Expertise
and insight
for the future

Sefika Bezirganoglu

Securing Cloud with Palo Alto Networks Firewalls

Metropolia University of Applied Sciences

Master of Engineering Information Technology

Master's Thesis

11 November 2020

Author Title Number of Pages Date	Sefika Bezirganoglu Securing Cloud with Palo Alto Networks Firewalls 33 pages + 1 appendix 11 November 2020
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Ville Jääskeläinen, Principal Lecturer

The Virtual Network, the fundamental building block in the cloud IaaS service, is working different way compared to traditional networks. Therefore, network devices such as firewalls should be configured differently. Default routing in the virtual network should be altered to make sure all traffic travels via the firewall. Some firewall features such as high availability is not working the same way compared to on-premises deployment, because of cloud limitations. Load balancer should be implemented instead of high availability feature. As we have new tools and a new environment, a new process to deploy firewalls in a cloud environment is needed.

The aim of this research was to find a process to implement a Palo Alto Networks firewall in Azure, which would standardize the configuration while minimizing the deployment time and create an implementation guide based on the selected process.

Azure Portal, Azure CLI and Azure Resource Manager Templates were evaluated for implementing the firewall. Azure Resource Manager Template was selected, as it is very fast and support automation.

An ARM template was created based on Palo Alto Networks “Azure Architecture Guide”. The ARM template uses parameters to create resources in Azure. To minimize the template file modification, parameters values are provided with a parameters file in .json format. Using separate parameters files allows to use the same ARM template to implement a firewall in different customer environments.

A Python script was developed to create parameters file in a correct format using an Excel file as input. The Excel file was used to collect information such as IP addresses, FQDNs etc. from customer.

The results of this study show how ARM templates can be used to build an infrastructure in Azure, including Palo Alto Networks firewalls, load balancers, virtual network, and subnets. Using ARM templates minimizes the time required for deployment significantly. Almost all process is automated where very little input needed from the expert, therefore it also minimizes the human error.

Keywords	Palo Alto Networks, Firewall, Azure Resource Manager Template

Contents

List of Figures

List of Abbreviations

ARM	Azure Resource Manager
CLI	Command Line Interface
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
NSG	Network Security Groups
UDR	User Defined Routes
OSI Model	Open Systems Interconnection Model
VM	Virtual Machine
DMZ	Demilitarized Zone (Perimeter Network)
FQDN	Fully Qualified Domain Name
OWASP	Open Web Application Security Project
RDP	Remote Desktop Protocol
SSH	Secure Shell
AV	Anti-Virus
IPS	Intrusion Prevention System
C2	Command and Control
PAYG	Pay As You Go. A payment model in Azure.
ELA	Enterprise License Agreement
NGFW	Next Generation Firewall
JSON	JavaScript Object Notation
VNet	Virtual Network resource in Azure
URL	Uniform Resource Locater
QoS	Quality of Services

1 Introduction

Cloud computing is growing fast, and many organizations are moving their systems to cloud to benefit increasing performance, reliability, and scalability while minimizing the overall cost of ownership and time to deployment.

In cloud, security is one of the most important areas that should be addressed. Network perimeters are not existing anymore, and increased availability comes with an increased attack surface. While cloud providers are responsible for securing the cloud infrastructure, configuration mistakes by organization experts, exposes organization's data to public internet.

Not every organization moves cloud with the cloud native solutions, which requires to use PaaS or SaaS resources. Some organizations prefer to have the IaaS model: to have more control on the resources, or just as a first step for their cloud journey. Organization using IaaS model is responsible not only the data security, but also security of the network, operating systems, and applications. Security appliances such as virtual firewalls add enhanced security features on application level in addition to security features provided by the cloud service provider.

Security vendors who have been providing on premises solutions are now bringing new products to a cloud and those solutions are working in a different way compared to on premises versions. As we have new tools and a new environment, a new process to deploy security devices, especially firewalls in a cloud environment should be created.

Telia Cygate is an ICT service provider, focusing on networks, security and cloud computing and it has 9 offices around Finland with more than 400 employees. Telia Cygate works as a partner for many of the biggest security vendors, and its customers expect Telia Cygate to guide and help them on their journey to a cloud.

1.1 Objective

The objective of this study is to develop a process for firewall implementation in the cloud environment. Well defined process and automation will improve the firewall implementation in a cloud environment and minimize the mistakes, therefore increase the security and quality of the implementation.

Microsoft Azure is one of the biggest public cloud providers, and it was selected in this study because it is the most used cloud provider in Finland based on the survey conducted by M-Brain Finland Oy (see Figure 1).

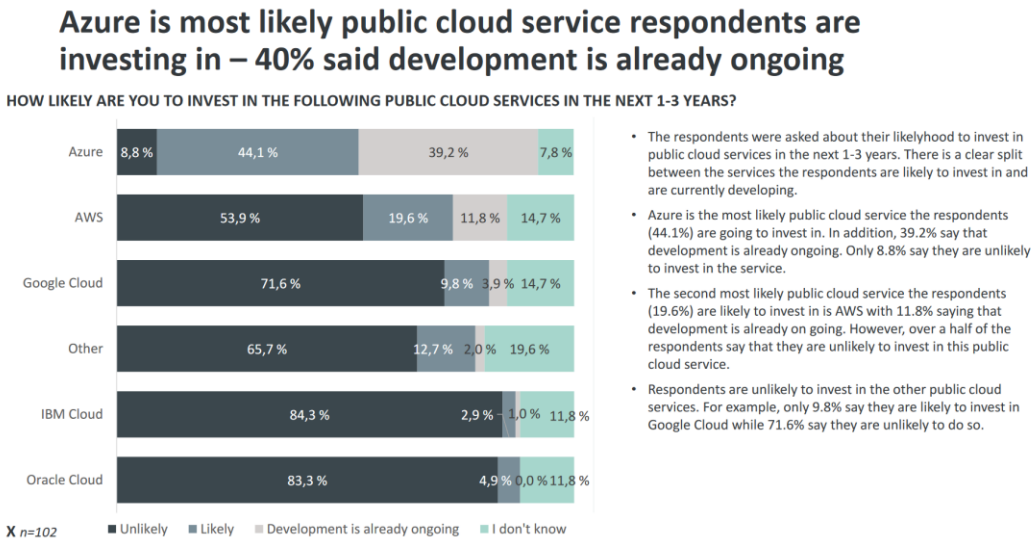

Figure 1. Investment on Public Cloud Services [1]

Palo Alto Networks is a global cybersecurity company, and its Next Generation Firewall (NGFW) was recognized by Gartner as the Leader in its 2019 Magic Quadrant for Network Firewalls for ability to execute and furthest position for completeness of vision.

> "We're honored that Gartner has recognized us as a Leader in eight consecutive Gartner Magic Quadrants for Network Firewalls," said Jesse Ralston, SVP, Products, Network Security at Palo Alto Networks. "In the last seven months, Palo Alto Networks has made significant improvements to the next-generation firewall to extend its leadership position. Now, the fastest-ever next-generation firewall from Palo Alto Networks has more than 60 new features and a revolutionary new DNS subscription." [2]

In this research firewall deployment options in a cloud were evaluated based on:

- Required skills by consultant
- required tools

- time required to complete the deployment.

Azure Resource Manager (ARM) templates with Azure Command Line Interface (CLI) was selected for deployment, because while it is minimizing the time required for the deployment, it also requires less programming skills.

Qualitive methods was used to conduct the research: Palo Alto Networks documentation, trainings, Azure documentation pages, and technical documents/discussions on the internet was used to acquire the technical knowledge. Azure cloud was used to develop and test the process.

2 Project Specifications and Plan

This chapter introduces the project specifications and project plan. The project output is a well-documented process which is based on a tested design, which is repeatable in Azure, and reduces deployment time. The process should be automated and manual task should be limited.

2.1 Project Plan

This subchapter explains the project plan for the research. Note that acquiring knowledge for Azure environment and Palo Alto Networks firewall implementation for the Azure continued until the solution was automated.

After solution was automated the process entered the Life Cycle where it should be tested and introduced to the team. Based on test results or team feedbacks it should be updated and tested again.

