CloudBridge for Microsoft Azure Deployment Guide

www.citrix.com

Contents

Introduction

Welcome to the CloudBridge deployment guide for Microsoft Azure cloud.

CloudBridge provides connectivity between your enterprise datacenters and the Microsoft cloud hosting provider, Azure, making Azure a seamless extension of the enterprise network. CloudBridge encrypts the connection between the enterprise datacenter and Azure cloud so that all data transferred between the two is secure.

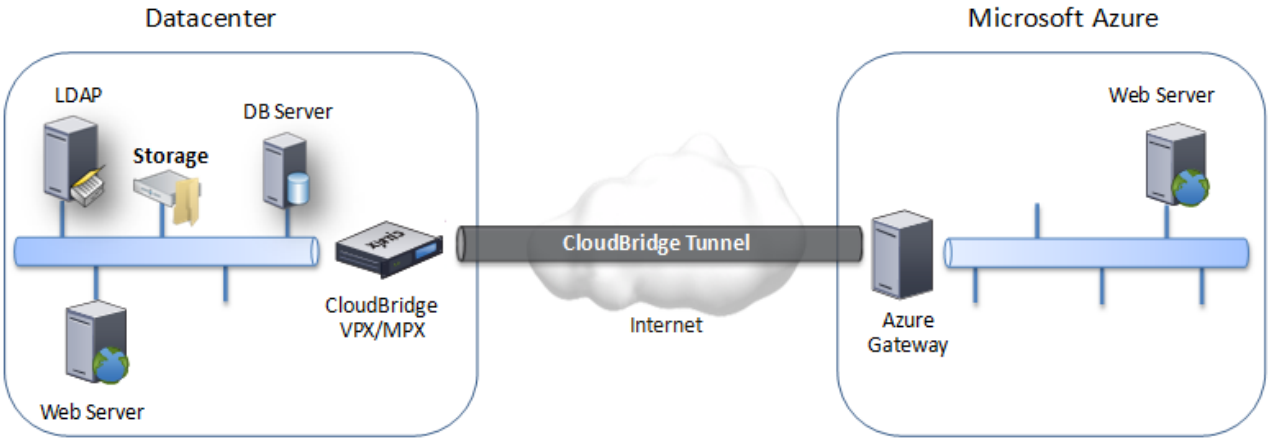
CloudBridge is a complete network solution—available as a standalone physical or virtual appliance, or integrated into NetScaler Platinum edition—enabling enterprises to transparently shift web and application servers to the cloud while keeping the database safely within the enterprise datacenter.

About This Guide

This guide assumes you are using a CloudBridge MPX appliance or VPX virtual appliance. Here you will find complete, step-by-step instructions for configuring all CloudBridge components, including the CloudBridge appliance, and detailed configuration steps for setting up the CloudBridge.

How CloudBridge Works

To implement the Citrix CloudBridge solution, you connect a datacenter to Azure cloud by setting up a tunnel between a CloudBridge appliance that resides in the datacenter and a gateway that resides in the Azure cloud. This tunnel is called a *CloudBridge tunnel*. The CloudBridge appliance in the datacenter and the gateway in Azure cloud are the end points of the CloudBridge tunnel and are called *peers* of the CloudBridge tunnel.



A CloudBridge tunnel between a datacenter and Azure cloud uses the open-standard Internet Protocol security (IPSec) protocol suite to secure communications between peers in the CloudBridge tunnel. In a CloudBridge tunnel, IPSec ensures:

- Data integrity
- Data origin authentication
- Data confidentiality (encryption)
- Protection against replay attacks

IPSec uses the tunnel mode in which the complete IP packet is encrypted and then encapsulated. The encryption uses the Encapsulating Security Payload (ESP) protocol, which ensures the integrity of the packet by using a HMAC hash function and ensures confidentiality by using an encryption algorithm. The ESP protocol, after encrypting the payload and calculating the HMAC, generates an ESP header and inserts it before the encrypted IP packet. The ESP protocol also generates an ESP trailer and inserts it at the end of the packet.

The IPSec protocol then encapsulates the resulting packet by adding an IP header before the ESP header. In the IP header, the destination IP address is set to the IP address of the CloudBridge peer.

Peers in the CloudBridge tunnel use the Internet Key Exchange version 1 (IKEv1) protocol (part of the IPSec protocol suite) to negotiate secure communication, as follows:

1. The two peers mutually authenticate with each other, using pre-shared key authentication, in which the peers exchange a text string called a *pre-shared key* (PSK). The pre-shared keys are matched against each other for authentication. Therefore, for the authentication to be successful, you must configure the same pre-shared key on each of the peers.

2. The peers then negotiate to reach agreement on:
    - An encryption algorithm
    - Cryptographic keys for encrypting data on one peer and decrypting it on the other.

    This agreement upon the security protocol, encryption algorithm and cryptographic keys is called a *Security Association (SA)*. SAs are one-way (simplex). For example, when a CloudBridge tunnel is set up between a CloudBridge appliance in a datacenter and a gateway in an Azure cloud, both the datacenter appliance and the Azure gateway have two SAs. One SA is used for processing out-bound packets, and the other SA is used for processing inbound packets. SAs expire after a specified interval of time, which is called the *lifetime*.

Example of CloudBridge Configuration and Data Flow

As an illustration of CloudBridge, consider an example in which a CloudBridge tunnel is set up between CloudBridge appliance CB_Appliance-1 in a datacenter and gateway Azure_Gateway-1 in Azure cloud.

CB_Appliance-1 also functions as an L3 router, which enables a private network in the datacenter to reach a private network in the Azure cloud through the CloudBridge tunnel. As a router, CB_Appliance-1 enables communication between client CL1 in the datacenter and server S1 in the Azure cloud through the CloudBridge tunnel. Client CL1 and server S1 are on different private networks.

On CB_Appliance-1, the CloudBridge tunnel configuration includes an IPSec profile entity named CB_Azure_IPSec_Profile, a CloudBridge tunnel entity named CB_Azure_Tunnel, and a policy based routing (PBR) entity named CB_Azure_Pbr.

The IPSec profile entity CB_Azure_IPSec_Profile specifies the IPSec protocol parameters, such as IKE version, encryption algorithm, and hash algorithm, to be used by the IPSec protocol in the CloudBridge tunnel. CB_Azure_IPSec_Profile is bound to IP tunnel entity CB_Azure_Tunnel.

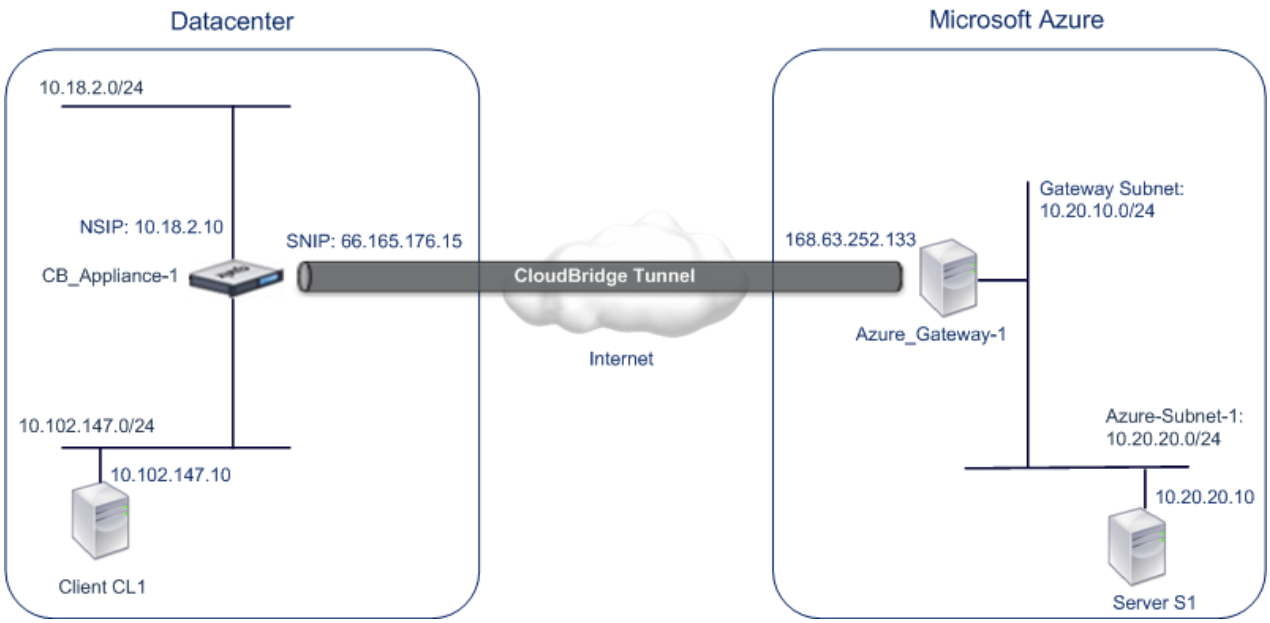
CloudBridge tunnel entity CB_Azure_Tunnel specifies the local IP address (a public IP (SNIP) address configured on the CloudBridge appliance), the remote IP address (the IP address of the Azure_Gateway-1), and the protocol (IPSec) used to set up the CloudBridge tunnel. CB_Azure_Tunnel is bound to the PBR entity CB_Azure_Pbr.

The PBR entity CB_Azure_Pbr specifies a set of conditions and a CloudBridge tunnel entity (CB_Azure_Tunnel). The source IP address range and the destination IP address range are the conditions for CB_Azure_Pbr. The source IP address range and the destination IP address range are specified as a subnet in the datacenter and a subnet in the Azure cloud, respectively. Any request packet originating from a client in the subnet in the datacenter and destined to a server in the subnet on the Azure cloud matches the conditions in CB_Azure_Pbr. This packet is then considered for CloudBridge processing and is sent across the CloudBridge tunnel (CB_Azure_Tunnel) bound to the PBR entity.

On Microsoft Azure, the CloudBridge tunnel configuration includes a local network entity named My-Datacenter-Network, a virtual network entity named Azure-Network-for-CloudBridge-Tunnel, and a gateway named Azure_Gateway-1.

The local (local to Azure) network entity My-Datacenter-Network specifies the IP address of the CloudBridge appliance on the datacenter side, and the datacenter subnet whose traffic is to traverse the CloudBridge tunnel. The virtual network entity Azure-Network-for-CloudBridge-Tunnel defines a private subnet named Azure-Subnet-1 in Azure. The traffic of the subnet traverses the CloudBridge tunnel. The server S1 is provisioned in this subnet.

The local network entity My-Datacenter-Network is associated with the virtual network entity Azure-Network-for-CloudBridge-Tunnel. This association defines the remote and local network details of the CloudBridge tunnel configuration in Azure. Gateway Azure_Gateway-1 was created for this association to become the CloudBridge end point at the Azure end of the CloudBridge tunnel.



The following table lists the settings used in this example.

Entity	Name	Details
Settings highlight of the CloudBridge tunnel setup		
IP address of the CloudBridge tunnel end point (CB_Appliance-1) in the datacenter side	66.165.176.15	
IP address of the CloudBridge tunnel end point (Azure_Gateway-1) in the Azure	168.63.252.133	
Datacenter Subnet , the traffic of which is to traverse the CloudBridge tunnel	10.102.147.0/24	
Azure Subnet , the traffic of which is to traverse the CloudBridge tunnel	10.20.0.0/16	
Settings on CloudBridge appliance CB_Appliance-1 in Datacenter		
	SNIP1(for reference purposes only)	66.165.176.15
IPSec profile	CB_Azure_IPSec_Profile	• IKE version = v1 • Encryption algorithm = AES • Hash algorithm = HMAC SHA1
CloudBridge tunnel	CB_Azure_Tunnel	• Remote IP = 168.63.252.133 • Local IP= 66.165.176.15 • Tunnel protocol = IPSec • IPSec profile= CB_Azure_IPSec_Profile
Policy based route	CB_Azure_Pbr	• Source IP range = Subnet in the datacenter =10.102.147.0-

		10.102.147.255 • Destination IP range =Subnet in Azure =10.20.0.0-10.20.255.255 • IP Tunnel = CB_Azure_Tunnel
Settings on Microsoft Azure		
Public IP Address of the Azure_Gateway-1		168.63.252.133
Local Network	My-Datacenter-Network	• VPN Device IP address =SNIP address of the CloudBridge appliance = 66.165.176.15 • Address space= Subnet in datacenter =10.102.147.0/24
Virtual Network	Azure-Network-for-CloudBridge-Tunnel	• Address Space= 10.20.0.0/16 • Subnet in Azure=Azure-Subnet-1= 10.20.20.0/24 • Local Network=My-Datacenter-Network • Gateway Subnet=10.20.10.0/24

Following is the traffic flow in the CloudBridge tunnel:

1. Client C1 sends a request to server S1.
2. The request reaches CloudBridge appliance CB_Appliance-1.
3. The request packet in CB_Appliance-1 matches the condition specified in the PBR entity CB_Azure_Pbr as the source IP address and the destination IP address of the request packet belonging to the source IP range and destination IP range, respectively, set in CB_Azure_Pbr.
4. Because CloudBridge tunnel entity CB_Azure_Tunnel is bound to CB_Azure_Pbr, the appliance prepares the packet to be sent across the CB_Azure_Tunnel.
5. For CloudBridge tunnel CB_Azure_Tunnel, CB_Appliance-1 checks the stored IPSec security association (SA) parameters for processing outbound packets, as agreed between CB_Appliance-1 in the datacenter and Azure_Gateway-1 in the Azure cloud. The IPSec Encapsulating Security Payload (ESP) protocol in the CloudBridge appliance uses these SA parameters for outbound packets to encrypt the request packet.
6. The ESP protocol ensures the packet's integrity by using a HMAC hash function and the packet's confidentiality by using the AES encryption algorithm. The ESP protocol, after encrypting the request packet and calculating the HMAC, generates an ESP header and then inserts it before the encrypted IP packet. The ESP protocol also generates an ESP trailer and then inserts it at the end of the encrypted IP packet.
7. The IPSec protocol encapsulates the resulting packet by adding an IP header before the ESP header. The destination address in the IP header is the IP address of Azure-gateway-1, and the source address is the SNIP2 address.
8. The resulting packet is sent to Azure_Gateway-1. There is
9. Azure-gateway-1, upon receiving the packet from CB_Appliance-1, decapsulates the packet by removing the IPSec IP header.
10. Azure-gateway-1 then checks the stored IPSec security association (SA) parameters for processing inbound packets, as agreed between CB_Appliance-1 and Azure_Gateway-1. The IPSec ESP protocol on Azure_Gateway-1 uses these SA

parameters for inbound packets, and the ESP header of the decapsulated request packet, to decrypt the packet.

