**Załącznik nr 1a do SIWZ**

**Przedmiotem zamówienia jest dostawa nowego sprzętu komputerowego i oprogramowania dla Katolickiego Uniwersytetu Lubelskiego Jana Pawła II z podziałem na części:**

**FORMULARZ OFEROWANYCH PARAMETRÓW TECHNICZNYCH**

**Część 1 - Dostawa urządzeń sieciowych:**

Zadanie 1. Dostawa sprzętowego urządzenia firewall typ A (1szt):

|  |  |  |
| --- | --- | --- |
| **Nazwa oferowanego urządzenia** |  | |
| **Producent** |  | |
| **Typ/model/kod producenta** |  | |
| **Sprzętowe urządzenie firewall typ A – 1 szt.** | | |
| **Minimalne wymagane parametry** | | |
| 1.Zaoferowane urządzenie musi posiadać metalową obudowę o wysokości nie większej niż 1RU i musi być przystosowane do montażu w szafie teleinformatycznej 19”.  2.Urządzenie musi być dostarczone wraz z elementami montażowymi do szafy 19”, jeśli nie są one integralną częścią urządzenia.  3.~~Całkowite rozmiary urządzenia nie mogą być większe niż (wysokośćxszerokośćxgłębokość): 43 x 43 x 40cm.~~ Całkowite rozmiary urządzenia nie mogą być większe niż (wysokośćxszerokośćxgłębokość): 4,5 x 45 x 40cm.  4.Układ chłodzenia urządzenia musi być skonstruowany w taki sposób, aby powietrze było chwytane z przodu urządzenia a gorące powietrze było wydmuchiwane z tyłu urządzenia.  5.Urządzenie musi być przystosowane do pracy w temperaturze od -5 do 40 stopni Celsjusza.  6. Urządzenie na panelu czołowym musi posiadać świetlną sygnalizację co najmniej następujących stanów urządzenia: wystąpiła awaria zasilacza, wystąpiła krytyczna awaria urządzenia, co najmniej jedno połączenie VPN jest zestawione.  7. Urządzenie musi umożliwiać monitorowanie temperatury procesorów urządzenia, temperatury zasilacza/zasilaczy oraz prędkości obrotowej wentylatorów.  8. Urządzenie musi się automatycznie wyłączyć w przypadku wykrycia temperatury grożącej uszkodzeniem podzespołów urządzenia.  9. Urządzenie musi posiadać wbudowane co najmniej 8 miedzianych portów 1000BASE-T.  10. Urządzenie musi umożliwiać rozbudowę o co najmniej 6 miedzianych portów 1000BASE-T lub o co najmniej 6 światłowodowych portów SFP ze wsparciem dla wkładek 1000BASE-SX i wkładek 1000BASE-LX.  11. Urządzenie musi posiadać 1 miedziany port 1000BASE-T dedykowany do zarządzania.  12. Urządzenie musi posiadać 1 port konsoli RJ-45.  13. Urządzenie musi posiadać co najmniej 2 porty USB 2.0 i umożliwiać podłączenie do nich zewnętrznej pamięci flash do kopiowania plików z i na wewnętrzną pamięć flash urządzenia.  14. Urządzenie musi być wyposażone w co najmniej 8GB pamięci flash.  15. ~~Urządzenie musi być wyposażone w co najmniej 12GB pamięci RAM~~. Urządzenie musi być wyposażone w co najmniej 8GB pamięci RAM.  16. Urządzenie musi być wyposażone w procesor 4 rdzeniowy.  17. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.  18. ~~Urządzenie musi posiadać zasilacz prądu zmiennego 230V o mocy nie większej niż 100W~~. Urządzenie musi posiadać zasilacz prądu zmiennego 230V o mocy nie większej niż 110W.  19. Urządzenie musi być wyposażone w 1 dysk SSD o pojemności co najmniej 120GB.  20. Maksymalna wydajność urządzenia dla usługi firewalla IPv4 i IPv6 nie może być mniejsza niż 2Gbps.  21. Wydajność urządzenia dla ruchu typu multi-protocol dla usługi firewalla IPv4 i IPv6 nie może być mniejsza niż 1Gbps.  22. Wydajność urządzenia nie może być mniejsza niż 650Mbps dla równocześnie włączonej usługi firewalla i ochrony przed nieznanymi (ang. zero-day) zagrożeniami i filtrowania www.  23. Urządzenie musi obsługiwać co najmniej 20.000 nowych połączeń na sekundę.  24. Urządzenie musi obsługiwać co najmniej 500.000 równoczesnych połączeń.  25. Urządzenie dla pakietów o rozmiarze 64 bajtów musi oferować wydajność nie mniejszą niż 700.000 pakietów na sekundę.  26. Urządzenie musi być wyposażone w sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji szyfrowania algorytmami DES/3DES/AES i oferować wydajność szyfrowania nie mniejszą niż 300Mbps.  27. Urządzenie musi umożliwiać równoczesną obsługę co najmniej 750 tuneli VPN wykorzystujących IPsec.  28. Urządzenie musi umożliwiać równoczesną obsługę co najmniej 750 tuneli VPN wykorzystujących SSL.  29. Urządzenie musi obsługiwać co najmniej 200 sieci VLAN.  30. Urządzenie musi umożliwiać konfigurację wirtualnych firewalli. Wymagana jest obsługa co najmniej 2 wirtualnych firewalli oraz możliwość licencyjnego zwiększenia liczby wirtualnych firewalli do co najmniej 30.  31. Urządzenie musi być wyposażone w sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji porównywaniu ciągów znaków z wykorzystaniem wyrażeń regularnych.  32. Urządzenie musi obsługiwać ramki Ethernet typu Jumbo (o rozmiarze 9216 bajtów).  