Protecting Web Applications and Servers from Cyber Threats via-ICAP integration with OPSWAT

The Problem

Enterprises are exposed to malware through several attack vectors. Common ways that malware reaches companies is through email attachments and file sharing mechanisms. Companies have spent billions of dollars on email security solutions to isolate suspicious attachments. However, web applications that accept file uploads are another attack vector that have not been adequately protected against malware. As an example, a corporate recruiter may receive a resume in response to a job posting and that document could contain malware that gets shared inadvertently with hiring managers. Enterprises need effective, multi-layered defenses against web application vulnerabilities and cyberthreats to protect against malicious file uploads, viruses, malware, or other inappropriate content.

Solution

VMware NSX Advanced Load Balancer (Avi Networks) provides protection against web application attacks with an intelligent web application firewall. The platform has added malware protection and content sanitization capabilities for web applications through *ICAP integration for malware scanning with OPSWAT*.

Avi has developed technology integrations with anti-malware technologies including OPSWAT and LastLine (now part of VMware) to enable real time inspection of web traffic for malware and vulnerabilities. Policies and configured workflows enable file blocking and removal, or redactions of sensitive information before leaving the network.

How it Works?

VMware NSX Advanced Load Balancer and WAF provides ICAP (Internet Content Adaptation Protocol) based integration with OPSWAT. With this integration, the WAF can be configured to route untrusted traffic and file uploads through the OPSWAT MetaDefender ICAP server to secure it from malware, trojans, ransomware, and zero-day threats. The OPSWAT MetaDefender ICAP server scans files simultaneously using multiple commercial AV engines, anti-virus software for vulnerabilities disarms unknown content, detects vulnerable binaries, and detects and blocks sensitive data.

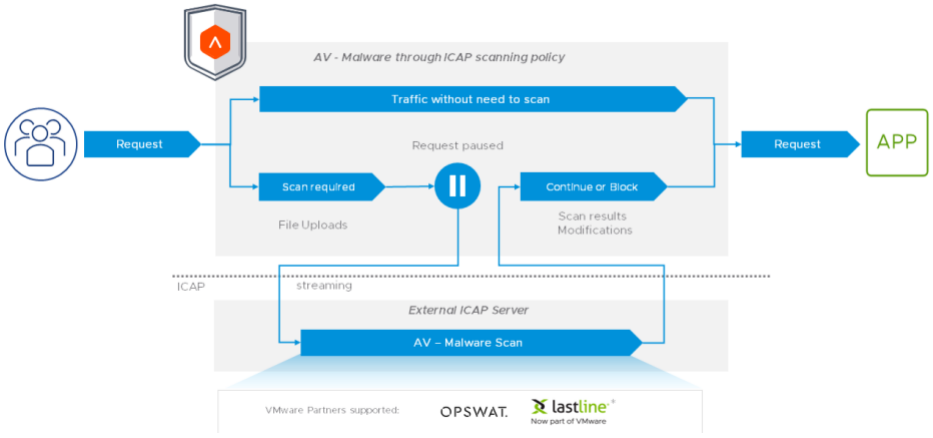
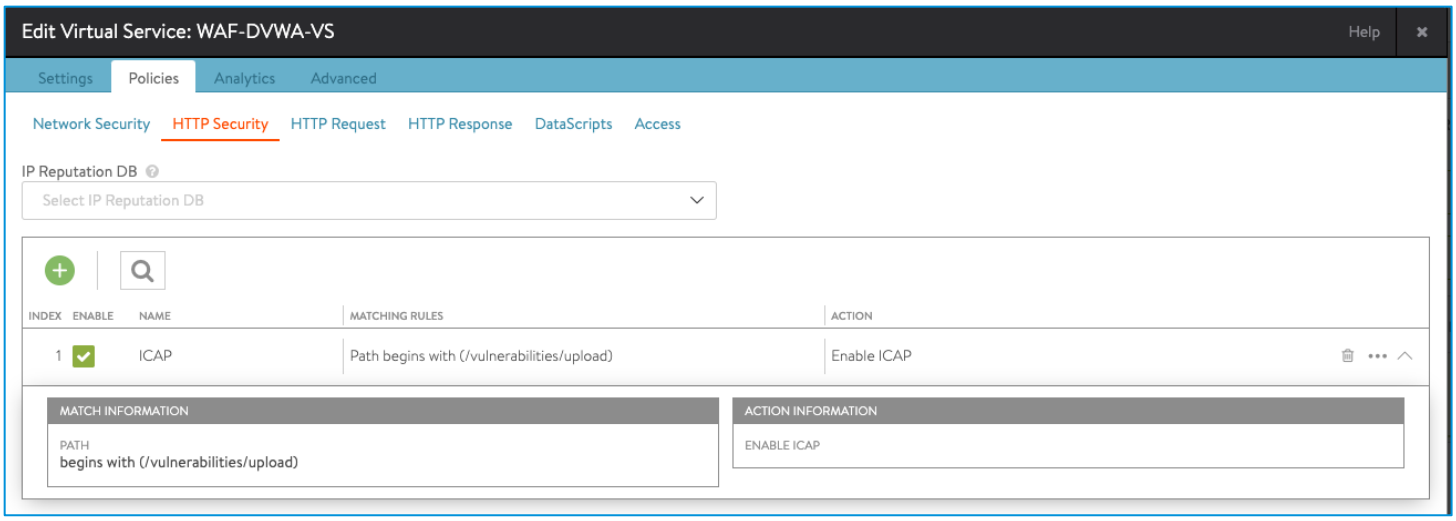


