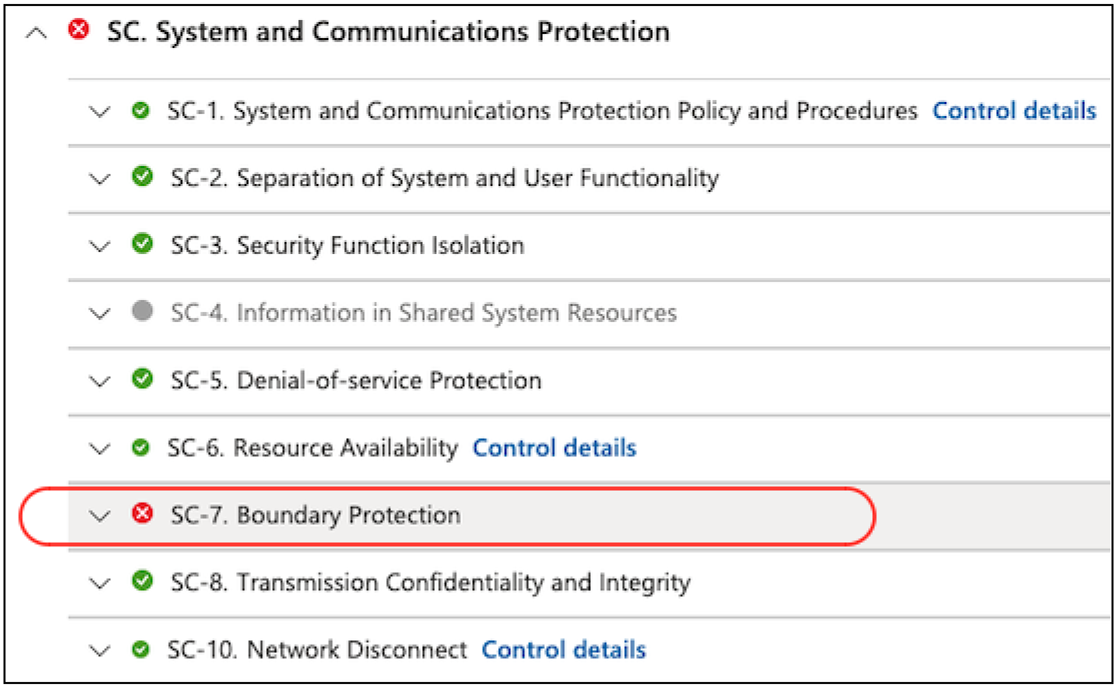
Lab #18: **Implement NIST 800-53: SC-7 (“Boundary Protection”)**

Purpose:

- We’ll be implementing the SC-7 control (“Boundary Protection”) of NIST SP 800-53 in our **Regulatory Compliance** section of **Microsoft Defender for Cloud**.



✗ SC. System and Communications Protection

- ✓ SC-1. System and Communications Protection Policy and Procedures Control details
- ✓ SC-2. Separation of System and User Functionality
- ✓ SC-3. Security Function Isolation
- ● SC-4. Information in Shared System Resources
- ✓ SC-5. Denial-of-service Protection
- ✓ SC-6. Resource Availability Control details
- ✗ SC-7. Boundary Protection
- ✓ SC-8. Transmission Confidentiality and Integrity
- ✓ SC-10. Network Disconnect Control details

Tasks:

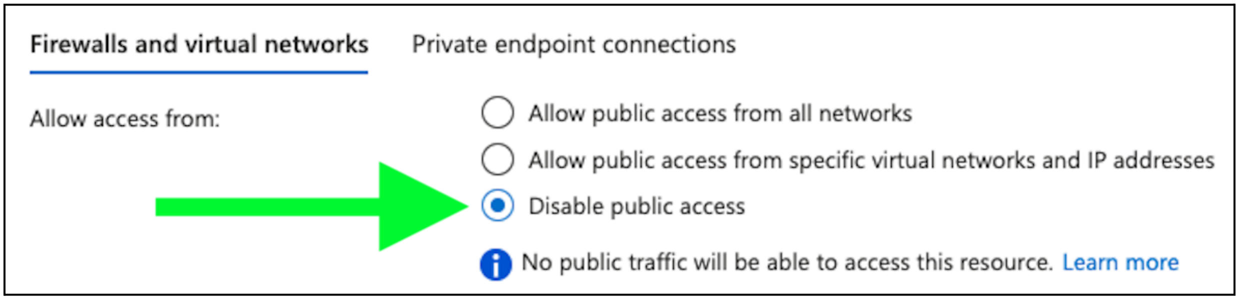
1. **Configure Firewall and Private Link for Azure Key Vault**
   - Configure the Firewall in Key Vault
   - Configure the Private Endpoint in Key Vault
2. **Configure Firewall and Private Link for Azure Storage**
   - Disable Blog public access
   - Configure the Firewall in Azure Storage
   - Configure the Private Endpoint in Azure Storage
3. **Observe the Topology in Network Watcher**
4. **Validate that Private Endpoint is working in windows-vm**
5. **Configure NSG for the Subnet**
6. **Check the compliance status of SC-7**

Task 1: **Configure Firewall and Private Link for Azure Key Vault**

Configure the Firewall in Key Vault:

1. **Azure** portal > **Key Vault** > **Networking** >

2. Under **Firewalls and Virtual Networks**, select **Disable public access** > select **Apply**.



Allow access from:

○ Allow public access from all networks

○ Allow public access from specific virtual networks and IP addresses

● Disable public access

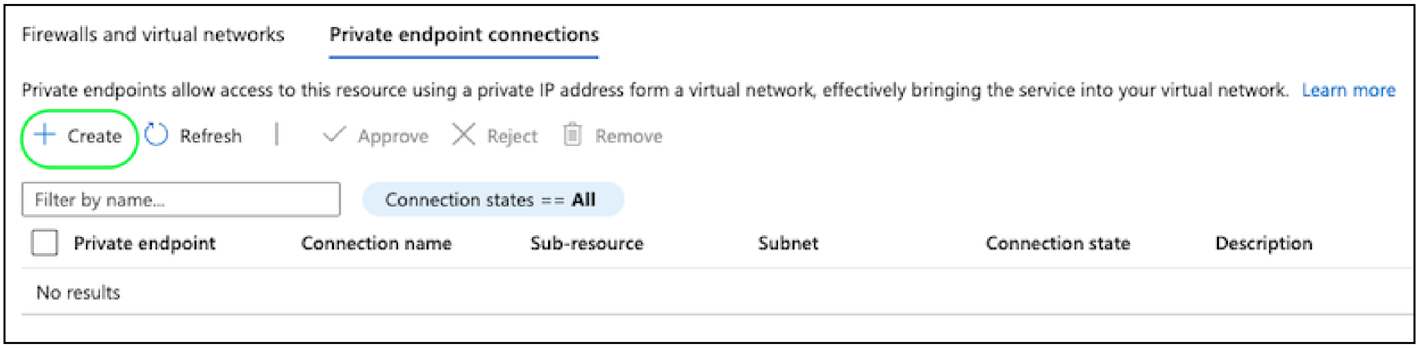
No public traffic will be able to access this resource. Learn more

