Katowice 27.05.2021

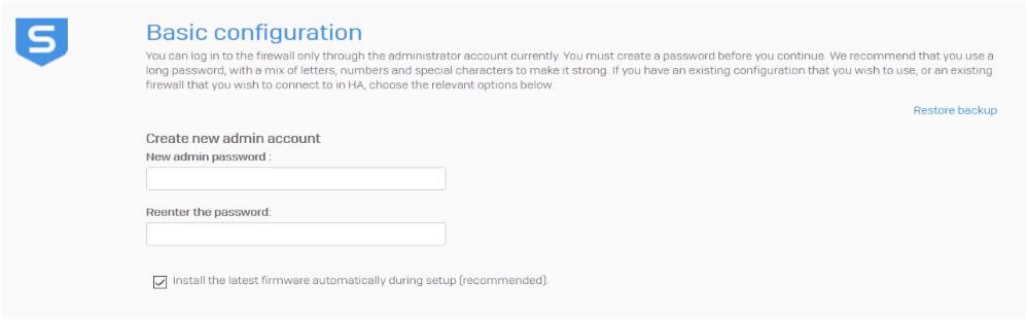
# Poradnik konfiguracji urządzenia
## Sophos XG Series firewall

### Spis treści

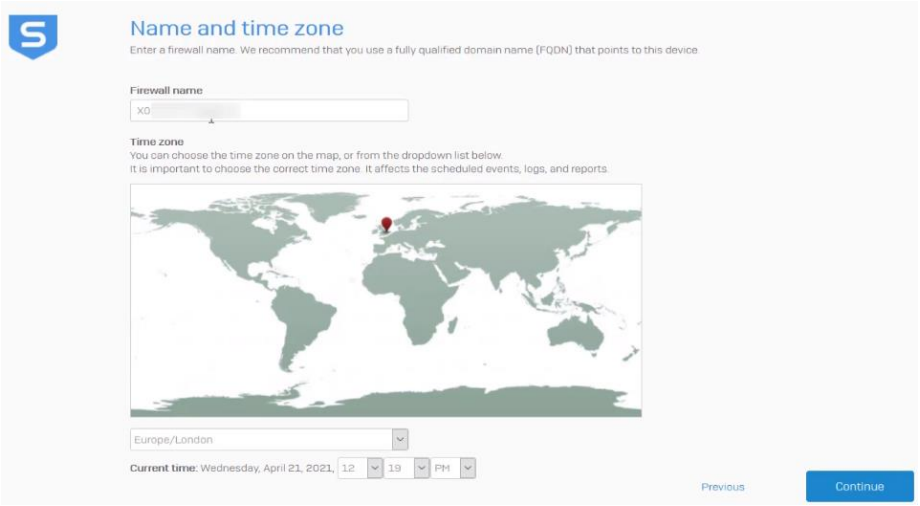
# Wstępna konfiguracja

*Aby, skonfigurować urządzenie musimy podłączyć je przez port LAN do komputera, a następnie przejść na adres: [https://172.16.16.16:4444](https://172.16.16.16:4444).*

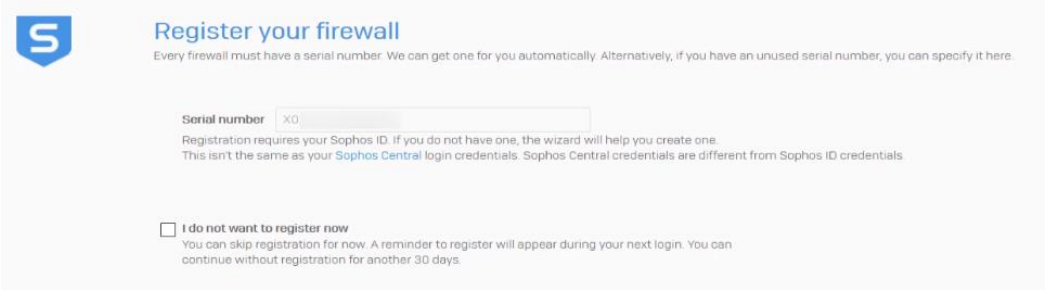
Pierwszym krokiem jest utworzenie silnego hasła dla konta administratora oraz wyrażenie zgody na pobranie najnowszego oprogramowania do urządzenia.



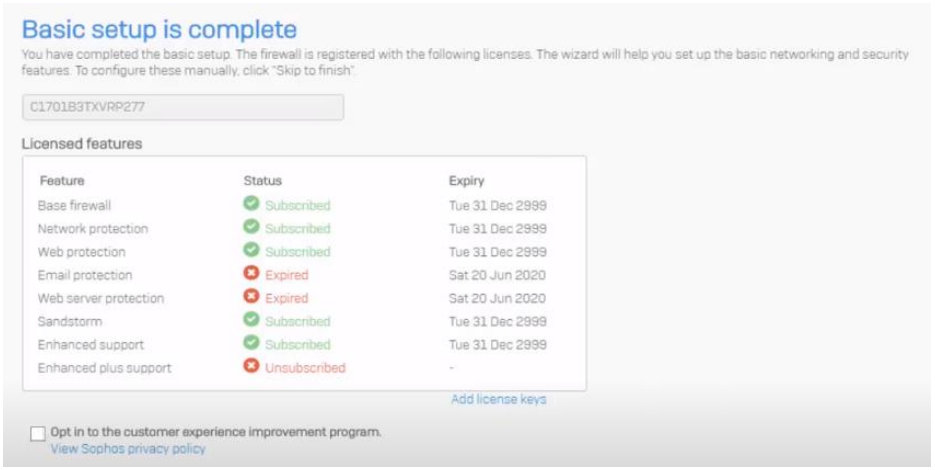

Następnie musimy wybrać nazwę urządzenia oraz strefę czasową.



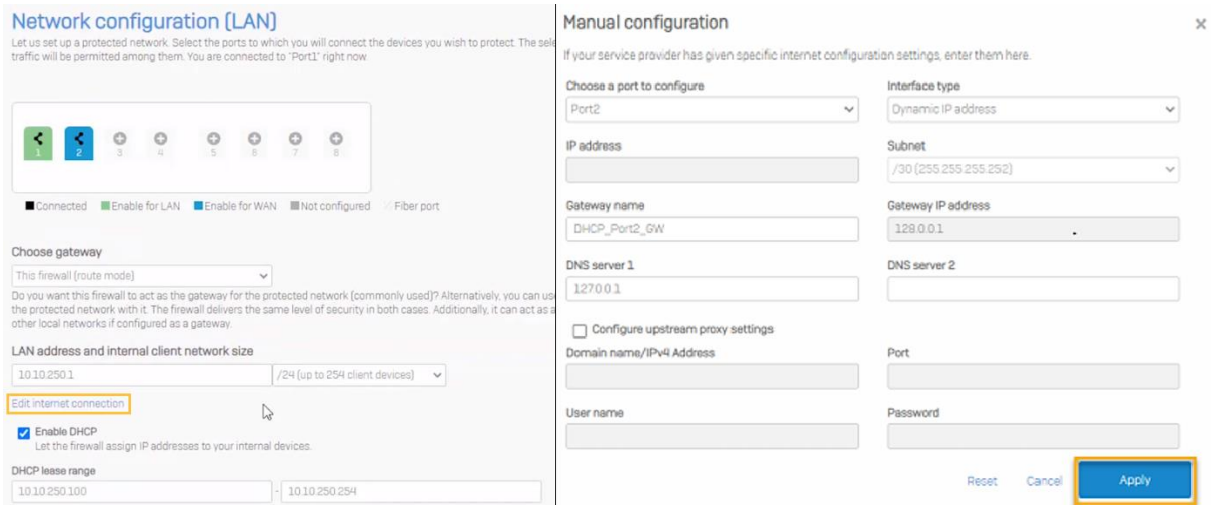

Możemy zarejestrować nasze urządzenie od razu lub zrobić to później.



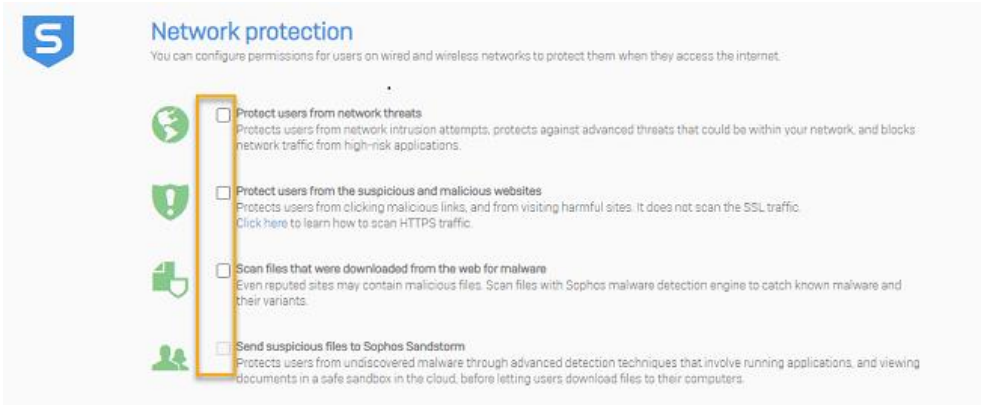
Jeśli zarejestrujemy urządzenie to zobaczymy listę usług, które obejmuje nasza licencja.



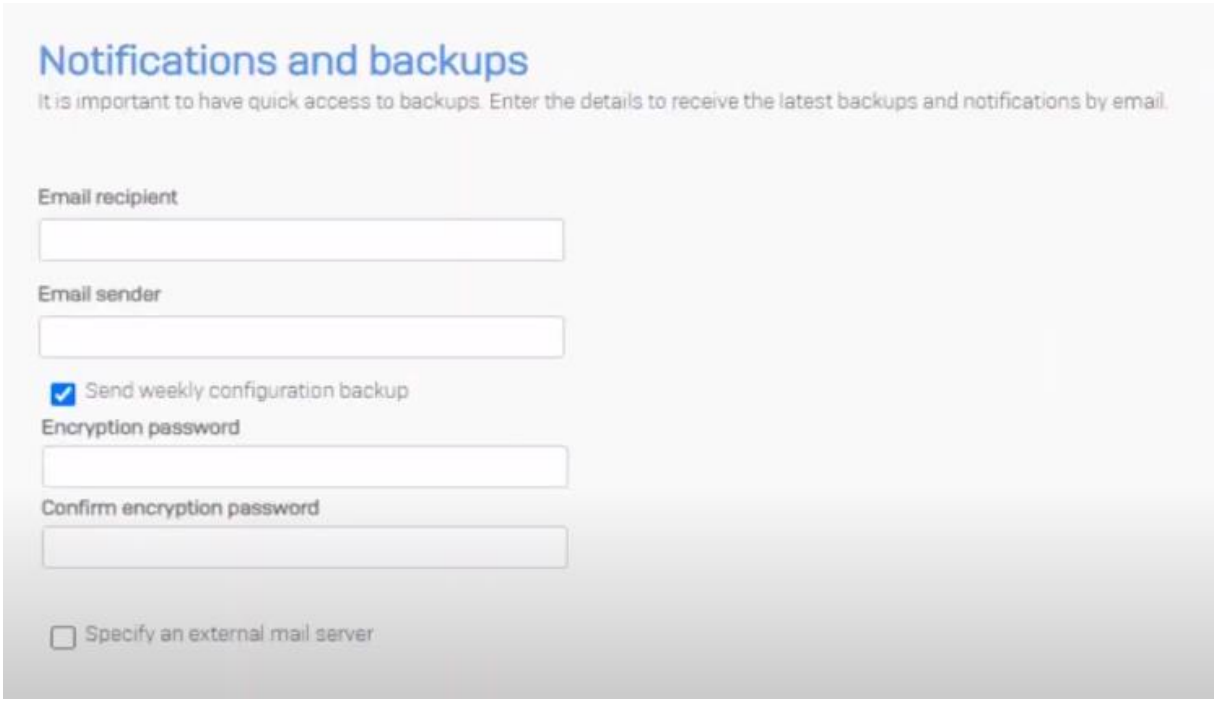

Wybieramy jakie funkcje będą pełnić porty w naszym urządzeniu oraz jaką rolę będzie pełnił nasz UTM (rolę routera lub mostu). Wybieramy adres dla sieci LAN, maskę, zakresy DHCP i edytujemy połączenie z internetem.



