SOPHOS

# Funkcje Sophos Firewall


## Sophos Firewall

### Najważniejsze cechy

- Architektura Xstream zapewnia wyjątkowo wysoki poziom widoczności, ochrony i wydajności dzięki strumieniowemu przetwarzaniu pakietów.
- Inspekcja TLS Xstream oferuje wysoką wydajność, obsługę TLS 1.3 bez obniżania wersji (bez downgradingu), działanie niezależne od portów, polityki klasy enterprise z gotowymi wyjątkami, unikalną widoczność na pulpitach oraz narzędzia do rozwiązywania problemów z kompatybilnością.
- Silnik Xstream DPI zapewnia strumieniowe skanowanie i ochronę dla IPS, AV, filtrowania WWW, kontroli aplikacji oraz inspekcji TLS w ramach jednego, wydajnego silnika.
- Xstream Network Flow FastPath automatycznie przyspiesza zaufany ruch w sposób inteligentny i sterowany politykami.
- Xstream SD-WAN umożliwia wybór łącza na podstawie wydajności, przekierowanie ruchu bez wpływu na działanie (zero-impact re-routing), monitoring SD-WAN, narzędzia do orkiestracji SD-WAN dla wielu lokalizacji oraz akcelerację FastPath ruchu tuneli IPsec VPN.
- Interfejs zaprojektowany specjalnie do tego celu z interaktywnym centrum sterowania wykorzystuje wskaźniki „sygnalizacji świetlnej” (czerwony, żółty, zielony), aby jednym rzutem oka wskazać obszary wymagające uwagi.
- Control Center zapewnia natychmiastowy wgląd m.in. w kondycję punktów końcowych, nierozpoznane aplikacje na macOS i Windows, aplikacje chmurowe i shadow IT, podejrzane ładunki (payloady), ryzykownych użytkowników, zaawansowane zagrożenia, ataki sieciowe, niepożądane strony WWW i wiele więcej.
- Zoptymalizowana nawigacja „dwa kliknięcia do każdego widoku” w połączeniu z inteligentnym wyszukiwaniem pozwala szybko dotrzeć do potrzebnych ustawień i informacji.
- Widget Policy Control Center monitoruje aktywność polityk (biznesowych, użytkowników i sieci) oraz śledzi polityki nieużywane, wyłączone, zmienione i nowe.
- Ujednolicony model polityk łączy reguły firewalla, NAT i inspekcji TLS na jednym ekranie, z możliwością grupowania, filtrowania i wyszukiwania.
- Usprawnione zarządzanie regułami firewalla dla dużych zestawów reguł obejmuje własne grupowanie automatyczne i ręczne oraz funkcje podglądu „na najechanie” wraz ze wskaźnikami egzekwowania reguł.
- Każda reguła firewalla oferuje czytelne podsumowanie zastosowanych mechanizmów ochrony i kontroli: AV, sandboxing, IPS, filtrowanie WWW, kontrolę aplikacji, kształtowanie ruchu (QoS) oraz Heartbeat.
- Wstępnie zdefiniowane polityki IPS, WWW, aplikacji, TLS i kształtowania ruchu (QoS) przyspieszają wdrożenie i ułatwiają dostosowanie do typowych scenariuszy (np. CIPA, standardowe polityki dla środowiska biurowego i inne).
- Sophos Security Heartbeat™ łączy endpointy Sophos z firewallem, wymieniając status bezpieczeństwa i telemetrię, co pozwala natychmiast wykryć urządzenia w złej kondycji lub skompromitowane.
- Active Threat Response identyfikuje aktywnych atakujących, blokuje ich działania i automatycznie reaguje, korzystając z feedów zagrożeń dostarczanych przez SophosLabs, analityków MDR oraz źródła zewnętrzne.
- Synchronized Application Control automatycznie rozpoznaje, klasyfikuje i umożliwia kontrolę wszystkich nieznanych aplikacji macOS/Windows w sieci.
- Cloud Application Visibility pozwala od razu wykrywać shadow IT oraz oferuje kształtowanie ruchu jednym kliknięciem.
- Symulator testów polityk umożliwia symulowanie i testowanie reguł firewalla oraz polityk WWW według użytkownika, adresu IP i pory dnia.
- User Threat Quotient wskazuje użytkowników o podwyższonym ryzyku na podstawie ostatniej aktywności przeglądania oraz wyzwalaczy ATP.
- API konfiguracyjne dla wszystkich funkcji ułatwia integrację z narzędziami RMM/PSA.
- Integracja z chmurowym NDR zwiększa skuteczność wykrywania aktywnych przeciwników.
- Wbudowana brama ZTNA w każdym firewallu upraszcza bezpieczny dostęp do aplikacji z dowolnego miejsca.
- Zarządzanie i raportowanie w chmurze Sophos Central dla wielu firewalli zapewnia polityki grupowe oraz jedną konsolę dla wszystkich produktów Sophos z obszaru bezpieczeństwa IT.
- Uproszczony kreator konfiguracji umożliwia szybkie uruchomienie „prosto po wyjęciu z pudełka” w zaledwie kilka minut.
- Wdrożenie i konfiguracja typu zero-touch nowych firewalli przez Sophos Central.
- Płynna integracja z Sophos MDR i XDR.

