

## Case Study:

### We Have Found the Enemy and the Enemy is Us.

#### Business Issue

A lawyer from a medium sized law firm opened email with exe attachment that was a zero-day malware item. The malware infected the computer, which set up a rogue email server. The rogue email server started sending out spam, which in one day got the company on the Spam Blacklist effectively blocking all outgoing email. We need to protect the company from malicious rogue POP email servers and other unauthorized outgoing traffic to allow mail to flow and business and billing to resume.

#### Solution

We replaced the “business class” router with a Cisco ASA5505. The Cisco is a true business router and allows a much more granular level of control to the type of internet traffic to your network. In this case, since the client used Exchange email, we were able to configure the Cisco router to block mail traffic of all types except to and from the Exchange mail server itself. Once mail was blocked we were able to get the firm off the black lists and mail functioned properly.

#### Results

People make mistakes and clicking on a questionable email attachment happens. Use of a better router is an investment in not having small mistakes cause big, expensive and time consuming problems for a small business. Additionally it allowed us to block a few time-wasting websites and sped up download speeds for everyone in the office.



**APERIO**  
Information Technology Administrators