
## Cel szkolenia?

**Celem szkolenia FORTINET TWO – FortiGate + FortiClient** jest wyposażenie uczestników w praktyczne umiejętności oraz specjalistyczną wiedzę dotyczącą konfiguracji, zarządzania i monitorowania urządzeń FortiGate oraz rozwiązania FortiClient EMS. Szkolenie koncentruje się na skutecznym wdrażaniu polityk bezpieczeństwa, ochronie urządzeń końcowych oraz zapewnieniu bezpiecznych połączeń sieciowych. Uczestnicy nauczą się, jak efektywnie zarządzać dostępem do sieci, wykrywać i neutralizować zagrożenia oraz optymalizować poziom bezpieczeństwa infrastruktury IT w organizacji.

## Dla kogo?

Szkolenie zostało stworzone z myślą o inżynierach bezpieczeństwa i administratorach systemów, którzy na co dzień zarządzają, konfigurują i monitorują urządzenia FortiGate. To idealna propozycja dla specjalistów świadomych wyzwań związanych z dynamicznym rozwojem infrastruktury sieciowej oraz rosnącą potrzebą zapewnienia najwyższego poziomu ochrony. Podczas szkolenia uczestnicy zdobędą praktyczne umiejętności w zakresie zabezpieczania połączeń sieciowych z wykorzystaniem FortiClient EMS, co pozwoli im skutecznie zarządzać politykami bezpieczeństwa i zminimalizować ryzyko cyberzagrożeń w swoich organizacjach.

## Jak szkolimy?

Nasze szkolenie to dynamiczne połączenie merytorycznej wiedzy z praktycznymi ćwiczeniami, które pozwalają natychmiast zastosować zdobyte umiejętności w codziennej pracy. Dzięki interaktywnej formule – łączącej inspirujące mini wykłady z angażującymi warsztatami – uczestnicy nie tylko zdobywają cenną wiedzę, ale także uczą się, jak skutecznie wdrażać ją w swoim środowisku zawodowym.

Podczas szkolenia dbamy o komfort uczestników, zapewniając przerwy kawowe oraz lunch.

**Na zakończenie każdy uczestnik otrzymuje certyfikat potwierdzający ukończenie specjalistycznego szkolenia.**

## Czas trwania?

Szkolimy w godzinach od 9:00  do 14:00.

## Kto prowadzi szkolenie?

### Adrian Kamizela

Inżynier pracujący w Akademii BB, wyspecjalizowany w zakresie szeroko pojętej technologii IT, w tym sieci komputerowych i bezpieczeństwa systemów komputerowych oraz komputerowych systemach zarządzania i sterowania.
Na co dzień pracuje przy wdrożeniach technologii UTM i rozwiązywaniu problemów sieciowych naszych Klientów, a także realizuje audyty bezpieczeństwa danych w systemach informatycznych i sieci ICT oraz KRI i KSC.
Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności dot. urządzeń Fortinet są liczne certyfikaty (FCF Fortinet Certified Fundamentals, FCA Fortinet Certified Associate, FCP Fortinet Certified Professional Network Security, FCSS Fortinet Certified Solution Network Security).

### Jakub Szablewski

Inżynier pracujący w Akademii BB, posiadający kilkuletnie doświadczenie w administrowaniu systemami teleinformatycznymi. Na co dzień pracuje przy wdrożeniach technologii UTM i pomaga naszym Klientom chronić ich sieci i dane przed zagrożeniami
Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności dot. urządzeń Fortinet są liczne certyfikaty (FCF Fortinet Certified Fundamentals, FCA Fortinet Certified Associate, FCP Fortinet Certified Professional Network Security, FCSS Fortinet Certified Solution Network Security).

## Agenda szkolenia:

I. Wstęp

1. Powitanie i wprowadzenie do szkolenia
   a) Oficjalne powitanie uczestników oraz przedstawienie planu szkolenia.
   b) Krótkie omówienie struktury i harmonogramu zajęć.
   c) Zapoznanie uczestników z celami szkolenia oraz oczekiwanymi rezultatami.
2. Prezentacja Rozwiązań Fortinet
   a) Przegląd ekosystemu Fortinet oraz jego roli w ochronie sieci.
   b) Omówienie kluczowych funkcji FortiGate i FortiClient EMS Cloud.
   c) Wskazanie korzyści wynikających z integracji tych technologii.

