Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING
WHITE PAPER

5G Security VNFs & the Emergence of the Services-Based Firewall

A Heavy Reading white paper produced for Clavister

clavister®

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

INTRODUCTION

The fluid nature of technology and shifting business models has meant that, since their existence, communications service providers (CSPs) on some level have always been managing some form of network transformational event.

In this regard, the previous five years have been no different, except for one major consideration: the cadence, complexity and number of events encapsulated in the transformation roadmap must be assessed as approaching unprecedented levels.

For instance, during this period CSPs have navigated scaling their 4G networks, embarked on a cloudification journey via network functions virtualization (NFV), which not only virtualized and moved services to the cloud, but also rearchitected where services and underlying compute platforms could be deployed. Specifically, we're referring to the greater thrust to push services to the edge thereby achieving alignment with the spirit of complementary technologies, such as 5G.

While these events on their own represent a major undertaking that will restructure the technology amalgam of service provider networks, the subsequent and ambitious push to commercialize 5G in the next 24-48 months only serves to push the complexity needle to the highest register.

Despite the complexity, each of these transformation initiatives, fortunately, converge to facilitate a greater goal: the ubiquitous availability of high-bandwidth, ultra-low-latency services anywhere in the network. While this model intuitively can only facilitate the monetization of the cloud, perhaps more importantly, it finally achieves total alignment with end-user anywhere, anytime service availability and business continuity expectations.

However, these customers not only expect superior service performance, they also expect CSPs without exception to keep their data and devices protected. Thus, CSPs must also recalibrate their security strategies to reflect the fact that in the cloud, services execute without limitations, which means that threat vectors are omnipresent.

Accordingly, the focus of this white paper is to discuss how the cloud is redefining the role of security products. Specifically, the white paper considers the role of an emerging class of services-based firewall (SBFW) designed to support the advanced capabilities that 5G networks and beyond will require.

THE RISE OF THE SERVICES-BASED CLOUD

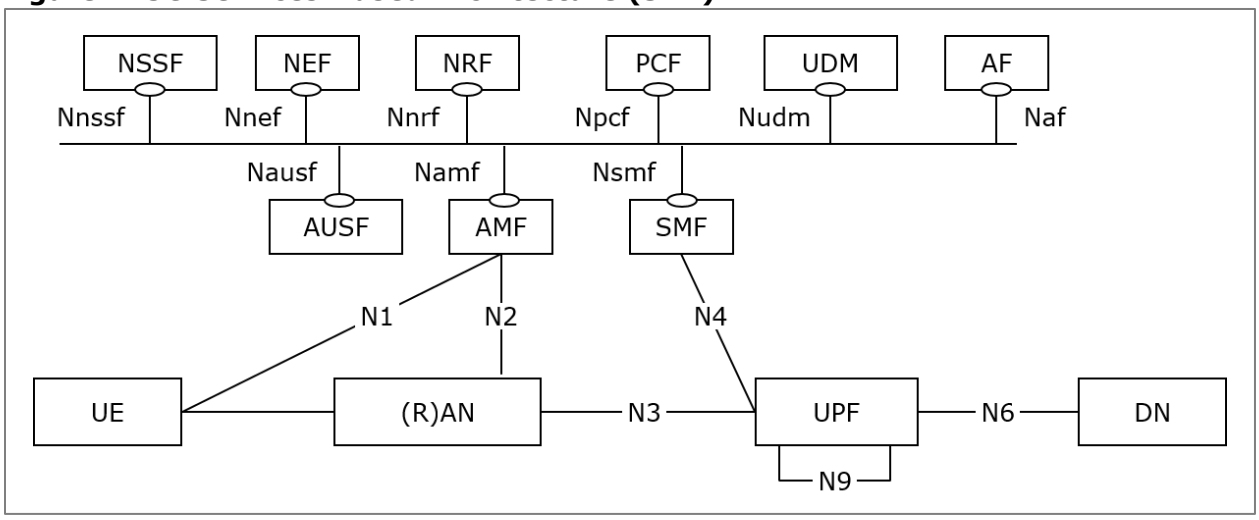
NFV and 5G are now both exerting a profound influence on service delivery. Perhaps the best way to illustrate this is that CSPs are not only moving services and applications to the virtualized cloud, but also now navigating a process that is redefining service delivery and related security strategies.

One of the outcomes of this services focus is that whether centralized or distributed, cloud-based applications will be required to expose service-related application programmability interfaces (APIs) anywhere in the network without restriction.

While this requirement is applicable to NFV, it also has driven the design philosophy of the 5G next-generation core network (NGC), which harmonizes traditional IP Multimedia Subsystem (IMS)-based and Evolved Packet Core (EPC) elements into a single software-based core. As shown in **Figure 1**, this core network is also referred to as a services-based architecture (SBA), since for the first time in core design there is a specific function defined to support API exposure.

This function is supported by the network exposure function (NEF) and is central to the core network, since it not only enables API exposure, but also works closely with two additional new functions: the network resource function (NRF), which supports service discovery; and the network slice selection function (NSSF), which supports network slice instances. These three new components together empower a services-based model.

