**Azure Security Sample Solutions**

Contents

[1. Build a perimeter network to help protect applications with a firewall and NSG and UDR 5](#_Toc512003186)

[1.1 Purpose 5](#_Toc512003187)

[1.2 Executive Summary 5](#_Toc512003188)

[1.3 Architecture 5](#_Toc512003189)

[1.4 Detailed Environment description 6](#_Toc512003190)

[1.5 Artifacts repository 18](#_Toc512003191)

[1.6 PowerShell Scripts 18](#_Toc512003192)

[1.6.1 Create a VNet and three subnets 18](#_Toc512003193)

[1.6.2 Create a VM in existing subnet 18](#_Toc512003194)

[1.6.3 Create a NSG and associate to subnet. 18](#_Toc512003195)

[1.6.4 Enable IP Forwarding for the NVA 18](#_Toc512003196)

[1.6.5 Create UDR 18](#_Toc512003197)

[1.6.6 Associate UDR to Subnets 18](#_Toc512003198)

[1.7 Conclusion 18](#_Toc512003199)

[1.8 References 19](#_Toc512003200)

[2. Secure hybrid connection with ExpressRoute 20](#_Toc512003201)

[2.1 Purpose 20](#_Toc512003202)

[2.2 Executive Summary 20](#_Toc512003203)

[2.3 Architecture 20](#_Toc512003204)

[2.4 Detailed environment description 21](#_Toc512003205)

[2.5 Artifacts repository 23](#_Toc512003206)

[2.6 PowerShell Scripts 23](#_Toc512003207)

[2.7 Conclusion 23](#_Toc512003208)

[2.8 References 24](#_Toc512003209)

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Authors | Remarks |
| 04-09-2018 | 1.0 | Nagendra Kasturi, Arumugam Amlan and Veeravenkat Satyanarayan | Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**DISTRIBUTION LIST**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | *Version* | *Name* | *Date* |
|  |  |  |  |  |
|  |  |  |  |  |

1. Build a perimeter network to protect applications with the firewall and NSG and UDR

## Purpose

This solution describes how to protect your virtual network in Azure by using Network Security groups, user defined routes and a firewall appliance created from market place. The virtual network contains multiple subnets – for firewall appliance, webservers and application servers.

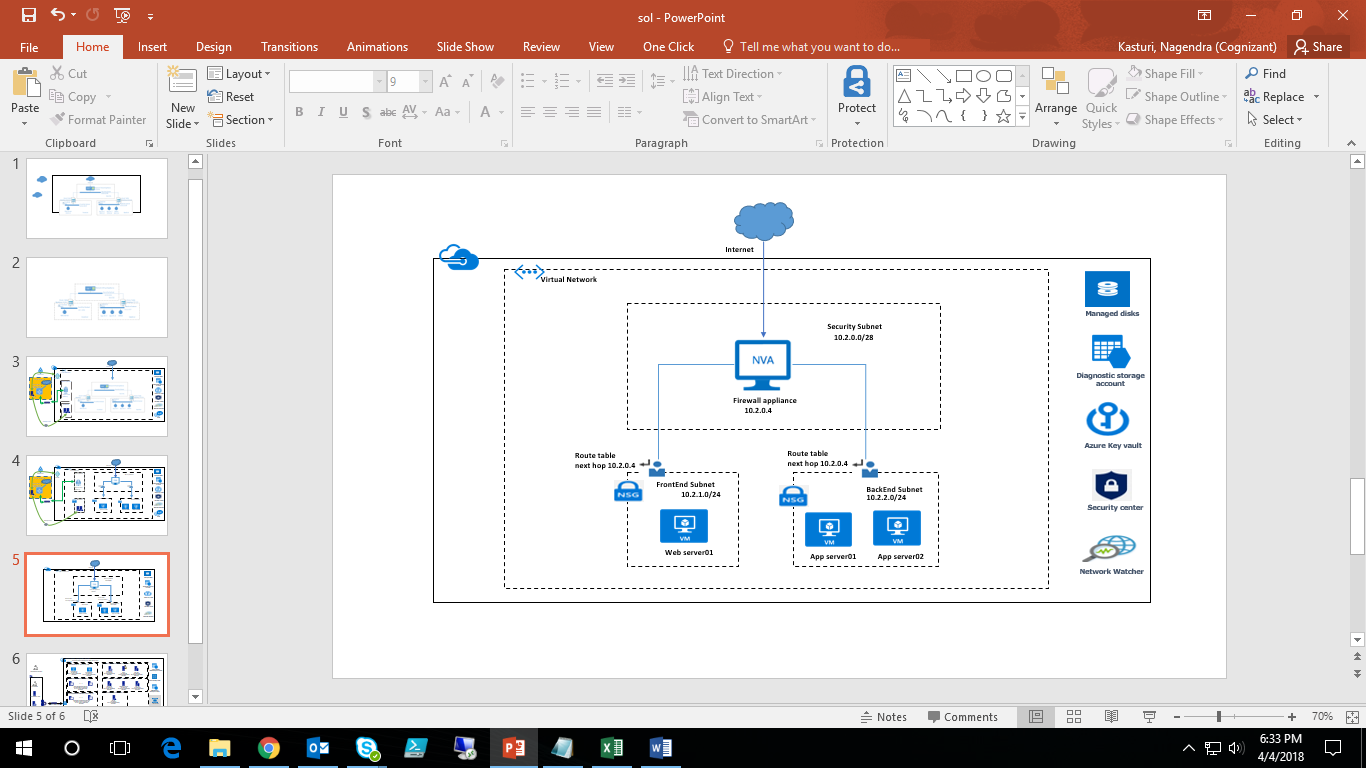
## Executive Summary

This design shall only be covering about securing Azure Virtual network and shall function as one of the baseline inputs for securing a virtual network in Azure using NSG and UDR.

This Solution is part of Azure Security best practices that includes Network, compute and storage security.

This design is focused on securing a virtual network with multiple subnets using a firewall appliance and user defined routes and network security groups. The deployment here is done by using PowerShell scripts and before starting the deployment install latest AzureRM PowerShell modules.

