KHZG-Erfahrungsberichte

Martin Weiß
Senior Sales Engineer Public

SOPHOS

Krankenhauszukunftsgesetz - Fördertatbestände

- 01: Notaufnahme
- 02: Patientenportal
- 03: Pflege- und Behandlungsdokumentation
- 04: Entscheidungsunterstützung
- 05: Medikationsmanagement
- 06: Krankenhausinterner digitaler Leistungsprozess
- 07: Leistungsabstimmung und Cloud-Computingsysteme
- 08: Versorgungsnachweissystem Betten
- 09: Telemedizinische Netzwerke
- 10: IT- und Cybersicherheit
- 11: Anpassung von Patientenzimmern bei Epidemien

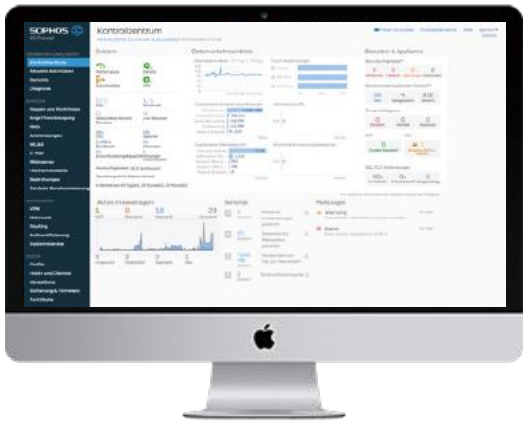
SOPHOS

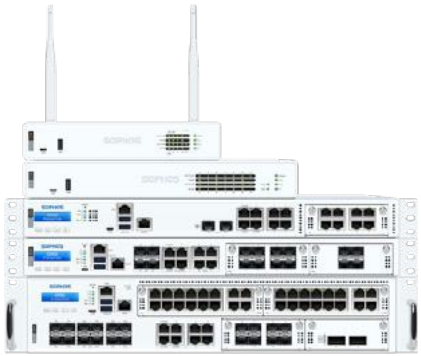
Krankenhauszukunftsgesetz (KHZG/KHZF)

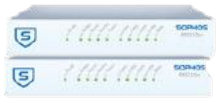
- Maßnahmen müssen Stand der Technik entsprechen
- Schutz von Netzwerken, Zonierung, VPN, IDS/IPS, ZTNA
- Interoperabilität muss gewährleistet sein
- Systeme zur Detektion von Informationssicherheits-Vorfällen (u. a. SOC & MDR) werden explizit gefördert
- Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen

Optimale Sicherheit für Ihre Organisation

Sophos Firewall







Einfaches Management

Sofortige Sichtbarkeit

Kompletter Schutz

Synchronized Security

Maximale Performance

Zentrales Management

SOPHOS

Flexible Deployment Optionen

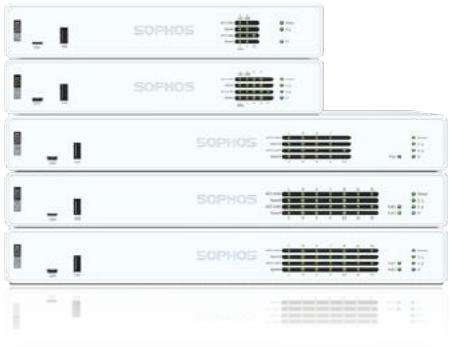
XGS Series Appliance

Software oder Virtual Appliance

Public Cloud (AWS/Azure)

