IPsec Tunneling for Azure

Reference Architecture

VERSION: 1.0

UPDATED: Feb 2016

Copyright Notices

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

Table of Contents

1 Introduction

Microsoft's Azure cloud is attractive to the growing number of companies who wish to expand or migrate their existing on-premises infrastructure to use easily configurable, on-demand resources. This is especially true where Microsoft infrastructure is extensively deployed in-house as the services offered by Microsoft in Azure will be very familiar.

Azure presents a rich environment and offers a variety of Microsoft software and services. There are also thousands of third party applications and a wide selection of open source tools and operating environments. As such, Azure allows for quick and inexpensive configuration, test and deployment of existing and new applications.

However, when considering extending on-premises resources into the cloud, or adding new cloud based services, it is important, if not critical, to ensure that security is not compromised.

1.1 Document Purpose

This document describes how to set up a secure tunnel between an on-premises LoadMaster and the Azure Cloud.

1.2 Intended Audience

This document applies to:

- Cloud and Network Architects
- System and Security Administrators
- Developers requiring secure access to Cloud based resources

.

2 LoadMaster and IPsec Tunneling

KEMP’s LoadMaster can be configured as the endpoint of a site to site VPN tunnel. This, coupled with its many additional features, make it a simple to manage, cost effective solution compared to the overhead of purchasing and configuring additional systems or software for this purpose.

Once established, the tunnel provides seamless connection to the Azure Cloud, where the on-premises system can control access to remote services and connect to various resources in the cloud. One such application might be to extend load balancing to additional real servers running in the cloud as a way of adding additional capacity at times of peak demand, or perhaps as part of a strategy to migrate applications to the cloud with no disruption to the business.

There are also advantages in being able to connect to the many PaaS offerings in the Azure cloud, as though they were on-premises, as a way to avoid the overhead of maintaining the equivalent infrastructure in-house. Since these services are used on-demand, this can be more effective than consuming data center footprint to operate those services, and the capital expenditure and IT overhead that entails.

2.1 Setting Up an IPsec Tunnel

The following section describes how to set up a LoadMaster as the on-premises end point for a secure tunnel as shown in Figure 1.

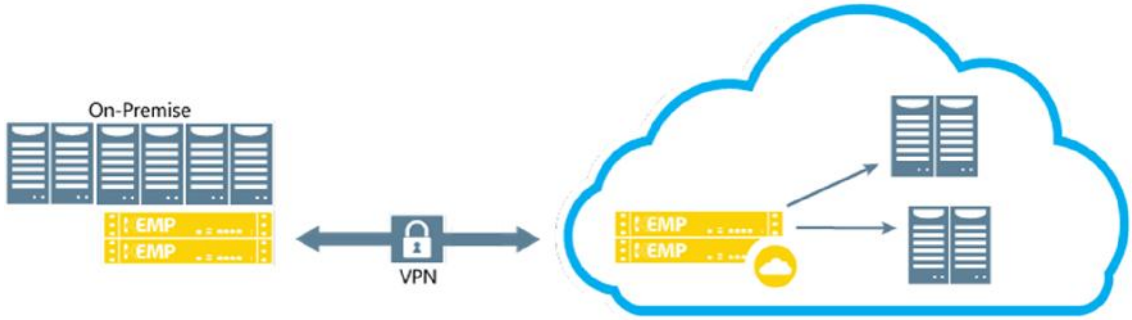
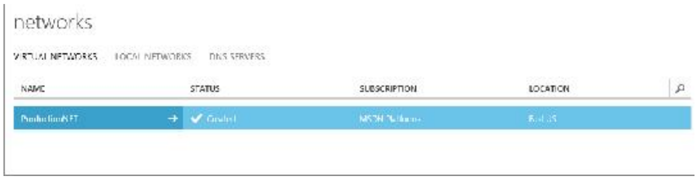


Fig. 1

Additional resources are accessible via the tunnel allowing for use of IaaS resources in the cloud as well as access to – or creation of – additional cloud based services. Note that a high availability pair of LoadMasters is recommended in such a configuration.

2.2 Implementation

This example assumes that an application, such as Microsoft SharePoint, has been deployed in the Azure cloud, and must be securely connected to the on-premises network.

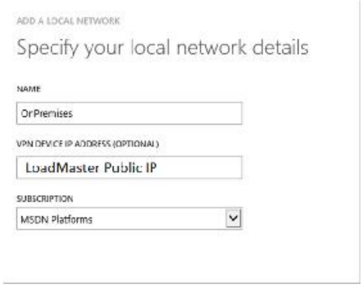


networks

NAME	STATUS	SUBSCRIPTION	LOCATION
ProductionNET	✓ Created	MSDN Platforms	East US

Fig. 2

Figure 2 shows an Azure Virtual Network previously set up to support a SharePoint environment.