***<u>Note</u>*: We've now enabled the firewall for our *Key Vault*.**

Configure the Private Endpoint in Key Vault:

***<u>Note</u>*: We want to update our Key Vault from being publicly-exposed to only being privately accessible through our virtual network and subnet.**

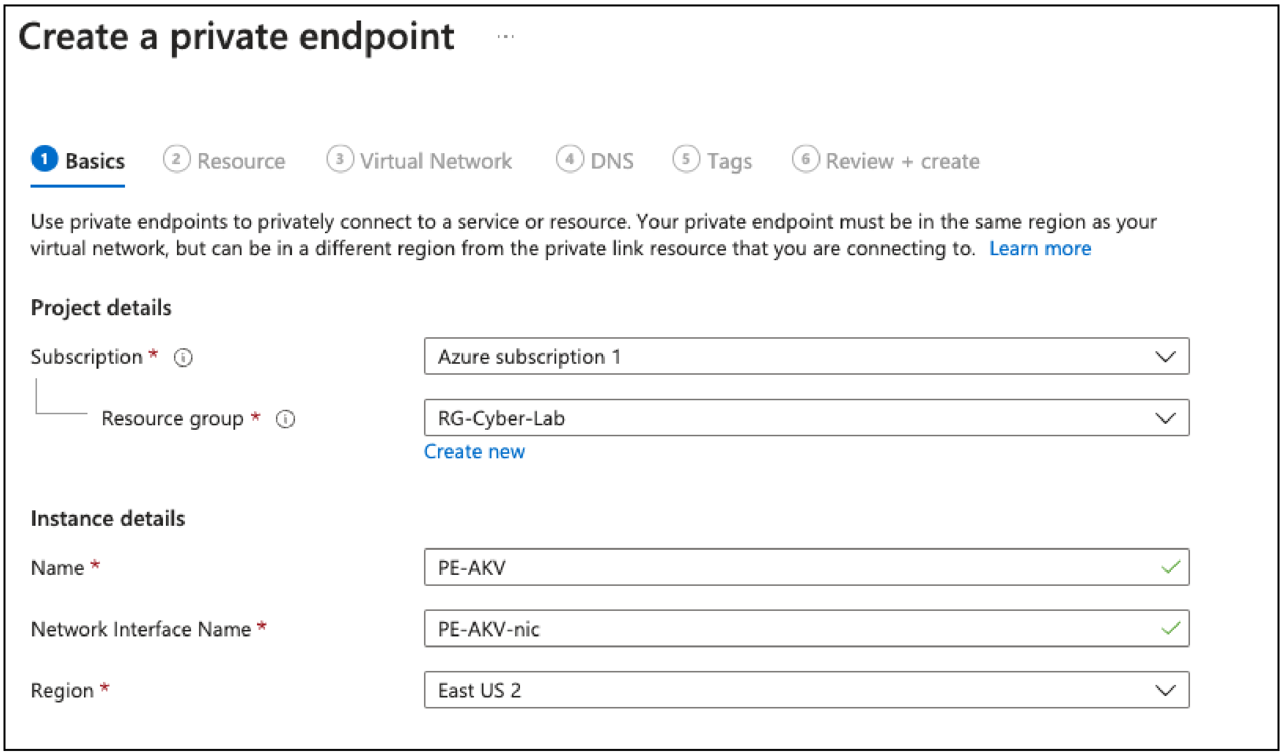
1. **Azure** portal > **Key Vault** > **Networking** >
2. Select **Private Endpoint Connections** > select **Create**.



Private endpoints allow access to this resource using a private IP address form a virtual network, effectively bringing the service into your virtual network. Learn more

□ Private endpoint	Connection name	Sub-resource	Subnet	Connection state	Description
No results					

3. Fill out the necessary fields.



Create a private endpoint ...

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * : Azure subscription 1

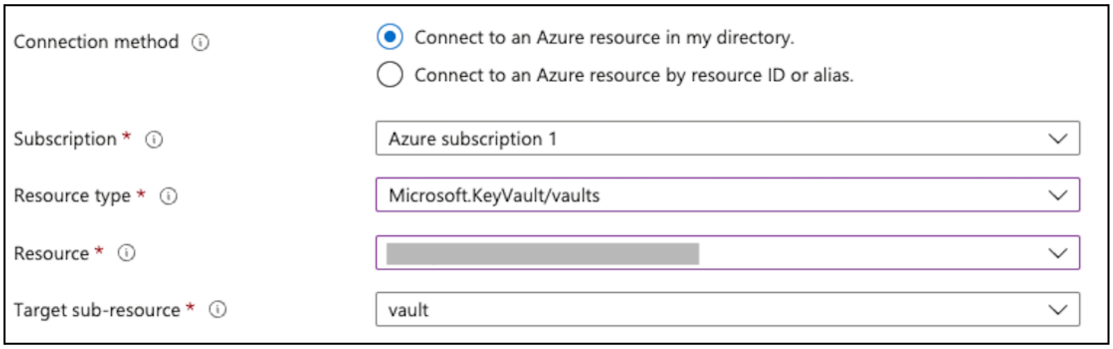
Resource group * : RG-Cyber-Lab

Instance details

Name * : PE-AKV

Network Interface Name * : PE-AKV-nic

Region * : East US 2



Connection method ⓘ
● Connect to an Azure resource in my directory.
○ Connect to an Azure resource by resource ID or alias.

Subscription * ⓘ: Azure subscription 1

Resource type * ⓘ: Microsoft.KeyVault/vaults

Resource * ⓘ: [redacted]

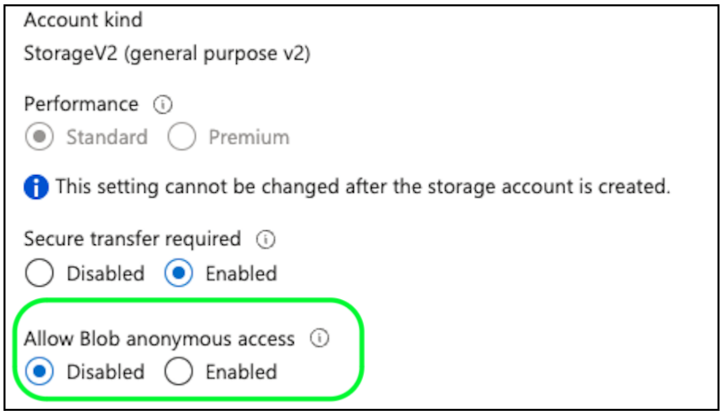
Target sub-resource * ⓘ: vault

4. Select **Review + Create**.

Task 2: Configure Firewall and Private Link for Azure Storage

Disable Blog public access:

1. **Azure** portal > **Storage accounts** > **Configuration** >
2. Ensure that the **Allow Blob anonymous access** field is disabled.



Account kind
StorageV2 (general purpose v2)

Performance ⓘ
● Standard ○ Premium

ⓘ This setting cannot be changed after the storage account is created.

