White Paper

Getting on the Road to SDN

Attacking DMZ Security Issues with Advanced Networking Solutions

By Bob Laliberte, Senior Analyst

March 2014

This ESG White Paper was commissioned by NEC and is distributed under license from ESG.

Contents

The Network Needs to Transform

To better meet the needs of the business, organizations have been rapidly transforming their IT environments. The legacy, extremely static environments are being replaced by highly virtualized and dynamic environments capable of rapid change. This transformation is evident in many of the top IT initiatives reported by respondents to ESG research.

Organizations continue to increase their use of server virtualization, which, according to ESG research, has consistently been a top IT priority over the last several years, including 2013.[1] This technology has made significant strides in helping organizations to consolidate server infrastructure and more importantly, as organizations become more comfortable with the technology, leverage it to create more dynamic and flexible environments.

Another area that organizations have seen tremendous benefits from is consolidating data centers. By eliminating regional data centers into fewer yet larger centralized data centers, organizations have dramatically reduced infrastructure and application costs. However, the remaining data centers are also far more complex and subject to rapid scale, which they need to accommodate.

As a result, the network is under much greater pressure to deliver applications over larger and more complex environments. Unfortunately, legacy network architectures were not designed to handle these highly dynamic environments. While a new VM can be spun up in a matter of minutes, configuring a change in the network could take hours if not days or weeks. Proprietary hardware and software lock organizations into a single vendor and drive up costs for training and operation. Organizations need technologies that can enable an environment, not be a bottleneck.

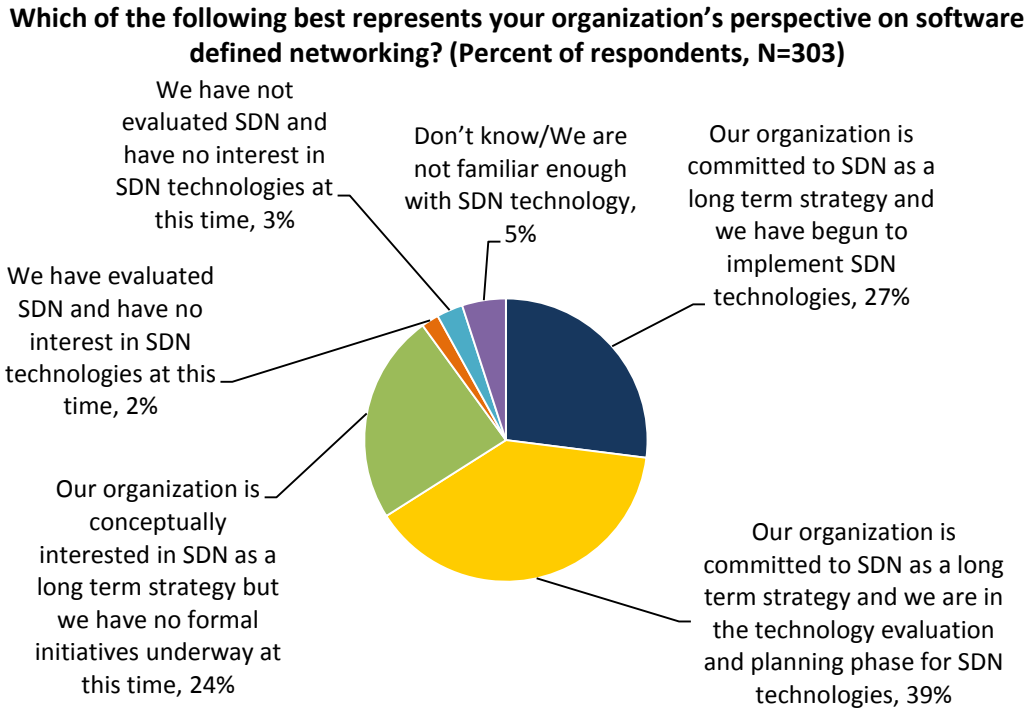
To that end, software-defined networking (SDN) holds significant promise to turn the network into an enabler of modern IT environments and not a bottleneck. The concept of SDN is to externalize the control plane to a centralized controller or other service. By centralizing the controller or service, opening APIs, and using software to program the network, SDN can help to eliminate the manual processes, configuration inflexibility, and latency challenges associated with device-centric networking.

