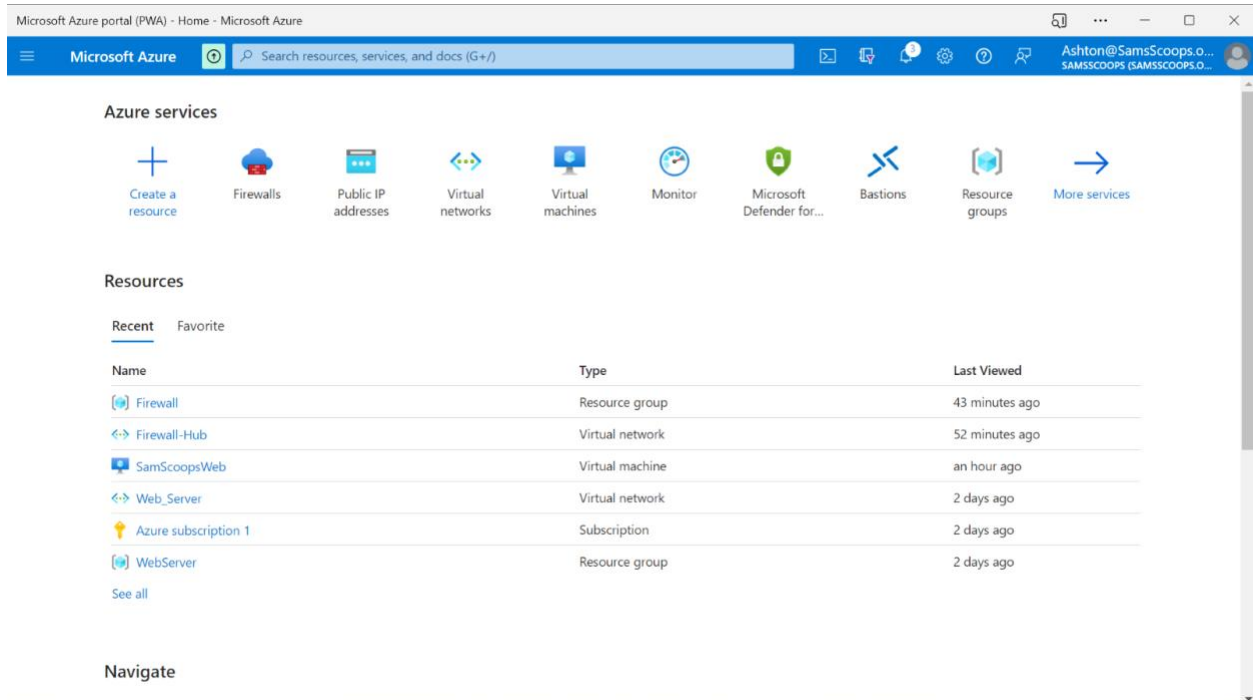


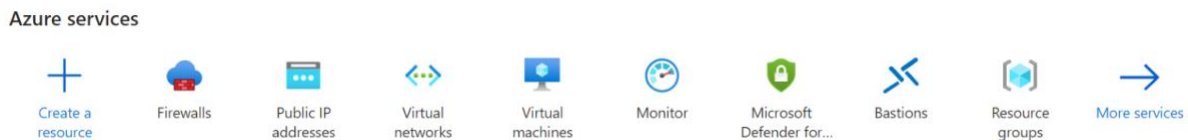
# Azure Firewall Deployment and Configuration

## Step 1: Firewall deployment

1. Sign into your Azure subscription from the [Azure portal](#).



2. On the Azure home page select **Firewalls** under the Azure services bar.



3. Select **Create Firewall**.

Microsoft Azure portal (PWA) - Firewalls - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+/I)

Ashton@SamsScoops.o...  
SAMSSCOOPS (SAMSSCOOPS.O...)

Home >

## Firewalls

SamsScoops (SamsScoops.onmicrosoft.com)


+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals **Azure subscription 1** Resource group equals **all** Location equals **all** Add filter

Showing 0 to 0 of 0 records.

No grouping List view

Name	Type	Resource group	Location	Subscription
------	------	----------------	----------	--------------



**No firewalls to display**

Cloud-native network security to protect your Azure Virtual Network resources

[Create firewall](#)

[Learn more about Azure Firewall](#)

[Give feedback](#)

1. Subscription: Select your subscription.
2. For the resource group, select the **Firewall** resource group from the dropdown, created in the earlier activity.
3. Give the firewall instance the name "ScoopsFirewall".
4. For the region, select the same location that you have used previously.
5. For the Firewall SKU, select **Standard** from the Firewall SKU selection boxes.
6. For Firewall management, select **Use Firewall rules (classic) to manage this firewall**.
7. For **Choose a virtual network**, select **Use existing** and select the **Firewall-Hub** network for the virtual network created in a previous activity.
8. For the Public IP address, select **Add new** and give it the name "FirewallScoops", select **OK**.

