

Firewall mit Xstream SD-WAN

- ein sicherer Grundpfeiler -

Mario Winter & Stefan Vogt
Sophos Sales Engineering
11.10.2022

SOPHOS

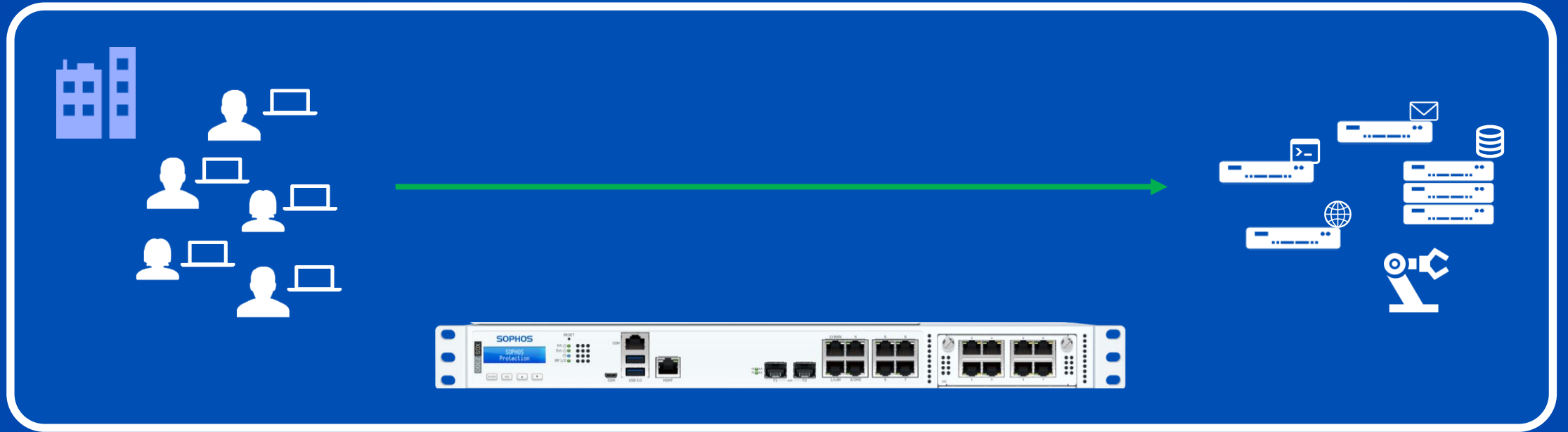
Agenda

- Sichere VPN Lösungen von heute
- Sophos Firewall und SD-WAN
- Zentrales Management der Sophos Firewalls
- Die neue Arbeitsweise von überall und jederzeit

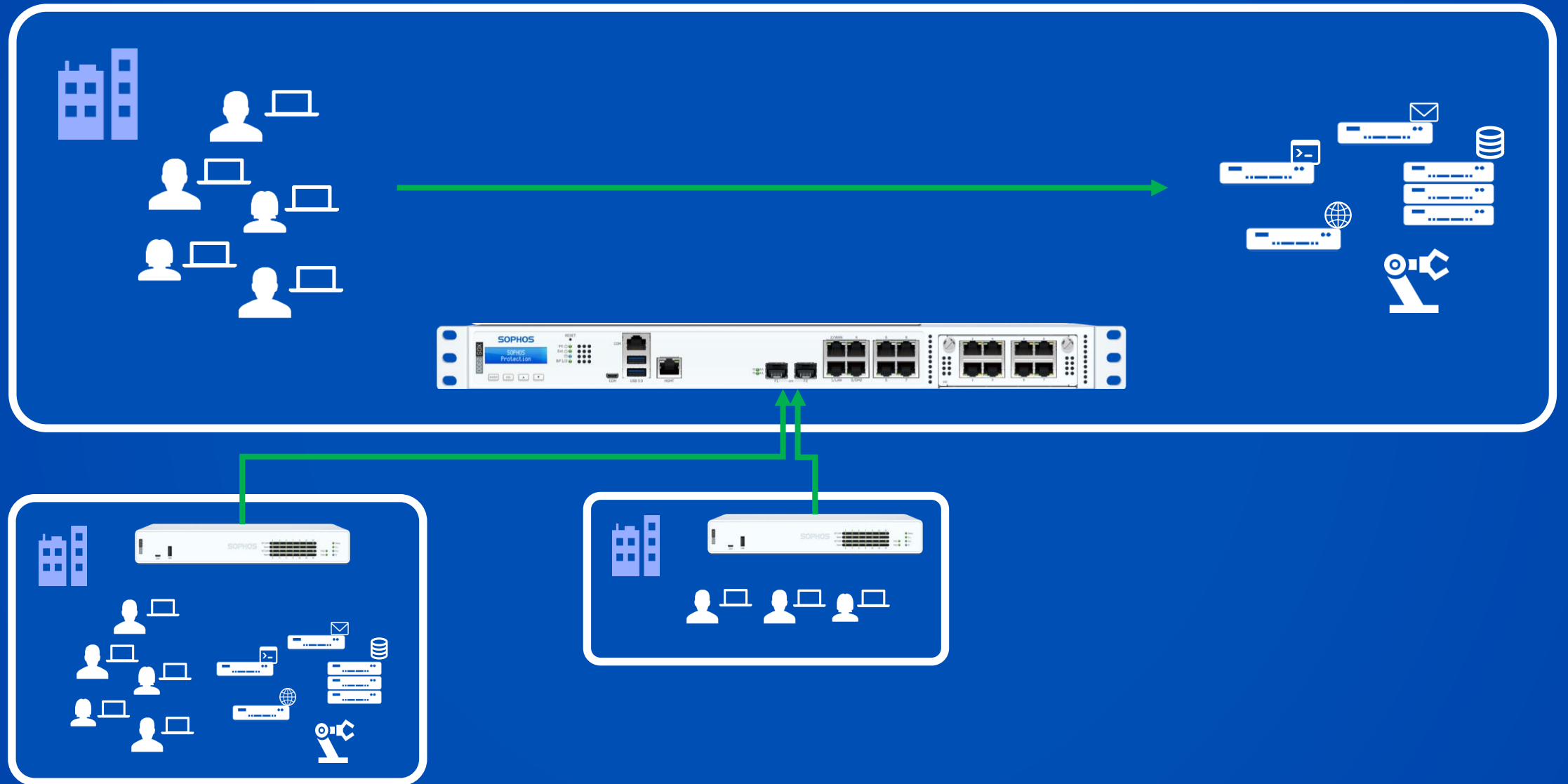
Es war einmal...



