SOPHOS

PURECLOUD

Sophos Firewall and SD-WAN

Sophos Whitepaper April 2021

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

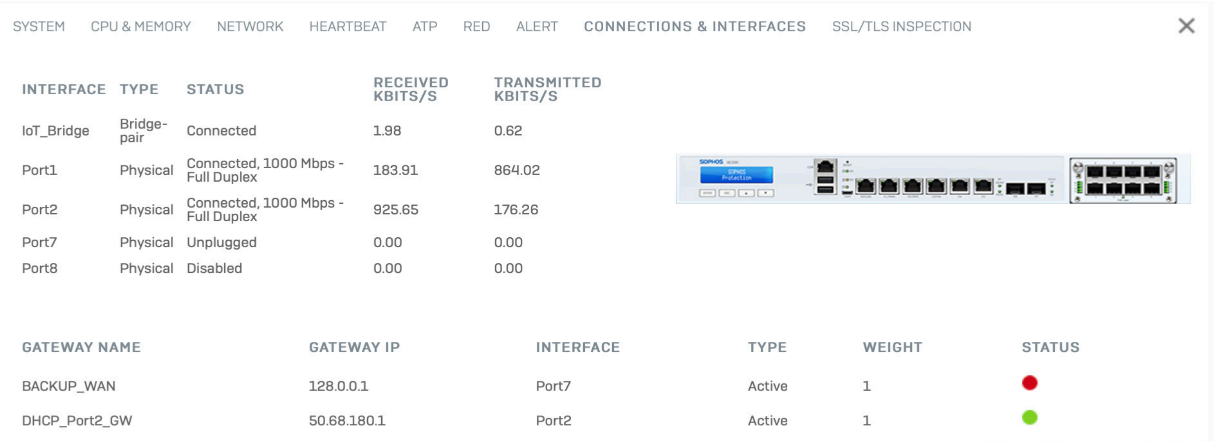
Sophos Firewall integrates the essential SD-WAN features and capabilities most organizations need to achieve their desired goals. In this section, we'll have a look at the SD-WAN capabilities of Sophos Firewall.

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.

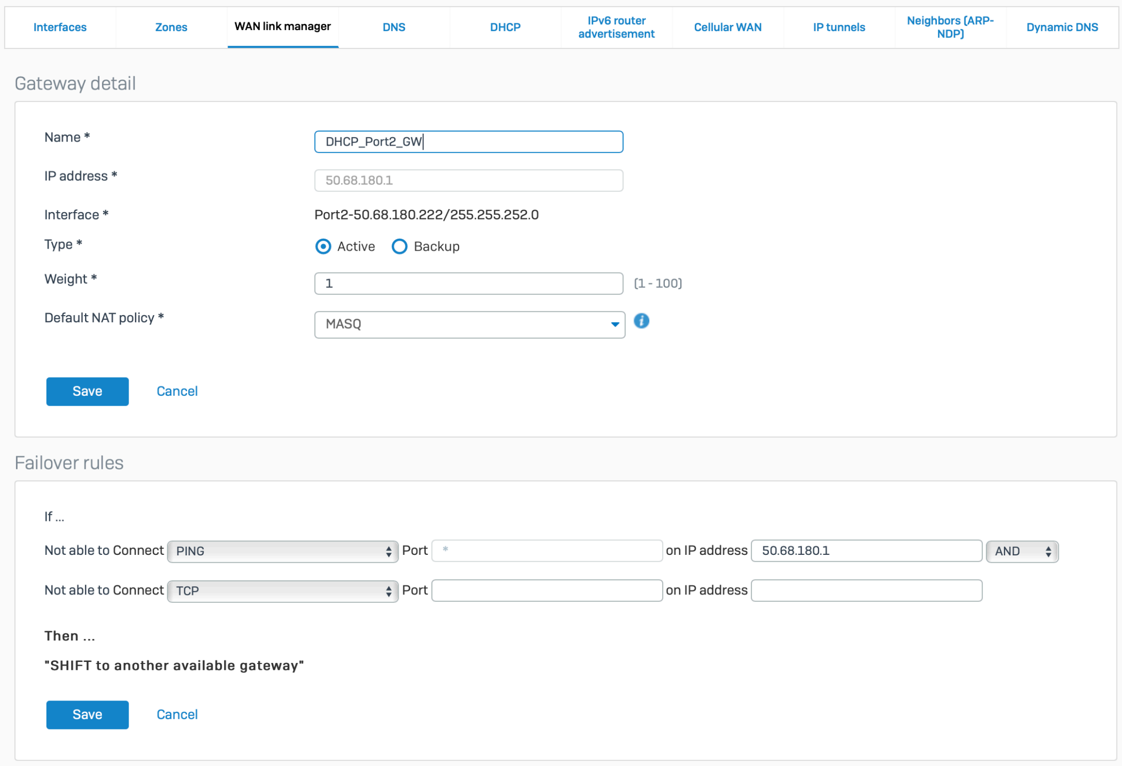
Firewall also offers essential WAN link monitoring, balancing, and failover capabilities.