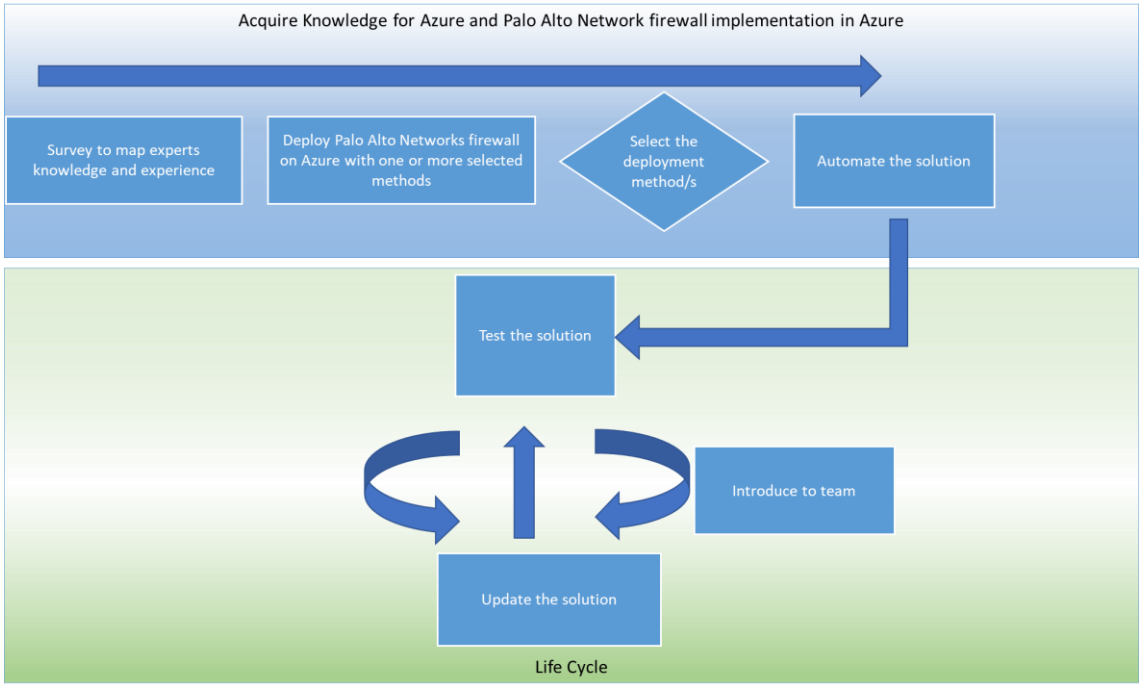

Figure 2. Project Plan

While this project was ongoing Palo Alto Networks published a new document for Architecture for Azure and implementation guide based on the reference architecture. For this reason, the project focus changed from creating an implementation guide to automation of the implementation.

3 Firewalls in Cloud Environment

This chapter provides technical knowledge required to deploy Palo Alto Networks vm-series firewall to Azure.

3.1 Cloud Computing

Cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. "by NIST (US The National Institute of Standards and Technology). [3]

Microsoft Azure defines cloud computing as "is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud")".[4]

There are various definitions of the cloud computing, but they all have common points: shared pool of resources with easy to deploy and released. NIST lists the essential characteristics of the cloud as below: [3]

- on-demand self-service
- broad network access
- resource pooling
- rapid elasticity
- measured service.

3.1.1 Cloud Deployment Models

NIST defines four deployments models for cloud:

- Private Cloud: It is owned by one business or organization. The organization is responsible to purchase, configure and management of the hardware and software. Network Infrastructure also organization responsibilities.

- Public Cloud: It is owned by cloud provider and services are offered to public and reachable via internet. Cloud infrastructure is deployed and managed by the cloud provider.

- Community Cloud: It is owned by two or more organizations with a shared interest.

- Hybrid Cloud: It is combination of two or more cloud deployment models: public, private and community cloud. Organizations prefer this model if they do not want to move some of their data to public cloud because of legal requirements

3.1.2 Cloud Service Models

In public cloud there are 3 service model, which defines the level of the responsibilities

- Infrastructure as a Service (IaaS): Cloud service provider provides and manage computing (servers, virtual machines), networking and storage resources. Consumer is able to run software they choose including the operating systems and applications.

- Platform as a Service (PaaS): Cloud service provider responsible from computing infrastructure and middleware, and provides environment for the development, deployment, and administration tools to consumer. Consumer does not have control over operating system but have control over the configuration settings for the application.

- Software as a Service (SaaS): Cloud provider provides and manage software application in a cloud infrastructure addition to PaaS.

3.1.3 Shared Responsibility Model

Cloud service provider and organization are both responsible for the security, but based on the cloud service model, the area of the responsibilities change as shown in Figure 3. Regardless of the service model, organization is always responsible for data, endpoints, account, and access management.

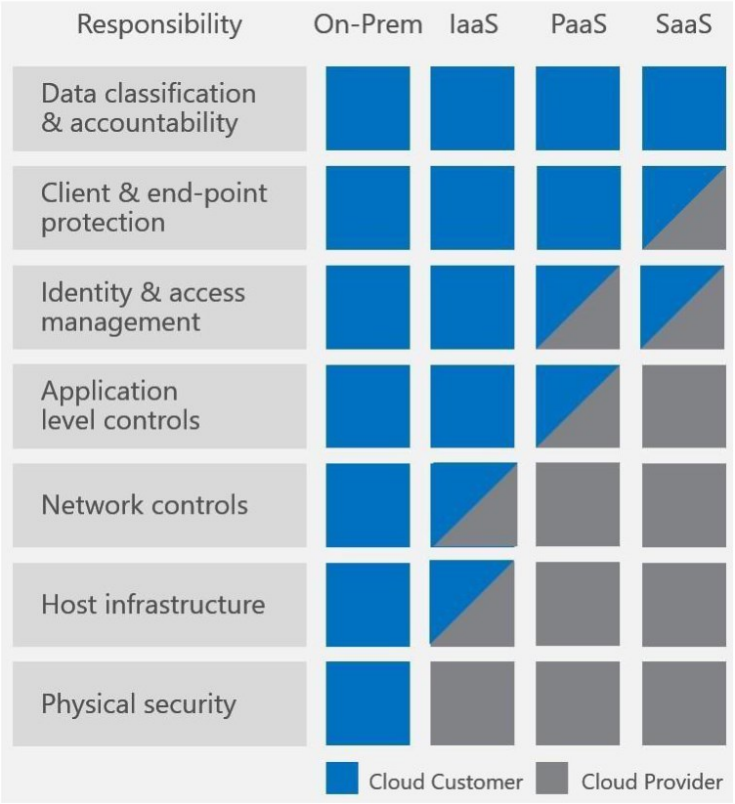

Figure 3. Shared responsibility model [5]

3.1.4 Cloud Native Security Tools

Infrastructure as a Service model allows consumers to create their own virtual network in a cloud. Azure offers below listed options for the network security:

- Network Security Rules (NSG): They provide basic network level access control. Traffic based on IP address and Port numbers can be allowed or denied.
- User Defined Routes (UDR): They alter the default routing tables in virtual network and route the defined traffic enters and leaves virtual network through specific location or device.
- Forced tunneling: Using UDR consumer can ensure that the services they own are not allowed to initiate a connection to internet.
- Virtual network security appliances: NSG, UDR and Forced tunneling provides a level of security in the Open Systems Interconnection model (OSI model) network

and transport layer. Virtual Network Security appliances will provide security for the higher levels.

- VPN Gateways: In hybrid cloud environment consumer can connect on-premises resources to public cloud resources with VPN tunnels over Internet.
- Express Route: Consumers who needs highest level of security for their cross-premises connections will prefer to use dedicated WAN link.

3.2 Best Practices for Azure Network Security

Azure Fundamentals Documentation for security lists the best practices for the network security as below [6]:

Use strong network controls

Azure recommends to centralize:

- Management of core network functions such as ExpressRoute, virtual network and subnet provisioning, and IP addressing.
- Governance of network security elements, such as network virtual appliance functions such as ExpressRoute, virtual network and subnet provisioning, and IP addressing.

Logically segment subnets

- Do not assign allow rules with broad ranges.
- Segment the larger address space into subnets.
- Create network access controls between subnets using network security group.
- Avoid small virtual networks and subnets to ensure simplicity and flexibility.
- Simplify network security group rule management by defining application security group.

Adopt a Zero Trust approach

- Give conditional access to resources based on device, identity, assurance, and network location using Azure AD conditional access.
- Enable port access only after workflow approval.
- Grant temporary permissions to perform privileged tasks, which prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it.

Control routing behaviour

When one creates a Virtual Machine (VM) on an Azure virtual network, the VM can connect to any other VM on the same virtual network, even if the other VMs are on different subnets. Azure recommends to configure user defined rules when deploying a security appliance for a virtual network.

Use virtual network appliances

Network security groups and user-defined routing can provide a certain measure of network security at the network and transport layers of the OSI model. Enabling security at high level of the stack requires to deploy virtual network security appliances provided by Azure partners. Network security capabilities of virtual network security appliances include: firewalling, intrusion detection/intrusion prevention, vulnerability management, application control, network-based anomaly detection, web filtering, antivirus, and Botnet protection.

