White Paper

The Distributed Cloud: Automating, Scaling, Securing & Orchestrating the Edge

Prepared by

Jim Hodges
Senior Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.juniper.net

October 2015

Introduction

Whether utilized to scale and optimize existing data centers, or to support the creation of network functions virtualization (NFV)-enabled telco data centers, cloud architectures are now rapidly becoming a mainstream design element of the telecom domain.

However, while conceptually straightforward, in practice the cloud has many faces and subtle, but potent, nuances that can be leveraged to adapt to specific implementation requirements. One of the new cloud profiles that is emerging is the distributed cloud, which is optimally positioned to meet customer demand for delivery of applications at the network edge.

Therefore, the purpose of this white paper is to define the technical advantages of a distributed cloud edge network from an automation and orchestration perspective, as well as to document the value proposition and specific use cases that are well-suited to leveraging this approach vs. a centralized cloud architecture.

The Distributed Cloud: Architecture & Attributes

As noted above, the architectural frameworks for telecom network design have shifted in favor of the cloud. While the telecom cloud is often portrayed as a disruptive approach that emerged without warning, it can also be argued that it is actually a logical progression, given that IP services have been supported in an operations/ business support system (OSS/BSS) context in telecom data centers for several years.

At the same time, the trend to build "cloudified" non-telecom data centers to rapidly deliver and scale services is also an industry-accepted practice among enterprise customers. Based on these factors, extending the concept to include telecom virtualized network functions (VNFs) utilizing a cloud delivery model makes considerable sense to support all-IP, real-time service delivery.

Still, originally at least, it was assumed that telecom data centers would mirror the massive centralized cloud architectures of over-the-top (OTT) providers. However, as the concept of Distributed NFV (D-NFV) continues to gain market momentum for edge network services, the outcome is the emergence of the concept of distributed cloud, giving service providers a competitive differentiator from OTT providers.

Although subject to further industry definition, there is general consensus that the definitional characteristic of a distributed cloud is the extension of a suite of NFV capabilities to the edge while still benefiting from a centralized orchestration model. Therefore, in this white paper, we define the distributed cloud as a cloud that supports the ability to orchestrate, scale, secure and perform policy enforcement for VNFs at the service provider edge or even at the customer premises.

The value of this approach, as shown in **Figure 1**, is the ability to create "localized" clouds that can scale and apply policies in response to complex service-level agreement (SLA) and end-user service requirements. In this context, localization translates into the ability to place VNFs at optimal locations in the network to meet user and regulatory requirements. Since these capabilities are not supported in traditional legacy edge points today, it represents a potentially massive opportunity to enhance service agility and delivery.