INTERFACE	TYPE	STATUS	RECEIVED KBITS/S	TRANSMITTED KBITS/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	176.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

GATEWAY NAME	GATEWAY IP	INTERFACE	TYPE	WEIGHT	STATUS
BACKUP_WAN	128.0.0.1	Port7	Active	1	●
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	●

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



Gateway detail

Name * DHCP_Port2_GW

IP address * 50.68.180.1

Interface * Port2-50.68.180.222/255.255.252.0

Type * ● Active ○ Backup

Weight * 1 (1 - 100)

Default NAT policy * MASQ

Save Cancel

Failover rules

If ...

Not able to Connect PING Port * on IP address 50.68.180.1 AND

Not able to Connect TCP Port on IP address

Then ...

"SHIFT to another available gateway"

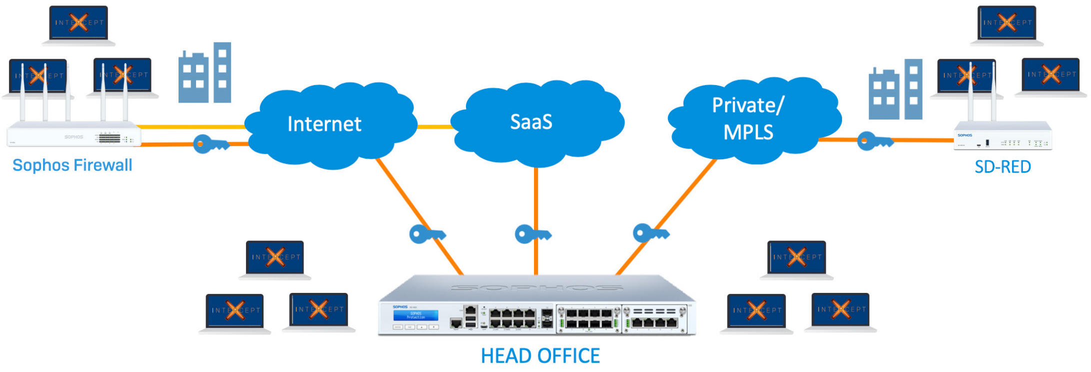
Save Cancel

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

Branch Office Connectivity

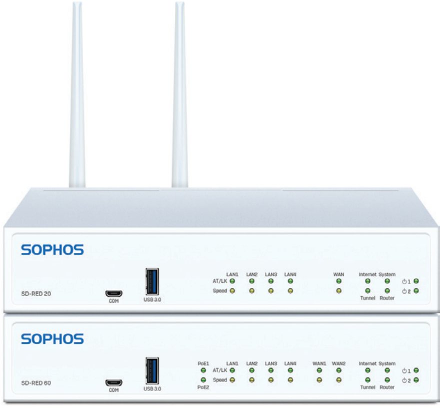
Another core component of SD-WAN is the ability to connect remote and branch locations with the central headquarters for the purpose of sharing data, enabling transactions, and delivering cloud applications.

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.



