Validated Reference Design
NetScaler and Microsoft Azure

This guide focuses on providing guidelines to customers on implementing NetScaler on Microsoft Azure based on their use cases.
Table of Contents

Overview NetScaler VPX 3
Overview NetScaler in Microsoft Azure 3
Limitations and Usage Guidelines 3
Use Cases 4
  Production Delivery for Web and XenDesktop Applications 4
  Hybrid Cloud Designs 4
  Business Continuity 5
  Development and Testing 5
Azure Network Architecture 5
  NetScaler VPX on Azure 6
  Traffic Flow through Port Address Translation 7
  Traffic Flow through Network Address Translation 8
  Assign Multiple IP (MIP) Addresses 9
  Create a VM with Multiple NIC Interfaces 10
  Port Usage Guidelines 11
Configuration Steps 12
  Provisioning the Resource Group 12
  Creating a Network Security Group 12
  Configuring a Virtual Network and Subnets 12
  Configuring the Second Subnet 12
  Configuring a Storage Account 13
  Provisioning the NetScaler Instance 13
VM Creation with PowerShell 14
  Creating a VM with Multiple IP addresses 14
  Creating a VM with Multiple NICs using PowerShell 14
Configuring the NetScaler Port Translation 15
Additional References 15
Overview NetScaler VPX

Citrix NetScaler is an all-in-one application delivery controller that makes applications run up to five times better, reduces application ownership costs, optimizes the user experience and ensures that applications are always available by using:

• Advanced L4-7 load balancing and traffic management
• Proven application acceleration such as HTTP compression and caching
• An integrated application firewall for application security
• Server offloading to significantly reduce costs and consolidate servers

As an undisputed leader of service and application delivery, Citrix NetScaler is deployed in thousands of networks around the world to optimize, secure and control the delivery of all enterprise and cloud services. Deployed directly in front of web and database servers, NetScaler combines high-speed load balancing and content switching, http compression, content caching, SSL acceleration, application flow visibility and a powerful application firewall into an integrated, easy-to-use platform. Meeting SLAs is greatly simplified with end-to-end monitoring that transforms network data into actionable business intelligence. NetScaler allows policies to be defined and managed using a simple declarative policy engine with no programming expertise required.

Overview NetScaler in Microsoft Azure

The NetScaler VPX virtual appliance is available as an image in the Microsoft Azure Marketplace. NetScaler VPX on Microsoft Azure Resource Manager (ARM) enables customers to leverage Azure cloud computing capabilities and use NetScaler load balancing and traffic management features for their business needs. You can deploy NetScaler VPX instances on ARM either as standalone instances or as high availability pairs in active-active or active-standby modes.

Limitations and Usage Guidelines

• The Azure architecture does not accommodate support for the following features:
  Clustering
  IPv6
  Gratuitous ARP (GARP)
  L2 Mode
  Tagged VLAN
  Dynamic Routing
  Virtual MAC (vMAC)
  USIP
  CloudBridge Connector

• The Intranet IP (IIP) feature is not supported, because Azure does not provide the pool of IP addresses required for this feature. IIP is frequently used in VOIP, SIP, or server-initiated-connection deployment.
• If you expect that you might have to shut down and temporarily deallocate the NetScaler VPX virtual machine at any time, assign a static Internal IP address while creating the virtual machine. If you do not assign a static internal IP address, Azure might assign the virtual machine a different IP address each time it restarts, and the virtual machine might become inaccessible.

• In an Azure deployment, only the following NetScaler VPX models are supported: VPX 10, VPX 200, and VPX 1000. These virtual appliances can be deployed on any instance type that has two or more cores and more than 2 GB memory. See the NetScaler VPX datasheet: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-vpx-data-sheet.pdf

• The 'deployment ID' that is generated by Azure during virtual machine provisioning is not visible to the user in ARM. You cannot use the deployment ID to deploy NetScaler VPX appliance on ARM.

Use Cases

Compared to alternative solutions that require each service to be deployed as a separate virtual appliance, NetScaler on Azure combines L4 load balancing, L7 traffic management, server offload, application acceleration, application security and other essential application delivery capabilities in a single VPX instance, conveniently available via the Azure Marketplace. Furthermore, everything is governed by a single policy framework and managed with the same, powerful set of tools used to administer on-premise NetScaler deployments. The net result is that NetScaler on Azure enables several compelling use cases that not only support the immediate needs of today’s enterprises, but also the ongoing evolution from legacy computing infrastructures to enterprise cloud datacenters.

