Azure and F5 WAF in the cloud

Lior Rotkovtich, 2016-26-10

What's New ?

Microsoft Azure created a new dashboard called *Security Center* which provides security visibility for Azure customers. The Security Center Dashboard provides fast deployment and easy management of F5 WAF in the cloud in Microsoft's Azure infrastructure.

This article describes the solution and how it can be deployed with just a few clicks.

Azure Security Center and F5 WAF in the Cloud Key Benefits:

- Deploy WAF in minutes
- Easy two tabs configuration
- Immediate security with rapid deployment policy
- Optimized and effective security policy by default
- Security Center incident notifications

Solution overview

F5 is now integrated into the Azure Security Center dashboard that provides cloud customers the ability to manage their security exposure level. Once an Azure customer implements a web application, a suggestion is given via the Security Center to deploy WAF protection for the application.

The WAF configuration is done with a simple two tabs setup which can be completed in minutes. This simple setup is done via the Security Center GUI that utilizes an automated iApp on the BIG-IP without any user intervention.

Once deployed, the WAF in the cloud rapid policy provides immediate detection and mitigation of common attack vectors against web application as well as application DDoS attacks. The Security Center display notification on application security incidents against the application.

Adding a WAF from Security center

Any Azure customer that owns an application running on port 80 or 443, and doesn't have WAF protection will get a notification message from the Azure Security Center with a suggestion to install a WAF. Clicking on the application or virtual machine will present the "Web application Firewall not installed " message. Clicking on the message reveals the option to: "Add web application firewall" as illustrated in figure 1

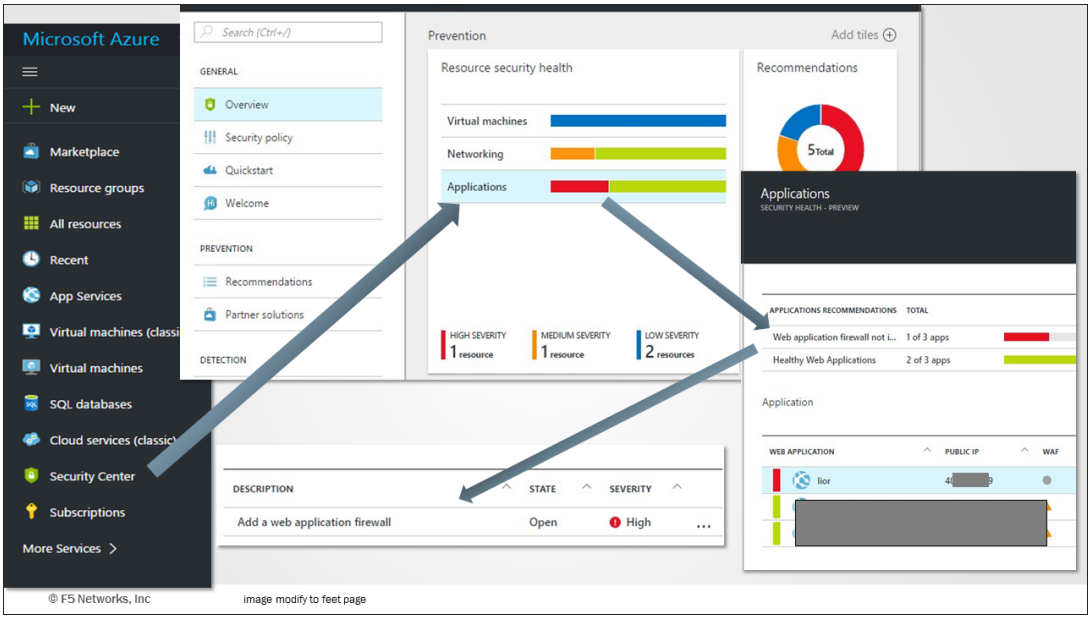

Figure 1: Azure Security Center provide suggestion to install Web Application Firewall

WAF Deployment - Configuration Steps

The two-tab configuration is easy to use because most of the configuration is pre-defined for you and there are only few items that require your input. Figure 2 illustrates the two-tab configuration and the items that you need to provide are marked below in bold:

Step1: Virtual Machine Configuration

The first tab configures the virtual machine settings.

The only configuration information needed here is the host name and password.

- Number of machines to deploy – default
- **Host – provide a host name**
- **Password – type your password**
- Pricing tier – default
- Resource group -default
- Location – default
- Subscription – default

Step2: WAF information

The second tab configures the WAF.

To complete the WAF deployment you should provide a license. The security blocking level enables the optimized rapid deployment policy setting. Keeping the default as Medium is good for most cases. You can also choose your Application Type to provide more accurate protection.

