Wymiana routera brzegowego na Sophos XG Firewall

Stan początkowy

- router brzegowy z AV, IPS, serwerem VPN
- lokalne zabezpieczenie antywirusowe na stacje końcowe i serwery
- sieć bezprzewodowa zbudowana w oparciu o indywidualne punkty dostępowe klasy domowej

Wymagania klienta

- obsłużenie dwóch symetrycznych łączy internetowych po 100 Mbps każde
- zestawienie do 50 połączeń klienckich VPN (SSL i L2TP-IPSec) i do 10 tuneli VPN IPSec
- minimum 8 interfejsów 1Gbit RJ45
- zabezpieczenie antymalware i antyspam dla lokalnego serwera poczty
- możliwość ograniczania dostępu do witryn internetowych dla ok. 70 pracowników
- skanowanie ruchu internetowego (AV, IPS) dla pracowników i serwerów
- ustawienie reguł wykorzystania pasma przez kluczowe dla firmy usługi

Pierwszy kontakt

Zgłosił się do nas klient, który szukał alternatywy dla wykorzystywanego dotychczas w jego firmie **routera brzegowego**, posiadającego nieliczne mechanizmy bezpieczeństwa (silnik AV, IPS/IDS), prosty web filtering i serwer VPN dla połączeń klienckich i tunelowych. Rozwiązanie, które było dotychczas używane, oprócz sporego już wieku, który determinował jego prędkość i funkcjonalność, nie nadążało już za konkurencją pod względem oferowanych możliwości w zakresie ochrony znajdujących się za nim urządzeń. Dodatkowo produkt, który był wystarczający 5 lat wcześniej, wraz z rozwojem firmy stał się wąskim gardłem, ze względu na niewielką liczbę portów i praktycznie zerowe opcje rozbudowy.

Wybór klienta padł na **Sophos XG**. Na tym etapie klient nie wiedział zbyt wiele o samym rozwiązaniu, natomiast skusiła go promocja, w ramach której istniała możliwość otrzymania urządzenia za darmo przy zakupie pakietu subskrypcji na okres 3 lat. Dodatkowo klient wykorzystywał w domu darmowe narzędzie do ochrony urządzeń Windows i Mac – **Sophos Home**, z którego możliwości był tak bardzo zadowolony, iż nie poprzestał na wersji 100% darmowej, ograniczonej do 3 urządzeń i posiadającej jedynie klasyczne zabezpieczenie antymalware, ale wykupił wersję **Premium**, w ramach której miał możliwość zabezpieczenia do 10 urządzeń, przy wykorzystaniu najnowszych technologii **Deep Learning** i antiransomware.

Skontaktował się właśnie z nami, gdyż przekonał go status partnerski, posiadany przez **Sun Capital sp. z o.o.** oraz bliskość siedzib naszych firm.

W trakcie rozmowy okazało się, iż wstępnie wytypowany przez niego, jako najbardziej optymalny, pakiet subskrypcji **EnterpriseGuard**, w skład którego wchodzą subskrypcje **Network i Web Protection**, może nie zabezpieczyć firmy w 100%. W wewnętrznej sieci klient posiadał dodatkowo własny serwer pocztowy, który również mógłby zostać zabezpieczony przy użyciu brzegowej bramki antywirusowej i antyspamowej. Jakby tego było mało, klient narzekał również na sieć bezprzewodową w głównym budynku firmy, w którym znajdują się m.in. biura oraz sala konferencyjna, jednak zdążył się już dowiedzieć, że **Sophos XG** może być kontrolerem sieci bezprzewodowej, obsługującym dedykowane punkty dostępowe **Sophos APX** i funkcjonalność taka jest zawarta w podstawowej licencji (tzw. Base License), która jest dostarczana w cenie każdego urządzenia **Sophos XG**.

Sophos Platinum Partner

Sun Capital sp. z o.o.
ul. Ołtaszyńska 92c/6
53-034 Wrocław

https://suncapital.pl

tel.: +48 71 360 81 00
email: sprzedaz@suncapital.pl

Na obecnym etapie klient prezentował ogólną znajomość oferty Sophos, w związku z czym poprosił o dobranie rozwiązania zabezpieczającego dla stacji końcowych i serwerów, którym chciał zastąpić wykorzystywany dotychczas produkt, z którym miał coraz większe problemy – głównie związane z konsolą centralnego zarządzania. Ponadto, jako osoba wykorzystująca oprogramowanie **Sophos Home** oraz aktywnie korzystająca z Internetu i śledząca pojawiające się co jakiś czas doniesienia o atakach ransomware na firmy i instytucje, chciał mieć produkt, który zabezpieczy jego i jego firmę przed tego typu zagrożeniami.

