Virtual Firewall Appliances - Trust Misplaced?

By Chris Brenton

When we deploy a firewall to protect a corporate network, we typically install it as an appliance on the perimeter. As organizations move their assets into public IaaS space, many are attempting to mimic this same security posture. Products like Check Point’s Virtual Appliance for Amazon are designed to fit this need. But can a virtual firewall appliance really provide the same level of risk mitigation as a physical firewall appliance? In other words, can we extend the same level of trust to a virtual firewall appliance that we do to their physical counterparts? To answer that question, we’ll need to dig into the architecture.

The Classic Firewall Install

Figure 1 shows the traditional method of deploying a firewall. This could be a single organization with multiple DMZs, or multiple corporations hosted at a co-location facility.

Note that each server is connected to a unique switch, which is then routed into the firewall. The servers are logically segregated from from each other, as the only routed path between networks is through the firewall. Further, we would describe these servers as physically segregated from each other, as the only point of connectivity between the servers is through the firewall. In other words, pull the firewall out of the mix, and there is no possible way for the servers to talk to each other or the Internet. This is one of the security benefits of physical segregation.
A Virtual Firewall Appliance

Figure 2 shows an identical configuration, only applied to an IaaS cloud with a virtual firewall appliance.

While this configuration is logically identical, it obviously has different physical characteristics. To start, there is a software connection between the servers via the hypervisor. The possibilities of a malicious user breaking out of a virtual machine has been well documented. It is a risk that most administrators understand they are accepting. Note however that there is a second software connection between the systems, namely the virtual switch.

While it may appear that multiple virtual switches have been deployed, in reality most solutions deploy a single software switch, which is then broken up into multiple logical partitions. This is done to minimize the resource impact to the host server. Brad Hedlund of Dell has done some excellent work in validating this functionality. So beyond the potential software bridge in the hypervisor, we have a second potential bridge within the virtual switch.

Also in Figure 2, note the position of the firewall. It logically sits outside of the virtual switch, which means it is unable to negate any risks that may exist within the virtual switch itself. This means that if a savvy attacker figures out how to jump between logical partitions, the firewall is unable to provide any risk mitigation.

So while Figures 1 and 2 are logically identical, physically Figure 2 includes two additional risks:

- Hypervisor as a potential software bridge
- Virtual switch as a potential software bridge
Mitigating The Risks of a Virtual Switch

Fortunately, we have some options available to us if we need a higher level of risk mitigation than what is provided by a virtual firewall appliance. The first is to leverage a hypervisor based firewall. VMware’s vShield is probably one of the best known products in this vertical. A hypervisor based firewall moves the firewall to the other side of the virtual switch, thus mitigating any risks within the switch itself. A logical example is shown in Figure 3.

The problem with hypervisor based firewalls is that they are vendor specific. For example vShield only runs on VMware’s own hypervisor, and is not supported by KVM, Zen or any other hypervisor solution. Further, your public provider may not support hypervisor based firewalls, so this may not even be an option. Even if they do, hypervisor based firewalls require the use of introspection which brings with it its own additional risks in a public cloud environment. So ultimately you may simply be trading one set of risks for another.

Your other option is to simply leverage the firewall software built into most modern day operating systems. Host based firewalls control traffic as they pass in and out of the virtual machine, so they are more than capable of negating any potential risks within the virtual switch. This option is also the least expensive, as the firewall is already present within the operating system. Finally, this option is also the most portable. If you move the VM to another cloud, the
protection afforded by the host based firewall obviously moves with it. This is not true for any of the other firewall solutions discussed earlier in this post.

Wow, how often do we see the cheapest solution being the most flexible and providing the highest level of risk mitigation? ;-)