# Base Firewall

## Ogólne zarządzanie

- Dedykowany, usprawniony interfejs oraz sprawne zarządzanie regułami firewalla dla dużych zbiorów reguł – z grupowaniem, podglądem „na pierwszy rzut oka” i wskaźnikami egzekwowania.
- Obsługa uwierzytelniania dwuskładnikowego (OTP) dla dostępu administracyjnego, portalu użytkownika oraz IPsec i SSL VPN .
- Zaawansowane logowanie oraz narzędzia diagnostyczne w GUI (np. przechwytywanie pakietów).
- Wysoka dostępność (HA) – klaster dwóch urządzeń w trybie active-active lub active-passive, z konfiguracją Quick HA typu plug-and-play oraz obsługą wielu redundantnych łączy synchronizacji.
- Pełny interfejs wiersza poleceń (CLI) dostępny z poziomu GUI.
- Administracja oparta na rolach z integracją Azure AD dla jednokrotnego logowania (SSO).
- Automatyczne powiadomienia o aktualizacjach firmware oraz łatwy, zautomatyzowany proces aktualizacji z możliwością wycofania zmian (dostępne tylko dla klientów z ważnym wsparciem).
- Wielokrotnego użytku, wyszukiwalne definicje obiektów systemowych dla sieci, usług, hostów, okresów czasu, użytkowników i grup, klientów oraz serwerów.
- Samoobsługowy portal użytkownika.
- Śledzenie zmian konfiguracji.
- Elastyczna kontrola dostępu do usług według stref.
- Powiadomienia e-mail lub pułapki SNMP (SNMP trap).
- Obsługa SNMP v3 oraz NetFlow.
- Obsługa centralnego zarządzania przez Sophos Central (dostępne tylko dla klientów z ważnym wsparciem).
- Kopia zapasowa i odtwarzanie konfiguracji: lokalnie, przez FTP lub e-mail; na żądanie oraz cyklicznie (codziennie/tygodniowo/miesięcznie) – z opcją mapowania portów podczas wymiany urządzenia na nowsze.
- Obsługa certyfikatów Let’s Encrypt dla: WAF, SMTP, konfiguracji TLS, logowania do hotspotu, konsoli Web Admin, portalu użytkownika, captive portalu, portalu VPN oraz portalu SPX.
- API do integracji z rozwiązaniami firm trzecich.
- Możliwość zmiany nazw interfejsów.
- Opcja zdalnego dostępu dla wsparcia Sophos Support.
- Chmurowe zarządzanie licencjami przez MySophos.

## Firewall, sieć i routing

- Stanowy firewall z głęboką inspekcją pakietów (DPI).
- Architektura przetwarzania pakietów Xstream zapewnia bardzo wysoki poziom widoczności, ochrony i wydajności dzięki strumieniowemu przetwarzaniu pakietów.
- Inspekcja TLS Xstream: wysoka wydajność, obsługa TLS 1.3 bez obniżania wersji (bez downgradingu), niezależność od portów, polityki klasy enterprise, unikalna widoczność na pulpitach oraz narzędzia do rozwiązywania problemów z kompatybilnością.
- Silnik Xstream DPI oferuje strumieniowe skanowanie i ochronę dla IPS, AV, filtrowania WWW, kontroli aplikacji oraz inspekcji TLS w ramach jednego, wydajnego silnika.
- Xstream Network Flow FastPath automatycznie zapewnia inteligentną akcelerację ruchu zaufanych aplikacji, ruchu VPN IPsec oraz ruchu szyfrowanego TLS – zgodnie z politykami.
- Polityki oparte o użytkownika, grupę, czas lub sieć.
- Polityki dostępu czasowego per użytkownik/grupa.
- Egzekwowanie polityk między strefami, sieciami lub według typu usługi.
- Izolacja stref oraz polityki oparte o strefy.
- Domyślne strefy: LAN, WAN, DMZ, LOCAL, VPN oraz Wi-Fi.
- Własne strefy w LAN lub DMZ.
- Konfigurowalne polityki NAT (w tym maskarada IP) oraz pełna obsługa obiektów – z możliwością przekierowania lub forwardowania wielu usług w jednej regule; kreator reguł NAT pozwala szybko tworzyć złożone reguły w kilku kliknięciach.
- Wielokrotnego użytku definicje obiektów sieciowych dla wszystkich reguł oraz globalne, inteligentne wyszukiwanie pełnotekstowe.
- Ochrona przed zalewaniem ruchem (flood protection): blokowanie DoS, DDoS oraz skanowania portów.
- Blokowanie krajów na podstawie geo-IP.
- Routing: statyczny, multicast (PIM-SM) oraz dynamiczny: RIP, BGP, OSPFv3 (IPv6), BGPv6.
- CZarządzanie trasami zaawansowane: klonowanie tras statycznych i ich włączanie/wyłączanie, redystrybucja tras dynamicznych BGP do OSPFv3, opcje tras Blackhole oraz ECMP (Equal-Cost Multi-Path) do równoważenia obciążenia.
- Obsługa proxy upstream.
- Routing multicast niezależny od protokołu z IGMP snooping.
- Mostowanie (bridging) z obsługą STP oraz przekazywaniem rozgłoszeń ARP.
- Obsługa VLAN DHCP oraz tagowania VLAN.
- Obsługa mostów VLAN (VLAN bridge).

- Obsługa ramek jumbo (Jumbo Frames).
- Możliwość włączania i wyłączania interfejsów fizycznych.
- Obsługa Wireless WAN (niedostępne w wdrożeniach wirtualnych).
- Agregacja łączy interfejsów 802.3ad (LACP).
- Pełna konfiguracja usług DNS, DHCP i NTP.
- Dynamiczny DNS (DDNS).
- Certyfikacja w programie IPv6 Ready Logo.
- Delegowanie prefiksu DHCP dla IPv6 (DHCPv6 Prefix Delegation).
- Obsługa tunelowania IPv6, w tym 6in4, 6to4, 4in6 oraz szybkiego wdrażania IPv6 (6rd) przez IPsec.

