SOP Modify WAF Configuration

Status of SOP:

Endorsed.

Related Platform	Component
Azure	Azure Web Application Firewall

Problem

How to modify Azure Web Application Firewall (WAF) configuration?

POSSIBLE CAUSE:

- Service request from application team to modify WAF mode.

What is Azure Web Application Firewall (WAF)

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

WAF on Application Gateway is based on Core Rule Set (CRS) 3.1, 3.0, or 2.2.9 from the Open Web Application Security Project (OWASP). The WAF automatically updates to include protection against new vulnerabilities, with no additional configuration needed.

WAF MODES

The Application Gateway WAF can be configured to run in the following two modes:

Detection mode: Monitors and logs all threat alerts. You turn on logging diagnostics for Application Gateway in the Diagnostics section. You must also make sure that the WAF log is selected and turned on. Web application firewall doesn't block incoming requests when it's operating in Detection mode.

For all NON-PROD applications WAF mode is Detective in BHP environment.

Prevention mode: Blocks intrusions and attacks that the rules detect. The attacker receives a "403 unauthorized access" exception, and the connection is closed. Prevention mode records such attacks in the WAF logs.

For all PROD applications WAF mode is Preventive in BHP environment.

NATURE OF REQUEST:

A ServiceNow request would be received to modify Application Gateway WAF mode.

PROCESS:

Raise an Normal Change Request

To modify WAF configuration, please raise a Normal Change Request Please go to page 20 of the below *Change Control document* :

Service Management: As-Is Change Management (ServiceNow)

Please select the respective Cloud Factory assignment group when raising a change request in Service Now

- Cloud Network - Hub Connectivity - Azure

Solution

1. Go to the desired repository based on the ServiceNow request

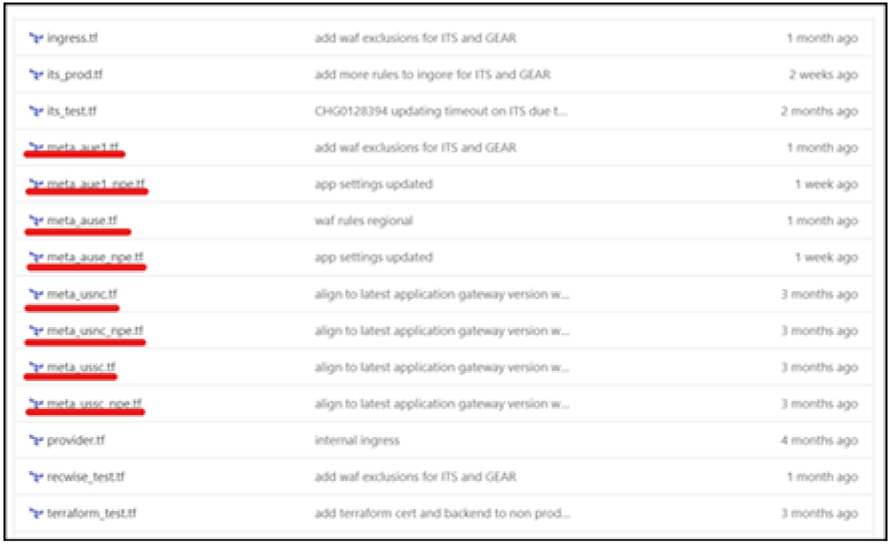
- If the request is for Application Gateway V1 WAF, go to below repository:

  https://gitlab.com/bhp-clodfactory/azure-foundations/legacy-ingress

- If the request is for Application Gateway V2 WAF, go to below repository:

  https://gitlab.com/bhp-cloudfactory/azure-foundations/internal-ingress

Sample files in the repository are highlighted in below screenshot:



ingress.tf	add waf exclusions for ITS and GEAR	1 month ago
its_prod.tf	add more rules to ingore for ITS and GEAR	2 weeks ago
its_test.tf	CHG0128394 updating timeout on ITS due t...	2 months ago
meta_aue1.tf	add waf exclusions for ITS and GEAR	1 month ago
meta_aue1_npe.tf	app settings updated	1 week ago
meta_ause.tf	waf rules regional	1 month ago
meta_ause_npe.tf	app settings updated	1 week ago
meta_usnc.tf	align to latest application gateway version w...	3 months ago
meta_usnc_npe.tf	align to latest application gateway version w...	3 months ago
meta_ussc.tf	align to latest application gateway version w...	3 months ago
meta_ussc_npe.tf	align to latest application gateway version w...	3 months ago
provider.tf	internal ingress	4 months ago
recwise_test.tf	add waf exclusions for ITS and GEAR	1 month ago
terraform_test.tf	add terraform cert and backend to non prod...	3 months ago

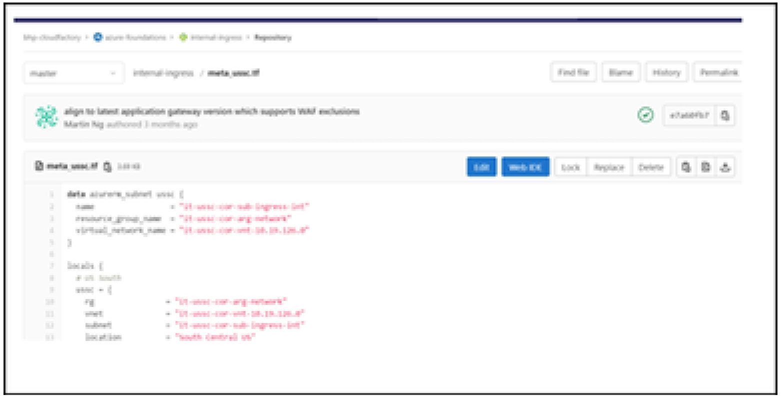
File names with “***meta”*** as a prefix are the files where WAF mode would be changed.

