SOPHOS
Security made simple.

Sophos XG Firewall on Microsoft Azure

Quick Start Guide

Document date: Tuesday, September 20, 2016

Contents

1 Overview

Sophos XG Firewall on Azure is a solution to run XG Firewall on Microsoft Azure. Therefore an Azure account is required to be able to use Sophos XG Firewall on Azure.

This guide describes how you can deploy and run Sophos XG Firewall on Azure.

2 Deployment of Sophos XG Firewall on Azure

Please follow the steps outlined here to create a fresh XG Firewall deployment to a new resource group within the Microsoft Azure environment. The process involves creating a new VM instance, selecting a subscription, making network and storage settings for the VM instance and finally purchasing it.

To create the VM instance, proceed as follows:

1. **Log on to Azure using your Microsoft Azure account.**
2. **Click *New* and search for *Sophos*.**
   A list of deployable items appears.
3. **Select *Sophos XG Firewall* and click *Create*.**
   A configuration dialog opens.

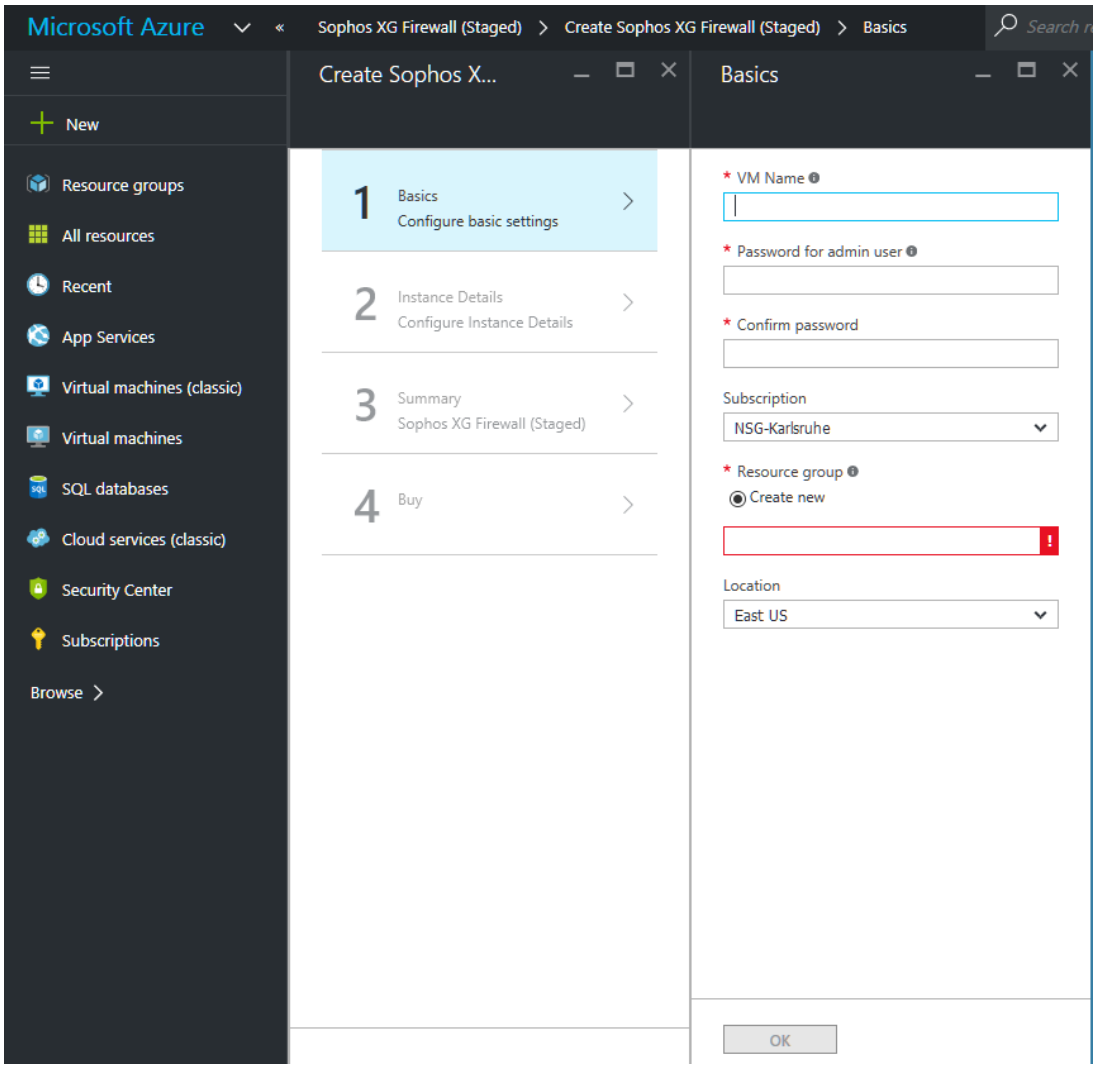

Figure 1 Create VM Instance

4. **Make the following basic settings:**

VM Name: Enter a name for the VM instance.