Production Delivery

Enterprises actively embracing Azure as an infrastructure-as-a-service (IaaS) offering for production delivery of applications can now front-end those applications with the same cloud networking platform used by the largest websites and cloud service providers in the world. Extensive offload, acceleration and security capabilities can be leveraged to enhance performance and reduce costs.

Hybrid Cloud Designs

With NetScaler on Azure, hybrid clouds that span enterprise datacenters and extend into Azure can benefit from the same NetScaler cloud networking platform, significantly easing the transition of applications and workloads back and forth between a private datacenter and Azure. The full suite of NetScaler capabilities, ranging from intelligent database load balancing with DataStream to unprecedented application visibility with AppFlow® and real-time monitoring and response with Action Analytics, can be leveraged with NetScaler on Azure.
**Business Continuity**

Enterprises looking to use Azure as part of their disaster recovery and business continuity plans can rely upon NetScaler global server load balancing running both on-premise and within Azure to continuously monitor availability and performance of both enterprise datacenters and Azure environments, ensuring users are always sent to the optimal location.

**Development and Testing**

Enterprises running production delivery on-premise but using Azure for development and testing can now include NetScaler within their Azure test environments, speeding time-to-production due to better mimicry of the production implementation within their test environments. In each use case, network architects can also leverage Citrix CloudBridge—configured either as a standalone instance or as feature of a NetScaler platinum edition instance—to secure and optimize the connection between the enterprise datacenter(s) and the Azure Cloud, thereby speeding data transfer/synchronization and minimizing network costs.

**Network Architecture**

In ARM, a NetScaler VPX virtual machine (VM) resides in a virtual network. By default, a NetScaler VPX provisioned in Azure will operate in single-IP mode described in the following section.

A virtual Network Interface Card (NIC) is created on each NetScaler VM. The network security group (NSG) configured in the virtual network is bound to the NIC, and together they control the traffic flowing into the VM and out of the VM.

The NSG forwards the requests to the NetScaler VPX instance, and the VPX instance sends them to the servers. The responses from the servers follow the same path in reverse. You can configure NSG to control a single VPX VM, or with subnets and virtual networks and control traffic in multiple VPX VM deployments.

The NIC contains network configuration details such as the virtual network, subnets, internal IP address and Public IP address.

While on ARM, it is good to know the following IP addresses used to access the VMs:

- Public IP (PIP) address is the Internet-facing IP address configured directly on the virtual NIC of the NetScaler VM. This allows you to directly access a VM from the external network without the need to configure inbound and outbound rules on the NSG.
- NetScaler IP (NSIP) address is internal IP address configured on the VM. It is non-routable.
- Virtual IP address (VIP) is configured by using the NSIP and a port number. Clients access NetScaler services through the PIP address, and when the request reaches the NIC of the NetScaler VPX VM or the Azure load balancer, the VIP gets translated to internal IP (NSIP) and internal port number.
• Internal IP address is the private internal IP address of the VM from the virtual network's address space pool. This IP address cannot be reached from the external network. This IP address is by default dynamic unless you set it to static. Traffic from the internet is routed to this address according to the rules created on the NSG. The NSG works with the NIC to selectively send the right type of traffic to the right port on the NIC, which depends on the services configured on the VM.

Note: In this document, PIP, VIP, and Instance Level PIP (ILPIP) mean the same thing and are used interchangeably.

The following figure shows how traffic flows from a client to a server through a NetScaler VPX instance provisioned in ARM.

How NetScaler VPX Works on Azure

In an on-premise deployment, a NetScaler VPX instance requires, at least three IP addresses:

• Management IP address, called the NetScaler IP (NSIP) address
• Subnet IP (SNIP) address for communicating with the server farm
• Virtual server IP (VIP) address for accepting client requests

In an Azure deployment, only one IP address (a private (internal) address) is assigned to an instance during provisioning through DHCP.