Next-Gen XGS Series Appliances

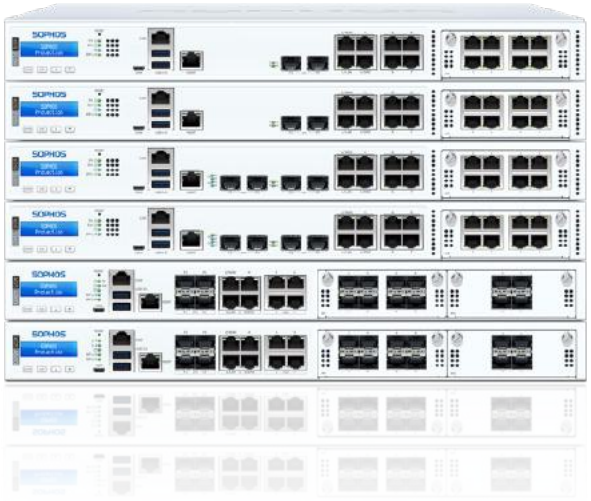
SMB und Aussenstellen



DESKTOP

XGS 87, 87w, 107, 107w
XGS 116, 116w, 126, 126w, 136, 136w

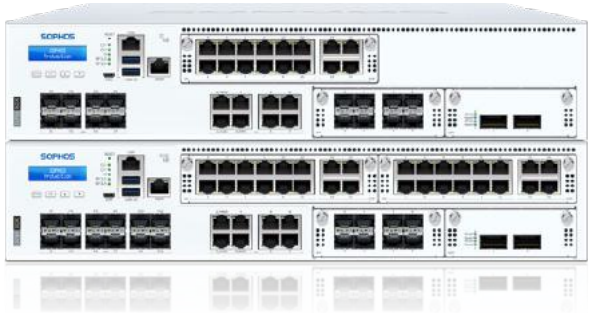
DISTRIBUTED EDGE



1HE RACKMOUNT

XGS 2100, XGS 2300, XGS 3100, XGS 3300
XGS 4300, XGS 4500

ENTERPRISE EDGE



2HE RACKMOUNT

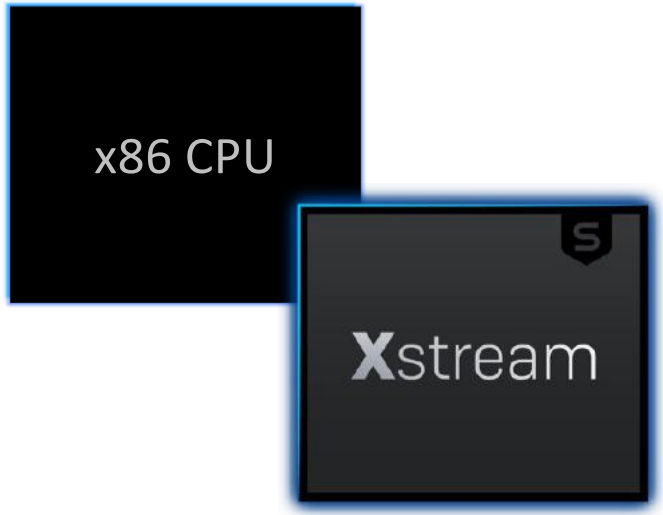
XGS 5500
XGS 6500
XGS 7500
XGS 8500

SOPHOS

Architektur

SOPHOS

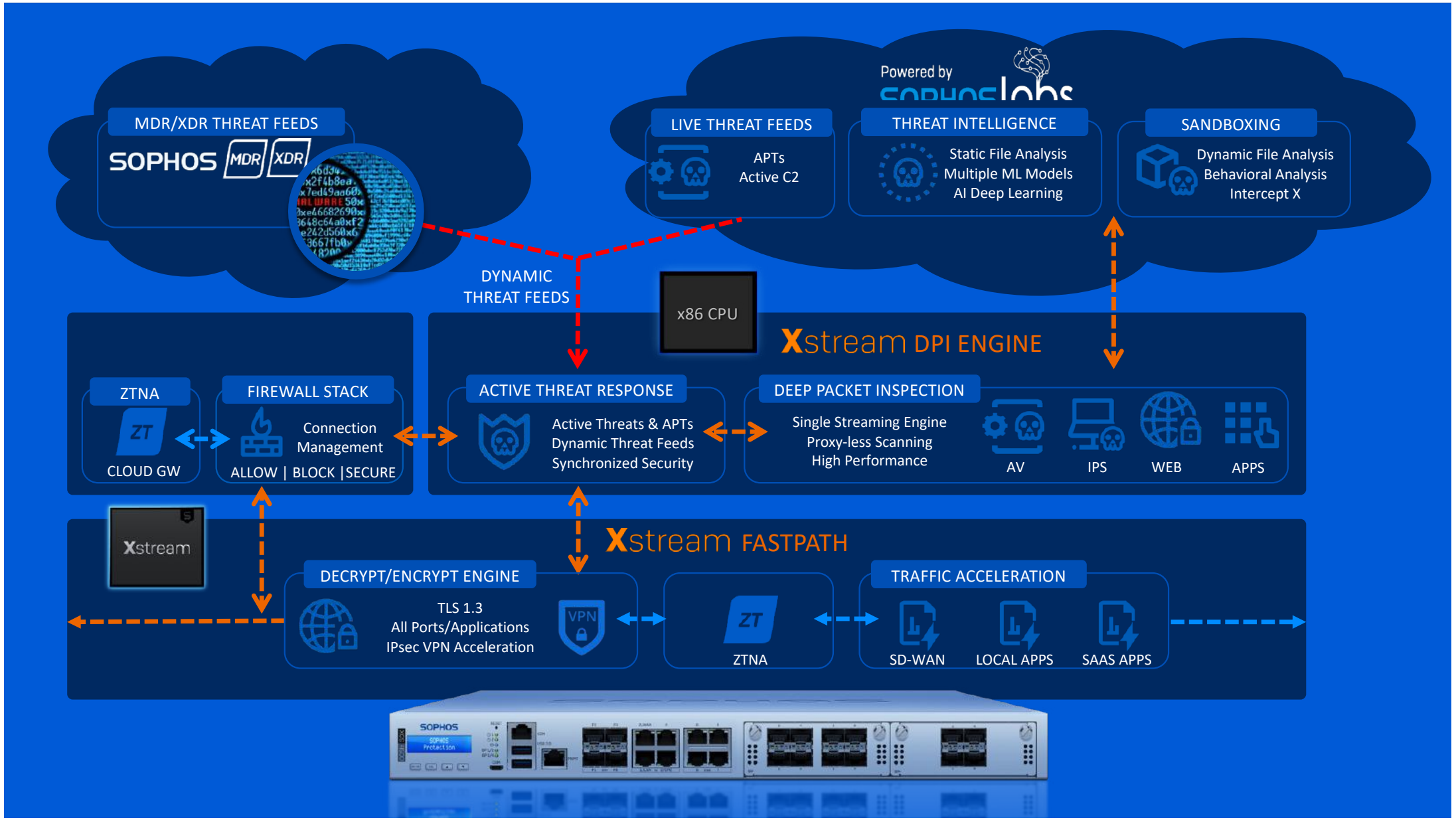
Sophos XGS Hardware Beschleunigung



Neue Dual Prozessor Architektur
x86 CPU plus Sophos eigener
Xstream Flow Processor

