Załącznik nr 2 a dla części nr 1
Nr postępowania EZP-252-23/2022

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest:

Zakup i wdrożenie systemów teleinformatycznych oraz usług służących poprawie poziomu cyberbezpieczeństwa.

Część nr 1. Dostawa sprzętu, usługi oraz serwis

Zamawiający oczekuje dostawy, instalacji konfiguracji poniższych elementów oraz świadczenia usług w zakresie:

1. Biblioteka taśmowa
2. Rozbudowa pamięci RAM
3. UTM
4. Bramka SMS
5. Migracja i rozszerzenie obecnie posiadanej licencji ESET
6. Usługi
7. Monitoring zasobów krytycznych
8. Serwis 24/7
9. Szkolenia z cyberbezpieczeństwa

1. Biblioteka Taśmowa

Biblioteka taśmowa		**Ilość**	**1 szt.**
Wymagane minimalne parametry techniczne			
Obudowa	Do zamontowania w szafie rack, maksymalnie 2U.		
Napęd	LTO-8 SAS – 1 sztuka możliwość rozbudowy o drugi napęd. Zamawiający wymaga dostarczenia kabla do podłączenia z serwerem.		
Liczba slotów	Minimum 24 kieszenie na taśmy (urządzenie powinno być dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka.		
Pojemność	Wymagana pojemność bez kompresji – minimum 288 TB		
Wyposażenie	Urządzenie musi być wyposażone w czytnik kodów kreskowych, kabel zasilający i sieciowy oraz kabel koniecznego do podłączenia do odpowiedniego kontrolera serwera (długość kabla min. 1m) umożliwiającego komunikację z urządzeniem oraz wszystkimi zainstalowanymi napędami. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych o pojemności bez kompresji minimum 12TB każdy w ilości 12 szt wraz z 1		

	nośnikiem czyszczącym, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem oraz wyposażone w naklejki z kodami kreskowymi.
Karta SAS HBA	Zamawiający wymaga wyposażenie serwera Dell R540 ST: 4QFJQF3 w kompatybilną kartę SAS HBA umożlwiającą podłączenie oferowanej biblioteki.
Gwarancja i oświadczenia	36 miesięcy w miejscu instalacji urządzenia.

2. Rozbudowa pamięci RAM

Rozbudowa pamięci RAM	**Ilość**	**1 kpl.**
Wymagane minimalne parametry techniczne		
Zamawiający wymaga rozbudowy dwóch serwerów aplikacyjnych Dell R540 (ST: 6QFJQF3, ST:5QFJQF3). Każdy serwer należy rozbudować o 128GB pamięci. Oferowane Pamięci muszą być kompatybilne z posiadanymi serwerem o minimalnym taktowaniu 3200MT/s. Oferowane pamięci muszą być objęte gwarancją przez 36 miesięcy.		

3. UTM

UTM	**Ilość**	**1 kpl.**
Wymagane minimalne parametry techniczne		
OBSŁUGA SIECI 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. **ZAPORA KORPORACYJNA (Firewall)** 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.		

10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

INTRUSION PREVENTION SYSTEM (IPS)

12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

KSZTAŁTOWANIE PASMA (Traffic Shapping)

21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,

c. Skaner heurystyczny.

31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.

52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
58. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
61. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

62. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
68. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
69. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
70. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
71. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
72. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
73. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
74. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
75. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,

b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

76. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
77. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

RAPORTOWANIE

78. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
79. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
80. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
81. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
82. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
83. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
84. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
85. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

86. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
87. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
88. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
89. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
90. Urządzenie ma posiadać usługę DNS Proxy.
91. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

92. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
93. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
94. Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od potwierdzenia awarii.

PARAMETRY SPRZĘTOWE

95. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
96. Liczba portów Ethernet 10/100/1000Mbps – min.5.
97. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
98. Przepustowość Firewall (1518 bajtów UDP) – minimum 1Gbps.

99. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1Gbps.
100. Przepustowość filtrowania Antywirusowego – minimum 260Mbps.
101. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 200Mbps.
102. Maksymalna liczba tuneli VPN IPSec – minimum 50.
103. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 5.
104. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20.
105. Obsługa interfejsów 802.11q (VLAN) – minimum 128
106. Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 6 000 nowych sesji/sekundę.
107. Urządzenie nie ma limitu na liczbę użytkowników.
108. Liczba reguł filtrowania – minimum 4 096.
109. Liczba tras statycznego routingu – minimum 512.
110. Liczba tras dynamicznego routingu – minimum 1 000.

SZKOLENIE

Zamawiający wymaga zdalnego szkolenie technicznego poświęconego urządzeniom dostarczanym w przetargu do ochrony styku sieci firmowej z Internetem firmy obejmujące zagadnienia:

111. Rozpoczęcie pracy z urządzeniem
112. Zbieranie logów i monitorowanie
113. Konfiguracja sieci
114. Translacja adresów sieciowych (NAT)
115. Przekierowanie połączeń
116. Filtrowanie ruchu sieciowego (Firewall)
117. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń
118. Ochrona aplikacji
119. Użytkownicy i uwierzytelnianie
120. Konfiguracja usługi katalogowej
121. Wirtualne sieci prywatne (VPN)
122. SSL VPN

4. Bramka SMS

Bramka SMS		**Ilość**	**1 szt.**
Wymagane minimalne parametry techniczne			
Procesor	Minimum 4 rdzenie o taktowaniu 1.2GHz		
Pamięć wewnętrzna	Minimum 4GB		
Obsługiwane Częstotliwości	UMTS 800/850/900/AWS/1900/2100 MHz GSM/GPRS 850/900/1800/1900 MHz		
Interfejsy	1x HDMI, 2x USB, 1xRJ45		
Slot na kartę SIM	Tak		
Przepustowość	odbiór wiadomości: do 30 SMS/min wysyłanie wiadomości: do 30 SMS/min		
Funkcjonalność	• Wysyłanie, Odbiór SMS (foldery wiadomości: Skrzynka odbiorcza, Skrzynka nadawcza, Elementy wysłane) • Wysyłanie, Odbiór MMS • Wysyłanie SMS do pojedynczych użytkowników lub grup • Wysyłanie wiadomości o konkretnej porze (harmonogram wysyłek) • Ograniczanie wysyłania w określonych godzinach (np. między 08:00-18:00)		

	• Tryb konwersacji w folderach (wiadomości są pogrupowane wg numeru telefonu). Łatwo śledzisz historię komunikacji z danym użytkownikiem • Obsługa różnych typów wiadomości (SMS/SMS wieloczęściowy/Flash SMS/MMS/SMS binarny/kody USSD/WAP Push link) • Szablony wiadomości • Książka adresowa (zarządzanie odbiorcami, grupami odbiorców) • Import odbiorców z pliku CSV • Monitoring usług i serwerów (np serwer WWW, serwer poczty email) wysyłanie alertów sms i SNMP Traps • Automatyczna odpowiedź na odebrane wiadomości • Przekierowanie Email na SMS • Przekierowanie SMS na Email • Przekierowanie SMS przychodzących do zewnętrznego skryptu (callback URL) • Funkcja czarnej listy do wykluczania numerów • Plugin do Outlooka umożliwiający wysyłanie SMS-ów bezpośrednio z aplikacji • Cyfrowe wejście i wyjście sterowane przez SMS • Uwierzytelnianie wieloskładnikowe (MFA) • Funkcja eskalacji wiadomości • Kopia zapasowa na FTP • Okresowe czyszczenie folderów • Automatyczne tworzenie kopii zapasowych na FTP • Cykliczne wysyłanie SMS w określonych odstępach czasu • Wsparcie dla wielu użytkowników (użytkownicy zarządzają prywatnymi folderami: Skrzynka odbiorcza, Skrzynka nadawcza, Elementy wysłane) • Alerty SMS z czujnika Temperatury i wilgotności • Wsparcie dla Unicode (narodowe zestawy znaków) • Interfejs API do wysyłania i odbioru wiadomości z zewnętrznych programów • Wielojęzyczny (angielski, francuski, hiszpański, niemiecki, polski) interfejs webowy • Klient NTP • Klient SNMP • Wbudowany serwer www • Wbudowana baza danych • Wbudowany serwer email • Nowoczesny responsywny interfejs webowy • Wsparcie dla raportów doręczenia • Obsługa HTTPS • Mechanizm watchdog nadzorujący pracę modemu 3G • Obsługa Failover (możliwość utworzenia klaster HA dla 2 urządzeń) • Szybkość transmisji danych HSPA+ do 21 Mb/s przy pobieraniu i 5,7 Mb/s przy wysyłaniu (z możliwością wyłączenia/wyłączenia) • Obsługa zewnętrznych czujników temperatury
Gwarancja	Minimum 3 lata gwarancji

