IV. SZCZEGÓŁOWE WYMAGANIA DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA

I. Specyfikacja urządzenia Next Generation Firewall (NGFW)

1. Urządzenie NGFW musi być wyposażone w:
    a. Interfejsy sieciowe:
        - co najmniej 2 światłowodowe interfejsy sieciowe o przepustowości 100 Gbps,
        - co najmniej 10 światłowodowych interfejsów sieciowych o przepustowości 10 Gbps,
        - co najmniej po 2 porty światłowodowe osobne dla Data Plane (transmisja i odbiór danych) i Control Plane (zarządzanie stanem klastra i synchronizacja) koniecznych do połączenia urządzeń w klaster z najwyższą możliwą przepustowością dla tych interfejsów również na dystansie 10 km;
    b. redundantne zasilacze typu AC z możliwością wymiany hot-swap oraz muszą przewidywać redundancję zasilania z zachowaniem następujących cech:
        - awaria połowy zasilaczy zainstalowanych w urządzeniu nie może wpływać na działanie urządzenia;
        - odłączenie połowy przyłączy elektrycznych nie może zakłócać działania urządzenia,
        - wymiana zasilacza oraz kabli musi być możliwa bez wyłączania urządzenia,
    c. Efektywnie dostępna dla użytkownika przestrzeń dyskowa o pojemności nie mniejszej niż 480GB działająca w co najmniej RAID-1, przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi),
2. Dla urządzenia muszą zostać dostarczone:
    a. wkładki światłowodowe jednomodowe w ilości co najmniej 2, to znaczy, że zamawiający wymaga, aby wszystkie porty dostarczonego urządzenia z interfejsami sieciowymi 100 Gbps były wypełnione wkładkami 100 Gbps, o zasięgu transmisji nie mniejszym niż 10 km;
    b. wkładki światłowodowe jednomodowe w ilości co najmniej 10, to znaczy, że zamawiający wymaga, aby wszystkie porty dostarczonego urządzenia z światłowodowymi interfejsami sieciowymi 10 Gbps były wypełnione wkładkami 10 Gbps o zasięgu transmisji nie mniejszym niż 10 km;
    c. niezbędna liczba wkładek światłowodowych, jednomodowych do interfejsów umożliwiających połączenie urządzenia w klaster (z maksymalną liczbą nadmiarowych połączeń HA – np. rozwiązanie typu „dual fabric link” i „dual control link”) z najwyższą możliwą przepustowością dla tych interfejsów również na dystansie 10km;
3. Urządzenie NGFW musi spełniać co najmniej następujące parametry wydajnościowe:

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

a. przepustowość firewalla (ang. throughput): co najmniej 50 Gbps dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (Firewall, IPS, antywirus, anty-spyware, kontrola aplikacji, włączone logowanie),
b. minimalna liczba nowych sesji na sekundę: 600 000,
c. obsługa co najmniej 20 milionów jednoczesnych sesji,
d. Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na urządzeniu NGFW zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako Enterprise Mix/Enterprise Testing Conditions/appmix lub dla równoważnego modelu ruch. Przy czym przez równoważny model ruchu rozumie się taki ruch:
   - dla którego wymagane parametry wydajnościowe są osiągane w ruchu całościowym (up/down) i jednocześnie
   - w którym rozkład procentowy ruchu wybranych protokołów wykorzystujących pakiety różnej wielkości, przy pomocy których realizowane są różne aplikacje (np. youtube, facebook, google, gmail, ssh, smtp z załącznikami) jest przedstawiony w tabeli poniżej:

Protokół	**Udział w %**
HTTP	15%
HTTPS	60%
SMTP, IMAP, POP3, FTP, SMB i inne	22%
DNS	3%

Zamawiający dopuszcza odchylenie od przedstawionych wielkości udziałów dla poszczególnych protokołów o 10 punktów procentowych w górę albo w dół.

4. Urządzenie NGFW musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site, bazując na ustawieniach routingu (tzw. routing-based VPN) i spełniać co najmniej następujące parametry wydajnościowe:
   a. minimum 15 Gbps dla IPSEC VPN
   b. minimum 1 000 tuneli IPSEC VPN (site-to-site).

