Siedlce, dnia 4 grudnia 2019 r.

INSPEKCJA WETERYNARYJNA
MAZOWIECKI WOJEWÓDZKI
LEKARZ WETERYNARII
Paweł Jakubczak

WYKONAWCY

- wszyscy -

Nasz znak: WIW-AD.272.97.2019
Dot. sprawy nr: pismo z dnia:

Wyjaśnienie oraz zmiana treści specyfikacji istotnych warunków zamówienia

Działając na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843) Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach przesyła odpowiedzi na zadane pytania Wykonawcy dotyczące treści specyfikacji istotnych warunków zamówienia w postępowaniu o udzielenie zamówienia publicznego nr sprawy: WIW-AD.272.97.2019 na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach** - Pakiet 6: Dostawa urządzeń firewall:

Pytanie nr 1: W specyfikacji Pakiet 6: Dostawa urządzeń firewall jest zapis o gwarancji 36 miesięcy oraz zapis "Do urządzeń powinny być załączone min. 3 miesięczne licencje ..." co jest sprzeczne z zasadami świadczenia gwarancji przez producentów urządzeń zabezpieczenia brzegu sieci komputerowej - firewall. Czy Zamawiający zgodzi się aby okres gwarancji był zgodny z zaoferowanym okresem licencji na urządzenie?

Odpowiedź nr 1: Zamawiający nie wyraża zgody. Zamawiający oczekuje od Wykonawców zaoferowania 3 miesięcznej licencji. Stosowna zmiana zostanie naniesiona do treści specyfikacji istotnych warunków zamówienia

Pytanie nr 2: Czy zamawiający zgodzi się na okres gwarancji 12 miesięcy?

Odpowiedź nr 2: Zamawiający wyraża zgodę na zaoferowanie urządzenia z 12 miesięcznym terminem gwarancji. Stosowna zmiana zostanie naniesiona do treści specyfikacji istotnych warunków zamówienia.

W związku z powyższym, działając na podstawie art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843) Wojewódzki Inspektorat Weterynarii z siedzibą w Siedlcach informuje, iż dokonał zmiany treści specyfikacji istotnych warunków zamówienia w postępowaniu o udzielenie zamówienia publicznego nr sprawy WIW-AD.272.97.2019 na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach**.

Zapisy Rozdziału XVI SIWZ – Szczegółowy opis przedmiotu zamówienia otrzymują brzmienie zgodnie z treścią Załącznika nr 1 do niniejszego zawiadomienia.

W pozostałym zakresie Specyfikacja Istotnych Warunków Zamówienia pozostaje niezmieniona.

MAZOWIECKI WOJEWÓDZKI
LEKARZ WETERYNARII
lek. wet. Paweł Jakubczak

Załącznik nr 1

ROZDZIAŁ XVI SIWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **dostawa oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach** w następujących ilościach i o następujących parametrach technicznych:

Pakiet nr 6: Dostawa urządzeń firewall:

Lp.	Przedmiot zamówienia	Opis - Parametry techniczne	Ilość zamawiana	Wielkość opakowania	Wymagany termin gwarancji
1.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, 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 dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).	2	szt.	**12 miesięcy u producenta urządzenia**

		5. Interface (GUI) do konfiguracji firewalla 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 etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.			

		11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia 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. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA**			

		21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. 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 odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site			

		(klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 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. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.			

		52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 62. Rozwiązanie powinno wspierać technologię Link Aggregation. **POZOSTAŁE ROZWIĄZANIA USŁUGI I FUNKCJE**			

		63. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 68. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 69. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 70. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 71. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https. 72. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 73. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 74. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.			

		75. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 76. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 77. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 78. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 79. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 80. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 81. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 82. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 83. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 84. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 85. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu			

		zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 86. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE** 87. Urządzenie ma być wyposażone w dysk o pojemności co najmniej 250 GB. 88. Liczba portów Ethernet 10/100/1000Mbps – min. 12. 89. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 90. Przepustowość Firewalla – min. 5 Gbps 91. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps. 92. Przepustowość filtrowania Antywirusowego – min. 850 Mbps 93. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps. 94. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500 95. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100 96. Obsługa min. VLAN 256 97. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę. 98. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 99. Urządzenie powinno być nielimitowane na użytkowników. 100. Każde z urządzeń musi mieć możliwość pracy jako drugie w klastrze HA dwóch urządzeń niniejszej			

		specyfikacji, działających co najmniej w trybie Active/Passive 101. Wykonawca przy udziale pracownika Zamawiającego przeprowadzi wymianę dwóch urządzeń NETASQ U 150S zainstalowanych w lokalizacji: siedziba główna Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach, ul. Kazimierzowska 29, 08-110 Siedlce. Wykonawca przeniesie konfigurację jednego obecnego urządzenia na dostarczone urządzenie, drugie urządzenie skonfiguruje do pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzeń powinny być załączone **3 miesięczne licencje** dla następujących usług urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja.			
2.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.	2	szt.	**12 miesięcy u producenta urządzenia**

		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 dawać możliwość 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 firewalla 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 etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny			

		serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia 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. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do			

		pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. 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 odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów.			

		Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL.			

		39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 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. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory.			

		49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.			

		60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA** 62. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 63. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 64. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 65. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 66. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 67. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 68. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 71. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP).			

		72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 79. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 80. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.			

		81. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 82. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 83. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 84. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 85. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE** 86. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 87. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 88. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 89. Przepustowość Firewalla – min. 3,5 Gbps 90. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps. 91. Przepustowość filtrowania Antywirusowego – min. 400 Mbps 92. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps. 93. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100.			

		94. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 95. Obsługa min. VLAN 64 96. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 97. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 98. Urządzenie powinno być nielimitowane na użytkowników. 99. Urządzenie musi być wyposażone dodatkowo w nośnik pamięci flash o pojemności minimum 64 GB (gwarancja na pamięć min. 12 miesięcy) 100. Wykonawca dostarczy dedykowane rozwiązanie do tworzenia raportów w formie maszyny wirtualnej do zainstalowania w środowisku zamawiającego dla wszystkich urządzeń niniejszej specyfikacji. 101. Wykonawca przy wsparciu pracownika Zamawiającego wymieni urządzenia NETASQ U 70S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie, ul. Lechicka 21, 02-156 Warszawa oraz urządzenia NETASQ U 30S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce, ul. Składowa 8A, 07-411 Ostrołęka. Wykonawca przeniesie konfigurację obecnych urządzeń na dostarczone urządzenia. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzenia powinny być załączone **3 miesięczne** licencje dla następujących usług urządzenia: Firewall z			

		mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja. Wykonawca przeprowadzi jednodniowe warsztaty techniczne ze wszystkich urządzeń niniejszego pakietu w języku polskim dla dwóch pracowników Zamawiającego w siedzibie i na urządzeniach Wykonawcy w terminie do 31 marca 2020 roku.			

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr.

_____ dnia __ __ 2019 rok

_____

(podpis osób wskazanych w dokumencie uprawniającym do wystąpienia w obrocie prawnym lub posiadającym pełnomocnictwo)

Nr sprawy: WIW-AD.272.97.2019

Załącznik nr 5 do SIWZ

SPECYFIKACJA OFEROWANEGO PRZEDMIOTU ZAMÓWIENIA

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **dostawę oprogramowania i sprzętu komputerowego dla Wojewódzkiego Inspektoratu Weterynarii z siedzibą w Siedlcach,**

Pakiet 6: Dostawa urządzeń firewall:

—	Parametry Zamawiającego		Oferowane przez Wykonawcę parametry*	
Lp.	**Przedmiot zamówienia**	**Opis - Parametry techniczne**	**Przedmiot zamówienia (nazwa, producent, numer katalogowy***	**Parametry techniczne***
1.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, 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 dawać możliwość 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 firewalla 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 etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)**		

		10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia 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. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu		

		IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. 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 odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner.		

		27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)** 29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL.		

		37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 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. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.		

		47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)**		

		54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 62. Rozwiązanie powinno wspierać technologię Link Aggregation. **POZOSTAŁE ROZWIĄZANIA USŁUGI I FUNKCJE**		

		63. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 68. Urządzenie musi posiadać usługę DNS Proxy. **ADMINISTRACJA URZĄDZENIEM** 69. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 70. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 71. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https. 72. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 73. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 74. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego		

		zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 75. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 76. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 77. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 78. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 79. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 80. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 81. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 82. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.		

		83. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 84. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 85. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 86. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE** 87. Urządzenie ma być wyposażone w dysk o pojemności co najmniej 250 GB. 88. Liczba portów Ethernet 10/100/1000Mbps – min. 12. 89. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 90. Przepustowość Firewalla – min. 5 Gbps 91. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps. 92. Przepustowość filtrowania Antywirusowego – min. 850 Mbps 93. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps. 94. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500		

