Mike Nelson – SV article

Alternative Virtual Firewall and IPS Solutions for vSphere

Someone asked me not too long ago what I thought was going on with VMware's vShield product offering. With VMware announcing their new partnership with Catbird, then going out and buying Bluelane and PacketMotion, I'm not sure anyone knows which turn the suite of vShield products will take next. What I am sure of is that there are plenty of alternatives out there, and some that I feel are better than any vShield product, that can provide you with a wide range of capabilities in a virtual Firewall or IPS appliance.

To be fair, I only have limited experience with all of the vShield products, and have only used the vShield Zones (included in an Enterprise Plus license) and vShield Edge products in actual hands-on work. The Zones product was easy enough to install and configure, but as I later discovered, it is also not very efficient. When Zones is installed in a Cluster, all of the hosts must have Zones installed, and every single VM's traffic passes through those Zone virtual appliances that were installed when you set it up. Even if you do not want a VM's traffic to be passed through the Zone's very basic a rudimentary firewall, it does and it really slows things down (that's why it is called "Slow-path"). The Edge product did not fare any better in my experiences. It has limitations when it comes to using it on a cluster that has only a Standard vSwitch in use instead of a vDS (Virtual Distributed Switch), and it always seemed to be doing a lot of work (it was generating huge amounts of network traffic and the VM's CPU was through the roof) when practically nothing was going on in the Cluster. With the VMSafe's "Fast-path" API's now being used by partners, I am hopeful that these will make a turnaround for the better.

Let's talk about some good alternatives that you should consider. Of course, many of the big network vendors have virtual appliances of their commercial products that are well supported that could be used, but in smaller environments and labs, where initial upfront and ongoing maintenance costs are a large factor in every buying decision, there are some really great Open Source products to have a look at.

When hunting for Virtual Appliances (VA's), many of them can be found at VMware's Virtual Appliance Marketplace. Although, now I use Google more than ever since over the years it has become way to difficult to search and determine what is truly Open Source and what is not on that site. It has definitely leaned towards catering to the partners instead of the community, which is sad (remember when VMware embraced the Community instead of pushing it to the back of the line?).

In the field of firewalls, I am a fan of the old standards. Firewalls like IPCOP, SmoothWall (now called Express), Monowall, and even Vyatta are my favs. These packages work tightly right alongside the Linux (and some Windows OS) kernels and provide solid protection amongst other capabilities that have been integrated. They may not have an ultra-rich GUI for administration, or even all of the feature sets of the commercial products, but all of them provide the basics of packet inspection, NAT, and rules, and sometimes that is all you need. Many of them go way beyond though, essentially trumping the expensive commercial offerings, by adding support for SNMP, reverse proxy, traffic shaping, wireless, VPN, and much more. I personally like using the Vyatta Community appliances, as they have a very similar CLI feel as their Cisco counterparts, and they deliver a rock solid open source product.

When you talk about implementing a virtual Intrusion Protection Systems (IPS), many of the firewalls that I mentioned, and others available, have these capabilities built-in. The Cisco ASA product has literally hundreds of features, but they all come at a cost. If you are planning to implement an IPS, you should also implement an Intrusion Detection System (IDS). If you don't understand the difference between the two systems, and don't worry, not many folks do, please check out this PDF from the SANS Institute website. Ideally, these are contained within a single appliance with the IPS connected to your outside parameter network, and the IDS connected to a vSwitch inside the firewall. Today's implementations of virtual networking make all of these types of connections very possible with some time spent on configuration. Vendors like Catbird (mentioned earlier), Stonesoft, and Sourcefire provide such appliances, but at a commercial price. The mature and all too familiar Snort package (with the Snorby front-end and other requirements) heads the list of my favorites, along with Bro and Suricata. I recently implemented Bro and was really impressed at its feature set and ease of configurations and installation. It made me think of how far along these products have really come since the early days of using Snort for more than just a proxy. Since then, Bro has taken over my top spot in this category. Other to check out would be Smooth-Sec and Siem-Live (both based on Suricata), along with some great Live CD's that I use very frequently like the NIST (a definitive defacto standard for anyone in networks and security) and the Security Onion.

If you don't need or want the overhead costs of implementing and maintaining a commercially available virtual firewall or IPS/IDS appliance for your shop, give these a try and find out what fits your needs. After all, they are virtuals, so they can be created and deleted just like that.