## Architecture



**Figure 1 Architecture**

## 1.4 Detailed Environment description

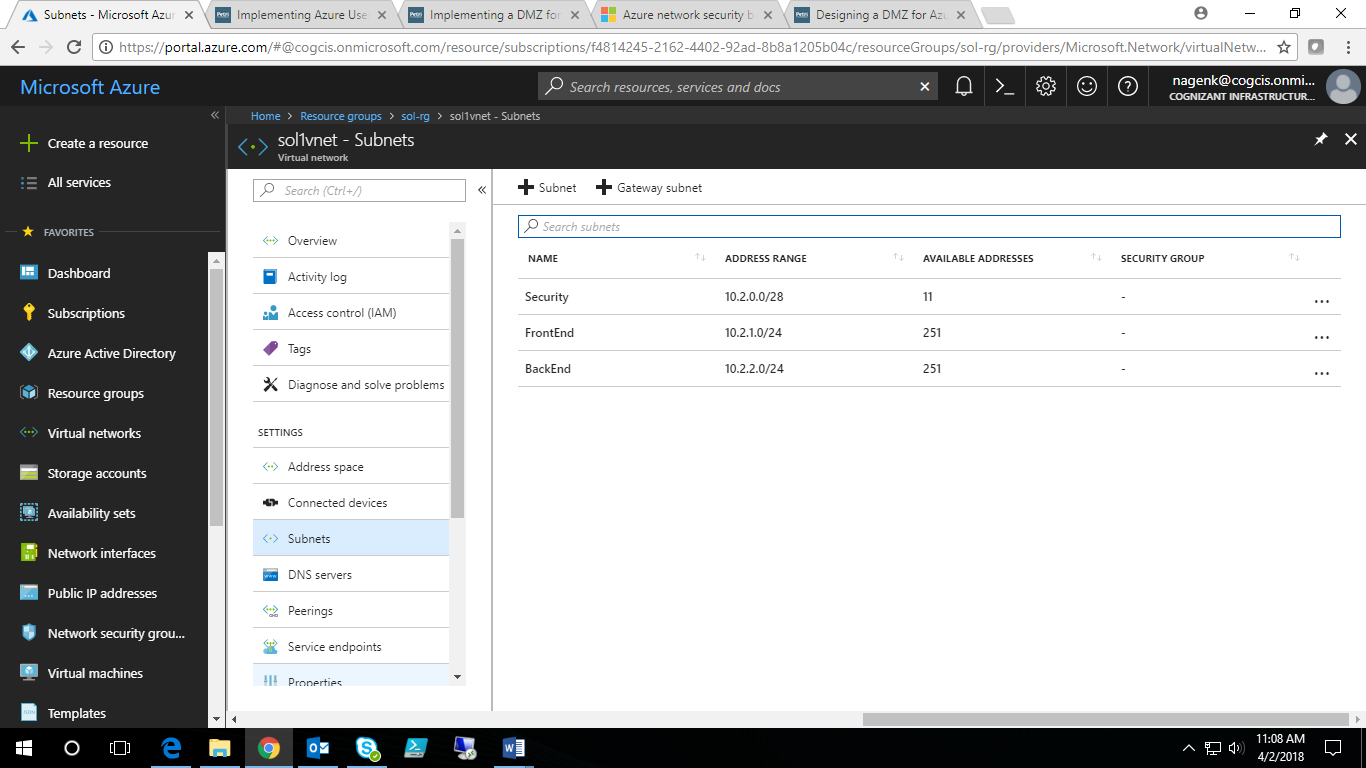
* In this scenario, a subscription contains the following resources:

**Resource Group:**

* A resource group is a containerthat holds all the resources.In this example all the resources are created in a Single resource group in any Azure region as per the requirement.

**Virtual network**:

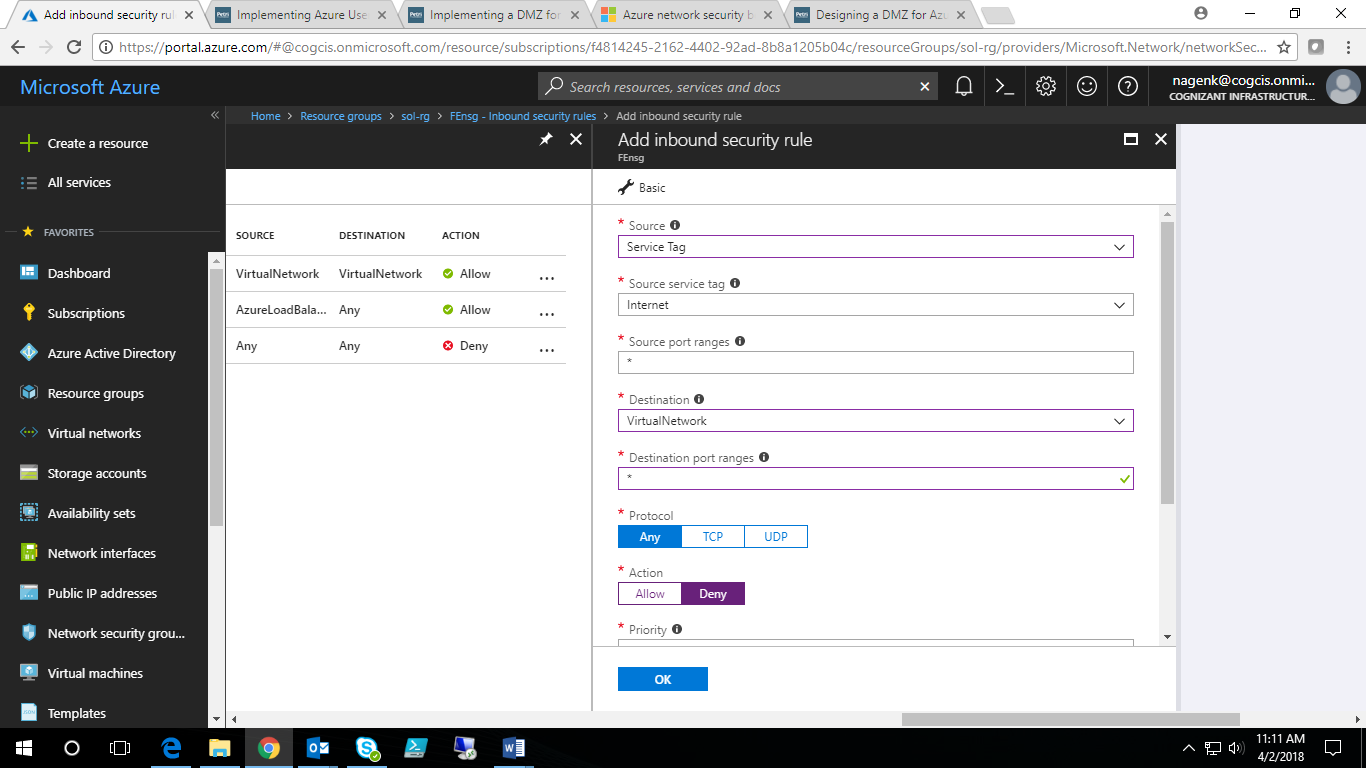
* The virtual network is divided into three subnets, for security, webservers and application servers.



**Figure 2 Virtual Network and Subnets**

**Network security groups (NSGs)**:

* The Network Security Group in this example is that it contains only one rule, which is to deny internet traffic to the entire virtual network. This Network Security Group is then bound only to the Frontend and Backend subnets (not the Security subnet).
* Create two NSGs, one called FrontEnd and one called BackEnd. Each will be configured with an identical single inbound security rule, as shown below.



