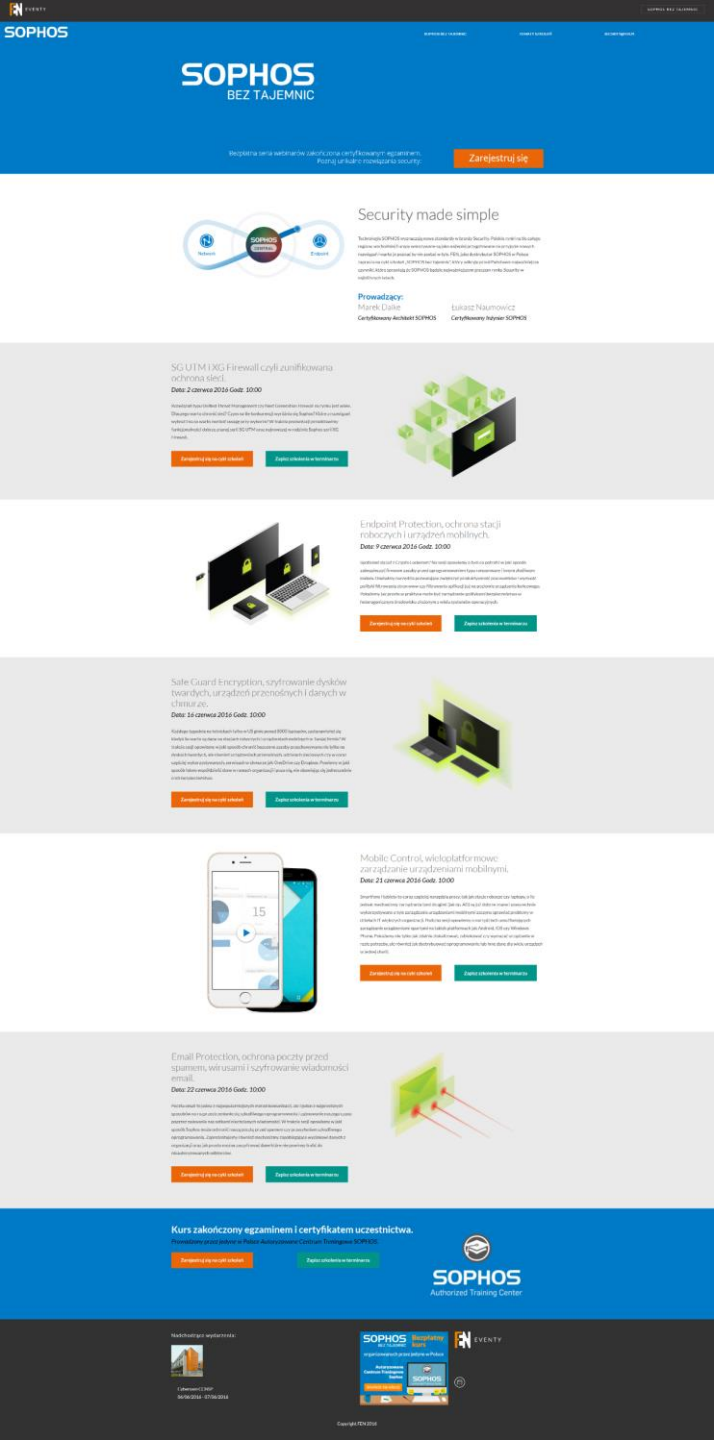
SOPHOS BEZ TAJEMNIC

Sophos SG UTM i XG Firewall
zunifikowana ochrona sieci

Marek Dalke
Sophos Certified Architect & Authorized Trainer
Konsorcjum FEN Sp. z o.o.

02.06.2016



http://event.fen.pl/sophos-bez-tajemnic

Certyfikat uczestnictwa

- Certyfikat w formie cyfrowej (PDF) potwierdzający uczestnictwo w cyklu webinarów „SOPHOS bez tajemnic”.
- Dokument wysyłany na adres mailowy wprowadzony podczas rejestracji.

Warunki uzyskania

- Obecność na min 3 sesjach w ramach cyklu „SOPHOS bez tajemnic”.
- Zaliczenie egzaminu końcowego z tematyki kursu.

Egzamin

- Test wyboru, ok. 20 pytań.
- Link do testu udostępniony mailowo i podczas ostatniej sesji.
- Czas na zaliczenie to 14 dni licząc od daty ostatniej sesji (do 6 lipca 2016).
- Zaliczenie oznacza prawidłową odpowiedź na przynajmniej 80% pytań.
- Do egzaminu można podchodzić wielokrotnie.

SOPHOS Home

W ramach cyklu, każdy z uczestników dostanie dostęp do darmowej licencji SOPHOS Home do niekomercyjnego użytkowania.

σοφός

(mądry, doświadczony)

Sophos w pigułce

1985
ROK ZAŁOŻENIA
Abingdon, UK

$450M
OBRÓT w FY15
(APPX.)

2,400
PRACOWNICY
(APPX.)

HQ
OXFORD, UK

200,000+
KLIENCI

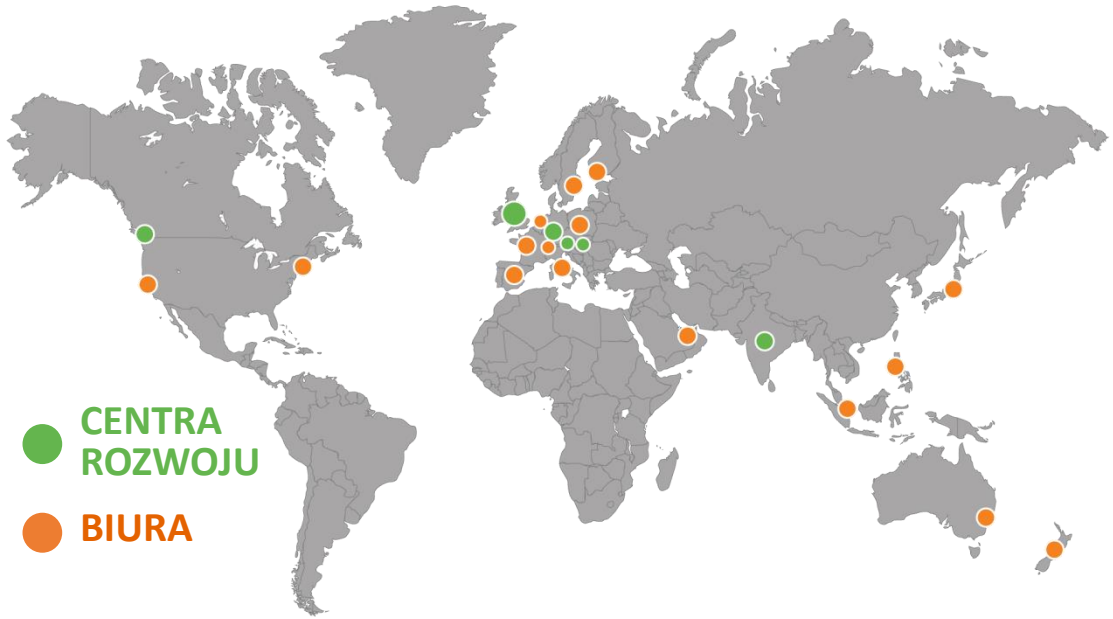
100M+
UŻYTKOWNICY

90+%
ODNOWIENIA
Poziom najwyższy na rynku

15,000+
PERTNERZY

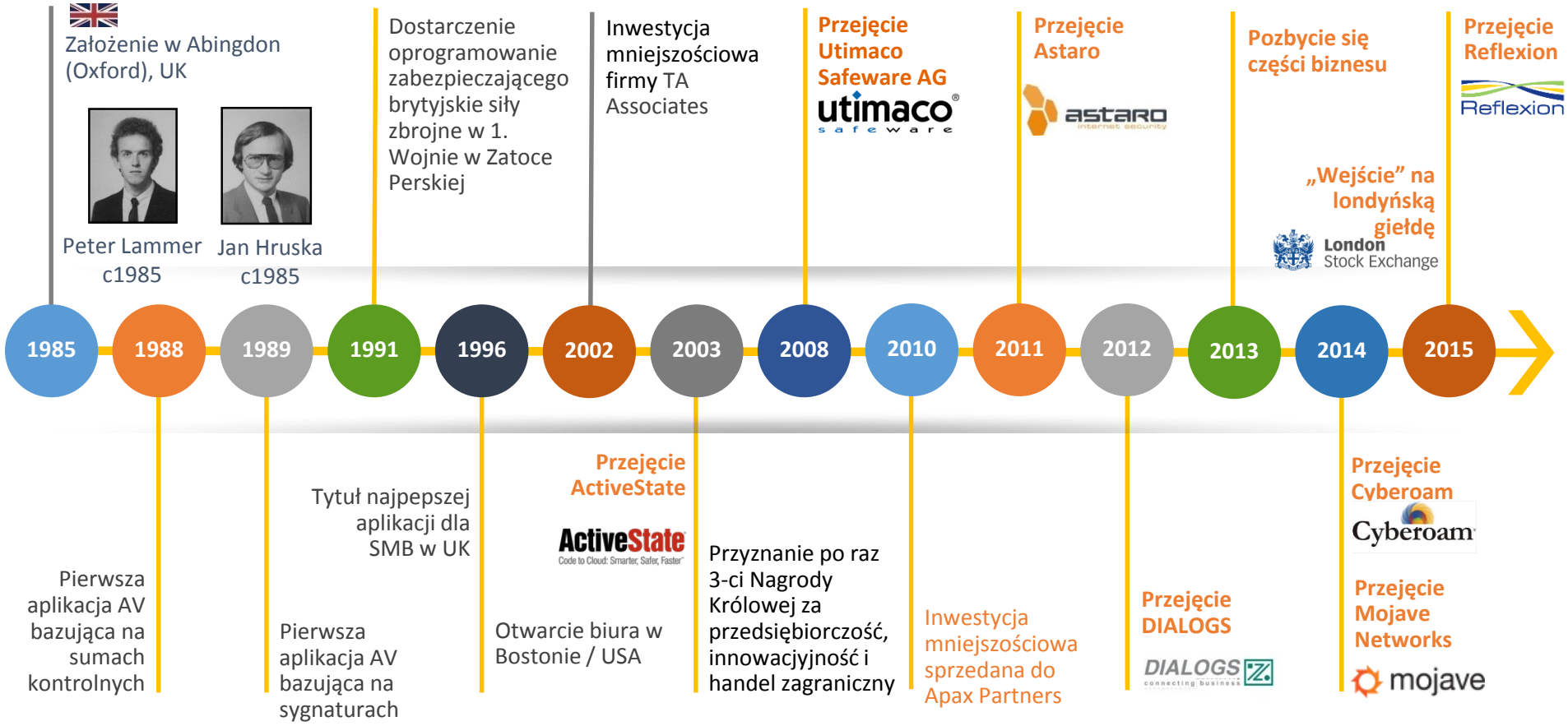
PARTNERZY **OEM**:

