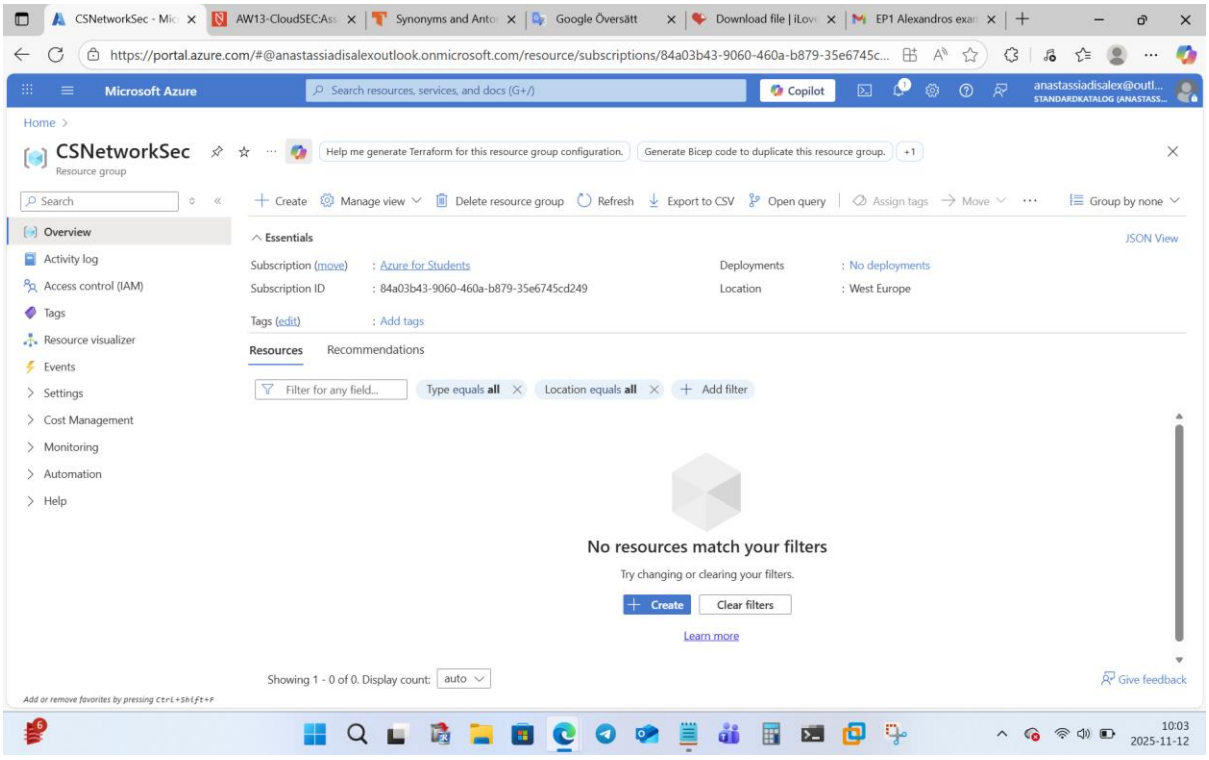
TASKS:

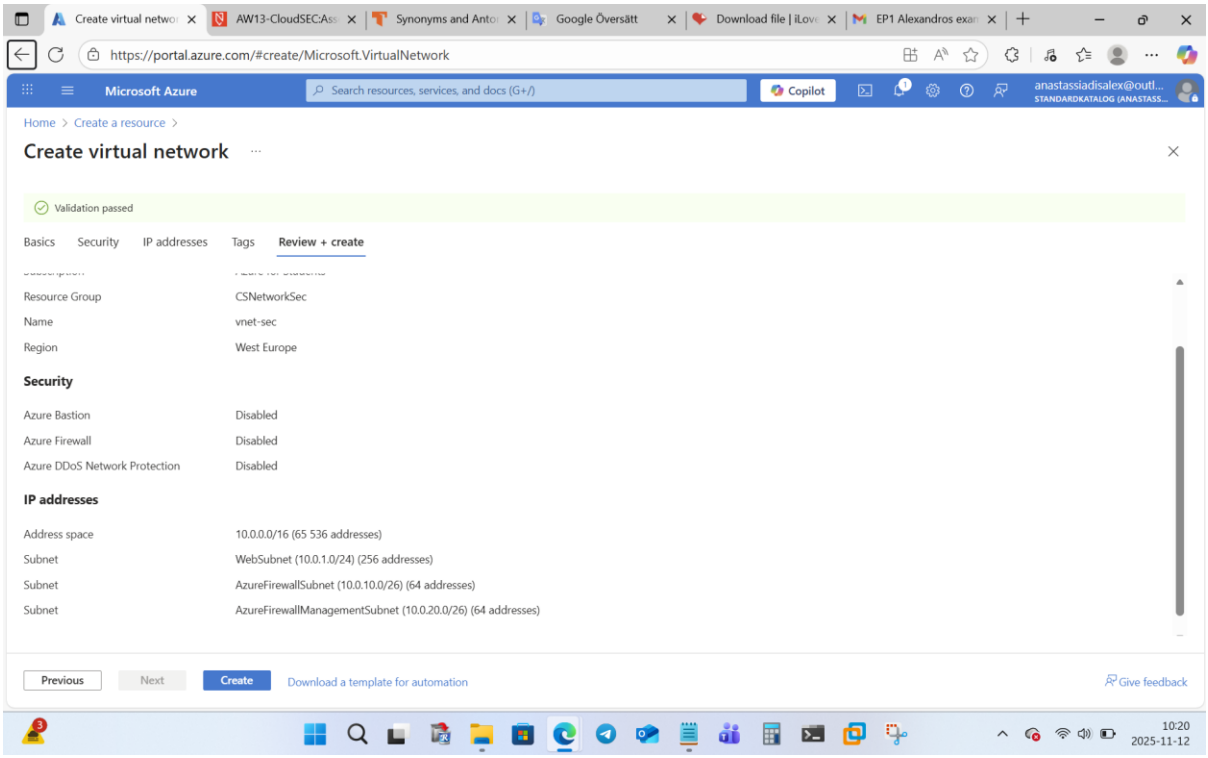
1. Do – I did create a resource group in the west europe location with the name “CSNetworkSec”.