To avoid this limitation, you can deploy a NetScaler VPX instance in Azure with a single IP architecture, where the three IP functions of a NetScaler appliance are multiplexed onto one IP address. This single IP address uses different port numbers to function as the NSIP, SNIP, and VIP.
Traffic Flow Through Port Address Translation

In an Azure deployment, when you provision the NetScaler VPX instance as a virtual machine (VM), Azure assigns a Public IP address and an internal IP address (non-routable) to the NetScaler virtual machine. Inbound and Outbound rules are defined on the NSG for the NetScaler instance, along with a public port and a private port for each rule defined. The NetScaler instance listens on the internal IP address and private port.

Any external request is received on the NetScaler VPX VM’s virtual NIC. The NIC is bound to the NSG, which specifies the private IP and private port combination for where to translate the request’s destination address and port (the Public IP address and port). ARM performs the port address translation (PAT) to map the Public IP address and port to the internal IP address and private port of the NetScaler virtual machine, and then forwards the traffic to the VM.

The following figure shows how Azure performs port address translation to direct traffic to the NetScaler internal IP address and private port.
In this example, the Public IP address is assigned to the VM is 140.x.x.x, and the internal IP address is 10.x.x.x. When the inbound and outbound rules are defined, public HTTP port 80 is defined as the port on which the client requests are received, and a corresponding private port, 10080, is defined as the port on which the NetScaler VM listens. The client request is received on the Public IP address 140.x.x.x at port 80. Azure performs port address translation to map this address and port to internal IP address 10.x.x.x on private port 10080 and forwards the client request.

For information about port usage guidelines while, see Port Usage Guidelines.

For information about NSG and access control lists, see https://azure.microsoft.com/en-in/documentation/articles/virtual-networks-nsg/.

### Traffic Flow Through Network Address Translation

You can also request a Public IP (PIP) address for your NetScaler VM (instance level). If you use this direct PIP at the VM level, you don’t need to define inbound and outbound rules to intercept the network traffic. The incoming request from the Internet is received on the VM directly. Azure performs network address translation (NAT) and forwards the traffic to the internal IP address of the NetScaler instance.

The following figure shows how Azure performs network address translation to map the NetScaler internal IP address.

In this example, the Public IP assigned to the NSG is 140.x.x.x and the internal IP address is 10.x.x.x. When the inbound and outbound rules are defined, public HTTP port 80 is defined as the port on which the client requests are received, and a corresponding private port, 10080, is defined as the port on which the NetScaler virtual machine listens. The client request is received on the Public IP address (140.x.x.x). Azure performs network address translation to map the PIP to the internal IP address 10.x.x.x on port 10080, and forwards the client request.

**Note:** NetScaler VPX VMs in high availability are controlled by external or internal load balancers that have inbound rules defined on them to control the load balancing traffic. The external traffic is first intercepted by these load balancers and the traffic is diverted according to the load balancing rules configured, which has backend pools, NAT rules, and health probes defined on the load balancers.
Assign Multiple IP (MIP) Addresses

An Azure Virtual Machine (VM) has one or more network interfaces (NIC) attached to it. Any NIC can have one or more static or dynamic public and private IP addresses assigned to it. Assigning multiple IP addresses to a VM enables the following capabilities:

- Hosting multiple websites or services with different IP addresses and SSL certificates on a single server.
- Serve as a network virtual appliance, such as a firewall or load balancer.
- The ability to add any of the private IP addresses for any of the NICs to an Azure Load Balancer back-end pool. In the past, only the primary IP address for the primary NIC could be added to a back-end pool. To learn more about how to load balance multiple IP configurations, read the Load balancing multiple IP configurations article.

Scenario

A VM with a single NIC is created and connected to a virtual network. The VM requires three different private IP addresses and two public IP addresses.

The IP addresses are assigned to the following IP configurations:

- **IPConfig-1**: Assigns a dynamic private IP address (default) and a static public IP address.
- **IPConfig-2**: Assigns a static private IP address and a static public IP address.
- **IPConfig-3**: Assigns a dynamic private IP address and no public IP address.

Every NIC attached to a VM has one or more IP configurations associated to it. Each configuration is assigned one static or dynamic private IP address. Each configuration may also have one public IP address resource associated to it. A public IP address resource has either a dynamic or static public IP address assigned to it. To learn more about IP addresses in Azure, read the IP addresses in Azure article. You can assign up to 250 private IP addresses to each NIC. While you can assign multiple public IP addresses to each NIC, there are limits to how many public IP addresses that can be used in an Azure subscription. See the Azure limits article for details.