Deploy perimeter networks for security zones

Azure recommends using a perimeter network (DMZ) for all high security deployments to enhance the level of network security and access control for Azure resources. Azure or a third-party solution can be used to provide an additional layer of security between resources and the Internet.

Azure native controls: Azure firewall and the web application gateway firewall in application gateway offers basic security with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, Fully Qualified Domain Name (FQDN) filtering, support for Open Web Application Security Project (OWASP) core rule sets, and simple setup and configuration.

Third-party offerings: Next-Generation Firewall (NGFW) and other third-party offerings that provide familiar security tools and significantly enhanced levels of network security can be found in Azure Marketplace. Configuration might be more complex, but a third-party offering might allow one to use existing capabilities and skillsets.

Avoid exposure to the internet with dedicated WAN links

Cross-premises connectivity allows the company to connect its on-premises networks to Azure virtual networks. Two cross-premises connectivity solutions are available:

- Site-to-site VPN

- Azure ExpressRoute.

Optimize uptime and performance

Use Load balancing to increase the availability and performance. For this Azure provides four options:

- Azure application gateway: an HTTP web traffic load balancer.
- External load balancer: for connections from devices located on the internet
- Internal load balancer: for connections from devices in the Azure virtual network
- Traffic manager: allows load balance of the services based on the location of the user.

Disable RDP/SSH access to virtual machines

Remote Desktop Protocol (RDP) and Secure Shell (SSH) enable the management of VMs from remote locations. Direct RDP and SSH access to VMs from internet should be disabled as attackers can use brute force techniques to gain access to virtual machines.

Point-to-site VPN, site-to-site VPN or Express route can be used to connect to VMs with RDP and SSH.

Secure critical Azure service resources to only virtual networks

Virtual network service endpoints extend virtual network private address space, and the identity of virtual network to the Azure services, over a direct connection. Endpoints allow to secure critical Azure service resources to only virtual networks. Traffic from virtual network to the Azure service always remains on the Microsoft Azure backbone network.

3.3 Next Generation Firewalls

Here are the features of the Palo Alto Networks firewall that adds value to security as a Next Generation firewall.

- Threat Prevention: protects the network from advanced threats by identifying and scanning all traffic – applications, users, and content – across all ports and protocols.
- Antivirus (AV) Profile: Scan traffic for the viruses, and detects infected files being transferred with the application. Based on the defined action traffic can be blocked or alert is created in the threat log.

- Anti-Spyware Profile: Detects spyware downloads and connections initiated by spyware and command-and-control (C2) malware.
- Vulnerability Protection Profile: Determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.
- Global Protect: Provides security for mobile end users by allowing easy and secure connection to corporate network or cloud.
- WildFire: cloud-based malware detection and multiple analysis identifies previously unknown malware and generates signatures that can be used to detect and block the malware by firewall.
- PAN-DB URL Filtering: Allows all web-traffic to be compared against the URL filtering database and based on category security, QoS, decryption, and Captive Portal policies can be enforced.
- DNS security: cloud-based analytics platform providing access to DNS signatures generated using advanced predictive analysis and machine learning.

Palo Alto Networks provides physical appliances and virtualized firewalls (VM-Series). VM-Series firewall is supported in AWS, Azure, Google cloud, vmWare, ESXi, NSX, open stack, KVM, cmWare, vCloudAir and Microsoft Hyper-V

Type of VM-Series firewall provided by Palo Alto Networks are listed in the table below.

Table 1. VM-Series firewall capacities and requirements [7 p.22]

	VM-100	VM-300	VM-500	VM-700
CPU cores	2/2	2/4	2/8	2/16
Minimum memory	6.5GB	9GB	16GB	56GB
Minimum disk capacity	60GB	60GB	60GB	60GB
Maximum Sessions	250,000	819,200	2,000,000	10,000,000
Security rules	1,500	10,000	10,000	20.000
Security zones	40	40	200	200
IPSec VPN tunnels	1000	2000	4000	8000
SSL VPN tunnels	500	2000	6000	12,000

Vertical scaling, also known as *scale up* and *scale down*, means increasing or decreasing virtual machine (VM) sizes in response to a workload. Horizontal scaling, also referred to as *scale out* and *scale in*, where the number of VMs is altered depending on the workload.[8] Because of throughput restrictions scale out is a preferable method for firewalls in a cloud.

3.4 Palo Alto Networks VM-Series firewall in Microsoft Azure

Palo Alto Networks VM-Series firewall can be deployed to Azure as a resource which is offered via Azure public Marketplace. Different licensing and size options are available for the VM-Series firewall deployment in Azure.

3.4.1 Licensing Options

VM-Series firewalls can be licensed using one of the below licensing models. Selected licensing model cannot be changed for the resource after it is created. If different licensing model is needed, then resource should be deleted and added with correct license model.

- Use-based Licencing or Pay as you go (PAYG): The license is purchased from Azure public Marketplace and it is billed hourly. Only available for VM-300 with below bundles:

Bundle 1: VM-300 capacity license, Threat Prevention license (IPS, AV, malware prevention) and premium support

Bundle 2: VM-300 capacity license, Threat Prevention license (IPS, AV, malware prevention), DNS Security, GlobalProtect, WildFire, PAN-DB URL Filtering License and premium support

Firewalls are licensed and ready for use after deployment.

- Bring Your Own License: The license can be purchased from a partner, reseller or from Palo Alto Networks. License should be deployed to appliance with authorization code.
- Enterprise License Agreement (ELA): It provides a fixed price licensing option, where license token pools allow to deploy any model of the VM-Series. Based on the firewall model specified number of tokens will be deduct from the license token pool. ELA deployments use a single license authorization code which allow automation of deploying firewalls in the cloud.[9]

3.4.2 Creating VM-series firewall in Azure

Palo Alto Networks VM-series firewall deployment requires below listed resources in Azure.

- Virtual machine: D-series: General Purposes: 1-4 CPU, 4GB-64 GB RAM

Table 2. VM-Series mapping to Azure virtual machine sizes [7 p. 22]

Virtual Machine Size	VM-100	VM-300	VM-500	VM-700
Standard DS3_v2 (4 Interfaces)	Recommended	Recommended	x	x
Standard DS4_v2 (8 Interfaces)	x	x	Recommended	x
Standard DS5_v2 (8 Interfaces)	Supported	Supported	Supported	Recommended

- Multiple virtual NICs: Minimum three NICs one for each Management, Trust and Untrust interfaces
- Virtual Network and Subnets: If no virtual network exist new one should be created. New subnets will be created, one for each firewall interfaces
- Storage account
- Public IP addresses: One for Management interface, outbound traffic from VNet, and also Load balancer or Application gateway external interface.
- Availability Sets: For High availability AS should be defined for firewalls. “An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.”[10]
- Load Balancer or Application Gateway: To distribute traffic between firewalls. One for Trust and Untrust subnets
- Network Security Groups and security rules: New NSGs should be created, one for each firewall interfaces.
- User Defined Routes: New UDRs should be created, one for each firewall interfaces.

3.4.3 Firewall Management with Panorama

Panorama provides centralized policy management and visibility for the network. Palo Alto Networks firewall implemented in the cloud can be managed by the cloud or on-premises Panorama. Panorama manages firewall configurations via templates and device groups.

Templates/Template stacks: Firewall device and network configurations is managed by templates: Templates are grouped with template stack, and template stack are applied to a selected firewall. Template stacks allow to build up a configuration using different templates as shown below.

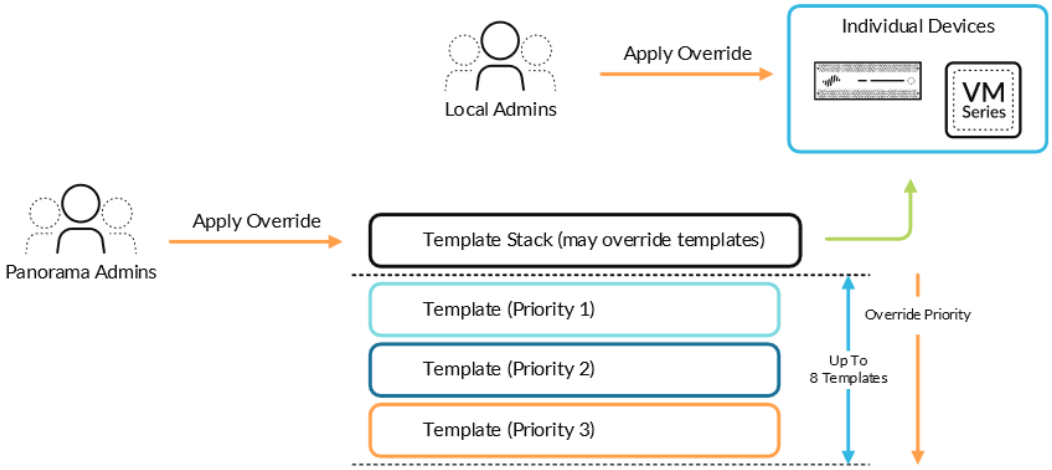

Figure 4. Panorama template stack and templates [11]

Device groups: Firewall policies and objects configuration is manged by the device groups. Device groups are built up as the hierarchical order and the order of the final configuration will build up as shown Figure 5.

