



## Cloud Access Manager 8.1.4

# How to Deploy Cloud Access Manager in a Virtual Private Cloud

**Copyright 2018 One Identity LLC.**

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.




**Patents**

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

**Trademarks**

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

**Legend**

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

# Contents

<b>Introduction</b> .....	<b>4</b>
Creating a virtual network .....	5
Configuring the SonicWALL device .....	7
Establishing the IPSec VPN connection .....	10
Creating the virtual machines .....	10
Preparing Cloud Access Manager hosts .....	12
Cloud Access Manager configuration .....	12
<b>About us</b> .....	<b>13</b>
Contacting us .....	13
Technical support resources .....	13

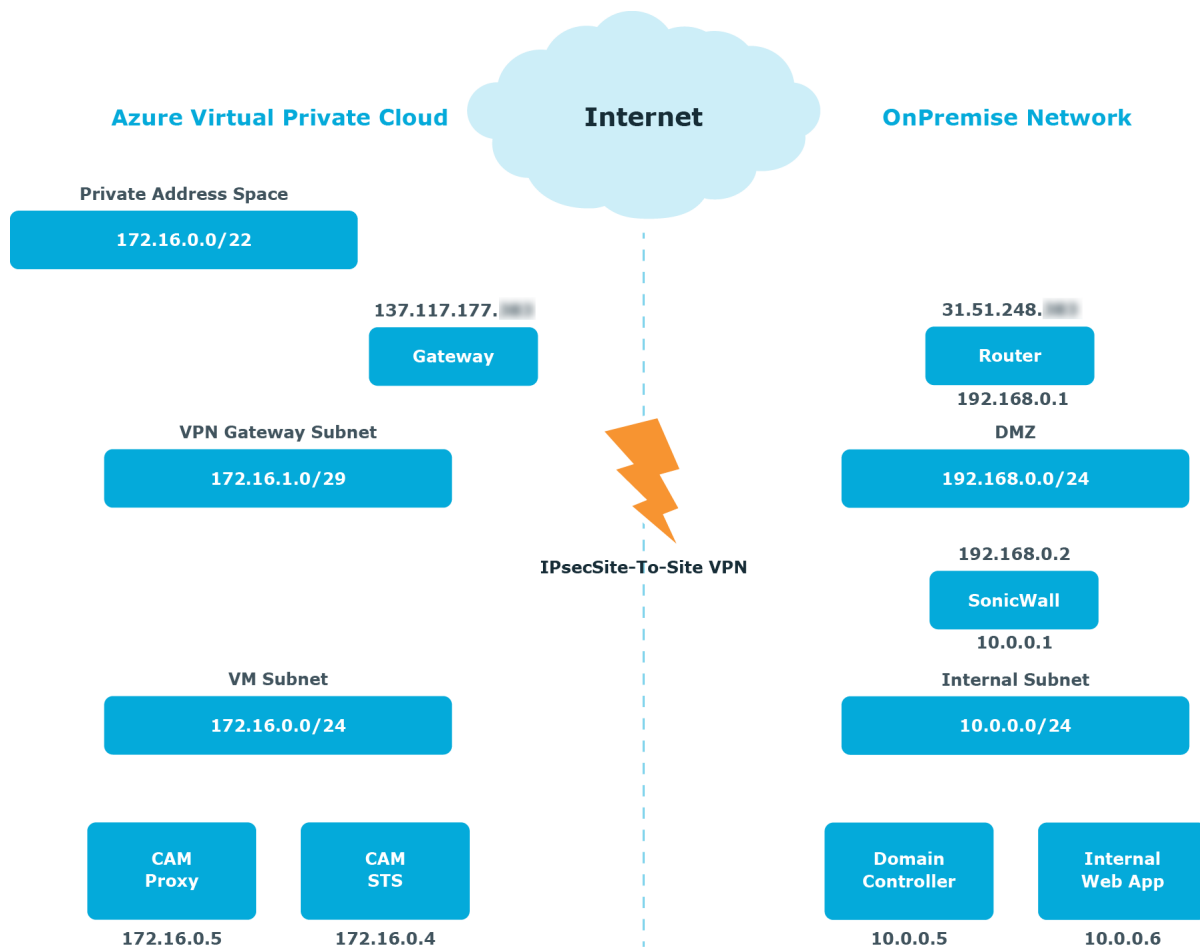
## Introduction

This guide describes how to deploy Cloud Access Manager within a virtual private cloud that is connected to your on-premise network using a site-to-site virtual private network (VPN). This enables you