Secure transfer required ⓘ
○ Disabled ● Enabled

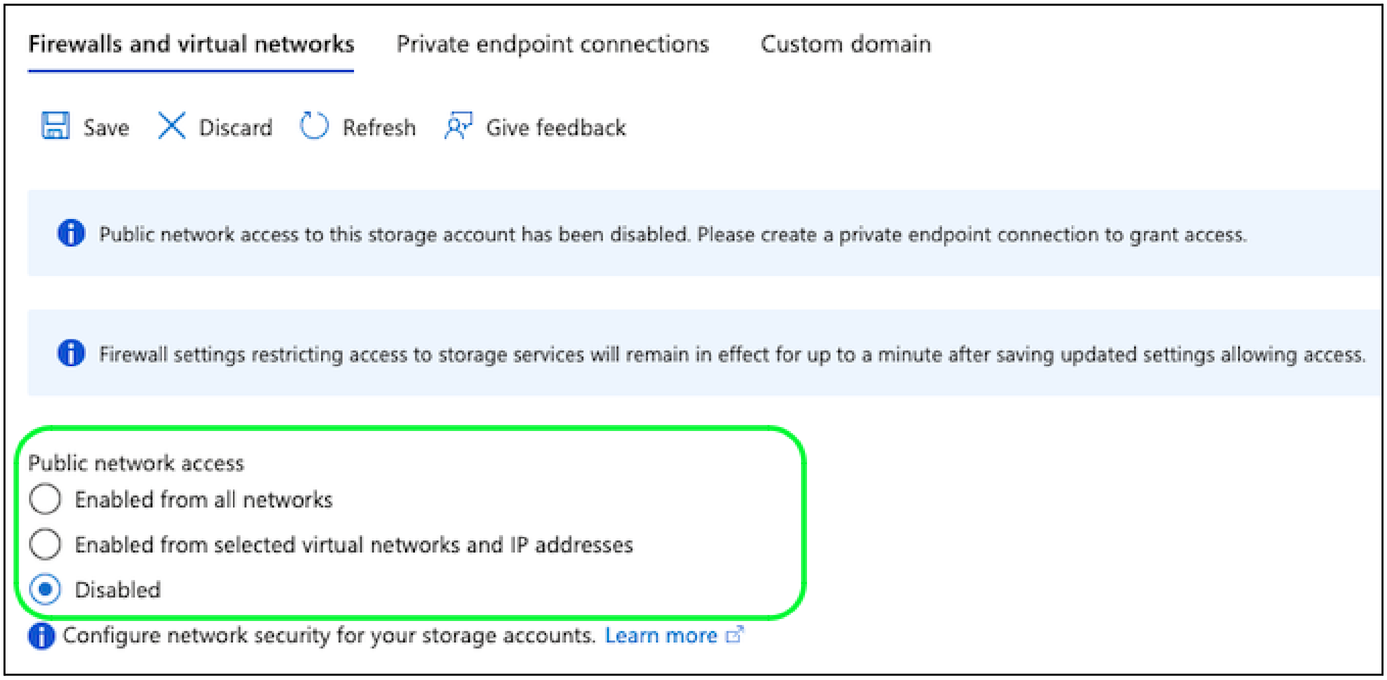
Allow Blob anonymous access ⓘ
● Disabled ○ Enabled

***Note**: This is required when needing to satisfy the 800-53 SC:7 control in Azure.*

Configure the Firewall in Azure Storage:

1. **Azure** portal > **Storage accounts** > **Networking** >

2. Under **Firewalls and Virtual Networks**, select **Disable public access** > select **Apply**.



Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

Public network access

○ Enabled from all networks

○ Enabled from selected virtual networks and IP addresses

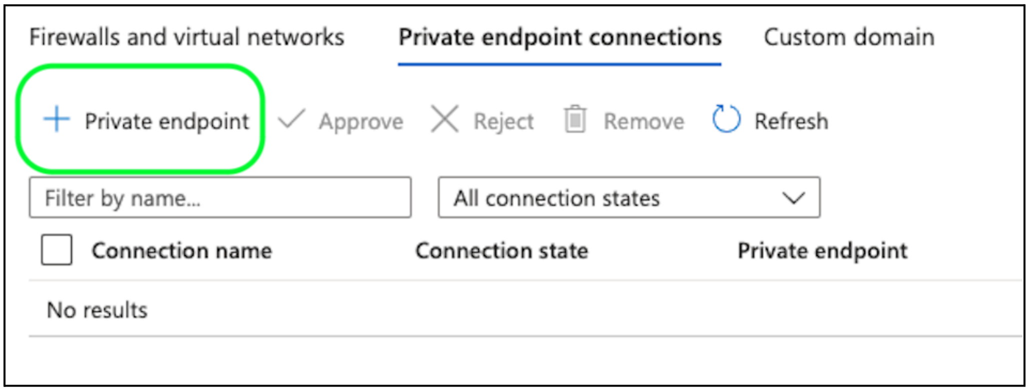
● Disabled

Configure network security for your storage accounts. Learn more

***Note**: We've now enabled the firewall for our **Storage account**.*

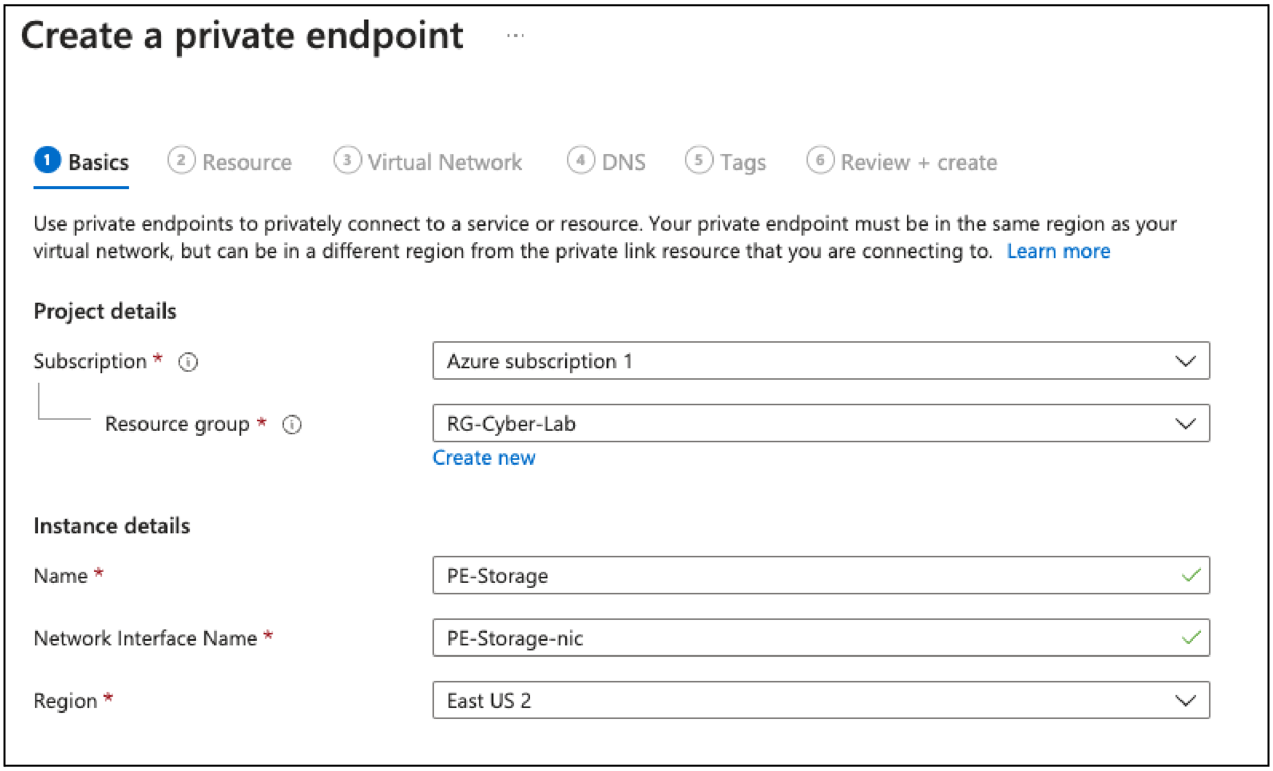
Configure the Private Endpoint in Azure Storage:

1. **Azure** portal > **Storage accounts** > **Networking** >
2. Select **Private Endpoint Connections** > select **+Private Endpoint**.



□ Connection name	Connection state	Private endpoint
No results		

3. Fill out the necessary fields.



Create a private endpoint ...

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * : Azure subscription 1

Resource group * : RG-Cyber-Lab

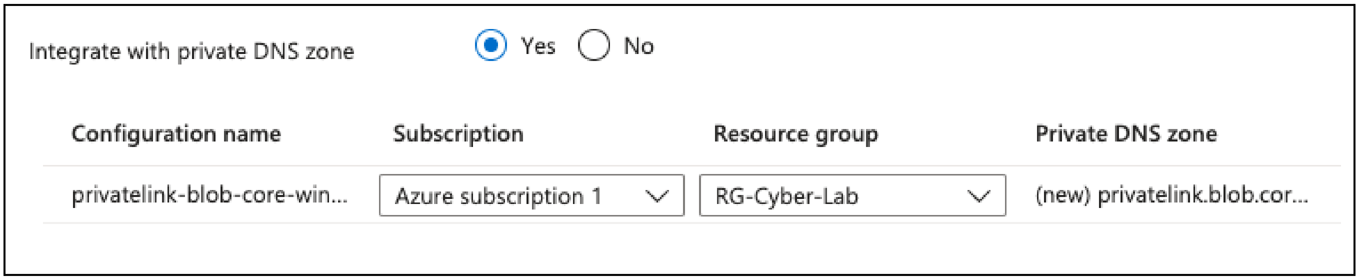
Create new

Instance details

Name * : PE-Storage ✓

Network Interface Name * : PE-Storage-nic ✓

Region * : East US 2



Integrate with private DNS zone ● Yes ○ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-blob-core-win...	Azure subscription 1	RG-Cyber-Lab	(new) privatelink.blob.cor...

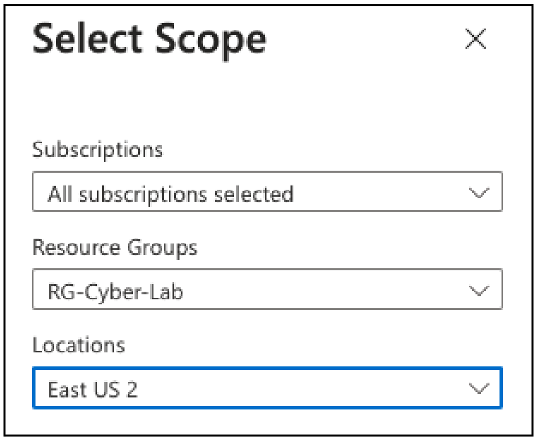
4. Select **Review + Create**.

Task 3: Observe the Topology in Network Watcher

1. **Azure** portal > **Network Watcher** > **Topology** >

> ***Note***: *This will display a network diagram of our resources in our Azure subscription. It allows us to get a sense of what's going on in our environment from a high level.*