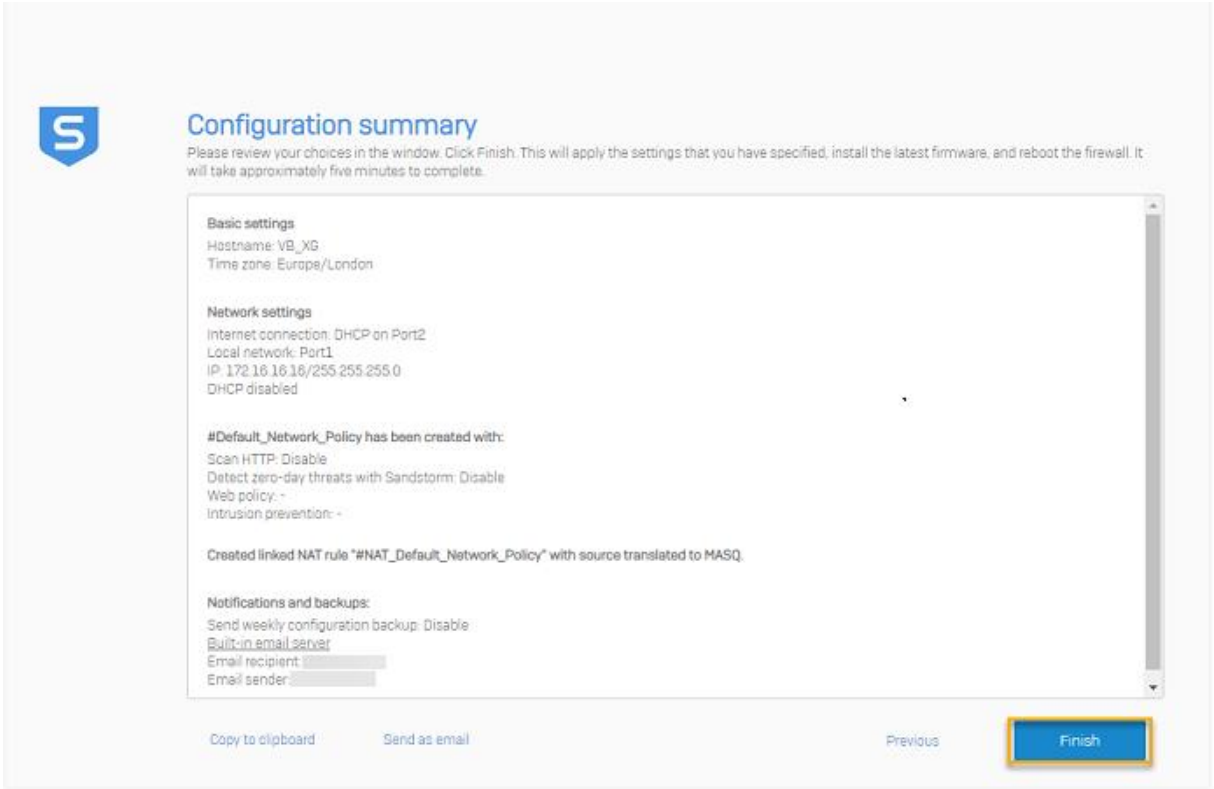

Następnym krokiem jest wybranie podstawowej ochrony jaką będzie spełniał nasz firewall.



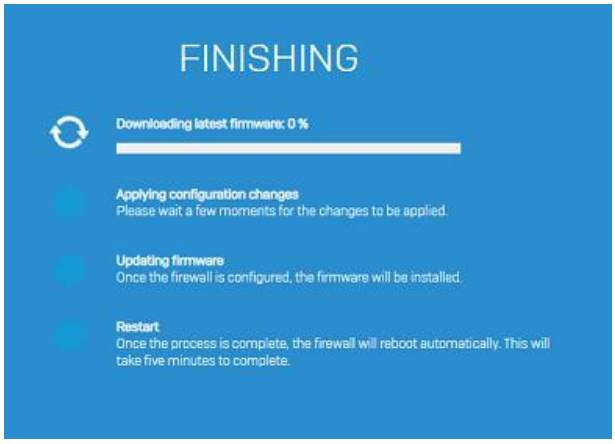
Wybieramy nadawcę oraz odbiorcę powiadomień i naszej kopii zapasowej oraz wybieramy hasło niezbędne do przywrócenia naszego backupu.




Jeśli wszystko się udało zobaczymy podsumowanie naszej konfiguracji.

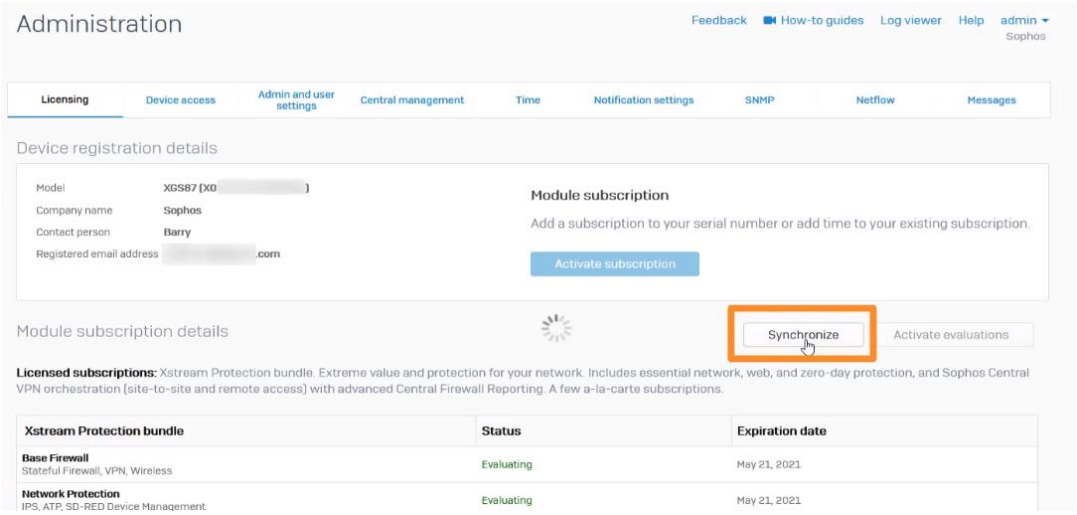


Następnie nasze urządzenie zacznie pobierać najnowsze oprogramowanie w celu aktualizacji.




Po ponownym uruchomieniu się XG firewalla oraz zalogowaniu się na konto administratora, dostaniemy się do interfejsu urządzenia i będziemy mogli utworzyć klucz zabezpieczeń do pamięci masowej.


Ostatnim krokiem wstępnej konfiguracji jest synchronizacja licencji. Przechodzimy do zakładki *Administration* → *Licensing* i wybieramy opcję *Synchronize*.

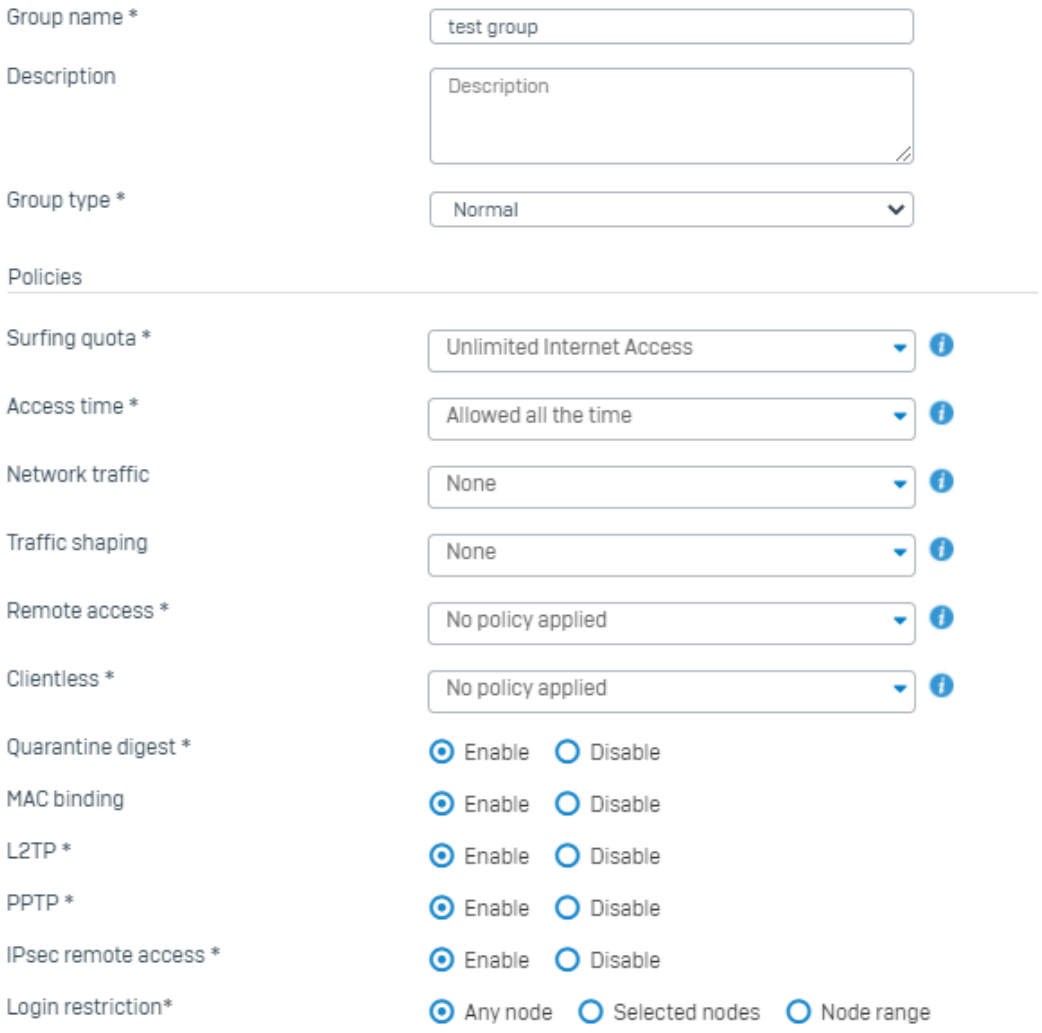


# Dodawanie użytkowników i grup

## Tworzenie grupy

Przechodzimy do zakładki *Authentication → Groups → Add i wybieramy:*

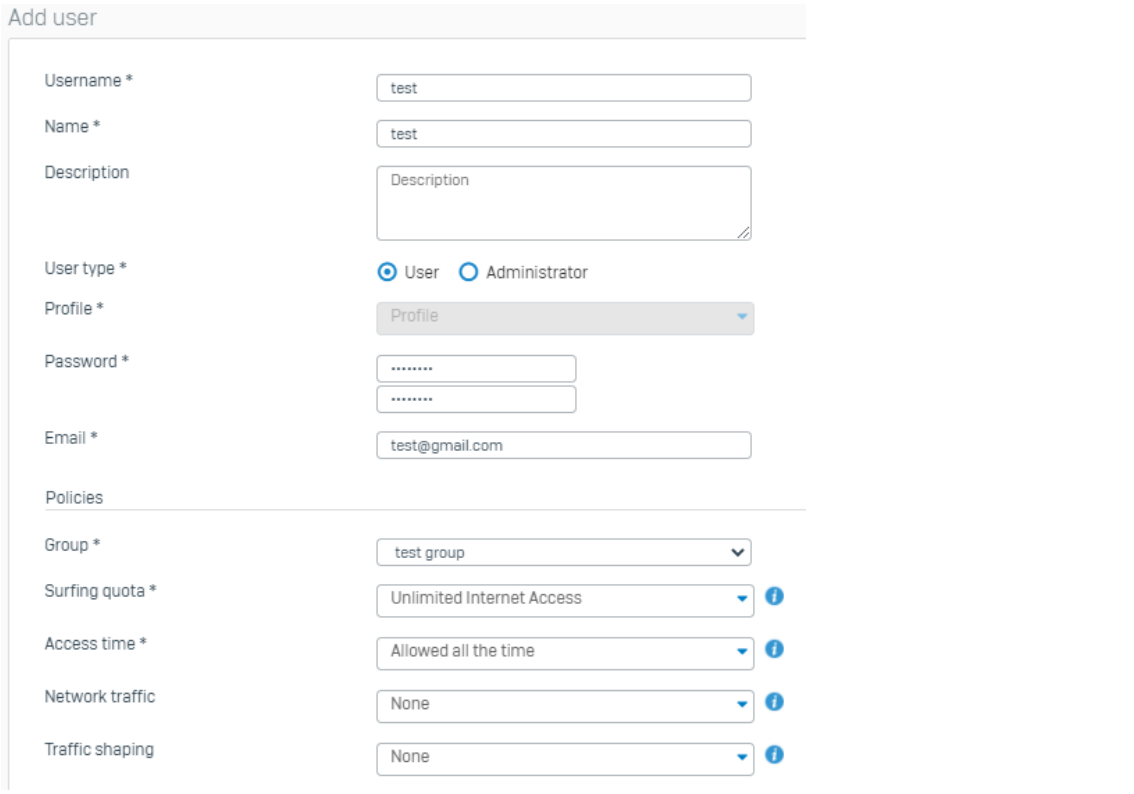
- Nazwę grupy
- Typ grupy
- Limit dostępu do internetu
- Czas dostępu
- oraz opcję związane z VPN