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

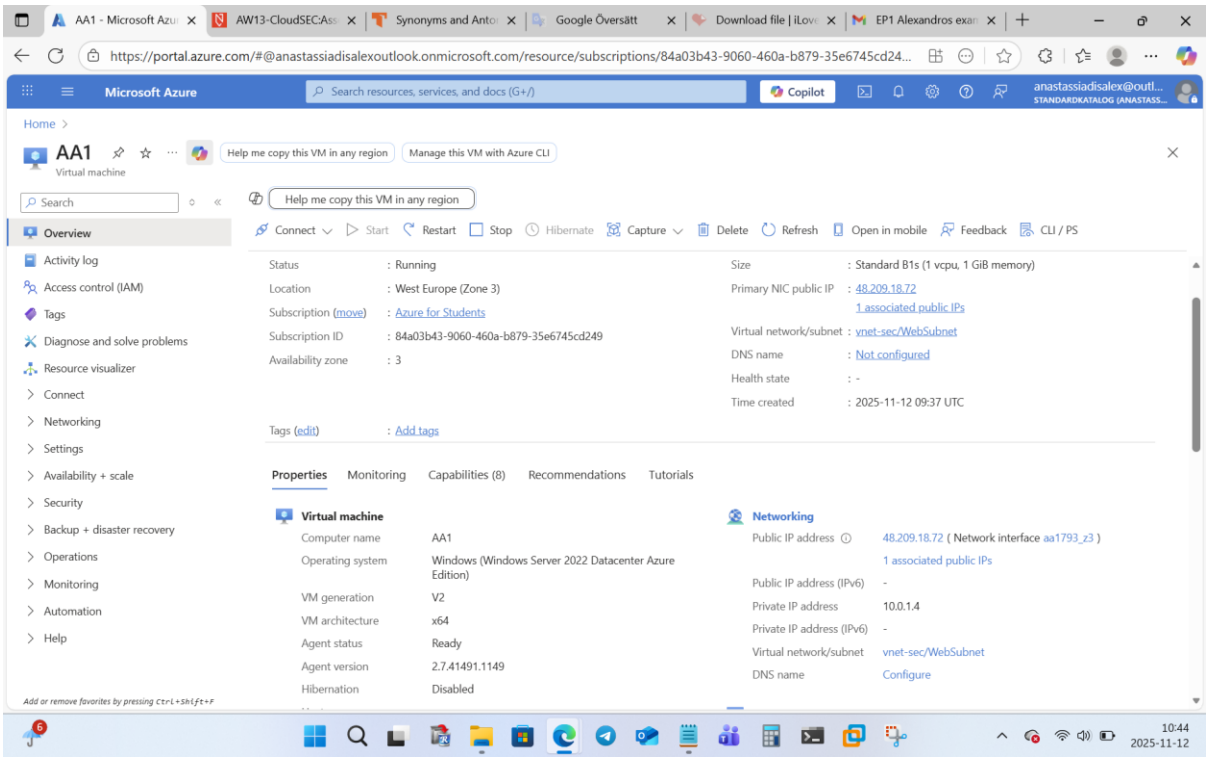
   Outcome – The resource group were successfully created as shown in the picture above as im in its overview page and displaying the location as well.



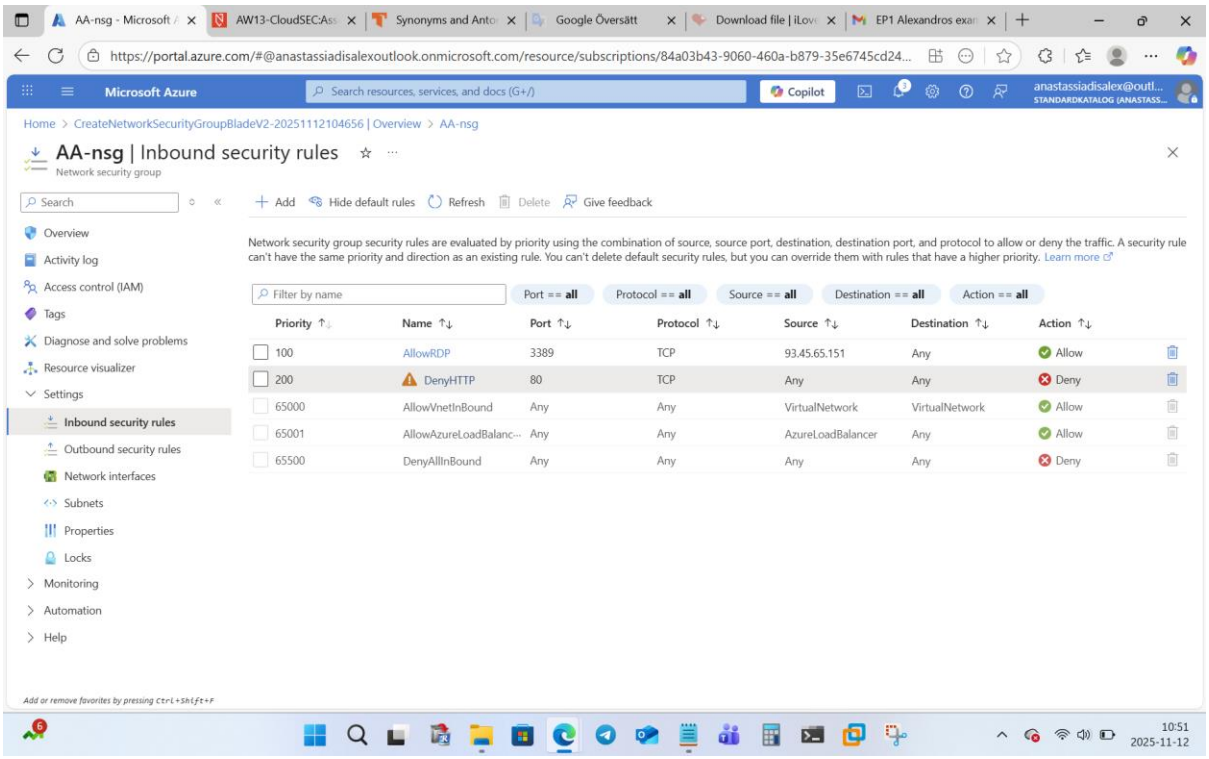
2. Now i have created a virtual network which is named accordingly “vnet-sec” as well the three subnets, “WebSubnet”, “AzureFirewallSubnet”, “AzureFirewallManagementSubnet”. The subnets is used to function as a seperator between the traffic inside as a company with different departments and is making 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.



