White Paper

Next-generation Connectivity and Security for Enterprise Mobility and Hybrid Cloud Environments

By Mark Bowker, ESG Senior Analyst
August 2016

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

Hybrid Cloud Environments and Enterprise Mobility—Networking Matters ........................................................................ 3
Keys to Success in a Mobile World ................................................................................................................................ 3
   The Workspace Delivery Platform .................................................................................................................................. 3
   Workspace Components: Working in Harmony .............................................................................................................. 4
Potential Networking Pitfalls ........................................................................................................................................ 5
   Performance ....................................................................................................................................................................... 5
   Security ............................................................................................................................................................................... 5
   Network-enabled Cloud Model ........................................................................................................................................... 6
   Management Controls ........................................................................................................................................................ 6
Virtual Networking Implications ............................................................................................................................................. 6
   Physical Network Challenges ........................................................................................................................................... 7
   Overcoming Network Challenges with Network Virtualization .......................................................................................... 8
   Data Center Micro-segmentation: Providing Ubiquitous Control ........................................................................................... 8
   Benefits of Micro-segmentation and Virtualized Networking ............................................................................................. 9
The Bigger Truth .................................................................................................................................................................... 10
Hybrid Cloud Environments and Enterprise Mobility—Networking Matters

Businesses are finally committing to hybrid cloud strategies on a large scale, partly because CIOs and CEOs are convinced of their benefits, and partly because they have become a business imperative, especially with the consumerization of IT. Today’s employees no longer consume information on one company-issued device, but instead they do so from a variety of endpoint devices. Additionally, a wide range of application delivery models have evolved—including software-as-a-service (SaaS), Web-based, Windows, and mobile applications—largely because of their convenience, flexibility, and ability to scale on demand.

No longer are all the data, applications, and IT resources locked up in physical data centers. Compounding the complexity of this current environment is the fact that these disparate solutions can be deployed in a variety of ways, including by being hosted in private, public, or hybrid clouds. Businesses are embracing and accelerating the adoption of these cloud consumption models primarily due to their global scalability and simplified access to mobile applications and data, along with enhanced IT management, and cost-effectiveness.

Now, the challenge has shifted to developing connectivity between all the devices, the on-premises resources, other application delivery models, and cloud providers. What really matters is having reliable, secure, low-latency, high-performing networks that create connections back to those data centers and into those cloud consumption models.

Commitment is one thing, and execution is another. In order to realize the potential of hybrid cloud infrastructures, some strategizing and planning has to be done. For starters, mobility strategies need to work in tandem with cloud computing strategies. This requires businesses to change how mission-critical applications are built, and how desktops are architected and managed. It also requires them to establish policies and processes, and provide data access on a global scale via virtualized networks. These networks must be able to scale out as needed in order to efficiently provision cloud resources because businesses require the flexibility to leverage new cloud services on demand, anywhere, and at any time. To no one’s surprise, all these challenges in modern mobile architectures are putting pressure on IT professionals to make sure resources are available and sufficiently robust to satisfy performance requirements and alleviate security risks.

Keys to Success in a Mobile World

The Workspace Delivery Platform

This fast pace of consumer technology innovation in conjunction with the onslaught of varied application and desktop delivery models have made managing and securing applications and devices difficult for even the most sophisticated IT shops. Add in the challenges of meeting compliance and government regulations, and it all comes out to a multi-front battle for IT.

This transformation to a user-centric, self-service computing model requires enterprises to rethink business mobility in a hybrid cloud environment. The digital workspace supports this transformation by providing a more efficient model for delivering and managing enterprise apps to users across all their devices—one that aggregates different applications, data delivery, devices, and consumption models like hybrid cloud environments. The workspace platform centralizes IT management, provisioning, and security on an intelligent infrastructure, and provides users with a common, easily accessible interface. Unlike the desktop of the client-server era, the digital workspace is not defined by a single image. It is the aggregation of all devices, and the apps and services required by users, securely managed and unified by common access and identity (see Figure 1).¹

By federating application and desktop environments within a single interface, a workspace delivery platform creates a user-centric computing model that provides many benefits, including:

- Creation of a modern mobility architecture to deliver apps and data with improved security, simpler management at lower costs, and access to applications and services across any device.
- A broad range of device and ownership models with increased security for data, applications, and infrastructure, allowing work and personal data to coexist on the same device.
- Secure, improved access and management of applications, email, browsing, and content from any device.
- Increased collaboration across corporate content without risk to privacy or data loss.
- Ubiquitous accessibility on any device, enhanced user experiences, and improved business processes.

