

SOPHOS



Sophos Firewall und SD-WAN

Inhaltsverzeichnis

Einleitung	2
SD-WAN-Funktionen in der Sophos Firewall	2
WAN-Verbindungen	2
Verbindungen mit Zweigstelle	3
VPN-Unterstützung und -Orchestrierung	7
Transparenz über Anwendungen und Routing	9
Übersicht und nächste Schritte	11

Einleitung

Nur wenige Begriffe im Bereich Networking haben für so viel Wirbel gesorgt wie SD-WAN (oder Software Defined Networking in a Wide Area Network). Innerhalb der Diskussion finden sich zu gleichen Teilen nützliche Informationen und verwirrende Phrasen. Die Folge des Ganzen: SD-WAN bedeutet nicht für jeden das Gleiche, und einige fragen sich immer noch, was genau sich hinter der Bezeichnung „SD-WAN“ eigentlich verbirgt.

Kunden erhoffen sich von SD-WAN vor allem Folgendes für ihr Netzwerk:

- **Geringere Konnektivitätskosten:** Herkömmliche MPLS(Multi-Protocol Label Switching)-Verbindungen sind teuer, weshalb Unternehmen vermehrt auf günstigere WAN-Optionen wie Kabel, DSL und 3G/4G/LTE zurückgreifen.
- **Geschäftskontinuität** Unternehmen benötigen Lösungen, die im Falle von WAN-Ausfällen- oder Unterbrechungen Redundanz, Routing und Failover sowie eine Beibehaltung der Sitzung gewährleisten können.
- **Qualität kritischer Anwendungen:** Unternehmen möchten Datenverkehr und die Performance von Anwendungen in Echtzeit sehen können, um die Sitzungsqualität unternehmenskritischer Anwendungen aufrechterhalten zu können.
- **Einfachere VPN-Orchestrierung für Zweigstellen:** Die standortübergreifende VPN-Orchestrierung ist oft kompliziert und zeitaufwändig. Daher sind Tools zum Vereinfachen und Automatisieren der Bereitstellung und Einrichtung so wichtig.

Bevor Sie eine bestimmte SD-WAN-Lösung in Betracht ziehen, sollten Sie sich zunächst darüber im Klaren sein, welche Ziele Sie genau verfolgen wollen.

SD-WAN-Funktionen in der Sophos Firewall

In die Sophos Firewall sind alle grundlegenden SD-WAN-Funktionen integriert, mit denen die meisten Unternehmen ihre Ziele wie gewünscht umsetzen können. In diesem Abschnitt behandeln wir die SD-WAN-Funktionen der Sophos Firewall.

WAN-Verbindungen

Zunächst zur WAN-Konnektivität: Flexible ISP- und WAN-Konnektivität sowie Redundanz und Failover im Falle eines Ausfalls sollten unbedingt berücksichtigt werden.

Die Sophos Firewall unterstützt mehrere WAN-Links (einschließlich Kupfer-, Glasfaser- sowie Wireless-Schnittstellenoptionen). Sie kann MPLS-Circuits mittels Ethernet-Handoff und VDSL über unser optionales SPF-Modem beenden.

Darüber hinaus bietet die Sophos Firewall essenzielle WAN-Link-Überwachung, Balancing sowie Failover-Funktionalität.

INTERFACE	TYPE	STATUS	RECEIVED KBYTES/S	TRANSMITTED KBYTES/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	●

Der Firewall-WAN-Linkstatus (im unteren Bereich des Schnittstellenstatus-Widgets angezeigt) ist über das Dashboard verfügbar.

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

Gateway detail

Name *

IP address *

Interface *

Type * Active Backup

Weight * (1 - 100)

Default NAT policy * ⓘ

Failover rules

If ...

Not able to Connect Port on IP address AND

Not able to Connect Port on IP address

Then ...

SHIFT to another available gateway

WAN-Link-Management in der Sophos Firewall, inklusive Balancing- und Failover-Regeln.

