## Contents

- Virtual and software appliances ........................................................................................................ 1
- Microsoft Hyper-V ............................................................................................................................. 2
  - Installing on Hyper-V ......................................................................................................................... 2
- Nutanix Prism ....................................................................................................................................... 12
  - Installing on Nutanix Prism Central .................................................................................................. 12
- KVM ..................................................................................................................................................... 19
  - Installing on KVM ................................................................................................................................. 19
- Software appliance ............................................................................................................................... 29
  - Installing on Windows .......................................................................................................................... 29
  - Installing on macOS ............................................................................................................................ 30
- VMware ............................................................................................................................................... 32
  - Installing on VMware .......................................................................................................................... 32
- XenApp ................................................................................................................................................. 39
  - Installing on XenApp ............................................................................................................................ 39
- Activating and registering XG Firewall ................................................................................................. 45

(2020/10/16)
1 Virtual and software appliances

You can install XG Firewall as a virtual or software appliance.

With XG Firewall virtual and software appliances, you can implement network security and Synchronized Security (for endpoints) within the virtual infrastructure. These appliances deliver the full security of the hardware appliances. You can manage these centrally through Sophos Central.

Virtual appliances

You can install XG Firewall as a virtual appliance on Nutanix Prism, VMware ESX and VMware ESXi, Microsoft Hyper-V 2008 and 2012, KVM (Kernel-based Virtual Machine), and Citrix XenApp platforms.

Software appliances

You can install XG Firewall as a software appliance on custom hardware over Windows or macOS systems.
2 Microsoft Hyper-V

You can deploy the XG Firewall virtual appliance on the Microsoft Hyper-V platform.

Prerequisites

• Install Microsoft Hyper-V Server 2008 or 2012 on a server that meets the minimum hardware requirements below. For instructions, go to Server 2008 or Server 2012.

• Install Hyper-V Manager (Hyper-V management software) on a management device that has network access to the server. For details, go to Hyper-V Manager.

Table 1: Minimum hardware requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>1</td>
</tr>
<tr>
<td>vRAM</td>
<td>4 GB minimum</td>
</tr>
<tr>
<td>vNIC</td>
<td>2</td>
</tr>
<tr>
<td>Primary disk</td>
<td>16 GB minimum</td>
</tr>
<tr>
<td>Report disk</td>
<td>80 GB minimum</td>
</tr>
</tbody>
</table>

If you don't meet the minimum requirements for new installations of Sfos 18.0, or if you’re migrating from an earlier version, XG Firewall goes into fail-safe mode.

CAUTION
Configure the vCPU and vRAM based on the purchased license. Don't exceed the maximum number of vCPUs specified in the license.

2.1 Installing on Hyper-V

You can deploy an XG Firewall VHD (Virtual Hard Disk) on Hyper-V platform.

1. Go to XG Firewall free trial and download the .zip file containing the VHD. Extract and save the image on the management device that has the Hyper-V Manager installed.

2. To deploy the VHD, follow these steps:
   a) Open the Hyper-V Manager. Go to Action > Connect to Server to connect to the host server.
b) Go to Action > New and select Virtual Machine.

c) Specify a name and location for the virtual appliance.
d) Select **Generation 1**.
### Specify Generation

Choose the generation of this virtual machine.

- **Generation 1**
  - This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

- **Generation 2**
  - This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠️ Once a virtual machine has been created, you cannot change its generation.

---

*More about virtual machine generation support*

---

**e) For Startup memory (vRAM), enter 4096 MB or higher.**
f) Select the network interface for the appliance.
g) Select the primary virtual hard disk. Select Use an existing virtual hard disk and select the extracted VHD file.

h) Verify the summary and select Finish.
The virtual machine’s basic setup is complete.

3. To add the network interface and auxiliary disk, follow these steps:
   a) Right-click the appliance and select **Settings**.
   b) Under **Hardware**, select **Network Adapter** and select **Add**.
c) To add an auxiliary disk, select **SCSI Controller**. Select **Hard Drive** and select **Add**.
d) Select the auxiliary disk.
To connect to the virtual appliance, right-click the appliance and select **Connect**.

XG Firewall will be installed on the server.

**4. Configure XG Firewall.**

a) Enter the administrator password **admin**.

b) Accept the Sophos end user license agreement.

The **Main menu** appears.

c) From the management device, go to **https://172.16.16.16**.

d) Select **Start** to open the initial setup wizard and complete the basic configuration.

**CAUTION**

The wizard won't start if you've changed the default password from the CLI console.

