Szkolenie Fireware Essentials & Network Security Essentials

SZKOLENIE DOTYCZĄCE KONFIGURACJI I ADMINISTRACJI ROZWIĄZANIAMI KLASY UTM WATCHGUARD

Nasi szkoleniowcy to nie tylko trenerzy, ale przede wszystkim **certyfikowani inżynierowie**, którzy na co dzień pracują przy wdrożeniach, w złożonych środowiskach u klientów.

NET COMPLEX
Bezpieczeństwo IT

WatchGuard

Dla kogo:

- Menedżerów różnych szczebli zarządzania IT,
- Administratorów i architektów sieci,
- Specjalistów IT,
- Menedżerów i specjalistów spoza obszaru IT.

Korzyści:

- Osoby uczestniczące w szkoleniu otrzymują darmowe materiały szkoleniowe: Przewodnik "Fireware Essentials Student Guide".
- Certyfikat ukończenia szkolenia od autoryzowanego partnera szkoleniowego WatchGuard.

Czas trwania:

- 4 dni x 8 godzin

Cena:

- 3990 zł netto

Cena zawiera:

- szkolenie
- pakiet materiałów szkoleniowych
- gadżety
- lunch, przerwy kawowe
- certyfikat autoryzowanego partnera WatchGuard

NET COMPLEX
Bezpieczeństwo IT

WatchGuard

Program szkolenia

I dzień

Administracja. Konfiguracja i zarządzanie Firebox

- Otwieranie i zapisywanie plików konfiguracyjnych;
- Konfigurowanie Fireboxa pod zdalną administrację;
- Dodawanie kluczy licencyjnych;
- Backup i przywracanie konfiguracji urządzenia;
- Dodawanie Firebox identification information.
- Aktualizacja systemu operacyjnego Fireware
- Domyślna ochrona przed zagrożeniami
- Ustawienia globalne, NTP i SNMP
- Podstawy zasad zapory

Wykrywanie zagrożeń

- Różne rodzaje ochrony przed zagrożeniami dostępne w Firebox'ie;
- Default Handling Packet – do czego służy?;
- Blokowanie adresów IP i portów używanych przez hackerów do atakowania sieci;
- Automatyczne blokowanie adresów IP, które generują podejrzany ruch

Logowanie i monitorowanie - WatchGuard Dimension

- Logowanie i wysyłanie powiadomień
- Konfiguracja Firebox'a do wysyłania wiadomości o logach;
- Widoczność Firebox dzięki WatchGuard Cloud
- Konfiguracja Dimension do rejestrowania w Firebox
- Logowanie do Dimension
- Monitorowanie za pomocą Firebox System Manager
- Monitorowanie za pomocą interfejsu Fireware Web UI
- Jak czytać komunikaty w dzienniku ruchu?
- Użycie Dimension do wyszukiwania logów;
- Raporty Dimension;
- Exportowanie raportów z Dimension do pliku CSV or PDF;
- Generowanie i zapisywanie raportów w regularnych odstępach czasu;
- Zmiana ustawień raportowania, zapisywanie i drukowanie raportów.

Program szkolenia

II dzień

Ustawienia sieciowe

- Konfigurowanie zewnętrznych interfejsów sieciowych za pomocą statycznego adresu IP, DHCP czy PPPoE;
- Konfigurowanie zaufanych i opcjonalnych interfejsów sieciowych;
- Używanie Fireboxa jako serwera DHCP;
- Dodawanie lokalizacji serwerów WINS / DNS do konfiguracji Firebox.
- Tryby routingu sieciowego
- DNS
- Typy interfejsów i aliasy
- Secondary network – obsługa podsieci w ramach jednego interfejsu
- sieci VLAN - ustawianie i działanie vLan
- Multi-WAN - Przełączanie awaryjne Multi-WAN
- Przepełnienie interfejsu Multi-WAN
- interfejsu Multi-WAN
- SD-WAN
- Static Routing
- Traffic Management
- Link Monitor
- Quality of Service (QoS)

NAT'owanie

- Formy NAT'a dostępne w Firebox'ie;
- Dynamic NAT – co to jest i jak skonfigurować?;
- Użyj Static NAT do ochrony Twoich publicznych serwerów.
- NAT 1-do-1

Program szkolenia

III dzień

Reguły Zapory Sieciowej

- Różnice między filtrem pakietów a polityką proxy;
- Dodawanie polityk do Policy Manager i konfigurowanie własnych zasad dostępu;
- Reguły zapory sieciowej
- Tworzenie niestandardowego pakietu filtrów;
- Użycie zaawansowanych właściwości polityk;
- Jak poprawnie ustawić kolejność reguł.

