Osielsko, 22.11.2022 r.

**Zainteresowani Wykonawcy**

**Zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina**

**IiZP.271.D.5.2022**

**Pytanie 1:**

**Część 3: Zakup Urządzenia UTM**

**Opisana przez Zamawiającego spcyfikacja wskazuje tylko na jednego producenta rozwiązań UTM – Fortinet. Czy zamawiający dopuszcza dostarczenie rozwiązania równoważnego o poniższej funkcjonalności:**

OBSŁUGA SIECI

1. Urządzenie pisiada 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 jest wyposażone w Firewall klasy Stateful Inspection.

3. Urządzenie obsługuje translacje adresów NAT n:1, NAT 1:1 oraz PAT.

4. Urządzenie umożliwiają 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 umożliwiają 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 możliwość budowania reguł firewall na podstawie: interfejsów

wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta

źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), 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 możliwość filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie

adresów mac.

8. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie

konfigurowalnych, zestawów reguł firewall.

9. Edytor reguł firewall posiada wbudowany analizator reguł, który wskazuje błędy i sprzeczności

w konfiguracji reguł.

10. Urządzenie ma możliwość uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP

(wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

11. Urządzenie ma możliwość wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras

routingu (np. routingu domyślnego).

12. System umożliwia budowanie reguł bezpieczeństwa w oparciu o definiowane przez

administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) jest 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.

14. Moduł IPS jest opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS

pochodził od zewnętrznego dostawcy.

15. Moduł IPS zabezpiecza przed co najmniej 10 000 ataków i zagrożeń.

16. Administrator ma możliwość tworzenia własnych sygnatur dla systemu IPS.

17. Moduł IPS wykrywa, ale również usuwa szkodliwą zawartość w kodzie HTML oraz

JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po

usunięciu zagrożenia.

18. Urządzenie umozliwia inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w

zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.

19. Administrator ma 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.

20. Urządzenie umozliwia ochronę między innymi przed atakami typu SQL Injection, Cross Site

Scripting (XSS) oraz złośliwym kodem Web2.0.

21. Po zakupie stosownej licencji moduł IPS zapewnia 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).

22. Urządzenie zapewnia automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie umożliwia kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną

i maksymalną wartość pasma.

24. Ograniczenie pasma lub priorytetyzacja reguły firewall jest możliwe względem pojedynczego

połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

25. Urządzenie umozliwia tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a

jedynie na śledzenie konkretnego typu ruchu (monitoring).

26. Urządzenie umozliwia kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie umozliwia zastosowanie jednego z co najmniej dwóch skanerów antywirusowych

dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

28. Co najmniej jeden z dwóch skanerów antywirusowych dostarcza w ramach podstawowej

licencji.

29. Administrator ma możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany

analizie skanerem antywirusowym.

30. Administrator ma 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

31. Urządzenie posiada mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą

niechcianą (SPAM).

32. Ochrona antyspam działa w oparciu o:

a. białe/czarne listy,

b. DNS RBL,

c. Skaner heurystyczny.

33. W przypadku ochrony w oparciu o DNS RBL administrator ma możliwość modyfikowania listy

serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam jest w formacie zgodnym z

formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

35. Urządzenie umożliwia stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja)

lub site-to-site (lokalizacja-lokalizacja).

36. Urządzenie wspiera co najmniej następujące typy sieci VPN:

a. PPTP VPN,

b. IPSec VPN,

c. SSL VPN.

37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.

38. Producent urządzenia mozliwość pobranie klienta VPN współpracującego z oferowanym

rozwiązaniem.

39. Klient SSL VPN jest dostępny z poziomu portalu uwierzytelniania (captive portal)

40. Urządzenie umozliwia funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek

awarii łącza dostawcy podstawowego (VPN Failover).

41. Urządzenie umozlwiia wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

42. Urządzenie umozliwia tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

43. Urządzenie posiada wbudowany filtr URL.

44. Filtr URL działa w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii

tematycznych stron internetowych.

45. Administrator ma możliwość dodawania własnych kategorii URL.

46. Administrator ma 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.

47. Administrator ma możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o

zablokowaniu strony.

48. Strona blokady umożliwia wykorzystanie zmiennych środowiskowych.

49. Filtr URL uwzględnia komunikację po protokole HTTPS.

50. Urządzenie umożliwia identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu

MIME.