Dobór rozwiązania

Aby spełnić wymagania klienta pod kątem wydajności i poziomu bezpieczeństwa, nasz inżynier zaproponował mu następujące rozwiązania:
- **Sophos XG 210** z dodatkowym modułem Flexi (dodatkowe 8 portów 1Gbit RJ45) oraz pakietem subskrypcji **FullGuard**, dzięki któremu zabezpieczone zostaną kluczowe elementy infrastruktury firmowej – komputery pracowników, serwery, poczta oraz zbudowana zostanie centralnie zarządzana sieć bezprzewodowa,
- **APX 320** – punkty dostępowe do zbudowania sieci bezprzewodowej w częściach wspólnych biurowca oraz w sali konferencyjnej,
- **Sophos Central Intercept X Advanced z EDR** dla stacji końcowych i serwerów.

Dzięki zastosowaniu produktów do ochrony marki **Sophos**, możliwe było wykorzystanie mechanizmu **Synchronized Security**, który zapewnia wymianę informacji pomiędzy poszczególnymi elementami systemu. Takie wzajemne przekazywanie danych pozwala na m.in. identyfikowanie na brzegu sieci nieznanych aplikacji internetowych uruchamianych na stacjach końcowych, co w dalszej fazie umożliwia przygotowanie zasad ruchu (np. ich blokowanie) i wykorzystania pasma (ograniczenie wykorzystywanej przez nie przepustowości łącza internetowego), czy blokowanie ruchu od i do stacji, których status bezpieczeństwa uległ obniżeniu (automatyczna izolacja stacji celem zatrzymania rozprzestrzeniania się wykrytego zagrożenia).

Antywirus nowej generacji, jakim jest **Sophos Intercept X**, dodatkowo wzbogacony o **EDR**, zapewnia klientowi bezpieczeństwo stacji końcowych i serwerów w przypadku, gdyby jakieś zagrożenia przedostały się przez Firewall brzegowy. Mechanizmy głębokiego uczenia (**Deep Learning**) oraz zabezpieczenia przed ransomware, dodatkowo podnoszą poziom ochrony, w pewnym stopniu eliminując negatywne skutki popełnienia błędów przez pracowników – jeśli nawet ktoś złapie się na phishing, to ewentualna utrata danych w wyniku zaszyfrowania przez ransomware, zostanie powstrzymana przez odpowiedni moduł. Mechanizm **EDR** pomoże w analizie przyczyn i skutków ataku oraz umożliwi sprawdzenie pozostałych elementów infrastruktury, czy nie zostały również nim dotknięte lub czy zagrożenie nie zagnieździło się w ich zasobach, czekając na detonację.

Zaproponowane rozwiązania

- brzegowy UTM Sophos XG 210 + pakiet subskrypcji FullGuard do ochrony sieci, użytkowników, poczty firmowej i zbudowania centralnie zarządzanej sieci WiFi
- punkty dostępowe Sophos APX 320
- Sophos SD-RED 20 dla zdalnej lokalizacji
- Sophos Intercept X Advanced z EDR dla stacji końcowych i serwerów do wdrożenia spójnej koncepcji bezpieczeństwa, zgodnej z ideą Synchronized Security

„Sophos dostarcza kompletny system bezpieczeństwa, który cechuje się prostym wdrożeniem, intuicyjną konfiguracją, bezproblemowym działaniem oraz najwyższą skutecznością w zapewnieniu ochrony dla kluczowych elementów infrastruktury IT w firmach od pojedynczych do kilkunastu tysięcy pracowników. Potwierdzają to bardzo wysokie oceny uzyskiwane w testach porównawczych oraz opinie klientów, dla których kluczową przewagą nad konkurencją jest wymiana informacji pomiędzy elementami systemu - filozofia Synchronized Security."

Sophos Platinum Partner

Sun Capital sp. z o.o.
ul. Ołtaszyńska 92c/6
53-034 Wrocław

https://suncapital.pl

tel.: +48 71 360 81 00
email: sprzedaz@suncapital.pl

Sophos XG Firewall to cała paleta rozwiązań sprzętowych - od małych, w obudowach typu desktop, po duże, do montażu w szafach serwerowych, zarówno o rozmiarze 1U, jak i 2U.

Dzięki tak bogatej ofercie, urządzenia te nadają się zarówno dla użytkowników domowych, małych i średnich firm, jak i dużych korporacji. Dodatkowa opcja zapewnienia wysokiej dostępności i klastrowania sprawia, że każda firma znajdzie bezpieczne rozwiązanie brzegowe dostosowane do swoich potrzeb.

