A New Strategy for an Enterprise Network Architecture

Ashton, Metzler
& Associates

Leverage Technology & Talent
for Success

Table of Contents

Introduction

The traditional enterprise architecture is often criticized as being expensive, complex and proprietary. One of the reasons for that characterization is that in the traditional enterprise devices, such as servers, storage, LAN switches, firewalls and load balancers are dedicated to a single service or application. This approach results in stranded capacity and hence leads to an increase in the overall cost of Enterprise IT. This approach also increases the time it takes to deploy a new service or application since new infrastructure must be designed, procured, installed and tested before a new service or application can go into production.

Another reason why the traditional architecture has such negative characteristics is because the key components of the infrastructure (e.g., compute, storage, networking) are hardware centric. Using networking as an example, network components such as switches and routers have traditionally been based on dedicated appliances and each appliance is itself based on dedicated hardware such as ASICs. The appliances are proprietary and the evolution of the ASIC's functionality is under the control of the provider of the appliance. Making matters worse, each appliance is configured individually and as a result, tasks such as provisioning and change management are very time consuming and error prone. One of the goals of this white paper is to describe some of the key industry trends that network organizations needs to support and which are very difficult, if not impossible to support with the traditional enterprise network architecture. Another goal is to describe some of the primary characteristics of an enterprise network architecture that enable network organizations to support those industry trends. The third goal of this white paper is to describe some of the principal components of NEC's network architecture.

Virtualization of the Local Area Network

As noted, the traditional enterprise architecture is hardware centric and is based on dedicated appliances. Several years ago, IT organizations began to adopt server virtualization whereby a physical server was partitioned in such a way that it appears to be multiple independent logical systems, usually referred to as virtual machines (VMs). One of the key factors driving the broad adoption of server virtualization is that it allows significant savings in both CAPEX and OPEX. Another key factor driving adoption is that server virtualization enables IT organizations to move a production VM between physical servers, which helps to:

- Streamline the provisioning of new applications;
- Improve backup and restoration operations;
- Enable zero-downtime maintenance

Unfortunately, in the traditional network architecture supporting the movement of a VM across a subnet boundary requires that the network be manually re-configured, which is a resource intensive, time consuming task.

For most IT organizations, the implementation of server virtualization was their first significant step towards moving away from an environment that was both hardware centric and comprised of dedicated servers and appliances and towards an environment that is often referred to as being a Software Defined Infrastructure (SDI). An SDI is the antithesis of the traditional enterprise architecture. For example, part of the promise of an SDI is that it will feature policy-based functionality. Applications will use that functionality to dynamically define its resource requirements in line with the company's security, compliance and performance requirements. That functionality will also cause the physical hardware that supports the SDI to be configured automatically to meet those requirements. This capability will facilitate more rapid application deployment and it will enable the IT function to be more responsive to business requirements.

A critical component of SDI is the network virtualization functionality that is provided by a Software Defined Network (SDN). The organization that is most closely associated with the development of SDN is the Open Networking Foundation (ONF). Whereas the traditional enterprise network architecture is closed and proprietary, the ONF has driven the development of open protocols such as OpenFlow to enable the deployment of standards-based SDN solutions. According to the ONF[1], "Implementing SDN via an open standard enables extraordinary agility while reducing service development and operational costs, and frees network administrators to integrate best-of-breed technology as it is developed."

Network virtualization isn't a new topic. IT organizations have implemented various forms of network virtualization for years; i.e., VLANs, VRF. However, unlike earlier forms of virtualization, in the context of an SDN network virtualization is end-to-end and it abstracts and pools network resources in a manner similar to how server virtualization abstracts and pools compute resources. These capabilities enable the creation of tenant-specific virtual networks whose topology is decoupled from the topology of the underlying physical network and it also enables IT organizations to dynamically create policy-based virtual networks to meet a wide range of requirements. Another one of the many advantages of an SDN-based architecture is that it centralizes control in the SDN controller which means that tasks such as provisioning and

[1] https://www.opennetworking.org/about/onf-overview

change management can be automated. Other advantages of an SDN-based architecture will be discussed in subsequent sections of this white paper.

Security beyond the Enterprise Perimeter

The *IBM X-Force Threat Intelligence Report 2016*[2] contains a statement that underscores the general trend of security intrusions. That statement is that, “It is safe to say that we have never before seen the magnitude and sophistication of online crime as we did in 2015—a trend that’s already proving to persist into 2016.”

