Wsparcie dla zapory sieciowej Sophos

Zalety zapory sieciowej Sophos:

Co nowego?

Sophos niedawno wypuścił nowej generacji urządzenia zapory sieciowej z serii XGS. Nowe modele mają architekturę dwuprocesorową z dedykowanymi procesorami Xstream Flow zapewniającymi bardzo wysoki poziom ochrony i wydajności.

Ochrona i wydajność

Nowa seria XGS umożliwia przyspieszenie zaufanego ruchu dzięki lepszemu monitorowaniu oraz głębokiej analizie pakietów TLS. Kontrola zaszyfrowanego ruchu pod kątem potencjalnych zagrożeń nie tylko zapewnia doskonałą ochronę ruchu sieciowego, ale nie wpływa na ogólną wydajność i przepustowość sieci.

Proste zarządzanie

Zapora ogniowa Sophos Firewall jest nie tylko bardzo łatwa do wdrożenia i zarządzania, ale stanowi także część najlepszego ekosystemu cyberbezpieczeństwa w branży. Rozwiązanie pozwala zarządzać wszystkimi produktami Sophos z poziomu jednego pulpitu, zapewnia integrację z ochroną punktów końcowych Sophos InterceptX, ale także umożliwia funkcji bezpieczeństwa Synchronized Security automatyczną identyfikację i izolowanie zagrożeń, a także wykrywanie ich w różnych produktach.

Najlepsze rozwiązanie w świetnej cenie

Ogólnie rzecz biorąc, zapora sieciowa Sophos Firewall oferuje doskonałe rozwiązania i większą liczbę funkcji w każdym przedziale cenowym. Rozwiązanie obejmuje wiele funkcji dostępnych bez żadnych opłat, w przypadku których konkurencja wymaga wykupienia dodatkowych licencji.

Rozważasz lub korzystasz z Fortinet lub PaloAlto? Zobacz dlaczego klienci wybierają zapory sieciowe Sophos:

Więcej funkcji w podobnej cenie

Urządzenia zapory sieciowej Sophos są bardzo funkcjonalne, łatwe w zarządzaniu, a teraz - po wprowadzeniu nowej serii XGS - oferują najlepszą w branży wydajność w każdym przedziale cenowym. Za podobną cenę Sophos oferuje funkcje raportowania w urządzeniach, zdalny dostęp VPN, centralne zarządzanie w chmurze i wiele więcej.

Konkurencja oferuje wiele możliwości. Jednak często łączy dostęp do nich z koniecznością zakupu licencji lub dodatkowych produktów i urządzeń, co bardzo zwiększa koszt.
Na przykład: pełne raportowanie, zdalny dostęp VPN, centralne zarządzanie i integracja pomiędzy produktami zwykle oznacza konieczność zakupu dodatkowego sprzętu i/lub licencji. Jeśli są w ogóle dostępne.

Skuteczniejsze zarządzanie bezpieczeństwem

Sophos Firewall zapewnia firmie dowolnej wielkości zaawansowaną ochronę przed zagrożeniami. Wydajne deszyfrowanie i głęboka analiza pakietów TLS oraz monitorowanie aplikacji to teraz tylko kilka kliknięć. Do tego bardzo łatwa orkiestracja VPN i jeden pulpit Sophos Central do zarządzania wszystkimi zaporami sieciowymi i produktami Sophos.

Konkurenci oferują podobne funkcje, ale ich konfigurowanie i wdrażanie jest bardziej złożone, niezależnie od tego, czy chodzi o reguły ochrony, pulpity i raportowanie, czy integrację produktów i centralne zarządzanie.

Lepszy ekosystem

Sophos to także zintegrowany i skuteczny ekosystem bezpieczeństwa z rozwiązaniami Sophos Central, Synchronized Security, wykrywaniem zagrożeń i podejmowaniem działań w przypadku różnych produktów XDR oraz unikalną usługą Managed Threat Response Service (MTR) – żaden inny dostawca nie oferuje naszego poziomu integracji.

Konkurenci mają bardzo rozdrobnione ekosystemy, które nie są tak dobrze zintegrowane, a PAN nie oferuje pulpitu zarządzania swoimi zaporami sieciowymi w chmurze. Oba ekosystemy są bardziej złożone w użytkowaniu i brakuje im korzyści płynących z integracji, które zapewnia Sophos.