Microsoft Azure portal (PWA) - Create a firewall - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Firewalls >

## Create a firewall

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more](#)

**Project details**

Subscription \* Azure subscription 1 (f7b5c2c8-674c-493b-9277-0693ca8d30af)

Resource group \* Firewall [Create new](#)

**Instance details**

Name \* ScoopsFirewall

Region \* West Europe

Availability zone ☯ None

[Review + create](#) [Previous](#) [Next: Tags >](#) [Download a template for automation](#)

Microsoft Azure portal (PWA) - Create a firewall - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Firewalls >

## Create a firewall

**i** Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. [Learn more](#)

**Firewall SKU**

☐ Basic

☒ Standard

☐ Premium

**Firewall management**

☐ Use a Firewall Policy to manage this firewall

☒ Use Firewall rules (classic) to manage this firewall

**Choose a virtual network**

☐ Create new

☒ Use existing

**Virtual network** Firewall-Hub (Firewall)

**Public IP address \*** (New) FirewallScoops [Add new](#)

**Forced tunneling** ☯ ☒ Disabled

[Review + create](#) [Previous](#) [Next: Tags >](#) [Download a template for automation](#)

1. Select **Review + create** then **create**. The firewall will now be deployed.

Microsoft Azure portal (PWA) - Microsoft.AzureFirewall-20230519150219 - Microsoft Azure

Home > Microsoft.AzureFirewall-20230519150219 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Deployment is in progress

Deployment name : Microsoft.AzureFirewall-202305... Start time : 5/19/2023, 3:02:21 PM  
Subscription : Azure subscription 1 (f7b5c2c8-... Correlation ID : 1d58a5fd-3277-40ad-9872-f6a1...  
Resource group : Firewall

Deployment details

Resource	Type	Status	Operation
ScoopsFirewall	Firewall	Created	Operation
FirewallScoops	Public IP address	OK	Operation

Give feedback  
Tell us about your experience with deployment

Microsoft Defender for Cloud  
Secure your apps and infrastructure  
[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials  
[Start learning today >](#)

Work with an expert  
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.  
[Find an Azure expert >](#)

Microsoft Azure portal (PWA) - ScoopsFirewall - Microsoft Azure

Home > Microsoft.AzureFirewall-20230519150219 | Overview

ScoopsFirewall  
Firewall

Search

Migrate to firewall policy Delete Lock Change SKU

Overview

Activity log

Access control (IAM)

Tags

Settings

DNS

Rules (classic)

Public IP configuration

Threat intelligence

Firewall Manager

Properties

Locks

Monitoring

Metrics

Dagnostic settings

Essentials

Resource group (move)  
[Firewall](#)

Location  
West Europe

Subscription (move)  
[Azure subscription 1](#)

Subscription ID  
f7b5c2c8-674c-493b-9277-0693ca8d30af

Virtual network  
[Firewall-Hub](#)

Provisioning state  
Succeeded

Tags (edit)  
[Click here to add tags](#)

Firewall SKU  
[Standard\(change\)](#)

Firewall subnet  
[AzureFirewallSubnet](#)

Firewall public IP  
[FirewallScoops](#)

Firewall private IP  
192.168.1.4

Management subnet  
-

Management public IP  
-

Private IP Ranges  
[IANA RFC 1918](#)

JSON View

## Step 2: Firewall application rules creation

The web server will need access to Google once it is set up, so you need to set up an application rule to allow outbound access. To do this, follow these steps:

1. From the Azure services bar select **Resource groups**.

## Azure services



Microsoft Azure portal (PWA) - Resource groups - Microsoft Azure

Home > **Resource groups**

SamsScoops (SamsScoops.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals **Azure subscription 1** Location equals **all** Add filter

Showing 1 to 6 of 6 records. No grouping List view

<input type="checkbox"/> Name ↑	Subscription ↑↓	Location ↑↓	
<input type="checkbox"/> DefaultResourceGroup-WEU	Azure subscription 1	West Europe	...
<input type="checkbox"/> Firewall	Azure subscription 1	West Europe	...
<input type="checkbox"/> NetworkWatcherRG	Azure subscription 1	West Europe	...
<input type="checkbox"/> ResourceMoverRG-eastus-west europe-ne	Azure subscription 1	North Europe	...
<input type="checkbox"/> ResourceMoverRG-polandcentral-west europe-ne	Azure subscription 1	North Europe	...
<input type="checkbox"/> WebServer	Azure subscription 1	West Europe	...

