Sophos XG Firewall na QNAP Turbo NAS – UTM, centrum multimedialne i dysk sieciowy w jednym

Czy zastanawialiście się kiedyś jak w tani, a jednocześnie skuteczny sposób zabezpieczyć własną sieć komputerową przed zagrożeniami zewnętrznymi? Czy borykacie się z problemem niewystarczającej ilości miejsca do przechowywania danych oraz trudnościami przy przydzielaniu dostępu do kluczowych informacji w firmie? Czy będąc użytkownikiem domowym, chcielibyście wykorzystać jedno urządzenie do zrealizowania tych wszystkich funkcji, dodatkowo mając możliwość podłączenia go pod telewizor, czyniąc z niego centrum multimediów, bez konieczności ponoszenia dodatkowych kosztów za licencję zabezpieczenia na brzegu sieci? Mamy dla Was doskonałe rozwiązanie - QNAP TurboNAS z Sophos XG Firewall, dostępnym w wersji komercyjnej, jak też całkowicie darmowej dla użytkowników domowych.

QNAP – potencjał tkwi w wirtualizacji

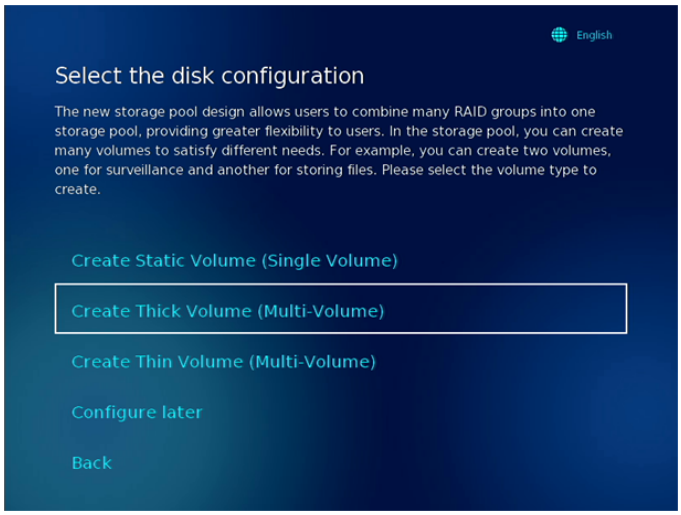
QNAP to tajwański producent pamięci sieciowych dla użytkowników domowych, małych i średnich firm, a także dużych korporacji, wymagających najlepszych i bezawaryjnych rozwiązań. W ofercie producenta znaleźć można całą gamę produktów – od małych, jedno kieszeniowych obudów typu desktop na dyski 2,5/3,5 cala, wyposażonych w jeden port Ethernet, dedykowanych do wykorzystania w domu, przez średniej wielkości 4-dyskowe NASy z 4 portami Ethernet dla małych i średnich firm, po duże, wyposażone w nawet 24 kieszenie obudowy do montażu w szafie serwerowej, posiadające porty 10 GbE (SFP+), obsługujące dyski SAS. Oferta producenta posiada także jeden ważny wyróżnik na tle konkurencji - NASy działające pod kontrolą systemu QTS 4.2 wspierają wirtualizację, dzięki której mamy możliwość skonfigurowania w obrębie jednego urządzenia większej ilości maszyn wirtualnych. Dzięki tej funkcji możliwe jest wykorzystanie takiego dysku sieciowego jako rozwiązania klasy UTM (Unified Threat Management) do zabezpieczenia sieci w domu lub firmie.

Sophos XG Firewall – UTM do zadań specjalnych

Rolę brzegowego zabezpieczenia sieci, organizacji routingu, obsługi DNS oraz kontroli i zarządzania ruchem sieciowym, pełnić będzie Sophos XG Firewall. To najmłodsze rozwiązanie klasy UTM w ofercie producenta z Abingdon, charakteryzuje się niedużymi wymaganiami sprzętowymi, obsługą różnych wariantów routingu sieciowego oraz wbudowanym serwerem VPN, wspierającym kilka kluczowych standardów połączeń. Produkt wyposażony jest też w silnik antywirusowy (Sophos) z opcją dual scan (Avira), do skanowania połączeń, narzędzia do kształtowania pasma, zabezpieczenie dla serwerów pocztowych i web serwerów, zarządzanie sieciami bezprzewodowymi i wiele innych. Sophos XG Firewall w wersji komercyjnej licencjonowany jest na wykorzystywaną ilość rdzeni procesora oraz obsługiwanej pamięci RAM. Dla użytkowników domowych brytyjski producent przygotował specjalną, darmową licencję, ograniczoną do maksymalnie 4 rdzeni procesora i 6 GB pamięci operacyjnej RAM, co jest ilością więcej niż wystarczającą dla potrzeb niewielkich sieci w domu.