51. Urządzenie umożliwia stworzenie listy stron dostępnych po protokole HTTPS, które nie będą

deszyfrowane.

52. Urządzenie oferuje możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

53. Urządzenie umozlwia 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.

54. Urządzenie umożliwia równoczesne użycie co najmniej 5 różnych baz LDAP.

55. Urządzenie umożliwia uruchomienie specjalnego portalu (captive portal), który ma zezwalać

na autoryzację użytkowników co najmniej w oparciu o protokoły:

a. SSL,

b. Radius,

c. Kerberos.

56. Urządzenie umożliwia transparentną autoryzację użytkowników w usłudze katalogowej

Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego

agenta.

58. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu

domeny.

59. Urządzenie posiada wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA

poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

60. Wbudowany moduł 2FA daje możliwość wykorzystania haseł TOTP w ramach tuneli

SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu

administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

61. Urządzenie umozliwia wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci

Internet (tzw. Load Balancing).

62. Mechanizm równoważenia obciążenia łącza internetowego działa w oparciu o następujące dwa

mechanizmy:

a. równoważenie względem adresu źródłowego,

b. równoważenie względem połączenia.

63. Mechanizm równoważenia obciążenia uwzględnia wagi przypisywane osobno dla każdego z

łączy do Internetu.

64. Urządzenie umozlwiia przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego

(tzw. Failover).

65. Urządzenie wspieramechanizm SD-WAN zapewniając automatyczną optymalizację i wybór

najkorzystniejszego łącza.

66. W zakresie SD-WAN urządzenie zapewnia obsługę mechanizmu SLA (monitorowanie

opóźnienia, jitter, wskaźnika utraty pakietów).

67. Monitorowanie dostępności łącza jest możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

68. Urządzenie umożliwia statyczne trasowanie pakietów.

69. Urządzenie Umożliwia trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego

oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

70. Urządzenie umożliwia trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy

Based Routing).

71. Urządzenie umożliwia dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły:

RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

72. Konfiguracja urządzenia jest możliwa z wykorzystaniem polskiego interfejsu graficznego.

73. Interfejs konfiguracyjny jest dostępny poprzez przeglądarkę internetową, a komunikacja ma

być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

74. Administrator ma możliwość wskazania do komunikacji innego portu niż 443 TCP.

75. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także

nakładającymi się) uprawnieniami.

76. Urządzenie oferuje możliwość wykorzystania wbudowanych profili administracyjnych

określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp

tylko do odczytu lub pełen odczyt i zapis.

77. Urządzenie umożliwia zarządzenia z poziomu konsoli (SSH)

78. Urządzenie umożliwia zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

79. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę

internetową, a komunikacja jest zabezpieczona za pomocą protokołu HTTPS.

80. Wbudowany webowy, graficzny interfejs administracyjny urządzenia oferuje narzędzia

diagnostyczne, co najmniej ping, traceroute, nslookup.

81. Wbudowany webowy, graficzny interfejs administracyjny oferuje narzędzia do

przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

82. Wbudowany webowy, graficzny interfejs administracyjny oferuje możliwość zdefiniowania

polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności

hasła.

83. Wbudowany webowy, graficzny interfejs administracyjny oferuje możliwość generowania

skryptów z czynności wykonywanych przez administratora ( script recording ).

84. System oferuje możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL,

certyfikatów, usług internetowych (web services).

85. Urządzenie oferuje portal uwierzytelniania (captive portal) dla użytkowników.

86. Urządzenie umożliwia zapisywanie logów na wbudowanym dysku.

87. Urządzenie umożliwia eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem

transmisji nieszyfrowanej jak i szyfrowanej (TLS).

88. Urządzenie umożliwia eksportowanie logów za pomocą protokołu IPFIX.

89. Urządzenie umożliwia 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

90. Urządzenie umożliwia odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury

producenta lub z dedykowanego serwera zarządzanego przez administratora.

91. Urządzenie umożliwia anonimizację logów co najmniej w zakresie adresu źródłowego oraz

nazwy użytkownika.

RAPORTOWANIE

92. Urządzenie posiada wbudowany w interfejs administracyjny system raportowania i

przeglądania logów zebranych na urządzeniu.