Organizations Are Turning to SDN

The concept of SDN has been around for a while, but it has only been in the last year or so that is has really dominated the conversation in the public. Virtually every established vendor and numerous startups have begun to trumpet the benefits of SDN solutions. Because of this, most organizations have heard about SDN and are now including it as part of their network strategy moving forward. Indeed, according to Figure 1, ESG research indicates that two-thirds of respondents to a recent survey are committed to SDN as a long-term strategy, whether they have actually begun to implement solutions (27%) or are merely evaluating technologies at this point (39%). While organizations may vary regarding how they define implementing an SDN solution (virtual switches, open flow enabled devices, etc.), it is clear that organizations believe that SDN will be the future of networking.

[1] Source: ESG Research Report, *2013 IT Spending Intentions Survey*, January 2013.

Figure 1. Organizations Plans to Deploy SDN

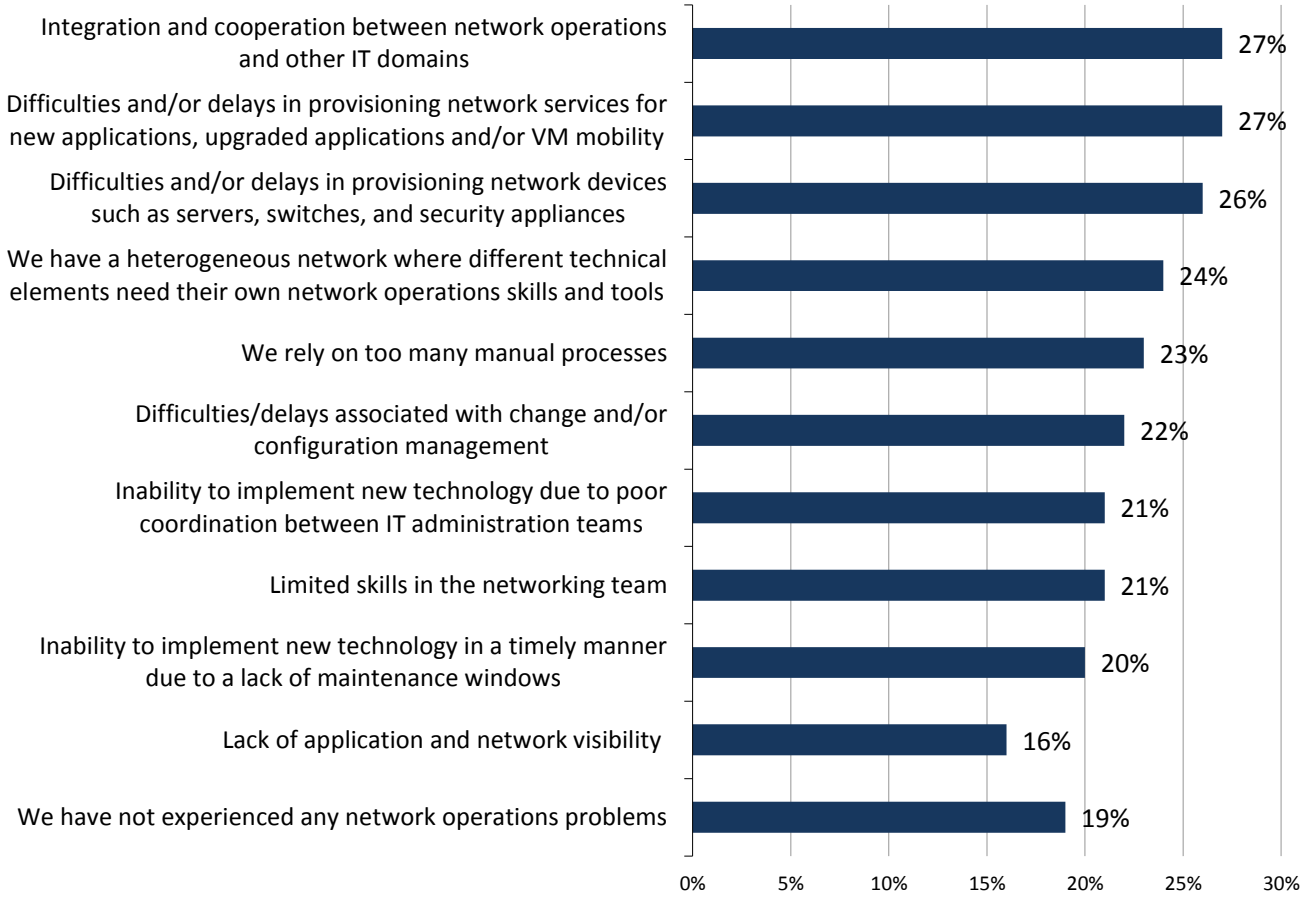


Source: Enterprise Strategy Group, 2014.