33. Urządzenie musi obsługiwać ramki XOFF zgodnie z definicją standardu 802.3x.  34. Urządzenie musi działać pod kontrolą 64-bitowego dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.  35. Urządzenie musi umożliwiać zarządzanie:  - przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.  - przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji  - programowo przez interfejs API dostępny przy pomocy protokołu https  - przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji.  36. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.  37. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.  38. Urządzenie musi umożliwiać konfigurację maksymalnej równoczesnej liczby sesji zdalnego zarządzania.  39. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.  40. Urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.  41. Urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.  42. Urządzenie musi umożliwiać uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Bases Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS i TACACS+.  43. Urządzenie musi posiadać zaawansowaną instrumentację pozwalającą na uzyskanie szczegółowej informacji o obciążeniu CPU przez każdy z procesów oddzielnie, z podziałem na procesy, w interwałach czasowych 5 minut, 1 minuta i 5 sekund.  44. Urządzenie nie może posiadać ograniczenia na liczbę równocześnie podłączonych urządzeń (komputerów, drukarek, telefonów, kamer ip, etc) do sieci chronionej.  45. Urządzenie musi umożliwiać realizację modelu wysokiej dostępności w trybach active-standby oraz active-active.  46. Urządzenie musi umożliwiać agregację portów w jeden port logiczny przy pomocy protokołu 802.3ad lub przy pomocy statycznej konfiguracji.  47. Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPFv2 i OSPFv3.  48. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania list kontroli dostępu dla ruchu multicastowego.  49. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.  50. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości 256, 384 i 512 bitów.  51. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) i Galois Message Authentication Code (GMAC).  52. Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19,20 i 21.  53. Urządzenie musi obsługiwać protokół DSA w przestrzeni krzywych eliptycznych (ECDSA).  54. Urządzenie musi obsługiwać protokół WCCPv2 .  55. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.  56. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay) dla IPv4 i IPv6.  57. Urządzenie musi współpracować z serwerami certyfikatów (CA) przy pomocy protokołu SCEP.  58. Urządzenie musi współpracować z zewnętrznymi serwerami uwierzytelnienia i autoryzacji z wykorzystaniem protokołów LDAP, RADIUS i TACACS+.  59. Urządzenie musi obsługiwać protokół NetFlow v9 (RFC 3954).  60. Usługa firewalla realizowane przez urządzenie musi wspierać tryb pracy w warstwie 3 (tryb routed) i tryb pracy w warstwie 2 (tryb transparentny).  61. Urządzenie musi umożliwiać grupowanie VLANów w transparentnym trybie pracy firewalla. Wymagana jest możliwość zdefiniowania co najmniej 8 takich grup po 4 VLANy. Każda tak zdefiniowana grupa musi umożliwiać realizację odrębnych list kontroli dostępu.  62. Urządzenie musi umożliwiać wdrożenia w scenariuszu z routingiem asymetrycznym.  63. Usługa firewalla realizowana przez urządzenie musi umożliwiać filtrowanie ruchu IPv4 i IPv6 w oparciu o sekwencyjne przetwarzanie reguł dostępu (ang. Access Control Entries) zorganizowanych w listy kontroli dostępu (ang. Access Controll List) przypisane do wybranych interfejsów urządzenia.  64. Listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:  - źródłowy i docelowy adres IPv4  - źródłowy i docelowy adres IPv6  - źródłowy i docelowy numer portu UDP  - źródłowy i docelowy numer portu TCP  - nazwy domenowej hosta źródłowego lub docelowego  - nazwa użytkownika w usłudze katalogowej Microsoft Active Directory  - nazwa grupy w usłudze katalogowej Microsoft Active Directory  - czas  65. Paremetry reguł wykorzystywane w listach kontroli dostępu muszą umożliwiać ich hierarchiczną organizację w grupy i wykorzystywanie ich przy budowaniu reguł dostępu.  66. Urządzenie nie może posiadać żadnych ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane.  67. Urządzenie musi realizować mechanizmy inspekcji aplikacyjnej i kontroli zgodności z formalną definicją protokołu dla następujących protokołów: DNS, ESMTP, FTP, H.323, HTTP, ICMP, MGCP, NETBIOS, PPTP, RSH, RTSP, SCCP, SIP, SNMP, SQLNET, RPC, TFTP.  68. Urządzenie musi umożliwiać inspekcję ruchu IPv4 z wykorzystaniem nagłówków: End of Options List, No Operation, Router Alarm.  