PRZEDMIOTEM ZAMÓWIENIA JEST:

1. Dostawa 2 szt. urządzeń zabezpieczeń firewall zgodnie ze specyfikacją opisaną w załączniku nr 1 w rozdziale I;
2. Świadczenie usługi asysty technicznej eksperta, o których mowa w załączniku nr 1 w rozdziale II;
3. Zorganizowanie i przeprowadzenie warsztatów szkoleniowych, o których mowa w rozdziale III.

TERMIN WYKONANIA ZAMÓWIENIA:

1. Wykonawca zobowiązany jest dostarczyć Urządzenia jednorazowo, nie później niż w ciągu 30 dni od daty zawarcia Umowy. Urządzenie uznaje się za dostarczone z chwilą potwierdzenia pozytywnej weryfikacji ilościowej przez Zamawiającego.
2. Uruchomienie oraz konfiguracja Urządzeń muszą zostać wykonane w ciągu 90 dni od dnia dostarczenia Urządzeń, w godzinach pracy urzędowania Administratora Systemów Informatycznych w OEIiZK.
3. Termin realizacji usługi asysty technicznej obejmuje okres od daty zawarcia umowy do upływu 30 dni od daty zakończenia wdrożenia Urządzeń.
4. Usługi szkoleniowe zostaną zorganizowane w ciągu 12 miesięcy od daty zawarcia Umowy, w terminach uzgodnionych w trybie roboczym po zawarciu Umowy.

OPIS PRZEDMIOTU UMOWY

I. Wykonawca musi dostarczyć i wdrożyć 2 sztuki systemów zabezpieczeń firewall pod adresami:
- ul. Raszyńska 8/10, 02-026 Warszawa
- ul. Nowogrodzka 73, 02-006 Warszawa

Dokładny opis wymagań dla pojedynczego systemu znajduje się poniżej:

1. System typu NGFW musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). Całość sprzętu i oprogramowania musi być wspierana przez tego samego producenta.
2. Urządzenie musi zapewniać takie funkcje jak:
    a) firewall z włączoną funkcją kontroli aplikacji (NGFW),
    b) inspekcję pakietów na poziomie aplikacji (DPI),
    c) wykrywanie i blokowanie prób ataków (IPS/IDS),
    d) ochrona przed złośliwym oprogramowaniem (anty-wirus, anty-malware, anty-spyware),
    e) analiza i kontrola szyfrowanego ruchu sieciowego SSL/TLS (SSL Inspection),
    f) zarządzanie pasmem i przydzielanie zasobów sieciowych określonym aplikacjom (QoS),
    g) możliwość integracji z systemami typu Threat Intelligence,
    h) mechanizmy monitorowania i reagowania w czasie rzeczywistym na zagrożenia występujące na urządzeniach końcowych (EDR),
    i) monitorowanie i automatyczne reagowanie na zaistniałe incydenty w ruchu sieciowym (XDR),
    j) filtrowanie treści internetowych na podstawie określonych kryteriów tj. określone kategorie, określone adresy URL, określone słowa kluczowe lub analiza reputacji stron internetowych (Web filtering),
    k) filtrowanie ruchu DNS i blokowanie dostępu do złośliwych domen (DNS filtering)
    l) filtrowanie ruchu SMTP, POP3 i IMAP z możliwością wykrywania i blokowania takich zagrożeń jak spam, phishing lub złośliwe załączniki,
    m) możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive oraz Active-Active

