BCCS355 Cloud Services

AWS Advanced Networking – Part A

INTRODUCTION

Many corporate customers have existing physical infrastructure located in local server rooms. However today, when there is a need to expand or enhance resilience, Cloud Services become a very attractive option.

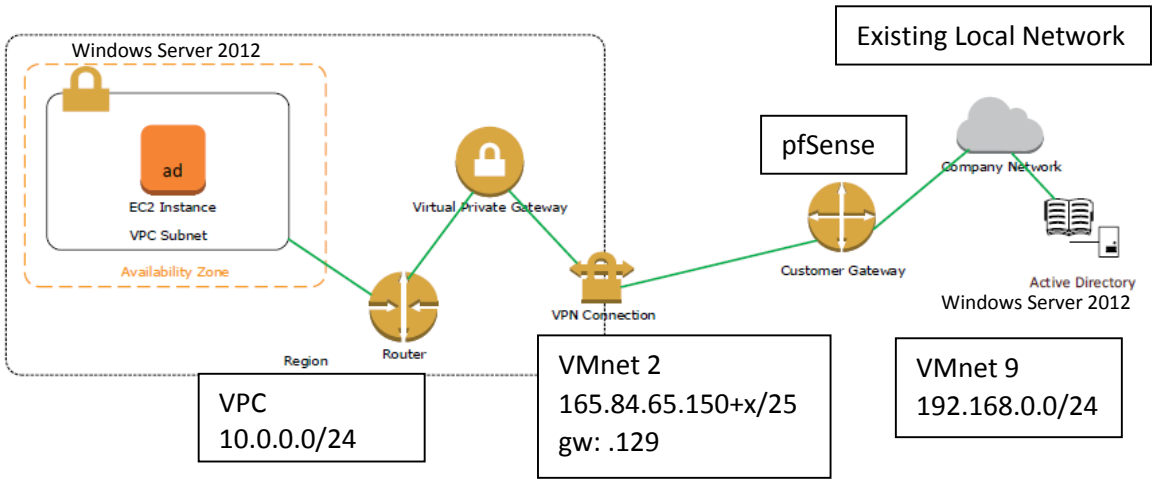
In the expanded infrastructure the corporate needs **a secure way** for the local physical infrastructure to interact with the new cloud infrastructure. Encrypted Virtual Private Networks provide a secure tunnel between these two.

OBJECTIVE

To set up a secure Virtual Private Network between local physical infrastructure (hosted in the classroom on VMWare) and new infrastructure in AWS.

TASK DESCRIPTION

In this exercise you will create a new AWS isolated subnet that will only allow access from an existing (physical) local network.
You will need to configure your own local network on VMware Workstation. Use a Windows Server 2012 VM, then install AD role and promote as DC (use 192.168.0.0/24).
You will create a Windows Server 2012 host on the isolated AWS VPC subnet and replicate a domain (CORPIT.LAN).
For easy IPSec configuration (used in the creation of the site-to-site VPN), set up a FreeBSD VM with pfSense firewall appliance installed. This will use VMNet9 for your local private network and VMNet2 to connect to the internet. The external network is 165.84.65.150+x/25 with the gateway of 165.84.65.129.



1. Use VMWare to Emulate Existing Infrastructure

The functioning local system will have AD installed and be able to browse to websites.

1.1. Set up a Windows Server 2012 clone as an AD Domain Controller of CORPIT.LAN on VMnet 9. The local network will be 192.168.0.0/24

1.2. Set up an empty machine VM (64bit FreeBSD option).

1.3. Alter this VM's settings so it has access to two networks VMnet 9 and VMnet 2.

1.4. Find and download the .iso image of pfSense LiveCD. Set your new VM to boot this .iso, then choose to install pfSense to the VM's local hard drive. Reboot to the installed pfSense.

1.5. Use the text based menu to set VMnet 9 as LAN and VMnet 2 as WAN, then set appropriate IP addresses on these interfaces, including .129 gateway address for WAN. After this you may restart into the Webconfigurator mode.
Future configuration will be done from your local 2012 Server's browser. You may need to disable** Internet Explorer Enhanced Security Configuration (IE ESC) to allow browsing to pfSense.
*** Only disable for the administrator.*

1.6. Ensure the local Windows Server can also browse to Internet sites before proceeding.

2. Configure the isolated subnet in AWS.

2.1. Create a new AWS VPC to ensure complete isolation – no Internet gateway is connected.

2.2. Create a subnet inside the VPC.

2.3. In this subnet add a Windows 2012 Server with no public IP address.

3. Create the AWS Virtual Private Network. This entails creating:

3.1. A Customer Gateway definition, referring to the address you gave your pfSense WAN (165.84.65.150+x)

3.2. A Virtual Private Gateway connected to your isolated VPC.

3.3. A VPN Connection, which connects together your Virtual Private Gateway and the Customer Gateway.

Any successful IPsec VPN connection relies on matching IPsec and ISAKMP (IKE) settings on both peers (endpoints) of the VPN. Therefore it is important that we gather the settings AWS is using by default before proceeding.

3.4. On the AWS VPN Connections page, select your connection definition and use Download Configuration.

4. Configure IPsec on your local pfSense Gateway.

4.1. A useful configuration link is http://www.heitorlessa.com/site-to-site-vpn-pfsense-and-amazon-vpc/.

4.2. Make sure you configure pfSense to also allow UDP traffic on the IPSec interface.

4.3. Once you have your VPN up you can login to your AWS Windows Server.
To get this access, download the Remote Desktop File from AWS and decrypt the admin password in the usual way.
DO NOT assign your AWS Server a public IP – you can access it another way. How?

4.4. Join the AWS Windows Server to the existing infrastructure domain, and then promote it as an additional domain controller.
DNS services may be replicated too if desired.

4.5. Can this Windows Server located in AWS browse to Internet sites?
Why or why not?
If it can't – what settings need to be changed to allow it to?

The decision of whether this cloud based server should be able to access the Internet will usually be based on a corporate policy decision.

Warning: The VPN connection costs money ($0.05 per hour) even if you are not using it so clean up when you have finished the lab. Deleting just the VPN connection is all that is required. Recreating the VPN later is ok, but the preshared key will change with the new VPN connection, so you will need to update the configuration.