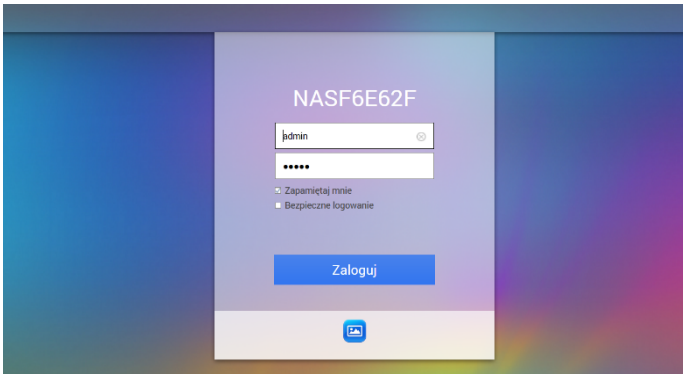
3… 2… 1… Start – przygotowanie środowiska

Naszą przygodę z zaadaptowaniem QNAP TS-253A do roli UTMa, rozpoczynamy od podłączenia urządzenia do monitora (przez złącze HDMI) oraz sieci LAN, na porcie 2 (najlepiej za routerem z obsługą DHCP). Po włączeniu zasilania i odczekaniu kilku chwil, możemy rozpocząć instalację niezbędnych komponentów, klikając “Smart Start Installation Guide”. W pierwszym kroku możemy zdecydować czy już na tym etapie chcemy zainstalować funkcje multimedialne. Pominięcie tego procesu spowoduje, że wszystkie wymagane do dalszej pracy aplikacje będziemy musieli doinstalować z poziomu konsoli zarządzania urządzeniem. Kolejny krok, to ustawienie trybu pracy dysku twardego. Do wyboru mamy kilka wariantów. My, wykorzystując jeden dysk wewnętrzny, rezygnujemy z konfiguracji RAID, pozostawiając Single Volume (opcja 1).



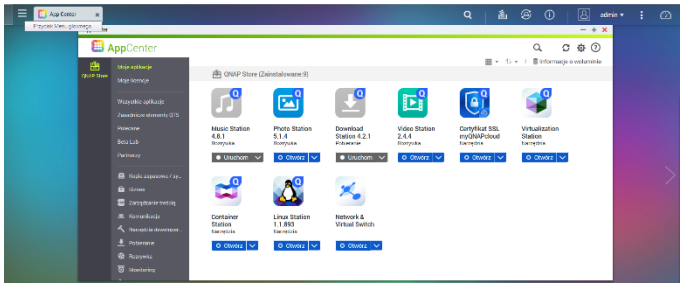
Ustawienia wprowadzone w tym miejscu będzie można później zmienić w konsoli zarządzającej urządzenia, warto jednak mieć na uwadze, że aby dodać nowy dysk pracujący w RAID, konieczne będzie jego sformatowanie. Następne ustawienia (szyfrowanie dysku, RAID, miejsce na snapshoty) możemy pozostawić bez wprowadzania zmian. Na kolejnym ekranie zobaczymy podsumowanie wcześniejszych ustawień. Po zatwierdzeniu, dysk twardy zostanie przygotowany do pracy z urządzeniem QNAP. Może to potrwać kilka minut, a urządzenie może się w międzyczasie zrestartować. Po zakończeniu operacji, na ekranie podłączonego monitora powinniśmy zobaczyć informację, że nie mamy zainstalowanego HD Station, chyba że wcześniej wyraziliśmy chęć zainstalowania funkcji multimedialnych - na tym etapie nie musimy się tym przejmować. To, co dla nas ważne, to adres IP urządzenia QNAP. Możemy go w prosty sposób znaleźć na routerze z funkcją DHCP, wśród przydzielonych adresów.

Znając adres IP urządzenia (załóżmy że jest to 192.168.2.100) oraz posiadając komputer podłączony do tej samej sieci co nasz QNAP, przechodzimy do strony administracji urządzeniem, wpisując adres http://192.168.2.100 (lub w wersji bezpiecznej https://192.168.2.100). Logujemy się korzystając ze standardowej nazwy użytkownika (admin) oraz hasła (admin).



W pierwszym kroku sprawdźmy, czy korzystamy z najnowszej wersji oprogramowania. W tym celu przechodzimy do Panelu sterowania -> Aktualizacja firmwaru. Jeśli po kliknięciu przycisku “Sprawdź aktualizacje” pojawi się nam nowa wersja, zainstalujmy ją, jeśli nie, możemy zamknąć to okno.