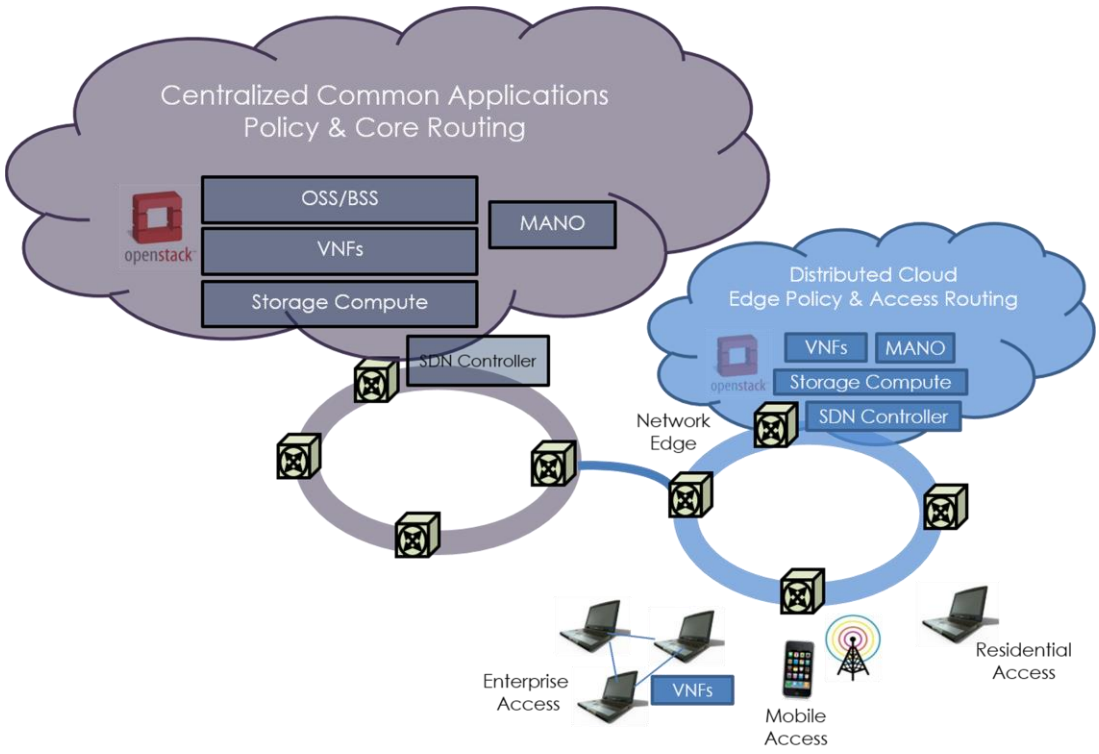
Moreover, since distributed clouds support the concept of separating the control and forwarding plane, there is full support for integration of software-defined networking (SDN) and NFV to support service chaining.

An important outcome of integrating SDN and NFV at the edge is that since both are open source-focused, it transforms the edge and customer premises from heavily vendor-specific implementations, based on utilizing closed proprietary software to an open software-based framework that delivers the ability to quickly spin up new services on shared commercial off-the-shelf (COTS) compute platforms.

However, the benefits of the distributed cloud go well beyond service provisioning and cloud management. Essentially, a distributed cloud presents several breakthrough opportunities for a broad range of critical network functions. We assess and document these below utilizing the following categories

- Scaling & VNF Orchestration
- Service Automation
- Service Chaining
- Security & Policy Enforcement

Figure 1: Distributed Cloud Functional Architecture



Source: Heavy Reading

Scaling & VNF Orchestration

One of the key drivers for the momentum of distributed clouds is that scale is a now a major issue for edge networks, given the growth of both mobile IP and enterprise broadband services. Since management and orchestration (MANO) enables central management of distributed applications, the network edge can scale elastically.

Stated another way: Unlike the legacy model, in which software was tied to specific hardware platforms with fixed scale, the distributed cloud represents the lowest-cost scaling model since it extends the concept of elastic application scaling, policy and core routing from a centralized cloud to the edge, to support an on-demand growth model.

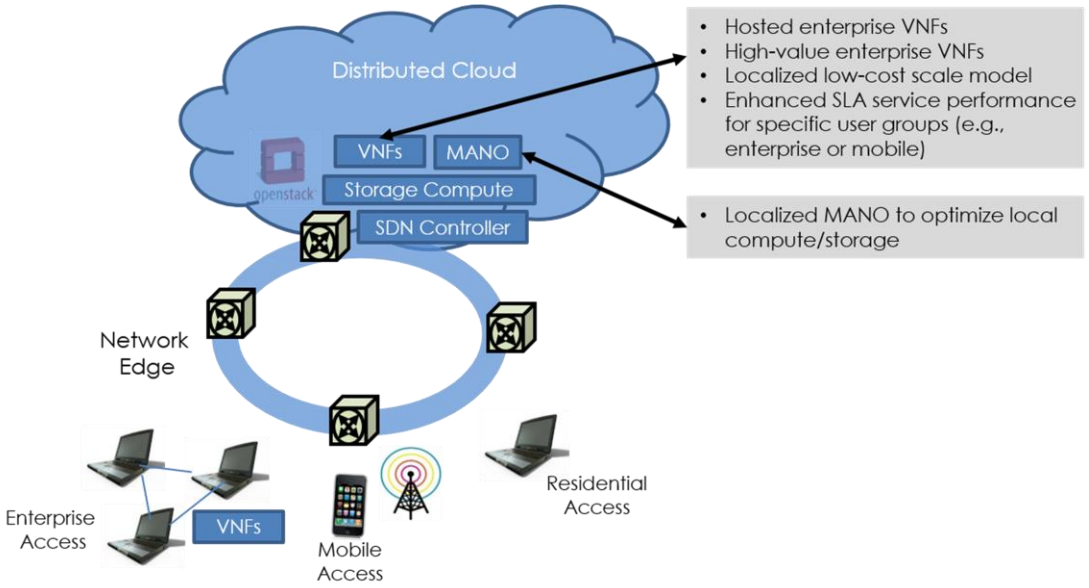
In addition, as shown in **Figure 2,** since the distributed cloud can support localized VNF orchestration if necessary, it provides enhanced survivability to support localized applications for users within the cloud.

