thalestct.com

THALES

Virtualized Networks and Real Risks: Best Practices for Securing Network Function Virtualization Environment

White Paper

Executive Summary

Network Functions Virtualization (NFV) is unleashing fundamental innovation in the way organizations buy, deploy, and operate network infrastructures. By leveraging open standards and commodity hardware, NFV delivers cost savings, enhanced flexibility, improved performance, and more. However, without the right safeguards, organizations can also see their vulnerabilities increase when they move to a Virtualized Network Functions (VNF) architecture. This white paper offers a detailed look at the unique security implications of adopting NFV approaches, and it provides a number of best practices to employ to ensure sensitive data and transmissions remain secure in these environments.

Introduction: The Promise of NFV

NFV enables significant innovation in the way networks are built, deployed, and managed. At a high level, NFV refers to the process of moving network functions and services—such as load balancing, domain name services, caching, and security functions such as firewalls and encryption and so on—from proprietary hardware and into virtualized environments that run on 'commodity' hardware.

Following is a brief overview of each approach and some of their key differences:

- **NFV (Network Function Virtualization).** The development of NFV was initially driven by communications service providers. They sought to speed the deployment of new network services. They found that proprietary hardware appliances they relied upon adversely affected their objectives and customer benefits. NFV enables organizations to programmatically define and execute the services that run on networks. NFV infrastructures are comprised of virtual network functions (VNF), the components that deliver specific services. By virtualizing physical functions, organizations can improve agility. In addition, it can reduce equipment size and power requirements, which helps reduce capital and operating expenses.

- **SDN (Software Defined Networking).** SDN grew out of campus data centers, and its use is emerging in cloud data centers. SDN employs network abstraction and provisioning, and it is an area in which new protocols such as OpenFlow and OpenDaylight are being introduced to foster flexible integration and interoperability. This is being driven by organizations such as the Open Networking Foundation[1], a formalized working group that's focused on developing and promoting standards in SDN.

NFV Advantages

By leveraging NFV, many organizations can realize two fundamental advantages:

- **Reduced Costs.** NFV has the potential to reduce organizations' dependence on purpose-built hardware and enable the move to more flexible, commodity-based systems, which can reduce (up-front) capital expenses. By gaining more flexibility to distribute workloads across commodity hardware, organizations can reduce the waste associated with over-provisioning. By leveraging the efficiency gains of virtualization, organizations can also reduce requirements for other significant indirect and hidden costs such as space, power, and cooling.

- **Increased agility.** Instead of being constrained by the need to procure, test, and deploy specialized hardware, organizations are able to more rapidly roll out new services by implementing software into their existing environments. As a result, organizations can more quickly respond with increased agility to new competitive threats and market opportunities. By leveraging industry standard hardware and virtualization, organizations can much more rapidly scale up or down to accommodate changing demands. Similarly, they can more quickly and easily adapt services, and deliver enhancements, and be responsive to customer feedback.

Due to the financial and operational benefits enabled by NFV, spending on NFV is expected to grow dramatically. For example, IHS estimates that between 2015 and 2020, spending on hardware, software, and services associated with NFV will grow five-fold, from $2.7 billion to $15.5 billion.[2]

The Security Considerations in NFV Environments

For organizations seeking to move to NFV or that have already done so, security is a fundamental consideration. First, NFV initiatives will be implemented in environments that continue to be targeted by advanced threats and victimized by large-scale breaches.

NFV represents a fundamentally new architectural approach. Given that, it's vital that security teams are integral to the procurement, development, testing, and roll out of NFV environments. It's important to recognize that, in spite of all their strategic and operational advantages, NFV implementations are susceptible to attacks, just like any other networks. Unlike other networks however, NFV implementations present heightened exposure in several regards.

Increased Complexity Expands Potential Vulnerabilities

Compared to traditional environments, the number of connections and virtual links increases in NFV environments, which can expand an organization's potential points of exposure. As the network ecosystem becomes more open and includes more layers, solutions, and vendors, more points of vulnerability are also introduced. The following sections outline a few of the risks posed in NFV environments.

Dynamic environments—NFVs ability to provide elastic on demand provisioning of network functions is at the heart of their appeal. From a security perspective however this means that the environment is no longer static and relatively predictable, instead VNFs are deployed in a flexible service chain to meet the service delivery requirements at any given time.

This dynamic agile environment provides challenges for traditional security models that rely on well-defined service insertion points (which may no longer exist) for deployment logically or physically inline. In addition, in a VNF environment, it's a lot faster to spin up a virtual function, but these rapid deployments can be hazardous if the proper security checks are not in place.