3. Urządzenie musi być wyposażone w co najmniej:
    a) 1 dedykowany port do zarządzania urządzeniem (Management port),
    b) 8 portów 10/100/1000 Base-T,
    c) możliwość rozbudowy o co najmniej 2 porty 10Gb SFP+, gdzie Zamawiający w późniejszym terminie będzie miał możliwość zainstalować we własnym zakresie odpowiednie wkładki SFP+ 10Gbps,
    d) w przypadku jeżeli w punkcie c) urządzenie wymaga dodatkowego modułu rozszerzeń, Wykonawca dostarczy wraz z urządzeniem taki moduł, umożliwiający uzyskanie wymaganego rezultatu tj. możliwość rozbudowy o 2 interfejsy optyczne SFP+ 10Gb,
    e) co najmniej 2 porty USB.
4. Parametry wydajnościowe urządzenia muszą zapewniać przepustowość minimum:
    a) Firewall – 18 Gbps,
    b) IPSec VPN – 5 Gbps,
    c) skanowanie antywirusowe – 3 Gbps,
    d) ochrona przed atakami IPS/IDS – 3 Gbps,
    e) przy włączeniu wszystkich usług oraz pełnym obciążeniu urządzenia – 2 Gbps.
5. Powyższe parametry wydajnościowe powinny być zachowane dla co najmniej 4 500 000 jednoczesnych połączeń i przy obciążeniu minimum 98 000 nowych połączeń na sekundę.
6. Interfejsy sieciowe systemu UTM muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI) oraz w trybie pasywnego nasłuchu (sniffer). Urządzenie musi mieć możliwość segmentacji sieci na odrębne domeny kolizyjne. Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
7. Urządzenie musi obsługiwać protokoły routingu dynamicznego BGP4, RIPv1/v2 i OSPFv2/v3.
8. System zabezpieczeń musi umożliwiać definiowanie reguł dla trasowania routingu (tzw. Policy-based routing).
9. System zabezpieczeń musi mieć możliwość obsługi protokołów IGMP, PIM, MSDP między różnymi segmentami sieci (Multicast routing).
10. System zabezpieczeń musi umożliwiać konfigurację agregacji interfejsów sieciowych co najmniej w trybach: LAP (IEEE 802.3AD dynamic), statycznym i failover.
11. System zabezpieczeń musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych. Serwer DHCP powinien również mieć możliwość pracy w trybie DHCP Relay z jednoczesną obsługą co najmniej 3 serwerów DHCP.
12. System zabezpieczeń musi umożliwiać obsługę zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
13. System zabezpieczeń musi umożliwiać konfigurację SD-WAN pozwalającą na ustawienie kilku interfejsów zewnętrznych, gdzie możliwe jest: automatyczne przełączanie ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich, równoważenie obciążenia pomiędzy tymi interfejsami oraz dystrybucję ruchu na podstawie jakości łącza.
14. System zabezpieczeń musi obsługiwać sieci VLAN poprzez znakowanie zgodne z IEEE 802.1Q. Interfejsy sieciowe L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. W ramach sieci VLAN muszą być obsługiwane 4094 znaczniki. Łącznie na wszystkich interfejsach razem musi być możliwe skonfigurowanie minimum 250 sieci VLAN
15. System zabezpieczeń musi wykorzystywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów

posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. Reguły translacji adresów NAT muszą być rozdzielne od polityk bezpieczeństwa.

16. System zabezpieczeń musi umożliwiać zestawienie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site w tym co najmniej:
    a) konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN),
    b) w ramach ustawień VPN muszą być obsługiwane mechanizmy szyfrowania co najmniej: DES, 3DES, AES128, AES192, AS256, AES-GCM-256 oraz mechanizmy uwierzytelniania co najmniej: SHA-2, MD5, IKE Pre-hared Key i certyfikaty,
    c) konfiguracja VPN musi obsługiwać PFS z wykorzystaniem algorytmów DH,
    d) konfiguracja VPN musi obsługiwać IPSec NAT traversal,
    e) dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN, w ramach której musi być wsparcie dla protokołów SSH, RDP, HTTP oraz wsparcie dla funkcjonalności Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML,
    f) możliwość autoryzacji użytkowników mobilnych w oparciu o protokoły RADIUS, LDAP, Active Directory lub lokalną bazę użytkowników,
    g) dla użytkowników mobilnych powinna być możliwość ustawienia dwuskładnikowego uwierzytelniania w oparciu o tokeny sprzętowe lub programowe.
17. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum: priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
    a) Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. System powinien móc weryfikować aplikację z założeniem identyfikacji na wszystkich 65 535 dostępnych portach.
    b) Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall.
    c) Firewall musi mieć możliwość wykrywania aplikacji tunelujących się protokołach HTTP lub HTTPS.
18. System zabezpieczeń musi umożliwiać konfigurację pasma sieci w zakresie oznaczania pakietów znacznikami (DiffServ), konfigurację ustawień dla dowolnego źródła, miejsca docelowego lub portu oraz klas dla różnego rodzaju ruchu sieciowego:
    a) QoS dla poszczególnych adresów IP lub podsieci,
    b) QoS w oparciu o polityki zapory sieciowej lub wybranej aplikacji,
    c) QoS per sesja na podstawie znaczników DSCP.
19. System zabezpieczeń musi zapewniać funkcjonalność Content Routingu w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
20. System zabezpieczeń w ramach konkretnych aplikacji musi umożliwiać kontrolę specyficznych akcji np. blokowanie rozmów głosowych w komunikatorach internetowych lub blokowanie wysyłania plików (pliki wykonywalne).
    a) W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP, system zabezpieczeń powinien posiadać możliwość ustawiania profili dla każdej aplikacji.
21. System zabezpieczeń musi umożliwiać blokowanie komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.