You need to activate and register XG Firewall.
3 Nutanix Prism

You can install the XG Firewall virtual appliance on the Nutanix Prism platform.
The first version validated with Nutanix AHV is XG Firewall 18.0 MR1.

Prerequisites

The AHV cluster must be running the below AOS (Acropolis), AHV, and Prism Central (PC) versions:
• AOS version: 5.15.x and later LTS release
• AHV version: AHV version bundled with AOS
• PC version: 5.15.x compatible with AOS version
• Nutanix AHV cluster registered to PC
• Partner VA version: Latest GA (LTS) release

Table 2: Minimum hardware requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>1</td>
</tr>
<tr>
<td>vRAM</td>
<td>4 GB minimum</td>
</tr>
<tr>
<td>vNIC</td>
<td>2</td>
</tr>
<tr>
<td>Primary disk</td>
<td>16 GB minimum</td>
</tr>
<tr>
<td>Report disk</td>
<td>80 GB minimum</td>
</tr>
</tbody>
</table>

If you don't meet the minimum requirements for new installations of SFOS 18.0, or if you're migrating from an earlier version, XG Firewall goes into fail-safe mode.

CAUTION
Configure the vCPU and vRAM based on the purchased license. Don't exceed the maximum number of vCPUs specified in the license.

3.1 Installing on Nutanix Prism Central

You can install XG Firewall QCOW2 disks on the Nutanix Prism Central platform.

Download the image disk

1. Go to XG Firewall free trial and download the .zip file containing the following QCOW2 disks:
   • PRIMARY-DISK.qcow2
- AUXILIARY-DISK.qcow2

2. Extract the .zip file and save the disks on the device from which you access Nutanix Prism Central.

**Upload the image to Nutanix Prism**

1. Sign in to the Nutanix Prism Central console.
2. From the top-left menu, go to **Virtual Infrastructure > Images**.

3. Click **Add Image**.
4. Click **Add File**.

5. Select one of the image files you extracted.
   Make sure that the selected **Image Type** is **Disk**.
You can enter a description in the **Image Description** field.

6. Repeat the last step for the second image.

After you've added both images, you should see them in the dialog.

7. Click **Next**.

8. Specify the settings for **Placement Method** and **Select Clusters** according to your needs.

9. Click **Save**.

10. Wait a few minutes and then refresh the browser.

    You'll find the newly created images in the images list.
Create the XG Firewall virtual machine

1. From the top-left menu, go to **Infrastructure > VMs**.

2. Click **Create VM**.

3. In **General Configuration**, enter a name for the VM and select a timezone.

4. In **Compute Details**, enter your desired number of virtual CPUs and RAM.
   Select a minimum of 4 GB of RAM.

5. In **Disks**, delete the CD-ROM that is shown by default.
   You must create a startup disk and a log disk for the VM.

6. Create a startup disk as follows:
   a) Click **Add New Disk**.
   b) In **Operation**, select **Clone from Image Service**.
      The startup disk will be cloned from the VM image you uploaded.
c) In **Bus Type**, select **SCSI**.

 ![Bus Type Selection](image)

 d) In **Image**, select **PRIMARY-DISK.qcow2**.

 ![Image Selection](image)

 e) Click **Add**.

    The startup disk is added.

7. **Create a log disk as follows:**

 a) **Click Add New Disk.**

 b) In **Operation**, select **Clone from Image Service**.

    The startup disk will be cloned from the VM image you uploaded.

 c) **Select the desired Bus Type** (for example, SCSI).

 d) In **Image**, select **AUXILIARY-DISK.qcow2**.

 e) **Click Add**.

    The log disk is added.

8. **Add a network interface for the VM:**

 a) In **Network Adapters (NIC)**, click **Add New NIC**.
b) In VLAN Name, select the desired VLAN. You can select DHCP first to check connectivity. We recommend that you change the VLAN to a static IP address later.

c) Click Add.

d) Repeat these substeps to add a second network interface.

XG Firewall requires two network interfaces.

9. Pin the VM to a host:
   a) In VM Host Affinity, click Set Affinity.

b) Select the desired host.

c) Click Save.

10. Click Save.

   The system shows a success message when the VM has been created with no error.

Configure XG Firewall

1. Find your newly created VM in the VM list and power it on.

2. Once it's powered on, click Launch console.
A window opens and shows the command line interface of XG Firewall.

3. Configure XG Firewall.
   a) Enter the administrator password `admin`.
   b) Accept the Sophos end user license agreement.
      The **Main menu** appears.
   c) From the management device, go to the configured IP address.
   d) Select **Start** to open the initial setup wizard and complete the basic configuration.