   Jeżeli wykorzystanie funkcji VPN IPSec wymaga zakupu dodatkowych licencji, to należy je przewidzieć w ofercie dla maksymalnej wydajności tej funkcji, w ramach wynagrodzenia wykonawcy. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.
5. Urządzenie NGFW musi dawać możliwość pracy w trybie wysokiej dostępności umożliwiając synchronizację stanu sesji i reguł polityki bezpieczeństwa między urządzeniami, aby zapewnić ciągłość działania w przypadku awarii jednego z urządzeń, pod warunkiem zakupu drugiego urządzenia przez Zamawiającego. Zamawiający rozumie przez to, że urządzenie NGFW może być w pełni sprawny opierając się na wyłącznie pojedynczym urządzeniu NGFW.

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

6. Urządzenie NGFW musi pozwalać na dynamiczne skalowanie systemu zgodnie z rosnącymi wymaganiami sieciowymi i biznesowymi Zamawiającego, dlatego urządzenie NGFW musi zapewniać możliwość rozbudowy (modyfikacji).
   Zamawiający wymaga co najmniej jednej z metod rozbudowy urządzenia NGFW będącego przedmiotem dostawy:
   a. Rozbudowa fizyczna/modułowa - urządzenie NGFW umożliwia dodawanie dodatkowych fizycznych kart, modułów lub innych rozwiązań sprzętowych w celu zwiększenia wydajności systemu,
   b. Zwiększenie wydajności przez licencje - urządzenie NGFW umożliwia skalowanie wydajności poprzez zakup dodatkowych licencji, które odblokują wyższe limity przepustowości bez potrzeby fizycznej rozbudowy urządzenia.
   c. Skalowanie przez klastrowanie - urządzenie NGFW powinno wspierać klastrowanie urządzeń NGFW, co pozwala na dodawanie nowych urządzeń w ramach jednej platformy. Dzięki temu można uzyskać zwiększenie wydajności poprzez dodanie nowych jednostek NGFW, które będą działały jako jeden skonsolidowany system ochrony sieciowej. W przypadku wyboru przez Wykonawcę tej metody, Zamawiający wymaga dostarczenia wszystkich niezbędnych komponentów klastra, którym umożliwi zwiększenie wydajności poprzez dodanie nowych jednostek NGFW, które będą działały jako jeden skonsolidowany system ochrony sieciowej, Zamawiający w przypadku tego skalowania rozumie jako urządzenie NGFW cały skonsolidowany system ochrony sieciowej. Zamawiający w przypadku tego skalowania rozumie jako urządzenie NGFW cały skonsolidowany system ochrony sieciowej. W takim wypadku Wykonawca musi zapewnić wszystkie niezbędne licencje i komponenty umożliwiające skalowanie, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.

   W wyniku rozbudowy urządzenia będącego przedmiotem dostawy, Zamawiający wymaga, aby urządzenie NGFW posiadało następujące właściwości (łącznie):

   a. przepustowości dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (Firewall, IPS, antywirus, anty-spyware, kontrola aplikacji, włączone logowanie): co najmniej 170 Gbps
   b. minimalna liczba nowych sesji na sekundę: 3 miliony,
   c. obsługa co najmniej 80 milionów jednoczesnych sesji,
   d. urządzenie NGFW musi mieć możliwość wyposażenia łącznie w:
      - co najmniej 4 światłowodowe interfejsy sieciowe 100G,
      - co najmniej 12 światłowodowych interfejsów sieciowych 10G.
7. Urządzenie NGFW musi umożliwiać działanie w co najmniej dwóch trybach pracy:
   a. routera (warstwa 3 modelu OSI),
   b. przełącznika (warstwa 2 modelu OSI).