Other key benefits are that it ensures the lowest possible latency model while also simplifying the managing of hybrid edge networks. Since it is predominately a software-scale model, it is possible to simply migrate traditional edge software applications to a pool of virtual machines (VMs), which are easier to manage. An additional benefit of this approach is that it reduces overall network traffic since not all traffic needs to be handled in the core.

From a service perspective, these capabilities can also support the provisioning of high-value and high-performance services for specific users in each distributed cloud, regardless of the performance profile of the centralized cloud. Additional service possibilities include support of hosted enterprise and wholesale services for special events in the distributed cloud, which are not technically feasible in today's legacy environment.

The outcome for network operators, as captured in the table below, is that the implementation of a distributed cloud can address traditional scale, service management and application ecosystem challenges that have been an entrenched reality of the legacy service edge for many years.

Figure 2: Distributed Cloud Service Scaling & VNF Orchestration



ATTRIBUTES	LEGACY SERVICE EDGE	DISTRIBUTED CLOUD EDGE
Compute Scale Potential	Poor: Dedicated Systems – unable to leverage underutilized resources	Excellent: Common Compute High Utilization Rate – Elastic Scale
Service Management	Poor: Vendor closed provisioning and management model	Excellent: Leverages open source management tools
Application Openness	Limited: Applications bound to specific vendor	Excellent: Opens up third-party support model

Source: Heavy Reading

Service Automation

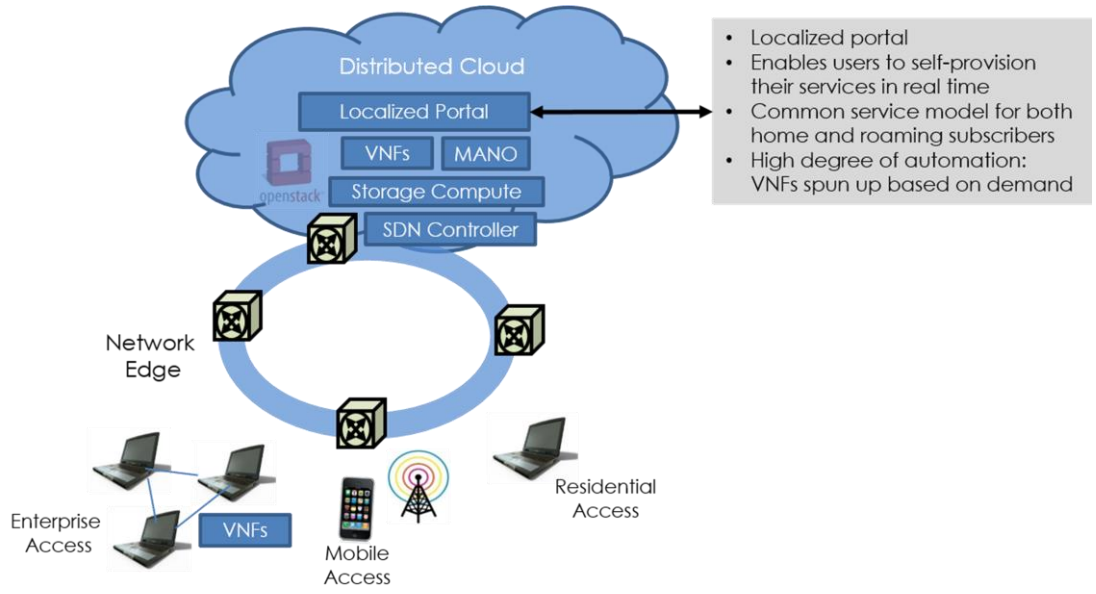
Another benefit of deploying services in the cloud is that it opens the door to a greater degree of orchestration in the service delivery process since VNFs as pure software resources can be provisioned, "spun up" and orchestrated in real time. This is not just a key enabler for service agility in terms of the time to launch new

