### Introduction to the Virtual Network Lab Scenario

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click on &quot;IaaS&quot; to advance to the Windows Azure Scenario</td>
<td>Windows Azure Infrastructure Services (IaaS) provides us with the capability to securely extend our On-premises Private Cloud network infrastructure to leverage the capabilities of Windows Azure Virtual Machines and Virtual Networks. This allows us to build a hybrid network infrastructure for our Private Cloud that combines the best of both worlds: the low-latency and high bandwidth networks available within our datacenter with the elastic, pay-as-you-go Windows Azure cloud platform.</td>
</tr>
<tr>
<td>2. Click to configure the &quot;CloudNet&quot; Virtual Network</td>
<td>In our lab scenario, we'll be connecting our existing On-premises network environment, with a local IP Address Space of 10.1.0.0/16 to a new Windows Azure Virtual Network, that we'll call &quot;CloudNet&quot; and use an IP Address Space of 10.2.0.0/16. Inside CloudNet, we can also build multiple subnets for placing different classes of VMs in different IP subnet ranges. Let's get started by creating &quot;CloudNet&quot; in the Windows Azure Management Portal.</td>
</tr>
</tbody>
</table>
## Create a Virtual Network

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click the &quot;NEW&quot; Button.</td>
<td>You can create a new Virtual Network from the &quot;Networks&quot; page in the Windows Azure Management portal.</td>
</tr>
<tr>
<td>2. Click &quot;Custom Create&quot;</td>
<td>When creating a new Virtual Network, there's two options: &quot;Quick Create&quot; and &quot;Custom Create&quot;. &quot;Quick Create&quot; can be used to quickly create an isolated Virtual Network in the Cloud. &quot;Custom Create&quot; can be used to create a new Virtual Network and securely connect it to your On-premises Datacenter via a Site-to-Site VPN tunnel for a Hybrid Cloud solution.</td>
</tr>
</tbody>
</table>
### Step-by-Step: Extend Your Network with Windows Azure Infrastructure Services

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Click to enter a Virtual Network Name.</td>
<td>Each Virtual Network you create needs a unique Name. The Virtual Network Name can be any name value, as long as it is unique within your Windows Azure subscription.</td>
</tr>
<tr>
<td>4.</td>
<td>Click to Pull Down &quot;Affinity Group&quot; List.</td>
<td>When defining a new Virtual Network, an &quot;Affinity Group&quot; allows us to bind the Virtual Network to a specific Windows Azure Datacenter Region. Once an Affinity Group is defined, any VMs that are placed on the Virtual Network are given the same &quot;Affinity&quot; relationship, which is used by Windows Azure to efficiently place VMs on the same Virtual Network to reduce physical network hops and reduce latency between VMs. This helps to improve network performance.</td>
</tr>
</tbody>
</table>

http://KeithMayer.com
5. Select "Create a new affinity group"

6. Click to pull down the Region list.
7. Select the "East US" Region.

8. Click to enter an "Affinity Group Name"

The "Affinity Group Name" is a unique name used to define the Affinity Group relationship. It can be any name value, as long as it is unique within your Windows Azure subscription.
9. Click the "Next" button.
### Configure DNS

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Click to enter the first &quot;DNS Server Name&quot;</strong></td>
<td>Next, we can define DNS Server properties for the new Virtual Network. The DNS Servers that we include in the properties of a Virtual Network are automatically assigned to VMs that are placed on this virtual network to be used for hostname resolution. This serves a similar function to including DNS Server options within a DHCP scope in an on-premises network. DNS Servers to which a Virtual Network is pointed can exist in Windows Azure VMs, can be on-premises DNS Servers, or can be public DNS Service Providers, depending on the needs of your application scenarios. In this lab, we'll assign two on-premises DNS Servers to be used by VMs on this new Virtual Network for hostname resolution.</td>
</tr>
</tbody>
</table>

http://KeithMayer.com
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Click to enter the IP Address of the first DNS Server.</td>
</tr>
<tr>
<td>3.</td>
<td>Click to enter a second DNS Server Name.</td>
</tr>
</tbody>
</table>
4. Click to enter the IP Address of the second DNS Server.
### Review the Lab Scenario