11. The resulting packet is the same packet as the one received by CB_Appliance-1 in step 2. This packet has the destination IP address set to the IP address of server S1. Azure_Gateway-1 forwards this packet to server S1.
12. S1 processes the request packet and sends out a response packet. The destination IP address in the response packet is the IP address of client CL1, and source IP address is the IP address of server S1.
13. The response packet reaches Azure_Gateway-1. Microsoft Azure checks the stored IPSec security association (SA) parameters for processing outbound packets, as agreed between CB_Appliance-1 and Azure_Gateway-1. Microsoft Azure encrypts and encapsulates the response packet in the same way that CB_Appliance-1 encrypted and encapsulated the request packet in steps 5, 6, and 7.
14. Azure_Gateway-1 sends the resulting packet to CB_Appliance-1.
15. CB_Appliance-1, upon receiving the packet from Azure_Gateway-1, decapsulates and decrypts the packet in the same way that Azure_Gateway-1 decapsulated and decrypted the request packet in steps 9 and 10.
16. The resulting packet is the same packet that was received by Azure_Gateway-1 in step 13. This response packet has the destination IP address set to the IP address of server CL1. CB_Appliance-1 forwards the response packet to client CL1.

Configuration Steps

For setting up a CloudBridge tunnel between your datacenter and Azure, you must install CloudBridge VPX/MPX in your datacenter, configure Microsoft Azure for the CloudBridge tunnel, and then configure the CloudBridge appliance in the data center for the CloudBridge tunnel.

Configuring a CloudBridge tunnel between a CloudBridge appliance in datacenter and Microsoft Azure consists of the following tasks:

1. **Setting up the CloudBridge appliance in the datacenter**. This task involves deploying and configuring a CloudBridge physical appliance (MPX), or provisioning and configuring a CloudBridge virtual appliance (VPX) on a virtualization platform in the datacenter.
2. **Configuring Microsoft Azure for the CloudBridge tunnel**. This task involves creating local network, virtual network, and gateway entities in Azure. The local network entity specifies the IP address of the CloudBridge tunnel end point (the CloudBridge appliance) on the datacenter side, and the datacenter subnet whose traffic is to traverse the CloudBridge tunnel. The virtual network defines a network on Azure. Creating the virtual network includes defining a subnet whose traffic is to traverse the CloudBridge tunnel to be formed. You then associate the local network with the virtual network. Finally, you create a gateway that becomes the end point at the Azure end of the CloudBridge tunnel.
3. **Configuring the CloudBridge appliance in the Datacenter for the CloudBridge tunnel**. This task involves creating an IPSec profile, an IP tunnel entity, and a PBR entity in the CloudBridge appliance in datacenter. The IPSec profile entity specifies the IPSec protocol parameters, such as IKE version, encryption algorithm, hash algorithm, and PSK, to be used in the CloudBridge tunnel. The IP tunnel specifies the IP address of both the CloudBridge tunnel end points (the CloudBridge appliance in datacenter and the gateway in Azure) and the protocol to be used in the CloudBridge tunnel. You then associate the IPSec

profile entity with the IP tunnel entity. The PBR entity specifies the two subnets, in the datacenter and in the Azure cloud, that are to communicate with each other through the CloudBridge tunnel. You then associate the IP tunnel entity with the PBR entity.

Points to Consider for a CloudBridge Tunnel Configuration

Before configuring a CloudBridge tunnel between a CloudBridge appliance in datacenter and Microsoft Azure, consider the following points:

1. The CloudBridge appliance must have a public facing IPv4 address (type SNIP) to use as a tunnel end-point address for the CloudBridge tunnel. Also, the CloudBridge appliance should not be behind a NAT device.
2. Azure supports the following IPSec settings for a CloudBridge tunnel. Therefore, you must specify the same IPSec settings while configuring the CloudBridge appliance for the CloudBridge tunnel.
    - IKE version = v1
    - Encryption algorithm = AES
    - Hash algorithm = HMAC SHA1
3. You must configure the firewall in the datacenter edge to allow the following.
    - Any UDP packets for port 500
    - Any UDP packets for port 4500
    - Any ESP (IP protocol number 50) packets
4. IKE re-keying, which is renegotiation of new cryptographic keys between the CloudBridge tunnel end points to establish new SAs, is not supported. When the Security Associations (SAs) expire, the tunnel goes into the DOWN state. Therefore, you must set a very large value for the lifetimes of SAs.
5. You must configure Microsoft Azure before specifying the tunnel configuration on the CloudBridge appliance, because the public IP address of the Azure end (gateway) of the tunnel, and the PSK, are automatically generated when you set up the tunnel configuration in Azure. You need this information for specifying the tunnel configuration on the CloudBridge appliance.

Setting Up the CloudBridge Appliance in the Datacenter

Before you set up a CloudBridge MPX or VPX in the datacenter, rack mount the MPX appliance or provision the VPX instance.

To rack mount a CloudBridge MPX appliance, follow the instructions for rack mounting a NetScaler MPX appliance. See http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-10/ns-instpk-install-ns-wrapper.html

To provision a CloudBridge VPX virtual appliance, apply the procedures for provisioning a NetScaler VPX virtual appliance. See http://support.citrix.com/proddocs/topic/netscaler-10/ns-gen-nsvpx-wrapper-con-10.html.

A CloudBridge appliance has both a command line interface (CLI) and a graphical user interface (GUI). The GUI includes a configuration utility for configuring the appliance. For initial access, all CloudBridge appliances ship with the default NetScaler IP address (NSIP) of 192.168.100.1 and default subnet mask of 255.255.0.0. You can assign a new NSIP and an associated subnet mask during initial configuration.

Initial Configuration Using the Configuration Utility

The configuration utility is accessed from a web browser. To configure the CloudBridge by using the Setup Wizard in the configuration utility, you need an administrative workstation or laptop configured on the same network as the appliance. You also need Java Runtime Environment (JRE) version 1.6 or later. You can use the Setup Wizard to configure the following initial settings:

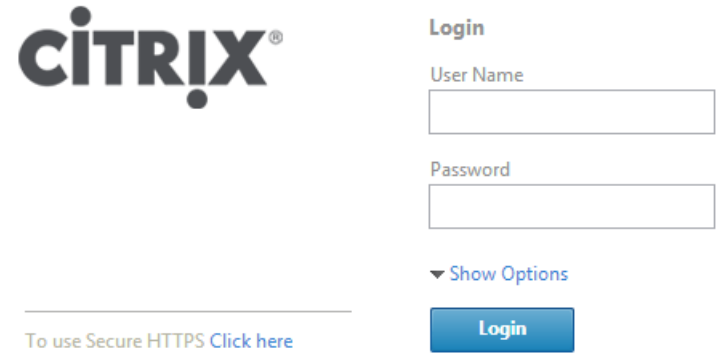
- System IP address and subnet mask
- Subnet or Mapped IP address and subnet mask
- Host name
- Default gateway
- Time zone
- Licenses
- Administrator password

Important: Before running the Setup Wizard, download your licenses from the Citrix web site and put them in a location on your workstation or laptop hard drive or another device, so that you can access them from your web browser during configuration.

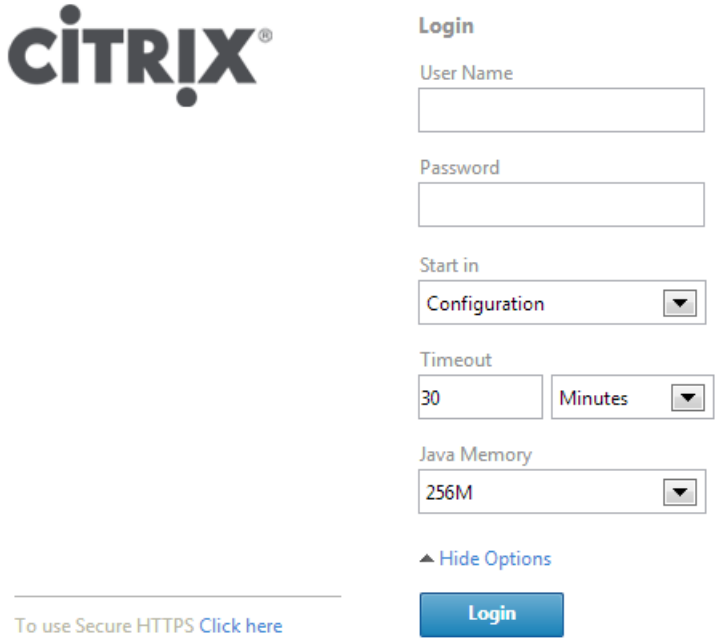
1. In a web browser, type http:// 192.168.100.1.

   Note: The operating system is preconfigured with a default IP address and associated subnet mask. The default IP address is 192.168.100.1 and the default mask is 255.255.0.0.

2. In **User Name** and **Password**, type the administrator credentials. The default username and password are nsroot and nsroot.



3. Click **Show Options**.
4. In **Start in**, select **Configuration**, and then click **Login**.



5. In the **Setup Wizard**, click **Next**, and then follow the instructions in the wizard.

Note: To prevent an attacker from compromising your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.

Configuring Microsoft Azure for the CloudBridge Tunnel

To create a CloudBridge tunnel configuration on Microsoft Azure, use the Microsoft Windows Azure Management Portal, which is a web based graphical interface for creating and managing resources on Microsoft Azure.

Before you begin the CloudBridge tunnel configuration on Azure cloud, make sure that:

- You have a user account for Microsoft Azure.
- You have a conceptual understanding of Microsoft Azure.
- You are familiar with the Microsoft Windows Azure Management Portal.

Note: The procedures for configuring Microsoft Azure for a CloudBridge tunnel might change over time, depending on the Microsoft Azure release cycle. Citrix recommends the following Microsoft Azure documentation for the latest procedures.