Password for admin user: Enter a password and confirm it in the next field.

Note – The password has to consist of at least 8 characters, containing at least one lower-case and one uppercase letter, a number and a special character.

Subscription: A subscription corresponds to a Sophos XG Firewall on Azure account and can be viewed in the *Subscriptions* dialog. If you have multiple accounts you can change the default subscription here.

Resource Group: Enter a name for the resource group.

Location: Select the data center where the VM instance should be deployed to.

5. **Click *OK* to proceed.**
The *Instance Details* configuration dialog opens.

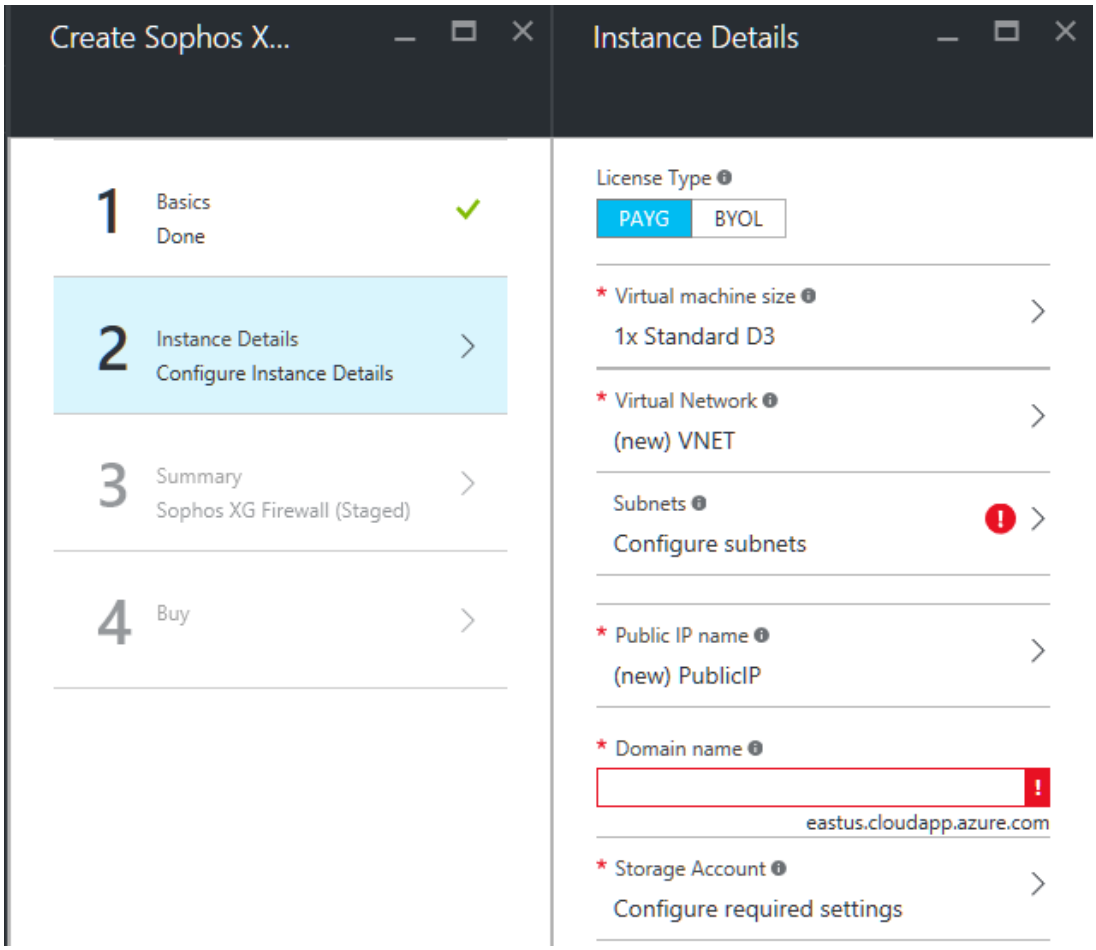

Figure 2 Instance Details

6. **Make the following settings:**
License Type: Select whether to pay hourly (*PAYG*) or to buy a Sophos license (*BYOL*).

