Załącznik nr 2a do zaproszenia
Szczegółowy opis przedmiotu zamówienia – cz. 1

Część 1 – urządzenia UTM

Przedmiotem zamówienia jest dostawa fabrycznie nowych urządzeń sieciowych na potrzeby Głównego Urzędu Geodezji i Kartografii. Dostarczone urządzenia są rozbudową istniejącej infrastruktury sieciowej opartej o urządzenia Fortinet.

Urządzenie do kompleksowej ochrony sieci (UTM) – 2szt.:

Fortigate 201E Hardware + 3 Year Hardware plus 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP) PN: FG-201E-BDL-950-36 lub równoważne, urządzenie musi spełniać następujące minimalne wymagania:

Lp	Minimalne parametry
1.	Dostarczone urządzenia muszą umożliwiać ich montaż w szafie rack 19". Wraz z urządzeniami wykonawca dostarczy wszystkie niezbędne elementy do montażu w szafie rack 19". Za pomocą dostarczonych urządzeń będzie można zbudować klaster HA - Active-Active lub Active-Passive. Dostarczone urządzenia muszą być w pełni kompatybilne z urządzeniem do zapisywania zdarzeń, analizy danych oraz raportowania FortiAnalyzer-200F.
2.	1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 2. Monitoring stanu realizowanych połączeń VPN. 3. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. 4. System realizujący funkcję Firewall musi dysponować minimum 2 portami WAN 1Gbps, 14 portami Ethernet 1Gbps , 4 gniazdami SFP 1Gbps, 2 portami 1Gbps HA/Management oraz dedykowanym złączem konsoli. 5. Urządzenie musi posiadać wbudowany wewnętrzny dysk SSD o pojemności min. 480 GB. 6. System musi umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 7. W zakresie Firewall'a obsługa nie mniej niż 2 milionów jednoczesnych połączeń oraz 135 tys. nowych połączeń na sekundę. 8. Przepustowość Firewall'a: nie mniej niż 20 Gbps UDP packets / 13,5 Mpps 9. Wydajność szyfrowania VPN IPSec nie mniej niż 7,2 Gbps, SSL VPN nie mniej niż 900MBps. 10. Możliwość pracy jako kontroler sieci WiFi oraz zarządzania dedykowanymi punktami dostępowymi, minimalna ilość obsługiwanych AP – 128szt. 11. System musi mieć możliwość logowania i raportowania do dedykowanego urządzenia. 12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji:

	a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection b. Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN d. Ochrona przed atakami - Intrusion Prevention System e. Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. f. Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP g. Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej wielkości pasma h. Kontrola aplikacji – system musi rozpoznawać aplikacje typu: P2P, botnet (C&C) i. Możliwość analizy ruchu szyfrowanego protokołem SSL j. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) k. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 2,2 Gbps 14. Wydajność skanowania ruchu z włączoną funkcją Antywirus - minimum 1,2 Gbps 15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: a. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site b. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności c. Praca w topologii Hub and Spoke oraz Mesh d. Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF e. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth 16. W ramach funkcji IPSec VPN, SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 18. Możliwość budowy minimum 10 oddzielnych (logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a. 19. Translacja adresów NAT adresu źródłowego i docelowego. 20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci. 21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ 22. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) 23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Ponadto administrator systemu musi mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. 24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP

