SOPHOS

Sophos Firewall und SD-WAN

Sophos-Whitepaper April 2021

Inhaltsverzeichnis

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

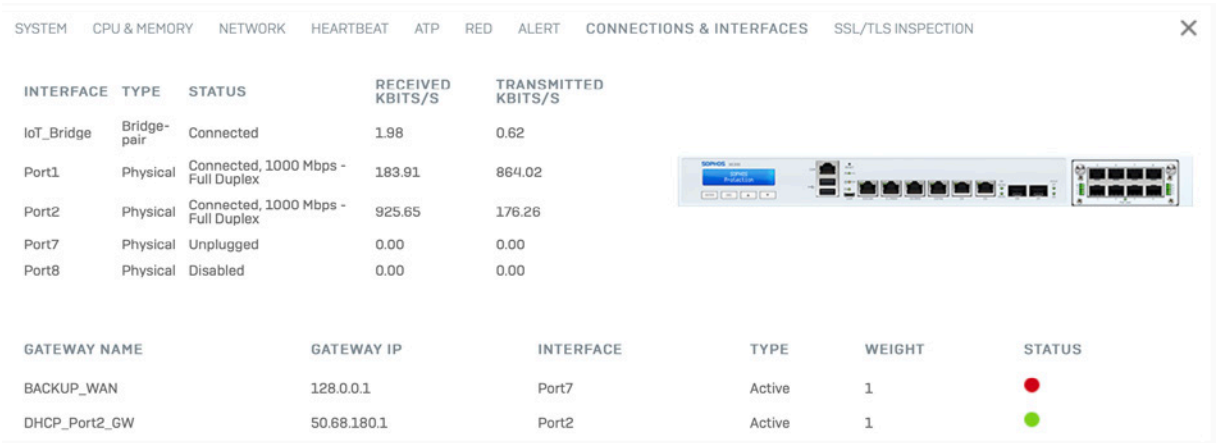
In die Sophos Firewall sind alle grundlegenden SD-WAN-Funktionen integriert, mit denen die meisten Unternehmen ihre Ziele wie gewünscht umsetzen können. In diesem Abschnitt behandeln wir die SD-WAN-Funktionen der Sophos Firewall.

WAN-Verbindungen

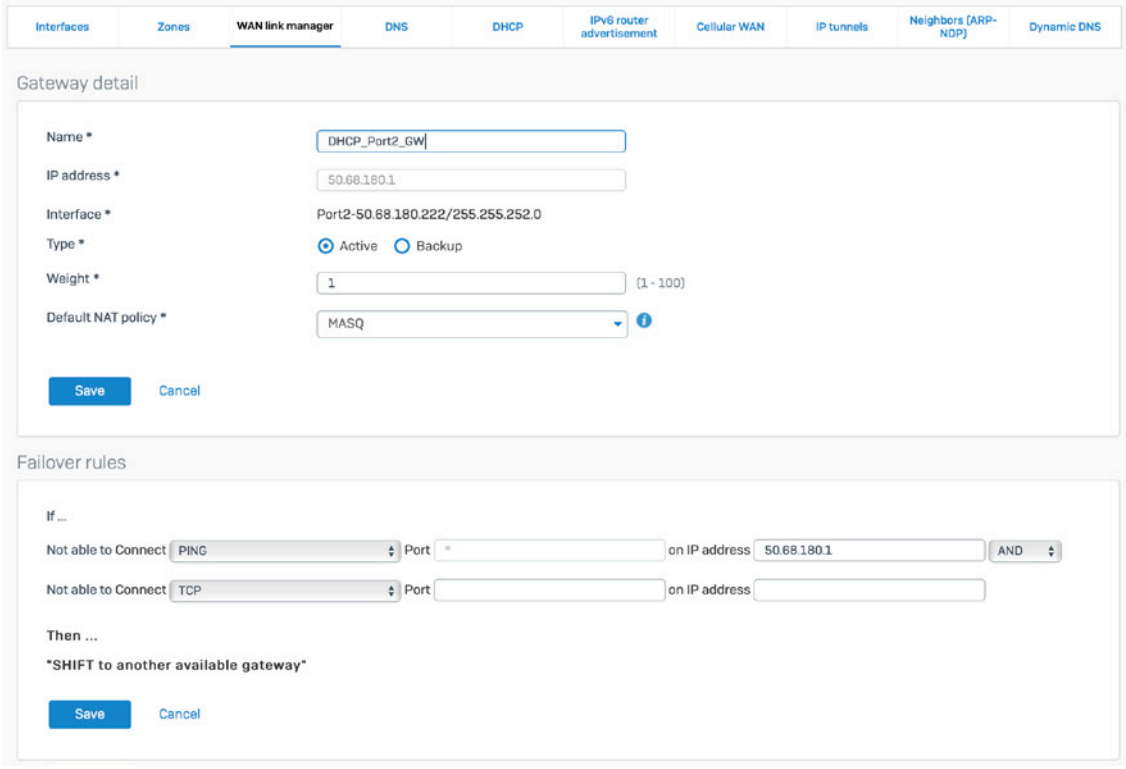
Zunächst zur WAN-Konnektivität: Flexible ISP- und WAN-Konnektivität sowie Redundanz und Failover im Falle eines Ausfalls sollten unbedingt berücksichtigt werden.