Die Bereitstellung von SD-RED-Geräten könnte nicht einfacher sein: Sie müssen nur die Seriennummer des Geräts in Ihrer Firewall vermerken und das Gerät an die Zweigstelle senden. Nach Anschluss des Geräts in der Zweigstelle verbindet es sich mit unserem cloudbasierten Einrichtungsservice und stellt automatisch eine sichere Tunnelverbindung zu Ihrer Sophos Firewall her. Dafür sind keinerlei technische Kenntnisse erforderlich.

The screenshot shows the configuration page for SD-RED in the Sophos Firewall management console. The page is divided into three main sections: RED settings, Uplink settings, and RED network settings. At the top, there is a navigation bar with tabs for various configuration areas: Interfaces, Zones, WAN link manager, DNS, DHCP, IPv6 router advertisement, Cellular WAN, IP tunnels, Neighbors (ARP-NDP), and Dynamic DNS. The 'Interfaces' tab is currently selected.

RED settings

- Branch name * (text input)
- Type (dropdown menu, currently set to RED 15)
- RED ID * (text input)
- Tunnel ID * (dropdown menu, currently set to Automatic)
- Unlock code * (text input)
- Firewall IP/hostname * (text input)
- 2nd firewall IP/hostname (text input)
- Use 2nd IP/hostname for (radio buttons: Failover (selected), Load balancing)
- Description (text area)
- Device deployment (radio buttons: Automatically via provisioning service (selected), Manually via USB stick)

Uplink settings

- Uplink connection (radio buttons: DHCP (selected), Static)
- 3G/UMTS failover (checkbox: Enable)

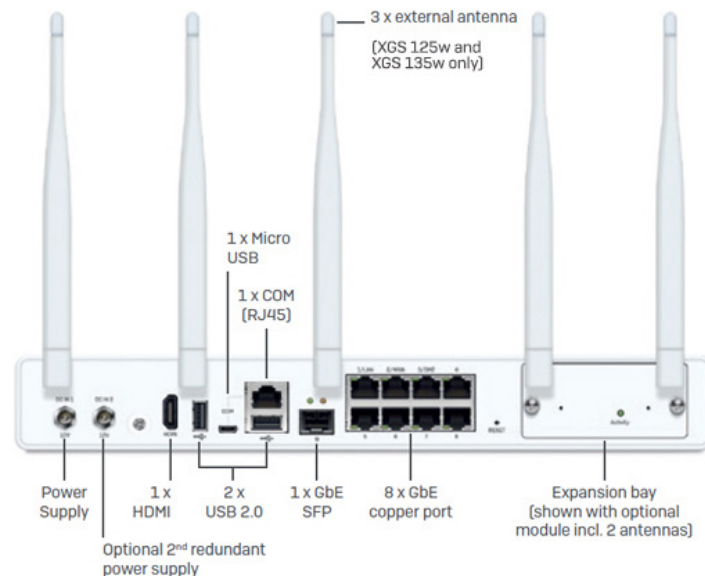
RED network settings

- RED operation mode (radio buttons: Standard/unified (selected), Standard/split, Transparent/split)
- RED IP * (text input)
- RED netmask (dropdown menu, currently set to /24 (255.255.255.0))
- Zone (dropdown menu, currently set to LAN)
- Configure DHCP (toggle switch: ON)
- RED DHCP range (two text input fields)
- MAC filtering type (text: No configured MAC address lists found)
- Tunnel compression (checkbox: Enable)
- RED MTU (text input, currently set to 1500, with a range of 578 to 1500)

At the bottom of the configuration area, there are two buttons: 'Save' and 'Cancel'.

Sophos SD-RED ermöglicht eine flexible, sichere und erschwingliche Anbindung von Zweigstellen per SD-WAN.

Unsere XGS Series Desktop Appliances eignen sich ebenfalls ideal als SD-WAN-Konnektivitäts-Lösungen für Zweigstellen. Sie bieten flexible Konnektivitäts-Optionen wie VDSL und Wireless als Ergänzung zu Kupfer- und Glasfaserschnittstellen und unterstützen unsere robusten SD-RED-Tunnel.