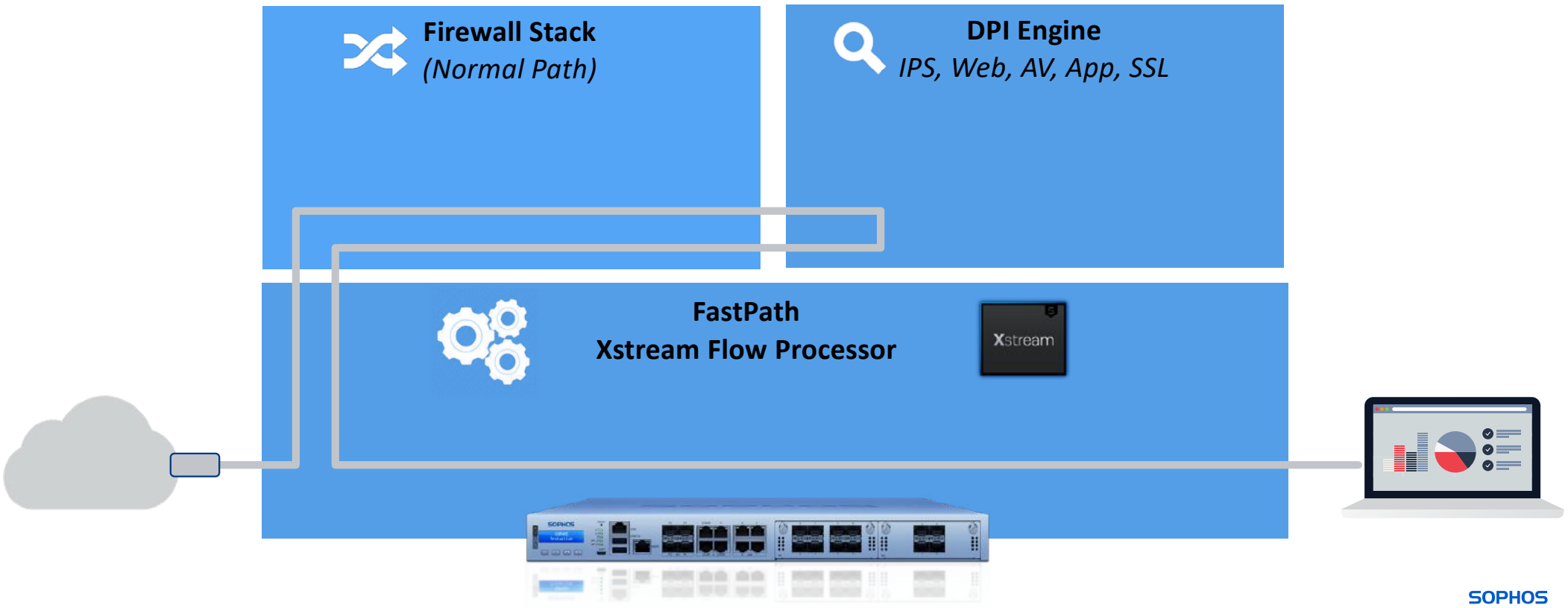
x86 CPU (AMD)
Routing, Connection Management,
Deep Packet Inspection, TLS Inspection

Xstream Flow Processor (Marvell NPU)
Xstream Hardware FastPath
IPsec Beschleunigung


MDR/XDR THREAT FEEDS
SOPHOS MDR XDR
Powered by SOPHOS labs
LIVE THREAT FEEDS
APTs
Active C2
THREAT INTELLIGENCE
Static File Analysis
Multiple ML Models
AI Deep Learning
SANDBOXING
Dynamic File Analysis
Behavioral Analysis
Intercept X
DYNAMIC
THREAT FEEDS
x86 CPU
Xstream DPI ENGINE
ZTNA
ZT
CLOUD GW
FIREWALL STACK
Connection
Management
ALLOW | BLOCK |SECURE
ACTIVE THREAT RESPONSE
Active Threats & APTs
Dynamic Threat Feeds
Synchronized Security
DEEP PACKET INSPECTION
Single Streaming Engine
Proxy-less Scanning
High Performance
AV
IPS
WEB
APPS
Xstream
Xstream FASTPATH
DECRYPT/ENCRYPT ENGINE
TLS 1.3
All Ports/Applications
IPsec VPN Acceleration
VPN
ZT
ZTNA
TRAFFIC ACCELERATION
SD-WAN
LOCAL APPS
SAAS APPS
SOPHOS

