SOPHOS

Sophos Firewall Deployment Options and Common Scenarios

Sophos Firewall
Version: 19.5v1

[Additional Information]
Sophos Firewall
FW1005: Sophos Firewall Deployment Options and Common Scenarios

November 2022
Version: 19.5v1

Sophos Firewall Deployment Options and Common Scenarios

In this chapter you will learn what platforms can be used to deploy Sophos Firewall, and some of the common ways in which it is deployed.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

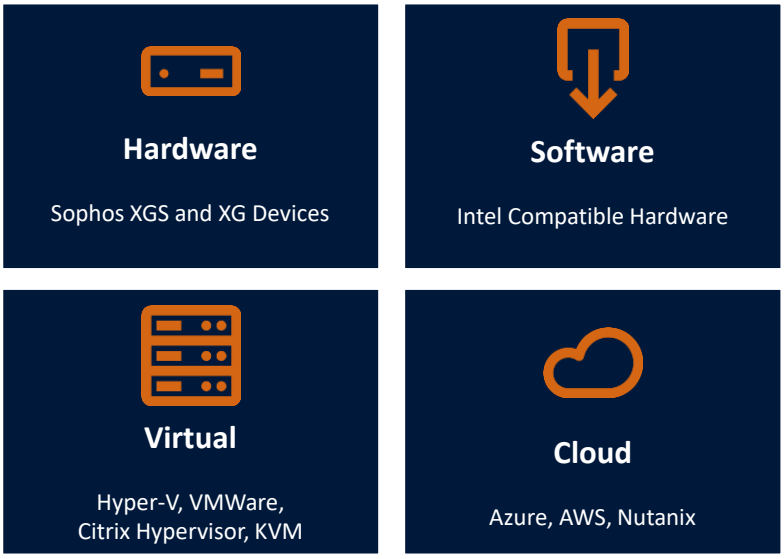
- ✓ How Sophos Firewall acts as a zone-based firewall with identity-based policies
- ✓ The multiple layers of protection provided to detect and block attacks

DURATION

11 minutes

In this chapter you will learn what platforms can be used to deploy Sophos Firewall, and some of the common ways in which it is deployed.

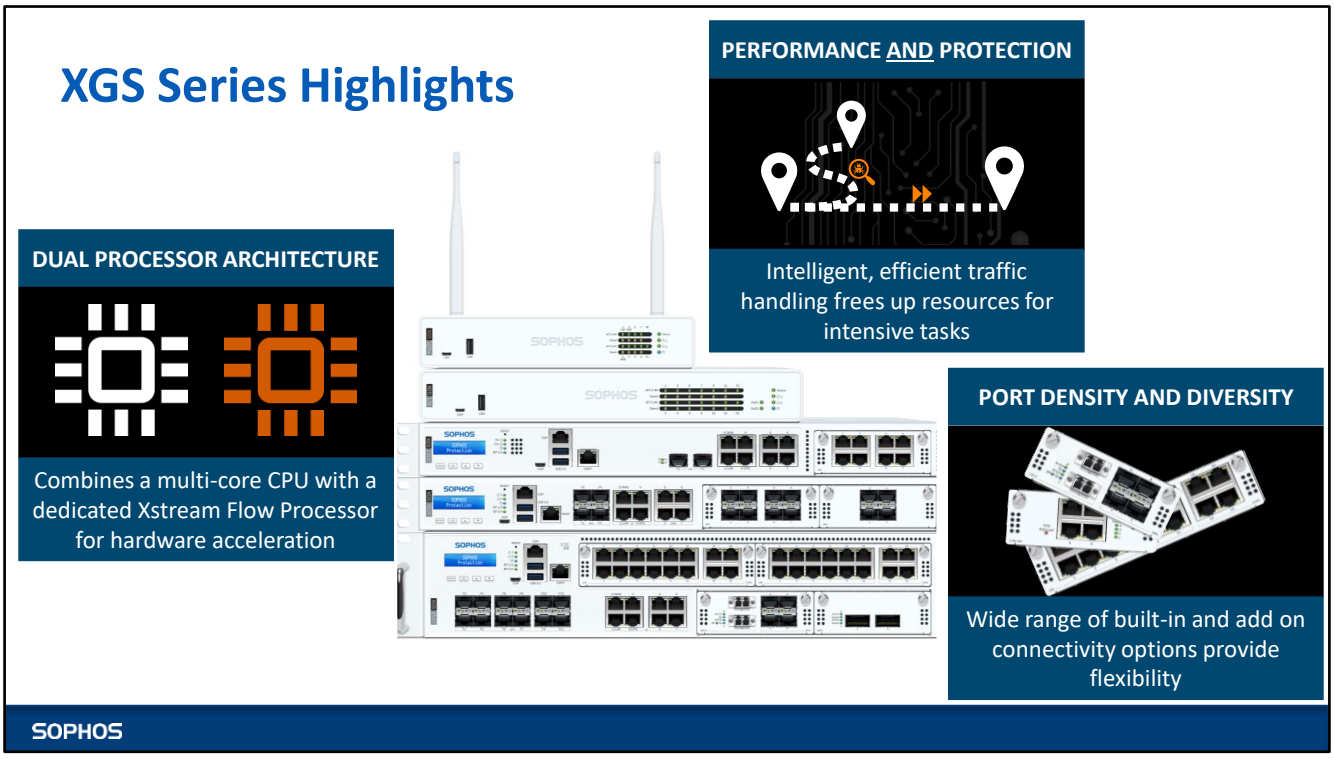
Deployment Options



Sophos Firewall can be deployed in four ways:

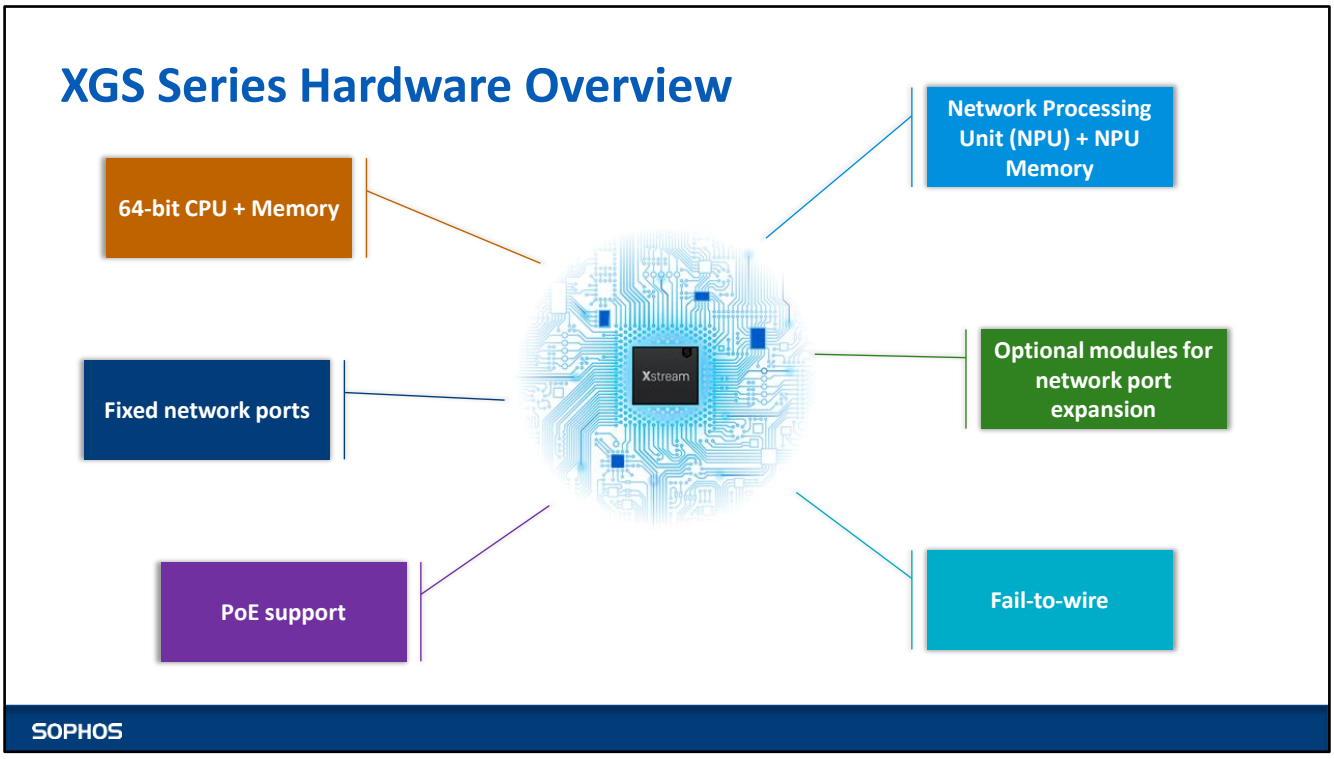
- As a hardware device. Sophos XGS and XG devices come pre-loaded and ready to go
- As software installed onto Intel compatible hardware
- As a virtual device running on the most common hypervisors, including VMware, Citrix Hypervisor, Microsoft Hyper-V and KVM
- And finally, Sophos Firewall can be deployed into the cloud on Azure, Amazon Web Services, and into the Nutanix ecosystem.

However you choose to deploy Sophos Firewall, it uses the same software and provides the same functionality regardless of form-factor.



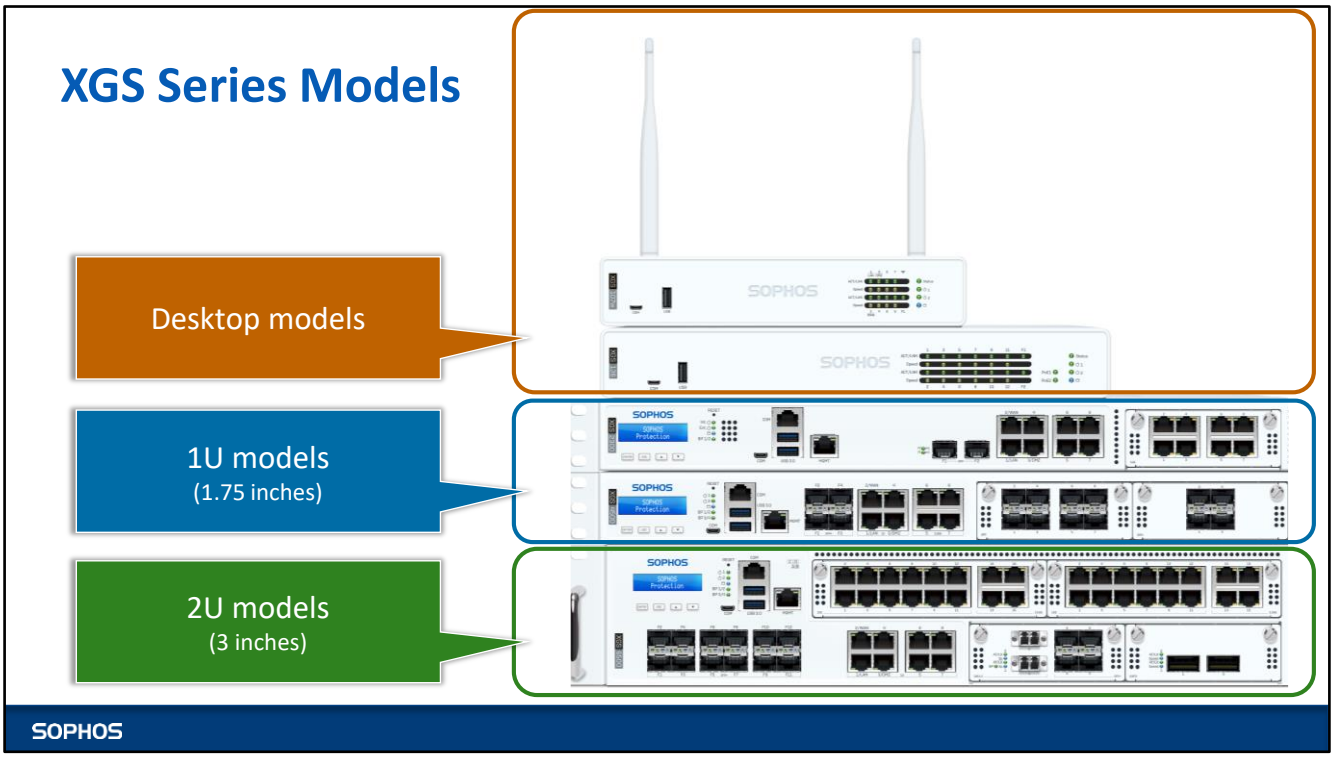
The XGS series of devices for Sophos Firewall provides excellent performance and protection. Intelligent and efficient traffic handling frees up resources for intensive tasks, such as TLS inspection. This is possible with the dual processor architecture, which pairs a multi-core CPU with a dedicated Xstream Flow Processor for hardware acceleration.