69. Urządzenie musi umożliwiać inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload.  70. Jeśli pakiet IPv4/IPv6 został pofragmentowany, urządzenie musi odtworzyć oryginalny pakiet kontrolując przy tym kolejność fragmentów i ich intergralność .  71. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby równocześnie odtwarzanych z fragmentów pakietów IPv4/IPv6 per każdy interfejs urządzenia realizujący usługę firewalla.  72. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby fragmentów w ramach jednego odtwarzanego pakietu.  73. Urządzenie musi umożliwiać skonfigurowanie maksymalnego dopuszczalnego okresu czasu, w którym musi otrzymać wszystkie fragmenty niezbędne do odtworzenia pakietu.  74. Urządzenie musi umożliwiać skonfigurowanie mechanizmu randomizującego numery sekwencyjne nowych połączeń TCP.  75. Urządzenie musi umożliwiać nadpisanie wartości MSS w nagłówku TCP.  76. Urządzenie musi umożliwiać zaawansowane badanie stanu każdej sesji TCP w zakresie:  - sprawdzania opcji TCP, usuwania opcji TCP i odrzucania segmentów z opcjami TCP  - poprawności pola TCP ACK  - poprawności sekwencjonowania segmentów TCP (seq-past-window) ze wsparciem mechanizmów akceleracji sieci WAN wprowadzających przesunięcie numerów sekwencyjnych TCP  - weryfikacji sumy kontrolnej segmentu TCP  - weryfikacji pola TCP SACK ALLOW  - weryfikacji wielkości okna TCP  - usuwania flagi URG  - usuwania segmentów przekraczających maksymalny rozmiar (MSS)  - usuwania segmentów z flagą SYN i z flagami SYN/ACK, jeśli zawierają one dane  77. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.  78. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych półotwartych połączeń TCP zestawionych do hosta lub do grupy hostów.  79. Urządzenie musi umożliwiać zresetowanie otwartego połączenia TCP, jeśli przez określony okres czasu przez połączenie nie przesyłano żadnych danych.  80. Urządzenie musi umożliwiać inspekcję ruchu HTTP w zakresie:  - zgodności z formalną definicją protokołu  - ukrywania nagłówka Server w odpowiedzi HTTP  - filtrowania dopuszczalnych metod HTTP  - filtrowania dopuszczalnych typów MIME  - filtrowania dopuszczalnych adresów URL  81. Urządzenie musi umożliwiać inspekcję ruchu SMTP w zakresie:  - zgodności z formalną definicją protokołu ESMTP  - ukrywania wiadomości powitalnej serwera  - filtrowania długości wydawanych komend  - filtrowania listy odbiorców dłuższej niż określona liczba  - filtrowania długości adresu nadawcy  - filtrowania długości pola MIME  - filtrowania dopuszczalnych typów MIME  82. Urządzenie musi umożliwiać inspekcję ruchu DNS w zakresie:  - zgodności z formalną definicją protokołu DNS  - filtrowania długości wiadomości  - filtrowania po typie zapytania  - randomizowania numeru identyfikacyjnego wiadomości  - weryfikacji zgodności numeru indentyfikacyjnego zapytania i odpowiedzi  - blokowania innych odpowiedzi niż pierwsza (ochrona przed atakiem dns spoofing i dns poisoning)  83. Urządzenie musi zapewniać mechanizmy pozwalające na blokowanie aplikacji tunelowanych z użyciem portu 80 w tym blokowanie komunikatorów internetowych i aplikacji typu peer-to-peer.  84. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6.  85. Urządzenie musi wspierać mechaniz translowania adresów sieciowych NAT dla ruchu multicastowego.  86. Urządzenie musi umożliwiać więcej niż 65535 dynamicznych translacji PAT do pojedynczego zewnętrznego adresu IP.  87. Urządzenie musi umożliwiać konfigurację czasu ważności translacji PAT.  88. Urządzenie wykonując dynamiczne translacje PAT do puli zewnętrznych adresów IP, musi równomiernie korzystać ze wszystkich zdefiniowanych w puli adresów.  89. Urządzenie musi umożliwiać konfigurację następujących mechanizmów zarządzania jakością przesyłania danych (Quality of Service):  - obsługa kolejki priorytetowej o konfigurowalnej długości przez każdy interfejs urządzenia realizujący usługę firewalla– pakiety umieszczone w tej kolejce zostaną obsłużone przed innymi pakietami umieszczonymi w innych kolejkach  - policing – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez odrzucanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps. Policing musi być obsługiwany dla ruchu wchodzącego i wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.  - shaping – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez buforowanie pakietów z  dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps konfigurowalną z granularnością co najmniej 8kbps. Zbuforowane pakiety są wysyłane w późniejszym okresie czasu, gdy sumaryczna przepustowość strumieni danych będzie niższa niż zadana wartość w bps. Shaping musi być obsługiwany co najmniej dla ruchu wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.  