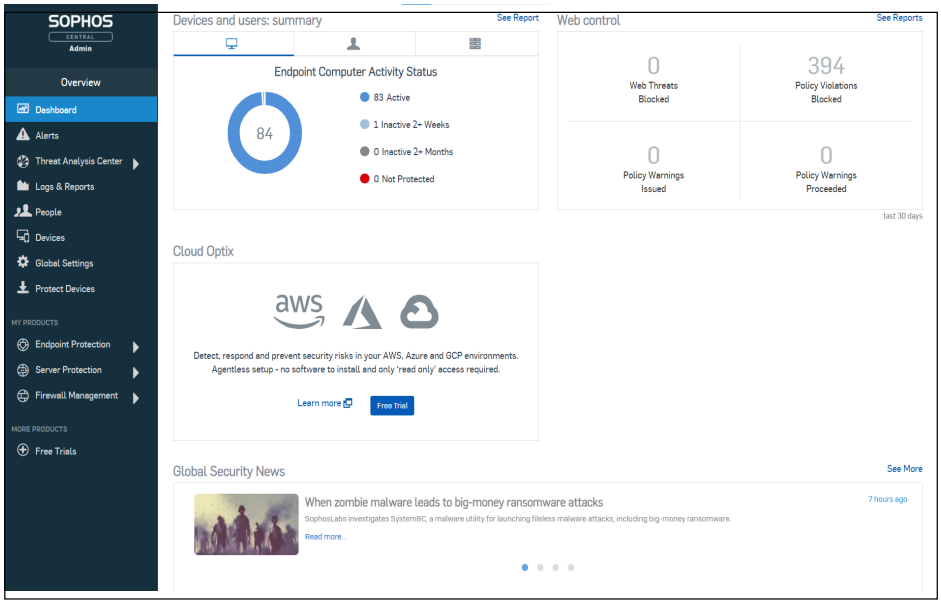
*Mając na uwadze poruszaną tematykę bezpieczeństwa IT oraz respektując życzenie klienta, nie podajemy danych firmy, której dotyczy ten przypadek.

Dodatkowe potrzeby klienta

W późniejszym czasie okazało się, że dodatkowym atutem oferty **Sophos** jest możliwość podłączenia zdalnej lokalizacji bezpiecznym, zarządzanym z konsoli administracyjnej Firewalla, tunelem IPSec. Wykorzystano w tym celu urządzenie **Sophos SD-RED 20**, które poza prostą konfiguracją i wysoką przepustowością, nie wymaga odrębnej, podlegającej odnowieniu subskrypcji, gdyż korzysta z modułów aktywowanych na Firewallu, do którego jest podłączone.

Ogólne wrażenia

Tym, co klient najbardziej ceni sobie w zaproponowanym i wdrożonym rozwiązaniu, jest prostota w implementacji, konfiguracji i zarządzaniu. Po wstępnym skonfigurowaniu nowych elementów, codzienna obsługa nie nastręcza wielu problemów, a możliwość obsługiwania wszystkich rozwiązań **Sophos** z jednej, centralnej konsoli administracyjnej dostępnej przez przeglądarkę internetową skraca czas niezbędny do sprawdzenia stanu ochrony infrastruktury firmowej. Brak dodatkowego serwera zarządzającego dla antywirusa w lokalnej sieci to z jednej strony oszczędność zasobów, z drugiej zaś realne korzyści finansowe, ponieważ nie zachodzi konieczność przeprowadzania czynności obsługowych na dodatkowej maszynie. Antywirus w ramach **Sophos Central** to także niewymagająca dodatkowych konfiguracji łączność pomiędzy stacjami końcowymi będącymi poza firmą i serwerem zarządzającym – komunikacja nawiązywana jest z każdego miejsca, gdzie stacja jest podłączona do Internetu, dzięki czemu mamy pewność, że **Sophos** na komputerach jest zaktualizowany, a status zgłoszony do konsoli przedstawia stan aktualny – bez znaczenia, czy pracownik jest w firmie, czy poza nią.



Dalsze plany

W przyszłości klient rozważa dodanie drugiego urządzenia **Sophos XG 210**, do konfiguracji wysokiej dostępności (active-passive) oraz wdrożenie zabezpieczenia dla urządzeń mobilnych – nie tylko smartfonów i tabletów, ale także kilkunastu komputerów z systemem Windows 10, które wraz z mobilnymi handlowcami przemieszczają się po całej Polsce. **Sophos Mobile**, jako jeden z elementów zestawu produktów **Sophos Central**, nie wymaga żadnej infrastruktury zarządzającej po stronie sieci klienta, zatem wdrożenie takiego rozwiązania ogranicza się do instalacji agentów na urządzeniach oraz konfiguracji produktu w webowym interfejsie administracyjnym **Sophos Central**.

Sophos Platinum Partner

Sun Capital sp. z o.o.
ul. Ołtaszyńska 92c/6
53-034 Wrocław

https://suncapital.pl

tel.: +48 71 360 81 00
email: sprzedaz@suncapital.pl