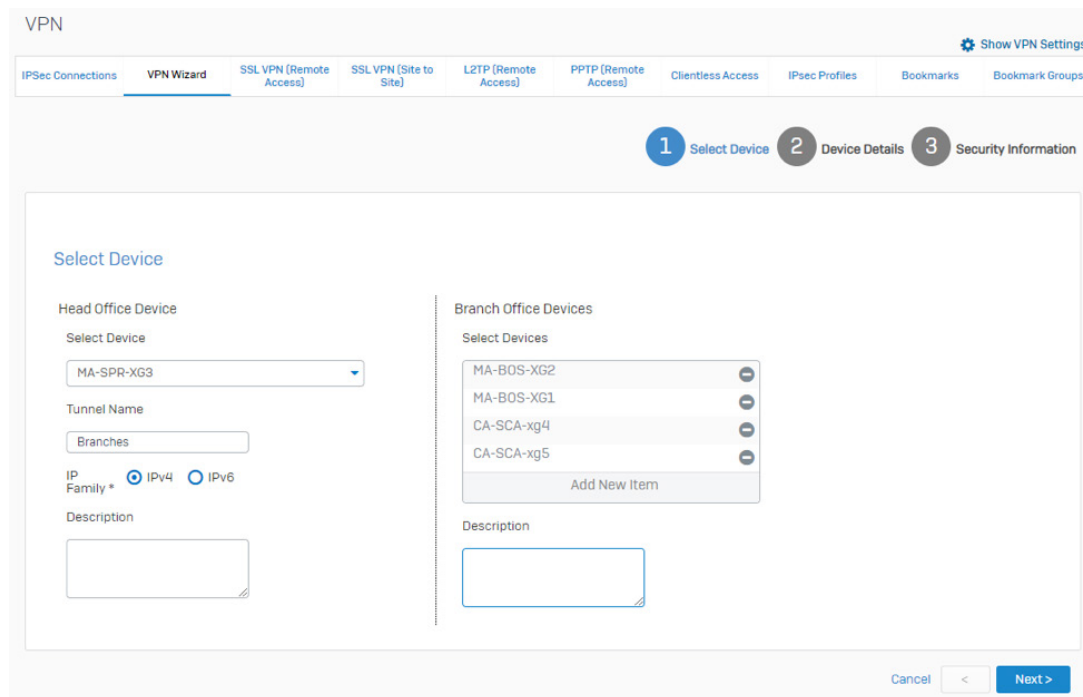
Ausgewählte Desktop-Modelle, wie die hier angezeigte XGS 135w, bieten LTE-/Wireless-, VDSL-, Kupfer- und Glasfaser-WAN-Verbindungsoptionen.

VPN-Unterstützung und -Orchestrierung

Weitere wichtige Funktionen zum Erreichen vieler SD-WAN-Ziele sind eine robuste VPN-Unterstützung und eine zentralisierte VPN-Orchestrierung.

Die Sophos Firewall unterstützt alle Standard-Standort-zu-Standort-VPN-Optionen, einschließlich IPsec und SSL. Wir bieten sogar unseren eigenen einzigartigen SD-RED-Layer-2-Tunnel mit Routing an, der in Situationen mit hoher Latenz, z. B. über Satellitenverbindungen, äußerst robust und zuverlässig ist.

Der Sophos Firewall Manager und der Central Firewall Manager bieten zentralisierte Tools für die standortübergreifende VPN-Orchestrierung, mit denen sich ganz einfach ein vermaschtes Netz aus VPN-SD-WAN-Verbindungen einrichten lässt.



Assistent im Sophos Firewall Manager zur VPN-Orchestrierung.

Zudem verfügt die Sophos Firewall über eine flexible Failback-Option zum automatischen Rückgriff auf die primäre VPN-Verbindung, wenn ein WAN-Link wiederhergestellt wird.

The screenshot displays the 'Connection group details' configuration page in the Sophos Firewall management console. At the top, a navigation bar includes tabs for '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)', and 'IPsec policies'. The main content area is titled 'Connection group details' and contains the following sections:

- Name ***: A text input field with the placeholder 'Enter Name' and a user icon.
- Select connection(s)**: A section with two columns: 'Available connections' (containing a search box with 'type to search...' and 'No record') and 'Member connections' (empty). A note states: 'Order of connections in "Member connections" column indicates failover preference'.
- Mail notification**: A checkbox labeled 'Enable' which is currently unchecked.
- Automatic failback**: A checkbox labeled 'Enable' which is checked.