File names containing ***“npe”*** are the files for NON-PROD environment and file names without ***“npe”*** are for PROD environment. These files follow below naming convention:

meta_region_environment.tf

2. Select the **meta** file according to the environment **PROD/NON-PROD and region** as mentioned in the request.

Reference screenshot of the meta file is given below:



bhp-cloudfactory > azure-foundations > internal-ingress > Repository
master
Find file
Blame
History
Permalink
Edit
Web IDE
Lock
Replace
Delete

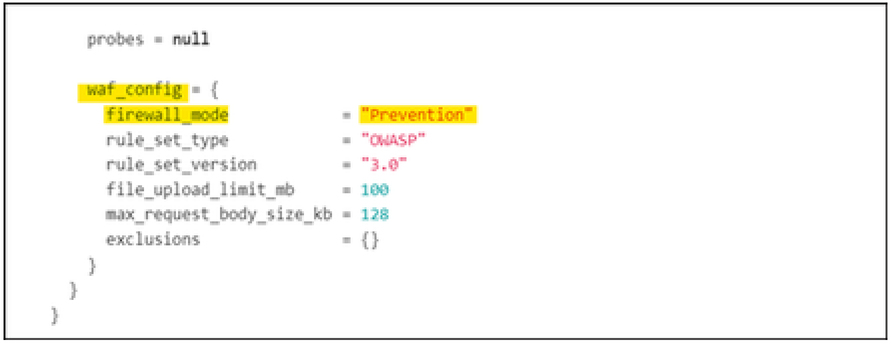
internal-ingress / meta_ussc.tf

align to latest application gateway version which supports WAF exclusions
Martin Ng authored 3 months ago

meta_ussc.tf

```
data azurerm_subnet ussc {
  name                 = "1t-ussc-cor-sub-ingress-int"
  resource_group_name  = "1t-ussc-cor-arg-network"
  virtual_network_name = "1t-ussc-cor-vnt-10.19.126.0"
}

locals {
  # US South
  ussc = {
    rg       = "1t-ussc-cor-arg-network"
    vnet     = "1t-ussc-cor-vnt-10.19.126.0"
    subnet   = "1t-ussc-cor-sub-ingress-int"
    location = "south central us"
```

3. In **waf_config** section of the file, change the firewall mode as per the request.



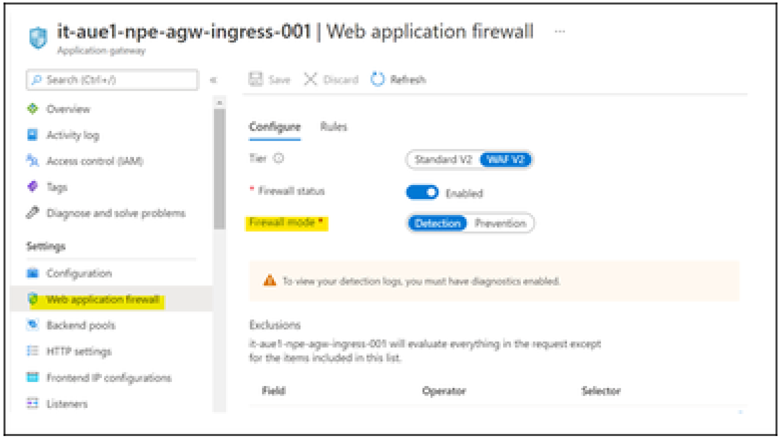
```
    probes = null

  waf_config = {
    firewall_mode            = "Prevention"
    rule_set_type            = "OWASP"
    rule_set_version         = "3.0"
    file_upload_limit_mb     = 100
    max_request_body_size_kb = 128
    exclusions               = {}
  }
 }
}
```

4. After you make the changes in the file, respective workspace workflow will be triggered.

5. Go to the Terraform workspace and apply the changes.

6. To validate the WAF mode, go to Azure portal and open Application Gateway pane based on application name shared in the request.

7. Click on “**Web application firewall**” under **Settings** and check the **Firewall mode**.



it-aue1-npe-agw-ingress-001 | Web application firewall

Application gateway

Tier: Standard V2 [✓ WAF V2]

* Firewall status: Enabled

Firewall mode *: [✓ Detection] Prevention

To view your detection logs, you must have diagnostics enabled.

Exclusions

it-aue1-npe-agw-ingress-001 will evaluate everything in the request except for the items included in this list.

Field	Operator	Selector