Protecting Applications with LoadMaster and KEMP WAF

Reference Architecture

VERSION: 1.0
UPDATED: Mar 2016

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

Table of Contents

1 Introduction

Application vulnerabilities are perhaps the largest known attack vector, and this is particularly true in the Cloud where they can be exposed to more risk than is typically present in a well-secured data center.

When organizations chose to run some or all of their business in the public cloud, they must still observe the same requirements for security and compliance that they would implement on-premises.

With the rise in SSL traffic on the internet, the potential for application specific attacks increases, so a solution which can efficiently address the need to mitigate such attacks is required. This is where the integrated features of KEMP's LoadMaster can work together and provide cost effective protection for applications and services deployed in the Azure cloud.

1.1 Document Purpose

This document discusses how LoadMaster can help reduce risk and achieve compliance for cloud based applications and services. While not a complete solution in itself, the LoadMaster provides elements which can form part of a broader strategy to ensure compliance to mandates such as PCI-DSS and HIPAA.

1.2 Intended Audience

This document applies to:

- Cloud and Network Architects
- System and Security Administrators.
- Line-of-Business Management

2 KEMP WAF Overview

KEMP's Application Firewall Pack combines Layer 7 Web Application Firewall protection with a range of application delivery services including intelligent load balancing, intrusion detection, intrusion prevention as well as edge security and authentication.

The WAF component in LoadMaster incorporates ModSecurity , the world's most deployed web application firewall engine. It leverages threat intelligence and research from information security provider, Trustwave. Customers with a subscription receive automatic updates as new threats are identified and mitigated.

With WAF enabled, the LoadMaster can secure against threats such as the OWASP Top Ten, cross-site scripting and threats that might compromise credit card data, to name a few.   In addition, since KEMP's WAF is based on ModSecuriy, customers can create their own custom rule sets at no charge.

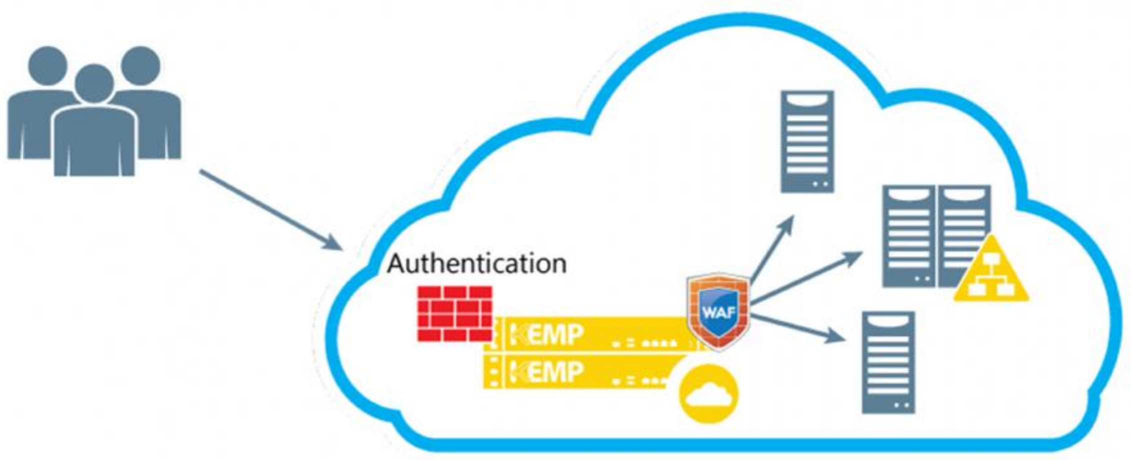
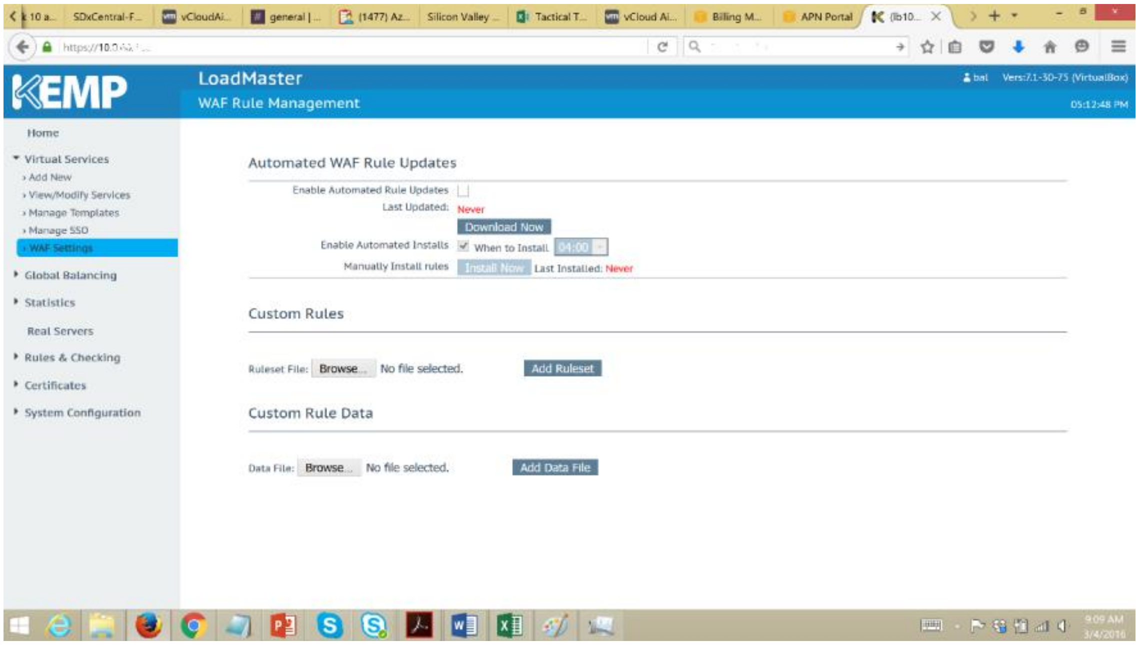


