

TASKS:

1. Do – I did create a resource group in the west europe location with the name “CSNetworkSec”.

Why – Usually to keep things under control and a place to put the resources in.

Outcome – The resource group were successfully created as shown in the picture above as im in its overview page and displaying the location as well.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with various tabs and a search bar. Below it, the main title is 'CSNetworkSec' under 'Resource group'. On the left, there's a sidebar with links like 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings', 'Cost Management', 'Monitoring', 'Automation', and 'Help'. The main content area has a section titled 'Essentials' with details: 'Subscription (move) : Azure for Students', 'Subscription ID : 84a03b43-9060-460a-b879-35e6745cd249', 'Tags (edit) : Add tags', 'Deployments : No deployments', and 'Location : West Europe'. Below this, there's a 'Resources' section with a 'Filter for any field...' dropdown set to 'Type equals all' and 'Location equals all'. A large central area displays a message: 'No resources match your filters' with a link 'Try changing or clearing your filters.' Below this are 'Create' and 'Clear filters' buttons. At the bottom, there's a status bar with icons and the date/time '10:03 2025-11-12'.

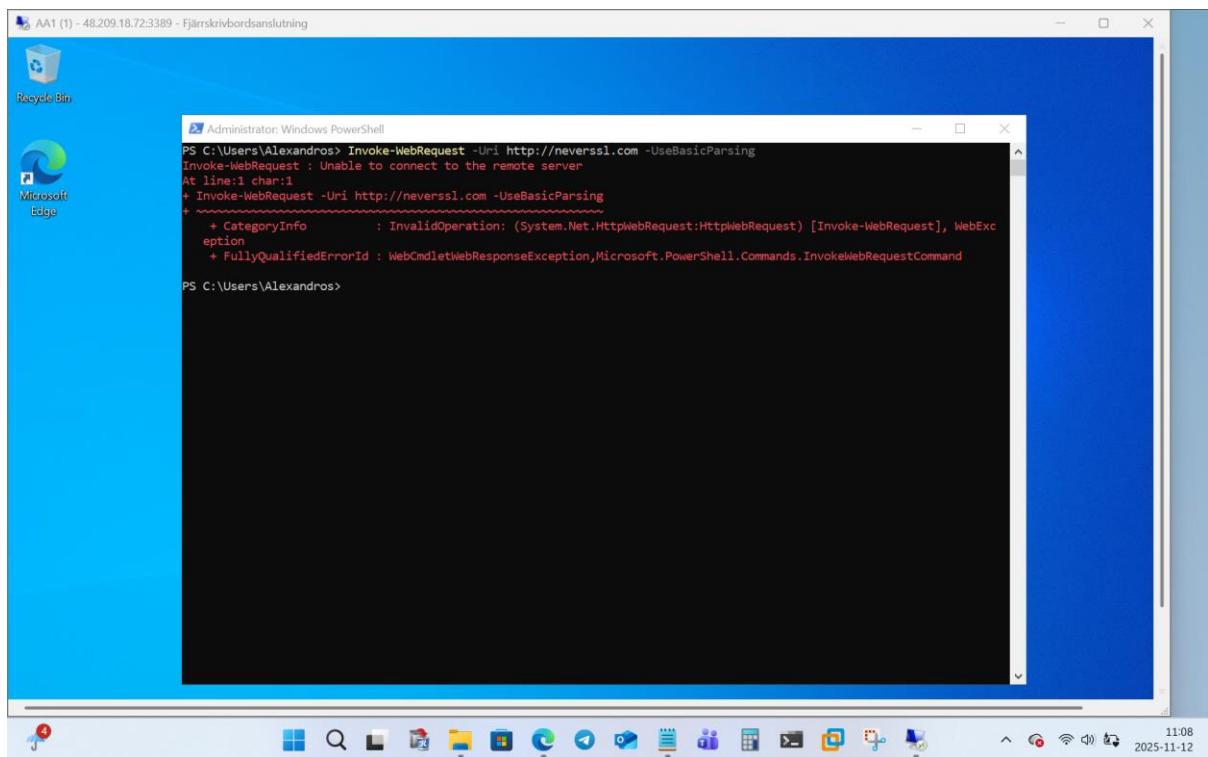
2. Now i have created a virtual network which is named accordingly “vnet-sec” as well the three subnets, “WebSubnet”, “AzureFirewallSubnet”, “AzureFirewallManagementSubnet”. The subnets is used to function as a seperator between the traffic inside as a company with different departments and is making sure everything is working. As i validated the names of the subnets the WebSubnet was fine but when i put in the Firewall names it automatically showed /26 prefix and the names werent functioning without making it as a firewall as well as a firewall management. But all thre were created fine and the firewall subnets were automatically put into the size of prefix /26 as expected for Azure Firewall deployments. Also the azure firewall is requiring two subnets reserved to differentiate between firewall traffic and management operations.