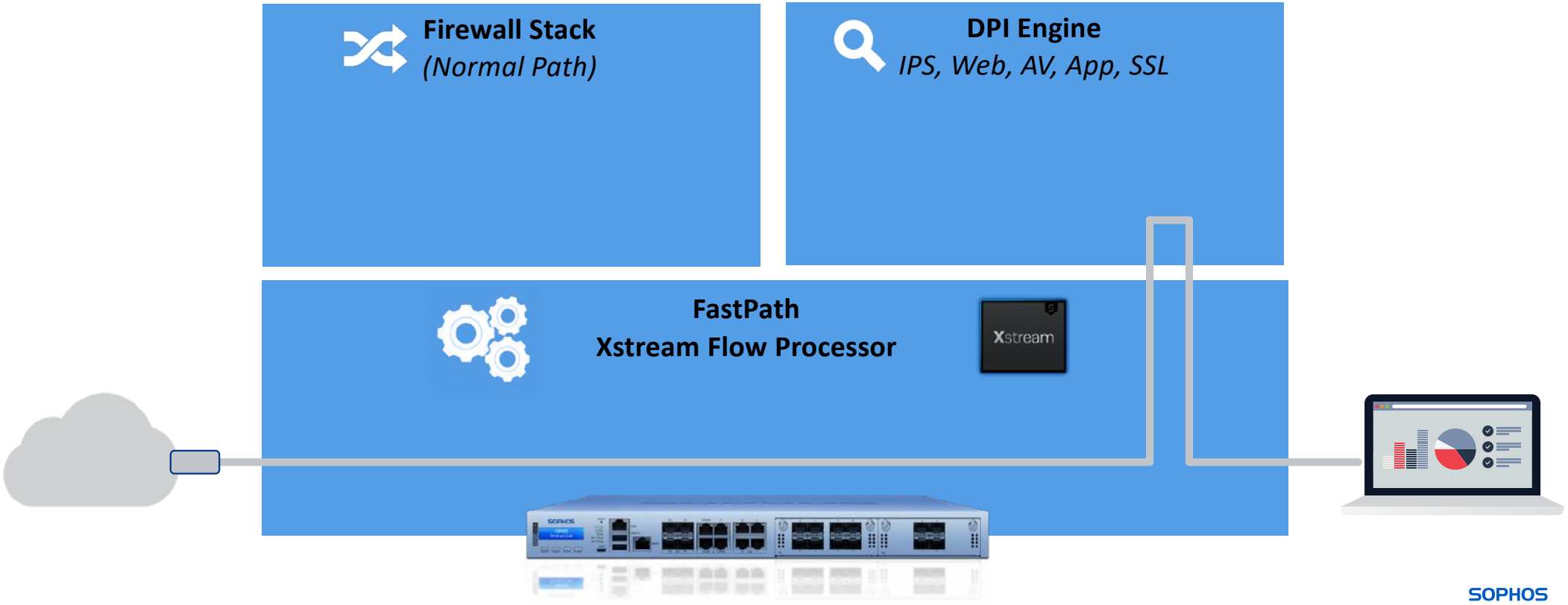
Meeting Webinar

Schritt 1) Initiale Übermittlung von Paketen an Kernel & DPI Engine über SlowPath



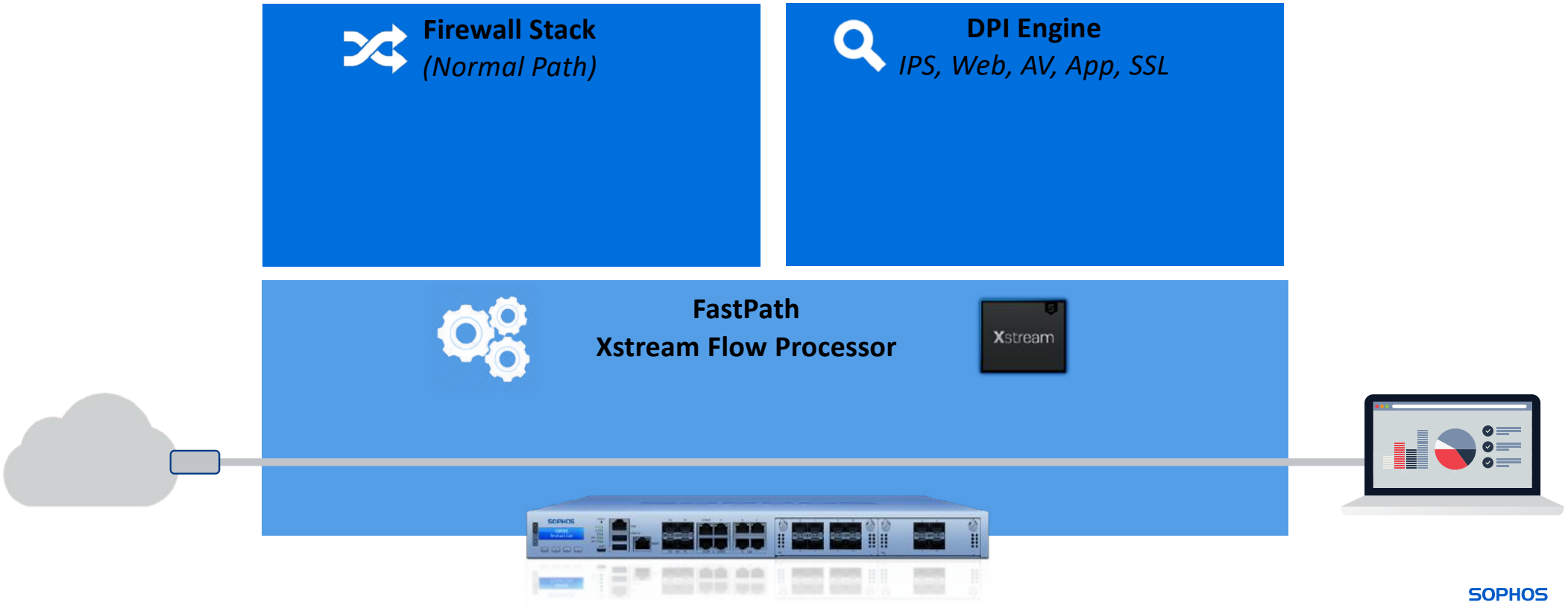
Meeting Webinar

Schritt 2) Die Firewall übergibt den Datenfluss an die DPI-Engine zur Sicherheitsüberprüfung



