

Know Thy Firewall
by
Raymond E. Muth, CPA, CISA, CISSP, CITP
President, BankLogic.Net, CPAs & Consultants

It is important to keep in mind that safeguarding customer information is a process that never ends. Within your security profile, there are few components more vital than your firewall and firewall administration. As FedLine Advantage implementations via broadband Internet access are occurring this year for most community banks, this issue has become even more critical. Therefore it is a good time to review your firewall policy.

Within a firewall there are defined rules popularly referred to as the “firewall ruleset”. These rules define what kind of traffic comes in and what kind of traffic goes out. For example, if you are a bank that does not perform any sort of web hosting or provide e-mail services on-site, you should have a very tightly defined ruleset that prevents access to any ports on your firewall or to the rest of your internal protected network. On the other hand, if your bank provides an array of services like web hosting, Internet banking and e-mail services, this necessitates opening ports for those services. In that instance, your ruleset will define who can get to those ports.

You may be surprised to learn that the source of viruses and spyware can often be traced to a poorly defined outgoing firewall ruleset. A ruleset that permits music downloads for any employee can sometimes cause computers on that network to be infected. A ruleset that defines what sites authorized employees can visit, greatly reduces that risk. Monitoring outbound packets that are blocked by the firewall is also a practice that can help with early detection of outbreaks.

The latest firewalls with improved graphical interfaces and reporting capabilities have significantly demystified the technical complexity of firewall administration. In many cases a bank’s technical staff may effectively administer their own firewall(s). However, the non-technical aspect of firewall administration, defining the firewall policy is just as important. For example the firewall administrator or whoever actually maintains the firewall should not be the person who approves firewall changes.

You should maintain a written policy specifically defining the firewall’s policy. It can be just a few paragraphs specifying what services are allowed in which directions to which networks and hosts. You should also have a policy detailing who may make changes to the firewall policy, how changes are submitted and who must approve them. At first this may sound like yet another onerous policy. But consider that all core banking systems generate reports for access changes which should be reviewed on a daily basis. This helps to reduce transaction risk. The same kind of reporting should be developed for your network access including firewall access changes. Reviewing these reports helps to reduce reputation risk.

An issue we routinely see when reviewing a bank's firewall ruleset in the course of our vulnerability assessment is that former vendors hired by the bank to set up its network or firewall, retain access to the firewall. In the worst case scenario, what sometimes follows is administrative access to the network for the vendor as well. In other words, they have the keys to all your customer information.

One final word of caution regarding FedLine Advantage, the Fed establishes a VPN (virtual private network) session via your Internet connectivity. Be very careful with this. If your bank allows certain kinds of remote VPN access, it is theoretically possible for someone to pull up a FedLine Advantage session off-site if they have a USB token. And we are aware that some banks permit their employees to take home their USB tokens for disaster recovery purposes. It is our recommendation that your IT auditor or IT security professional scrutinizes your FedLine Advantage implementation and follows up on the implementation during their audit or security assessment.

Send e-mail to raymuth@banklogic.net