Figure 1: 5G Services-Based Architecture (SBA)



Source: 3GPP TS23.501 V15.2.0 (2018-06)

While this approach undeniably represents a major advance in how services are developed and exposed, it's important to focus on additional attributes of the SBA that may not be initially understood.

The first consideration is the changing nature of the services themselves. While 4G supports virtualized networks, the 5G SBA is the first architecture designed to support cloud-native microservices, which decompose service function into highly reusable components to support a "building block" approach for new service development.

This approach not only promises to radically shorten development cycles, but also represents a lower-cost approach, since smaller teams can be deployed to independently create new microservices to run with mature existing foundational microservices. Also, given the extremely high level of software optimization, these microservices are no longer "service silo" constrained and thus can run on any compute platform, including those at the edge of the network.

This opens the door to moving service innovation much closer to the end user consuming the application, thereby taking a significant step in reducing application-based latency – because microservices are not only fully distributed, but also run in an environment in which

the control (i.e., signaling) plane and user (i.e., application) plane are functionally separated. This lowers application latency by optimizing compute resources.

In contrast, the initial design of 4G networks did not support control and user plane functional separation. However, this has recently changed with the standardization of the Control and User Plane Separation (CUPS) specification, which defines a fully separated architecture for the EPC. CUPS was developed in response to two basic network requirements.

The first was to enhance the scale of EPCs nodes as 4G NFV cloud networks continue the mass onboarding of subscribers and secondly to provide an interworking bridge with 5G. Essentially, this approach enables a CSP to launch 5G using only the 5G New Radio (NR) radio access network (RAN) with the CUPS-enabled EPC, rather than deploying the NGC architecture depicted in **Figure 1**.

This approach, referred to as *non-standalone (NSA)* 5G, is desirable because it eliminates the implementation complexity and capex costs associated with the NGC while maximizing EPC investment. The drawback of this strategy is that it doesn't support network slicing, which is a vital cog in achieving the promise of a services-based architecture.

Hence, adoption of an NSA strategy is considered by some CSPs as an unnecessary interim step that will only serve to delay revenues from high-value 5G use cases and ultimately limit market competitiveness. These CSPs are more likely to deploy both the NR and NGC SBA together, in a configuration referred to as *standalone (SA)* mode.

REDEFINING SECURITY ENFORCEMENT

Regardless of whether the 5G launch is achieved via NSA or SA architectures, the adoption of a services-based architecture will have profound impacts on security requirements and enforcement models. There are several factors that must be considered.

First, the era of low latency and decomposed microservices means that security virtualized network functions (VNFs) must be designed to meet much lower response time tolerances. Secondly, 5G as a truly distributed cloud network architecture means that security functions can no longer be enforced at traditional network ingress/egress perimeter points.

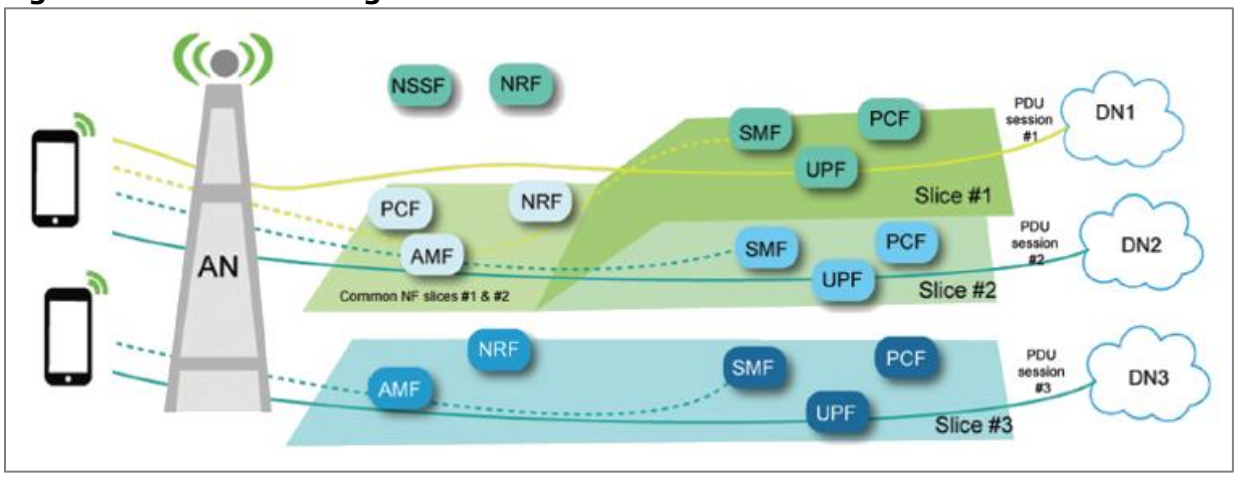
Instead, security becomes a prominent concern in every corner of the network, on both the control and user planes. To be clear, this doesn't mean that established and effective security functions such as traffic encryption, traffic filtering, intrusion detection system (IDS), traffic shaping and deep packet inspection (DPI) are no longer valid; instead, it means that where these capabilities are supported shifts from a static model to a fluid model based on where applications are running in the cloud.