Usługi bezpieczeństwa - Fireware Web UI

- Przegląd usług bezpieczeństwa
- Globalnie skonfigurowane usługi bezpieczeństwa Web UI
- Usługa zapobiegania włamaniom
- Kontrola aplikacji
- Omówienie interfejsu Web UI
- Nawiązanie połączenia z Web UI i logowanie
- Nawigacja i zarządzenie Web UI
- Blokowanie połączeń z wybranych krajów z wykorzystaniem geolokalizacji
- Blokowanie połączeń z wybranych adresów IP

Program szkolenia

Reguły Zapory Sieciowej w trybie Proxy

- Cele polityk proxy;
- Konfigurowanie proxy DNS, aby chronić serwer DNS;
- Zapobieganie utracie danych
- Serwer Proxy
- Uniemożliwienie użytkownikom wysyłania plików na zewnętrzny serwer FTP.
- Serwer proxy
- Skanowanie antywirusowe i proxy
- APT Blocker
- VoIP
- Serwery proxy SMTP, IMAP i POP3
- Zasady HTTP-proxy i akcje proxy
- WebBlocker oraz proxy HTTP i HTTPS
- Zasady HTTPS-proxy 187
- Akcje zawartości i akcje routingu

E-mail Proxy i blokowanie spamu

- Ograniczenie rodzajów połączeń do serwera SMTP;
- Modyfikacja dopuszczalnego rozmiaru wiadomości;
- Blokowanie i zezwalanie - wg treści i nazw plików;
- Filtrowanie maili wg nazwy załącznika;
- Kontrolowanie ruchu POP3 i blokowanie załączników;
- Aktywacja i konfiguracja spam Blocker'a;
- Określanie podejmowanych działań w razie wykrycia spamu;
- Wykluczanie wiadomości z określonych źródeł;
- Monitorowanie aktywności spam Blocker’a.

Program szkolenia

Ustawienia URL filteringu

- Blokowanie ruchu HTTP na podstawie adresu URL;
- Zezwalanie na pobieranie plików na podstawie ich rodzaju;
- Dostosowywnie komunikatu blokowania do swoich potrzeb;
- Konfigurowanie wyjątków dla źródła aktualizacji przez HTTP-Proxy;
- Ustawianie ograniczeń czasowych i transmisji danych do przeglądania stron www;
- Aktywacja Web Blocker'a;
- Konfiguracja profilów Web Blocker`a;
- Dodawanie wyjątków;
- RED – co to jest i jak działa?; konfiguracja Reputation Enabled Defense.

Instalacja i konfigurowanie modułów

- Jak działają sygnatury i jak chronią Twoją sieć;
- Instalacja i konfigurowanie Gateway AntiVirus;
- Instalacja i konfigurowanie APTBlocker;
- Instalacja i konfigurowanie Data Loss Prevention;
- Instalacja i konfigurowanie the Intrusion Prevention Service;
- Instalacja i konfigurowanie Application Control;
- Instalacja i konfigurowanie Botnet Detection.

Program szkolenia

IV dzień

Autoryzacja użytkowników

- Uwierzytelnianie - jak działa z Firebox'em;
- Jakie typy uwierzytelniania możemy zastosować?;
- Używanie Fireboxa do uwierzytelnienia użytkowników i grup;
- Modyfikowanie limitów czasowych sesji użytkownika;
- Użyj Firebox'a by stworzyć niestandardowy certyfikat web server.
- Korzyści i wady każdego obsługiwanego typu uwierzytelnienia
- Portal uwierzytelniania Firebox

Mobilny VPN

- Mobilny VPN - wprowadzenie
- Wybieranie właściwych dla twojej sieci mobilnych VPN (Virtual Private Network);
- Mobilna sieć VPN z IKEv2
- Mobilna sieć VPN z SSL
- Mobilna sieć VPN z L2TP
- Mobilna sieć VPN z IPSec
- Skonfiguruj Firebox w celu umożliwienia połączeń mobilnych VPN;
- Generowanie plików konfiguracyjnych dla użytkowników Mobile VPN;
- Instalowanie i korzystanie z klienta mobile VPN na zdalnym urządzeniu

Program szkolenia

Branch Office VPN - Łączenie lokalizacji tunelem VPN

- Wprowadzenie do BOVPN
- Jak działa BranchOffice VPN?;
- Topologia VPN
- Typy BOVPN
- Różnice między typami BOVPN;
- Algorytmy i protokoły IPSec VPN
- Zasady ruchu VPN
- Jak skonfigurować ręcznie BOVPN między dwoma Firebox'ami.
- BOVPN i NAT
- BOVPN i dynamiczne publiczne adresy IP
- BOVPN przez TLS
- Topologie BOVPN
- Rozwiązywanie problemów z tunelami BOVPN

Jesteśmy certyfikowanym Centrum Szkoleniowym WatchGuard w Polsce!

WatchGuard Certified Training Partner

Net Complex Sp. z o.o.

ul. Wita Stwosza 5, Bielsko-Biała

Dodatkowe pytania prosimy kierować na adres e-mail:
training@netcomplex.pl;
lub bezpośrednio do osoby, która jest Państwa opiekunem handlowym.
Tel.: 33 816 04 11 / 33 472 03 18