SOPHOS

Sophos Firewall and SD-WAN

Contents

Introduction

Few terms in networking have generated as much buzz as SD-WAN (or Software Defined Networking in a Wide Area Network). All that buzz has been accompanied by equal doses of useful information and confusing rhetoric. As a result, SD-WAN has grown to mean different things to different people, while some are still trying to figure out exactly what it means.

Fundamentally, SD-WAN is often about achieving one or more of these four networking objectives:

‣ **Reduce connectivity costs:** Traditional MPLS (Multi-Protocol Label Switching) connections are expensive so organizations are shifting to more affordable broadband WAN options such as cable, DSL, and 3G/4G/LTE

‣ **Business continuity:** Organizations require solutions that provide redundancy, routing, failover, and session preservation in the event of a WAN failure or outage

‣ **Quality of critical applications:** Organizations are seeking real-time visibility into application traffic and performance in order to maintain session quality of mission-critical business apps

‣ **Simpler branch office VPN orchestration:** VPN orchestration between locations is often complex and time consuming, which is why having the tools to simplify and automate deployment and setup is critical

When considering an SD-WAN solution, it's very important to understand and prioritize your desired goals and objectives before diving into any particular solutions or features.

SD-WAN Features in Sophos Firewall

Sophos Firewall integrates the essential SD-WAN features and capabilities most organizations need to achieve their desired goals. In this section, we'll have a look at the SD-WAN capabilities of Sophos Firewall.

WAN Links

We'll start with the fundamentals of WAN connectivity: flexible ISP and WAN connectivity, as well as redundancy and failover in the event of an outage, are important considerations.
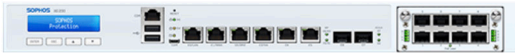
Firewall offers support for multiple WAN links, including a variety of copper, fiber, and even cellular interface options. It can terminate MPLS circuits using ethernet handoff and VDSL through our optional SPF modem.

Firewall also offers essential WAN link monitoring, balancing, and failover capabilities.

Firewall WAN Link Status is shown in the bottom of this interface status widget available via the dashboard.

Sophos Firewall WAN Link Management, including balancing and failover rules.

Branch Office Connectivity

Another core component of SD-WAN is the ability to connect remote and branch locations with the central headquarters for the purpose of sharing data, enabling transactions, and delivering cloud applications.

Features such as affordable, flexible, and zero-touch or low-touch deployment are very desirable in order to make this as painless and cost-effective as possible, while still supporting a variety of enterprise connectivity requirements.
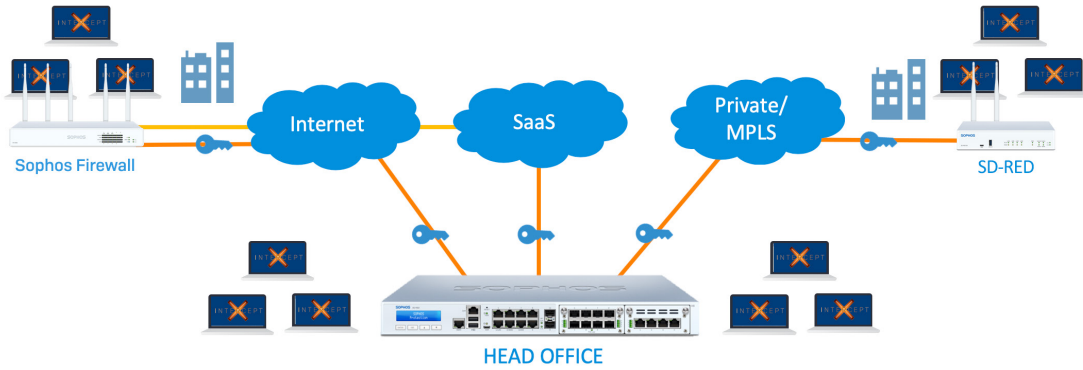
Sophos Firewall and SD-RED devices offer tunnel options to simply and affordably connect branch offices via SD-WAN.

Sophos has long been a pioneer in the area of zero-touch branch office deployment and connectivity with our unique SD-RED devices. These affordable devices are extremely easy for a non-technical person to deploy, and provide a robust secure Layer 2 tunnel between the device and a central Firewall.
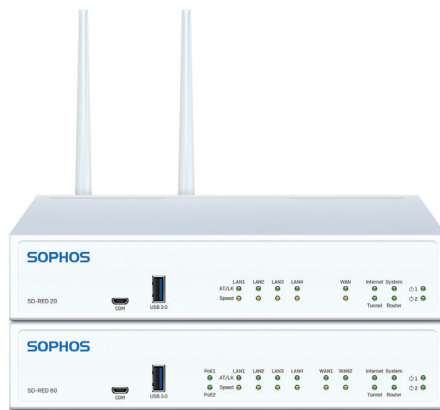
Sophos SD-RED devices offer an affordable, zero-touch solution to SD-WAN branch connectivity.