services, it also enables end users to manage and personalize their services via a self-service portal.

An added value of the distributed cloud is that it extends the reach of software-as-a-service (SaaS) services to the edge and is strongly aligned with the future and emerging requirements to support scaling of Internet of Things (IoT) application integration at the edge.

Open source approaches at the edge in a distributed cloud also have a profound effect on automation. For example, as **Figure 3** shows, we are now starting to see the emergence of software automation tools that are built on OpenStack to enable deployment and provisioning. The value of this approach is that it can locally orchestrate the network, compute and storage layer when integrated with the MANO layer to support centralized service orchestration. One example is Ubuntu OpenStack, which supports OpenStack-compliant system management tools for distributed clouds.

Figure 3: Distributed Cloud Service Automation Architecture



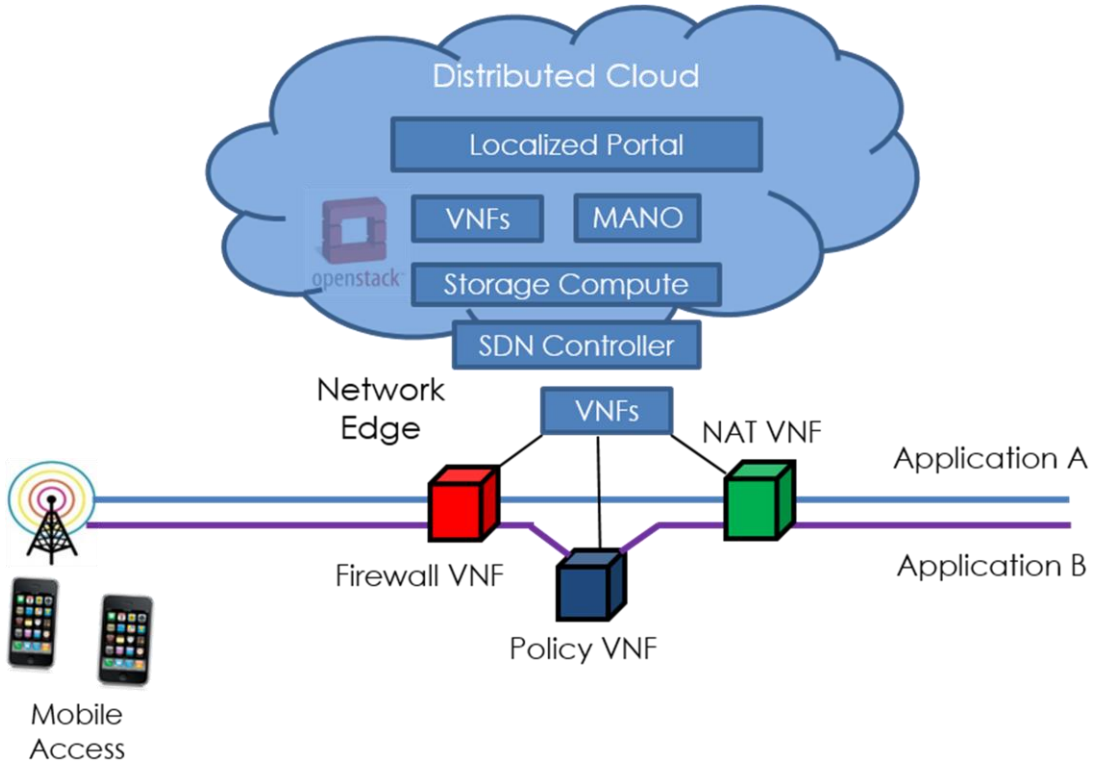
Source: Heavy Reading

Service Chaining