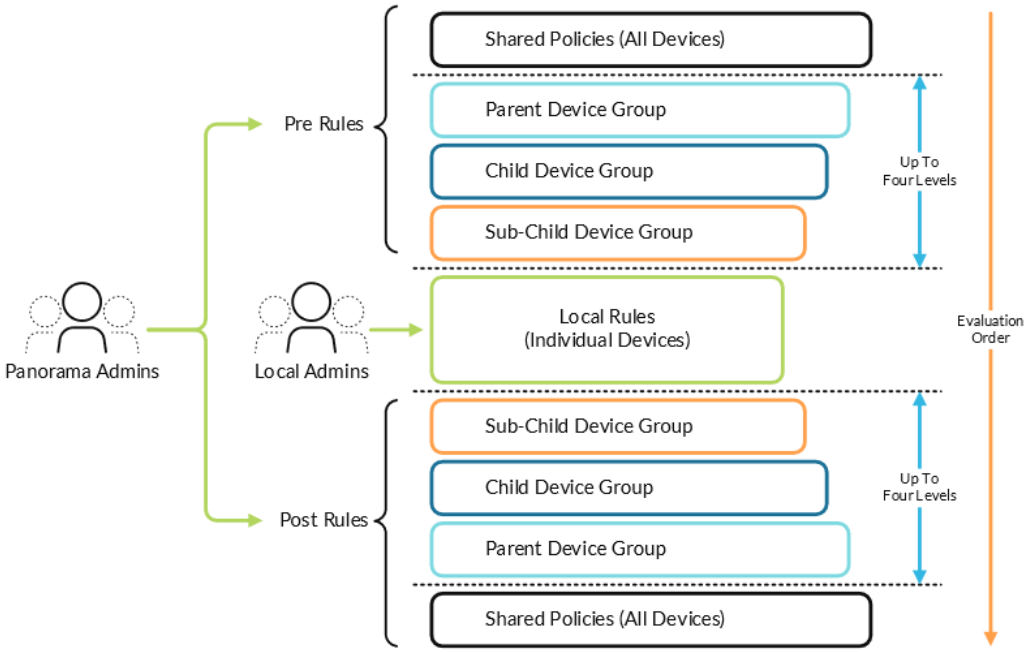

Figure 5. Panorama device groups and policy evaluation [11]

Panorama implementation is optional, and if cloud option will be used Panorama should be deployed in the VNet which is created only for Panorama. VNet peering should be configured between Firewall VNet and Panorama VNet to allow traffic between firewall management interfaces and Panorama.

3.4.4 Transit VNet Design Model

Palo Alto Networks published a design guide “Reference Architecture Guide for Azure” and two development guides “Deployment Guide for Azure Transit VNet Design Model” and “Deployment Guide for Azure Transit VNet Design Model (Common Firewall Option)” for deploying VM-Series firewall on Azure. There are two design models: Transit VNet model and Transit VNet model (Common Firewall Option). Both models introduce a transit-VNet where all other VNets are connected. The difference between these models is that Common Firewall option uses same firewall peers for both inbound and outbound traffics.

Figure 6 shows the network diagram for the VNet Design Model (Common Firewall Option)[12]. Transit VNet is most likely the standard for each implementation while Panorama, Gateway and Web Servers and Containers will be optional based on customer requirements.

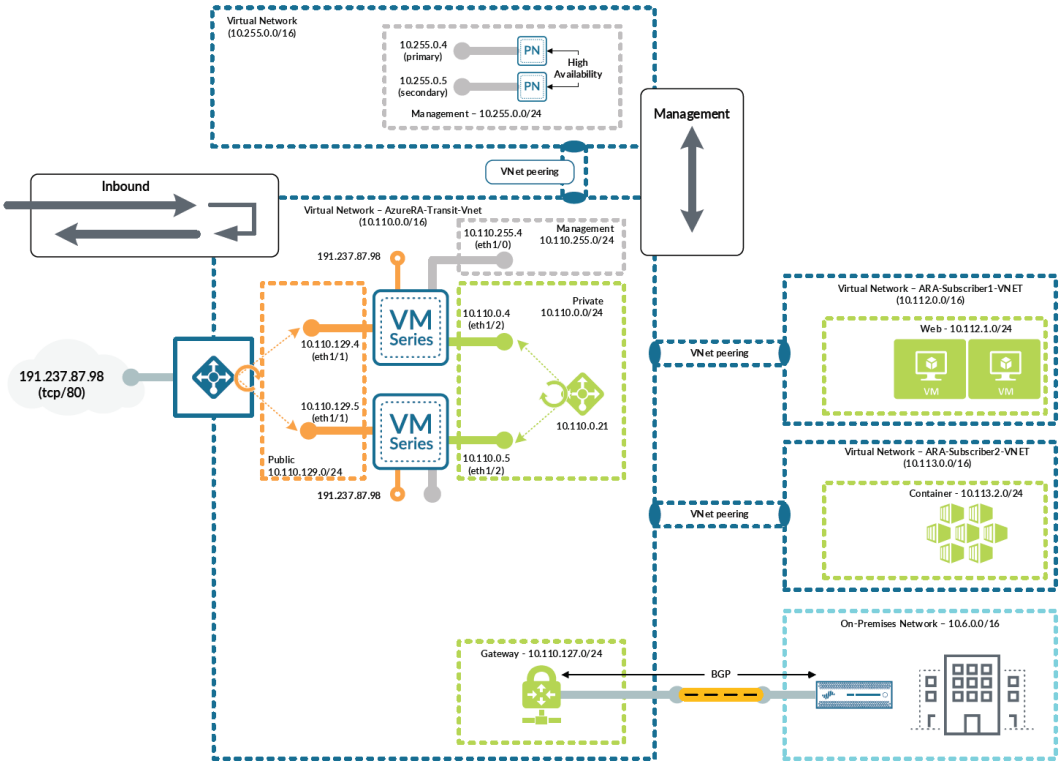

Figure 6. Transit VNet Common Firewall

In Transit VNet model, resources are deployed on different virtual networks that connected with hub and spoke topology. Transit VNet, where firewall and load balancers are located, is the hub of the topology and the traffic between the other virtual networks, and the traffic to/from the Internet always travel via it. VNet peering will allow traffic to be routed between the VNets and User Defined Routes (UDR) will be used to alter default routing, and forwards traffic via the firewalls.

Here are the default routes created for each subnet in Azure when a new virtual network is created:

Table 3. Azure Default Routes [13]

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

User Defined Rules for Management Subnets (see Table 4) will block the traffic from management subnet to other subnets in same Virtual networks, as new route with Next hop type with “None” indicates traffic will be dropped.

Table 4. User Defined Routes for Management Subnet [12 p.67]

Route name	Address prefixes	Next hop type	Next hop address
Blackhole-Public	10.110.129.0/24	None	-
Blackhole-Private	10.110.0.0/24	None	-

For subnets Private, Web, and Containers: UDR-default route with next hop 10.110.0.21 (Internal Load Balancer’s IP address) will be created. The traffic towards to internet will routed to firewall via the internal load balancer. Traffic to Public and Management subnets will be dropped using the route with Next hop type “None”.

Like UDR-default route Web and Containers Subnets will route traffic to each other via the 10.110.0.21. This way the traffic between the Virtual Networks travels via firewall.

3.5 Methods for firewall deployment

3.5.1 Manual deployment with Azure Portal

Azure Portal is a web based graphical interface, which allow to manage Azure subscriptions. With Azure Portal resources can be created, managed, and monitored. Azure Portal is user friendly and easy to use. But it is slow as a web page and resource creation and configuration takes longer time than with other methods.

3.5.2 Deployment with Azure CLI and Azure PowerShell

It is also possible to create and configure Azure resources with commands. Commands are long and each resource should be created and configured with separate commands. It will take time and is error prone. An example of CLI command which creates a firewall resource is shown below.

```
az vm create -- subscription <subscription-id> --resource-group <resource group name>
--name <FW-Hostname> --location <region-name> --nics <mgmtnic eth1nic eth2nic > --
size Standard_D3_V2 --image paloaltonetworks:vmseries1:byol:9.0.1 --plan-name byol -
-plan-product vmseries1 --plan-publisher paloaltonetworks --authentication-type
password --admin-username <admin-user> --admin-password <admin-pwd>
```

3.5.3 Deployment with Azure Resource Manager

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables one to create, update, and delete resources in an Azure account using Azure Power Shell, Azure CLI, REST API and client SDKs.

