Is Cisco’s ASA a Headache-in-Waiting?

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Reader Noman Bari, B.S.Electronics, CCNA, CCDA, CCNP, CCDP, CCSA,CIW Security Analyst, CompTIA Linux+ Certified and MCSE wrote to me some time ago from Karachi, Pakistan with a thoughtful comment on Cisco’s new multifunctional ASA security appliance. With his kind permission and collaboration, here are his thoughts.

* * *

I [NB] am writing this e-mail to learn your views on a new security box from Cisco. In summary, Adaptive Security Appliance (ASA) is a multi-function security appliance which integrates firewall, IPSec and SSL VPN, intrusion prevention, virus filtering and network quarantine in a single device.

I have been thinking about this development from Cisco. Surely putting all the eggs in one basket is never a good idea.

If all the functionality of security is taken care of by one single box and if that box gets compromised then it will be a serious problem. It is widely known that there is no such thing as 100% security. At some time in the near or distant future we will hear that there are security holes found in the working of ASA and they can lead to a security breach.

There will be critics who will say that since ASA comes with all the bells and whistles therefore it will be extremely hard if not impossible to compromise its security but what if a person with malicious intent is able to do it? And this will happen – it’s just a matter of time.

The job of the marketing guys is to show everyone a rosy picture. I am not blaming them: it’s what they get paid for. But its our job as techies to filter out useful stuff from what they say.

My analysis is that ASA is an excellent device for small- to mid-size companies to save costs, for ease of management and so on, depending upon the nature of their mission-critical work. However, for enterprise-level security, I would rather go with a layered approach with multiple defenses to protect my network.

Although I am here in Karachi I believe that effective security requirements are valid for every organization in any part of the world. What you and Mr Bruce Schneier write in your security newsletters is equally useful for me here in Pakistan. My vision gets broadened.

* * *

Need I [MK] say more? My only comment is “Wow! I got mentioned in the same sentence as Bruce Schneier! Cool!” Well, OK, that’s not very useful for readers, so here’s a link to the Cisco page describing their ASA 5500 product:
Now take two of those and a glass of water and I’m sure you’ll be fine in the morning.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 Noman Bari & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.