



Azure Firewall Playbook Document



MANNAI TRADING CO. WLL

Member of Mannai Corporation QPSC

MICROSOFT SOLUTIONS

**Your Complete Guide to
achieve Digital
Transformation**



Contents

1. Overview	3
2. AzureFirewall-BlockIP-addToIPGroup	3
Deployment Instruction	5
Prerequisites	6
Post Deployment	6
3. Firewall connector documentation	6
This connector supports Service Principal Authentication type	6
4. Actions supported by Firewall custom connector	7



1. Overview

Azure Firewall is a cloud-based network security service, sitting at the edge of the Azure virtual network resources, to provide additional security beyond what is offered by NSGs.

This integration allows to automate response to Microsoft Sentinel incidents which contains IPs. It contains the basic connector component, with which you can create your own playbooks that interact with Azure Firewall, Azure Firewall Policy and IP Groups.

2. AzureFirewall-BlockIP-addToIPGroup

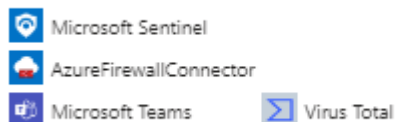
Purpose: This playbook allows blocking/allowing IPs in Azure Firewall. It allows to make changes on IP groups, which are attached to rules, instead of make direct changes on Azure Firewall. It also allows using the same IP group for multiple firewalls.

Type: Sentinel Trigger

Uses: When a new Sentinel incident is created, this playbook gets triggered and performs below actions

1. An adaptive card is sent to the SOC channel providing IP address, Virus Total report, showing list of existing firewalls in the Resource group and providing an option to add IP Address to IPGroups or Ignore.
2. If SOC user confirms yes, the IP Address gets added to IPGroups under IPAddress section and incident will get updates with endpoint information, summary of the action taken and virus total scan report.
3. Else, incident will get updates with endpoint information and summary of the action taken.
4. Update the firewall tags "configuration" as key and "sentinel" as value.
5. Connectors in use

Connectors in use





This is the adaptive card SOC will receive when playbook is triggered:

Flow 5:41 PM

Suspicious IP - Azure Sentinel

Medium Incident Suspicious IP

Incident description

A suspicious activity was detected in the organization. IPs are attached.

[Click here to view the Incident](#)

IP Address : 5.199.130.188

Virus Total Report

Country : DE

Continent : EU

ASN : 24961

As_Owner : myLoc managed IT AG

Total Votes :

Malicious : 3


Positive Votes : 0

Suspicious : 0

Number of reports saying that is Undetected : 10

Network : 5.199.128.0/20

Incident configuration:




Close Azure Sentinel incident?

Close incident - Benign Positive

Change Azure Sentinel incident severity?

Medium

Azure Firewall Actions



Lior Tami (l-tami@microsoft.com) used Power Automate to send this notification. [Learn more](#)

[Add this IP Address to the IP Group](#) [Ignore](#)

Select an IP Group :

Select an option

Sentinel-BlockIP-Group

BlockAccessTo-IPGroup



Comment example:

```
Azure Firewall Playbook performed the following action :-

IP Address : 103.65.202.106

Virus Total Report :

Country : IN
Continent : AS
ASN : 138239
AS_Owner : Vaishnavi Online Internet Services Pvt. Ltd.

Total Votes :-

Malicious : 0
Positives Votes : 0
Negative Votes : 0
Suspicious Votes: 0
Number of reports saying that is Undetected : 0
Network : 103.65.202.0/23

Action Taken in Azure Firewall :-

Added IP Address 103.65.202.106 to the below Azure Firewall Configuration :-

Firewall name : AzureFirewall
Rule Collection name : AzureFirewallDenyCollection
Rule name : Rule2021-03-26T08:07:16Z
```

Deployment Instruction

1. Azure Firewall connector needs to be deployed prior to the deployment of this playbook under the same subscription.
2. Azure Firewall connector need to be authenticated with a Service Principal that has permissions over Azure Firewall.
3. This playbook will query IP Groups that exist in the resource group of Microsoft Sentinel workspace. Make sure to create IP Groups and attach them to Azure Firewall rules prior to running the playbook. You can change the source of the IP groups in the playbook itself after deployment.
4. **Permissions required for this playbook:** This playbook **Gets** and **Updates** IP groups. The registered application/Service Principal that is authenticated to the connector needs to have the following RBAC Roles:
 - **Contributor** on the IP Groups in the Microsoft Sentinel resource group.
5. To use VirusTotal connector, get your Virus Token API key.



