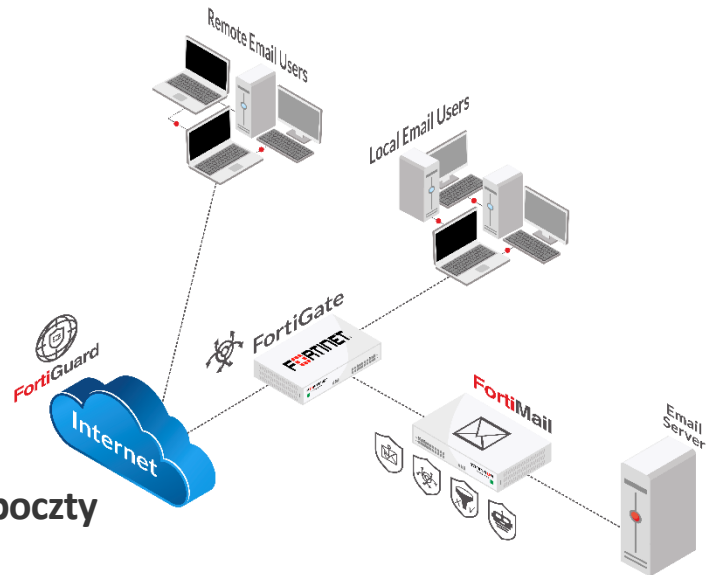


## SZKOLENIE

# FortiMail Perfect

Poznaj możliwości skutecznej ochrony poczty



## Cel szkolenia?

Naszym celem jest dostarczenie uczestnikom konkretnej wiedzy na temat budowania ochrony przed zdarzeniami i incydentami bezpieczeństwa pochodzącymi z poczty elektronicznej korzystając z rozwiązania FortiMail.

Zależy nam na przekazaniu wiedzy, która pozwoli Ci na rozpoczęcie administracji urządzeniami FortiMail. Zapoznanie z protokołem SMTP umożliwi Ci swobodniejszą analizę maili oraz wybór odpowiedniej techniki ochrony na przykładzie rozwiązania FortiMail.

Ponadto w naszym laboratorium nauczymy Cię jak poprawnie skonfigurować urządzenie, monitorować zagrożenia związane z pocztą elektroniczną, izolować je oraz jak im zapobiegać.

## Dla kogo?

Szkolenie **przeznaczone jest dla** inżynierów bezpieczeństwa i administratorów ds. bezpieczeństwa, zajmujących się zarządzaniem urządzeniami FortiMail oraz chętnych rozszerzyć swoją wiedzę na temat administracji FortiMailem w zakresie monitorowania zagrożeń oraz incydentów związanych z pocztą elektroniczną.

## Jak szkolimy?

Szkolenie realizowane jest w formie mini wykładów oraz ćwiczeń praktycznych. Łączy w sobie fachową wiedzę merytoryczną z praktycznymi przykładami jej wykorzystania w środowisku pracy. W ramach spotkania zapewniamy przerwy kawowe oraz lunch. Szkolenie zakończone jest certyfikatem. Po ukończeniu szkolenia uczestnicy otrzymują certyfikat potwierdzający odbycie specjalistycznego szkolenia.

## Czas trwania?

Szkolimy w godzinach od 9:00 do 16:00.

## Kto prowadzi szkolenie?



### Jacek Baron

Ekspert w dziedzinie rozwiązań bezpieczeństwa systemów i sieci teleinformatycznych. Szkoleniowiec i wdrożeniowiec z ponad 15 letnim doświadczeniem. Specjalizuje się w projektowaniu i wdrażaniu kompleksowej architektury bezpieczeństwa, obejmującej zarówno aspekty technologiczne jak i organizacyjne. Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności są liczne certyfikaty i autoryzowane certyfikaty Producentów takich jak: Fortinet, Cisco, VMware, Veeam, Eset, Sophos, F-Secure, Qnap.



### **Tomasz Baron**

Trener pracujący w Akademii BB, posiadający wieloletnie doświadczenie w branży IT, na co dzień pracujący przy wdrożeniach technologii UTM i rozwiązywaniu problemów sieciowych naszych Klientów. Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności dot. urządzeń Fortinet są liczne certyfikaty (m. in. NSE4, NSE5, NSE7) oraz setki zadowolonych administratorów IT, których Tomek miał okazję przeszkolić.