For many organizations, it is not about making a shift simply for the sake of implementing a new architecture, but it is about solving a specific problem. In the same survey, organizations were asked to identify operational problems stemming from their network infrastructure. Two out of the top three most-cited responses were related to the difficulty in provisioning network devices and network services (see Figure 2), essentially, highlighting the fact that the network has indeed become the bottleneck and there is a need to resolve this issue. The most-cited complaint was the ability to integrate with other domains—something that has become far more important in highly virtualized environments as all the technology domains have become tightly interdependent. It also addresses the need for automation and orchestration for those building out a private cloud environment. Further down the list, organizations reported that there are still too many manual processes, again creating a bottleneck.

Figure 2. Network Operations Problems

To the best of your knowledge, has your organization experienced any of the following network operations problems? (Percent of respondents, N=303, multiple responses accepted)

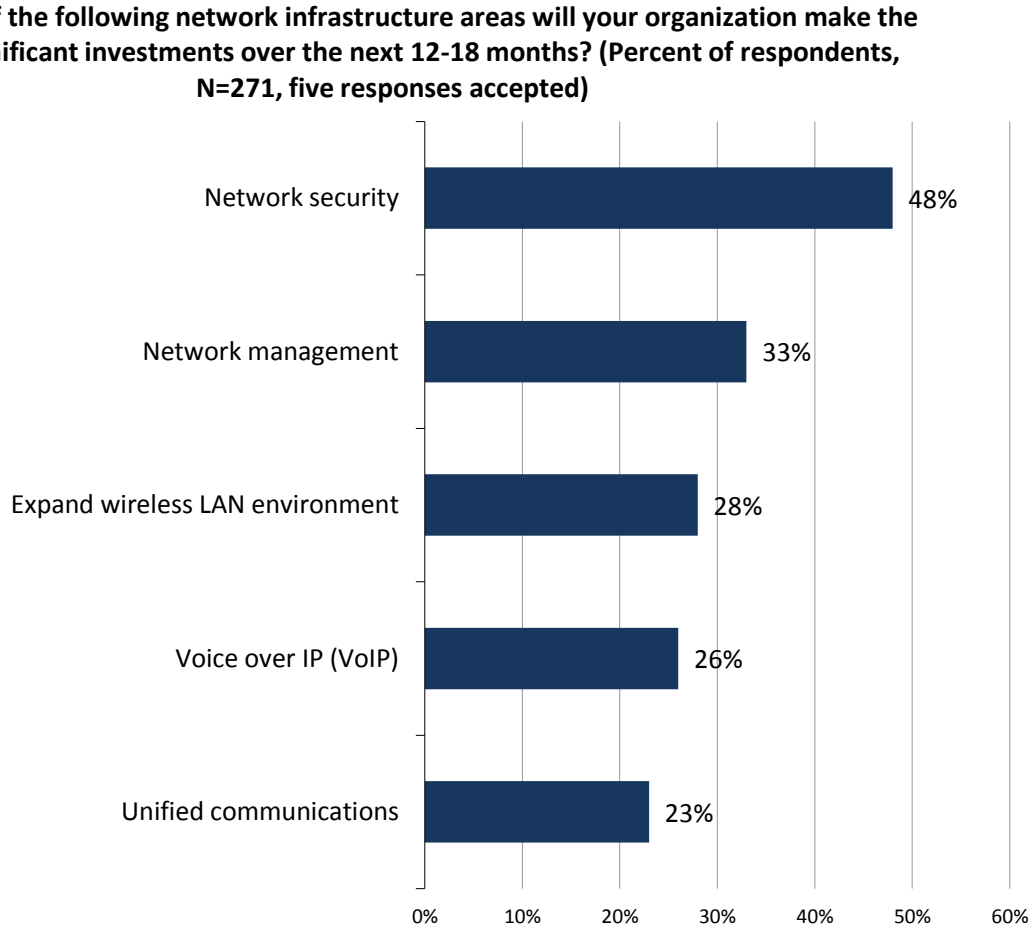


Source: Enterprise Strategy Group, 2014.