## Xstream SD-WAN

- Profile Xstream SD-WAN obsługują wiele typów łączy WAN, w tym VDSL, DSL, łącza kablowe, LTE/komórkowe oraz MPLS.
- SLA oparte o parametry wydajności automatycznie wybierają najlepsze łącze WAN na podstawie jittera, opóźnień (latency) lub utraty pakietów.
- Równoważenie obciążenia SD-WAN między wieloma łączami: z wagami round-robin lub strategiami utrzymania sesji (session persistence).
- Przekierowanie bez wpływu na działanie (zero-impact re-routing) utrzymuje sesje aplikacji, gdy parametry łącza spadają poniżej progów i następuje przełączenie na łącze o lepszej wydajności.
- Wykresy monitoringu SD-WAN zapewniają wgląd w czasie rzeczywistym w opóźnienia, jitter i utratę pakietów dla wszystkich łączy WAN.
- Akceleracja Xstream FastPath dla ruchu tuneli IPsec w SD-WAN.
- Synchronized SD-WAN (funkcja Synchronized Security) wykorzystuje większą precyzję i wiarygodność identyfikacji aplikacji dzięki wymianie informacji z Synchronized Application Control pomiędzy endpointami zarządzanymi przez Sophos a Sophos Firewall.
- Routing aplikacyjny po preferowanych łączach realizowany przez reguły firewalla lub routing oparty o polityki (policy-based routing).
- Rozbudowana obsługa VPN, w tym IPsec oraz SSL VPN.
- Unikalny tunel Sophos RED warstwy 2 z obsługą routingu.

## Podstawowe kształtowanie ruchu i limity

- Elastyczne kształtowanie ruchu (QoS) oparte na sieci lub użytkownikach (rozszerzone opcje kształtowania ruchu WWW i aplikacji są dostępne w ramach subskrypcji Web Protection).
- Limity transferu per użytkownik – dla wysyłania/pobierania lub łącznego ruchu; limity cykliczne lub jednorazowe (niecykliczne).
- Optymalizacja VoIP w czasie rzeczywistym.
- Oznaczanie DSCP.

## Bezpieczna sieć bezprzewodowa

- Proste wdrożenie plug-and-play punktów dostępowych Sophos (tylko seria APX) – urządzenia automatycznie pojawiają się w Control Center firewalla.
- Centralny monitoring i zarządzanie AP oraz klientami Wi-Fi dzięki wbudowanemu kontrolerowi sieci bezprzewodowej.
- Mostowanie AP do LAN, VLAN lub osobnej strefy z opcjami izolacji klientów.
- Obsługa wielu SSID na każde radio, w tym SSID ukrytych.
- Wsparcie dla różnych standardów bezpieczeństwa i szyfrowania, w tym WPA2 Personal oraz WPA2 Enterprise.
- Możliwość wyboru szerokości kanału.
- Obsługa IEEE 802.1X (uwierzytelnianie RADIUS) z serwerem podstawowym i zapasowym.
- Obsługa 802.11r (fast transition) dla szybszego roamingu.
- Obsługa hotspotu: (własne) vouchery, „hasło dnia” lub akceptacja regulaminu (T&C).
- Dostęp gościnny do internetu z opcją „walled garden” (lista wyjątków/dopuszczonych stron).
- Dostęp do sieci Wi-Fi zależny od czasu (time-based access).
- Tryb mesh: powtarzanie sygnału i mostowanie w sieci kratowej (dla wspieranych AP).
- Automatyczna selekcja kanałów i optymalizacja w tle.
- Obsługa logowania przez HTTPS.

## Uwierzytelnianie

- Synchronized User ID w ramach Synchronized Security umożliwia przekazywanie do firewalla informacji o aktualnie zalogowanym użytkowniku Active Directory z endpointów Sophos – bez instalowania agenta na serwerze AD ani na komputerze użytkownika.
- Uwierzytelnianie przez: Active Directory, eDirectory, RADIUS, LDAP oraz TACACS+.
- Serwerowe agenty uwierzytelniania dla Active Directory SSO: STAS, SATC.
- Single sign-on (SSO): Active Directory, eDirectory, RADIUS Accounting.
- SSO z Azure AD dla administratorów – dostęp do konsoli WebAdmin.
- SSO z Azure AD dla użytkowników – uwierzytelnianie dostępu do internetu przez captive portal.
- Transparentne AD SSO z wymuszonym HSTS, umożliwiające handshaki Kerberos i NTLM przez HTTP lub HTTPS.
- Import grup z Azure AD oraz wsparcie RBAC (role-based access control).
- Klienckie agenty uwierzytelniania dla Windows, macOS (OS oraz Linux (32/64-bit).

- Uwierzytelnianie SSO w przeglądarce: transparentne, uwierzytelnianie proxy (NTLM) oraz Kerberos.
- Captive Portal w przeglądarce.
- Certyfikaty uwierzytelniania dla iOS i Android.
- Usługi uwierzytelniania dla IPsec, SSL, L2TP oraz PPTP.
- Obsługa uwierzytelniania Google Chromebook w środowiskach z Active Directory oraz Google G Suite.
- Integracja z Google Workspace przez klienta LDAP wraz z SSO dla Google Chromebook.
- Uwierzytelnianie oparte o API.

## Portale samoobsługowe użytkownika i VPN

- Obsługa SSO Entra ID (Azure AD) dla portalu VPN.
- Możliwość pobrania Sophos Authentication Client.
- Możliwość pobrania klienta zdalnego dostępu SSL (Windows) oraz plików konfiguracyjnych (pozostałe systemy).
- Dostęp do informacji o hotspotach.
- Zmiana nazwy użytkownika i hasła.
- Podgląd własnego wykorzystania internetu.
- Dostęp do wiadomości w kwarantannie oraz zarządzanie listami blokuj/zezwalaj per użytkownik (wymaga Email Protection).