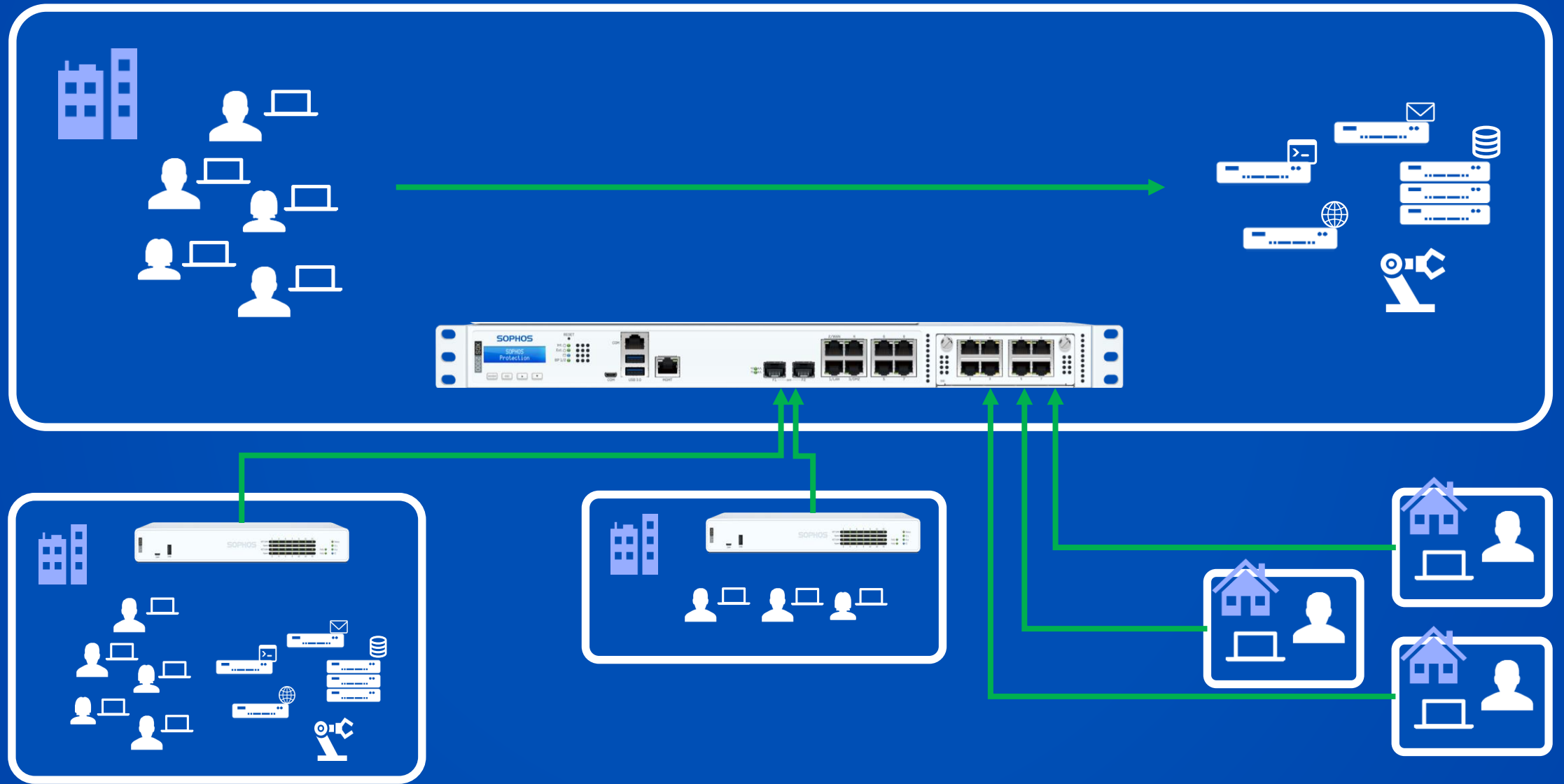
Das sichere interne Netz der Firma



Sichere Standortanbindungen via VPN



Arbeiten von Zuhause oder Unterwegs via VPN



Sicherer Fernzugriff - Sophos Portfolio



Software-Installation möglich
bzw. Einsatz von integriertem
VPN

IPSec / SSL VPN

Kombination mit SD-RED ideal

SD-RED oder Sophos Firewall
Hardware

Komfortabler Zugang ohne
Anmeldung

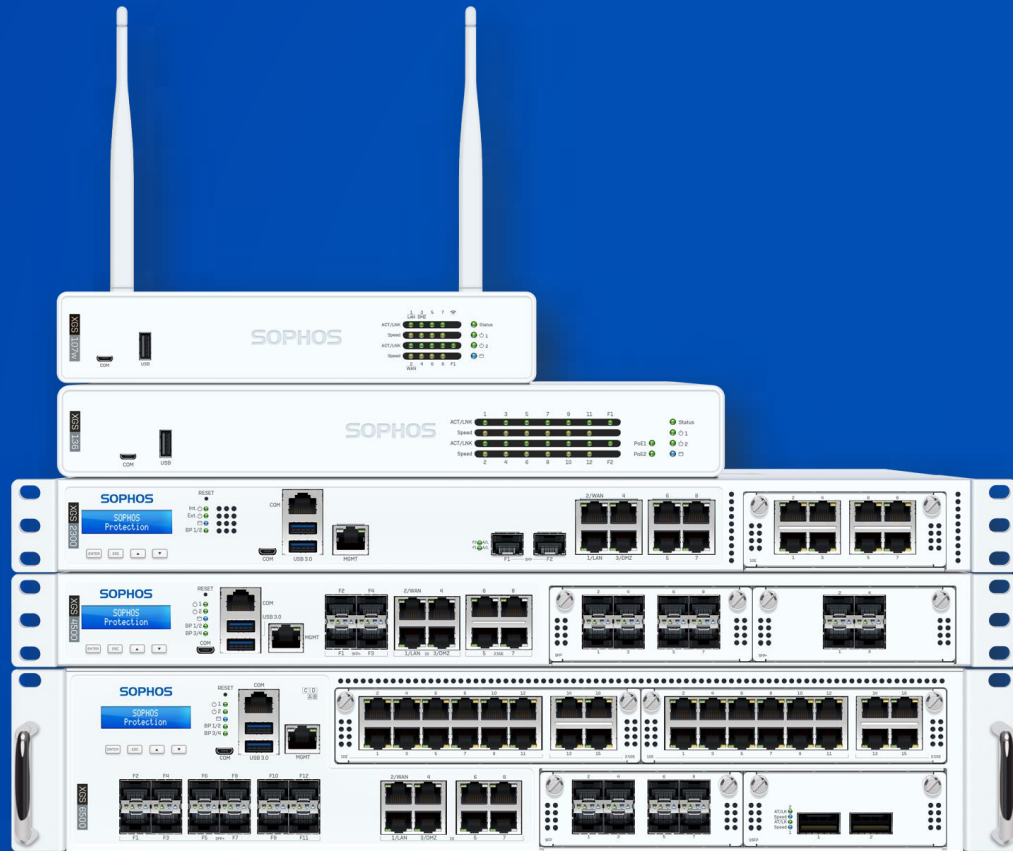
IoT Geräte

Clientless oder Software-
Installation

Keine direkte Verbindung mit
der Firmeninfrastruktur

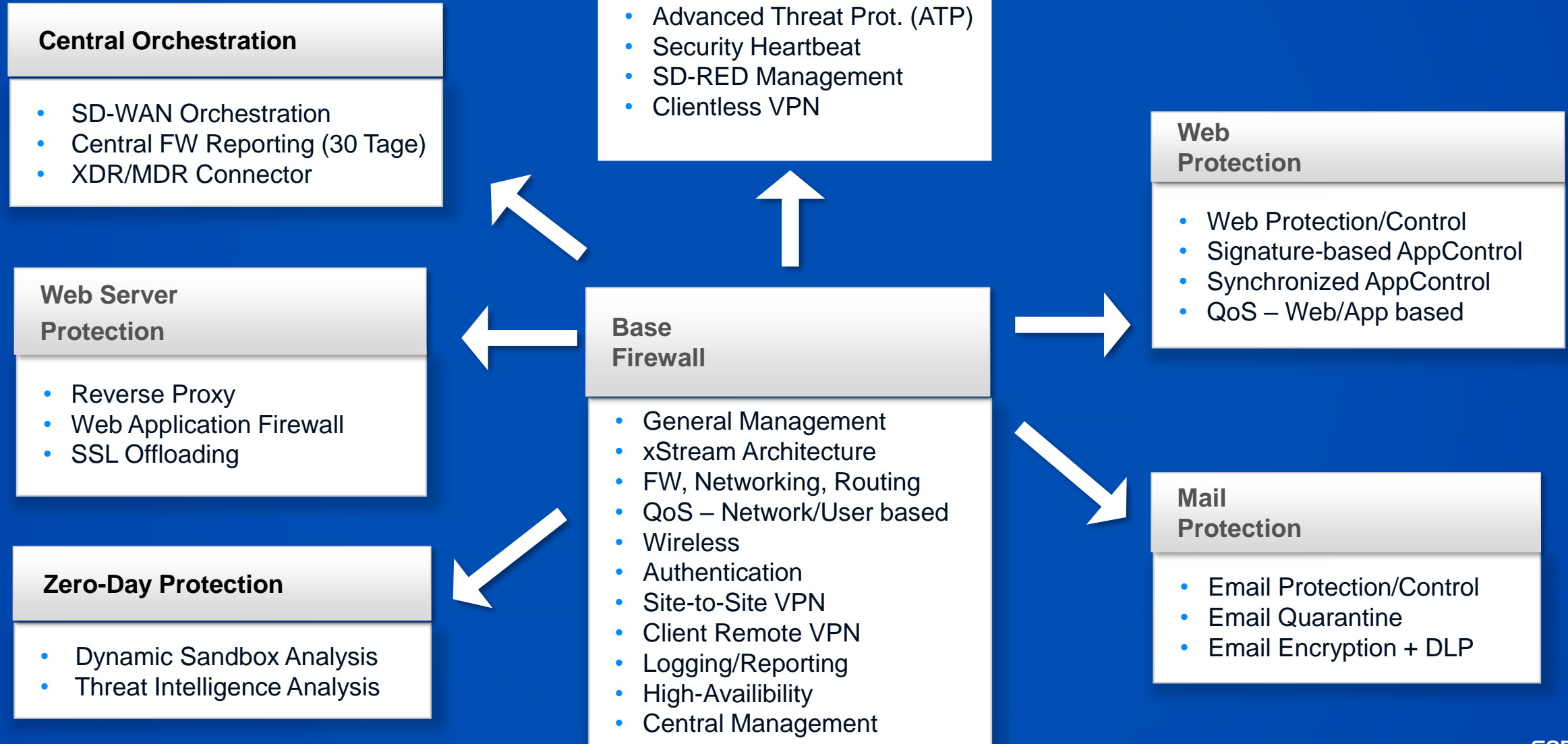