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

8. Urządzenie NGFW musi obsługiwać protokół Ethernet z pełną obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych ze standardem 802.1q oraz umożliwiać tworzenie subinterfejsów na interfejsach pracujących w trybach L2 i L3.
9. Urządzenie NGFW musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach, w szczególności musi mieć zdefiniowane w systemie co najmniej dwa konta typu:
    a. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu,
    b. Operator, który ma możliwość tylko odczytu konfiguracji.
10. Urządzenie NGFW musi wspierać translację adresów IP (NAT), zarówno statyczną, jak i dynamiczną. Reguły NAT muszą być odrębne od reguł polityk bezpieczeństwa, aby nie tworzyły zależności od konfiguracji tych polityk.
11. Urządzenie NGFW musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej:
    a. oznaczania pakietów znacznikami DiffServ,
    b. priorytetyzację aplikacji, ustawienie pasma maksymalnego i gwarantowanego,
    c. tworzenia co najmniej 8 klas ruchu sieciowego,
12. Urządzenie NGFW musi oferować ochronę przed atakami typu DoS, umożliwiając limitowanie liczby jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
13. Urządzenie NGFW musi obsługiwać protokoły routingu co najmniej OSPF (wersja 2 i 3), BGP, oraz BFD. Centralny komponent musi obsługiwać nie mniej niż 20 wirtualnych routerów z odrębnymi tabelami routingu.
14. Urządzenie NGFW musi obsługiwać nie mniej niż 10 wirtualnych firewalli i posiadać możliwość rozbudowy do co najmniej 20 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:
    a. tablic routingu
    b. polityk bezpieczeństwa obejmujących:
        - system IPS,
        - system ochrony antymalware/antyspyware,
        - system ochrony antywirus,
        - koncentratory VPN dla zdalnego dostępu.
15. Zamawiający wymaga dostarczenia licencji na nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów w chwili dostarczenia urządzenia NGFW. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.
16. Urządzenie NGFW musi wspierać mechanizm PBR (Policy-Based Routing), umożliwiający przekierowanie ruchu z pominięciem tablicy routingu.
17. Polityka bezpieczeństwa urządzenia NGFW musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS.
18. Urządzenie NGFW musi umożliwiać zdefiniowanie nie mniej niż 5 000 reguł polityki bezpieczeństwa oraz obsługę minimum 200 stref bezpieczeństwa.

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

19. Urządzenie NGFW musi umożliwiać rozpoznawanie aplikacji niezależnie od numeru portu, na którym działa aplikacja. Rozpoznawanie musi odbywać się co najmniej na podstawie sygnatur aplikacji. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzeniu NGFW numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą działać na wszystkich dostępnych 65 535 portach. Urządzenie musi automatycznie rozpoznawać predefiniowane aplikacje wspierane przez producenta (np. Skype, Tor, BitTorrent, eMule, UltraSurf) oraz aplikacje tunelujące się przez protokoły HTTP lub HTTPS. Ponadto, urządzenie musi pozwalać na ręczne tworzenie sygnatur nowych aplikacji bezpośrednio na firewallu. W przypadku gdy producent nie dostarcza takiej funkcjonalności, Zamawiający dopuszcza dostarczenie zewnętrznego narzędzia w formie oprogramowania, dostarczonego na koszt Wykonawcy oraz bez ponoszenia przez Zamawiającego jakichkolwiek dodatkowych kosztów w terminie późniejszym, z licencją zapewniającą możliwość użytkowania i aktualizacji przez czas nieograniczony i bez możliwości jej wypowiedzenia, realizującego funkcjonalność tworzenia nowych definicji aplikacji, importowanych następnie przez komponent zarządzający lub centralny.
20. Urządzenie NGFW musi umożliwiać włączenie systemu wykrywania i zapobiegania włamaniom (IPS - Intrusion Prevention System), z możliwością automatycznej aktualizacji sygnatur w okresie gwarancji, pod warunkiem zakupu odpowiedniej licencji przez Zamawiającego. System IPS musi mieć możliwość działania w warstwie 7 modelu OSI. Baza sygnatur IPS musi być przechowywana bezpośrednio na urządzeniu, regularnie i automatycznie aktualizowana, a jej sygnatury muszą pochodzić od tego samego producenta, co urządzenie NGFW. Moduł IPS musi oferować możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie adresu IP (zarówno źródłowego, jak i docelowego) oraz rozpoznania aplikacji bez względu na numery portów, na których działa.
21. Urządzenie NGFW musi umożliwiać włączenie funkcjonalności Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji, jeżeli Zamawiający zakupi odnośną licencję. Moduł AV musi umożliwiać uruchamianie per aplikacja (ang. application/services) oraz wybrany dekoder taki jak np. http, smtp, imap, pop3, ftp, smb itp. Baza sygnatur AV musi mieć możliwość przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent urządzenia, na którym realizowana jest ta funkcja. Moduł AV musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji bez względu na numery portów, na których działa.
22. Urządzenie NGFW musi umożliwiać włączenie ochrony przed atakami typu Spyware w okresie gwarancji, jeżeli Zamawiający zakupi odnośną licencję. Baza sygnatur anty-spyware musi mieć możliwość przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji bez względu na numery portów, na których działa.

