VPN Service Provisioning via Virtual Router Deployment and Quantum Key Distribution

A. Aguado[1], V. López[2], J. Martinez-Mateo[1], M. Peev[3], D. López[2] and V. Martín[1]
[1]*Center for Computational Simulation, Universidad Politécnica de Madrid 28660 Madrid, Spain*
[2]*Telefonica Investigacion y Desarrollo, Ronda de la Comunicacion s/n 28050 Madrid. Spain*
[3]*Huawei Technologies Duesseldorf GmbH, Riesstrasse 25, 80992 Munchen. Germany*
e-mail: a.aguadom@fi.upm.es

Abstract: Here we demonstrate, for the first time, VPN services integrated within a virtual router using QKD to perform encryption and authentication. Any management operation is also secured using QKD, providing a whole quantum-safe ecosystem.
OCIS codes: (270.5568) Quantum Cryptography; (060.4785) Optical security and encryption; (060.4250) Networks.

1. Introduction

The continuous demands for higher bandwidths and new services have driven network infrastructures and their management architectures towards more flexible and adaptive solutions. The Software Defined Networking (SDN) paradigm, created as a response to these challenges, has the capability to control network resources on demand. This flexibility allows for a higher degree of experimentation and a faster deployment of new services and applications, be these based on new physical devices or not. On the other hand, Network Functions Virtualization (NFV) [1] allows the replacement of network functions (e.g. routing, deep packet inspection, firewalling), traditionally run in dedicated hardware appliances, by software running in a virtual image on commodity servers. Virtualization brings simplicity to the network and reduce costs for both, deploying and operating the infrastructure. Nonetheless, this solution entails certain vulnerabilities, as management architectures are usually abstracted in a single centralized management and orchestration (MANO) entity, and configuration commands and files must be remotely transferred among distributed points-of-presence (PoP). However, not only the control plane operations are at a risk, but also the communications among enterprises' premises must be secured. These entities usually rely on current protocols to provide secure connectivity and virtual private network (VPN) services to connect distributed sites. Technology advances, including but not restricted to quantum computing, are on their way to compromise the crypto primitives used to secure these remote communications. More specifically, conventional public and private key exchange (transport and generation) algorithms, which rely on the assumed complexity of certain mathematical problems could potentially be fully compromised. When speaking about critical infrastructures and private enterprise information exchange, the security is a must, as all data from control and data planes must be kept confidential.

Quantum Key Distribution (QKD) [2] allows for the unlimited and secure growth of a private key between two points that are connected by a quantum channel. This channel, typically implemented using an optical fiber, is used to transport the qubits: photons embodying the quantum properties on which the security of the protocol relies. QKD technology allows to upper-bound the maximum information that is leaked out, i.e. QKD is an Information-Theoretic Secure primitive. Thus, the keys produced by a correct QKD implementation are of the highest possible quality. Further advantages include forward and backward security and the principle immunity of key generation to any algorithmic cryptanalysis, be it quantum or not, rendering QKD to be a quantum-safe technology. On the other hand, factors such as noise or absorptions that do not impact classical cryptography, are important for QKD, potentially reducing its performance. However, QKD brings an additional physical security layer to an optical network [3] that is qualitatively different from all classical techniques. In consequence, QKD is an opportunity to enhance the security in current networks to keep safe both data and control [4] plane communications. This work proposes the automation of VPN services between virtual routers, using QKD keys integrated in IPsec sessions to provide an authenticated and encrypted channel for quantum-safe communications between distributed premises.

2. Control Plane and Node Architectures

The goal is to automate the deployment of a quantum-safe network service for both, control and data, planes, all supported by NFV techniques. The quantum-safe service must provide connectivity between two endpoints (two

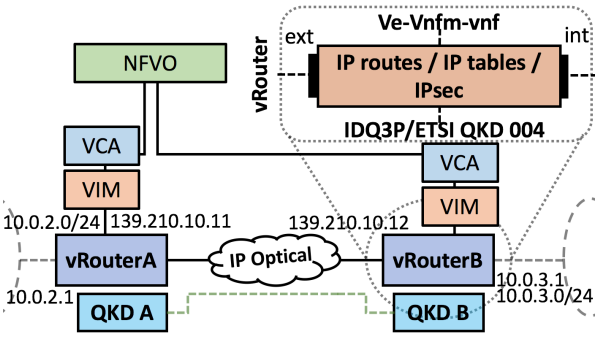

Fig. 1. Proposed architectural and node solutions

separated sites of an enterprise, two data centers, etc.), which host enough computational and storage resources to deploy virtual network functions (VNFs). In that sense, the proposed architectural solution is based on the ETSI NFV MANO ISG and the Open Source MANO (OSM) proposals [1,5]. This architecture can be logically divided into three different layers: *the NFV Orchestrator (NFVO)*, which takes care of lifecycle management of NFV services and orchestrates the different elements of the architecture (in our case, co-located with a full NFV MANO stack in one of the two domains); the *VNF Configuration and Abstraction (VCA) module [5]*, which manages the VNFs lifecycle and configuration; and the *Virtual Infrastructure Manager (VIM)*, in charge of controlling the underlying network, computing and storage infrastructure on which the NFV services are built upon. This architecture is distributed into two domains, both hosting an instance of a VCA and VIM, and one of them hosting also the NFVO.