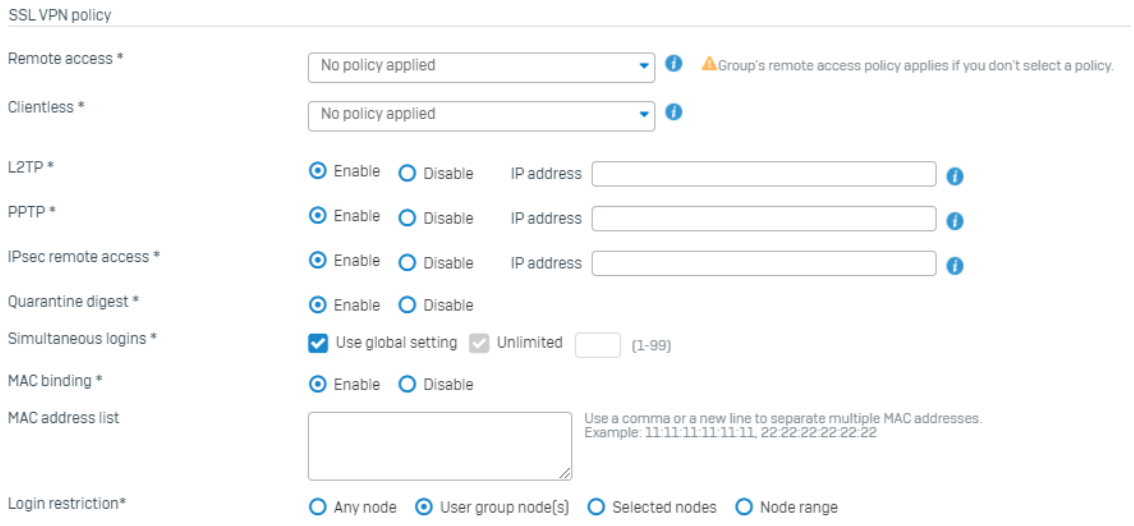


## Tworzenie użytkownika

Przechodzimy do zakładki *Authentication → Users → Add i wybieramy:*

- Nazwę użytkownika
- Nazwę
- Typ użytkownika
- Hasło
- Email
- Grupę do jakiej ma należeć
- Limit dostępu do internetu
- Czas dostępu
- oraz politykę połączenia SSL VPN

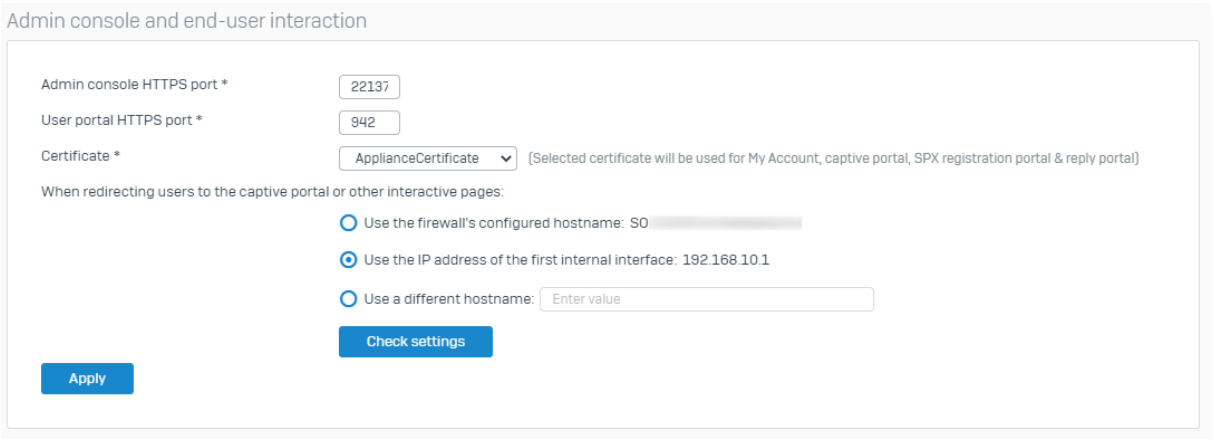


## Zmiana portu konsoli

Przechodząc do zakładki *Administrtion → Admin and user settings*.

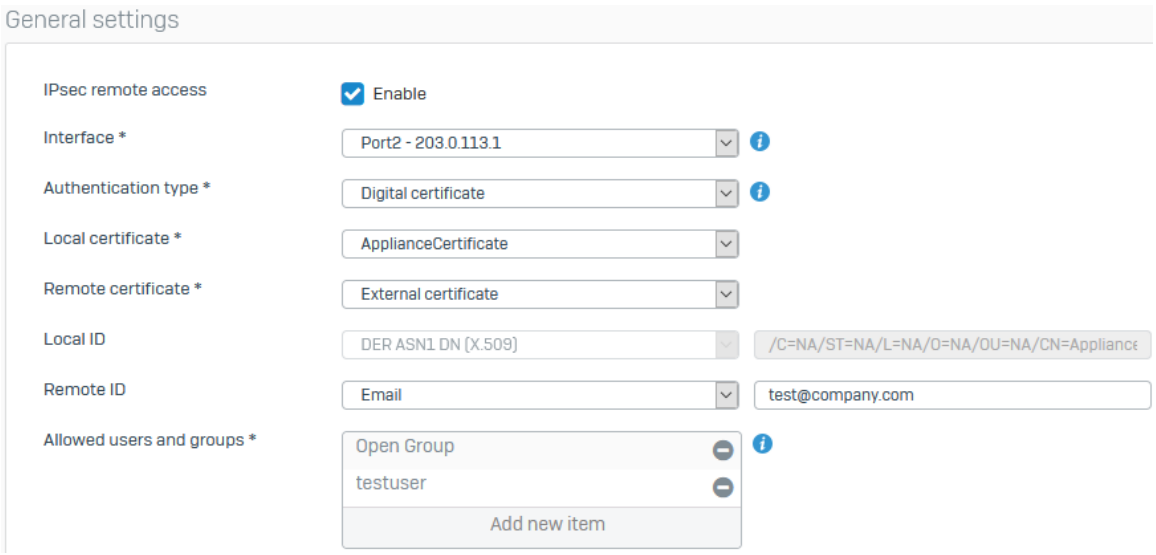
Tutaj możemy zmienić domyślny port łączenia się z interfejsem użytkownika oraz administratora.




## Konfiguracja VPN

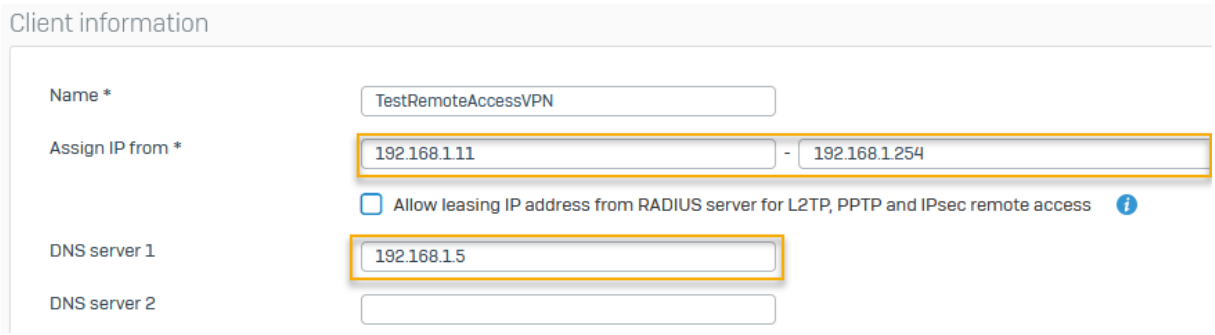
Aby skonfigurować VPN musimy przejść do zakładki *VPN → IPsec (remote access)*
W ustawieniach ogólnych wybieramy:

- Dostęp zdalny IPsec: włączony
- Interfejs: *Port sieci WAN*
- Sposób poświadczenia: *klucz lub certyfikat*
- Lokalny i zdany identyfikator
- oraz grupę lub użytkowników, którzy będą mogli logować się przez klienta VPN.



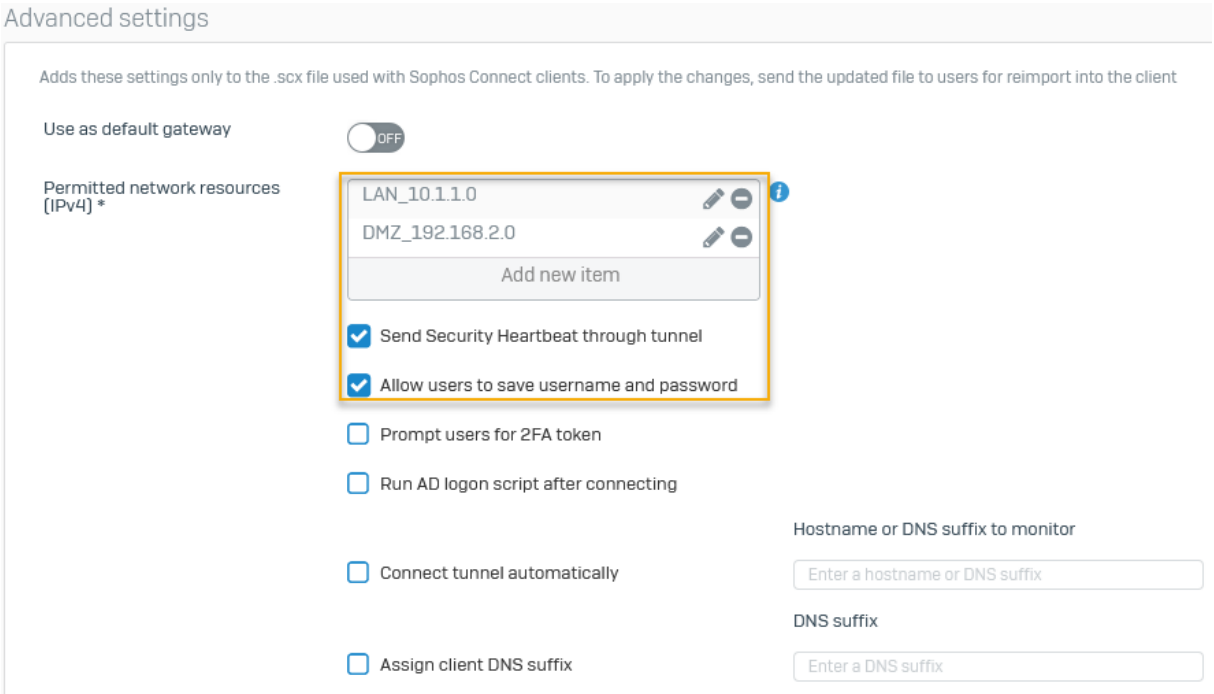
W sekcji informacje o kliencie wybieramy:

- Nazwę połączenia
- Zakres przypisywanych adresów
- oraz serwery DNS




Należy pamiętać, aby zakres przydzielanych adresów dla klientów VPN był w innej podsieci niż zakres adresów dla sieci LAN.

