**Szkolenie – UTM/NGFW**

**Szkolenie**

1. Szkolenie podstawowe (wdrożeniowe) – odbywające się przy okazji wdrożenia i konfiguracji urządzeń UTM/NGFW w siedzibie Zamawiającego.
2. Szkolenie z zakresu wdrożonych urządzeń UTM/NGFW, dla **3** **osób**, średniozaawansowanych i zaawansowanych (wcześniej pracujących na urządzeniach), minimum 3 dniowe, maksymalnie 5 dniowe, obejmujące cały niżej wymieniony zakres materiału szkoleniowego, prowadzone przez certyfikowanego (z administracji dostarczonych urządzeń UTM/NGFW) inżyniera lub trenera.

Szkolenie musi zawierać elementy warsztatowe i opierać się na zadaniach praktycznych realizowanych w przygotowanym labie z urządzeniami UTM/NGFW. Szkolenie musi być prowadzone na wersji firmware zastosowanej podczas wdrożenia na urządzeniach Zamawiającego. Szkolenie musi być prowadzone przez praktyka posiadającego co najmniej 3-letnie doświadczenie w zakresie wdrażania zaproponowanymi urządzeniami UTM/NGFW oraz ważny certyfikat inżynierski wystawiony przez Producenta.

Wykonawca pokryje koszty zakwaterowania i pełnego wyżywienia (śniadanie, obiad, kolacja). Zamawiający pokrywa koszty dojazdu swoich pracowników. W przypadku miejsca szkolenia, gdzie łączny czas dojazdu PKP/PKS/MZK jest dłuższy niż 1 godzina (od siedziby Zamawiającego), Wykonawca pokryje koszty zakwaterowania w dniu poprzedzającym szkolenie. Zakwaterowanie w hotelu (co najmniej trzygwiazdkowym) nie może być oddalone od miejsca szkolenia więcej niż 15 minut pieszo.

Szkolenie powinno zostać zrealizowane w jednym terminie dla 3 osób. Termin szkoleń Wykonawca musi ustalić z Zamawiającym, w taki sposób aby nie kolidowało z wdrożeniem.

Zakres szkolenia powinien zawierać elementy:

* Wprowadzenie do urządzeń UTM/NGFW i podstawowa konfiguracja:
	+ Opis urządzeń i zastosowanej technologii,
	+ Tryby pracy NAT/Transparent,
	+ Konfiguracja sieci i routingu,
	+ SD-WAN - Load Balancing oraz redundancja łącz Internetowych,
	+ System Dashboard i moduły systemu,
	+ Administracja urządzeniem (WWW, CLI),
	+ Wirtualizacja VDOM,
* Polityki zapory sieciowej:
	+ Koncepcja firewall w urządzeniach UTM/NGFW,
	+ Tworzenie obiektów dla reguł firewall,
	+ Translacja adresów NAT i Virtual IP,
	+ Internet Service Database,
* Inspekcja ruchu SSL i metody dystrybucji certyfikatów,
* Omówienie trybów pracy urządzenia – Proxy i Flow,
* Logowanie i powiadomienia. Konfiguracja przekazywania logów do FortiAnalyzera. Obsługa FortiAnalyzer:
	+ Dodawanie urządzeń,
	+ Bezpieczna komunikacja,
	+ Zarządzanie logami i archiwizacja,
	+ Backup i przywracanie po awarii,
	+ Aktualizacja firmware,
	+ Zarządzanie dyskiem,
	+ Konfiguracja syslog. Parsowanie logów syslog (Windows Server i Linux),
	+ Przeglądanie logów i mechanizmy wyszukiwania,
	+ Integralność logów,
	+ Fetcher Management,
	+ FortiSOC: Indicator of Compromise, Event Handlers, Outbreak Alerts, Playbooks,
	+ Projektowanie i przeglądanie raportów. Dataset – zapytania do bazy danych,
* Wykorzystanie FortiCloud i FortiView,
* Konfiguracja funkcji ochronnych (profile bezpieczeństwa):
	+ Ochrona antywirusowa i integracja z FortiSandbox,
	+ Content Disarm and Reconstruction,
	+ Filtrowanie antyspamowe,
	+ System IPS / DoS Policy,
	+ Kontrola ruchu WWW / blokowanie URL / DNS Filter,
	+ Kontrola aplikacji,
	+ Reputacja klienta,
	+ Data Leakage Prevention (DLP),
	+ Web Application Firewall (WAF),
	+ Zabezpieczanie poprzez DNS Filter i Fabric Connectors,
* Uwierzytelnianie użytkowników. Integracja z usługami katalogowymi w oparciu o FSSO:
	+ Tworzenie reguł firewall w oparciu o grupy użytkowników,
	+ Konta użytkowników gości,
	+ Dwuskładnikowa autoryzacja – FortiToken,
* Konfiguracja rozwiązania dwuskładnikowego uwierzytelniania FortiToken i zabezpieczanie dostępu do usług,
* Konfiguracja protokołu 802.1x,
* Optymalizacja ruchu sieciowego (kształtowanie pasma),
* Konfiguracja połączeń VPN – IPSec VPN i SSL VPN, VXLAN, ADVPN,
* Konfiguracja FortiClient do bezpiecznego łączenia z siecią FortiGate poprzez VPN, wykorzystanie modułów AV, integracja z FortiGate,
* Diagnostyka i rozwiązywanie problemów FortiGate i FortiAnalyzer. Troubleshooting – rozwiązywanie problemów:
	+ Analiza logów (na urządzeniu i na FortiAnalyzer),
	+ Możliwości CLI,
	+ Sniffer/Packet Capture,
	+ Debug Flow,
	+ Diagnostyka i rozwiązywanie problemów z VPN, Firewall, routingu, FSSO.
* Konserwacja i bieżąca obsługa systemu. Aktualizacja urządzeń UTM/NGFW.
* Dobre praktyki – co i jak koniecznie należy skonfigurować na urządzeniach UTM/NGFW w celu zwiększenia bezpieczeństwa sieci LAN.