IPsec Tunneling for Azure

Reference Architecture

VERSION: 1.0

UPDATED: Feb 2016

Copyright Notices

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,   including commercial applications, and to alter it and redistribute it   freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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.
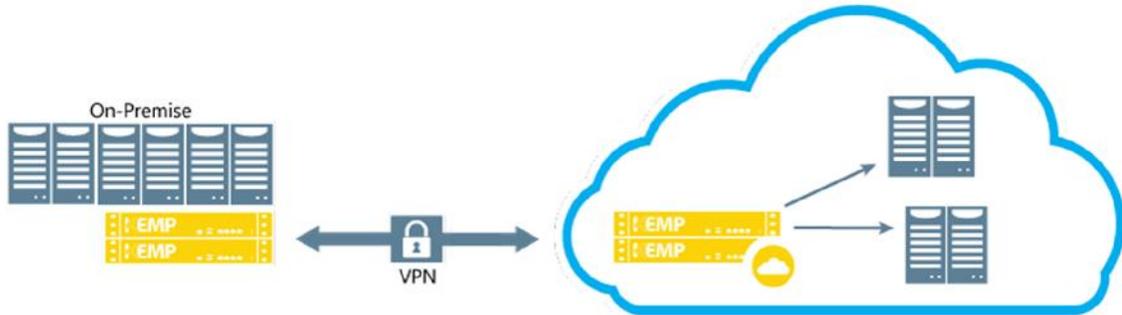

Fig. 1

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.

Fig. 2

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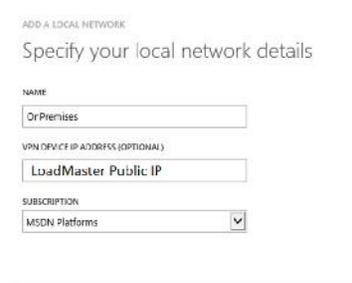

Fig. 3

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.
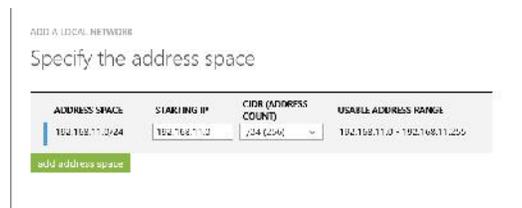

Fig. 4

Specify the on premises network

.

Fig. 5

New Local Network Created

Fig. 6

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

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"
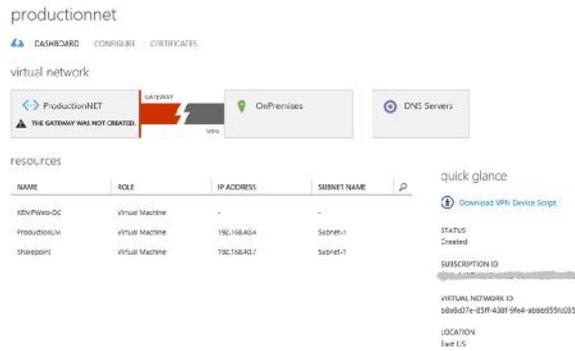
Fig. 8

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.
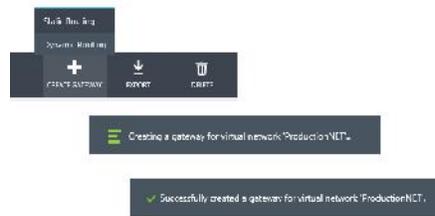

Fig. 9

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.
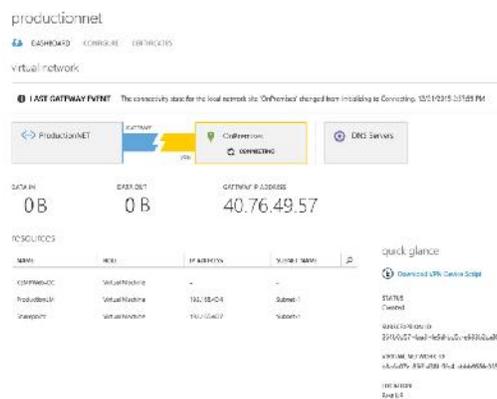

Fig. 10

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.

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.

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".
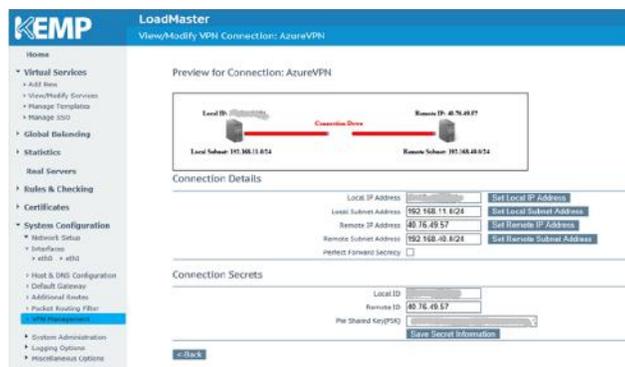
Fig. 14

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.
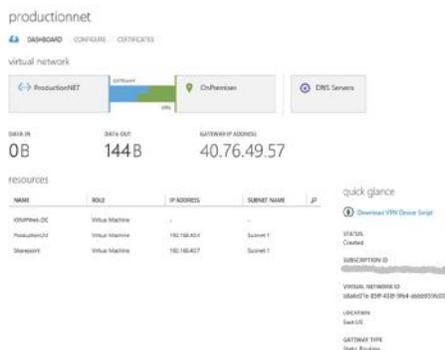

Fig 15

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.
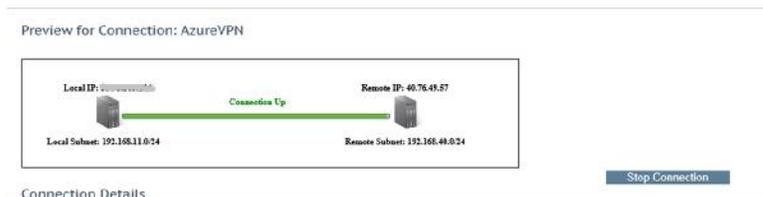

Fig. 16

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/

13

Document History

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

14