Prerequisites

1. Deploy Azure Firewall Logic Apps custom connector (AzureFirewallConnector) under the same resource group.
2. Create IP Groups and attach them to Azure Firewall rules prior to running the playbook
3. Create a Service Principal which the Azure Firewall connector will use, and grant Contributor permissions to it on the IP groups.
4. Assign "Contributor" role of the service principal to AzureFirewallConnector
5. To use VirusTotal connector in this playbook, get your [Virus Total API key](#). Otherwise, erase these steps or replace them with other TI sources.
6. Add Teams connection
7. Teams Group Id and Teams Channel ID required

Post Deployment

Authorize connections

once deployment is complete, you will need to authorize each connection.

1. Click the Microsoft Sentinel connection resource
2. Click edit API connection
3. Click Authorize
4. Sign in
5. Click Save
6. Repeat steps for other connection such as Teams connection and Virus Total (For authorizing the Virus Total API connection, the API Key needs to be provided)
7. Authorize the Azure Firewall custom connector by following the below mentioned steps.
 - a. Navigate to playbook
 - b. Click Edit
 - c. Find the action with the name 'Lists all Azure Firewalls in a resource group', 'Gets the specified Azure Firewall', 'Creates or updates the specified Azure Firewall', 'Updates tags for Azure Firewall resource' in the workflow.
 - d. Click Change connection [Enter Connection name, ClientId, SecretKey and TenantId captured from Microsoft Entra ID.]

3. Firewall connector documentation

This connector supports Service Principal Authentication type.

Microsoft Entra ID Service principal

To use your own application with the Microsoft Sentinel connector, perform the following steps:

1. Register the application with Microsoft Entra ID and create a service principal. Learn how.
2. Get credentials (for future authentication).
3. In the registered application blade, get the application credentials for later signing in:
 - a. Tenant Id: under Overview
 - b. Client ID: under Overview
 - c. Client secret: under Certificates & secrets.
4. Grant permissions to Azure Firewall, IP Groups or Azure Firewall Policies.
 - a. In the relevant resources of the above, go to Settings -> Access control (IAM)



- b. Select Add role assignment.
 - c. Select the role you wish to assign to the application: Contributor role.
 - d. Find the required application and save. By default, Microsoft Entra ID applications aren't displayed in the available options. To find your application, search for the name and select it.
- 5. Authenticate**
6. In this step we use the app credentials to authenticate to the Sentinel connector in Logic Apps.
7. In the custom connector for Azure Firewall, fill in the required parameters (can be found in the registered application blade) - Tenant Id: under Overview - Client Id: under Overview - Client Secret: under Certificates & secrets

4. Actions supported by Firewall custom connector

Component	Description
Create or Update a firewall	Action used to create and update a firewall
Add a new rule	Action used to add new rules.
Add an IP address to an existing rule	Action used to add an IP address to an existing rule of the Firewall.
Update Threat Intel allow list	Update Threat intel allow list of the firewall
Update Tags	Update Tags.
Get Firewall	action used to fetch list of firewall details
List All Azure Firewalls in Subscription	Action used to fetch the details of Azure Firewalls in Subscription.
List Azure Firewalls in Resource Group	Action used to fetch the list of azure Firewall in the resource group.
Get firewall policy information	Action used to fetch the details of firewall policy information.
Deletes the specified Firewall Policy	Action used to delete the specified the firewall policy.
Lists all Firewall Policies in a resource group	Action used to lists all Firewall Policies in a resource group.
Gets all the Firewall Policies in a subscription	Action used to gets all the Firewall Policies in a subscription.
Creates or updates the specified Firewall Policy	Action used to create or updates the specified Firewall Policy.
Gets the specified ipGroups	Action used to gets the specified ipGroups.
Deletes the specified IP Groups	Action used to deletes the specified IP Groups.
Creates or updates an IP Groups in a specified resource group	Action used to create or updates an IP Groups in a specified resource group.
Updates tags of an IpGroups resource	Action used to updates tags of an IpGroups resource.
Gets all IP Groups in a subscription	Action used to gets all IP Groups in a subscription.
Ip Groups - List By Resource Group	Action used to IP Groups - List By Resource Group.