This document presents the essentials of Azure virtual network by stepping through a process, screen by screen, of creating and configuring an Azure virtual network with gateways to establish a site-to-site and point-to-site connectivity. The local approach, a conceptual model and implementation steps are as the following:

1. First plan vnet your deployment
   - IP address space
   - Subnet scheme
   - S2S and P2S
   - DNS and gateway
   - PKI and cert distribution and management

2. Create vnet accordingly

3. Import certificate

4. Generate gateway

5. Distribute VPN device and client apps and test the connectivity
Sample Hybrid Cloud with Azure Vnet

- **On-premises**: 192.168.x.x/16
- **Site-to-Site VPN**: 5.5.5.5
- **Point-to-Site VPN**: 172.16.0.x/24
- **Windows Server 2012 R2** as a VPN gateway

**Microsoft Azure Virtual Network Site**

- **Collab-Tier**: 10.2.3.0/24
  - SharePoint
- **Data-Tier**: 10.2.2.0/24
  - SQL
- **Backend**: 10.2.1.0/24
  - dc1/dns 10.2.1.4/24
  - dc2/dns 10.2.1.5/24

**Microsoft Azure Virtual Network (fooNet) - 10.2.x**

- **Load-Balancer**: fe3 10.2.4.0/24
- **Frontend**: fe2 10.2.4.0/24
- **Availability Set**
  - fe3
  - fe2
  - fe1

© 2015 Yung Chou.
Logical Steps to Establish Azure Vnet

1. First plan your vnet deployment including:
   - IP address space
   - Subnet scheme
   - S2S and P2S
   - DNS and gateway
   - PKI and cert distribution and management

2. Create vnet accordingly

3. Import certificate

4. Generate gateway

5. Distribute VPN device and client apps and test the connectivity
Register DNS References

- Register your DNS for vnet to reference, as applicable.
• For redundancy, plan and register multiple DNS references.
- Verify registered DNS entries are in place.
Creating and Configuring Azure Vnet

• Start creating your Azure virtual network by clicking +NEW button on the lower left corner, then NETWORK SERVICES, and so on as shown.
• Specify a region where the vnet is to be deployed. The dropdown list displays all Azure locations available.
• Specify the DNS references for this vnet.

• Notice that without specifying a DNS reference, Azure will perform the name resolution automatically. With a DNS reference in place, the name resolution becomes the responsibility of those VMs deployed to the vnet.
• As applicable, include site-to-site/point-to-site configurations.
• Allocate a designated address space, 172.16.0.0./24, for devices with point-to-site connectivity.

<table>
<thead>
<tr>
<th>ADDRESS SPACE</th>
<th>STARTING IP</th>
<th>CIDR (ADDRESS COUNT)</th>
<th>USABLE ADDRESS RANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.0/24</td>
<td>172.16.0.0</td>
<td>/24 (256)</td>
<td>172.16.0.1 - 172.16.0.254</td>
</tr>
</tbody>
</table>

![Point-to-Site Connectivity Diagram](image-url)
• For site-to-site connectivity, reference the public IP of a designated on-premises VPN gateway device and allocate an address space for devices to be connected from a remote site behind the on-premises VPN gateway device.
• Allocate an address space, here 10.2.0.0/20, for the vnet and configure subnet IP schemes.
• Either site-to-site or point-to-site connectivity requires a subnet for Azure to deploy gateway instances on a subscriber’s behalf on the Azure side.

• Azure automatically generates a gateway subnet with CIDR /29 triggered by a user’s clicking the “add gateway subnet” button to signify the completion of a subnet configuration.
• The vent is now successfully created. Click the vnet name to view the details. And as needed, click DASHBOARD to view the created vnet instance.
• On the DASHBOARD page, a gateway in red indicates the gateway is not yet functional.

• Notice at the bottom black menu bar, there is a “CREATE GATEWAY” button indicating a gateway generation process has not yet been successfully carried out, which is necessary for a gateway to become functional.

• A gateway generation process references an x.509 certificate which is listed in CERTIFICATES page.