Fig. 1

With data breaches being commonplace, the damage to the revenues and reputation of a business can be devastating. Deploying LoadMaster as part of a broader security strategy can provide an integrated, easy to deploy solution at lower cost than trying to maintain a solution built from the many point products available in the cloud and from third parties.

2.1 WAF implementation example

Where WAF is licensed for a LoadMaster, the WAF Rule Management screen will appear as below:



Automated WAF Rule Updates

Enable Automated Rule Updates □

Last Updated: Never

Enable Automated Installs ☑ When to Install 04:00

Manually Install rules Last Installed: Never

Custom Rules

Ruleset File: No file selected.

Custom Rule Data

Data File: No file selected.

Fig. 2

This provides the option for customers with a subscription to upload the commercial WAF Rule Set and receive automated updates. These regular updates provide:

- data loss prevention (DLP)
- mitigation of the OWASP Top Ten common vulnerabilities
- real-time threat protection for packaged & custom applications
- support for organizational PCI-DSS compliance requirement

Within an organization, there may be a need to customise and add rules to meet specific security criteria. A typical example of how to implement such custom rules is shown in the next section.

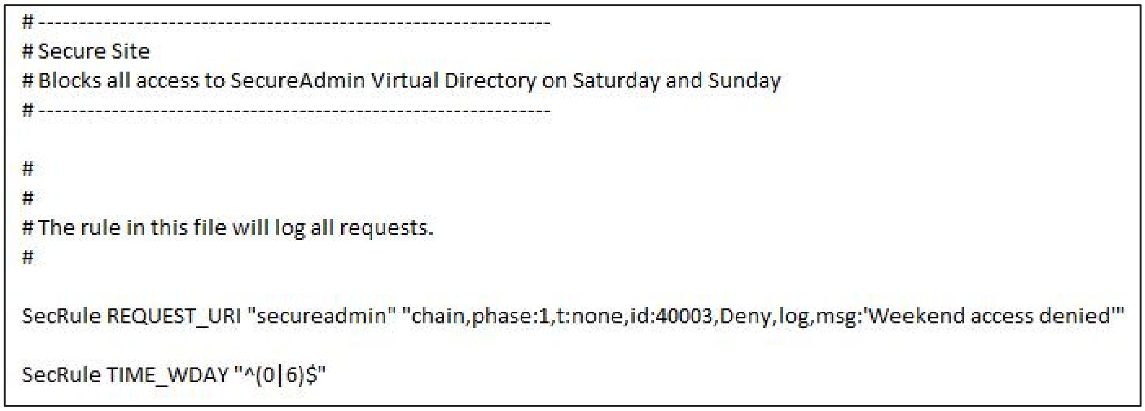
2.2 Implementing Custom Rules

In this example, a .NET web application has been developed to run in Azure's Platform as a Server (PaaS) offering.

To meet a contrived corporate security mandate, a particular segment of this site, the /SecureAdmin virtual directory, must only be accessible during weekdays, within regular business hours and from a single source IP Address.