Meeting Webinar

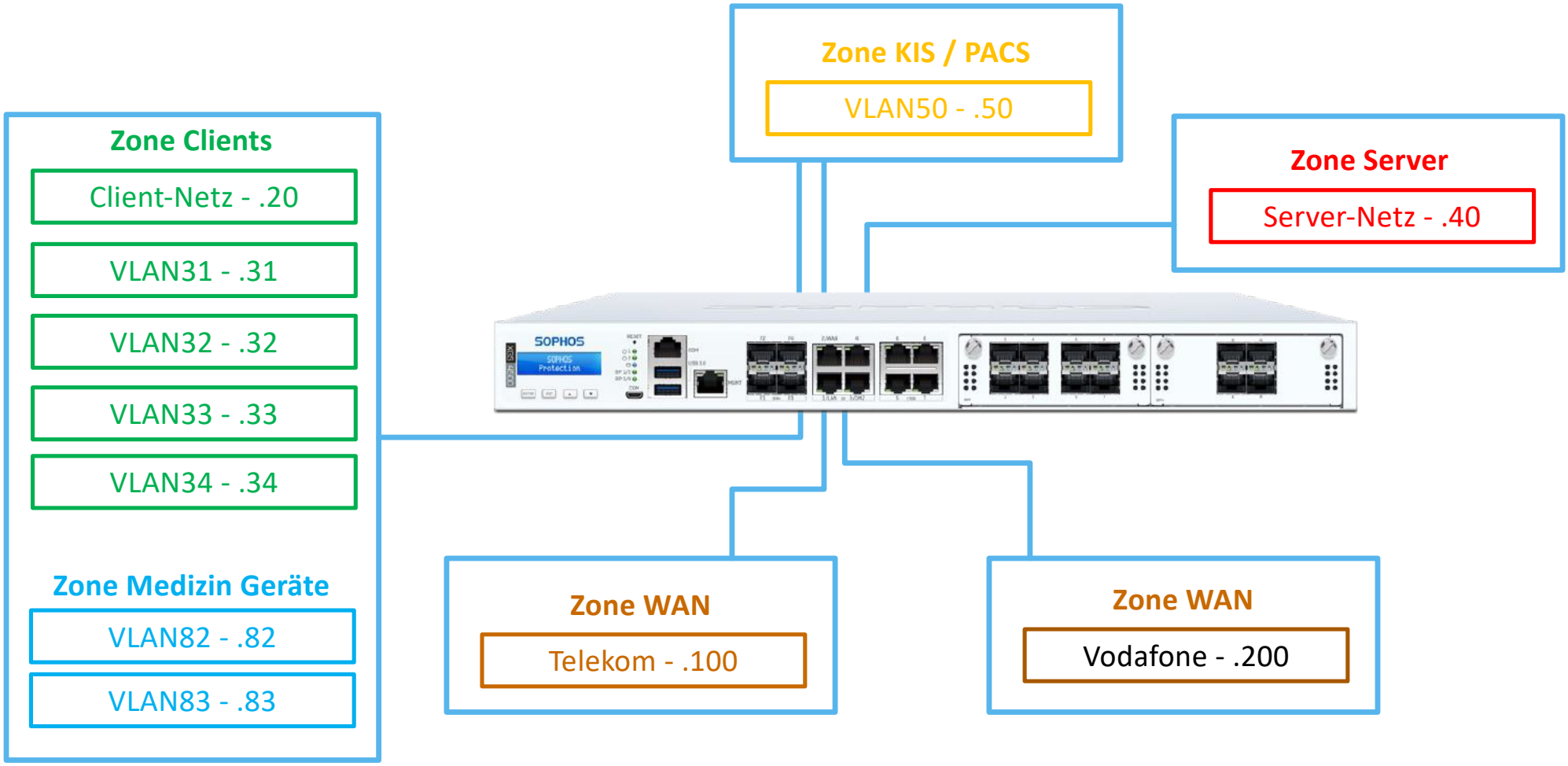
Schritt 3) Wenn der Datenstrom als sicher eingestuft wird, kann die DPI-Engine an den Xstream-Flow-Prozessor übergeben werden