Deploying SD-RED devices couldn't be easier: You simply note the serial number of the device in your Firewall, and ship the device to the remote location. Any non-technical person at the remote site simply connects the device and it will contact our cloud-provisioning service automatically to establish a secure tunnel connection with your Sophos Firewall.

Interfaces	Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement	Cellular WAN	IP tunnels	Neighbors (ARP-NDP)	Dynamic DNS

RED settings

Branch name *	
Type	RED 15
RED ID *	
Tunnel ID *	Automatic
Unlock code *	
Firewall IP/hostname *	
2nd firewall IP/hostname	
Use 2nd IP/hostname for	◉ Failover ○ Load balancing
Description	
Device deployment	◉ Automatically via provisioning service ○ Manually via USB stick

Uplink settings

Uplink connection	◉ DHCP ○ Static
3G/UMTS failover	☐ Enable

RED network settings

RED operation mode	◉ Standard/unified ○ Standard/split ○ Transparent/split
RED IP *	
RED netmask	/24 (255.255.255.0)
Zone	LAN
Configure DHCP	ON
RED DHCP range	
MAC filtering type	No configured MAC address lists found
Tunnel compression	☐ Enable
RED MTU	1500 [576 to 1500]

Save   Cancel

Sophos SD-RED offers a flexible, secure, and affordable SD-WAN branch office connectivity solution.

Our desktop XGS Series appliances also make excellent branch office SD-WAN connectivity solutions with flexible connectivity options including VDSL and cellular in addition to copper and fiber interfaces, and support for our robust SD-RED tunnels.
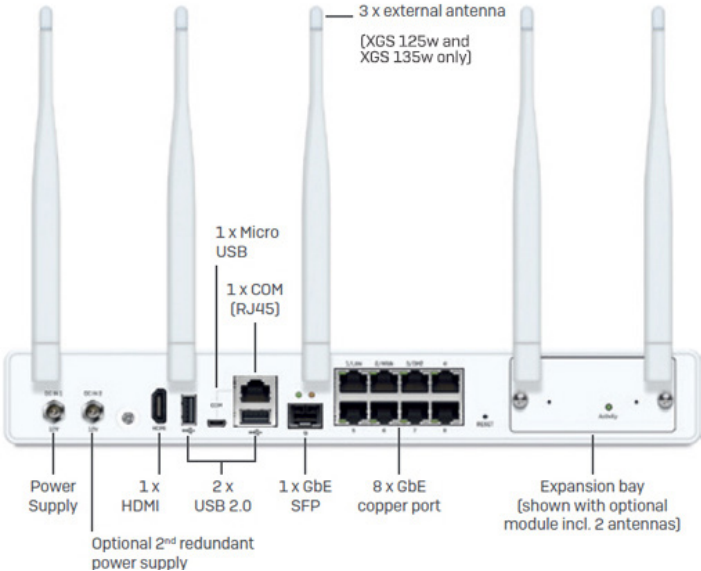

Select desktop models like the XGS 135w shown here come with options for LTE/cellular, VDSL, copper, or fiber WAN connectivity options.

VPN Support and Orchestration

Other important capabilities for achieving many SD-WAN objectives are robust VPN support and centralized VPN orchestration.

Sophos Firewall supports all the standard site-to-site VPN options you expect, including IPSec and SSL. We even offer our own unique SD-RED Layer 2 tunnel with routing that's extremely robust and proven reliable in high-latency situations such as over satellite links.

Sophos Firewall Manager and Central Firewall Manager provide centralized multi-site VPN orchestration tools to easily set up a mesh of VPN SD-WAN connections.
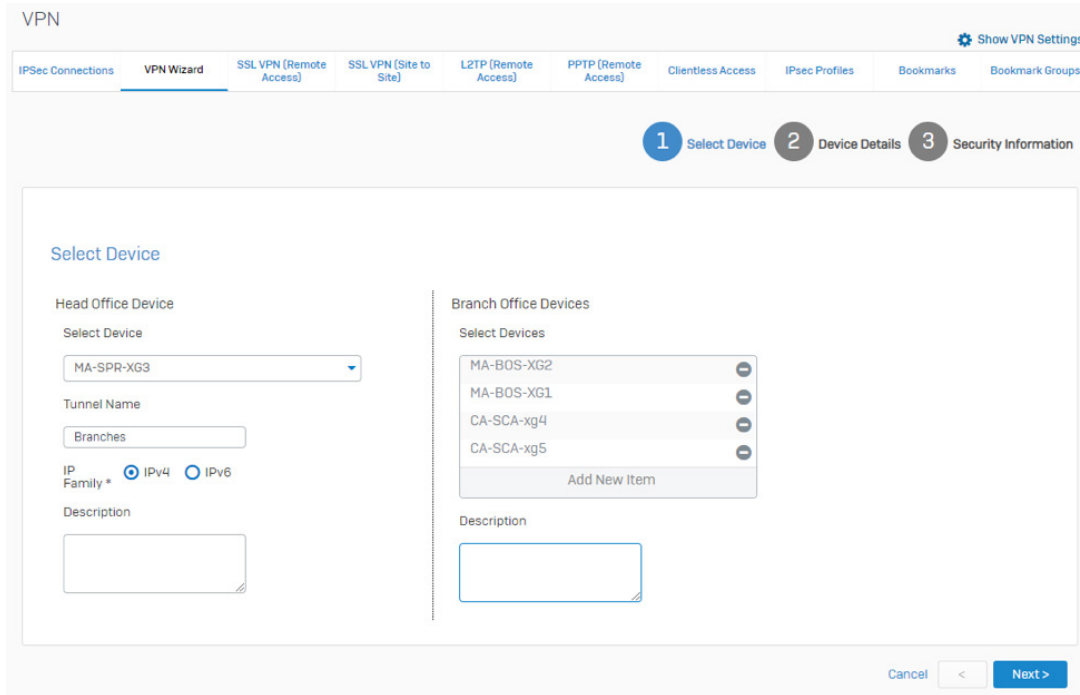
Sophos Firewall Manager VPN Orchestration Wizard.

