

Szkolenie z zakresu UTM FORTINET

PROGRAM SZKOLENIA FortiGate - Administracja

Dzień 1

1. Systemy FortiGate Unified Threat Management – Wprowadzenie
2. Wstępna konfiguracja systemu
 - połączenie za pomocą Command Line Interface (CLI)
 - połączenie za pomocą GUI
 - konfiguracja połączeń sieciowych
3. Ustawienia systemowe i administracyjne
 - konfiguracja globalnych ustawień systemowych
 - konfiguracja użytkowników typu administrator
 - włączenie serwisów FortiGuard i automatycznych aktualizacji
4. Logowanie i monitoring
 - eksport danych z GUI Monitoring
 - konfiguracja logowania dla zdarzeń systemowych
 - rejestracja i konfiguracja FortiAnalyze'a
 - konfiguracja alertów mailowych
5. Polityka zapory ogniowej – podstawy
 - tworzenie obiektów dla reguł zapory ogniowej
 - tworzenie przykładowej polityki zapory ogniowej
 - testowanie polityki zapory ogniowej
6. Polityka zapory ogniowej - dodatkowe opcje
 - reguły uwierzytelniające użytkowników
 - dodatkowa informacja podczas uwierzytelniania i przekierowywanie URL
 - konfiguracja dostępu opartego o Virtual IP (DNAT)
 - tworzenie IP Pool (SNAT)
 - zarządzanie pasmem i priorytety
7. Połączenia SSL VPN i PPTP
 - ustawienia SSL VPN
 - konfiguracja reguł zapory ogniowej dla SSL VPN
 - testowanie konfiguracji SSL VPN
 - PPTP VPN
8. Skanowanie antywirusowe
 - globalne ustawienia modułu AV
 - konfiguracja profili ochrony (ang. Protection Profile)
 - testowanie profile ochrony dla skanowania AV
 - detekcja wirusów w przesyłkach pocztowych
9. Filtracja Antyspamowa
 - konfiguracja serwisu FortiGuard-AntiSpam
 - konfiguracja funkcjonalności Banned Word Filtering
 - skanowanie AV i filtrowanie spamu
10. Filtr Webowy
 - konfiguracja lokalnych Web URL i filtrowanie po zawartości stron
 - testowanie filtrowania po kategoriach

Dzień 2

1. Bieżąca obsługa, tryb transparentny i filtrowanie aplikacji IM/P2P
 - odtwarzanie konfiguracji systemu
 - zmiana trybu pracy (praca w trybie transparentnym)
 - filtrowanie aplikacji IM/P2P
2. Diagnostyka w systemach FortiOS
 - sniffowanie pakietów
 - podglądanie tablicy sesji
 - tryb debugowania
3. Wirtualne domeny i routing typu Inter-VDOM
 - zarządzanie VDOM'ami
 - konfiguracja VDOM'ów i testowanie połączeń typu Inter-VDOM
4. Routing statyczny i oparty o polityki (Policy Routing)
 - funkcjonalność Dead Gateway Detection (DGD)
 - dodawanie reguł dla Policy Routes i wpisów do statycznego routingu
 - weryfikowanie i testowanie routing
5. System przeciwdziałania włamaniom (IPS - Intrusion Prevention System)
 - sygnatury IPS
 - anomalie IPS
6. Autentykacja
7. Połączenia IPsec VPN
 - a) Połączenia IPsec VPN oparte o routing
 - konfiguracja interfejsów IPsec i polityk VPN'owych
 - konfiguracja redundantnych połączeń VPN
 - konfiguracja dynamicznego routingu opartego na OSPF
 - testowanie połączeń VPN i konfiguracji OSPF
 - b) Połączenia IPsec VPN oparte o politykę zapory ogniowej
 - konfiguracja serwera DHCP dla zdalnych użytkowników
 - konfiguracja połączenia IPsec VPN typu zdalny dostęp
 - funkcja Internet Browsing
 - konfiguracja oprogramowania typu klient FortiClient