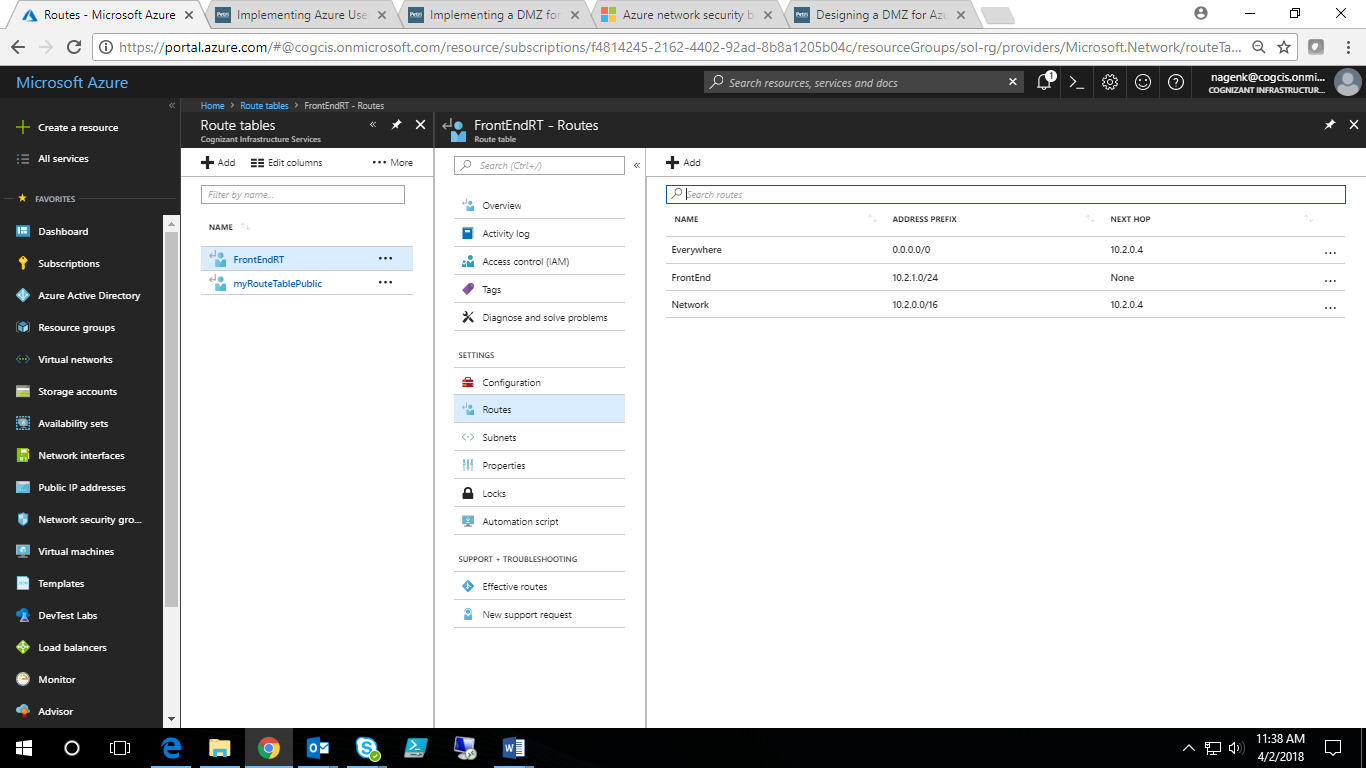
**Figure 3 NSG Rule**

* Associate the FENSG with the FrontEnd subnet and the BENSG with the BackEnd subnet. You can add extend the rules in the NSG’s to provide extra level of security between your FrontEnd subnet and BackEnd subnets based on the requirement.

**User defined routing (UDR)**:

* We need to override default routing between the virtual network subnets and route via the virtual firewall appliance.
* It’s critical to remember to enable IP Forwarding in conjunction with User Defined Routing. IP Forwarding allows it to receive traffic not specifically addressed to the appliance and then forward that traffic to its ultimate destination.
* All traffic must route via the firewall in the security subnet. This requires one routing table for the BackEnd subnet and another for the FrontEnd subnet with at least two rules:
  + **Override internal routing**: We must override the default routes between the FrontEnd and BackEnd subnets with a rule for the virtual network.
  + **Override global routing**: All traffic to all other destinations (0.0.0.0/0) must be routed via the firewall, too.
* The below are the rules for FrontEnd Subnet.

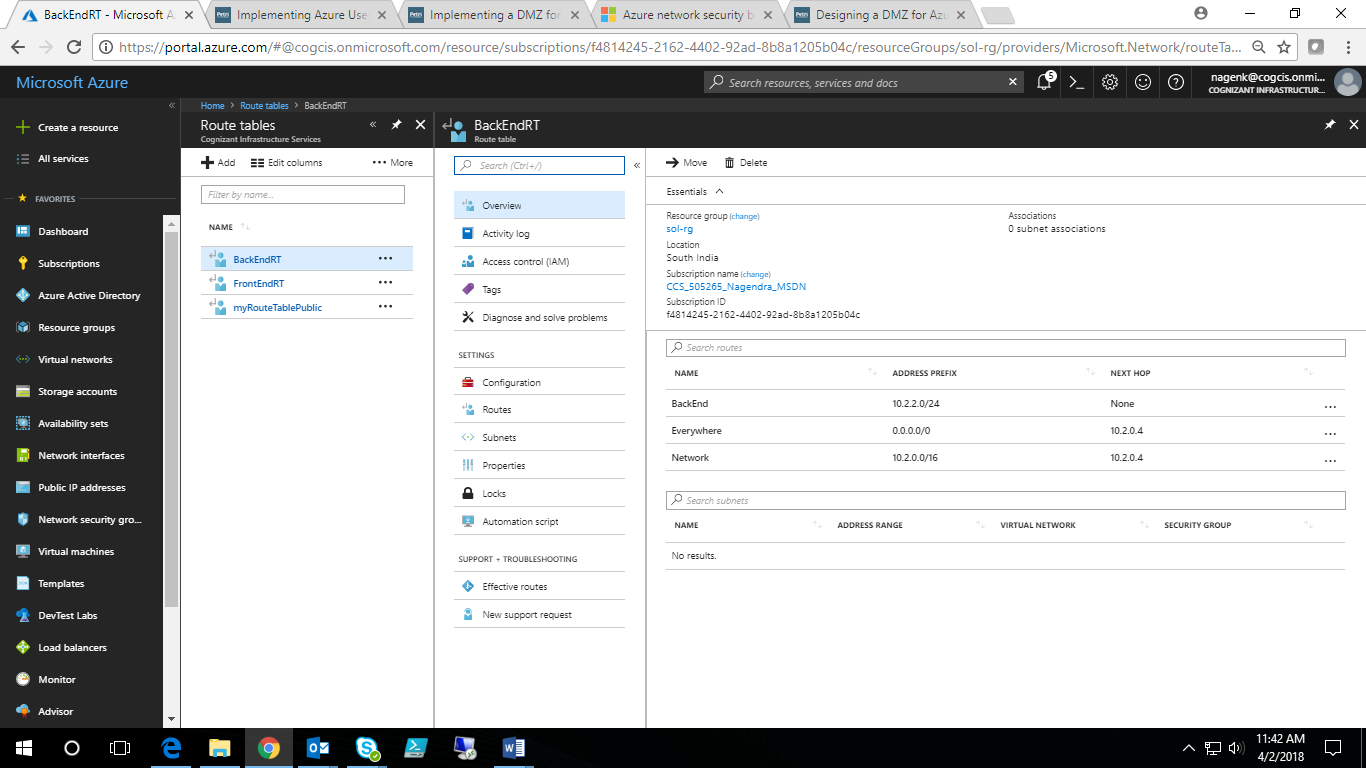
|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop Type** | **Next Hop Address** |
| Network | 10.2.0.0/16 | Virtual appliance | 10.2.0.4 |
| Everywhere | 0.0.0.0/0 | Virtual appliance | 10.2.0.4 |
| FrontEnd | 10.2.1.0/24 | Virtual network | N/A |



**Figure 4 Route Table for FrontEnd Subnet**

* The below are the rules for BackEnd Subnet.