To accomplish this, a custom ModSecurity rule can be created and added to the Virtual Service on the KEMP LoadMaster. The rule can be a simple chain rule, meaning the rule will only allow access when all of the Parts 1, 2 and 3 have been satisfied. This rule is broken down into three sections based on the security requirements.

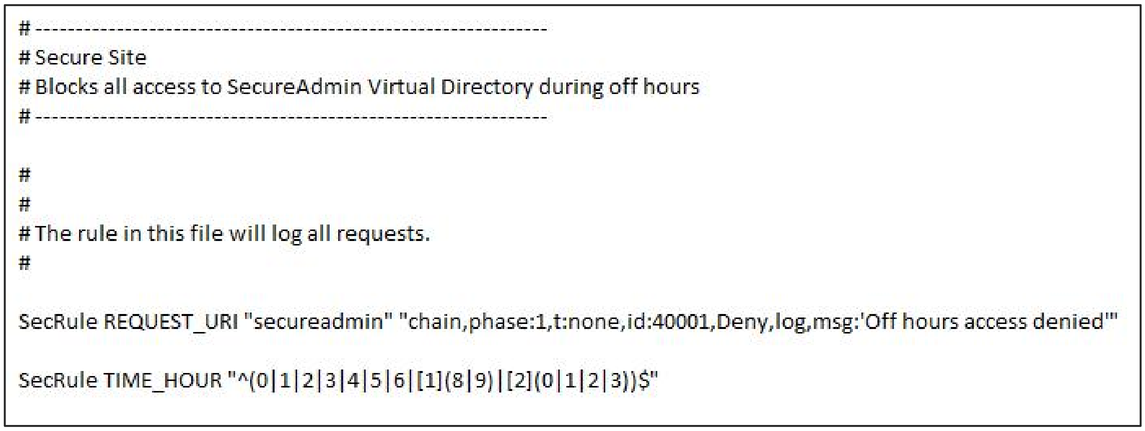
Part 1: Do NOT allow access Saturday or Sunday:



```
# ---------------------------------------------------------------
# Secure Site
# Blocks all access to SecureAdmin Virtual Directory on Saturday and Sunday
# ---------------------------------------------------------------

#
#
# The rule in this file will log all requests.
#

SecRule REQUEST_URI "secureadmin" "chain,phase:1,t:none,id:40003,Deny,log,msg:'Weekend access denied'"

SecRule TIME_WDAY "^(0|6)$"
```

Fig. 3

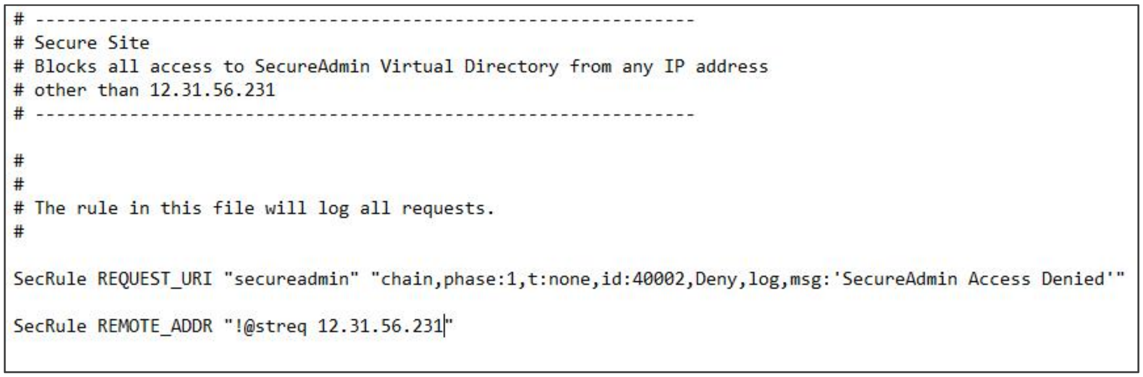
Part 2: Do NOT allow access during off hours (6PM – 7AM):



```
# ---------------------------------------------------------------
# Secure Site
# Blocks all access to SecureAdmin Virtual Directory during off hours
# ---------------------------------------------------------------

#
#
# The rule in this file will log all requests.
#

SecRule REQUEST_URI "secureadmin" "chain,phase:1,t:none,id:40001,Deny,log,msg:'Off hours access denied'"

SecRule TIME_HOUR "^(0|1|2|3|4|5|6|[1](8|9)|[2](0|1|2|3))$"
```