2. Select **Scope** > select our subscription, resource group (RG-Cyber-Lab), and location (East US 2).



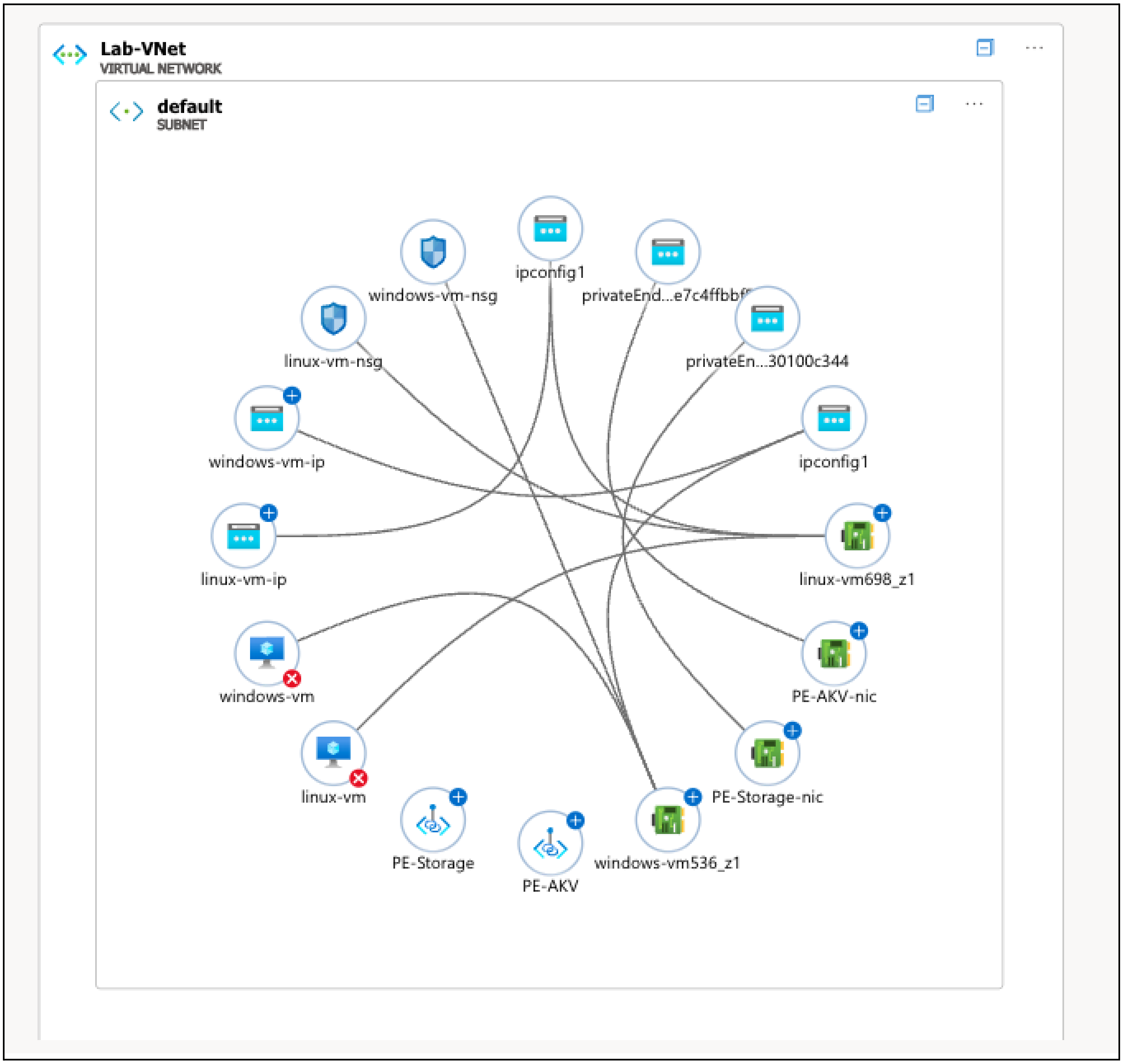
Select Scope

Subscriptions: All subscriptions selected

Resource Groups: RG-Cyber-Lab

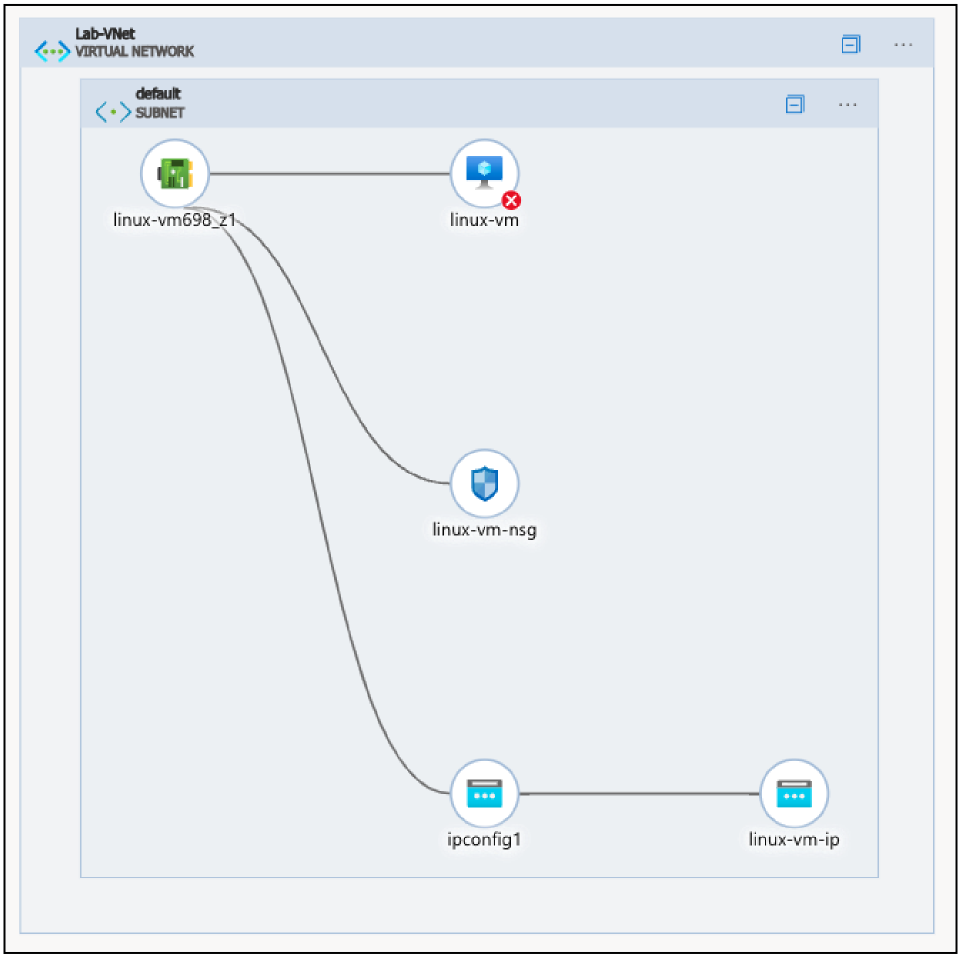
Locations: East US 2

3. We now can view our lab resources within our lab virtual network.

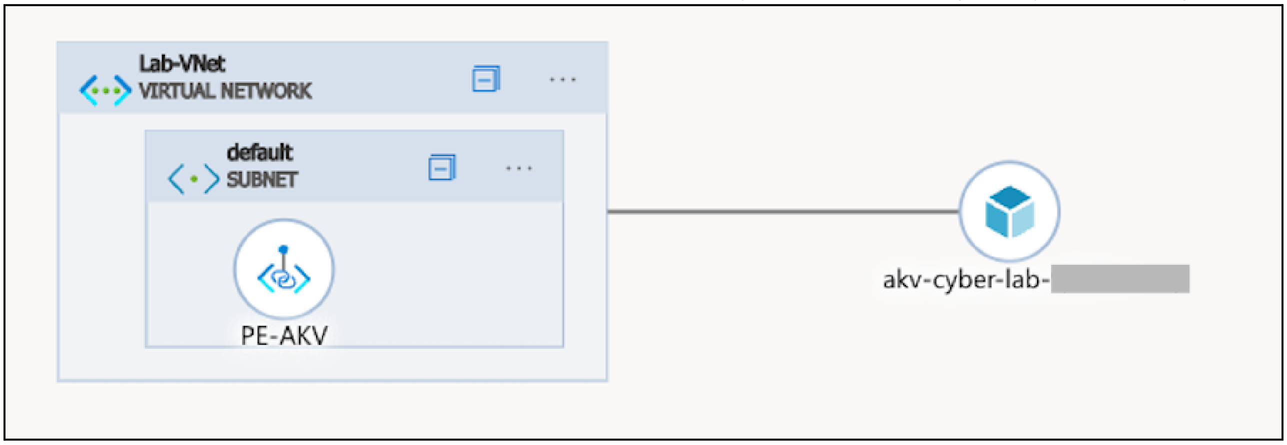


4. We can dig further:

a. Ex. We'll select ou Linux NIC (linux-vm698_z1). We can see that this NIC's attached VM (linux-vm), it's NSG (linux-vm-nsg), and it has its own associated IP address (linux-vm-ip).