5. Migracja i rozszerzenie obecnie posiadanej licencji ESET

Zamawiający informuje, że jest w posiadaniu licencji ESET PROTECT Essential ON-PREM liczba stanowisk: 300 szt. identyfikator publiczny:333-23K-RA8; termin ważności licencji 2023-11-27.

W ramach zamówienia Zamawiający oczekuje uzyskania stanu docelowego ESET PROTECT Entry ON-PREM; liczba stanowisk: 450; termin ważności licencji 5 lat od daty zamówienia wraz z migracją konsoli SMC do środowiska zwirtualizowanego, hiperwizor: VMware ESXi wersja 7. W trakcie prac musi zostać zapewniony nadzór przedstawicielowi Zamawiającego nad wykonywanymi pracami jak również musi zostać zademonstrowany proces kolejnych aktualizacji konsoli. Wykonawca zainstaluje szablon maszyny wirtualnej konsoli w wirtualizatorze klienta i dokona konfiguracji adresów IP dla nowej konsoli oraz konsoli tymczasowej utworzonej na potrzeby przyszłych aktualizacji.
W ramach dostawy Wykonawca zapewni szkolenie dla 2 osób - administratorów ESET w zakresie:

- ESET PROTECT - architektura i omówienie komponentów.
- Instalacja serwera ESET PROTECT.
- ESET PROTECT - omówienie funkcji serwera.
- Zarządzanie administratorami i ich uprawnieniami
- Polityki i dziedziczenie
- Apache HTTP Proxy.
- ESET Management Agent - zdalna instalacja i omówienie możliwości
- Grupy statyczne i dynamiczne.
- Zadania klienta, serwera oraz wyzwalacze.
- Zdalna instalacja klienta ESET.
- Omówienie funkcji podstawowych i zaawansowanych klienta EES.
- Ochrona antywirusowa.
- Zarządzanie aktualizacją.
- Zapora osobista
- Moduł antyspamowy.
- Powiadomienia.
- Raportowanie
- Kontrola dostępu do stron internetowych
- Kontrola dostępu do urządzeń
- Wdrożenie maszyny wirtualnej ESET PROTECT MDM
- Wdrożenie klienta ESET Endpoint Security for Android

Długość szkolenia musi wynosić minimum 14 godzin a liczba godzin szkoleń w ciągu jednego dnia nie może przekroczyć 7 godzin. Szkolenie pracowników musi zostać przeprowadzone w ciągu 90 dni licząc od pierwszego dnia obowiązywania umowy. Zamawiający dopuszcza szkolenie on-line, w przypadku prowadzenia szkoleń stacjonarnych Zamawiający zapewnia salkę niezbędną do ich prowadzenia.

6. Usługi

Usługi	**Ilość**	**1 kpl.**
Wymagane minimalne parametry techniczne		
1. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury w miejscach wskazanych przez Zamawiającego. 2. Zamawiający wymaga instalacji dostarczonej pamięci RAM w dwóch posiadanych serwerach aplikacyjnych oraz skorygowania przydzielonych zasobów RAM na potrzeby maszyn wirtualnych. 3. Wymagane jest zainstalowanie i podłączenie biblioteki taśmowej oraz przeprowadzenie min. 2 godzinnego szkolenia z obsługi urządzenia.		