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.



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

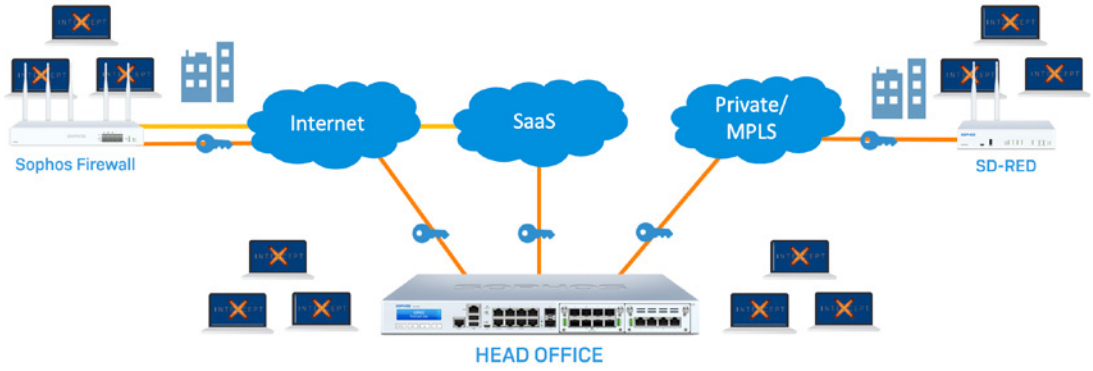


WAN-Link-Management in der Sophos Firewall, inklusive Balancing- und Failover-Regeln.

Verbindungen mit Zweigstelle

Eine weitere Kernkomponente von SD-WAN ist die Möglichkeit, Remote- und Zweigstellen-Standorte mit der Hauptniederlassung zu verbinden, um Daten auszutauschen, Transaktionen zu ermöglichen und Cloud-Anwendungen bereitzustellen.

Ebenfalls wünschenswert ist eine einfache, erschwingliche, flexible Bereitstellung mit minimaler oder ganz ohne Benutzerinteraktion, die gleichzeitig verschiedenste Konnektivitäts-Anforderungen erfüllt.

