2107 Wilson Boulevard | Suite 510
Arlington, VA 22201

703.841.5500 tel
703.841.5501 fax

www.onpointcorp.com

Expedited Implementation of a Web Application Firewall

May, 2015
Dan Schulman,
Information Security, Risk, Compliance and Cybersecurity Expert
OnPoint Consulting, Inc.

Synopsis

OnPoint Consulting implemented a cybersecurity solution which protected a customer application that was vulnerable to a specific security threat. While a complete review of the Security and the System Development Lifecycle (SDLC) process was ideal, cost and timing were prohibitive of a complete application-level code rewrite. OnPoint's solution mitigated the risk while introducing new protections and new functionality – including new growth opportunities for the customer – all within weeks and with zero impact to the customer's operations.

The Problem

One of OnPoint federal customer's operated a legacy internet-facing web application which was flagged during a Department of Homeland Security (DHS) audit for running vulnerable software. DHS, along with the agency's own Information Assurance department, determined that immediate action was necessary, up to and including removal of the application from the network. However, this interagency application, which is critical to the operation of many agencies including Department of State, Department of Defense, Federal Aviation Administration, and US Customs and Border Protection simply could not be taken offline. Options presented included redeveloping the application with modern versions of .NET, Adobe ColdFusion, SharePoint, Oracle WebLogic, and others. None of these were feasible in the short timeframe and tight budget constraints within the current fiscal year. OnPoint's customer and their internal customers were stuck with no readily available solution.

The Solution

OnPoint cybersecurity stepped in. While some protections were currently in place, OnPoint saw an opportunity to mitigate the current situation while increasing the network's overall defense posture. OnPoint presented a solution to continue using the application as is with no changes to current system operation by adding an additional layer of cybersecurity protection. OnPoint performed both risk and mission requirement analyses and determined that the functionality and availability of the application were stable, in addition, the internal customer was happy with the current application (and unhappy with the thought of redevelopment costs). Keeping the application as is and simply placing a new Web Application Firewall (WAF) in front of it was determined to be the best short-term option.

A Web Application Firewall, also known as a Reverse Proxy, is common technology and is an integral part of a security defense model in a DMZ. This device receives traffic on behalf of the web server the traffic is intended for, decrypts it (if applicable), inspects it, and then re-encrypts it (if applicable) to its "real" destination.

OnPoint's customer, who had been using "all-in-one" network security appliances, approved of OnPoint's plan after being shown that the legacy architecture was no longer adequate to handle modern cyber threats. OnPoint showed that the new device would not only mitigate the current risk as seen by IA and the CIO's office, but would also add new protections, new functionality, and provide service growth opportunities for other internal Federal customers. One specific and important improvement was the implementation of SSL/TLS inspection. By leveraging the SSL certificate and private key from the server itself, the WAF is able to inspect potentially malicious traffic before it gets to the server – traffic that the network would otherwise be blind to.

Working concurrently with OnPoint's customer and a network protection vendor, OnPoint analyzed options, requirements, performance metrics, and other pertinent information the customer deemed appropriate and procured a physical device within two weeks. An architecture was developed, change was submitted, development environment tests were run, and a maintenance window determined within another week.

The change was implemented the following week and a solution was in place. From start to finish, OnPoint implemented this short term solution in about five weeks – well before the 3-month deadline given by the CIO's office. This gave our customer much needed time to properly develop a new application and remove the vulnerable software for good.

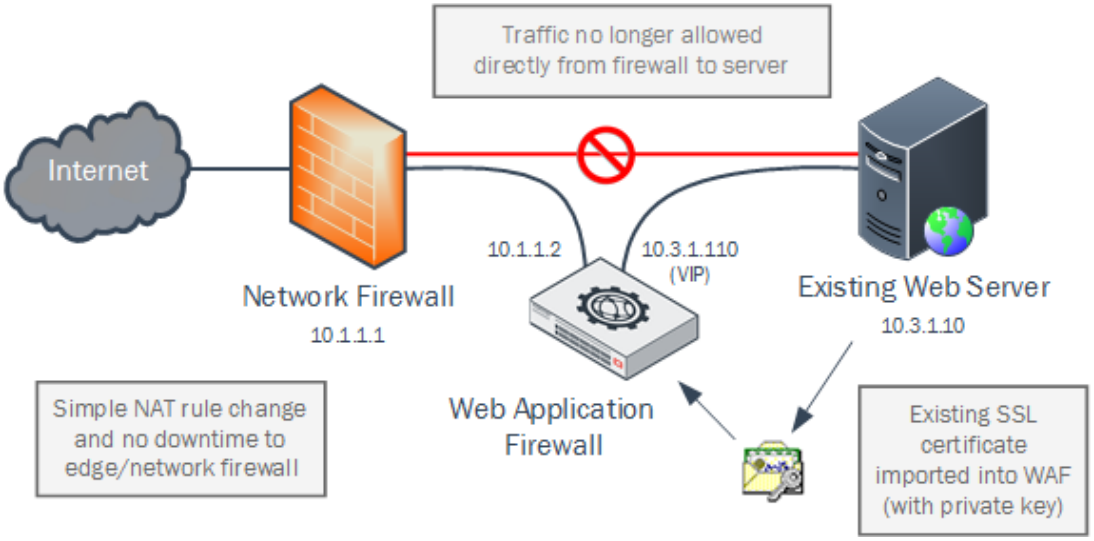

Figure 1 – Logical Example of the Solution

More information

Microsoft's article "Security Best Practices to Protect Internet Facing Web Servers" has more information that is concise and easy to read, including implementation of a WAF. The article is located at: http://social.technet.microsoft.com/wiki/contents/articles/13974.security-best-practices-to-protect-internet-facing-web-servers.aspx. *(Please note: By clicking this link you will be leaving OnPoint's website. Neither OnPoint nor its parent organization(s) are responsible for content on other websites.)*

Update since the authoring of this article

The application being protected by this Web Application Firewall was the target of an aggressive cyber-attack in May, 2015. The WAF analyzed over ten-thousand connection attempts which included automated SQL injection and directory traversal attempts, and equally importantly, enabled the server to remain operational during the incident. As the information was sent over an HTTPS connection and was encrypted, the edge firewall could not inspect the high layer traffic and therefore allowed all of it.

After the event, the inclusion of the WAF on the network was analyzed. If the WAF was not in place enabling TLS inspection, a denial of service situation due to a server crash would have likely been the best case scenario. The worst-case scenario: successful exfiltration of a database housing Federal Personally Identifiable Information and Intellectual Property. Good news – the WAF performed as planned.

About OnPoint

OnPoint Consulting, Inc (OnPoint) is a cybersecurity and technology firm delivering secure IT infrastructure, enterprise systems, and classified solutions for the U.S. federal government. Our specialized strategy, cyber and technology capabilities are changing the way our clients improve performance, effectively deliver results and manage risk. OnPoint holds ISO 9001:2008, ISO 20000-1:2011, ISO 27001:2005 certifications and a CMMI Maturity Level 3 rating. OnPoint is a wholly owned subsidiary of Sapient Government Services, a global consulting company part of Publicis.Sapient. Follow OnPoint on Twitter, LinkedIn and Facebook.