**Steps**

1. **Click to Configure Site-to-Site VPN Tunnel**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click to Configure Site-to-Site VPN Tunnel</td>
<td>So far, we've configure &quot;CloudNet&quot; as a Windows Azure Virtual Network with 2 DNS Servers. Our next steps are to configure the Site-to-Site VPN connection for this Virtual Network, define our IP Address Spaces for our On-premises Network and Virtual Network, and create a new Gateway Subnet for our virtual VPN Gateways that will terminate this Site-to-Site connection in the Windows Azure cloud. Let's go back to the Windows Azure Management Portal and step through creating this Site-to-Site VPN.</td>
</tr>
</tbody>
</table>
## Configure Site-to-Site VPN

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click to select the option for a Site-to-Site VPN.</td>
<td>Windows Azure Infrastructure Services includes both Point-to-Site and Site-to-Site VPN connectivity options. Point-to-Site VPNs permit client devices to securely connect to a Windows Azure Virtual Network. Site-to-Site VPNs permit our entire On-premises Network to be securely connected to a Windows Azure Virtual Network to form a Hybrid Cloud Network Fabric. Once the Site-to-Site VPN is established, the Windows Azure Virtual Network functions as a remote Datacenter network connected to our On-premises Wide Area Network (WAN). In this lab, we'll be defining a Site-to-Site VPN for our Windows Azure Virtual Network.</td>
</tr>
</tbody>
</table>
2. Click the "Next" button.

3. Click to enter a name for the Local On-premises Network.

On the "Site-to-Site Connectivity" Page, we'll need to define a Name for our local On-premises network. We'll also need to define the public IPv4 address for our On-premises VPN Gateway (or firewall with IPSec Site-to-Site VPN capabilities) and the internal IPv4 address space for the range of addresses present within our local On-premises network.
4. Click to enter the public IP Address for the On-premises VPN gateway device.

5. Click to enter a Starting IP Address for the Local On-premises IP Address Space.
### Step-by-Step: Extend Your Network with Windows Azure Infrastructure Services

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Click to enter a Starting IP Address for the Local On-premises IP Address Space.</td>
</tr>
<tr>
<td>7.</td>
<td>Click to pull-down the list of CIDR subnet mask values.</td>
</tr>
</tbody>
</table>
8. Click to scroll down.

9. Select "/16 (65536)"
### Step-by-Step: Extend Your Network with Windows Azure Infrastructure Services

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Click the &quot;Next&quot; button.</td>
</tr>
<tr>
<td>11.</td>
<td>Click the &quot;Add Gateway Subnet&quot; button.</td>
</tr>
</tbody>
</table>

---

Next, we'll need to define the internal IPv4 address space for our Windows Azure Virtual Network. This defines the range of IPv4 addresses that we wish to make available for assignment to VMs that are placed on this virtual network. Once an IP address is assigned to a VM, the VM retains this same IP address regardless of VM state. If a VM is deleted and recreated, it is possible that the VM will be assigned a new IPv4 address from this range.

Within a Virtual Network Address Space, we can also add multiple subnets which each provide a subset of IP addresses from the overall Address Space. This is useful for assigning...
different ranges of IP addresses to different types of VMs by placing VMs on the appropriate Virtual Subnet when they are provisioned.

In this lab, we'll accept the default Virtual Network Address Space configuration, as it matches the needs of our lab scenario.

When defining a Site-to-Site VPN, we'll also need to define a Gateway Subnet in our Windows Azure Virtual Network. The Gateway Subnet is a virtual subnet in Windows Azure where our virtual VPN Gateways will be provisioned for terminating our Site-to-Site VPN tunnel in the Windows Azure cloud.

