SOP Add Azure Firewall Rule

Status of SOP:

Endorsed.

Related Platform	Component
Azure	Azure Firewall

Problem

How to add Azure Firewall rule?

POSSIBLE CAUSE:

- Service request from application team to add a new rule on Azure Firewall

What is Azure Firewall?

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

NATURE OF REQUEST:

A ServiceNow request would be received to add a rule at Azure firewall.

WORKFLOW OF SERVICENOW REQUEST:

1. Once ServiceNow request is received. Open request item (RITM) mentioned in the ServiceNow request. Look for below two items in the request: -

   a). Attachment containing application firewall rules to be implemented.

   b). Application architecture diagram -> This is required to get a view of the current application architecture and how all other rules are implemented.

If the architecture diagram is missing in RITM. Drop an email to requester asking for the same and only then proceed with the request

2. Analyze the requested firewall rules mentioned in RITM for below checkpoints:

   a). Verify if the requested ports are present under "**Azure Firewall Core Rules**" section of the below document. If yes, then implementation is not required. As the core rules mentioned in this section are implemented for all 4 regions in Azure and do not need to be requested by application teams.

   https://spo.bhpbilliton.com/sites/cloud/SitePages/AzureNetworkSegmentation.aspx

   b). Verify that the request is not for any of the ports mentioned below as the following firewall rule requests will be rejected: -

      ** Port 25 SMTP: all traffic in Azure must be encrypted as per Cyber security controls, only ports 465 and 587 encrypted SMTP are allowed.

      ** Port 22 and 3389 remote access to VMs from desktops: CyberArk and Citrix should be used for secure remote access.

      ** Port 1433 direct SQL Server access from desktops: SQL to SQL is allowed but otherwise a jump box must be used for remote administration, no desktop shall access SQL in Azure directly.

      ** Unencrypted MQTT: Only encrypted MQTT is allowed.

Check "Azure Firewall Rule" section of the below doc for more information.

https://spo.bhpbilliton.com/sites/cloud/SitePages/AzureNetworkSegmentation.aspx

PROCESS:

Raise a Normal Change Request

Once all the above required pre checks are performed, open a Normal Change Request, and procure necessary approvals before implementing the change.

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

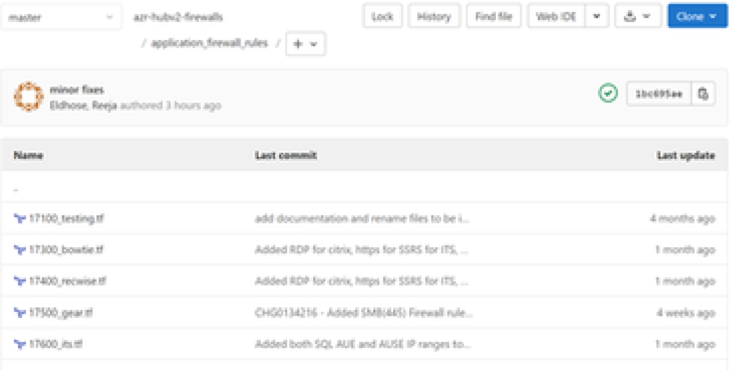
- Cloud Network - Hub Connectivity - Azure

Solution

1. Go to below repository to add the application rule. Different rule files are present under this repository **(FIG 1)**.

https://gitlab.com/bhp-cloudfactory/azure-foundations/azr-hubv2-firewalls/-/tree/master/application_firewall_rules