CISCO
IBM
JUNIPER NETWORKS
lenovo
CITRIX
rackspace

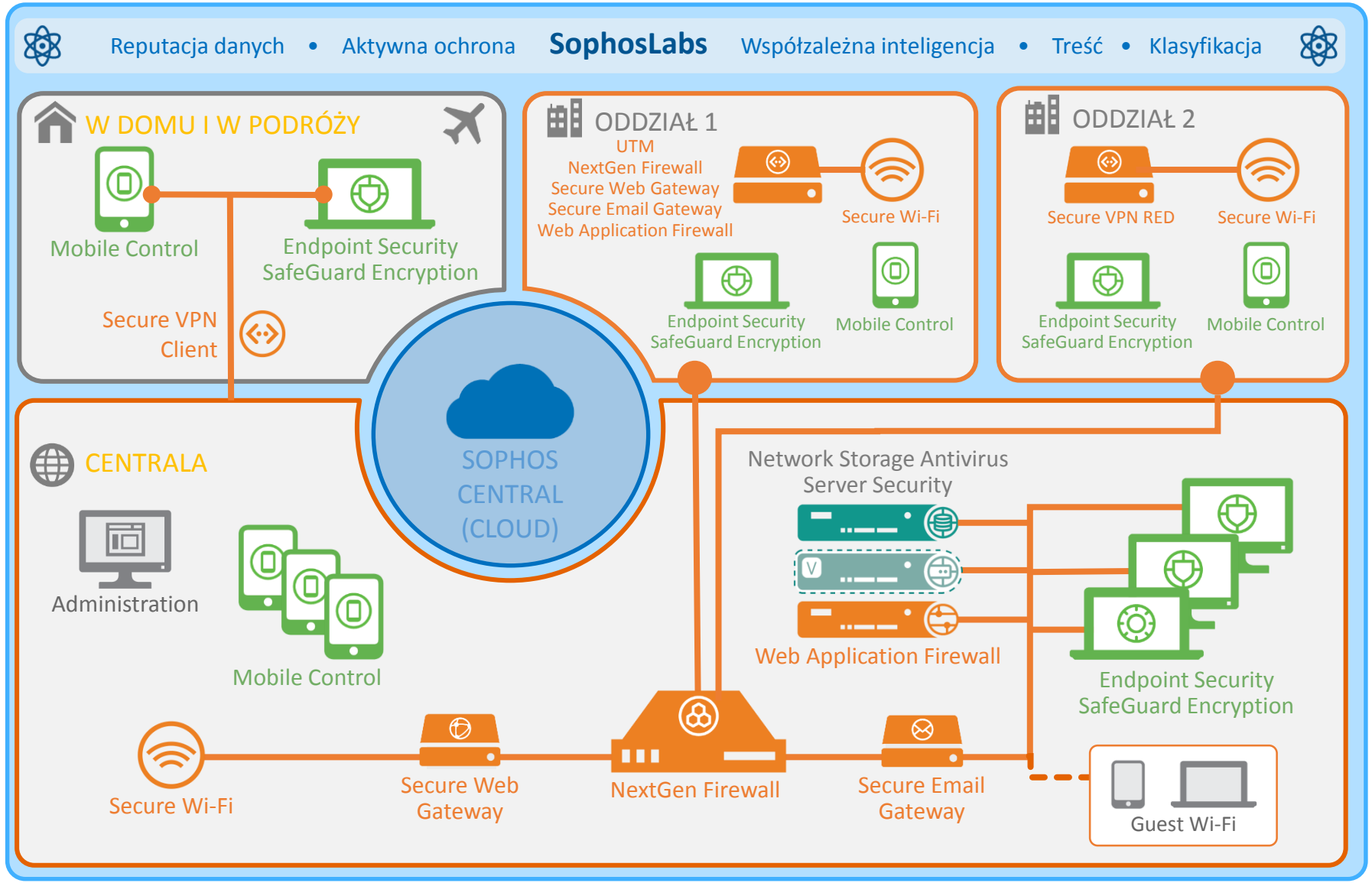


Sophos - Historia

Ewolucja od aplikacji do kompletnego bezpieczeństwa IT



Sophos – kompleksowa ochrona środowiska IT



Enduser and Server Security

- Enduser Protection
- SafeGuard Encryption
- Mobile Control
- Virtual Security
- Server Security
- Network Storage AV

Network Security

- Next-Gen Firewall
- UTM
- Secure Web Gateway
- Secure VPN
- Secure Wi-Fi
- Secure Email Gateway
- Sophos RED

Sophos SG UTM & XG Firewall

SG Series

UTM 9.4

(Astaro)

XG Series

SF-OS v15

(Cyberoam)

Wspólna platforma sprzętowa

Różne oprogramowanie

Możliwa migracja (SG Series is XG Ready)

Które z rozwiązań wybrać?

decyzja należy wyłącznie do klienta lub partnera

Oba rozwiązania warte polecenia

SG Series

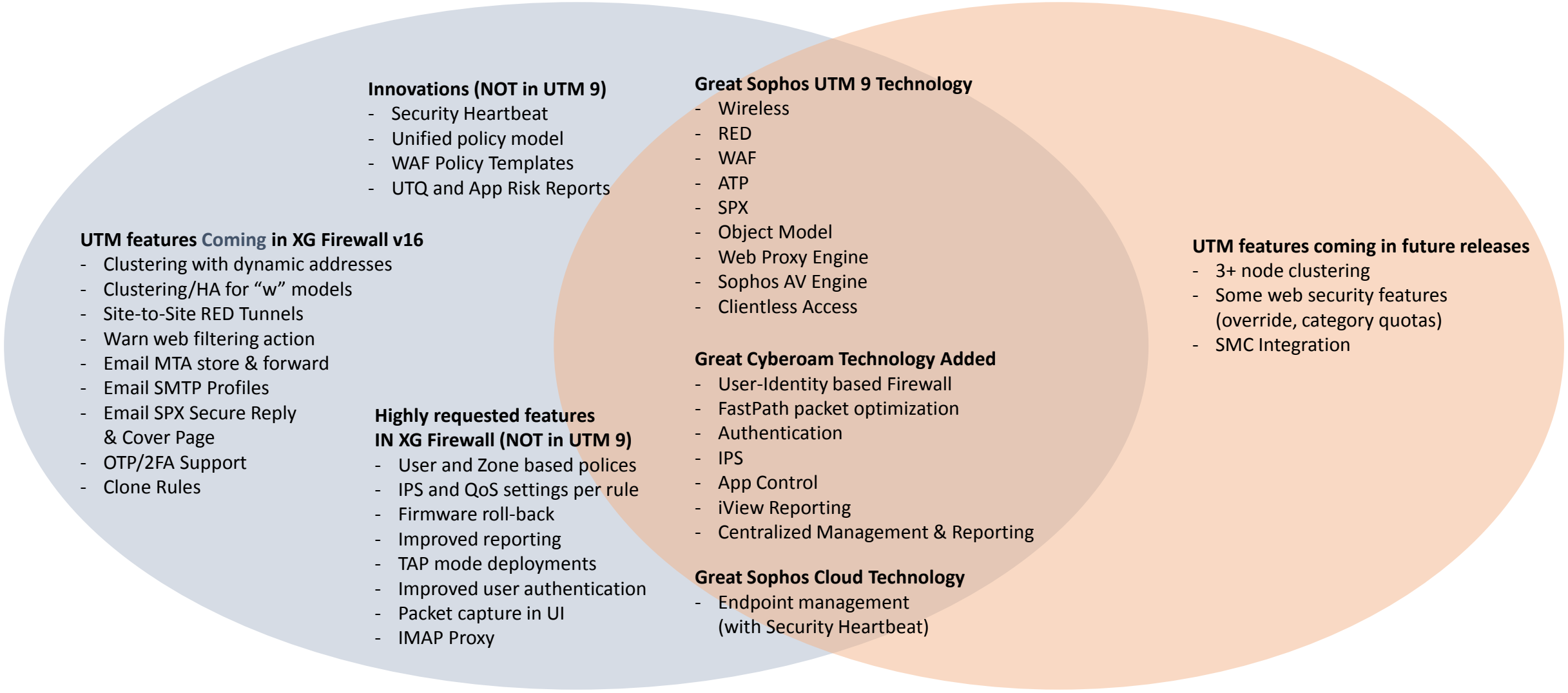
- Sprawdzone rozwiązanie
- Zażyłość i przyzwyczajenie
- Nowa wersja UTM 9.4 (kolejne już na roadmapie)
- Nowe szanse sprzedaży (Sandstorm)