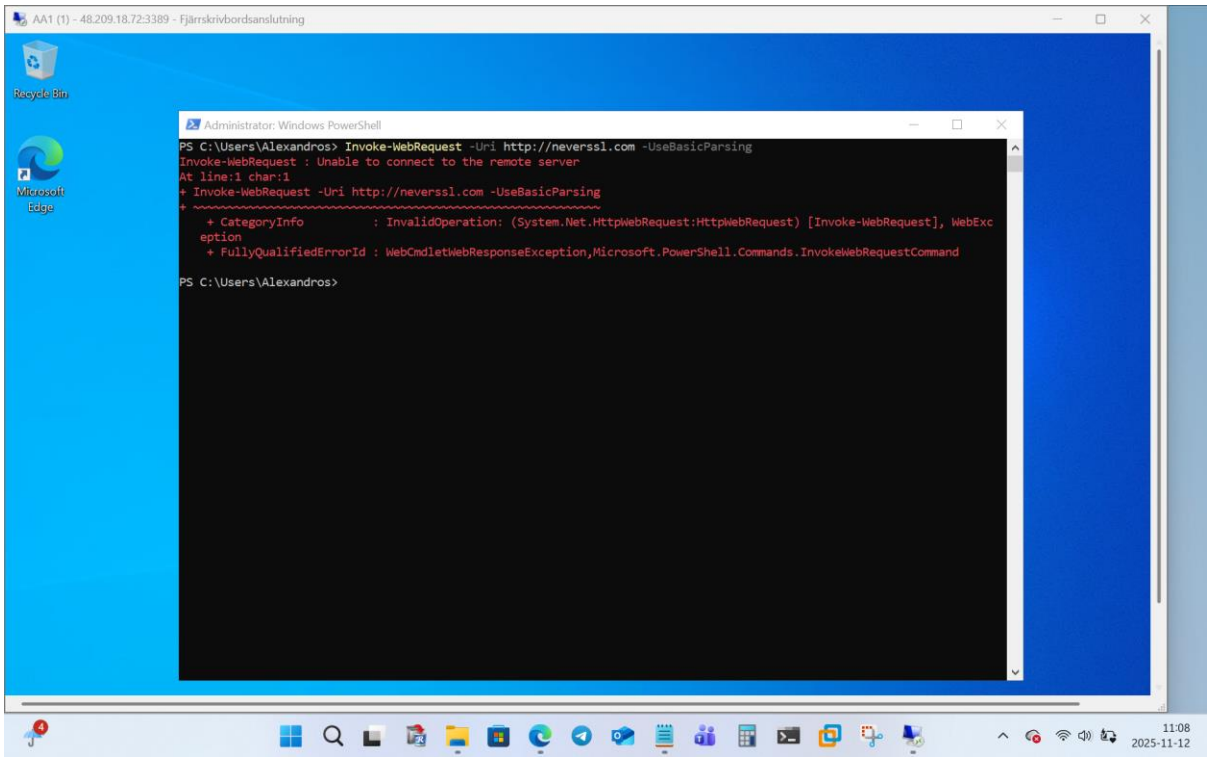
3. I made a VM called AA1 with the image of windows server 2022 inside the subnet of WebSubnet that is located in the virtual network created before (vnet-sec). The virtual machine has to have a public IP address to make sure it can connect to using RDP (remote desktop protocol) in the lab environment 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.