One of the key drivers for implementing NFV and SDN in parallel is to transform the network from a static network routing model to a dynamic service chaining model. The key benefit of service chaining is that it can apply application specific policy and consume only specific network resources that are necessary instead of following a static consume all in path network resources approach. This is accomplished by orchestrating and applying policies via an SDN controller for Layer 2/3 and via Layer 4-7 MANO orchestrated VNFs.

Architecturally, as shown in **Figure 4**, the distributed cloud is an optimal location to support service chaining since SDN controllers and NFV MANO distributed VNFs can both be deployed in the distributed cloud.

Figure 4: Distributed Cloud Service Chaining Architecture



Source: Heavy Reading

Security & Policy Analytics-Driven Enforcement

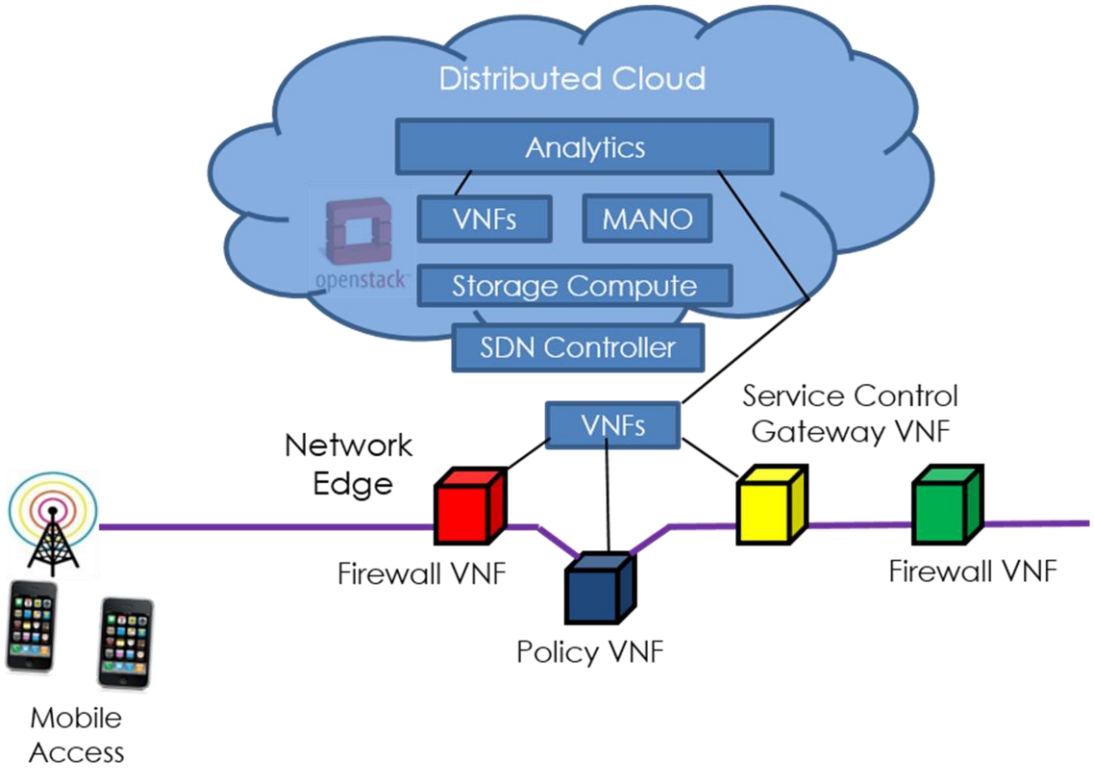
The advance of IP services in general and virtualized IP services are also redefining how security and policy enforcement are conducted at the edge. In addition to service chaining, the edge network is also now poised to support a much greater degree of what we define as security and policy analytics-driven enforcement. This is because the addition of analytics in a distributed cloud enables a much finer degree of security and policy application enforcement, since the network data can be analyzed on a real-time basis.