< Previous Page 1 of 1 Next > Give feedback

1. Open the **Firewall** resource group, and select the **ScoopsFirewall** firewall.

Microsoft Azure portal (PWA) - Firewall - Microsoft Azure

Home > Resource groups > **Resource groups**

SamsScoops (SamsScoops.onmicrosoft.com)

+ Create Manage view Delete resource group Refresh Export to CSV

Filter for any field... Search Add filter More (1)

Showing 1 to 3 of 3 records. ☐ Show hidden types No grouping List view

<input type="checkbox"/> Name ↑	Type ↑↓	Location ↑↓	
<input type="checkbox"/> Firewall-Hub	Virtual network	West Europe	...
<input type="checkbox"/> FirewallScoops	Public IP address	West Europe	...
<input type="checkbox"/> ScoopsFirewall	Firewall	West Europe	...

< Page 1 of 1 >

**Firewall** Resource group

Overview

Activity log Access control (IAM) Tags Resource visualizer Events

**Settings**

Deployments Security Policies Properties Locks

**Cost Management**

Cost analysis Budgets Cost alerts (preview)

**Essentials** JSON View

**Resources** Recommendations (1)

Filter for any field... Type equals **all** Add filter More (1)

Showing 1 to 3 of 3 records. ☐ Show hidden types No grouping List view

<input type="checkbox"/> Name ↑	Type ↑↓	Location ↑↓	
<input type="checkbox"/> Firewall-Hub	Virtual network	West Europe	...
<input type="checkbox"/> FirewallScoops	Public IP address	West Europe	...
<input type="checkbox"/> ScoopsFirewall	Firewall	West Europe	...

< Page 1 of 1 >

1. On the **ScoopsFirewall** page, under **Settings**, select **Rules (classic)**.

Microsoft Azure portal (PWA) - ScoopsFirewall - Microsoft Azure

Home > Resource groups > Firewall > ScoopsFirewall

### ScoopsFirewall | Rules (classic)

Firewall

Search Refresh

This firewall can be managed by Azure Firewall Manager. →

NAT rule collection Network rule collection Application rule collection

+ Add NAT rule collection

Priority	Name	Action	Rules
No results			

When a DNAT rule is matched, an implicit corresponding network rule to allow the translated traffic is added. [Learn more](#)

1. Select the **Application rule collection** tab.

Microsoft Azure portal (PWA) - ScoopsFirewall - Microsoft Azure

Home > Resource groups > Firewall > ScoopsFirewall

### ScoopsFirewall | Rules (classic)

Firewall

Search Refresh

This firewall can be managed by Azure Firewall Manager. →

NAT rule collection Network rule collection Application rule collection

+ Add application rule collection

Priority	Name	Action	Rules
No results			

Azure infrastructure application rule collection is enabled by default. [Learn more](#)

1. Select **Add application rule collection**.
2. For **Name**, type "AppRule1".
3. For **Priority**, type "200".
4. For **Action**, select **Allow**.
5. Under **Rules**, **Target FQDNs**, for **Name**, type "Allow-Google".
6. For **Source type**, select **IP address**.

7. Type **172.16.1.0/24** for the source.
8. For **Protocol:port**, type "http, https".
9. For **Target FQDNS**, type "www.google.com".

Microsoft Azure portal (PWA) - Add application rule collection - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+)

Ashton@SamsScoops.o... SAMSSCOOPS (SAMSSCOOPS.O...)

Home > Resource groups > ScoopsFirewall

### Add application rule collection

Name \* AppRule1 ✓

Priority \* 200 ✓

Action \* Allow ✓

Rules

FQDN tags

name	Source type	Source	FQDN tags
	IP address	*, 192.168.10.1, 192.168.10.0/24, 192.1...	0 selected

! FQDN tags may require additional configuration. [Learn more](#)

Target FQDNs

name	Source type	Source	Protocol:Port	Target FQDNs
Allow-Google ✓	IP address	172.16.1.0/24 ✓	http, https ✓	www.google.com ✓
	IP address	*, 192.168.10.1, 192.168.10.0/...	http, http:8080, https, mssql:...	www.microsoft.com, *microso...