90. Wraz z urządzeniem należy dostarczyć oprogramowanie klienckie służące do zestawiania połączeń IPsec i SSL VPN z komputerów stacjonarnych działających pod kontrolą systemów operacyjnych Microsoft Windows XP/Vista/7 – 32 i 64-bity, Mac OS X 10.5 i 10.6 i Linux.  91. Wraz z urządzeniem należy dostarczyć oprogramowanie klienckie służące do zestawiania połączeń IPsec i SSL VPN z urządzeń mobilnych działających pod kontrolą Apple IOS oraz Google Android.  92. Urządzenie musi umożliwiać uwierzytelnienie użytkowników zestawiających połączenia VPN przy pomocy nazwy użytkownika i hasła, z wykorzystaniem serwerów haseł jednorazowych lub certyfikatów.  93. Baza użytkowników wykorzystywana przez urządzenie w procesie uwierzytelnienia użytkowników zestawiających połączenia VPN może być zdefiniowana lokalnie na urządzeniu lub zdefiniowana na. na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS i LDAP.  94. Urządzenie musi umożliwiać autoryzację użytkowników przy pomocy atrybutów użytkownika przypisanych w usłudze katalogowej Microsoft Active Directory lub innej.  95. Urządzenie musi umożliwiać przypisanie adresu IP użytkownikom nawiązującym połączenie VPN z lokalnie zdefiniowanej puli adresów IP, przy pomocy zewnętrznego serwera IP, przy pomocy statycznego przypisania po stronie usługi katalogowej Microsoft Active Directory lub innej.  96. Urządzenie musi rozpoznawać i umożliwiać filtrowanie co najmniej 1100 aplikacji a w tym co najmniej następujące: Skype, Dropbox, eDonkey, Bittorent, Gnutella, Google Docs, Google Talk, iCloud, Megaupload, RapidShare, YouTube, Facebook, Google Plus, ssh, dns, http, ftp, sip, rtp, TOR.  97. Urządzenie do rozpoznawania aplikacji musi wykorzystywać sygnatury, heurystykę i badanie treści umożliwiając rozpoznanie aplikacji również wtedy, gdy działają na portach niestandardowych.  98. Urządzenie w ramach rozpoznawanych aplikacji webowych musi umożliwiać detekcję tak zwanych mikroaplikacji w celu granularnego filtrowania czynności, które może wykonać użytkownik korzystający z danej aplikacji webowej.  99. Urządzenie w stosunku do rozpoznawanych webowych aplikacji umożliwiających transfer i współdzielenie plików musi umożliwiać zablokowanie wgrywania plików na przestrzeń dyskową udostępnianą przez tę aplikację.  100.Urządzenie musi umożliwiać tworzenie reguł filtrowania aplikacji w oparciu o typ urządzenia wykorzystywanego do nawiązania połączenia.  101.Urządzenie musi umożliwiać tworzenie reguł filtrowania w opraciu o nazwę użytkownika lub nazwę grupy, do której należy użytkownik. Informacje na temat użytkownika i grup, do których należy użytkownik urządzenie musi pobierać z Microsoft Active Directory lub z innych serwerów usług katalogowych dostępnych przy pomocy protokołu LDAP.  102.Urządzenie współpracując z Microsoft Active Directory musi umożliwiać transparentną identyfikację użytkownika w sposób nie wymagając żadnych dodatkowych akcji ze strony użytkownika.  103.Urządzenie musi umożliwiać aktywną identyfikację użytkownika przy pomocy przeglądarki internetowej z wykorzystaniem protokołów NTLM lub Kerberos.  104.Urządzenie musi umożliwiać wykorzystanie aktywnej metody identyfikacji użytkownika w przypadku, gdy metoda transparentna nie dostarczy informacji o tożsamości użytkownika.  105.Urządzenie musi umożliwiać raportowanie aktywności użytkowników historycznie i na bieżąco.  106.Wszystkie funkcje ochronne oraz zastosowane technologie włącznie z systemem operacyjnym muszą pochodzić od tego samego producenta.  107.Dokumentacja do urządzenia musi być publicznie dostępna na stronie internetowej producenta.  108.Producent musi publikować na swojej stronie internetowej informacje o wykrytych lukach bezpieczeństwa w urządzeniu.  109.Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refubrished/odnowionych (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).  110.Urządzenie musi pochodzić z legalnego kanału sprzedaży producenta urządzenia. Kupujący zastrzega sobie możliwość weryfikacji numerów seryjnych dostarczonego urządzenia u producenta w celu sprawdzenia czy urządzenie pochodzi z legalnego kanału sprzedaży.  111.**Urządzenie musi być objęte co najmniej 3 letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. W ramach w/w serwisu należy zapewnić dostęp do aktualizacji mechanizmów dynamicznego rozpoznawania aplikacji przez okres 5 lat.** | | |
| Dane teleadresowe punktu serwisowego (adres, nr telefonu, faksu, email) | |  |

