

Stanford University's Department of Electrical Engineering Bulletproofs Researchers' Remote Workstations



An all-purpose security appliance, based on Astaro Security Linux, keeps intruders from invading the remote workstations of hundreds of researchers at Stanford University's Department of Electrical Engineering in Palo Alto, California.

Researchers in the Department of Electrical Engineering engage in just about every aspect of technology, ranging from holography to radar remote sensing. However, Joe Little, a principle systems architect and a researcher in the department, needs to apply security applications right at the home front. He must strive to balance two conflicting problems -- how to make a key department in a major research university open to the world, and, at the same, how to keep researchers' systems from being constantly probed and attacked.

Little says, "We have security updates available in various platforms. Getting the staff to maintain security on these systems has been difficult."

In turn, he has taken a three-step approach to providing better security enforcement. First, access to public services is being restricted to central systems when possible. Each researcher has a virtual Web server, based on SW-Soft's Virtuoso Universal Server, that essentially runs on the central systems. This arrangement enables a researcher to configure and to manage his or her own system, but Little controls the security on those machines.

Next, each researcher's workstation gets moved to a private network when possible. These researches then use a Virtual Private Network, or VPN, which allows authenticated users to establish secure channels over the public Internet to this closed network. Little says, "The private network and VPN solution keep attackers from actually seeing a lot of the systems that aren't going to be easily maintained."

Since the researchers' systems are out of sight, the third step consisted of providing researchers with transparent access to their systems via the public Internet or a private network from anywhere in the world.

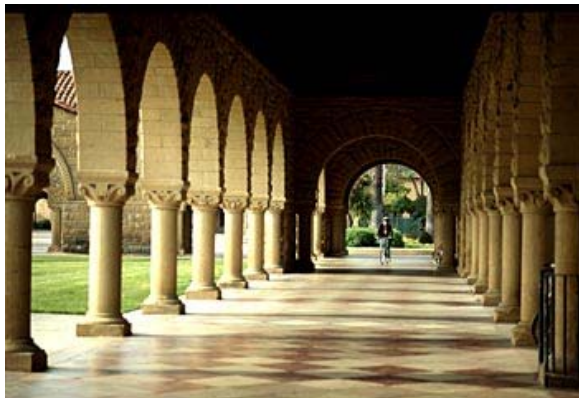
After researching the gamut of security products, Little downloaded the free trial copy of Astaro Security Linux from Astaro Corp., Burlington, Massachusetts. He bought it after four months of testing. Little says, "The- try-before-you-buy capability enabled us to see how well the product would fit into our environment." This software product, which sells for about \$390 per ten users, turns an inexpensive server to an all-purpose security device capable of handling the VPN connection, the authentication, as well as providing a firewall, anti-virus protection and proxy services for Web and email.



Little runs the Astaro Security Linux on a \$1,500 Dell PowerEdge 1400 server. Together these products provide the VPN which acts as a gateway onto the public Internet for as few as 50 remote users or up to as many as 1,000 remote users. The security device supports researchers' remote workstations consisting of everything from Windows 2000 XP to Mac OSX to Linux.

The security device offers VPN interfaces for both the public Internet and for the University's private network. For example, one interface connects to the logical private network overlaid on top of the public Internet for the VPN. The interface on the public Internet acts as a gateway for VPN workstations to access the private networks within Stanford.

The security device also can act as a firewall between systems on the private network and the public Internet. To get access to the public Internet, these systems must pass back and forth through the security device.



The open systems nature of a Linux security product didn't bother Little. He says, "It was a selling point for us. Because we're a university, we get nervous about products built on a proprietary operating system (OS). For example, Windows NT/2000 OS has a notorious security reputation. So, we'd have to think twice about buying a Windows-based security product."

Little says that the security device doesn't require much software maintenance. In fact, Astaro Security Linux runs as an application server on top of a hardened OS. He says, "Since a lot of security products run as an application on top of a general purpose OS, you'll have to manage the underlying OS, be it Windows or Sun Solaris. This means work."

On the other hand, Little adds Astaro Security Linux functions in a self-contained entity capable of automatically updating itself for changes, such as virus updates. "This was another key buying point," he says.

The security device is hard for an intruder to tamper with. A "chroot" or chroot root environment exists for every service the software offers, effectively sand boxing each service – providing untrusted code that limits the ability of the intruder to do risky things. Little says, "If one could possibly exploit one service, one couldn't possibly take over the entire system."

The security device also supports standard authentication mechanisms. Remote access to the security device uses SSH Remote access to the Web services uses SSL. The VPN workstation uses IPSEC with its secure authentication components, or PPTP, the Microsoft authentication components.

Little says by running the Astaro Security Linux on systems with multiple processors, one could deploy a security system throughout the entire campus. In fact, Little says that the university is looking for a firewall solution for all of the departments. "Our solution might be modeled for the rest of the university," he says.

<http://www.stanford.edu>