22. System zabezpieczeń musi umożliwiać konfigurację blokowania komunikacji z wybranymi adresami IP, adresami domenowymi oraz ustawienie blokowania komunikacji w oparciu o reputację adresów IP lub domen.
23. System zabezpieczeń musi mieć moduł filtrowania stron WWW w zależności od kategorii treści stron bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza filtra stron WWW musi być regularnie aktualizowana w sposób automatyczny. Moduł filtrowania stron WWW powinien umożliwiać:
    a) określenie rodzaju akcji dla nieskategoryzowanych stron www,
    b) tworzenie białych/czarnych list wyjątków dla filtrowania zawartości URL,
    c) określenie akcji podejmowanych na podstawie reputacji adresu URL,
    d) filtrowanie treści w oparciu o typy MIME,
    e) blokowanie plików cookies dla określonych domen,
    f) wysyłanie modyfikowalnego komunikatu do użytkownika o tym dlaczego dostęp do strony WWW został zablokowany,
    g) analizę treści dla protokołu HTTPS oraz wyłączenia inspekcji HTTPS dla wybranych kategorii stron WWW.
24. System zabezpieczeń musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
25. System zabezpieczeń musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw DNS oraz stron WWW (URL). Pobrane dane muszą być automatycznie wykorzystywane do blokowania lub wykrywania ruchu do tych zasobów.
26. System zabezpieczeń musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
27. System firewall musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny.
28. System zabezpieczeń urządzenia musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu HTTPS dla ruchu wychodzącego do serwerów zewnętrznych oraz ruchu przychodzącego do serwerów placówki. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji umożliwiającej co najmniej: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wykrywanie i blokowanie wirusów i złośliwego kodu (ochrona anty-wirus, anty-spyware, anty-malware), filtrację plików, danych i URL.
    a) Baza sygnatur dla modułu inspekcji antywirusowej musi być przechowywana na urządzeniu i powinna być regularnie aktualizowana w sposób automatyczny, nie rzadziej niż co 12 godzin.
    b) Rozwiązanie antywirusowe musi mieć możliwość skanowania plików o maksymalnym rozmiarze co najmniej 20MB oraz skanowania plików wielokrotnie skompresowanych w archiwach.
    c) Moduł antywirusowy powinien umożliwiać tworzenie wyjątków dla określonych adresów URL, typów plików lub sygnatury pliku MD5.
29. System zabezpieczeń urządzenia musi posiadać osobny zestaw polityk definiujący ruch SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
30. System zabezpieczeń musi zapewniać inspekcję szyfrowanej komunikacji SSH.
31. System zabezpieczeń musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