(FIG 1)



minor fixes
Eldhose, Reeja authored 3 hours ago
1bc695ee

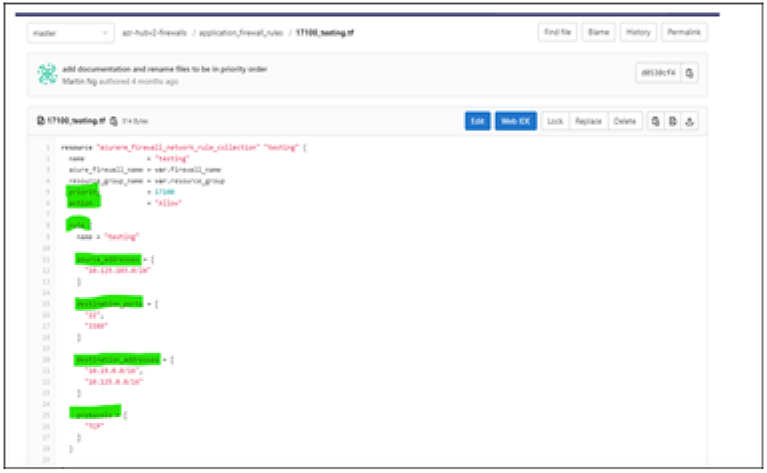
Name	Last commit	Last update
..		
17100_testing.tf	add documentation and rename files to be i...	4 months ago
17300_bowtie.tf	Added RDP for citrix, https for SSRS for ITS, ...	1 month ago
17400_recwise.tf	Added RDP for citrix, https for SSRS for ITS, ...	1 month ago
17500_gear.tf	CHG0134216 - Added SMB(445) Firewall rule...	4 weeks ago
17600_its.tf	Added both SQL AUE and AUSE IP ranges to...	1 month ago

2. Copy one of existing rule files and create a new file with below naming convention:

<priority>_<app name>.tf

For e.g. 1000_abc.tf

3. Open the newly created file and modify the highlighted details as per SNOW request to implement the new rule and save the file.



master
azr-hubv2-firewalls / application_firewall_rules / 17100_testing.tf
Find file
Blame
History
Permalink
Edit
Web IDE
Lock
Replace
Delete

add documentation and rename files to be in priority order
Martin Ng authored 4 months ago

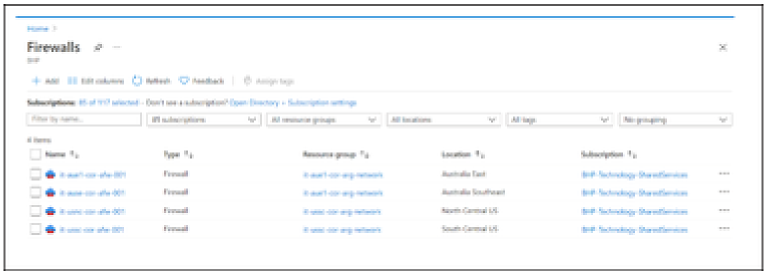
17100_testing.tf

```
resource "azurerm_firewall_network_rule_collection" "testing" {
  name                = "testing"
  azure_firewall_name = var.firewall_name
  resource_group_name = var.resource_group
  priority            = 17100
  action              = "Allow"

  rule {
    name = "testing"

    source_addresses = [
      "10.125.105.0/26"
    ]

    destination_ports = [
      "22",
      "3389"
    ]

    destination_addresses = [
      "10.19.0.0/16",
      "10.125.0.0/16"
    ]

   protocols = [
      "TCP"
    ]
  }
}
```

4. Go to the terraform workspace and trigger the workflow.

5. Once the workflow is successfully triggered, go to the Azure portal to validate the rule.

6. Search for **Firewalls** service on Azure portal. There are four firewalls configured one for each region. Rules will be implemented in all four regions after successful workflow trigger.