A VPN is composed of routers and their connections. When deploying a VPN, both ends are asked to create one virtual router on each side. This virtual router is composed of different layers and interfaces (Fig. 1). It communicates with the local QKD system, via the southbound interface, using an API (e.g. IDQ3P protocol [6] or the ETSI GS QKD 004 [7]). The access to the QKD domains is granted on demand by the VCA, which creates a bridge between the virtual router and the physical host to permit accessing the key material whenever this is needed (e.g. during the installation process). Together with the packet/optical network interconnecting both domains, a QKD link or network must be running between both points, as the ones shown in [3]. The core of the virtual router contains the IP layer operations (routing table, port mapping, NAT and IPsec policies), which are configured by the VCA, following the incoming topology request from the NFVO. This node communicates via the northbound interface with the VCA module, to allow the necessary configuration and lifecycle management.

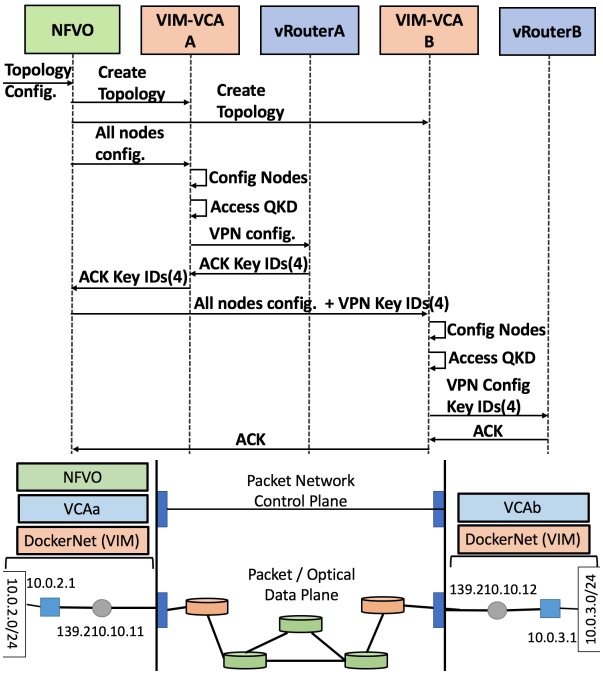

Fig 2 top) Workflow for the QKD-enabled VPN service automation; bottom) logical distribution of the scenario

3. Proposed Workflow

The designed workflow to provision QKD-enabled VPN is shown in Fig. 2 (top). Initially, the NFVO receives a request in order to provision a VPN service. The connectivity requirements of the service are then distributed to the two separated endpoints, where two instances of VCA and VIM are hosted. The NFVO transmits the connectivity information to both VIM instances. Additionally, the orchestrator also distributes initial configuration commands to each domain, in order to provide a final working environment to the end user. Among other configurations (gateway and routing configuration, installation of necessary packages, initialization of internal services), the NFVO transmits to the VCAs the instructions to create the VPN between the two virtual routers. Key synchronization plays an important role in this operation, as it is required to be orchestrated by the centralized MANO. Upon receipt, the first VCA (VCAa) handles the instruction with no key IDs for the sessions. The VCAa then creates a tunnel between the local host (IDQ3P port 5323) and the virtual router to grant access to the key store. After that, the VCAa instructs the virtual router to configure the VPN at its side, gathering the QKD-generated keys and their IDs. The VCAa then returns the key IDs to the NFVO, which later proceeds to send a similar instruction to the VCA on the other end (VCAb) to proceed as VCAa, but sending the valid key IDs to be used by the virtual router. Both virtual routers configure the authenticated and encrypted IPsec (tunnel mode) channels using the QKD-generated keys and creating the necessary security policies and associations.

4. Experimental Scenario and Results

In order to demonstrate the proposed solution, we have implemented the stack and the required extensions using different software and hardware platforms. The VIM is a container platform-based on Docker, which allows to create virtual networks using containers and OpenVSwitches. Among others, it allows users to control their networks via the SDN controller, to attach to physical interfaces, to create VLAN networks, etc. The VCA is composed of a set of scripts and processes which are remotely controlled by the NFVO. Finally, the orchestrator is implemented to receive requests, distribute them across the connected VIMs, gather topological information and forward configuration commands to the remote VIMs and VCAs. The physical testbed comprises two servers,

connected via MX240 routers and an optical triangle composed by ADVA FSP3000, as logically shown in Fig. 2 (bottom). The experimental results of this demonstration are two-fold: firstly, we expose the control plane integration of QKD keys into SSH sessions for setting up a two-layered hybrid secure protocol, following the solution proposed in [4]; secondly, we show the setting up operations for the VPN service, together with traffic captures showing the deployed and running IPsec-based QKD-enabled VPN service between the separated virtual routers.

