



## Cyberbezpieczeństwo i Administracja NGFW / UTM . 4 dniowe szkolenie stacjonarne dla administratorów sieci - WatchGuard Fireware Essentials.

Numer usługi 2025/12/09/146961/3202146

7 380,00 PLN brutto  
6 000,00 PLN netto  
230,63 PLN brutto/h  
187,50 PLN netto/h

NET COMPLEX  
SPÓŁKA Z  
OGRANICZONĄ  
ODPOWIEDZIALNOŚĆ  
CIĄ

Brak ocen dla tego dostawcy

📍 Bielsko-Biała  
🏢 Usługa szkoleniowa  
📄 stacjonarna  
🕒 32:00 h  
📅 24.11.2026 do 27.11.2026

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Administratorzy sieci, osoby odpowiedzialne za cyberbezpieczeństwo w przedsiębiorstwach

### Szkolenie stacjonarne WatchGuard Fireware Essentials (4 dni)

Profesjonalne, **autoryzowane szkolenie** prowadzone przez specjalistów Net Complex, dedykowane administratorom IT i osobom odpowiedzialnym za bezpieczeństwo sieci, które chcą zdobyć praktyczną wiedzę dot. konfiguracji i utrzymania urządzeń WatchGuard klasy UTM/NGFW.

### Czas trwania:

4 dni intensywnych zajęć (8 godzin dziennie), z bogatym programem praktycznym i teoretycznym

### Grupa docelowa usługi

### Co obejmuje:

- Konfiguracja i administracja Fireboxem oraz oprogramowaniem Fireware
- Zarządzanie politykami, usługami subskrypcyjnymi (Total Security, Basic, itp.)
- Monitorowanie, raportowanie, VPN, NAT, kontrola aplikacji i ochrona przed zagrożeniami

### W cenie szkolenia:

- Materiały szkoleniowe
- Gadżety
- Lunch i przerwy kawowe
- Certyfikat ukończenia (od autoryzowanego centrum szkoleniowego i Złotego Partnera WatchGuard - (Net Complex)

**Minimalna liczba uczestników**

2

<b>Maksymalna liczba uczestników</b>	7
<b>Data zakończenia rekrutacji</b>	17-11-2026
<b>Forma prowadzenia usługi</b>	stacjonarna
<b>Liczba godzin usługi</b>	32
<b>Podstawa uzyskania wpisu do BUR</b>	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

## Cel

### Cel edukacyjny

Poznanie struktury i funkcji WatchGuard Firebox

Praktyczne umiejętności w konfiguracji zapory sieciowej, usług bezpieczeństwa, VPN i uwierzytelniania użytkowników. Wiedza z zakresu zaawansowanych zabezpieczeń (APT Blocker, WebBlocker, HTTPS Proxy, Intelligent AV, DNS WatchGuard).

Możliwość zdobycia międzynarodowego certyfikatu producenta – WatchGuard Firewall Essentials (egzamin online).

Uczestnik po ukończeniu szkolenia potrafi skutecznie zarządzać bezpieczeństwem sieci

### Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi skonfigurować urządzenie WatchGuard Firebox	Poprawnie skonfigurowane środowisko testowe w laboratorium szkoleniowym	Obserwacja w warunkach rzeczywistych
Uczestnik rozpoznaje i wdraża polityki bezpieczeństwa oraz potrafi zarządzać regułami ruchu sieciowego	Samodzielne utworzenie i wdrożenie reguł polityk filtrowania	Obserwacja w warunkach rzeczywistych
Uczestnik zna mechanizmy UTM i umie zarządzać bezpieczeństwem (IPS, AV, APT, web filtering)	Dostosowanie konsoli zarządzania	Obserwacja w warunkach rzeczywistych

## Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

## Program

### Dzień I

- Administracja. Konfiguracja i zarządzanie Firebox (NTP i SNMP; Podstawy zasad zapory...),
- Wykrywanie zagrożeń (Default Handling Packet; blokowanie adresów IP i portów; rodzaje ochrony przed zagrożeniami),
- Logowanie i monitorowanie - WatchGuard Dimension (WatchGuard Cloud; Raporty Dimension; Fireware Web UI).