- http://www.windowsazure.com/en-us/manage/services/networking/cross-premises-connectivity/

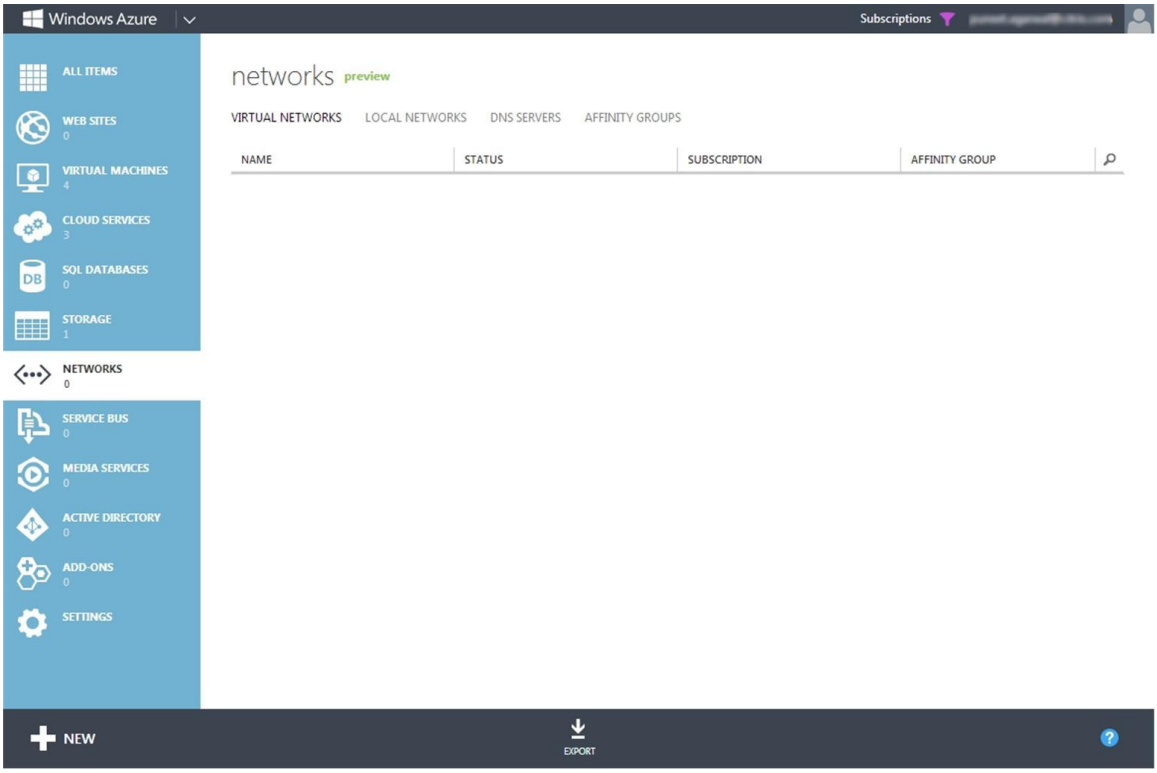
To configure a CloudBridge tunnel between a datacenter and an Azure cloud, perform the following tasks on Microsoft Azure by using the Microsoft Windows Azure Management Portal:

- **Create a local network entity**. Create a local network entity in Windows Azure for specifying the network details of the datacenter. A local network entity specifies the IP address of the CloudBridge tunnel end point (the CloudBridge appliance) on the datacenter side and the datacenter subnet whose traffic is to traverse the CloudBridge tunnel.
- **Create a new Virtual Network.** Create virtual network entity that defines a network on Azure. This task includes defining a private address space, where you provide a range of private addresses and subnets belonging to the range specified in the address space. The traffic of the subnets will traverse the CloudBridge tunnel. You then associate a local network entity with the virtual network entity. This association lets Azure create a configuration for a CloudBridge tunnel between the virtual network and the data center network. A gateway (to be created) in Azure for this virtual network will be the CloudBridge end point at the Azure end of the CloudBridge tunnel. You then define a private subnet for the gateway to be created. This subnet belongs to the range specified in the address space in the virtual network entity.
- **Create a gateway in Windows Azure**. Create a gateway that becomes the end point at the Azure end of the CloudBridge tunnel. Azure, from its pool of public IP addresses, assigns an IP address to the gateway created.
- **Gather the public IP address of the gateway and the pre-shared key**. For a CloudBridge tunnel configuration on Azure, the public IP address of the gateway and the pre-shared Key (PSK) are automatically generated by Azure. Make a note of this information. You will need it for configuring the CloudBridge tunnel on the CloudBridge appliance in datacenter.

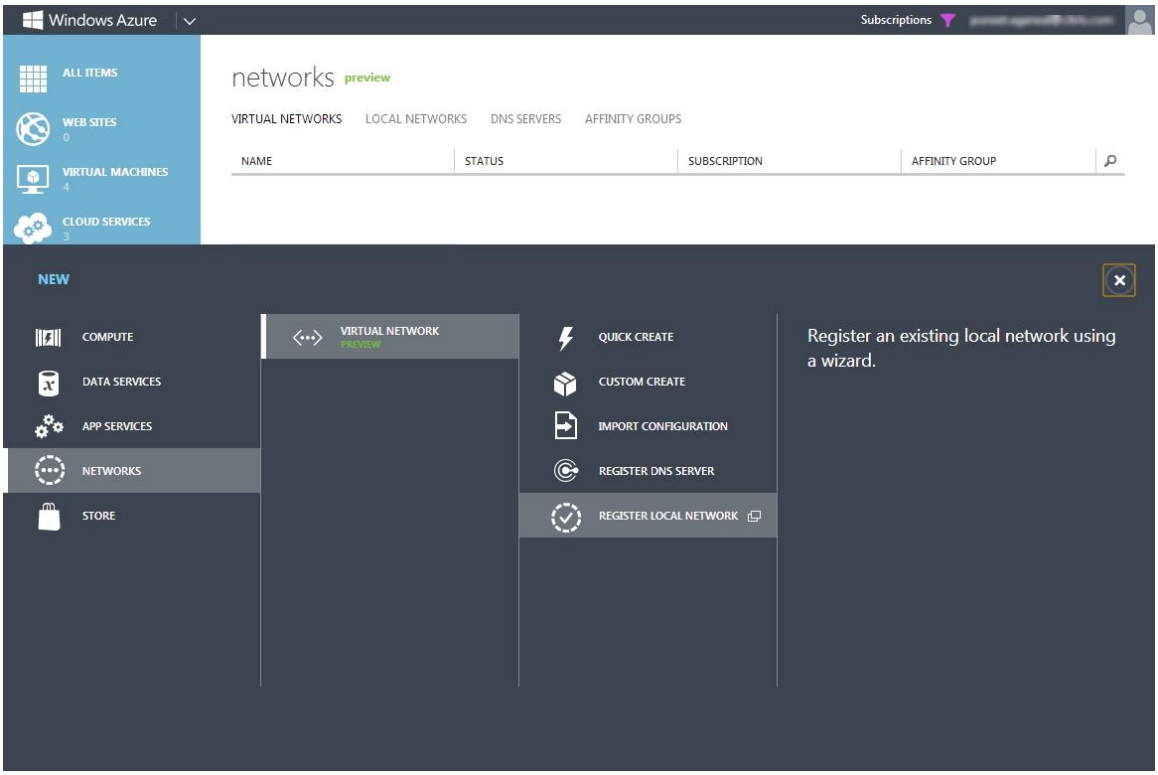
To specify a local network by using the Microsoft Windows Azure Management Portal

1. In the left pane, click **NETWORKS**.

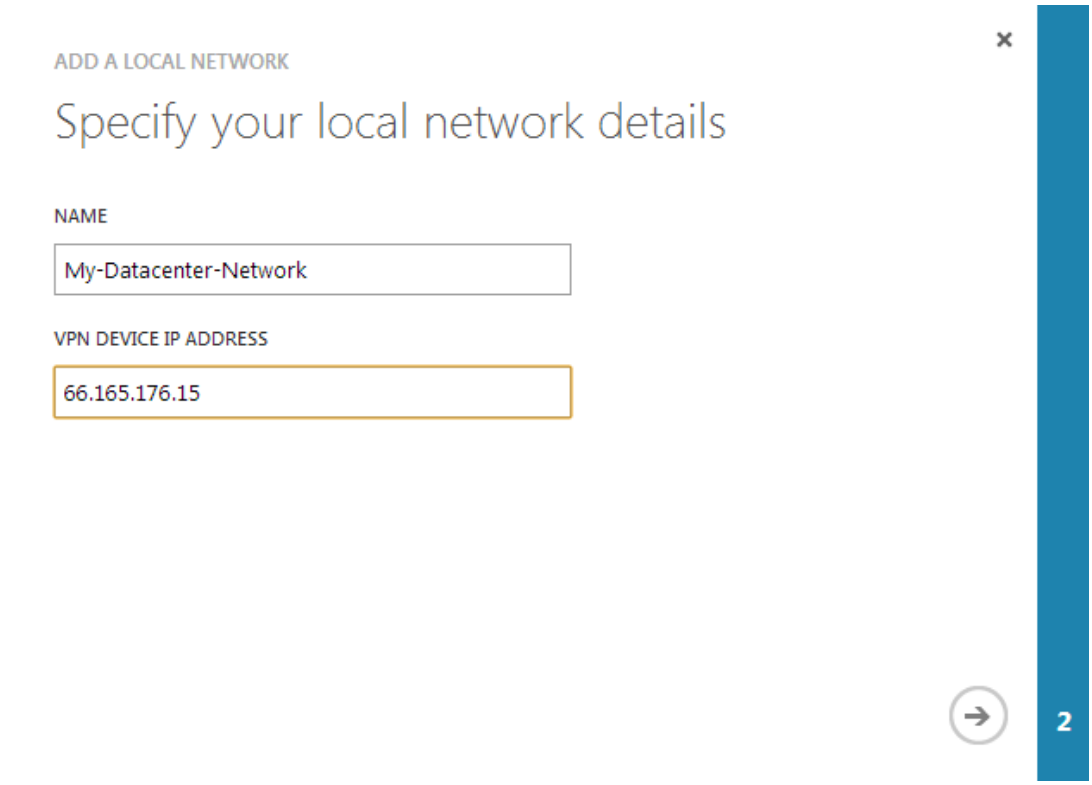
2. In the lower left-hand corner of the screen, click **+ NEW.**



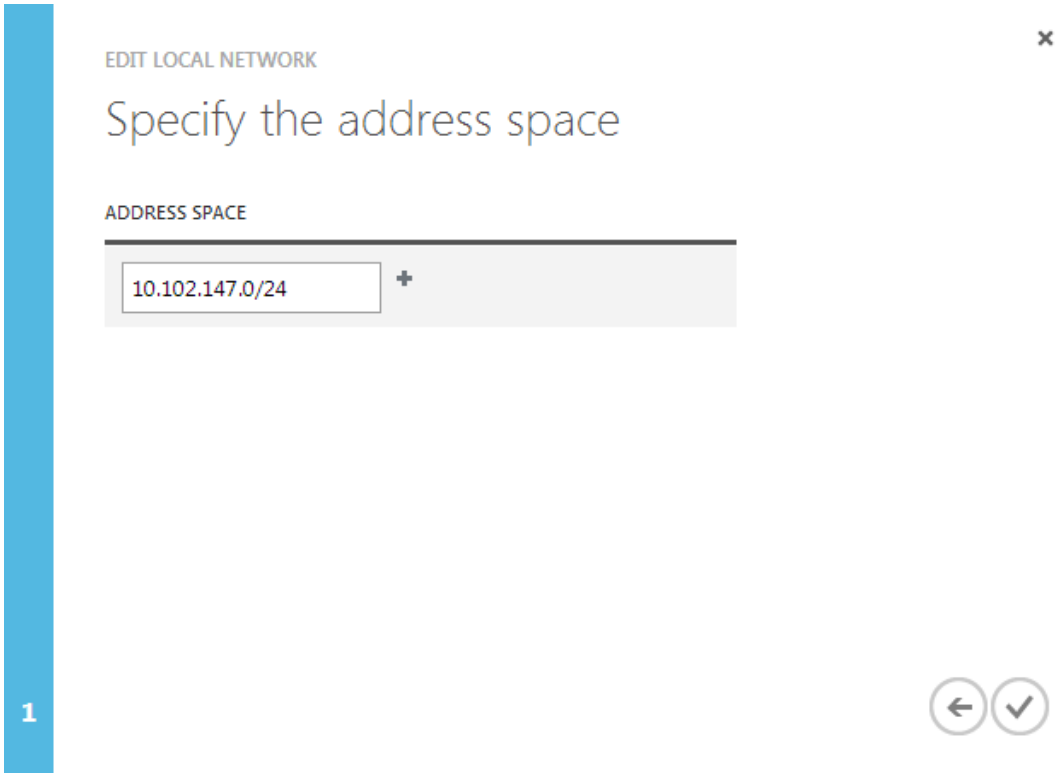
3. In the **NEW** navigation pane, click **NETWORK**, then click **VIRTUAL NETWORK**, and then click **REGISTER LOCAL NETWORK**.



