SOPHOS

Cybersecurity made simple.

Sophos XG Firewall Virtual Appliance Microsoft Hyper-V

getting started guide

Contents

1 Introduction

The Getting Started Guide describes how to download and deploy Sophos XG Firewall Virtual Appliance on Microsoft Hyper-V.

Base Configuration

If the following minimum server requirements are not met, XG Firewall will go into failsafe mode:

1. One vCPU
2. 2 GB vRAM
3. 2 vNIC
4. Primary Disk: Minimum 4 GB
5. Auxiliary Disk: Minimum 80 GB

Note
SFOS 17 supports hard drives with a maximum of 512 GB.

Note
For optimal XG Firewall performance, configure vCPU and vRAM according to the license you have purchased. Do not exceed the maximum number of vCPUs specified in the license.

2 Installation procedure

Make sure that Microsoft Hyper-V Server 2008/2012 has been installed in your network. To install Microsoft Hyper-V Server, refer to the instructions:

- http://technet.microsoft.com/en-us/library/dd283085(v=ws.10).aspx
- http://technet.microsoft.com/en-us/library/hh831620.aspx

1. Download the .zip file containing VHD disks from https://secure2.sophos.com/en-us/products/next-gen-firewall/free-trial.aspx and save it to your machine.
2. Launch the Hyper-V Manager. Go to **Action > Connect to Server** to connect to the host server on which you wish to deploy the VHD template. The following screen appears:
3. Go to **Action > New** and select **Virtual Machine**.

   It opens New Virtual Machine Wizard.
4. Name the virtual appliance.
5. Select Generation 1.
6. Set virtual memory for the appliance. For **Startup memory** (vRAM), enter 2048 MB (recommended) or higher.
7. Choose the network interface for the appliance.
8. Choose the primary virtual hard disk. Select **Use an existing virtual hard disk** and browse to select the file that you extracted.
9. Complete the basic setup. Verify the configuration summary and click **Finish**.

   Note
   This completes the basic setup of VM. To complete the Sophos XG Firewall installation you need to add network interface and auxiliary disk.

10. Configure the settings for virtual appliance. Right-click the virtual appliance that you created and click **Settings**.
11. Add network adapter to the virtual appliance. Under **Hardware**, select **Network Adapter** and click **Add**.

    a) To specify the network adapter configurations, refer to the image below.
12. Add auxiliary disk to the appliance. Under **Add Hardware**, click **SCSI Controller** and select **Hard Dive**.

    a) Click **Add** and then browse to select the Auxiliary disk.
13. Connect to the virtual appliance. Right-click the virtual appliance and click **Connect**.

    Sophos XG Firewall has been installed on your virtual machine.

    a) To continue to the **Main Menu**, enter the administrator password '`admin`'.
14. Accept EULA.

3 Configuring XG Firewall

1. Browse to "https://172.16.16.16" from the management computer.
2. Click **Start** to begin the wizard and follow the on-screen instructions.

> **Note**
> The wizard will not start if you have changed the default administrator password from the console.

3.1 Activation and Registration

1. Review and accept the License Agreement. You must accept the Sophos End User License Agreement (EULA) to proceed further.
2. Register Your Firewall. Enter the serial number, if you have it. You can also use your UTM 9 license if you are migrating.

   Otherwise, you can skip registration for 30 days or start a free trial.

   a) You will be redirected to the MySophos portal website. If you already have a MySophos account, specify your sign-in credentials under “Login”. If you are a new user, sign up for a MySophos account by filling in the details under “Create Sophos ID”.

   b) Complete the registration process.

   Post successful registration of the device, the license is synchronized and the basic setup is done.
3. Finish the basic setup. Click **Continue** and complete the configurations through the wizard. When you finish the process, the Network Security Control Center appears.

You can now use the navigation pane to the left to navigate and configure further settings.

3.2 Basic Configuration

You can:

1. Set up Interfaces
2. Create Zones
3. Create Firewall Rules
4. Set up a Wireless Network

1. To set up interfaces:

   a) You can add network interfaces and RED connections in the **Configure > Network > Interfaces** menu.

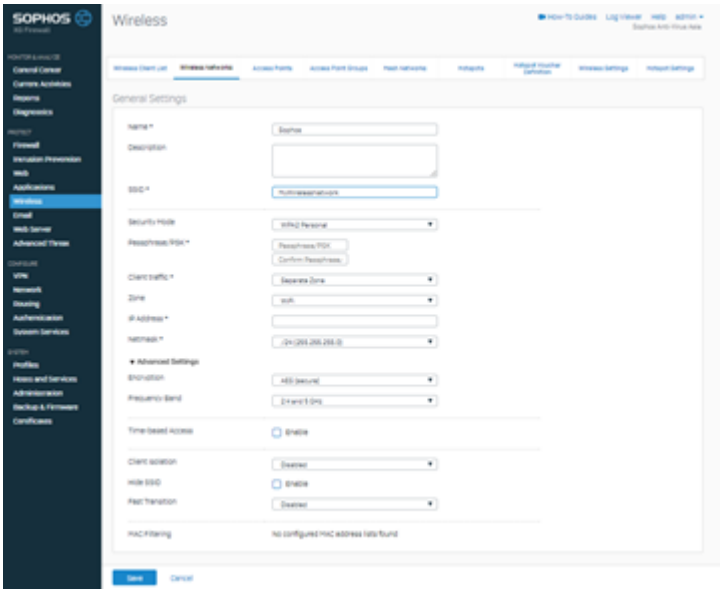
   b) You can add wireless networks in the **Protect > Wireless > Wireless Networks** menu. SSIDs will also be shown in the interfaces menu once created.

   c) You can add access points in **Protect > Wireless > Access Points**.