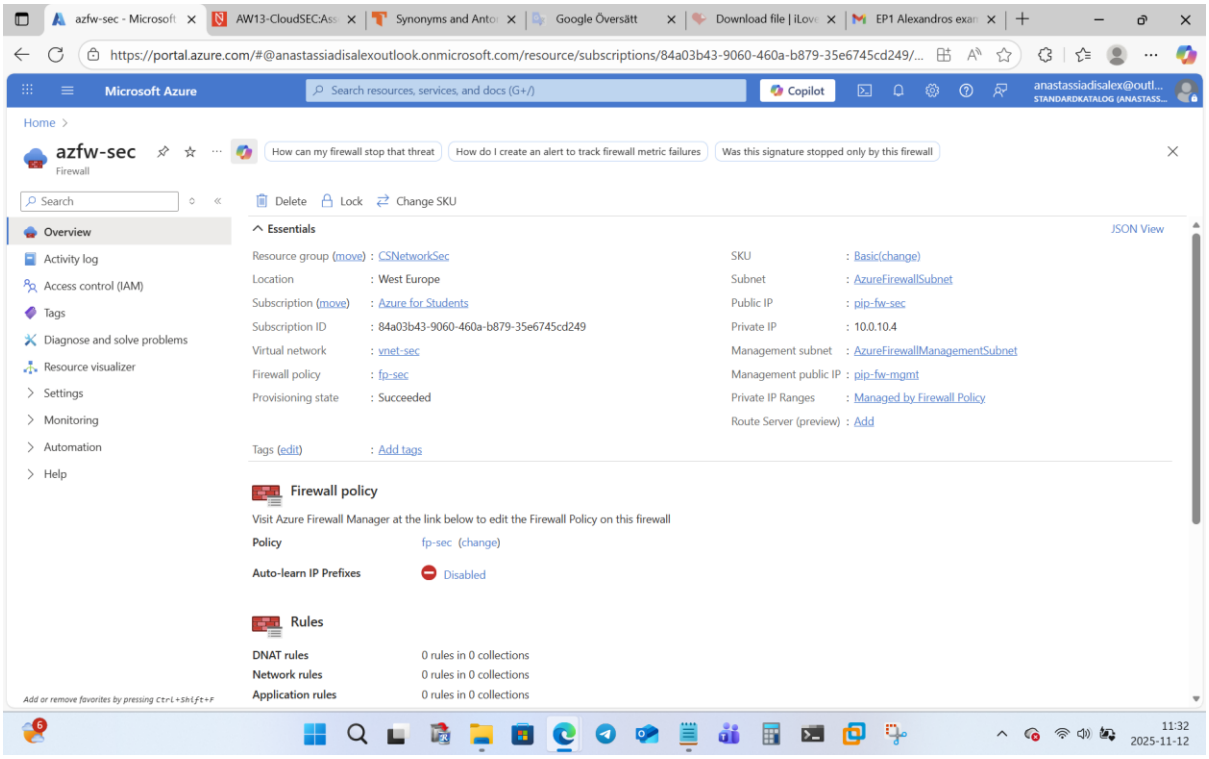
4. I made two inbound security rules in my newly created NSG AA-nsg. One is allowing RDP (TCP 3389) from my IP the other one to deny HTTP (TCP 80) from any source. The NSG in the subnet is going to provide base traffic filtering for all the resources created in that specific subnet. I am expecting to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



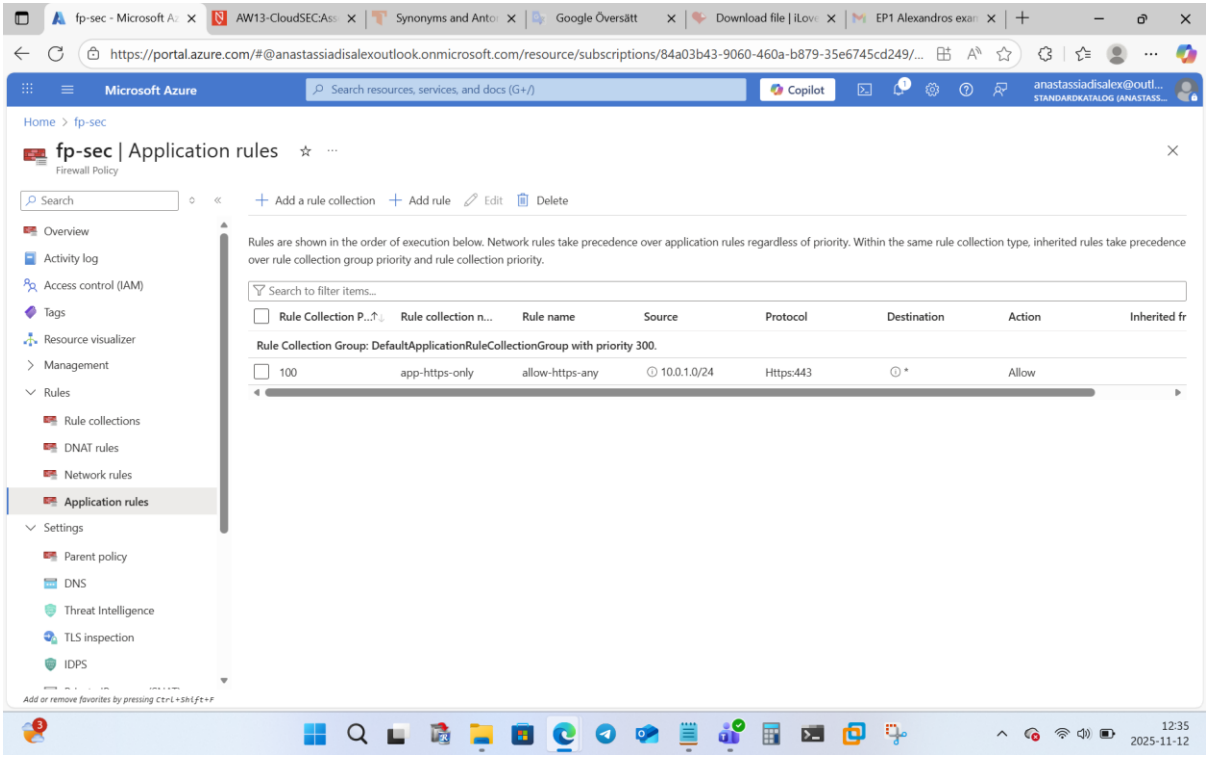
5. I connected to the VM through RDP and then went into powershell and typed the command provided in the text and the NSG rule which were supposed to deny port 80 blocked the HTTP connection as it should. I saw an error that said the connection failed which confirmed to me that the rule is in place and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