Zonenkonzept

SOPHOS

Zonenkonzept



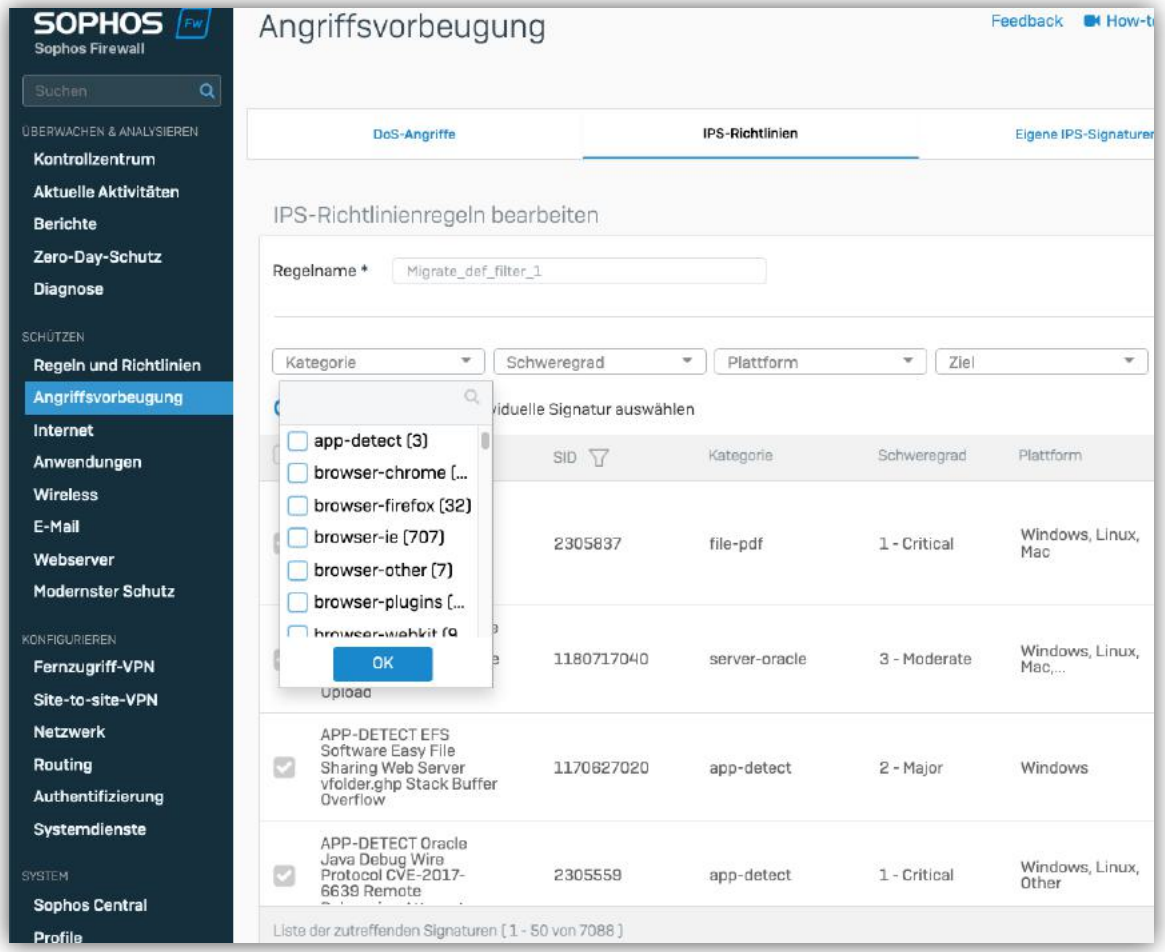
Intrusion Prevention System (IPS)

Wie funktioniert es?

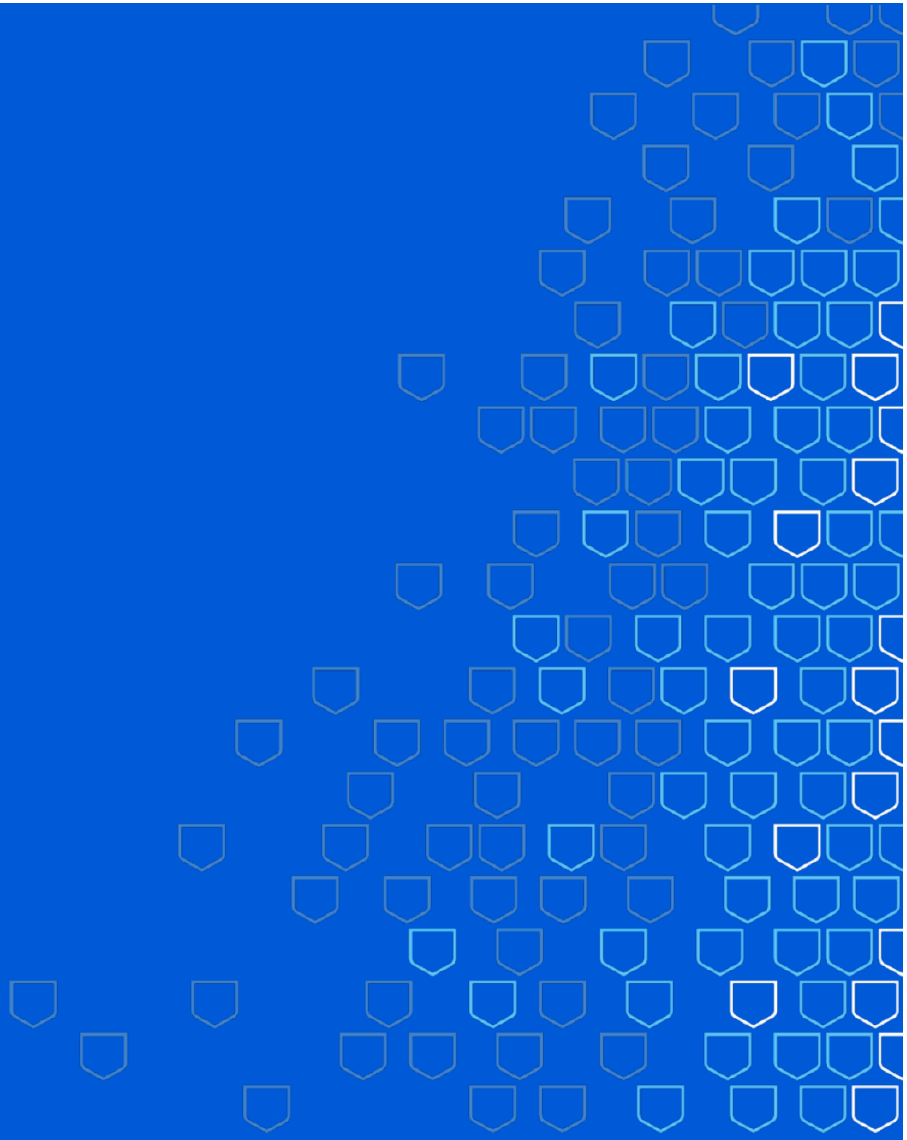
- Untersucht den Netzwerkverkehr auf Anzeichen von Exploits
- Kann Angriffe auf Betriebssysteme, Netzwerk-Stacks, Server, Endpunkte, Browser, Anwendungen und mehr erkennen

