SDN and the Transformation of the Software-Defined Data Center

Software-Defined Networking (SDN) is starting to have a profound impact on not just the data center network, but network security as well. As networking vendors are now hitting the market with programmable switches, network controllers and orchestration tools, the initial early hype around is now giving way to real and implementable solutions. As SDN becomes a strategic topic for IT networking and infrastructure teams, it shouldn’t be planned in isolation, but instead as a component of a larger data center evolution.

This transformation started a decade ago with x86 hypervisors delivering greater IT efficiency through server virtualization. But as cloud computing drove further evolution of Infrastructure-as-a-Service (IaaS) with greater agility and elasticity, those concepts have spilled over network virtualization and SDN, as well as into Software-Defined Storage, Software-Defined WAN, etc. Many analysts and pundits have variously termed Software-Defined Data Center (SDDC), or SDI/SDx (SD Infrastructure/Anything).

Network security is also being impacted. Firewalls, intrusion prevention, and other security appliances have traditionally been deployed as hardware devices at discrete points in the physical network, such as the ingress/egress point at the network edge. But as security needs to increasingly be deployed throughout the network to counter against advanced threats inside the perimeter, there are challenges maintaining visibility and control with dynamic and logical network flows in increasingly software-defined environments. With the profound and fundamental changes to data center infrastructure, constricting traffic through a few fixed static inspection points would negate many of the benefits of Infrastructure-as-a-Service agility.

“SDx is a collective term that encapsulates the growing market momentum for improved standards for infrastructure programmability and data center interoperability driven by automation inherent to cloud computing” – Gartner Research
Introducing the SDN Security Framework

Network security needs to evolve as well. Fortinet’s vision is that security is itself a fundamental layer of IT infrastructure, as essential as compute, storage, and networking; hence Security needs to transform to become “Software-Defined” as well – in other words as agile and elastic as other data center infrastructure. Fortinet is introducing the SDN Security Framework to define how security solutions need to evolve for Software-Defined Networks and Data Centers.

While integration with the SDN controller or platform is one key means of achieving agile network security, it is equally important to be able integrate with hypervisors, cloud management, and intelligence and analytics tools.

Virtual firewalls can be deployed down at the virtual switching layer even closer to the VM workloads to gain more visibility to east-west VM traffic and data, and also can be more flexibly deployed as the data center grows. As the data center extends to the hybrid cloud, virtual appliances are also the only option to bring network security to public cloud providers where physical appliances are not allowed.

Hardware appliances, while still needing to be deployed in advance, can gain some flexibility through Virtual Domains (VDOM) and VLAN’s. With scale-up hardware achieving highly cost-effective throughput of above 100Gbps to 1Tbps and beyond, service providers and others can more flexibly manage ever growing capacity with up to thousands of logical VDOM instances per physical device.

Platform Orchestration and Automation

The security platform needs to be able to support dynamic changes in the compute, networking or other infrastructure layers, such as for the onboarding of a tenant or adding a new server instance to an existing workload. The benefits of using on-demand cloud services, for example, would be negated if it takes days or weeks to manually provision security via human administrators, or even worse, putting data and services into production without secure and compliant controls.

A better model is that these administrative changes can be automated by orchestrating security management with hypervisors, SDN controllers and other infrastructure platforms. For example, for a highly elastic cloud application, when a new VM instance is spun up on a virtualization host, the hypervisor can notify the SDN controller to set up the appropriate switch ports and VLAN’s, and also dynamically route the flows through a virtual or physical firewall that has been notified to apply the proper security policies for that workload.

Single Pane-of-Glass Management

As data center workloads become more dynamic, there can be protection or compliance gaps if a different security posture is applied depending on whether the workload is physical or virtual, or running in a private cloud or public cloud, or whether it is protected by a physical or virtual firewall. Security management needs to be able to ensure a single pane-of-glass view of security policies and events across the hybrid cloud, regardless of where a workload is running and how it is being protected.

Security management itself can be delivered more as a service as well, such as by running policy and logging engines in virtual machines or even hosted as a SaaS application in the cloud.
Platform Extensibility & Ecosystem Integration

Security appliances and management products can no longer be isolated from the rest of the infrastructure, but must be cognizant of realtime changes in the data center. Security solutions therefore must be built on an extensible platform that can integrate and communicate with other infrastructure through programmable API’s and other interface points. These could either be through open standards or proprietary interfaces – both have their pros and cons historically for interoperability, time-to-market, and other considerations.