Następnie należy skonfigurować bibliotekę taśmową oraz posiadane oprogramowanie do backupu. Wykonawca uwzględni i wykona przynajmniej poniższe rekomendacje centrum e-zdrowia w obszarze systemu kopii zapasowej:

a) Wykonanie przeglądu czy system kopii zapasowych działa prawidłowo i czy wykonuje swoje zadanie zgodnie z zadanym harmonogramem.

b) Wykonywanie kopii bezpieczeństwa zgodnie z harmonogramem - raz dziennie kopia różnicowa lub przyrostowa oraz raz w tygodniu pełna kopia.

c) Weryfikację czy wykonane kopie zapasowe faktycznie pozwolą na odtworzenie całych systemów wraz z danymi i konfiguracją.

d) Wykonywane kopie zapasowe nie mogą być podłączone jako zasób sieciowy.

e) Wykonanie testów odtworzenia systemów w izolowanym środowisku. Działanie takie powinno odbywać się cyklicznie.

f) Stosowanie strategii 3-2-1: a. Należy przechowywać co najmniej 3 kopie zapasowe. b. Co najmniej 2 z nich powinny być przechowywane na różnych nośnikach. c. Co najmniej 1 z nich powinna być odizolowana od pozostałych oraz sieci lokalnej (odmiejscowienie)

g) Przygotowanie planu działania na scenariusz utraty systemu kopii zapasowych razem z kopiami – powołanie nowej maszyny, instalacja OS oraz systemu kopii, wgranie kopii konfiguracji systemu kopii, podłączenie kopii zapasowych.

h) System kopii zapasowych powinien być w dedykowanej podsieci. Przepuszczony ruch pomiędzy hostami i systemem kopii powinien być minimalny, niezbędny – określone porty. System kopii powinien działać na dedykowanych kontach bez praw administratora domenowego.

Wykonawca po dostarczeniu rozwiązania oraz wykonanej konfiguracji przeprowadzi szkolenie dla 3 administratorów Zamawiającego, po którym będą oni w stanie samodzielnie obsługiwać system backupu oraz stosować rekomendacje centrum e-zdrowia w obszarze systemu kopii zapasowej.

4. Należy zainstalować dostarczaną kartę SAS HBA do serwera kopii.
5. Zamawiający wymaga instalacji oraz konfiguracji urządzenia UTM w lokalizacji Zamawiającego znajdującej się w Kielcach.
6. Należy zestawić tunel VPN pomiędzy główną lokalizacją wyposażoną w UTM firmy Stormshield a nowo dostarczanym UTM oraz asystować w skutecznym dołączeniu stacji roboczych podłączanej lokalizacji zdalnej Zamawiającego do pracy w domenie systemu Windows
7. Konfiguracja łącza zapasowego LTE w trybie failover w głównej lokalizacji Zamawiającego wraz z dostarczeniem urządzenia i okablowania niezbędnego do sprawnego funkcjonowania łącza z posiadanym UTM. Należy skonfigurować VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń ze wszystkimi 4 lokalizacjami zamawiającego wyposażonych w UTM. Kartę z odpowiednim łączem dostarczy Zamawiający.

7. Monitoring zasobów krytycznych

Zamawiający wymaga konfiguracji środowiska do monitorowania krytycznych zasobów infrastruktury IT a w szczególności infrastruktury środowiska HIS. Monitorowanie ma na celu zapobieganie, poprzez

informowanie z odpowiednim wyprzedzeniem administratorów szpitala, o potencjalnych problemach oraz zagrożeniach w dostępności usług oraz serwisów (tj. brak miejsca na dysku, brak pamięci operacyjnej, błędy systemów operacyjnych, błędy usług środowiska HIS, brak dostępności do urządzeń sieciowych oraz usług).
Konfiguracja musi obejmować przygotowanie serwera monitorowania, przygotowanie oraz personalizację szablonów, konfigurację powiadomień, szkolenie z obsługi oraz podpięcie co najmniej serwerów/usług środowiska HIS działającego u Zamawiającego, w szczególności wymienionych w tabeli „minimalny zakres aplikacji/usług do nadzoru".
Dodatkowo, poprzez sprzętową bramkę SMS , zostaną skonfigurowane niezależne powiadomienia SMS o najważniejszych błędach (karta SIM zostanie dostarczona przez Zamawiającego).