**CAUTION**
The wizard won't start if you've changed the default password from the CLI console.

You need to activate and register XG Firewall.
4 KVM

You can deploy the XG Firewall virtual appliance on the KVM (Kernel-based Virtual Machine) platform.

**Prerequisites**

- You must have a server with x86 architecture with a recent Linux kernel and one of these processors:
  - Intel processor with VT (virtualization technology) extensions
  - AMD processor with SVM extensions (AMD-V)
- Check if the CPU supports Intel VT or AMD-V, using these commands:
  - Intel VT: `grep --color vmx /proc/cpuinfo`
  - AMD-V: `grep --color svm /proc/cpuinfo`
- Install the virt-manager (Virtual Machine Manager) application on a management device to manage the KVM. For details, go to KVM FAQs.

**Table 3: Minimum hardware requirements**

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>1</td>
</tr>
<tr>
<td>vRAM</td>
<td>4 GB minimum</td>
</tr>
<tr>
<td>vNIC</td>
<td>2</td>
</tr>
<tr>
<td>Primary disk</td>
<td>16 GB minimum</td>
</tr>
<tr>
<td>Report disk</td>
<td>80 GB minimum</td>
</tr>
</tbody>
</table>

If you don’t meet the minimum requirements for new installations of SFOS 18.0, or if you’re migrating from an earlier version, XG Firewall goes into fail-safe mode.

**CAUTION**
Configure the vCPU and vRAM based on the purchased license. Don’t exceed the maximum number of vCPUs specified in the license.

### 4.1 Installing on KVM

You can deploy an XG Firewall QCOW2 disk on KVM platform.

1. Go to XG Firewall free trial and download the .zip file containing the QCOW2 disk. Extract and save the disk on the device that has the virt-manager installed.
2. To connect to the server, open the virt-manager and go to **File > Add Connection**.
3. Enter a name and select the QEMU/KVM connection.
4. To import the XG Firewall image for the primary disk, select the `.qcow2` file and select **Open**.
5. Select the storage location and select **Forward**.
6. Set virtual memory (vRAM) to 4096 MB or higher and CPU to 1.
7. Select the following **Advanced options**:
   a) Network interface of the host device.
   b) Fixed MAC address, if required.
   c) Set **Virt Type** to **kvm**.
   d) Chipset architecture.
   e) Select **Customize configuration before install** and select **Finish**.
8. Specify the advanced settings for **Disk 1** (primary disk):

   **Disk bus**: **Virtio**
   
   **Storage format**: **qcow2**
9. To add the auxiliary disk, go to **Add Hardware** > **Storage**. Under **Select managed or other existing storage**, select the auxiliary disk.
10. To configure the network settings for the appliance, go to **Add Hardware > Network**. Specify the host device, MAC address and device model.
11. To specify the network interface cards.
   
   a) For **Virtual Network Interface (NIC 1)**, set **Device model** to **Hypervisor default**.
b) For Virtual Network Interface (NIC 2), set Device model to Virtio.
12. Select **Begin Installation**.
   XG Firewall will be installed on the server.
13. Configure XG Firewall.
   a) Enter the administrator password `admin`.
   b) Accept the Sophos end user license agreement.
   The **Main menu** appears.
   c) From the management device, go to `https://172.16.16.16`.
   d) Select **Start** to open the initial setup wizard and complete the basic configuration.

**CAUTION**
The wizard won't start if you've changed the default password from the CLI console.

You need to activate and register XG Firewall.
5 Software appliance

You can deploy the XG Firewall software appliance on custom hardware over Windows and macOS systems.

**Prerequisites**

**Table 4: Minimum hardware requirements**

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interface cards</td>
<td>2</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB minimum</td>
</tr>
<tr>
<td>HDD or SSD</td>
<td>10 GB minimum</td>
</tr>
<tr>
<td></td>
<td>64 GB recommended</td>
</tr>
<tr>
<td>USB pen drive</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

If you don't meet the minimum requirements for new installations of SFOS 18.0, or if you're migrating from an earlier version, XG Firewall goes into fail-safe mode.

**CAUTION**

Configure the vCPU and vRAM based on the purchased license. Don't exceed the maximum number of vCPUs specified in the license.

5.1 Installing on Windows

You can deploy an XG Firewall ISO image on a Windows server.