XG Series

- Innowacyjne rozwiązanie
- Nowe funkcje i możliwości
- Nowa wersja v16 w połowie 2016
- Nowe szanse sprzedaży (Heartbeat)

Funkcjonalności XG vs SG

Podjęcie decyzji o migracji tak proste, jak sam proces



Innovations (NOT in UTM 9)
- Security Heartbeat
- Unified policy model
- WAF Policy Templates
- UTQ and App Risk Reports

UTM features Coming in XG Firewall v16
- Clustering with dynamic addresses
- Clustering/HA for “w” models
- Site-to-Site RED Tunnels
- Warn web filtering action
- Email MTA store & forward
- Email SMTP Profiles
- Email SPX Secure Reply & Cover Page
- OTP/2FA Support
- Clone Rules

Highly requested features IN XG Firewall (NOT in UTM 9)
- User and Zone based polices
- IPS and QoS settings per rule
- Firmware roll-back
- Improved reporting
- TAP mode deployments
- Improved user authentication
- Packet capture in UI
- IMAP Proxy

Great Sophos UTM 9 Technology
- Wireless
- RED
- WAF
- ATP
- SPX
- Object Model
- Web Proxy Engine
- Sophos AV Engine
- Clientless Access

Great Cyberoam Technology Added
- User-Identity based Firewall
- FastPath packet optimization
- Authentication
- IPS
- App Control
- iView Reporting
- Centralized Management & Reporting

Great Sophos Cloud Technology
- Endpoint management (with Security Heartbeat)

UTM features coming in future releases
- 3+ node clustering
- Some web security features (override, category quotas)
- SMC Integration

https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/Datasheets/Unified/sophos-sf-os-vs-utm-feature-list.pdf?la=en

https://blogs.sophos.com/2015/11/09/xg-firewall-faq

Powody dla których warto rozważyć zakup SG lub XG?

Ponieważ obie platformy …

SG Series

XG Series

1. są proste w obsłudze
2. są wydajne
3. integrują wiele usług bezpieczeństwa
4. oferują wbudowane raportowanie
5. pochodzą od lidera branży bezpieczeństwa

SOPHOS

Sophos SG (UTM9)

Sophos SG - dostępne modele

Hardware Appliance	SG 85 (new)	SG 105 / 115	SG 125 / 135	SG 210 / 230	SG 310 / 330	SG 430 / 450	SG 550	SG 650
								
Category	Small Desktop	Small Desktop	Small Desktop	Medium Midrange 1U	Medium Midrange 1U	Medium Midrange 1U	Large High-end 2U	Large High-end 2U
Network Ports (standard)	4	4	8	6	8 & 2 SFP	8 (FleXi Port)	8 (FleXi Port)	8 (FleXi Port)
FleXi Port Expansion Bays	n/a	n/a	n/a	1	1	2	3	4
Maximum Ports	4	4	8	14	18	24	24	32
Redundancy	n/a	n/a	n/a	n/a	n/a	2 SSD (RAID) & 2nd hot-swap power optional (SG 450 only)	2 hot-swap SSD (RAID) 2 hot-swap power supplies	2 hot-swap SSD (RAID) 2 hot-swap power supplies
Wireless	Integr. 802.11n optional	Integr. 802.11n optional	Integr. 802.11ac optional	n/a	n/a	n/a	n/a	n/a

Moduły bezpieczeństwa

new

Sandstorm Protection

- Cloud based sandboxing
- Evasive threat protection
- Policy control
- Detailed reporting

Wireless Protection

- Wireless Controller for Access Points
- Multi-Zone (SSID) support
- Hotspot Support

Essential Firewall

- Stateful Firewall
- Object based rules
- User self-service portal

Network Protection

- Intrusion Prevention (IPS)
- Client & Site-to-Site VPN
- Quality of Service (QoS)
- Advanced Threat Prot. (ATP)

Web Server Protection

- Reverse Proxy
- Web Application Firewall
- Antivirus

Web Protection

- URL Filtering Policies
- Web Threat Protection
- Application Control

Mail Protection

- Anti Spam & Phishing
- Dual Virus Protection
- DLP & Encryption

Licencjonowanie

Moduły ochrony	Subskrypcje indywidualne	Pakiet BasicGuard *	Pakiet FullGuard
Essential Firewall (Licencja Bazowa) Network Firewall, NAT, Native Windows Remote Access	Tak	Tak	Tak
Network Protection IPSec/SSL, ATP, VPN, IPS, QoS, DoS	Tak	Basic	Full
Web Protection URL Filtering, Application Control, Dual Engine Antivirus	Tak	Basic	Full
Email Protection Anti-spam, Email Encryption and DLP, Dual Engine Antivirus	Tak	Basic	Full
Wireless Protection Wireless Controller, Multi-SSID Support, Captive Portal, Hotspot	Tak	Basic	Full
Webserver Protection Web Application Firewall, Reverse Proxy, Antivirus	Tak	-	Full
Sandstorm Protection Cloud-based Sandboxing	Tak	Opcja	Opcja

ToalProtect = FullGuard + Hardware

Rejestracja i zarządzanie licencjami https://myutm.sophos.com

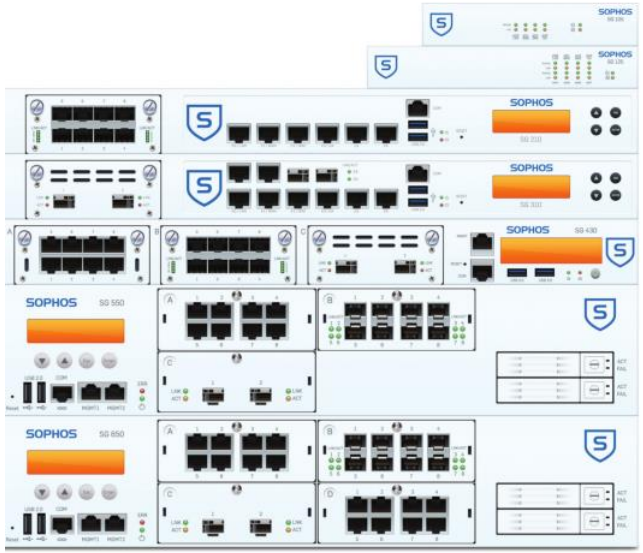
- dotyczy SG105/105w, SG115/115w (https://www.sophos.com/en-us/support/knowledgebase/118423.aspx)

Sophos UTM Sizing Guide

SOPHOS
Security made simple.

Sizing Guideline

Sophos UTM 9.3 - SG Series Appliances



2. Make first estimate — using the calculated "Total UTM User" number

Take the "Total UTM User" and make a first estimate for the required SG Series hardware appliance within the following diagram:

- Each line shows the range of users recommended when only using this single subscription.
- Please ensure all numbers include users connected via VPN, RED and wireless APs.

Subscription Profile

Rule of thumb:

- Estimate that adding Wireless Protection, Webserver Protection or Endpoint Protection to any of the subscription profiles mentioned above will decrease range by 5-10% each.

3. Check for specific throughput requirements

Depending on the customer's environment there might be specific throughput requirements driving an adjustment of your first estimate to a higher (or even lower) unit.

These requirements are typically based on the following two factors:

The maximum available internet uplink capacity

The capacity of the customer's internet connection (up- and downlink) should match the average throughput rate that the selected unit is able to forward (depending on the subscriptions in use).

For instance if the download or upload limit is only 20 Mbps then there is no great benefit in using an SG 230 instead of an SG 210, even though the calculated total number of users is around 100. In that case even an SG 210 might be sufficient because it can perfectly fill the complete internet link even with all UTM features enabled.

However data might not only be filtered on its way to the internet but also between internal network segments. Hence consider internal traffic that traverses the firewall as well in this assessment.

Specific performance requirements based on customer experience or knowledge

If the customer knows their overall throughput requirements among all connected internal and external interfaces (e.g. based on their past experience) then check whether the selected unit is able to meet these numbers.

For instance the customer might have several servers located within a DMZ and want to get all traffic to those servers from all segments to be inspected by the IPS. Or the customer may have many different network segments that should be protected against each other (by using the FW packet filter and/or the Application Control feature). In this case consider that the unit must scan the complete internal traffic between all segments.

Further questions to ask in order to find out if there are any other performance requirements:

- How many site-to-site VPN tunnels are required?
- How many emails are being transferred per hour - on average/at peak times?
- How much web traffic (Mbps and requests/s) is being generated - on average/at peak times?
- How many web servers should be protected and how much traffic is expected - on average/at peak times?

The following section provides detailed performance numbers to help determine whether the selected appliance meets all individual requirements.

Sophos SG Series Hardware performance numbers

The following table provides performance numbers by traffic type measured within Sophos testing labs. Realworld numbers represent throughput values achievable with a typical/real life traffic mix, maximum numbers represent best throughput achievable under perfect conditions, e.g. using large packet sizes.