Below this is the 'Failover condition' section, which defines the trigger for failover:

- If ...**: 'Not able to Connect' with a dropdown menu set to 'PING' and a 'Port' input field.
- And**: 'Not able to Connect' with a dropdown menu set to 'Select' and a 'Port' input field.
- on Remote VPN server**: A label indicating the target of the connection test.
- Then**: The action 'SHIFT to next active connection'.

IPSec-VPN-Failover- und automatische Failback-Optionen der Sophos Firewall.

Transparenz über Anwendungen und Routing

Anwendungspfad-Auswahl und -Routing spielen für das Erreichen bestimmter SD-WAN-Ziele ebenfalls eine große Rolle, da sie für unternehmenskritische Anwendungen wie VoIP die Qualität gewährleisten und die Latenz minimieren.

Natürlich lässt sich nur das routen, was auch erkannt wird. Aus diesem Grund sind eine verlässliche Identifizierung von Anwendungen und Transparenz entscheidend. Hier bieten die Sophos Firewall und Sophos Synchronized Security enorme Vorteile. Synchronized Application Control liefert 100%ige Transparenz über alle Anwendungen im Netzwerk und erleichtert so die Identifizierung unternehmenskritischer, verschleierter und benutzerdefinierter Anwendungen.

Synchronized SD-WAN, eine Funktion von Synchronized Security, bietet weitere Vorteile für das SD-WAN-Anwendungs-Routing. Synchronized SD-WAN macht sich den Umstand zunutze, dass Anwendungen durch den Austausch synchronisierter Application-Control-Daten zwischen mit Sophos verwalteten Endpoints und der Sophos Firewall eindeutig und zuverlässig bestimmt werden können. Jetzt lassen sich auch bisher nicht identifizierte Anwendungen zu den SD-WAN-Routing-Richtlinien hinzufügen. Kunden profitieren so von einer Application-Routing-Kontrolle und -Zuverlässigkeit, bei der andere Firewalls nicht mithalten können.

Applications How-to guides Log viewer Help admin Sophos

Application filter **Synchronized Application Control** Cloud applications Application list Traffic shaping default

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
<input type="checkbox"/> Skype ...office16\lync.exe	VoIP	Found on 1 Endpoints	739	2017-10-10 07:39	HAPPED
<input type="checkbox"/> Skype <ProgramFiles>...\phone\skype.exe	VoIP	Found on 1 Endpoints	739	2017-10-10 07:39	HAPPED
<input type="checkbox"/> Skype Applications/.../MacOS/Skype	VoIP	Found on 1 Endpoints	15270	2019-03-26 19:31	CUSTOMIZED
<input type="checkbox"/> Skype for Business Applications/.../Skype for Business	VoIP	Found on 2 Endpoints	154797	2019-04-05 15:28	CUSTOMIZED

Synchronized Application Control erkennt alle Anwendungen im Netzwerk, wodurch sich unternehmenskritische Anwendungen einfacher priorisieren und routen lassen.

Darüber hinaus ermöglicht die Sophos Firewall anwendungs-basiertes Routing und Pfadauswahl in jeder Firewall-Regel, auch nach Benutzer und Gruppe. Mit richtlinienbasierten Routing-Kontrollen können Sie das Routing entweder über die primäre oder die Backup-Gateway-WAN-Verbindung definieren und für eine Replay-Ausrichtung konfigurieren. In Kombination sorgen diese Funktionen dafür, dass wichtiger Anwendungsverkehr einfach über die optimale WAN-Schnittstelle geleitet werden kann.

The screenshot displays the configuration interface for SD-WAN policy routing. At the top, there are navigation tabs: Static routing, SD-WAN policy routing (selected), Gateways, BGP, OSPF, Information, Upstream proxy, Multicast (PIM-SM), and RIP.

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

Richtlinienbasiertes SD-WAN-Routing bietet flexible Tools zum Routen von kritischem Anwendungsdatenverkehr.

Die Sophos Firewall enthält zudem vollständig qualifizierte Domain-Name(FQDN)-Objekte für gängige SaaS-Cloud-Dienste und wird mit Tausenden FQDN-Host-Definitionen ausgeliefert, die sich ganz einfach erweitern lassen.

