November 2, 2016

Open Source Firewalls

CYBERSECURITY, DIGITAL & TECHNOLOGY, RISK ADVISORY/INTERNAL AUDIT
BY SCHNEIDER DOWNS PROFESSIONAL

***Geek warning:** some tech knowledge required for this article – or at least willingness to look stuff up. This article was repurposed from Matt Dunn's personal blog, MaDwall Security, for Schneider Downs Our Thoughts On… Matt Dunn is an In-Charge Associate in Schneider Downs' Risk Advisory Practice.*

Constantly hearing about another batch of consumer routers getting compromised in bulk? Consider making an unused PC/server with a couple of network cards into a powerful firewall to better protect your network. These work well for home use, or even in many businesses. The open source firewalls listed here are very configurable, with VLAN support, etc.

Requirements

A computer with at least two network ports is required. This could be an old, but stable, PC that you have laying around that you can throw a PCI or PCI-E network adapter in to get two or more ethernet ports. Or it could be a server, or a platform designed for building your own firewall, such as the *PC Engines APU*.

Processing power and RAM can be pretty minimal for home, small business and some medium-sized businesses. A single core processor and 1GB of RAM may be plenty of power for a home network, but probably not enough for an environment with hundreds or thousands of users. The amount of processing power and RAM needed depends on what firewall features you are using, such as adding on an IPS/IDS like SNORT®, and the amount of traffic passing through your firewall. For business use it would be ideal to use something with redundant power supplies, RAID and readily available replacement parts. Many of these firewalls can also run as Virtual Machines (VMs).

Things to Keep in Mind with Virtual Machine Firewalls

For edge firewalls, a physical device is highly recommended. Say you have a remote office with one VMware server. Sure, it has plenty of extra network ports, CPU, RAM,etc., but don't forget about situations like the following: Consider an example where the virtualized firewall provides an OpenVPN or IPsec tunnel back to HQ and is the only link home. VMware needs an update that requires a reboot, but there are no IT staff at the remote location. You connect to Vsphere and you gracefully shut down all of your VMs before rebooting the VMware box. But, oops! You shut down your firewall, which means your remote location no longer has Internet or VPN connectivity. Darn. Now someone physically needs to get things booted back up at the remote location. If you had a dedicated firewall, your VPN link would still be up and you could reboot your VMware server without issue. Virtualization is great, but there are situations where it will cause you more problems than any money you might have saved by not investing in a physical device.

Firewalls

Below are a few open source firewall options. Test a couple different ones out to see what fits your needs. There are other options out there, but below are some of the most popular. Wikipedia has a decent list of firewalls that are free and paid https://en.wikipedia.org/wiki/Comparison_of_firewalls

pfSense firewall – pfSense® is an open source firewall platform that is FreeBSD based. It is a great open source firewall platform with enough add-ins and advanced configuration options to suit most. This is the open source firewall that MaDwall Security is most familiar with and would recommend to anyone.

Excellent overview of the different PFsense features and settings on version 2.2.2 https://www.youtube.com/watch?v=dfix8WsNSHc

OPNsense® – Recommended by M0n0wall , since M0n0wall has shut down. OPNsense is another FreeBSD-based open source firewall.

Smoothwall® – Smoothwall is a Linux-based open source firewall option.

As always, contact Schneider Downs if you have more specific or detailed questions about open source firewalls and visit Schneider Downs Technology Services webpage to learn about the services we offer.

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.

© 2024 Schneider Downs. All rights-reserved. All content on this site is property of Schneider Downs unless otherwise noted and should not be used without written permission.