Azure Security Center:

**Networking:**

1. Missing NSG for Subnets:

Some of the subnets doesn’t have NSG by default. Navigate to the respective subnets and the appropriate NSG rules for the subnets.

b. Apply Just in Time Access Control (Not Required):

This is not recommended, As only the user who has write access to VM can able to login.

**Note:** So if someone, who don’t have write access to VM in Azure Portal, can’t access or raise a request to login.

FYI: <https://www.thomasmaurer.ch/2018/07/azure-just-in-time-vm-access/#prettyPhoto>

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

c. Add a next gen firewall for Public IP Endpoints

It has a pricing model and its basically firewall in front of the Public Endpoints.

FYI:<https://docs.microsoft.com/en-us/azure/security-center/security-center-add-next-generation-firewall>

**IAM**:

1. Enable MFA:

Enable mfa for accounts with owner permission.

FYI: <https://docs.microsoft.com/en-gb/azure/active-directory/authentication/howto-mfa-userstates>

**Compute**:

1. Endpoint protection

Enable Microsoft Anti-malware on VM’s

FYI: <https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware>

b. System Updates

We can schedule System Updates from “Update management” from Azure Automation Account. Also, Some of the VM’s not support Azure Update management, We need to use ansible script to do patch updates.

c. Disk Encryption:

Azure Disk Encryption can be done using Azure keyvault and Service Principal. We have already script to enable encryption for new VM’s. For existing VM’s, we need to modify the script and test once.

FYI:<https://blogs.msdn.microsoft.com/ejarvi/2018/03/30/encrypting-data-disks-on-linux-with-azure-disk-encryption/>

d. Web Application Firewall

Azure App Gateway should be enabled and then we can configure WAF for Web Apps. It has a pricing model.

FYI: <https://docs.microsoft.com/en-us/azure/application-gateway/overview>

**Data Security**:

1. Enable Auditing on SQL DB

Select Auditing on SQL DB and select ‘ON’.

b. Enable Auditing on SQL server

Select Auditing on SQL server and select ‘ON’.