



Top 10 Frequently Asked Internet Security Questions

Is a firewall enough security? NO! Often times even a properly configured firewall does not block allowed services such as mail and web traffic. In these environments, a firewall doesn't filter, block or even examine this traffic once allowed.

Is my firewall managed? Most credit unions answer this question "YES", while most of the time it is untrue. A managed firewall means that a trained Internet security expert can ensure the configuration is correct as well as keeping the software and security patches up-to-date, make appropriate changes, and can review logs for suspicious activity.

Does my ISP manage my firewall? Probably not! ISP's are connectivity experts, not security experts. Usually, they configure the firewall for the base level connectivity requirement and leave it as-is. Most never update the software. Usually an ISP only performs maintenance, which means if the device fails, they will replace it.

Should my firewall be monitored? Probably not! Most of the time, firewalls do not record the type of data needed to determine if a dangerous attack is happening. There is some value when added to an intrusion detection system, but by itself, there is little value.

Should I outsource my security management? Retaining highly qualified security engineers is not only difficult, but costly. Usually, it is far more cost effective to outsource the specific Internet security components including remote vulnerability assessments, firewall management, and intrusion detection and prevention.

How often do I need a full assessment? Federal regulation required these to be done on a regular basis. "Regular" means different things to different people. For the smallest of CU's, this should be done at least once every 3 years. For larger CU's, it should be done each year or every other year depending upon the specific CU.

Do I need an intrusion detection system (IDS)? If you host services (which means the server is in the CU network) such as email, a web site, online banking, etc. then using an IDS is HIGHLY encouraged. If you do not host any services but have many other potential attack sources such as inbound modems, partner connection, VPN etc, then using an IDS is MODERATE to HIGHLY encouraged. If you have broadband Internet access and unrestricted access to the Internet for your employees, IDS is MODERATELY encouraged.

Do I really need a penetration test? Few credit unions need to go to the expense of a full-blown penetration test. Most of the time, when asked to do a penetration test, a remote vulnerability assessment is all that is needed.

How often should I have a remote vulnerability assessment performed? If you host services, then monthly assessments is HIGHLY encouraged. If your Internet access is for outbound use only (web surfing, etc.), a quarterly assessment is usually sufficient.

Which systems should I test when doing a remote vulnerability assessment? All publicly accessible systems should be tested. This would include the firewall's public address, any public system such as a web site, email server, or FTP server that is hosted at the CU. Depending upon the CU environment, the Internet router may need to be tested as well. Most CU's have between 1 and 4 addresses that should be tested.

To have a Security Solutions™ representative contact your credit union, call CUNA Member Service at 800-356-8010, press 3, 8:00 a.m. - 4:30 p.m.