Sophos Firewall also offers a flexible failback option for automatic failback to the primary VPN connection when a WAN link is restored.

IPsec connections	SSL VPN (remote access)	SSL VPN (site-to-site)	Sophos Connect client	L2TP (remote access)	Clientless access	Bookmarks	Bookmark groups	PPTP (remote access)	IPsec policies

Connection group details

Name * [Enter Name]

Select connection(s)

Available connections   Member connections   Order of connections in "Member connections" column indicates failover preference

[type to search...]

No record

Mail notification   ☐ Enable

Automatic failback   ☑ Enable

Failover condition

If ...

  Not able to **Connect *** [PING] **Port** [ ]

And

  Not able to **Connect** [Select] **Port** [ ]

  on Remote VPN server

Then

  "SHIFT to next active connection"

Sophos Firewall IPSec VPN failover and automatic failback options.

Application Visibility and Routing

Another important feature for achieving certain SD-WAN objectives is application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP.

Of course, you can't route what you can't identify, so accurate, reliable application identification and visibility is critical. This is one area where Sophos Firewall and Sophos Synchronized Security provide an incredible advantage. Synchronized Application Control provides 100% clarity and visibility into all networked applications, providing a significant advantage in identifying mission-critical applications, especially obscure or custom applications.

Synchronized SD-WAN, a Synchronized Security feature, offers additional benefits with SD-WAN application routing. Synchronized SD-WAN leverages the added clarity and reliability of application identification that comes with the sharing of Synchronized Application Control information between Sophos-managed endpoints and Sophos Firewall. Now, previously unidentified applications can also be added to SD-WAN routing policies, providing a level of application routing control and reliability that other firewalls can't match.

Synchronized Application Control identifies 100% of all networked applications, making it easy to prioritize and route mission critical applications.

Sophos Firewall also enables application-based routing and path selection in every firewall rule, including by user and group. Granular policy-based routing (PBR) controls provide the ability to define routing through either the primary or backup gateway WAN connection and configure for replay direction. Together, these features make it easy to direct important application traffic out the optimal WAN interface.

Sophos Firewall and SD-WAN

SD-WAN policy-based routing provides flexible tools for routing critical application traffic.

Sophos Firewall also includes predefined Fully Qualified Domain Name (FQDN) objects for popular SaaS cloud services, with thousands of FQDN hosts definitions included right out of the box and the option to easily add more.

Pre-defined FQDN Host Objects simplify path selection and application-based routing.

Summary and What's Next

Sophos Firewall includes many innovative solutions to help organizations reach their SD-WAN objectives, from great WAN connectivity options to our unmatched application visibility and great routing options to our unique SD-RED edge appliances.

Sophos Firewall SD-WAN capabilities:

‣ **Multiple WAN link options** with MPLS (ethernet handoff), VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, and failover

‣ **A pioneer in branch office SD-WAN** connectivity with our SD-RED zero-touch deployment devices and robust VPN, as well as our innovative XGS Series desktop models

‣ **Excellent VPN support** for IPSec, SSL, SD-RED secure L2 w/routing, and central multi-site VPN orchestration via SFM or CFM

‣ **Unique application control and visibility** with Synchronized App Control, and cloud app visibility with live connection monitoring and bandwidth utilization, plus out-of-the-box support for major cloud applications

‣ **Application routing** over preferred links via firewall rules or policy-based routing

Sophos continues to invest in SD-WAN capabilities in upcoming Sophos Firewall releases, including enhancements to link monitoring and selection, new SD-RED devices, zero-touch firewall, and VPN orchestration tools in Sophos Central.

Sophos Firewall offers a powerful, flexible network connectivity and security solution for every type of network. Read our Firewall Solution Brief to see how Sophos Firewall is solving today's top problems with network protection, providing the best firewall visibility, protection, and response in the industry.

SOPHOS