The outcome is that we move from a statically-defined policy architecture to a real-time policy enforcement architecture that leverages policy databases and security gateway software to define which services and network capabilities users have access to, or the level of service.

These capabilities, in turn, are well-suited for simplifying the delivery of wholesale services, multi-tenant services, SaaS and even security-as-a-service (SECaaS). The addition of analytics further enhances service delivery, since it supports the ability to access user profile performance and dynamically adapt the network to ensure that service quality metrics are being met.

As captured in **Figure 5**, these capabilities and services are very difficult to introduce and manage in the legacy service edge.

Figure 5: Distributed Cloud Security & Policy Architecture



ATTRIBUTES	LEGACY SERVICE EDGE	DISTRIBUTED CLOUD EDGE
Real-Time Analytics	Low Value: Network is unable to respond to real-time analytics trends	High Value: Supported and integrated with service chains
User Application Policy	Complex implementation and support of only general application policy rules	Straightforward implementation that supports specific user application policy rules

Source: Heavy Reading

Distributed Cloud Use Case: vCPE

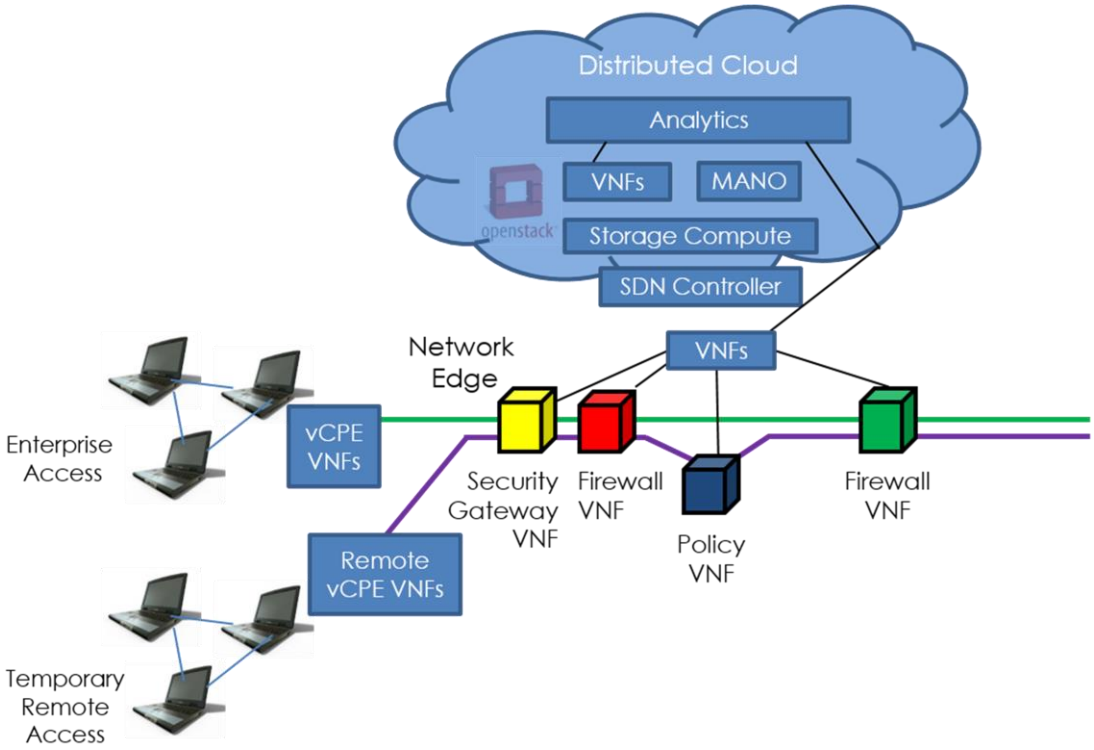
In this section, we document a use case that captures in greater detail the benefits of scaling, securing and orchestrating services at the network edge via distributed clouds. The use case selected is virtual customer premises equipment (vCPE).