Detailreiche Nachverfolgung

Synchronized Security – Integration mit Intercept X



Sophos Firewall

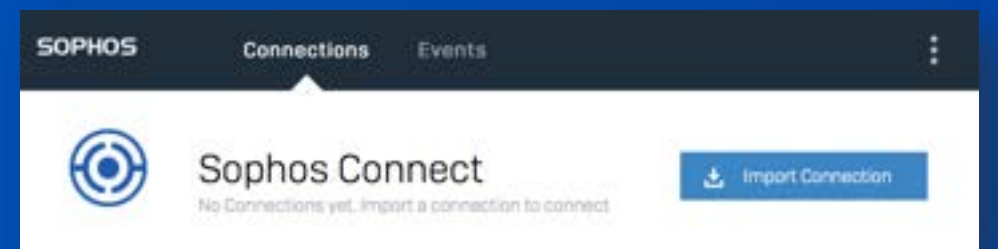
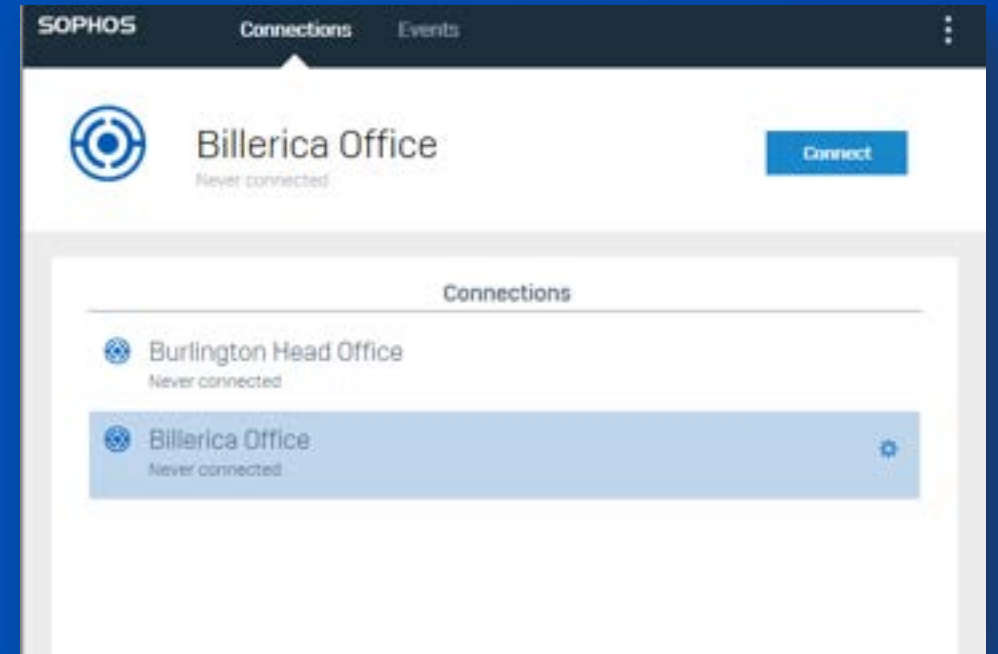
Sophos Firewall



Remote Access

Sophos Connect Client

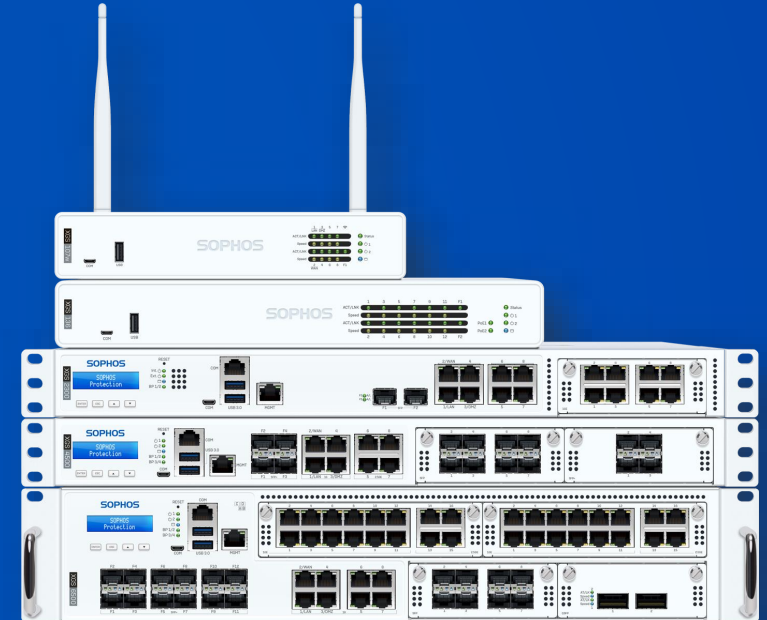
- IPsec und SSL VPN Client
- Für Windows und Mac OS
- Zwei-Faktor Authentifizierung möglich
- Benutzerspezifische Zugriffssteuerung
- Synchronized Security
- Einfacher Rollout durch MSI-Installationspaket + Konfigurationsdatei
- Eine Konfigurationsdatei für alle User (IPsec)
- Kostenfrei