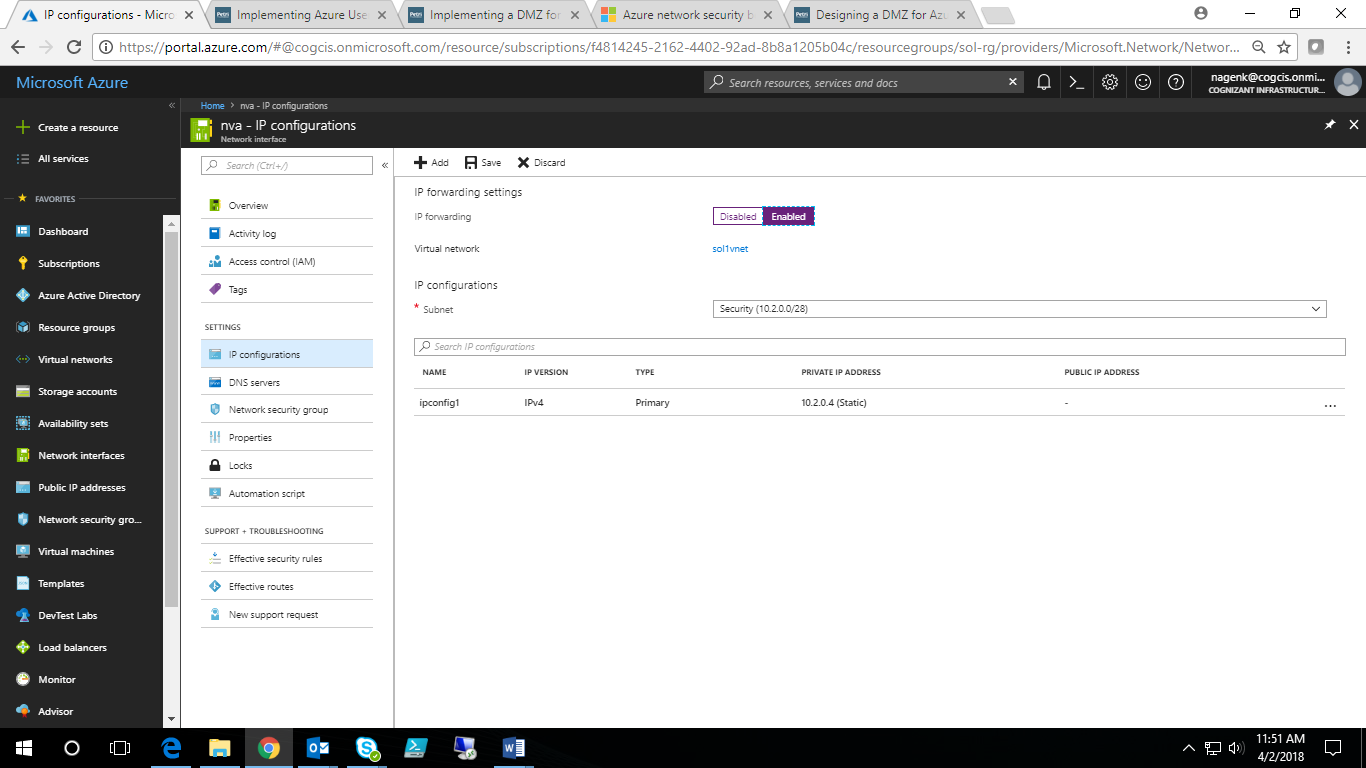
|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop Type** | **Next Hop Address** |
| Network | 10.2.0.0/16 | Virtual appliance | 10.2.0.4 |
| Everywhere | 0.0.0.0/0 | Virtual appliance | 10.0.0.4 |
| BackEnd | 10.2.2.0/24 | Virtual network | N/A |



**Figure 5 Route Table for BackEnd Subnet**

**Virtual firewall appliance**:

* The firewall appliance provides application-layer security between the Internet and the virtual network, and between the virtual network and virtual machines within the network.
* This is a virtual machine that runs a third-party firewall like Palo-alto, Barracuda etc., that can be deployed from Azure marketplace. In addition to the virtual machine pricing, appliance license and bill should be checked with the vendor.
* You must enable IP forwarding for the virtual NIC of this virtual appliance to allow it to route and redirect traffic.
* To enable IP forwarding manually, go to NIC of firewall appliance. In Setting choose IP configurations and Enable IP forwarding.



**Figure 6 Enable IP Forwarding through portal**

* To enable IP forwarding using PS script please refer the PS script in the artifacts repository.

**Virtual Machines**:

* Create One webserver in frontend subnet, two app vm’s.
* Please refer the PS scripts in the artifacts repository to create the VM’s.

**Virtual Machines Security Best Practices**:

* **Install Antimalware software at every azure Virtual machine in the environment**

We can use antimalware software from different security vendors such as Microsoft, Symantec, Trend Micro, and Kaspersky etc. Microsoft Antimalware for Azure Cloud Services and Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software

Brief Description / Solution Code Snippet is available here:

<https://blogs.technet.microsoft.com/ukplatforms/2017/07/31/azure-resource-manager-arm-automate-installation-of-vm-extensions-using-powershell-and-json/>

* **Virtual Machine Disk should be encrypted.**

Azure Disk Encryption for Windows and Linux IaaS VM’s are used to protect and safeguard your data to meet your organizational security and compliance commitments.

Brief Description / Solution Code Snippet is available here:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/security-center-disk-encryption.md>

* **Critical Virtual Machine should be backed up always**

Brief Description / Solution Code Snippet is available here:

<https://docs.microsoft.com/en-us/azure/backup/scripts/backup-powershell-sample-backup-encrypted-vm>

* **Manage virtual machine access using just in time (preview)**

Brute force attacks commonly target management ports as a means to gain access to a VM. If successful, an attacker can take control over the VM and establish a foothold into your environment. One way to reduce exposure to a brute force attack is to limit the amount of time that a port is open. Management ports do not need to be open at all times. They only need to be open while you are connected to the VM, for example to perform management or maintenance tasks. When just in time is enabled Security Center uses Network Security Group (NSG) rules, which allows the access to management ports to a specific amount of time (1 to 24 Hours)

Brief Description / Solution Code Snippet is available here:

<http://www.brainscale.com/enabling-just-time-vm-access/>

* **We should ensure that all latest OS patches**

We should ensure that all latest OS patches are applied vendors like Microsoft,

Apple and RedHat (Applying updates to an encrypted Azure IaaS Red Hat VM using Yum Update) periodically release hotfixes, service packs and security patches to correct known defects in their operating systems. These patches cover the security holes, keeping hackers from further exploiting the security flaws.

* **Complex password policy should be set at each Azure Virtual machine**
* Enforce Password History
* Maximum Password Age
* Minimum Password Age
* Minimum Password Length
* Passwords Must Meet Complexity Requirements
* Passwords must have at least six characters.
* Passwords can’t contain the user name or parts of the user’s full name, such as his first name.
* Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.
* Create one NVA, one webserver in frontend subnet, two app vms maintaining aforesaid Security Best Practices.
* Please refer the PS scripts in the artifacts repository to create the VM’s.

**Managed disks**:

* Managed disks are true managed resources in the resource group, just like other resources. Microsoft is handling the storage on your behalf. All the VM’s in this example are created using managed disks.

**Azure Key vault**:

* All the VM disks are encrypted (BEK, KEK encryption for windows workloads and DM-crypt for Linux workloads).
* When you need encryption to be enabled on a running VM in Azure, Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication. For this purpose, you can create a new ad application or use the existing ad application.