**Note**: Multiple IP addresses cannot be assigned to resources created through the classic deployment model.
Create a VM with multiple NICs interfaces

You can create virtual machines (VMs) in Azure and attach multiple network interfaces (NICs) to each of your VMs. Multi NIC is a requirement for many network virtual appliances, such as application delivery and WAN optimization solutions. Multi NIC also provides more network traffic management functionality, including isolation of traffic between a front end NIC and back end NIC(s), or separation of data plane traffic from management plane traffic.

Scenario

This document will walk through a deployment that uses multiple NICs in VMs in a specific scenario. In this scenario, you have a two-tiered IaaS workload hosted in Azure. Each tier is deployed in its own subnet in a virtual network (VNet). The front end tier is composed of several web servers, grouped together in a load balancer set for high availability. The back end tier is composed of several database servers. These database servers will be deployed with two NICs each, one for database access, the other for management. The scenario also includes Network Security Groups (NSGs) to control what traffic is allowed to each subnet, and NIC in the deployment. The figure below shows the basic architecture of this scenario.
Port Usage Guidelines

You can configure additional inbound and outbound rules in NSG when creating the NetScaler VM or after the VM is provisioned. Each inbound and outbound rule is associated with a public port and a private port.

Before configuring NSG rules, note the following guidelines regarding the port numbers you can use:

1. The following ports are reserved by the NetScaler virtual machine. You cannot define these as private ports when using the Public IP address for requests from the Internet.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   However, if you want Internet-facing services such as the VIP to use a standard port (for example, port 443), you have to create port mapping by using the NSG. The standard port is then mapped to a different port that is configured on the NetScaler for this VIP service.

   For example, a VIP service might be running on port 8443 on the NetScaler instance but be mapped to public port 443. So, when the user accesses port 443 through the Public IP, the request is actually directed to private port 8443.

2. Public IP address does not support protocols in which port mapping is opened dynamically, such as passive FTP or ALG.

3. Azure load balancer does not work with Public IP address. High availability does not work for traffic that uses PIP associated with VPX instance instead of PIP configured on the load balancer. For more information about configuring NetScaler VPX HA in ARM, see Configuring NetScaler VPX in High Availability Mode in Azure.

4. In a NetScaler Gateway deployment, you need not configure a SNIP address, because the NSIP can be used as a SNIP when no SNIP is configured.

   **Note:** You must configure the VIP address by using the NSIP address and some nonstandard port number. For call-back configuration on the backend server, the VIP port number has to be specified along with the VIP URL (for example, url:port).

   **Note:** In ARM, a NetScaler VPX VM is associated with two IP addresses. Public IP address and Internal IP address. While the external traffic connects to the PIP, the internal IP address or the NSIP is non-routable. To configure VIP in VPX, use this combination of internal IP address and port number.

   **Example:** If the VPN virtual server FQDN is vip.test.com, and the VPN virtual server is running on port 8443, the call-back URL will be: https://vip.test.com:8443.
Section 2: Configuration Steps

Provisioning the Resource Group

On the Microsoft Azure Portal page (https://portal.azure.com), log into the Azure Resource Manager portal with your user name and password. (In the ARM portal, clicking an option in one pane opens a new pane to the right. Navigate from one pane to another to configure your device.)

Create a new resource group to serve as a container for all your resources. Use the resource group to deploy, manage, and monitor your resources as a group.

Create a Network Security Group

Create a network security group (NSG) to assign inbound and outbound rules to control the incoming and outgoing traffic within the virtual network. NSG allows you to define security rules for a single virtual machine and also to define security rules for a virtual network subnet.

Configuring a Virtual Network and Subnets

Virtual networks in ARM provide a layer of security and isolation to your services. VMs and services that are part of the same virtual network can access each other.

For example, create a virtual network with a reserved CIDR block of 192.168.0.0/16 and two subnets having CIDR blocks as 192.168.1.0/24 and 192.168.2.0/24 respectively.

In the Create virtual network pane, enter the following values, and then click Create.

- Name of the virtual network
- Address space – type the reserved IP address block for the virtual network
- Subnet – type the name of the first subnet (you will create the second subnet later in this step)
- Subnet address range – type the reserved IP address block of the subnet
- Resource group – select the resource group created earlier from the drop-down list

Configuring the second subnet

Select the newly created virtual network from the All Resources pane and in the Settings pane, click Subnets.