1. Go to XG Firewall free trial and download the XG Firewall software (ISO) image on your computer.
2. Insert a standard USB pen drive that has the specified minimum space. You will need the pen drive to install the ISO.
3. To install the ISO using Windows utility, follow these steps:
   a) Go to Win32 Disk Imager and download Win32 Disk Imager.
   b) Start the utility. The utility looks for IMG files. To allow the utility to find the downloaded ISO file, change the file filter to *. *. Select the **Sophos Firewall ISO** file.
   c) To install the ISO on the pen drive, select the USB pen drive. Installing the ISO will erase the pen drive’s existing data.
4. To install XG Firewall on the server, follow these steps:
   a) For the pen drive to start, you may need to change the BIOS settings.
   b) Connect a monitor, keyboard, and a serial cable to the server.
   c) When the prompt to start installation appears, type y and press Enter. You will receive two prompts.
d) When installation is complete, remove the pen drive and restart the server. A first-time restart will take a few minutes. XG Firewall is installed as a software appliance.

5. Configure XG Firewall.
   a) From the management device, go to https://172.16.16.16.
   b) Select Start to open the initial setup wizard and complete the basic configuration.

   **CAUTION**
   The wizard won’t start if you’ve changed the default password from the CLI console.

You need to activate and register XG Firewall.

### 5.2 Installing on macOS

You can deploy an XG Firewall ISO image on a macOS server.

1. Go to XG Firewall free trial and download the XG Firewall software (ISO) image on your computer.
2. Insert a standard USB pen drive that has the specified minimum space. You will need the pen drive to install the ISO.
3. To install the software on macOS, follow these steps:
   a) Open the disk utility included in macOS.
   b) Locate the pen drive.
   c) Go to **Partitions**, make the following changes and select **Apply**.
      - Volume scheme: 1 partition
      - Format: Free Space
   d) Open a terminal window and go to the ISO location.
   e) To convert the ISO file into a new format, run the command:
      
      ```
      hdiutil convert -format UDRW -o sf.img.dmg SW-SFOS_15.01.0-376.iso
      ```
   f) The converted ISO will be renamed sf.img.dmg.
   g) Run the **diskutil** list and locate the path of the pen drive.
   h) To write the converted ISO to the pen drive, use the following command for reference:
      
      ```
      dd if=./sf.img.dmg of=/dev/rdisk9 bs=1m
      ```
      
      The pen drive’s path is /dev/disk9. Replace this with the path used on your computer.
      - The = path adds an r before the device path name. This is deliberate and enables RAW disk access. If you leave the r out, the process will be slower.
      - For the imaging to work on your system, you may need to run sudo dd <rest of command>.
      
      The process will take a few minutes. When the command prompt appears, you can remove the pen drive.

4. To install XG Firewall on the server, follow these steps:
   a) For the pen drive to start, you may need to change the BIOS settings.
   b) Connect a monitor, keyboard, and a serial cable to the server.
c) When the prompt to start installation appears, type `y` and press Enter.
   You will receive two prompts.

d) When installation is complete, remove the pen drive and restart the server. A first-time restart will take a few minutes.
   XG Firewall is installed as a software appliance.

5. Configure XG Firewall.

   a) From the management device, go to `https://172.16.16.16`.

   b) Select **Start** to open the initial setup wizard and complete the basic configuration.

   **CAUTION**
   The wizard won't start if you've changed the default password from the CLI console.

You need to activate and register XG Firewall.
6 VMware

You can deploy the XG Firewall virtual appliance in a VMware ESX or VMware ESXi environment.

**Prerequisites**

- Install VMware ESX or VMware ESXi 5.0 or later on a server that meets the minimum hardware requirements below.
- Install vSphere Client (VMware management software) on a management device that has network access to the server.

For instructions, go to the vSphere installation and setup guide.

**Table 5: Minimum hardware requirements**

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>1</td>
</tr>
<tr>
<td>vRAM</td>
<td>4 GB minimum</td>
</tr>
<tr>
<td>vNIC</td>
<td>2</td>
</tr>
<tr>
<td>Primary disk</td>
<td>16 GB minimum</td>
</tr>
<tr>
<td>Report disk</td>
<td>80 GB minimum</td>
</tr>
</tbody>
</table>

If you don't meet the minimum requirements for new installations of SFOS 18.0, or if you're migrating from an earlier version, XG Firewall goes into fail-safe mode.

**CAUTION**

Configure the vCPU and vRAM based on the purchased license. Don't exceed the maximum number of vCPUs specified in the license.

### 6.1 Installing on VMware

You can deploy an XG Firewall OVF image in a VMware environment.