Security vendors and their ecosystem partners must ideally deliver out-of-box security solutions for leading infrastructure platforms that can be easily configured and deployed by most enterprises without custom programming or other glue. However, vendors should also look to make their platforms flexible for service providers, more advanced enterprises and other technology partners to be able to integrate other SDN controllers, orchestration platforms, cloud management, and visibility and analytics tools of their choice.

However, as web server VM’s and other infrastructure are being spun up and down to scale quickly, IT also needs to ensure that firewalls and other protections are applied with appropriate policies to ensure privacy and confidentiality of sensitive user or corporate data, lest risk alienating the very constituencies that organizations are trying to reach more closely. But in order to secure infrastructure transparently without slowing down or disrupting the business, IT organizations are looking to automate the deployment and provisioning of security engines and policies seamlessly with the provisioning of virtual machines, virtual ports, and other software-defined infrastructure.

Use Cases for SDN Security

SDN Security defines a generalized security architecture framework that can be applied to a variety of business and IT use cases, but a few key ones are emerging commonly for enterprises and service providers deploying virtualization, cloud and SDN technologies.

Auto-Scaling/Auto-Provisioning Protection for Elastic Workloads

Many organizations are looking to accelerate their business by connecting more closely with customers or consumers through social media or web-based initiatives. These mobile, social and multimedia applications need to be able to be deployed rapidly and scale virally in response to end-user demand, hence internal IT teams and cloud service providers alike are being driven to deliver highly elastic IaaS services to line-of-business development teams.

Securing East-West Traffic in Virtual Environments

Studies have shown that in modern data centers up to 75-80% of data center traffic is east-west rather than north-south, as VMware ESX and other hypervisors began to leverage virtual networking not just for allocating network bandwidth, but also for load-balancing, high-availability, and other value added benefits. In addition, much of that east-west traffic is virtual inter-VM traffic that may stay on in the vswitch rather than leaving the physical host, making it increasingly difficult to inspect traffic with hardware security appliances that sit higher up in the physical network.

Organizations are increasingly looking to virtualized firewalls and security appliances that can sit on the vswitch and be inline to inspect virtual traffic, and that can follow VM’s across the virtual data center, such as maintaining stateful inspection during live VM migration or having distributed firewall rules that work across host clusters and irrespective of changes to logical IP’s, ports or MAC addresses.

Network virtualization and SDN are further abstracting the network and exacerbating visibility and control challenges, such as tunneling VXLAN or other overlay/underlay traffic, making LAN traffic invisible to physical Layer 3 security gateways, or spanning traffic across clouds and out of the control of on-premise security devices.
Enabling Micro-Segmentation in Consolidated Data Centers

Data center consolidation is increasing IT efficiency through the use of technologies like server virtualization and network virtualization, but aggregating more sensitive data and users in shared and increasingly multi-tenant environments. This is concentrating risk and potential exposure, particularly as IT is looking adopt flatter and more open networks that enable more scalable infrastructure.

Organizations are looking to micro-segmentation approaches that can provide fine-grained firewalling across flat networks but without disrupting application and users. SDN platforms are increasingly adding policy-based consoles that can define higher-level policies based on users, roles and other meta-data, which can then be orchestrated with security management to transparently deploy a “honeycomb” of fine-grained trust zones in coordination with the software-defined network flows.

Network Function Virtualization (NFV)

Network Function Virtualization (NFV) takes the notion of virtual firewalls load-balancing, and other L4-L7 network and security appliances – aka virtualized network functions (VNF) - several steps further to support provider requirements for commoditization and service manageability. Firewalls and other security VNF’s must be able to support service insertion and service chaining interoperable on more commoditized NFV hardware, leading to lower costs, higher scalability, and better manageability. These benefits lower provider capex and opex costs, enable efficiency and savings that can also be passed down to provider tenants and clients.