**Diagnostic storage account:**

* A diagnosticstorage account to storevirtual machines diagnostic logs.

**Storage Security Best Practices:**

* **Always encrypt virtual disks and disk storage of the Virtual Machine**

Brief Description / Solution Code Snippet is available here:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/security-center-disk-encryption.md>

* **Use Role Based Access control to secure storage account**

Each Azure subscription has an Azure Active Directory. Users, groups, and applications from that directory can be granted access to manage resources in the Azure subscription that use the Resource Manager deployment model. This type of security is referred to as Role-Based Access Control (RBAC)

Access is granted by assigning the appropriate RBAC role to users, groups, and applications, at the right scope.

**Subscription Level access:**

* To grant access to the entire subscription, we can assign a role at the subscription level.

**Resource Level Access:**

* You can assign specific roles to users, groups, and applications to grant access on specific resources, such as storage accounts.

**Resource Group Level Access:**

* You can assign specific roles to users, groups, and applications to grant access on all of the resources in a resource group.

**Roles for storage include (but are not limited to) the following roles:**

* Owner, Contributor, Reader, Storage Account Contributor, User Access Administrator, Virtual Machine Contributor

**Few Examples**:

* You can give specific users the ability to access the storage account keys, while other users can view information about the storage account, but cannot access the storage account keys.
* **Storage Account Contributor** – They can manage the storage account – they can read the subscription's resource groups and resources, and create and manage subscription resource group deployments. **They can also access the storage account keys**, which in turn means they can access the data plane.
* **User Access Administrator** – They can **manage user access to the storage account**. For example, they can grant Reader access to a specific user.
* **Reader** – They can view information about the storage account, except secrets

**Reference Link**s:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide>

<https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-manage-access-powershell>

* **Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures**

Brief Description / Solution Code Snippet is available here:

**Reference Link:**

<https://social.technet.microsoft.com/wiki/contents/articles/35988.azure-file-storage-implementing-restricted-access-with-powershell-and-net.aspx>

**Security Center:**

* Azure Security Center helps you optimize and monitor network, compute, storage security by providing security recommendations, monitor the state of security configuration and alerting you to threats.

**Azure Security Centre – Why should I use it?**

Monitor security across on-premises and cloud workloads

* Apply policy to ensure compliance with security standards
* Find and fix vulnerabilities before they can be exploited
* Use access and application controls to block malicious activity
* Leverage advanced analytics and threat intelligence to detect attacks
* Simplify investigation for rapid threat response

**Billing – Azure Security Center**

Security Center is offered in two tiers.

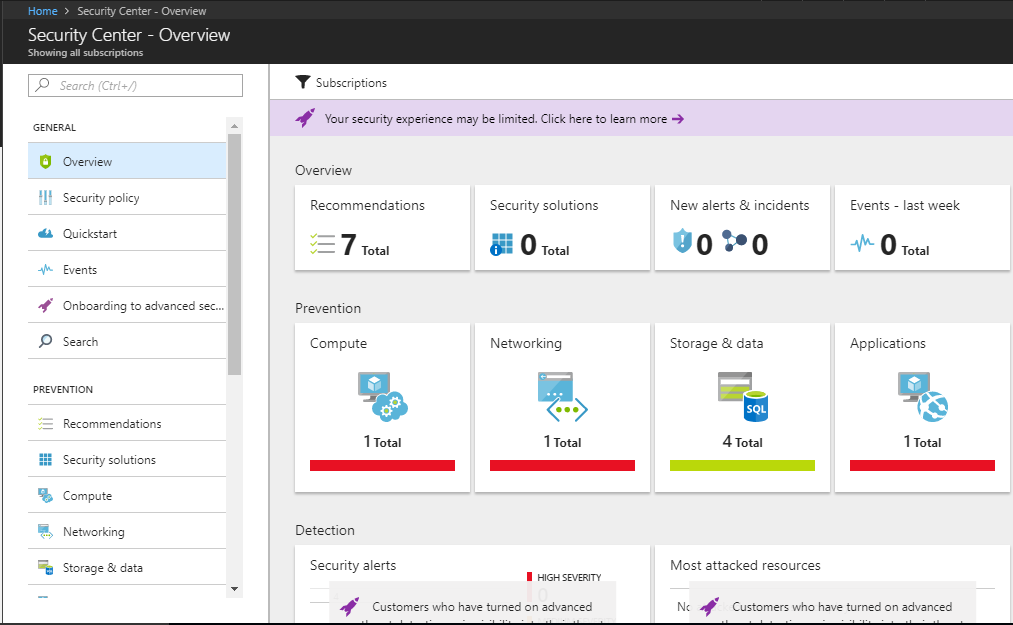
* The Free tier provides visibility into the security state of your Azure resources, basic security policy, security recommendations, and integration with security products and services from partners.
* The **Standard tier** adds advanced threat detection capabilities, including threat intelligence, behavioral analysis, anomaly detection, security incidents, and threat attribution reports. The Standard tier is free for the first 60 days. Should you choose to continue to use the service beyond 60 days, we automatically start to charge for the service. To upgrade, select Pricing Tier in the security policy.
* So we should initialize at **Standard tier**

**Which Azure resources are monitored by Azure Security Cent**er**?**

These are

* Virtual machines (VMs) (including Cloud Services)
* Azure Virtual Networks
* Azure SQL service
* Azure Storage account
* Azure Web Apps (in App Service Environment)
* Partner solutions integrated with your Azure subscription such as a web application firewall on VMs and on App Service Environment

**Security Center - Overview**



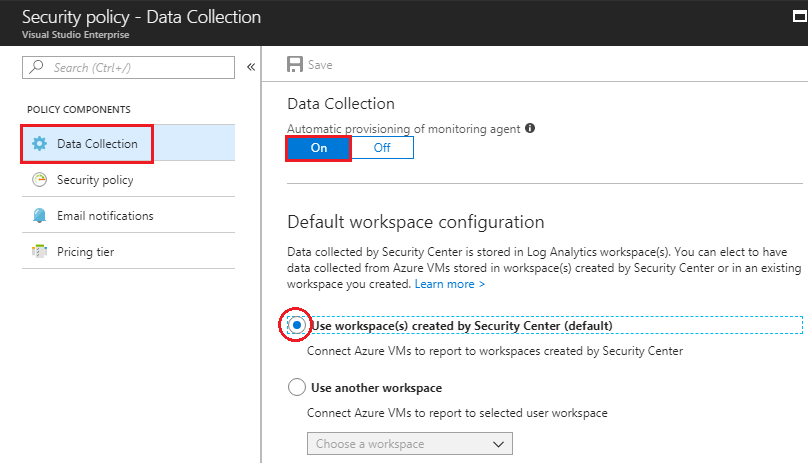
**Set security policies in Azure Security Center**