One of the most promising initial applications for the distributed cloud is at the customer premises through the virtualization of customer premises equipment (vCPE). As we have touched upon, the two main drivers are to lower capex and to introduce much needed service flexibility and agility.

We believe that vCPE will have a profound impact, helping mitigate the quagmire of inflexible legacy equipment deployed in residences (e.g., cable head-ends), and more importantly in enterprises, where the application model has evolved into a slow-delivery and high-cost new service model, because of the limited vendor interworking and dedicated hardware configurations necessary to support even basic services.

As shown in **Figure 6**, by deploying vCPE in the enterprise it is no longer necessary to deploy dedicated firewalls or security gateways. Instead, vCPE VNFs that support these applications can run on a commoditized server, which greatly reduces cost to introduce and to maintain. Moreover, new software applications can also run in the same environment, which greatly shortens time to market.

Figure 6: vCPE Architecture



Source: Heavy Reading

As a result, vCPE can potentially undo decades of entrenched, proprietary networks in a very manageable and progressive way. It's also important to note that vCPE is extremely well-suited to leveraging the power of service chaining. By utilizing service chains, it becomes possible to chain vCPE links based on specific enterprise user requirements.

An example would be to assign and implement specific user privileges for individual users in terms of which applications or network capabilities they can utilize within the enterprise, and even which devices or terminals can be used for remote or temporary users. Enforcing this level of access could be accomplished via policy VNFs, dynamic routing capabilities and potentially analytics to monitor specific user profiles.

Juniper vCPE Implementation

In this section, we examine how Juniper's product portfolio has been optimized to support the vCPE use case documented in the previous section. This information is provided by Juniper.

Enterprise VPN Service Chains (Virtual CPE)

Virtualizing network services such as firewall, intrusion detection, content filtering, anti-virus, carrier-grade network address translation (CGNAT), deep packet inspection (DPI), distributed denial of service (DDoS) detection, secure socket layer (SSL) gateway and media cache – services that, until recently, have been deployed as specialized appliances – gives service providers the flexibility to offer new services without having to deploy new equipment at the customer premises (CPE).

Virtualized services are deployed in pools of servers that can be located locally to provider edge (PE) routers, customer premises edge, regionally in metro areas or in centralized data centers, depending on the performance requirements of the service (e.g., latency) and business constraints of the service provider (availability of space, power and cooling).

By leveraging cloud automation, Contrail Cloud, MX Series routers (physical or virtual) and vSRX for security services, customers can order services from providers that can be provisioned automatically and inserted into customer virtual private networks (VPNs) for immediate use.

Benefit

The combination of Contrail Cloud, MX and vMX routers, and vSRX security services provides an agile platform that allows network service providers to offer new services to their existing customer base. The compute infrastructure required to support the services can grow with service uptake, and the mix of services deployed can match customers' individual needs.

This enables network service providers to reinvent how they deliver services and opens up the possibility of new types of service offerings that align with the needs of their customers, while at the same time being able to turn up these services in minutes rather than weeks. The security services that require customization per customer can be instantiated with vSRX instances that focus on solving individual customer needs.