4. In the **ADD A LOCAL NETWORK** wizard, in the **specify your local network details** screen, set the following parameters:
    - **NAME**
    - **VPN DEVICE IP ADDRESS**

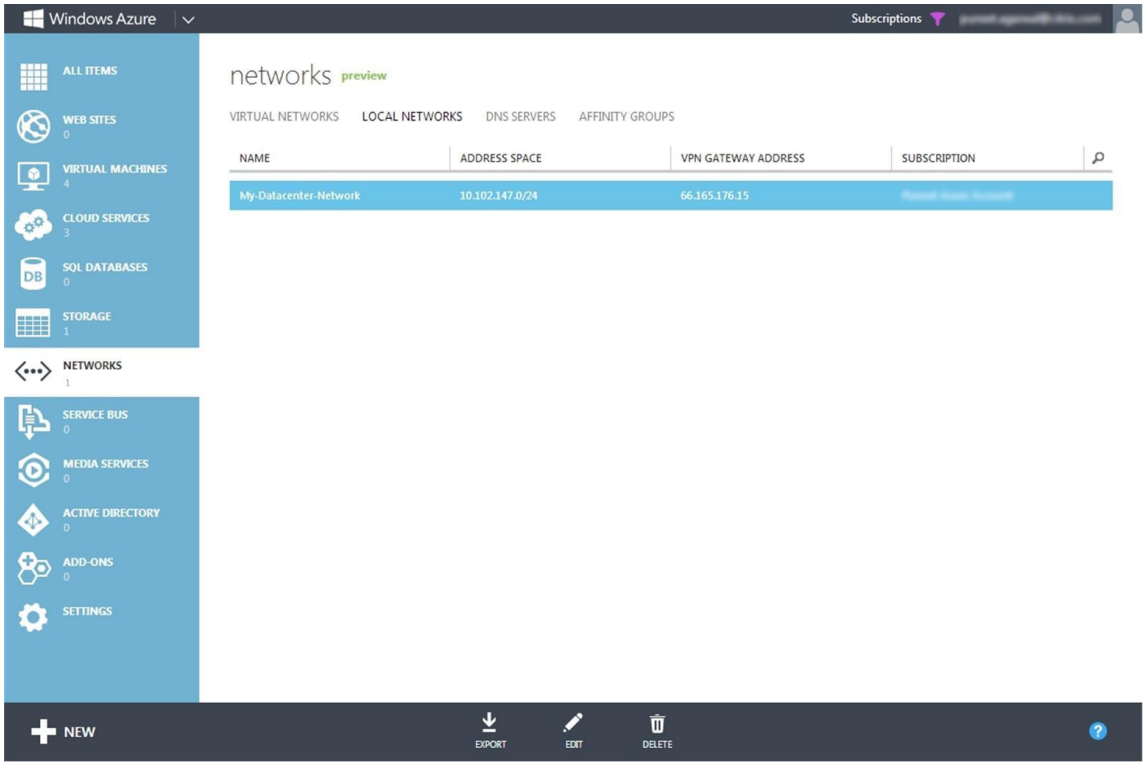


5. In the lower right corner of the screen, click **->** (forward arrow mark).
6. On the **Specify the address space** screen, set the following parameter:
   - **ADDRESS SPACE**



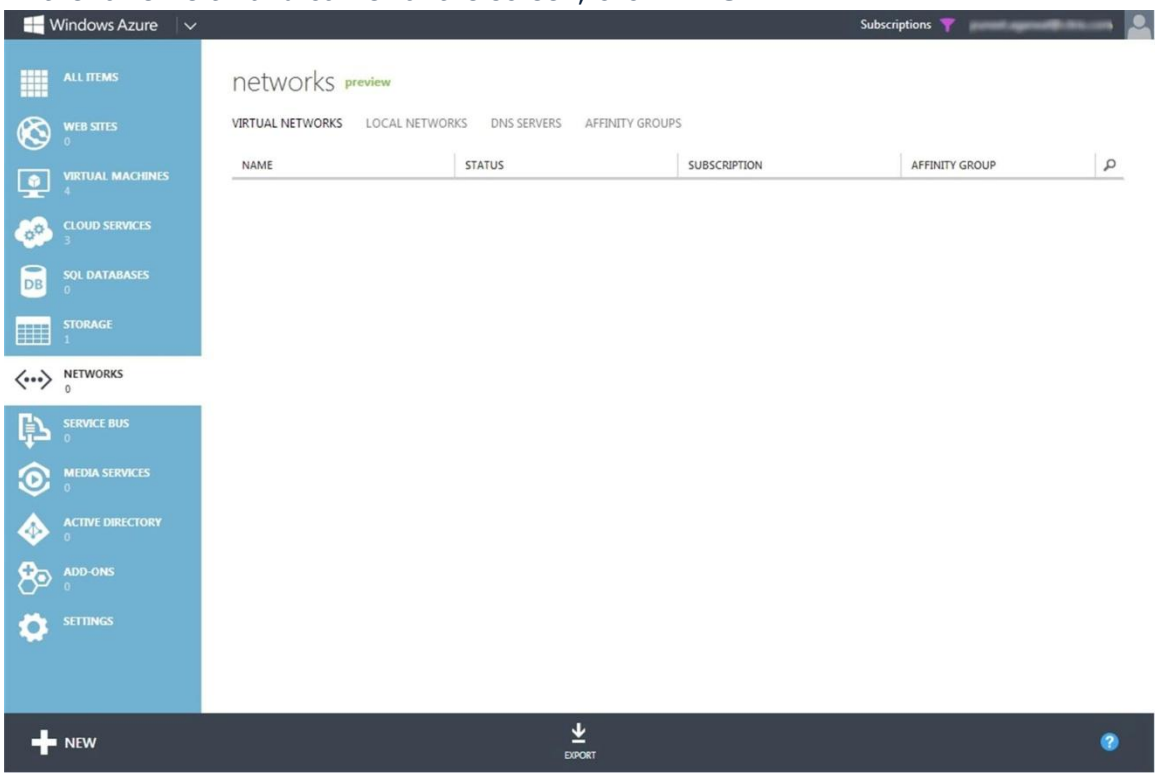
7. In the lower right corner of the screen, click the check mark.

8. The local network entity is created in Windows Azure. You can verify it on the portal's **LOCAL NETWORK** tab.

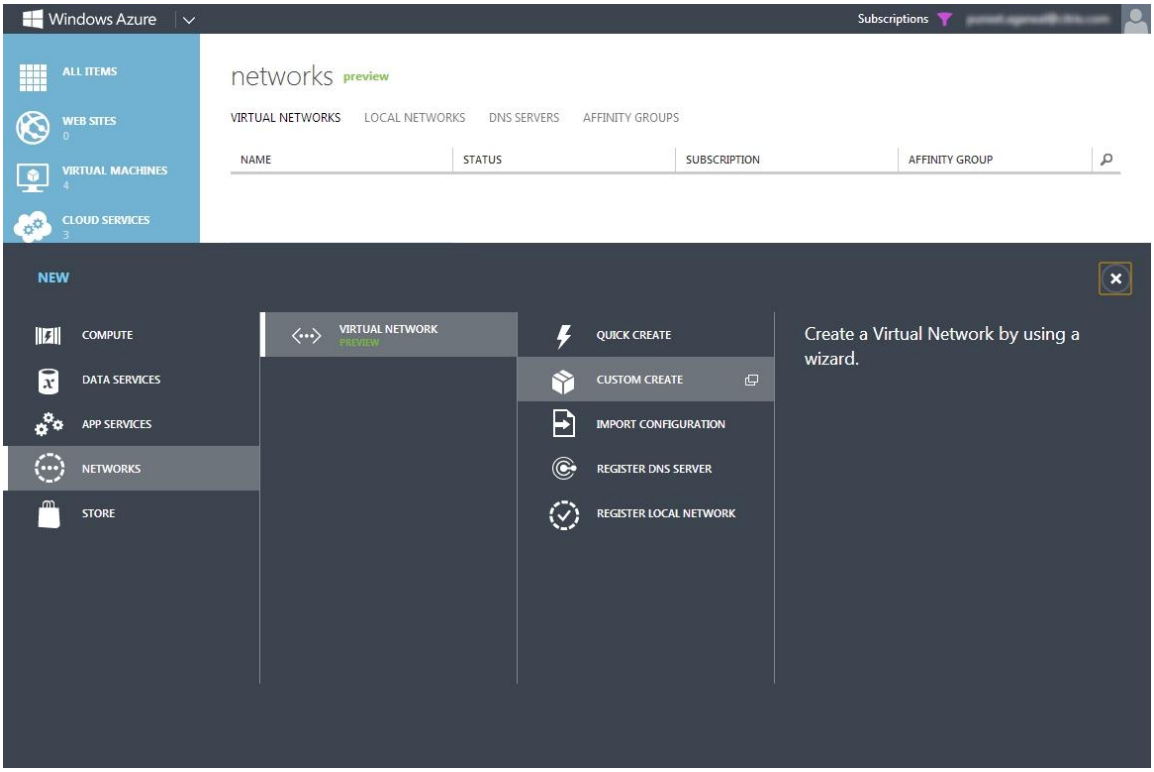


To create a virtual network in Azure by using the Microsoft Windows Azure Management Portal

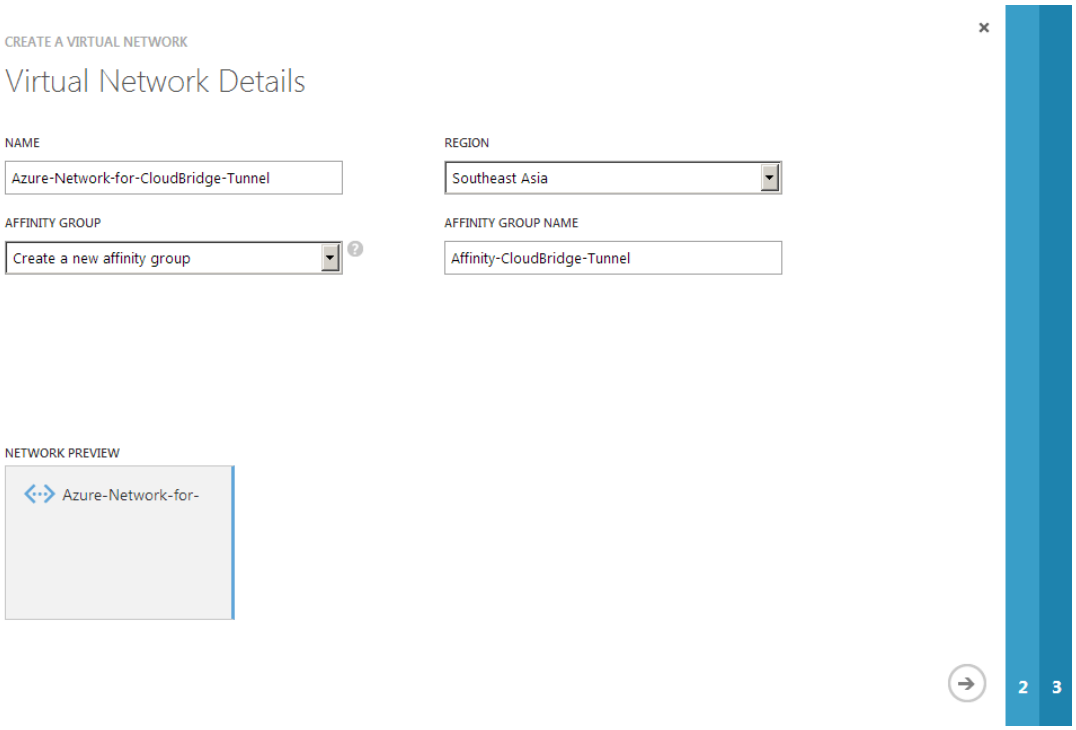
1. In the left pane, click **NETWORKS**.
2. In the lower left-hand corner of the screen, click **+ New**.



3. In the **NEW** navigation pane, click **NETWORK**, then click **VIRTUAL NETWORK**, and then click **CUSTOM CREATE**.

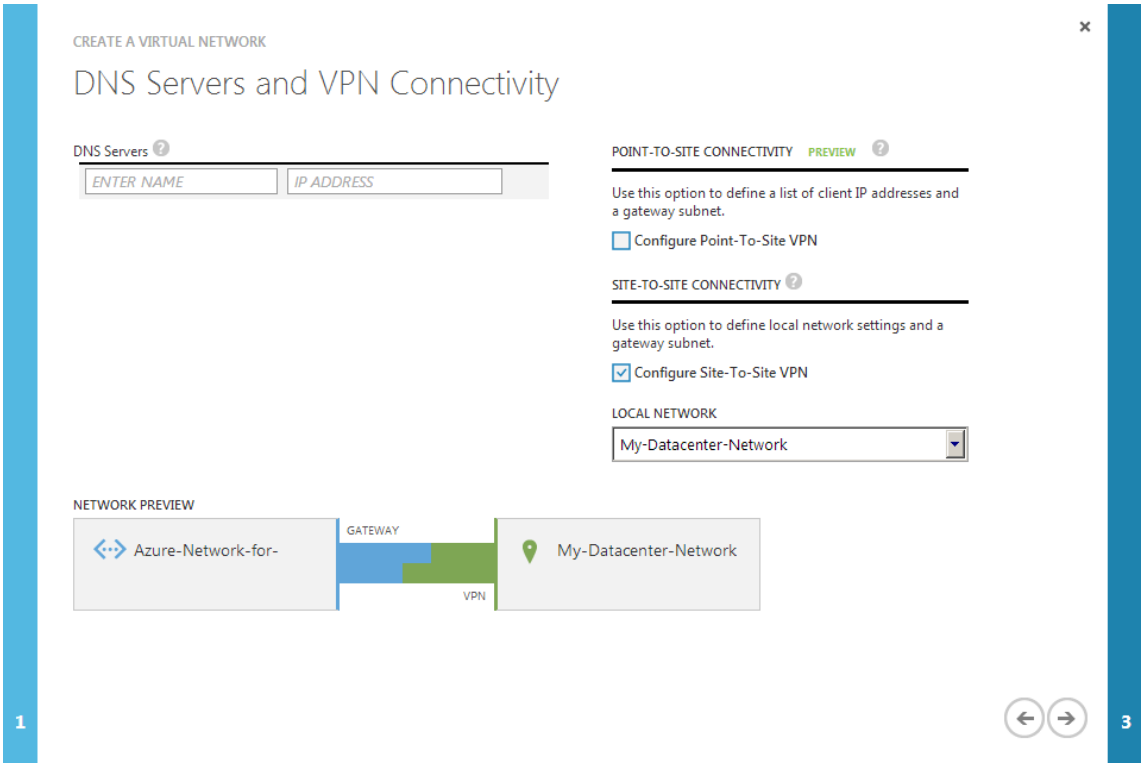


4. In the **CREATE A VIRTUAL NETWORK** wizard, in the **Virtual Network Details** screen, set the following parameters:
   - **NAME**
   - **AFFINITY GROUP**
   - **REGION**
   - **AFFINITY GROUP NAME**