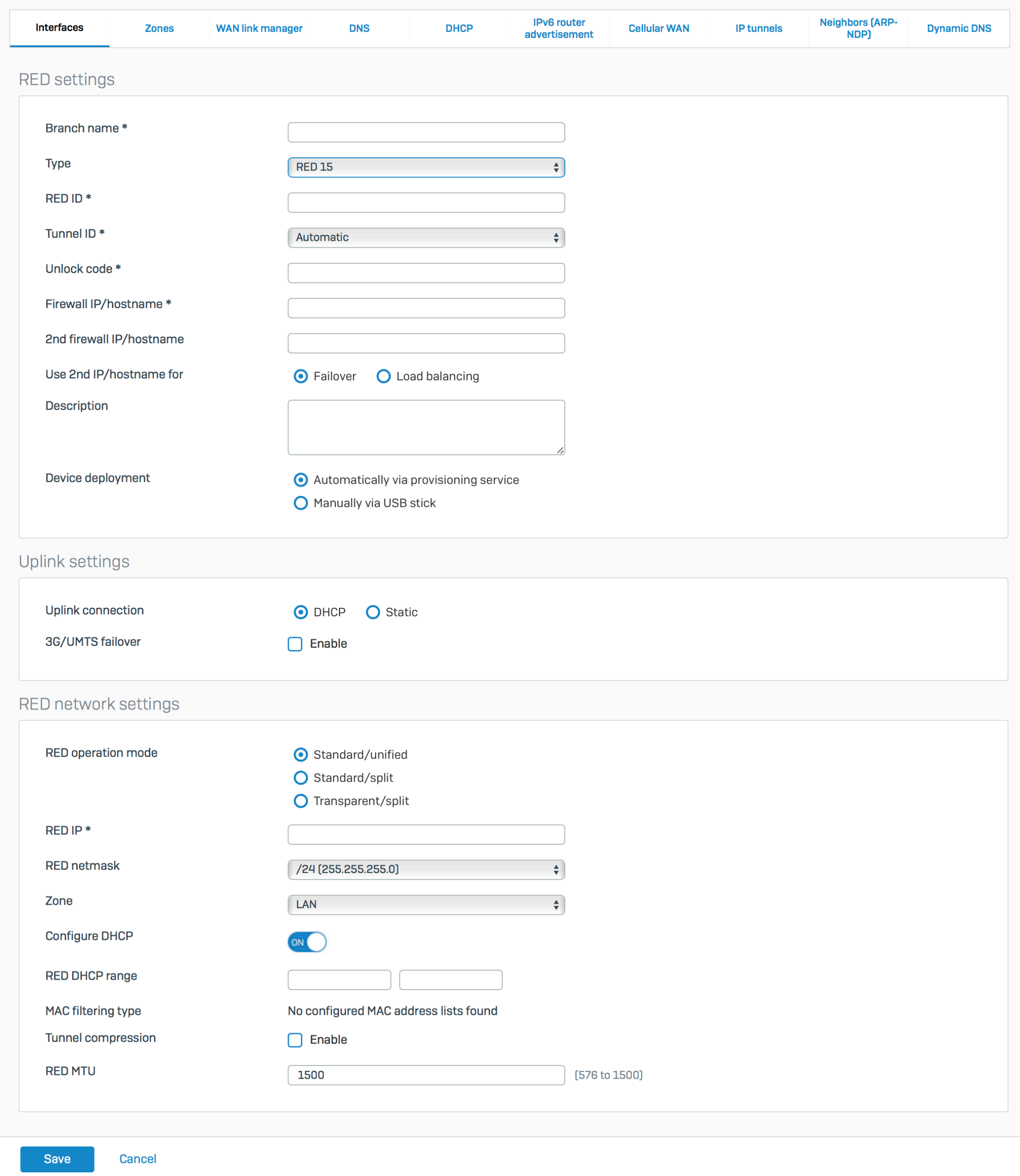
Sophos Firewall and SD-RED devices offer tunnel options to simply and affordably connect branch offices via SD-WAN.

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.



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

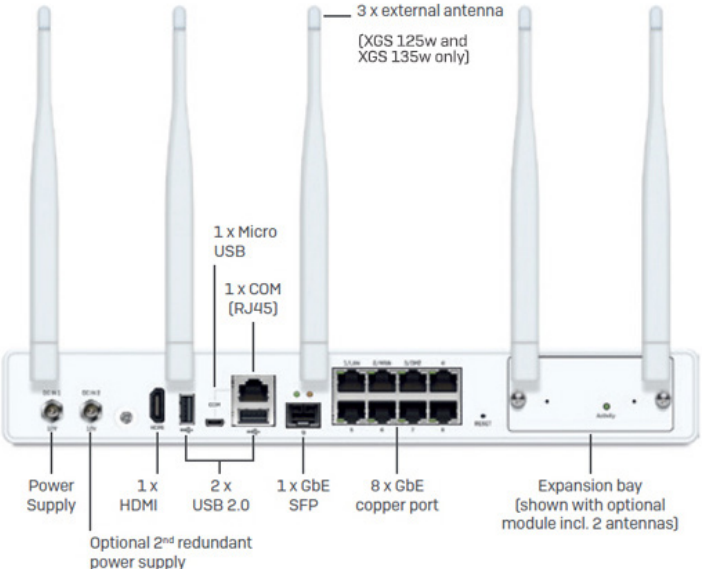
Uplink connection	● DHCP ○ Static
3G/UMTS failover	□ Enable

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)

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.