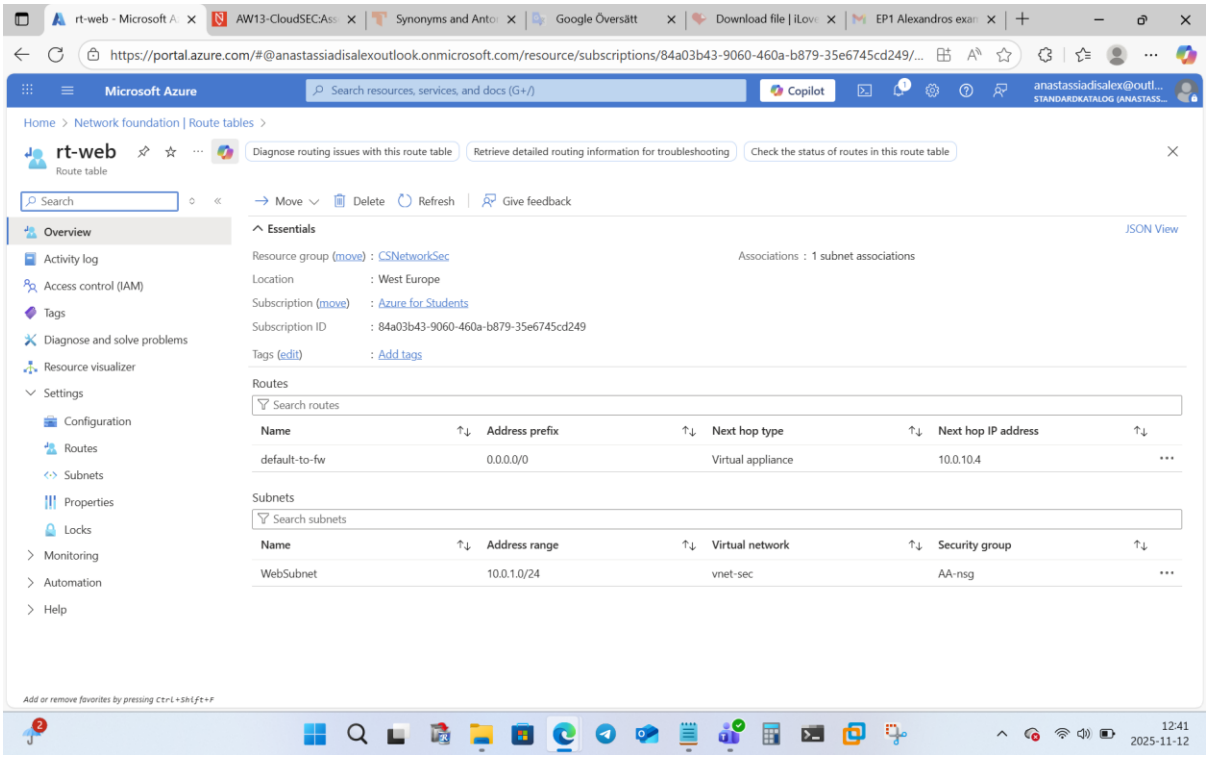
6. I created Azure Firewall with the provided name “azfw-sec” with the firewall policy (fp-sec) also two IP addresses one for management and the other one for data. A basic SKU needs their own management subnet so it can manage all the updates and configurations on its own. I then saw the firewalls private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



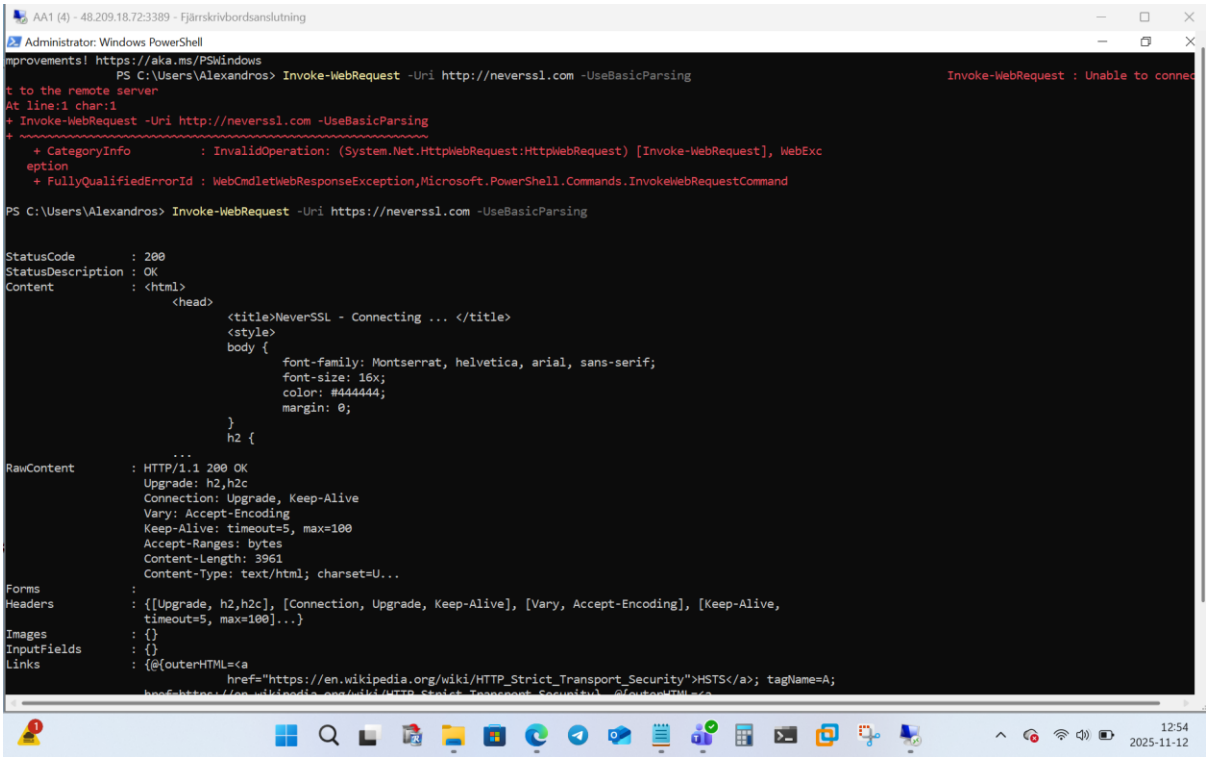
7. I made an application rule collection called app-https-only within the firewall policy (fp-sec) which is allowing outbound traffic HTTPS from the WebSubnet to all destinations. The collection is making sure that only encrypted and secured web connections are being made and approved. As i only accepted 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.