Please note that none of these numbers are guaranteed as performance may vary in a real life customer scenario based on user characteristics, application usage, security configurations and other factors. For detailed information please refer to the "Sophos UTM - Performance Test Methodology" document.

Small - Desktop

Model	SG 105/w rev.1	SG 115/w rev.1	SG 125/w rev.1	SG 135/w rev.1
Performance Numbers				
Firewall max.[1] (Mbps)	1,500	2,300	3,100	6,000
Firewall Realworld[2] (Mbps)	1,140	1,630	2,100	3,650
ATP Realworld[2] (Mbps)	1,060	1,470	1,490	2,680
IPS max.[1] (Mbps)	350	500	750	1,500
IPS all rules (Mbps)	175	200	320	590
FW + ATP + IPS max.[1] (Mbps)	310	450	680	1,340
FW + ATP + IPS Realworld[2] (Mbps)	160	190	310	445
App Ctrl Realworld[2] (Mbps)	1,020	1,430	1,790	3,000
VPN AES max.[3] (Mbps)	325	425	500	1,000
VPN AES Realworld[4] (Mbps)	175	220	295	490
Web Proxy plain[5] (Mbps)	215	380	475	850
Web Proxy – AV[5] (Mbps)	90	120	200	350
Web requests/sec[5] – AV	380	500	900	1,650
Maximum recommended connections				
New TCP connections/sec	15,000	20,000	24,000	36,000
Concurrent TCP connections	1,000,000	1,000,000	2,000,000	2,000,000
Concurrent IPsec VPN tunnels	80	145	175	250
Concurrent SSL VPN tunnels	35	55	75	120
Concurrent Endpoints	10	20	30	40
Concurrent Access Points	10	20	30	40
Concurrent REDs (UTM/FW)	10/30	15/60	20/80	25/100

1. 1518 byte packet size (UDP), default rule set
2. NSS Perimeter Mix (TCP/UDP)
3. AES-NI with AES (ECM where possible (UDP)
4. NSS Core Mix (TCP/UDP)
5. Throughput: 100kByte files, requests/sec: 1Kbyte files (numbers are for single scan, throughput will decrease by 15-20% when dual scan is activated)
6. Technical limit

Sizing Guide: https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/SalesGuidance/sophos-sg-series-sizing-guide.pdf?la=en

Sandstorm Protection

Sandbox w chmurze

- Nowa działająca w chmurze technologia określana mianem next-generation sanbox.
- Narzędzie do wykrywania, blokowania i raportowania ataków celowanych, zagrożeń zero-day (nieznanych) czy evasive (wymijających).
- Odizolowane środowisko wykorzystywane do kontrolowanego uruchamiania podejrzanego kodu dołączonego do korespondencji email lub oprogramowania pobieranego przez web celem analizy pod kątem malware.
- Prosta i szybka integracja z Sophos UTM, Web Gateway, Emal Gateway (XG Firewall pod koniec roku)
- Wymagana osobna licencja

Sandstorm wykorzystywany jest do dodatkowej analizy ponad 20 rodzajów plików:

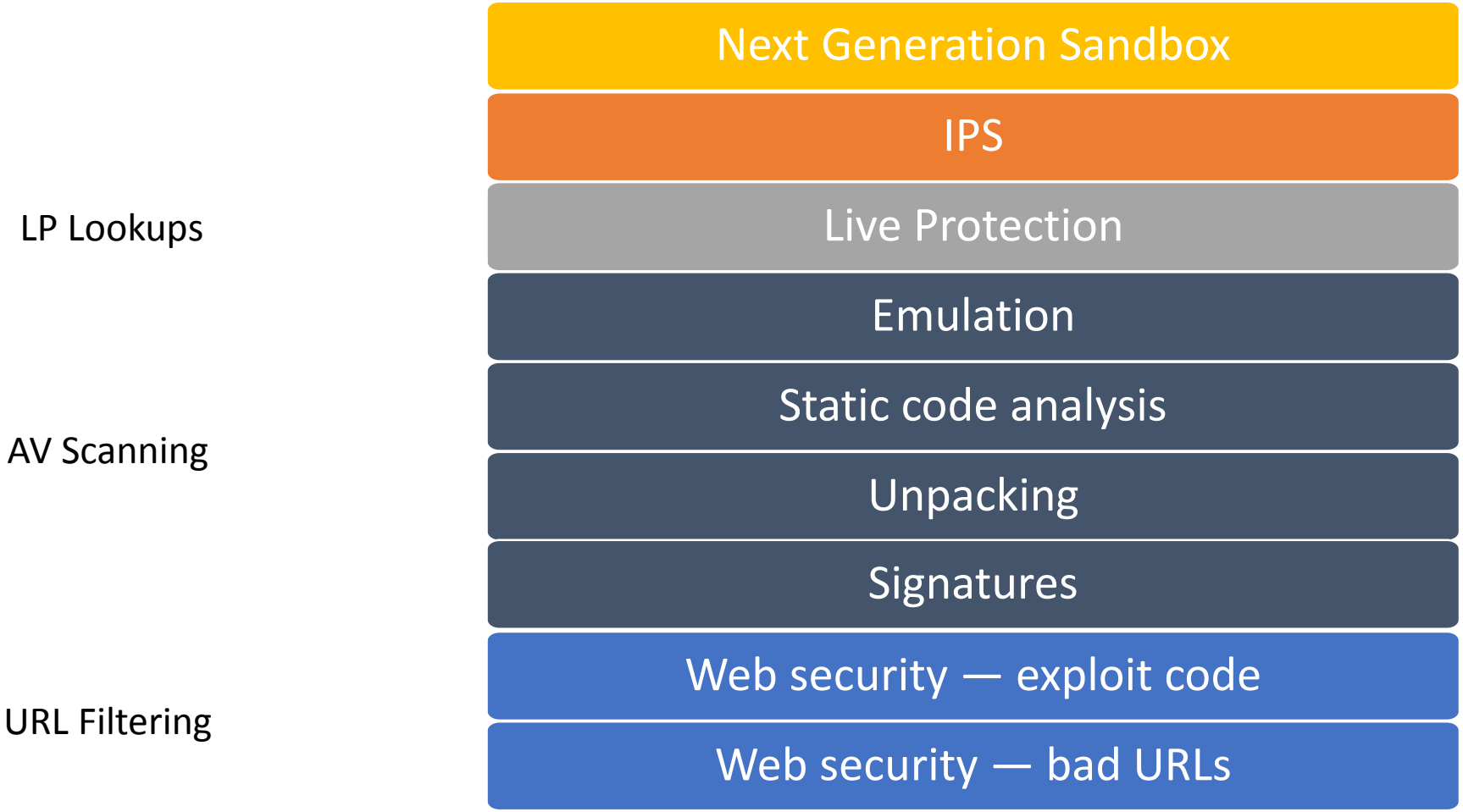
✓ wykonywalnych (*.exe, *.com, *.dll)

✓ dokumentów Word (*.doc, *.docx, *.docm, *.rtf)

✓ dokumentów PDF (*.pdf)

✓ archiwów (*.zip, *.bgzip, *.gzip, *.rar, *.tar, *.lha/lzh, *.7z, *.cab)

Sandstorm - rozszerzona ochrona



Jak to działa? Sophos Sandstorm

UTM 9.4 - Porównanie z konkurencją

	Sophos UTM *Elevated* 9.4	Fortinet 20-90	Dell SonicWall TZ Series	WatchGuard XTM
Network Firewall Protection	✓	✓	✓	✓
Advanced Threat Protection	✓	✓	✓	✓
Advanced Sandboxing	✓ new			
Sophos Authentication Agent	✓ new	✓		✓
Secure Web Gateway	✓	✓	✓	✓
Complete Email: AV, AS, Encrypt, DLP	✓	+1box	+1box	+1box
Dual antivirus engines	✓			
Secure Wi-Fi	✓	✓	✓	✓
Reverse Proxy	✓			
Web Application Firewall (WAF)	✓	+1box	+1box	
User Portal	✓	✓		
Full Reporting	✓	+1box	+1box	+1box
Best TMG Feature Parity	✓			