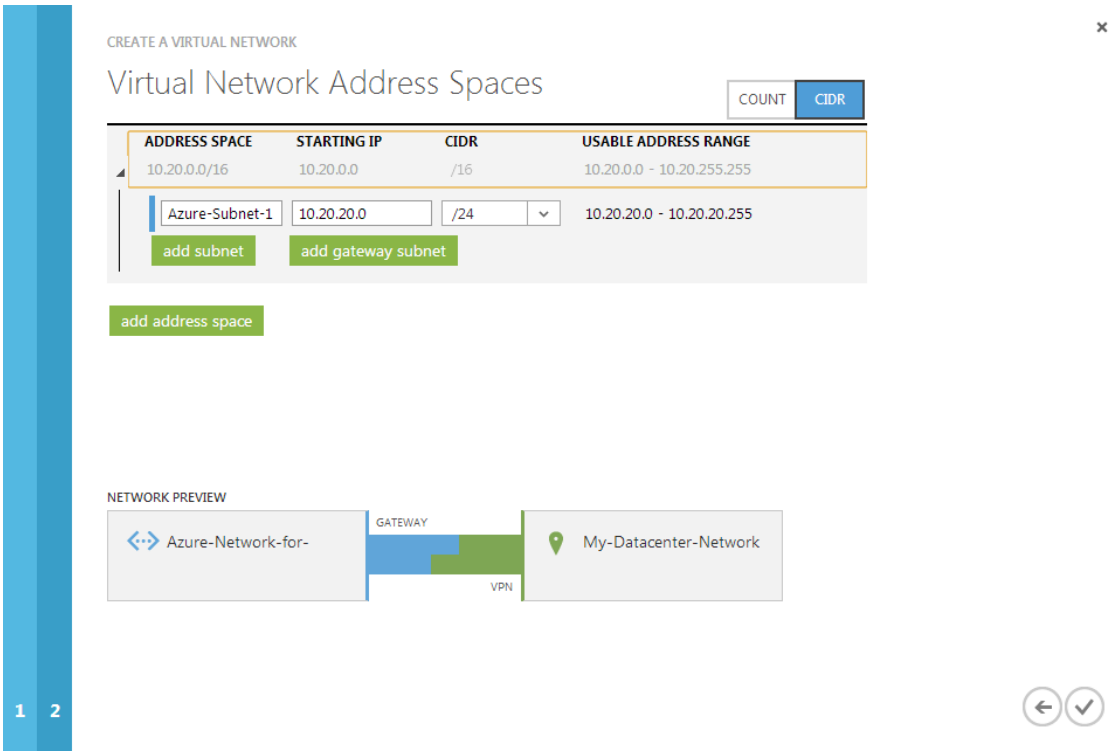


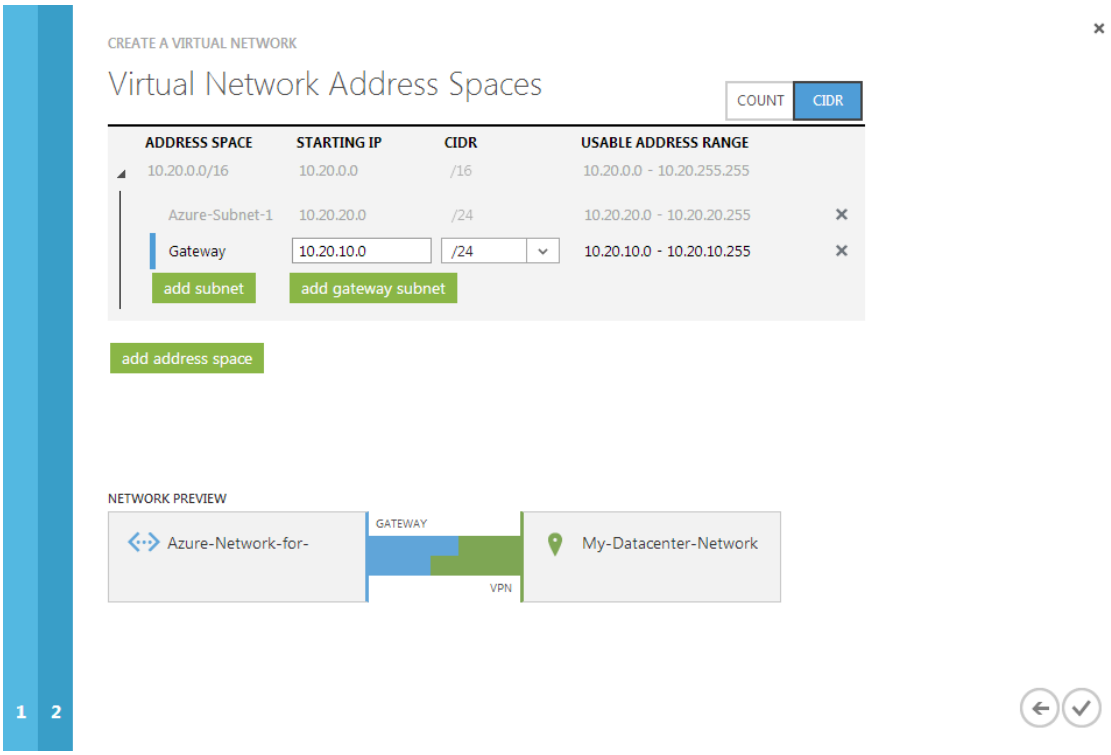
5. Click **->** (forward arrow mark) in the lower right-hand corner of the screen.

6. In the **DNS Servers and VPN Connectivity** screen, in **SITE-TO-SITE CONNECTIVITY**, select **Configure Site-To-Site VPN** and set the following parameter:
    - **LOCAL NETWORK**



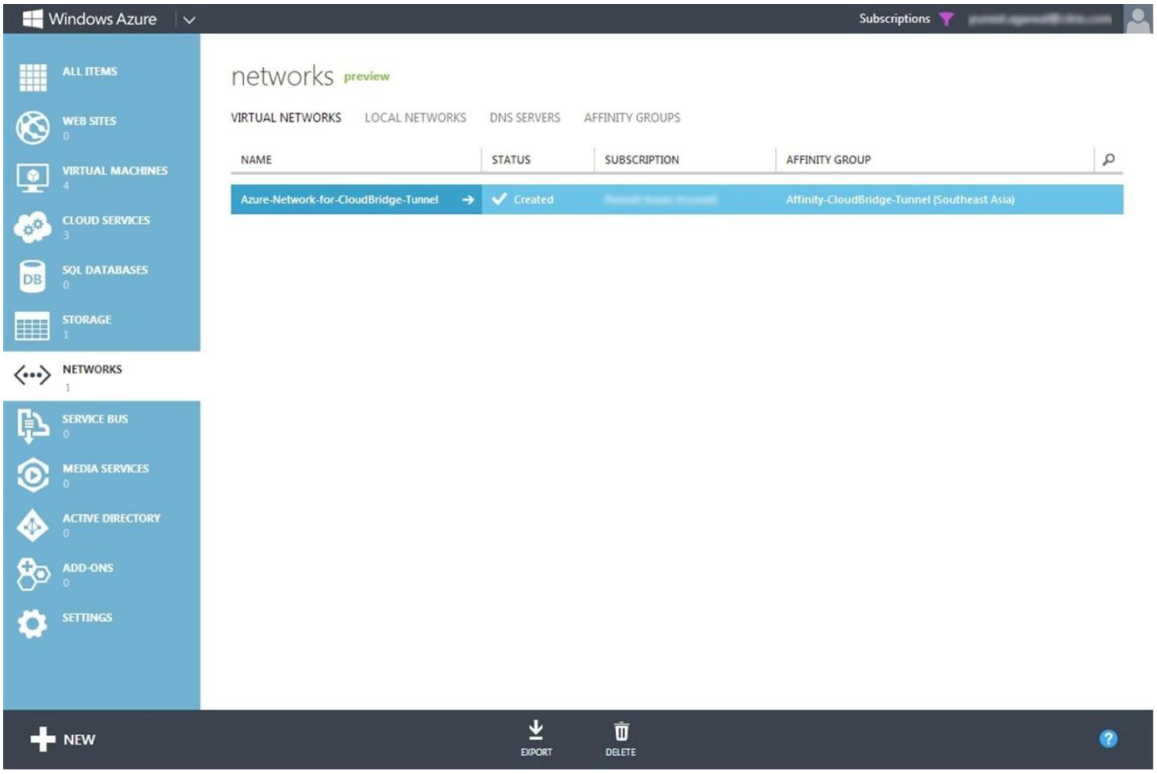
7. In the **Address Space and Subnets** screen, set the following parameters:
    - **ADDRESS SPACE**
    - **SUBNETS**
    - **Gateway**





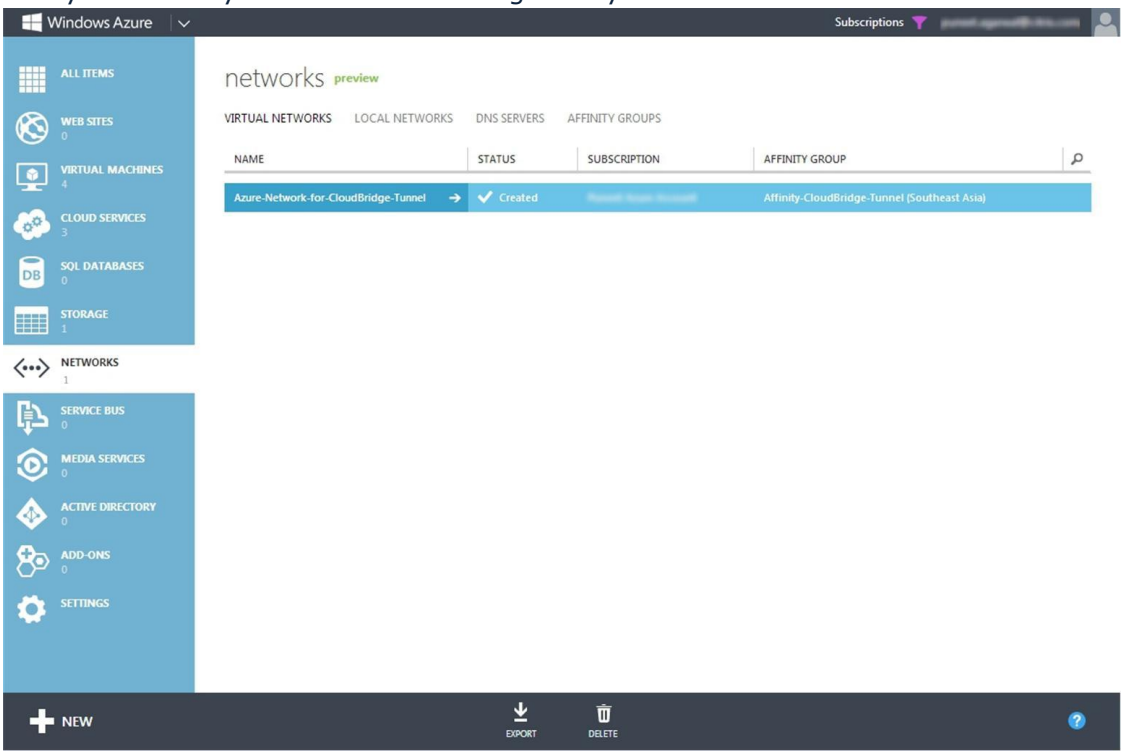
8. Click the check mark in the lower right-hand corner of the screen.