to rent virtual machines, hosted by a third party, rather than purchase hardware to host on-premise. The example in this guide describes how to use the Windows Azure platform with a SonicWALL VPN device. Virtual private clouds from other Cloud providers, such as Amazon, and other VPN devices supporting IPsec site-to-site can also be used.

For information on deploying Cloud Access Manager on-premise, please refer to the *One Identity Cloud Access Manager Installation Guide*.

Figure 1 illustrates how to extend an on-premise network into a Windows Azure virtual private cloud to deploy Cloud Access Manager off-premise. A SonicWALL VPN device connects the on-premise network to the cloud network to enable access to the cloud network, just like any other remote office and allows the virtual machines in the cloud network to behave as if they were on-premise. You can use the on-premise VPN device to restrict access to and from the cloud network if required.

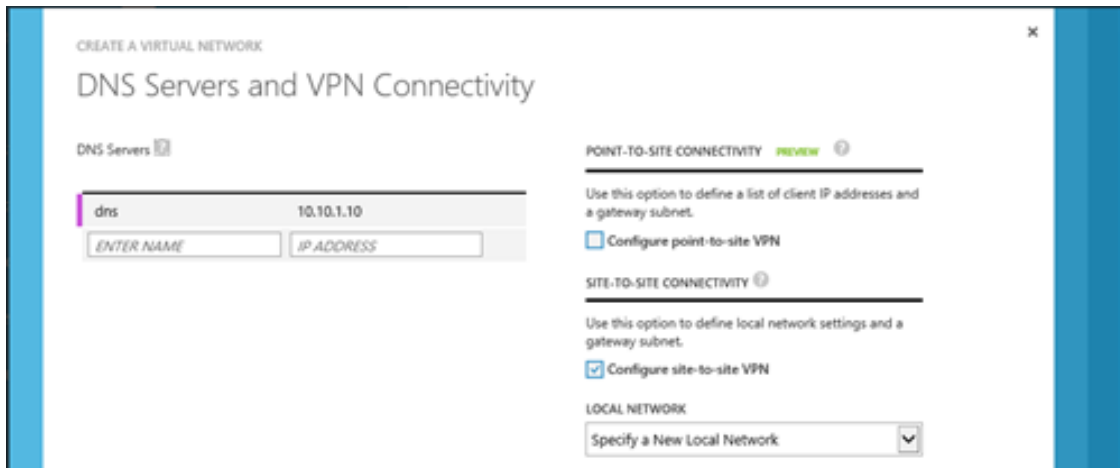
Figure 1: Extending an on-premise network