**Workspace Components: Working in Harmony**

A comprehensive digital workspace platform is comprised of many components and technologies, all of which must work in harmony in order to achieve the end goal of securely delivering applications and data to users.

Identity and access management (IAM) plays a key role in advanced digital workspaces. For example, enterprises that deploy digital workspaces can use any device—BYOD or corporate—while IT administrators automate application
distribution and updates on the fly. This ability exists because IAM transcends every application, across every device. Other key features of IAM include enabling enterprise single sign-on (SSO), which allows users to access the disparate apps and systems they need without complex passwords or configuration steps. Conversely, it ensures that access to apps can be turned off at a single point, protecting against data loss. It further delivers one-touch access to nearly any app from any device. Succinctly stated, IAM provides one infrastructure for managing users across multiple app types and device types.

Workspaces support a wide range of applications—SaaS, mobile, Web, desktop, Windows, etc.—all from one place. This is pivotal to streamlining data access, maintaining productivity from anywhere, and simplifying IT management.

With enterprise mobility management (EMM), another key facet of digital workspaces, enterprises can gain control over the proliferation of devices across all platforms through unified security and management, while offering self-service access to apps on users’ choice of devices. They can set and manage policies for the user that travel with the devices and applications based on a variety of factors, e.g., network location, user location, or the time of day. Enterprises can manage all devices from one central console regardless of the device type, its operating system, or its owner. EMM containerization provides complete separation of corporate and personal data, protecting corporate data at the user, application, device, and network levels.

In order to realize all these capabilities, it is important for digital workspaces to have an intelligent network for the necessary connectivity and security it offers. In fact, this virtualized network is the very bedrock of cloud computing, and the foundation of digital workspaces.

**Potential Networking Pitfalls**

When thinking about potential pitfalls and business challenges associated with hybrid clouds and business mobility, it doesn’t take long to come up with a short list of three usual suspects: performance, security, and management controls. It should come as no surprise that the networking aspects of these three challenges have reached high-priority status throughout many enterprises.

**Performance**

Many organizations are upping the ante by implementing new hybrid cloud strategies, including connecting their data centers to private, public, and hybrid clouds. This allows them to consume both on-premises and cloud-based resources, and increases their mobility. However, performance can take a big hit if these strategies fail to reach their potential, e.g., businesses may find access to certain cloud environments creates more latency and delays than others. Virtual private networks (VPNs), for example, let you route traffic directly from apps and devices to the cloud providers, which minimizes performance hits. Additionally, traditional network approaches may slow performance due to bandwidth issues while network virtualization automatically can scale up bandwidth for peak traffic loads.

The only way to reduce latency without compromising security is by minimizing transit hops. Hypervisor integration, found in network virtualization, expedites host traffic between firewalls by typically slashing the number of network hops required when moving from one host to another. With network virtualization, the control plane allows the distributed firewall to be replicated across all the hosts in the environment, which reduces the complexity and still provides greater speed and security.

**Security**

Security is a mission-critical issue that has only become more complex as IT infrastructures have evolved across multiple distributed computing paradigms. In hybrid cloud environments, networks are responsible for connecting server and storage pools with IT users. However, as a result of inconsistent network security between cloud providers and businesses,
organizations have been reluctant to send anything more sensitive than their lowest tier data to hybrid clouds, which, because of their semi-public nature, are more vulnerable to security attacks.

Cloud computing can create tension between performance and security. Not all cloud providers will support encryption, so information may be sent in the open on the Internet without permission. Where encryption is available, using it may increase latency and impact performance.

**Network-enabled Cloud Model**

There are vendors who enable organizations to safely move mission-critical applications to the cloud and protect them without sacrificing security, performance, or control. These companies employ a network-enabled cloud (NEC) model combining the control, protection, and performance advantages of private clouds with the cost-effectiveness and elasticity of public cloud services.

NEC providers employ virtual private networks that connect to any cloud compute or IT service environments offered by third-party partners. This allows these providers to take advantage of elastic compute, which makes it easy to adjust network and cloud resources on demand. It also gives these businesses secure, high-performance connections. By taking traffic off the Internet and routing it directly to a cloud provider, enterprises can take advantage of a highly secure connection between the VPN and the cloud, and reduce latency.

NEC capabilities appeal to customers who are looking to leverage the same tools, technologies, and skills that they already have, while delivering new hybrid cloud capabilities.