The XGS series includes a wide range of built-in and add on connectivity options, providing the flexibility to adapt to most environments.



Each XGS Series unit contains both a 64-bit CPU with system memory as well as a Xstream Flow Processor, also known as a Network Processing Unit or NPU, with its own memory. In addition to the fixed network ports, which increase with the unit model, there are optional modules that provide flexible options for expanding the network port selection.

The XGS Series includes support for PoE, or Power over Ethernet, ports (802.3ad and 802.3at) and fail-to-wire, which can allow traffic to pass through the unit if power is lost. Fail-to-wire and PoE can be available both onboard and with additional modules depending on the unit model.



XGS Series units come in five variants:

- Desktop models, with and without built-in wireless
- 1U server rack models, as short or long devices, with the lower range models being around 10cm less in depth
- And 2U server rack models

All of he 1U and 2U models come with rackmount wings, and either include rails, or have rails as an option. For the desktop models, rackmount wings are optional.

[Additional Information]
https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-firewall-br.pdf

XGS Desktop Models

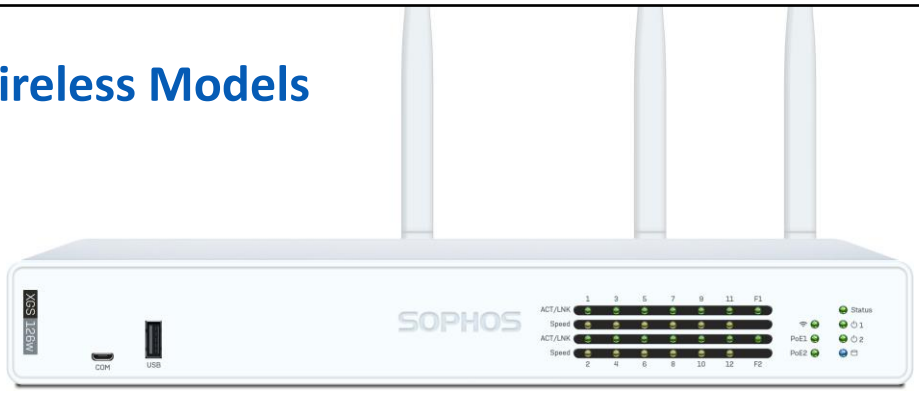
	87/87w	107/107w	116/116w	126/126w	136/136w
CPU (Cores/Threads)	2/2		4/4	2/4	
MEMORY	4 GB			6 GB	8 GB
STORAGE	16 GB	64 GB			
FIXED PORTS	5	9		14	
VDSL SFP MODEM	Optional				
3G/4G MODULE	n/a		Optional		
POWER	Single	Optional Dual PSU			

SOPHOS

All the desktop models are available both with and without wireless built-in and come with a single power supply. All desktop models except the base XGS 87 have the option to plug in a second power supply.

There is an optional user replaceable 3G/4G LTE module available for desktop XGS Series units, except the 87 and 107.

XGS Wireless Models



	87w	107w	116w	126w	136w
ANTENNA	2			3	
RADIOS	1				
STANDARDS	802.11a/b/g/n/ac Dual Band				
OPTIONAL WIRELESS MODULE	n/a		2x2 MIMO 802.11n/ac Dual Band		

SOPHOS

The wireless desktop models all have a single 802.11a/b/g/n/ac dual band radio. As there is only a single radio, these can only broadcast on either 2.4Ghz or 5Ghz, not both simultaneously.

The XGS 116w, 126w, and 136w also have the option for a second wireless module that is 802.11n/ac dual band. This addition allows the device to broadcast on both 2.4Ghz and 5Ghz band simultaneously and provide better coverage.