Standort-Anbindung

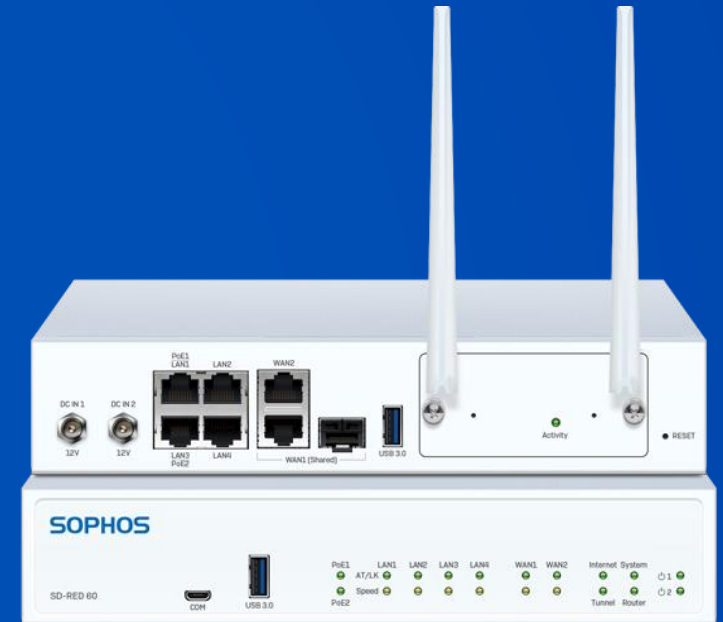
Site-to-Site VPN Technologien

- IPsec Site-to-Site
 - Xstream FastPath: Sehr hohe Performance
 - Route-based & Policy-based VPN
 - IKEv2 Support
 - Kompatibilität mit allen anderen Herstellern
 - Unterstützt automatische Failover-Mechanismen
 - Zentrale VPN Orchestration via Sophos Central

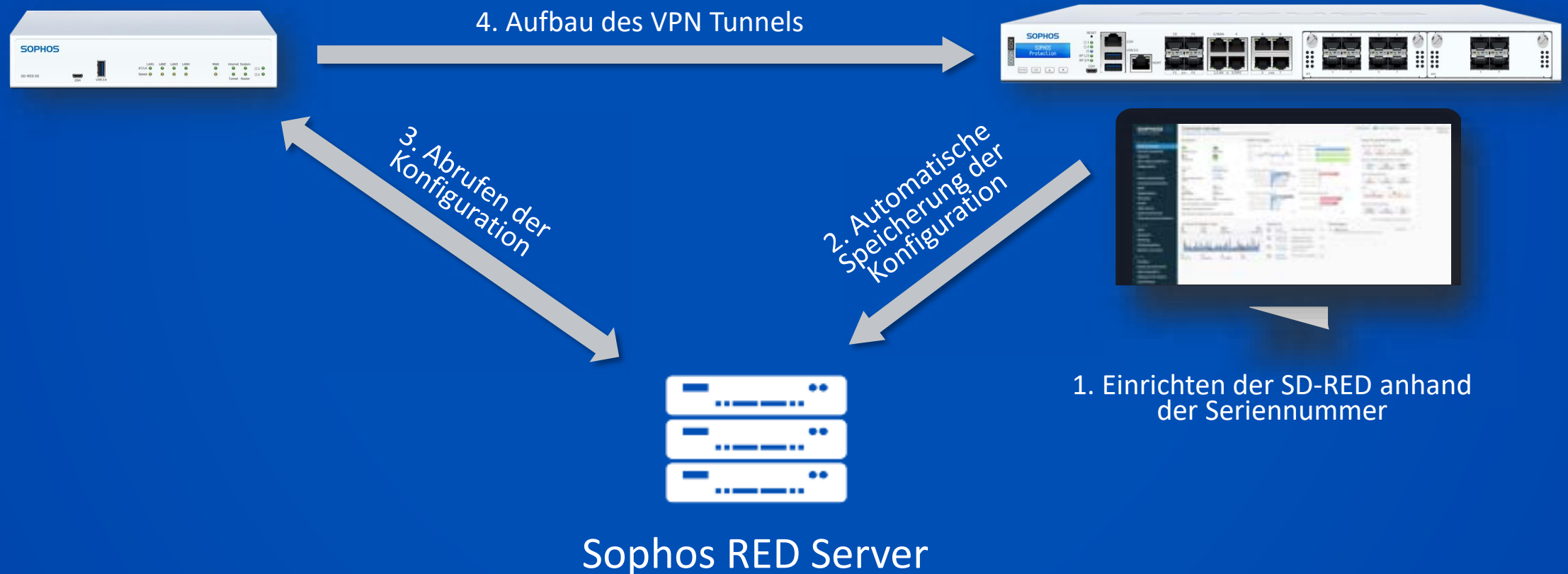


Sophos SD-REDs

- „Plug-and-Protect“-Bereitstellung
 - Schnelle Inbetriebnahme von Außenstellen, Home-Office, Filialen, etc.
- Flexible Konfiguration
 - Full-Tunnel oder Split-Tunnel
- Synchronized Security
 - Nur Firmengeräte bekommen Zugriff über den Tunnel
- Flexible Konnektivitätserweiterungen
 - WiFi Modul oder 3G/4G Modul
 - SFP Port



Sophos SD-RED – Die Plug 'n' Protect Lösung



SD-WAN

SOPHOS

Was versteht man unter SD-WAN?

Konnektivitätskosten senken

- ✓ Herkömmliche MPLS-Verbindungen sind teuer
- ✓ Umstellung auf mehrere kostengünstigere WAN Leitungen

Aufrechterhalten der Produktivität

- ✓ Lösungen, die elegant mit WAN-Ausfällen und -Verlusten umgehen können
- ✓ Wunsch nach Redundanz, Routingmöglichkeiten, Fail-Over

Vereinfachen Sie die Konnektivität von Außenstellen

- ✓ Die VPN-Orchestrierung zwischen Standorten ist komplex und zeitaufwändig
- ✓ Wunsch nach Tools zur Vereinfachung und Automatisierung der Bereitstellung und Einrichtung

Optimieren Sie die Leistungen der Anwendungen

- ✓ Echtzeit-Visibilität über Anwendungsverkehr und -leistung
- ✓ Aufrechterhaltung der Qualität von geschäftskritischen Anwendungen

SD-WAN Profile

- Routingstrategien
- Lastverteilungsmöglichkeiten
- Gewichtung der WAN Leitungen
- SLAs pro Profil einstellbar
 - Latenz
 - Jitter
 - Paketverlust
- Health-Check der WAN Leitungen

Routingstrategie

Erstes verfügbares Gateway
Leitet Datenverkehr an das erste verfügbare Gateway weiter, wenn SLA deaktiviert ist.

Lastverteilung
Lastverteilung zwischen allen verfügbaren Gateways oder Gateways, welche die SLA erfüllen.

Lastverteilungsmethode

Round-Robin Persistenz-Typ der Sitzung Verbindung

Gateways *

Gateways auswählen

Zugewiesene Gateways

WAN-Glasfaser

WAN-DarkFiber

WAN-DSL02


WAN-DSL01

1 WAN-DarkFiber (1-100)

2 WAN-Glasfaser (1-100)

3 WAN-DSL01 (1-100)

4 WAN-DSL02 (1-100)



SLA

SLA-Strategie

Hochohle Qualität
Leitet Datenverkehr an das performanteste Gateway weiter, Lastverteilung nur, wenn es zwei oder mehr Gateways mit der besten SLA-Performance gibt.

Benutzerspezifisches SLA
Leitet Datenverkehr an das erste Gateway weiter, das die SLA erfüllt. Lastverteilung zwischen allen Gateways, welche die SLA erfüllen. Falls kein Gateway die SLA erfüllt, wird die konfigurierte Routingstrategie angewendet.