On-Demand Self Service

Service providers are being increasingly driven by enterprise tenants to not only provide elastic infrastructure, but also offer services on an on-demand, pay-as-you-go basis. Hence providers are looking to offer security and network services through self-service catalogs and marketplaces and charge by hourly, monthly or other metering schemes. In addition, to deliver a seamless tenant experience, security provisioning should be seamlessly orchestrated into tenant virtual networks with transparent deployment, metering and billing.

SaaS Multi-Tenancy

As cloud services and managed services are increasingly being delivered from efficient and elastic multi-tenant infrastructure, rather than from dedicated or customer premise equipment (CPE), management tools and platforms need to become multi-tenant aware. Security policy and event management can be delegated to each tenant to reduce cloud admin costs, ideally through online web interfaces to fulfill a more SaaS-like experience. Provider admins must also be able to have a global provider view, in addition to being able to troubleshoot delegated administrative views for a single tenant.
Secure the Private Cloud with Fortinet

Fortinet has been delivering solutions for both physical and virtual networks for several years, and is investing aggressively in a comprehensive strategy for SDN Security. Fortinet leverages a scale-up and scale-out data center approach combining the benefits of both high-performance hardware and virtual appliances with common FortiOS consolidated security platform and FortiGuard threat research and content services.

- **FortiGate** hardware appliances – Scale-up hardware with proprietary ASIC architecture to keep up with increasing core network speeds up to the largest provider and hyperscale networks. Virtual domain technology allows firewall capacities of up to 1.2Tbps to be flexibly managed and delegated as virtual services to up to 3000 tenant VDOM’s per device.
- **FortiGate-VM** virtual appliances – Scale-out virtual appliances that provide firewall, IPS and consolidated network security that support all leading hypervisors as well as major public cloud platforms.

Extend the Fortinet Security Fabric to the Cloud

The Fortinet Security Fabric is the communications interface that delivers seamless security across the entire attack surface. It enables organizations to securely and elastically scale protection to their private cloud infrastructure and workloads, and to segment both within the cloud and between endpoints, enterprise networks, and the cloud as follows:

- **Scalable**—provides highly elastic FortiGate and FortiWeb protection that is orchestrated to automatically scale with private cloud workloads and applications.
- **Aware**—integrated with underlying private cloud infrastructure to be agile and provide protection that is seamless with changes to the underlying environment.
- **Secure**—applies FortiGuard threat intelligence globally to segment the data center across private and hybrid cloud, and between the cloud and the endpoint and network in an organization.
- **Actionable**—integrated into SIEM and other analytics in the data center and cloud, with ability to orchestrate changes to FortiGate and other Fortinet security policy/posture automatically in response to incidents and events.

- **Open**—built on a highly extensible platform with programmatic APIs (REST and JSON) and other interfaces to integrate with hypervisors, SDN controllers, cloud management, orchestration tools and software-defined data center.

For example, the physical or virtual firewalls interface and network with the communication and collaboration elements contained in the Fortinet Security Fabric to determine what network intelligence is shared across the enterprise.

Fortinet SDN Security Portfolio

Fortinet’s SDN Security solution unifies the FortiGate platform together with a broad portfolio of products, technologies and services into a cohesive solution for securing SDN and SDDC environments, including:

- **FortiGate** SDN integration – Out-of-the-box solutions with leading SDN platforms, such as FortiGate-VMX for VMware and integration with Cisco’s Application-Centric Infrastructure (ACI)
- **FortiManager** and **FortiAnalyzer** management solutions – Centralized policy for physical, virtual and cloud environments, that can be deployed on-premise or in the cloud.
- **FortiCloud** and **FortiPrivateCloud** – SaaS-based central management solutions for enterprises and service providers
- **Fortinet Developer Network (FNDN)** – Extensible FortiManager API’s provide programmable interfaces for custom orchestration and automation with SDN controllers and other infrastructure, with staffed development support via an online resource portal
- **Fortinet’s Programmable Network Partnership Ecosystem** – Dozens of technology partners working with Fortinet’s SDN Security platform to integrate SDN controllers, orchestration platforms, programmable switches, and centralized policy and analytics solutions
- **Other Fortinet Security Solutions** – Additional networking and security solutions available as both physical and virtual appliances, including FortiWeb-VM web security, FortiMail mail security, FortiSandbox-VM advanced threat detection, and FortiADC-VM application delivery controllers