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl, www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

23. Zarządzanie urządzeniem NGFW (w tym zarządzanie regułami/politykami bezpieczeństwa) musi odbywać się za pomocą linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę internetową. Dostęp do urządzenia oraz zarządzanie z sieci muszą być chronione za pomocą szyfrowania komunikacji.
24. **[Dodatkowo punktowane] Integracja z oprogramowaniem Panorama (Palo Alto Networks).** Dodatkowe punkty będą przyznane, jeżeli urządzenie NGFW integruje się z posiadanym przez Zamawiającego systemem zarządzania Panorama (Palo Alto Networks), który jest centralnym narzędziem do zarządzania rozległym systemem NGFW Zamawiającego, składającym się z 4 urządzeń Palo Alto Networks PA-5410. Przy czym urządzenie NGFW musi umożliwiać integrację z Panorama co najmniej w taki sposób, aby umożliwić centralne zarządzanie politykami bezpieczeństwa oraz monitorowanie logów w jednym miejscu.
25. **[Dodatkowo punktowane] Dekrypcja TLS 1.3**. Dodatkowe punkty będą przyznane za rozwiązanie, w którym urządzenie NGFW będzie umożliwiać dekrypcję ruchu zaszyfrowanego z wykorzystaniem TLS w wersji 1.3, w celu sprawdzenia przez silniki IPS/AV/Spyware.
26. **[Dodatkowo punktowane] Rozszerzona ilość interfejsów 10 Gbps**. Dodatkowe punkty będą przyznane, jeżeli urządzenie NGFW jest wyposażone łącznie w co najmniej 16 światłowodowych interfejsów sieciowych o przepustowości 10 Gbps.
27. **[Dodatkowo punktowane] Funkcjonalności ML/AI**. Dodatkowe punkty będą przyznane za rozwiązanie, w którym urządzenie NGFW będzie wykorzystywać w ramach modułów IPS/AV/Spyware technologię Uczenia Maszynowego lub „Sztucznej Inteligencji”.
28. Urządzenie NGFW musi być dostarczone z najnowszą (na dzień złożenia oferty) wersją oprogramowania systemowego (firmware) lub z wersją oprogramowania rekomendowaną przez producenta oferowanego rozwiązania. Jeżeli urządzenia są fabrycznie wysyłane z inną wersją oprogramowania to wykonawca zobowiązany jest do dostarczenia wersji najnowszej lub wersji rekomendowanej przez producenta (na nośniku, poprzez wskazanie jej lokalizacji w portalu producenta z możliwością jej pobrania, lub też poprzez pobranie jej bezpośrednio na urządzenie itp.)
29. W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki muszą pozostać w całości u zamawiającego. Nie przewiduje się opcji demontażu nośników danych i pozostawienia u zamawiającego fragmentów nośników z danymi, np. talerzy dysków.
30. Urządzenie NGFW musi działać przy zasilaniu z jednej fazy 230V/50Hz z sieci elektrycznej. Dostarczone kable zasilające muszą być zakończone wtyczką pasującą do gniazd C14 bez wykorzystania adapterów.
31. Urządzenie NGFW musi być przystosowane do montażu w szafie Rack 19”.

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

II. Wymagania dotyczące współpracy już posiadanego przez Zamawiającego rozległego systemu NGFW z elementami dostarczonymi w ramach niniejszego postępowania przetargowego, jeżeli Zamawiający nie skorzysta z prawa opcji.