## Podstawowe opcje VPN

- ➦VPN site-to-site: SSL, IPsec, AES 256-bit / 3DES, PFS, RSA, certyfikaty X.509, klucz współdzielony (PSK).
- ➦Tunel Sophos RED site-to-site VPN (lekki i odporny mechanizm zestawiania połączeń).
- ➦Akceleracja Xstream FastPath dla ruchu tuneli IPsec (zarówno site-to-site, jak i remote access).
- ➦Narzędzia importu, monitoringu i zarządzania AWS VPC.
- ➦Obsługa L2TP i PPTP.
- ➦VPN oparty o trasy (route-based VPN) z selektorami ruchu.
- ➦Zdalny dostęp: SSL, IPsec oraz obsługa klientów VPN dla iPhone/iPad/Cisco/Android.
- ➦Obsługa IKEv2.
- ➦Stanowy failover HA dla połączeń IPsec (RBVPN, PBVPN oraz remote access) bez utraty sesji podczas przełączenia w scenariuszach HA.
- ➦Monitoring stanu tuneli IPsec VPN przez SNMP.
- ➦Zaawansowane funkcje IPsec: unikalne PSK oraz DH-Group 27–30 / RFC6954.
- ➦Klient SSL dla Windows oraz pobieranie konfiguracji przez portal użytkownika.

## Sophos Connect Client

- Uwierzytelnianie: PSK, PKI (X.509), token oraz XAUTH.
- Obsługa SSO Entra ID (Azure AD).
- Wsparcie Synchronized Security i Security Heartbeat dla użytkowników łączących się zdalnie.
- Inteligentny split tunneling dla optymalnego routingu ruchu.
- Obsługa NAT-Traversal.
- Client monitor – graficzny podgląd statusu połączenia.
- Obsługa klientów: macOS (IPsec) oraz Windows (SSL/IPsec).

# Ochrona sieci

## Intrusion Prevention (IPS)

- Wysokowydajny, nowej generacji silnik IPS z DPI z selektywnymi wzorcami IPS, które można stosować per regułę firewalla, aby maksymalizować wydajność i ochronę.
- Tysiące sygnatur.
- Szczegółowy wybór kategorii.
- Obsługa własnych sygnatur IPS.
- IPS Policy Smart Filters – dynamiczne polityki, które automatycznie aktualizują się wraz z dodawaniem nowych wzorców.

## Active Threat Response i Security Heartbeat™

- Active Threat Response automatycznie monitoruje i blokuje APT oraz inne zagrożenia identyfikowane przez feedy Sophos X-Ops Threat Feeds. Zapewnia to zaawansowaną ochronę przed botami i aktywnymi przeciwnikami próbującymi łączyć się ze złośliwymi celami, wykorzystując wielowarstwowe mechanizmy detekcji: DNS, AFC oraz reguły firewalla.
- Active Threat Response automatycznie monitoruje i blokuje zagrożenia wskazane przez feedy MDR/XDR publikowane przez analityków SOC Sophos lub SOC klienta/partnera – gdy Sophos Firewall z Xstream Protection działa łącznie z usługami Sophos MDR/XDR.
- Active Threat Response automatycznie monitoruje i blokuje także feedy stron trzecich (third-party threat feeds) pochodzące ze źródeł threat intelligence branżowych, sektorowych lub regionalnych – przy użyciu Xstream Protection.
- Sophos Synchronized Security Heartbeat natychmiast oznacza skompromitowane urządzenia statusem czerwonego Heartbeat, jeśli próbują skontaktować się z dowolnym wskaźnikiem zagrożenia (IOC) wykrytym przez Active Threat Response i powiązane feedy. Status Heartbeat jest również monitorowany przez endpointy zarządzane przez Sophos i udostępniany firewallowi wraz ze szczegółami takimi jak: host, użytkownik, proces, liczba incydentów oraz czas kompromitacji.

- Warunki Sophos Security Heartbeat można przypisywać do dowolnej reguły firewalla, aby automatycznie ograniczać dostęp do zasobów i segmentów sieci dla urządzenia skompromitowanego – do momentu jego oczyszczenia.
- Sophos Firewall może także automatycznie uruchamiać ochronę przed ruchem bocznym (lateral movement). Gdy zarządzany endpoint zostanie skompromitowany, firewall informuje wszystkie „zdrowe" endpointy Sophos, aby odrzucały ruch z tego urządzenia, skutecznie je izolując – nawet w obrębie tego samego segmentu LAN.

## Zarządzanie urządzeniami SD-RED

- Centralne zarządzanie wszystkimi urządzeniami SD-RED.
- Brak ręcznej konfiguracji: automatyczne zestawienie połączenia przez chmurową usługę provisioningu.
- Bezpieczny, szyfrowany tunel z użyciem cyfrowych certyfikatów X.509 oraz szyfrowania AES 256-bit.
- Wirtualny Ethernet zapewniający niezawodny transfer całego ruchu pomiędzy lokalizacjami.
- Zarządzanie adresacją IP z centralnie definiowaną konfiguracją serwerów DHCP i DNS.
- Możliwość zdalnego cofnięcia autoryzacji urządzeń SD-RED po określonym czasie braku aktywności.
- Kompresja ruchu w tunelu.
- Opcje konfiguracji portów VLAN.

## VPN bez klienta (Clientless VPN)

- Unikalny, szyfrowany portal samoobsługowy Sophos w technologii HTML5, zapewniający dostęp bez instalowania klienta i obsługujący połączenia RDP, SSH, Telnet oraz VNC.