Some of the other observations that were made in the IBM report include:

- In 2015 the total number of leaked records (i.e., emails, credit card numbers, passwords and other personally identifiable information) was over 600 million.
- TalkTalk, a UK-based telecom group was penetrated in 2015 by a group whose goal was to take their data hostage and get a ransom for its return. The total damage to TalkTalk was estimated to be 35 million British pounds.
- By 2019 cybercrime will become a 2.1 trillion dollar problem.

One of the reasons for the growing sophistication of online crime is the growing involvement of highly skilled hackers who are affiliated with organized crime[3]. That’s a significant development and it’s led to the creation of increasingly sophisticated criminal organizations that operate with the professionalism and structure of legitimate enterprises. However, a recent article on insider threat statistics[4] highlighted the fact that focusing just on external threats leaves a company vulnerable to other types of security breaches. According to that article, the greatest volume of security breaches come from ignorant or careless user actions that inadvertently cause security breaches.

The traditional approach to data center security has been to implement security appliances such as firewalls and IDS/IPS at the perimeter and have those appliances analyze traffic flowing in and out of the data center; a.k.a., north-south traffic. One limitation of that approach is that once a hacker has managed to penetrate the perimeter, the hacker is free to roam around the data center. Another limitation is that due to changing application architectures, today the vast majority of traffic is between devices within a data center; a.k.a., east-west traffic. Those limitations, combined with the dramatic growth in cybercrime and the extent of user-induced security breaches indicate that the traditional approach to security isn’t working. What is needed is a Zero Trust architectural approach that builds security into the architecture rather than layering it on as an afterthought and that also adopts a philosophy of “never trust, always verify” based on micro-segmentation. Micro-segmentation is a security technique that is based on the ability of the SDN controller to ensure that each tenant-specific virtual network has complete isolation from all of the other tenant-specific virtual networks. The capability enables fine-

[2] http://www-03.ibm.com/security/xforce/downloads.html
[3] http://www.csoonline.com/article/2938529/cyber-attacks-espionage/cybercrime-much-more-organized.html
[4] http://www.isdecisions.com/insider-threat/statistics.htm

grained security policies to be assigned to data center applications, down to the level of a network interface, based on policies established by the network organization.

Enabling Mobility

There are two distinct components of the trend towards increased mobility. One of those components is that workloads, which once were static, are becoming increasingly mobile. An example of that type of mobility is the previously mentioned movement of VMs between physical servers either within a data center or between data centers. Unfortunately, in the traditional enterprise network architecture moving a VM across a subnet boundary requires time-consuming, manual intervention which negates some of the advantages of server virtualization. Another one of the many advantages of the decoupling of the virtual networks from the physical networks that is associated with a SDN is that it enables VMs to cross subnet boundaries without requiring any manual intervention.

The other component of the movement towards increased mobility is that in the current environment the vast majority of employees require mobile access for at least part of their day, whether they are within a company facility or at an external site. Provisioning acceptable end-to-end services for users is always challenging. These challenges are exacerbated when the user is using a cellular network due to the high delay and packet loss that is often associated with those networks as well as the increased ease of snooping that traffic.

There is a broad movement to implement a policy based approach to all aspects of IT, including networking. Policies can be based on a hierarchical system of rules designed to deal with the complexities of the environment, and to manage the relationships among users, services, SLAs, and device level performance metrics. As mentioned, a key characteristic of an SDI is that it will feature a policy-based approach that enables applications to identify its resource requirements. More specifically, as was also mentioned, the capability to create tenant-specific virtual networks enables IT organizations to dynamically create policy-based virtual networks to meet a wide range of requirements, such as those that are necessary to support mobile users.

Better Quality of Experience with Real Time Applications

The 2016 State of the WAN Report contained the results of a survey in which the respondents were given 15 factors and were asked to indicate the factors that were driving their organization to change their WAN. Supporting real-time applications such as voice and video came in third behind increase security and reduce cost. This recent market research indicates that in spite of the fact that real-time applications such as VoIP and video have been widely deployed for years, ensuring acceptable performance of real-time applications is both challenging and something that IT organizations recognize that they must get better at. One of the reasons why supporting real time applications like voice and video is so challenging is the combination of the volume of traffic they generate and the great growth in that usage. For example, according to a recent article[5]:

- VoIP traffic will reach 158 petabytes monthly in 2016
- Between 2016 and 2021, VoIP traffic will grow at a 9.1% CAGR

Another reason why supporting real-time applications is so challenging is because the performance of these applications is very sensitive to relatively small amounts of delay, packet loss and jitter. End user quality of experience with these applications can be significantly impacted by other applications in the network. Isolating these issues in traditional networks can be very challenging and time consuming.