- **License token – provide you BYOL BIG IP WAF licenses**
- Security blocking level – default
- **Application type – choose your application type**
- Protected application – default (port 80)
    - Web application public IP
    - Internal server port
- Protected application – default (port 443)

- Protected application – default (port 443)
  - Web application public IP
  - Internal server port

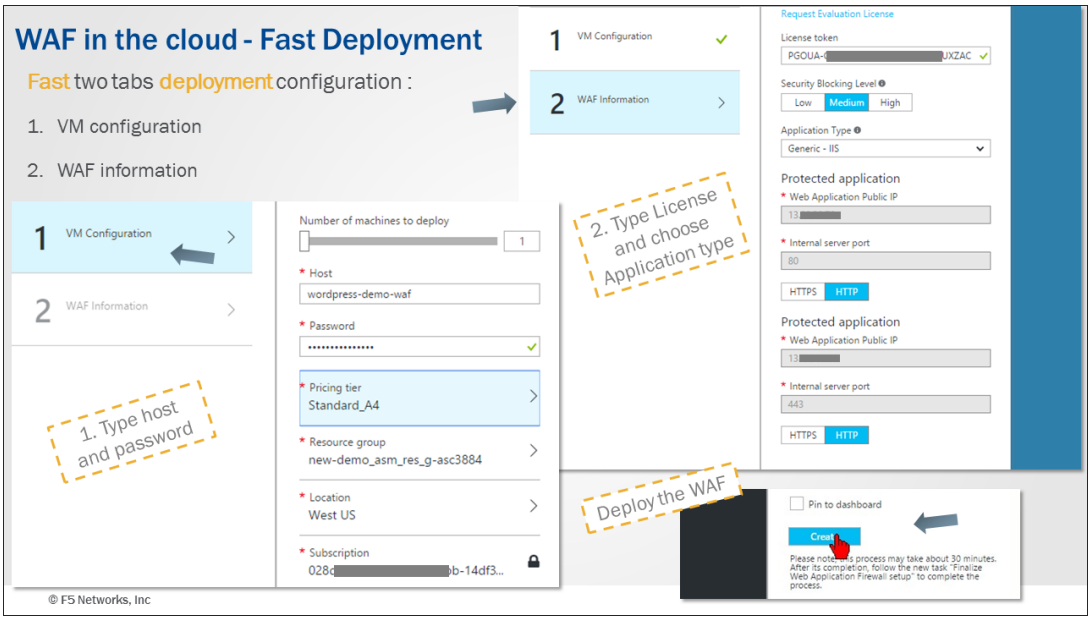

Figure 2: VM configuration and WAF information two tabs fast deployment

The WAF in the cloud deployment process begins once you click **Create**. The deployment mechanism will automatically configure all the necessary components including VLANs, self IPs, virtual IPs, pools, and logging profiles. The automatic process will also create an ASM policy, assign it to the virtual server, and configure the ASM blocking settings for you. This default configuration is highly efficient and provides detection and mitigation of known web application attacks.

Switching to protection mode

Once the installation is complete, there are two IP addresses to associate with the web application.

1. The current IP address used by clients to access the web application. This IP address is not protected by the WAF.
2. The new IP address that is assigned and includes the WAF protection. This IP address will become the IP address of the application once we decide to move to protected mode.

The reason we now have two IP addresses is to allow smooth transition from the unprotected environment to the protected environment and to eliminate false positive. While most deployments pass the false positive tests without any issues, web applications can be complex and therefore it is important to complete this step in any WAF deployment. We call it the **staging period**, in which the site administrator interacts with the application via the newly protected IP address to verify that traffic is passing.

The security center displays the “Pending WAF finalization” notification since the traffic is still routed through the unprotect IP address. Once the staging tests are complete, the WAF admin can route the traffic to the protected environment by clicking **Restrict traffic.** This will make the protected IP address as the primary site address that users will access the site. The Security center will then indicate that the application is protected by marking a green icon next to the application.

Remember that WAF *policy builder* is running and will automatically fine tune the policy as it inspects the traffic passing through it. False positives can loosen the policy by reducing security checks, and other prevention options can tighten the policy by increasing security checks.