# Ochrona WWW (Web Protection)

## Web Protection and Control

- Ochrona WWW z wykorzystaniem strumieniowego DPI lub inspekcja w trybie jawnego proxy (explicit proxy).
- Tryb explicit proxy obsługuje uwierzytelnianie per połączenie dla wielu użytkowników korzystających z tego samego źródłowego adresu IP.
- Rozszerzona Advanced Threat Protection.
- Baza filtrowania URL z milionami stron w 92 kategoriach, wspierana przez SophosLabs.
- Limity czasu surfowania (surfing quota) per użytkownik/grupa.
- Polityki dostępu czasowego per użytkownik/grupa.
- Skanowanie pod kątem malware: blokowanie wirusów, web malware, trojanów i spyware w HTTP/S, FTP oraz poczcie webowej.
- Zaawansowana ochrona przed web malware z emulacją JavaScript.
- Live Protection – chmurowe zapytania w czasie rzeczywistym najnowsze informacje threat intelligence.
- Drugi, niezależny silnik detekcji (Avira) do podwójnego skanowania (dual-scanning).
- Skanowanie w trybie rzeczywistym lub wsadowym.
- Ochrona przed pharmingiem.
- Wymuszanie ograniczeń tenantów dla Microsoft 365 (O365).
- Wykrywanie i egzekwowanie tunelowania protokołów SSL.
- Walidacja certyfikatów.
- Wysokowydajne cache'owanie treści WWW.
- Wymuszone cache'owanie aktualizacji Sophos Endpoint.
- Filtrowanie typów plików wg MIME-type, rozszerzeń oraz typów aktywnej zawartości (np. ActiveX, applety, cookies itd.).
- Wymuszanie YouTube for Schools per polityka (użytkownik/grupa).
- Wymuszanie SafeSearch (DNS-based) dla głównych wyszukiwarek per polityka (użytkownik/grupa).
- Monitoring i egzekwowanie słów kluczowych: logowanie, raportowanie lub blokowanie treści WWW pasujących do list słów kluczowych, z możliwością wgrywania własnych list.
- Blokowanie potencjalnie niepożądanych aplikacji (PUA).
- Możliwość tymczasowego obejścia polityk WWW dla nauczycieli lub personelu – dostęp do zablokowanych stron/kategorii może być czasowo odblokowany; rozwiązanie jest w pełni konfigurowalne i zarządzane przez wybranych użytkowników.
- Egzekwowanie polityk per użytkownik/grupa na Google Chromebookach.

## Widoczność aplikacji chmurowych

- Widget w Control Center pokazuje ilość danych wysyłanych i pobieranych do aplikacji chmurowych, klasyfikowanych jako: nowe, zatwierdzone (sanctioned), niezatwierdzone (unsanctioned) lub tolerowane.
- Wykrywanie Shadow IT „na pierwszy rzut oka".
- Możliwość zejścia do szczegółów: użytkownicy, ruch i dane.
- Dostęp do polityk kształtowania ruchu jednym kliknięciem.
- Filtrowanie użycia aplikacji chmurowych wg kategorii lub wolumenu.
- Szczegółowy, konfigurowalny raport użycia aplikacji chmurowych z pełną historią (historical reporting).
- Synchronized App Control automatycznie identyfikuje, klasyfikuje i umożliwia kontrolę wszystkich nieznanych aplikacji Windows i macOS w sieci, dzięki wymianie informacji pomiędzy endpointami zarządzanymi przez Sophos a firewallem.

## Ochrona i kontrola aplikacji

- Kontrola aplikacji oparta o sygnatury – wzorce (patterns) dla tysięcy aplikacji
- Cloud Application Visibility and Control umożliwia wykrywanie shadow IT.
- App Control Smart Filters pozwalają tworzyć dynamiczne

polityki, które automatycznie aktualizują się wraz z dodawaniem nowych wzorców.

- Wykrywanie i kontrola „mikroaplikacji” (micro app discovery and control).
- Kontrola aplikacji w oparciu o: kategorię, charakterystykę (np. zużycie pasma i wpływ na produktywność), technologię (np. P2P) oraz poziom ryzyka.
- Egzekwowanie polityk kontroli aplikacji per użytkownik lub per reguła sieciowa.

### Kształtowanie ruchu WWW i aplikacji

- Rozszerzone opcje QoS według kategorii WWW lub aplikacji –pozwalają ograniczać albo gwarantować wysyłanie/pobieranie (upload/download) lub łączny ruch, ustawiając priorytet i bitrate (indywidualnie lub współdzielone).

## Ochrona DNS (DNS Protection)

### Chmurowa usługa DNS

- Usługa rozwiązywania nazw domen (DNS).
- Wysokowydajny DNS w chmurze.
- Wspierany przez SophosLabs i AI.
- Blokuje złośliwe adresy URL już na etapie zapytania DNS (DNS lookup).
- Szczegółowe mechanizmy zgodności (compliance) umożliwiają blokowanie niepożądanych stron według kategorii.
- Zarządzanie z poziomu Sophos Central.

## NDR Essentials

### Network Detection and Response

- Chmurowy NDR.
- Wspierany przez AI.
- Wykrywa zaszyfrowaną komunikację zagrożeń bez deszyfrowania TLS.
- Wykrywa algorytmy generowania domen (DGA).
- Ocenia potencjalne zagrożenia i generuje alerty dla zdarzeń przekraczających ustawiony próg.
- Pełne wsparcie raportowania i logowania.

## Zero-Day Protection

### Dynamiczna analiza w sandboxie

- Pełna integracja z panelem (dashboardem) Twojego ekosystemu bezpieczeństwa Sophos.
- Inspekcja plików wykonywalnych i dokumentów z zawartością wykonywalną, w tym
  - in. .exe, .com, .dll, .doc, .docx, .docm, .rtf, PDF, a także archiwów zawierających takie pliki: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet.
- Zaawansowana analiza behawioralna, sieciowa i pamięciowa.
- Wykrywanie prób omijania sandboxa (sandbox evasion).
- Uczenie maszynowe (w tym deep learning) skanuje wszystkie „upuszczone” pliki wykonywalne (dropped executables).
- Wbudowane mechanizmy ochrony przed exploitami oraz CryptoGuard z technologii Sophos Intercept X.
- Szczegółowe raporty o złośliwych plikach – ze zrzutami ekranu oraz możliwością zwolnienia pliku z poziomu dashboardu (file release).
- Opcjonalny wybór centrum danych oraz elastyczne polityki dla użytkowników i grup: typy plików, wykluczenia i działania po analizie.
- Obsługa jednorazowych linków do pobrania (one-time download links).