NEC and Software Defined Infrastructure

In 2011, NEC became a founding member of the ONF and in that same year, NEC introduced its ProgrammableFlow Networking Suite, the first commercially available SDN product to use the OpenFlow protocol. This Suite is currently comprised of an SDN controller, a management console, physical and virtual network switches as well as hybrid switches that are compatible with both OpenFlow-based and traditional networks. The management console supports the automatic visualization of the virtual and physical network topology as well as the tracking of flow patterns and traffic information. Over 600 organizations have adopted NEC's ProgrammableFlow Networking Suite and have used it to implement some of the largest and most complex networks in the world.

A key component of NEC's ProgrammableFlow Networking Suite is the Virtual Tenant Network (VTN) application. That application provides the security that is inherent with micro-segmentation by enabling the creation of virtual networks that are isolated and secure and each of which has its own network policy. Users of the application can design and deploy networks with the look and feel of a conventional L2 or L3 network. Once designed, the network will automatically be mapped onto the underlying physical network and then configured on the individual switches. The functionality provided by the VTN application reduces the complexity and time-consuming manual labor that is associated with the traditional enterprise architecture. In addition to driving for open SDN solutions by incorporating protocols such as OpenFlow into their solution, NEC has contributed their VTN application to OpenDaylight[6], which is an open source community that is dedicated to creating open SDN solutions.

NEC has recently announced its Smart Enterprise Strategy targeted to deliver the benefits of an SDI to the LAN (SD-LAN). A key aspect of this strategy is the integration of software defined networks with both real time applications and security. The integration of NEC's Unified Communication line of products with its Software Defined Networking Suite improves quality of

[5] http://www.ironpaper.com/webintel/articles/voip-market-stats/
[6] https://wiki.opendaylight.org/images/0/0e/NEC_VTN_Model_0606.pdf

experience by automating traditionally arduous tasks such as quality of service provisioning and by providing real time network flow level visibility. On the security side, NEC is integrating traditional network perimeter protection with SDN, enabling protection from cyber attacks from within the network. By automating this process, NEC has eliminated many of the manual steps required to protect mission critical assets.

The ProgrammableFlow Networking Suite is supported by an ecosystem of partners such as Microsoft, HPE, Palo Alto Networks, Red Hat, Sonicwall, and Dell. The ProgrammableFlow SDN Controller has integrated network and compute orchestration with OpenStack, as well as Microsoft System Center Virtual Machine Manager.

Summary

Enterprise IT infrastructure has traditionally been hardware centric and based on dedicated appliances. Driven in part by the need to operate more like a public cloud provider, enterprise IT infrastructures are going through a fundamental transformation to move away from being hardware defined to become software defined. Two of the primary characteristics of an SDI are that the infrastructure is designed to leverage software innovation over hardware innovation and to feature automation over manual operations.

IT organizations that are in the process of either refreshing their existing infrastructure or implementing new infrastructure should focus on the value provided by a software defined approach to infrastructure as well as to vendors with a proven track record of delivering software-centric solutions. From a network perspective, a software-centric approach provides measurable value in a variety of ways including enabling:

- Network virtualization which among other benefits enables the dynamic movement of workloads between servers;
- Policy-based virtual networks to meet a variety of requirements, including those of mobile users;
- Micro-segmentation of the network which enhances security by enabling each tenant-specific virtual network to have complete isolation from all other tenant-specific virtual networks;
- Better quality for real time applications by keeping the performance of these applications from being impacted by the traffic generated by other applications.

Over 600 organizations have already adopted NEC’s ProgrammableFlow Networking Suite and have used it to implement some of the largest and most complex networks in the world. A key component of this Suite is the VTN application which features micro-segmentation for added security and which also reduces the complexity and time-consuming manual labor that is associated with the traditional enterprise architecture. NEC has recently announced its Smart Enterprise Strategy targeted to deliver the benefits of an SDI to the LAN. One of the key aspects of this strategy is to integrate software defined networks with both real time applications and security. The ProgrammableFlow Networking Suite is supported by an ecosystem of partners such as Microsoft, HPE, Palo Alto Networks, Red Hat, Sonicwall, and Dell. In addition, the ProgrammableFlow SDN Controller has integrated network and compute orchestration with OpenStack, as well as Microsoft System Center Virtual Machine Manager.