



## FOR IMMEDIATE RELEASE

### Redspin Introduces Firewall Configuration Analysis Tool for Financial Institutions

**Research shows 30% of firewalls violate their organization's security policy**

**SANTA BARBARA, CA, March 20, 2007** -- Pink Floyd may have wanted to “tear down the wall,” but that is an IT manager’s worst nightmare. New research from security auditing firm Redspin Inc. has shown there is good reason for financial institutions to be afraid—nearly one in three firewalls isn’t doing what its builder intended. To help banks and credit unions address these problems, Redspin is introducing a new software tool, the Redspin Firewall Configuration Analysis Tool (CAT), which simplifies and automates the complex problem of auditing firewalls and identifying configuration problems by creating a visual representation of the firewall rules.

Redspin uses CAT as part of its security audits to quickly analyze firewalls for banks and credit unions. In addition, Redspin is making the CAT publicly available at no charge for the next 90 days. Everyone interested in examining their organization’s firewall configuration can use an online version of the Redspin Firewall CAT available at <http://www.redspin.com/tools>.

“Everyone thinks firewalls are solid,” said Redspin President John Abraham. “It’s the basic assumption you build the rest of your network security on. Unfortunately that turns out to be a bad assumption. We logged firewall configuration problems during a year’s worth of security audits and found that 30% of them violate their organization’s own security policy. That’s not good.”

Firewall configurations consist of Access Control Lists (ACLs) which are strings of configuration code that include network addresses, protocols, and vendor specific commands. They may be easy to understand individually, but as a whole can be very difficult to read and analyze because they are order dependent. Also, they are affected by the firewall’s implicit default rules—those rules that affect every other rule but are not shown in the configuration file. This can introduce errors in implementation. Many IT administrators typically have wide-ranging responsibilities rather than a network engineering focus and may inadvertently overlook these subtleties.

The new Redspin Firewall CAT addresses this problem by automating the verification of firewall ACLs. CAT performs two key functions not available in any other firewall audit tool. On the back-end, it detects ACL errors by mimicking the firewall’s thought process and analyzing the rules the same way that the firewall does. Then, on the front-end, it creates an easy-to-comprehend picture of everything that the firewall allows and denies. With this visual representation an

IT administrator can easily see the net result of the ACLs without manually analyzing the entire configuration file.

“It can be tough to review a configuration file. Policy violations aren’t obvious,” said Abraham. “Our experience shows that many times a security hole will be introduced when two rules conflict. Considering that both implicit default rules and the order of ACLs affect how the firewall will interpret the configuration file, it is not surprising that so many firewalls violate security policy. By automating the analysis, Redspin’s new tool will help banks and credit unions find these problems themselves.”

Other issues that the Redspin Firewall CAT pinpoints include redundant rules, blocked/dead rules, simple typos, insecure protocols, unintended remote access, and lack of adequate logging/monitoring. Redspin uses the tool during audits to highlight risk in firewalls. In a year’s worth of firewall analysis, they found at least one of the above errors in every single firewall. Redspin security engineers also find that firewalls are often unnecessarily overcomplicated. Of those analyzed that do violate their own security policy, an average of 60% of the rules in the configuration file were unnecessary.

#### **About Redspin, Inc.**

Redspin is a leading independent audit firm specializing in network security and compliance by providing objective IT [security auditing services](#) to financial institutions, casinos, e-commerce, retailers, ATM providers, Automated Clearing Houses (ACHs), utilities, and defense contractors nationally. Redspin provides penetration tests, FFIEC IT audits and other assessment services for nearly 30% of the banks in California. For more information visit [www.redspin.com](http://www.redspin.com).

#### **CONTACT:**

Deb Montner, Montner & Associates, 203-226-9290, [dmontner@montner.com](mailto:dmontner@montner.com)

# # #