Consequently, security enforcement must pivot to a pure software-driven mode that is cloud-native and matched to service execution, in contrast to the traditional approach of grafting on security measures at strategic network perimeters.

While the need to make this transition is unquestionable, it does inject additional complexity into security processes. One embodiment that illustrates the complexity of managing security VNFs in the distributed cloud is 5G network slicing.

As shown in **Figure 2**, network slicing is much more than simply reserving specifically dedicated radio resources for services. In contrast, network slicing is a dynamic process in which services can be allocated end-to-end network resources to create a virtual logical network for *each* service.

Figure 2: Network Slicing Reference Architecture – Common and Individual Slices



Source: 3GPP

This is intricate enough in its own right, but injecting additional complexity in the security monitoring process is the fact that network slices, as illustrated in **Figure 2**, may not only be single individual logical service slices, but can also support shared common slices, aligned with the concept of microservice reuse.

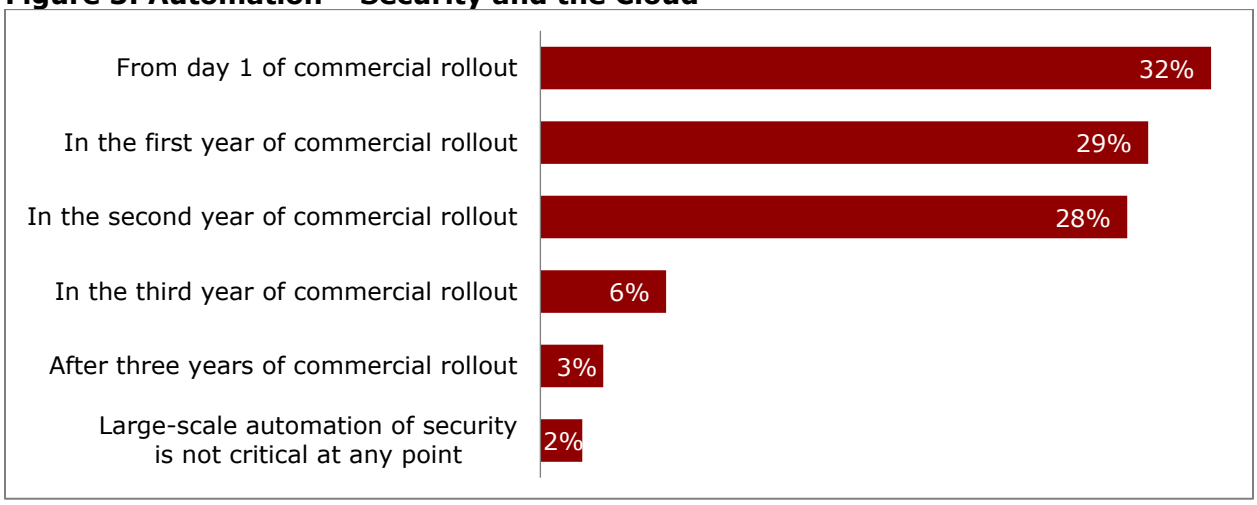
In a security context, factoring in that these multifaceted network slices will be supporting low-latency services, it effectively means that human intervention and human enforced policies will no longer be a viable strategy.

Instead, security must be automated and able to apply security policies on a service level, which is not supported today but will become table stakes with 5G and network slicing. While the application of leveraging automated policies is still being defined, it will likely apply to any policy that impacts service execution. Initial policy examples include applying different encryption levels, managing access lists and bandwidth usage profiles as even white and blacklists for admission control.

While 5G will provide a strong impetus to adopt automated processes, it should also be noted that even before 5G, a significant number of CSPs had reached the conclusion that automation would be necessary to meet the security requirements of their virtualized cloud-based services.

As a proof point, as shown in **Figure 3**, in a Security Perception Study survey that was conducted by Heavy Reading in the fourth quarter of 2017, nearly a third of CSP respondents – 32 percent – stated that automation was a critical security requirement for cloud-based services from day one of commercial launch. Moreover, 29 percent believed that automation would be needed in the first year of commercial service. Taken together, 61 percent of CSPs view automation as a critical capability with a small and immediate implementation window.