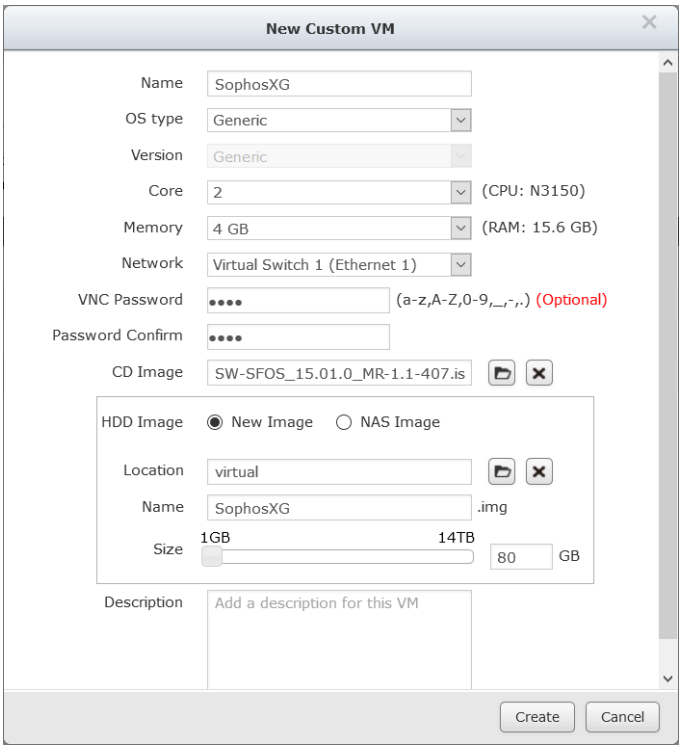
Mając zainstalowaną najnowszą wersję QTS, musimy skonfigurować wirtualny przełącznik. Dzięki niemu będziemy mogli podłączyć urządzenie QNAP do sieci lokalnej Sophos XG Firewall, odseparowując je tym samym od internetu. Pozwoli nam to na zachowanie pełnej kontroli oraz zabezpieczenie dostępu do urządzenia z zewnątrz. Ponieważ w ramach urządzenia dostępna jest wirtualizacja, wirtualny przełącznik będziemy mogli wykorzystać także do podłączenia do sieci innych wirtualnych maszyn. Konfigurację przełącznika sieciowego uruchamiamy w “Virtualization Station”. Jeśli wcześniej ta usługa nie była zainstalowana, można ją w prosty sposób dodać, wyświetlając centrum aplikacji (App Center), wyszukując potrzebną nam aplikację i klikając na niej Zainstaluj.



Proces jest całkowicie automatyczny, a po jego zakończeniu na pulpicie powinna pojawić się nowa ikona, uruchamiająca dodaną aplikację. Przejdźmy więc do niej (Virtualization Station) i rozpocznijmy konfigurację sieci (Network Settings). Dodajmy dwa wirtualne przełączniki (Add Virtual Switch), pracujące w trybie Bridge, każdy działający dla innej fizycznej karty sieciowej. Zapewni nam to łączność pomiędzy NASem, maszyną wirtualną (Sophos XG Firewall) oraz naszą siecią lokalną, to której podłączone jest urządzenie oraz komputer wykorzystywany do konfiguracji środowiska.

Po wstępnej konfiguracji sieci, możemy dodać maszynę wirtualną. Pozostańmy zatem w Virtualization Station i wybierzmy z menu “Create VM”. Zalecamy utworzenie niestandardowej maszyny wirtualnej (Create Custom VM), w której będziemy mieli więcej możliwości konfiguracji, pozwalających nam dopasować wydajność Sophos XG Firewall do naszych potrzeb oraz możliwości urządzenia QNAP. Przy założeniu, że nasz NAS wyposażony jest w 8GB pamięci RAM, dla maszyny wirtualnej możemy śmiało przeznaczyć 4GB RAMu oraz

2 rdzenie procesora (mamy procesor 4-rdzeniowy). Taka konfiguracja powinna zapewnić bezproblemową pracę dla max. 50 urządzeń podłączonych do sieci lokalnej. Jeśli te parametry okażą się niewystarczające, zawsze będzie można zmienić je później. Aby wprowadzić zmiany w ustawieniach maszyny wirtualnej, konieczne jest jej wyłączenie. Na tym etapie musimy także mieć pobrany obraz płyty instalacyjnej (Software Appliance) oraz musimy skopiować go do urządzenia NAS. Obraz ten wskazujemy przy tworzeniu maszyny wirtualnej w CD Image. HDD Image pozwala nam natomiast ustawić lokalizację, nazwę oraz rozmiar dysku maszyny wirtualnej. Wszystkie parametry można ustawić jak na poniższym zrzucie ekranu, zachowując ścieżki zgodne z występującymi na urządzeniu.



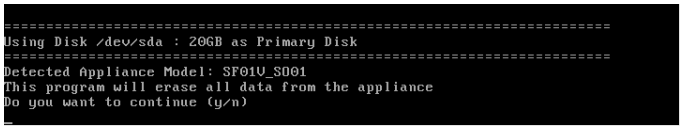
W kolejnym kroku musimy jeszcze dokonać edycji parametrów utworzonej wcześniej maszyny wirtualnej. W tym celu przechodzimy do listy maszyn wirtualnych i klikamy na nazwie maszyny utworzonej przed chwilą. Po załadowaniu informacji o urządzeniu, w prawym górnym rogu klikamy przycisk "Virtual Machine Settings". Przycisk ten jest aktywny i umożliwia wprowadzanie dodatkowej konfiguracji wyłącznie kiedy maszyna wirtualna jest wyłączona. W ustawieniach zmieniamy:

- Boot Options - First Boot Device na CDROM,
- Hard Disk - Controler na SATA,
- Autostart - Enable.