XGS 1U Models

XGS 3100

XGS 4300

	2100	2300	3100	3300	4300	4500
CPU (Cores/Threads)	2/4	2/4	4/4	4/8	6/12	8/16
MEMORY	8 GB		12 GB	16 GB	32 GB	
STORAGE	120 GB		240 GB			2 x 240 GB SW RAID
FIXED PORTS	10		12			
FLEXIPORT BAYS	1				2	
POWER	Optional External PSU					Optional Hot Swappable PSU

SOPHOS

The XGS Series 1U devices all include an Ethernet management port that allows you to connect to the WebAdmin on https://10.0.1.1:4444. All 1U devices have an optional external PSU that can be mounted on the back of the unit so as not to take up additional rack space, except the XGS 4500, which has an optional internal hot swappable PSU. 1U devices also include either 1 or 2 FlexiPort bays.

XGS 2U Models

XGS 5500

XGS 6500

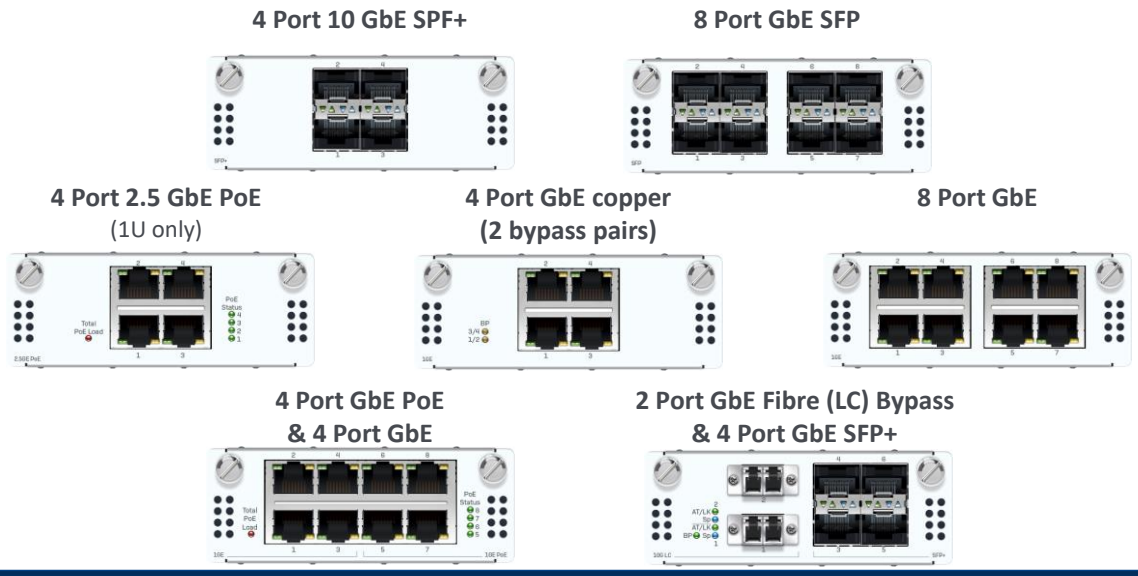
	5500	6500
CPU (Cores/Threads)	16/32	24/48
MEMORY	64 GB	80 GB
STORAGE	2 x 480 HW RAID	2 x 480 HW RAID
FIXED PORTS	16	20
FLEXIPORT BAYS	2	
NIC EXPANSION BAYS	1	2
POWER	2	2

SOPHOS

The largest XGS Series 2U units include hardware RAID storage, 2 FlexiPort bays and 2 internal hot swappable power supplies.

These units also include 1 or 2 NIC expansion bays, that can be used to add a module that has 4 x 2.5 GbE ports and 12 x GbE ports .

FlexiPort Modules



SOPHOS

Here you can see the FlexiPort modules that are available for the 1U and 2U models, apart from the 4 port 2.5 GbE PoE, which is only available of the 1U models.

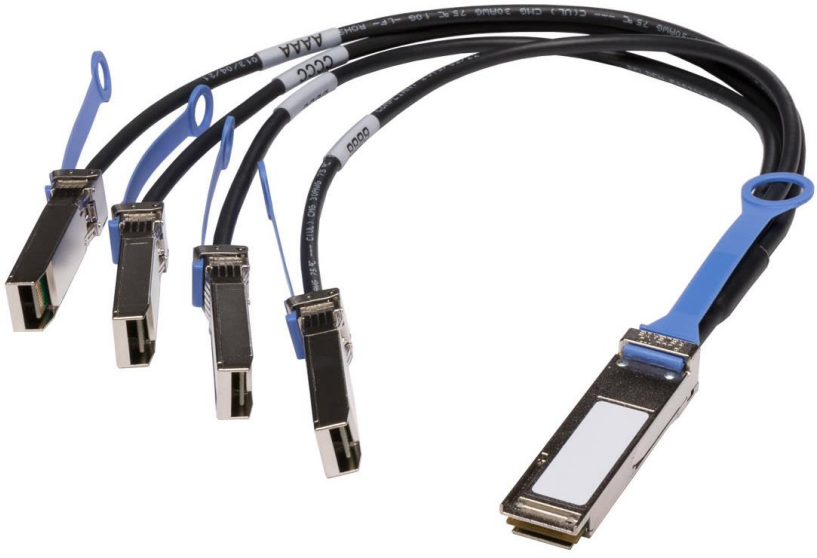
There are three other FlexiPort modules available only for the 2U devices:

- 8 port 10GbE SFP+
- 2 port 10 GbE fiber (LC) Bypass & 4 port 10 GbE SFP+
- 2 port 40 GbE QSFP+

Additionally, there is a VSDL SFP for all models that allows you to connect a DSL modem via SFP.