Figure 3: Automation – Security and the Cloud



Question: At what point in your company's commercial rollout of virtualized offerings using NFV/SDN/cloud technologies does large-scale automation of security become critical?
Source: Heavy Reading Security Perception Study 4Q17 (N=100)

THE EMERGENCE OF THE SERVICES-BASED FIREWALL

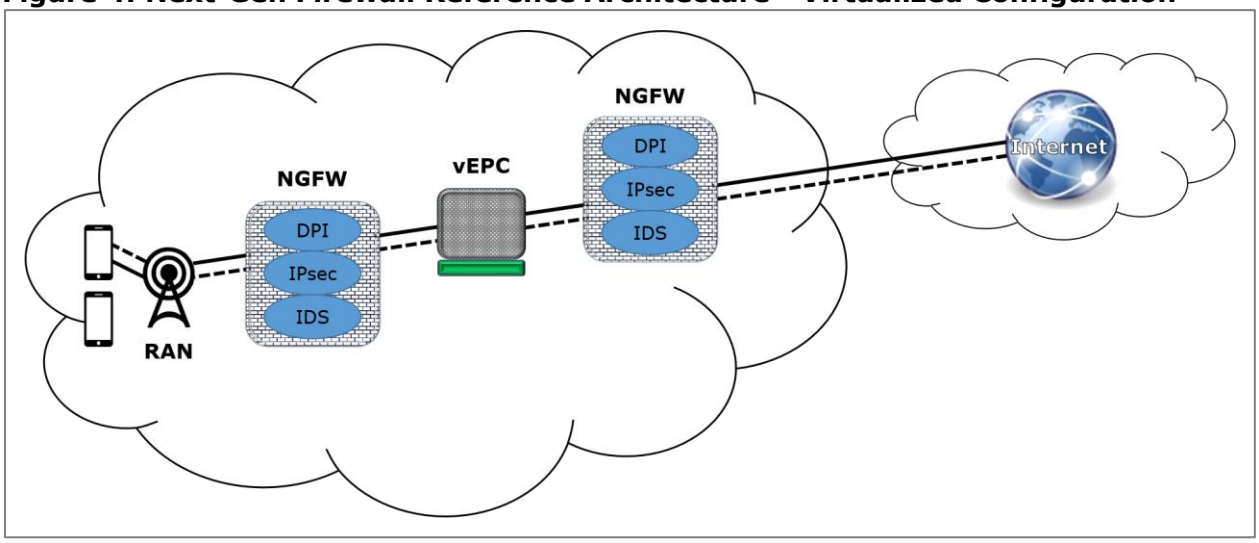
The adoption of distributed cloud-based services not only demands the implementation of automated and services-based security policies, but will also impact the deployment of analytics and identity management techniques. In an analytics framework, security demands that the appropriate triggers focusing on event data collection, application usage, centralized correlation and automated pattern and trend detection be deployed universally throughout the network. Similarly, identity management will need to be deployed anywhere in the network where services are supported – not only to validate network components and thwart rogue elements, but also because technologies such as 5G have a much greater focus on validating user identities or even Internet of Things (IoT) devices.

There are several considerations in play here. To effectively manage 5G slice-based services, identity management will be more complex, given that there will be a much greater focus on exchanging and validating users and IoT devices sharing data between distributed databases, including potentially public cloud databases. And identity management will become more complex not only because of distributed databases, but also because it must be performed at much greater speeds to avoid driving up the delay budget of low-latency services.

Taken together, these changes are redefining existing security platforms, including next-generation firewalls (NGFWs). These firewalls, which have been deployed in volume, already play a strategic role in 4G networks, since early security experiences in 4G deployments highlighted the need to not only manage basic network access, NAT translation and load balancing, but also support DPI and intrusion detection/prevention.

Thus, as shown in **Figure 4**, NGFWs have been deployed in virtualized configurations to augment virtualized EPC (vEPC) overall security performance, leveraging advanced packet inspection to detect malware and other attack vector signatures. In addition, while not illustrated in the figure, many operators continue to utilize appliance-based firewalls, which do not deliver the same scale and deployment flexibility as virtualized NGFWs.

