



May 02, 2005

## Test Run: RSA's SecurID Appliance

**Now, small and midsize businesses can have two-factor authentication minus high costs and management complexities.**

By Christopher Beers  
Secure Enterprise

Two-factor authentication should appeal to any security-savvy business, but the cost and complexity of access management have largely limited its use to enterprise customers. Now, small and midsize businesses can get in on the act with RSA Security's SecurID Appliance. It's easy to manage and available in 10-, 25-, 50-, 100-, 150- and 250-user versions.

The 1U rackmounted device runs a hardened Microsoft Windows 2003 Server. The front of the appliance sports a jog dial, LCD status panel and four network interfaces, two of which have gigabit capability.

Within minutes, I set up the SecurID Appliance in our Syracuse University Real-World Labs<sup>®</sup> using the new Web interface and Internet Explorer (6.0 or higher is required because of ActiveX integration). I connected my laptop to the device using a crossover cable and set the date, administrator password and network parameters. The device then reset automatically. Next, I loaded my license data and SecurID token seed data, and set up a token and associated pin for the administrator account. This enabled two-factor authentication.

### Easy User-Account Creation

I created two user accounts, assigned each tokens and resynchronized the SecurID tokens--it took a mere two clicks of the mouse. When configured from the Web interface, user-account information is stored in a local database, which is perfect for small and midsize businesses. The advanced interface lets you retrieve user information from external sources.

Using documentation from RSA's Web site, I set up the SecurID appliance to allow communication with our Nokia Secure Access System 2.1.0 SSL VPN device--a common setup for small businesses. To complete all the steps, I had to get into the advanced screen, where you can control every aspect of the underlying RSA Authentication Manager 6.0 software.

All advanced tasks are accomplished using a Microsoft ActiveX Terminal Services client--really slick. You get full control of the appliance through the Web browser. Some of the advanced links start the appropriate piece of RSA Authentication Manager automatically inside terminal services, but if that fails, you can get full access by selecting the remote desktop link. To finish the SSL VPN gateway integration, I had to modify the Agent Host entry created to contain a shared

#### Highlights

- Clean, easy-to-use Web interface
- Single-vendor support for the 1U appliance
- Advanced features available if needed

SecurID Appliance, starts at \$4,000 for 10 users.  
RSA Security, (800) 495-1095, (781) 515-5000.  
[www.rsasecurity.com](http://www.rsasecurity.com)

encryption key between our SSL VPN and the SecurID appliance--something that should be offered in the Web interface.

Configuration of the SSL VPN so it can communicate with the SecurID appliance is well-documented at [rsasecured.com](http://rsasecured.com). In fact, you can find integration instructions for more than 300 partner appliances there. After creating an authentication method using the SecurID RADIUS service, I created two users corresponding to the ones created in the SecurID appliance. Upon selecting the SecurID authentication method instead of a local password in the SSL VPN, I could try two-factor authentication. The entire setup, including racking the appliance, initial setup, and the integration of the two devices, took just 35 minutes.

Authenticating with the test accounts from the SSL VPN worked as advertised. The first time a new user authenticates, he or she must enter only the one-time password appearing on the token. The SSL VPN then prompts the user to set up a PIN and reauthenticate with the new PIN plus the next one-time password shown on the token. Further authentication requires two pieces of data--something the user knows (a PIN) and something he or she has (the numbers displayed on the token).

### **Enterprise Customers Can Play, Too**

The SecurID appliance is a great fit for enterprise customers, too, given the advanced features of Authentication Manager 6.0. With the base version of Authentication Manager, the appliance allows for one replica so you can run the appliance in high-availability mode. Using the advanced remote-desktop screens, you can configure advanced options, including integration in your LDAP or Active Directory service. However, the native Authentication Manager screen will be painful on your eyes after coming from a modern Web interface.

RSA SecurID Appliance is easy to use, and I enjoyed its interface face-lift. What's more, customers will have one place to call for hardware and software support--including Windows 2003 Server help--and a 9x5 support contract for the first year.

RSA has struck gold with this. One wonders how the vendor intends to sell its standalone software package, but I guess there are those customers who need more than 250 tokens--and who love to interact with an outdated X-Widget GUI.

*Christopher T. Beers is Lead Unix Architect at Syracuse University. Write to him at [ctbeers@syr.edu](mailto:ctbeers@syr.edu).*