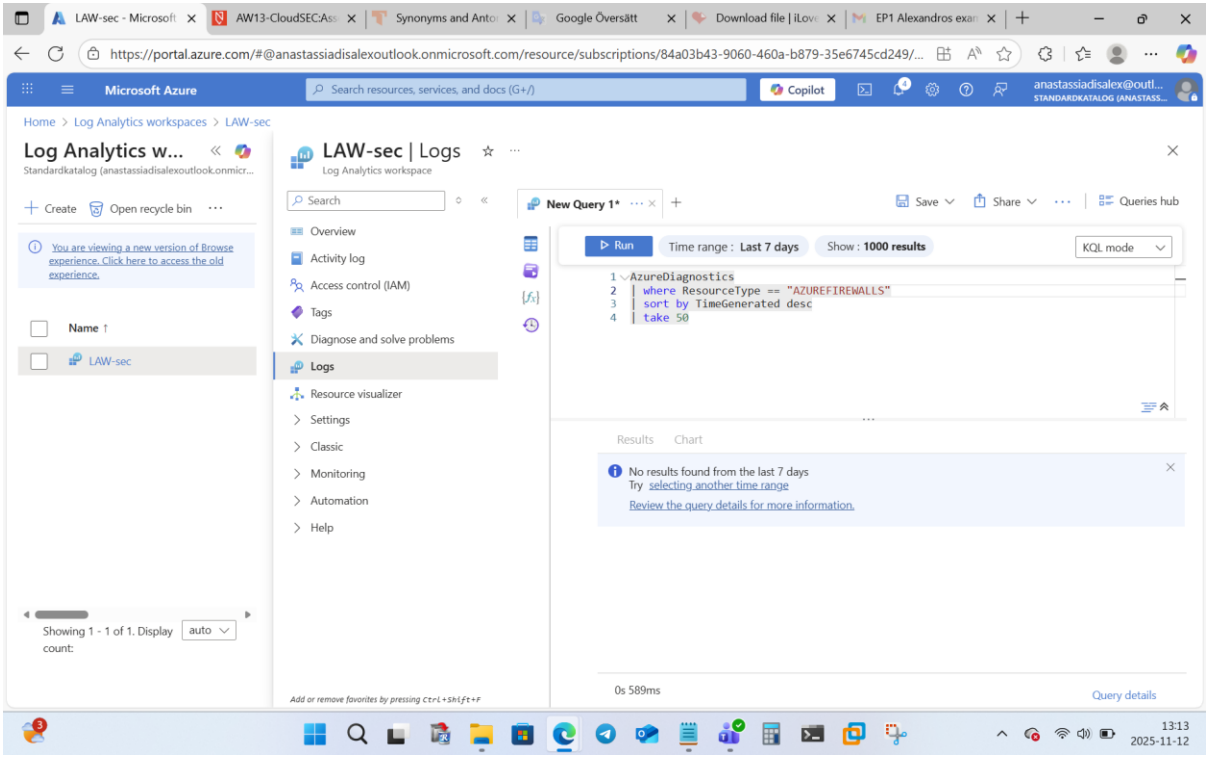
8. I made a route table with the name of rt-web within the CSNetworkSec RG and made a default route of 0.0.0.0/0 and pointing to the private ip of the firewall as the next hop that i wrote down before. After that i associated it with the subnet (WebSubnet) so all of the outbound traffic in the VM is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