SOPHOS

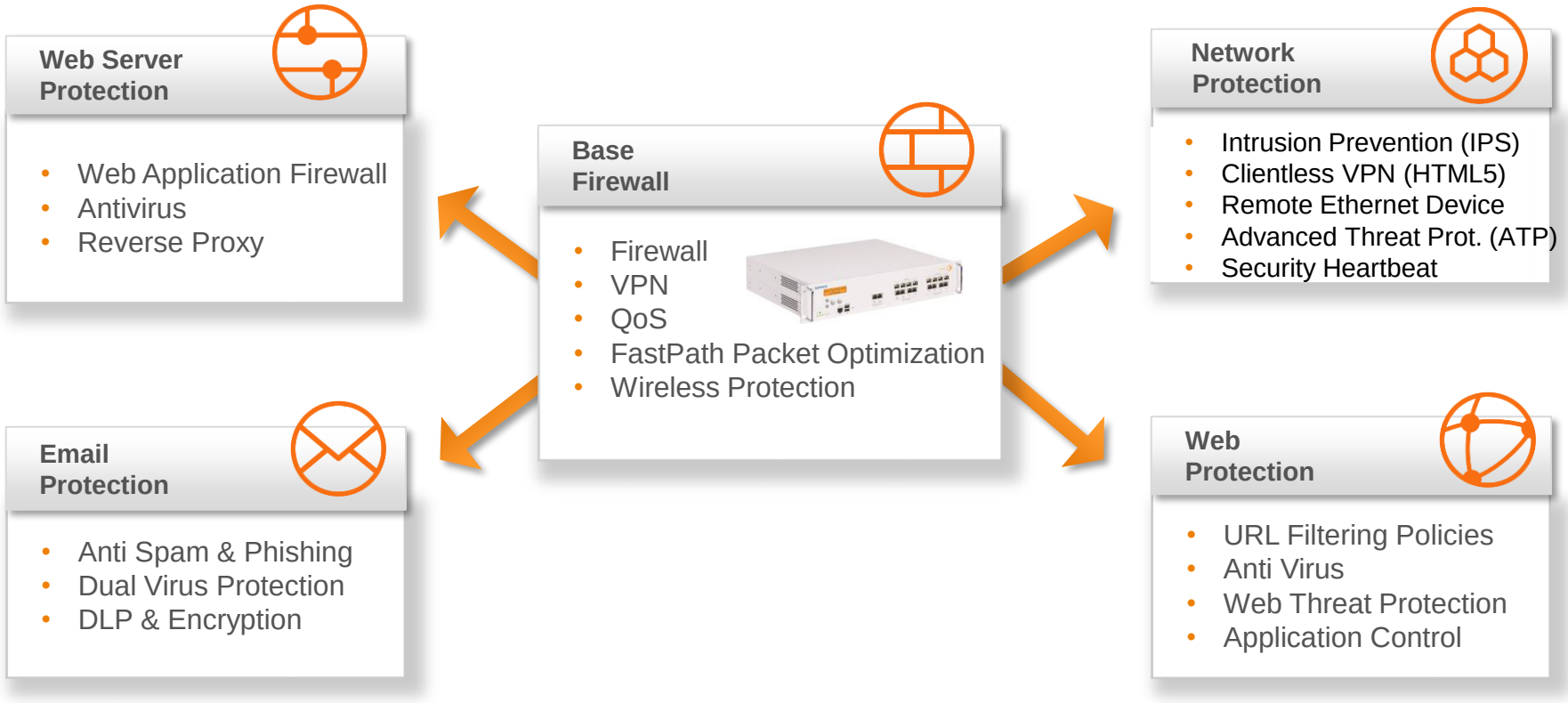
Sophos XG Firewall (SF-OS)

Sophos XG - dostępne modele

Hardware Appliance	XG 85	XG 105 / 115	XG 125 / 135	XG 210 / 230	XG 310 / 330	XG 430 / 450	XG 550	XG 650	XG 750
									
Category	Small Desktop	Small Desktop	Small Desktop	Medium Midrange 1U	Medium Midrange 1U	Medium Midrange 1U	Large High-end 2U	Large High-end 2U	Large High-end 2U
Network Ports (standard)	4	4	8	6	8 & 2 SFP	8 (FleXi Port)	8 (FleXi Port)	8 (FleXi Port)	8 (FleXi Port)
FleXi Port Expansion Bays	n/a	n/a	n/a	1	1	2	3	4	8
Maximum Ports	4	4	8	14	18	24	24	32	64
Redundancy	n/a	n/a	n/a	n/a	n/a	2 SSD (RAID) & 2nd hot-swap power optional (SG 450 only)	2 hot-swap SSD (RAID) 2 hot-swap power supplies	2 hot-swap SSD (RAID) 2 hot-swap power supplies	2 hot-swap SSD (RAID) 2 hot-swap power supplies
Wireless	Integr. 802.11n optional	Integr. 802.11n optional	Integr. 802.11ac optional	n/a	n/a	n/a	n/a	n/a	n/a

Sizing Guide: https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/SalesGuidance/sophos-xg-series-sizing-guide.PDF?la=en

Moduły bezpieczeństwa



Licencjonowanie

Moduły ochrony	Subskrypcje indywidualne	Pakiet EnterpriseGuard	Pakiet FullGuard
Base Firewall (Licencja Bazowa) Network Firewall, NAT, SSL and IPSec VPN Complete Wireless Protection	Tak	Tak	Tak
Network Protection IPS, RED/HTML5, ATP, Security Heartbeat*	Tak	Tak	Tak
Web Protection URL Filtering, Dual AV, Application Control	Tak	Tak	Tak
Email Protection Antispam, AV, SPX, DLP	Tak	Opcja	Tak
Webserver Protection Web Application Firewall, Reverse Proxy, Antivirus	Tak	Opcja	Tak

EnterpriseProtect = EnterpriseProtect + Hardware
ToalProtect = FullGuard + Hardware

Rejestracja i zarządzanie licencjami https://secure2.sophos.com/en-us/login.aspx

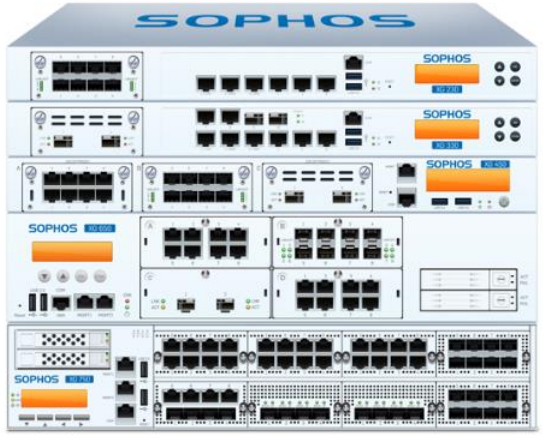
*wymaga Cloud Endpoint Protection Advanced lub Cloud Enduser Protection

Sophos XG Sizing Guide

SOPHOS
Security made simple.

Sizing Guidelines

Sophos XG Firewall - XG Series Appliances

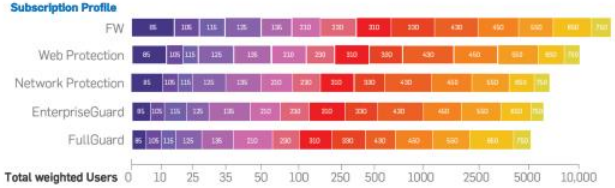


2. Make a first estimate — using the calculated "Total weighted User" number

Take the "Total weighted User" and make a first estimate for the required XG Series hardware appliance within the following diagram:

- Each line shows the range of users recommended when only using this single subscription.
- Please ensure all numbers include users connected via VPN, RED and wireless APs.

Subscription Profile



Rule of thumb:

- Estimate that using Wireless Protection or Webserver Protection with any of the profiles mentioned above will decrease range by 5-10% each.

3. Check for specific throughput requirements

Depending on the customer's environment there might be specific throughput requirements driving an adjustment of your first estimate to a higher (or even lower) unit.

These requirements are typically based on the following two factors:

The maximum available internet uplink capacity

The capacity of the customer's internet connection (up- and downlink) should match the average throughput rate that the selected unit is able to forward (depending on the subscriptions in use).

For instance if the download or upload limit is only 20 Mbps then there is no great benefit in using an XG 230 instead of an XG 210, even though the calculated total number of users is around 100. In that case even an XG 210 might be sufficient because it can perfectly fill the complete internet link even with all UTM features enabled.

However, data might not only be filtered on its way to the internet but also between internal network segments. Hence consider internal traffic that traverses the firewall as well in this assessment.

Specific performance requirements based on customer experience or knowledge

If the customer knows their overall throughput requirements among all connected internal and external interfaces (e.g. based on their past experience) then check whether the selected unit is able to meet these numbers.

For instance the customer might have several servers located within a DMZ and want to get all traffic to those servers from all segments to be inspected by the IPS. Or the customer may have many different network segments that should be protected against each other (by using the FW packet filter and/or the Application Control feature). In this case consider that the unit must scan the complete internal traffic between all segments.

Further questions to ask in order to find out if there are any other performance requirements:

- How many site-to-site VPN tunnels are required?
- How many emails are being transferred per hour - on average/at peak times?
- How much web traffic (Mbps and requests/s) is being generated - on average/at peak times?
- How many web servers should be protected and how much traffic is expected - on average/at peak times?

The following section provides detailed performance numbers to help determine whether the selected appliance meets all individual requirements.

Sophos XG Series Hardware performance numbers

The following table provides performance numbers by traffic type measured within Sophos testing labs. "Realworld" numbers represent throughput values achievable with a typical/real life traffic and protocol mix as defined by NSS Labs. Maximum numbers represent best throughput achievable under perfect conditions, e.g. using large packet sizes with UDP traffic only at full CPU load.