Benutzerspezifisches SLA

Maximale Latenz (1-80000 ms) [Empfohlene SLA-Werte](#)

Maximaler Jitter (1-80000 ms)

Maximaler Paketverlust (0-100 %)

Zustandsprüfung

Protokoll

Ping TCP

Prüfziel *

IP-Adresse

Port

Zustandsprüfungsversuche

Intervall zwischen Prüfungen (1-3600 Sekunden)

Antwortzeitlimit (1-10 Sekunden)

Maßnahme

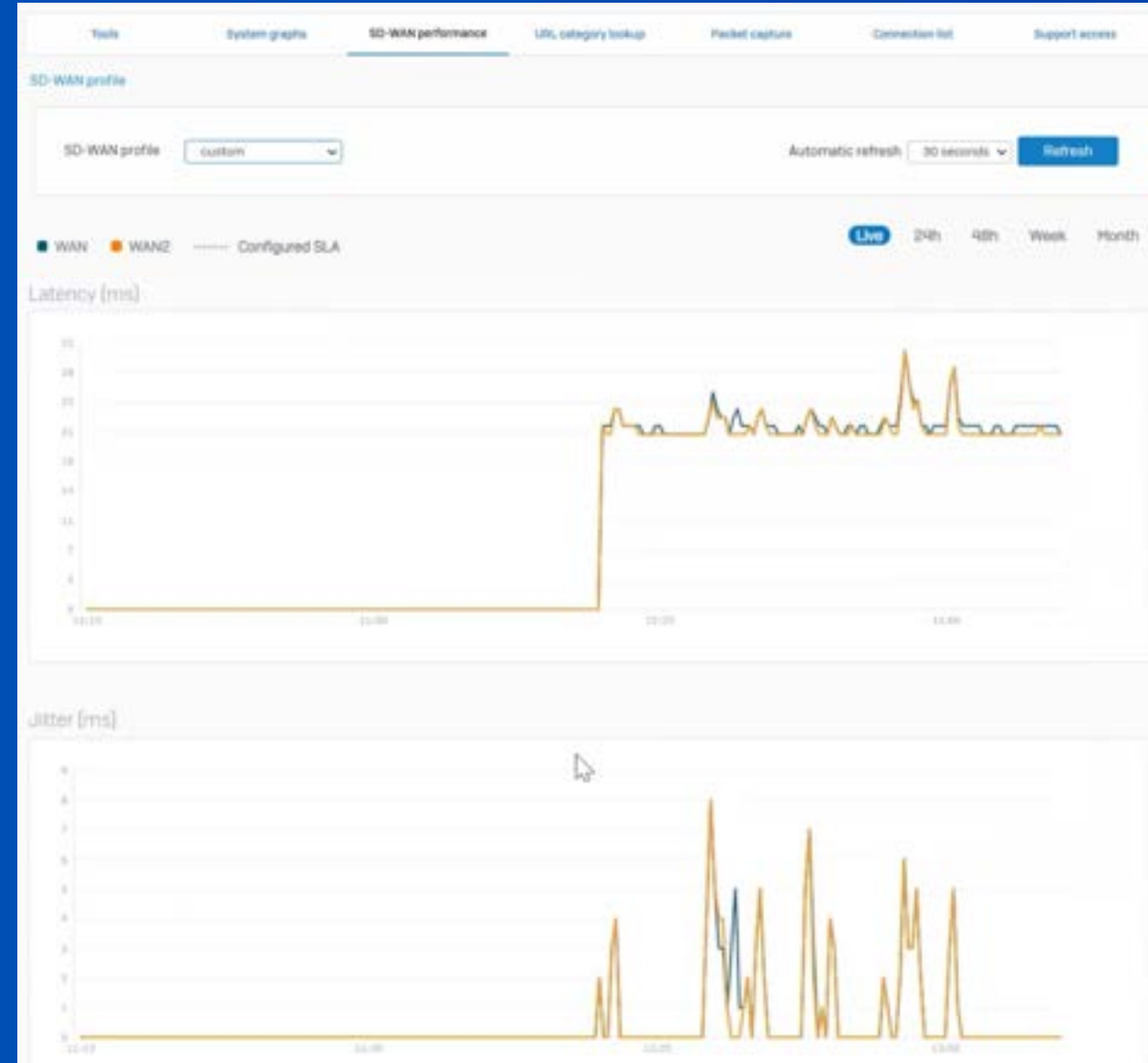
Gateway deaktivieren nach (1-10 aufeinander folgenden Fehlschlägen)

Gateway aktivieren nach (1-10 aufeinander folgenden Antworten)

Stichprobengröße für SLA (5-100 Stichproben)

SD-WAN Monitoring

- SD-WAN Monitoring Ansicht
- Filtermöglichkeiten
 - Pro WAN Leitung
 - Dauer in Zeit
- Separate Überwachung von
 - Latenz
 - Jitter
 - Packetverlust



SD-WAN Routing

- Gezieltes Routing von z.B. WAN oder VPN Traffic – abhängig von:
 - Reihenfolge
 - Gewichtung
 - SLAs
 - Health-Check

The screenshot shows the configuration page for a routing rule in a Sophos SD-WAN environment. The interface is organized into several sections:

- Name:** A text field containing "VoIP-Routing".
- Beschreibung:** A text area with the placeholder "Eingabe Beschreibung".
- Verkehrskennzeichner (Traffic Classifier):**
 - Eingehend schrittweise:** A dropdown menu set to "Beliebig".
 - DSCP-Markierung:** A dropdown menu set to "DSCP-Markierung wählen".
 - Quelle netzwerke:** A list containing "NET-Sydney" with a "Neues Element hinzufügen" button below it.
 - Ziel netzwerke:** A list containing "Internet IPv4" with a "Neues Element hinzufügen" button below it.
 - Dienste:** A dropdown menu set to "Beliebig" with a "Neues Element hinzufügen" button below it.
 - Anwendungsobjekt:** A list containing "VoIP & Conferencing Apps" with a "Neues Element hinzufügen" button below it.
 - Benutzer oder Gruppen:** A dropdown menu set to "Beliebig" with a "Neues Element hinzufügen" button below it.
- Linkauswahl-Einstellungen (Link Selection Settings):**
 - Radio buttons for "SD-WAN-Profil auswählen" (selected) and "Primäre und Reserve-Gateways".
 - A dropdown menu for "SD-WAN-Profil auswählen" set to "mein SD-WAN Profil".

Sophos Central Firewall Management

SOPHOS

Central Management für Sophos Firewall

- Kostenfreie Verwaltung über Sophos Central
- Central bietet
 - Verwaltung
 - Backup Management
 - Reporting
 - Alert Management
 - XDR
 - SD-WAN Orchestration



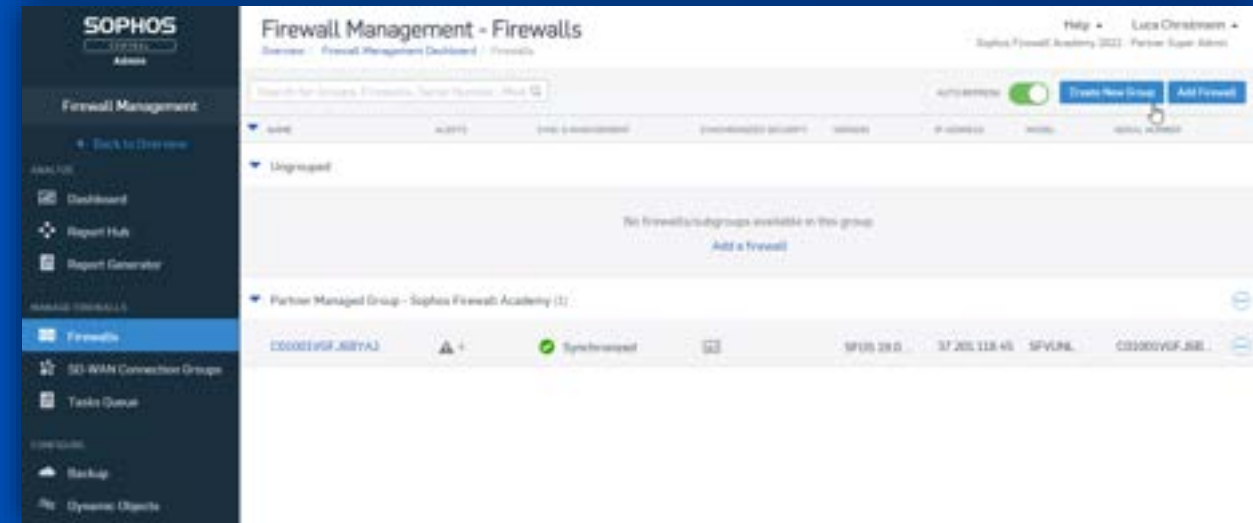
Sophos Central Management



- Registrierung der Firewall kann über Username/Passwort oder OTP erfolgen
- Firewalls können auf Wunsch vom Partner eingesehen werden