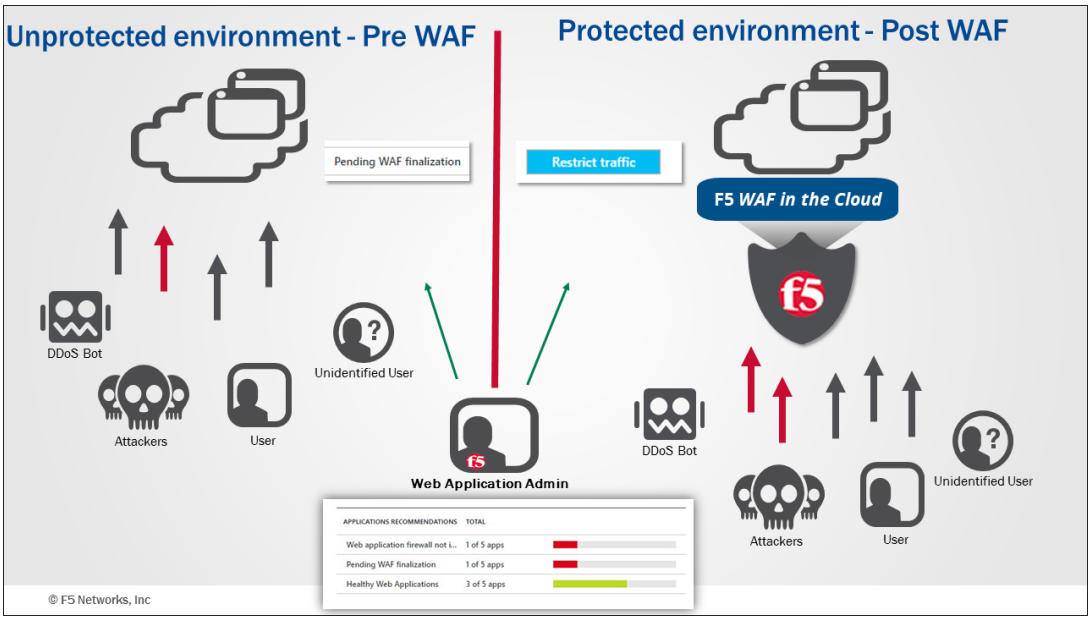

Figure 3: The administrator should verify false positive then route traffic to the protected environment with restrict traffic.

Mitigation and incident reporting

Once the traffic is routed to the protected environment, the Azure Security Center will present notifications on the security alerts tab. This information is collected from the WAF and categorizes risks:

Blue – No risk for your web application or data. But you might want to look at these notifications when you have time.

Green – No major risk to your web application or data. However, you should examine these items.

Red – There is a risk to your web application or data due to malicious payload. It is highly recommended to examine these items.

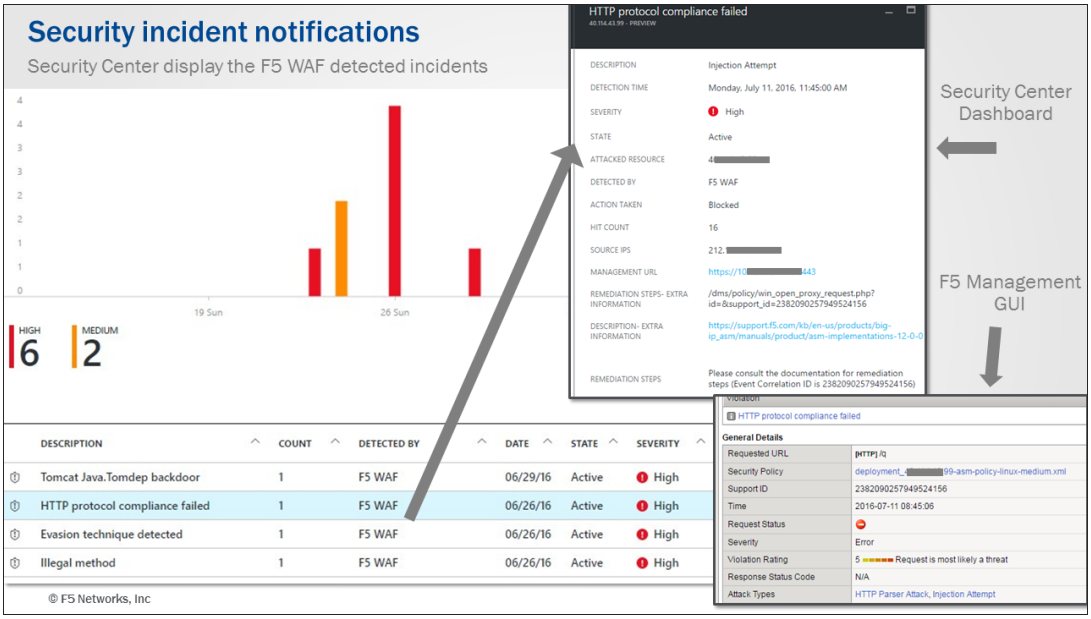

Figure 4: An example Security incident notification

As shown in Figure 4, each notification includes the requests details:

- **Attack type description**: indicates the attack type
- **Time and date**: when the incident occurred
- S**ource IP**: the offending source IP
- **Action taken**: was the request blocked or is this just a notification
- **Management URL**: a link to the F5 WAF GUI. Clicking it will open a new window that allows login to the F5
- **Remediation step**s – Extra information: A link to display the requests in the F5 WAF GUI which will display the specific incident (including support ID) for tracking.

Best practices for WAF management should be followed and are beyond the scope of this document.

General information:

*WAF in the cloud deployments allows flexibility with WAF management, a*t any time, you can:

- Add an additional application behind the WAF
- Revert application security policies to the default settings
- Unlink an application from the WAF
- Delete a WAF deployment

Ongoing management

- Accessing the F5 WAF GUI - fully manage the box.
- Attack Signature update – is supported
- Logging – configuring the ASM request log to send traffic to any syslog / SIEM system within Azure.

Support

- Azure Security Center support --is done via Azure GUI
- F5 ASM support – the WAF in the cloud solution is fully supported by F5

More resources:

To learn more or to access the instructions we recommend you to read the Manual.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113