II. FORTIGATE

3. Konfiguracja Podstawowych Ustawień Sieciowych
   a) Adresacja IP i przypisywanie interfejsów.
   b) Konfiguracja routingu oraz serwerów DNS.
   c) Optymalizacja ustawień wydajności i bezpieczeństwa.
4. Integracja z LDAP / Active Directory
   a) Powiązanie FortiGate z infrastrukturą katalogową (LDAP, AD).
   b) Automatyczna autoryzacja użytkowników VPN.
5. Użycie VPN na FortiGate
   a) Konfiguracja i Zarządzanie VPN (IPSec i SSL)
      - Omówienie typów VPN oraz ich zastosowań.
      - Różnice między VPN IPSec a SSL.
   b) Tworzenie i Konfiguracja Tuneli SSL VPN
      - Konfiguracja polityk i zasad ruchu SSL VPN.
      - Analiza logów i statystyk SSL VPN.
   c) Tworzenie i Konfiguracja Tuneli IPsec-VPN.

- Konfiguracja polityk i zasad ruchu VPN.
- Analiza logów i statystyk VPN.

III. FORTIANALYZER

6. Integracja FortiGate z FortiClient EMS Cloud
   a) Instalacja i Konfiguracja FortiClient EMS Cloud
      - Omówienie wymagań i procesu wdrożenia.
   b) Integracja FortiClient EMS z FortiGate
      - Konfiguracja synchronizacji urządzeń i polityk bezpieczeństwa.
   c) Omówienie Panelu Administracyjnego
      - Przegląd funkcji zarządzania urządzeniami końcowymi.
7. Konfiguracja FortiClient EMS Cloud
   a) Konfiguracja Profili Ochronnych
      - Definiowanie polityk zabezpieczeń dla urządzeń końcowych.
   b) Konfiguracja Pakietów Instalacyjnych
      - Tworzenie i wdrażanie pakietów FortiClient dla różnych typów urządzeń.
      - Centralne zarządzanie aktualizacjami i zgodnością.
   c) Monitorowanie i Zarządzanie Urządzeniami Końcowymi
      - Śledzenie aktywności użytkowników i potencjalnych zagrożeń.
      - Zdalne usuwanie lub izolowanie zagrożonych urządzeń.
   d) Polityki Zabezpieczeń dla Użytkowników Zdalnych
      - Definiowanie zasad dostępu dla pracowników zdalnych.

IV. ZAKOŃCZENIE

8. Podsumowanie i Sesja Q&A
   a) Omówienie kluczowych zagadnień poruszonych podczas szkolenia.
   b) Otwarta sesja pytań i odpowiedzi dla uczestników.
9. Zakończenie i Testy Wiedzy

## Dlaczego warto?

**Po szkoleniu uczestnicy będą potrafili:**

- Konfigurować i zarządzać urządzeniami FortiGate oraz rozwiązaniem FortiClient EMS.
- Tworzyć i wdrażać polityki bezpieczeństwa w celu ochrony sieci oraz urządzeń końcowych.
- Monitorować ruch sieciowy i analizować zagrożenia za pomocą narzędzi Fortinet.
- Optymalizować poziom zabezpieczeń infrastruktury IT w organizacji.
- Efektywnie zarządzać dostępem do sieci, uwzględniając różne scenariusze uwierzytelniania.
- Wykrywać i neutralizować zagrożenia z wykorzystaniem mechanizmów FortiGate i FortiClient EMS.
- Konfigurować bezpieczne połączenia VPN dla użytkowników zdalnych.
- Automatyzować zadania administracyjne i stosować najlepsze praktyki w zarządzaniu bezpieczeństwem.

**B&B Prosta Spółka Akcyjna**

ul. Walentego Roździeńskiego 2A | 41-946 Piekary Śląskie

www.b-and-b.pl | biuro@b-and-b.pl