! mssql: SQL should be enabled in proxy mode. This may require additional configuration. [Learn more](#)

**Add**

1. Select **Add** and after a short time the rule will be created.

Microsoft Azure portal (PWA) - ScoopsFirewall - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+)

Ashton@SamsScoops.o... SAMSSCOOPS (SAMSSCOOPS.O...)

Home > Resource groups > Firewall > ScoopsFirewall

### ScoopsFirewall | Rules (classic)

Overview Activity log Access control (IAM) Tags Settings DNS Rules (classic) Public IP configuration Threat intelligence Firewall Manager Properties Locks Monitoring Metrics Diagnostic settings

« Refresh

NAT rule collection Network rule collection Application rule collection

+ Add application rule collection

Priority	Name	Action	Rules
200	AppRule1	Allow	> 1 rule. ...

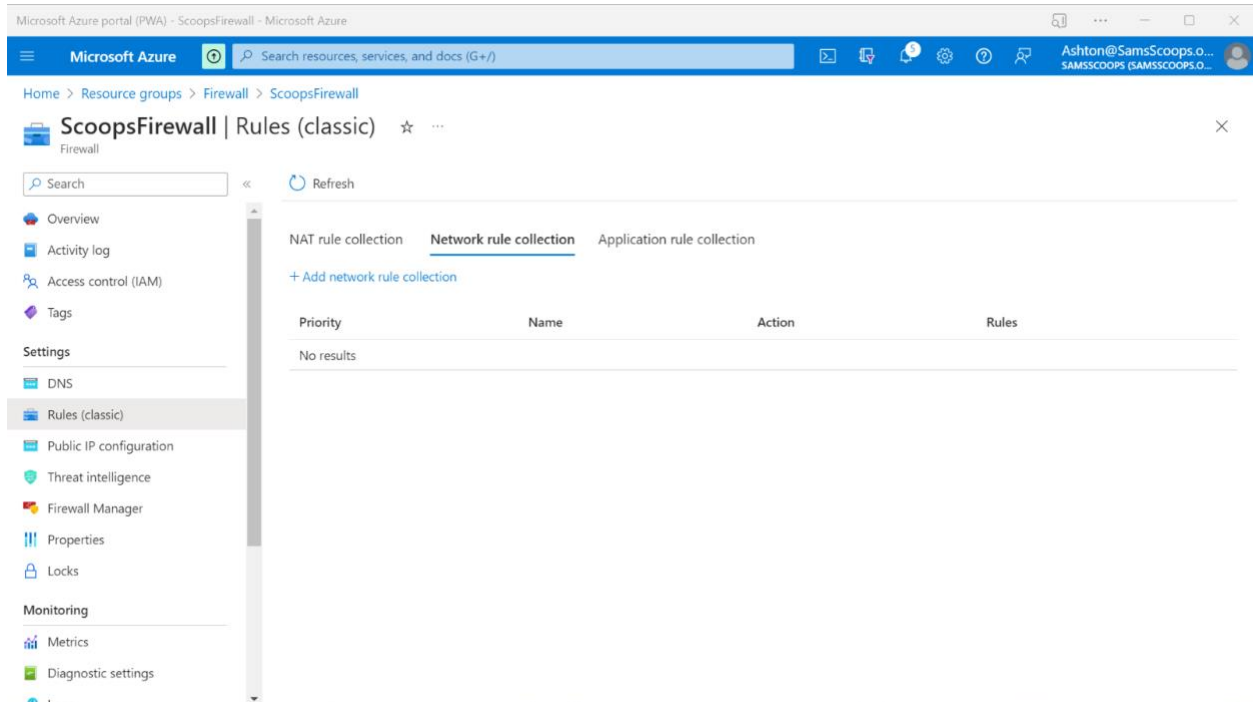
! Azure infrastructure application rule collection is enabled by default. [Learn more](#)

## Step 3: Firewall network rule creation



The web server will also need to use DNS to resolve IP addresses so you need to create a network rule to allow this. Follow these steps to do this:

1. Select the **Network rule collection** tab.
2. Select **Add network rule collection**.



1. For **Name**, type "Net-Rule1".
2. For **Priority**, type "200".
3. For **Action**, select **Allow**.
4. Under **Rules**, **IP addresses**, for **Name**, type "Allow-DNS".
5. For **Protocol**, select **UDP**.
6. For **Source type**, select **IP address**.
7. Type **172.16.1.0/24** for the **Source**.
8. For **Destination type** select **IP address**.
9. For **Destination address**, type **209.244.0.3,209.244.0.4** (These are public DNS servers operated by Level3).
10. For **Destination Ports**, type "53".