	25. Baza filtra WWW w pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator musi mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW. 26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. 27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu b. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP c. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory 28. Funkcja kontrolera sieci bezprzewodowej WiFi: a. Centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM) b. Przepustowość dla sieci WiFi nie mniejsza niż 40Gb/s c. Obsługa minimim 128 punktów dostępowych d. Elastyczne mechanizmy QoS dla sieci WiFi w tym możliwość definiowania parametrów usług per punkt dostępowy/SSID/klient sieci WiFi e. Zarządzanie pasmem radiowym punktów dostępowych: i. automatyczna adaptacja do zmian w czasie rzeczywistym ii. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia) iii. dynamiczne przydzielanie kanałów radiowych iv. wykrywanie, eliminacja i unikanie interferencji v. równoważenie obciążenia punktów dostępowych vi. automatyczna dystrybucja klientów pomiędzy punkty dostępowe f. Mapowanie SSID do segmentów VLAN w sieci przewodowej i. 1:1 ii. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty) iii. tunelowanie ruchu klientów do kontrolera g. Obsługa mechanizmów bezpieczeństwa: i. 802.11i, WPA2, WPA ii. 802.1X z EAP (PEAP, EAP-TLS, EAP-FAST) iii. możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID iv. możliwość profilowania użytkowników: 1. przydział sieci VLAN 2. przydział list kontroli dostępu (ACL)

	v. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509 vi. ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników h. Obsługa ruchu unicast i multicast IPv4: i. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym) ii. obsługa konwersji ruchu multicast do unicast i. Obsługa mobilności (roamingu) użytkowników (L2 i L3) j. Obsługa mechanizmów QoS: i. 802.1p, WMM, TSpec ii. ograniczanie pasma per użytkownik iii. Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu k. Obsługa dostępu gościnnego: i. przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony) ii. możliwość kreowania użytkowników z określeniem czasu ważności konta l. Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne oraz usługi bezpieczeństwa 29. Możliwość analizy ruchu pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji w warstwie 7 30. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: a. ICSA lub EAL4 dla funkcji Firewall b. ICSA lub NSS Labs dla funkcji IPS c. ICSA dla funkcji: SSL VPN, IPSec VPN d. ICSA dla funkcji Anti-Malware. 31. Systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3.	W ramach zamówienia Wykonawca dostarczy licencje aktywacyjne dla wszystkich wymienionych funkcjonalności, uprawniające do używania ww. funkcji oraz pobierania aktualizacji baz zabezpieczeń minimum w okresie gwarancji.
4.	1. Gwarancja na bazie świadczenia gwarancyjnego producenta sprzętu przez okres minimum 36 miesięcy. Wykonawca zapewnia, że dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji producenta sprzętu. Z dostawą sprzętu Wykonawca zobowiązuje się dostarczyć dokument wydany przez producenta lub jego polskiego przedstawiciela, potwierdzający że sprzęt jest nowy (potwierdzająca data produkcji), pochodzi z oficjalnego kanału dystrybucji, pochodzi z bieżącej produkcji i objęty jest wsparciem serwisowym producenta. 2. Okres gwarancji rozpoczyna się od daty podpisania protokołu odbioru końcowego. 3. Serwis gwarancyjny świadczony w miejscu instalacji sprzętu.

	4. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) w ciągu 1dnia roboczego od momentu zgłoszenia usterki w trybie 8x5xNBD. 5. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. 6. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.

Dodatkowe wymagania przedmiotowe:

a. Podmiot, który będzie świadczył serwis gwarancyjny urządzeń musi posiadać autoryzację producenta urządzeń – dokument potwierdzający spełnianie wymogu należy załączyć do oferty; dokument musi zawierać nazwę (firmę) podmiotu świadczącego serwis gwarancyjny urządzeń,
b. Oferując rozwiązanie równoważne do rozwiązania wskazanego przez Zamawiającego, Wykonawca zobowiązany jest wykazać, że rozwiązanie równoważne spełnia wszystkie wymagania, przy zachowaniu cech technicznych, funkcjonalnych i jakościowych urządzenia. Przez wykazanie równoważności Zamawiający rozumie wykonanie stosownych porównań i analiz, których wyniki należy załączyć do oferty. Zamawiający wymaga dostarczenia urządzeń w postaci komercyjnych platform sprzętowych.
c. Wykonawca dostarczy sprzęt będący przedmiotem zamówienia do siedziby Zamawiającego pod adresem: Główny Urząd Geodezji i Kartografii, ul. Jana Olbrachta 94b, 01-102 Warszawa