### Dzień II

- Ustawienia sieciowe (DNS, aliasy, sieci VLAN, Multi-Wan, SD-WAN, Quality of Service (QoS)NAT'owanie:
  1. Formy NAT'a dostępne w Firebox'ie,
  2. Dynamic NAT – co to jest i jak skonfigurować?
  3. Użyj Static NAT do ochrony Twoich publicznych serwerów,
  4. NAT 1-do-1.

### Dzień III

- Reguły Zapory Sieciowej (Policy Manager; konfiguracja; ustawianie),
- Usługi bezpieczeństwa - Fireware Web UI,
- Reguły Zapory Sieciowej w trybie Proxy (DNS; serwer DNS; serwer Proxy; APT Blocker; VoIP; proxy SMTP, IMAP i POP3; WebBlocker oraz proxy HTTP i HTTPS; Zasady HTTPS-proxy 187; E-mail Proxy i blokowanie spamu; Ustawienia URL filtering; Instalacja i konfigurowanie modułów).

### Dzień IV

- Autoryzacja użytkowników (uwierzytelnianie; typy; grupy; niestandardowy certyfikat web server),
- Mobilny VPN (VPN z IKEv2; VPN z SSL; VPN z L2TP; VPN z IPSec),
- Branch Office VPN - Łączenie lokalizacji tunelem VPN:
  1. Wprowadzenie do BOVPN,
  2. Jak działa BranchOffice VPN?
  3. Topologia VPN,
  4. Typy BOVPN,
  5. Różnice między typami BOVPN,
  6. Algorytmy i protokoły IPSec VPN,
  7. Zasady ruchu VPN,
  8. Jak skonfigurować ręcznie BOVPN między dwoma Firebox'ami,
  9. BOVPN i NAT,
  10. BOVPN i dynamiczne publiczne adresy IP,
  11. BOVPN przez TLS,
  12. Topologie BOVPN,
  13. Rozwiązywanie problemów z tunelami BOVPN.

## Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 380,00 PLN
Koszt przypadający na 1 uczestnika netto	6 000,00 PLN
Koszt osobogodziny brutto	230,63 PLN
Koszt osobogodziny netto	187,50 PLN

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Piotr Mrowiec

Piotr Mrowiec to certyfikowany inżynier i trener WatchGuard, specjalizujący się w cyberbezpieczeństwie, zwłaszcza w obszarze uwierzytelniania wieloskładnikowego (MFA), firewalli oraz ochrony tożsamości użytkowników. Na co dzień prowadzi szkolenia i webinaria dla klientów Net Complex, w których dzieli się wiedzą o praktycznych aspektach zabezpieczania sieci firmowych. Występował m.in. podczas Kongresu Bezpieczeństwa Sieci, gdzie omawiał różnice między incydemem a naruszeniem oraz rolę MFA w ochronie organizacji. Jako ekspert podkreśla znaczenie edukacji, audytów i świadomego podejścia do zagrożeń - łącząc doświadczenie techniczne z umiejętnością przekazywania wiedzy.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

+ DODATKOWO WYKRACZAMY POZA STANDARDOWY PROGRAM PORUSZAJĄC WYBRANE ZAGADNIENIA:

- Deep Inspection - certyfikat https,
- Traffic Shaping,
- Multi-WAN + SD-WAN.

Omawiamy też najnowsze, stale aktualizowane funkcjonalności WatchGuard:

- DNS WatchGuard,
- Intelligent AV,
- Access Portal,
- AuthPoint.

**DODATKOWO:**

- kontakt z trenerem po realizacji
- dostęp do zamkniętej społeczności SLACK dla administratorów sieci

## Adres

ul. Wita Stwosza 5  
43-300 Bielsko-Biała  
woj. śląskie

## Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe
- Bezpłatny parking, wspólna integracja, przerwy kawowe i lunch

## Kontakt



**Karolina Błasiak**

**E-mail** [k.blasiak@netcomplex.pl](mailto:k.blasiak@netcomplex.pl)

**Telefon** (+48) 798 396 359