3. I made a VM called AA1 with the image of windows server 2022 inside the subnet of WebSubnet that is located in the virtual network created before (vnet-sec). The virtual machine has to have a public IP address to make sure it can connect to using RDP (remote desktop protocol) in the lab environment so i can try out the firewall and network configurations. In the overview page of the VM it can show that it's up and running as well as its IP address and name and network specifications.

4. I made two inbound security rules in my newly created NSG AA-nsg. One is allowing RDP (TCP 3389) from my IP the other one to deny HTTP (TCP 80) from any source. The NSG in the subnet is going to provide base traffic filtering for all the resources created in that specific subnet. I am expecting to be able to connect to the VM through RDP as well as denying every request on HTTP.

Priority ↑	Name	Port ↑	Protocol	Source ↑	Destination ↑	Action ↑
100	AllowRDP	3389	TCP	93.45.65.151	Any	Allow
200	DenyHTTP	80	TCP	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

5. I connected to the VM through RDP and then went into powershell and typed the command provided in the text and the NSG rule which were supposed to deny port 80 blocked the HTTP connection as it should. I saw an error that said the connection failed which confirmed to me that the rule is in place and working fine as it should.



6. I created Azure Firewall with the provided name “azfw-sec” with the firewall policy (fp-sec) also two IP addresses one for management and the other one for data. A basic SKU needs their own management subnet so it can manage all the updates and configurations on its own. I then saw the firewalls private IP address to the use it later on when making the route table for the outbound traffic.

Setting	Value
Resource group	CSNetworkSec
Location	West Europe
Subscription	Azure for Students
Subnet	AzureFirewallSubnet
Public IP	pip-fw-sec
Private IP	10.0.10.4
Management subnet	AzureFirewallManagementSubnet
Management public IP	pip-fw-mgmt
Private IP Ranges	Managed by Firewall Policy
Route Server (preview)	Add

7. I made an application rule collection called app-https-only within the firewall policy (fp-sec) which is allowing outbound traffic HTTPS from the WebSubnet to all destinations. The collection is making sure that only encrypted and secured web connections are being made and approved. As i only accepted the HTTPS rule and not accepted the HTTP so all unsafe traffic is being denied as a standard. Which is making sure that everything is secure, i assume that the outbound HTTPS requests is going to work out fine while HTTP will not succeed which is showing the rule in action.

Rule Collection P..	Rule collection n...	Rule name	Source	Protocol	Destination	Action	Inherited fr
<input type="checkbox"/>	100	app-https-only	allow-https-any	10.0.1.0/24	Https:443	Allow	

8. I made a route table with the name of rt-web within the CSNetworkSec RG and made a default route of 0.0.0.0/0 and pointing to the private ip of the firewall as the next hop that i wrote down before. After that i associated it with the subnet (WebSubnet) so all of the outbound traffic in the VM is now passing through the firewall. Now i will see the route and proving that everything with the traffic is secure through the firewall.

The screenshot shows the Microsoft Azure portal interface. The URL is https://portal.azure.com/#@anastassiadisalexoutlook.onmicrosoft.com/resource/subscriptions/84a03b43-9060-460a-b879-35e6745cd249/. The page title is "rt-web - Microsoft Azure". The left sidebar shows the route table configuration with sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (Configuration, Routes, Subnets, Properties, Locks), Monitoring, Automation, and Help. The main content area displays the "Essentials" section with resource group, location, and subscription details. Below this is a table for "Routes" with one entry: default-to-fw (Address prefix: 0.0.0.0/0, Next hop type: Virtual appliance, Next hop IP address: 10.0.10.4). There is also a table for "Subnets" with one entry: WebSubnet (Address range: 10.0.1.0/24, Virtual network: vnet-sec, Security group: AA-nsg).