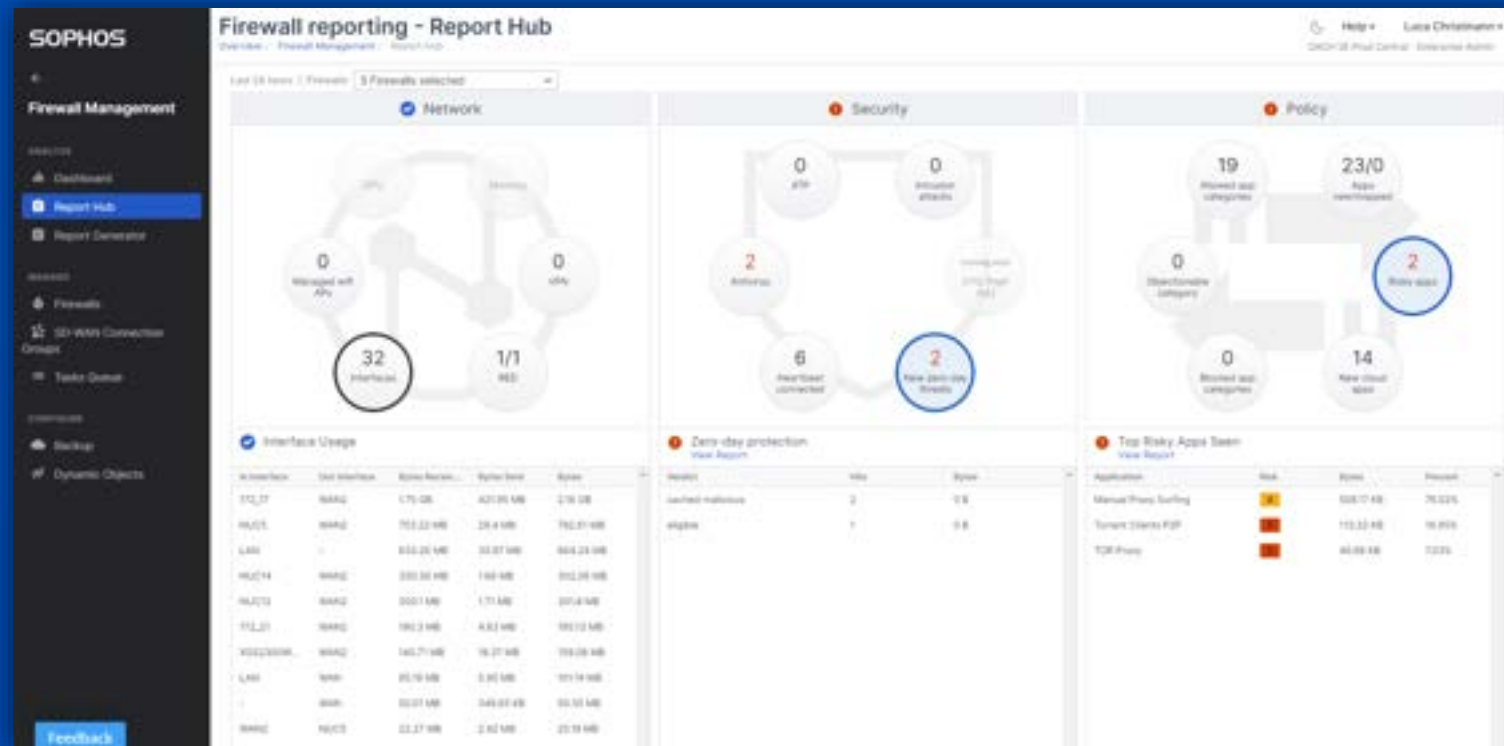
Zentrale Konfiguration der Firewalls

- Templates von Firewall Konfigurationen erstellen
- Ausrollen von Konfigurationen
 - Auf einzelne Firewalls
 - Gruppenbasierend auf mehrere Firewalls
- Vererbung von Konfiguration über Sub-Gruppen
- Zentrales und zeitbasiertes Installieren von Firmware Updates möglich
- Zentrale Speicherung von Konfigurations-Backups



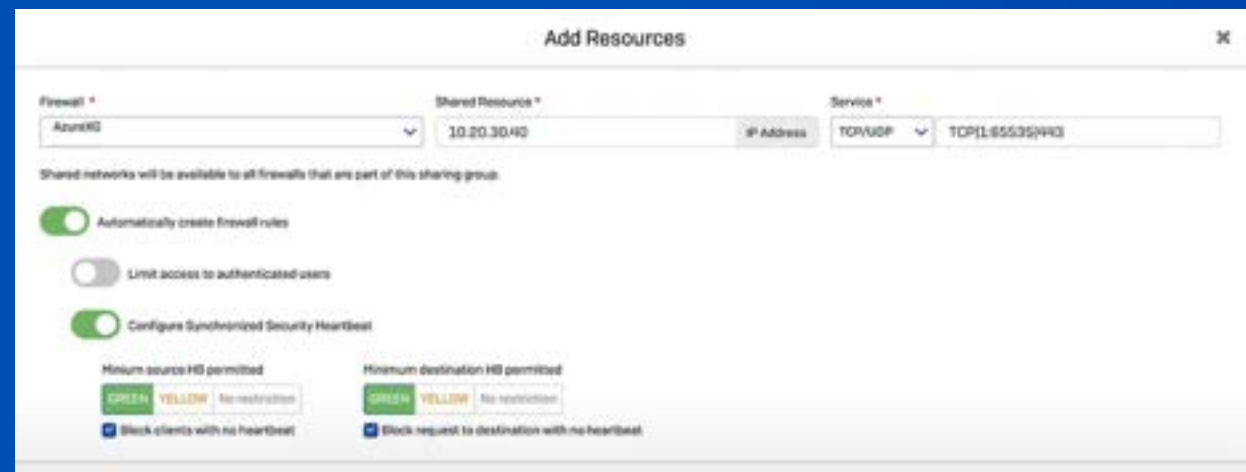
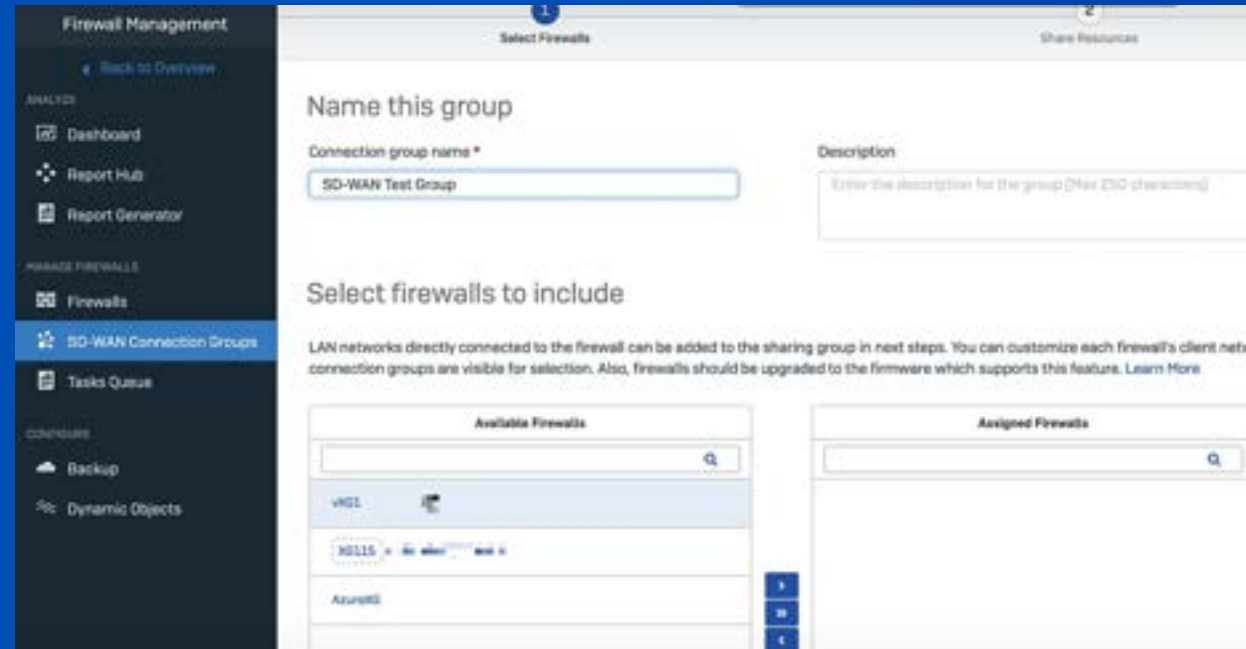
Central Firewall Reporting