3 x external antenna
(XGS 125w and XGS 135w only)
1 x Micro USB
1 x COM (RJ45)
Power Supply
1 x HDMI
2 x USB 2.0
1 x GbE SFP
8 x GbE copper port
Expansion bay (shown with optional module incl. 2 antennas)
Optional 2nd redundant power supply

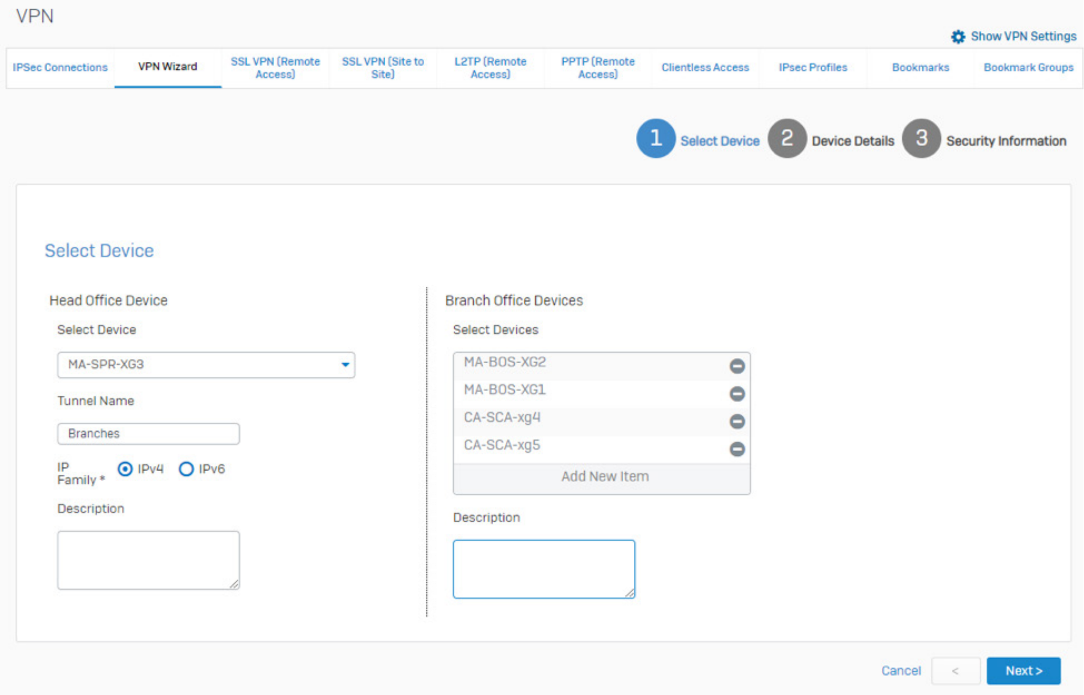
Select desktop models like the XGS 135w shown here come with options for LTE/cellular, VDSL, copper, or fiber WAN connectivity options.

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.



Select Device

Head Office Device

Select Device: MA-SPR-XG3

Tunnel Name: Branches

IP Family *: ● IPv4 ○ IPv6

Description:

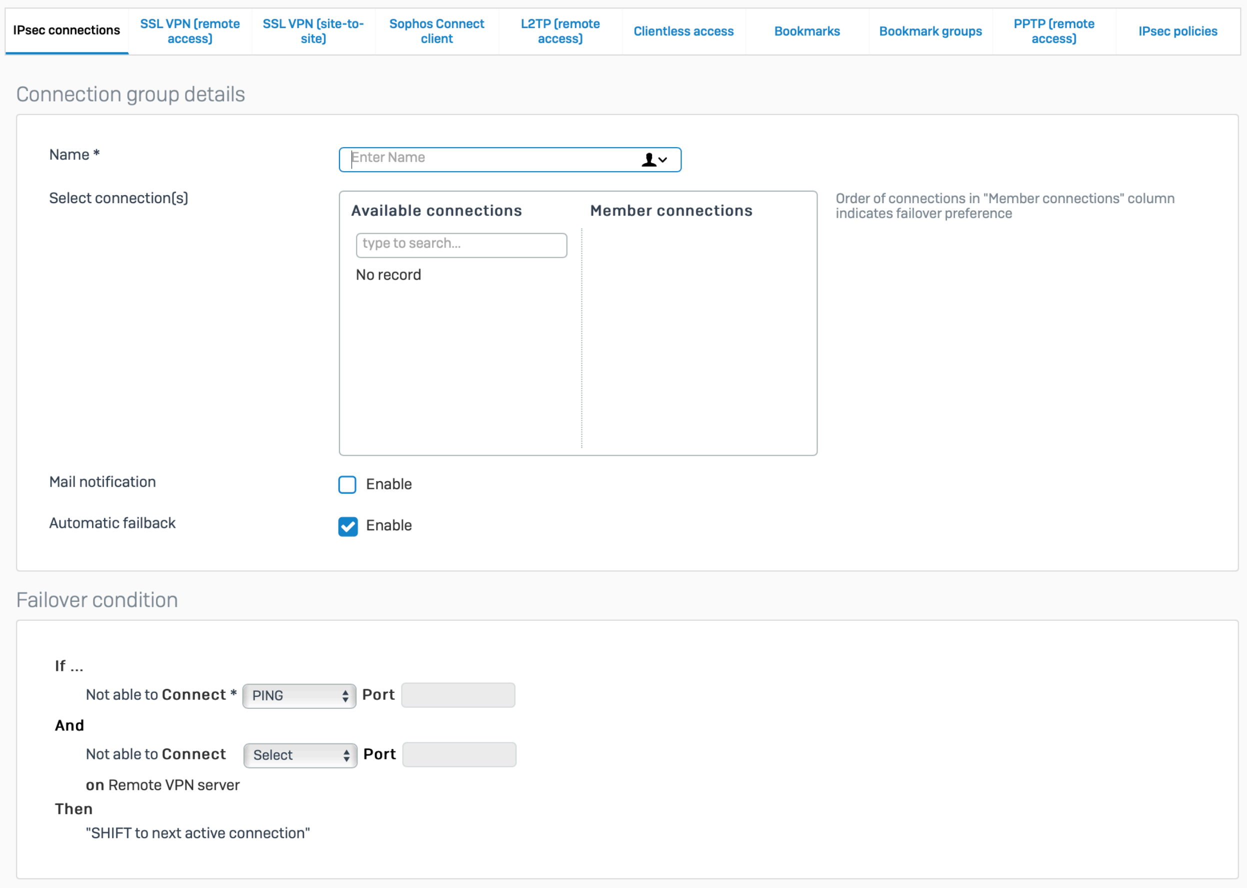
Branch Office Devices

Select Devices:
MA-BOS-XG2
MA-BOS-XG1
CA-SCA-xg4
CA-SCA-xg5

Description:

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.



Connection group details

Name * Enter Name

Select connection(s)

Available connections | Member connections

type to search...

No record

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

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"