- Now the traffic is routed through the Azure Firewall that is inspecting and looking at connections more thorough and the firewall policy is allowing HTTPS because of the rule we created before that is ensuring safe traffic. When I tested it in the PowerShell it shows that HTTP request to the neverssl.com failed at the same time as HTTPS request to google.com went perfectly fine.

```

AAI (4) - 48.209.18.72:3389 - Fjärrskrivbordsanslutning
Administrator: Windows PowerShell
Administrator: PS C:\Users\Alexandros> Invoke-WebRequest -Uri http://neverssl.com -UseBasicParsing
Invoke-WebRequest : Unable to connect to the remote server
At line:1 char:1
+ Invoke-WebRequest -Uri http://neverssl.com -UseBasicParsing
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+ FullyQualifiedErrorMessage : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS C:\Users\Alexandros> Invoke-WebRequest -Uri https://neverssl.com -UseBasicParsing

StatusCode       : 200
StatusDescription : OK
Content          : <html>
                    <head>
                        <title>NeverSSL - Connecting ... </title>
                        <style>
                            body {
                                font-family: Montserrat, helvetica, arial, sans-serif;
                                font-size: 16px;
                                color: #444444;
                                margin: 0;
                            }
                            h2 {
                                ...
                            }
                    
```

The PowerShell window shows two commands. The first command, `Invoke-WebRequest -Uri http://neverssl.com -UseBasicParsing`, fails with an error message: "Invoke-WebRequest : Unable to connect to the remote server". The second command, `Invoke-WebRequest -Uri https://neverssl.com -UseBasicParsing`, succeeds, returning the HTML content of the NeverSSL website. The content includes the title "NeverSSL - Connecting ...", a style block for the body, and a header section with various HTTP headers like Upgrade, Connection, Vary, Keep-Alive, Accept-Encoding, Accept-Ranges, Content-Length, and Content-Type.

10. I enabled a logging diagnostics on the firewall azfw-sec and then sent the application rule logs and the network rule logs to a log analytic workspace i created called LAW-sec. The logs record is proving how firewall is making policies stronger in real time use even if it worked or not for me. I ran the query and tried different queries with the help of AI to test if something is working but i read that it can take some time to process so. Although it didn't work i was expecting to see all the denying entry point for HTTP traffic as well as the allowance for HTTPS that it was going to confirm that the firewall successfully block HTTP and allow HTTPS.

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The left sidebar lists navigation options: Home, Log Analytics workspaces, LAW-sec (selected), Standardkatalog (anastassiadisalexoutlook.onmicrosoft.com), Create, Open recycle bin, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs (selected), Resource visualizer, Settings, Classic, Monitoring, Automation, and Help. A search bar at the top right contains the placeholder 'Search resources, services, and docs (G+)'. Below the search bar is a 'New Query' button with the text 'Run' and a dropdown menu showing 'Time range: Last 7 days', 'Show: 1000 results', and 'KQL mode'. The main content area displays a KQL query:

```

1 | AzureDiagnostics
2 | where ResourceType == "AZUREFIREWALLS"
3 | sort by TimeGenerated desc
4 | take 50
    
```

The results section indicates 'No results found from the last 7 days. Try selecting another time range. Review the query details for more information.' The bottom status bar shows '0s 589ms' and 'Query details'.

Screenshots of RG overview page and activity logs below:

Microsoft Azure

Resource groups < CSNetworkSec

You are viewing a new version of Browse experience. Click here to access the old experience.