Features

- Höchste Sicherheitseffektivität und Leistung
- Von den SophosLabs erstellte und kuratierte Signaturen zusammen mit Cisco Talos-Signaturen
- Empfohlen von den NSS Labs
- Granulare Kategorien erleichtern die Feinabstimmung von Leistung/Schutz



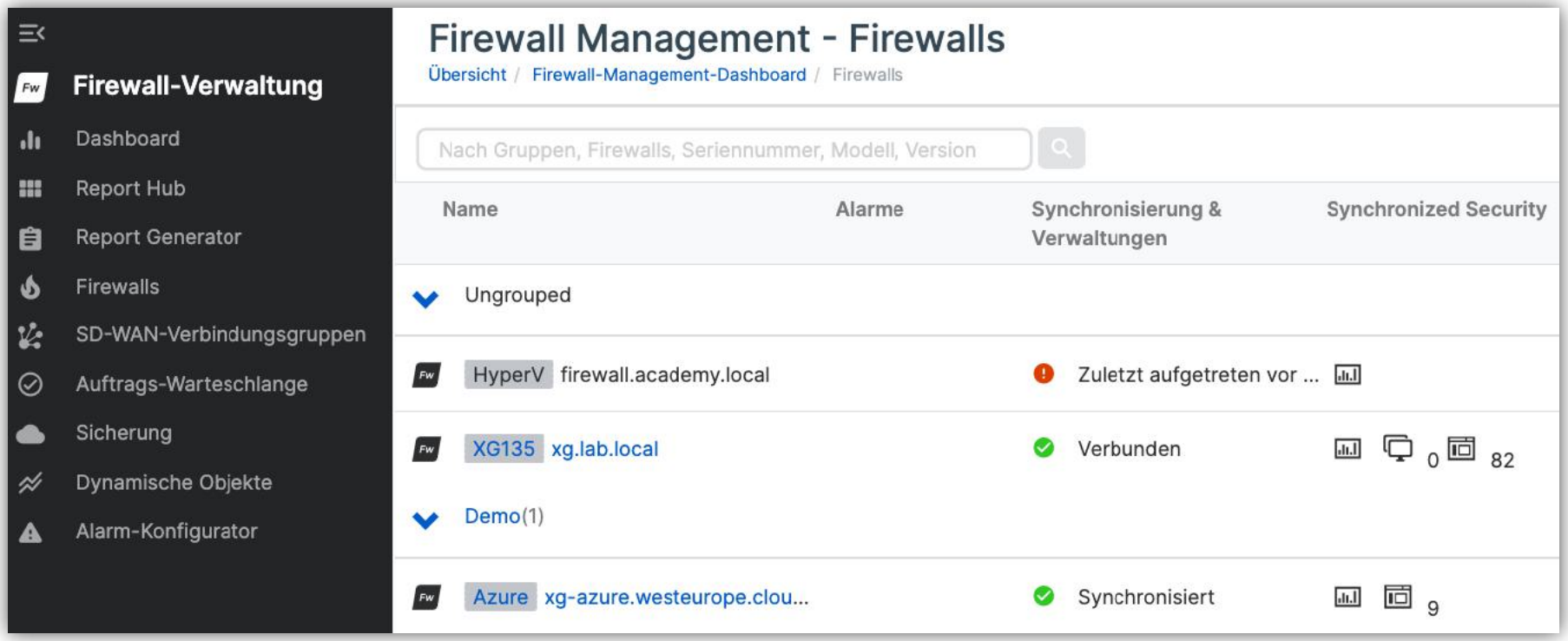
Central Management



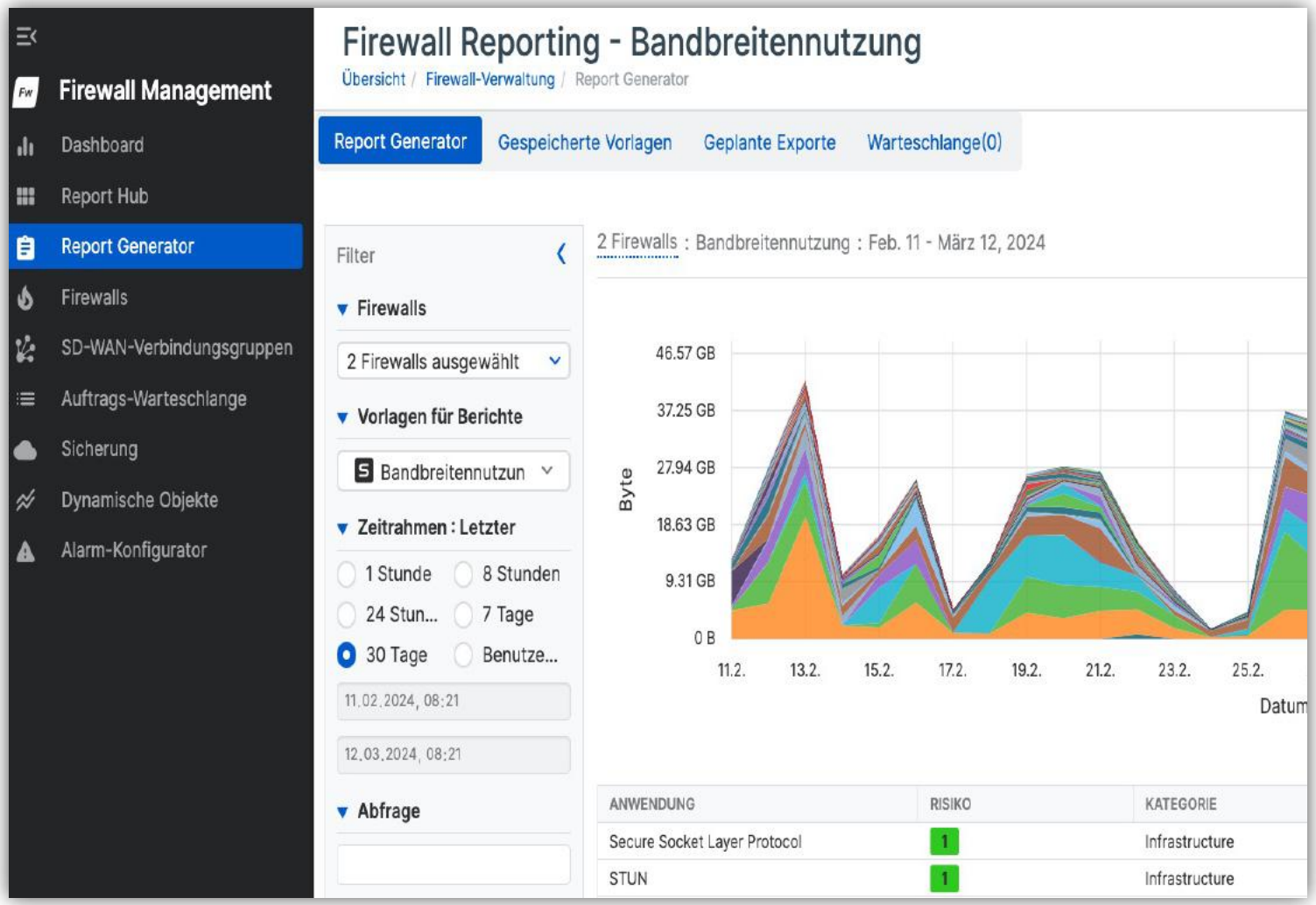
SOPHOS

Central Management

- Erstellung von Firewall Gruppen (inkl. Policy)
- Definition von globalen Objekten



Reporting


Firewall Management
Dashboard
Report Hub
Report Generator
Firewalls
SD-WAN-Verbindungsgruppen
Auftrags-Warteschlange
Sicherung
Dynamische Objekte
Alarm-Konfigurator
Firewall Reporting - Bandbreitennutzung
Übersicht / Firewall-Verwaltung / Report Generator
Report Generator
Gespeicherte Vorlagen
Geplante Exporte
Warteschlange(0)
Filter
Firewalls
2 Firewalls ausgewählt
Vorlagen für Berichte
Bandbreitennutzun
Zeitrahmen : Letzter
1 Stunde
8 Stunden
24 Stun...
7 Tage
30 Tage
Benutze...
11.02.2024, 08:21
12.03.2024, 08:21
Abfrage
2 Firewalls : Bandbreitennutzung : Feb. 11 - März 12, 2024
46.57 GB
37.25 GB
