Transforming Cloud Datacenter Security for Business Mobility Using Smart Networking

WHITE PAPER

vmware®

Transformation Overview

Introduction

Organizations that invest in proprietary applications and data for competitive advantage in their industries only succeed by making those investments available to employees, customers, and partners that drive revenue and opportunity. Securing those investments requires a fresh perspective as the types of devices accessing the cloud datacenter are changing rapidly and new workloads, such as VDI desktops, are appearing more regularly alongside server workloads. These changes alter the potential attacks and potential threats to datacenters whose security primarily stands firm at the perimeter, however, within the data center the security is weak.

By combining VMware NSX with the AirWatch Tunnel and/or VMware Horizon View, organizations are able to bridge the device to datacenter security gap in a way that both increases the overall security of the cloud datacenter and makes it far simpler to manage security through defining and delegating application and services to specific users. This enables IT to increase security while lowering the access and authentication burden on the users.

Many organizations have invested heavily in the development of secure private cloud datacenters. Datacenters are rich with expensive, proprietary applications and sensitive data all of which are intended for authorized access by users in a number of different access scenarios. Currently, when access to applications and data is required from outside the corporate network, organizations employ strong perimeter security and provide a secure VPN gateway to allow connections into the private cloud. Companies recognize the value in datacenter security and invest money and time into securing their stored data. Securing the data center helps protect customer-facing and revenue generating information that in the long run, helps run the business and secure a company's future. This difficult balancing act inhibits IT's agility because the need to secure cloud datacenter applications and data is often at odds with rapidly developing new access models and entitling access to them as the business identifies new opportunities.

While companies see the value in securing their data in datacenters, they still must balance the security risks. As more and more different types of devices are introduced to the workplace, organizations need to balance the payoff from leveraging their applications and data use cases with the exposure to a diverse set of devices, operating systems, and endpoint security profiles. Once inside the cloud datacenter, users in a secure perimeter-centric design have nearly unlimited access to adjacent workloads. Modern attacks exploit the perimeter-centric defense by hitching a ride from authorized users using secure VPN connections. From there, they move laterally within the datacenter on to more sensitive data and applications. While a user may have access to data in the data center, there is still information an IT department may not want to make available to all users, but the current design of datacenter security lacks a way of preventing this instance.

IT requires a solution that solves this challenge of securing proprietary applications and data in the cloud datacenter and is available only to users and devices that are delegated safe for access. VMware NSX solves this challenge through user-level micro-segmentation. The VMware NSX approach offers several differentiated advantages over traditional security approaches.

Differentiated Advantages to Traditional Security

- Automated provisioning
- Automated move/add/change for workloads
- Distributed policy enforcement at every virtual interface
- In-hypervisor, scale-out distributed firewalling baked into the kernel itself

VMware offers VMware NSX with Horizon Workspace Suite, a compelling solution to the challenge of an ever-changing world of business mobility.

About VMware NSX

VMware NSX is the network virtualization platform for the Software-Defined Data Center (SDDC). NSX enables organizations to treat their physical network as a pool of transport capacity, with network and security services attached to virtual machines with a policy-driven approach. VMware NSX offers customers network virtualization through isolation, network segmentation and security, as well as advanced security and automation at a lower cost than using traditional physical networking infrastructure. The cost savings are achieved first by eliminating the need for custom designed physical gear for networking in favor of using basic-functionality switches such as the physical layer for physical NICs (pNICs) in vSphere hosts running VMware NSX. Cost savings are also achieved through lower operational expense, made possible by simplifying and automating security services definition and deployment. This is achieved through the integration into VMware vSphere and intuitive workflows.

Network isolation describes the capability of NSX to use a physical network infrastructure as a transport medium for fully isolated networks to traverse. The isolation is so complete that the IP addressing of the virtual network can be the same or different from the physical network. It can even be a different type, such as running IPv6 over an IPv4 network. This form of network isolation is most useful in multi-tenant or multi-use scenarios, such as Dev, Test or Production. In these scenarios, you can provision entire networks that are duplicates of each other but operate separately and without conflict.

Network segmentation and security are the key value propositions for VMware NSX. Traditionally, network segmentation is a function of a physical firewall or router, designed to allow or deny traffic between network segments or tiers. An example is segmenting traffic between a web tier, application tier and database tier. Traditional processes for defining and configuring segmentation are time consuming and highly prone to human error, resulting in a large percentage of security breaches. Implementation requires deep and specific expertise in device configuration syntax, network addressing and application ports and protocols. Traditional network segmentation approaches are generally based on network port definitions and involve physical connectivity, therefore requiring additional or certain kinds of hardware and specific product expertise to for successful implementation.