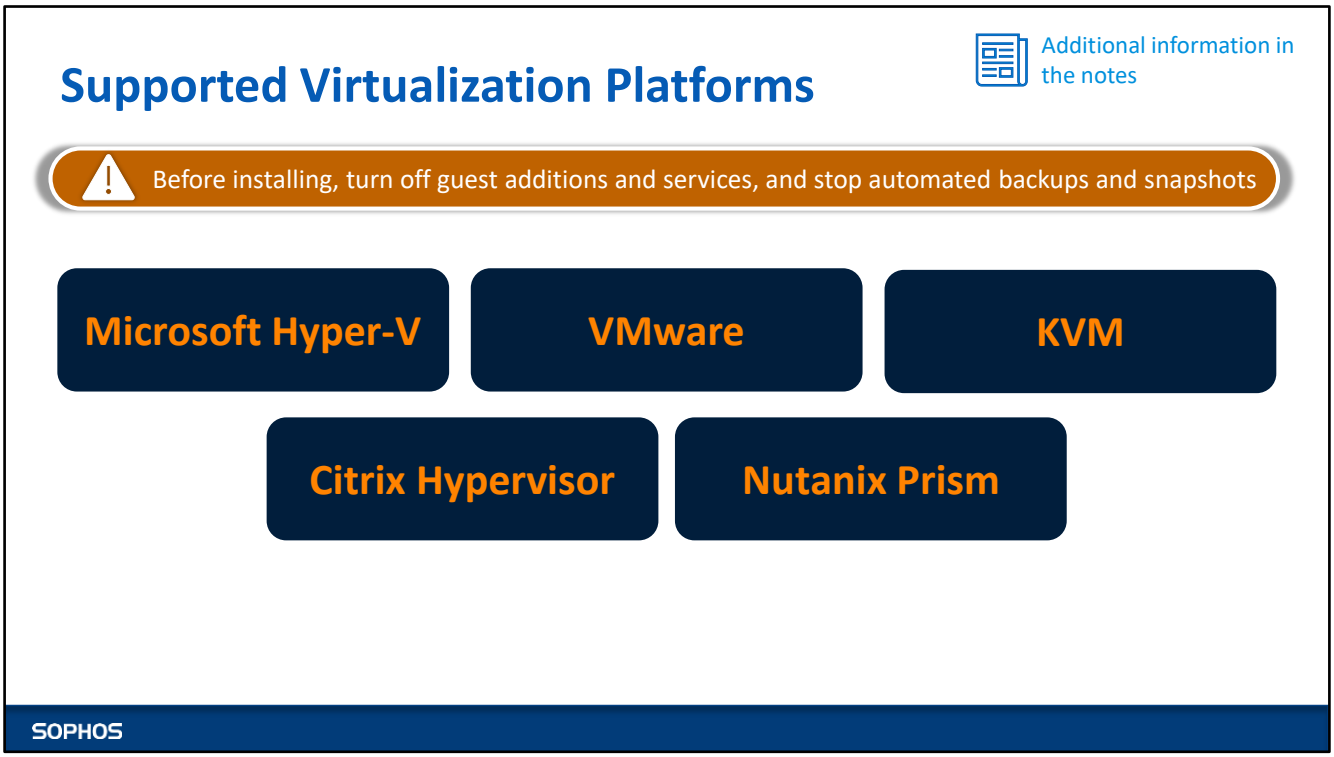
Please note that FlexiPorts modules are not hot swappable and require the device to be powered off to install.