- Kostenfreies Reporting für 7 Tage für alle Kunden
- Xstream Protection bietet 30 Tage und Advanced Features
- Bis zu 365 Tage durch zusätzliche Lizenz möglich
- Report Hub für die Übersicht



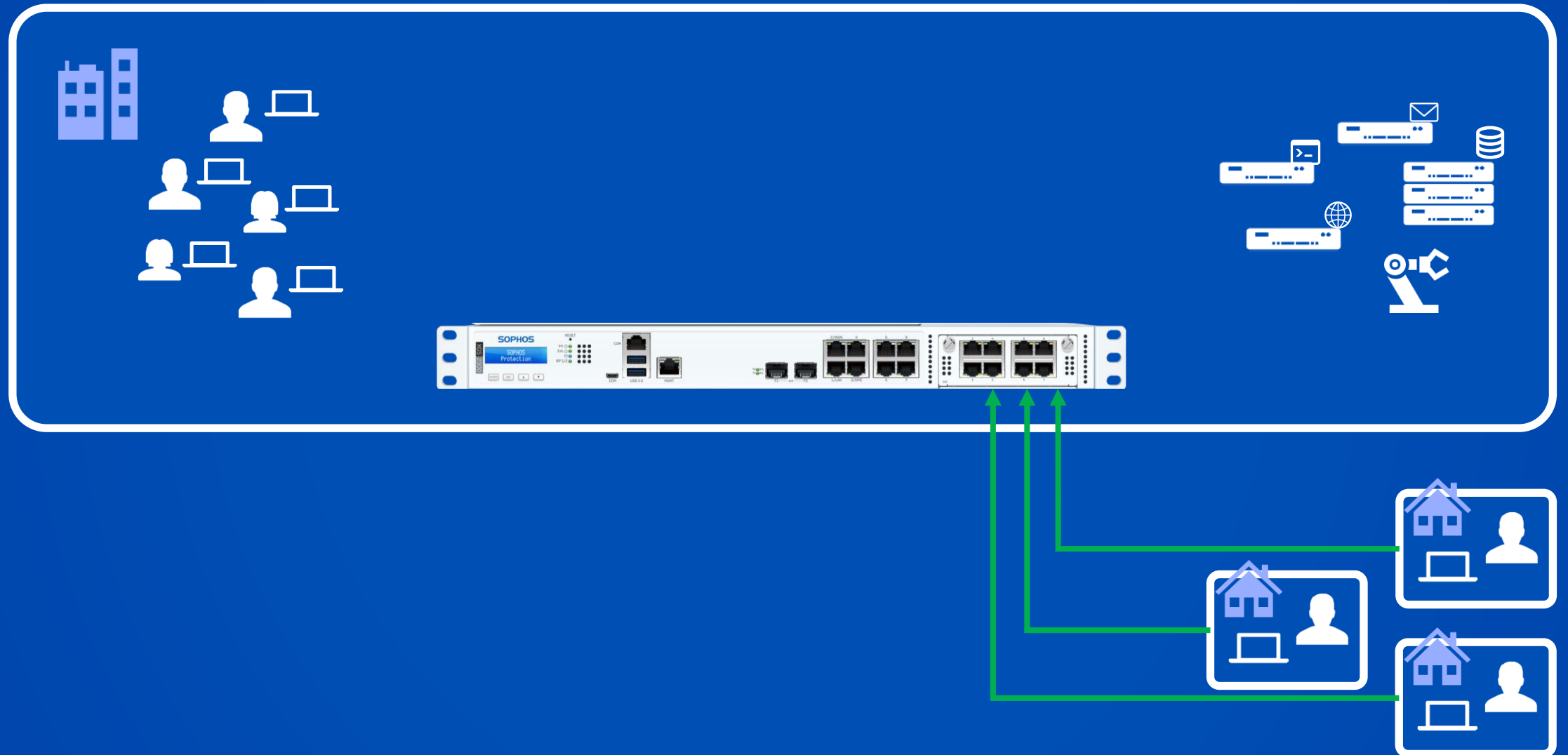
SD-WAN VPN Orchestration

- Einfache Verbindung von mehreren Standorten über Sophos Central
- Verwendet Route Based VPN für die Verbindung
- Innerhalb von wenigen Minuten konfiguriert
- Erstellt optional auch Firewall Regeln und Routen



