports secured multi-tenant network collocation. The future work includes evaluation of NPLDP, SVTEP and the proposed router framework.

References

1. Chowdhury, N.M.K., Boutaba, R.: A survey of network virtualization. Comput. Netw. **54**, 862–876 (2010)
2. Nimkar, A.V., Ghosh, S. K.: Towards full network virtualization in horizontal iaas federation: security issues. J. Cloud Comput.: Adv. Syst. Appl., SpringerOpen **2**(19), 19:1–19:13 (2013)
3. Fischer, A., Botero, J., Till Beck, M., de Meer, H., Hesselbach, X.: Virtual network embedding: a survey. Commun. Surv. Tutorials IEEE **15**, 1888–1906 (2013)
4. Fan, P., Chen, Z., Wang, J., Zheng, Z., Lyu, M.: Topology-aware deployment of scientific applications in cloud computing. In: 2012 IEEE 5th International Conference on Cloud Computing (CLOUD), pp. 319–326, June 2012
5. Egi, N., Greenhalgh, A., Handley, M., Hoerdt, M., Huici, F., Mathy, L.: Fairness issues in software virtual routers. In: Proceedings of the ACM Workshop on Programmable Routers for Extensible Services of Tomorrow, PRESTO '08. ACM, New York, NY, USA, pp. 33–38 (2008)
6. Rathore, M., Hidell, M., Sjdin, P.: Data plane optimization in open virtual routers. In: Networking 2011, Lecture Notes in Computer Science, vol. 6640, pp. 379–392, Springer Berlin Heidelberg (2011)
7. Mattos, D.M.F., Ferraz, L.H.G., Costa, L.H.M.K., Duarte, O.C.M.B.: Evaluating virtual router performance for a pluralist future internet. In: Proceedings of the 3rd International Conference on Information and Communication Systems, ICICS '12. ACM, New York, NY, USA, pp. 4:1–4:7 (2012)
8. Lakshman, T.V., Nandagopal, T., Ramjee, R., Sabnani, K., Woo, T.: The softrouter architecture. In: Third Workshop on Hot Topics in Networks HotNets-III, ACM, San Diego, CA, USA, Nov 2004
9. Bozakov, Z., Papadimitriou, P.: Openvroute: an open architecture for high-performance programmable virtual routers. In: IEEE 14th International Conference on High Performance Switching and Routing (HPSR), pp. 191–196 (2013)
10. Sarrar, N., Feldmann, A., Uhlig, S., Sherwood, R., Huang, X.: Fibium-towards hardware accelerated software routers. EuroView 2010 (poster session) **9**, 1–17 (2010)
11. Louati, W., Houidi, I., Zeghlache, D.: Autonomic virtual routers for the future internet. In: Proceedings of the 9th IEEE International Workshop on IP Operations and Management, IPOM '09, Springer-Verlag, Heidelberg, pp. 104–115 (2009)
12. Nimkar, A.V., Ghosh, S.K.: A theoretical study on access control model in federated systems. In: Communications in Computer and Information Science, Recent Trends in Computer Networks and Distributed Systems Security, vol. 420, pp. 310–321, Springer Berlin Heidelberg (2014)
13. Bozakov, Z.: An open router virtualization framework using a programmable forwarding plane. SIGCOMM Comput. Commun. Rev. **40**(4), 439–440 (2010)
14. Bozakov, Z.: Architecture and algorithms for virtual routers as a service. In: 2011 IEEE 19th International Workshop on Quality of Service (IWQoS), pp. 1–3 (2011)
15. Wang, Y., Keller, E., Biskeborn, B., van der Merwe, J., Rexford, J.: Virtual routers on the move: live router migration as a network-management primitive. SIGCOMM Comput. Commun. Rev. **38**, 231–242 (2008)