The Virtualization Practice

White Paper:

Segmentation Firewalls within Virtual & Cloud Environments

Edward L. Haletky

Analyst – Virtualization & Cloud Security
The Virtualization Practice

Version 1.0 January 2016

Sponsored by:

FORTINET

Abstract

When discussing virtualization security, I am often asked "where do you place the firewalls?" My answer has always been the same: "between your trust zones." This is the strength of the internal segmentation firewall (ISFW). It fits within virtual and cloud environments between your trust zones, acting as a gateway if necessary, but primarily as an edge firewall within your environment. ISFWs, unlike distributed firewalls, act as boundaries. You need both an ISFW and a distributed firewall construct to provide defense in depth within any virtual, cloud, or physical environment.

Table of Contents

Introduction

I am often asked “where do you place firewalls within virtual and cloud environments?” My answer is always “between your trust zones.” The followup question is often “can I just use a distributed firewall?” The answer is not always a yes or a no, but in general, an edge firewall between trust zones allows you to do more things than standard distributed firewalls do. A properly designed secure environment relies on both internal segmentation firewalls and distributed firewalls to achieve defense in depth. The key to using an ISFW is not to layer on your network more bandwidth requirements than necessary, but to inline a firewall where necessary to protect a group of systems. The systems in that group all trust each other, hence the term “trust zone.” Within trust zones one policy may apply, while between trust zones another policy may apply. The ISFW’s role is to apply the necessary policy between trust zones.

I. Virtual & Cloud Environments

There are many trust zones within any virtual and cloud environment, many of them related not to the running of workloads but to the management of the environment. The same holds true for physical environments. Taken all together, there are many different trust zones and therefore a need for differing levels of security. Here are just a few trust zones outside the realm of standard workloads:

- Management
- Storage
- Live migration or vMotion
- Fault tolerance

And here are a few that exist within many data centers:

- Middleware
- Databases
- Multiple applications
- Enterprise management, such as identity management
- Security tools
- Networking tools
- Compliance, such as PCI, HIPAA, GLBA, etc.

When we look at an existing data center with virtual environments and extend that into the cloud, we are often looking at a huge swath of technology, the components of which may or may not need to talk to each other. When we also pull in compliance, we start to see an increase in the need to

segment our data from other parts of our environment. This is achieved not by having a centralized firewall with a million and one rules, but by using internal segmentation firewalls with the specific rules necessary for the workloads in use.

ISFWs Are Inline

ISFWs are inline between trust zones. Let us take the following example (Figure 1) of a simple set of trust zones within a data center. We have smart devices, some number of physical machines, and many machines within the virtual environment. The virtual environment has virtualization management workloads, normal workloads (in which the physical machines participate), and DMZ workloads. Within the normal workloads are subzones that enterprise management and security management use to provide identity management (such as through Active Directory) and log analysis (for security breaches). Both of these subzones exist but should not be accessible by everyone and everything within the normal workloads.