However, when it comes to delivering services for the network, one area stands above the rest. That would be network security. Indeed, network security is a top network challenge, with 56% of respondents citing it as such, which is not surprising considering that information security was the most-cited IT priority for 2013.[2] [3] As a result, organizations are also planning to make significant investments in network security area this year, with almost half the respondents (48%) selecting this as a top area of spend (see Figure 3).[4] Furthermore, for those organizations deploying or planning to deploy SDN solutions, network security (firewall, IDS, IPS) was also reported (65%) as the top area of focus.[5]

[2] Source: ESG Research Report, *2013 IT Spending Intentions Survey*, January 2013.
[3] Source: ESG Research Report, *The Evolving State of the Network*, December 2013.
[4] Source: ESG Research Brief, *2013 Networking Spending Trends*, March 2013.
[5] Source: ESG Research Report, *The Evolving State of the Network*, December 2013.

Figure 3. Most Significant Areas of Network Investments



Source: Enterprise Strategy Group, 2014.

Probably the hardest part of making a transition to a new architecture is how and where to get started. Given the focus on network security, as both a significant challenge and top area of investment, it make senses to see how an SDN cloud can help to improve security. Typically, when trying to justify a new technology, organizations need to have a quick win that has an impact and delivers value. That win, in turn, helps to get additional budget dollars for follow on projects. SDN is no different, and while the transition to modern data centers appears to be moving at an accelerated pace, it doesn't mean IT has a blank check. SDN purchases still need to be justified. Given that ESG research indicates that half of the organizations are dealing with a flat IT budget, SDN solutions really need to demonstrate value.[6]

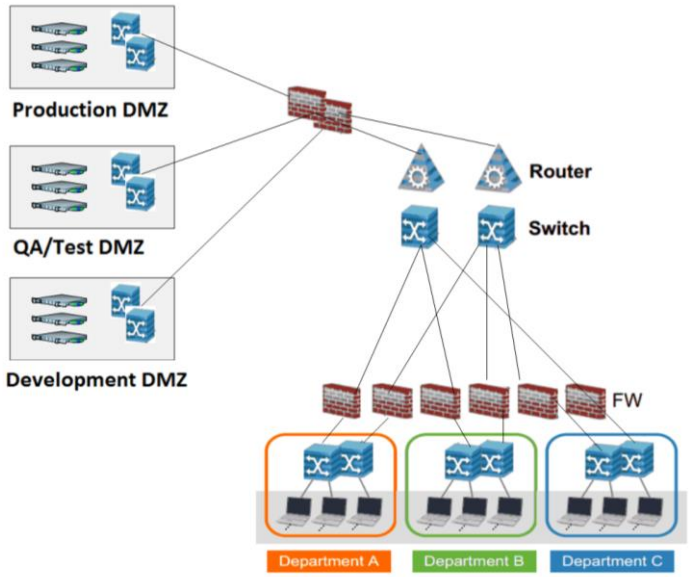
[6] Source: ESG Research Report, *2013 IT Spending Intentions Survey*, January 2013.

An Example of SDN in Action

Since network security is top of mind for most organizations, it would useful to take a look at an example of how SDN can be used as a cost-effective solution to enhance network security or in this case, more specifically, how it can improve a Demilitarized Zone (DMZ – a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet[7]) in computer networking. For this example, we will examine how an NEC ProgrammableFlow SDN solution comprised of a controller and open flow-enabled switches can effectively replace a legacy switch and firewall environment to provide greater flexibility and value.

Typical DMZ environments look something like the one outlined in Figure 4. This example DMZ represents a classic defense in-depth strategy that leverages dual firewalls. In this case, there are separate DMZ environments for production, QA/test, and development. However, leveraging legacy networking infrastructure means that there are multiple physical firewalls to maintain. This is not only costly to build out and maintain, but also creates a challenge for the IT team to ensure that network policies are aligned across each firewall. As a result, organizations deploying this model may find it difficult to keep up with rapid changes occurring as new applications or application upgrades are rolled out.

