WatchGuard Fireware - podstawy

Szkolenie dotyczące konfiguracji i administracji rozwiązaniami klasy UTM WatchGuard

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

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 producenta: „Fireware Essentials Student Guide".
· Certyfikat ukończenia szkolenia od autoryzowanego partnera szkoleniowego WatchGuard.

Czas trwania:

3 dni x 8 godzin

Cena:

2990 zł netto

cena zawiera:
· szkolenie
· pakiet materiałów szkoleniowych, gadżety
· lunch, przerwy kawowe
· certyfikat autoryzowanego partnera WatchGuard

Organizator: Net Complex Sp. z o.o., ul. Cieszyńska 79, 43-300 Bielsko-Biała, NIP: 5472165461. Autoryzowany partner szkoleniowy firmy WatchGuard.

Program szkolenia

I dzień

Administracja

· Otwieranie i zapisywanie plików konfiguracyjnych;
· Konfigurowanie Fireboxa pod zdalną administrację;
· Dodawanie kluczy licencyjnych;
· Backup i przywracanie konfiguracji urządzenia;
· Dodawanie Firebox identification information.

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.

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.

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.

Dzień II

Reguły Zapory Sieciowej

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

Reguły Zapory Sieciowej w trybie Proxy
· Cele polityk proxy;
· Konfigurowanie proxy DNS, aby chronić serwer DNS;
· Uniemożliwienie użytkownikom wysyłania plików na zewnętrzny serwer FTP.

Email 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.

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.

Dzień III

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.

Dimension
· Konfiguracja Firebox'a do wysyłania wiadomości o logach;
· 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.

Łączenie lokalizacji w tunelu VPN
· Jak działa BranchOffice VPN?;
· Różnice między typami BOVPN;
· Jak skonfigurować ręcznie BOVPN między dwoma Firebox'ami.

Mobilny VPN
· Wybieranie właściwych dla twojej sieci mobilnych VPN (virtual private network);
· 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.

Wszelkie informacje dotyczące szkoleń dostępne są na stronie internetowej www.netcomplex.pl - w zakładce Szkolenia.

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

Net Complex.
Chronimy Sferę It. Skuteczniej.

NET COMPLEX Bezpieczeństwo IT
Net Complex Sp. z o.o.
ul. Cieszyńska 79
43-300 Bielsko-Biała
tel. 33 472 03 18 | 33 816 04 11
faks: 33 486 70 02 | kom.: 506 872 270
e-mail: netcomplex.@netcomplex.pl
www.netcomplex.pl
NIP: 5472165461 REGON: 365444659
Bank ING: 37 1050 1070 1000 0090 3104 7385