IP host	IP host group	MAC host	FQDN host	FQDN host group	Country group	Services	Service group
Add Delete							
<input type="checkbox"/>	Name	Description					Manage
<input type="checkbox"/>	Amazon Cloudfront						✎ 🗑
<input type="checkbox"/>	Apple Services						✎ 🗑
<input type="checkbox"/>	Dropbox						✎ 🗑
<input type="checkbox"/>	Google API Hosts	Access to Google APIs for Chromebook SSO auth					✎ 🗑
<input type="checkbox"/>	Google Chrome Web Store	Access to Google Web Store and other Google Services					✎ 🗑
<input type="checkbox"/>	GotoAssist						✎ 🗑
<input type="checkbox"/>	GotoMeeting						✎ 🗑
<input type="checkbox"/>	GotoMyPC						✎ 🗑
<input type="checkbox"/>	GotoTraining						✎ 🗑
<input type="checkbox"/>	GotoWebinar						✎ 🗑
<input type="checkbox"/>	Microsoft Services						✎ 🗑
<input type="checkbox"/>	Netflix						✎ 🗑
<input type="checkbox"/>	Other Citrix domains						✎ 🗑
<input type="checkbox"/>	Podio						✎ 🗑
<input type="checkbox"/>	Salesforce						✎ 🗑
<input type="checkbox"/>	Sharefile						✎ 🗑
<input type="checkbox"/>	Slava						✎ 🗑
<input type="checkbox"/>	Zoom	Zoom VoIP and Meetings					✎ 🗑
<input type="checkbox"/>	box.com						✎ 🗑
<input type="checkbox"/>	iCloud						✎ 🗑

Vordefinierte FQDN-Host-Objekte erleichtern die Pfadauswahl und anwendungsbasiertes Routing.

Übersicht und nächste Schritte

Die Sophos Firewall bietet eine Vielzahl innovativer Lösungen, um Unternehmen beim Erreichen ihrer SD-WAN-Ziele zu unterstützen. Hierzu zählen die WAN-Konnektivitäts-Optionen, die branchenweit unübertroffene Transparenz über Anwendungen, herausragende Routing-Optionen und unsere einzigartigen SD-RED Edge Appliances.

Sophos Firewall SD-WAN-Funktionen:

- **Mehrfache WAN-Link-Optionen** mit MPLS (Ethernet-Handoff), VDSL, DSL, Kabel und 3G/4G/LTE-Mobilfunk mit essenzieller Überwachung, Balancing und Failover
- **Komfortable Zweigstellen-Anbindung per SD-WAN** dank Zero-Touch-Bereitstellung unserer SD-RED-Geräte und robustem VPN sowie unseren innovativen Desktop-Modellen der XGS Series
- **Herausragende VPN-Unterstützung** für IPSec, SSL, sicheren SD-RED-Layer-2-Tunnel mit Routing und zentrale standortübergreifende VPN-Orchestrierung per SFM oder CFM
- **Einzigartige Anwendungskontrolle und Transparenz** dank Synchronized App Control; Transparenz über Anwendungen in der Cloud mit Echtzeitüberwachung von Verbindungen und Bandbreitennutzung, dazu Unterstützung gängiger Cloud-Anwendungen
- **Routing von Anwendungen** über Vorzugsverbindungen mittels Firewallregeln oder Richtlinien

Wir arbeiten intensiv an weiteren SD-WAN-Funktionen für künftige Releases der Sophos Firewall. Geplant sind unter anderem eine noch bessere Link-Überwachung und Auswahl, neue SD-RED-Geräte, Zero-Touch-Firewall sowie VPN-Orchestrierungs-Tools in Sophos Central.

Mit der Sophos Firewall erhalten Unternehmen eine leistungsstarke, flexible Netzwerkkonnektivitäts- und Sicherheitslösung für jeden Netzwerktyp. In unserem [Firewall Solution Brief](#) erfahren Sie, wie die Sophos Firewall mit branchenführender Firewall-Transparenz, -Sicherheit und -Reaktionsleistung die Kernprobleme beim Netzwerkschutz löst.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de