Figure 4. Traditional DMZ Environment

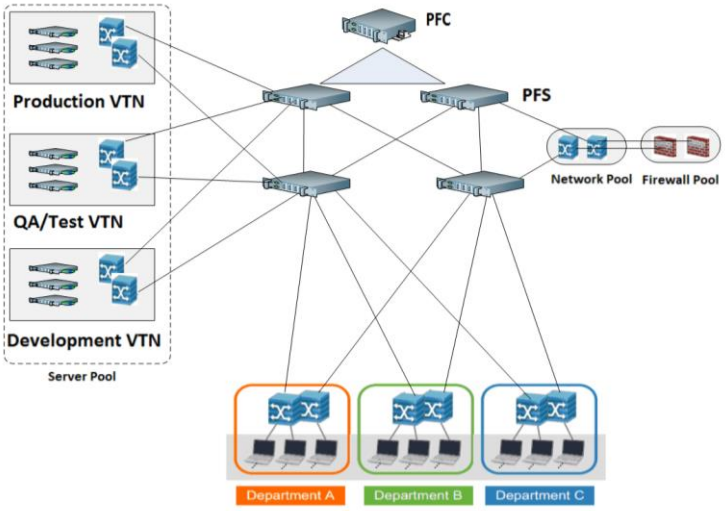


Source: NEC, 2013.

However, applying SDN solutions to the same environment can yield very different results. By leveraging an SDN solution, organizations can dramatically reduce or consolidate the number of network devices and firewalls deployed and, in some cases, may be able to eliminate the physical firewalls. Figure 5 outlines how an NEC SDN solution taking advantage of a ProgrammableFlow controller and switches can create and utilize pools of network and firewall resources capable of providing virtual separation, isolation, and filtering to better control traffic between departments, as well as traffic into and out of the DMZ. In this environment, both the firewall and network become pooled resources that are controlled through the ProgrammableFlow controller and, as such, can be rapidly allocated or reallocated to accommodate the needs of the business.

[7] Source: Wikipedia

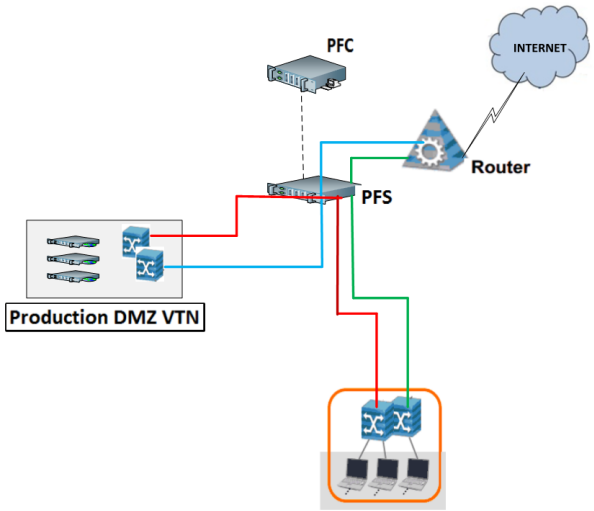
Figure 5. Leveraging SDN in the DMZ



Source: NEC, 2013.

To demonstrate the effectiveness of this solution, Figure 6 shows how each flow is separate. While isolated from one another, they also have the ability to communicate with resources in the DMZ, in the LAN or in the internet.

Figure 6. Independent Flows in the DMZ



Source: NEC, 2013.

Benefits of SDN in DMZ

This SDN enabled environment allows organizations to develop, test, and host web applications that leverage dedicated virtual networks. As a result, organizations can simultaneously develop and test on separate environments. Therefore, a load test in the QA/test environment will not impact development, or interrupt production. This is an important distinction for organizations that have adopted agile application development practices and require this level of flexibility and speed to accelerate their processes. In addition, in this example, you will note the need for multiple firewalls is greatly diminished. NEC claims that early pilots show this factor to be as much as 75-80%.

The Bigger Truth

Organizations need to transition to modern IT environments to keep pace with a dynamic global market. This means reevaluating how things are done in every area, including the DMZ. As organizations place more focus on the application and application development cycle, anytime the process can be accelerated should be a welcome improvement. And with the rapid advances taking place in the network, this is a good area to revisit, and perhaps to pilot.

Organizations also need to understand that making this transition does not require wholesale replacement of an entire network, but is more about finding critical areas where significant benefits can be achieved quickly. To that end, organizations need to examine their current environment and determine which areas could benefit from SDN, like the DMZ example highlighted in this paper.

While SDN technology is still evolving, some vendors can provide established and proven solutions. NEC was the first company to bring a commercially available OpenFlow controller to market and continues to evolve the technology and services ecosystem. The ProgrammableFlow controller and switches used in this example demonstrate how an organization can begin to transform its network leveraging SDN solutions.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com