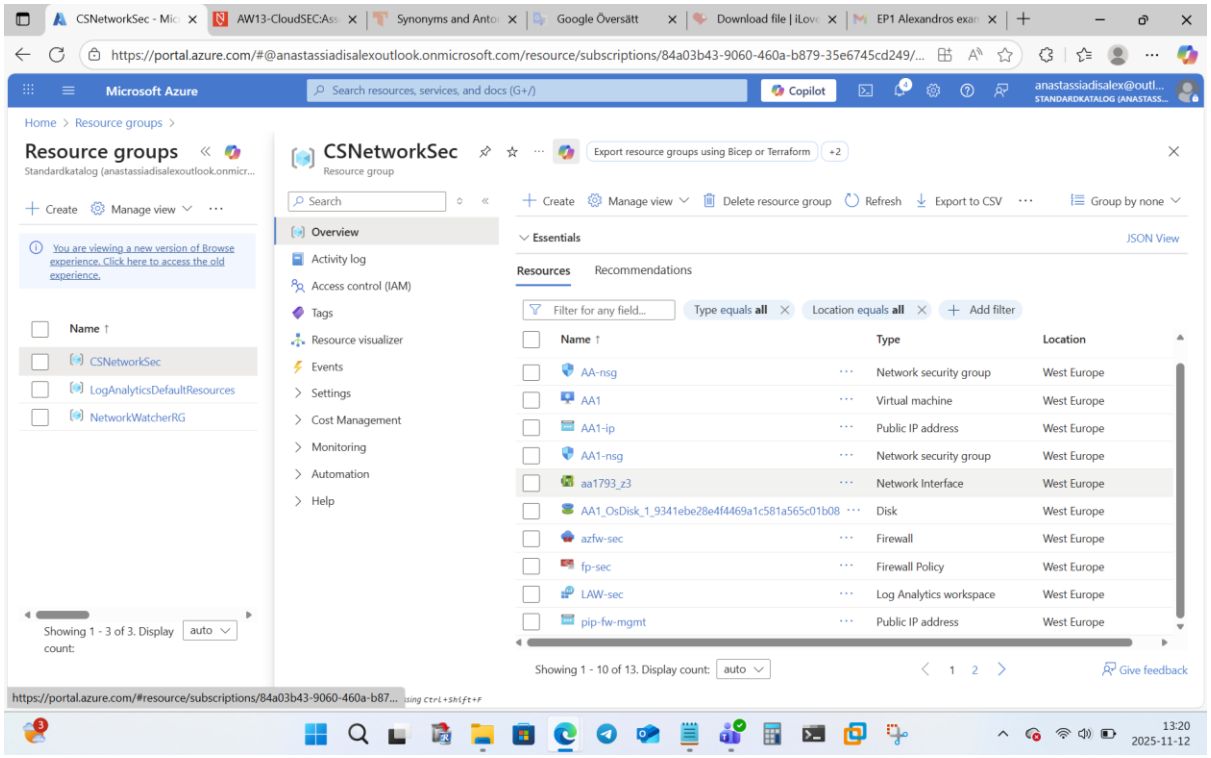
9. Now the traffic is routed through the Azure Firewall that is inspecting and looking at connections more thorough ans the firewall policy is allowing HTTPS because of the rule we created before that is ensuring safe traffi. When i tested it in the powershell it shows that HTTP request to the neverssl.com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