Microsoft Azure portal (PWA) - Add network rule collection - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+)

Ashton@SamsScoops.o... SAMSSCOOPS (SAMSSCOOPS.O...)

Home > Resource groups > ScoopsFirewall

## Add network rule collection

Name \* Net-Rule1 ✓

Priority \* 200 ✓

Action \* Allow ✓

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addr...	Destination Ports
Allow-DNS ✓	UDP ✓	IP address ✓	172.16.1.0/24 ✓	IP address ✓	209.244.0.3,209.2... ✓	53 ✓
	0 selected ✓	IP address ✓	*, 192.168.10.1, 192... ✓	IP address ✓	*, 192.168.10.1, 192... ✓	8080, 8080-8090, *

Service Tags

name	Protocol	Source type	Source	Service Tags	Destination Ports
	0 selected ✓	IP address ✓	*, 192.168.10.1, 192.168... ✓	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... ✓	time.windows.com ✓	8080, 8080-8090, *

Add

### 1. Select **Add**.

Microsoft Azure portal (PWA) - ScoopsFirewall - Microsoft Azure

Microsoft Azure Search resources, services, and docs (G+)

Ashton@SamsScoops.o... SAMSSCOOPS (SAMSSCOOPS.O...)

Home > Resource groups > Firewall > ScoopsFirewall

## ScoopsFirewall | Rules (classic)

Overview

Activity log

Access control (IAM)

Tags

Settings

DNS

Rules (classic)

Public IP configuration

Threat intelligence

Firewall Manager

Properties

Locks

Monitoring

Metrics

Diagnostic settings

Log

Refresh

Updating firewall

NAT rule collection Network rule collection Application rule collection

+ Add network rule collection

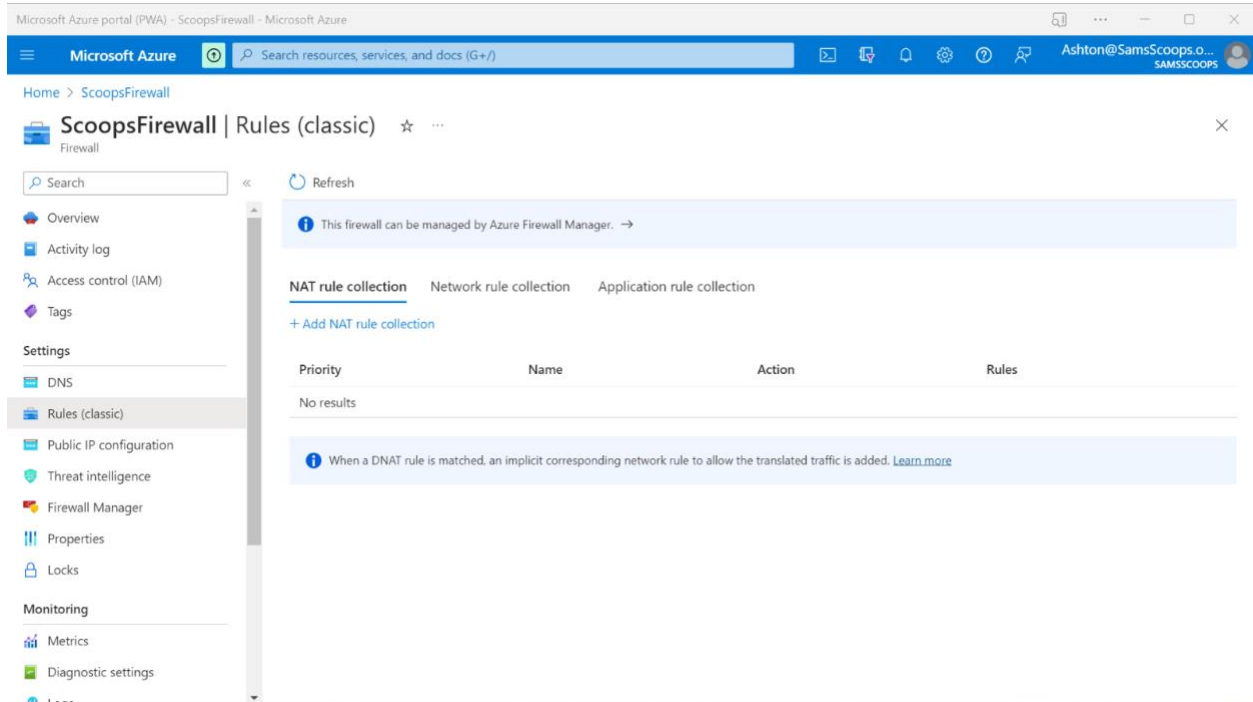
Priority	Name	Action	Rules
200	Net-Rule1	Allow	> 1 rule. ...