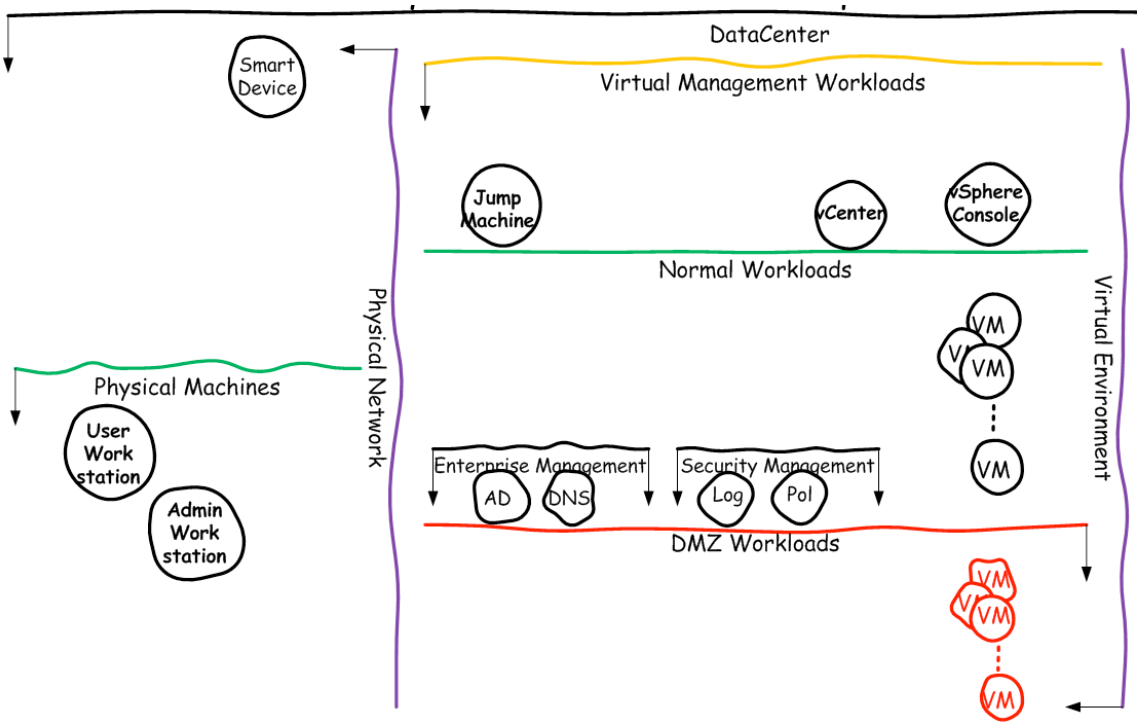

Figure 1: Several Possible Data Center Trust Zones

How should we secure these trust zones? First, how should we secure just the physical side? Once we know that, can we then extend the concept into the virtual and cloud environments? We can do this by using physical firewalls as well as per-system defense in depth. If we look at Figure 2, it is apparent that we can add quite a bit of firewall to handle our requirements. There are edge firewalls between the outside and the inside, and between the cloud and the inside. However, within the inside, we switch tactics and make our policies less draconian and more pinpointed to our needs. That is the strength of an ISFW. We can set up one ISFW for wireless while using another to enter the management network of the virtualization environment from the physical side.

4 Segmentation Firewalls within Virtual and Cloud Environments

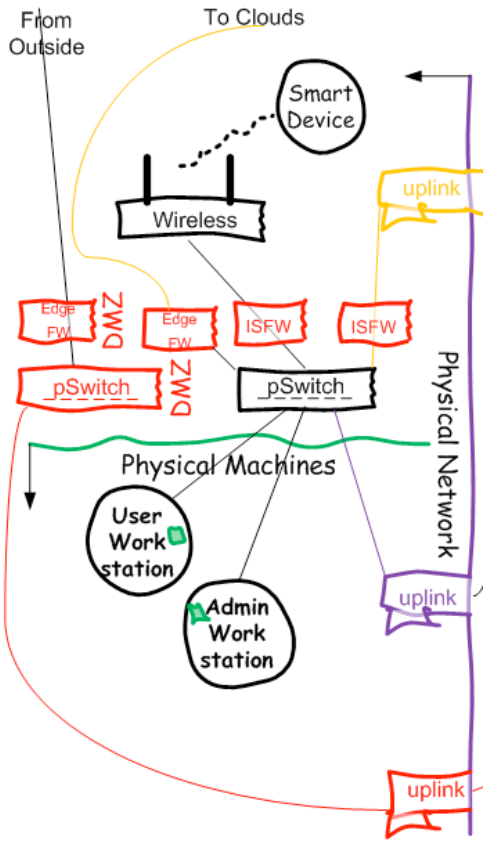

Figure 2: Physical Security with ISFW

In Figure 2, we split the internal segmentation firewall logically into two distinct firewalls, one for wireless and one leading into the uplink used purely for virtualization management. This is the physical side of the management layer, used to represent each hypervisor. Access to this network is like entering the doors to your data center. You secure those with cameras, identity checks, etc. The ISFW, in this case, acts as the virtual camera. It should be able to handle identity tracking, which is common within most next-generation firewalls, such as those from Fortinet.