9. The virtual network is created in Windows Azure and is listed on the **VIRTUAL NETWORK** tab.

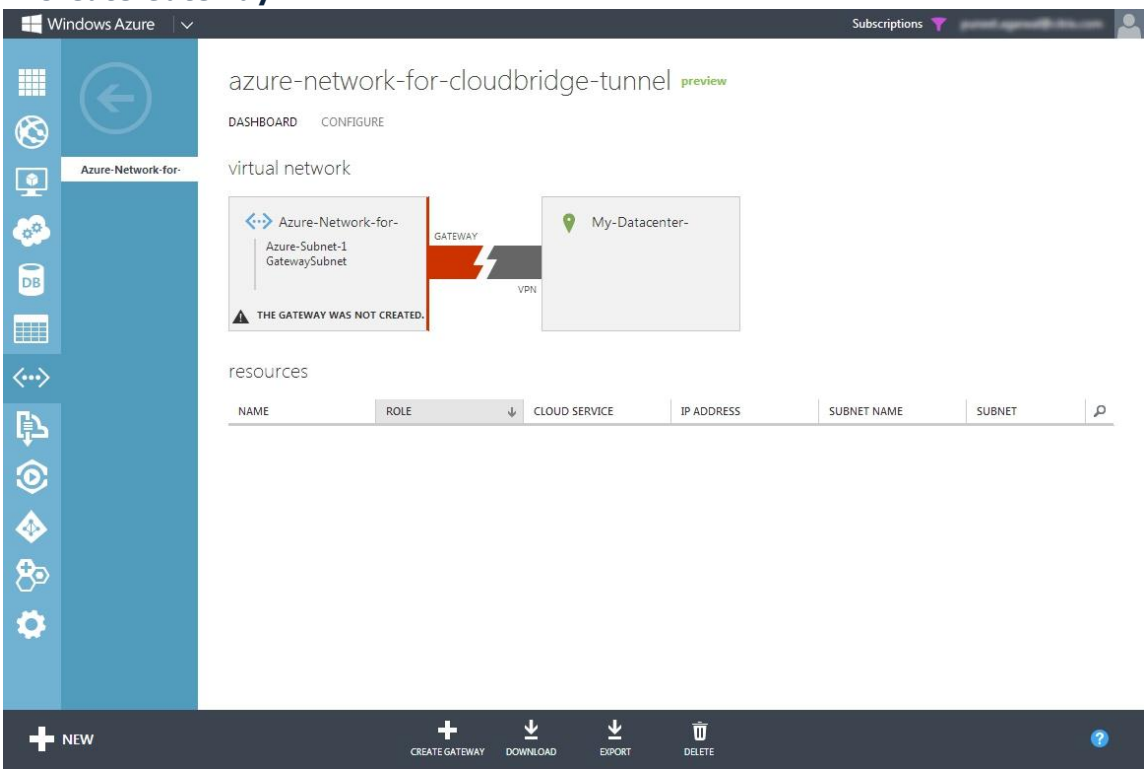


To create a gateway by using the Microsoft Windows Azure Management Portal

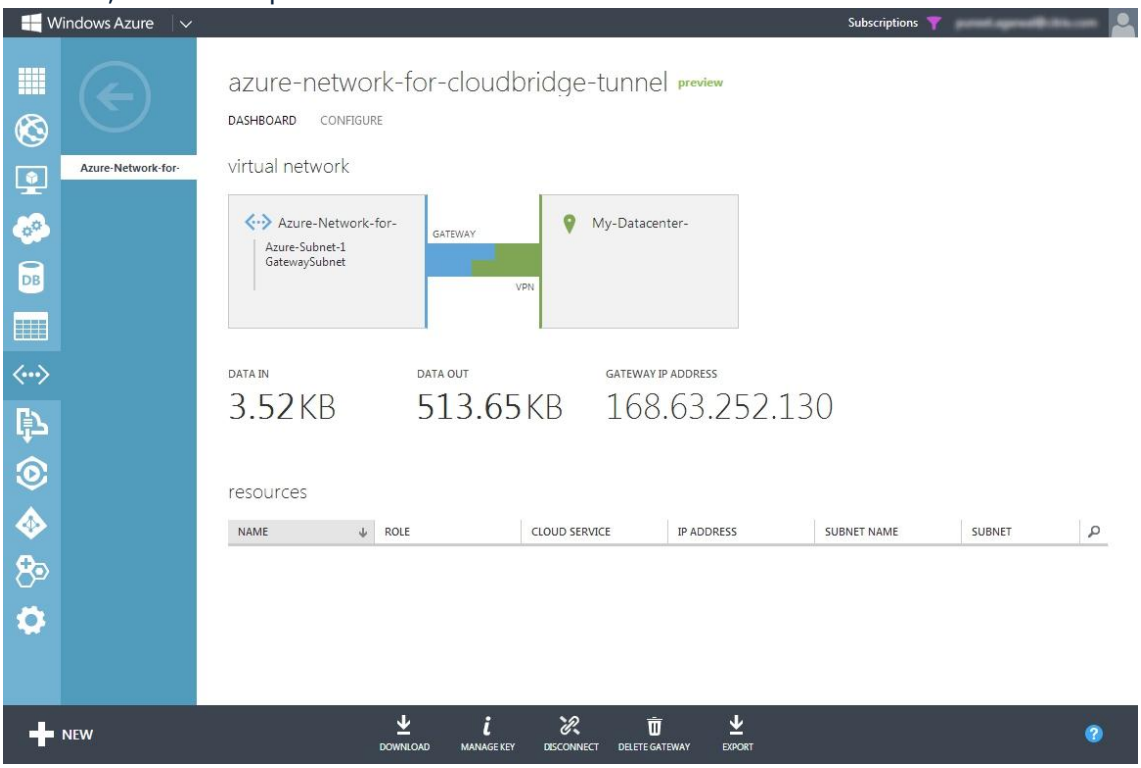
1. In the left pane, click **NETWORKS**.
2. On the **Virtual Network** tab, in the **Name** column, click the virtual network entity for which you want to create a gateway.



3. On the **DASHBOARD** page of the virtual network, at the bottom of the page, click **+ Create Gateway**.

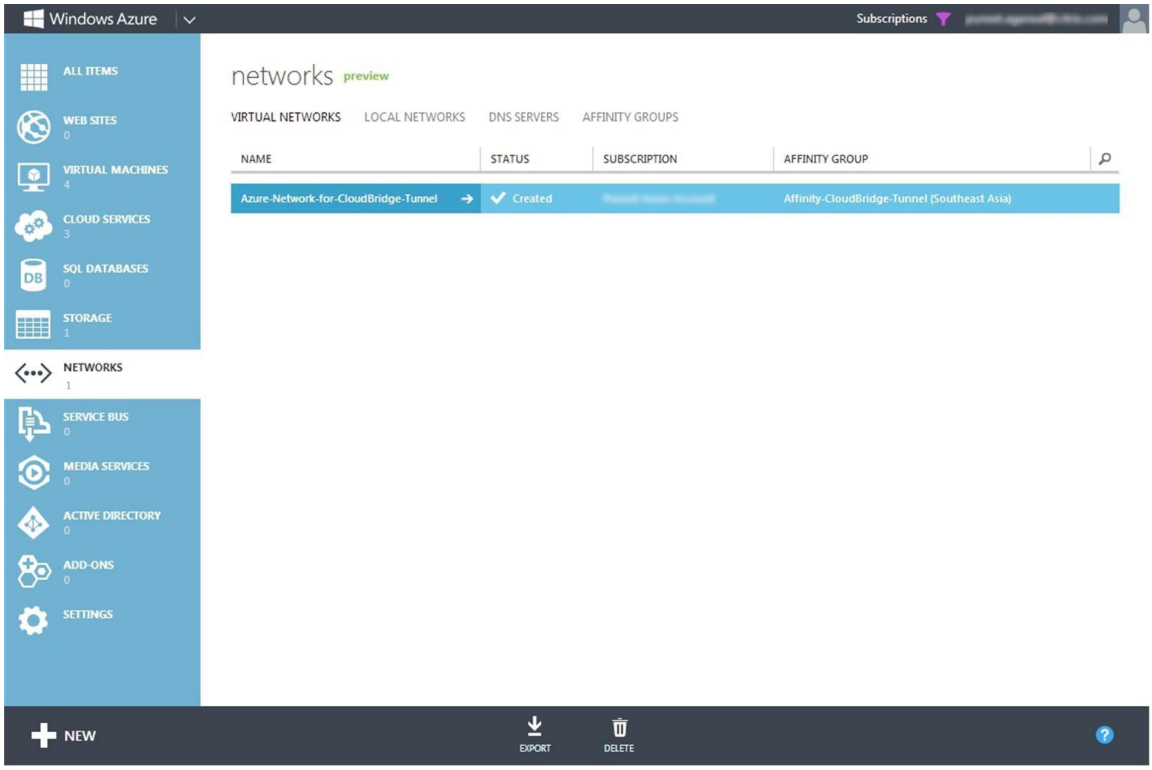


4. When prompted to confirm you want the gateway created, click **YES**. Creating the gateway can take up to 15 minutes.
5. When the gateway is created, the **DASHBOARD** page displays the gateway IP address, which is a public IP address.

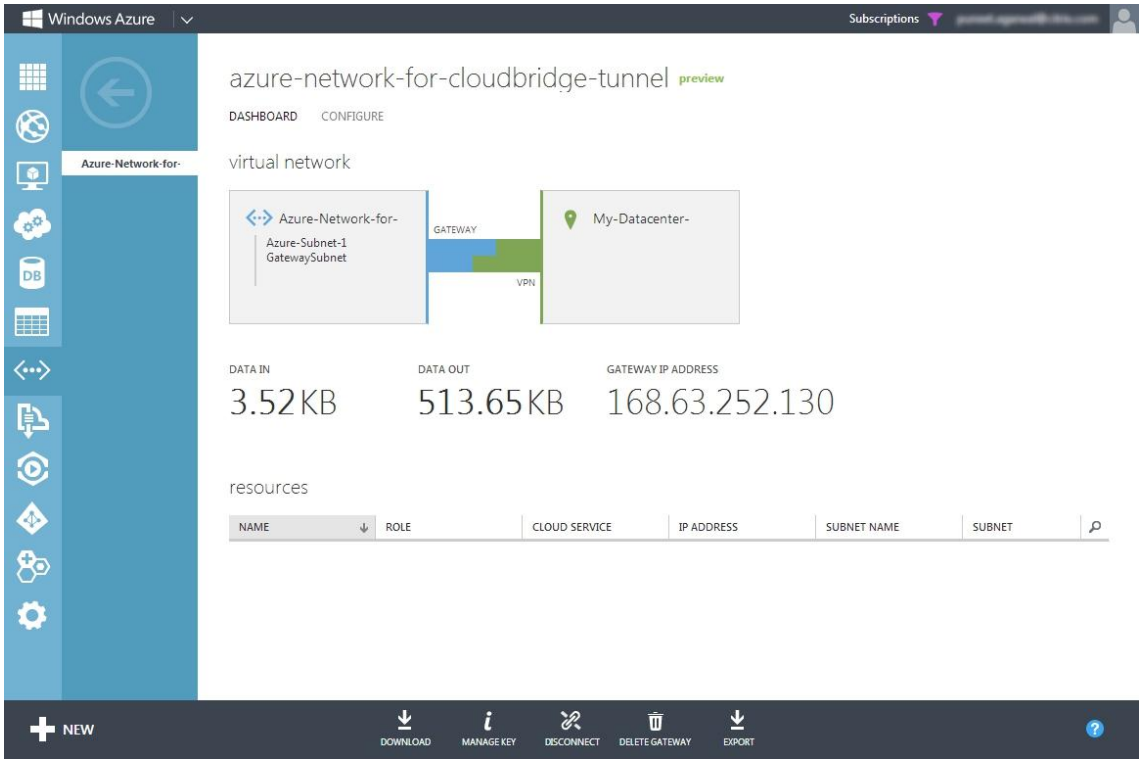


To gather public IP address of the gateway and the pre-shared key information by using the Microsoft Windows Azure Management Portal

1. In the left pane, click **NETWORKS**.
2. On the **Virtual Network** tab, in the **Name** column, click the virtual network entity.

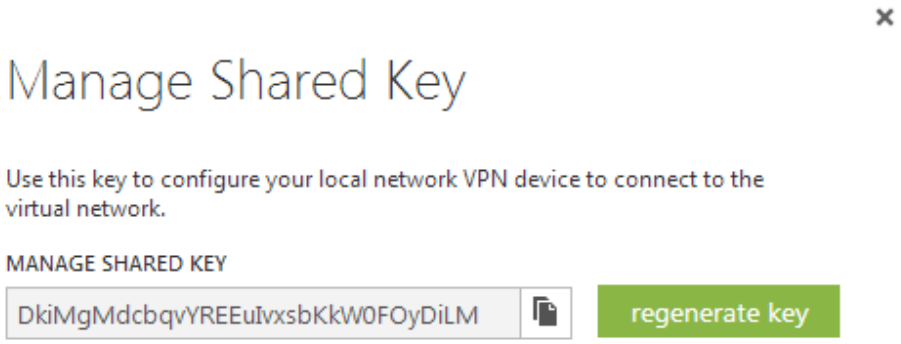


3. On the **DASHBOARD** page of the virtual network, copy the **Gateway IP Address**.



4. For the Pre Shared Key (PSK), at the bottom of the page, click **MANAGE KEY.**

5. In the **MANAGE SHARED KEY** dialog box, copy the **SHARED KEY**.



Configuring the CloudBridge Appliance in the Datacenter for the CloudBridge Tunnel

To configure a CloudBridge tunnel between a datacenter and an Azure cloud, perform the following tasks on the CloudBridge appliance in the datacenter. You can use either the CloudBridge command line or the configuration utility:

- **Create an IPSec profile**. An IPSec profile entity specifies the IPSec protocol parameters, such as IKE version, encryption algorithm, hash algorithm, and PSK, to be used by the IPSec protocol in the CloudBridge tunnel.
- **Create an IP tunnel with IPSec protocol and associate the IPSec profile to it**. An IP tunnel specifies the local IP address (a public SNIP address configured on the CloudBridge appliance), remote IP address (the public IP address of the gateway in Azure), protocol (IPSec) used to set up the CloudBridge tunnel, and an IPSec profile entity. The created IP tunnel entity is also called the CloudBridge tunnel entity.
- **Create a PBR rule and associate the IP tunnel to it**. A PBR entity specifies a set of conditions and an IP tunnel (CloudBridge tunnel) entity. The source IP address range and the destination IP range are the conditions for the PBR entity. You must set the source IP address range to specify the datacenter subnet whose traffic is to traverse the tunnel, and the destination IP address range to specify the Azure subnet whose traffic is to traverse the CloudBridge tunnel. Any request packet originated from a client in the subnet on the datacenter and destined to a server in the subnet on the Azure cloud matches the source and destination IP range of the PBR entity. This packet is then considered for CloudBridge processing and is sent across sent across the CloudBridge tunnel associated with the PBR entity.

