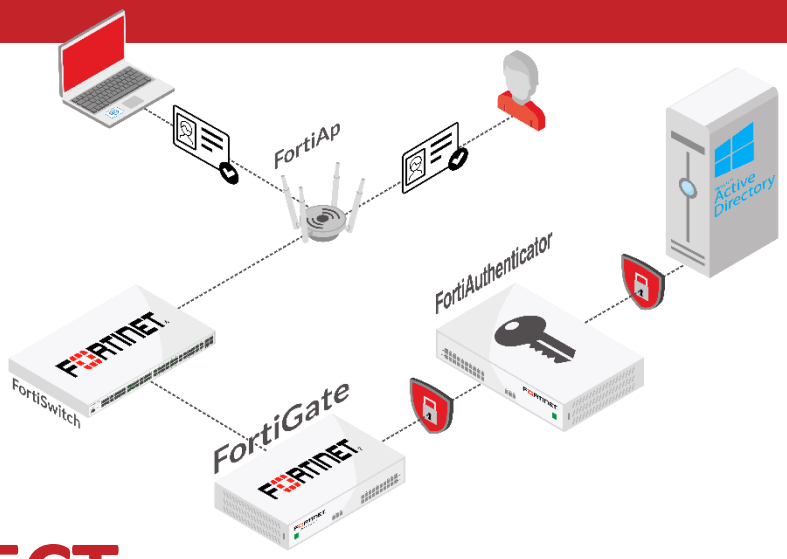

SZKOLENIE

FORTINET PERFECT

Kompleksowa ochrona sieci

Cel szkolenia?

Naszym celem jest dostarczenie specjalistom IT i bezpieczeństwa sieciowego solidnej wiedzy na temat wdrożenia podstawowych zabezpieczeń sieci firmowych wykorzystując zaawansowany Next Generation Firewall - **FortiGate**, oraz wiedzy na temat wdrożenia systemu do zarządzania tożsamością oraz centralnym punktem uwierzytelnienia w sieci - **FortiAuthenticator**.

Podczas szkolenia uczestnicy dowiedzą się jak od podstaw skonfigurować funkcje ochronne FortiGate, oraz jak zapewnić bezpieczny dostęp zdalny do ich instytucji. Bez zbędnej teorii, skupiając się na praktycznych wskazówkach trenera skonfigurują własną jednostkę FortiGate, poznają zasady zapory, uwierzytelniania użytkowników, SSL VPN, IPsec-VPN oraz sposoby ochrony sieci przy użyciu profili bezpieczeństwa.

Ponadto, każdy z uczestników będzie miał okazję przeprowadzić wdrożenie swojego własnego systemu do zarządzania uwierzytelnianiem oraz tożsamością - FortiAuthenticator, podczas którego pozna tajniki integracji obu rozwiązań i korzyści z niej płynących. Każdy z uczestników skonfiguruje swoją maszynę w celu zweryfikowania różnych metod uwierzytelnienia użytkowników oraz urządzeń w swojej sieci z wykorzystaniem protokołu 802.1x oraz wdroży dwuskładnikowe uwierzytelnianie z wykorzystaniem **FortiToken Mobile**.

Dla kogo?

Szkolenie przeznaczone jest dla inżynierów bezpieczeństwa i administratorów systemów zajmujących się zarządzaniem, konfiguracją i monitorowaniem urządzeń **FortiGate**, którzy jednocześnie są świadomi zagrożeń jakie wynikają ze stale rosnącej ilości sprzętu (często prywatnego), który uzyskuje dostęp do zasobów instytucji i stoją przed wyzwaniem zabezpieczenia dostępu do ich sieci korporacyjnych przy wykorzystaniu **FortiAuthenticator**.

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.

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, WitchSecure, Qnap.

Agenda szkolenia:

I.	**PODSTAWY ZARZĄDZANIA UTM**
1.	**KONFIGURACJA SIECIOWA**
a)	KONFIGURACJA URZĄDZEŃ Z POZIOMU CLI – PORUSZANIE SIĘ; KOMENDY SHOW / GET
b)	ADRESACJA IP; RODZAJE INTERFEJSÓW
c)	DNS; SERWER USŁUGI DNS
d)	ROUTING STATYCZNY
e)	BACKUP KONFIGURACJI RĘCZNY / GUI / USB
f)	BACKUP KONFIGURACJI AUTOMATYCZNY
2.	**BACKUP USTAWIEŃ**
a)	BACKUP RĘCZNY / GUI / USB
b)	BACKUP AUTOMATYCZNY
II.	**FIREWALL**
1.	**POLITYKI FIREWALLA**
a)	TWORZENIE OBIEKTÓW / ADRESÓW / SERWISÓW / PRZEDZIAŁÓW CZASOWYCH
b)	ZASADY DZIAŁANIA POLITYK FIREWALLA / PRZYKŁADY REGUŁ
2.	**POLITYKI OCHRONY DOS**
a)	TWORZENIE OBIEKTÓW / ADRESÓW / SERWISÓW / PRZEDZIAŁÓW CZASOWYCH
b)	ZASADY DZIAŁANIA POLITYK FIREWALLA / PRZYKŁADY REGUŁ
3.	**ZARZĄDZANIE PASMEM**
a)	TWORZENIE POLITYK
b)	TWORZENIE PROFILI
III.	**PROFILE UTM**
1.	ANTIVIRUS
a)	TWORZENIE PROFILI / METODY SKANOWANIA (PROXY / FLOW)
b)	SKANOWANIE PORTÓW; OGRANICZENIA
c)	BLOKOWANIE; SPRAWDZANIE LOGÓW
2.	**WEB FILTER**
a)	TWORZENIE PROFILI / METODY SKANOWANIA (PROXY / FLOW)
b)	SKANOWANIE PORTÓW; OGRANICZENIA
c)	BLOKOWANIE; SPRAWDZANIE LOGÓW
3.	**DNS FILTER**

a) ZASADY DZIAŁANIA / TWORZENIE PROFILI
b) KONTROLA ZAPYTAŃ WG. WZORCÓW PRODUCENTA
c) RĘCZNA KONTROLA ZAPYTAŃ

4. APPLICATION CONTROL
a) ZASADY DZIAŁANIA / TWORZENIE PROFILI
b) KONTROLA APLIKACJI / GRUP
c) TWORZENIE WYJĄTKÓW

5. INTRUSION PREVENTION
a) ZASADY DZIAŁANIA / TWORZENIE PROFILI
b) KONTROLA OCHRONY NA PODSTAWIE SYGNATUR
c) TWORZENIE WYJĄTKÓW

IV. VPN

1. SSL-VPN
a) ZASADY DZIAŁANIA / KONFIGURACJA DOSTĘPU
b) DOSTĘP DO PORTALU WEB / MOŻLIWOŚCI AUTO-KONFIGURACJI
c) TRYB PEŁNEGO TUNELOWANIA / ZASADY DOSTĘPU

2. IPSEC DIALUP
a) ZASADY DZIAŁANIA / KONFIGURACJA DOSTĘPU
b) TWORZENIE POLITYK I KONTROLA RUCHU

3. IPSEC SITE-TO-SITE
a) KONFIGURACJA TUNELI MIĘDZY DWOMA FG
b) POLITYKI DOSTĘPU / LOGOWANIE RUCHU

V. PORADY DOŚWIADCZONEGO ADMINA

1. **DOBRE PRAKTYKI**
a) WDROŻENIE OCHRONY ANTYWIRUSOWEJ – INTEGRACJA Z FORTISANDBOX CLOUD
b) PODWÓJNE UWIERZYTELNIENIE – WDROŻENIE TOKENÓW 2FA

2. **LOGOWANIE / ALERTOWANIE/ DEBUGOWANIE**
a) PRZEGLĄDANIE LOGÓW
b) KONFIGURACJA POWIADOMIEŃ
c) DEBUG RUCHU / ROZWIĄZYWANIE PROBLEMÓW

VI. FORTIAUTHENTICATOR

1. WPROWADZENIE DO FORTIAUTHENTICATOR
a) ZAPOZNANIE SIĘ Z PRODUKTEM - FORTIAUTHENTICATOR
b) OMÓWIENIE MOŻLIWOŚCI FORTIAUTHENTICATOR
c) PRZEDSTAWIENIE MOŻLIWOŚCI WDROŻENIA

2. LICENCJONOWANIE
a) OMÓWIENIE LICENCJONOWANIA
b) PRZEDSTAWIENIE RÓŻNIC LICENCJONOWANIA W ZALEŻNOŚCI OD TYPU WDROŻENIA

3. WDROŻENIE MASZYNY FORTIAUTHENTICATOR
a) OMÓWIENIE WYMAGANYCH ZASOBÓW
b) INSTALACJA MASZYNY WIRTUALNEJ FORTIAUTHENTICATOR

4. KONFIGURACJA MASZYNY FORTIAUTHENTICATOR
a) KONFIGURACJA USTAWIEŃ SIECIOWYCH
b) INTEGRACJA Z SERWEREM LDAP
c) INTEGRACJA Z FORTIGATE

5. SHOWCASE W WYKONANIU FORTIAUTHEN TICATOR
a) UWIERZYTELNIANIE DWUSKŁADNIKOWE Z WYKORZYSTANIEM FORTITOKEN MOBILE
b) UWIERZYTELNIANIE URZĄDZEŃ ZA POMOCĄ MAB
c) UWIERZYTELNIENIE UŻYTKOWNIKÓW W SIECIACH PRZEWODOWYCH ORAZ BEZPRZEWODOWYCH