3.5.4 Deployment with Azure Resource Manager Templates

ARM templates are used to deploy or modify Azure resources. It uses templates and parameters to create and configure the resources. Templates can be deployed with or without the parameters file. Resource Manager templates are very efficient way to deploy repeatable and tested designs to Azure. When the template is created and tested, with the different parameters files same template can be used for different environments.

3.6 Azure Resource Manager Templates

ARM template is a JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group, subscription, management group, or tenant. The template can be used to deploy the resources consistently and repeatedly. [14]

The Resource Manager template is declarative syntax which defines the resources will be deployed, their properties and dependency information to be sure resources are created in the correct order. If possible, resources will be created in parallel and deployment will be faster.

The template has the following sections: [14]

- Parameters: Values which will be used during deployment that allow the same template to be used with different environments.
- Variables: Values which can be constructed for example from parameter values.
- User-Defined functions: Customized functions can be created to simplify the template.
- Resources: Defines the resources which should be deployed. Resources definition includes properties and values for the resource.
- Output: Return values from the deployed resources.

Parameters file can be used to provide parameters values for the template. If parameters file is not provided, defaultValue defined in the template file will be used. If no value for the parameter is defined in the parameters file or defaultValue in the template file, Azure CLI will ask for the value when deployment started.

Here is the example for the template and parameters files for deploying Public IP address.

Template file

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
```

```
    "Location": {
      "defaultValue": "westeurope",
      "type": "string"
    },
    "publicIPAddresses_PublicWebServerIP_name": {
      "defaultValue": "WebServerIP_public",
      "type": "String"
    },
  },
    "variables": {},
    "resources": [
     {
        "type": "Microsoft.Network/publicIPAddresses",
        "apiVersion": "2020-05-01",
        "name": "[parameters('publicIPAddresses_PublicWebServerIP_name')]",
        "location": "[parameters('Location')]",
        "sku": {
          "name": "Standard"
        },
        "properties": {
          "publicIPAddressVersion": "IPv4",
          "publicIPAllocationMethod": "Static",
          "idleTimeoutInMinutes": 4,
          "dnsSettings": {
            "domainNameLabel": "public-web",
            "fqdn":               "[concat(parameters('publicIPAddresses_PublicWeb-
ServerIP_name'),'.',parameters('Location'),'.cloudapp.azure.com')]"
          },
          "ipTags": []
        }
      }
  ]
  }
```

Parameters file