Please follow below steps

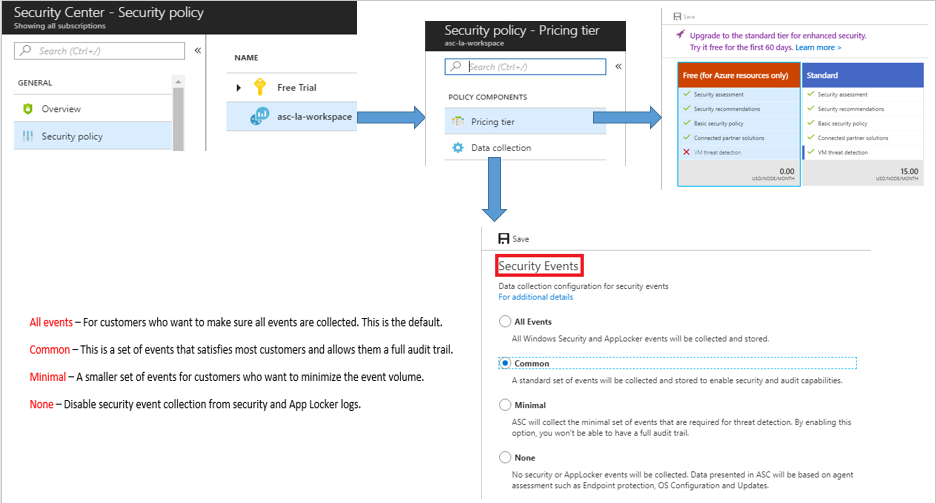
* **Step 1**: Data collection in Azure Security Center
* **Step 2**: Enable/Disable Available security policy definitions
* **Step 3**: Provide security contact details in Azure Security Center
* **Step 4**: Upgrade to Security Center Standard tier for enhanced security

**Data collection in Azure Security Center**

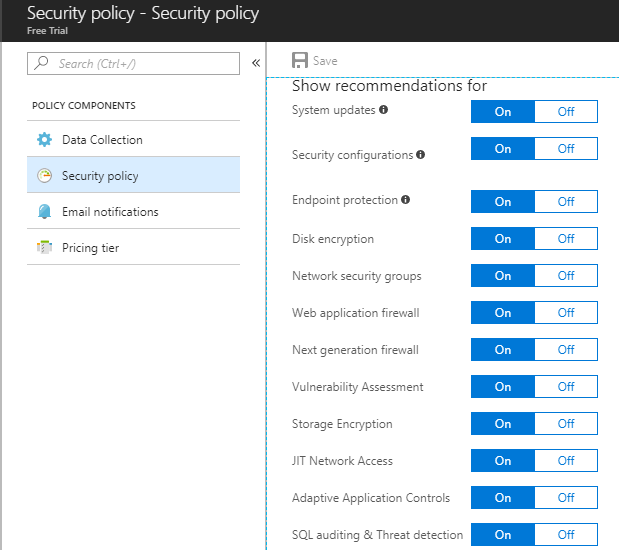
* Security Center collects data from your Azure virtual machines (VMs) and non-Azure computers to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis.
* Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, logged in user, and tenant ID. The Microsoft Monitoring Agent also copies crash dump files to your workspace
* Security Center uses Microsoft Monitoring Agent to collect Security Data from Azure Virtual Machine
* When data collection is enabled, Microsoft Monitoring Agent is automatically provisioned on all the existing and new supported virtual machines that are deployed as a subscription
* We can enable Data Collection in following way described in picture
* You can choose default workspace or use another workspace



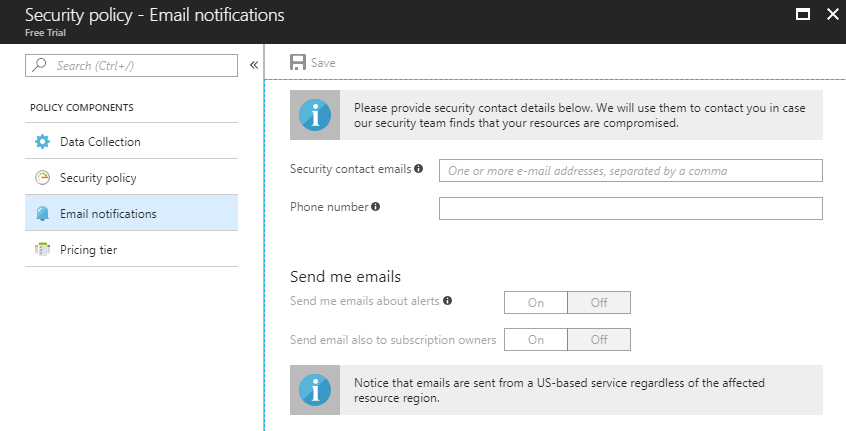
Here in this picture we created a Workspace named asc-la-workspace, we can set pricing tier as Standard set security events as “**Common**”



**Recommendation List – Based on Prevention**

****

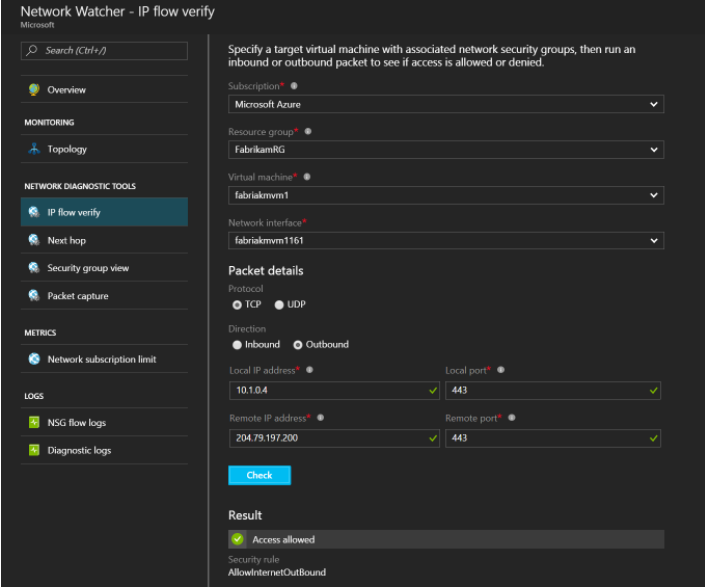
**Email Notification**

****

In this way we can enable data collection in azure Security Center which help us prevent and detect vulnerabilities.

**Network Watcher:**

* By using Network Watcher, Monitor and diagnose networking issues without logging in to your virtual machines (VMs).
* Use NetworkWatcher to test the connectivity between the VM’s, for traffic analytics
* Topology provides overall view, starts from Resource Group to Virtual machine. Interconnections between the resources.
* It routes the incoming packet to next hop. It captures each data which is in and out from the virtual machine. Those captured data are stored in storage account.
* If any issue occurred on the connection between Security subnet and Frontend subnet, we can able to capture flow logs related to traffic by NSG flow logs. This is defined by 5-tuple information like Source IP, Destination IP, Source Port, Destination Port and Protocol.
* IP flow verify checks if a packet is allowed or denied to or from a virtual machine based on 5-tuple information.



* Connection troubleshooting is verifying a possibility to establishing a direct TCP connection from a Virtual machine to an endpoint.

## Artifacts repository

## PowerShell Scripts

### 1.6.1 Create a VNet and three subnets

### 1.6.2 Create a VM in existing subnet

### 1.6.3 Create a NSG and associate to subnet.

### 1.6.4 Enable IP Forwarding for the NVA

### 1.6.5 Create UDR

### 1.6.6 Associate UDR to Subnets

## 1.7 Conclusion

This solution is complete way of protecting and isolating the network. This design allows for monitoring traffic in both directions, and protects not just the inbound application server but enforces network security policy for all servers on this network. Also, depending on the appliance used, full traffic auditing and awareness can be achieved.