12. Click the "Complete" button.
### Provision the Virtual VPN Gateway

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. Click on the name of the new virtual network. | The new Virtual Network configuration has been defined. Next, we'll need to provision the VPN gateways on each side of the Site-to-Site VPN connection to bring up the tunnel between the new Windows Azure Virtual Network and the On-premises Network.  
First, let's provision the virtual VPN Gateway on the Windows Azure side of the Site-to-Site tunnel. |
| 2. Click the "Dashboard" tab. | }

http://KeithMayer.com
3. Click the "Create Gateway" button.

4. Click "Dynamic Routing"

When creating a virtual VPN Gateway in Windows Azure, you can select "Static Routing" or "Dynamic Routing" depending on the requirements and capabilities of your On-premises VPN Gateway and network configuration.

In this lab, we'll be using a "Dynamic Routing" configuration.
5. Click the "Yes" button.
### Review the Lab Scenario

**Steps**

1. **Click to configure On-premises VPN Gateway**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>We've finished configuring our Virtual Network in Windows Azure, now we'll need to configure our On-premises Site-to-Site VPN Gateway. Our On-premises VPN Gateway has a few requirements: it needs to support IPsec Site-to-Site common security standards and it also needs to have a routable IPv4 public IP Address assigned to the external network interface of this gateway. The gateway cannot be located behind a NAT firewall.</td>
</tr>
</tbody>
</table>

In our lab, we'll be using a Windows Server 2012 server as our On-premises VPN Gateway device.

---

[Image: Windows Azure Virtual Networks Hybrid Cloud Network Fabric]

IP Address Space: 10.1.0.0/16

IP Address Space: 10.2.0.0/16
### Configure the On-Premises VPN Gateway

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click the &quot;Download VPN Device Script&quot; link.</td>
<td>To simplify the configuration of an On-premises VPN Gateway, the Windows Azure Management Portal provides a downloadable VPN Device Configuration Script that can be used as a template for configuring the On-premises Gateway.</td>
</tr>
<tr>
<td>2. Click to pull-down the Vendor list.</td>
<td>Select the vendor, platform and operating system for the On-premises VPN Gateway that is being used to download an appropriate configuration script template.</td>
</tr>
</tbody>
</table>
3. Click to select "Microsoft Corporation".

4. Click the "Complete" button.
5. Click the "Open" button.

6. Click "Try an app on this PC"
7. Select "Notepad".

8. Click to maximize the Notepad window.
9. Click on the scrollbar to scroll down. The On-premises VPN Device Script includes generic placeholders that we'll need to replace with the specific configuration information for our Windows Azure Site-to-Site VPN and Virtual Network.

In the next few steps, we'll replace these placeholders with the public IPv4 Address of our Windows Azure virtual VPN Gateway, the IPv4 Address Space for our Windows Azure Virtual Network, and the Pre-shared Key used to authenticate our Site-to-Site VPN Tunnel connection.

10. Click to select the <SP_AzureGatewayIpAddress> text. First, we'll find all occurrences of the placeholder tag representing the public IPv4 Address of the virtual VPN Gateway and replace each occurrence with the actual public IPv4 Address.
11. Click to copy this text to your clipboard.

12. Click the "Edit" menu.
13. Select "Replace..."

14. Click in the "Find what:" field.
Step-by-Step: Extend Your Network with Windows Azure Infrastructure Services

| Step 15 | Select "Paste"
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 16</td>
<td>Click &quot;Internet Explorer&quot; to switch back to the Windows Azure Management Portal.</td>
</tr>
</tbody>
</table>
17. Click to select the Windows Azure VPN Gateway public IP Address. Back in the Windows Azure Management Portal, we can copy the public IPv4 Address assigned to the virtual VPN Gateway to our clipboard so that we can easily paste this value into the VPN Device Configuration Script.

18. Select "Copy"
19. Click "Notepad" to switch back to the VPN Config Script.

20. Click in the "Replace with:" field.
21. Select "Paste".

22. Click the "Replace All" button.
23. Click the "Cancel" button.

24. Click to enter the Windows Azure Virtual Network Address Space range.

Next, we'll replace the placeholder text for the IPv4 Address Space of the Windows Azure Virtual Network with the actual IPv4 Address Space configured for the Virtual Network in this lab.
25. Click to enter the network routing metric. The Azure Network Metric allows the assignment of a particular routing metric, or weight, to this Site-to-Site VPN. Common values range from 1 to 10, but should conform to the routing metrics used within your On-premises Wide Area Network (WAN) for consistency.