Najważniejsze funkcje naszych rozwiązań

Ogólne: Czego używasz obecnie jako zapory internetowej? Czy jest coś, co można by zrobić lepiej? (użyj poniższych pytań, żeby zrozumieć, które z poniższych obszarów są problematyczne)	Funkcje zapory Sophos — dlaczego robimy to lepiej:
Ochrona: Czy miały miejsce jakieś ataki, naruszenia lub pojawiło się złośliwe oprogramowanie? Czy może Pan powiedzieć w jaki sposób? Czy stosowana jest analiza szyfrowania TLS? IPS? ML? Sandoboxy? Jeśli nie, to dlaczego? **Wydajność**: Jaka jest wydajność zapory sieciowej przy włączonej najwyższej ochronie? Jak zarządzana jest wydajność najważniejszego ruchu SaaS, Cloud i VoIP?	Architektura Xstream zapewnia optymalną wydajność i ochronę Procesory Xstream Flow z serii XGS zapewniają przyspieszenie sprzętowe dla zaufanego ruchu Najlepsza w branży analiza Xstream TLS 1.3 z niezrównaną inteligencją i widocznością Silnik Xstream DPI z najnowszą generacją IPS, AV, monitoringiem sieci i aplikacji powstrzymuje znane zagrożenia Ochrona przed atakami zero-day dzięki technikom głębokiego uczenia i dynamicznemu sandbxingowi Integracja z punktami końcowymi Synchronized Security pozwala automatycznie zidentyfikować i odizolować zagrożenia
Widoczność: Czy potrafi Pan odpowiedzieć na podstawowe pytania dotyczące użytkowników najwyższego ryzyka, aktywnych zagrożeń, niechcianych aplikacji, ukrytego IT, zawartości zaszyfrowanego ruchu, podejrzanych pobrań? **Zarządzanie**: Jak obecnie zarządzane jest bezpieczeństwo IT? Z iloma produktami i dostawcami Państwo współpracują? Czy któreś z używanych produktów mogą zostać zintegrowane ze sobą?	Świetne pulpity i zintegrowane raportowanie zapewniają natychmiastowy wgląd bez konieczności ponoszenia dodatkowych kosztów Jeden pulpit Sophos Central do zarządzania wszystkimi zaporami sieciowymi i produktami Sophos Integracja Synchronized Security punktów końcowych pozwalająca udostępniać status i dane telemetryczne zaporze sieciowej Wygoda użytkownika - łatwe i intuicyjne narzędzia umożliwiające wykonanie zaawansowanych zadań, jak np. orkiestracja VPN. Wbudowana inteligencja i wiedza ułatwiająca tworzenie złożonych reguł pod nadzorem SophosLabs
Sieć: Jak zarządzany jest zdalny dostęp? Jak połączone są zdalne lokalizacje i filie? Jaka jest strategia SD-WAN?	Elastyczna łączność modułowa pasująca do każdej sieci (miedzianej, światłowodowej, bezprzewodowej, komórkowej) Prosty i bezpłatny dostęp zdalny do sieci VPN dzięki integracji z ZTNA Prosta sieć zdalna z kreatorami konfiguracji SD-RED i VPN Zoptymalizowana wydajność aplikacji dzięki routingowi SD-WAN

SOPHOS

Urządzenia zapory sieciowej nowej generacji - serii XGS

Wszystkie urządzenia z serii XGS mają architekturę dwuprocesorową, łączącą wielordzeniowy procesor CPU z dedykowanym procesorem Xstream Flow zapewniającym przyspieszanie sprzętowe.

Małe i średnie firmy oraz oddziały: doskonałe desktopowe urządzenia z serii XGS, łączność typu "wszystko w jednym"

SOHO (OGRANICZONA FUNKCJONALNOŚĆ) | MAŁE BIURO | ODDZIAŁY | ODDZIAŁY

XGS87(w) | XGS107(w) | XGS116(w) | XGS126(w) | XGS136(w)

Opcjonalny drugi, dodatkowy zewnętrzny zasilacz

Modułowe gniazdo (dla modułów LTE lub 2 modułów Wi-Fi dla modeli) | Wbudowane PoE