Figure 1: VMware NSX ALB (Avi) and WAF – ICAP integration Architecture

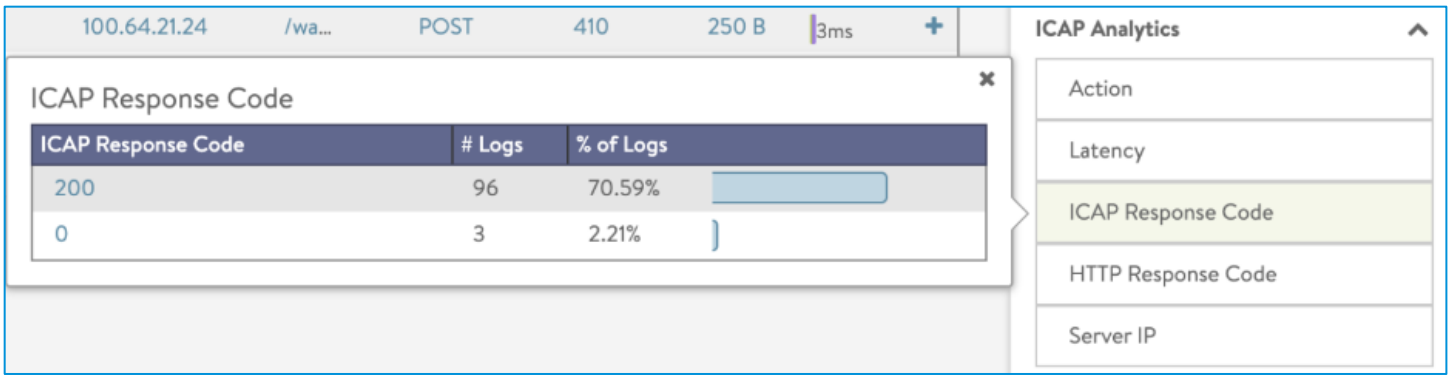
HTTP Security Policies with "Enable ICAP" Action

The process to enable malware scanning with ICAP integration is a simple, point-and-click process in the Avi Controller UI. A new policy is created to match on a path for file uploads and the ICAP action is triggered.



Integrated Analytics with ICAP policy

The Avi Platform already includes powerful analytics to provide visibility to application insight, WAF hits, SSL status, and DDoS attacks. With the ICAP integration, the ICAP response codes are captured and displayed as part of the Avi log analytics capabilities for further analysis and troubleshooting.



Summary

The anti-malware integrations offered by VMware are available as part of the scalable software-defined architecture of the load balancing and WAF platform which can be deployed across data center or cloud environment. Together with OPSWAT, the platform offers enhanced, scalable application security for enterprise web applications.