a. Wymagania szczegółowe

	Zainstalowane w ramach konfiguracji usługi rozwiązanie musi spełniać następujące minimalne wymagania:
1	umożliwiać monitorowanie systemów operacyjnych, urządzeń sieciowych, łączy internetowych, baz danych, procesów
2	obsługiwać co najmniej systemy operacyjne rodziny Windows i Linux
3	posiadać mechanizmy monitorowania plików logów (plików tekstowych)
4	gromadzić dane w bazie danych i obsługiwać co najmniej MySQL, mariaDB, PostgreSQL,Oracle
5	posiadać prekompilowanych agentów na systemy rodziny Windows oraz Linux
6	umożliwiać weryfikację poprawności pracy agentów monitorowania
7	umożliwiać definiowanie odrębnych parametrów monitorowania oraz wartości progowych dla różnych rodzajów serwerów w zależności od ich konfiguracji i roli.
8	umożliwiać definiowanie grup serwerów w zależności od ich konfiguracji i roli
9	gromadzić i utrzymywać informacje historyczne monitorowanych elementów infrastruktury.
10	udostępniać za pośrednictwem interfejsu graficznego informacje o skonsolidowanym stanie serwerów w czasie rzeczywistym.
11	udostępniać za pośrednictwem interfejsu graficznego informacje o aktualnych listach problemów wymagających reakcji.
13	powiadamiać administratorów o niedostępności monitorowanych serwerów i urządzeń.
14	szyfrować komunikację pomiędzy serwerem monitorowania a agentami
15	mieć możliwość monitoringu zarówno agentowego jak i bezagentowego.
16	realizować dostęp do systemu monitorowania poprzez konta dla upoważnionych użytkowników i chronić je hasłem
17	umożliwiać elastyczne definiowanie widoków dla użytkowników w zależności od ich roli, potrzeb oraz uprawnień.
18	monitorować wydajność i pojemność zasobów sprzętowych serwerów: a) procesory, b) pamięć operacyjna, c) przestrzenie dyskowe, d) interfejsy sieciowe.
19	musi umożliwiać wysyłanie powiadomień o zdarzeniach zarówno przez email jak i SMS
20	musi umożliwiać prezentowanie danych historycznych w postaci wykresów
21	musi posiadać szablony konfiguracyjne zawierające predefiniowane ustawienia monitorowania
22	musi automatycznie wyliczać SLA dla wybranych serwisów
23	musi umożliwiać prezentacje wizualną infrastruktury np. za pomocą map sieci
24	musi umożliwiać budowania własnych szablonów monitorowania
25	musi mieć możliwość dynamicznego dodawania elementów do monitorowania (np. dynamicznie budować listę dysków systemu operacyjnego i dodawać do nich parametry do monitorowania)
26	musi monitorować zadane parametry i na podstawie zadanych granicznych wartości generować odpowiednio ostrzeżenia lub błędy
27	musi obsługiwać SNMP

30	musi monitorować usługi systemu HIS i ERP działającego u Zamawiającego
31	musi monitorować pracę systemu PACS działającego u Zamawiającego
32	musi monitorować bazy danych, co najmniej Oracle, MySQL, PostgreSQL
33	musi monitorować działania bramek HL7, działających u Zamawiającego
35	musi umożliwiać monitorowanie parametrów wydajnościowych systemu HIS działającego u zamawiającego
36	musi zapewniać narzędzie (aktualizator) umożliwiające powiadamiające o wszystkich opublikowanych krytycznych uaktualnieniach HIS, które będzie posiadało zdolność ich pobrania do zasobów Zamawiającego.
37	musi obejmować usługę instalacji i konfiguracji uaktualnień, o których mowa w wierszu powyżej.
38	musi być możliwość uruchomienia serwera monitorowania jako maszyny wirtualnej

