# Perimeter Defense: the Reverse Proxy

Michael Ryan
CEO
South River Technologies

Nearly all businesses protect vital internal assets by means of a firewall: a software- or hardware-based solution that sits between the corporate LAN and the external internet. These firewalls are designed to limit, regulate, and monitor traffic that passes between the public internet and the private corporate LAN. Unfortunately, as hacking techniques get more sophisticated, it is possible to hack through a firewall using various spoofing and packet injection methods. When these methods are successful, your data is at risk.

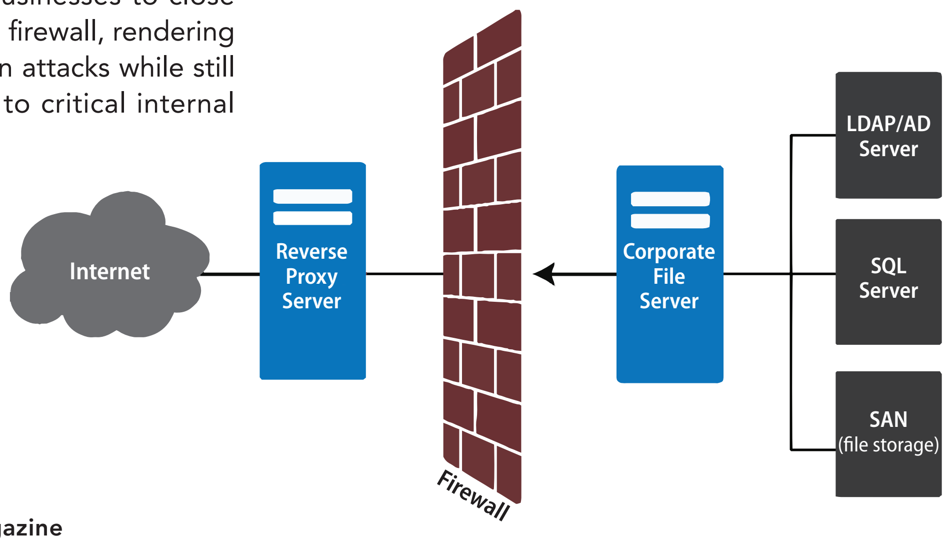
How can your company protect against attackers getting into your LAN through the firewall? While the easiest option would be to trim the attack vectors by closing all inbound firewall entry points, this might not be the most practical. With today's workforce becoming more mobile and remote, the need for employees to have access to shared network resources while on the road is vital. Closing down firewall ports and cutting off access for remote employees is simply not plausible in today's environment.

Another option open to businesses comes in the form of a reverse proxy. A reverse proxy is a hardware or software solution which allows businesses to close down inbound access through the firewall, rendering it impervious to malicious injection attacks while still allowing remote workers access to critical internal shared data.

Businesses require internet connectivity in order to survive and operate. This pipeline to the outside world enables internal users to access global resources, share files, and leverage email communications. A firewall strategically placed between the outside world and the internal LAN enables system administrators to monitor traffic and regulate what types of data are permitted into the LAN.

For example, if you have an FTP- or SFTP-based file server installed on premise, you will most likely have ports 20, 21, or 22 open on the firewall, with routing rules defined to push data to your file server over those ports. If you have a corporate WebDAV or Sharepoint server, traffic for those internal services would most likely travel through your firewall on well-known port 80 for unsecured access, or 443 for TLS access.

While firewalls do a good job of monitoring traffic, analyzing packets, and upholding the quality of data that arrives into the network, we can't get around one common denominator. In general, firewalls need to allow outside connections through the firewall to internal data



In general, firewalls need to allow outside connections through the firewall to internal data sources.

sources. Any open port permitting inbound traffic is a potential attack vector for intruders. No matter how secure the firewall claims to be, there will always be a risk of intrusion if the vector exists.

A good analogy is your home. Every home has doors and windows. The most secure scenario for the homeowner is one where all doors and windows in your home are closed, locked, and the blinds drawn. Once you open a window or a door, your home is at risk. It is true that you can place a sentry at every open door and window, but there is still a chance that someone, or something, will be able to sneak past the sentry and enter the home. It could be a physical intrusion, or a visual intrusion through a camera or video monitoring device. The key takeaway is this: a risk of intrusion exists for every attack vector.

This creates quite a predicament.

As businesses, we need to allow outside communication to enter our LAN. Employees are on the go, working remotely, or sharing key information with prospects, partners, and customers. With more employees being remote, how can we share information safely?

One of the solutions is to employ a reverse proxy server. Often sold as two solutions, a reverse proxy will commonly have a component residing inside your firewall and another component residing outside. The internal component is able to securely 'dial out' to the external component through an outbound-only rule on the firewall over a non-standard arbitrary port. Once the internal server has, like an SFTP server, securely established its presence with the external reverse proxy server, the external DMZ-based server will begin listening on behalf of the internal server. This external server in the DMZ now acts as a secure proxy server, delivering data securely to the internal server through the pre-established connection(s).

If new connections are necessary, the internal and DMZ-based servers negotiate a new outbound connection from the internal server to the DMZ, consistently ensuring that outbound-only connections are generated through the firewall.

For CISOs and CTOs who are facing the complexity of balancing a secure LAN environment with open access to email and file resources for your employees, software vendors may have information on reverse proxy options for existing applications. A reverse proxy server will enable you to close down more inbound ports on your corporate firewall, decreasing the number of attack vectors and increasing overall security for your organization.

### About the Author:

**Michael Ryan** *is the CEO of South River Technologies, a global provider of cybersecurity solutions targeting organizations in need of enterprise file sharing and collaboration for their distributed workforce. Mr. Ryan has over 20 years of experience in cybersecurity, initially designing frame-relay encryption networks to secure banking transactions in Europe in the mid 1990's. Today Mr. Ryan leads SRT's engineering team to deploy leading-edge security principals for customers in the healthcare and financial markets.*

SRT