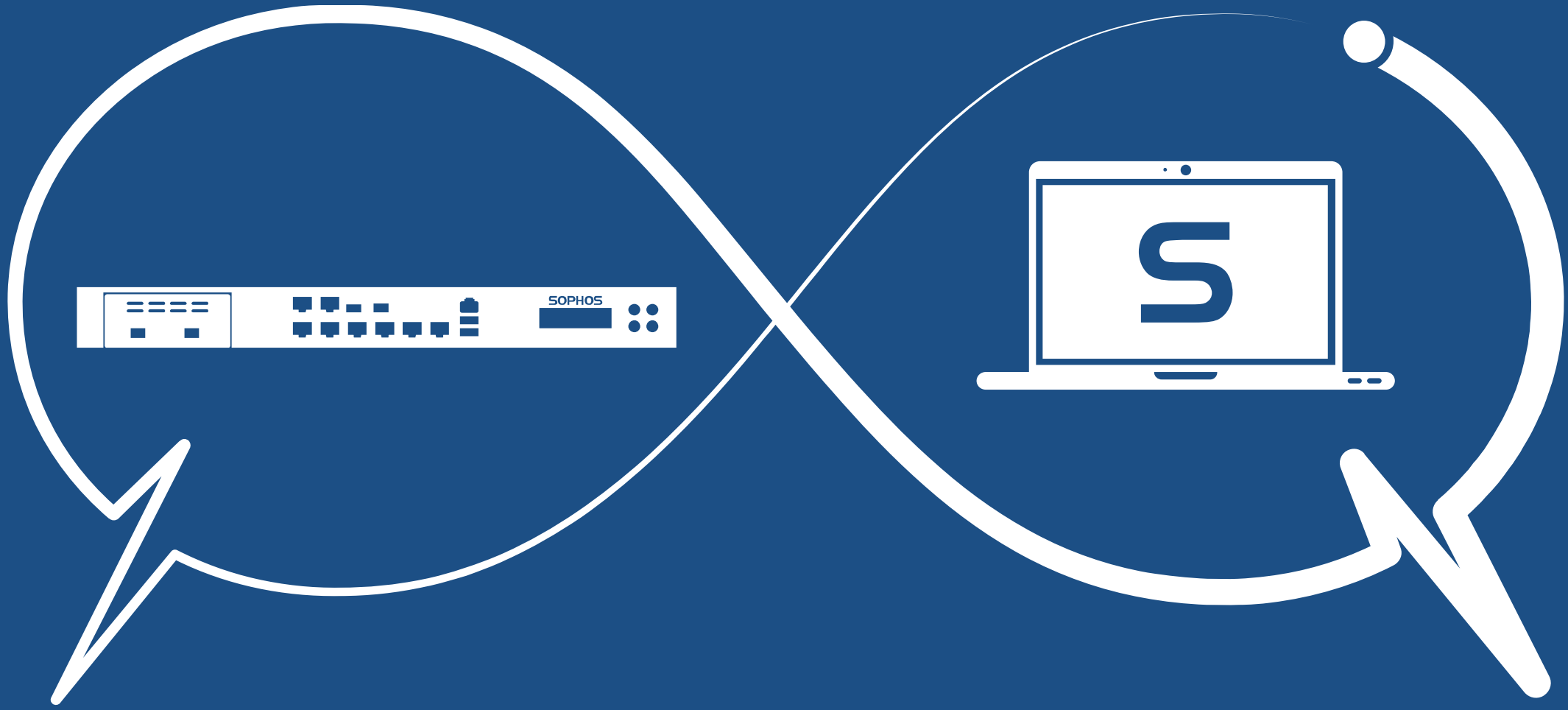
Please note that none of these numbers are guaranteed as performance may vary in a real life customer scenario based on user characteristics, application usage, security configurations and other factors. Hence these numbers should only be used as a rough sizing guideline.

Small - Desktop

Model	XG 85/w rev.1	XG 105/w rev.2	XG 115/w rev.2	XG 125/w rev.2	XG 135/w rev.2
Performance Numbers					
Firewall max. [1] (Mbps)	2,000	3,000	3,500	5,000	7,000
IPS max. [1] (Mbps)	510	700	900	1,040	1,750
IPS Realworld [2] (Mbps)	75	98	103	180	232
Web Proxy – AV (Mbps)	330	430	520	590	1,400
Web Proxy – AV Realworld [2] (Mbps)	75	187	234	307	427
IPS + Web Proxy – AV Realworld [2] (Mbps)	31	36	42	58	95
IPS + App Ctrl + WebFilter Realworld [2] (Mbps)	25	27	30	75	133
VPN AES max. [1] (Mbps)	200	300	350	410	950
VPN AES Realworld [1] (Mbps)	50	75	90	105	240
Maximum recommended connections					
New TCP connections/sec	12,000	27,500	27,500	35,000	82,000
Concurrent TCP connections	2,000,000	3,200,000	6,000,000	6,200,000	8,200,000
Concurrent IPsec VPN tunnels	200	300	500	750	1000
Concurrent Access Points	5	10	20	30	40
Concurrent REDs (UTM/FW) [4]	5/10	10/30	15/80	20/80	25/100

1. 1518 byte packet size (UDP), default rule set
2. Avg. of Data Center, Enterprise Perimeter, Higher Education, European Mobile, Financial Network protocol mixes at 50% CPU Usage
3. HTTP traffic
4. UTM=Full content scanning of RED traffic on XG appliance, FW=packet filtering only

Sizing Guide: https://partnerportal.sophos.com/en-us/medialibrary/PartnerPortal/Files/Tools/SalesGuidance/sophos-xg-series-sizing-guide.PDF?la=en



SECURITY HEARTBEAT™

Your firewall and endpoints are finally talking

Trzy filary Sophos Security Heartbeat

Security Heartbeat™

Przyspieszone wykrycie	Aktywna Identyfikacja	Automatyczna odpowiedź
Spójna ochrona stacji i sieci pozwala na szybszą identyfikację nieznanych zagrożeń. Ciągłą komunikacja pozwala wykryć podejrzane zachowania.	Identyfikacja zainfekowanej stacji znacząco skraca czas potrzebny na ustalenie źródła zagrożenia.	Skompromitowane stacje automatycznie izolowane są przez zaporę sieciową do czasu usunięcia szkodliwego oprogramowania.
Krótki czas decyzji	**Szybkie śledztwo**	**Ograniczone pole rażenia**

Security Heartbeat – zabezpieczenia nowej generacji

Bezpieczeństwo może być kompleksowe

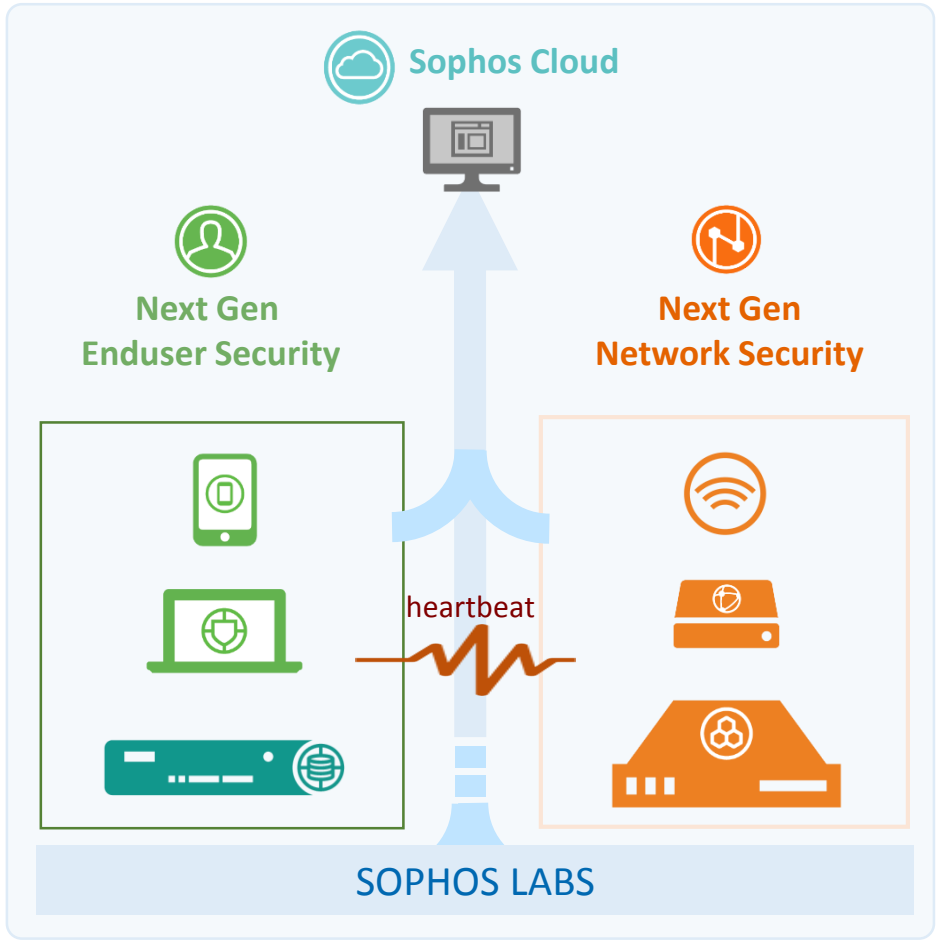
Rozwiązanie ma zaspokajać wszystkie możliwe potrzeby klienta