Dodatkowo musimy wyposażyć naszą maszynę wirtualną w jeszcze jedną kartę sieciową. Możemy ją dodać, klikając przycisk "Add Device", znajdujący się u góry strony. Nowe urządzenie jest typu Network, Mode: Virtual Switch 2. Reszta parametrów może pozostać bez zmian. W tym momencie mamy gotową maszynę wirtualną, na której musimy zainstalować Sophos XG Firewall.

Instalacja Sophos XG Firewall

W tym celu musimy uruchomić maszynę (wybierając ją z listy i klikając przycisk "Start"). Następnie klikamy przycisk "Console", który w nowym oknie przeglądarki wyświetla nam konsolę naszej maszyny wirtualnej. Dostęp do konsoli możemy mieć także za pośrednictwem klienta VNC (np. TightVNC), zestawiając połączenie do adresu IP urządzenia QNAP, na porcie wymienionym we właściwościach maszyny wirtualnej. Domyślnie, jeśli jest to pierwsza działająca maszyna wirtualna, port, na którym możliwe jest połączenie VNC to 5900. Uruchomienie maszyny wirtualnej z bootowalnego medium, jakim jest obraz Sophos XG Firewall Software Appliance, spowoduje rozpoczęcie procedury instalacji UTMa, w tym założenie wirtualnego dysku twardego lub sformatowanie dysku już istniejącego. Aby rozpocząć instalację, należy wcisnąć przycisk 'y' i zatwierdzić wybór naciskając Enter, kiedy na ekranie pojawi się stosowny komunikat.

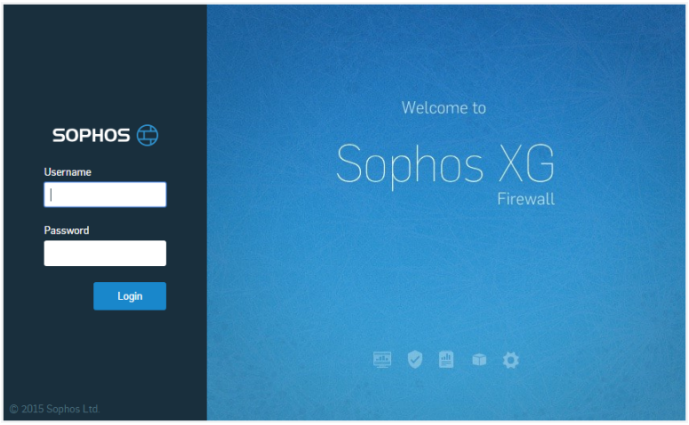


Po kilku minutach, zostaniemy poproszeni o usunięcie płyty instalacyjnej oraz ponowne uruchomienie maszyny wirtualnej. Mając na uwadze, że zmian w maszynie wirtualnej możemy dokonać wyłącznie, kiedy jest ona wyłączona, musimy nieznacznie zmodyfikować procedurę zakończenia tego etapu instalacji. Kiedy w konsoli wyświetli się komunikat proszący o potwierdzenie restartu maszyny wirtualnej,

nie klikamy 'y', tylko w zarządzaniu wirtualizacją urządzenia QNAP (Virtualization Station) zatrzymujemy maszynę wirtualną (klikając przycisk Power i wybierając Force Shutdown). W kolejnym kroku musimy zmienić priorytet bootowania, aby start systemu odbywał się z lokalnego dysku twardego. W tym celu wyświetlamy ustawienia maszyny wirtualnej (Virtual Machine Settings)