**Management Controls**

Hybrid cloud domains present multi-faceted management challenges. This is because in the hybrid world, compute, network, and storage resources have to be managed across multiple domains. However, virtualized networks ease IT management since everything can be controlled and centralized in the data center.

Once again, virtual networks play a pivotal role in hybrid cloud management. They do this by enabling network services to be abstracted from firmware into individual control layers, leading to more flexible networks that provide better support for hybrid environments.

**Virtual Networking Implications**

With the enormous growth in mobile devices and applications accessing business-critical resources, limiting users’ access inside the firewall is key to preventing unauthorized access and cyber threats. Any cyber-attack can readily move from the mobile application to internal servers, exposing a large attack surface.

Instead of having a traditional network with appliances and physical IT infrastructures, the network is virtualized into a pool of transport capacity. In this highly virtualized environment, all of those networking and security policies are built in at the virtual machine (VM) or mobile application workload so they immediately know what to do without going out to a physical network. With software-defined networking, enterprises can provide VPNs or other virtualized networks on a per-app or per-user basis that go into off-premises cloud-based resources, and dynamically set the policies that travel with that application or employee.

It’s easy to see that delivering secured digital workspaces while achieving business mobility is no mean feat. But with the right EMM and network solution, enterprises can connect hybrid clouds, various types of applications, and data to every mobile device and every mobile operating system.

What are the traditional network challenges and how can they be overcome with network virtualization?
Physical Network Challenges

Some organizations may try to secure some platforms by establishing different zones for each—e.g., zones for databases, finance, marketing, etc.—with different physical firewalls inside each zone. However, this kind of networking can be difficult to implement, may require lots of physical infrastructure, and can be labor-intensive, since networking teams are forced to manage multiple VLANs, access control lists (ACLs), and disparate firewall solutions that may require many interfaces that must be configured compatibly.

Figure 2. Physical Network Environments without Virtualized Networking

Businesses operating in these physical environments are always striving to satisfy the constant demand for more workloads and more networks that must be manually provisioned on a box-by-box basis, which means configuring all the porting, firewalls, LANs, and ACLs.

Complicating matters further, these manual network configurations and fragmented management operations open the door to human error. Even if all these management challenges are overcome, organizations still don’t have visibility into threats happening inside the devices, and are still vulnerable to unpredictable user behaviors. The ongoing challenge for IT is ensuring that these resources are securely segmented but easily accessible.

With all this physical networking in place, data access can still be compromised by third parties who have local or remote access to data centers. For example, there are two options for entry: access to a VM in its own DMZ with restricted access to applications inside the firewall, or access to an internal restricted VM pool via a jump box. Once third parties have penetrated a data center, it’s very difficult to control and restrict their movements. This is where software-defined networking can help.

Even though security is continually improving, perimeter firewalls are not enough to protect against attacks on east-west network traffic inside the data center. As a result, users are vulnerable to threats from various sources, such as compromised websites, malware, and even their colleagues. At a point when the IT world is moving swiftly toward software-defined technologies, physical networks have become challenging assets that make it hard to scale in highly virtualized compute environments.
Overcoming Network Challenges with Network Virtualization

Managing data center access with network virtualization provides in-depth, dynamically applied protection of VMs and other mobile applications. With network virtualization, organizations can do the same things with networks that they’re able to do with virtual machine implementations—namely clone, snapshot, replicate, and secure the networks.

Network virtualization limits access to applications and network services inside data centers by enabling organizations to set up firewalls at the virtual network interface cards (NIC) of VMs. This allows them to apply security policies or firewall rules on a per-user or per-app basis.

Network virtualization also brings order to IT infrastructures by allowing IT administrators to create zero-trust rules that restrict data center access. These firewall rules limit the amount of damage that can be done because users only have access to individual virtual machines or servers, and cannot jump from those individual VMs to others. This is an important deterrent to hackers who break into data center workloads intending to move with impunity from VM to VM. With network virtualization, IT is able to create boundaries for third parties—such as developers, contractors, or anyone else roaming through data centers—that restrict east-west traffic and limit access to services.

Data Center Micro-segmentation: Providing Ubiquitous Control

Restricting data center access down to individual workloads is based on the concept of micro-segmentation, which enables security that automatically follows VMs across devices and locations, and gives each VM its own perimeter defense. Micro-segmentation provides the ability to create security based on either individual network segments, or different groups, such as internal sales and finance. It also ensures that individual networked VMs are all protected or isolated from one another, leaving potential attackers on the outside. If a user’s mobile app becomes compromised, the potential exposure can be easily contained to just that user. While all this isolation and segmentation is taking place, users are still able to fully access other services and capabilities as needed.