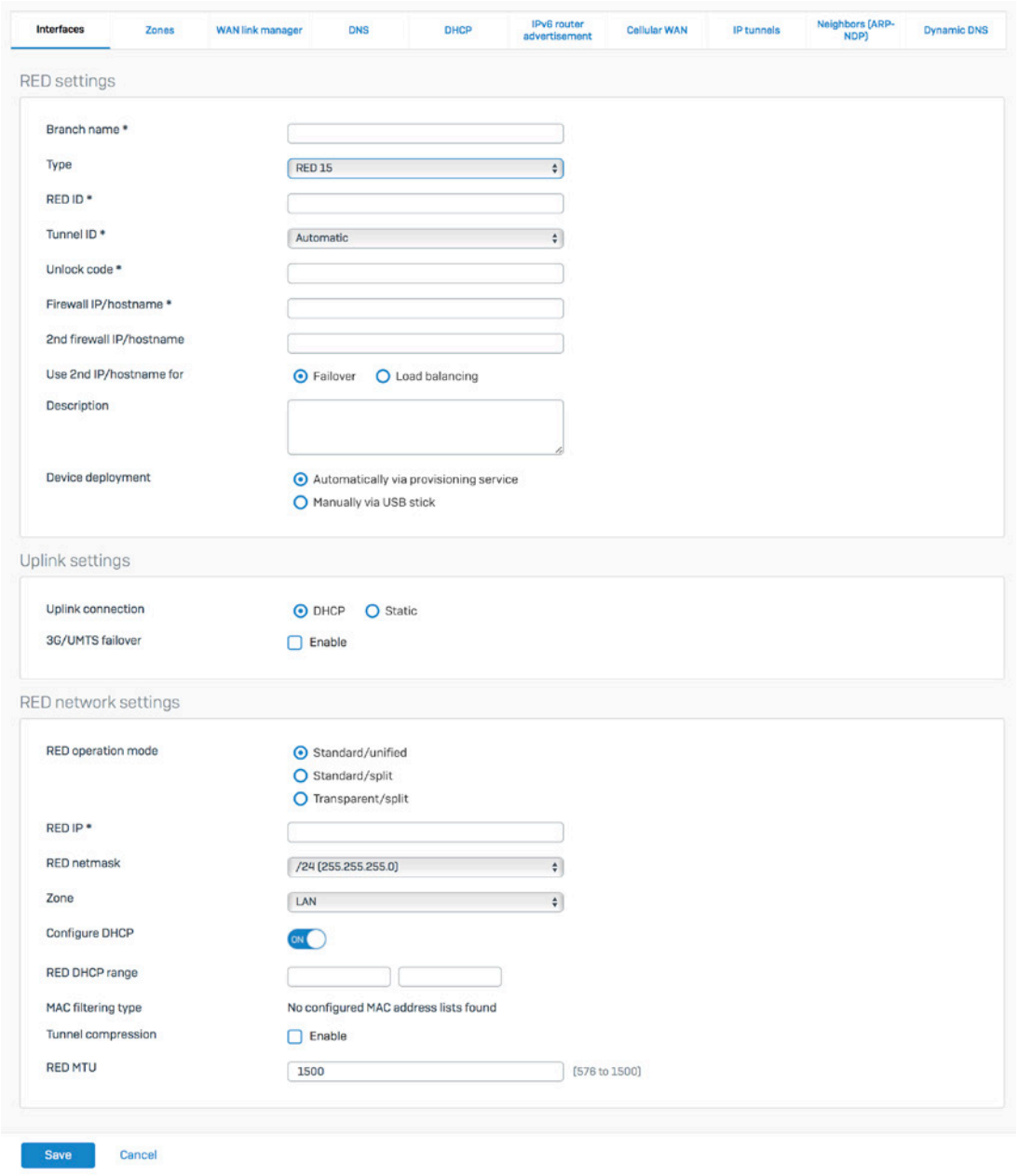


Die Sophos Firewall und SD-RED-Geräte bieten Tunneloptionen, mit denen sich Zweigstellen komfortabel und erschwinglich per SD-WAN anbinden lassen.

Dank unserer SD-RED-Geräte sind wir Vorreiter bei der Zero-Touch-Bereitstellung und -Anbindung von Zweigstellen. Unsere erschwinglichen Geräte lassen sich ganz einfach ohne Techniker einrichten und stellen einen robusten, sicheren Layer-2-Tunnel zwischen dem Gerät und einer zentralen Firewall her.