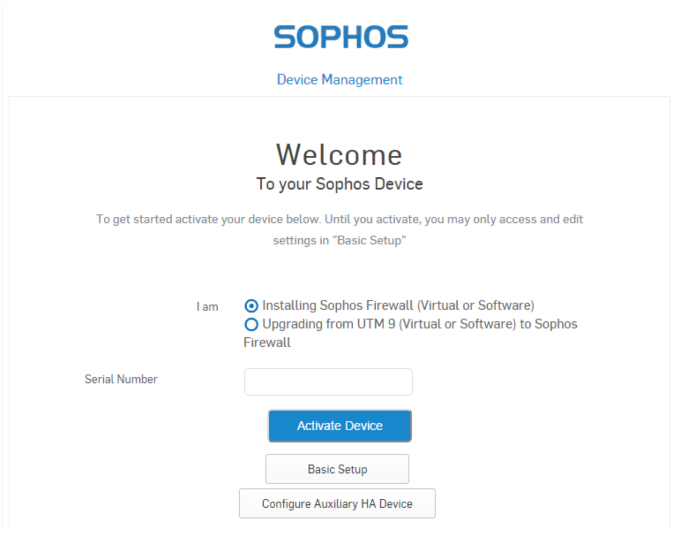
i w sekcji Boot Options ustawiamy First Boot Device na HDD. Po dokonaniu tej zmiany możemy uruchomić maszynę wirtualną. W konsoli powinniśmy zobaczyć postęp instalacji SFOS (Sophos Firewall Operating System), po którym zostaniemy poproszeni o podanie hasła. Domyślne hasło, podobnie jak nazwa domyślnego administratora, to admin. Na kolejnym ekranie musimy zatwierdzić warunki umowy licencyjnej (naciskając przycisk A). W menu mamy kilka pozycji, które możemy przeglądać i modyfikować - dla nas, na obecnym etapie ważne będzie, aby dostać się do interfejsu administracyjnego urządzenia z poziomu przeglądarki internetowej. Aby zobaczyć jaki adres IP ma nasze urządzenie, przechodzimy do menu 1 (Network Configuration), a dalej do Interface Configuration (również 1). Domyślnie, adres IP pierwszego interfejsu to 172.16.16.16. Jeśli nasza sieć lokalna korzysta z innej adresacji, to musimy zmienić ten adres na zgodny z adresacją sieci (np. 192.168.2.200). Niestety, musimy zrobić to ręcznie, gdyż na tym etapie Sophos XG Firewall nie pobiera automatycznie adresu z usługi DHCP naszego routera - ważne, aby nadany przez nas adres był wolny, niewykorzystywany w tym czasie przez inne urządzenie w sieci.

Po dokonaniu zmiany adresu, na komputerze, na którym mamy uruchomioną konsolę, w przeglądarce internetowej spróbujmy wyświetlić stronę administracji urządzeniem (nawiązując do naszego przykładu, w którym adres Sophos XG Firewall ustawiliśmy na 192.168.2.200), która powinna być dostępna na adresie https://192.168.2.200:4444. Powinniśmy zobaczyć komunikat o błędzie certyfikatu - to dobrze, ponieważ korzystamy z niezaufanego certyfikatu i taki błąd jest normalny, a wynika z tego, że nasz certyfikat wykorzystywany do zabezpieczenia połączenia z konsolą administracyjną, nie został wystawiony przez zaufany organ certyfikacji. W zależności od przeglądarki musimy wyświetlić opcje zaawansowane i otworzyć niezaufaną stronę lub też dodać wyjątek, aby uzyskać połączenie.



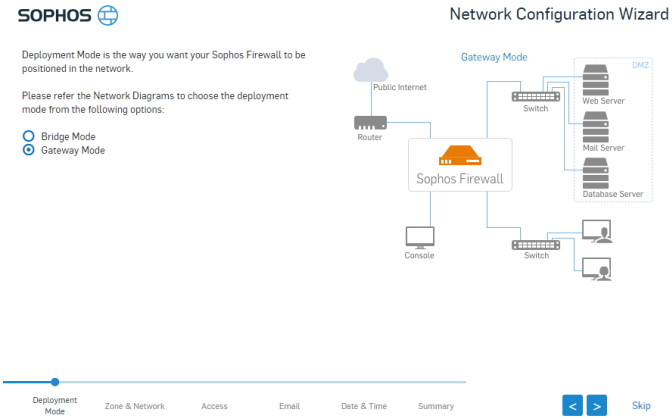
Podstawowa konfiguracja Sophos XG Firewall

Na ekranie startowym musimy zalogować się do administracji, korzystając z domyślnej nazwy użytkownika (admin) oraz hasła (admin). Przed nami kreator, w którym aktywujemy urządzenie oraz skonfigurujemy podstawowe parametry. W pierwszym kroku musimy aktywować urządzenie. W tym celu wprowadzamy numer seryjny urządzenia, który otrzymaliśmy od Sophos po wypełnieniu formularza pobierania wersji trial, home lub też po zakupie rozwiązania komercyjnego. Ważne, aby na tym etapie mieć połączenie z internetem, ponieważ wymaga tego aktywacja urządzenia.