Monitoring zasobów krytycznych – minimalny zakres aplikacji/usług do nadzoru	
Aplikacje/usługi systemu HIS/ERP	
Eskulap NT	Monitorowanie w zakresie dostępności usługi/aplikacji w ramach dostępnego interfejsu testowego (weryfikacja automatycznej procedury testowej).
Eskulap EDM	
Eskulap eRecepta (P1)	
Eskulap eSkierowanie (eRefferal)	
Eskulap eZWM	
Eskulap NMVS	
Eskulap Serwer JGP	
Eskulap EWUŚ	
Eskulap RZM	
Eskulap NG (Pulpit Lekarski)	
Impuls Portal	
Impuls Harmonogramy	
Serwery aplikacyjne oraz bazodanowe	
Windows	Monitoring serwerów aplikacyjnych (Eskulap oraz Impuls) w zakresie podstawowych parametrów m.in. wykorzystania zasobów dyskowych, pamięci RAM, utylizacji procesora.
Linux	Monitoring serwerów bazy danych (Eskulap oraz Impuls) oraz serwera Docker w zakresie podstawowych parametrów m.in. Wykorzystania zasobów dyskowych, pamięci RAM, utylizacja procesora.
Inne	
Dostęp do Internetu	Powiadomienie o braku dostępności punktów w siec zew. np. brama zew., serwisy DNS zew.
Baza danych Oracle	Monitorowanie podstawowych parametrów działania bazy danych Oracle m.in. dostępność, działanie procesu nasłuch, zajętość przestrzeni tabel, zajętość obszaru FRA.

b. Wymagania dotyczące instalacji

Instalacja odbędzie się na infrastrukturze wskazanej przez Zamawiającego, spełniającej następujące minimalne wymagania:

- Procesor 6 rdzeniowy (vCPU)

- 16 GB RAM
- 300 GB miejsca na dysku

Zamawiający oczekuje instalacji środowiska w postaci maszyny wirtualnej. Wykonawca zainstaluje maszynę wirtualną w wirtualizatorze klienta i dokona konfiguracji adresów IP. Dopuszczone jest zastosowanie oprogramowanie typu Open Source, pod warunkiem możliwości wykupienia wsparcia producenta.

c. Szkolenia

Wraz z wdrożeniem zostanie przeprowadzone szkolenie dla 3 administratorów Zamawiającego z dostarczonego rozwiązania, po którym będą w stanie samodzielnie administrować rozwiązaniem, dodawać nowe usługi/urządzenia do kontrolowania oraz zarządzać otrzymywanymi powiadomieniami. Wykonawca musi również przekazać dokumentację administratora. W zakresie gotowych produktów, dopuszczalna jest dokumentacja w języku angielskim. Zamawiający zapewnia salkę niezbędną do prowadzenia szkoleń.

d. Gwarancja

Na dostarczone rozwiązanie, Wykonawca musi zapewnić 12 miesięczną gwarancję i serwis, w ramach których będzie usuwał błędy dostarczonej usługi oraz wykonywał aktualizacje minimum raz na kwartał. Błędy w działaniu usługi, muszą być usuwane w ciągu 6 dni roboczych. Wykonawca zobowiązany jest zapewnić 12 miesięczną możliwość konsultacji i wsparcia w zakresie administracji wdrożonym rozwiązaniem i rekonfiguracją systemu w przypadku zmian w środowisku informatycznym Zamawiającego.

8. Serwis 24/7

Zamawiający wymaga zapewnienia serwisu 24/7/365 dni w roku dla obsługi awarii systemów operacyjnych i bazodanowych w trybie 24x7. Zamawiający wymaga możliwości telefonicznego zgłoszenia awarii, których można będzie dokonywać poza standardowymi godzinami pracy serwisu. Zamawiający oczekuje świadczenia serwisu w trybie 24/7 przez okres 20 m-cy od daty podpisania Umowy.

Wykonawca musi zapewnić gotowość do usuwania zdarzeń serwisowych dotyczących uszkodzeń Infrastruktury i MBD obejmujących:

a) obsługę serwisową MBD wraz z uruchomionymi instancjami:

- instalacje stand-alone

- instalacje MBD RAC (Linux),

b) obsługę serwisową serwerów aplikacyjnych Windows Server,

c) obsługę serwisową serwerów z systemem Linux,

d) obsługę serwisową serwerów aplikacji skonteneryzowanych (Docker),

e) obsługę serwisową usług oraz aplikacji wdrożonych systemów (co najmniej w zakresie uruchomienia i podłączenia do bazy),