### Statyczna analiza threat intelligence

- Wszystkie pliki zawierające aktywny kod pobierane z WWW lub trafiające do firewalla jako załączniki e-mail (m.in. pliki wykonywalne oraz dokumenty z zawartością wykonywalną: .exe, .com, .dll, .doc, .docx, .docm, .rtf, PDF) oraz archiwa zawierające te typy plików (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) są automatycznie wysyłane do analizy threat intelligence.
- Pliki są sprawdzane względem rozbudowanej bazy threat intelligence SophosLabs oraz analizowane przez wiele modeli uczenia maszynowego, aby identyfikować nowe i nieznane odmiany malware.
- Rozbudowane raportowanie obejmuje: widget w dashboardzie dla przeanalizowanych plików, szczegółową listę plików wraz z wynikami analizy oraz raport pokazujący rezultat działania każdego z modeli ML.

## Centralna orkiestracja

### Orkiestracja SD-WAN

- Orkiestracja SD-WAN i VPN z prostym, zautomatyzowanym kreatorem tworzenia tuneli VPN site-to-site między lokalizacjami –z doborem optymalnej architektury (hub-and-spoke, full mesh lub wariant mieszany).
- Obsługa tuneli IPsec, SSL oraz RED, z płynną integracją z funkcjami SD-WAN w zakresie priorytetyzacji aplikacji, optymalizacji routingu oraz wykorzystania wielu łączy WAN dla większej odporności i wydajności.

### Central Firewall Reporting Advanced

- 30 dni chmurowego przechowywania danych do raportowania historycznego firewalla, z zaawansowanymi funkcjami zapisywania, harmonogramowania i eksportu raportów niestandardowych.

## Integracja XDR i MDR

- Integracja z Sophos XDR i MDR w celu dostarczania telemetrii oraz threat intelligence na potrzeby threat huntingu i analizy.
- Sophos Active Threat Response wykorzystuje feedy zagrożeń od analityków MDR i XDR, aby automatycznie identyfikować, blokować i izolować aktywne zagrożenia w sieci.
- Telemetria IoC w ramach Synchronized Security zbiera kluczowe informacje o zagrożeniu, użytkownikach, procesach oraz urządzeniu, które zostało skompromitowane.

# Ochrona poczty

## Email Protection and Control

- EmSkanowanie poczty z obsługą SMTP, POP3 i IMAP.
- Usługa reputacyjna z monitoringiem „wybuchów" spamu (spam outbreak monitoring) oparta o opatentowaną technologię wykrywania powtarzalnych wzorców.
- Blokowanie spamu i malware już w trakcie transakcji SMTP.
- Ochrona antyspamowa DKIM i BATV.
- Greylisting spamu oraz ochrona SPF (Sender Policy Framework).
- Weryfikacja odbiorców dla błędnie wpisanych adresów e-mail.
- Drugi niezależny silnik antymalware (Avira) do podwójnego skanowania.
- Live Protection – chmurowe sprawdzanie w czasie rzeczywistym pod kątem najnowszych informacji threat intelligence.
- Automatyczne aktualizacje sygnatur i wzorców.
- Obsługa smart host dla wychodzących relayów.
- Wykrywanie typu plików / blokowanie / skanowanie załączników.
- Akceptacja, odrzucenie lub porzucenie zbyt dużych wiadomości.
- Wykrywanie linków phishingowych w wiadomościach e-mail.
- Gotowe reguły skanowania treści lub możliwość tworzenia własnych reguł wg różnych kryteriów, z precyzyjnymi opcjami polityk i wyjątkami.
- Obsługa szyfrowania TLS dla SMTP, POP i IMAP.
- Automatyczne dodawanie podpisu do wszystkich wiadomości wychodzących.
- Archiwizacja poczty (Email archiver).
- Indywidualne listy blokowania i zezwalania nadawców per użytkownik – zarządzane z portalu użytkownika.

## Zarządzanie kwarantanną poczty

- Podsumowania kwarantanny spamu (digest) oraz opcje powiadomień.
- Kwarantanna malware i spamu z wyszukiwaniem i filtrowaniem wg daty, nadawcy, odbiorcy, tematu i powodu – z opcją zwalniania i usuwania wiadomości.
- Samoobsługowy portal użytkownika do podglądu i zwalniania wiadomości z kwarantanny.

## Szyfrowanie poczty i DLP

- Szyfrowanie SPX (zgłoszenie patentowe w toku) dla jednokierunkowego szyfrowania wiadomości.
- Samoobsługowa rejestracja odbiorcy oraz zarządzanie hasłem SPX.
- Możliwość dodawania załączników do bezpiecznych odpowiedzi SPX.
- Pełna transparentność – bez dodatkowego oprogramowania i bez potrzeby instalacji klienta.
- Silnik DLP z automatycznym skanowaniem e-maili i załączników pod kątem danych wrażliwych.
- Gotowe listy kontroli treści (CCL) dla typów danych wrażliwych, m.in. PII, PCI, HIPAA i innych – utrzymywane przez SophosLabs.