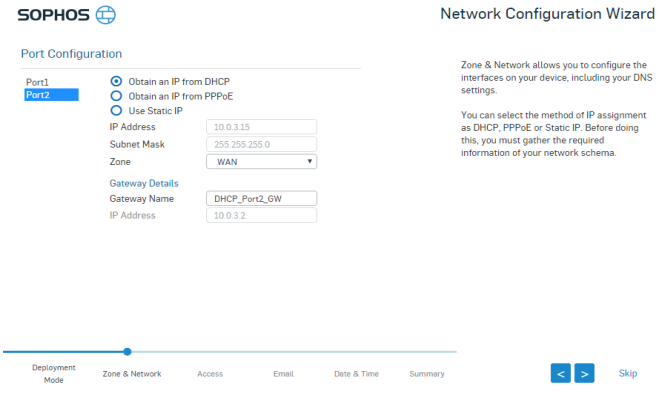


Klikając przycisk Basic Setup, mamy możliwość skonfigurowania parametrów połączenia WAN na drugim porcie wirtualnej maszyny Sophos XG Firewall. Jeśli mamy połączenie z internetem oraz wprowadziliśmy numer seryjny urządzenia, możemy kliknąć przycisk Activate Device. Poprawna aktywacja zostanie nam zakomunikowana wyświetleniem zielonego powiadomienia. Jeśli będzie coś nie tak, pojawi się czerwone powiadomienie, które w większości przypadków będzie informowało o problemach z połączeniem internetowym, choć nie zawsze. Po poprawnej aktywacji, powinniśmy zobaczyć kolejny ekran, na którym możemy zarejestrować urządzenie. Proces ten przypisuje konkretne urządzenie Sophos XG Firewall do konta w MySophos. W nowym oknie, które pojawiło się na ekranie, możemy wskazać dane konta MySophos, do którego ma zostać dołączone urządzenie lub też założyć nowe konto MySophos. Po poprawnym sparowaniu urządzenia z kontem, możemy zsynchronizować licencję (Synchronize License). Proces ten spowoduje aktywację na urządzeniu subskrypcji, przypisanych do niego w MySophos.

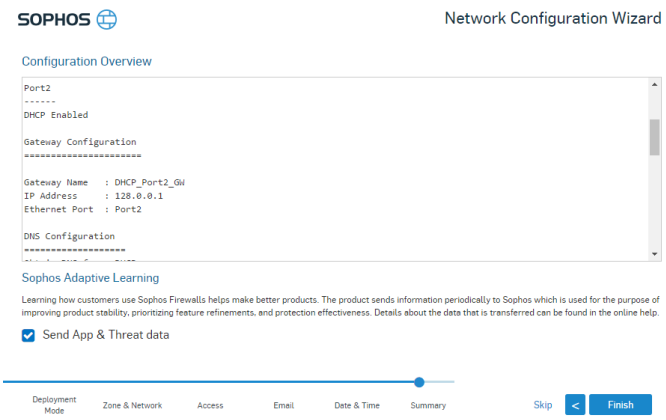
Po zakończeniu etapu wstępnego, możemy przejść do podstawowych konfiguracji. Producent po raz kolejny zadbał, aby proces konfiguracji urządzenia był jak najprostszy, w związku z czym po raz kolejny musimy przebrnąć przez kreator. Warto nadmienić, że w każdej chwili będziemy mogli pominąć wizard, klikając Skip, wiązać się to będzie z koniecznością skonfigurowania wszystkich komponentów ręcznie. Na pierwszym ekranie klikamy Start. Drugi ekran wymaga od nas dokonania wyboru trybu pracy urządzenia.



Skoro decydujemy się na uruchomienie naszego Sophos XG Firewall jako głównego urządzenia zabezpieczającego i zarządzającego siecią na bramie internetowej, to wybieramy tryb Gateway. Kolejny krok, to konfiguracja portów.



Możemy ustawić parametry na nowo lub też skorzystać z wcześniej skonfigurowanych wartości. Warto poprawnie, zgodnie z późniejszym przeznaczeniem interfejsów, ustawić odpowiednie strefy (Zone), gdyż większość konfiguracji urządzenia bazuje właśnie na połączeniach pomiędzy strefami. W następnym kroku definiujemy podstawowy serwer DNS dla naszej sieci. Na razie możemy zostać przy ustawieniach domyślnych (pobraniu adresu DNS z serwera DHCP). Ustawienia te będzie można zmienić na późniejszym etapie konfiguracji urządzenia. Następny ekran, to ustawienia zabezpieczeń sieci. Na obecnym etapie możemy włączyć ten komponent, ustawiając wszystkie polityki na None. Kolejny element, to konfiguracja serwera pocztowego. Tutaj musimy wskazać dane serwera pocztowego, konta do autoryzacji, adresu z którego oraz na który będą wysyłane maile oraz typu połączenia, aby otrzymywać na email najważniejsze komunikaty z naszego UTMa. Przedostatnim krokiem jest skonfigurowanie strefy czasowej. Zalecamy wybranie strefy Europe/Warsaw i włączenie automatycznej synchronizacji z domyślnym serwerem czasu NTP. Na ostatnim ekranie możemy znaleźć podsumowanie wcześniej wprowadzonych ustawień.