```
{
            "$schema":  "https://schema.management.azure.com/schemas/2015-01-01/de-
ploymentParameters.json#",
            "contentVersion": "1.0.0.0",
            "parameters": {
                        " publicIPAddresses_PublicWebServerIP_name ": {
                                    "value": "webserver01"
                        },
            }
}
```

When above template and parameters file is used for the deployment, a public IP address with FQDN webserver01.westeurope.cloudapp.azure.com will be created. Webserver01 is derived from parameters file but westeurope (location info) is derived from the defaultValue for the Location under template file parameters section.

4 Implementation and Verification

After initial knowledge for the Azure environment and Palo Alto Networks firewall is acquired, Transit VNet and required resources are added to Azure subscription using Azure portal. Using a portal is very convenient way for the expert who has been deploying firewalls to on-premises networks, but it is the slowest method.

Palo Alto Networks “Azure Architecture Guide” [7] is used to implement the firewall to Azure. After configuring the resources based on Transit VNet common firewall option, Resource Group information was exported to the ARM template. A template file which has static values, is modified to be able to use parameters. This way using parameters file, template file can be used with different environments without any modification.

Unfortunately exporting a template from Resource Group level, cause some extra work. It required a lot of clean up as some of the resources are defined in two different places: Security rules are configured as a separate resource and also under Network Security Group resource.

Firewall resources was not correctly created, and related code had to be replaced using resource level template. Therefore, using resource templates and combining them to one template would be a better option.

4.1 Implementation Steps with Azure Portal

Here are the steps to follow for adding one firewall using Azure Portal (see Figure 7). Similar steps are used to create for other resources.

- Click on “Create a resource”.
- Use “palo alto” as a keyword in search field to list the resources provided by Palo Alto Networks
- Select “VM-Series Next-Generation Firewall form Palo Alto Networks”
- Select licencing model: BYOL option used for this research.

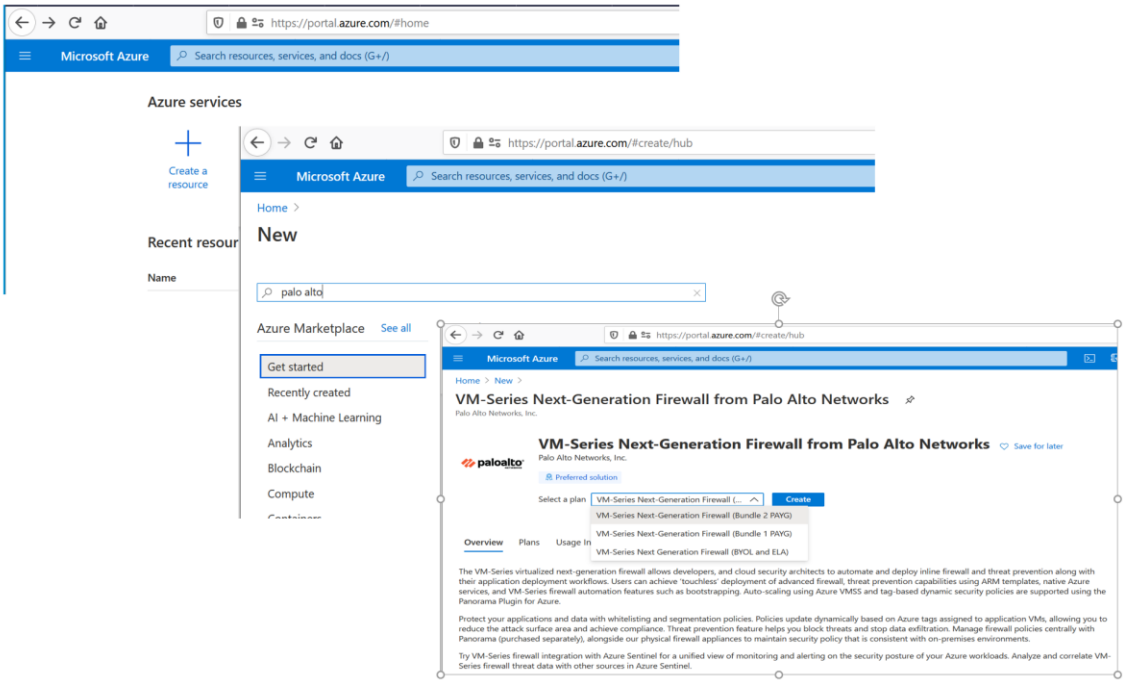

Figure 7. Adding Firewall via Azure Portal