The configuration utility combines all these tasks in a single wizard called the CloudBridge wizard.

To create an IPSEC profile by using the CloudBridge command line

At the CloudBridge command prompt, type:

- **add ipsec profile** <name> -**psk** <string> **-ikeVersion v1**

To create an IPSEC tunnel and bind the IPSEC profile to it by using the CloudBridge command line

At the CloudBridge command prompt, type:

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol** IPSEC –**ipsecProfileName** <string>

To create a PBR rule and bind the IPSEC tunnel to it by using the CloudBridge command line

At the CloudBridge command prompt, type:

- add **pbr** <pbrName> ALLOW –**srcIP** <subnet-range> -**dstIP** <subnet-range> **-ipTunnel** <tunnelName>
- **apply pbrs**

Sample Configuration

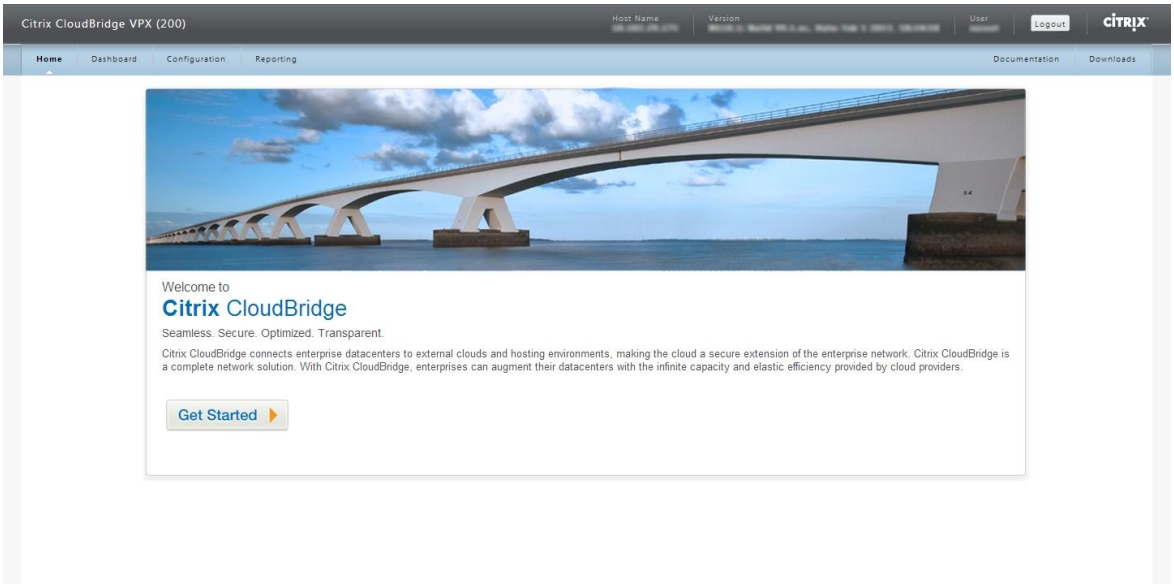
The following commands create all settings of CloudBridge appliance CB_Appliance-1 used in Example of CloudBridge Configuration and Data Flow.

```
> add ipsec profile CB_Azure_IPSec_Profile -psk DkiMgMdcbqvYREEuIvxsbKkW0FOyDiLM -ikeVersion v1 –lifetime 31536000
Done

> add iptunnel CB_Azure_Tunnel 168.63.252.133 255.255.255.255 66.165.176.15 –protocol IPSEC –ipsecProfileName CB_Azure_IPSec_Profile

Done

> add pbr CB_Azure_Pbr-srcIP 10.102.147.0-10.102.147.255 –dstIP 10.20.0.0-10.20.255.255 –ipTunnelCB_Azure_Tunnel
Done

> add apply pbrs
Done
```

To configure a CloudBridge Tunnel in CloudBridge appliance by using the configuration utility

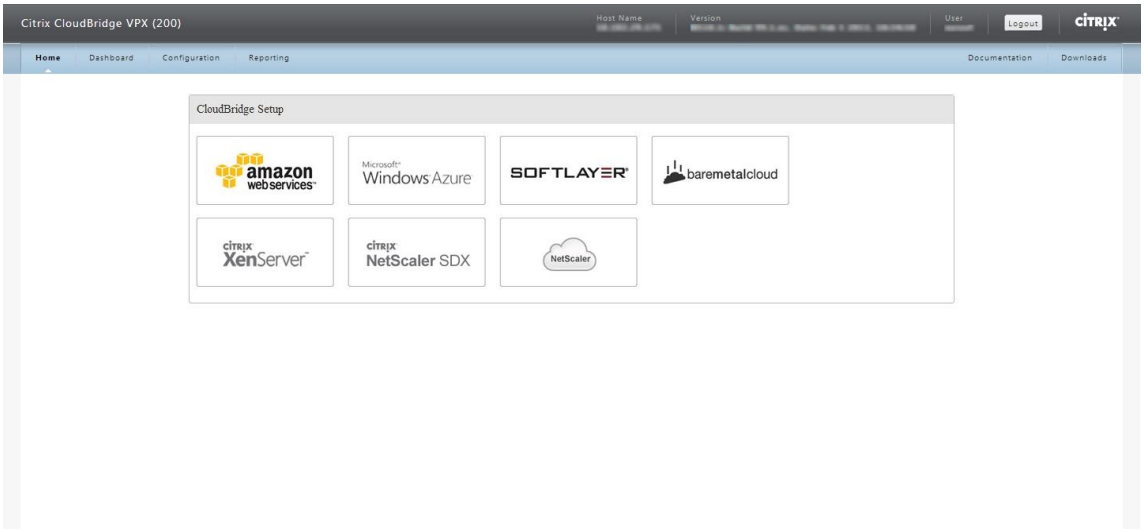
1. Access the configuration utility by using a web browser to connect to the IP address of the CloudBridge appliance in the datacenter.
2. On the **Configuration** tab, in the navigation pane, click **CloudBridge**.
3. In the right pane, under **Getting Started**, click **Create/Monitor CloudBridge**.

4. Click **Get Started**.



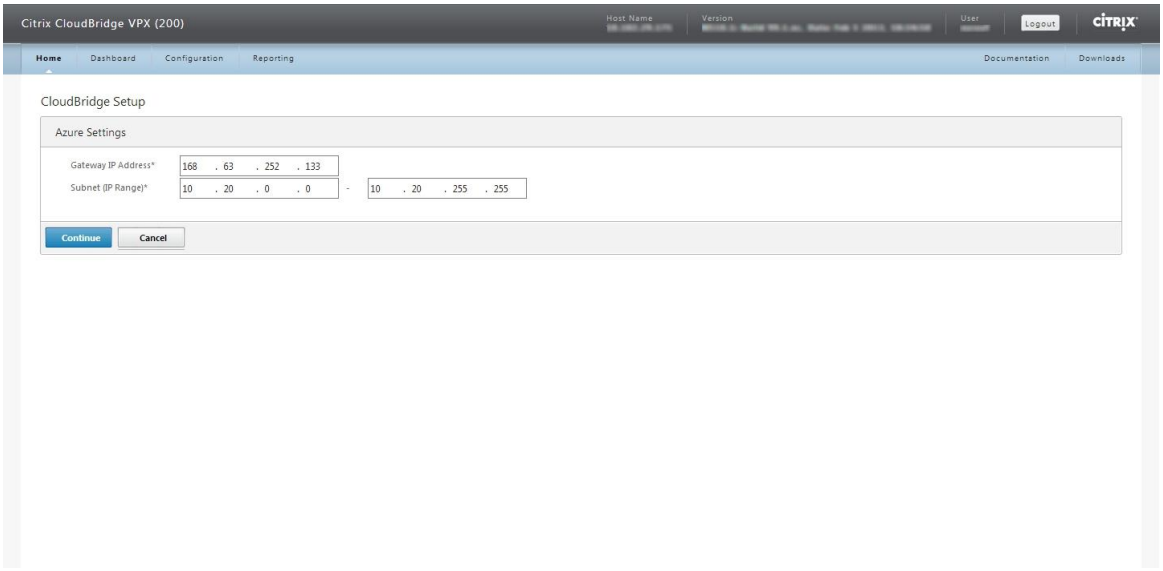
Note: If you already have any network bridge configured on the CloudBridge appliance, this screen does not appear, and you are taken to the **CloudBridge Setup** pane.

5. In the **CloudBridge Setup** pane, click **Microsoft Windows Azure**.

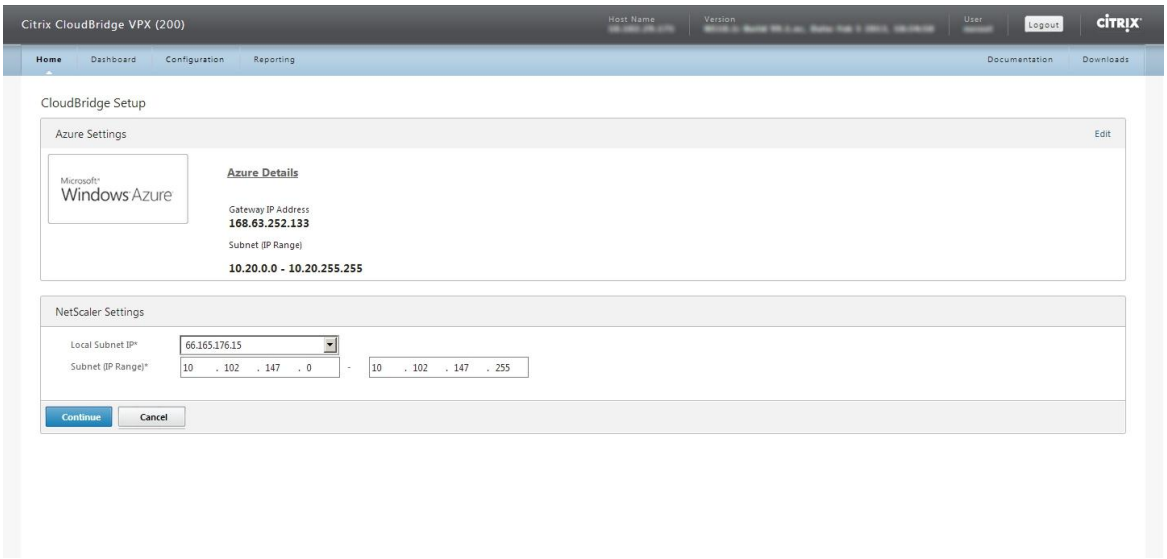


6. In the **Azure Settings** pane, in the **Gateway IP Address*** field**,** type the IP address of the Azure gateway**.** The CloudBridge tunnel is then set up between the CloudBridge appliance and the gateway. In the **Subnet (IP Range)*** text boxes, specify a subnet range (in Azure

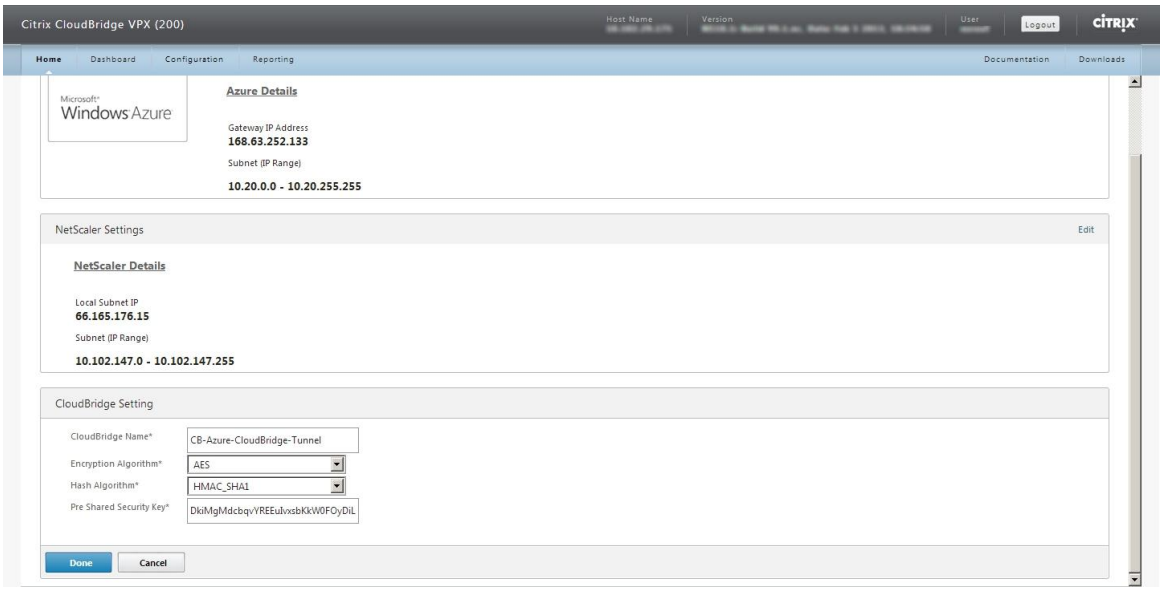
cloud), the traffic of which is to traverse the CloudBridge tunnel. Click **Continue**.