Name ↑

- CSNetworkSec
- LogAnalyticsDefaultResources
- NetworkWatcherRG

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

Showing 1 - 3 of 3. Display count: auto

Search resources, services, and docs (G+)

Export resource groups using Bicep or Terraform +2

Overview

Essentials

Resources Recommendations

Filter for any field... Type equals all Location equals all + Add filter

Name	Type	Location
AA-nsg	Network security group	West Europe
AA1	Virtual machine	West Europe
AA1-ip	Public IP address	West Europe
AA1-nsg	Network security group	West Europe
aa1793_z3	Network interface	West Europe
AA1_OsDisk_1_9341eb2e8ef4469a1c581a565c01b08	Disk	West Europe
azfw-sec	Firewall	West Europe
fp-sec	Firewall Policy	West Europe
LAW-sec	Log Analytics workspace	West Europe
pip-fw-mgmt	Public IP address	West Europe

Showing 1 - 10 of 13. Display count: auto

Give feedback

https://portal.azure.com/#resource/subscriptions/84a03b43-9060-460a-b879-35e6745cd249... using Ctrl+Shift+F

13:20 2025-11-12

Microsoft Azure

Resource groups < CSNetworkSec

You are viewing a new version of Browse experience. Click here to access the old experience.

Name ↑

- CSNetworkSec
- LogAnalyticsDefaultResources
- NetworkWatcherRG

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

Showing 1 - 3 of 3. Display count: auto

Search resources, services, and docs (G+)

Export resource groups using Bicep or Terraform +2

Overview

Essentials

Resources Recommendations

Filter for any field... Type equals all Location equals all + Add filter

Name	Type	Location
pip-fw-sec	Public IP address	West Europe
rt-web	Route table	West Europe
vnet-sec	Virtual network	West Europe

Showing 11 - 13 of 13. Display count: auto

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

13:20 2025-11-12

The screenshot shows the Azure Activity log for the 'CSNetworkSec' resource group. The log lists 26 entries, all of which are successful ('Succeeded'). The operations include creating or updating resources, validating deployments, and creating or updating virtual machines. Most of these actions were performed by the user 'anastassiadisalex' on Wednesday, November 1, 2025. The log also includes a few entries from 'Azure for Students'.

Action	Details	Time	User
Create or update re	Succeeded	12 minutes ...	Wed Nov 1... Azure for Students
Create or update re	Succeeded	17 minutes ...	Wed Nov 1... Azure for Students
Create Deployment	Succeeded	19 minutes ...	Wed Nov 1... Azure for Students
Validate Deployment	Succeeded	19 minutes ...	Wed Nov 1... Azure for Students
Create or Update V	Succeeded	23 minutes ...	Wed Nov 1... Azure for Students
Create or Update V	Succeeded	30 minutes ...	Wed Nov 1... Azure for Students
Create or Update V	Succeeded	30 minutes ...	Wed Nov 1... Azure for Students
Create or Update V	Succeeded	31 minutes ...	Wed Nov 1... Azure for Students
Create or Update R	Succeeded	33 minutes ...	Wed Nov 1... Azure for Students
Health Event Resolv	Resolved	33 minutes ...	Wed Nov 1... Azure for Students
Restart Virtual Mac	Succeeded	33 minutes ...	Wed Nov 1... Azure for Students
Create or Update V	Succeeded	41 minutes ...	Wed Nov 1... Azure for Students
Create or Update R	Succeeded	41 minutes ...	Wed Nov 1... Azure for Students
Validate Deployment	Succeeded	43 minutes ...	Wed Nov 1... Azure for Students
Validate Deployment	Succeeded	43 minutes ...	Wed Nov 1... Azure for Students
Create or Update F	Succeeded	46 minutes ...	Wed Nov 1... Azure for Students
Creates or updates	Succeeded	47 minutes ...	Wed Nov 1... Azure for Students
			NFV Resource Provider

Summary:

NSG (Network Security Groups) is a basic subnet filtering that is able to control both inbound and outbound traffic that is based on either ports, IP addresses or even protocols. The azure firewall is different and much more advanced and better with protection. If the NSG is more of a first layer defense with the virtual network the firewall is the rest that is more advanced and deeper filtering for the traffic. Im taking away from the logs and the test environment that NSG is able to allow or block the traffic by different ports, although the firewall is by itself and even more thorough safety by putting HTTPS only filtering into play and also to know everytime a connection or likewise is being made. So it's fair to say that together they build a pretty solid security plan that is a defense in depth kind of thing with multiple layers.