Zadanie 2. Dostawa sprzętowego urządzenia firewall typ B (2szt):

|  |  |  |
| --- | --- | --- |
| **Nazwa oferowanego urządzenia** | |  |
| **Producent** | |  |
| **Typ/model/kod producenta** | |  |
| **Sprzętowe urządzenie firewall typ B – 2 szt.** | | |
| **Minimalne wymagane parametry** | | |
| 1. Urządzenie musi posiadać metalową obudowę.  2. Całkowite rozmiary urządzenia nie mogą być większe niż (wysokość x szerokość x głębokość): 4.5x 21 x 18 cm.  3. Całkowita waga urządzenia nie może przekraczać 1,8 kilograma.  4. Urządzenie musi być przystosowane do pracy w temperaturze od 0 do 40 stopni Celsjusza.  5. Urządzenie na panelu czołowym musi posiadać świetlną sygnalizację co najmniej następujących stanów urządzenia: wystąpiła krytyczna awaria urządzenia, co najmniej jedno połączenie VPN jest zestawione.  6. Urządzenie musi posiadać wbudowane co namniej 8 miedzianych portów  100BASE-TX w tym co najmniej 2 porty muszą wspierać PoE zgodnie z 802.3af.  7. Urządzenie musi posiadać 1 port konsoli RJ-45.  8. Urządzenie musi posiadać co najmniej 2 porty USB 2.0 i umożliwiać podłączenie do nich zewnętrznej pamięci flash do kopiowania plików z i na wewnętrzną pamięć flash urządzenia.  9. Urządzenie musi być wyposażone w co najmniej 128MB pamięci flash.  10. Urządzenie musi być wyposażone w co najmniej 512MB pamięci RAM.  11. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.  12. Urządzenie nie może posiadać żadnych elementów ruchomych takich jak wentylatory.  13. Maksymalna wydajność urządzenia dla usługi firewalla IPv4 i IPv6 nie może być mniejsza niż 150Mbps.  14. Urządzenie musi obsługiwać co najmniej 4.000 nowych połączeń na sekundę.  15. Urządzenie musi obsługiwać co najmniej 10.000 równoczesnych połączeń.  16. Urządzenie dla pakietów o rozmiarze 64 bajtów musi oferować wydajność nie mniejszą niż 85.000 pakietów na sekundę.  17. Urządzenie musi być wyposażone w sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji szyfrowania algorytmami DES/3DES/AES i oferować wydajność szyfrowania nie mniejszą niż 100Mbps.  18. Urządzenie musi umożliwiać równoczesną obsługę co najmniej 10 tuneli VPN wykorzystujących IPsec.  19. Urządzenie musi obsługiwać co najmniej 3 sieci VLAN.  20. Urządzenie musi działać pod kontrolą 32-bitowego dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.  21. Urządzenie musi umożliwiać zarządzanie:  - przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.  - przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji  - programowo przez interfejs API dostępny przy pomocy protokołu https  - przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji.  22. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.  23. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.  24. Urządzenie musi umożliwiać konfigurację maksymalnej równoczesnej liczby sesji zdalnego zarządzania.  25. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.  26. Urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.  27. Urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.  28. Urządzenie musi umożliwiać uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Bases Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS i TACACS+.  29. Urządzenie musi posiadać zaawansowaną instrumentację pozwalającą na uzyskanie szczegółowej informacji o obciążeniu CPU przez każdy z procesów oddzielnie, z podziałem na procesy, w interwałach czasowych 5 minut, 1 minuta i 5 sekund.  30. Urządzenie nie może posiadać ograniczeń na liczbę urządzeń w sieci chronionej (komputerów, drukarek, telefonów, kamer ip, etc).  31. Urządzenie musi umożliwiać agregację portów w jeden port logiczny przy pomocy protokołu 802.3ad lub przy pomocy statycznej konfiguracji.  32. Urządzenie musi obsługiwać protokoły dynamicznego routingu RIP, OSPFv2 i OSPFv3.  33. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania list kontroli dostępu dla ruchu multicastowego.  34. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.  35. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości 256, 384 i 512 bitów.  36. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128,  192 i 254 bitów w trybie pracy Galois/Counter Mode(GCM) i Galois Message Authentication Code (GMAC).  37. Urządzenie musi obsługiwać protokół WCCPv2.  38. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.  39. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay) dla IPv4 i IPv6.  40. Urządzenie musi współpracować z serwerami certyfikatów (CA).  41. Urządzenie musi współpracować z zewnętrznymi serwerami uwierzytelnienia i autoryzacji z wykorzystaniem protokołów LDAP, RADIUS i TACACS+.  42. Urządzenie musi obsługiwać protokół NetFlow v9 (RFC 3954).  43. Usługa firewalla realizowane przez urządzenie musi wspierać tryb pracy w warstwie 3 (tryb routed) i tryb pracy w warstwie 2 (tryb transparentny).  44. Urządzenie musi umożliwiać grupowanie VLANów w transparentnym trybie pracy firewalla.  45. Usługa firewalla realizowana przez urządzenie musi umożliwiać filtrowanie ruchu IPv4 i IPv6 w oparciu o sekwencyjne przetwarzanie reguł dostępu (ang. Access Control Entries) zorganizowanych w listy kontroli dostępu (ang. Access Controll List) przypisane do wybranych interfejsów urządzenia.  46. Listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:  - źródłowy i docelowy adres IPv4  - źródłowy i docelowy adres IPv6  - źródłowy i docelowy numer portu UDP  - źródłowy i docelowy numer portu TCP  - nazwy domenowej hosta źródłowego lub docelowego  - nazwa użytkownika w usłudze katalogowej Microsoft Active Directory  - nazwa grupy w usłudze katalogowej Microsoft Active Directory  - czas  47. Parametry reguł wykorzystywane w listach kontroli dostępu muszą umożliwiać ich hierarchiczną organizację w grupy i wykorzystywanie ich przy budowaniu reguł dostępu.  48. Urządzenie nie może posiadać żadnych ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane.  49. Urządzenie musi realizować mechanizmy inspekcji aplikacyjnej i kontroli zgodności z formalną definicją protokołu dla następujących protokołów: DNS, ESMTP, FTP, H.323, HTTP, ICMP, MGCP, NETBIOS, PPTP, RSH, RTSP, SCCP, SIP, SNMP, SQLNET, RPC, TFTP.  50. Urządzenie musi umożliwiać inspekcję ruchu IPv4 z wykorzystaniem nagłówków: End of Options List, No Operation, Router Alarm.  51. Urządzenie musi umożliwiać inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload.  52. Jeśli pakiet IPv4/IPv6 został pofragmentowany, urządzenie musi odtworzyć oryginalny pakiet kontrolując przy tym kolejność fragmentów i ich integralność .  53. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby równocześnie odtwarzanych z fragmentów pakietów IPv4/IPv6 per każdy interfejs urządzenia realizujący usługę firewalla.  54. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby fragmentów w ramach jednego odtwarzanego pakietu.  55. Urządzenie musi umożliwiać skonfigurowanie  maksymalnego dopuszczalnego okresu czasu, w którym musi otrzymać wszystkie fragmenty niezbędne do odtworzenia pakietu.  56. Urządzenie musi umożliwiać skonfigurowanie mechanizmu randomizującego numery sekwencyjne nowych połączeń TCP.  57. Urządzenie musi umożliwiać nadpisanie wartości MSS w nagłówku TCP.  58. Urządzenie musi umożliwiać zaawansowane badanie stanu każdej sesji TCP w zakresie:  - sprawdzania opcji TCP, usuwania opcji TCP i odrzucania segmentów  z opcjami TCP  - poprawności pola TCP ACK  - poprawności sekwencjonowania segmentów TCP  (seq-past-window)  ze wsparciem mechanizmów akceleracji sieci WAN wprowadzających przesunięcie numerów sekwencyjnych TCP  - weryfikacji sumy kontrolnej segmentu TCP  - weryfikacji pola TCP SACK ALLOW  - weryfikacji wielkości okna TCP  - usuwania flagi URG  - usuwania segmentów przekraczających maksymalny rozmiar (MSS)  - usuwania segmentów z flagą SYN i z flagami SYN/ACK, jeśli zawierają one dane  59. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.  60. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych półotwartych połączeń TCP zestawionych do hosta lub do grupy hostów.  61.- Urządzenie musi umożliwiać zresetowanie otwartego połączenia TCP, jeśli przez określony okres czasu przez połączenie nie przesyłano żadnych danych.  