Select the subscription, resource group to create resource in, region, firewall admin user and password as shown in Figure 8. Resource group can be created or use an already exist resource group. If existing resource group will be used there shouldn't be any other resource in the resource group.

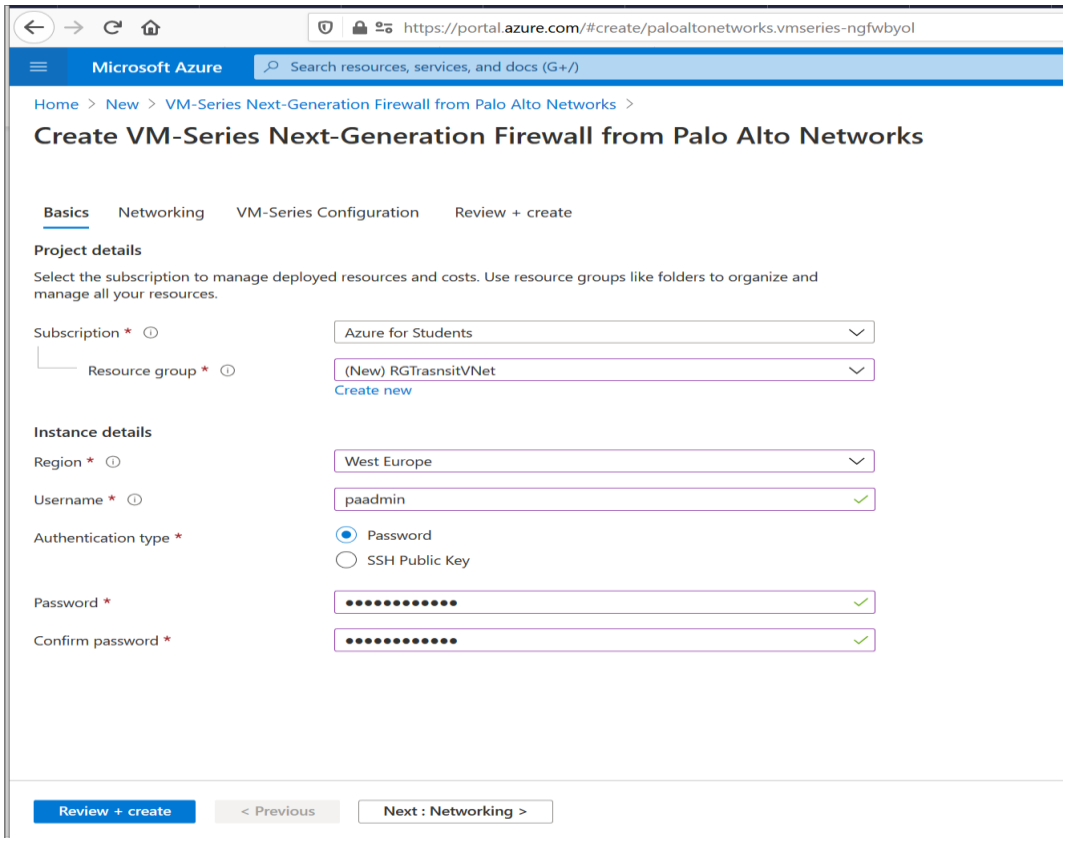

Figure 8. Adding Firewall via Azure Portal Basics

Select the virtual network and choose subnets for the firewall interfaces. Existing virtual network can be used or a new one will be created (see Figure 9).

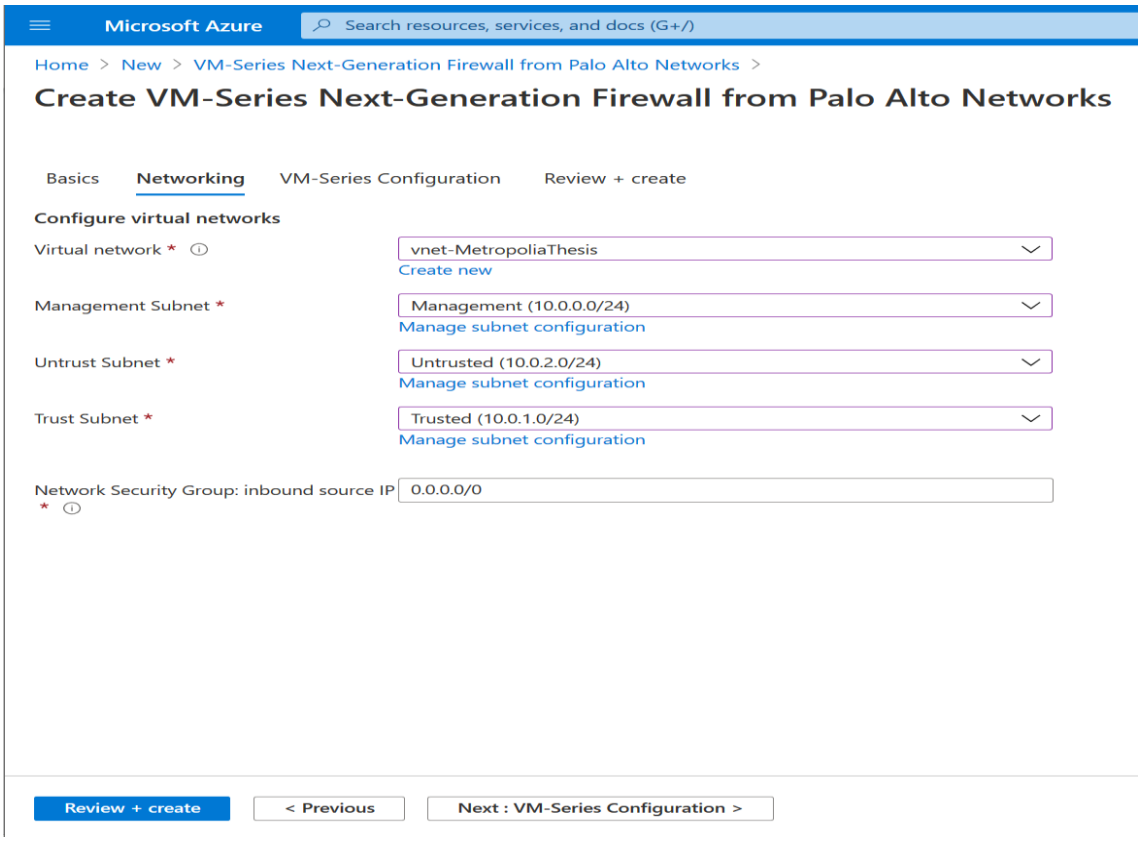

Figure 9. Adding Firewall via Azure Portal Networking

Select or create a new Public IP address, DNS name, VM name and virtual machine size as shown in Figure 10. Public IP address will be assigned to firewall management interface.

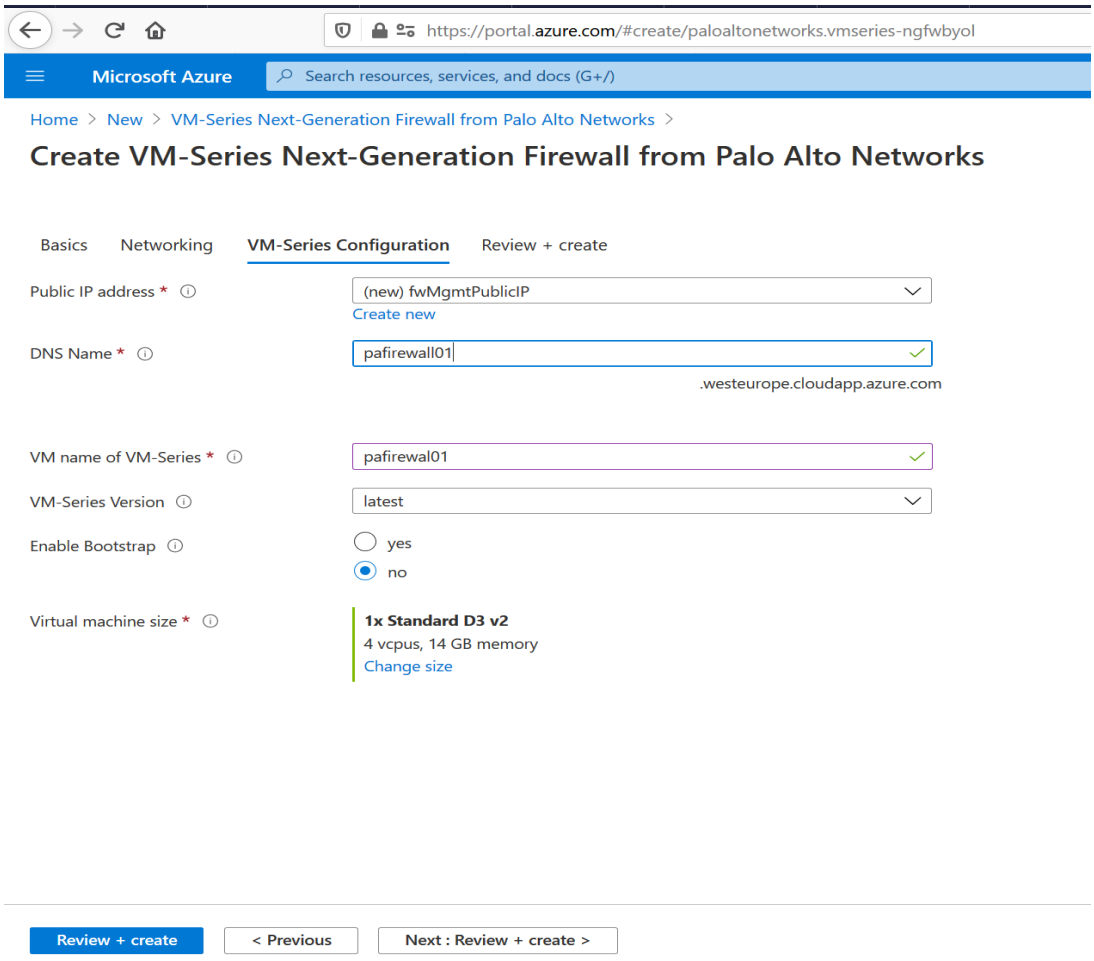

Figure 10. Adding Firewall via Azure Portal VM-Series Configuration

After all the information provided, Azure Portal will validate the configuration. If validation is passed, “Create” button will be highlighted and resource will be created when it is clicked (see Figure 11). “Download a template for automation” link will allow to get template for the resource which is a firewall in this example (see Figure 12).

If validation fails, the error message informing why the validation failed will be shown. Using Back button, parameter which caused the validation error can be browsed and fixed.

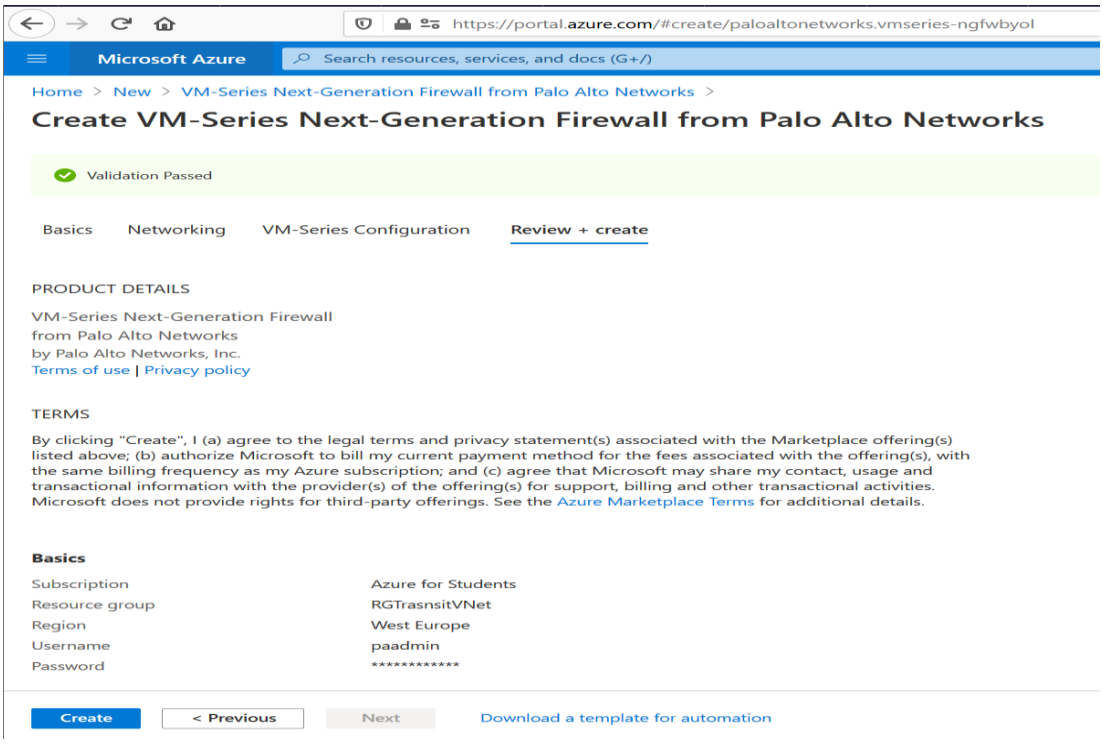

Figure 11. Adding Firewall via Azure Portal Validation

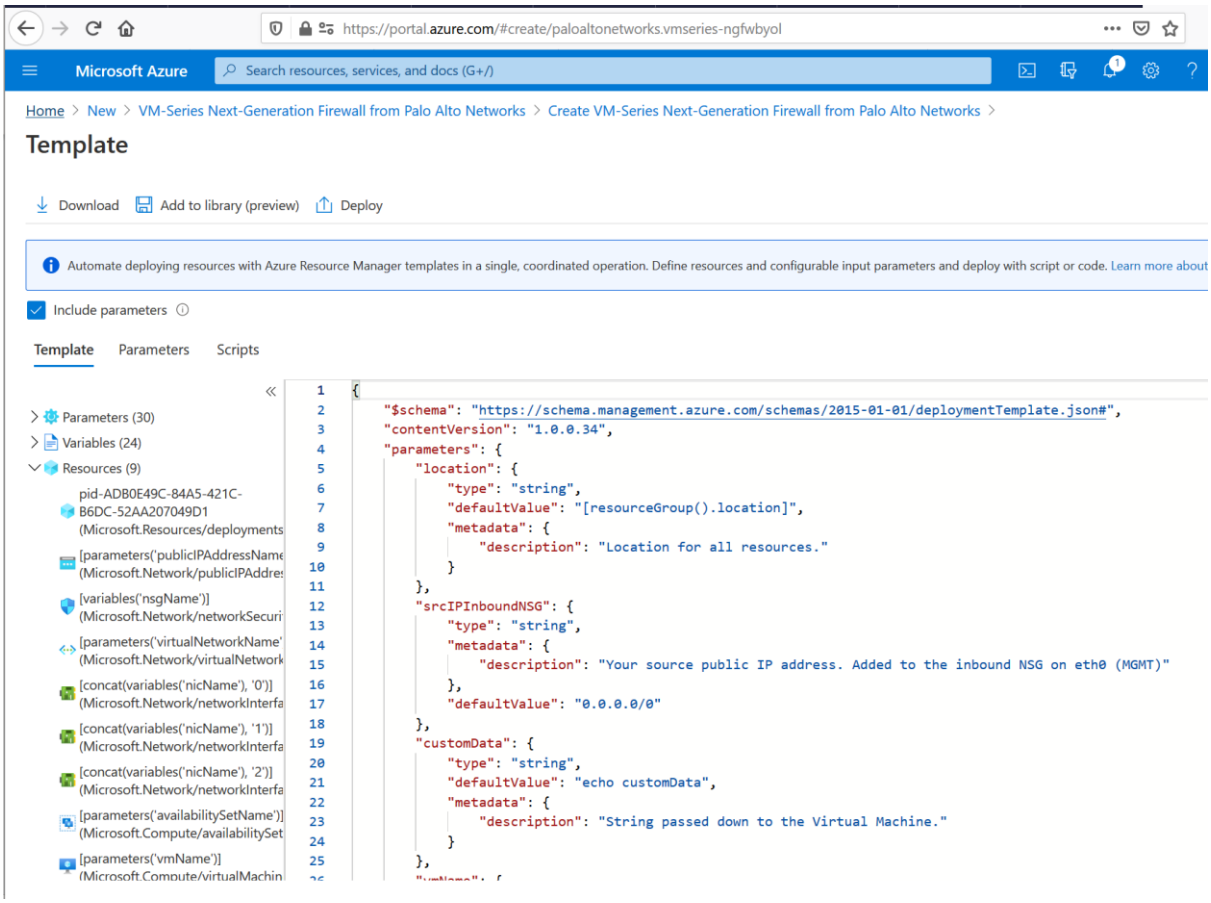

Figure 12. Adding Firewall via Azure Portal Template

4.2 Creating Parameters File

To collect the information for different environments, an excel file template was created. Excel contains information such as IP Addresses, FQDN names, and customer name prefix to able to create resources. This file can be filled by a customer or by an expert. After excel file is filled it should be saved as CSV format.

A Python script was developed to create parameters file based on the data collected with excel. When creating the deployment steps, aim was to minimize the needed manual modifications for ARM templates and parameters file. This will eliminate the spelling mistakes and any expert can use it even if they do not have experience with programming languages.

Here is the part of the python script, which load the .csv file and convert it to .json file which defines the parameters.