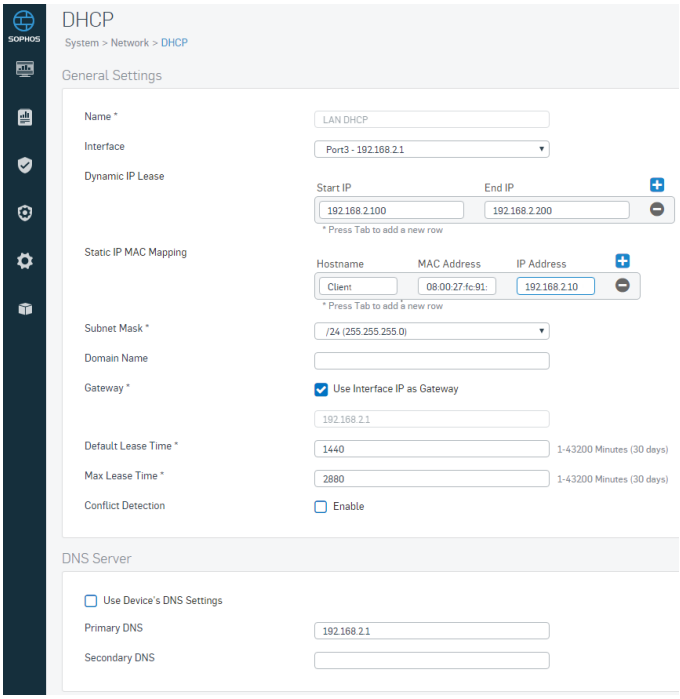


Po upewnieniu się, że wszystko jest OK, możemy zakończyć kreator, klikając przycisk Finish i zatwierdzając OK wprowadzenie zmian w wymienionych komponentach. W tym momencie Sophos XG Firewall zostanie uruchomiony ponownie i wprowadzone zostaną zmiany w konfiguracji.

Konfiguracje w administracji XG Firewall

Po zalogowaniu się do webadministracji (jeśli zmianie uległ adres IP, należy skorzystać z nowego, wywołując interfejs administracyjny po HTTPS, na porcie 4444, np. https://192.168.2.200:4444), możemy skonfigurować według naszych potrzeb wszystkie moduły wchodzące w skład Sophos XG Firewall. Zaczynamy od skonfigurowania serwera DHCP, dbającego o nadawanie adresów IP dla urządzeń znajdujących się w sieci lokalnej (w tym także samego NASa, którego będziemy niejako chować za UTMem).

Aby skonfigurować serwer DHCP, należy nadać mu nazwę, powiązać z określonym interfejsem (LAN) i ustawić zakres przydzielanych adresów (zgodnie z adresacją interfejsu). Konieczne jest także ustawienie maski podsieci, bramy domyślnej (można wybrać użycie adresu IP interfejsu sieciowego jako adresu bramy) oraz czasów dzierżawy. Konfiguracja pozostałych parametrów nie jest obowiązkowa. Na ekranie konfiguracji DHCP, warto sprawdzić jaki adres IP został przydzielony dla naszego urządzenia QNAP (IPv4 Lease Table) i od razu zrobić dla niego statyczną dzierżawę, aby nie ulegał on zmianie.

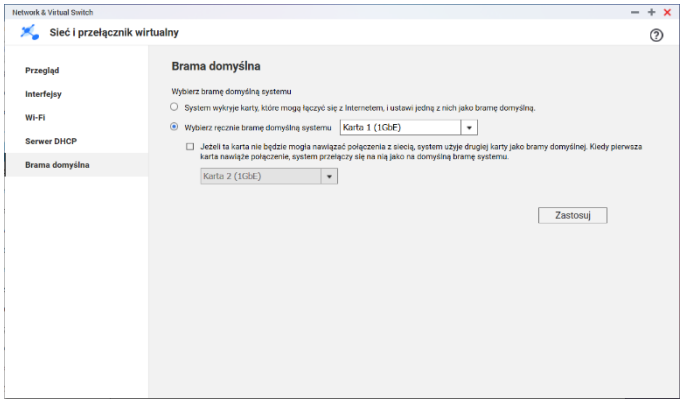


Najprawdopodobniej będzie to pierwszy adres z ustawionego przez nas zakresu. Rezerwacji można dokonać w konfiguracji serwera DHCP. Będzie nam potrzebny MAC adres urządzenia oraz jego nazwa. Obydwie te wartości znajdziemy w tabeli dzierżawy. Mając je zapisane (skopiowane), możemy kliknąć na utworzonym wcześniej serwerze DHCP dla LAN i w „Static IP MAC Mapping" możemy dodać dzierżawę. Statyczny adres, przydzielony dla urządzenia, musi być poza zakresem ustawionym dla dynamicznej adresacji.

Kolejny element, który w przyszłości będziemy konfigurować, to reguły ruchu. Na obecnym etapie wystarczy nam jedna, utworzona automatycznie, umożliwiającą połączenie komputerów z sieci lokalnej do internetu. Dobrze jest także już teraz zmienić domyślne hasło administratora (w System -> Administration -> Device Access -> Default Admin Password Settings). To oczywiście tylko podstawowe elementy, które należy sprawdzić i skonfigurować – wszystkie inne ustawienia, w tym polisy bezpieczeństwa, niestandardowe przekierowania portów czy dodatkowe reguły ruchu powinny zostać skonfigurowane z uwzględnieniem zasady – mniej otwartego dostępu, znaczy bezpieczniej – jeśli czegoś nie jesteśmy pewni, nie zmniejszajmy naszego bezpieczeństwa, otwierając niepotrzebnie dostęp do naszej sieci i pracujących w niej urządzeń.