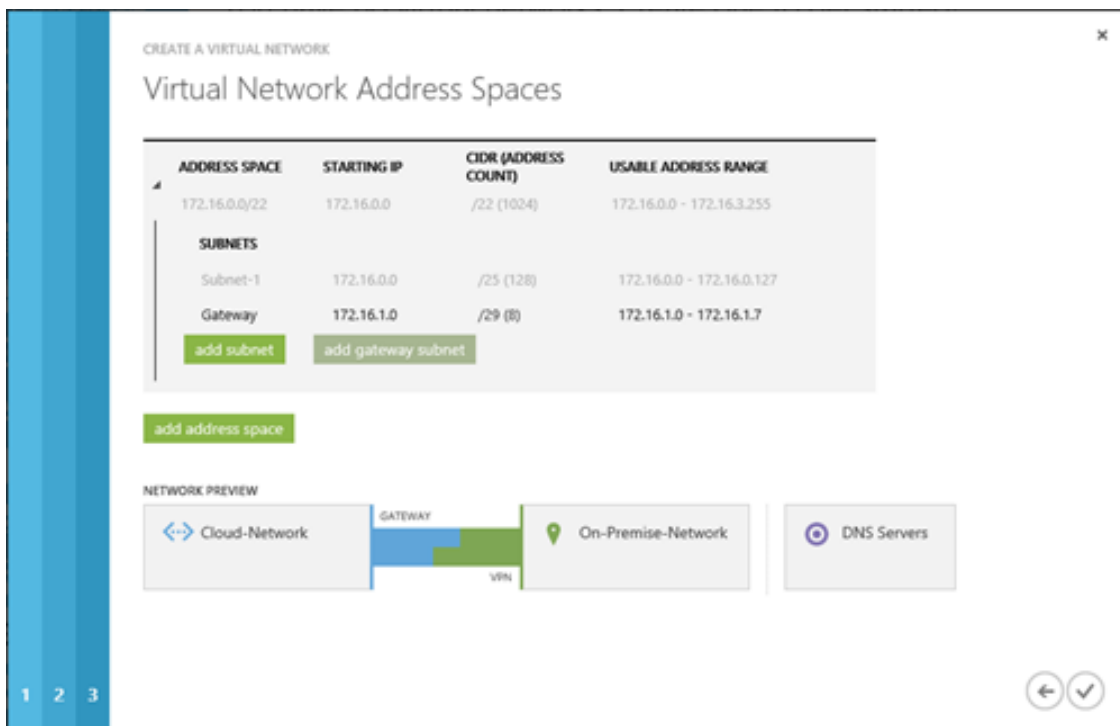
## Creating a virtual network

### To create a virtual network using Windows Azure

1. From the Windows Azure portal, click **Create a virtual network** to start the wizard.
2. On the **DNS Servers and VPN Connectivity** tab, enter the IP address of at least one Active Directory Domain Name System (DNS) server residing on the on-premise network.
3. Select the **Configure site-to-site VPN** check box.



4. On the **Site-to-Site Connectivity** tab, enter the address space used by the on-premise network and the public IP address used by the SonicWALL VPN device.
5. On the **Virtual Network Address Spaces** tab, enter the address space to use for the virtual network. This must not clash with the on-premise network.
6. Add a subnet to use for the virtual network.
7. Add a gateway subnet. This subnet is used for the Windows Azure VPN Gateway endpoint to enable routing between the on-premise network and the cloud network. The Windows Azure VPN Gateway endpoint uses two IP addresses from this subnet to set up its routing.



8. Complete the wizard and wait a few moments while the virtual network is created.

- Return to the network dashboard and click **CREATE GATEWAY**, then select **Static Routing**.
- When it has been created, the public IP address of the Windows Azure VPN Gateway is displayed. A shared key is also generated. Click **MANAGE KEY** to view the shared key.

## Configuring the SonicWALL device

### To configure a SonicWALL device

- Create a new security object for the virtual network.

The screenshot shows the SonicWALL Network Security Appliance configuration dialog. The fields are as follows:

Name:	Cloud-Network
Zone Assignment:	VPN
Type:	Network
Network:	172.16.0.0
Netmask:	255.255.252.0

Below the fields is a 'Ready' status bar and 'OK' and 'Cancel' buttons.

- If not already present, create a new security object for your on-premise network.

The screenshot shows the SonicWALL Network Security Appliance configuration dialog. The fields are as follows:

Name:	Internal Network
Zone Assignment:	LAN
Type:	Network
Network:	10.0.0.0
Netmask:	255.255.255.0

Below the fields is a 'Ready' status bar and 'OK' and 'Cancel' buttons.

- Create a virtual private network (VPN) Policy.
- Select a **Policy Type** of **Site-to-Site**.
- Select an **Authentication Method of IKE using Preshared Secret**.
- In the **IPsec Primary Gateway Name or Address** field, enter the GATEWAY IP ADDRESS displayed on the **Virtual Network** page of the **Windows Azure Management Portal**.
- In the **Shared Secret** field, enter the VPN KEY obtained from the Windows Azure network dashboard.