Home >

Firewalls

BHP

+ Add | Edit columns | Refresh | Feedback | Assign tags

Subscriptions: 85 of 117 selected – Don't see a subscription? Open Directory + Subscription settings

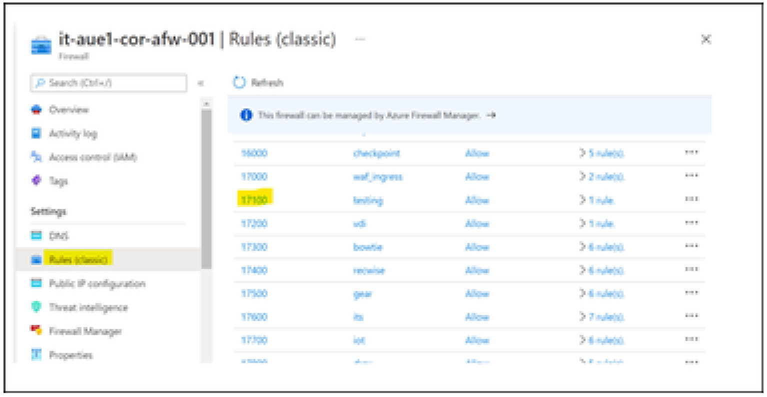
Filter by name... | 85 subscriptions | All resource groups | All locations | All tags | No grouping

4 items

Name	Type	Resource group	Location	Subscription
it-aue1-cor-afw-001	Firewall	it-aue1-cor-arg-network	Australia East	BHP Technology SharedServices
it-aase-cor-afw-001	Firewall	it-aue1-cor-arg-network	Australia Southeast	BHP Technology SharedServices
it-usnc-cor-afw-001	Firewall	it-usnc-cor-arg-network	North Central US	BHP Technology SharedServices
it-ussc-cor-afw-001	Firewall	it-ussc-cor-arg-network	South Central US	BHP Technology SharedServices

7. Click on any of the firewall and then click on **Rules (classic)** under **Settings**. Choose the newly implemented rule **(FIG a).** Azure Firewall rules will be added under "**Network rule collection**" for IP Addresses **Rules (FIG b)**.

FIG (a)



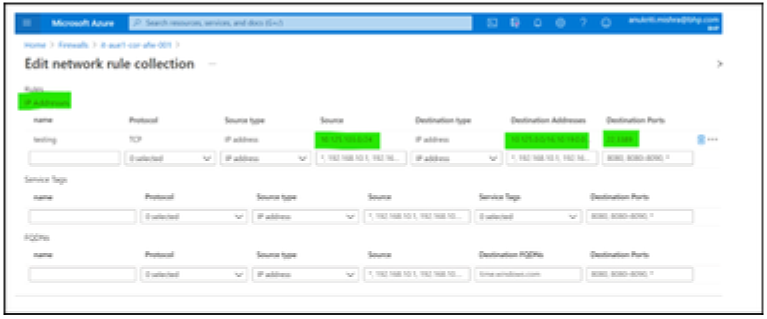
it-aue1-cor-afw-001 | Rules (classic)

Firewall

This firewall can be managed by Azure Firewall Manager. →

16000	checkpoint	Allow	> 5 rule(s).
17000	waf_ingress	Allow	> 2 rule(s).
17100	testing	Allow	> 1 rule.
17200	vdi	Allow	> 1 rule.
17300	bowtie	Allow	> 6 rule(s).
17400	recwise	Allow	> 6 rule(s).
17500	gear	Allow	> 6 rule(s).
17600	its	Allow	> 7 rule(s).
17700	iot	Allow	> 6 rule(s).

FIG (b)



Home > Firewalls > it-aue1-cor-afw-001 >

Edit network rule collection

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addresses	Destination Ports
testing	TCP	IP address	[illegible]	IP address	[illegible]	22, 3389
	0 selected	IP address	*, 192.168.10.1, 192.16...	IP address	*, 192.168.10.1, 192.16...	8080, 8080-8090, *

Service Tags

name	Protocol	Source type	Source	Service Tags	Destination Ports
	0 selected	IP address	*, 192.168.10.1, 192.168.10....	0 selected	8080, 8080-8090, *

FQDNs

name	Protocol	Source type	Source	Destination FQDNs	Destination Ports
	0 selected	IP address	*, 192.168.10.1, 192.168.10....	time.windows.com	8080, 8080-8090, *

8. Once rule is successfully implemented and validated at your end, drop an email to the requester to validate from application point of view.