Przykładowa konfiguracja ustawień zaawansowanych:




Jeśli włączymy opcję *Use as default gateway* połączenie VPN będzie pozwalało na dostęp do wszystkich zasobów (wszystkie sieci LAN, WAN, DMZ). Jeżeli pozostawimy tą opcję wyłączoną będziemy musieli utworzyć nowy element, a następnie dodać sieć w *Permitted network resources (IPv4).*

*Permitted network resources* – wybrane zasoby

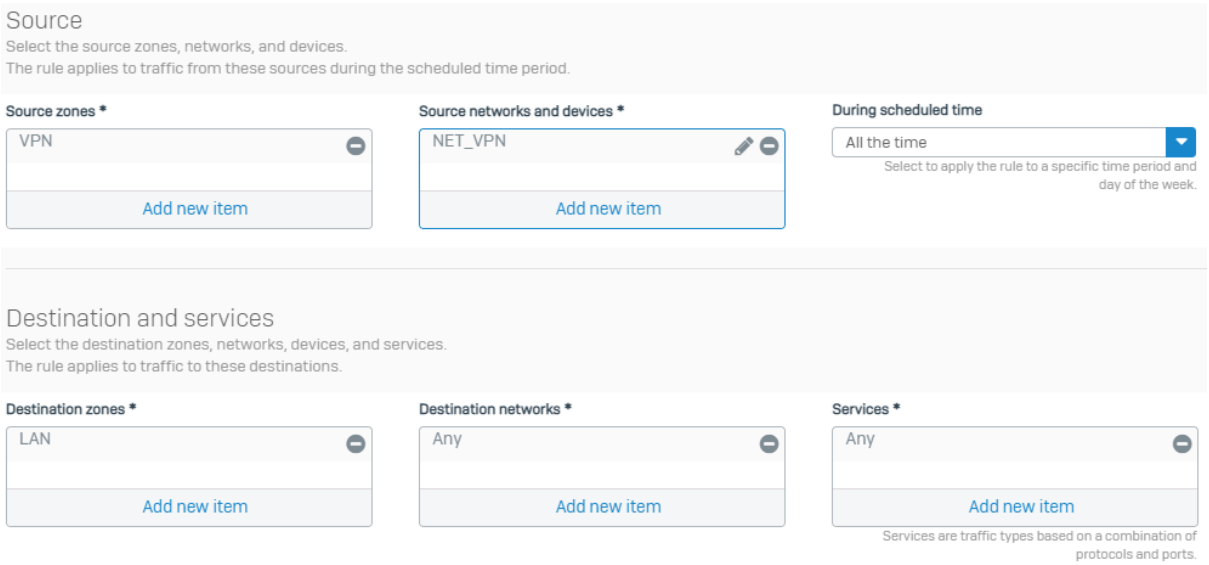
*Use as default Gateway* – dostęp do wszystkich zasobów

Jeśli wybierzemy wszystkie interesujące nas opcje klikamy *Apply* i możemy wyeksportować nasze połączenie, a następnie pobrać klienta.

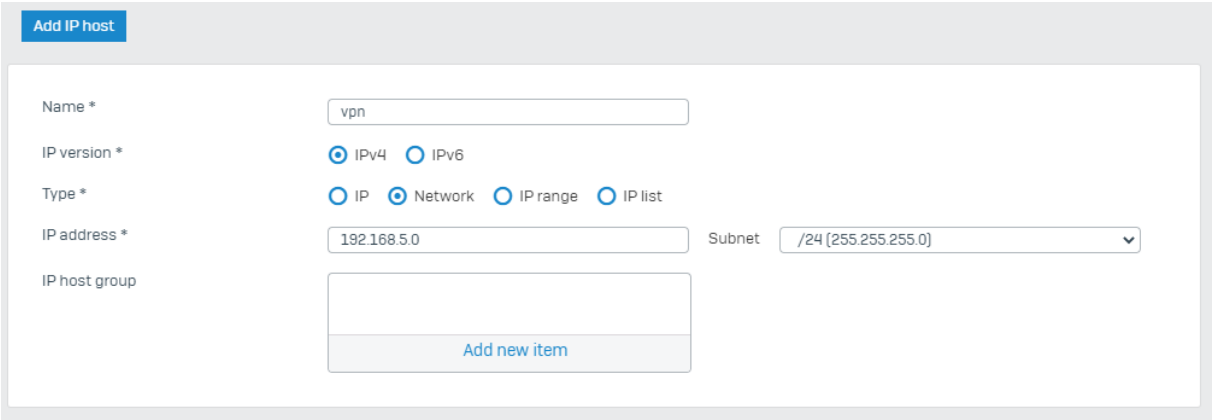

Po ustawieniu VPN musimy dodać go do zapory. Przechodzimy do zakładki *Rules and policies → Firewall rules → Add firewall rule → New firewall rule.*

- Nazwa: VPN to LAN
- Akcja: akceptuj

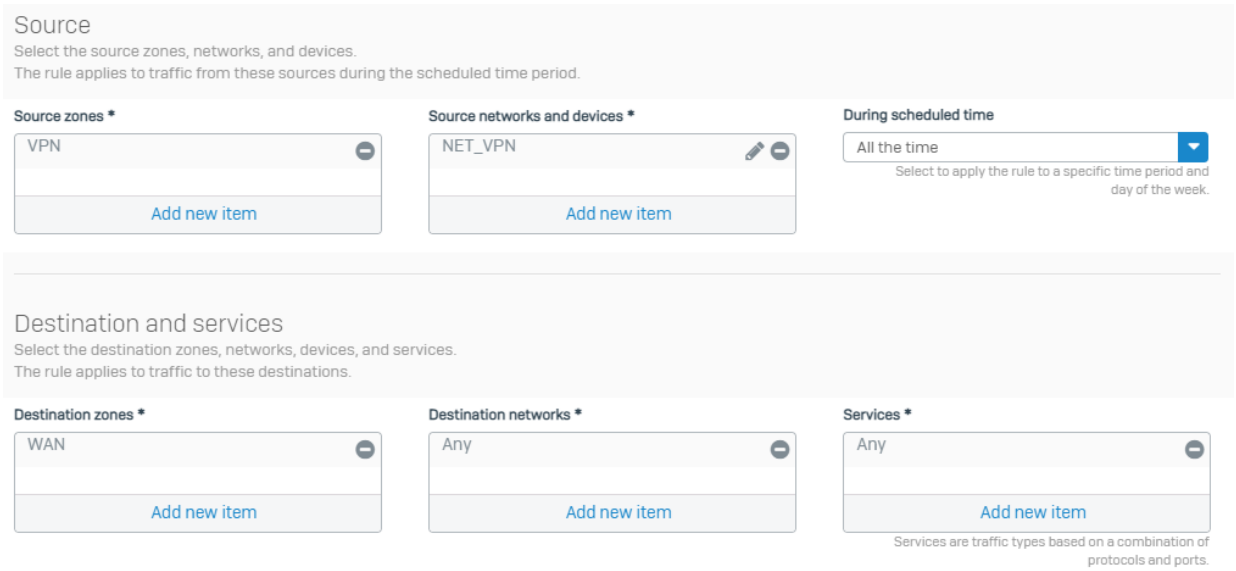
I następnie wybieramy VPN jako źródło, a LAN jako miejsce docelowe.




W *Source networks and devices* tworzymy nowy element sieci o adresie sieci VPN.

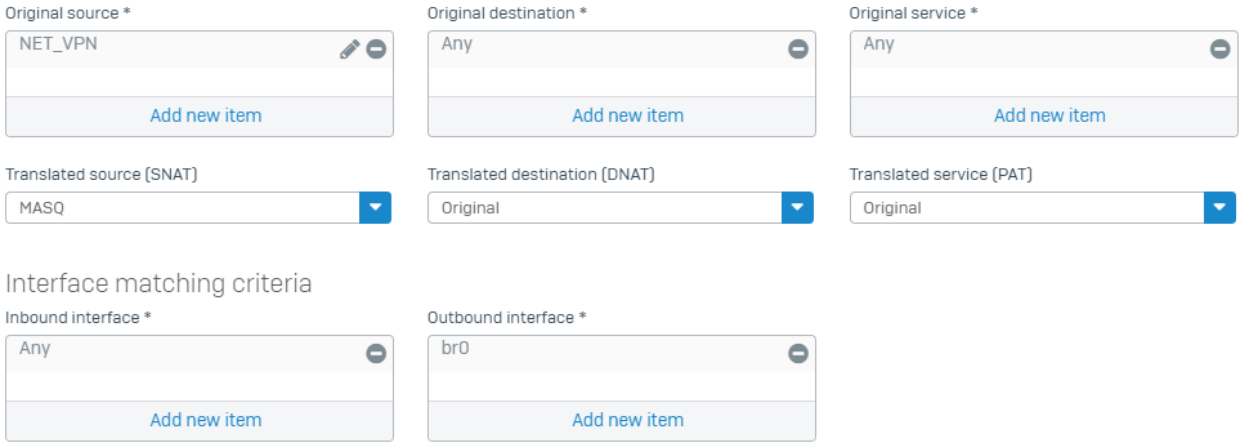


Analogicznie tworzymy zasadę VPN to WAN z tym wyjątkiem, że miejscem docelowym będzie sieć WAN.



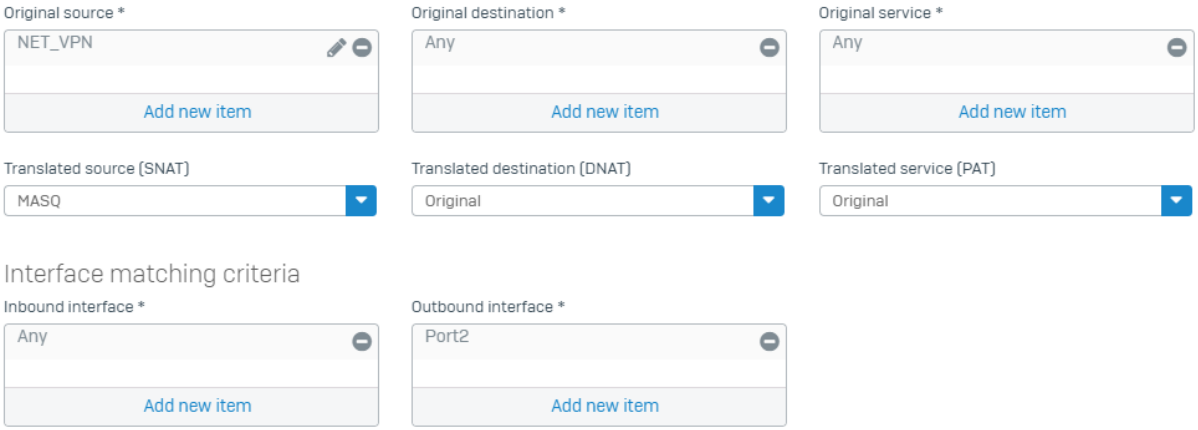

Następnym krokiem będzie utworzenie reguł NAT, które będą tłumaczyć adresy z sieci VPN na sieć LAN oraz WAN. Przechodzimy do *Rules and policies → NAT rules → Add NAT rule → New NAT rule.*

- Nazwa: VPN TO LAN
- Źródło: *element sieci VPN*
- Źródło translacji: MASQ
- Interfejs wychodzący: br0 (LAN)

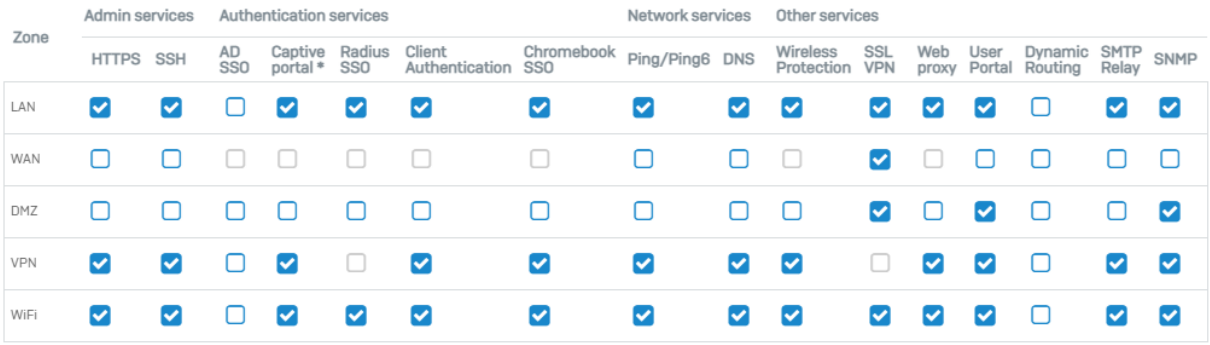


Następnie tworzymy podobną regułę dla połączenia VPN to WAN:

- Nazwa: VPN TO WAN
- Źródło: *element sieci VPN*
- Źródło translacji: MASQ
- Interfejs wychodzący: Port2 (WAN)




Aby, użytkownik korzystający z VPNa miał dostęp do konsoli urządzenia musimy zmienić ustawienia dostępu do urządzenia. W tym celu przechodzimy do *Administration → Devices access*. W wierszu VPN wybieramy interesujące nas ustawienia dostępu.