7. In the **NetScaler Settings** pane, from the **Local Subnet IP***drop-down list, select a publicly accessible SNIP address configured on the CloudBridge appliance. In **Subnet (IP Range)*** text boxes, specify a local subnet range, the traffic of which is to traverse the CloudBridge tunnel. Click **Continue**.



8. In the **CloudBridge Setting** pane, in the **CloudBridge Name** text box, type a name for the CloudBridge that you want to create.



9. From the **Encryption Algorithm** and **Hash Algorithm** drop-down lists, select the AES and HMAC_SHA1 algorithms, respectively. In the **Pre Shared Security Key** text box, type the security key.
10. Click **Done**.

Monitoring the CloudBridge Tunnel

You can view statistics for monitoring the performance of a CloudBridge tunnel between the CloudBridge appliance in the datacenter and Microsoft Azure. To view CloudBridge tunnel statistics on the CloudBridge appliance, use the CloudBridge command line. To view CloudBridge tunnel statistics in Microsoft Azure, use the Microsoft Windows Azure Management Portal.

Displaying CloudBridge Tunnel Statistics in the CloudBridge Appliance

The following table lists the statistical counters available for monitoring CloudBridge tunnels on a CloudBridge appliance.

Statistical counter	**Specifies**
Bytes Received	Total number of bytes received by the CloudBridge appliance through all the configured CloudBridge tunnels since the appliance was last started.

Bytes Sent	Total number of bytes sent by the CloudBridge appliance through all the configured CloudBridge tunnels since the appliance was last started.
Packets Received	Total number of packets received by the CloudBridge appliance through all the configured CloudBridge tunnels since the appliance was last started.
Packets Sent	Total number of packets sent by the CloudBridge appliance through all the configured CloudBridge tunnels since the appliance was last started.

All these counters are reset to 0 when the CloudBridge appliance is restarted. They do not increment during the following phases:

- Internet Key Exchange (IKE) authentication (pre-shared key) phase on any configured CloudBridge tunnel.
- IKE Security Association (SA) establishment phase on any configured CloudBridge tunnel.

To display CloudBridge tunnel statistics by using the CloudBridge command line

At the CloudBridge command prompt, type:

- **stat ipsec counters**

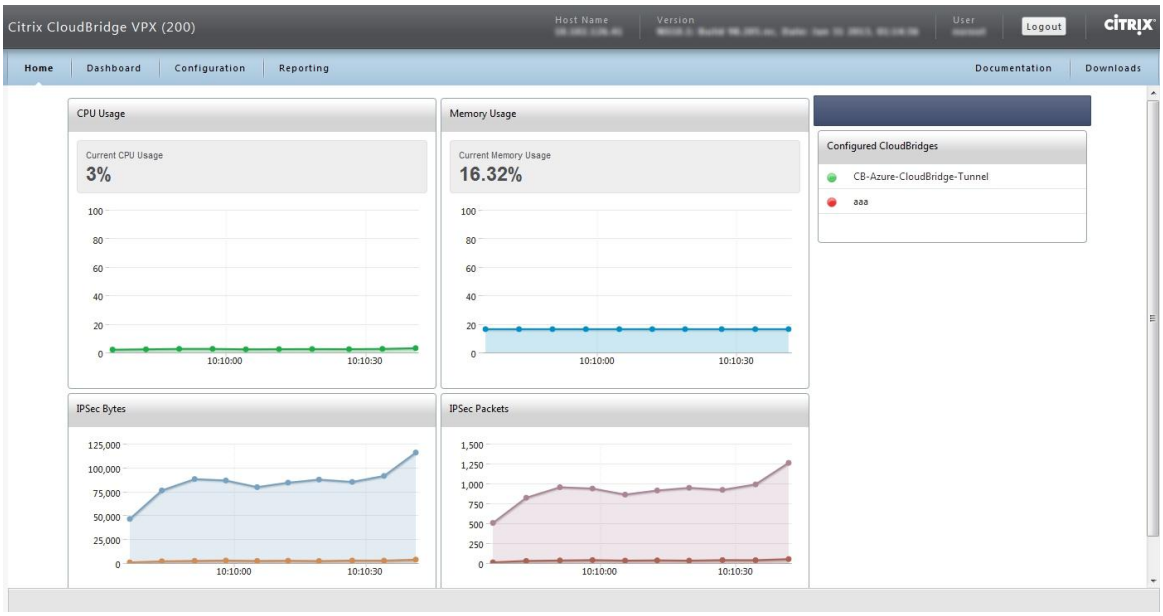
Example

```
> stat ipsec counters

Secure tunnel(s) summary

                    Rate (/s)       Total
Bytes Received      0               2811248
Bytes Sent          0               157460630
Packets Received    0               56787
Packets Sent        0               200910
Done
>
```

To display CloudBridge tunnel statistics by using the Configuration utility

1. Access the configuration utility by using a web browser to connect to the IP address of the CloudBridge appliance.

2. On the **Home** tab, the **IPSec Bytes** and **IPSec Packets** charts display the statistics of all the CloudBridge tunnels configured on the CloudBridge appliance.



Displaying CloudBridge Tunnel Statistics in Microsoft Azure

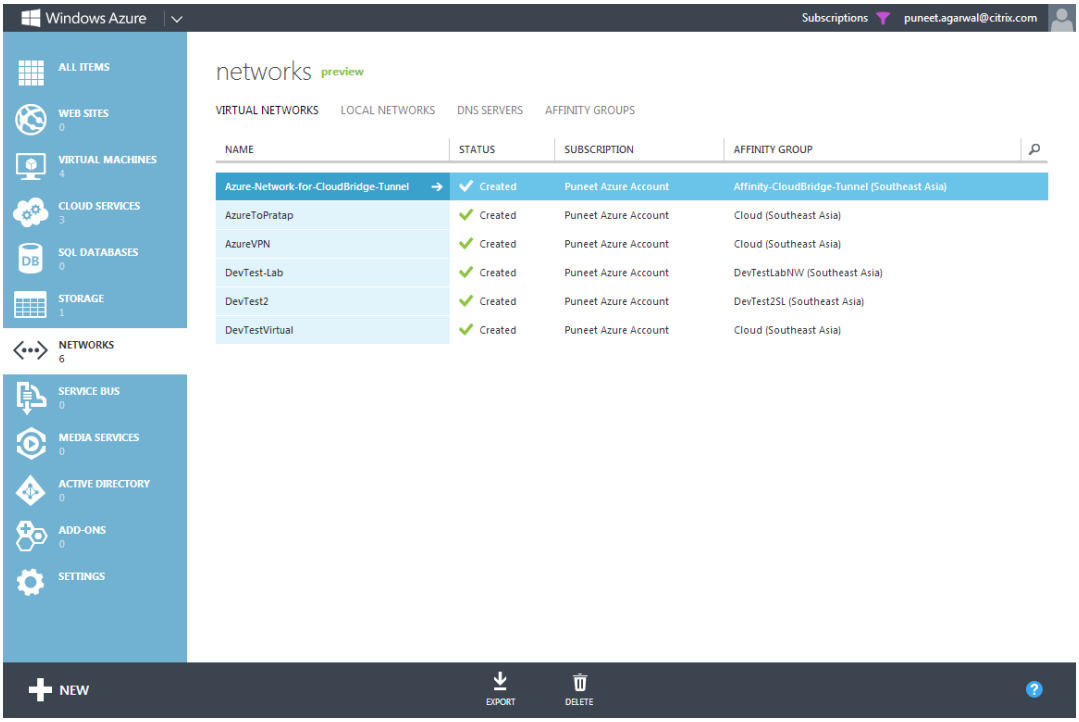
The following table lists the statistical counters available for monitoring CloudBridge tunnels in Microsoft Azure.

Statistical counter	Specifies
DATA IN	Total number of kilobytes received by the Azure gateway through the CloudBridge tunnel since the gateway was created.
DATA OUT	Total number of kilobytes sent by the Azure gateway through the CloudBridge tunnel since the gateway was created.

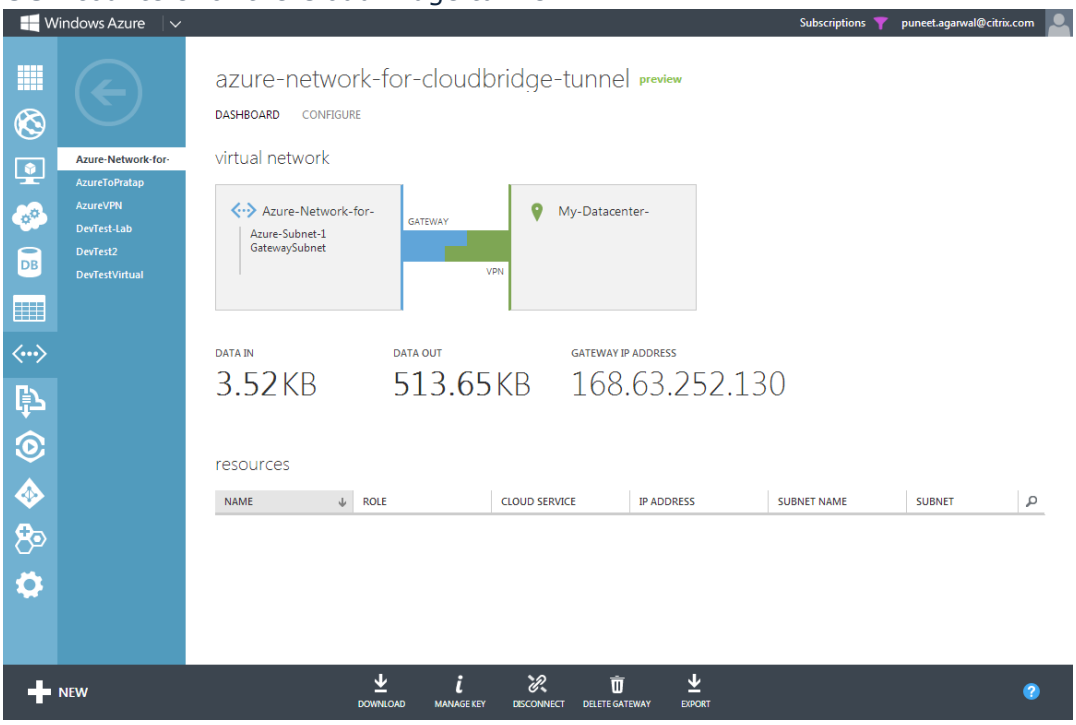
To display CloudBridge tunnel statistics by using the Microsoft Windows Azure Management Portal

1. Log on to the Windows Azure Management Portal (https://manage.windowsazure.com/) by using your Microsoft Azure account credentials.
2. In the left pane, click **NETWORKS**.

3. On the **Virtual Network** tab, in the **Name** column, select the virtual network entity associated with a CloudBridge tunnel whose statistics you want to display.



4. On the **DASHBOARD** page of the virtual network, view the **DATA IN** and **DATA OUT** counters for the CloudBridge tunnel.



Getting Service and Support

Citrix® offers a variety of resources for support with your Citrix environment, including the following:

- The Knowledge Center is a self-service, Web-based technical support database that contains thousands of technical solutions, including access to the latest hotfixes, service packs, and security bulletins.
- Technical Support Programs for both software support and appliance maintenance are available at a variety of support levels.
- The Subscription Advantage program is a one-year membership that gives you an easy way to stay current with the latest product version upgrades and enhancements.
- Citrix Education provides official training and certification programs on virtually all Citrix products and technologies.

For more information about Citrix services and support, see the Citrix Systems Support Web site at http://www.citrix.com/lang/English/support.asp.

You can also participate in and follow technical discussions offered by the experts on various Citrix products at the following sites:

- http://community.citrix.com
- http://twitter.com/citrixsupport
- http://forums.citrix.com/support