Porty 2.5GE

Model	Specyfikacje			Przepustowość		
	PORTY/ SLOTY ROZSZERZEŃ	MAKS LICZBA PORTÓW (W TYM MODUŁÓW)	W-MODEL*	FIREWALL (MBPS)	OCHRONA PRZED ZAGROŻENIAMI (MBPS)	XSTREAM SSL/TLS (MBPS)
XGS87(w)	5/-	5	Wi-Fi 5	3 700	240	375
XGS107(w)	9/-	9	Wi-Fi 5	7 000	330	420
XGS116(w)	9/1	9	Wi-Fi 5	7 700	685	650
XGS126(w)	14/1	14	Wi-Fi 5	10 500	900	800
XGS136(w)	14/1	14	Wi-Fi 5	11 500	1,000	950

Distributed Edge - elementy sieci zapewniające bezstratność i wysoką przepustowość: Montaż w szafie serwerowej serii XGS 1U — wydajność i wszechstronność

BIURO ŚREDNIEJ WIELKOŚCI | ŚREDNIEJ WIELKOŚCI FIRMA Z WIELOMA ODDZIAŁAMI | ŚREDNIEJ WIELKOŚCI FIRMA Z WIELOMA ODDZIAŁAMI

XGS2100/2300 | XGS3100/3300 | XGS4300 | XGS4500

Opcjonalny dodatkowy, zewnętrzny zasilacz

Opcjonalna wewnętrzna dodatkowa moc

Jedno gniazdo flexiport | Opcjonalne PoE

Podwójne gniazda flexiport| Opcjonalne PoE

Wbudowane porty 2.5GE

Modele 1U	Specyfikacje			Przepustowość		
	PORTY/ SLOTY ROZSZERZEŃ	MAKS LICZBA PORTÓW (W TYM MODUŁÓW)	W-MODEL*	FIREWALL (MBPS)	OCHRONA PRZED ZAGROŻENIAMI (MBPS)	XSTREAM SSL/TLS (MBPS)
XGS2100	10/1	18	nie dotyczy	30 000	1 250	1 100
XGS2300	10/1	18	nie dotyczy	35 000	1 400	1 450
XGS3100	12/1	20	nie dotyczy	38 000	2 000	2 470
XGS3300	12/1	20	nie dotyczy	40 000	2 770	3 130
XGS4300	12/2	28	nie dotyczy	75 000	4 800	8 000
XGS4500	12/2	28	nie dotyczy	80 000	8 390	10 600

Enterprise Edge - elementy sieci zapewniające wydajną i bezpieczną komunikację w firmie: Seria XGS do montażu w szafie serwerowej 2U – Bezkompromisowa wydajność, łączność, redundancja

WIĘKSZA FIRMA Z WIELOMA ODDZIAŁAMI

XGS5500 | XGS6500

Wewnętrzny dodatkowy zasilacz typu hot-swap

Dodatkowy dysk SSD i wentylator z możliwością wymiany podczas pracy

Stałe porty miedziane i światłowodowe 10G oraz dwie standardowe gniazda flexiport

Jedno, wysoko wydajne gniazdo flexiport

Dwa, wysoko wydajne gniazda flexiport

Modele 2U	Specyfikacje			Przepustowość		
	PORTY/ SLOTY ROZSZERZEŃ	MAKS LICZBA PORTÓW (W TYM MODUŁÓW)	W-MODEL*	FIREWALL (MBPS)	OCHRONA PRZED ZAGROŻENIAMI (MBPS)	XSTREAM SSL/TLS (MBPS)
XGS5500	16/3	48	nie dotyczy	100 000	12 390	13 500
XGS6500	20/4	68	nie dotyczy	115 000	17 050	16 000

SOPHOS

Wsparcie dla zapory sieciowej Sophos

Licencje dla zapory sieciowej Sophos

Pakiet Xstream Protection pozwala zapewnić sieci najwyższy poziom bezpieczeństwa. Każda z subskrypcji może zostać również zakupiona indywidualnie.