Figure 4: Next-Gen Firewall Reference Architecture - Virtualized Configuration

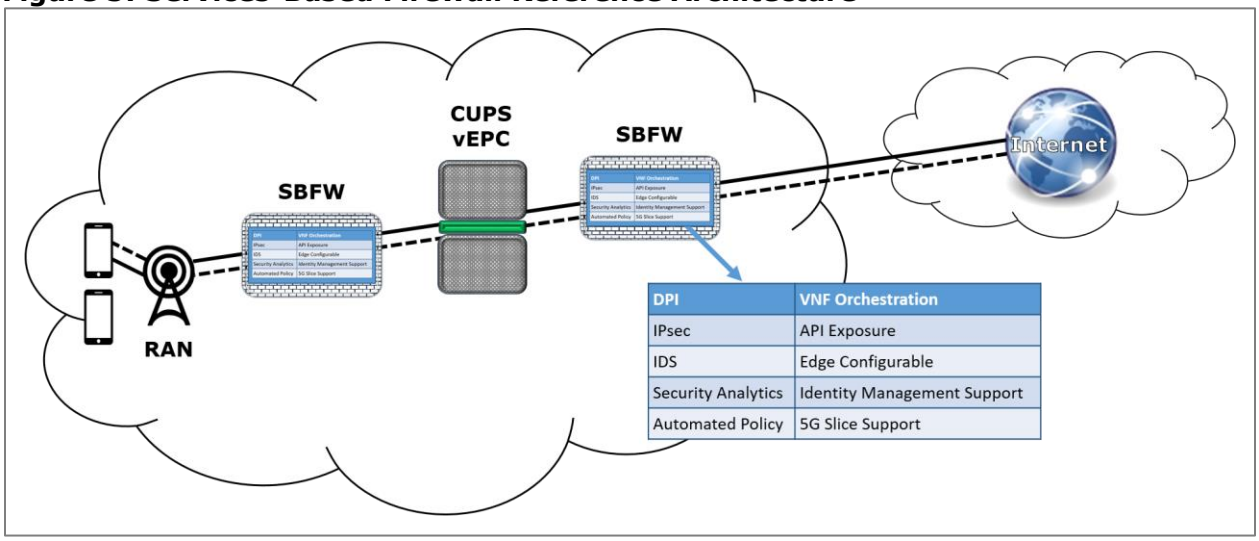


Source: Heavy Reading

4G networks and the NGFWs that support them empower CSPs to take initial steps to monetize and enhance service innovation in the cloud. However, the dynamic nature of the cloud is also driving additional changes – changes that will demand a greater focus on the integration of automated processes/policies and analytics into security enforcement points such as NGFW.

To this end, the lineage of NGFWs is giving way to a new type of firewall that supports these advanced capabilities, *plus* the ability to utilize these capabilities in a service-aware state. This type of firewall has a much broader and more intelligent view of service execution, including microservices support, API orchestration and services-based slices, reflecting the fact that 5G demands a more advanced portfolio of security VNFs to get the job done. Since networks are now becoming fully services based, firewalls must also adopt a service focus. Given this linkage, as shown in **Figure 5**, a new class of firewall, which we refer to as the services-based firewall (SBFW), is now coming to market.

Figure 5: Services-Based Firewall Reference Architecture



Source: Heavy Reading

The SBFW represents a breakthrough in security enforcement, since it is not only designed to be deployed in fully distributed clouds supporting microservices, but is also much more software-programmable than NGFWs and well suited to supporting distributed configurations, with fully autonomous control and user planes.

Therefore, as shown in **Figure 6**, SBFWs integrate a much richer suite of security capabilities. Features that an SBFW (but not an NGFW) will typically support include: 5G slice support, security analytics integration, native API exposure support, automated policies and advanced identity management techniques.

Figure 6: NGFW vs. SBFW

Attribute	NGFW	SBFW
Virtualized firewall	✓	✓
DPI	✓	✓
IDS	✓	✓
IPSec	✓	✓
Automated security policy	×	✓
Software configurable at the edge	×	✓
Security analytics integration	Limited	✓
5G SBA architecture optimized	×	✓
Effective 5G security slice enforcement	×	✓
API exposure support	Limited	✓
Advanced control plane signaling validation	×	✓
Orchestration of security VNFs at the edge	×	✓
Identity-driven policy enforcement	Limited	✓

Source: Heavy Reading

SERVICES-BASED FIREWALL USE CASES

As we have documented, SBFWs will indelibly alter how security services are delivered in the cloud. And of course, a key consideration in this process is the way SBFWs enable an expanded range of security capabilities in a services setting. Accordingly, to capture the services on a more granular level, this section presents two distinct use cases: one focusing on the delivery of managed security services for enterprise customers, and one documenting the role of an SBFW in enhancing security services in the 5G RAN.