1 Open Networking Foundation (ONF) is a user-driven organization dedicated to the promotion and adoption of Software-Defined Networking (SDN) through open standards development. URL, https://www.opennetworking.org/index.php

2 IHS, "NFV Market to Grow More than 5-Fold Through 2019, Says IHS", July 2015, URL: http://news.ihsmarkit.com/press-release/technology/network-functions-virtualization-market-worth-over-15-billion-2020-says-ihs

Increased complexity and reduced isolation—The security in any NFV environment depends on multiple software components that includes the hypervisor, orchestration and management tools as well as the individual VNFs in a deployed service chain. Unlike physical controls, which provide well defined boundaries and separation between network elements, in an NFV environment nearly all software components can communicate directly with each other. Multiple redundant paths, devices and a lack of clear boundaries breaks the model of good isolation and segregation assumed by traditional security models.

Encryption Key Generation and Management—Encryption is an essential component for most NFV deployments. For example in vCPE (virtual Customer Premise Equipment) or SD-WAN (Software Defined WAN) environments many network functions can exist either at the customer premises or in the cloud but encryption of network traffic must be deployed on premises to ensure secure cloud and WAN connectivity.

Any encryption scheme is only as good as the quality of the encryption keys used which must be completely random and frequently changed. While physical encryption appliances can rely on good hardware random number generators and tamper protected enclosures, encryptor VNFs may be deployed on white box switches, general purpose x86 servers or other equipment which can neither generate nor store keys securely.

Administration Layer Exposure

To take full advantage of virtualized network functions, organizations will be looking to establish additional management layers that will enable unified management of virtualized services and components. These management layers will be essential in realizing enhanced operational agility.

However, this centralized management layer also creates a single point of attack and failure. Many NFV deployments are being built using OpenStack, an open source architecture that enables central control of computing, storage, and networking resources. These environments typically run on some type of general-purpose operating system (OS), such as Linux, which is vulnerable to a range of attacks, including distributed denial-of-service (DDoS) attacks, data injection, mis-directions, incorrect configurations, and more.

The threat is significant: If attackers can gain access to administrative controls, they can make changes to the whole underpinning of the network. Not only could network traffic be rerouted, load balancing mechanisms disabled, but security mechanisms such as firewalls could be disabled, encryption could be bypassed or disabled and so on.

Exposure of Interfaces and Transmissions

NFV networks introduce new architectural layers, and new transmissions that are sent between all the different elements within and across these layers. Compounding matters is that these transmissions can be comprised of a number of different protocols and APIs, and each protocol may have its own security requirements. Some protocols may be new and introduce unanticipated vulnerabilities, be prone to misconfiguration, or lack proper safeguards. If traffic flows are spoofed, attackers can control traffic and bypass policies and security mechanisms. Transmissions will also be vulnerable to lawful intercept, including government wiretapping.

Structural Layer Compromises

Within NFV environments, a structural layer exists that's comprised of network, software, and server resources. These resources can be susceptible to range of compromises, including fibre tapping, data injection, sniffing, and siphoning. In addition, the host of a system connected to a VNF can be compromised, and then used to perpetrate attacks. For example, a DDoS attack can be waged to destabilize other network elements.

Internal Threats Will Proliferate

NFV environments may increase an organization's exposure to breaches associated with malicious insiders, inadvertent or accidental exposure, and exposure from machine-to-machine and virtualized network functions. In NFV environments, dynamic "physical" and virtual access increases. This will further expand the number of groups and individuals that can potentially access data, resulting in increased threats. At the same time, the complexity and dynamic nature of these environments can also result in diminished control for internal IT and security teams, inhibiting their ability to manage internal staff's access to both physical and virtual resources.

Higher Bandwidth Increases Scope of Exposure

Along with NFV adoption, organizations will increasingly be leveraging higher bandwidth systems, including 100 Gbps networks. Just as these higher bandwidth connections enable authorized users to gain access to more data and transactions, they can also offer the same advantages for unauthorized attackers and malicious insiders. Within the next few years, combined with the rollout of 5G networks, intelligence and data will continue to move closer to the network edge, where it may be even more susceptible to attack.

Innovative Applications will Fuel Change and Risk

For many organizations, the very reason for leveraging NFV is to support innovative initiatives and approaches, including Internet of things (IoT), mobile devices and applications, wearable technologies, robotics, virtual reality, big data, and so on. While these different approaches vary greatly, they all have one thing in common: They'll result in massive increases in data transmission volumes. As NFV environments support these innovations, their characteristics and threats will also be evolving, while the potential scope associated with a compromise will also be increasing.