1. Jeśli urządzenie NGFW nie obsługuje natywnej integracji z centralnym systemem zarządzania Panorama (Palo Alto Networks), Wykonawca musi na własny koszt:
    a. przenieść wskazane przez Zamawiającego polityki bezpieczeństwa i konfiguracji między posiadanymi przez Zamawiającego urządzeniami NGFW (Palo Alto Networks, model PA-5410) a dostarczonym urządzeniem NGFW;
    b. dostarczyć komponent zarządczy pracujący w trybie wysokiej dostępności, pozwalający na centralne zarządzanie politykami bezpieczeństwa, protokołami routingu, umożliwiający zarządzanie łącznie co najmniej 10 dowolnymi urządzeniami NGFW. Komponent zarządczy może być dostarczony w postaci dedykowanego urządzenia z oprogramowaniem lub w postaci maszyny wirtualnej (virtual appliance) działającej pod kontrolą hipernadzorcy KVM (Zamawiający jest w posiadaniu infrastruktury bazującej na hipernadzorcy KVM). Wykonawca zapewni wszystkie niezbędne licencje i komponenty, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.
    W przypadku konieczności łączenia się do komponentu zarządczego za pośrednictwem oprogramowania nie działającego na systemach operacyjnych z rodziny GNU/LINUX wykonawca musi dostarczyć licencję na system obsługujący to oprogramowanie wraz z licencją i oprogramowaniem umożliwiającym pracę zdalną na tym systemie co najmniej 10 administratorom, umożliwiając im równoległe zarządzanie komponentem centralnym), z możliwością niezależnej pracy. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc.
2. Musi być możliwy import reguł zgodnych z rozwiązaniami SNORT lub Suricata do modułów systemu wykrywania i zapobiegania włamaniom IPS.
3. Wykonawca musi wyposażyć urządzenie NGFW będący przedmiotem dostawy w:
    a. wkładki światłowodowe jednomodowe - Zamawiający wymaga, aby wszystkie porty dostarczonego urządzenia z interfejsami sieciowymi o przepustowości 100 Gbps były wypełnione wkładkami o przepustowości 100 Gbps, o zasięgu transmisji nie mniejszym niż 10 km;
    b. wkładki światłowodowe jednomodowe - Zamawiający wymaga, aby wszystkie porty dostarczonego urządzenia z interfejsami sieciowymi o przepustowości

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

10 Gbps były wypełnione wkładkami 10 Gbps o zasięgu transmisji nie mniejszym niż 10 km;

c. wkładki światłowodowe, jednomodowe do interfejsów koniecznych do połączenia urządzenia w klaster (z maksymalną liczbą nadmiarowych połączeń HA – np. rozwiązanie typu „dual fabric link" i „dual control link") z najwyższą możliwą przepustowością dla tych interfejsów również na dystansie 10 km;

III. Wymagania dotyczące współpracy już posiadanego przez Zamawiającego rozległego systemu NGFW z elementami dostarczonymi w ramach niniejszego postępowania przetargowego, jeżeli Zamawiający skorzysta z prawa opcji.

1. Wykonawca dostarczy drugie urządzenie NGFW opisane w części IV Specyfikacja urządzenia Next Generation Firewall (NGFW).
2. Jeśli urządzenia NGFW nie obsługują natywnej integracji z centralnym systemem zarządzania Panorama (Palo Alto Networks), Wykonawca musi na własny koszt:
   a. przenieść wskazane przez Zamawiającego polityki bezpieczeństwa i konfiguracji między posiadanymi przez Zamawiającego urządzeniami NGFW (Palo Alto Networks, model PA-5410) a dostarczonymi urządzeniami NGFW.
   b. dostarczyć komponent zarządczy pracujący w trybie wysokiej dostępności, pozwalający na centralne zarządzanie politykami bezpieczeństwa, protokołami routingu, umożliwiający zarządzanie łącznie co najmniej 10 urządzeniami NGFW. Komponent zarządczy może być dostarczony w postaci dedykowanego urządzenia z oprogramowaniem lub w postaci maszyny wirtualnej (virtual appliance) działającej pod kontrolą hipernadzorcy KVM (Zamawiający jest w posiadaniu infrastruktury bazującej na hipernadzorcy KVM). Wykonawca zapewni wszystkie niezbędne licencje i komponenty, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.

      W przypadku konieczności łączenia się do komponentu zarządczego za pośrednictwem oprogramowania nie działającego na systemach operacyjnych z rodziny GNU/LINUX wykonawca musi dostarczyć licencję na system obsługujący to oprogramowanie wraz z licencją i oprogramowaniem umożliwiającym pracę zdalną na tym systemie co najmniej 10 administratorom, umożliwiając im równoległe zarządzanie komponentem centralnym), z możliwością niezależnej pracy. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc.
3. Wykonawca dostarczy licencje potrzebne do uruchomienia funkcjonalności wykrywania i zapobiegania włamaniom IPS (ang. Intrusion Prevention System),

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

antywirus, anty-spyware, o którym mowa w punktach 20, 21, 22 części IV Specyfikacja urządzenia Next Generation Firewall (NGFW) na takich samych warunkach, jak w przypadku zamówienia podstawowego i za cenę wskazaną w ofercie wykonawcy złożonej w niniejszym postępowaniu o udzielenie zamówienia publicznego.

