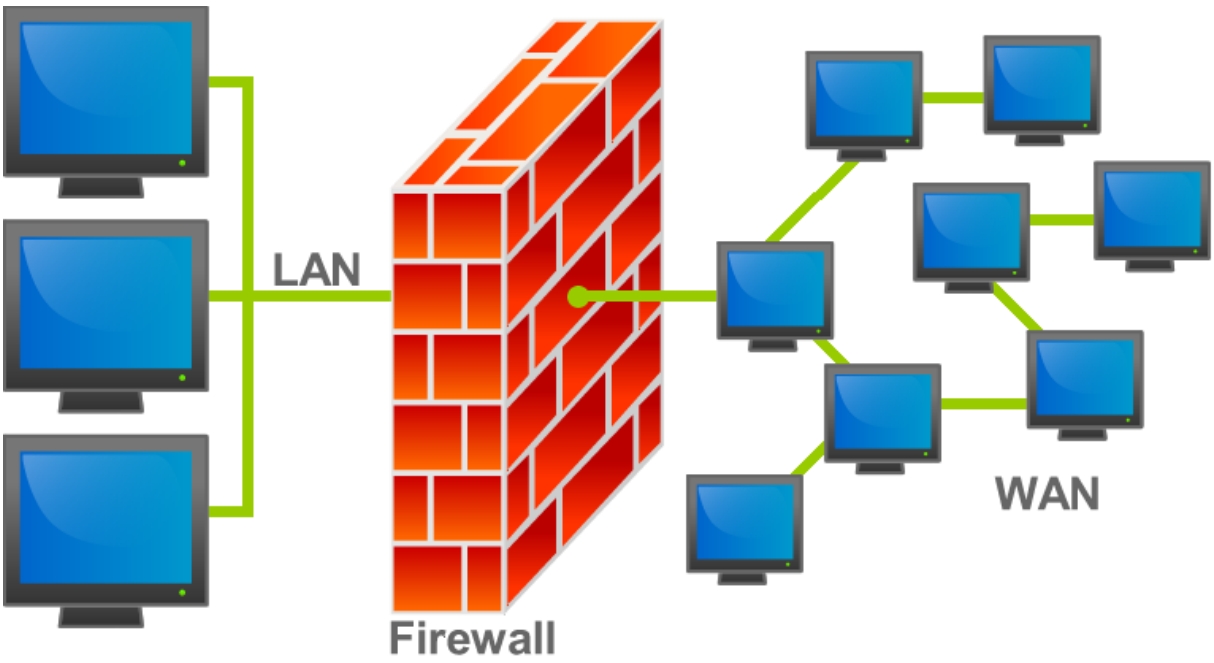
Zapora sieciowa (firewall)

Firewall jest to program lub urządzenie sieciowe, które ma za zadanie kontrolować przepływ danych pomiędzy siecią zewnętrzną a wewnętrzną oraz decydować, które z nich mają prawo wejść, a które zostaną zablokowane. Jest to pierwsza linia obrony przed atakami z zewnątrz.



Podstawowe zadania zapory sieciowej

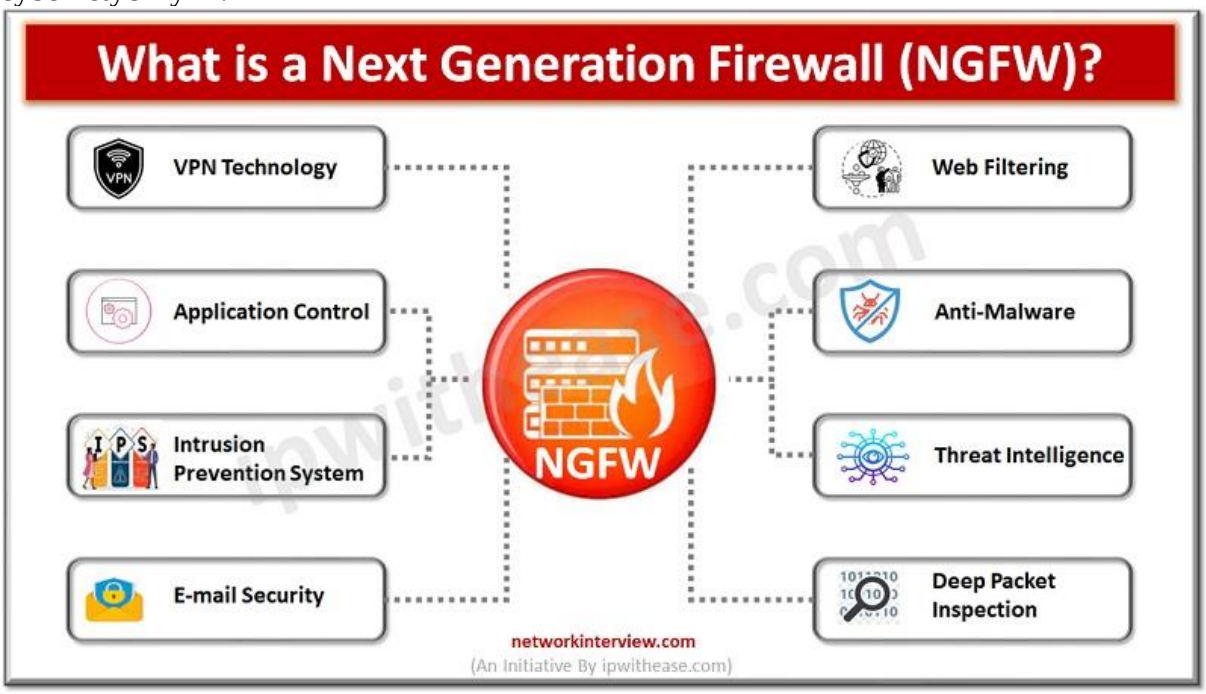
Do podstawowych zadań zapory sieciowej, którymi są zapewnienie użytkownikowi bezpieczeństwa oraz ochrona przed atakami z zewnątrz, można zaliczyć również:

- Monitoring sieci – zbieranie informacji o użytkownikach oraz ilości przesyłanych danych;
- Filtrowanie pakietów – czyli przepuszczanie bądź odrzucanie pakietów, w zależności od zdefiniowanej reguły;
- Blokowanie dostępu do sieci bądź usług – pozwala to na zablokowanie konkretnego serwera bądź usługi dla określonej grupy użytkowników;
- Uwierzytelnianie użytkowników – za pomocą haseł bądź klucza prywatnego można sprawdzić tożsamość użytkownika, a tym samym wykryć potencjalnego włamywacza;
- Tworzenie sieci VPN – wirtualna sieć prywatna jest swego rodzaju tunelem, przez który realizowany jest ruch w ramach sieci prywatnej za pośrednictwem sieci publicznej. Zastosowanie VPN zwiększa bezpieczeństwo użytkowników dzięki możliwości szyfrowania danych. Co więcej poprzez kompresje pakietów bardzo dobrze sprawdza się na wolnych łączach. Z VPN wiąże się także pojęcie tunelowania, które odnosi się do przesyłania niezabezpieczonych protokołów pakietów TCP przez bezpieczny protokół SSH. Wirtualne sieci często używane są w krajach z wysoką cenzurą jak Chiny, bądź krajach gdzie użytkownicy są inwigilowani przez rząd;
- Rejestrowanie połączeń sieciowych – zapisywanie historii połączeń w postaci logów. Dzięki takim informacjom, administrator jest w stanie dokonać poprawek w konfiguracji zapory, czy wykryć intruza

Klasyfikacja zapór sieciowych

Podstawowy podział zapór to zapory sprzętowe oraz programowe. Pierwsze z nich odnoszą się do specjalistycznego sprzętu. Często do urządzenia jest dostarczane oprogramowanie. Programowe zapory różnią się od swoich sprzętowych odpowiedników tym, iż potrzebują do działania komputera z systemem operacyjnym oraz skonfigurowanego połączenia internetowego. Powyższy podział nie jest jednak jedynym, zapory możemy podzielić także na:

- **Zapory filtrujące** – monitorują pakiety, które przepływają przez zaporę i przepuszczają lub odrzucają pakiety zgodnie z ustalonymi wcześniej regułami. Filtrowanie odbywa się po nagłówkach TCP/IP, można dzięki temu zablokować użytkownikowi daną usługę sieciową jak WWW. Zapory filtrujące działają na niskim poziomie sieciowym – warstwa sieciowa oraz transportowa modelu OSI;
- **Zapory ogniowe z inspekcją stanową:** Zapory te, zwane także dynamicznym filtrowaniem pakietów, monitorują stan aktywnych połączeń i określają legalność pakietów na podstawie informacji o stanie. Zapory ogniowe z inspekcją stanową zapewniają większą kontrolę i bezpieczeństwo w porównaniu do zapór filtrujących pakiety.
- **Zapory warstwy aplikacji:** Zapory te działają w warstwie aplikacji modelu OSI i zapewniają głęboki wgląd w dane specyficzne dla aplikacji. Potrafią wykrywać i blokować złośliwą zawartość, taką jak ataki polegające na wstrzykiwaniu SQL, skrypty między witrynami (XSS) i inne luki w zabezpieczeniach na poziomie aplikacji, zapewniając integralność danych przetwarzanych przez aplikacje generowane przez AppMaster.
- **Zapory sieciowe nowej generacji (NGFW):** Zapory te łączą tradycyjne funkcje zapór sieciowych z zaawansowanymi funkcjami zabezpieczeń, takimi jak zapobieganie włamaniom, usługi bezpiecznych bram internetowych i piaskownica, aby zapewnić kompleksową ochronę przed wyrafinowanymi zagrożeniami cybernetycznymi.



- **Zapora aplikacji sieci Web (WAF):** Zapory te w szczególności chronią aplikacje internetowe przed typowymi atakami w warstwie aplikacji, takimi jak wstrzykiwanie SQL, wykonywanie skryptów między witrynami i zdalne dołączanie plików. W kontekście platform no-code takich jak AppMaster, WAF może zapewnić dodatkową warstwę bezpieczeństwa dla generowanych aplikacji internetowych.