## Step 4: Firewall NAT rules creation

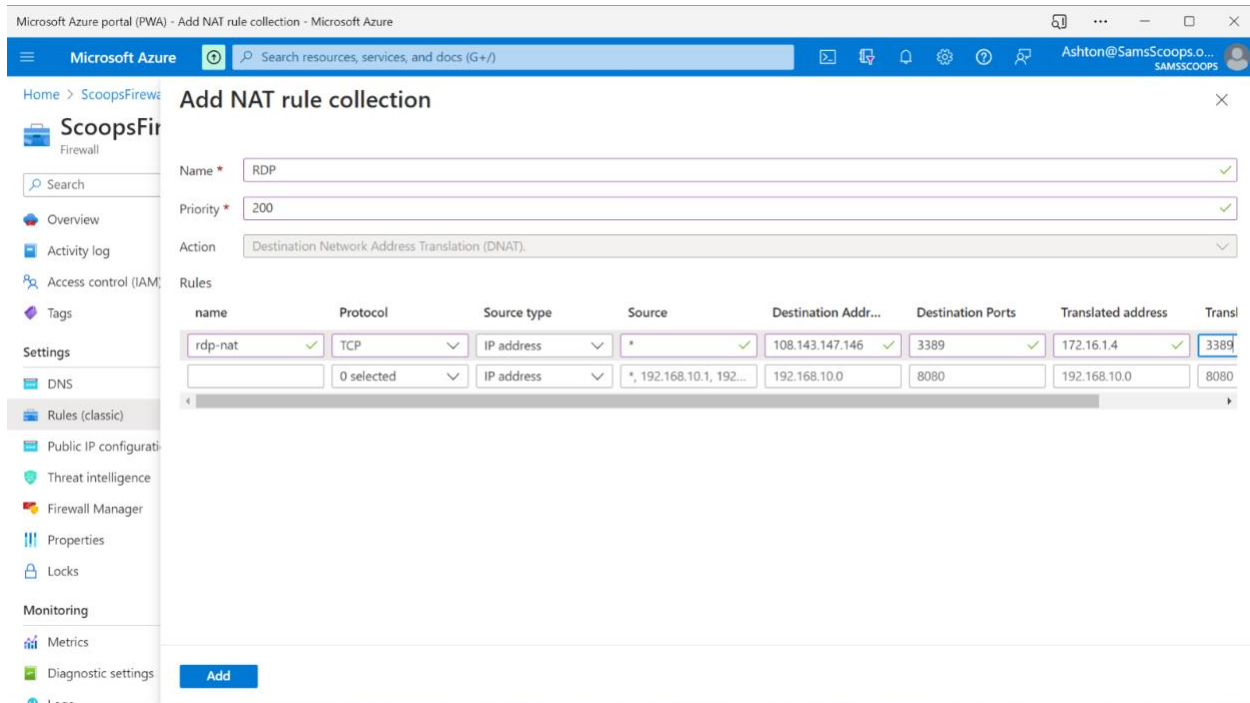
To allow the web developer to set up the web server you need to provide remote access to the VM. Follow these steps to create a destination NAT rule for RDP:

### 1. Select the **NAT rule collection** tab.

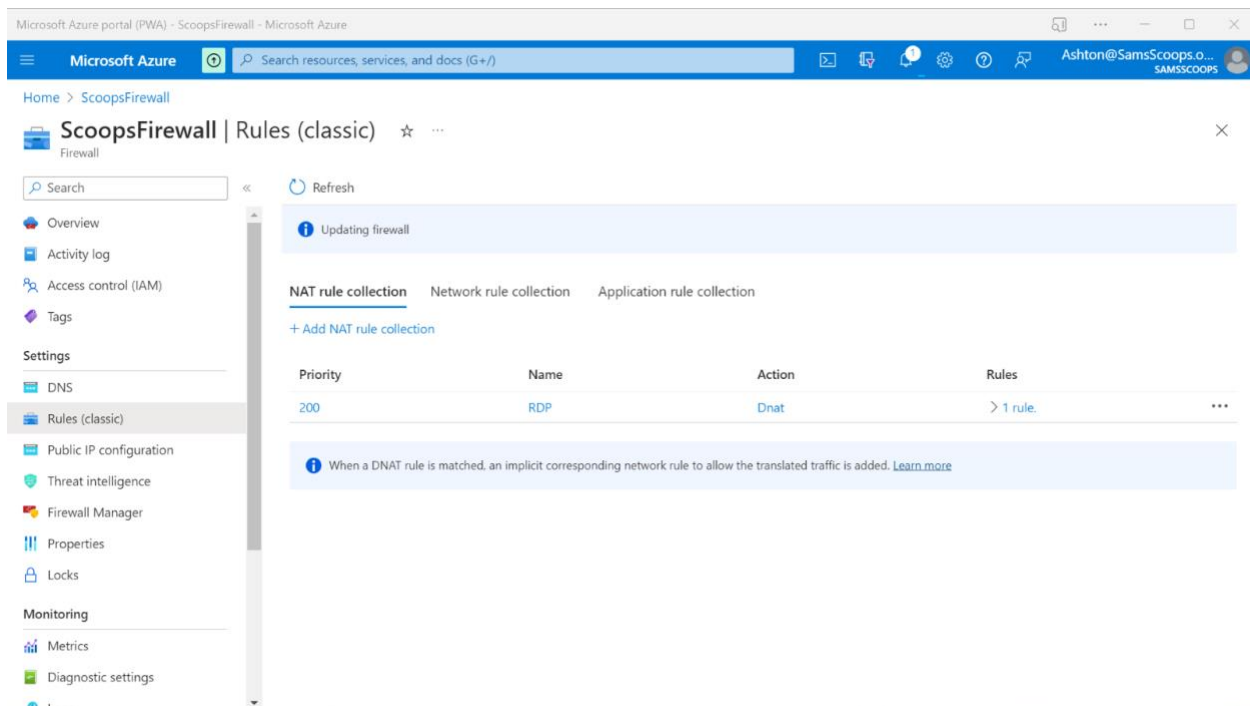
## 2. Select **Add NAT rule collection**.



1. For **Name**, type "rdp".
2. For **Priority**, type "200".
3. Under **Rules**, for **Name**, type "rdp-nat2".
4. For **Protocol**, select **TCP**.
5. For **Source type**, select **IP address**.
6. Type ".\*(\* = anything)" for the **Source**.
7. For **Destination address**, type the firewall public IP address.
8. For **Destination Ports**, type "3389".
9. For **Translated address**, type the **SamScoopsWeb** virtual machines private IP address.
10. For **Translated port**, type "3389".



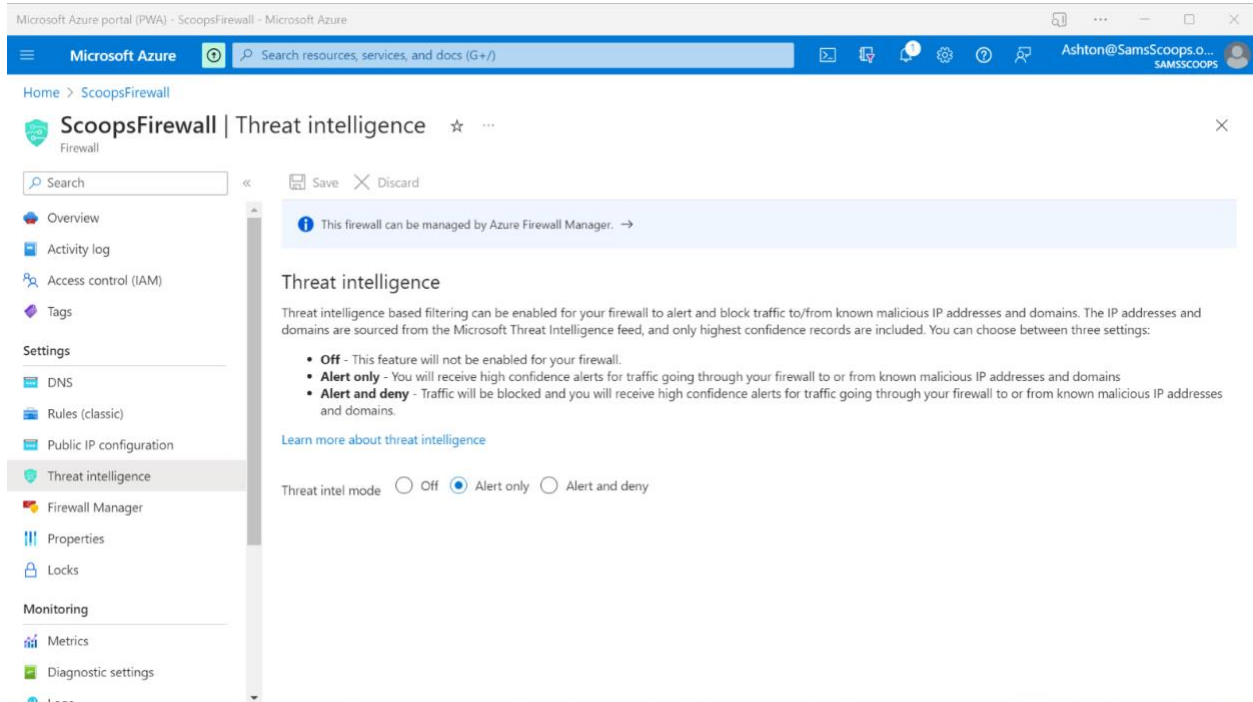
1. Select **Add**.