Considerations and Best Practices

Whether an organization is just beginning to formulate an NFV approach or has already implemented the technology in production, there are several factors that should be taken into consideration in order to establish a strong security posture.

Leverage Strong Encryption and Authentication

As outlined above, NFV environments compound existing risks and create new areas of exposure. However, while much will be new, securing these environments will also entail employing some of the same fundamental approaches that have been required for some time. This includes the following three key tactics:

- Encryption. Organizations will need to encrypt data, wherever it is stored, transmitted, and used. The use of high speed network encryption in particular is of the utmost importance in NFV environments. For secure and efficient deployments in NFV environments, look for encryption platforms that feature both in-band and out-of-band security management capabilities.

- Key management. Securely storing and managing the keys associated with data encryption is an imperative. As the use of encryption expands, organizations soon find that key management emerges as a significant challenge. Quite simply, if encryption keys are lost or stolen, encrypted assets will also be exposed to loss and theft. Consequently, strong, centralized, and highly reliable key storage and management are essential.

- Access controls. Organizations will need to establish intelligent controls over user access. In NFV environments, organizations need to ensure only authorized users, systems, and processes are allowed to access or control other systems. This requires strong, multi-factor authentication capabilities.

Take a Holistic Approach

In today's technology and threat landscape, it's clear that no one solution or approach will address all of an organization's security requirements, and that becomes even more the case in the wake of NFV adoption. Ultimately, security teams will need to take a holistic approach to gain an adaptable, comprehensive set of defenses. In many environments, a mix of hardware and software-based solutions will be required to accommodate all of an organization's performance, availability, and security objectives.

In addition, standards will be another important part of the equation. The reality is that for most organizations, VNFs are being employed along with legacy network infrastructures. As outlined above, several standards are emerging in the NFV domain, and it will be important for organizations to leverage these standards in order to foster optimal interoperability and ensure continuous availability.

Establish a Profile of the Environment and Assets

In devising a sound security framework, it is important to take a concrete audit of the environment in place. This includes profiling these key aspects:

Data. Some assets managed within the organization will be obvious in terms of needing protections, such as regulated data like personally identifiable information and payment card data. However, as security teams go through the process of profiling their environments, it's important that they take a more objective and complete view of data and its risk. In this regard, it will be important to determine how long data will be useful, both to the organization and to a potential attacker. For example, given the increasing data analytics capabilities available, even data with a brief life span—such as real-time bidding data, voice traffic, and so on—can expose an organization if attackers can analyze large volumes of this data and identify patterns and trends. By assessing their data and environments in a more holistic fashion, security teams will be able to establish intelligent policies for security and data retention.

Traffic. Within new and evolving NFV deployments, it will be vital to understand data flows, including connections among devices and applications, and to establish controls around these aspects where needed.

Hardware. Even with the virtualization and software abstraction that characterizes NFV deployments, ultimately hardware still exists. Security teams need to understand ownership of each specific element, including such aspects as where it is hosted, how it is protected, who can access it, how many administration teams support it, and so on. In multi-vendor environments, it is important to have clearly defined boundaries in terms of when data leaves a specific organization's control such as a trusted supply chain in a manufacturing and distribution environment. For each system, teams need to verify capacity and associated vulnerabilities. For example, could an attacker remotely initiate 10 simultaneous functions and overwhelm the system? In the event of a compromise, is there a way to compartmentalize an infected element to keep other systems safe?

Ensure Scale

Whether it's in the area of storage, traffic, systems, users, or virtually any other facet, the numbers in most organizations only go in one direction—up. With the introduction of NFV, those trends won't just continue, they'll accelerate. Consequently, it will be vital to leverage security mechanisms that can provide the scale required to accommodate more keys, more devices, more users, more connections, and more applications.

The ability to scale to accommodate more authentication demands will also be a vital requirement. Organizations will need to be able to support the authentication of more users to devices and applications, and also to support authentication between devices and central control systems, for example, to enable trusted firmware and software updates.

Plan for Disasters

Just like IT teams need to have disaster plans in place for infrastructure, so do security teams. While it's not a trivial effort, it's critical to establish plans, not just for a natural disaster, but a disastrous breach. Security teams can't take short cuts in reducing risk. Instead, they need to plan for the worst, understand which assets are most critical, and establish a plan to safeguard those assets, even if a disastrous breach should occur. This entails employing multi-layer safeguards in NFV networks, including at the data and control layers, and leveraging data encryption.