Breakout Interface Support



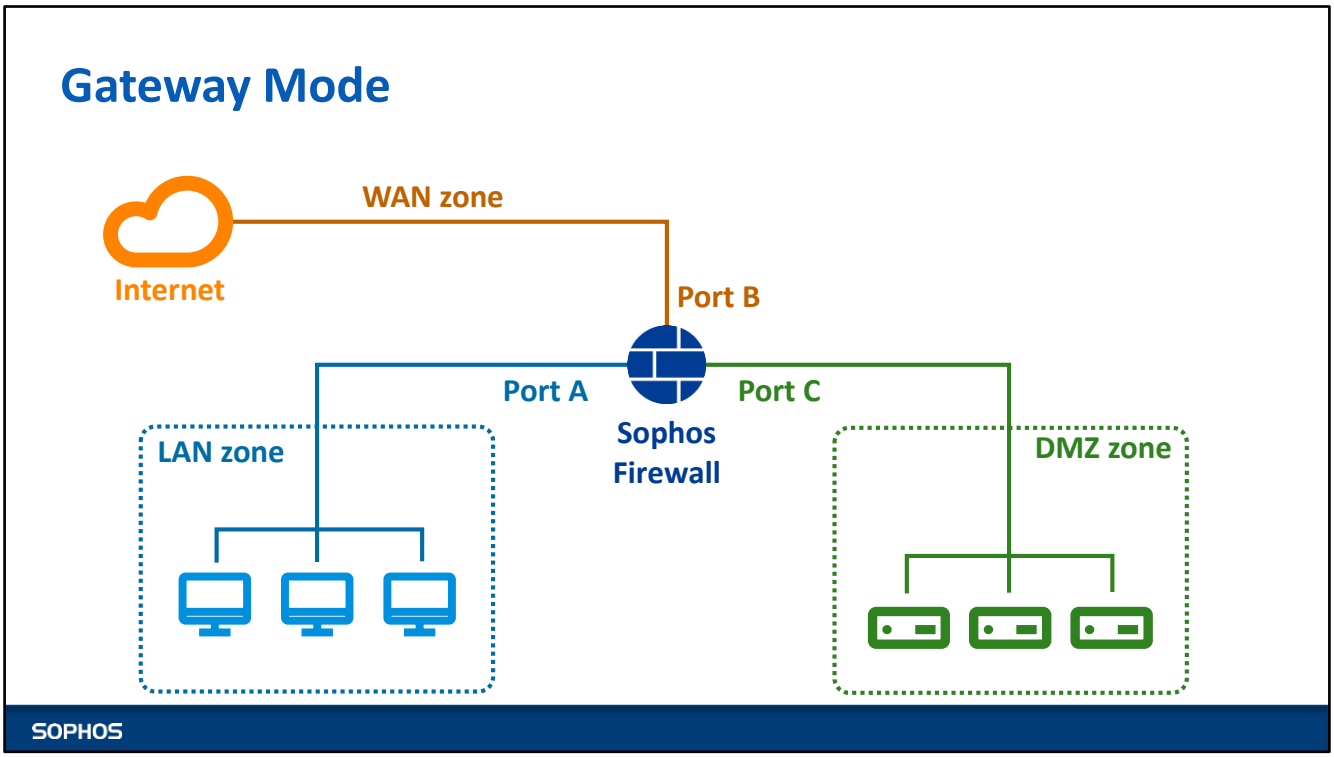
SOPHOS

Sophos Firewall supports breakout cables for 40 gigabit interfaces, splitting them into 10 gigabit interfaces using DAC or fiber breakout cables.



It is important to install Sophos Firewall on one of the supported virtualization platforms and their tested versions shown in the online help. These platforms have been tested and are known to work with the Sophos Firewall Operating System (SFOS).

[Additional Information]
Sophos Firewall: Supported virtualization platforms:
https://docs.sophos.com/nsg/sophos-firewall/19.5/Help/en-us/webhelp/onlinehelp/VirtualAndSoftwareAppliancesHelp/vs_VirtualSoftwareApplianceIntro/index.html

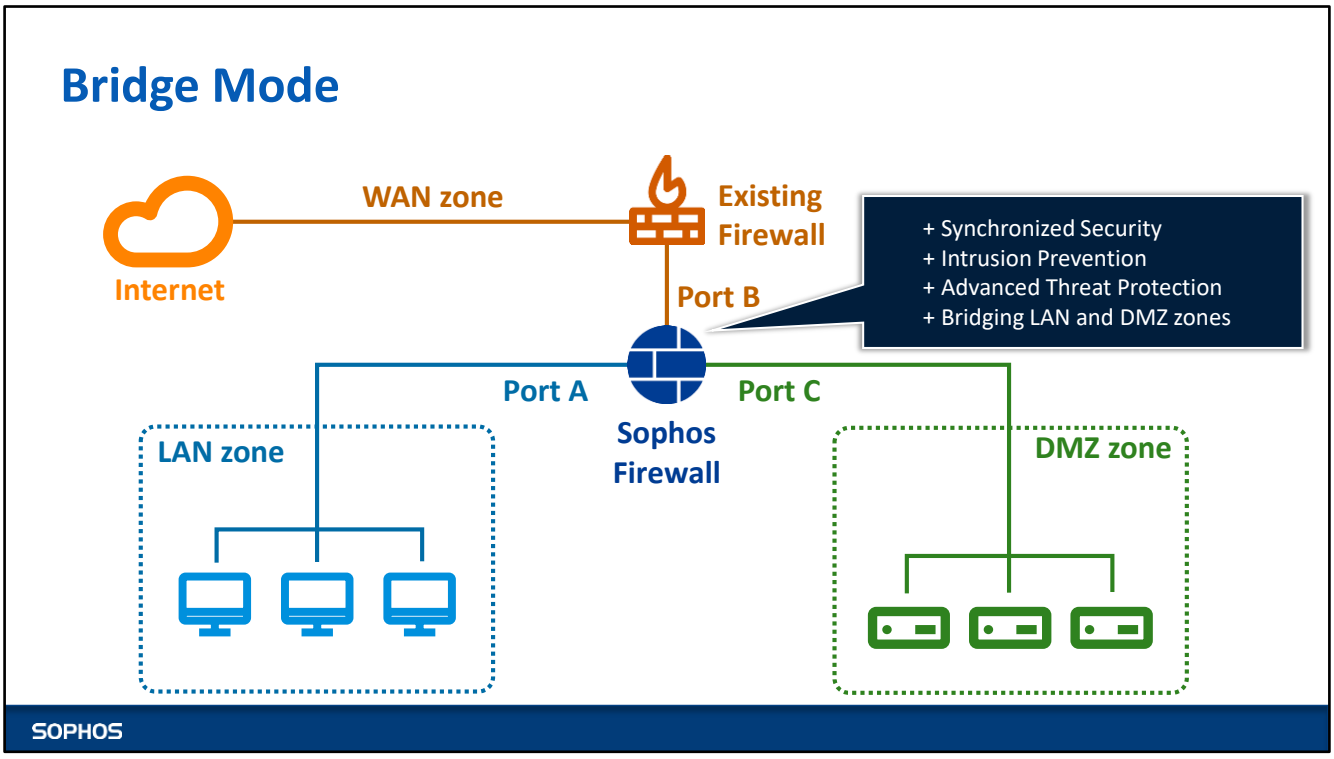


Let’s take a minute to look at some of the most common ways Sophos Firewall is deployed.

The most common scenario is where you are looking to replace an aging firewall and need to protect your internal network. Sophos Firewall is deployed to handle both the core routing and as the first-line of defense against network threats.

This is shown here with Sophos Firewall in gateway mode. Port A is configured for the LAN zone, Port B for the WAN, and Port C for the DMZ. Any network threats trying to go to either the LAN or the DMZ zone will be stopped by the firewall.