VII. PODSTAWY PRACY Z FORTIANALYZER

1. OPIS LICENCJONOWANIA / WYMAGANIA SYSTEMOWE
a) WYBÓR LICENCJI; UTWORZENIE KONTA FORTICLOUD; POBRANIE OPROGRAMOWANIA
b) PRZYGOTOWANIE ZASOBÓW VMWARE / HYPER-V; INSTALACJA I KONFIGURACJA MASZYNY

2. KONFIGURACJA URZĄDZENIA

a)	KONFIGURACJA URZĄDZENIA DO PRACY W SIECI
b)	KONTA ADMINISTRACYJNE / USTAWIENIA
3.	**INTEGRACJA Z FORTIGATE**
a)	PODŁĄCZENIE FG Z FAZ
b)	TRYBY PRACY / ZARZĄDZANIE ADOM
c)	ODCZYT LOGÓW / MOŻLIWOŚCI PERSONALIZACJI WIDOKU
4.	**ZARZĄDZANIE PRZECHOWYWANIEM DANYCH**
a)	POLITYKI LOGOWANIA / ANALIZA; ARCHIWUM
b)	FORWARDOWANIE; ROLOWANIE; BACKUP / LOGÓW
VIII.	**LOGOWANIE I ALERTOWANIE**
1.	**EFEKTYWNOŚĆ LOGOWANIA**
a)	JAK LOGOWAĆ / JAK ODCZYTYWAĆ LOGI
b)	FILTROWANIE LOGÓW / SZUKANIE ZDARZEŃ
c)	LOGI W CZASIE RZECZYWISTYM
2.	**ALERTY I FORTISOC**
a)	KONFIGURACJA I WYKRYWANIE ZDARZEŃ
b)	AUTOMATYZACJA POWIADOMIEŃ
c)	ANALIZA INCYDENTÓW
3.	**ZARZĄDZANIE PASMEM**
a)	TWORZENIE POLITYK
b)	TWORZENIE PROFILI
IX.	**RAPORTY**
1.	**TWORZENIE RAPORTÓW**
a)	KONFIGURACJA ZAKRESÓW / SZABLONÓW / MAKR RAPORTÓW
b)	PERSONALIZACJA / SPOLSZCZENIE WYGLĄDU
2.	**AUTOMATYZACJA**
a)	HARMONOGRAM RAPORTÓW
b)	DOSTARCZENIE NA ŻYCZENIE

Dlaczego warto?

Po szkoleniu uczestnicy będą potrafili:

- Wdrożyć i skonfigurować FortiAuthenticator
- Przeprowadzić integrację FortiAuthenticator z FortiGate oraz Active Directory pod kątem uwierzytelniania dwuskładnikowego
- Skonfigurować FortiAuthenticator do przewodowego i bezprzewodowego uwierzytelnienia 802.1x, uwierzytelnienia na podstawie adresów MAC
- Zablokować dostęp do stron w sieci za pomocą kilku metod.
- Stworzyć obiekty i grupy dla reguł firewall.
- Wdrożyć moduł antywirusowy w celu zabezpieczenia sieci przed szkodliwym oprogramowaniem.
- Skonfigurować moduł IPS i monitorować próby nieautoryzowanego dostępu.
- Sprawnie zarządzać dostępem do poszczególnych aplikacji (lokalnych, chmurowych oraz webowych).
- Skonfigurować połączenia SSL-VPN oraz IPsec-VPN dla bezpieczeństwa połączeń sieciowych.
- Wdrożyć uwierzytelnianie dwuetapowe dla użytkowników końcowych z wykorzystaniem FortiToken Mobile lub kodów wysyłanych na adres email.
- Zestawić tunel IPsec między 2 lokalizacjami/ urządzeniami dla bezpiecznej integracji sieci LAN to LAN (site to site).
- Wdrożyć FortiAnalyzer w swojej sieci lokalnej.
- Skonfigurować Fortianalyzer do wykrywania podatności oraz analizy logów.
- Skonfigurować domeny Administracyjne (ADOM) oraz zarządzać nimi.
- Wygenerować raport zdarzeń sieciowych z poszczególnych segmentów sieci.
- Stworzyć harmonogram raportów sieciowych w celu zachowania ciągłości informacji na temat zdarzeń w sieci.

- Skonfigurować moduł FortiSoc w celu analizy podatności sieci na ataki.
- Analizować zdarzenia wykryte przez moduł FortiSoC i umiejętnie na nie reagować.
- Przywrócić logi oraz ustawienia gdy urządzenie ulegnie awarii.

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 Roździeńskiego 2a

41-946 Piekary Śląskie

www.b-and-b.pl

biuro@b-and-b.pl