62. Urządzenie musi umożliwiać inspekcję ruchu HTTP w zakresie:  - zgodności z formalną definicją protokołu  - ukrywania nagłówka Server w odpowiedzi HTTP  - filtrowania dopuszczalnych metod HTTP  - filtrowania dopuszczalnych typów MIME  - filtrowania dopuszczalnych adresów URL  63. Urządzenie musi umożliwiać inspekcję ruchu SMTP w zakresie:  - zgodności z formalną definicją protokołu ESMTP  - ukrywania wiadomości powitalnej serwera  - filtrowania długości wydawanych komend  - filtrowania listy odbiorców dłuższej niż określona liczba  - filtrowania długości adresu nadawcy  - filtrowania długości pola MIME  - filtrowania dopuszczalnych typów MIME  64. Urządzenie musi umożliwiać inspekcję ruchu DNS w zakresie:  - zgodności z formalną definicją protokołu DNS  - filtrowania długości wiadomości  - filtrowania po typie zapytania  - randomizowania numeru identyfikacyjnego wiadomości  - weryfikacji zgodności numeru indentyfikacyjnego zapytania i odpowiedzi  - blokowania innych odpowiedzi niż pierwsza (ochrona przed atakiem dns spoofing i dns poisoning)  65. Urządzenie musi zapewniać mechanizmy pozwalające na blokowanie aplikacji tunelowanych z użyciem portu 80 w tym blokowanie komunikatorów internetowych i aplikacji typu peer-to-peer.  66. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6.  67. Urządzenie musi wspierać mechaniz translowania adresów sieciowych NAT dla ruchu multicastowego.  68. Urządzenie musi umożliwiać więcej niż 65535 dynamicznych translacji PAT do pojedynczego zewnętrznego adresu IP.  69. Urządzenie musi umożliwiać konfigurację czasu ważności translacji PAT.  70. Urządzenie wykonując dynamiczne translacje PAT do puli zewnętrznych adresów IP, musi równomiernie korzystać ze wszystkich zdefiniowanych w puli adresów.  71. Urządzenie musi umożliwiać konfigurację następujących mechanizmów zarządzania jakością przesyłania danych (Quality of Service):  - obsługa kolejki priorytetowej o konfigurowalnej długości per każdy interfejs urządzenia  realizący usługę firewalla– pakiety umieszczone w tej kolejce zostaną obsłużone przed innymi pakietami umieszczonymi w innych kolejkach  - policing – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez odrzucanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps. Policing musi być obsługiwany dla ruchu wchodzącego i wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.  - shaping – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez buforowanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps konfigurowalną z granularnością co najmniej 8kbps. Zbuforowane pakiety są wysyłane w późniejszym okresie czasu, gdy sumaryczna przepustowość strumieni danych będzie niższa niż zadana wartość w bps. Shaping musi być obsługiwany co najmniej dla ruchu wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.  72. Wszystkie funkcje ochronne oraz zastosowane technologie włącznie z systemem operacyjnym muszą pochodzić od tego samego producenta.  73. Wraz z urządzeniem należy dostarczyć oprogramowanie klienckie służące do zestawiania połączeń IPsec i SSL VPN z komputerów stacjonarnych działających pod kontrolą systemów operacyjnych Microsoft Windows XP/Vista/7 – 32 i 64-bity, Mac OS X 10.5 i 10.6 i Linux  74. Wraz z urządzeniem należy dostarczyć oprogramowanie klienckie służące do zestawiania połączeń SSL VPN z urządzeń mobilnych działających pod kontrolą Apple IOS oraz Google Android.  75. Dokumentacja do urządzenia musi być publicznie dostępna na stronie internetowej producenta.  76. Producent musi publikować na swojej stronie internetowej informacje o wykrytych lukach bezpieczeństwa w urządzeniu.  77. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refubrished/odnowionych (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).  78. Urządzenie musi pochodzić z legalnego kanału sprzedaży producenta urządzenia. Kupujący zastrzega sobie możliwość weryfikacji numerów seryjnych dostarczonego urządzenia u producenta w celu sprawdzenia czy urządzenie pochodzi z legalnego kanału sprzedaży.  79**. Urządzenie musi być objęte co najmniej 1 rocznym serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.** | | |
| Dane teleadresowe punktu serwisowego (adres, nr telefonu, faksu, email) |  | |

