Securing NFV the smart way

In October 2012, ETSI proposed the concept of NFV, established the NFV-ISG group, and set out the following action plan, which was accepted industry-wide: construct decoupled, efficient, and open next-gen networks using NFV. But, since then, the severity and frequency of network attacks increased, compromising the potential of NFV.

By Liu Maojun

More NFV-related technologies have been developed, verified, and passed integration testing. Operators are attracted by the efficiency and agility that NFV brings, especially in cutting OPEX and promoting rapid innovation and breakthrough services.

But, cloud security issues have cast a shadow over NFV, representing an ever-present threat to telcos and users. A security incident in a telecoms network can have immediate and disastrous effects, interrupting services, compromising user privacy, enabling telecoms fraud, and damaging operators' brand equity.

A changing security landscape

Traditional telecoms network functions run on dedicated hardware using dedicated software. Although the closed nature of these network functions is a disadvantage that NFV remedies, it is in fact an advantage for network security due to mutually independent hardware platforms, closed dedicated software, and a trusted internal network.

NFV changes the network security environment, however, due to resource pools based on cloud computing and open network architecture. Cloud computing and virtualization technology decouple software, so NFV networks face the same security challenges as cloud computing and virtualization. Thanks to the agility and O&M efficiency of NFV networks, attacked networks can potentially be abandoned and resources recycled, enabling disasters to be quickly isolated, a response that's impossible in traditional networks. Network functions, network links, and even entire networks can be rapidly redeployed, enabling fast disaster recovery. At the same time, though, security threats have become more diverse.

The major threats

A new high-risk area – the virtual layer: Resource virtualization is the foundation of cloud computing and the main feature that differentiates NFV networks from traditional networks. The virtual layer provides unified computing resources based on generalized hardware to the layers above, and is the basis of all VMs and service software. If the virtual layer is breached, all VMs come under direct attack with disastrous consequences.

Resource sharing breaks physical boundaries: Resource sharing is vital for the agility and efficiency of NFV networks, but it means the user no longer has complete control over resources. A single physical server may run several different tenants' VMs, and a single tenant's VM might be distributed across different physical servers. Multi-tenancy resource sharing and breaking physical boundaries introduce the risks of data leaks, data residue, and attacks.

Traditional security policy failures: Virtualized networks have no physical network boundaries, rendering traditional security measures based on physical divisions ineffective. Thus, VMs are vulnerable to attacks between VMs on the same host. Moreover, the static policies of traditional security solutions cannot be automatically adjusted or respond to migrations, expansion, and other scenarios that lead to security policy failures.

Layered architecture and multi-vendor integration: After NFV introduces the virtual layer, a trusted link is needed between the infrastructure, platform, and service layers to secure each layer from the bottom up. Multi-vendor integration makes it difficult to coordinate security policies and determine responsibility for security problems, and requires more effective network security monitoring capabilities.

Open source and third party software: Because NFV extensively uses open source and third-party software, it faces the same security vulnerabilities as both, threats which most companies aren’t equipped to respond to.

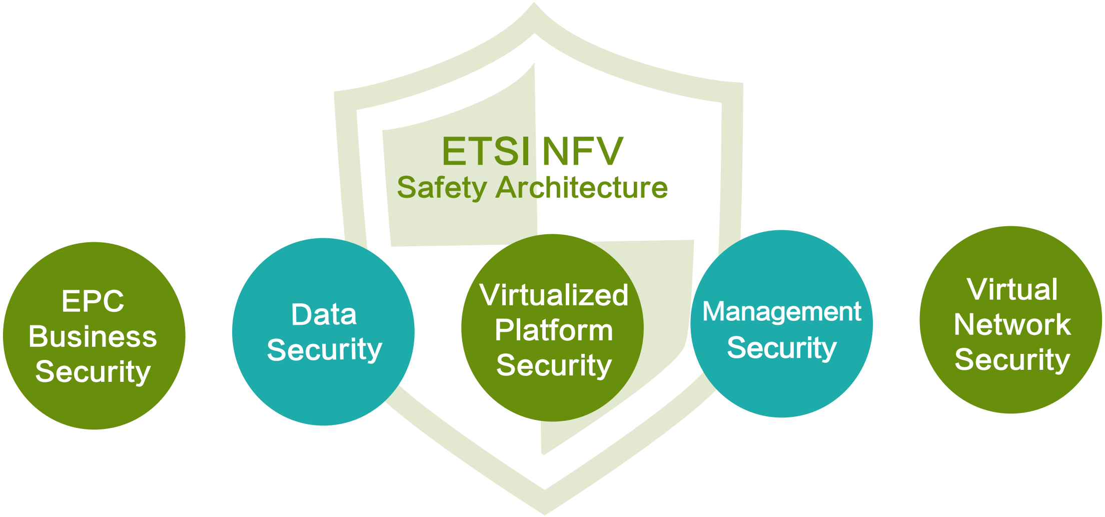
The solution

The security architecture for NFV must be multi-layered and include the following features:

Enhanced virtual layer: Hardening and patching virtual platform security can counteract software vulnerabilities. System tailoring minimizes the service system by deleting unnecessary software packages, which reduces system-wide security risks. Supplementary methods include security codes, open port scanning, minimized authority control, and anti-virus software.

Resource sharing: Isolating resources between different VMs on the same physical machine on the virtual layer can prevent data theft and malicious attacks between VMs because resource use by a given VM isn’t impacted by the surrounding VMs. Users can only access their own VM resources, including hardware, software, and data, thus ensuring VM isolation and security.

Isolating resources between different VMs on the same physical machine on the virtual layer can prevent data theft and malicious attacks between VMs because resource use by a given VM isn’t impacted by the surrounding VMs.



New security policies: Service orchestration via NFV has given rise to dynamic new forms of security policies. To deal with initialization, capacity adjustment, upgrades, migration, and security termination of network services (NS) and virtualized network functions (VNF), a security management and orchestration center is necessary to coordinate security protection across layers. This involves collecting information about each layer and tenant, analyzing system security status, developing security policies and measures, and deciding how to deploy them.

Three layers of firewalls: A physical firewall on the physical infrastructure sub-layer, a virtual firewall on the virtual infrastructure sub-layer, and a firewall deployed as a VNF on the service layer can mitigate the lack of physical boundaries in the network and protect all layers.

A security ecosystem: Given that the openness and flexibility of NFV is attracting more users and encouraging more services, a security ecosystem is necessary with multi-layer collaboration. Standardization, an alliance of developers, open source communities, and industry alliances can achieve this, but it will be a long and complicated process that requires the concerted effort of all.

An industry first

Cloud security threats in the NFV era present a long-term challenge. As NFV security technology continues to develop, automated and virtualized protection systems with robust security models will enable NFV networks to flourish.

As a leader in the field of NFV, Huawei has released the industry's first security solution for NFV. Its bottom-up, outside-in, and multi-layered architecture rapidly adjusts security policies based on network status, with centralized security monitoring enabling operators to visualize security status.

In January 2017, Huawei became an executive member of the Cloud Security Alliance. As part of the group, Huawei works with the other nine members to ensure the security of cloud services. Huawei's years of experience in cloud and telecoms security will help operators complete NFV cloud transformation efficiently, quickly, and securely.