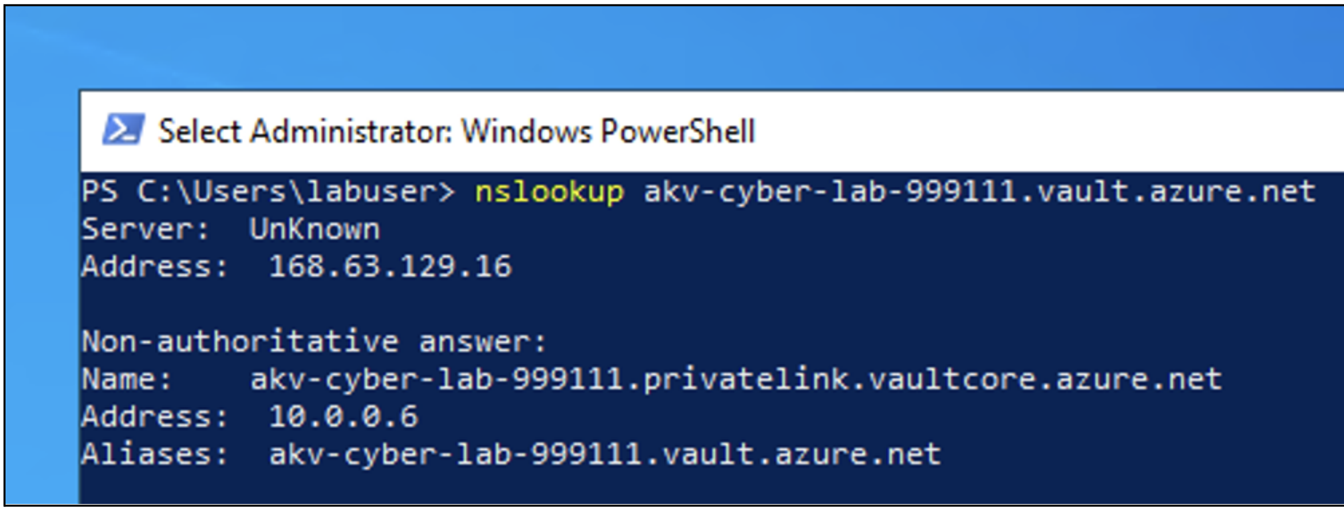
b. Ex. we'll now select one of our private endpoints (PE-Storage, PE-AKV). We see that PE-AKV is associated with a subnet that is attached to our Azure Key Vault instance (akv-cyber-lab-***).



Task 4: Validate that Private Endpoint is working in windows-vm

1. **Azure** portal > **Virtual Machines** > power on windows-vm > locate the public IP for windows-vm.
2. Connect to windows-vm (using Microsoft Remote Desktop).
    a. Note: The windows-vm public IP needs to match the IP assigned in the NSG settings.
3. Open **PowerShell**.
4. Check the IP address of our Key Vault instance.

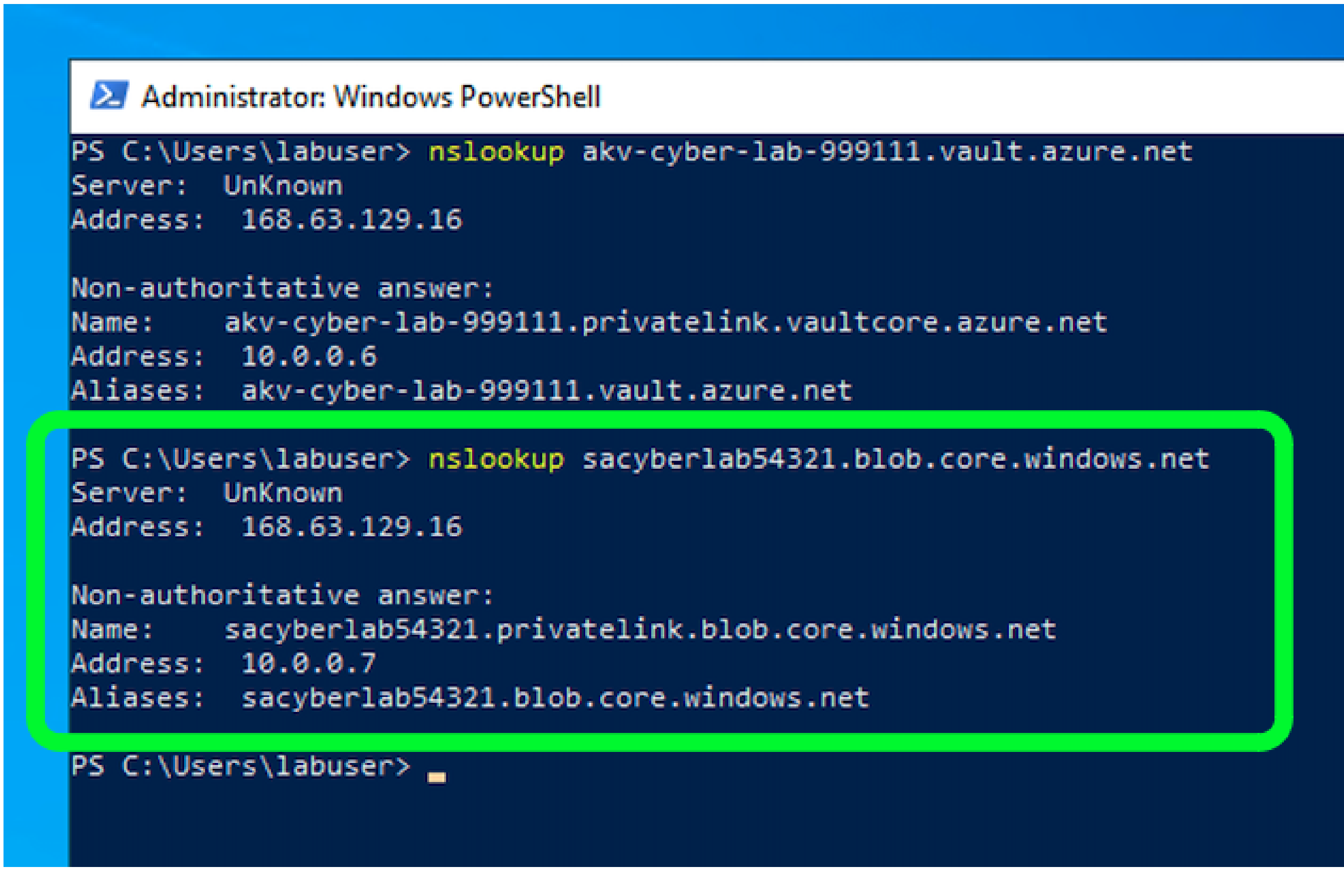
   a. Locate the Vault URL (in Key Vault instance **Overview** page).
      i. akv-cyber-lab-999111.vault.azure.net
   b. nslookup akv-cyber-lab-999111.vault.azure.net



```
PS C:\Users\labuser> nslookup akv-cyber-lab-999111.vault.azure.net
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    akv-cyber-lab-999111.privatelink.vaultcore.azure.net
Address:  10.0.0.6
Aliases:  akv-cyber-lab-999111.vault.azure.net
```

***Note**: We can tell that Private Endpoint is working since it's resolving to a **private IP** address (10.0.0.6) within our subnet's range.*