UWAGA dotycząca przedmiotu zamówienia:

1.W przypadku, gdy przedmiot zamówienia zostaje opisany poprzez wskazanie znaków towarowych lub pochodzenia, Zamawiający informuje, iż zapis ten jest jedynie przykładowym i stanowi wskazanie dla Wykonawcy jakie cechy powinien posiadać towar będący przedmiotem niniejszej części zamówienia. Zamawiający dopuszcza realizację zamówienia poprzez zastosowanie produktów równoważnych. Zamawiający przez podanie nazw własnych produktów, określa minimalne parametry techniczne, funkcjonalne, cechy użytkowe oraz jakościowe (m.in.: przeznaczenie, możliwości, posiadane narzędzia, interfejs itp.), jakim powinny odpowiadać produkty równoważne, aby spełniały stawiane wymagania.

2.Ilekroć w opisie przedmiotu zamówienia zawartym w SIWZ wskazane zostały normy, znaki towarowe, patenty lub pochodzenie, Zamawiający dopuszcza rozwiązania równoważne.

3.Za ofertę równoważną Zamawiający uzna tę, która spełnia wszystkie wymagania Zamawiającego oraz w której zaoferowane parametry techniczne i funkcjonalne są identyczne lub nie gorsze niż wskazane w SIWZ.

4.Ewentualne wskazanie przez Zamawiającego nazwy producenta ma na celu określenie klasy, funkcjonalności, przeznaczenia oprogramowania będącego przedmiotem zamówienia i służy ustaleniu standardu, nie wskazuje natomiast na konkretny wyrób lub konkretnego producenta.

Zaproponowany sprzęt ma zapewniać ciągłość pracy infrastruktury sieciowej Zamawiającego. Wszelkie nazwy własne użyte w opisie przedmiotu zamówienia bez określenia równoważności wskazują na dotychczasowe wyposażenie pracowni komputerowych, w których będzie instalowane oprogramowanie. Kompatybilność

wyposażenia z zakupionym oprogramowaniem pozwoli na osiągnięcie zaplanowanych celów dydaktycznych

**UWAGA:**

**NIEWYPEŁNIENIE WIERSZY: „NAZWA OFEROWANEGO URZĄDZENIA”, „PRODUCENT”, „TYP/MODEL/KOD PRODUCENTA”, KTÓRE TO JEDNOZNACZNIE IDENTYFIKUJĄ OFEROWANE URZĄDZENIE ZOSTANIE POTRAKTOWANY, JAKO NIESPEŁNIENIE MINIMALNYCH WYMAGAN ZAMAWIAJĄCEGO, CO BĘDZIE SKUTKOWAŁO ODRZUCENIEM OFERTY.**

.................................... dnia ......................... 2014r.

......................................................................

Podpis i pieczęć osoby/osób

upoważnionej/ych do reprezentowania Wykonawcy