Virtual Machine Size: Select the desired size of the VM instance.

Virtual Network: Select or create a virtual network for the instance to be placed in.

Subnets: Configure subnets for WAN and LAN zone:

- **WAN subnet name:** Enter a WAN subnet name.
- **WAN subnet address prefix:** Enter a WAN subnet address prefix.
- **LAN subnet name:** Enter a LAN subnet name.
- **LAN subnet address prefix:** Enter a LAN subnet address prefix.

Public IP name: Select or create a public IP:

- **Name:** Enter a name for the public IP.
- **Assignment:** Select either *Dynamic* or *Static* assignment.

Domain name: Enter the name of the domain the instance should belong to.

Note – The domain name will be appended by the Azure domain which is displayed below the text field.

Storage Account: Configure the storage account for disk Blobs and diagnostics:

- **Name:** Enter the name for the storage account.

  Note – The name must consist of 3-24 characters. Only lower case characters and numbers are allowed.

- **Performance:** Select to use *Standard* performance.

  Note – *Premium* is currently not supported.

- **Replication:** Select the requested replication strategy.

7. **Click *OK*.**
   The summary opens. As soon as the validation passed, you can proceed purchasing.

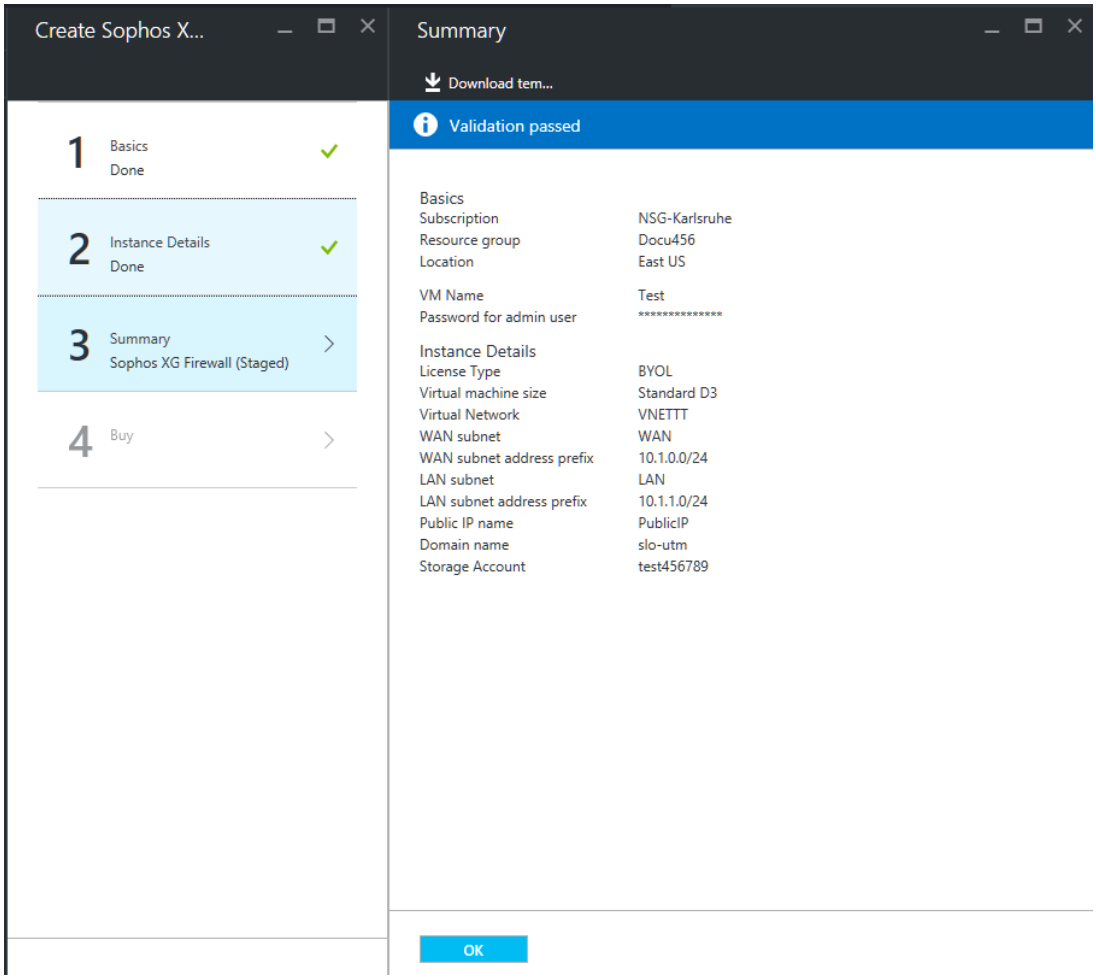

Figure 3 Validation

8. **Click *OK*.**
   The purchase dialog opens.
9. **Click *Purchase*.**
   The deployment starts.