27.94 GB
18.63 GB
9.31 GB
0 B
Byte
11.2.
13.2.
15.2.
17.2.
19.2.
21.2.
23.2.
25.2.
Datum
ANWENDUNG
RISIKO
KATEGORIE
Secure Socket Layer Protocol
1
Infrastructure
STUN
1
Infrastructure

Mehrwerte in der Sophos Firewall

- Synchronized Security
- Zone Based Firewalling
- IKEv2 und Route based VPN
- Enterprise NAT
- SD-WAN policy-based routing
- Sophos Connect
- Next Generation IPS
- Xstream Architecture
- Light Touch Deployment
- Central Integration

Die nächsten Schritte

Entscheidungsvorlage für IT-Leiter und Geschäftsführer

Jetzt downloaden

Podcast

Cybersecurity für kritische Infrastrukturen – was KRITIS-Unternehmen aus gesetzlicher Sicht beachten müssen mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB.

Zum Podcast

IT-Sicherheitsgesetz und Kritis

Das neue IT-Sicherheitsgesetz 2.0 betrifft nicht nur KRITIS-Betreiber in Deutschland, sondern auch deren Lieferanten in anderen Ländern. Weitere Informationen erhalten Sie auf unserer Webseite.

sophos.de/it-sicherheitsgesetz

Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

gesundheitswesen@sophos.de

SOPHOS

SOPHOS