		95. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100 96. Obsługa min. VLAN 256 97. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę. 98. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 99. Urządzenie powinno być nielimitowane na użytkowników. 100. Każde z urządzeń musi mieć możliwość pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji, działających co najmniej w trybie Active/Passive 101. Wykonawca przy udziale pracownika Zamawiającego przeprowadzi wymianę dwóch urządzeń NETASQ U 150S zainstalowanych w lokalizacji: siedziba główna Wojewódzkiego Inspektoratu Weterynarii z/s w Siedlcach, ul. Kazimierzowska 29, 08-110 Siedlce. Wykonawca przeniesie konfigurację jednego obecnego urządzenia na dostarczone urządzenie, drugie urządzenie skonfiguruje do pracy jako drugie w klastrze HA dwóch urządzeń niniejszej specyfikacji. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzeń powinny być załączone **3 miesięczne** licencje dla następujących usług		

		urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja.		
2.	Urządzenie zabezpieczenia brzegu sieci komputerowej - firewall	Dostawa urządzenia nowego i nie regenerowanego, o nie gorszych parametrach technicznych niż wskazano poniżej: **OBSŁUGA SIECI** 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, 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 dawać możliwość 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 firewalla 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 etc.) przy wykorzystaniu		

		obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator powinien mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). **INTRUSION PREVENTION SYSTEM (IPS)** 10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.		

		13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia 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. **KSZTAŁTOWANIE PASMA (Traffic Shapping)** 17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. **OCHRONA ANTYWIRUSOWA** 21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów		

		antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. 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 odrzucenia. **OCHRONA ANTYSPAM** 25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. **WIRTUALNE SIECI PRYWANTE (VPN)**		

		29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. **FILTR DOSTĘPU DO STRON WWW** 36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.		

		41. Administrator powinien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 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. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie powinno posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. **UWIERZYTELNIANIE** 48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory.		

		49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie powinna wymagać instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie powinna wymagać modyfikacji schematu domeny. **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** 54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.		

		57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA** 62. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 63. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 64. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 65. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 66. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 67. Urządzenie musi posiadać usługę DNS Proxy.		

		ADMINISTRACJA URZĄDZENIEM 68. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim. 70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 71. Komunikacja powinna móc odbywać się na porcie innym niż https (443 TCP). 72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup		

		konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. **RAPORTOWANIE** 79. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 80. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 81. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 82. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 83. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 84. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 85. Dodatkowy system powinien umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy **PARAMETRY SPRZĘTOWE**		

		86. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 87. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 88. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 89. Przepustowość Firewalla – min. 3,5 Gbps 90. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps. 91. Przepustowość filtrowania Antywirusowego – min. 400 Mbps 92. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps. 93. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100. 94. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 95. Obsługa min. VLAN 64 96. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 97. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 98. Urządzenie powinno być nielimitowane na użytkowników. 99. Urządzenie musi być wyposażone dodatkowo w nośnik pamięci flash o pojemności minimum 64 GB (gwarancja na pamięć min. 12 miesięcy) 100. Wykonawca dostarczy dedykowane rozwiązanie do tworzenia raportów w formie maszyny wirtualnej do zainstalowania w		

		środowisku zamawiającego dla wszystkich urządzeń niniejszej specyfikacji. 101. Wykonawca przy wsparciu pracownika Zamawiającego wymieni urządzenia NETASQ U 70S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie, ul. Lechicka 21, 02-156 Warszawa oraz urządzenia NETASQ U 30S zainstalowanego w lokalizacji: Zakład Higieny Weterynaryjnej w Warszawie Oddział Terenowy w Ostrołęce, ul. Składowa 8A, 07-411 Ostrołęka. Wykonawca przeniesie konfigurację obecnych urządzeń na dostarczone urządzenia. Proces przenoszenia przez Wykonawcę konfiguracji i produkcyjne uruchomienie transmisji danych na dostarczanym urządzeniu nie może wpływać na utrzymanie ciągłości transmisji danych w trakcie godzin pracy. Wymieniane urządzenia pozostaną u Zamawiającego. 102. Do urządzenia powinny być załączone **3 miesięczne** licencje dla następujących usług urządzenia: Firewall z mechanizmem Intrusion Prevention System, WIRTUALNE SIECI PRYWANTE (VPN), FILTR DOSTĘPU DO STRON WWW, OCHRONA ANTYWIRUSOWA, OCHRONA ANTYSPAM. Zakres funkcjonalny wymienionych usług urządzenia w okresie realizacji licencji czasowych powinien być zgodny i nie mniejszy niż określa niniejsza specyfikacja.		

		Wykonawca przeprowadzi jednodniowe warsztaty techniczne ze wszystkich urządzeń niniejszego pakietu w języku polskim dla dwóch pracowników Zamawiającego w siedzibie i na urządzeniach Wykonawcy w terminie do 31 marca 2020 roku.		

*do wypełnienia przez Wykonawcę, zapisy „Tak", „Zgodnie", czy „Spełnia" „Jak obok" nie będą akceptowane, należy podać precyzyjnie rzeczywisty oferowany parametr. Wypełniają Wykonawcy składający ofertę na dany pakiet.

_____ dnia __ __ 2019 rok

_____

(pieczęć i podpis)