Click +Subnet and create the second subnet by entering the following details.

- Name of the second subnet
- Address range – type the Reserved IP address block of the second subnet
- Network security group – select the NSG from the drop-down list
Configuring a Storage Account

The ARM IaaS infrastructure storage includes all services where we can store data in the form of blobs, tables, queues, and files. You can also create applications using these forms of storage data in ARM.

Create a storage account to store all your data.

Click +New > Storage > Storage account.

In the Create Storage account pane, enter the following details:

• Name of the account
• Deployment mode – make sure to select Resource Manager
• Account kind – select General purpose from the drop-down list
• Replication – select Locally redundant storage from the drop-down list
• Resource group – select the newly created resource group from the drop-down list
• Click Create.

Configuring an Availability Set

An availability set guarantees that at least one VM is kept up and running in case of planned or unplanned maintenance. Two or more VMs under the same 'availability set' are placed on different fault domains to achieve redundant services.

Click +New and search for availability set.

Select Availability set entity from the list. Click Create.

In the Create availability set pane, enter the following details:

• Name of the set
• Resource group – select the newly created resource group from the drop-down list
• Click Create.

Provisioning the NetScaler Instance:

Create an instance of NetScaler VPX in the virtual network. Obtain the NetScaler VPX image from the Azure marketplace, and then use the Azure Resource Manager portal to create a NetScaler VPX instance.

Before you begin creating the NetScaler VPX instance, make sure that you have created a virtual network with required subnets in which the instance will reside. You can create virtual networks during VM provisioning, but without the flexibility to create different subnets. For information about creating virtual networks, see [http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/](http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/)

Optional: Configure DNS server and VPN connectivity to allow a VM to access Internet resources.

**Note:** Citrix recommends that you create resource group, network security group, virtual network, and other entities before you provision the NetScaler VPX VM, so that the network information is available during provisioning.

• Click +New > Networking.
• Click See All and in the Networking pane, click Citrix NetScaler VPX Bring Your Own License.
• Click Create.

**Note:** As a quick way to find any entity on ARM portal, you can also type the name of the entity in the Azure Marketplace search box and press <Enter>. Type NetScaler in the search box to find the Citrix NetScaler images.
• Select NetScaler 11.0 VPX Bring Your Own License.
• Populate your details.
• Purchase and Deploy my NetScaler, after passing the validation.
• It is recommended to set your IP Addresses to Static.

Note: Ensure to select the latest image. Your Citrix NetScaler image might have the release number in the name.

Create a VM with multiple IP addresses using PowerShell

The steps that follow explain how to create an example VM with multiple IP addresses, as described in the scenario. Change variable names and IP address types as required for your implementation.

These configuration Steps covered are:

Create a VM with multiple IP addresses
Add IP addresses to a VM
Add IP addresses to a VM operating system
Validation (Windows)
Validation (Linux)

Please refer to the following Microsoft Azure documentation located here:


Create a VM with multiple NICs using PowerShell

The steps that follow explain how to create an example VM with multiple NIC interfaces, as described in the scenario. Change variable names and values as required for your implementation.

These configuration Steps covered are:

Create the back-end VMs
Start your script
Create necessary resources for your VMs
Create the NICs and back-end VMs
Run the script

Please refer to the following Microsoft Azure documentation located here:

Configure the NetScaler Port Translation

- Click on Network Interfaces for your VM, the NetScaler.
- Click on your Network security group.
- Click on Inbound security rules.
- Allow SSH and HTTP in the Security Group for Inbound connections.

At this point, you can log into the NetScaler instance and configure the features and settings desired for your Azure environment.

**Note:** When logging into the NetScaler for the first time, the wizard may ask for a Subnet IP address. This is not required on NetScaler Azure instances as they only use a single IP address for all functions. Skip this step when prompted and continue to the default configuration login page.

### Additional References

**Deploying Citrix NetScaler VPX on Microsoft Azure**

https://docs.citrix.com/en-us/netscaler/11/getting-started-with-vpx/deploy-vpx-on-azure.html#par_rich-text_4

**Microsoft Azure Documentation**


**Assign multiple IP addresses to virtual machines using PowerShell**


**Create a VM with multiple NICs using PowerShell**

About Citrix

Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler MPX, NetScaler SDX, NetScaler, CloudBridge and AppFlow are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.