Clarify, Investigate Roles, Services of Third Parties

Virtually all rganizations today rely on a complex mix of internal resources and services from hosting providers, cloud vendors, software vendors, service providers, and more. These ecosystems are only getting more complex as NFV implementations take hold. Enterprise security teams can't make assumptions about the safeguards of their partners. It will be vital to vet vendors' security practices and establish absolute clarity around how various responsibilities are handled and divided.

It's important to recognize that data owners are ultimately responsible for the data entrusted to them. When signing up for NFV and/or SDN services, security teams can't assume that sufficient security mechanisms will be instituted. This will require investigation and validation of the details of the controls in place. In outsourced environments, adhering to best practices like separation of duties will be particularly vital. For example, where practical, organizations can retain a high degree of visibility and auditability by retaining control of cryptographic keys when encrypted data is distributed in external environments.

Exercise Due Diligence in Service and Solution Investments

For many organizations, the move to NFV will entail making a number of new investments, including in new security systems and services. In this effort, management will need to exercise due diligence in researching solutions and vendors.

Fundamentally, it is critical to get answers to a number of questions:

- Is the solution part of a vendor's core competency?
- Does the vendor have a strong track record and proven pedigree, or is it difficult to get proof points of customer deployments and results?
- What kinds of staff are available to support the implementation and operation of the solution?

Testing a prospective solution or service is critical. Where possible, do negative testing, assessing what happens if a specific component fails in the network. Monitor aspects like latency, overhead, and end-to-end response time in order to ensure an offering is aligned with performance requirements of the specific use case.

This doesn't necessarily mean an organization has to make large investments in deploying and testing solutions internally. From a security perspective, it can be a great idea to leverage third parties, such as independent testing providers and standards bodies. These third parties can often make it very easy and cost effective for organizations to validate solutions.

Maintain a Security Team

When it comes to staffing, leadership may look to network operations teams to support security efforts in NFV environments. However, this can be a risky approach. The network team's focus has to be on keeping the network up and running. As a general rule, the time and resources of these staff members will be fully consumed in meeting these demands.

Most enterprises need a team that has a 100 percent security focus, with specialists dedicated to keeping up with changing attacks, breaches, standards, and mandates. When new vulnerabilities are announced, organizations need teams or individuals whose charter is to assess the environment and determine whether any equipment is vulnerable, and, if so, take responsibility for remediating or alerting the teams needed to handle remediation.

Conclusion

By leveraging NFV, organizations can stand to gain a broad range of advantages—but any gains can quickly be negated if gaps in the new network are exploited and a data breach occurs. As organizations leverage NFV in their environments, security teams can implement a number of measures to ensure that NFV environments—and the assets flowing through them—remain secure.

SafeNet High Speed Encryptors

The SafeNet High Speed Encryption solutions enable organizations to effectively address the demands of employing encryption in dynamic NFV environments. SafeNet High Speed Encryptors deliver high assurance, Layer 2 network security. These solutions can secure an organization's most sensitive network transmissions, whether they're transporting data, real-time video, or voice. As they move across NFV and physical networks, between data centers, to the last mile, and up to the cloud and back again.

SafeNet High Speed Encryptors deliver robust, proven security. These platforms have been scrutinized, vetted, and certified by a range of organizations, including the U.S. Government's Federal Information Processing Standard (FIPS), Common Criteria, the North Atlantic Treaty Organization (NATO), the U.S. Department of Defense Unified Capabilities Approved Products List (UC APL), and more.
SafeNet High Speed Encryptors deliver end-to-end, authenticated encryption and strong, client-side key management. These solutions feature set and forget management capabilities that streamline administration and deliver lower total cost of ownership than other network encryption alternatives. SafeNet High Speed Encryptors also provide optimized performance, introducing minimal processing overhead and offering microsecond latency.

SafeNet Virtual High Speed Encryptors

Today, as many organizations are looking to improve the agility and cost efficiency of their infrastructures, they are increasingly harnessing NFV and SDN approaches. SafeNet Virtual High Speed Encryptors canhelp organizations secure transmissions in these environments. SafeNet Virtual High Speed Encryptors can run on standard x86 server hardware and all leading hypervisors. The hardened virtual appliance's entire life cycle can be automated through standard NFV-based infrastructures and orchestration frameworks such as OpenStack.

SafeNet High Speed Encryption solutions are available for sale to the U.S. Federal Government through Thales Trusted Cyber Technologies.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com