32. System zabezpieczeń musi posiadać funkcję analizy behawioralnej w oparciu o platformę typu „Sand-Box" z możliwością pracy w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej). Analiza powinna obejmować co najmniej pliki pobierane i przesyłane przez protokoły takie jak HTTP/HTTPS, SMTP, POP3, IMAP oraz FTP.
    a) Administrator musi mieć możliwość konfiguracji rodzaju pliku (EXE, DLL, PDF, MS Office, Java, SWF) oraz kierunek przesyłania (odbieranie, odbieranie/wysyłanie) do określenia ruchu poddanego analizie typu „Sand-Box".
    b) System zabezpieczeń musi mieć możliwość generowania raportów dla każdego analizowanego pliku tak, aby administrator miał możliwość sprawdzenia, które pliki i z jakiego powodu zostały uznane za złośliwe oraz sprawdzić, którzy użytkownicy te pliki pobierali.
    c) System zabezpieczeń powinien umożliwiać ustawienie kwarantanny dla podejrzanych plików oraz blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.
    d) W przypadku integracji z zewnętrznymi rozwiązaniami typu „Sand-Box", system zabezpieczeń musi zapewniać możliwość przechwytywania i przesyłania (do rozwiązania zewnętrznego) plików różnych typów (EXE, DLL, PDF, MS Office, Java, SWF) przechodzących przez firewall, w celu ochrony przed zagrożeniami typu Zero-Day. Systemy zewnętrzne na podstawie przeprowadzonej analizy muszą aktualizować firewall sygnaturami nowo wykrytych złośliwych plików.
33. System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS i DDoS (co najmniej: IPSec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Port Scan, IP Source Route, ARP/IP Spoofing) wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
34. System zabezpieczeń musi być wyposażony w funkcję anty-spam, w ramach której powinien umożliwiać:
    a) kwarantannę wiadomości e-mail przesyłanych protokołem SMTP,
    b) oznaczenie wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail,
    c) blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail,
    d) możliwość tworzenia białych/czarnych list, w oparciu o które, system zezwala lub odmawia wysyłania wiadomości e-mail do określonych nadawców lub odbiorców,
    e) możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.
35. System zabezpieczeń musi obsługiwać uwierzytelnianie użytkowników z wykorzystaniem: Active Directory, LDAP, RADIUS, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
36. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP.
37. System zabezpieczeń musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze Active Directory, z czego co najmniej 2 z nich nie mogą wymagać instalacji dodatkowego oprogramowania na stacjach końcowych użytkowników.
38. System zabezpieczeń musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych.

39. System zabezpieczeń musi mieć możliwość limitowania dostępu do sieci określonym użytkownikom w oparciu o „quoty" czasowe lub na podstawie transferu danych co najmniej dla komunikacji HTTP.
40. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA – Multi-Factor Authentication) per user/grupa w celu autentykacji. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, SAML 2.0.
41. System zabezpieczeń musi dostarczać mechanizmy identyfikacji urządzeń w sieci, w tym co najmniej: identyfikację systemu operacyjnego, otwartych portów i usług.
42. System zabezpieczeń powinien zapewniać podstawowe funkcje ochrony punktów końcowych typu EDR. Jeżeli konieczna jest dodatkowa licencja powinna zostać dołączona do urządzenia. Licencja ta powinna umożliwiać obsługę do 150 stacji końcowych na urządzenie UTM.
43. W ramach usługi Endpoint Detection & Response system zabezpieczeń powinien oferować minimum:
    a) wykrywanie kontekstowe (ochrona przed Ransomware, wykrywanie ataków bez plikowych),
    b) ochronę przed exploitami,
    c) ochronę przed manipulacją (anty-tampering),
    d) izolację punktu końcowego,
    e) zdalny restart i ponowna instalacja agenta,
    f) odczyt sprzętu i oprogramowania na urządzeniu końcowym,
    g) wykrywanie niechronionych punktów końcowych,
    h) śledzenie działań użytkownika w konsoli zarządzania.
44. Agent instalowany w ramach funkcji EDR powinien być dostępny w co najmniej dwóch wersjach (na systemy Windows, Linux). Obecność agenta w systemie punktu końcowego nie może zakłócać pracy rozwiązania antywirusowego zainstalowanego w systemie.
45. Zrządzanie systemem musi się odbywać z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dopuszczalna jest instalacja dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. Zarządzanie za pomocą linii poleceń powinno być dostępne przez protokół SSH lub poprzez dedykowany port w urządzeniu.
46. Dostęp do urządzenia i zarządzanie z sieci musi być zabezpieczony kryptograficznie (poprzez szyfrowanie komunikacji). System powinien pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach oraz umożliwiać zarządzanie poszczególnymi elementami systemu jednocześnie przez wielu administratorów. Uwierzytelnianie administratorów powinno być możliwe poprzez wykorzystanie: bazy lokalnej, serwera LDAP, RADIUS, TACACS+. System musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej dwie metody (np. baza lokalna, LDAP i RADIUS).
47. System zabezpieczeń musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online oraz w trybie offline z możliwością aktualizacji konfiguracji według zdefiniowanego harmonogramu. Dostępne powinno być również rozwiązanie umożliwiające edycję konfiguracji urządzenia, które jest nieaktywne.
48. System zabezpieczeń musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej: o ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron WWW. System musi umożliwiać tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub

automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV. System zabezpieczeń powinien umożliwiać stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni (co najmniej 7 dni).

49. System zabezpieczeń musi zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania. Komunikacja z tymi systemami musi być szyfrowana.
50. Dopuszczalne jest wykorzystanie narzędzia zewnętrznego lub dedykowanej aplikacji od producenta urządzenia do wykonywania raportów opisanych powyżej lub wykorzystanie narzędzia w chmurze dostarczanego przez producenta urządzenia.
51. System zabezpieczeń musi umożliwiać dostęp do urządzenia w trybie graficznym za pomocą przeglądarki internetowej, w którym możliwe będzie pełne zarządzanie i konfiguracja urządzenia w tym minimum:
    a) konfiguracja sieci, ustawienia poszczególnych interfejsów, VLAN, ustawienia routingu statycznego i dynamicznego, definiowanie Multi-WAN i failover,
    b) konfiguracja polityk bezpieczeństwa, tworzenie i edycja reguł firewall, ustawienia NAT, przekierowanie portów, reguły dostępu, przypisywanie polityk do grup interfejsów,
    c) zarządzanie usługami bezpieczeństwa wymienionymi powyżej w punkcie b.,
    d) monitorowanie i diagnostyka pracy urządzenia, w tym co najmniej podgląd aktywnych połączeń i sesji, statystyk interfejsów i usług, przeglądanie logów i zdarzeń bezpieczeństwa,
    e) zarządzanie użytkownikami i uwierzytelnianiem, w tym ustawienia użytkowników i grup na urządzeniu lub konfiguracji integracji z usługami takimi jak LDAP, RADIUS, Active Directory, ustawienia MFA.

II. Dodatkowe wymagania

1. Wykonawca wraz z urządzeniami dostarczy wszelkie niezbędne licencje na oprogramowanie zainstalowane w urządzeniu w formie 36-cio miesięcznej subskrypcji.
2. Wykonawca zapewni gwarancję producenta dla przedmiotu zamówienia oraz zapewni wsparcie przy zgłaszaniu ewentualnych awarii przez okres trwania subskrypcji.
3. Wykonawca nie później niż w ciągu 10 dni od dnia zawarcia Umowy ma obowiązek przekazać Zamawiającemu informacje dot. zgłaszania i obsługi zgłoszeń gwarancyjnych, w tym minimum:
    a) Sposób zgłaszania awarii;
    b) Dane Wykonawcy – adresy, numery telefonów, adresy poczty elektronicznej;
    c) Instrukcje dotyczące przeglądania statusu umowy/subskrypcji oraz urządzeń nią objętych;
    d) Instrukcje pobierania poprawek i nowych wersji oprogramowania ze strony internetowej dla urządzeń i oprogramowania bez ponoszenia dodatkowych kosztów.
4. Powyższe dane i instrukcje Wykonawca dostarczy w formie pisemnej lub za pomocą poczty elektronicznej.
5. W przypadku jakichkolwiek zmian danych, o których mowa jest powyżej, Wykonawca niezwłocznie poinformuje o tym Zamawiającego w formie pisemnej lub za pomocą poczty elektronicznej.
6. Zgłoszenie awarii może być dokonywane w postaci zgłoszenia telefonicznego lub za pomocą poczty elektronicznej. W przypadku zgłoszenia telefonicznego, Zamawiający potwierdzi je za pomocą poczty elektronicznej.
7. Wykonawca będzie przyjmował zgłoszenia awarii w dni robocze co najmniej w godzinach 8:00-16:00.

