



From: www.csoonline.com

Network Security: Three open-source options

Evolutionary IT's Joseph Guarino explains how to achieve network security the open way (Third in a series on open-source security solutions)

Joseph Guarino, CSO

June 18, 2010

Free and open-source software (FOSS) is everywhere. Its offerings span far and wide in the technology industry. The networking space is an excellent example of FOSS, with feature-packed firewalls, routers, VPNs and even UTMs, for nearly every need. In this article I will introduce you to a few of the commercially-supported open-source network security options currently available in the marketplace today. With open-source networking you can enjoy the benefits of lower costs, greater security, flexibility, extensibility and full enterprise support. Here are three examples.

Endian

Endian is a feature-rich, unified threat management (UTM) system that offers a stateful firewall, VPN (IPSec/OpenSSL), gateway anti-malware, anti-spam, QOS/Bandwidth Management, IPS and proxy functionality. It is available as a software solution to build on your own hardware or a variety of optimized appliances that scale to meet your network security needs. Like all other competitive offerings in this space, the community edition offers core functionality with the commercial version offering even more features; plus commercial support.

The Endian web-based administrative interface is slick and easy to use. Its dashboard feature offers a real time comprehensive view of your Endian system and the network it is protecting. Endian also offers a centralized management feature, "Endian Network," a centralized web-based management/monitoring solution for multiple Endian products. The Endian Hotspot add-on module supports the creation of a secure wireless hotspot by allowing for captive portal, secure wireless via SSL VPN, a dedicated ticketing system, and RADIUS. Endian offers a great balance between a rich feature set and functionality.

Also see "5 Open-source Desktop Security Applications"

Untangle

Untangle is a feature packed UTM network security solution with a comprehensive set of security features: firewall, VPN (OpenVPN/SLL), routing, QOS, anti-malware defense, anti-phishing, anti-spam services, intrusion prevention, and Web content filtering. Its simple web GUI uses the metaphor of a rack allowing for quick and easy management of all aspects of the system. Enhanced reporting with interactive drilldown allows you to get a bird's eye view of what's going on in your network as well as export data to PDF/HTML.

General management features like automatic software updates for its core and associated signatures are welcome additions to any network/security administrator. The product comes in an open source edition (with all the features above). There are several commercial bundled versions that cater to SMB and educational environments. Commercial add-ons such as Commtouch, for enhanced spam blocking, an enhanced policy manager, commercial Web filtering solution from eSoft, WAN load balancing and failover, an active directory connector, and Kaspersky anti-virus vastly expand the offering.

Vyatta

Vyatta is an open source router, firewall VPN solution. It features support for a wide array of advanced routing protocols (BGP, OSPF, RIP, etc.), intrusion prevention, URL filtering, and WAN load balancing, to name a few. Vyatta has a focus on routing and security features and aims itself competitively squarely against the Cisco Systems of the closed-networking world. Vyatta offers its solution in many forms: hardware appliance, deployment on your own standard X86 hardware, virtualized (Xen/Vmware), or even cloud deployment. For management, it offers an intuitive web interface or a tried and true CLI (Command Line Interface.)

Also see "Seven Firefox plug-ins that improve privacy"

The CLI is Cisco IOS/Juniper JUNOS like so most "old schoolers" will feel right at home. Vyatta is a compelling offering for those looking for a quality routing and security solution with all the benefits of open source.

Conclusion

As you can see from these three examples, open source has a great deal to offer in the network security realm. The next time you're making a purchasing decision make sure you consider these quality open security solutions and you will see how cost, increased uptime, security and overall stability are improved.

Joseph Guarino is owner and senior consultant of [Evolutionary IT](#), a Boston-based IT and business consulting firm. You may contact him through his website or follow/connect with him on Twitter ([evolutionaryit](#)) or LinkedIn.

© CXO Media Inc.