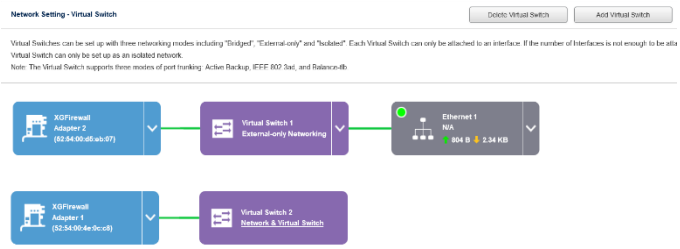
QNAP w LANie za Sophos XG Firewall

Ostatni element, który należy skonfigurować, aby ukryć urządzenie QNAP i wszystkie działające na nim usługi za NATem, czyli za naszym UTMem Sophos XG Firewall, jest zmiana konfiguracji sieci w wirtualnym przełączniku. Tym razem do wirtualnego przełącznika dostajemy się w zarządzaniu siecią urządzenia QNAP (nie z poziomu Virtualization Station), przechodząc do Panelu Sterowania -> Sieć i dalej klikając w link „Network & Virtual Switch". W nowym oknie wybieramy sekcję „Brama domyślna" i ustawiamy jako domyślną bramę, interfejs sieciowy, który w Sophos XG Firewall jest interfejsem LAN (Karta 1).



Teraz przechodzimy do Virtualization Station -> Network Settings i zmieniamy konfigurację połączeń. Virtual Switch 1, powiązany z drugim portem fizycznym urządzenia QNAP oraz siecią WAN w Sophos XG Firewall, zmieniamy na tryb pracy „External-only". Drugi switch zostawiamy w trybie „Bridged". Takie ustawienie spowoduje, że pierwszy przełącznik będzie pracował wyłącznie w trybie dostępu do internetu na drugim

porcie fizycznym urządzenia (do tego portu podłączamy kabel internetowy), z którym połączony jest interfejs WAN Sophos XG Firewall, ale nie jest połączone urządzenie QNAP – uzyskujemy w ten sposób separację usług działających na NASie od internetu. Drugi przełącznik natomiast pracuje w trybie Bridge, czyli współdzieli pierwszy port urządzenia pomiędzy QNAP, maszynę wirtualną Sophos XG Firewall oraz sieć lokalną (LAN; do tego portu możemy podłączyć dodatkowy switch lub access point, aby mieć możliwość obsługi dodatkowych urządzeń przewodowych i bezprzewodowych.



W naszym środowisku, jako switch dla sieci lokalnej oraz punkt dostępowy dla sieci bezprzewodowej zastosowaliśmy router MikroTik Routerboard RB2011UiAS-2HnD-IN, pracujący w trybie Bridge. Router ten posiada 2 anteny o bardzo dobrym pokryciu sygnałem (2,4GHz) oraz wbudowany, dziesięcioportowy switch (5 x 1Gbps i 5 x 100 Mbps). Można zastosować także dowolny switch bez obsługi sieci bezprzewodowej (będzie tańszy) i wykorzystać jeden z dostępnych w ofercie Sophos Access Pointów. Przewagą zastosowania punktu dostępowego Sophos, nad innym urządzeniem do obsługi sieci bezprzewodowej, jest możliwość zarządzania wszystkimi AP Sophos z konsoli administracyjnej Sophos XG Firewall, bez konieczności logowania się do innej konsoli, aby zmienić parametry pracy sieci WiFi.

Co dalej? Czy warto?

Teraz, kiedy mamy skonfigurowane już całe środowisko, możemy zrezygnować z korzystania z innego routera na brzegu sieci i podłączyć bezpośrednio internet do urządzenia QNAP (prosto z gniazdka lub też przez modem dla połączeń PPPoE). W zależności od wymagań naszego dostawcy usług internetowych, może być konieczne maskowanie adresu fizycznego interfejsu WAN w Sophos XG Firewall lub też podanie firmie dostarczającej nam internet, nowego adresu MAC naszego urządzenia brzegowego. Tak zbudowana i zabezpieczona sieć, oparta na urządzeniu QNAP TurboNAS oraz wykorzystująca jako brzegowy UTM Sophos XG Firewall, pozwoli nam na bezpieczne korzystanie z internetu na wszystkich urządzeniach podłączonych do sieci lokalnej. Dodatkowo dostaniemy możliwość sterowania dostępem do usług działających na urządzeniu QNAP z sieci lokalnej oraz internetu. QNAP TurboNAS to także miejsce do przechowywania danych, którego ilość zależy wyłącznie od naszych preferencji i wielkości zastosowanych dysków twardych, a po podłączeniu urządzenia do wyświetlacza przy użyciu kabla HDMI, uzyskamy centrum multimedialne, wyposażone w szereg aplikacji, do wykorzystania na co dzień. Pamiętajmy, że wszystko to otrzymujemy w ramach jednego urządzenia, co dodatkowo wpłynie na ograniczenie zużycia energii elektrycznej.

Artykuł powstał przy współpracy FEN, autoryzowanego dystrybutora rozwiązań Sophos i QNAP w Polsce, oraz firmy SunCapital, platynowego partnera Sophos.