Bezpieczeństwo jako system działa lepiej

Nowe możliwości dzięki współpracy na wielu płaszczyznach

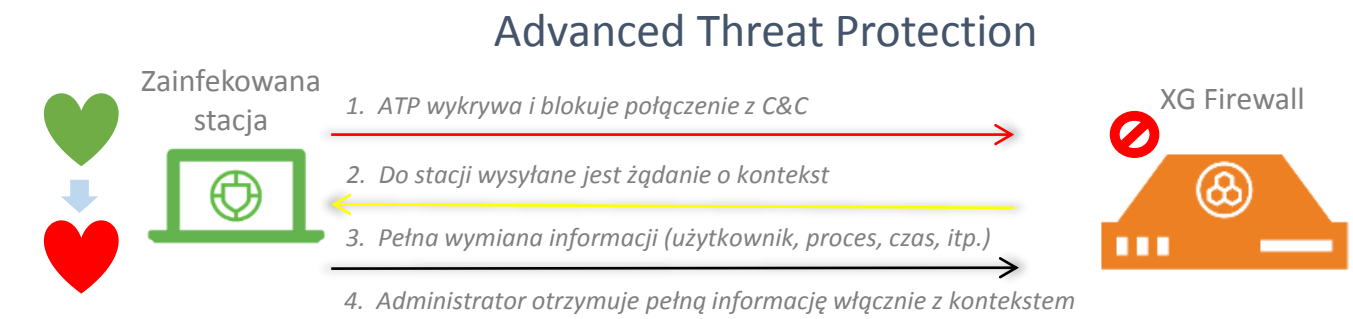
Bezpieczeństwo może być proste

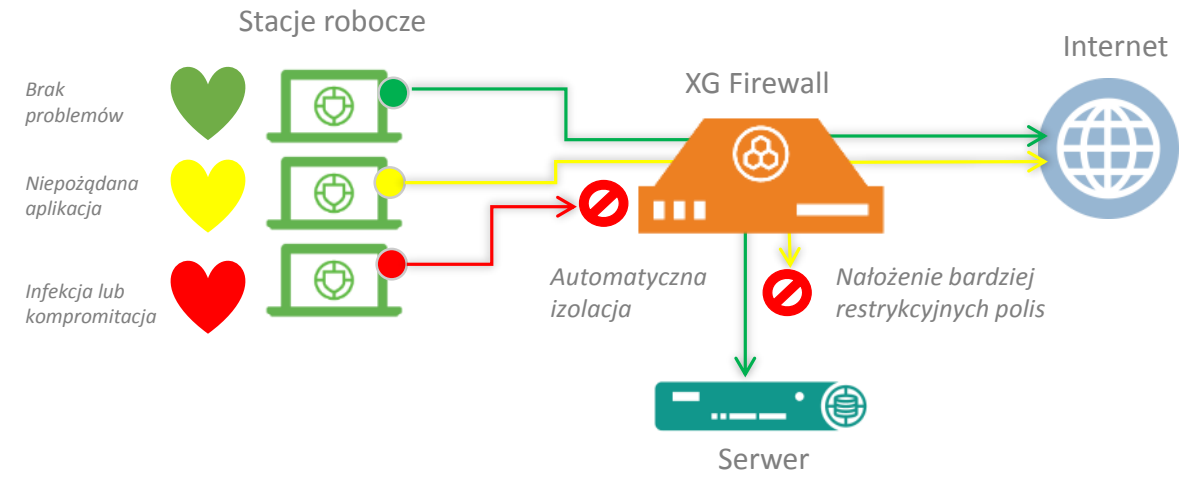
Platforma, sposób wdrożenia, licencjonowanie, doświadczenie użytkownika



Security Heartbeat – zasada działania

Zapora sieciowa i stacje robocze współpracując przyczyniają się do zwiększenia poziomu ochrony przed zagrożeniami



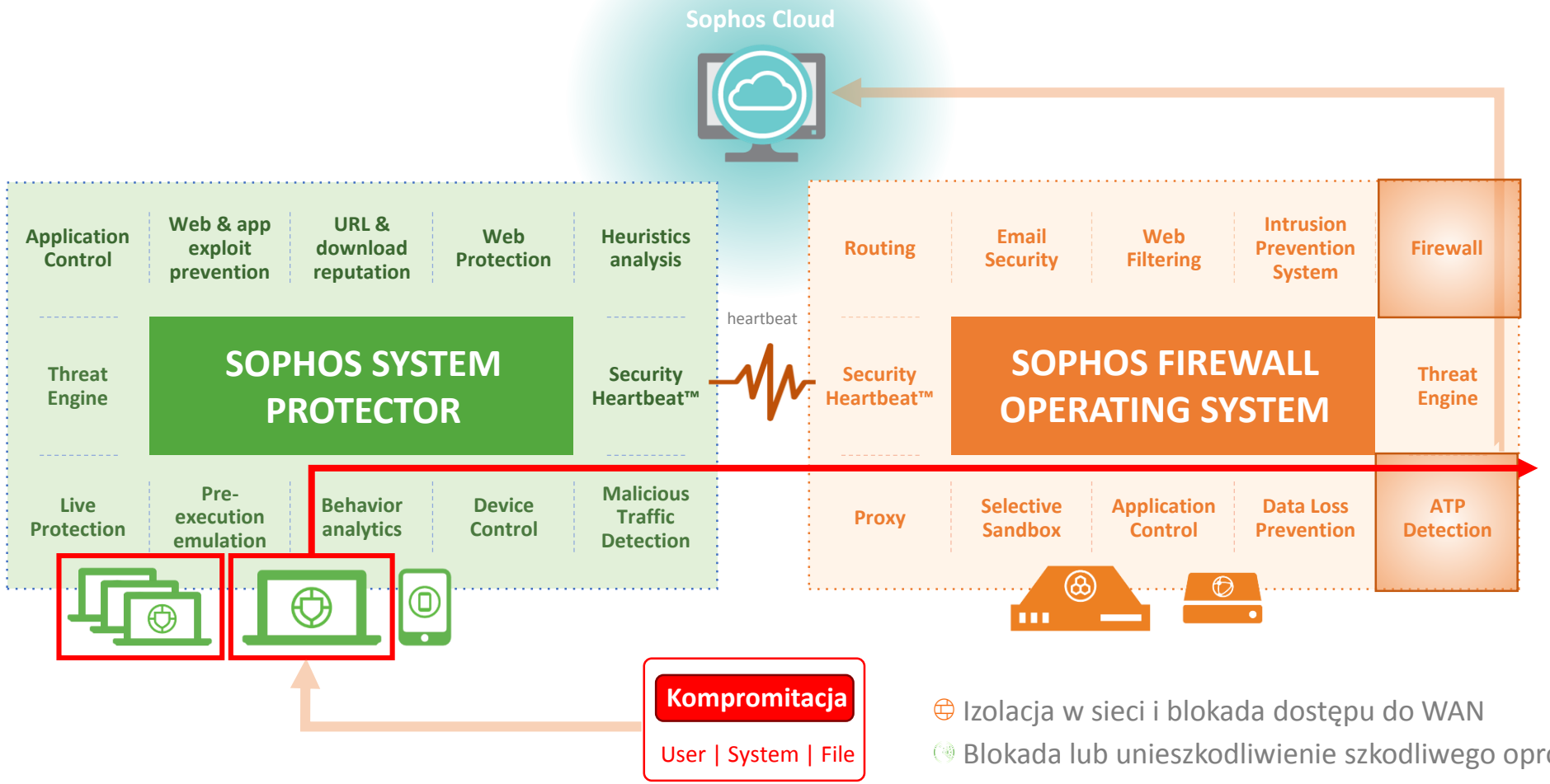


- **Przyspieszone wykrycie**
  Spójna ochrona stacji i sieci pozwala na szybszą identyfikację nieznanych zagrożeń. Ciągłą komunikacja pozwala wykryć podejrzane zachowania.

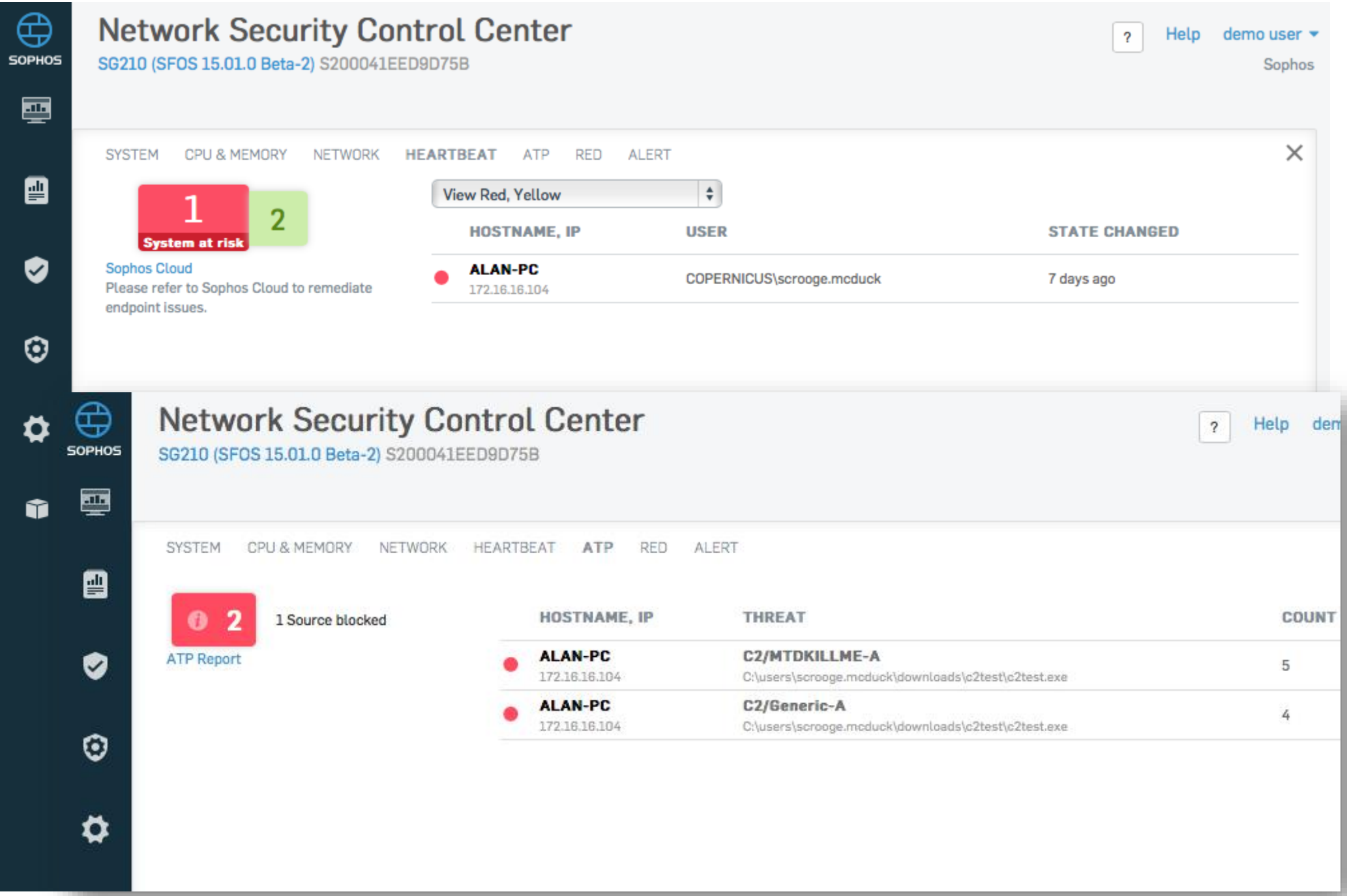
- **Aktywna Identyfikacja**
  Identyfikacja zainfekowanej stacji znacząco skraca czas potrzebny na ustalenie źródła zagrożenia