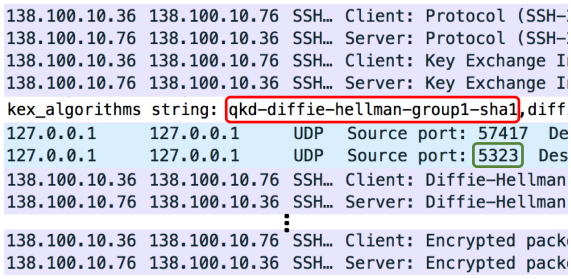

Fig 3 SSH message exchange for the hybrid QKD and Diffie-Hellman key exchange

Fig. 3 shows a subset of the SSH messages exchanged between the NFVO and the remote stack. After the initial client/server handshake, the NFVO and the remote VIM agree a key exchange algorithm for the session. In this case (highlighted in red), the preferred key exchange algorithm combines Diffie-Hellman and QKD, combining both keys to secure the session. The next messages include the UDP messages to extract a valid key and key ID from the emulated QKD systems (IDQ3P, port 5323), as well as the subsequent encrypted packets.

Fig. 4 shows different captures showing the proposed workflow and the VPN service deployment. Fig. 4a shows the bridge created by the VCA to provide access from the virtual router to the local key store. That process allows to redirect the incoming request (which comes across the Docker management network) to the local IDQ3P server, listening in the localhost interface of the host machine. The bridge is terminated whenever the VPN creation process finalizes on the virtual router. Fig. 4b shows how ICMP (ping) traffic is securely forwarded between both virtual routers, via Encapsulating Security Payload (ESP). This demonstrates that, when terminated, the setting up process implements a fully operational network and its required connectivity. Finally, Fig. 4c shows how the service data (in our case, the access to a redis database) is encrypted and authenticated between both virtual routers. The top part shows the two packets before and after passing through the virtual router when retrieving topological information from the redis database. Below one can see the header information of the secured packet as it traverses the network between the virtual routers A and B, as well as the information decryption before and after the packet traverses the second virtual router (the open data shows topological information stored in the Redis database).

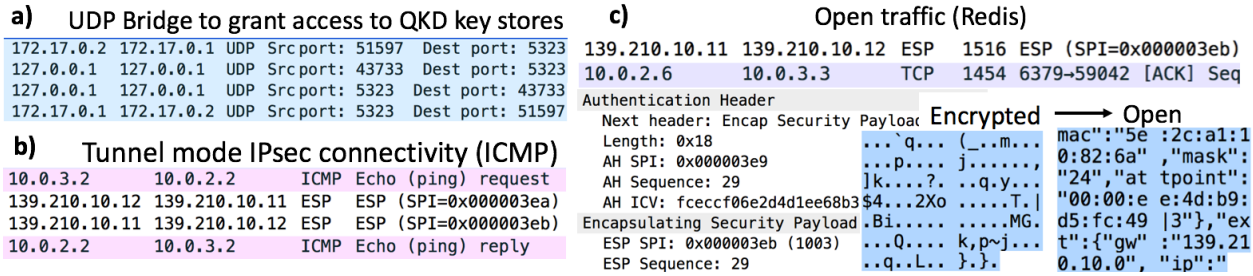

Fig 4 a) shows the IDQ3P messages passing through the bridge created by the VCA between the virtual router and the key store, b) shows the final connectivity across the VPN and c) shows how the traffic is finally secured for a given service (Redis database)

5. Conclusions

This work demonstrates and showcases, for the first time, a whole quantum-safe ecosystem to secure modern network paradigms and their associated services. We propose an automation workflow for VPN service deployment between two virtual routers using QKD keys, all orchestrated by the NFV MANO architecture. Any communication channel from both, control and data plane, integrates QKD keys in different ways to provide quantum-safe services.

Acknowledgements

We thank the Spanish Ministry of Economy and Competitiveness, for the grant CVQuCo, TEC2015-70406-R.

References

[1] ETSI: Network Function Virtualization (NFV): Architectural Framework, ETSI GS NFV 002 v.1.1.1, (2013)

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, Mar. 2002.

[3] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, "QKD in Standard Optical Telecommunications Networks," in *QuantumComm 2009*, LNICS, vol. 36, pp. 142-149, 2009 (arXiv:1006.1858)

[4] A. Aguado, et. al.: "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks", in Journal of Optical Communications and Networking, Vol. 9, Issue 10, pp. 819-825 (2017).

[5] [Online] "OSM Release Two: a technical overview": https://osm.etsi.org/images/OSM-Whitepaper-TechContent-ReleaseTWO-FINAL.pdf

[6] [Online] IDQuantique ID3100 Clavis2: http://www.idquantique.com/.

[7] ETSI: Quantum Key Distribution: Application Interface ETSI GS QKD 004 V1.1.1 (2010-12)