4. Musi być możliwy import reguł zgodnych z rozwiązaniami SNORT lub Suricata do modułów systemu wykrywania i zapobiegania włamaniom IPS.
5. System nowych urządzeń NGFW musi działać w trybie wysokiej dostępności **HA** (High Availability), zapewniając pełną redundancję i synchronizację stanu sesji, reguł polityki, oraz stanu urządzeń. W przypadku awarii jednego z urządzeń, system musi automatycznie przełączać ruch na drugie urządzenie NGFW bez zakłóceń.
6. System nowych urządzeń NGFW działający w trybie wysokiej dostępności **HA** (High Availability), pozwala na dynamiczne skalowanie systemu zgodnie z rosnącymi wymaganiami sieciowymi i biznesowymi Zamawiającego, poprzez zastosowanie jednej z poniższych metod rozbudowy.

   Zamawiający wymaga, aby system nowych urządzeń NGFW mógł być dynamicznie skalowaniu za pomocą co najmniej jednej z niżej wymienionych metod:

   a. Rozbudowa fizyczna/modułowa - urządzenia NGFW umożliwiają dodawanie dodatkowych fizycznych kart, modułów lub innych rozwiązań sprzętowych w celu zwiększenia wydajności systemu,
   b. Zwiększenie wydajności przez licencje - urządzenia NGFW umożliwiają skalowanie wydajności poprzez zakup dodatkowych licencji, które odblokują wyższe limity przepustowości bez potrzeby fizycznej rozbudowy urządzeń.
   c. Skalowanie przez klastrowanie - urządzenie NGFW powinno wspierać klastrowanie urządzeń NGFW, co pozwala na dodawanie nowych urządzeń w ramach jednej platformy. Dzięki temu można uzyskać zwiększenie wydajności poprzez dodanie nowych jednostek NGFW, które będą działały jako jeden skonsolidowany system ochrony sieciowej. W przypadku wyboru przez Wykonawcę tej metody, Zamawiający wymaga dostarczenia wszystkich niezbędnych komponentów klastra, którym umożliwi zwiększenie wydajności poprzez dodanie nowych jednostek NGFW, które będą działały jako jeden skonsolidowany system ochrony sieciowej, Zamawiający w przypadku tego skalowania rozumie jako urządzenie NGFW cały skonsolidowany system ochrony sieciowej. W takim wypadku Wykonawca musi zapewnić wszystkie niezbędne licencje i komponenty umożliwiające skalowanie, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę.

   W wyniku rozbudowy, o której mowa w punkcie 6. Zamawiający wymaga, aby Wykonawca dostarczył komponenty niezbędne do rozbudowy systemu (zwane dalej komponentami rozbudowy) tak, aby system urządzeń NGFW działał w trybie wysokiej

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

dostępności **HA Active/Pasive** (ang. High Availability) i posiadał następujące właściwości:

a. przepustowości dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (Firewall, IPS, antywirus, anty-spyware, kontrola aplikacji, włączone logowanie): co najmniej 170 Gbps
b. minimalna liczba nowych sesji na sekundę: 3 miliony,
c. obsługa co najmniej 80 milionów jednoczesnych sesji,
d. system musi być wyposażony łącznie w:
e. co najmniej 4 światłowodowe interfejsy sieciowe 100 Gbps
f. co najmniej 12 światłowodowych interfejsów sieciowych 10 Gbps

7. W wyniku rozbudowy, o której mowa w punkcie 6. Zamawiający wymaga, aby Wykonawca dostarczył komponenty niezbędne do rozbudowy systemu (zwane dalej komponentami rozbudowy) tak, aby urządzenia NGFW działały w trybie wysokiej dostępności **HA** (ang. High Availability) i posiadał następujące właściwości:
   a. przepustowości dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (Firewall, IPS, antywirus, anty-spyware, kontrola aplikacji, włączone logowanie): co najmniej 170 Gbps
   b. minimalna liczba nowych sesji na sekundę: 3 miliony,
   c. obsługa co najmniej 80 milionów jednoczesnych sesji,
   d. system musi być wyposażony łącznie w:
   e. co najmniej 4 światłowodowe interfejsy sieciowe 100 Gbps
   f. co najmniej 12 światłowodowych interfejsów sieciowych 10 Gbps