- obsługę serwisową serwera Eskulap: HIS, LIS, RIS i PACS

- obsługę serwisową serwera Eskulap: NT, serwera wydruków, EDM,

f) obsługę serwisową kontrolerów domen (AD), serwerów wydruku, CA,

g) obsługę serwisową środowisk wirtualnych,

h) obsługę serwisową systemu backupu, w ramach którego Wykonawca wykona procedurę backupu i restore całego środowiska minimum raz na rok. Z przeprowadzonych prac Wykonawca udostępni materiał w formie video,

i) obsługę serwisową zdarzeń niepożądanych, zidentyfikowanych przez Monitoring Zasobów Krytycznych,

j) obsługę serwisową zdarzeń uniemożliwiających pracę użytkowników w systemach części białej i szarej szpitala

k) usługi doradcze w ramach doboru rozwiązań w IT (infrastruktura, oprogramowanie),

l) identyfikację przyczyn wystąpienia awarii infrastruktury eksploatowanej przez Klienta (serwerów aplikacyjnych i bazodanowych oraz zasobów dyskowych związanych z serwisowanym oprogramowaniem aplikacyjnym).

9. Szkolenia z cyberbezpieczeństwa

Zamawiający wymaga przeprowadzenia szkoleń dla 25 pracowników podmiotu w zakresie:

1. Kadry pracowniczej
   a) polityka haseł – praktyczne podejście i narzędzia wspomagające;
   b) Vhishing / ID Call Hijacking – aspekty bezpieczeństwa telefonów;
   c) zagrożenia związane z nieznanym sprzętem – jak np. nieznany pendrive może zaszkodzić całej instytucji;
   d) Spear Phishing – wszystko co „powiesz" (w sieci) może zostać użyte przeciwko Tobie – praktyczne aspekty „zachowania" w sieci;
   e) ataki Bruteforce / Ataki Słownikowe – podstawowe metody łamania haseł;
   f) Web Archive – Internet nie zapomina;
   g) pliki Cookies – czym są popularne „ciasteczka";
   h) metadane – czyli dane o danych;
   i) Phishing / Spoofing – nigdy nie wiesz kto jest po drugiej stronie;
   j) socjotechniki – podstawowe definicje i przykłady użycia;
   k) Data Leak – czym jest i jakie zagrożenia niesie;
   l) dobre praktyki - kilka zasad podnoszących bezpieczeństwo.

2. Kadry zarządzającej:

Część I:

   a) zakres przedmiotowy i podmiotowy obowiązywania przepisów dotyczących cyberbezpieczeństwa;
   b) obowiązki podmiotów publicznych;
   c) obowiązki podmiotu publicznego uznanego za operatora usługi kluczowej;
   d) struktura krajowego systemu cyberbezpieczeństwa;
   e) zadania i rola CSIRT NASK - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.

Część II

   a) wprowadzenie do wymagań Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
   b) omówienie założeń wdrożenia (SZBI);

c) zakres i granice (SZBI);
d) polityka bezpieczeństwa informacji (SZBI);
e) cele bezpieczeństwa informacji (SZBI);
f) podejścia do szacowania ryzyka;
g) audyty (SZBI);
h) przegląd zarządzania – rola w procesie doskonalenia (SZBI);
i) kluczowe czynniki skutecznego spełnienia wymagań bezpieczeństwa informacji.

3. Czas trwania szkolenia min. 3 godziny. Szkolenia muszą być przeprowadzone przez specjalistów spełniających wymagania określone w Zarządzeniu Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 roku z uwzględnieniem rekomendacji Centrum e-Zdrowia w zakresie budowy systemów cyberbezpieczeństwa. Zamawiający przekaże listę osób do szkolenia na etapie podpisywania Umowy.

4. Zamawiający zapewnia salkę niezbędną do prowadzenia szkoleń.

5. Wykonawca przeszkoli wskazany przez Zamawiającego personel w terminie ustalonym z Zamawiającym, co potwierdzi protokołem z przeprowadzonego szkolenia oraz wydaniem imiennych zaświadczeń o przebytym szkoleniu.

6. Do oferty należy dołączyć:
a) Certyfikat wdrożonej normy ISO 27001.

.....
podpis
elektroniczny kwalifikowany
lub podpis **zaufany** lub **osobisty**
osoby/-ób uprawnionej/-ych do
reprezentowania Wykonawcy