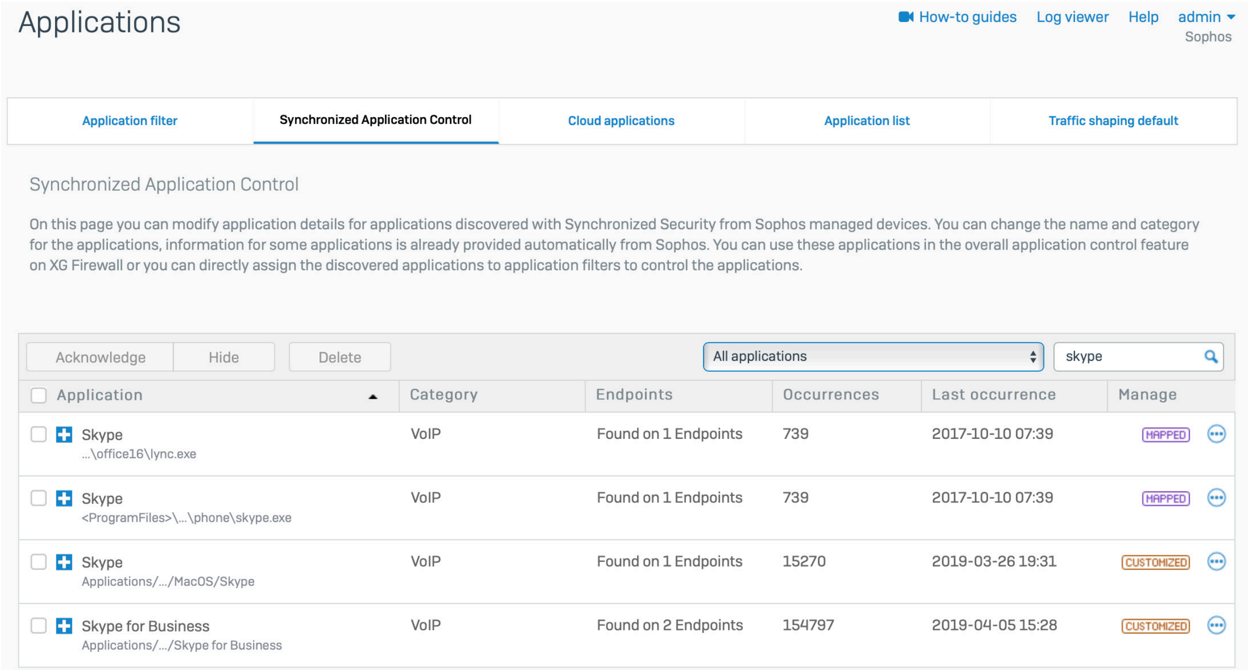
Sophos Firewall IPSec VPN failover and automatic failback options.

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.



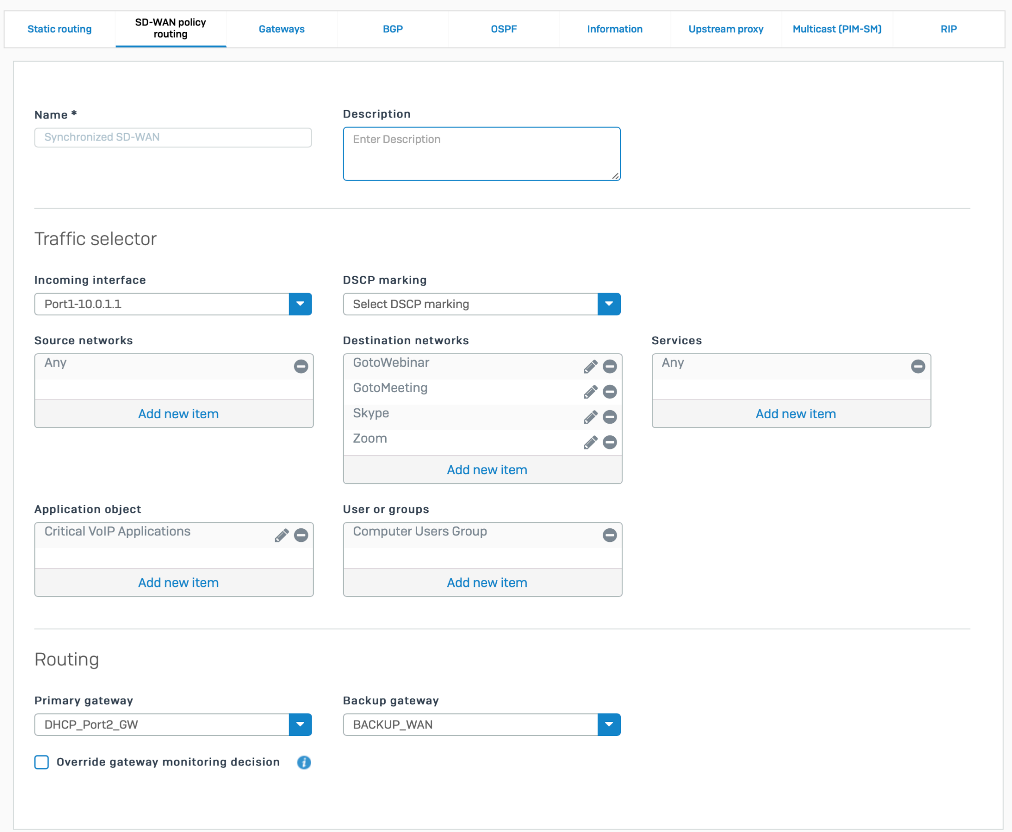
Synchronized Application Control

On this page you can modify application details for applications discovered with Synchronized Security from Sophos managed devices. You can change the name and category for the applications, information for some applications is already provided automatically from Sophos. You can use these applications in the overall application control feature on XG Firewall or you can directly assign the discovered applications to application filters to control the applications.