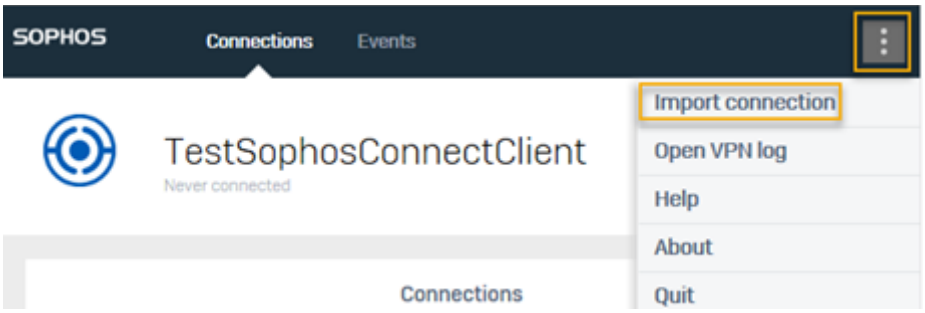
| Zone | Admin services | | Authentication services | | | | | Network services | | Other services | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | HTTPS | SSH | AD SSO | Captive portal * | Radius SSO | Client Authentication | Chromebook SSO | Ping/Ping6 | DNS | Wireless Protection | SSL VPN | Web proxy | User Portal | Dynamic Routing | SMTP Relay | SNMP |
| LAN | ☑ | ☑ | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | ☑ | ☑ |
| WAN | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ |
| DMZ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ | ☑ |
| VPN | ☑ | ☑ | ☐ | ☑ | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | ☑ | ☑ | ☐ | ☑ | ☑ |
| WiFi | ☑ | ☑ | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | ☑ | ☑ |

Po zainstalowaniu klienta musimy wybrać połączenie, aby to zrobić wypakowujemy wcześniej pobrany plik *nazwa.tar*. Po wypakowaniu mamy do wyboru dwa pliki jeden o rozszerzeniu *.scx* i drugi o rozszerzeniu *.tgb*.

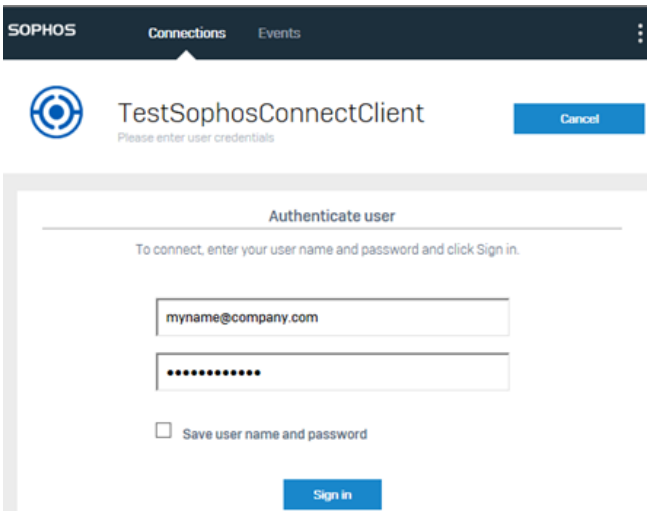
*.scx* – to plik zawierający ustawienia zaawansowane (zalecany)

*.tgb* – to plik zawierający jedynie podstawową konfigurację

W kliencie wybieramy opcje: *Import connection*, a następnie wybieramy interesujący nas plik.



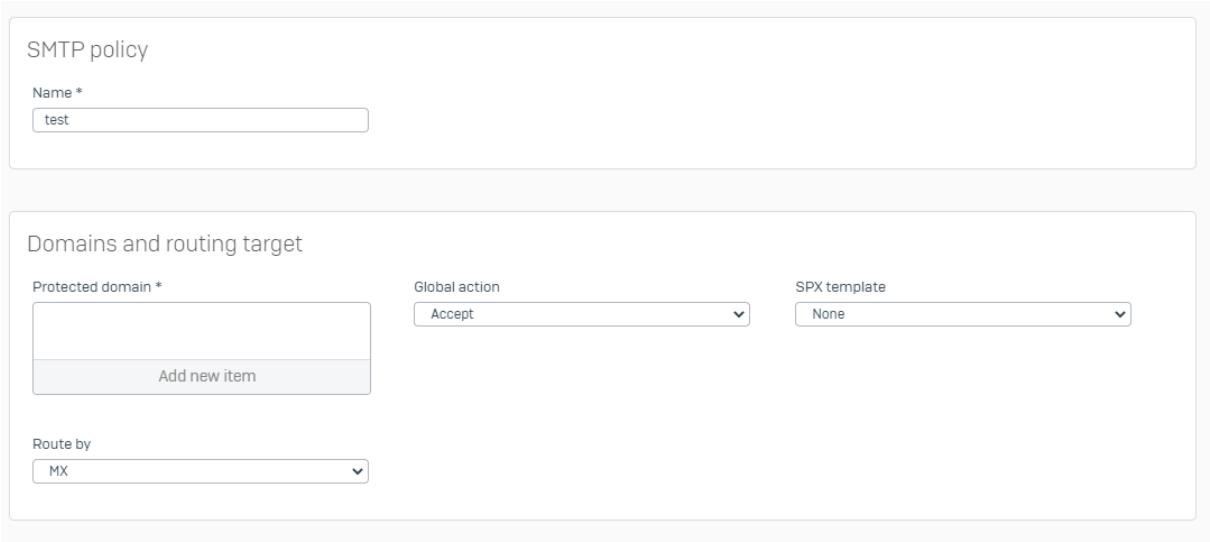

Ostatnim krokiem jest zalogowanie się na wybranego użytkownika.



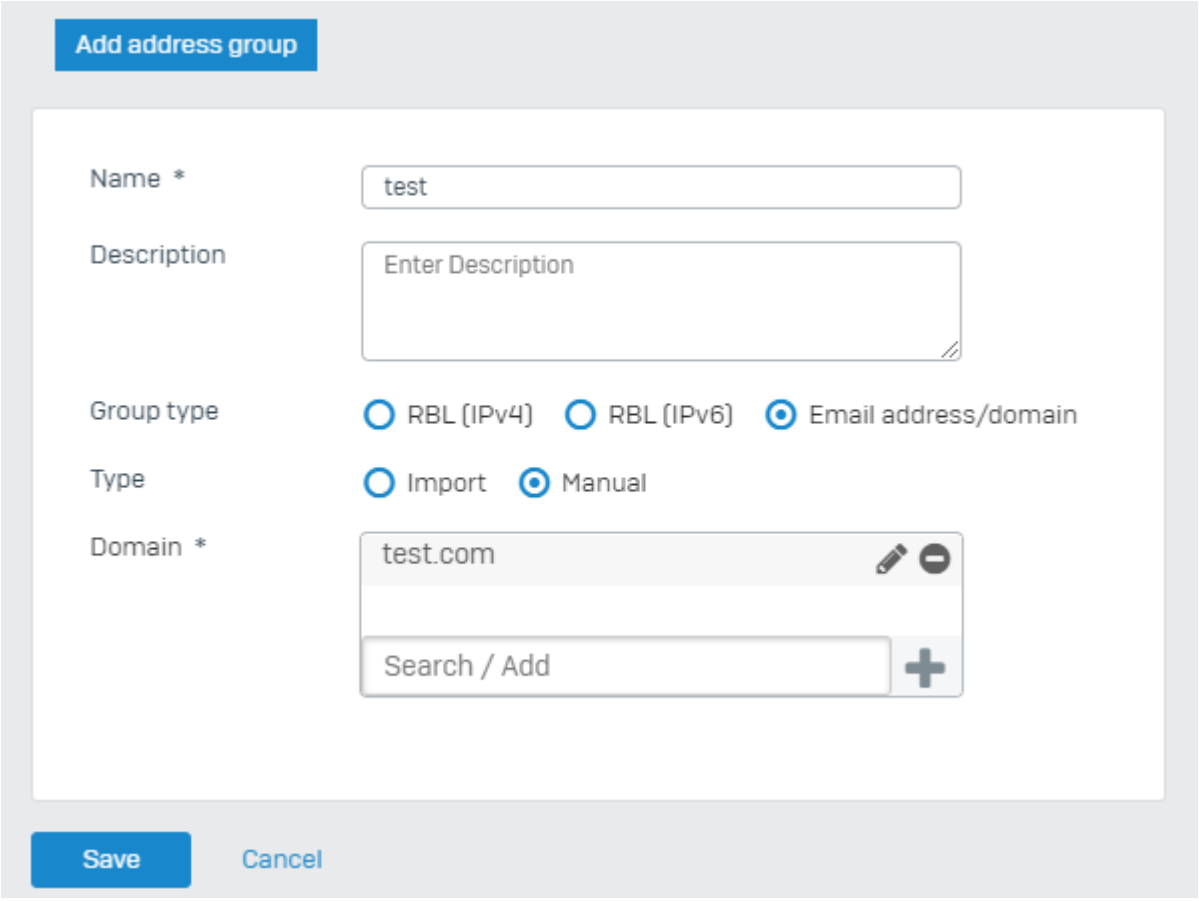
# Konfiguracja email

## SMTP route and scan

Przechodzimy do zakładki *Email → Policies & exceptions → Add policy → SMTP route and scan*.