Detail

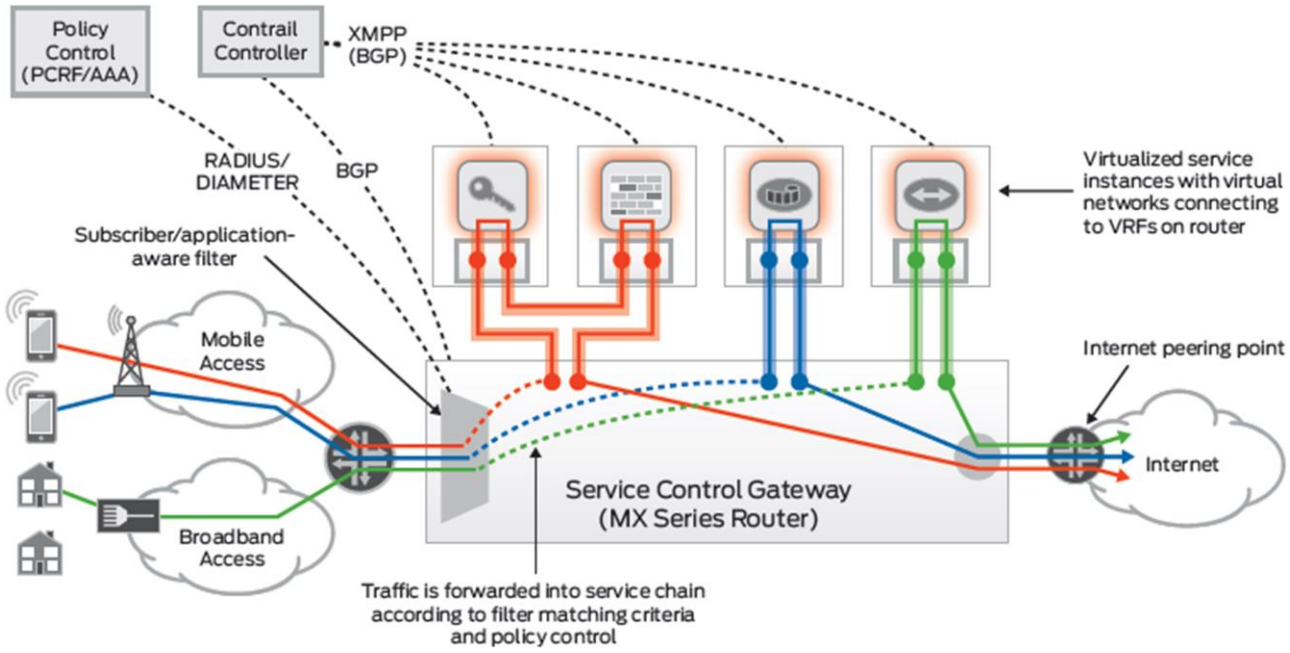
In this use case, virtualized appliances are inserted into the data path between two physical networks, allowing network service providers to offer additional services to existing Layer 3 VPN customers. Rather than extending customer VPNs to a centralized data center (although this is possible), data centers are more likely to be located close to the PE routers (in the same metro area or colocated with PE routers).

The intent is to attach virtualized appliances to customer VPNs to support services such as Internet access, security services (firewall, IDP, UTP, SSL) and media caching (content delivery network).

To form customer VPNs, each PE router is configured with a virtual routing function (VRF) for each customer with a connection to that PE, and each VRF contains the

interfaces that connect to that customer's sites. BGP is used to exchange routes between customer VRFs on all PE routers in the provider network, so a host on any customer site can reach destinations on any other site belonging to that customer. To form the custom service chain, these VRFs can be directed to the vSRX to perform the customer required security services.

Figure 7: Juniper Distributed Cloud Portfolio



Source: Juniper

Conclusion

Moving advanced network software-based functions to the edge via distributed clouds represents a new and innovative approach to extend cloud services. In the past, the edge model was based on the assumption that vendor interworking would be complex and cumbersome, with limited real-time personalization opportunities. With the distributed cloud, the edge is no longer a services or capacity bottleneck. Instead, it is transformed into a highly focused customer services cloud that introduces and supports new, unprecedented levels of automation, scalability, security and service delivery.