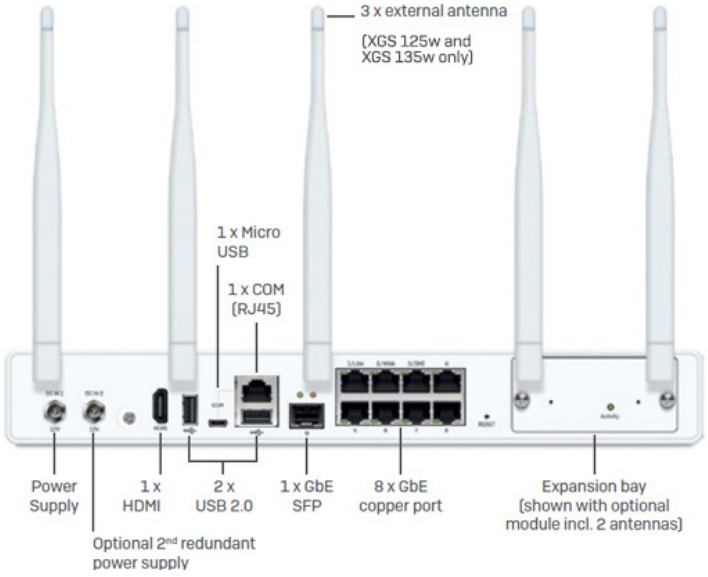
Sophos SD-RED-Geräte bieten eine erschwingliche Zero-Touch-Lösung für die Zweigstellen-Anbindung per SD-WAN.

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.



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.



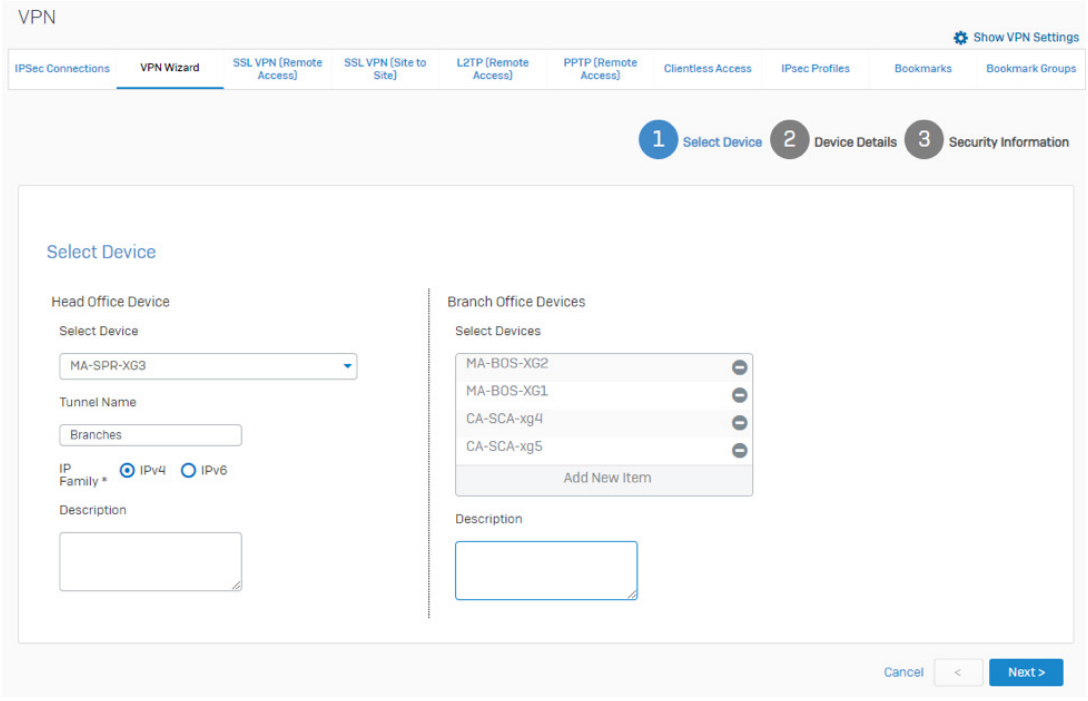
Ausgewählte Desktop-Modelle, wie die hier angezeigte XGS 135w, bieten LTE-/Wireless-, VDSL-, Kupfer- und Glasfaser-WAN-Verbindungsoptionen.