- **Automatyczna odpowiedź**
  Skompromitowane stacje automatycznie izolowane są przez zaporę sieciową do czasu usunięcia szkodliwego oprogramowania.

Security Heartbeat – zasada działania



- Izolacja w sieci i blokada dostępu do WAN
- Blokada lub unieszkodliwienie szkodliwego oprogramowania
- Identyfikacja & oczyszczenie pozostałych stacji



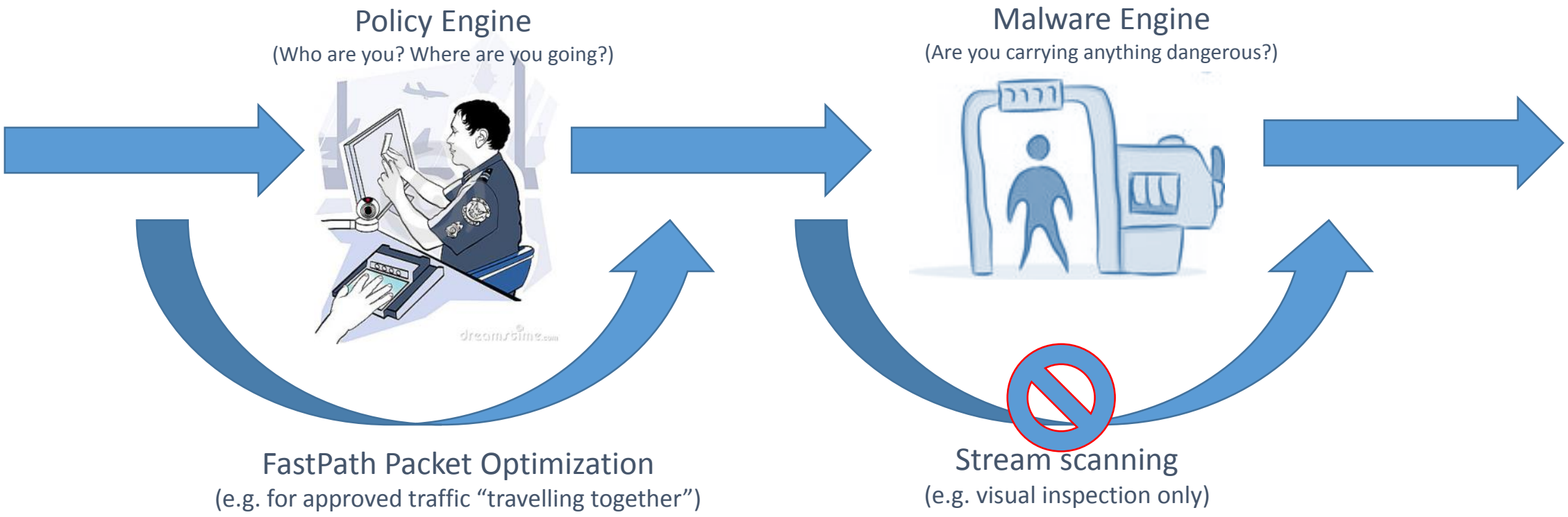
Security Heartbeat & Advanced Threats

- Przyspieszone wykrywanie
- Pozytywna identyfikacja
- Zautomatyzowana odpowiedź

- Natychmiastowy wgląd w skompromitowane systemy
  - Hostname, IP
  - Użytkownik
  - Czas
  - Rodzaj zagrożenia
  - Aplikacja / Proces
  - Ile razy incydent wystąpił

FastPath Packet Optimization

- Optymalizacja routingu i zapory sieciowej = większa wydajność
- Jeśli połączenie uznawane jest za zaufane, wszystkie powiązane pakiety kierowane są na szybką ścieżkę (z pominięciem zapory sieciowej) bezpośrednio do silnika Malware.
- Nie jest to skanowanie strumieniowe spotykane w rozwiązaniach konkurencji (podatność na malware). Sophos bezpieczeństwo traktuje bezkompromisowo!



Sophos XG na tle konkurencji

new Competitive differentiators
- Security Heartbeat
- Unified policy
- User Threat Quotient

new Comparative differentiators
- FastPath
- User-based Firewall Policies
- Discover Mode (TAP)

	Sophos XG Firewall	Fortinet 20-90	Dell SonicWall TZ Series	WatchGuard XTM
Network Firewall Protection	✓	✓	✓	✓
Advanced Threat Protection	✓	✓	✓	✓
Security Heartbeat™	✓ new			
Unified Policies	✓ new new			
User Risk Visibility (UTQ)	✓ new			
FastPath Packet Optimization	✓	✓		
Site to Site Remote user VPN	✓	✓	✓	✓
Secure Web Gateway	✓	✓	✓	✓
Complete Email: AV, AS, Encrypt, DLP	✓	$	$	$
Dual antivirus engines	✓			
Secure Wi-Fi	✓	✓	✓	✓
Reverse Proxy	✓			
Web Application Firewall (WAF)	✓	$	$	
User Portal	✓	✓		
Full Reporting	✓	$	$	$
Best TMG Feature Parity	✓			
Discover Mode Deployment (TAP)	✓ new	✓	✓	✓

SOPHOS

Dodatki do Sophos SG i XG

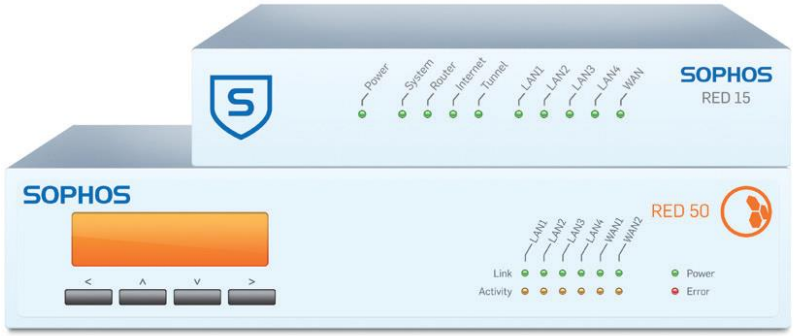
Sophos RED

Simple, plug & play branch office security

- Securely connect remote locations
- Completely configuration free
- Flexible deployment options
- Same protection for all offices
- Fully encrypted traffic
- Centrally managed
- No added licenses or maintenance

New RED 15w:

- Same wireless specs as SG 85w
  - 802.11n
  - 2x2:2 MIMO
  - Single radio
- Planned availability: End March 2016
- Supported with UTM 9.4



RED 15 and RED 50

RED 15w

Sophos Access Points Portfolio

New AP 15C (Support with UTM 9.4 only)

	AP 15	new *AP 15C*	AP 55	AP 55C	AP 100	AP 100C	AP 100X
							
Deployment	Desktop/wall	*Ceiling*	Desktop/wall	Ceiling	Desktop/wall	Ceiling	Outdoor wall-mount
	SOHO	*SOHO*	Larger offices, high density	Ceiling-mounted for larger offices	Enterprise dual-band/dual-radio	Enterprise dual-band/dual-radio	Enterprise dual-band/dual-radio
Maximum throughput	300 Mbps	*300 Mbps*	867 Mbps + 300 Mbps	867 Mbps + 300 Mbps	1.3 Gbps + 450 Mbps	1.3 Gbps + 450 Mbps	1.3 Gbps + 450 Mbps
Multiple SSIDs	8	*8*	8 per radio (16 in total)	8 per radio (16 in total)	8 per radio (16 in total)	8 per radio (16 in total)	8 per radio (16 in total)
Tech. Specification							
Supported WLAN Standards	WiFi 802.11n 2.4 GHz	WiFi 802.11n *2.4 GHz or 5 GHz*	WiFi 802.11ac 2.4 and 5 GHz	WiFi 802.11ac 2.4 and 5 GHz	WiFi 802.11ac 2.4 and 5 GHz	WiFi 802.11ac 2.4 and 5 GHz	WiFi 802.11ac 2.4 and 5 GHz
Number of radios	1	*1*	2	2	2	2	2
MIMO capabilities	2x2:2	*2x2:2*	2x2:2	2x2:2	3x3:3	3x3:3	3x3:3

Q&A