Once we enter the virtual environment, we need to consider our defense in depth even more. In Figure 3, we fill in the details of our networks. Specifically, we indicate where the various virtualization internal segmentation firewalls (vISFW) need to be placed. The simple reason is to provide edge gateway facility between virtualized trust zones, where changes in classification or levels of trust change. This is also done for basic security functions: for instance, between a DMZ and everything else, and between management constructs for the virtual environment, enterprise, or security and regular users. At any of these junctures, you may wish to place an ISFW to provide firewall edge functionality between the area to be protected and the lower level of trust.

Just think how we would add in a new trust zone, such as in a testing environment for load and security testing. To do that, we could use a 100% segregated environment that is only periodically used, or we could use vISFW instances to protect the environment and allow proper access. Since most testing environments use the same IP addresses in a protected enclave as used by production, we really would like NAT functionality. That only comes from edge devices and *not* distributed firewalls. Figure 3 shows how to add such a set of workloads. Edge-style firewalls are perfect between multiple trust zones where we want control over who enters them.

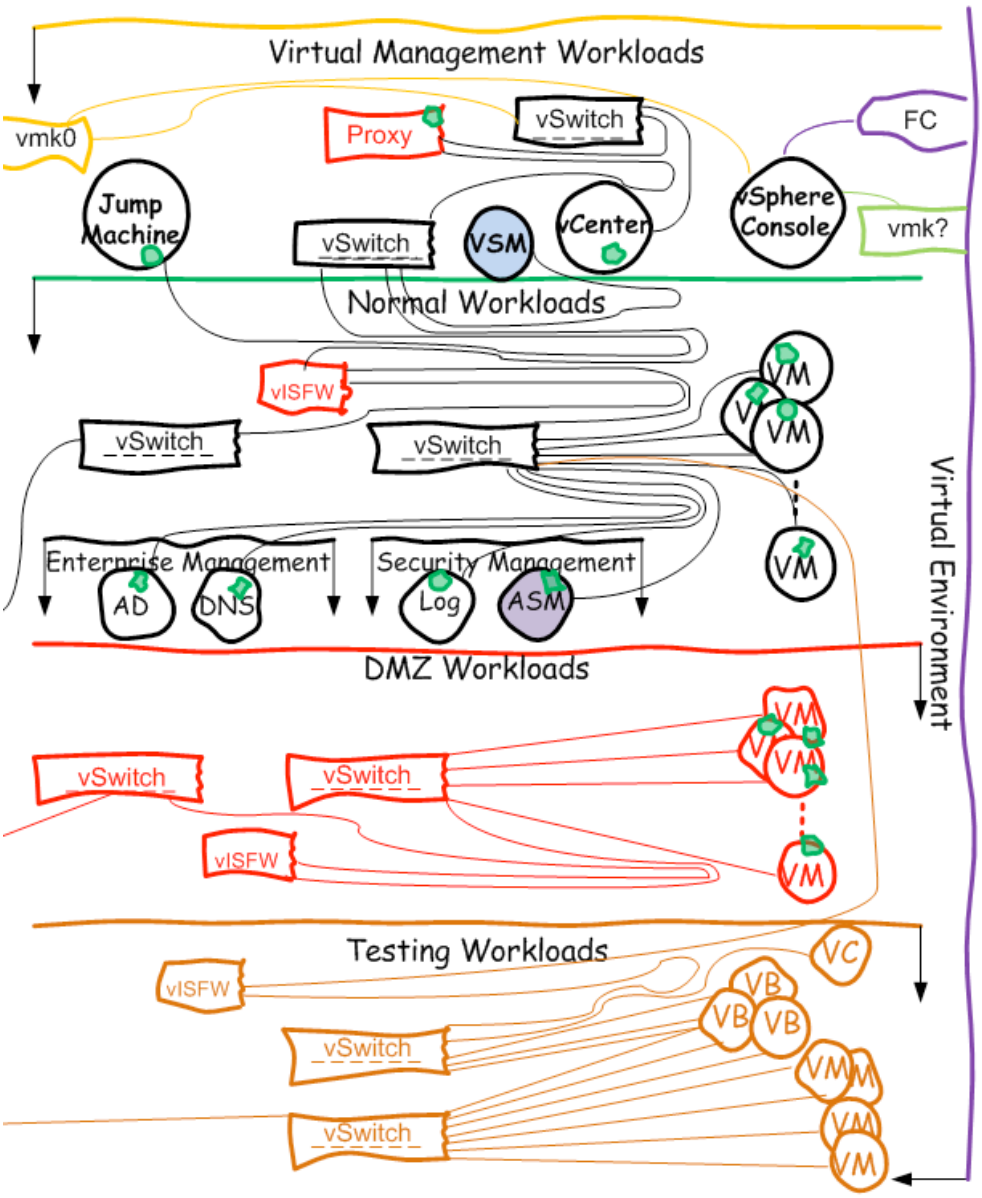

Figure 3: Virtual Internal Segmentation Firewalls

ISFW Simplifies

That is correct: an ISFW simplifies your firewall rules quite a bit. ISFWs not only sit inline between specific trust zones, but they allow you to have policy for only the trust zones involved. There is no need to have too many rules in play. You can simplify the rules to just the ones needed. Take Figure 3; the vISFW within normal workloads allows access to the virtual management workloads by passing only Active Directory, DNS, and security management (ASM) data and RDP. Nothing else need pass that firewall in order to access the jump machine within the virtual management workload. Active Directory and DNS could be set to just pass from within the virtual management

workloads to the enterprise management layer and not the other way around. It depends on how simple or complex you wish your rules to be.

The internal segmentation firewall allows pinpoint control over a specific set of elevation of privileges between one zone and another zone. Simplification of firewall rules implies better understanding of how to control interactions between trust zones, but it also moves us away from a single firewall through which everything has to route. ISFW simplifies network routing as well as lowers the per-firewall rules necessary for it to do its job. Within each trust zone, it is possible to then place a form of a distributed firewall to refine the security controls between entities within that trust zone. However, between trust zones, edge firewalls such as internal segmentation firewalls are required.

II. Conclusion