**SONICWALL** | Network Security Appliance

General | **Network** | Proposals | Advanced

---

**Security Policy**

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name: Azure

IPsec Primary Gateway Name or Address: 137.117.177.7

IPsec Secondary Gateway Name or Address: 0.0.0.0

---

**IKE Authentication**

Shared Secret: [Masked]

Confirm Shared Secret: [Masked]  Mask Shared Secret

Local IKE ID: IP Address [Empty]

Peer IKE ID: IP Address [Empty]

---

Ready

OK Cancel Help

- On the **Network** tab, select the local and remote network security objects created in steps 1 and 2.



**SONICWALL** Network Security Appliance

General Network **Proposals** Advanced

**Local Networks**

Choose local network from list Internal Network

Local network obtains IP addresses using DHCP through this VPN Tunnel

Any address

**Remote Networks**

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Choose destination network from list Cloud-Network

Ready

OK Cancel Help

- On the **Proposals** tab, select an **Exchange** type of **Main Mode** and an **Encryption** type of **AES-256**.

**SONICWALL** Network Security Appliance

General Network **Proposals** Advanced

**IKE (Phase 1) Proposal**

Exchange: Main Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

**Ipsec (Phase 2) Proposal**

Protocol: ESP

Encryption: AES-256

Authentication: SHA1

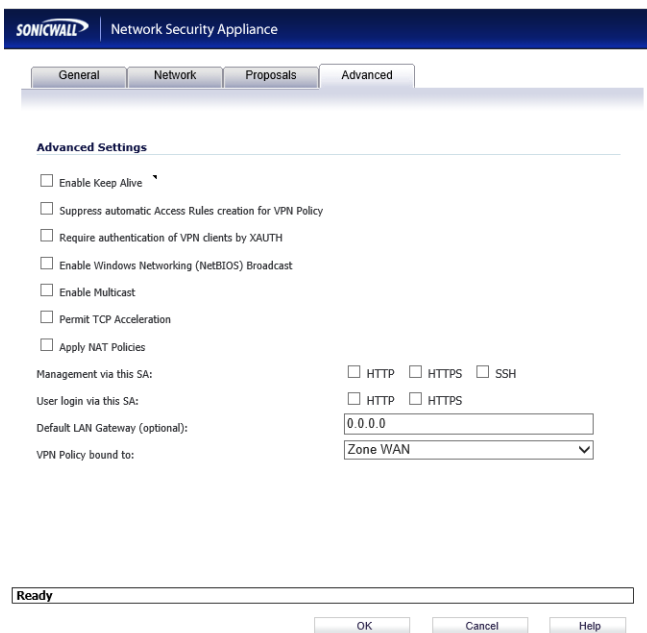
Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Ready

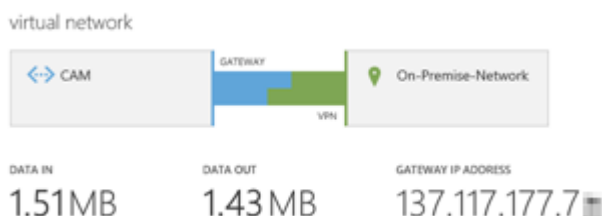
OK Cancel Help

- Finally, on the **Advanced** tab, in the **VPN Policy bound to:** field, select **Zone WAN** interface.



## Establishing the IPsec VPN connection

Within the Windows Azure user interface, navigate to the network dashboard and click **Connect** to establish the virtual private network (VPN) connection.