ADD A LOCAL NETWORK

Specify your local network details

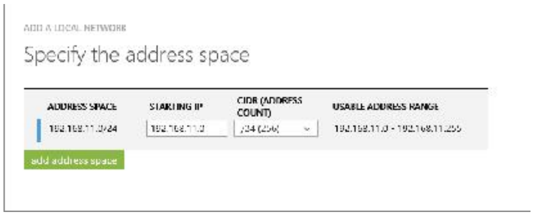
NAME: OnPremises

VPN DEVICE IP ADDRESS (OPTIONAL): LoadMaster Public IP

SUBSCRIPTION: MSDN Platforms

Fig. 3

Next, create a local network. Note that a public IP address is required for the “VPN Device” which in this case is the on-premises LoadMaster which, incidentally could be a physical appliance or a virtual instance, running in Hyper-V for example.



ADD A LOCAL NETWORK

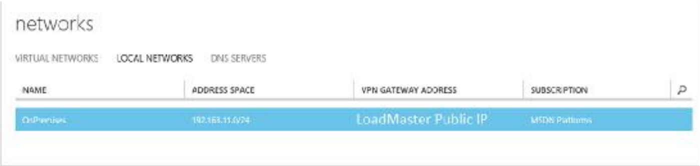
Specify the address space

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.11.0/24	192.168.11.0	/24 (256)	192.168.11.0 - 192.168.11.255

Fig. 4

Specify the on premises network

.



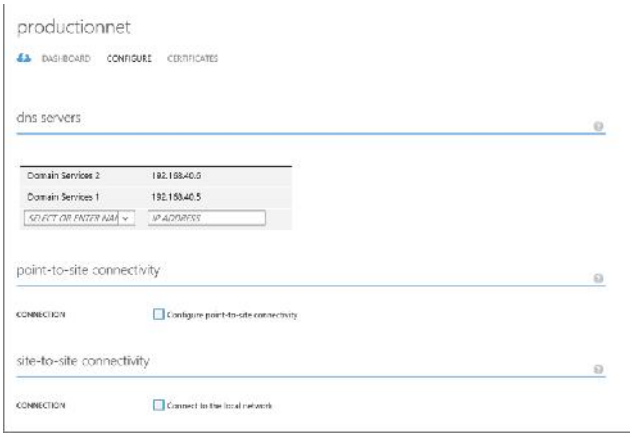
networks

VIRTUAL NETWORKS | LOCAL NETWORKS | DNS SERVERS

NAME	ADDRESS SPACE	VPN GATEWAY ADDRESS	SUBSCRIPTION
OnPremises	192.168.11.0/24	LoadMaster Public IP	MSDN Platforms

Fig. 5

New Local Network Created



productionnet

DASHBOARD | CONFIGURE | CERTIFICATES

dns servers

Domain Services 2	192.168.40.6
Domain Services 1	192.168.40.5
SELECT OR ENTER NAM	IP ADDRESS

point-to-site connectivity

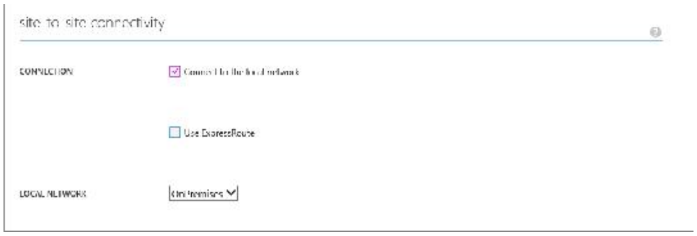
CONNECTION ☐ Configure point-to-site connectivity

site-to-site connectivity

CONNECTION ☐ Connect to the local network

Fig. 6

Open the Virtual Network and select Configure to define settings for the VPN tunnel



site-to-site connectivity

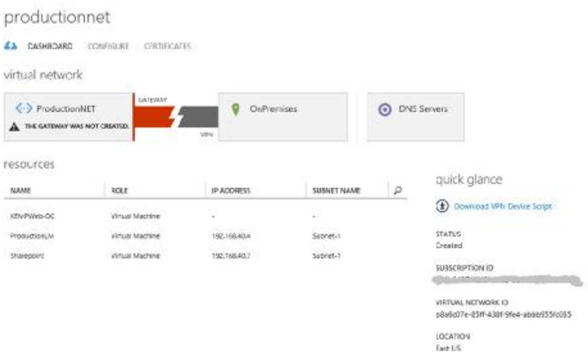
CONNECTION ☑ Connect to the local network

☐ Use ExpressRoute

LOCAL NETWORK OnPremises

Fig. 7

Under “site-to-site connectivity” select “Connect to the local network”. Confirm the Local Network created earlier is selected in the Local network and then select “Save”



THE GATEWAY WAS NOT CREATED.