## 1.8 References

|  |  |
| --- | --- |
| Reference Title | URL |
| Create Virtual Network with multiple subnets | <https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-powershell> |
| Create a VM with Managed disks | <https://stackoverflow.com/questions/46881847/create-azure-vm-using-powershell-with-managed-disks-using-market-place-image> |
| Create network security groups and associate to subnet | <https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic> |
| Create a route table and associate to subnet | <https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-powershell> |
| Encrypt the VM disks | <https://www.sqlchick.com/entries/2017/2/9/setting-up-azure-disk-encryption-for-a-virtual-machine-with-powershell> |
| Azure Security center | <https://docs.microsoft.com/en-in/azure/security-center/> |
| Network Watcher | <https://docs.microsoft.com/en-in/azure/network-watcher/> |
| Azure storage security | <https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide> |
| Antimalware Installation | <https://blogs.technet.microsoft.com/ukplatforms/2017/07/31/azure-resource-manager-arm-automate-installation-of-vm-extensions-using-powershell-and-json/> |
| Manage VM’s just in time | <http://www.brainscale.com/enabling-just-time-vm-access/> |
| Shared access signature | <https://social.technet.microsoft.com/wiki/contents/articles/35988.azure-file-storage-implementing-restricted-access-with-powershell-and-net.aspx> |

1. Secure hybrid connection with ExpressRoute

## 2.1 Purpose

This solution describes how to protect a hybrid connectivity with ExpressRoute in Azure by using Network Security groups, user defined routes and a firewall appliance created from market place. The virtual network contains multiple subnets – for firewall appliance, webservers and application servers is connected to on-premises network using an expressroute circuit. Traffic transits only the service provider network and the Microsoft Azure network, never touching the Internet.

## 2.2 Executive Summary

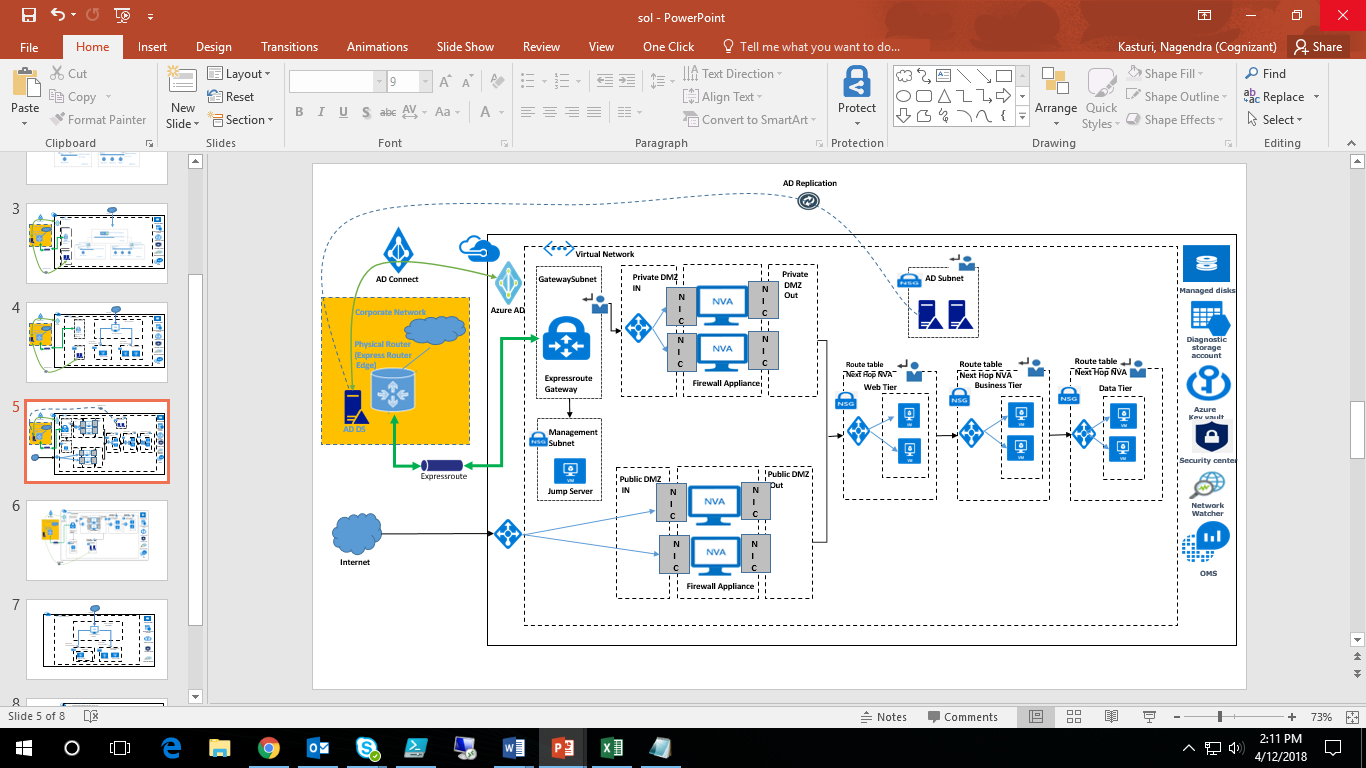
This design shall only be covering about securing a virtual network connected with on-premises network using expressroute.

This Solution is part of Azure Security best practices that includes Network, compute and storage security, AD, Identity and operations security.

This design is only focused on securing a virtual network which is connected to on-premises network using a firewall appliance and user defined routes and network security groups but not establishing hybrid cloud connectivity.

This solution also talks about Azure AD security best practices assuming that already there is a sync enabled between on-premise AD and Azure AD.