After the deployment succeeded, you can connect to the machine via the domain name you selected before (e.g. *https://xgdomain:4444*).

3 Registration of XG Firewall Device

Note – This section is valid only for licensing type *BYOL*.

To register an XG Firewall, proceed as follows:

1. **If you have no license yet, get a demo license on XG Firewall Free Trial.**
2. **Install XG Firewall.**
3. **Accept the license agreement.**
   Log on to XG Firewall and accept the license agreement (EULA) by clicking *I Accept*.
4. **Activate XG Firewall doing the following:**
   1. Select the installation option.
   2. Paste the serial number mailed to your registered email address.
   3. Click *Activate Device*.

      Note – Ensure that your current network configuration allows XG Firewall to connect to the Internet. If not, use *Basic Setup* to modify this setting.

5. **Register XG Firewall:**
   1. Click *Register Device*.
   2. Select whether to log in with your MySophos account or to *Register for MySophos*.
   3. Click *Continue* to complete the registration process.
6. **Make sure the license is synchronized:**
   1. Click *Initiate License Synchronization*.
   2. Click *Synchronize License*.
7. **Configure your device.**
   Click *Click Here* to run the Configuration Wizard which guides you through the initial configuration steps.

4 Configuration of XG Firewall for Specific Use Cases

The following section describes the configuration steps for incoming and outbound web traffic scanning for VDI (Virtual Desktop Infrastructure) clients.

4.1 Configuration for Incoming VDI Traffic

To configure XG Firewall for incoming VDI traffic, proceed as follows:

1. **Log in to your XG Firewall.**
2. **Navigate to *Protect > Firewall*, click *Add Firewall Rule* and select *Business Application Rule*.**
   The *Add Business Application Rule* page opens.

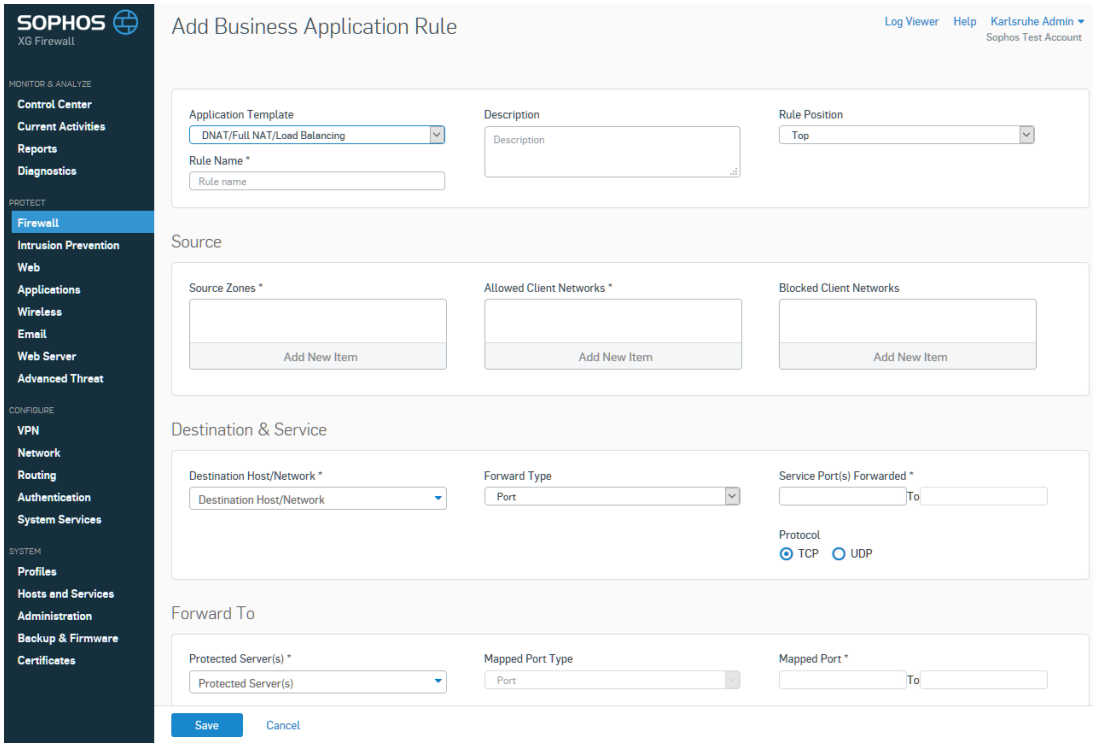

Figure 4 Add Business Application Rule

3. **Make the following settings:**
   Application Template: Select *DNAT/Full NAT/Load Balancing*.