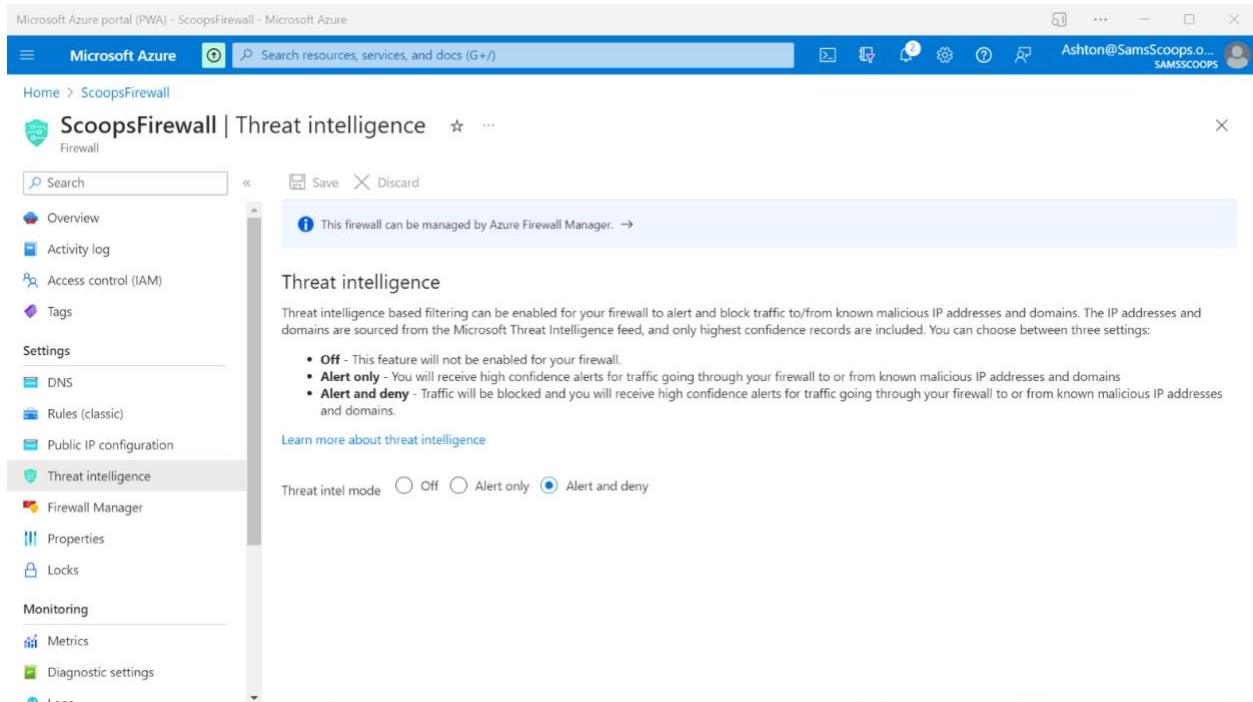
## Step 5: Advanced threat protection

Earlier you learned that one of the great advantages of using the Azure Standard Firewall is that you can create rules automatically for threat using Threat Intelligence. By default the firewall is set to only create threat alerts. Follow these steps to enable the alert and deny option.

1. On the **ScoopsFirewall** page, under **Settings**, select **Threat intelligence**.



1. For **Threat intel mode** select **Alert and deny**.



1. Select **Save**.