## 2.3 Architecture



**Figure 7 Architecture**

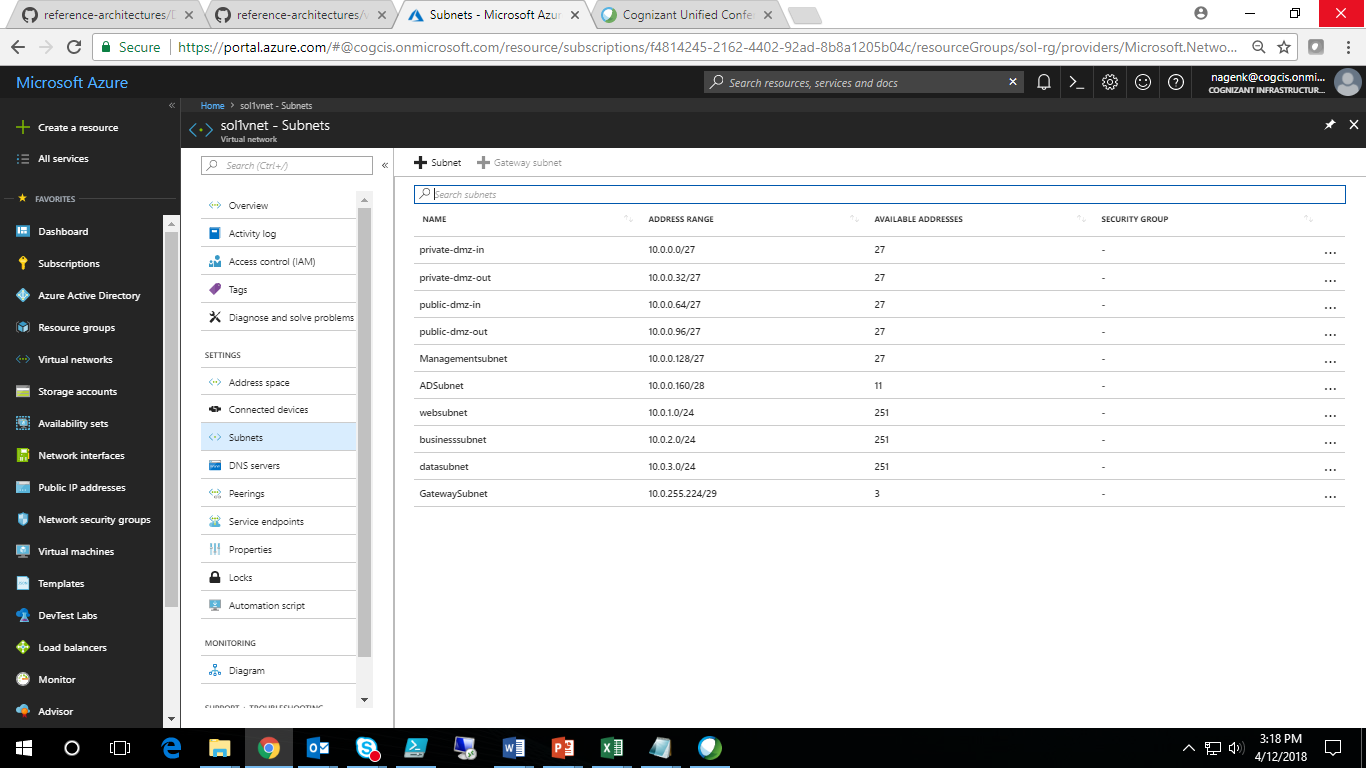
## 2.4 Detailed environment description

**Resource Group:**

* A resource group is a containerthat holds all the resources.In this example all the resources are created in a Single resource group in any Azure region as per the requirement.

**Virtual network**:

* The virtual network is divided into five subnets- Security Subnet, FrontEnd Subnet, BackEnd Subnet, GatewaySubnet and ADSubnet.
* A Virtual Network is created with address range 10.0.0.0/16. Below are the subnets that are created.



**Figure 8 Subnets**

**Network Connectivity:**

* Express route connectivity is selected here as it lets you create private connections between Microsoft datacenters and infrastructure that’s on your premises or in a colocation facility.
* Connectivity between your on-premises infrastructure and infrastructure hosted in Microsoft Azure is private and secure through your ExpressRoute circuit. Your traffic never traverses the public Internet when connecting to your own virtual machines or even connecting to other Microsoft Azure public services such as Storage and SQL Database through ExpressRoute.
* The security advantage is clear: the connection doesn’t traverse the Internet and therefore isn’t exposed to all the potential risks that are inherent in an Internet connection.
* After your ExpressRoute circuit has been provisioned you will need to create and link one or more virtual networks to the circuit. You can link multiple virtual networks to an ExpressRoute circuit from any region on the same continent. For example: West US and East US may connect directory as well as North Europe and West Europe. However, virtual networks created in West US and North Europe could not be linked together on the same circuit.

**Network security groups (NSGs)**:

* The Network Security Group in this example is attached at each subnet except GatewaySubnet.
* Please refer the excel that contains the nsg rules for various subnets.

**User defined routing (UDR)**:

* We need to override default routing between the virtual network subnets and route via the virtual firewall appliance. You can now use User Defined Routing (UDR) with ExpressRoute and VPN Gateways to force outbound and inbound cross-premises traffic to be routed to a network virtual appliance (NVA).
* It’s critical to remember to enable IP Forwarding in conjunction with User Defined Routing. IP Forwarding allows it to receive traffic not specifically addressed to the appliance and then forward that traffic to its ultimate destination.
* Route tables are created and associated to GatewaySubnet, ADSubnet, Web Tier, Business Tier and Data Tier subnets. Please refer the below excel for more details.

**Virtual firewall appliance**:

* The firewall appliance provides application-layer security between the Internet and the virtual network, and between the virtual network and virtual machines within the network.
* This is a virtual machine that runs a third-party firewall like Palo-alto, Barracuda etc., that can be deployed from Azure marketplace. In addition to the virtual machine pricing, appliance license and bill should be checked with the vendor.
* You must enable IP forwarding for the virtual NIC of this virtual appliance to allow it to route and redirect traffic.
* To enable IP forwarding manually, go to NIC of firewall appliance. In Setting choose IP configurations and Enable IP forwarding.

**Network, Subnets, NSG and UDR details:**

****

**Azure AD:**

* On-premises AD is synced with Azure AD by using AD Connect.

**Virtual Machines**:

* Create web tier, business tier and data tier VM’s, two ADDS servers and a Jumpserver.
* All the VM’s in the azure VNet are domain joined to additional domain controllers in ADSubnet.
* AD Replication is enabled between on-premises AD server and ADDS VM’s in Azure.

**Managed disks**:

* Managed disks are true managed resources in the resource group, just like other resources. Microsoft is handling the storage on your behalf. All the VM’s in this example are created using managed disks.

**Azure Key vault**:

* All the VM disks are encrypted (BEK, KEK encryption for windows workloads and DM-crypt for Linux workloads).
* When you need encryption to be enabled on a running VM in Azure, Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication. For this purpose, you can create a new ad application or use the existing ad application.

**Diagnostic storage account:**

* A diagnosticstorage account to storevirtual machines diagnostic logs.

**Security Center:**

* Azure Security Center helps you optimize and monitor network, compute, storage security by providing security recommendations, monitor the state of security configuration and alerting you to threats.

**Network Watcher:**

* By using Network Watcher, Monitor and diagnose networking issues without logging in to your virtual machines (VMs).
* Use NetworkWatcher to test the connectivity between the VM’s, for traffic analytics

**Operational Security:**

* With the help of Network Performance Monitor (NPM), Monitor network performance privately connected expressroute circuit between physical router and Gateway subnet.
* This can be achieved by install and configure monitoring agents on both on-premise and azure. Communication between on-premise and Azure taken care by configuring NSG rule.

## 2.5 Artifacts repository

## 2.6 PowerShell Scripts

## 2.7 Conclusion

The addition of an ExpressRoute Private Peering network connection can extend the on-premises network into Azure in a secure, lower latency, higher performing manner. NSG’s and UDR are used to secure the traffic in the azure virtual network.  Also, depending on the appliance used, full traffic auditing and awareness can be achieved.

## 2.8 References

|  |  |
| --- | --- |
| Reference Title | URL |
| Create Virtual Network with multiple subnets | <https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-powershell> |
| Create a VM with Managed disks | <https://stackoverflow.com/questions/46881847/create-azure-vm-using-powershell-with-managed-disks-using-market-place-image> |
| Create network security groups and associate to subnet | <https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic> |
| Create a route table and associate to subnet | <https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-powershell> |
| Encrypt the VM disks | <https://www.sqlchick.com/entries/2017/2/9/setting-up-azure-disk-encryption-for-a-virtual-machine-with-powershell> |
| Azure Security center | <https://docs.microsoft.com/en-in/azure/security-center/> |
| Network Watcher | <https://docs.microsoft.com/en-in/azure/network-watcher/> |
| Azure AD Best practices | https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices |
| Azure AD connect | https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect |
| Operational Security | https://docs.microsoft.com/en-us/azure/security/azure-operational-security |