VPN-Unterstützung und -Orchestrierung

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

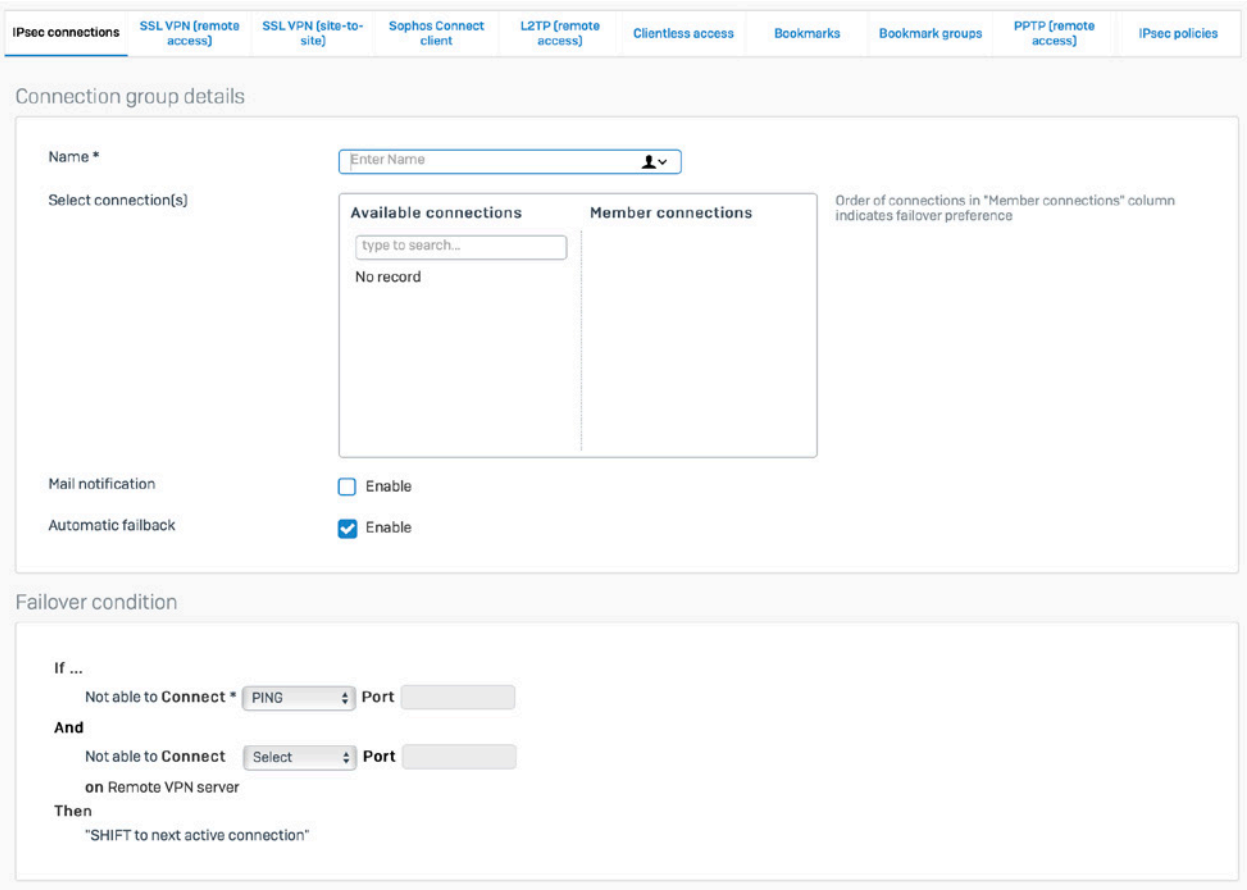
Die Sophos Firewall unterstützt alle Standard-Standort-zu-Standort-VPN-Optionen, einschließlich IPSec und SSL. Wir bieten sogar unseren eigenen einzigartigen SD-RED-Layer-2-Tunnel mit Routing an, der in Situationen mit hoher Latenz, z. B. über Satellitenverbindungen, äußerst robust und zuverlässig ist.

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.