FIGURE 3. Data Center Micro-segmentation Explained

Source: Enterprise Strategy Group, 2016
Benefits of Micro-segmentation and Virtualized Networking

There are many benefits of leveraging micro-segmentation and software-defined networking:

- **Inter- and Intra-data Center Connectivity**: Just as policies are created to govern everything from access to intelligent networks, to apps and scalability, so too are they applied to inter- and intra-data center connectivity. IT administrators need to set up common, automated policies only once, which are then applied to multiple hybrid computing environments as well as intra-data center connectivity. The end results are more standardized environments that streamline operations and reduce the need for manual intervention.

- **Policies for Mobile Apps**: Mobile apps are becoming increasingly sophisticated and popular as they meet and exceed the needs of mobile devices such as smartphones and tablets—many of which are sold with several apps bundled in as pre-installed software. These pre-installed packages include web browsers, email clients, calendars, and mapping programs. Now that mobility has gained so much ground in enterprise environments, employees are demanding access to secure mobile apps from corporate networks or third-party clouds. Policies that follow mobile applications without requiring resource- and labor-intensive network provisioning can be created in seconds.

- **Securing Apps and Access**: Virtualization and encapsulation at all layers of the network ensure there is no cross-talk between networks, and there is a controlled communication path within a single network. This ensures a granular level of security and policies based on logical groupings of VMs. Digital workspaces depend on the virtualized network for identity and access management, which play a key role in the functioning of these workspaces.

- **Scaling Bandwidth**: Elastic scalability is critically important to cloud service providers who find themselves competing in a very intense market. Offering the ability to automatically scale out and back rapidly in accordance with demand is an absolute requirement in this market segment, and network virtualization enables that capability to dynamically provision networks based on user needs.

- **Simplified Networking Management**: In virtualized networks, security policies can be quickly created, changed, and managed based on the operating system, the user, or the mobile workload. This simplicity exists because virtual networking solutions embed security functions into hypervisors. Additionally, by using a library of virtualized network functions, virtual networks can be built and managed without the complexity of traditional physical networking.

- **Automated Policies That Dynamically Follow Users and Virtual Machines**: Administrators can set policies that dynamically map to users based on roles, groupings, and even location—dependent of the underlying network infrastructure. Micro-segmentation provides ubiquitous control by leveraging the management plane and applying centrally administered policies to each VM as it is created. If one VM is compromised, enterprises are not going to have to deal with issues in the rest of their infrastructure. Nor will they have to deal with threats that might be inside a client-to-server hack. Organizations can scale knowing network security policies are intelligently following each workload.

- **Third-party Partner Integration**: The quality of network connectivity and secure storage between private data centers and cloud storage providers is a variable that puts off many businesses who would like to commit more resources to hybrid clouds. NEC providers work around that problem by employing virtual private networks that connect to cloud compute or IT service environments offered by third-party partners without having to traverse the Internet. Additionally, by working with partner security solutions, there is greater extensibility of security...
beyond just endpoints. These solutions protect operating systems, email servers, and browsers from such things as malware and zero-day threats.

Software-defined networking truly allows users to bridge endpoint security with data center security. This enables administrators to provide granular security controls for mobile workloads, create policy-defined network access for mobile apps and users, and limit the mobile access footprint within the data center to minimize cyber-attack surfaces.

The Bigger Truth

Backed by an ecosystem of network and cloud service providers, hybrid cloud is fulfilling its promise to deliver state-of-the-art business mobility infrastructures. As a result, users are becoming more comfortable with the idea of increasing the sensitivity of data they send to the cloud, and doubling down on their mobility commitments. Cloud service providers are offering the speed, efficiency, and flexibility to meet enterprise mobility demands.

Network virtualization has become both a very significant change agent and a critical component of success in this more progressive IT environment by enhancing security, performance, and management controls. With network virtualization, enterprises can leverage new mobile and cloud innovations on demand, and mobile computing environments like digital workspaces can offer enterprise-level security. IT benefits from streamlined operations through centralized and simplified network management.

The long-term potential for hybrid cloud platforms and enterprise mobility depends on global scale and access to virtual networks that unlock data while providing in-depth protection of mission-critical business workloads.