# Ochrona serwerów WWW

## Ochrona Web Application Firewall

- Reverse proxy.
- Mechanizm utwardzania URL z ochroną przed deep-linkingiem oraz atakami typu directory traversal.
- Mechanizm utwardzania formularzy (form hardening).
- Ochrona przed SQL injection.
- Ochrona przed cross-site scripting (XSS).
- Podwójne silniki antywirusowe (Sophos i Avira).
- Offloading szyfrowania HTTPS (TLS/SSL) – odciążenie serwerów z obsługi szyfrowania.
- Podpisywanie cookies przy użyciu podpisów cyfrowych.
- Routing oparty o ścieżkę (path-based routing).
- Egzekwowanie polityk Geo-IP.
- Własna konfiguracja szyfrów oraz wymuszanie wersji TLS.
- Wymuszanie HSTS oraz nagłówka X-Content-Type-Options.
- Obsługa protokołu Outlook Anywhere.
- Reverse authentication (offloading) dla uwierzytelniania formularzowego oraz Basic Authentication przy dostępie do serwera.
- Abstrakcja serwerów wirtualnych i fizycznych.
- Wbudowany load balancer rozkładający ruch pomiędzy wieloma serwerami.
- Możliwość granularnego pomijania wybranych kontroli, gdy jest to wymagane.
- Dopasowywanie żądań po sieci źródłowej lub wskazanych docelowych URL.
- Obsługa operatorów logicznych AND/OR.
- Wsparcie zgodności dla różnych konfiguracji oraz nietypowych wdrożeń.
- Opcje zmiany parametrów wydajności web application firewall.
- Opcja limitu rozmiaru skanowania.

- Zezwalanie lub blokowanie zakresów adresów IP.
- Obsługa symboli wieloznacznych (wildcard) dla ścieżek serwera i domen.
- Automatyczne dodawanie prefiksu/sufiksu na potrzeby uwierzytelniania.

# Raportowanie i logowanie

## Central Firewall Reporting

- Gotowe raporty z elastycznymi opcjami personalizacji.
- Raportowanie dla Sophos Firewall: urządzenia sprzętowe, programowe, wirtualne oraz chmurowe.
- Intuicyjny interfejs z graficzną prezentacją danych.
- Dashboard raportowy zapewnia szybki podgląd zdarzeń z ostatnich 24 godzin.
- Łatwa identyfikacja aktywności, trendów i potencjalnych ataków.
- Proste kopie zapasowe logów i szybkie ich odzyskiwanie na potrzeby audytów.
- Uproszczone wdrożenie bez konieczności posiadania specjalistycznej wiedzy technicznej.

## Central Firewall Reporting Advanced

- Raportowanie zbiorcze (aggregate) dla wielu firewalli.
- Zapisywanie własnych szablonów raportów.
- Raportowanie harmonogramowane.
- Eksport raportów do formatów PDF, CSV lub HTML.
- Przechowywanie danych do 1 roku na każdy firewall.
- Konektor do data lake MDR/XDR na potrzeby threat huntingu.

## Raportowanie On-box

**UWAGA**: Raportowanie Sophos Firewall jest dostępne bez dodatkowych opłat, ale dostępność poszczególnych logów, raportów i widgetów może zależeć od wykupionych licencji modułów ochrony.

- Setki raportów na urządzeniu z opcją raportów własnych, m.in.:dashboardy: Traffic, Security, User Threat Quotient; aplikacje: App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP; sieć i zagrożenia: Active Threat Response i threat feeds, Security Heartbeat, IPS, wireless, zero-day threat protection; VPN, Email; compliance: HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA.
- Monitoring aktywności bieżącej: kondycja systemu, aktywni użytkownicy, połączenia IPsec, użytkownicy zdalni, aktywne połączenia, klienci Wi-Fi, kwarantanna oraz ataki DoS.
- Monitoring wydajności łączy SD-WAN pod kątem jittera, opóźnień i utraty pakietów.
- Anonimizacja raportów.
- Wysyłka raportów do wielu odbiorców według grup raportów, z elastycznymi częstotliwościami.
- Eksport raportów jako HTML, PDF oraz Excel (XLS).
- Zakładki raportów.
- Konfigurowalna retencja logów według kategorii.
- Rozbudowany podgląd logów: widok kolumnowy i szczegółowy, zaawansowane filtrowanie i wyszukiwanie, linkowane ID reguł oraz personalizacja widoku danych.

# Centralne zarządzanie (Central Management)

## Sophos Central

- Chmurowe zarządzanie i raportowanie dla wielu firewalli: polityki grupowe oraz jedna konsola dla wszystkich produktów Sophos z obszaru bezpieczeństwa IT.
- Zarządzanie politykami grupowymi: obiekty, ustawienia i polityki zmieniasz raz, a następnie są automatycznie synchronizowane do wszystkich firewalli w grupie.
- Task Manager zapewnia pełny audyt historii oraz monitoring statusu zmian polityk grupowych.
- Zarządzanie kopiami konfiguracji: Sophos Central przechowuje 5 ostatnich kopii konfiguracji dla każdego firewalla, z możliwością przypięcia jednej kopii na stałe dla łatwego dostępu.
- Harmonogramowanie aktualizacji firmware z Sophos Central – automatyczne aktualizacje mogą być wdrażane w dowolnym czasie.
- Wdrożenie zero-touch: konfiguracja początkowa jest przygotowywana w Sophos Central i eksportowana na pendrive; przy uruchomieniu urządzenie ładuje konfigurację i automatycznie łączy się ponownie z Sophos Central.

## Zero Trust Network Access

- Wbudowana brama Sophos ZTNA zapewnia bezpieczny dostęp do aplikacji hostowanych za firewallem.
- Zarządzanie z poziomu Sophos Central.