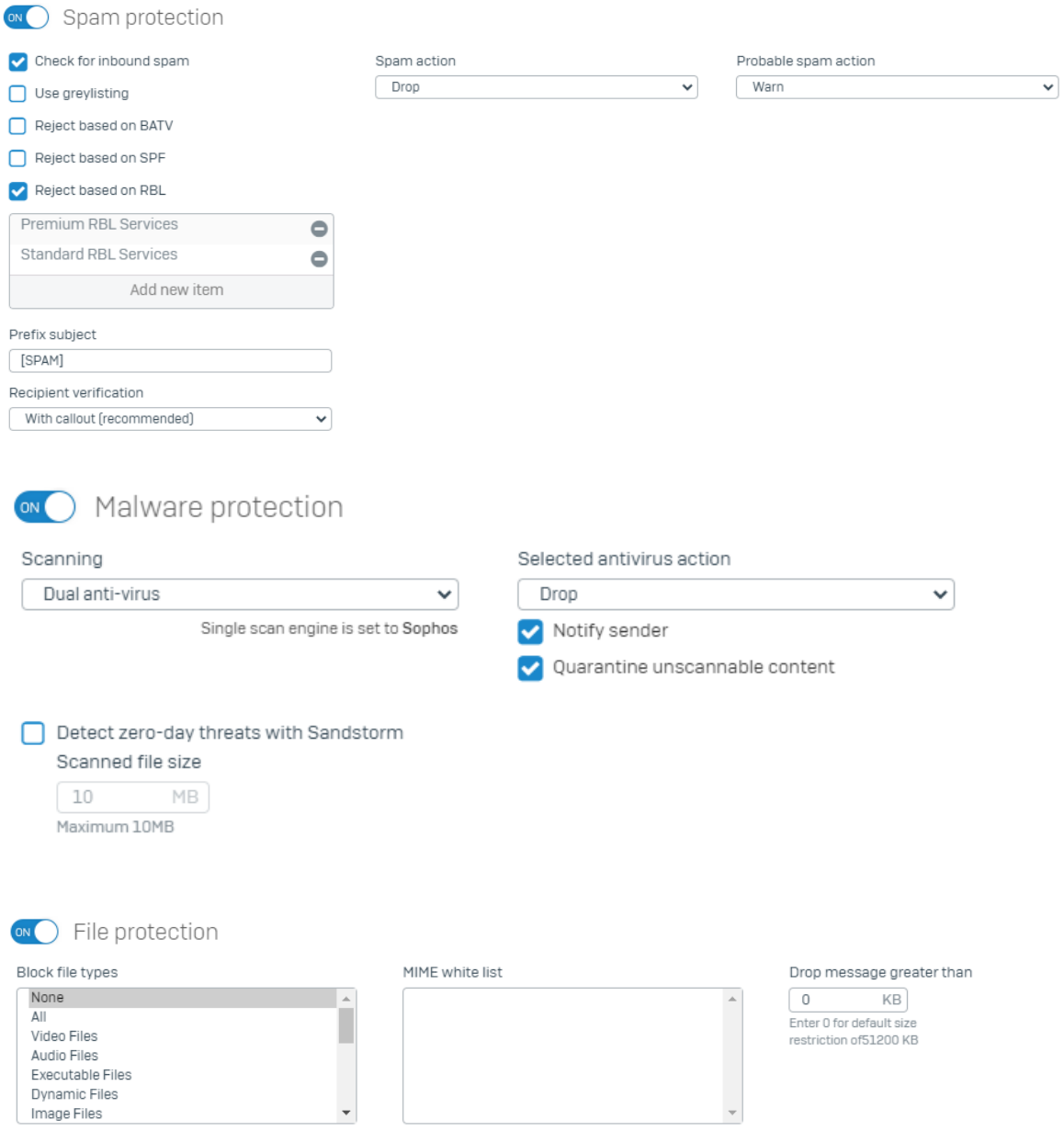



Dodajemy chronioną domenę.



Wybieramy interesujące nas opcje ochrony poczty

Przykładowa konfiguracja:

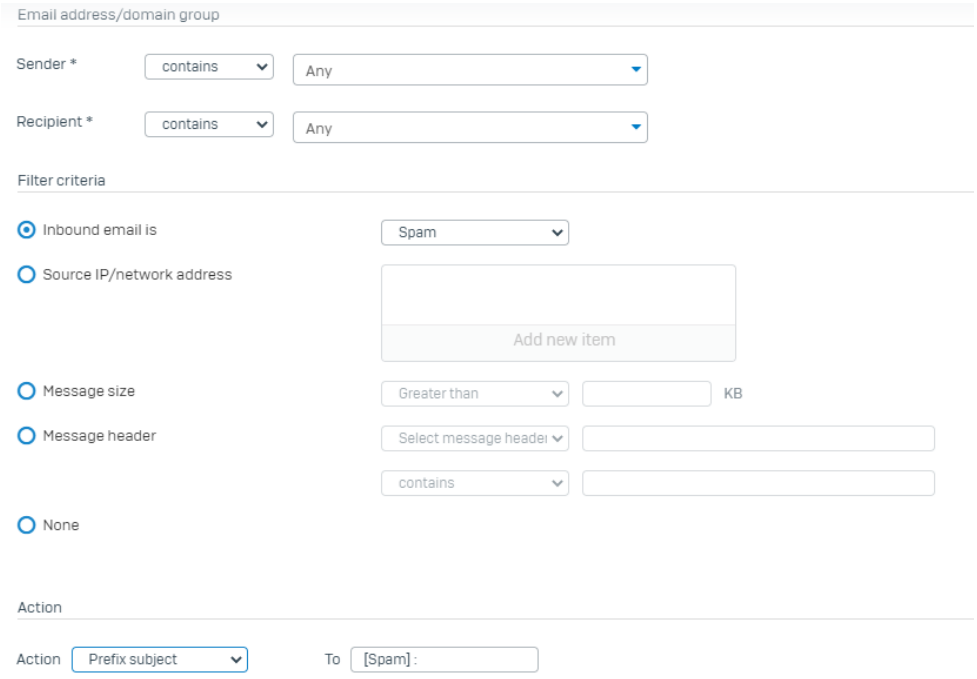



SMTP zaleca się tylko wtedy, gdy w sieci znajduję się serwer poczty.

## POP-IMAP scan

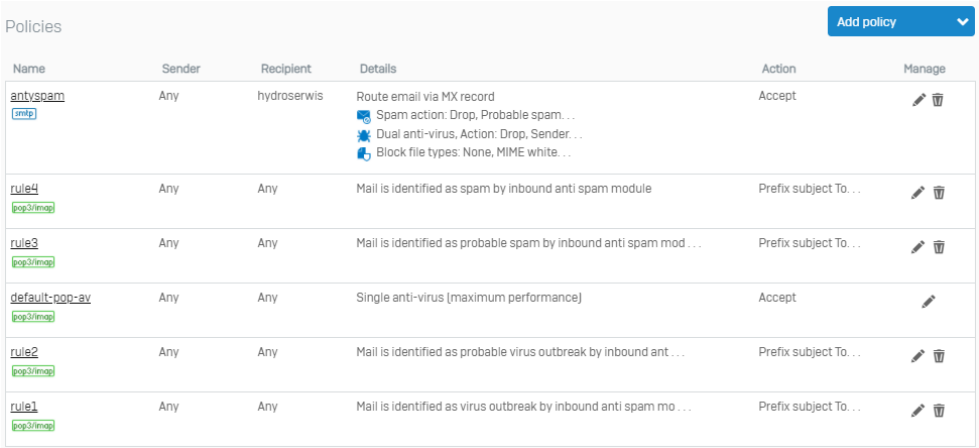
Przechodzimy do zakładki *Email → Policies & exceptions → Add policy → POP-IMAP scan.*

- Nazwa: rule3
- Nadawca: każdy
- Odbiorca: każdy
- Przychodzący email jest: Spamem
- Akcja: Prefix subject
- To: [Spam]:




Analogicznie tworzymy zasadę ochrony przed prawdopodobnym spamem, musimy jedynie wybrać *Probable Spam* w oknie *Inbound email is*.


Nie musimy tworzyć reguł ochrony przed wirusami, ponieważ takie reguły są już domyślnie utworzone.



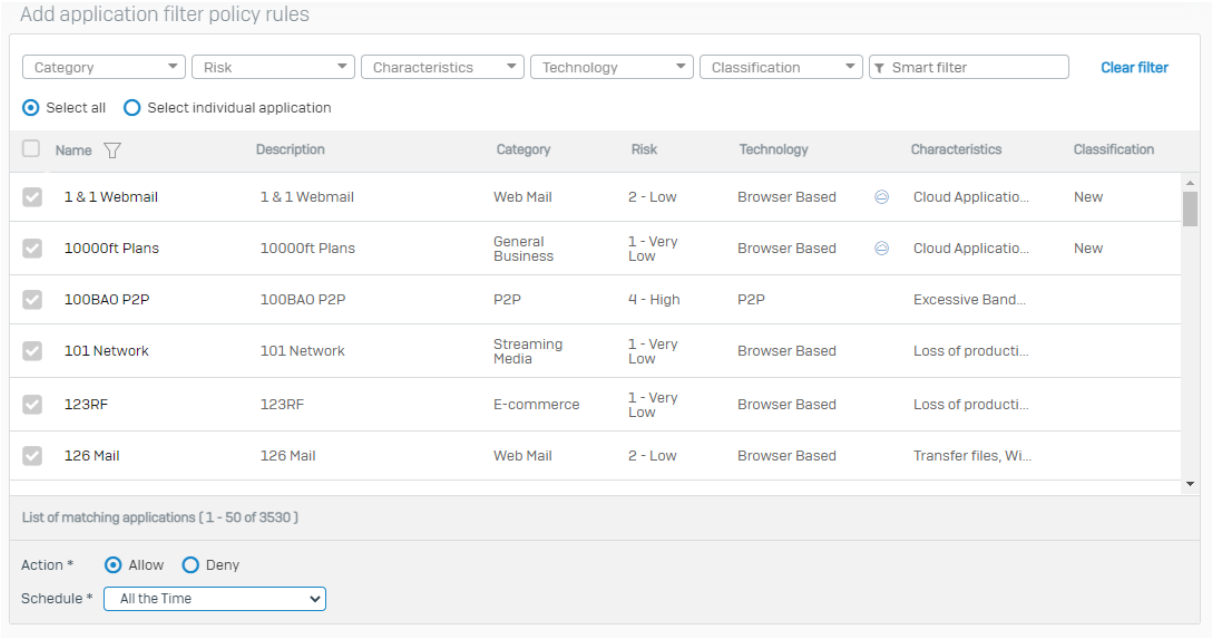
## Blokowanie aplikacji

Aby utworzyć filtr blokowania aplikacji przechodzimy do zakładki *Applications → Application filter → Add.*

Podajemy nazwę, wybieramy szablon i zapisujemy.

Następnie przy naszym nowo dodanym filtrze wybieramy opcję edytuj i dodaj.

Za pomocą kategorii, ryzyka, charakterystyki, technologii i klasyfikacji możemy wybrać aplikacje, które chcemy zablokować lub odblokować w zależności od tego wybieramy akcje: zezwól lub odmów oraz harmonogram, czyli dni lub godziny w jakich aplikacje będą blokowane.




Przykładowa konfiguracja filtru:

- Category = P2P
- Category = Gaming
- Risk = 4-High
- Risk = 5-Very High
- Category = Proxy and Tunnel
- Action: Deny
- Schedule: All the time

## Filtr stron internetowych

Przechodzimy do zakładki *Web → Policies → Add policy.*

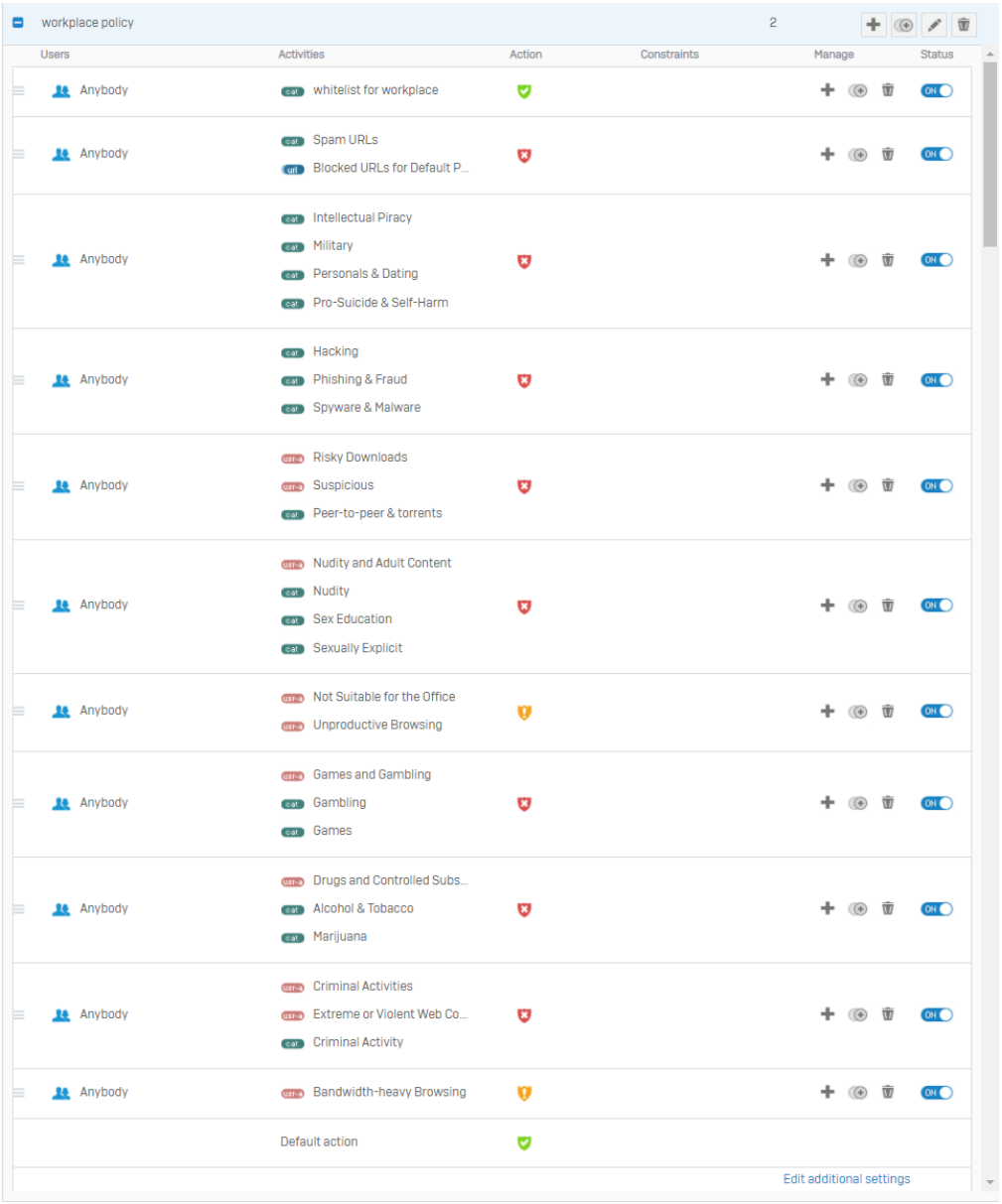
Podajemy nazwę filtru i wybieramy dodaj regułę.

