



CUNA CENTER FOR
RESEARCH & ADVICE

CUNA Internet Security Solutions

Powered by Red Cliff Solutions

Managed Firewall

MANAGEMENT

Firewall management consists of many critical elements to ensure the credit union security. Like any security device, it must be updated on a regular basis with the latest software patches. If your firewall has not been updated in the last few months (at a minimum), there could be serious security flaws.

Even more important is the way the firewall is configured. Even one wrong rule or filter could allow an attacker to gain access to your internal systems. The individual(s) managing your firewall need to have a strong security background as well as a thorough understanding of TCP/IP (the protocol used on the Internet).

During installation, it is very important to take into consideration the entire network. If some systems remain on the outside of the firewall, or are bridging the firewall, it can render the firewall useless by creating backdoors to your private network.

We can manage our own firewall

Credit unions that get personally involved with their network security are great. However, when the credit union hasn't spent the time and money to get their personnel properly trained, it can lead to misconfigurations that can lead to security breaches. When a credit union does spend the time and money to get personnel trained, those individuals often leave for more lucrative positions elsewhere. This leads to a cycle of spending and time wasted for the credit union.

My ISP manages our firewall

Many credit unions feel that because the ISP installed the firewall, they continue to manage it. What the ISP usually does is firewall MAINTENANCE. For most ISPs, this means that if the firewall breaks, they will fix it.

The vast majority of ISPs never update the firmware or software on the firewalls. This can lead to security problems. Additionally, the credit union often has no idea what ports or services are open on their firewall. The ISP could leave ports and services open that completely expose the credit union's network. ISPs are

usually not security experts; they are connectivity experts. Do not leave your members information security in the hands of your ISP.

We have a consultant manage our firewall

Outsourcing your firewall management is a good idea when proper steps have been taken. Unfortunately, many credit unions put their network security into the same hands as the person that fixes the printers. A computer expert doesn't make an Internet security expert. Just because someone can install a firewall, doesn't mean it has been installed properly. Serious holes could exist that may be compromised by an attacker. If you use a consultant to manage your firewall, ensure they have been properly trained in Internet security and TCP/IP.

FIREWALL MONITORING

Internet security monitoring is strongly recommended for certain credit unions, but does that really mean firewall monitoring? Most firewalls currently do not have the capability to do deep packet analysis, which is what allows a security system to identify malicious traffic. So firewall monitoring offered by many is simply log review. This has some basic value, but usually isn't worth the monthly fees. 24/7 monitoring of a firewall should only be done if the firewall has intrusion detection or intrusion prevention capabilities based on signature, protocol, and network analysis.

HARDWARE VS. SOFTWARE FIREWALL

Hardware firewalls, often referred to as "appliances" because they don't have any moving parts (other than fans), are far superior to software based firewalls. Anytime you simply load software onto an existing PC or server, you may have problems. Serious security issues can exist because operating systems may have flaws that can compromise your entire firewall. Usually a process of "hardening" the OS must be performed before loading the software. One missed service left open could be catastrophic. The CUNA Managed Firewall is an appliance with an operating system specifically written for Internet security.



CUNA

Credit Union National Association



CUNA CENTER FOR RESEARCH & ADVICE

The more moving parts you have on a system, the higher chance it has of failing. A failing motherboard, CPU, memory, or hard drive could take your Internet access down for hours or days. The CUNA Managed Firewall, being an appliance, has one of the lowest failure rates in the industry. If a failure does occur, the firewall will be replaced within 24 hours.

Appliances offer far greater performance. They have processors and other hardware specifically designed for high-speed data transfer, filtering and encryption.

THE CUNA SOLUTION

CUNA Internet Security Solutions can help assess the appropriate security steps required for your credit union, and recommend the appropriate solutions.

The CUNA Managed Firewall includes the following elements:

- **NetScreen firewall security appliance** – Netscreen is an industry leader in firewall technology. Their appliances have one of the lowest failure rates in the industry. They are cost effective while offering the highest levels of protection and flexibility.
- **Firmware and security patch updates** – CUNA Internet Security Solutions will keep your firewall up-to-date with the latest patches and firmware to ensure the highest degree of security. These updates are made in “maintenance” windows (usually after hours or weekends) defined by the credit union.
- **Policy changes** – All filter rules and other firewall configuration changes are made by CUNA Internet Security Solutions. Change requests happen within 48 hours but are usually done the same business day. Rule changes never disrupt the credit union operations and do not require a system reboot.
- **Consulting** – Have a question about a new online system or service that effects Internet security? Ask CUNA Internet Security Solutions. We can help you identify the best way to roll out your new services or answer questions you may have regarding proposed firewall changes.
- **Reporting** – The credit union security officer can receive read only access to real-time firewall information. Additionally, logs, which include in and out access as well as system event information, can be sent in email on a daily basis.
- **DMZ** – A demilitarized zone (DMZ) is a separate network segment that has different rules usually for access from the Internet. Often a DMZ is used for hosting web and email services. A DMZ can be used to increase the security of your network. Certain NetScreen firewalls can support 2 physically separate DMZ's in addition to the trusted and untrusted interfaces.
- **Flexibility** – The CUNA Managed Firewall solution can fit any Network topology with little or no network changes required. CUNA firewalls can support many modes of operation including NAT, route, and transparent (which remains invisible to your network). Additionally, the firewall can work with any Internet service provider supporting static addressing, dynamic addressing, and PPPoE. Lastly, the firewall can also be used as a DHCP server. This allows you to use the firewall to assign the network addressing information to local area network computers.
- **Virtual Private Networks** – Use the same firewall as a connection point for remote access and site-to-site VPNs. Save thousands of dollars each month through the use of VPN technology.
- **Off-Site Configuration Storage** – Each managed firewall has its configuration file saved at the CUNA Internet Security Solutions data center. This supports the credit union business continuity plan and can assist in rapid restoration of service.

CONTACT INFO

Stacey Norland | Research Analyst
CUNA Center for Research & Advice
Credit Union National Association, Inc.
5710 Mineral Point Road
Madison, WI 53705
E-mail: snorland@cuna.com
Phone: 800-356-9655 ext. 4317
Fax: 608-231-4027

To learn more, visit
securitysolutions.cuna.org



Credit Union National Association