```
def loadExcel():
    print ("Loading Excel..")
    inFile = open(CSV_FILENAME, 'r')
    ParameterList = []
    for line in inFile:
        test = line.strip()
        print(test)
        ParameterList.append(test)
    print(len(ParameterList), 'lines loaded.')
    return ParameterList


def convert():
    PList = loadExcel()
    i = 0
    j = len(PList)
    print(j)
    ParametersFile= open(OUTPUT_FILENAME, 'a')
    ParametersFile.write('{'+'\n')
    ParametersFile.write('\t'+'"$schema": "https://schema.manage-
ment.azure.com/schemas/2015-01-01/deploymentParameters.json#",'+'\n')
    ParametersFile.write('\t'+'"contentVersion": "1.0.0.0",'+'\n')
    ParametersFile.write('\t'+'"parameters": {' + '\n')
    while i < j:
        print(PList[i])
        #print (i,j)
        ParLine = PList[i]
        #print(ParLine)
        NewPar: List[str] = ParLine.split(";")
        NewPar1=NewPar[1]
        print(NewPar1)
        if NewPar1=="":
```

```
            NewPar1 = "null"

        if i==0:
            ParametersFile.write('\t\t'+'"Location": {'+'\n')
            ParametersFile.write('\t\t\t'+'"value": "'+ NewPar1
+'"\n')
            ParametersFile.write('\t\t'+'},'+'\n')
        if i == 1:
            ParametersFile.write('\t\t'+'"CustomerNamePrefix": {' +
'\n')
            ParametersFile.write('\t\t\t'+'"value": "' + NewPar1 +
'"\n')
            ParametersFile.write('\t\t'+'},' + '\n')
..
.
.
```

4.3 Implementation Steps with ARM templates

Here are the steps to deploy Transit VNet architecture in Azure.

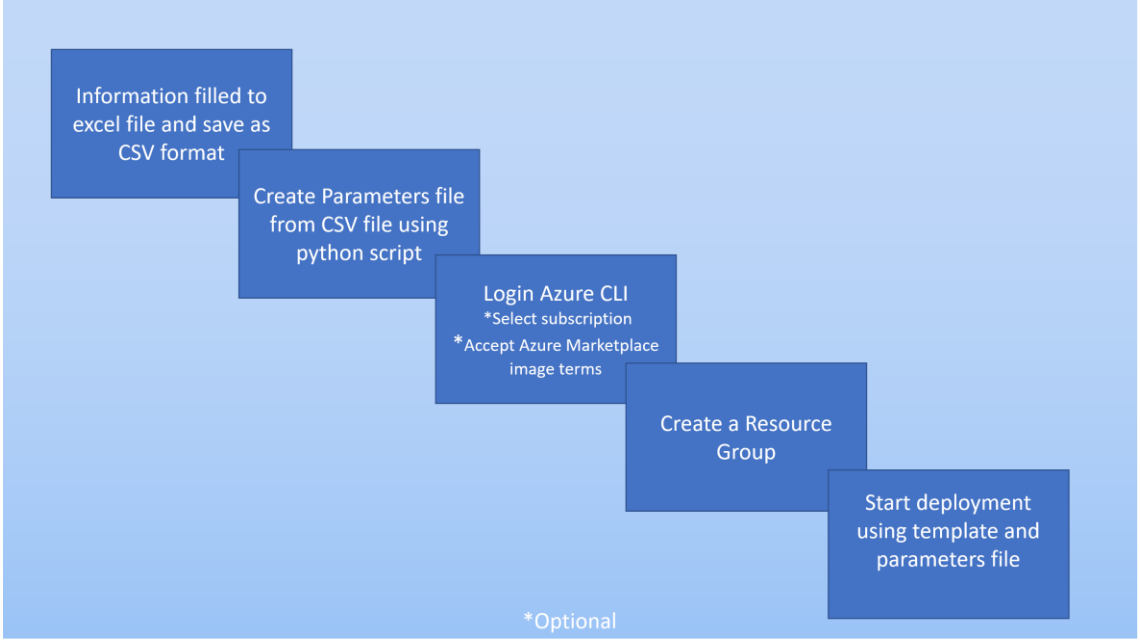

Figure 13. Implementation Steps

Detailed steps for the implementation are following:

- Collect the information with excel file
- Convert excel file to csv file
- Run the phyton script to create parameters file
- Using Azure CLI deploy the template on Azure
    - *#az login*

      This command will open a browser window and let user to login Azure Portal.
    - *#az account set –subscription*

      If the user has more than one subscription this command will set the subscription where the resources will be created.
    - *# az vm image terms accept --publisher paloaltonetworks --offer vmseries-flex --plan byol*

      This command will allow user to accept Azure Marketplace image terms.
    - *# az group create --name <ResouceGroupName> --location <location>*

      This command will create a new resource group in the location specified.

- *# az deployment group create --name <DeploymentName> --resource-group <ResouceGroupName> --template-file <"TemplateFile-Name.json"> --parameters <"ParametersFileName.json">*

This command will create the deployment and creates resources defined in the template file using the values provided in Parameters file.

4.4 Verify solution with expert team

Answers given by the experts to initial survey were indicating that although the experts have knowledge and experience implementing firewall on various cloud service providers, there was not any standard document and process in use. Most not all experts agreed to use the tools which will be created for the automation.

After ARM template and process are ready, they were introduced to team. As it shortens to deployment time and minimize the work for the experts, it is decided to use the solution in next deployment.

5 Discussions and Conclusions

The objective of this study was to develop a process for firewall implementation in the cloud environment. Well defined process and automation will improve the firewall implementation in a cloud environment and minimize the mistakes, therefore increase the security and quality of the implementation. Azure was selected as cloud provider and Palo Alto Networks was selected as firewall provider for this study. Palo Alto Networks published “Azure Architecture Guide” is used for the implementation.

Vendor approved architecture used in this study provides a well-designed standard implementation and it will be respected by the experts. Using validated ARM templates with parameters file allow to implement the solution in different environments very fast and it minimizes the mistakes. This will free the expert from manual tasks and allow expert to focus on enabling/configuring security features on the firewall.

Using device templates and combining them might be a better and faster approach to create the final ARM template. This should be the method to create ARM templates for different security vendors device implementations, or other blocks of the architecture.

The Cloud introduces a different way of working. When a new capability is introduced, instead of updating an existing resource, a new resource will be created. Therefore, implementation method should be repeatable.

The results of this study show how using the ARM templates changes the way of building an infrastructure on Azure. Whole infrastructure could be implemented, with the ready/approved template, without any network administration experience. World is changing and the Cloud is redefining the jobs in IT, and it does not leave option to IT professionals other than evolving with it. With this study ARM template was created for implementing Transit VNet block of the architecture. Other blocks of the architecture especially Panorama block might be used often by customers, and own ARM template can be created.

Firewalls are implemented with the ARM template, but basic configuration is missing. There are different approaches for firewall configuration: using bootstrap or creating set

commands, or using Panorama to configure the firewall. These approaches can be evaluated, and the selected approach can be automated to complete the reference architecture automation.

References

1 Arrow, 2019, SURVEY:IT infrastructure in Finnish companies. https://sahkoinen.fi/Arrow/cloudsummit2019_esitykset/Arrow%20Survey%20-%20IT%20infrastructure%20in%20Finnish%20companies%20-%20Survey%20Results%20-%2021112019.pdf

2 Palo Alto Networks, 19.09.2019, Press. https://www.paloaltonetworks.com/company/press/2019/palo-alto-networks-positioned-as-a-leader-in-gartner-magic-quadrant-for-network-firewalls-for-eighth-consecutive-time

3 NIST, 2013, NIST Cloud Computing Standards Roadmap. https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

4 Microsoft Azure, 2020, What is cloud computing. https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

5 Microsoft Azure, 10/16/2019, Shared responsibility in the cloud. https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

6 Microsoft Azure, 10.02.2019, Azure best practices for network security. https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

7 Palo Alto Networks, 2020, Reference Architecture Guide for Azure. https://www.paloaltonetworks.com/resources/guides/azure-architecture-guide

8 Microsoft Azure, 18.4.2019, Vertical autoscale with virtual machine scale sets, https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-vertical-scale-reprovision

9 Palo Alto Networks, 2020, VM-Series Enterprise License Agreement. https://docs.paloaltonetworks.com/vm-series/8-1/vm-series-deployment/license-the-vm-series-firewall/license-typesvm-series-firewalls/vm-series-ela

10 Microsoft Azure, 30.11.2018, Tutorial: Create and deploy highly available virtual machines with Azure PowerShell. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets

11 Palo Alto Networks, 19.8.2020, Deployment Guide – Panorama on Azure. https://www.paloaltonetworks.com/resources/guides/panorama-on-azure-deployment-guide

12 Palo Alto Networks, 19.8.2020, Deployment Guide for Azure. Transit VNet Design Model (Common Firewall Option). https://www.paloaltonetworks.com/resources/guides/azure-transit-vnet-deployment-guide-common-firewall-option

13 Microsoft Azure, 26.10.2017, Virtual network traffic routing. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

14 Microsoft Azure, 22.6.2020, What are ARM templates?.https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/overview

15 Palo Alto Networks. 2015a. PAN-EDU-201 Course Material

16 Microsoft Azure, 28.9.2020, Tutorial: Create and deploy your first ARM template. https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell

Survey used for current state analysis

1. Have you implemented a firewall in public cloud? If answer to this question is no, then you can skip questions 2-9
2. Which public cloud operator you have implemented firewall?
3. Which firewall (vendor) you have implemented?
4. Did you use any document/guide from cloud operator?
5. Did you use any document/guide form firewall vendor?
6. Did you use any Telia Cygate own document/guide?
7. When you implemented the firewall did you also configure cloud native security tools (access controls)?
8. Did you implement firewall in already existing network? Or do you need to configure it yourself?
9. Did you had any issue which is not addressed in the documents/guides? What was the issue?
10. Do you agree that having a Telia Cygate own document will easier the work next time? 1-5 (1- strongly disagree, 5 is strongly agree)
11. If there will automation(script) to implement firewall in cloud, would you use it?