• Before kicking off the process to generate a gateway, we first need to ensure and import, as applicable, an x.509 certificate is in place for establishing secure connections to the gateway instance(s) Azure is to deploy for the vnet.
- Clicking on CONFIGURE page, there are configurations details of this vnet.
- Scroll down for additional settings.
### Site-to-Site Connectivity

**Connection**
- [ ] Connect to the local network
- [ ] Use ExpressRoute

**Local Network**
- [ ] 10.0.0.0/16

### Virtual Network Address Spaces

<table>
<thead>
<tr>
<th>Address Space</th>
<th>Starting IP</th>
<th>CIDR (Address Count)</th>
<th>Usable Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.0.0/16</td>
<td>10.2.0.0</td>
<td>/20 (65536)</td>
<td>10.2.0.0 - 10.2.1.254</td>
</tr>
</tbody>
</table>

**Subnets**
- backend: 10.2.1.0 /24 (256) 10.2.1.0 - 10.2.1.254
- data: 10.2.2.0 /24 (256) 10.2.2.0 - 10.2.2.254
- callab: 10.2.3.0 /24 (256) 10.2.3.0 - 10.2.3.254
- frontend: 10.2.4.0 /24 (256) 10.2.4.0 - 10.2.4.254
- Gateway: 10.2.0.0 /16 (65536) 10.2.0.0 - 10.2.0.6

- [ ] add subnet
- [ ] add gateway subnet

- [ ] add address space
Creating Self-Signed Certificate Pair

• Here, the example uses makevcert.exe to generate a pair of self-signed certificates in .cer and .pfx formats.

• Both of the certificates are placed in the my, i.e. personal, certificate store.

• There are other ways to generate self-signed certificates including with IIS administration console, using Visual Studio, etc. Here makecert.exe is a tool for generate a certificate. Additional information is available at https://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.110).aspx.
• Open MMC and add a Certificates snap-in to operate on the generated certificates.
Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

<table>
<thead>
<tr>
<th>Snap-in</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Domain Services</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Active Directory Sites Services</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Active Directory Users and Computers</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>ActiveX Control</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>ADSI Edit</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Authorization Manager</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Certificates</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Component Services</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Computer Management</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Device Manager</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Disk Management</td>
<td>Microsoft and...</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Folder</td>
<td>Microsoft Cor...</td>
</tr>
<tr>
<td>Group Policy Object</td>
<td>Microsoft Cor...</td>
</tr>
</tbody>
</table>

Selected snap-ins:

- Console Root

Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

OK Cancel
• The generated certificates are in the user’s personal certificate store.
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:
- Active Directory Domain Services
- Active Directory Sites and Services
- Active Directory Users and Computers
- ActiveX Control
- ADST Edit
- Authorization Manager
- Certificates
- Component Services
- Computer Management
- Device Manager
- Disk Management
- Event Viewer
- Folder
- Group Policy Object

Selected snap-ins:
- Console Root
  - Certificates - Current User

Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
Here are the two generated and placed in the personal certificate store. The root cert is the public key, while pfx has the private key.
Export Pfx Certificate for VPN Clients

• Export the paired pfx certificate for distribution.
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.
• Export with the private key.
Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:
- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
  - Include all certificates in the certification path if possible
  - Delete the private key if the export is successful
  - Export all extended properties
- Microsoft Serialized Certificate Store (.SST)

Next  Cancel
• Secure the usage of the pfx certificate with a password.
• Save it in pfx format.
• Complete the export.
Exporting Root Certificate for Azure Vnet

• Also export the public key certificate for Azure to generate gateway a instance.
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.
• Do not include the private key in the root (i.e. x.509) certificate.
- Pick a preferred format.
• Save it as .cer format.
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

- **File Name**: C:\cert\fooNet.cer
- **Export Keys**: No
- **Include all certificates in the certification path**: No
- **File Format**: DER, Encoded Binary X.509 (*.cer)

The export was successful.
These two are ready for distribution. In this demo, the root cert is for generating Azure vnet gateways, while the pfx is for P2S VPN clients.
Upload Root Certificate to Azure Vnet

• To upload a certificate for a vnet, first click the vnet instance to display the details.
• And import a certificate from the CERTIFICATES page of the vnet.
• The uploaded certificate is the one with the public key of the paired certificates, namely the one in .cer format.
• The CERFITICATES page now shown a certificate in place.
Create Azure Vnet Gateway

- Now the vent is ready for generating gateway instances.
• Click CREATE GATEWAY to lick off the process.
• Generating gateway instances takes about 20 minutes, if not more.
Upon completing a gateway generation process, a gateway in yellow indicates its readiness at this time. A gateway in red means the gateway is not yet operational.

The read gateway here is for our site-to-site connectivity. It is not operational, due to a bogus public IP specified at the configuration time. If a valid public IP has been provided for the site-to-site gateway, it should be in yellow upon a successful gateway generation process.

Also notice successfully completing a gateway generation process also makes the configuration scripts for on-premises VPN gateway devices and VPN clients available for download.