1. Go to XG Firewall free trial and download the .zip file containing the XG Firewall OVF image. Extract and save the image on the device that has the vSphere client installed.
2. To deploy the OVF image, follow these steps:
   a) Use the vSphere client to sign in to the VMware host server using its IP address, username, and password.
b) Go to File and select **Deploy OVF Template**.

```
File
    New
    Deploy OVF Template...
    Export
    Report
    Browse VA Marketplace...
    Print Maps
    Exit
```

c) Select the file `sf_virtual` and select **Open**. When the file path opens in the vSphere client, select **Next**.
d) Verify the OVF template details.

e) Specify a name and location for the OVF template.
f) Select the host or cluster within which you want to deploy the OVF template. This image shows deployment on a standalone server. Configuration can differ in cluster environments.

g) Select the storage format to install the OVF template:
   - **Thick Provision Lazy Zeroed**: Space required for the virtual disk is allocated during disk creation. Data remaining on the physical device is not erased during creation, but is zeroed out on demand later on first write from the virtual machine. You can't convert this disk to a thin disk.
Sophos Firewall OS virtual and software appliances

- **Thick Provision Eager Zeroed**: Supports clustering features such as Fault Tolerance (FT). Space required for the virtual disk is allocated at the time of creation. Data remaining on the physical device is zeroed out when the virtual disk is created. May take longer to create disks in this format.

- **Thin Provision**: Minimum space required. Use this format to save storage space.

For details, go to VMware disk provisioning policies.

h) Select the networks to be used by the OVF template.

i) Verify the deployment settings and select **Finish**. XG Firewall will be installed on the server.
3. Configure XG Firewall.
   
a) Right-click XG Firewall. Select **Power** and then select **Power on**.

b) Enter the administrator password **admin**.

c) From the management device, go to **https://172.16.16.16**.

d) Select **Start** to open the initial setup wizard and complete the basic configuration.

**CAUTION**
The wizard won't start if you've changed the default password from the CLI console.
Sophos Firewall OS virtual and software appliances

You need to activate and register XG Firewall.
7 XenApp

You can deploy the XG Firewall virtual appliance on Citrix XenApp platform.

**Prerequisites**

- Install XenServer in your network.
- Install the XenCenter application on a management device to manage the XenServer.

For instructions, go to XenApp quick start guide.

<table>
<thead>
<tr>
<th>Table 6: Minimum hardware requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>vCPU</td>
</tr>
<tr>
<td>vRAM</td>
</tr>
<tr>
<td>vNIC</td>
</tr>
<tr>
<td>Primary disk</td>
</tr>
<tr>
<td>Report disk</td>
</tr>
</tbody>
</table>

If you don't meet the minimum requirements for new installations of SFOS 18.0, or if you're migrating from an earlier version, XG Firewall goes into fail-safe mode.

**CAUTION**

Configure the vCPU and vRAM based on the purchased license. Don't exceed the maximum number of vCPUs specified in the license.

### 7.1 Installing on XenApp

You can deploy an XG Firewall OVF image on the XenApp platform.

1. Go to XG Firewall free trial and download the .zip file containing the XG Firewall OVF image. Extract and save the image on the device that has XenCenter installed.
2. To deploy the OVF image, follow these steps:
   a) Start XenCenter. Select **Import Source** and select the OVF image.
b) Select **Location** to place the virtual machine. Go to **Import VM(s) to** and select the location. Alternatively, you can specify a **Home Server**.

c) Select **Storage** and specify the storage repository in the destination pool.
d) Select **Networking** and select the network interface through which the virtual appliance will connect to the internet.

e) For **OS Fixup Settings**, retain the default selection: **Don't use Operating System Fixup**.
f) Select Transfer VM Settings and specify the network settings.

g) Review the configuration summary.
h) To connect to the appliance, right-click the virtual appliance and select **Start**.
XG Firewall will be installed on the server.

3. Configure XG Firewall.
   a) Enter the administrator password `admin`.
   b) Accept the Sophos end user license agreement.
      The main menu appears.
   c) From the management device, go to `https://172.16.16.16`.
   d) Select **Start** to open the initial setup wizard and complete the basic configuration.

**CAUTION**
The wizard won't start if you've changed the default password from the CLI console.

You need to activate and register XG Firewall.
8 Activating and registering XG Firewall

You can activate XG Firewall and register it.

1. Review and accept the Sophos End User License Agreement (EULA).

2. To register XG Firewall, enter the serial number if you have one. Alternatively, you can start a free trial, which provides a temporary serial number, or skip registration for 30 days. If you’re migrating from UTM 9, you can enter its license.
3. You will be redirected to the MySophos portal. Create a Sophos ID or sign in and complete the registration.

   Once you register, the license is synchronized.

4. Complete the basic setup. Select Continue and complete the configuration through the wizard. When you finish the process, the web admin console appears.
You can configure the other settings, including interfaces, zones, wireless networks, and firewall rules. For details, go to online help.