   Rule Name: Enter a descriptive name for the rule.

   Destination Host/Network: Select the WAN interface of XG Firewall which is PortB.

   Protected Server(s): Select your VDI clients.

   Mapped Port: Enter the port or port range the rule should map traffic to. For example use

TCP port 3389 for RDP.

4. **Click *Save*.**

You can now proceed configuring XG Firewall for outgoing web traffic scanning.

4.2 Configuration for Outgoing Web Traffic Scanning

To configure XG Firewall for outgoing web traffic scanning, proceed as follows:

1. **Log in to your XG Firewall.**
2. **Navigate to *Protect > Firewall*, click *Add Firewall Rule* and select *Add User / Network Rule*.**
   The *Add User / Network Rule* page opens.

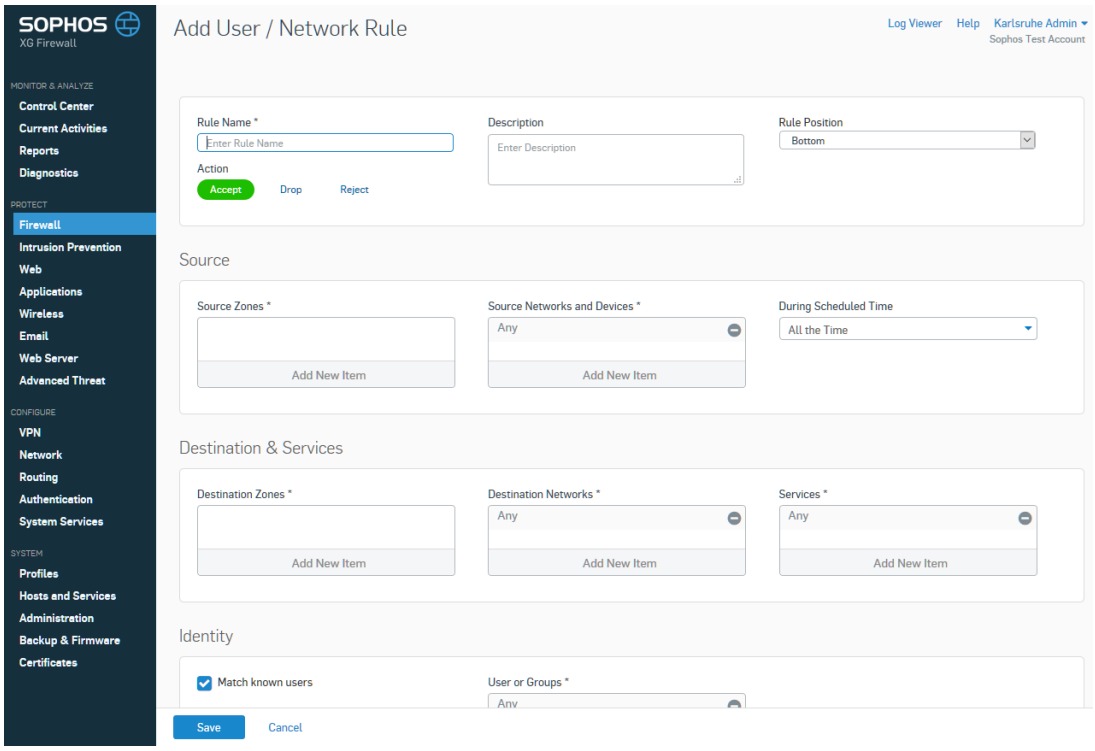

Figure 5 Add User / Network Rule

3. **Make the following settings:**
   Rule Name: Enter a descriptive name for the rule.

   Source Networks and Devices: Select the source networks and devices this policy should apply to.

   Malware Scanning: Enable the scanning modules you require.

   Rewrite source address (Masquerading): Enable masquerading for the outbound address.
4. **Click *Save*.**

Now the setup is finished and you are able to browse the web using your VDI solution.

Copyright Notice