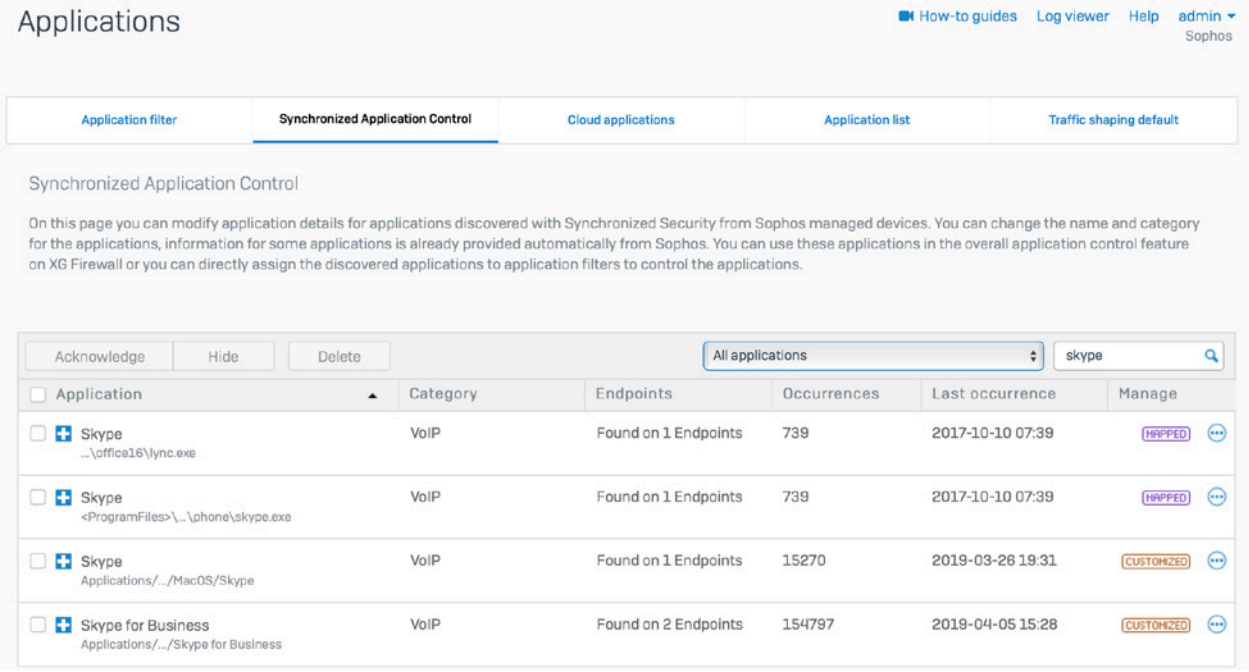
IPSec-VPN-Failover- und automatische Failback-Optionen der Sophos Firewall.

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.