Fig.4

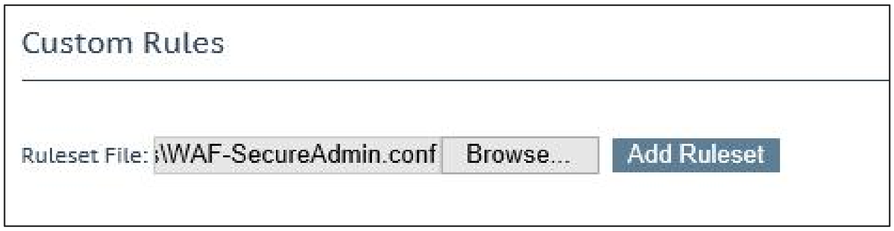
Part 3: Only allow access from IP Address 12.31.56.231:



```
# --------------------------------------------------------------
# Secure Site
# Blocks all access to SecureAdmin Virtual Directory from any IP address
# other than 12.31.56.231
# --------------------------------------------------------------

#
#
# The rule in this file will log all requests.
#

SecRule REQUEST_URI "secureadmin" "chain,phase:1,t:none,id:40002,Deny,log,msg:'SecureAdmin Access Denied'"

SecRule REMOTE_ADDR "!@streq 12.31.56.231"
```

Fig. 5

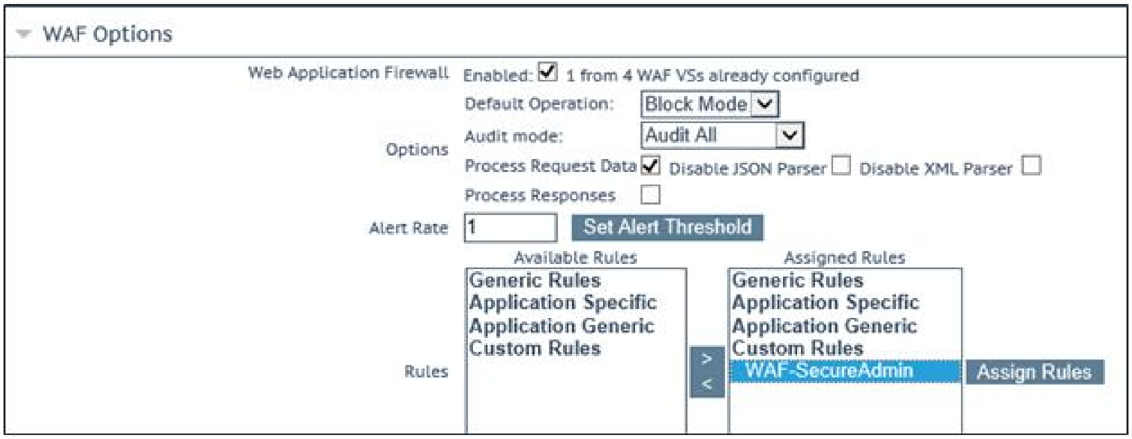
This set of rules can be composed in a simple text editor and saved with a .CONF extension. This can then be uploaded to the KEMP LoadMaster. Once the ModSecurity rule is added to the LoadMaster it can be selected within the Virtual Service.



Ruleset File: :\WAF-SecureAdmin.conf

Fig. 6

Within the WAF screen on the LoadMaster, simply browse and select the new configuration file for upload.



WAF Options

Web Application Firewall — Enabled: ☑ 1 from 4 WAF VSs already configured

Options
- Default Operation: Block Mode
- Audit mode: Audit All
- Process Request Data ☑ Disable JSON Parser □ Disable XML Parser □
- Process Responses □