Notice once a gateway is generated, it must be first removed before the vent can be deleted.
Download VPN Gateway Device Script

- Download the configuration script for an on-premises VPN gateway device.
• A VPN gateway device configuration script is vendor specific....
• and platform specific.
• Here the dropdown shows specific platforms supported for a Cisco's VPN gateway device.
- Here the dropdown shows specific platforms supported for a Juniper’s VPN gateway device.
• Note that Windows Server 2012 and later can run as a VPN gateway device with the RRAS server role.

• Once a script of a VPN gateway device is properly set with vendor information and downloaded, configure the device by running the scripts locally.
Download Azure VPN Client Packages

- For point-to-site connectivity, download an intended version of the configuration script of a VPN client.
As applicable, save the script for later distribution. Here, this demo employs the local machine as a VPN client and hence runs it locally.
The publisher of f6ff5a1d-9a33-4af0-bbda-8f60cbcc2603.exe couldn't be verified. Are you sure you want to run the program?

Learn more

Run
View downloads
Install Pfx Certificate for VPN Client

• The VPN client is successfully and locally installed.
• An Azure VPN client is placed at Network Connections applet and appears as an available network connection and disconnected.
Install Pfx Certificate for VPN Client

• Before a VPN client can connect, first acquire and install the pfx certificate which is paired with the certificate already imported into the target Azure vnet earlier.
• Here the certificate is installed on the current user’s, i.e. the personal, certificate store.
File to Import
Specify the file you want to import.

File name:
C:\Users\Administrator\Desktop\fooNet.pfx

Note: More than one certificate can be stored in a single file in the following formats:
- Personal Information Exchange - PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)
• The password was specified at the certificate export time earlier.
Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

Certificate store: Browse...
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

- Certificate Store Selected
- Content: PFX
- File Name: C:\Users\Administrator\Desktop\fooNet.pfx

The import was successful.
Connect via Point-to-Site VPN

- Prior to connecting to the Azure vnet, what the ipconfig returns

```plaintext
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\windows\system32>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection\ 11:
    Media State : Media disconnected
    Connection-specific DNS Suffix : Media disconnected

Wireless LAN adapter Wi-Fi:
    Media State : Media disconnected
    Connection-specific DNS Suffix : home

Ethernet adapter Ethernet:
    Connection-specific DNS Suffix : home
    Link-local IPv6 Address : fe80::bc86:c78a:b4cd:2c73x12
    IPv4 Address : 192.168.19.181
    Subnet Mask : 255.255.255.0
    Default Gateway : 192.168.19.69

Tunnel adapter isatap.home:
    Media State : Media disconnected
    Connection-specific DNS Suffix : home

Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Connection-specific DNS Suffix : 2001:0:9d38:99d7:3861:20f1:3f57:ec65
    IPv6 Address : 2001:0:9d38:99d7:3861:20f1:3f57:ec65
    Link-local IPv6 Address : fe80::3861:20f1:3f57:ec65
    Default Gateway : 

C:\windows\system32>
```
• Connect to the Azure vnet, foonet, with the installed VPN client.
• The local device has successfully connected to fooNet at this time.
Examine the connection details. The IP address, 172.16.0.3, is indeed from the address space specified for point-to-site subnet at the configuration time.
And ipconfig now shows the connection with fooNet.
• In Azure vnet DASHBOARD, there is one client connected at this time.
Export Vnet Configuration

- To backup a vnet configuration, click the EXPORT button while highlighting the vnet entry,
Must validate the subscription before exporting.
• An Azure vnet configuration is exported as an xml file, named as NetworkConfig.xml by default.
• Rename the file, as appropriate.
• This is the content of the NetworkConfig.xml file.

• To create/modify a vnet configuration offline, use a networkconfig.xml file like this as a template. Make and finalize changes before uploading the NetworkConfig.xml into Azure of a target subscription.

• For example, the following PowerShell statement updates the network configuration of the current Azure subscription to that in the local file, c:\temp\MyAzNets.netcfg.

  Set-AzureVNetConfig
  -ConfigurationPath "c:\temp\MyAzNets.netcfg"

• As of February of 2015, there is one and only one NetworkConfig.xml in an Azure subscription. And a successful uploading of a NetworkConfig.xml will override existing settings.
Microsoft Azure Important Information

• Compliance page
  • http://aka.ms/AzureCompliance
• Pricing model
  • http://aka.ms/AzurePricing
• What-If Calculator
  • http://aka.ms/Calculator
• Subscription and Service Limits, Quotas, and Constraints
  • http://aka.ms/Limits
• SLAs
  • http://aka.ms/AzureSLAs
Additional contents

http://yungchou.wordpress.com/rss
http://aka.ms/recommended
http://aka.ms/TR
http://aka.ms/532