Pakiet ochrony XStream	
Licencja podstawowa	Sieć, bezprzewodowa, architektura Xstream, nieograniczony dostęp zdalny VPN, VPN typu site-to-site, raportowanie
Ochrona sieci	Silnik Xstream TLS i DPI, IPS, ATP, Security Heartbeat™, SD-RED VPN, raportowanie
Ochrona sieci Web	Silnik Xstream TLS i DPI, bezpieczeństwo i monitorowanie sieci, monitorowanie aplikacji, raportowanie
Ochrona przed atakami Zero-Day	Analiza plików oparta o uczenie maszynowe i sandboxing, raportowanie
Orkiestracja ***	Orkiestracja SD-WAN VPN, zaawansowane raportowanie Central Firewall Reporting Advanced (30 dni), gotowość do obsługi MTR / XDR
Rozszerzone wsparcie	Wsparcie 24/7, aktualizacje, rozszerzona gwarancja wymiany sprzętu na czas określony

*Dostępne wkrótce

Ochrona niestandardowa:

Dostępny jest standardowy pakiet Standard Protection obejmujący podstawowe funkcje ochrony. Jednak ochrona poczty e-mail i serwera WWW dostępna jest osobno, jako dodatek do dowolnego pakietu.

Standardowy pakiet ochrony	
Licencja podstawowa	Sieć, bezprzewodowa, architektura Xstream, nieograniczony dostęp zdalny VPN, VPN typu site-to-site, raportowanie
Ochrona sieci	Silnik Xstream TLS i DPI, IPS, ATP, Security Heartbeat™, SD-RED VPN, raportowanie
Ochrona sieci Web	Silnik Xstream TLS i DPI, bezpieczeństwo i monitorowanie sieci, monitorowanie aplikacji, raportowanie
Rozszerzone wsparcie	Wsparcie 24/7, aktualizacje, rozszerzona gwarancja wymiany sprzętu na czas określony

Dodatkowe moduły ochrony	
Ochrona poczty	Wbudowana ochrona antyspamowa, AV, DLP, szyfrowanie
Ochrona serwera WWW	Zapora dla aplikacji internetowych

Zarządzanie i raportowanie z poziomu Sophos Central:

Wszystkie zapory ogniowe Sophos obejmują zarządzanie z poziomu chmury i podstawowe raportowanie bez konieczności ponoszenia dodatkowych opłat. Zalecane jest jednak dodanie zaawansowanego raportowania *Central Firewall Reporting Advanced* do zakupu każdej zapory sieciowej.

Raportowanie z poziomu platformy Sophos Central:	
Zaawansowane raportowanie Central Firewall Reporting (CFR)	Dodaje zaawansowane opcje zapisywania, planowania i eksportowania raportów oraz raportowanie dotyczące wielu zapór z możliwością przechowywania danych w chmurze przez okres do 1 roku

Elastyczne wdrożenia

Zapora sieciowa Sophos Firewall obsługuje różne platformy: chmurowe, wirtualne i programowe pozwalając spełnić najróżniejsze potrzeby.

aws Azure NUTANIX

intel Virtual

Lista kontrolna dla zapytań ofertowych

ZAPORA SIECIOWA SOPHOS:

- Urządzenie serii XGS
  - Moduły komunikacyjne/nadajniki-odbiorniki
    Drugi nadmiarowy zasilacz
  - Zestaw do montażu w stojaku
  - Urządzenie HA (aktywne-aktywne lub aktywne-pasywne)
  - Urządzenie wirtualne lub programowe

DODATKOWE OPCJE DOSTĘPU DO SIECI:

- Bezprzewodowe punkty dostępowe APX
- Urządzenia SD-RED
- ZTNA (Zero Trust Network Access) – inEAP

SUBSKRYPCJE NA OCHRONĘ I RAPORTY:

- Pakiet ochrony Xstream
  - Zaawansowana obsługa poczty (cloudemail)
  - Wbudowana ochrona poczty e-mail
  - Ochrona serwera WWW
- Subskrypcje HA dla aktywnych-aktywnych
  - Zaawansowane, scentralizowane raportowanie dla zapory sieciowej (Central Firewall Reporting, CFR)
  - Minimalne, zaawansowane raportowanie 1-5 CFR dla zapory sieciowej (narzędzie do określania dostępnej przestrzeni dyskowej znajduje się na stronie sophos.com/cfrsizing)

WSPARCIE I USŁUGI DLA ZAPORY SIECIOWEJ:

- Upgrade do Ulepszonego Wsparcia Technicznego Plus
- Czas świadczenie Usług Profesjonalnych

DODATKOWE PRODUKTY I USŁUGI SOPHOS:

- Sophos Intercept X Endpoint z XDR (udostępnia Synchronized Security)
- Usługa Managed Threat Response (MTR)

SOPHOS