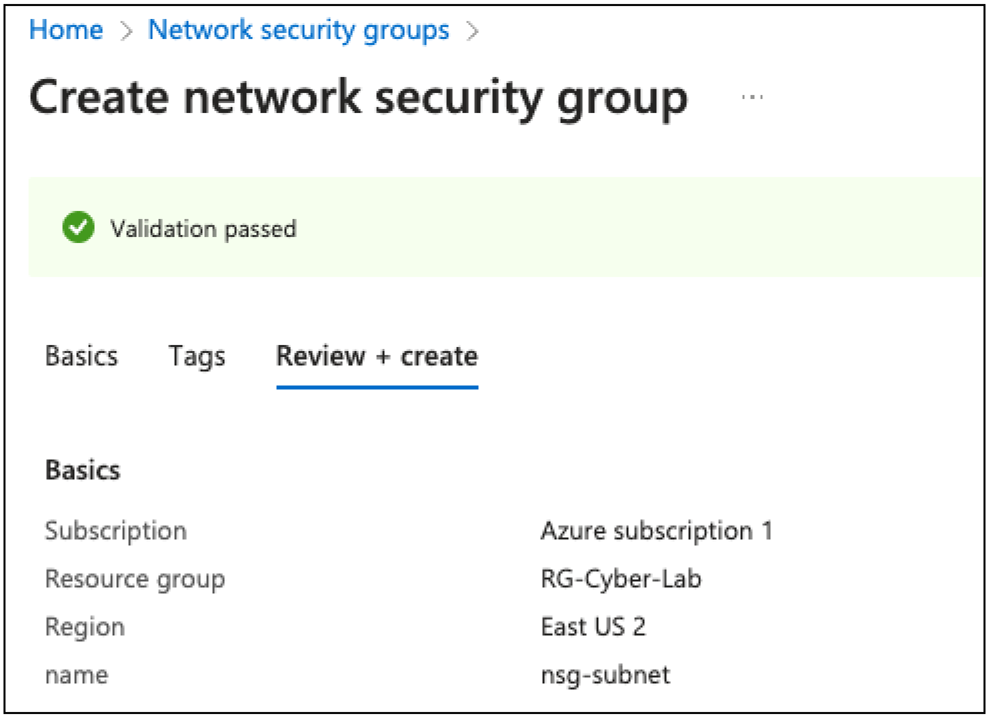
5. Check the IP address of our Storage Account.
   a. Locate the **Blog service** URL (in Key Vault instance **Endpoints** page).
      i. sacyberlab54321.blob.core.windows.net/
   b. nslookup akv-cyber-lab-999111.vault.azure.net



```
PS C:\Users\labuser> nslookup akv-cyber-lab-999111.vault.azure.net
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    akv-cyber-lab-999111.privatelink.vaultcore.azure.net
Address:  10.0.0.6
Aliases:  akv-cyber-lab-999111.vault.azure.net

PS C:\Users\labuser> nslookup sacyberlab54321.blob.core.windows.net
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    sacyberlab54321.privatelink.blob.core.windows.net
Address:  10.0.0.7
Aliases:  sacyberlab54321.blob.core.windows.net

PS C:\Users\labuser> _
```

Task 5: Configure NSG for the Subnet

1. **Azure** portal > **Network Security Groups** > **Create**



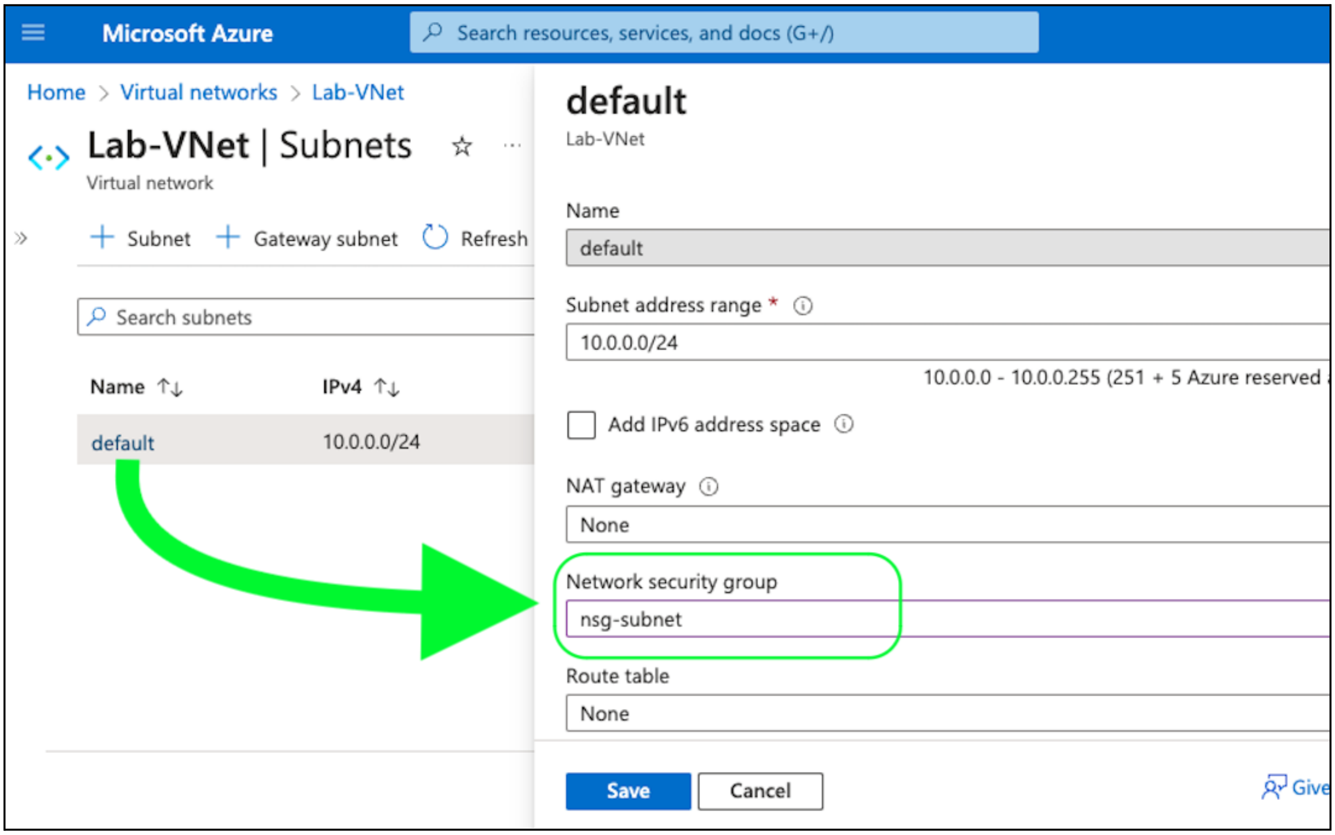
Create network security group

Validation passed

Basics

Subscription	Azure subscription 1
Resource group	RG-Cyber-Lab
Region	East US 2
name	nsg-subnet

2. Go to **Azure** portal > **Virtual Networks** > (select our Lab-VNet) > **Subnets**
   a. Select our **default** subnet > select **nsg-subnet** > **Save**.