Die Arbeitswelt im Wandel

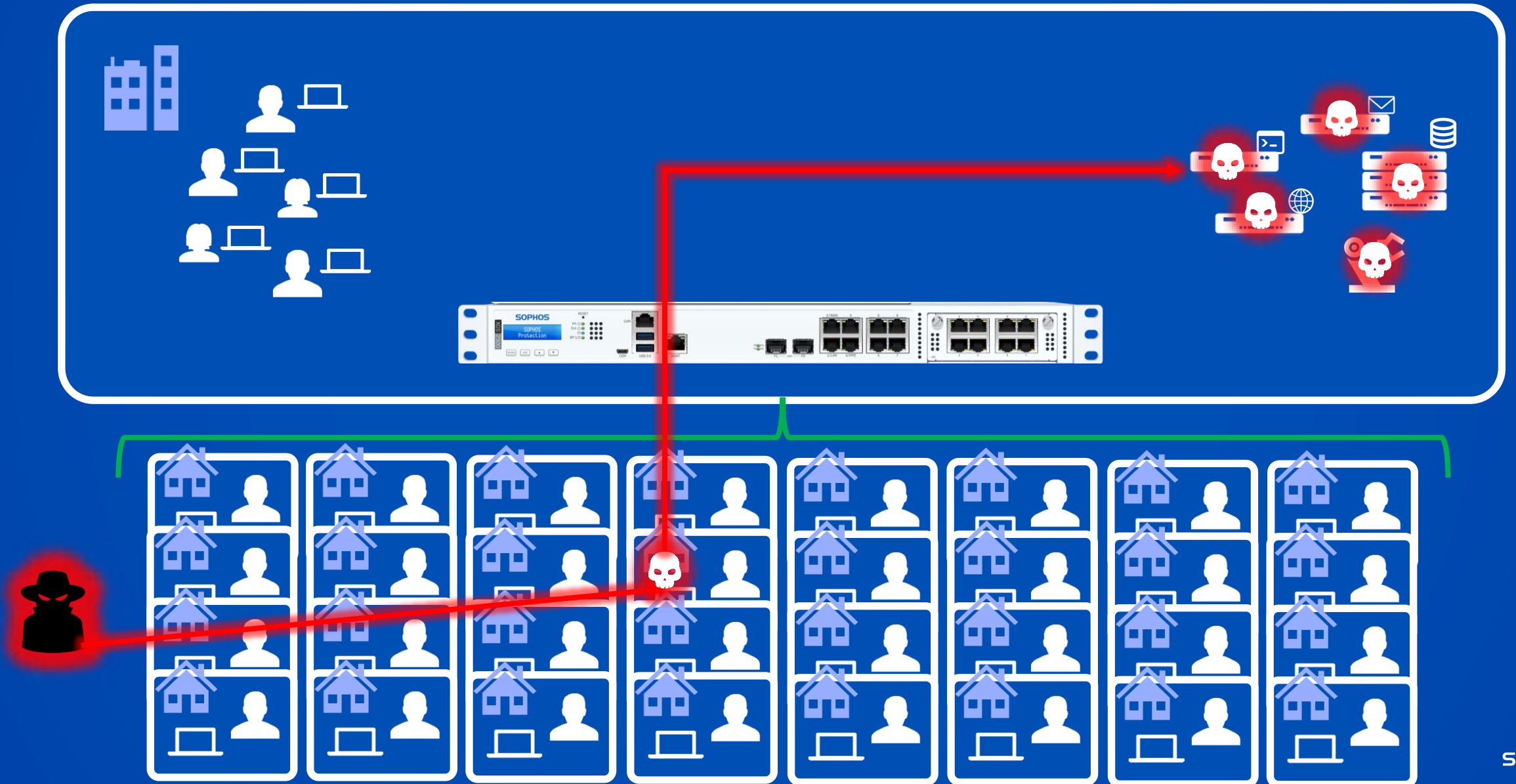
Die neue Arbeitsweise



Die neue Arbeitsweise



Wie sicher ist VPN eigentlich?



Ransomware Gruppen greifen gezielt VPN an

ZDNet / Sicherheit / Cyberkriminalität

Ransomware attackiert VPN und RDP

Ransomware wird immer gefährlicher. Hacker nutzen vor allem das Remote Desktop Protocol (RDP), und Virtual Private Networks (VPN) als Einfallstore. E-Mail-Phishing verliert dagegen an Bedeutung.

von Dr. Jakob Jung am 24. August 2020

INFOPPOINT SECURITY IT-Security Events Über Uns Kontakt

News: Remote Access VPNs rücken ins Visier von Ransomware-Angriffen

Ransomware

Remote Access VPNs rücken ins Visier von Ransomware-Angriffen

15.01.2021, San Jose | Autor: Herbert Wierer

f < t in



Sodinokibi-Ransomware nutzt VPN-Verbindung als Schwachstelle für die Attacke auf Travelex

golem.de IT-NEWS FÜR PROFIS

HOME TICKER VIDEOS VORGELESEN FORUM

Artikel, News, ... Suchen Golem.de jetzt wo

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE GEHALTSHECK | GOLEM-PC-PRODUKTVERGLEICH TO

RANSOMWARE

Colonial Pipeline über kompromittiertes Passwort gehackt

Der kürzlich gehackte Pipelinebetreiber Colonial äußert sich zu dem Vorgehen der Ransomware-Gruppe Darkside.

in Pocket speichern mykern

7. Juni 2021, 11:24 Uhr, Moritz Tremmel



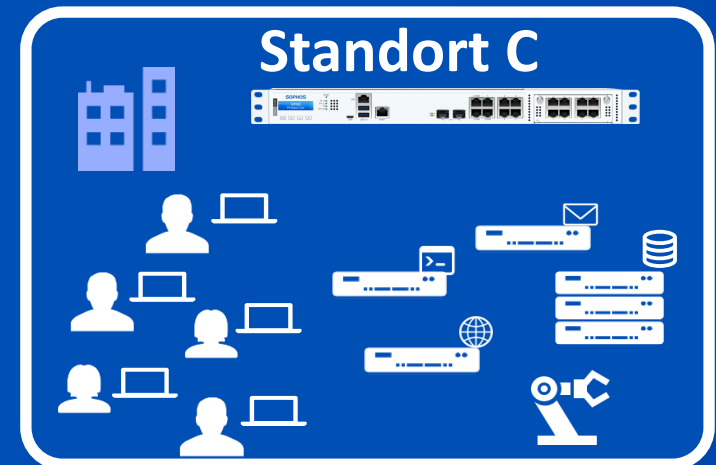
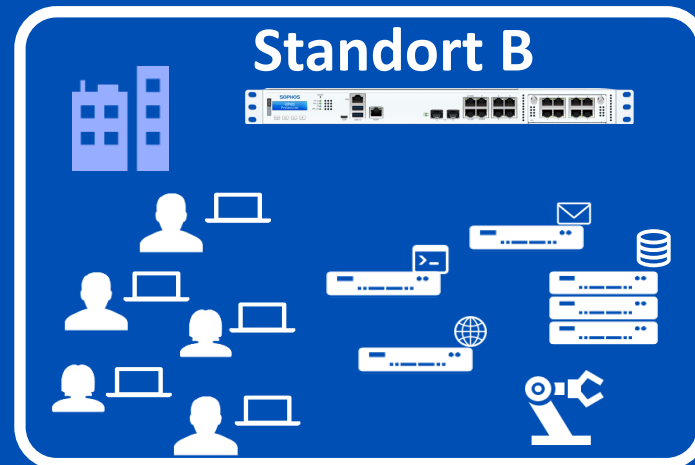
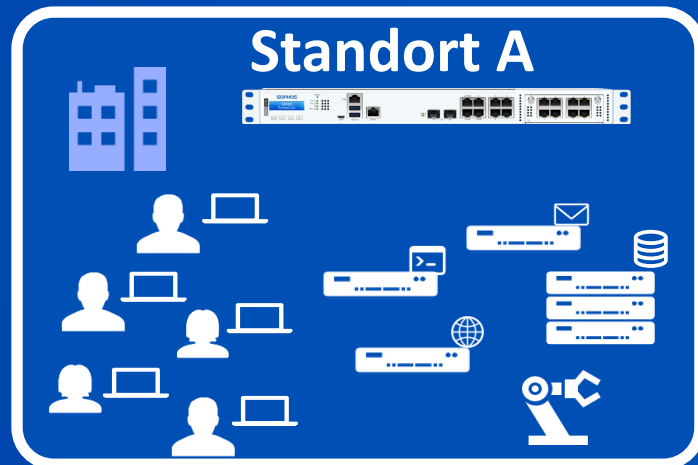
Die Treibstofftanks der betroffenen Colonial Pipeline

Der Pipeline-Betreiber Colonial wurde über kompromittierte Zugangsdaten gehackt. Laut einem Bericht des Magazins Bloomberg verschaffte sich die Angreifergruppe am 29. April 2021 Zugang zu dem internen Netz von Colonial. Dazu nutzten sie ein VPN-Konto, welches Angestellten den Fernzugriff auf das Netzwerk von Colonial ermöglicht.

ANZEIGE Google Anz Diese Werbung b Warum sehe ich dies

Herausforderungen von VPN

- Sicherheitsrisiko: „You’re ON The Network“
- Einschränkung: paralleler Zugriff auf verteilte Ressourcen
- Usability: Manuelle Einwahl statt „Always On“
- Verwaltungsaufwand: Regelwerk, Rollout & Update Clients
- Eingeschränkte Skalierbarkeit



ZTNA

Zero Trust Network Access



Mehr Infos...



Firewall Best Practices



In diesem Whitepaper erklären wir, wie Ransomware-Angriffe ablaufen, wie sie gestoppt werden können und mit welchen Best Practices für Ihre Firewall und Ihr Netzwerk Sie sich optimal schützen.



Firewall Buyer's Guide



Erfahren Sie in unserem deutschen Guide, wie die verschiedenen Sicherheitsanbieter abschneiden.



Wechsel-Angebot



Ersetzen Sie jetzt Ihre derzeitige Firewall durch eine Firewall von Sophos der XGS-Serie und erhalten Sie die Hardware Appliance und die dazugehörige Software vergünstigt!



Tipps & Tricks YT-Channel



Der Sophos Tipps & Tricks YouTube Channel enthält viele Informationen, zusammengefasst in thematisierten kurzen Videos. Nicht nur das Thema SD-WAN wird hier im Detail behandelt.