## **Agenda szkolenia:**

---

|        |   |
|--------|---|
| I.     | WSTĘPNA KONFIGURACJA FORTIMAIL W TRYBIE GATEWAY                   |
| 1.     | ZASADA DZIAŁANIA DNS  |
| II.    | KONFIGURACJA CHRONIONEJ DOMENY                                    |
| 1.     | POJEDYNCZY SERWER POCZTOWY  |
| 2.     | LOAD BALANCING  |
| III.   | OBSŁUGA SMTP PRZEZ FORTIMAIL                                      |
| 1.     | FORTIMAIL JAKO MTA DLA POCZTY PRZYCHODZĄCEJ I WYCHODZĄCEJ         |
| 2.     | WERYFIKACJA ADRESÓW ODBIORCÓW                                     |
| 3.     | FORTIMAIL JAKO PROXY DLA SESJI UWIERZYTELNIONYCH                  |
| IV.    | KONFIGURACJA I OMÓWIENIE REGUŁ ACCESS CONTROL                     |
| 1.     | NIEZBĘDNE POLITYKI DLA POPRAWNEJ OBSŁUGI RUCHU                    |
| V.     | OMÓWIENIE ZASAD DZIAŁANIA REGUŁ (IP POLICIES, RECIPIENT POLICIES) |
| VI.    | ANALIZA LOGÓW   |
| VII.   | TROUBLESHOOTING   |
| VIII.  | OMÓWIENIE I KONFIGURACJA PROFILU SESJI                            |
| IX.    | PROFILE ANTYSZPAMOWE DLA RUCHU PRZYCHODZĄCEGO                     |
| X.     | ANTYSZPAM DLA RUCHU WYCHODZĄCEGO                                  |
| XI.    | PROFILE ANTYWIRUSOWE  |
| 1.     | OMÓWIENIE ORAZ KONFIGURACJA INTEGRACJI Z SANDBOX                  |
| XII.   | PROFILE KONTROLI TREŚCI   |
| XIII.  | DLP   |
| XIV.   | WHITE/BLACK LISTY   |
| XV.    | OCHRONA PRZED BLACK LISTINGIEM                                    |
| XVI.   | KWARANTANNA   |
| XVII.  | INTEGRACJA Z LDAP   |
| XVIII. | ARCHIWIZACJA POCZTY W OPARCIU O POLITYKI                          |
| XIX.   | SZYFROWANIE POCZTY W OPARCIU O POLITYKI (IBE)                     |
| XX.    | RAPORTOWANIE  |
| XXI.   | PRZECHOWYWANIE POCZTY NA ZEWNĘTRZNYCH ZASOBACH                    |
| XXII.  | KONFIGURACJA HA   |

## Dlaczego warto?

Po szkoleniu uczestnicy będą potrafili:

- Wdrożyć urządzenie FortiMail w swojej infrastrukturze w trybie transparentnym, bramki (gateway) lub serwera.
- Używać serwera LDAP do zarządzania użytkownikami i uwierzytelniania ich
- Obsługiwać transmisję poczty e-mail przy użyciu najlepszych w swojej klasie technologii, takich jak SMTPS, SMTP przez TLS i szyfrowanie oparte na tożsamości (IBE)
- Ograniczać połączenia klientów, aby zablokować nadużycia MTA
- Wyeliminować spam, phishing i zagrożenia zero-day
- Zintegrować FortiMail z FortiSandbox, aby uzyskać zaawansowaną ochronę przed zagrożeniami (ATP)
- Zapobiegać przypadkowemu lub celowemu wyciekowi poufnych danych z użyciem HIPAA, GLBA, SOX
- Wdrożyć bezpieczny system dostarczania wiadomości z FortiMail na podstawie tożsamości (Identity-Based Encryption), S/MIME lub metody szyfrowania maili TSL
- Kontrolować użytkowników na podstawie reguł dla danej domeny z użyciem atrybutów LDAP
- Zarządzać kwarantanną, kolejką wiadomości
- Monitorować status łącza, przełączyć awaryjnych wraz z obsługą interfejsu nadmiarowego
- Zdiagnozować powszechne problemy związane z pocztą e-mail i FortiMail

## Jesteś zainteresowany ofertą?

Jeśli masz dodatkowe pytania lub chcesz zapoznać się z naszą ofertą zapraszamy do kontaktu z opiekunami handlowymi.



**B&B Jacek Baron**

Ul. Walentego Róźnieńskiego 2a

41-946 Piekary Śląskie

[www.b-and-b.pl](http://www.b-and-b.pl)

[biuro@b-and-b.pl](mailto:biuro@b-and-b.pl)