W kolumnie *users* możemy wybrać użytkowników, których będzie dotyczyła reguła.

W kolumnie *Activities*, a następnie *Add new item* wybieramy aktywności, kategorie stron, typy plików i grupy URL, które możemy dodać.

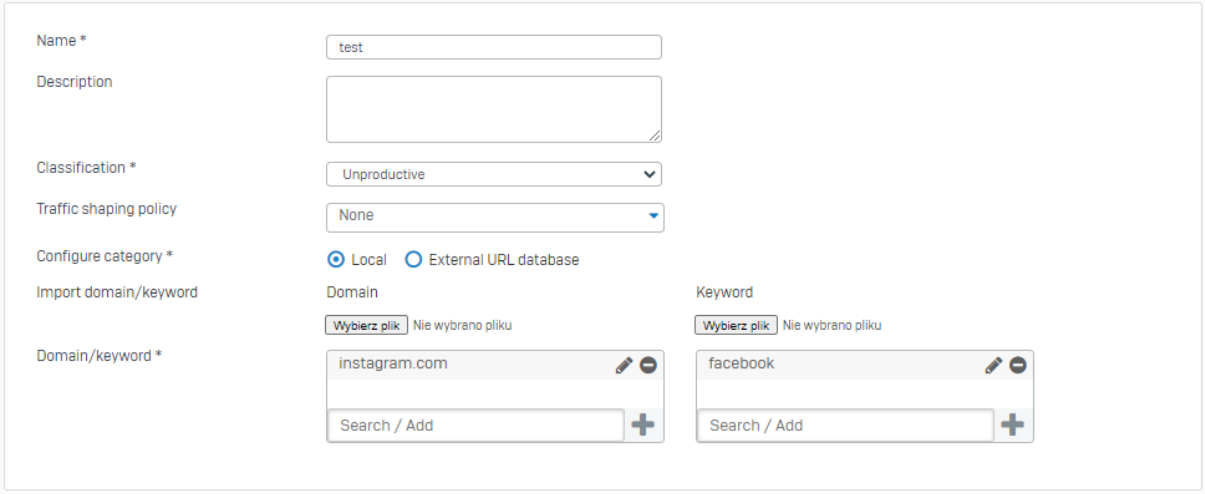
W kolumnie *Action* mamy do wyboru cztery rodzaje akcji, które możemy wykonać w związku z wejściem na wcześniej wybrane przez nas strony. Są to *Zezwól, Blokuj, Ogranicz, Ostrzegaj*.

Przykładowa konfiguracja:



Aby, utworzyć własną grupę stron internetowych musimy przejść do zakładki *Web → Categories → Add.*

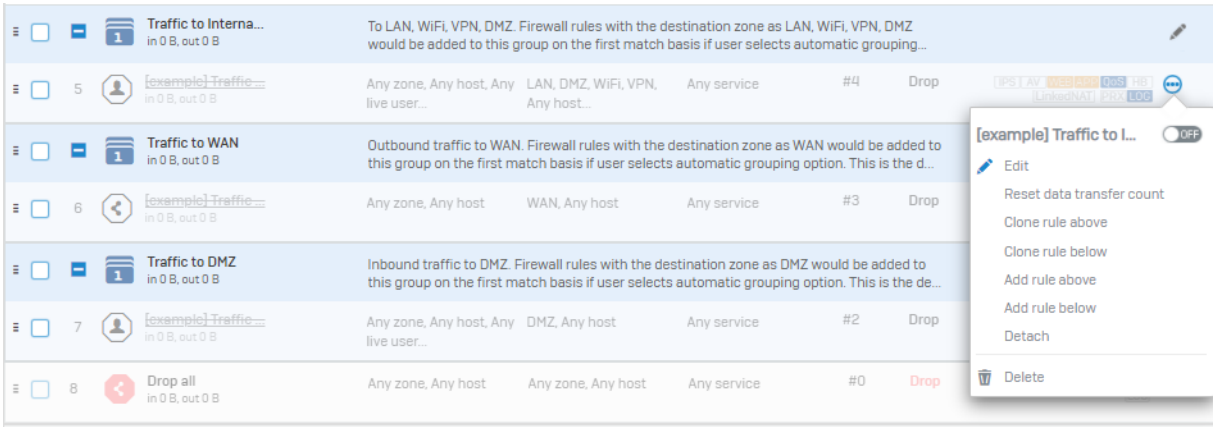
Tutaj podajemy nazwę grupy, wybieramy jak ma być klasyfikowana oraz co najważniejsze możemy podać blokowane domeny lub słowa kluczowe.




## Konfiguracja Firewalla

Przechodzimy do zakładki *Rules and policies → Firewall rules.*

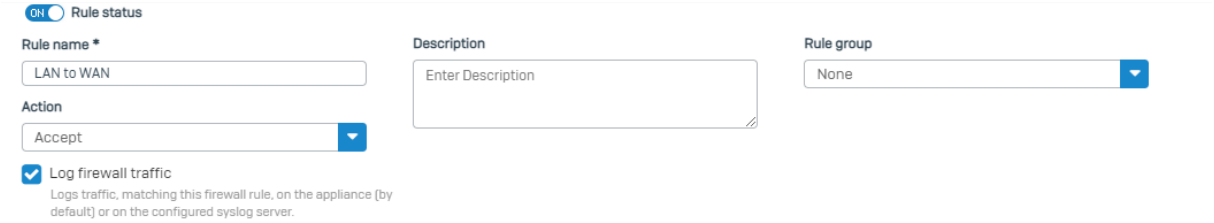
Pierwszym krokiem będzie usunięcie domyślnych reguł i grup. Aby, to zrobić wybieramy trzykropek obok reguły oraz wybieramy opcję Delete.



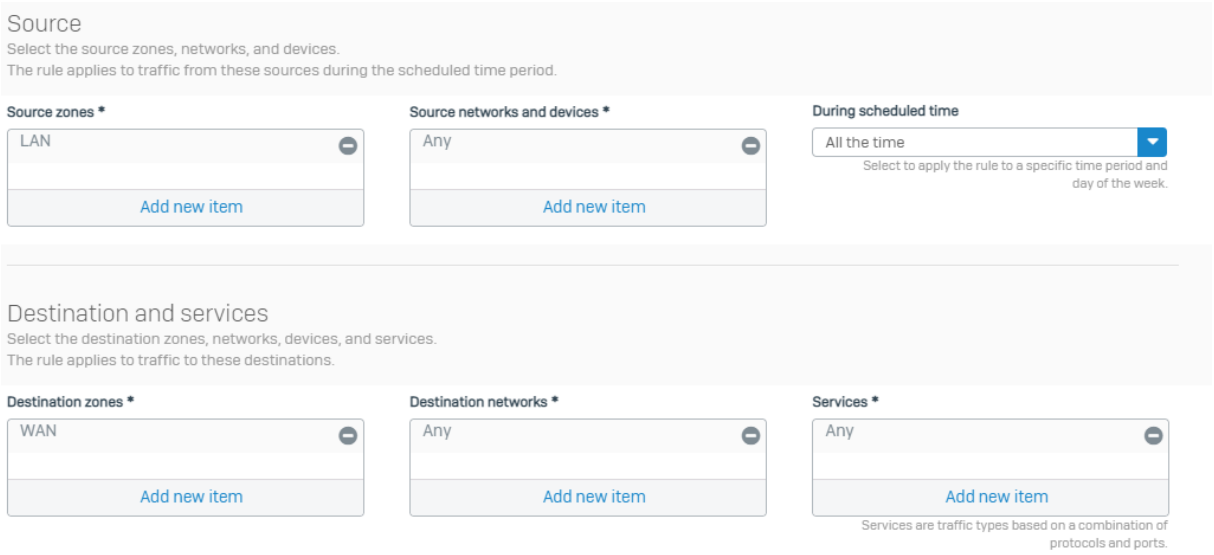
Aby, utworzyć nową regułę wybieramy *Add firewall rule*, a następnie *New firewall rule*.

Pierwsza reguła jaką utworzymy będzie odpowiedzialna za ruch z sieci lokalnej do sieci globalnej.

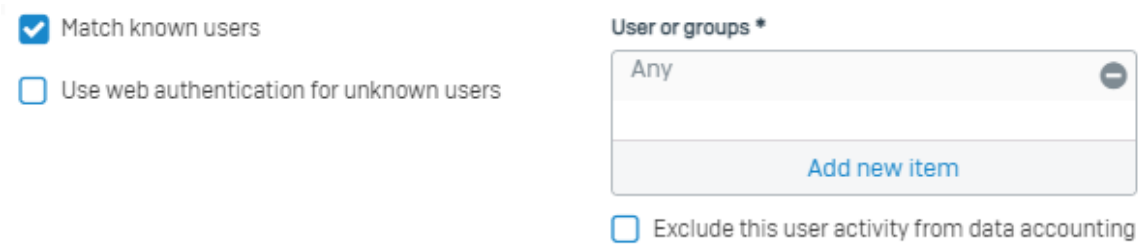
- Nazwa: LAN to WAN
- Akcja: akceptuj
- Reguła grupy: żadna
- Rejestruj ruch zapory: tak




Jako źródło wybieramy LAN, a jako miejsce docelowe WAN.

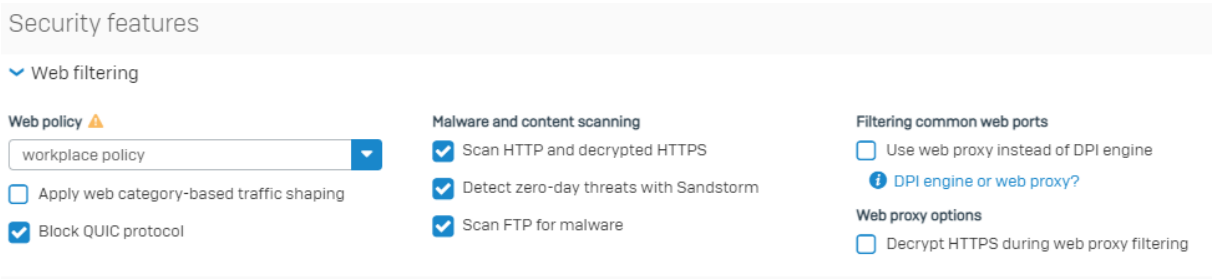



Jeśli chcemy, aby dostęp do internetu był tylko dla określonej grupy użytkowników możemy wybrać funkcję *Match known users* i wybrać grupę lub użytkowników.