Fortinet's internal segmentation firewall not only simplifies firewall rules between trust zones, but also simplifies routing within your environment. The use of virtualized internal segmentation firewalls simplifies routing so that you no longer need to route out of the virtual environment to a firewall. Routing is simply inline; no longer are hairpins necessary while simplifying required firewall rules. Fortinet's internal segmentation firewall does not displace the use of a distributed firewall, which controls access between virtual machines within the trust zone. You gain deeper defense in depth by extending the firewall concept into virtualized and cloud-based networks. What you do within a virtual environment works within many clouds as well, as well as segmenting between multiple public or private clouds in a true hybrid cloud deployment.

Using Fortinet's series of edge and internal segmentation firewalls, you gain the ability to use a unified management platform to control each, and you allow for one set of automation tools and scripts to be used.

ISFW will simplify your firewall control and routing requirements between trust zones. Extend your firewalls into your virtual environment and cloud environments.

III. About The Virtualization Practice

The Virtualization Practice, LLC, is a boutique analyst firm concentrating on virtualization and cloud technologies, companies, and organizations. If your product, organization, or company works in, fixes problems within, or enables virtual and cloud environments, we are interested in hearing from you. Our goal is to educate the market about what is out there for virtual and cloud environments.

Edward L. Haletky, aka Texiwill, is the author of VMware vSphere(TM) and Virtual Infrastructure Security: Securing the Virtual Environment as well as VMware ESX and ESXi in the Enterprise: Planning Deployment of Virtualization Servers, 2nd Edition. Edward owns AstroArch Consulting, Inc., which provides virtualization, security, and network consulting and development, and The

Virtualization Practice, where he is also an analyst. Edward is the moderator and host of the Virtualization Security Podcast as well as a guru and moderator for the VMware Communities Forums, providing answers to security and configuration questions. Edward is working on new books on virtualization.

IV. About Fortinet

Fortinet is a global leader and innovator in network security. Our mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a provider of network security appliances and security subscription services for carriers, data centers, enterprises, distributed offices, and MSSPs. Because of constant innovation of our custom ASICs, hardware systems, network software, management capabilities, and security research, we have a large, rapidly growing, and highly satisfied customer base, including the majority of the Fortune Global 100, and we continue to set the pace in the network security market. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond network security to help secure the extended enterprise.