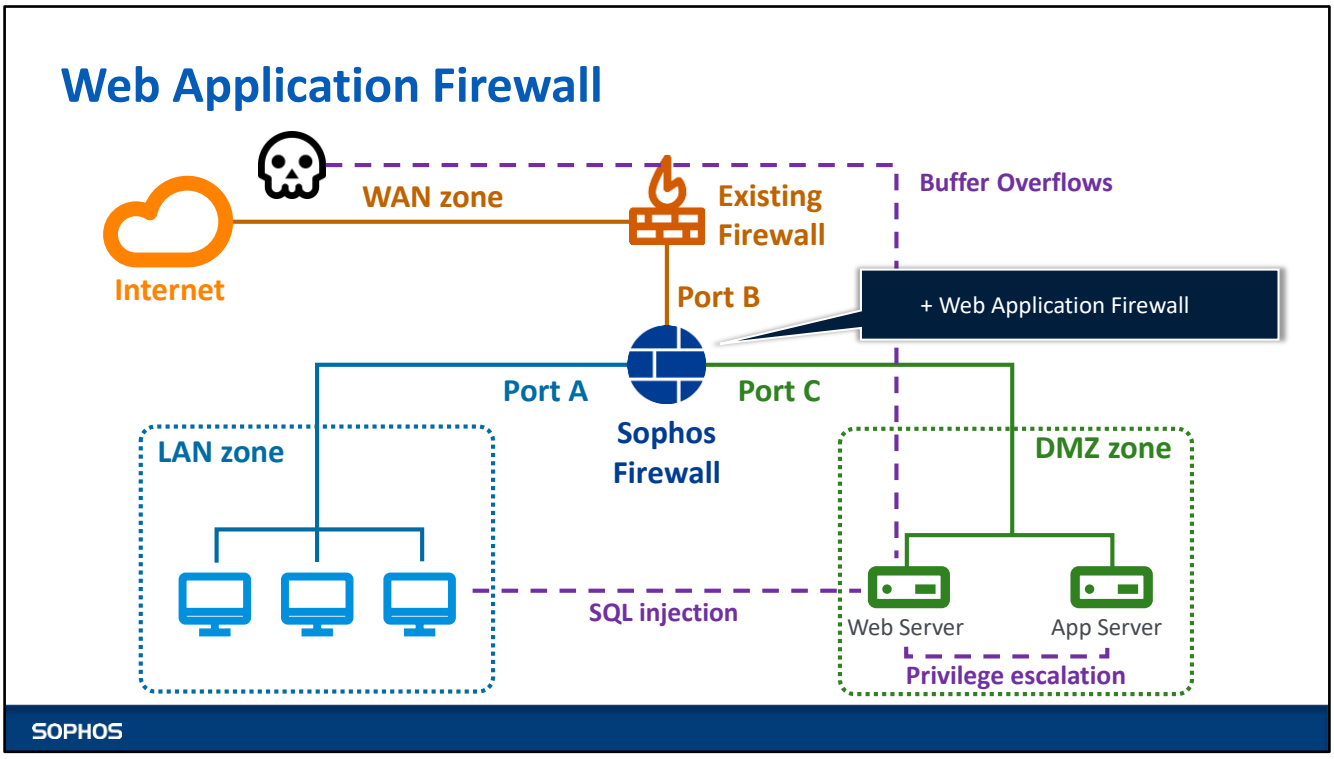
This is the type of deployment we will be focusing on in this course.



Another common type of deployment is where there is an existing firewall that handles the WAN connectivity that is not going to be replaced. This is often done to add additional protection capabilities not offered by the existing firewall.

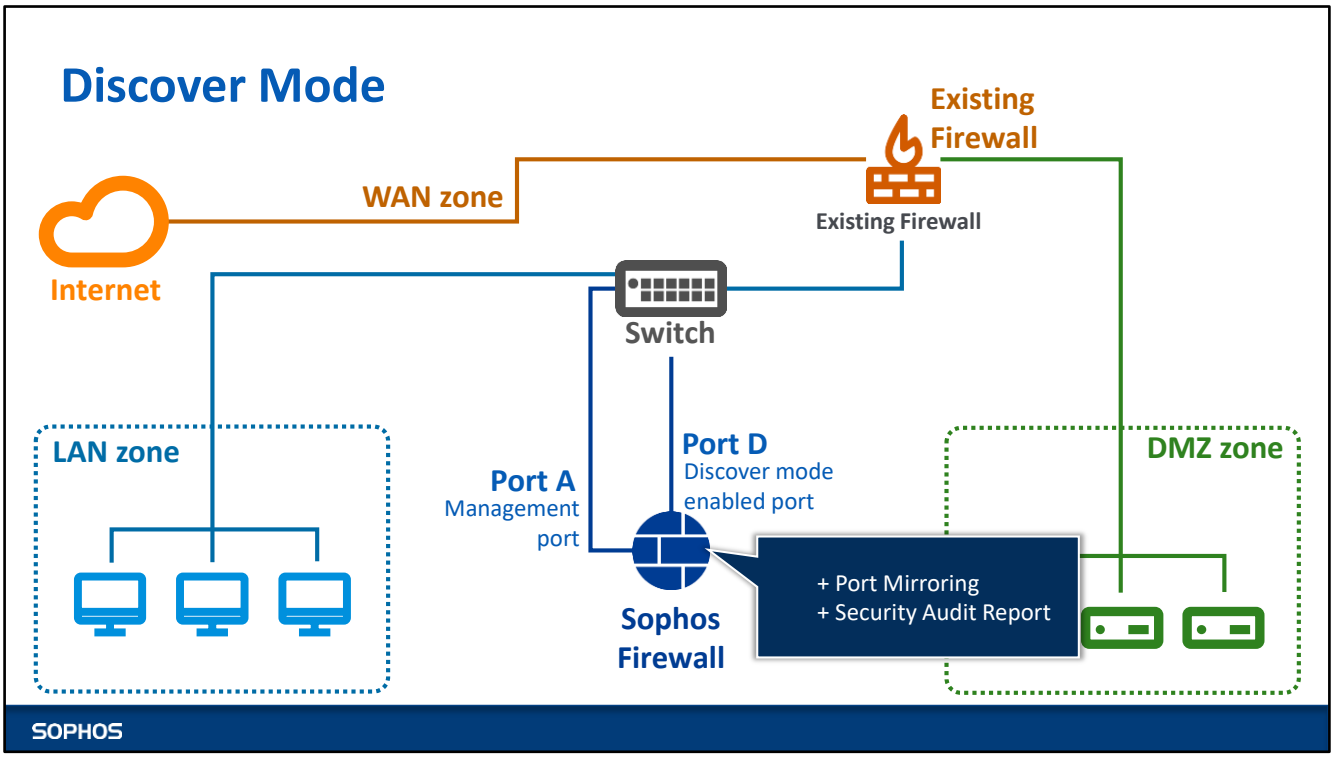
So that you do not need to change the IP address schema of the network, Sophos Firewall can be deployed in bridge mode, which is also known as transparent mode or inline mode.