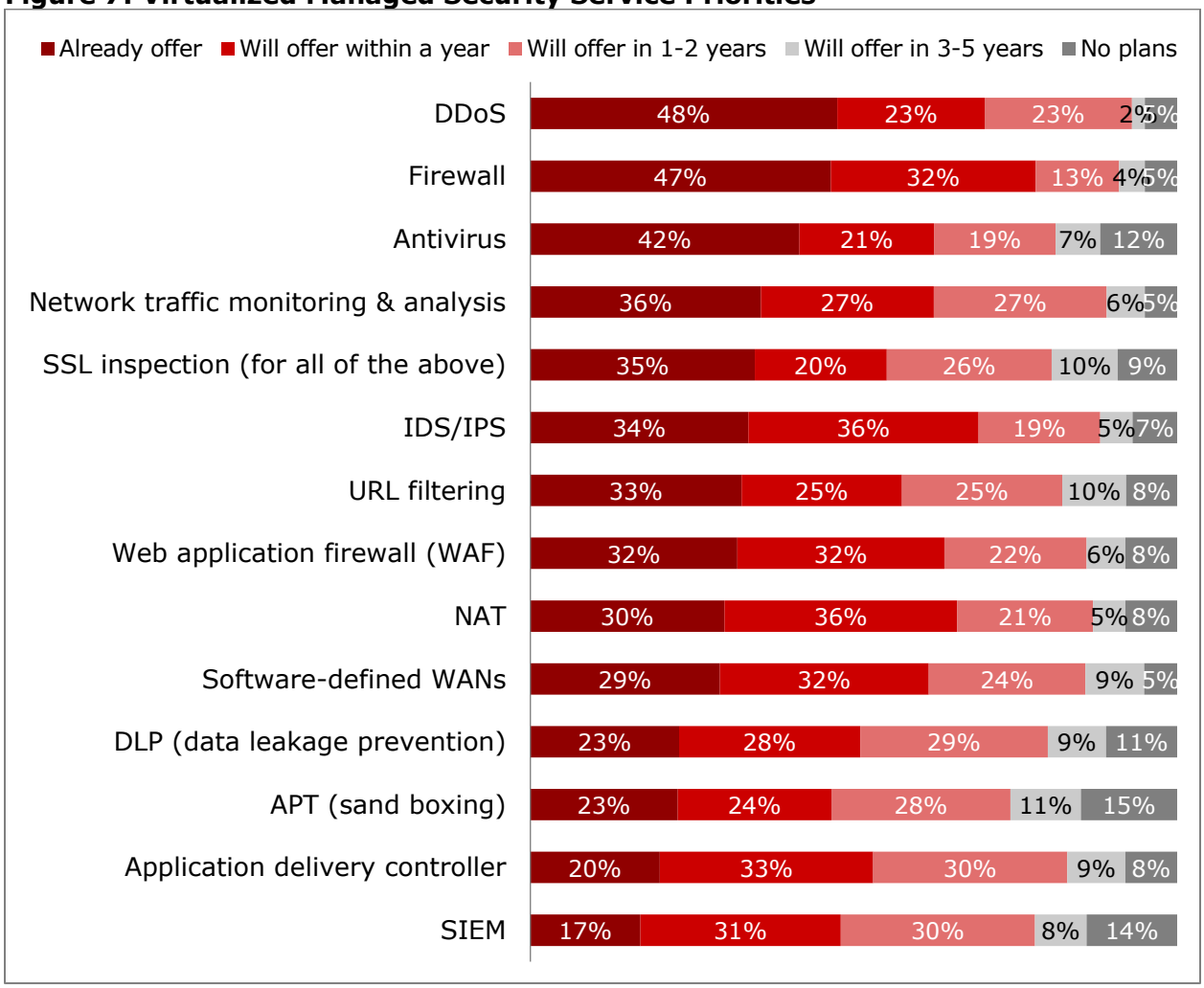
Private Network Slice Security Policies

One of the early factors that drove NFV deployments was the promise to leverage the cloud to achieve a major transformation in the enterprise. This transformation manifested itself in a few use cases, including using low-cost virtualized CPE (vCPE) compute platforms to achieve a more scalable and lower operational cost enterprise service delivery model. While vCPE on its own has been highly successful, the rollouts also revealed that enterprises were

looking to CSPs partners for their security requirements as the cadence and complexity of cyberattacks continued to accelerate.

As a result, progressive CSPs started selling virtualized firewalls to these enterprise customers through a hosted managed security services provider (MSSP) agreement. And as shown in **Figure 7**, based on input from the market perception study previously referenced, this strong demand curve has driven 47 percent of CSPs to deploy virtualized firewall services to meet the demands of their enterprise customers. Furthermore, 32 percent stated they planned to introduce virtualized firewall services within 12 months. Taken together, it appears that 79 percent of CSPs either currently offer or plan to support this service very soon.

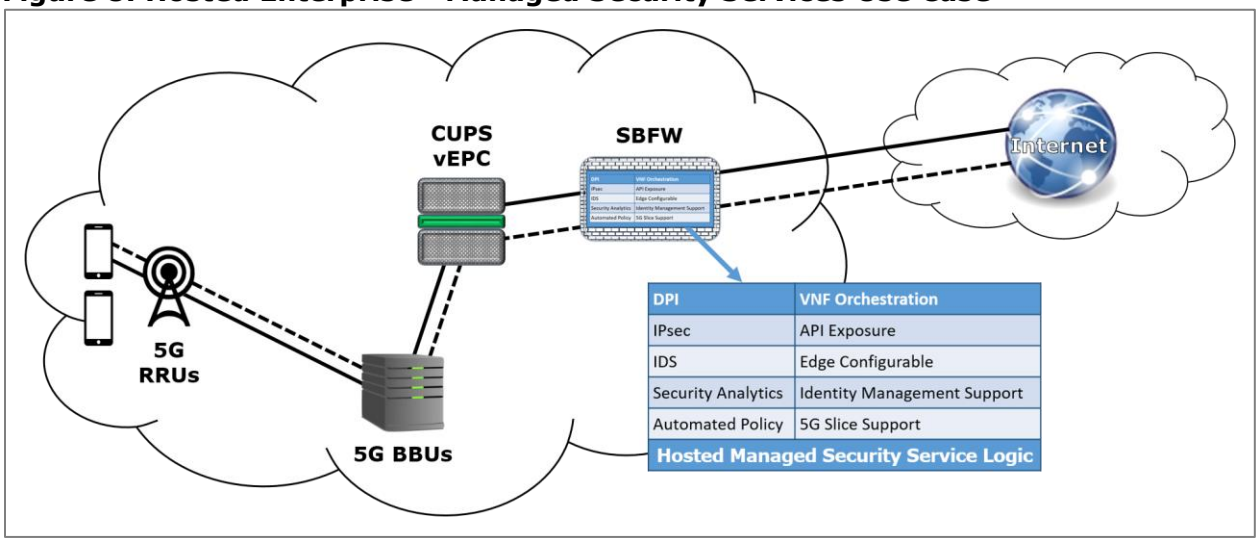
Figure 7: Virtualized Managed Security Service Priorities