NSX and Micro-segmentation

NSX introduces a network concept known as "micro-segmentation." Micro segmentation is the ability to apply fine-grained access policies for applications or network services. Micro-segmentation via NSX is made operationally feasible and cost effective due to the unique differentiation of the NSX logical distributed firewall. The NSX distributed firewall (DFW) is the cornerstone of the security capabilities in NSX, and is simple and elegant in its design and deployment. After deploying the NSX management plane (one VM appliance for the NSX Manager) and three control plane components (three NSX Controller VM appliances) an administrator easily pushes a set of vSphere Installable Bundles (VIBs) to the vSphere hosts in the clusters via the vSphere web client. From here, NSX is ready to enforce security policies down to the virtual NIC (vNIC).

Defining security policies around cloud datacenter applications and services is straightforward in NSX. Within NSX Manager is a tool called Service Composer where NSX administrators build security groups and policies in an intuitive way. Security policies are defined and applied to security groups, and the security groups themselves are populated dynamically, as opposed to a static method. Through Service Composer, a service is defined through a set of criteria, such as a VM name, custom tag, IP address, or vCenter entity. The service or application need not be running virtualized to be included in the definition. Once defined, the dynamic group and security policies are applied to all objects and entities that fit the criteria, regardless of where they are running in the infrastructure. This approach enables automated policy application and dynamic change control for the most exposed and sensitive applications and data in the cloud datacenter.

Securing Mobile Applications with VMware NSX and AirWatch Enterprise Mobility Management

In the business mobility world, there is a blurred line between work and personal devices, applications, and data. Mobile workers often need and expect to multitask between work and personal tasks. A per-device VPN connection is ill suited for this manner of work style because all traffic from the device will flow through the cloud datacenter's Internet connection when the corporate VPN connection is active, regardless of its personal or productive nature. This means that both authorized company-managed apps and personal unauthorized apps have equal access to the entire cloud datacenter.

Through the combination of AirWatch and NSX, organizations can complete the security bridge from the device to the cloud data center while leveraging the user, device and application validation. The first line of security is preventing personal or non-managed applications from using the secure cloud datacenter connection by enabling application tunneling through the AirWatch tunnel. When deploying an application with a per-app VPN configuration, the AirWatch administrator can ensure that only an entitled user on a validated device using an authorized application is accessing a secure cloud datacenter connection at a given time. The VPN tunnel is activated entirely in the background of the application launch and is transparent to the user. When the application is closed, the app VPN tunnel closes as well.

VMware NSX further secures this connection by ensuring the users of the AirWatch VPN tunnel are limited to accessing only the mobile applications and resources defined through the AirWatch console. Through an easy to use GUI, an NSX administrator can define each mobile application in the cloud datacenter in the NSX Manager's Service Composer as a dynamic security group just one time. Then, they can ensure

that only entitled users of AirWatch mobile applications can access authorized cloud datacenter resources, without overexposing sensitive datacenter information. This increased security posture comes without any inconvenience or interaction on the part of the users, who see only their applications launch via SSO or standard multi-factor authentication.

Securing VDI Desktops with VMware NSX and VMware Horizon View

Virtual Desktop Infrastructure (VDI) is not a new concept; though advances in display protocols, storage performance, and GPU-based 3D acceleration have driven adoption levels to all time highs. VDI is a compelling solution for organizations that wish to keep their business-critical Windows desktop applications and data in the datacenter, or are deploying many standardized desktops rapidly and securely, as in a mergers and acquisition scenarios.

Securing the desktop additions to the datacenter is a critical consideration for desktop and private cloud datacenter architects alike, as the user desktop workload profile is vastly different from the server workload profile. Server workloads, the traditional workload profile of the datacenter, tend to be very static. Applications are installed and updated infrequently, interactive console sessions are strongly discouraged and tightly controlled, and any changes required of the server workloads normally go through stringent change control. Server interaction with the Internet is usually very limited and typically involves responding in a highly structured way to specific types of access requests originating from the Internet.

Desktop workload profiles are in stark contrast to server workload profiles. Desktops are highly dynamic, as they are changing frequently in terms of application and OS updates, user customization and data creation or manipulation. New application requests are frequent and rarely follow change control. Additionally, users spend eight hours a day or more logged on interactively at the desktop console, accessing the Internet via email and web, therefore exposing users to phishing attacks and possible malware-infected sites. Indeed, an exploited VDI desktop is the crown jewel of any hacker hoping to exploit the treasures of an organizations' applications and data in the private cloud datacenter.

Securing VDI desktops through the combination of VMware NSX and VMware Horizon is an easy win. Private cloud datacenter exploits are most successful when attackers are able to compromise one or several workloads in the datacenter and then use these machines as a launching point to traverse the lax east-west controls on to other, more valuable targets. With VMware NSX, administrators are able to easily create a micro-segment for every desktop pool in the VDI deployment and limit network traffic strictly to entitled applications and data, thus blocking desktop to desktop or desktop to server malware or virus propagation. Using the NSX Manager Service Composer tool, administrators can create dynamic groups corresponding to the VDI desktop pools and NSX will automatically apply the relevant policy to all desktops in the pool without requiring static or manual updates, even if the desktop pool changes in size or configuration.