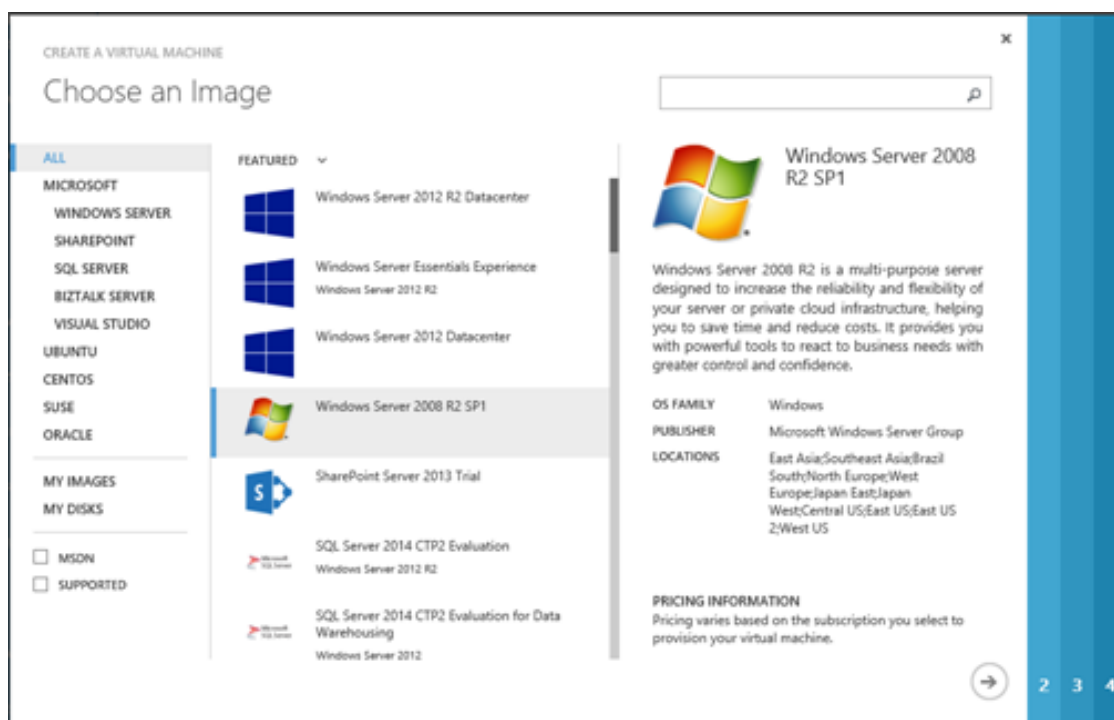


## Creating the virtual machines

This example uses two virtual machines and follows a typical production installation of Cloud Access Manager. For example, one machine for the proxy host and another machine for the Security Token Service (STS) host. Additional hosts can be added later if you need to increase capacity.

## To create a typical production installation of Cloud Access Manager

1. Create a new virtual machine for the proxy host using the **FROM GALLERY** wizard. Select the **Windows Server 2008 R2 SP1** Windows Azure image.



2. On the **Configuration** tab for the first virtual machine, set the size of the virtual machine to medium or higher.
3. On the **Configuration** tab for the second virtual machine, set the **Region/Affinity group/Virtual network** field to the name of the virtual network you created earlier.
  - NOTE:** This cannot be easily changed after the virtual machine has been created.
4. On the **Endpoints** tab, add **HTTP** and **HTTPS** endpoints to allow users to access the proxy from the Internet.

ENDPOINTS ?

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
HTTPS	TCP	443	443
HTTP	TCP	80	80

ENTER OR SELECT A VALUE ▼

5. Repeat the process to create a new virtual machine for the STS host; no Endpoints are required for the STS host.

6. Power up both virtual machines ensuring they can be accessed using the Remote Desktop client. To test connectivity over the virtual private network (VPN), connect using the private IP address rather than the public IP address for the virtual machine.

## Preparing Cloud Access Manager hosts

### ***To prepare the Cloud Access Manager***

1. Join the Security Token Service (STS) host to your Active Directory domain using the normal procedure.
2. Log in to the STS host as a domain admin and install Microsoft SQL Server 2012.
3. You do not need to join the proxy host to the domain.

## Cloud Access Manager configuration

### ***To configure Cloud Access Manager***

1. Perform a standard production installation as described in the *One Identity Cloud Access Manager Installation Guide*.
2. When you configure the wildcard DNS subdomain to use with Cloud Access Manager, the wildcard subdomain should resolve to the public Virtual IP (VIP) address of the proxy host. The VIP can be obtained from the Windows Azure UI by navigating to the Virtual Machine for the proxy host.
3. Add the external wildcard DNS subdomain to your internal DNS. Ensure that it resolves to the internal/private IP address of the proxy host. This will allow users on the on-premise network to access Cloud Access Manager over the virtual private network (VPN) connection instead of through the Internet.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product