Alert Rate: 1

Rules

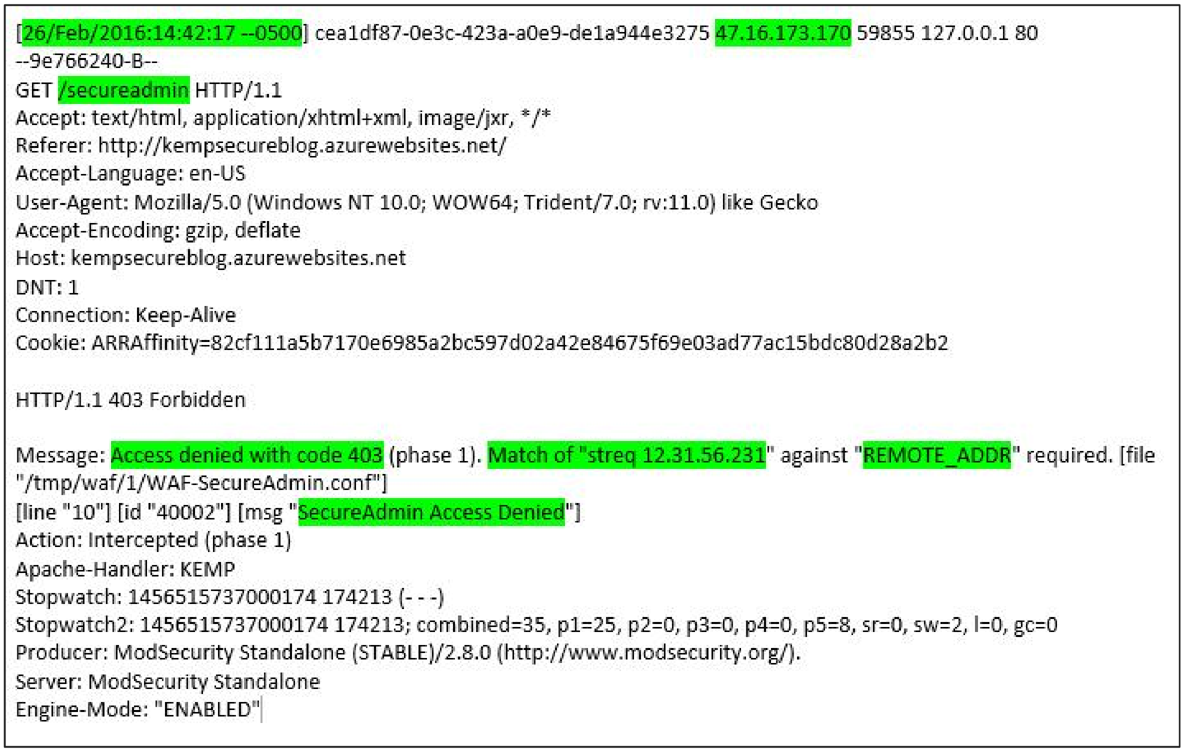
Available Rules	Assigned Rules
Generic Rules Application Specific Application Generic Custom Rules	Generic Rules Application Specific Application Generic Custom Rules WAF-SecureAdmin

Fig. 7

The LoadMaster will show that the new rule is now in place.

In addition to securing the Web App you can enable logging on the LoadMaster to track when the rule is triggered and access is blocked. This allows site administrators to track anomalous behaviour. For example, if access were attempted from a non-permitted IP this would be reported, along with the timestamp of when access was attempted.

This log entry shows that IP address 47.16.173.170 tried to access the /SecureAdmin virtual directory at 2:42PM on Friday, February 26, 2016. Since the time and day variables are permitted, this user was denied access due to the source IP address, which does not match 12.31.56.231.



```
[26/Feb/2016:14:42:17 --0500] cea1df87-0e3c-423a-a0e9-de1a944e3275 47.16.173.170 59855 127.0.0.1 80
--9e766240-B--
GET /secureadmin HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Referer: http://kempsecureblog.azurewebsites.net/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: kempsecureblog.azurewebsites.net
DNT: 1
Connection: Keep-Alive
Cookie: ARRAffinity=82cf111a5b7170e6985a2bc597d02a42e84675f69e03ad77ac15bdc80d28a2b2

HTTP/1.1 403 Forbidden

Message: Access denied with code 403 (phase 1). Match of "streq 12.31.56.231" against "REMOTE_ADDR" required. [file
"/tmp/waf/1/WAF-SecureAdmin.conf"]
[line "10"] [id "40002"] [msg "SecureAdmin Access Denied"]
Action: Intercepted (phase 1)
Apache-Handler: KEMP
Stopwatch: 1456515737000174 174213 (- - -)
Stopwatch2: 1456515737000174 174213; combined=35, p1=25, p2=0, p3=0, p4=0, p5=8, sr=0, sw=2, l=0, gc=0
Producer: ModSecurity Standalone (STABLE)/2.8.0 (http://www.modsecurity.org/).
Server: ModSecurity Standalone
Engine-Mode: "ENABLED"
```

Fig. 8

This simple example provides a glimpse into the sophisticated controls that could be implemented to ensure fine-grained adherence to security policies.

References

Additional supporting documents can be found at http://kemptechnologies.com/loadmaster-documentation. The following items in the feature description section address the example above and also provide additional information on configuration for virtual services and security.

- LoadMaster for Azure
- HA for Azure
- Application Firewall Pack (AFP)
- AFP Custom Rules
- Technical Note Rule Writing Guide

For more information on ModSecurity Custom Rules:
https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual

Document History

Date	Change	Reason for Change	Version	Resp.
Feb 2016	Initial release	First version	1.0	CB