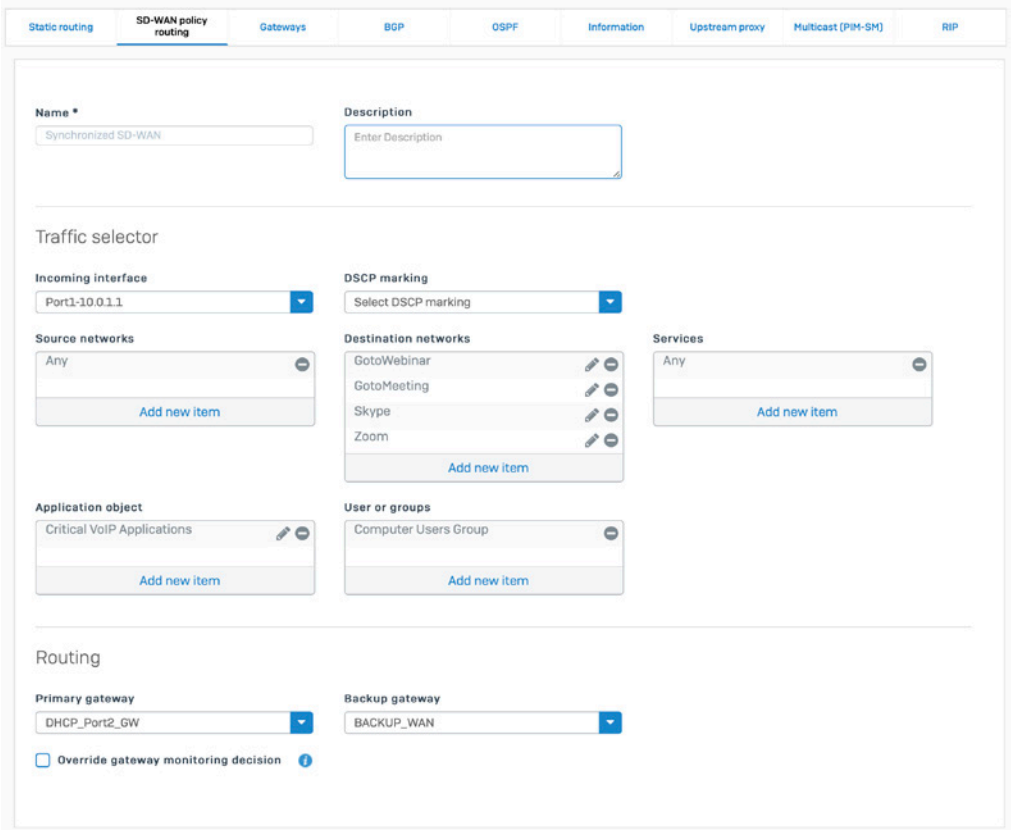
Natürlich lässt sich nur das routen, was auch erkannt wird. Aus diesem Grund sind eine verlässliche Identifizierung von Anwendungen und Transparenz entscheidend. Hier bieten die Sophos Firewall und Sophos Synchronized Security enorme Vorteile. Synchronized Application Control liefert 100%ige Transparenz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



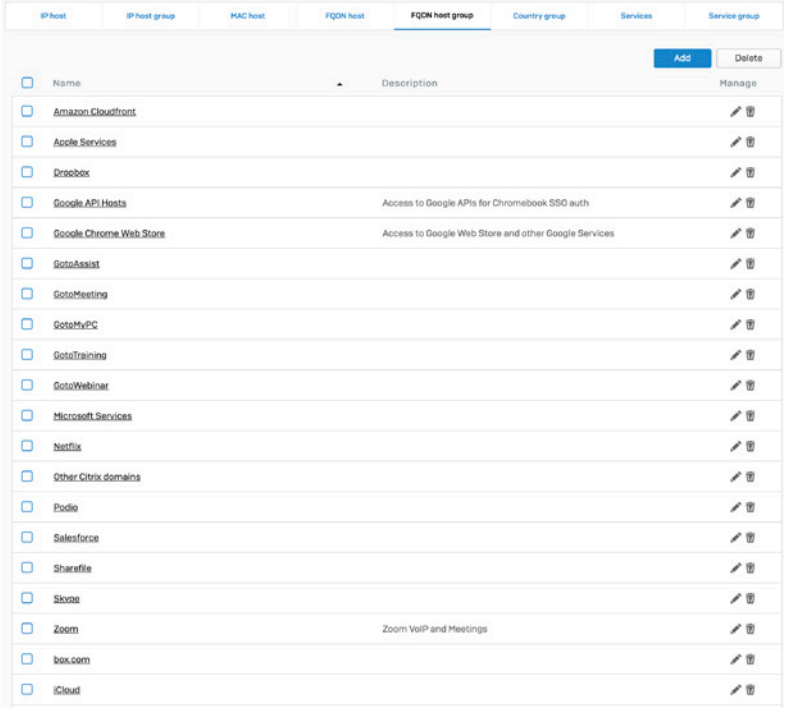
Synchronized Application Control erkennt alle Anwendungen im Netzwerk, wodurch sich unternehmenskritische Anwendungen einfacher priorisieren und routen lassen.

Darüber hinaus ermöglicht die Sophos Firewall anwendungsbasiertes 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.



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.



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

2021-04-07 WP-DE (PS)

SOPHOS