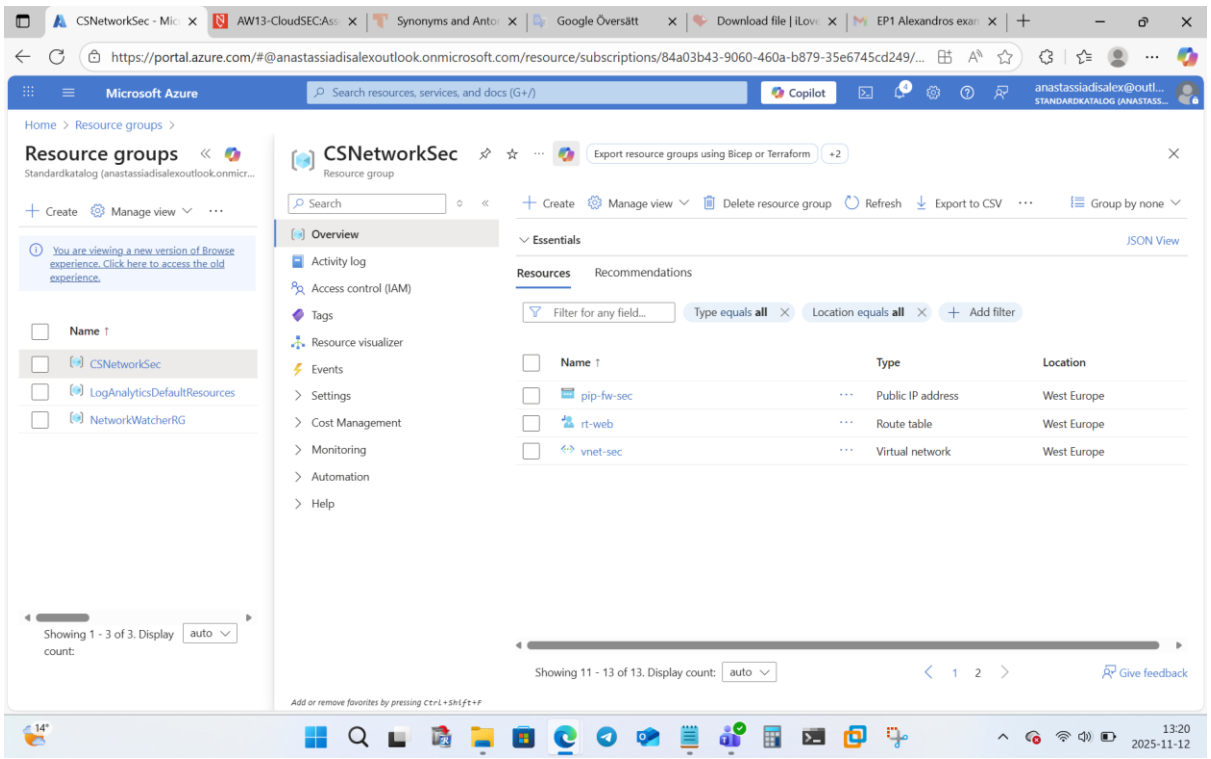


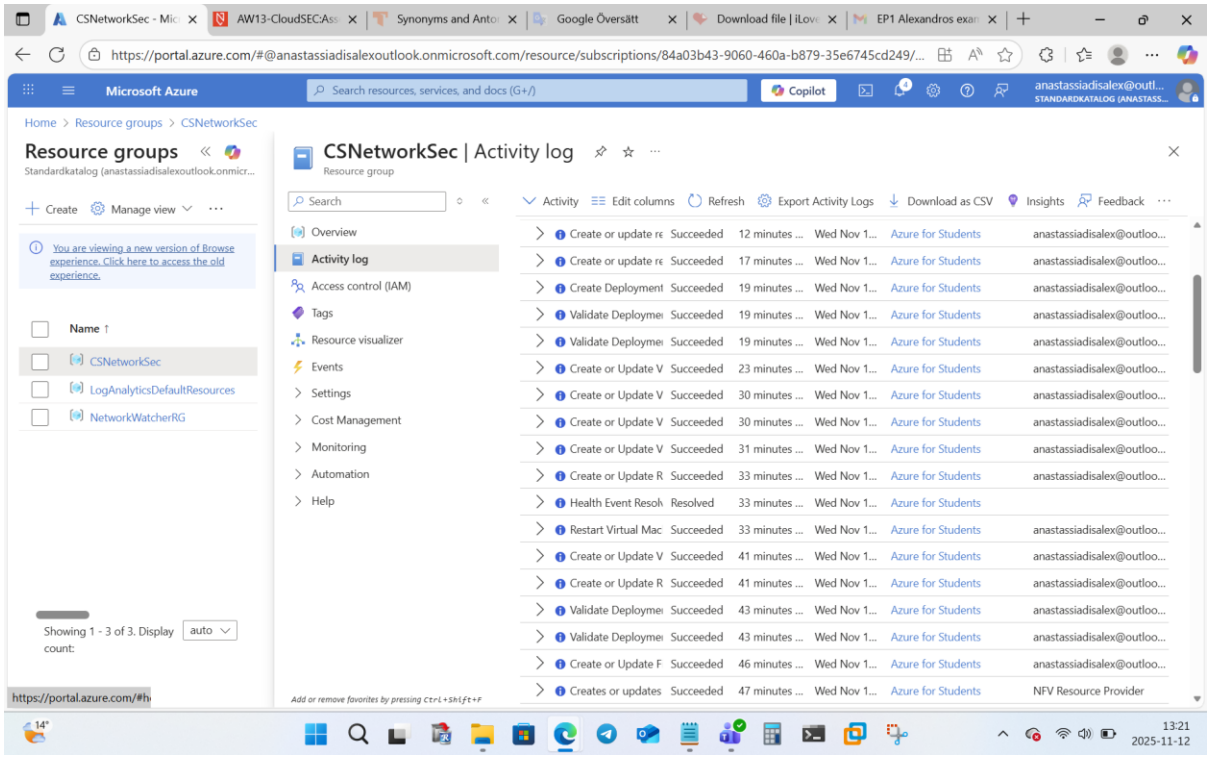
10. I enabled a logging diagnostics on the firewall azfw-sec and then sent the application rule logs and the network rule logs to a log analytic workspace i created called LAW-sec. The logs record is proving how firewall is making policies stronger in real time use even if it worked or not for me. I 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.



Screenshots of RG overview page and activity logs below:


CSNetworkSec - Mic
AW13-CloudSEC:Ass
Synonyms and Anto
Google Översätt
Download file | iLov
EP1 Alexandros exa
https://portal.azure.com/#@anastassiadisalexoutlook.onmicrosoft.com/resource/subscriptions/84a03b43-9060-460a-b879-35e6745cd249/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
anastassiadisalex@outl...
STANDARDKATALOG (ANASTASS...
Home > Resource groups >
Resource groups
Standardkatalog (anastassiadisalexoutlook.onmicr...
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name ↑
CSNetworkSec
LogAnalyticsDefaultResources
NetworkWatcherRG
Showing 1 - 3 of 3. Display count:
auto
CSNetworkSec
Resource group
Export resource groups using Bicep or Terraform
+2
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Create
Manage view
Delete resource group
Refresh
Export to CSV
Group by none
Essentials
JSON View
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_9341ebe28e4f4469a1c581a565c01b08
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
1
2
Give feedback
https://portal.azure.com/#resource/subscriptions/84a03b43-9060-460a-b87...
13:20
2025-11-12


CSNetworkSec - Mic
AW13-CloudSEC:Ass
Synonyms and Anto
Google Översätt
Download file | iLov
EP1 Alexandros exa
https://portal.azure.com/#@anastassiadisalexoutlook.onmicrosoft.com/resource/subscriptions/84a03b43-9060-460a-b879-35e6745cd249/...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
anastassiadisalex@outl...
STANDARDKATALOG (ANASTASS...
Home > Resource groups >
Resource groups
Standardkatalog (anastassiadisalexoutlook.onmicr...
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name ↑
CSNetworkSec
LogAnalyticsDefaultResources
NetworkWatcherRG
Showing 1 - 3 of 3. Display count:
auto
CSNetworkSec
Resource group
Export resource groups using Bicep or Terraform
+2
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Create
Manage view
Delete resource group
Refresh
Export to CSV
Group by none
Essentials
JSON View
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
1
2
Give feedback
Add or remove favorites by pressing Ctrl+Shift+F
13:20
2025-11-12



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, altough 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.