Name ↑↓	IPv4 ↑↓
default	10.0.0.0/24

default

Lab-VNet

Name: default

Subnet address range *: 10.0.0.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved

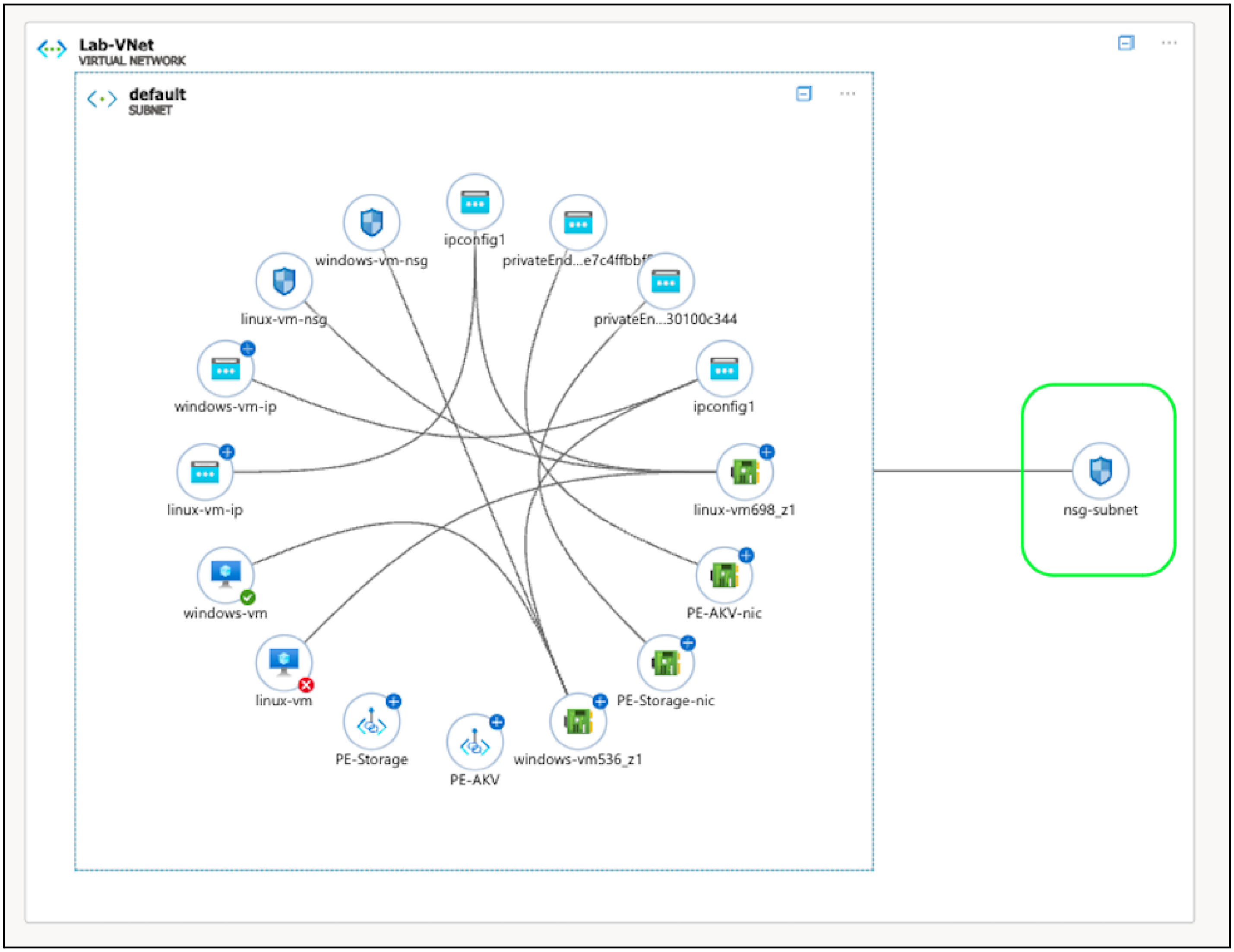
□ Add IPv6 address space

NAT gateway: None

Network security group: nsg-subnet

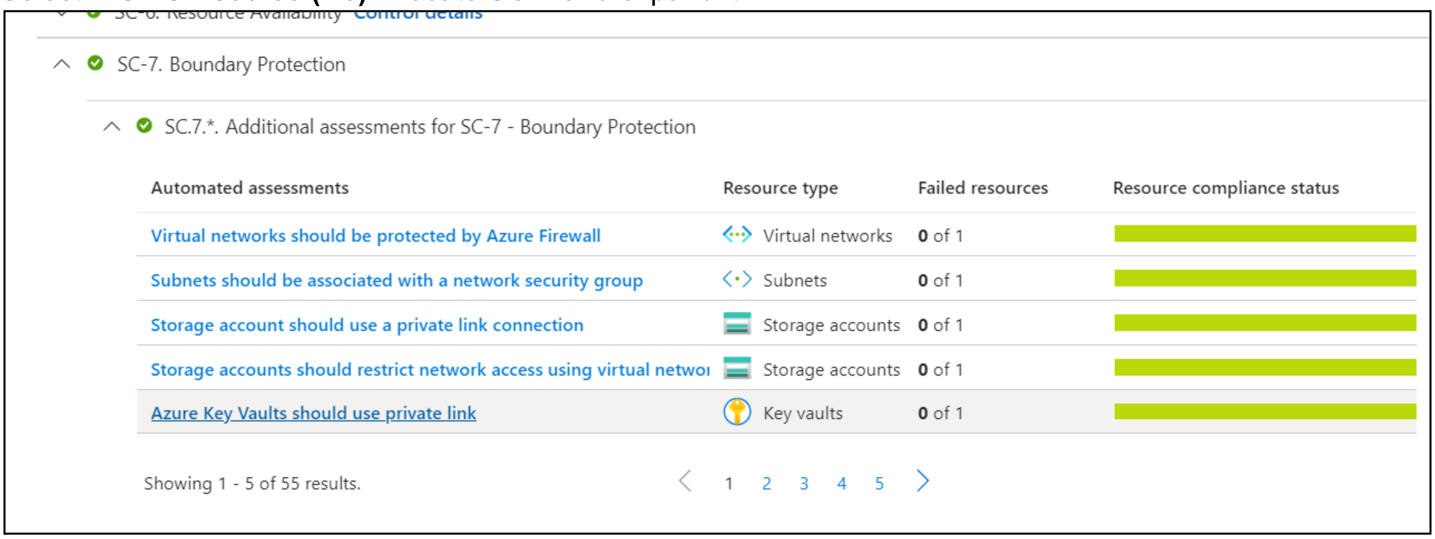
Route table: None

3. Go back to **Network Watcher** > **Topology** > the default subnet (with its newly-assigned NSG) appears



Task 6: Check the compliance status of SC-7

1. **Azure** portal > **Miscrosoft Defender for Cloud** > **Regulatory Compliance**
2. Select **NIST SP 800-53 (R5)** > locate **SC-7** and expand it.



SC-6. Resource Availability Control details

SC-7. Boundary Protection

SC.7.*. Additional assessments for SC-7 - Boundary Protection

Automated assessments	Resource type	Failed resources	Resource compliance status
Virtual networks should be protected by Azure Firewall	Virtual networks	**0** of 1	🟩
Subnets should be associated with a network security group	Subnets	**0** of 1	🟩
Storage account should use a private link connection	Storage accounts	**0** of 1	🟩
Storage accounts should restrict network access using virtual networ	Storage accounts	**0** of 1	🟩
Azure Key Vaults should use private link	Key vaults	**0** of 1	🟩

Showing 1 - 5 of 55 results.

< 1 2 3 4 5 >

***Note**: When we go back to **Regulatory Compliance**, we can see that we've satisfied the compliance requirements for NIST SP 500-53, SC-7 ("Boundary Protection").*

End:

- We've satisfied the compliance requirements for NIST SP 500-53, SC-7 ("Boundary Protection").
- We created private endpoints for our storage account and key vault instances, so they're only accessible within the private lab network. We also enabled the firewall for each instance, disabling public access from the internet. They used to be fully accessible on the public internet.