8. Wykonawca jest zobowiązany do potwierdzenia przyjęcia zgłoszenia awarii w terminie do 4 godzin od jego zgłoszenia za pomocą poczty elektronicznej na adres si@oeiizk.edu.pl lub telefonicznie na numer telefonu podany w zgłoszeniu.
9. Wykonawca jest zobowiązany do informowania Zamawiającego o statusie zgłoszenia dot. awarii za pośrednictwem poczty elektronicznej w minimalnym zakresie: informacji o statusie zgłoszenia oraz jego zmianie.
10. Wykonawca wykona wdrożenie dostarczonych urządzeń w następującym zakresie:
    a) Udzieli asysty technicznej przy konfiguracji urządzeń zgodnie ze złożoną ofertą jednak nie w mniejszym stopniu niż konfiguracja podstawowych funkcji tj.: aktywacja licencji, aktualizacja OS, konfiguracja interfejsów w tym Multi-WAN oraz SD-WAN zgodnie z wymogami dostawcy łącza internetowego oraz potrzebami zamawiającego, konfiguracja usługi lub serwera logowania, integracja z usługą Active Directory.
    b) Jeżeli do zbierania logów oraz przygotowywania raportów producent przewiduje zewnętrzne narzędzie, Wykonawca podczas wdrożenia wykona konfigurację takiego narzędzia oraz zaimplementuje jego obsługę w urządzeniach.
    c) Jeżeli rozwiązanie z podpunktu b) opiera się na specjalnie przygotowanej maszynie wirtualnej z serwerem logowania, to obraz takiej maszyny musi być przygotowany co najmniej dla rozwiązania Microsoft Hyper-V. Jeżeli producent nie wspiera takiego rozwiązania, to Wykonawca w ramach wdrożenia jest zobowiązany do przeprowadzenia konwersji z innej platformy wirtualizacyjnej.
11. Dopuszczalna jest asysta online, bez konieczności przyjazdu do placówek OEIiZK.
12. Asysta techniczna będzie realizowana przez eksperta posiadającego niezbędne doświadczenie oraz certyfikację u producenta dostarczonego urządzenia.
13. Wykonawca poświadcza, że posiada certyfikację ISO 27001, że personel techniczny asystujący przy wdrożeniu oraz świadczący wsparcie techniczne posiada certyfikację producenta.
14. Poświadczenie posiadanych uprawnień polega na przesłaniu skanów posiadanych certyfikatów i/lub zaświadczeń.
15. Wykonawca w ramach gwarancji udzieli powdrożeniowego wsparcia technicznego dla dostarczonych urządzeń.
16. W ramach powdrożeniowego wsparcia technicznego Wykonawca określi liczbę godzin do wykorzystania przez Zamawiającego w ramach okresu trwania subskrypcji bez ponoszenia dodatkowych opłat przez Zamawiającego, przy czym:
    a) Pakiet dostępnych godzin w ramach wsparcia opisanego w punkcie 4. nie może być mniejszy niż 20 godzin w całym okresie trwania subskrypcji;
    b) Do pakietu godzin powdrożeniowego wsparcia technicznego nie zalicza się czasu zgłoszenia i obsługi zgłoszenia awarii urządzenia;
    c) Wykonawca udostępni cennik godzin takiego wsparcia technicznego, który będzie obowiązywał Zamawiającego po przekroczeniu „darmowego” pakietu.
17. Dodatkowe, powdrożeniowe wsparcie techniczne nie dotyczy zakresu prac i konsultacji objętych asystą techniczną przy wdrożeniu urządzeń, tj. okresu do 30 dni od daty wdrożenia urządzeń tj. daty obustronnego podpisania protokołu wdrożeniowego.
18. Rozszerzenie licencji o kolejne funkcjonalności nie może powodować utraty praw gwarancyjnych do oprogramowania oraz nie może wymagać zgody Wykonawcy lub producenta.
19. Zamawiający wymaga, by dostarczone oprogramowanie sprzętowe było oprogramowaniem w wersji aktualnej (najnowszej opublikowanej przez producenta) na dzień poprzedzający dzień składania ofert.