NAME	ROLE	IP ADDRESS	SUBNET NAME
KEMPWeb-DC	Virtual Machine	-	-
ProductionLM	Virtual Machine	192.168.40.4	Subnet-1
Sharepoint	Virtual Machine	192.168.40.7	Subnet-1

STATUS
Created

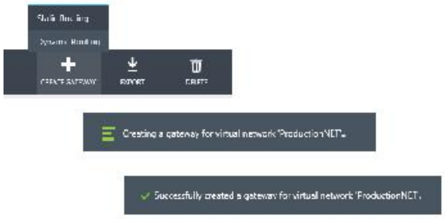
SUBSCRIPTION ID
[redacted]

VIRTUAL NETWORK ID
b8a6d07e-85ff-438f-9fe4-abbb955fc085

LOCATION
East US

Fig. 8

Once complete the dashboard will show the VPN connection between the Azure environment and the on-premises LoadMaster. Note the warning about the missing gateway.

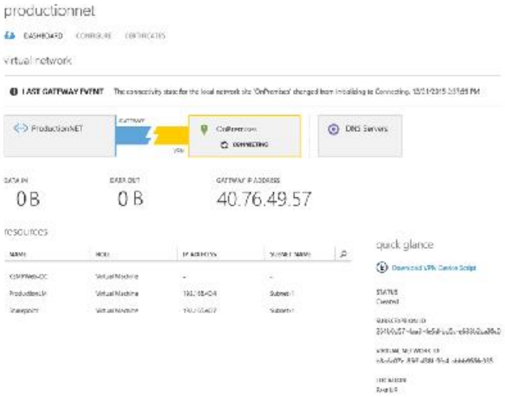


Creating a gateway for virtual network 'ProductionNET'.

Successfully created a gateway for virtual network 'ProductionNET'.

Fig. 9

To correct this, select “CREATE GATEWAY” in the tool bar and select “Static Routing”. This process will take several minutes while the gateway is set up.



LAST GATEWAY EVENT The connectivity state for the local network site 'OnPremises' changed from Initializing to Connecting. 12/21/2015 2:37:55 PM

CONNECTING

DATA IN
0 B

DATA OUT
0 B

GATEWAY IP ADDRESS
40.76.49.57

NAME	ROLE	IP ADDRESS	SUBNET NAME
KEMPWeb-DC	Virtual Machine	-	-
ProductionLM	Virtual Machine	192.168.40.4	Subnet-1
Sharepoint	Virtual Machine	192.168.40.7	Subnet-1

STATUS
Created

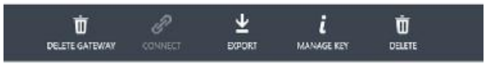
SUBSCRIPTION ID
[illegible]

VIRTUAL NETWORK ID
[illegible]

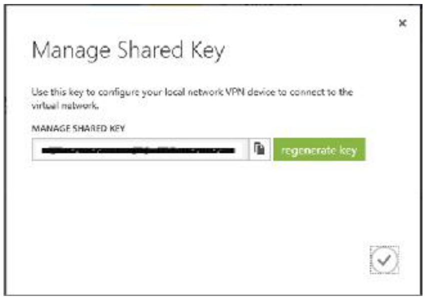
LOCATION
East US

Fig. 10

Now that the gateway has been configured, the Gateway IP address is displayed on the Dashboard screen. This address will be used later when setting up the LoadMaster.



Next, in the dashboard select "MANAGE KEY" at the bottom of the page. This will generate a shared key.



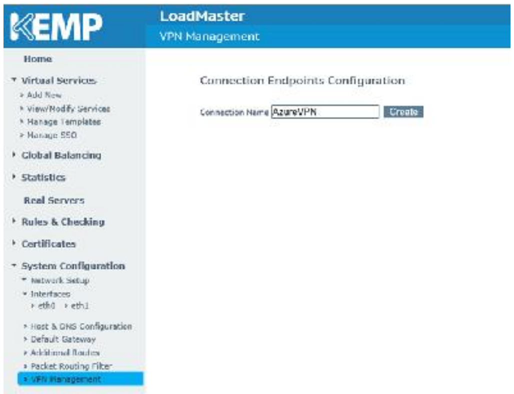
Manage Shared Key

Use this key to configure your local network VPN device to connect to the virtual network.