93. System raportowania i przeglądania logów wbudowany w system nie wymaga dodatkowej

licencji do swojego działania.

94. System raportowania posiada predefiniowane raporty dla co najmniej ruchu WEB, modułu

IPS, skanera Antywirusowego, skanera Antyspamowego.

95. System raportowania umożliwia wygenerowanie co najmniej 25 różnych raportów.

96. System raportowania umożliwia edycję konfiguracji bezpośrednio z poziomu raportu.

97. System raportowania umożliwia eksport wyników raportu do formatu CSV.

98. Urządzenie posiada możliwość rozbudowy o dedykowany system zbierania logów i

tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

99. Urządzenie umożliwia monitorowanie swojego stanu w wykorzystanie protokołu SNMP w

wersji 1, 2 i 3.

100. Urządzenie umożliwia monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a

także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

101. Urządzenie umożliwia stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

102. Urządzenie posiada wbudowany serwer DHCP z możliwością dynamicznego przypisywania

adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

103. Urządzenie pozwala na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw.

DHCP Relay).

104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

105. Urządzenie umożliwia stworzenia różnych konfiguracji DHCP dla różnych podsieci

skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia

bramy, serwerów DNS, nazwy domeny).

106. Urządzenie posiada usługę DNS Proxy.

107. Urządzenie posiada wsparcie dla Spanning-tree protocol (RSTP/MSTP).

108. Urządzenie oferuje wsparcie dla IEEE 802.1Q VLAN.

109. Urządzenie ma zaimplementowane Open API

110. Urządzenie psoada dwie niezależne partycje np. w celu zapewnienia działania na wypadek

awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu jest możliwe

zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym

innym momencie.

111. Urządzenie oferuje możliwość zwiększenia wydajności takich parametrów jak

przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez

zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego

urządzenia.

GWARANCJA I SERWIS

112. Urządzenie jest objęte gwarancją producenta na dostarczone element systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.

113. W okresie obowiązywania gwarancji zapewnione jest wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

114. Urządzenie ma wyposażone w dysk SSD o pojemności co najmniej 200 Gb.

115. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych

zasilaczy.

116. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.

117. Liczba portów światłowodowych 10Gbps – min. 2 z możliwością rozszerzenia do 6.

118. Urządzenie pozwala na instalację modułu rozszerzeń z poniższej listy:

a. Moduł z 8 interfejsami miedzianymi 10/100/1000Mbps

b. Moduł z 4 interfejsami miedzianymi 10Gbps

c. Moduł z 8 interfejsami światłowodowymi 1Gbps

d. Moduł z 4 interfejsami światłowodowymi 10Gbps

119. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G

pochodzącego od dowolnego producenta.

120. Urządzenie jest wyposażone w min. 2 różniące się typem, porty konsolowe. Przynajmniej

jeden port konsolowy ma być typu RJ45.

121. Przepustowość Firewall (1518 bajtów UDP) – minimum 18Gbps.

122. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum

10Gbps.

123. Przepustowość filtrowania Antywirusowego – minimum 3Gbps.

124. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 4Gbps.

125. Liczba tuneli VPN IPSec – minimum 1 000.

126. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300.

127. Liczba tuneli typu SSL VPN (tryb portalu) – minimum 300.

128. Obsługa interfejsów 802.11q (VLAN) – minimum 1336.

129. Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.

130. Urządzenie umożliwia budowanie klastrów wysokiej dostępności HA co najmniej w trybie

Active-Passive.

131. Urządzenie jest wyposażone w moduł TPM

132. Urządzenie nie ma limitu na liczbę użytkowników.

133. Liczba reguł filtrowania – minimum 32 768.

134. Liczba tras statycznego routingu – minimum 5 120.

135. Liczba tras dynamicznego routingu – minimum 10 000.

136. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.

Odp. Tak, zamawiający dopuszcza dostarczenie rozwiązania równoważnego zgodnie z powyższą specyfikacją

**Pytanie 2:**

**Dotyczy: Część 1 - Zakup macierzy dyskowej**

**Czy Zamawiający dopuści rozwiązanie, które w zamian podtrzymania bateryjnego przez 72h dopuści rozwiązanie, które realizuje zabezpieczenie pamięci cache zapisu po przez zapisanie danych na pamięć nieulotną?**

Odp. NIE