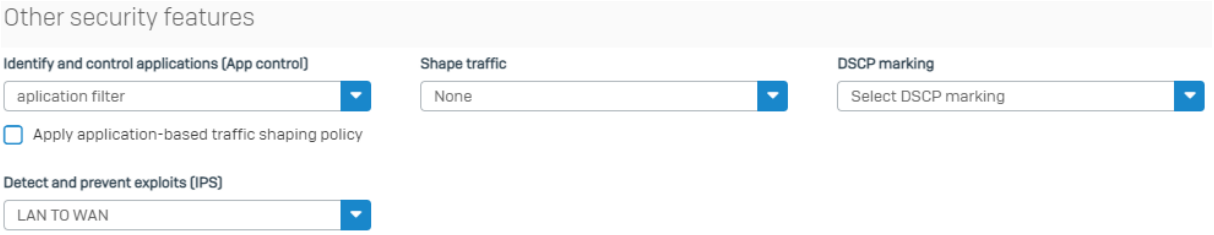


W sekcji *Security features* wybieramy wcześniej utworzoną politykę stron internetowych lub jedną z domyślnych polityk. Następnie zaznaczamy:

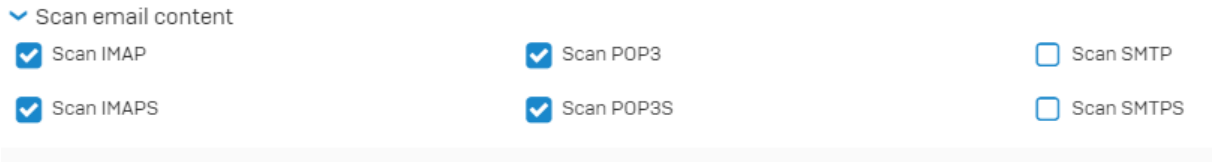
- Blokuj protokół *QUIC*
- Skanuj *HTTP* oraz deszyfrowane *HTTPS*
- Wykrywaj zagrożenia *zero-day* za pomocą *Sandstorm*
- Skanuj *FTP*




W *Other security featues* wybieramy wcześniej utworzony filtr aplikacji lub jeden z domyślnych filtrów, a w sekcji IPS wybieramy LAN TO WAN.



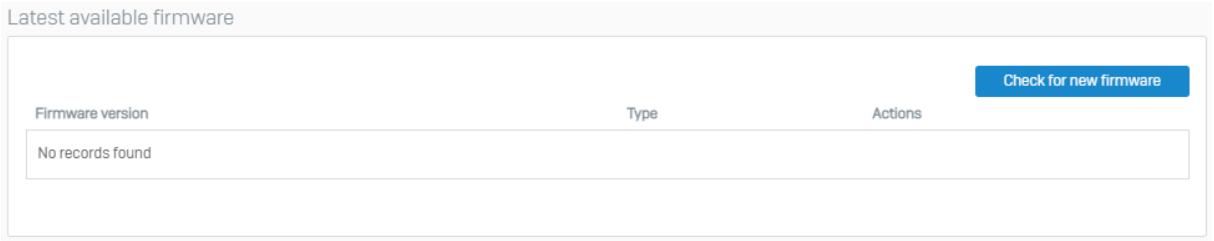

W sekcji skanowania poczty wybieramy skanowanie: *IMAP, IMAPS, POP3, POP3S.*



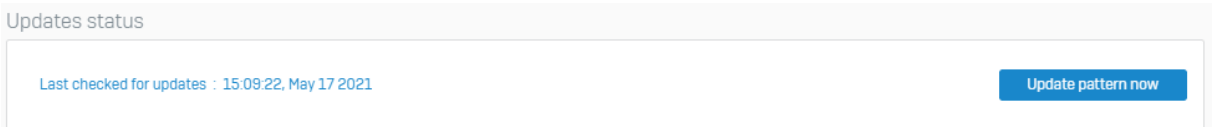

Zaleca się tworzenie osobnej zasady dla każdego ruchu przepływającego z sieci (np. LAN to WAN, VPN to LAN, itd.)

## Aktualizacje

Aby, zaktualizować urządzenie do najnowszej wersji musimy przejść do zakładki *Backup and firmware → Firmware*, a następnie wybrać opcję *Check for new firmware.*



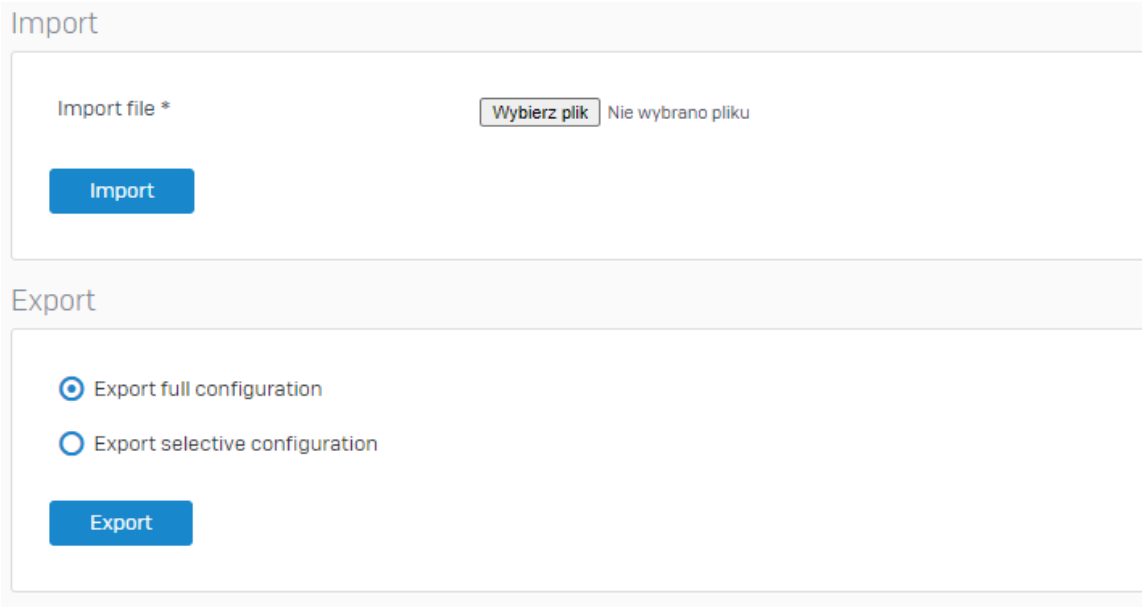

Aby, zaktualizować oprogramowanie przechodzimy do *Backup and firmware → Pattern updates* i wybieramy opcję *Update pattern now*.




## Kopia zapasowa i przywracanie

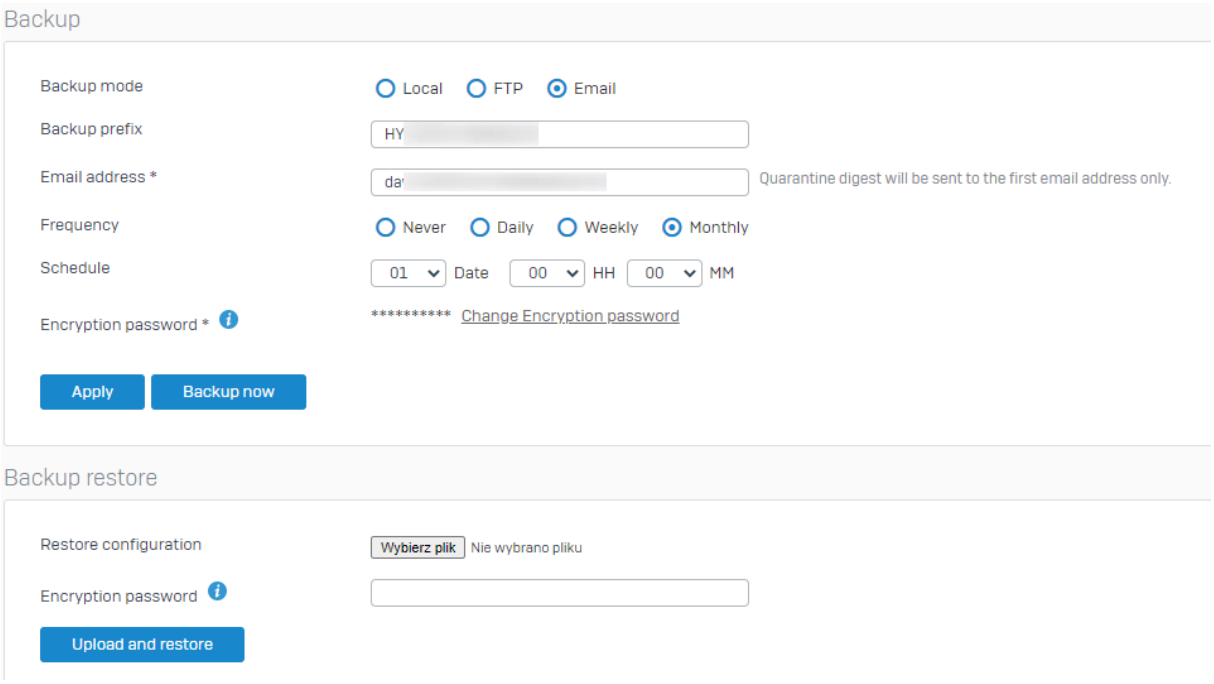
Aby, utworzyć kopie zapasową przechodzimy do zakładki *Backup & firmware → Import export.*

Wybierając opcję *Export full configuration*, a następnie *Export* pobierzemy kopię zapasową naszej konfiguracji.




Aby zaimportować konfigurację wybieramy plik z menu *Wybierz plik*, a następnie potwierdzamy przyciskiem *Import*.

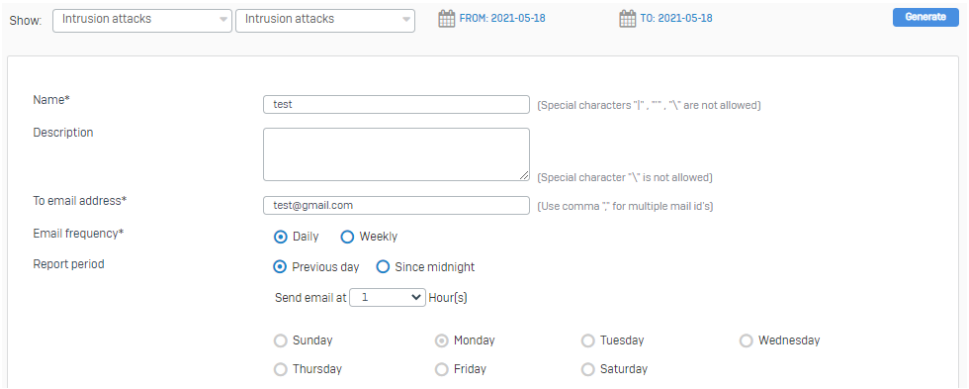
Ustawienia kopii zapasowej możemy zmienić w zakładce *Backup & firmware → Backup & restore*.



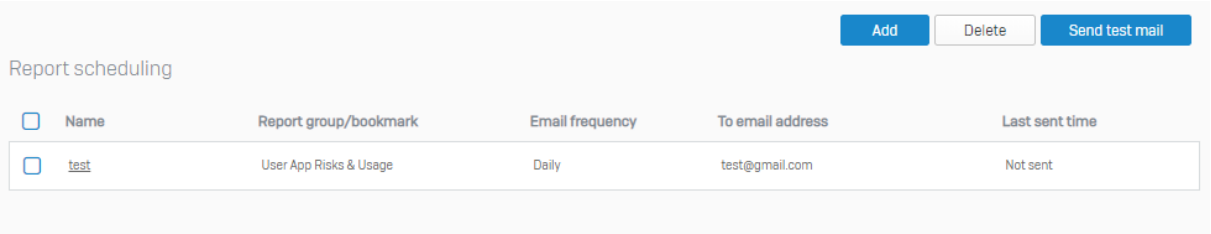

## Raportowanie

Dostęp do bieżących raportów mamy w zakładce *Reports*, ale jeśli chcemy sporządzić harmonogram raportów musimy przejść do zakładki z której chcemy sporządzić raport (Panel nawigacyjny, Aplikację i strony, Sieć i zagrożenia, VPN, Email). Następnie przechodzimy do *Schedule* i wybieramy:

- Pokaż: *wybieramy interesujące nas dane*
- Nazwę
- Adres email odbiorcy
- Częstotliwość wysyłania maili
- Okres raportowania
- oraz dzień i godzinę o której będzie wysyłany email



Jeśli chcemy usunąć harmonogram raportów przechodzimy do *Show Reports settings* → *Report scheduling.* Tutaj możemy dodawać i usuwać raporty oraz jest również możliwość wysłania maila testowego.




Sporządził:
*Dominik Jurczyński*