In this mode the clients on the network are unaware of the Sophos Firewall and traffic passes through without the IP address being changed, but still allowing Sophos Firewall to scan for and protect against threats.



Sophos Firewall may also be added to a network to protect web applications. There are often many components that make up a web application, including web servers, databases, file servers and so forth, but this means that there are also a wide range attacks that can be launched at them.

In the example here, the Sophos Firewall can protect the web application from common attacks including buffer overflows and SQL injection.

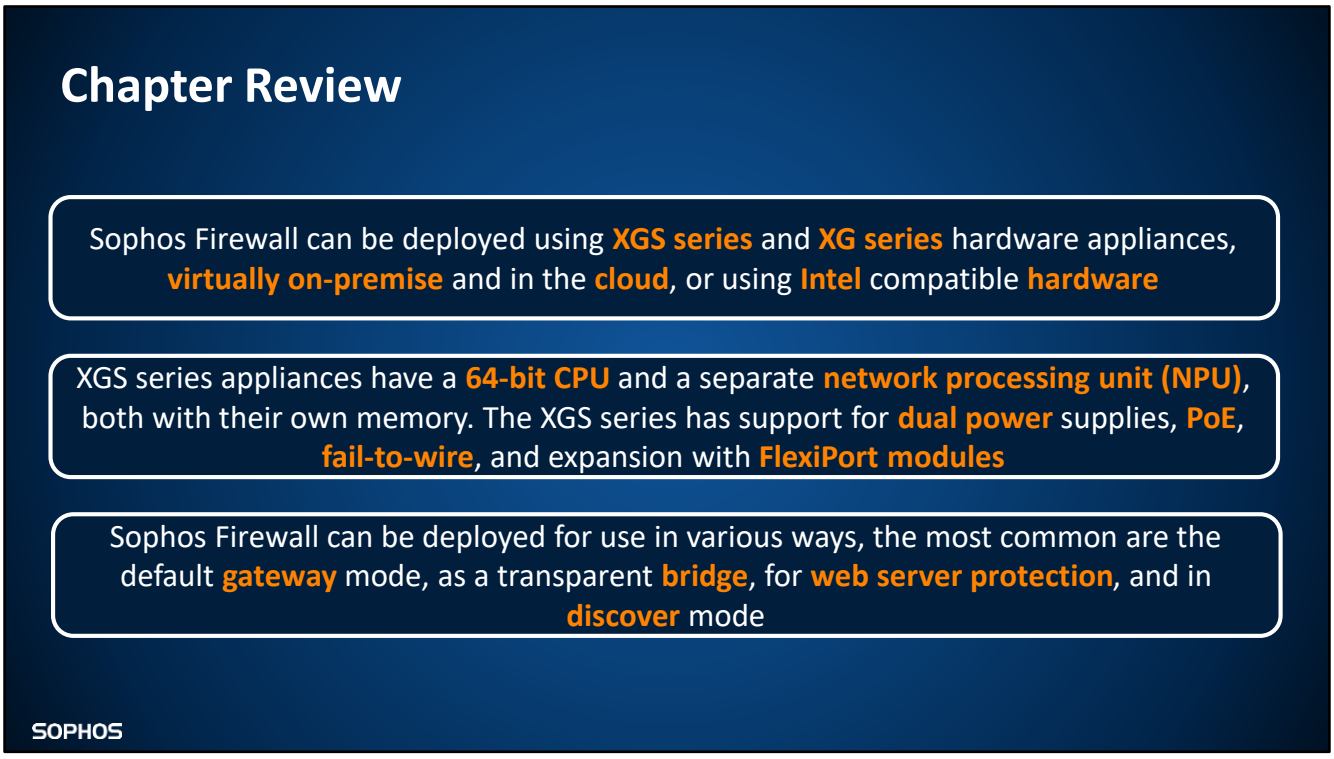


The last type of deployment we will look at is generally used for evaluating the capabilities of Sophos Firewall without the need to make any changes to the network.

In this example, the Sophos Firewall is connected to a port on the switch that has port mirroring enabled, so that a copy of all the traffic is sent to the Sophos Firewall.

While the Sophos Firewall cannot influence the live traffic on the network, it can log and report on what is sees, and from this you can see the additional protection it can add to the network.

This is called discover mode.



Here are the three main things you learned in this chapter.

Sophos Firewall can be deployed using XGS series and XG series hardware appliances, virtually on-premise and in the cloud, or using Intel compatible hardware.

XGS series appliances have a 64-bit CPU and a separate network processing unit (NPU), both with their own memory. The XGS series has support for dual power supplies, PoE, fail-to-wire, and expansion with FlexiPort modules.

Sophos Firewall can be deployed for use in various ways, the most common are the default gateway mode, as a transparent bridge, for web server protection, and in discover mode.


SOPHOS
Cybersecurity evolved.