☐ Application	Category	Endpoints	Occurrences	Last occurrence	Manage
☐ ➕ Skype ...\office16\lync.exe	VoIP	Found on 1 Endpoints	739	2017-10-10 07:39	MAPPED ⋯
☐ ➕ Skype <ProgramFiles>\...\phone\skype.exe	VoIP	Found on 1 Endpoints	739	2017-10-10 07:39	MAPPED ⋯
☐ ➕ Skype Applications/.../MacOS/Skype	VoIP	Found on 1 Endpoints	15270	2019-03-26 19:31	CUSTOMIZED ⋯
☐ ➕ Skype for Business Applications/.../Skype for Business	VoIP	Found on 2 Endpoints	154797	2019-04-05 15:28	CUSTOMIZED ⋯

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.



Name * Synchronized SD-WAN

Description Enter Description

Traffic selector

Incoming interface: Port1-10.0.1.1

DSCP marking: Select DSCP marking

Source networks: Any

Destination networks: GotoWebinar, GotoMeeting, Skype, Zoom

Services: Any

Application object: Critical VoIP Applications

User or groups: Computer Users Group

Routing

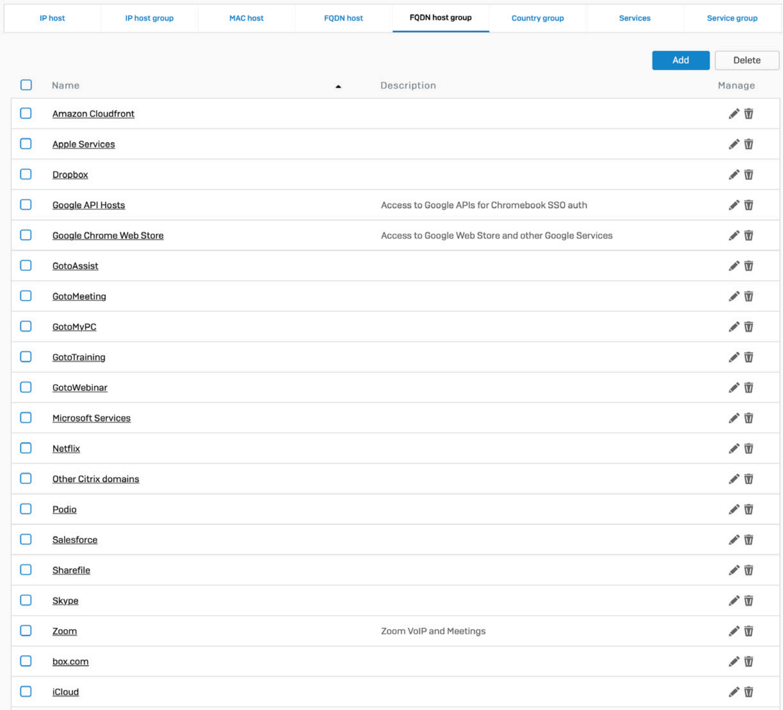
Primary gateway: DHCP_Port2_GW

Backup gateway: BACKUP_WAN

□ Override gateway monitoring decision

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.



□	Name	Description	Manage
□	Amazon Cloudfront		✎ 🗑
□	Apple Services		✎ 🗑
□	Dropbox		✎ 🗑
□	Google API Hosts	Access to Google APIs for Chromebook SSO auth	✎ 🗑
□	Google Chrome Web Store	Access to Google Web Store and other Google Services	✎ 🗑
□	GotoAssist		✎ 🗑
□	GotoMeeting		✎ 🗑
□	GotoMyPC		✎ 🗑
□	GotoTraining		✎ 🗑
□	GotoWebinar		✎ 🗑
□	Microsoft Services		✎ 🗑
□	Netflix		✎ 🗑
□	Other Citrix domains		✎ 🗑
□	Podio		✎ 🗑
□	Salesforce		✎ 🗑
□	Sharefile		✎ 🗑
□	Skype		✎ 🗑
□	Zoom	Zoom VoIP and Meetings	✎ 🗑
□	box.com		✎ 🗑
□	iCloud		✎ 🗑

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.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS

PURECLOUD