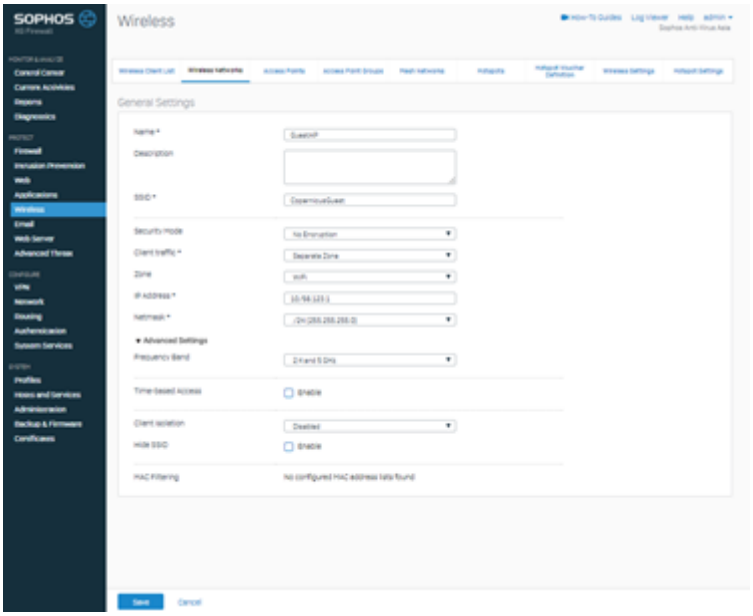
2. Zones are essential in creating firewall rules and, therefore, central to the security model in XG Firewall. If you wish to create custom zones in addition to the default zones, go to **Configure > Network > Zone**. You can use these custom zones when creating interfaces, and security policies.
3. You can create the following types of firewall rules in **Protect > Firewall > Add Firewall Rule**. Two types of firewall rules are available:

Option	Description
Business Application Rule	To secure a server or service, and allow internal or external users access to it, use a business application rule.
User/Network Rule	To control user access to web and application content, or to control traffic by source, service, destination, zone, and user, use a user/ network rule.

4. To set up a wireless network:
   a) Go to **Protect > Wireless > Wireless Networks**.
   b) Click **Add** to add a new wireless network.
   c) Configure the wireless network as shown in the image.



   The wireless network will be added successfully.
   d) Similarly, add another wireless network for guest access.



You can see both these wireless networks in **Protect > Network > Wireless Networks**.

e) Go to **Protect > Wireless > Access Point Groups**.

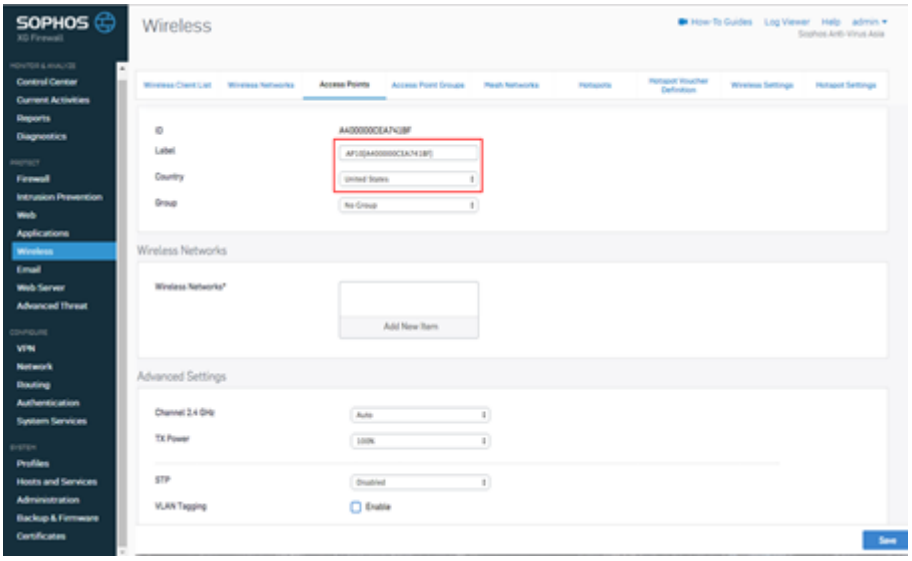
f) Click **Add** to add a new access point group.

g) Add both the wireless networks, and the new access point.

If new APs have been installed, you can view these in Control Center.

h) Click the pending APs to accept the new access points.

i) Configure the settings of the new APs as shown in the image.



j) Click **Save**.

4 Legal notices

Copyright © 2020 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.