26. Click to select the &lt;SP_PresharedKey&gt; text. Finally, we'll need to replace the placeholder text for the Pre-shared Key used to authenticate the Site-to-Site VPN tunnel with the actual Pre-shared Key value configured for the Windows Azure Virtual Network VPN Gateways.
27. Select "Copy"

28. Click on the "Edit" menu.
29. Select "Replace..."

30. Click in the "Find what:" field.

http://KeithMayer.com
Step-by-Step: Extend Your Network with Windows Azure Infrastructure Services

31. Click "Paste".

32. Click on "Internet Explorer" to return to the Windows Azure Management Portal.

http://KeithMayer.com
33. Click on the "Manage Key" button. Back in the Windows Azure Management Portal, we can click the "Manage Key" button to copy the Pre-shared Key used to authenticate the Site-to-Site VPN Tunnel to our clipboard for easy pasting into the VPN Device Configuration Script.

34. Click on the "Clipboard" button to copy the shared key to your clipboard.
35. Click on the "Complete" button.

36. Click on "Notepad" to return to the On-premises VPN Gateway Config Script.
37. Click in the "Replace with:" field.

38. Click "Paste"
39. Click the "Replace All" button.

40. Click the "Cancel" button.
41. Click on the "File" menu. We've completed the changes needed in the VPN Device Configuration Script for the On-premises VPN Gateway device.

Let's save this script as a new PowerShell script in a location that is accessible from the VPN Gateway device.

In this lab, we'll be using a Windows Server 2012 server as the On-premises VPN Gateway device.

42. Select "Save As..."
43. Click to enter a script filename.

44. Click the "Save" button.
45. Click the "Close" button.
<table>
<thead>
<tr>
<th>Provision the On-Premises VPN Device and Connect</th>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td>1. Click to select the Set-ExecutionPolicy cmdlet line in the script pane.</td>
<td>We've now switched to the server console of the Windows Server 2012 server that we'll be using as the On-premises VPN Gateway device in this lab. Prior to running the VPN Device Configuration Script, we'll need to ensure that PowerShell is configured to be able to run scripts locally that do not have a code-signing signature. We'll perform this task by setting the PowerShell Script Execution Policy to &quot;RemoteSigned&quot;.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Image" /></td>
<td>2. Click to run the Set-ExecutionPolicy PowerShell cmdlet.</td>
<td></td>
</tr>
</tbody>
</table>
3. Click the "Yes" button.

4. Click to switch tabs to the VPN Device Config Script. Now that we've configured PowerShell to be able to run local scripts that are not signed, we can switch to the VPN Device Configuration script and run it to configure Windows Server 2012 as a Site-to-Site VPN Gateway device in this lab.

When run, the script will install the Routing and Remote Access role services on Windows Server 2012 and configure the server with the necessary IPSec Tunnel information to allow the Tunnel to be connected and route network traffic.
5. Click the "Run" button to run the VPN Device Config Script.

6. Click the "Minimize" button.
Step-by-Step: Extend Your Network with Windows Azure Infrastructure Services

7. Click the "Connect" button.

Now that our configuration in both Windows Azure and our On-premises network is complete, we can connect both sides of the Site-to-Site Tunnel in the Windows Azure Management Portal.

8. Click the "Close" button to end this Guided Lab.

Congratulations! You've completed the configuration of a Windows Azure Virtual Network and Site-to-Site VPN Tunnel as a Hybrid Cloud Network Fabric.

Get Started with Windows Azure Virtual Networks today!
- Sign-up for a FREE 90-Day Windows Azure Trial at [http://aka.ms/AzureVMFreeTrial](http://aka.ms/AzureVMFreeTrial)