Question: When will your company offer the following virtualized managed security services?
Source: Heavy Reading Security Perception Study 4Q17 (N=97-102)

While this market has already experienced strong demand, we view the market as still only partially covered, since enterprises must also adapt to the security realities of a services-based world when 5G network commercial rollouts commence. As shown in **Figure 8**, this scenario involves the implementation of a distributed 5G RAN served by a vEPC CUPS-enabled packet core utilizing the NSA option, with an SBFW supporting security.

Figure 8: Hosted Enterprise - Managed Security Services Use Case



Source: Heavy Reading

One of the key benefits of deploying an SBFW in this scenario is that it puts in place the security mechanisms to thoroughly monitor and enforce security on mobile devices. As it stands today, even in the pre-5G world, malware represents a major threat; that threat will only intensify with 5G and network slicing.

Thus, enterprises must move to a policy of monitoring mobile devices for malware, and not simply let them connect to the Internet without any protection. This is where an SBFW and network slicing can add significant value. In **Figure 8**, the deployment of an SBFW allows the CSP to handle security between slices, while providing managed security services with the ability to screen and detect malware and enforce security policies in real time.

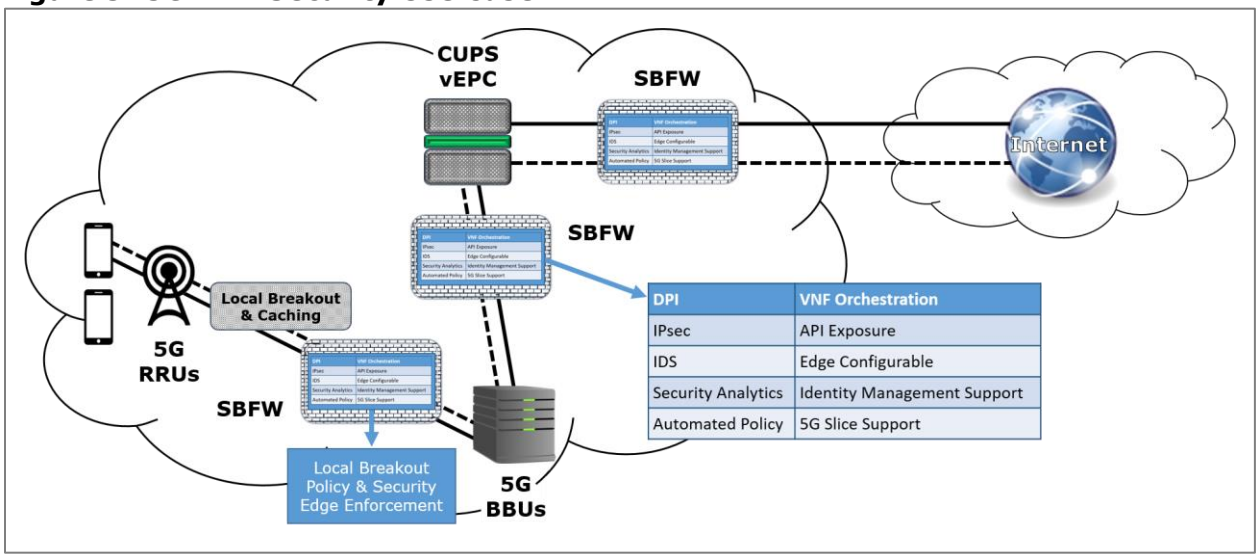
This is accomplished not only by utilizing virtualized analytics VNFs to create a services profile for the specific device, but also by leveraging identity management techniques to block information transfer requests initiated by the mobile device when concerns are noted. Soon, the SBFW VNFs will deliver additional value to this scenario through the support of automated security policies, in addition to enforcing policies for these same devices when they are executing a network slice-based service.

Edge Security for 5G RAN

The distributed nature of the 5G also demands innovation in security enforcement. Whereas in the past, including 4G, a single vendor delivered both the radio heads and baseband control portions – referred to as remote radio units (RRUs) and baseband unit (BBU), respectively – this will start to change with 5G.

As CSPs start to build out their 5G RAN, we expect that some CSPs will start to adopt a multi-vendor model, with the most likely scenario being one or more RRU vendors and a single BBU vendor. As shown in **Figure 9**, this new vendor model will drive new requirements to more effectively firewall the distributed RRU and BBU functions, since both become distributed cloud-based resources that must be secured by VNFs placed in close proximity to meet service performance tolerances.