# Funkcje zapory Sophos w ramach subskrypcji Podsumowanie

| | Pakiet Xstream Protection | | | | | | | Dostępne oddzielnie | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | *Pakiet ochrony standardowej* | | | | *Dostępny osobno* | | | | | |
| | Podstawowa zapora sieciowa | Ochrona sieci | Ochrona sieci Web | Ochrona DNS | Funkcje dostępne wyłącznie w pakiecie | Ochrona przed atakami typu zero-day | Centralna koordynacja | Centralna zapora sieciowa Raportowanie zaawansowane | Ochrona poczty elektronicznej | Ochrona serwera WWW |
| Zarządzanie ogólne (w tym HA) | • | | | | | | | | | |
| Architektura Xstream | • | | | | | | | | | |
| Zapora sieciowa, sieci i routing | • | | | | | | | | | |
| Xstream SD-WAN | • | | | | | | | | | |
| Podstawowe kształtowanie ruchu i limity | • | | | | | | | | | |
| Bezpieczna sieć bezprzewodowa | • | | | | | | | | | |
| Uwierzytelnianie | • | | | | | | | | | |
| Portal samoobsługowy dla użytkowników | • | | | | | | | | | |
| VPN (IPsec, SSL itp.) | • | | | | | | | | | |
| RED Site-to-Site VPN | • | | | | | | | | | |
| Klient VPN Sophos Connect | • | | | | | | | | | |
| Zapobieganie włamaniom (IPS) | | • | | | | | | | | |
| Aktywna reakcja na zagrożenia | | | | | | | | | | |
| Sophos X-Ops Threat Feeds | | • | | | | | | | | |
| Kanały informacyjne MDR/XDR dotyczące zagrożeń | | | | | • | | | | | |
| Strumienie zagrożeń stron trzecich | | | | | • | | | | | |
| Zsynchronizowane sygnały bezpieczeństwa | | • | | | | | | | | |
| Zarządzanie urządzeniami SD-RED | | • | | | | | | | | |
| VPN bez klienta | | • | | | | | | | | |
| Zsynchronizowana kontrola aplikacji | | | • | | | | | | | |
| Ochrona i kontrola sieci | | | • | | | | | | | |
| Ochrona i kontrola aplikacji | | | • | | | | | | | |
| Widoczność aplikacji w chmurze | | | • | | | | | | | |
| Kształtowanie ruchu internetowego i aplikacji | | | • | | | | | | | |
| Bezpieczeństwo i zgodność DNS | | | | • | | | | | | |
| Podstawy NDR | | | | | • | | | | | |
| Dynamiczna analiza piaskownicy | | | | | | • | | | | |
| Analiza informacji o zagrożeniach | | | | | | • | | | | |
| Koordynacja SD-WAN | | | | | | | • | | | |
| Centralne raportowanie danych dotyczących zapory sieciowej* | | 7 dni | 7 dni | 7 dni | 7 dni | 7 dni | 30 dni | Do 1 roku | 7 dni | 7 dni |
| Zaawansowane funkcje CFR | | | | | | | • | • | | |
| Ochrona i kontrola poczty elektronicznej | | | | | | | | | • | |
| Zarządzanie kwarantanną poczty elektronicznej | | | | | | | | | • | |
| Szyfrowanie poczty elektronicznej i DLP | | | | | | | | | • | |
| Ochrona za pomocą zapory sieciowej aplikacji internetowych | | | | | | | | | | • |
| Rejestrowanie/raportowanie w urządzeniu | • | • | • | • | • | • | • | • | • | • |
| Centralne zarządzanie Sophos** | | • | • | • | • | • | • | • | • | • |
| Brama ZTNA** | | • | • | • | • | • | • | • | • | • |

Uwaga: Niektóre funkcje nie są obsługiwane w modelach XGS 87 i XGS 88.
(raportowanie na urządzeniu, podwójne skanowanie antywirusowe, skanowanie antywirusowe WAF oraz funkcja agenta transferu wiadomości e-mail (MTA)). Opcje licencjonowania MSP różnią się nieznacznie od powyższych.
* Czas przechowywania danych jest szacunkowy i oparty na średnim wykorzystaniu sieci. Może się różnić w zależności od rzeczywistej ilości danych w logach. Narzędzie do szacowania pojemności pamięci.



** Zawarte w każdym pakiecie, wsparciu lub subskrypcji ochrony. Klienci posiadający wyłącznie licencję podstawową muszą dodać wsparcie, aby móc korzystać z tych funkcji.

## Plany wsparcia

| | ROZSZERZONE WSPARCIE (W zestawach Standard i Xstream Protection) | ROZSZERZONE WSPARCIE PLUS (dostępne jako aktualizacja z rozszerzonej pomocy technicznej) |
|---|---|---|
| Całodobowa pomoc techniczna dostępna na wielu kanałach (telefon, portal internetowy, czat), w tym pomoc zdalna i dostęp do bazy wiedzy oraz forów pomocy technicznej | • | • |
| Pobieranie oprogramowania układowego, aktualizacje i wydania serwisowe ** | • | • |
| Centralne zarządzanie Sophos, raportowanie i brama ZTNA | • | • |
| Zaawansowana wymiana sprzętu dla aktywnych urządzeń | • | • |
| Zaawansowana wymiana sprzętu dla pasywnego urządzenia HA* | | • |
| Zaawansowana wymiana sprzętu dla urządzeń SD-RED/APX | | • |
| Dostęp VIP (połączenia kierowane do starszych inżynierów) | | • |
| Zdalne doradztwo (2–8 godzin rocznie) | | • |

* Aby włączyć rozszerzoną ochronę RMA dla pasywnego urządzenia HA, aktywne urządzenie musi posiadać licencję wsparcia Enhanced Plus.
Szczegółowe informacje można znaleźć w przewodniku po usługach wsparcia Sophos.

** Uwaga: Aby otrzymywać aktualizacje oprogramowania układowego, do każdego zakupionego modułu należy dodać wsparcie techniczne.

Sprzedaż w Wielkiej Brytanii i na całym świecie Tel.: +44 (0)8447 671131
E-mail: sales@sophos.com

Sprzedaż w Ameryce Północnej
Bezpłatny numer: 1-866-866-2802
E-mail: nasales@sophos.com

Sprzedaż w Australii i Nowej Zelandii
Tel.: +61 2 9409 9100
E-mail: sales@sophos.com.au

Sprzedaż w Azji
Tel.: +65 62244168
E-mail: salesasia@sophos.com



25-04-16 FL-EN (MP)

SOPHOS