III. Zorganizowanie i przeprowadzenie warsztatów szkoleniowych:

1. Wykonawca przeprowadzi warsztaty powdrożeniowe wedle poniższego opisu oraz ilości osób.
2. Szkolenie będzie trwało nie mniej niż 3 dni ale nie dłużej niż 5 dni roboczych dla maksymalnie 2 osób, gdzie pojedynczy dzień szkolenia nie może przekraczać 8 godzin.
3. Szkolenie musi dotyczyć urządzeń zaoferowanych w ramach realizacji umowy i obejmować:
    a) Logowanie, poruszanie się i zarządzanie za pomocą interfejsu webowego;
    b) Zarządzanie dostępem użytkowników i konfiguracja urządzenia pod zdalną administrację;
    c) Zarządzanie licencjami;
    d) Aktualizacja systemu operacyjnego urządzenia;
    e) Wykonywanie kopii bezpieczeństwa konfiguracji systemu i jej przywracanie;
    f) Monitorowanie zdarzeń w logach, przeszukiwanie i odczytywanie logów;
    g) Konfiguracja logowania i wysyłania powiadomień (w tym integracja z zewnętrznymi narzędziami);
    h) Wykonywanie raportów dot. zdarzeń i eksportowanie do plików CSV, PDF;
    i) Konfigurowanie harmonogramu raportów, zapisywanie i ich drukowanie;
    j) Monitorowanie ruchu sieciowego i obciążenia interfejsów;
    k) Konfigurowanie interfejsów sieciowych w urządzeniu;
    l) Konfiguracja przełączania awaryjnego Multi-WAN
    m) Konfiguracja SD-WAN
    n) Omówienie i konfiguracja trybów routingu sieciowego;
    o) Konfiguracja sieci VLAN;
    p) Konfiguracja dynamicznego i statycznego NAT;
    q) Konfiguracja Quality of Service (QoS);
    r) Omówienie i zarządzanie politykami bezpieczeństwa;
    s) Konfigurowanie reguł zapory sieciowej;
    t) Konfigurowanie filtra pakietów sieciowych i tworzenie niestandardowych reguł;
    u) Blokowanie adresów IP i portów;
    v) Automatyczne blokowanie adresów IP generujących podejrzany ruch;
    w) Blokowanie połączeń z wybranych krajów (geolkalizacja);
    x) Konfigurowanie kontroli aplikacji;
    y) Konfigurowanie ochrony przed złośliwym oprogramowaniem;
    z) Konfiguracja filtra antyspamowego i działań przy wykryciu spamu;
    aa) Konfiguracja filtra URL: blokowanie stron WWW, pobieranie plików, profili blokujących i reputacji stron WWW;
    bb) Omówienie i konfiguracja „Site-to-Site” VPN
4. Szkolenie (oraz dokumentacja szkoleniowa) musi być prowadzone w języku polskim.
5. Preferowanym miejscem szkolenia jest Miasto st. Warszawa. Dopuszczalne jest szkolenie w ośrodku szkoleniowym poza terenem m. st. Warszawa, jednak w tym wypadku Wykonawca uwzględnia w ofercie również koszty organizacji takiego szkolenia w granicach województwa mazowieckiego wraz kosztami noclegu i wyżywienia, który organizuje w ramach szkolenia.
6. Za zgodą Zamawiającego warsztaty mogą zostać przeprowadzone na odległość, w trybie zdalnym uzgodnionym roboczo przez strony.
7. Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie warsztatów. Wykonawca zapewni co najmniej jedną osobę trenera, która posiada niezbędną wiedzę i doświadczenie do wykonania warsztatów, a w szczególności co najmniej 12-miesięczne doświadczenie praktyczne w przeprowadzaniu szkoleń z zakresu oferowanego rozwiązania.

8. Wykonawca powinien dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazę szkoleniową z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzania warsztatów dla osób dorosłych, tj. sale dostosowane do prowadzenia zajęć, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowanie i pomoce dydaktyczne niezbędne do wykonania zamówienia.