Figure 9: 5G RAN Security Use Case



Source: Heavy Reading

The deployment of an SBFW in this use case will also greatly enhance security monitoring and policy control. Since the RAN is now fully distributed, SBFW VNFs can be placed strategically close to both RRU and BBUs based on service requirements and even radio vendor security requirements. Since the 5G RAN will introduce a measure of "best of breed" into the radio domain, having the ability to deploy software firewall capabilities is also key to ensure that security policies are programmable – and, in the future, automated.

Another key consideration is service latency. One of the ways 5G will enable low-latency performance is to leverage the inherent cloud-compute capabilities of the 5G RAN. This is accomplished by the adoption of local breakout, in which VNFs are deployed close to RRUs to support local service delivery. This feature, shown in **Figure 9**, is crucial for delivering HD video by caching the application on site instead of backhauling to a centralized processing point. This approach will not only enhance 5G scalability, but also aligns with another distributed and complementary services-based architecture: multi-access edge computing (MEC).

In a security framework, given that service processing is now done locally, support of localized and programmable security VNFs supported by an SBFW are vital to provide application screening and application-level policy enforcement at every site in which RRUs are deployed.

CONCLUSION

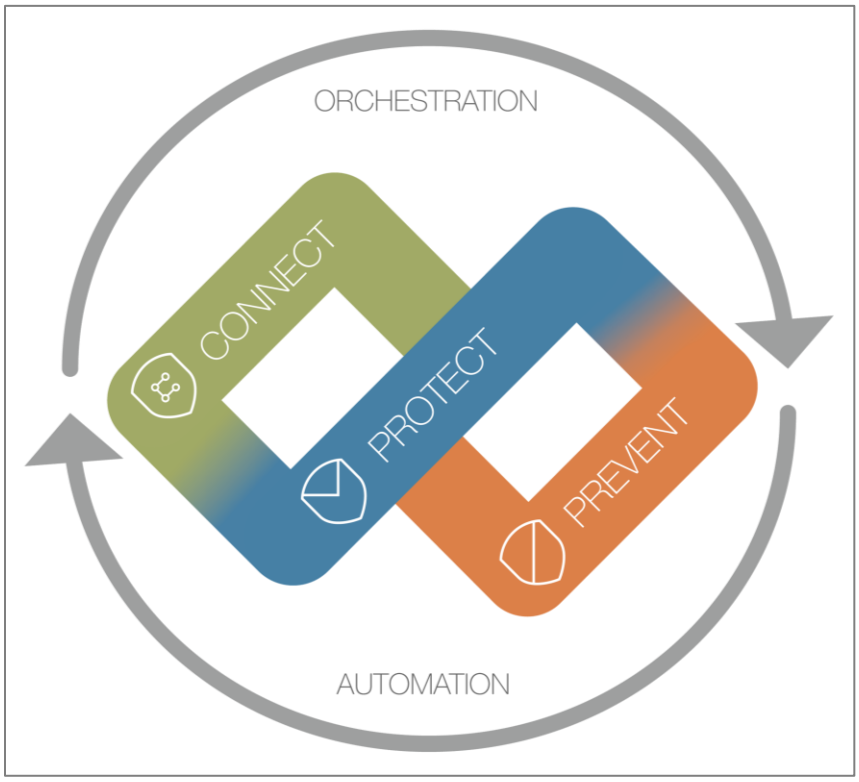
In only a few short years, CSPs have taken major strides forward to scale and foster service innovation in the cloud. But despite this advance, the advent of 5G will only serve to accelerate this process and ultimately result in CSPs implementing fully service-aware distributed core and radio compute resource-based networks.

In response, security resources must follow suit and embrace seamless integration and adoption of distributed, automated processes. And while these security requirements continue to be defined, as documented in this white paper, the emergence of the SBFW will play a crucial role in meeting both current and future cloud security service-driven requirements.

ABOUT CLAVISTER

This section provides an overview of Clavister's SBFW product development strategy. The information in this section was developed by Clavister.

The Clavister SBFW is a virtualized security solution that is ideal for multi-access edge computing (MEC) and next-generation core (NGC) networks because of its extreme resource efficiency and diversity in support for use cases. It provides advanced use cases in the areas of network connectivity, cyber-attack protection and proactive prevention, including traffic encryption, signaling validation, intrusion detection, and denial-of-service protection and mitigation.



Source: Clavister

Orchestrated by SDN/NFV controller integration through REST APIs, the solution can be deployed in both the edge and core networks. The same software provides the multiple use cases and is empowered by security analytics, artificial intelligence and closed-loop automation, providing the means to guarantee business continuity and protect customer integrity.

Clavister provides high-performance security VNFs today for 4G and pre-5G networks that handles solutions such as Gi firewalling, backhaul encryption and roaming security gateway. As traffic is increasing in CSPs networks scalability is key and with validated performance far exceeding others, Clavister provides a true cost-efficient solution empowering CSPs to offer security services to their customers as an MSSP.

Clavister is an expert cybersecurity company with more than 20 years of experience. Headquartered in Sweden and with customers in more than 150 countries, Clavister provides security solutions to communication service providers, enterprises and data centers.