MANAGE SHARED KEY: [redacted]

Fig. 12

Copy the Pre-Shared Key. This will be used on the LoadMaster when creating the tunnel end point. For the next step you will need to log into the LoadMaster and complete the following tasks.

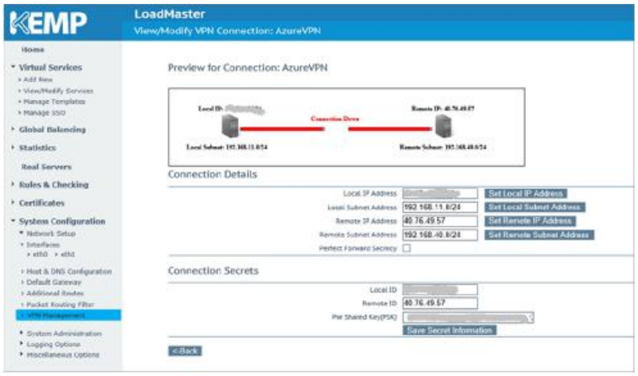


Connection Endpoints Configuration

Connection Name: AzureVPN

Fig. 13

Within the WUI of the on premises LoadMaster, select "VPN Management" under Network Setup. Enter a name for the VPN tunnel and click on "Create".



Preview for Connection: AzureVPN

Local IP: [redacted]
Remote IP: 40.76.49.57
Local Subnet: 192.168.11.0/24
Remote Subnet: 192.168.40.0/24

Connection Details

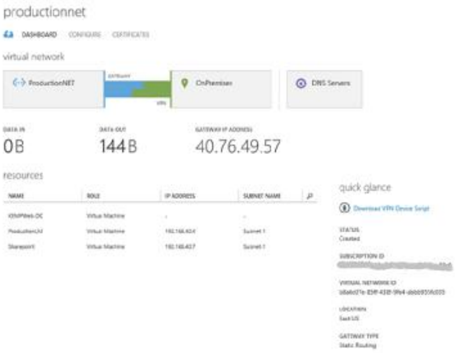
Local IP Address [redacted]
Local Subnet Address 192.168.11.0/24
Remote IP Address 40.76.49.57
Remote Subnet Address 192.168.40.0/24
Perfect Forward Secrecy □

Connection Secrets

Local ID [redacted]
Remote ID 40.76.49.57
Pre Shared Key(PSK) [redacted]

Fig. 14

Next, enter the connection information. The Remote IP Address can be found on the Azure VNET Dashboard and the local public IP address of the LoadMaster is the one used in Figure 3. Once this step is completed, the connection will become active.



DATA IN 0B
DATA OUT 144 B
GATEWAY IP ADDRESS 40.76.49.57

resources

NAME	ROLE	IP ADDRESS	SUBNET NAME
KEMPWeb-DC	Virtual Machine	-	-
ProductionLM	Virtual Machine	192.168.40.4	Subnet-1
Sharepoint	Virtual Machine	192.168.40.7	Subnet-1

STATUS
Created

SUBSCRIPTION ID
[redacted]

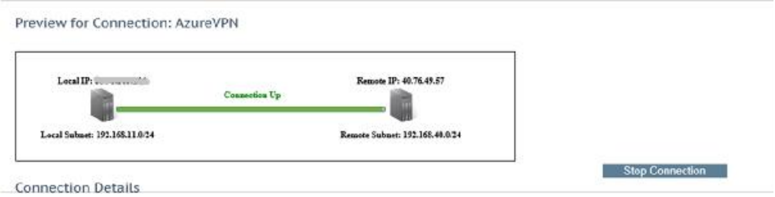
VIRTUAL NETWORK ID
[illegible]

LOCATION
East US

GATEWAY TYPE
Static Routing

Fig 15

In the Azure dashboard, an active connection is now shown between the production network in the cloud and the on-premises network, and user traffic can flow to the cloud based services.



Preview for Connection: AzureVPN

Local IP: [redacted]
Remote IP: 40.76.49.57
Local Subnet: 192.168.11.0/24
Remote Subnet: 192.168.40.0/24

Connection Details

Fig. 16

The on-Premises LoadMaster shows the connection is active, and if needed the LoadMaster can now be configured to connect to additional resources in the Azure cloud.

References

Additional supporting documents can be found at http://kemptechnologies.com/loadmaster-documentation. The following items in the feature description section address the example above and also provide additional information on configuration for virtual services, security and content switching.

- IPsec Tunnelling
- LoadMaster for Azure
- HA for Azure

Microsoft also provides details of setting up Azure networking and VPN: https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-site-to-site-create/

Document History

Date	Change	Reason for Change	Version	Resp.
Feb 2016	Initial release	First version	1.0	CB