8. Wykonawca musi wyposażyć urządzenia NGFW w:
   a. wkładki światłowodowe jednomodowe - Zamawiający wymaga, aby wszystkie porty dostarczonego urządzenia z interfejsami sieciowymi o przepustowości 100 Gbps były wypełnione wkładkami o przepustowości 100 Gbps, o zasięgu transmisji nie mniejszym niż 10 km;
   b. wkładki światłowodowe jednomodowe - Zamawiający wymaga, aby wszystkie porty dostarczonego urządzenia z interfejsami sieciowymi o przepustowości 10 Gbps były wypełnione wkładkami 10 Gbps o zasięgu transmisji nie mniejszym niż 10 km;
   c. wkładki światłowodowe, jednomodowe do interfejsów koniecznych do połączenia urządzenia w klaster (z maksymalną liczbą nadmiarowych połączeń HA – np. rozwiązanie typu „dual fabric link" i „dual control link") z najwyższą możliwą przepustowością dla tych interfejsów również na dystansie 10 km.

IV. Wymogi dotyczące instruktażu

1. Przeprowadzenie przez wykonawcę albo wskazane przez niego podmioty trzecie (ale zawsze na koszt i ryzyko wykonawcy) instruktaży w zakresie instalacji, konfiguracji i administracji

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl, www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

urządzeniem lub urządzeniami NGFW. Dopuszcza się przeprowadzenie instruktaży na urządzeniach wirtualnych posiadających konfigurację zgodną z dostarczanym Systemem.

2. W ramach dostarczonego przedmiotu zamówienia wykonawca musi zapewnić instruktaż dla maksymalnie 10 osób, przy czym instruktaż musi spełniać następujące warunki:

    a. konkretne terminy przeprowadzenia instruktażu wykonawca musi uzgodnić z zamawiającym, przy czym instruktaż musi być przeprowadzony przed podpisaniem protokołu zdawczo-odbiorczego,

    b. czas trwania instruktażu musi być wystarczający do zapoznania uczestników instruktażu z administracją urządzeniami, przy czym nie może być krótszy niż 5 dni robocze (5x8 godzin),

    c. instruktaż musi być połączony z praktyczną obsługą Systemu. Środowisko musi przygotować wykonawca (ćwiczenia praktycznie minimum 50% czasu trwania szkolenia),

    d. instruktaż musi się odbyć w języku polskim,

    e. każdy uczestnik instruktażu musi pracować przy osobnym stanowisku pracy,

    f. w ramach instruktażu konieczne jest dostarczenie dokumentacji obejmującej pełen zakres instruktażu w języku polskim lub angielskim,

    g. instruktaże muszą się odbyć w mieście będącym siedzibą zamawiającego lub za zgodą zamawiającego instruktaże mogą odbyć się w formie zdalnej (wideokonferencja),

    h. w ramach instruktaży należy przekazać kompletną wiedzę na temat konfiguracji i zarządzania dostarczanymi systemami, a w szczególności na temat (tematy powinny być omówione w czasie trwania obu szkoleń):

        - uruchomienia urządzenia NGFW,
        - zarządzanie licencjami w urządzeniu,
        - konfiguracji urządzenia NGFW do pracy w trybie wysokiej dostępności (HA),
        - reakcją na False-Positive zgłaszane przez silniki bezpieczeństwa,
        - konfiguracji nadmiarowej bramy domyślnej,
        - konfiguracji routingu w tym: definiowania dynamicznego routingu BGP praz OSPF wieloobszarowy, konfigurowania routingu statycznego, konfigurowania BFD dla wyżej wymienionych metod routingu, Policy based routingu,
        - uruchamiania i zarządzania wieloma systemami wirtualnymi w ramach pojedynczego systemu fizycznego oraz zarządzania nimi,
        - konfiguracja routingu i połączeń pomiędzy systemami wirtualnymi,

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10

- definicji polityk bezpieczeństwa,
- pełnego wykorzystywania funkcjonalności IPS,
- importu reguł IDP innych producentów,
- wykorzystania funkcjonalności kontroli aplikacji,
- wykorzystania funkcjonalności filtracji stron www,
- konfigurowania połączeń VPN site-to-site pomiędzy poszczególnymi urządzeniami,
- zarządzania użytkownikami: definiowanymi na systemie, definiowanymi w zewnętrznej bazie LDAP, z zewnętrznego systemu autoryzacji RADIUS,
- konfigurowania połączeń VPN client-to-site z wykorzystaniem różnych metod uwierzytelniania użytkowników,
- konfigurację logowania połączeń do zewnętrznych serwerów (najlepiej Elasticsearch i NetFlow),
- inspekcji SSL/TLS,
- mirroring rozszyfrowanego ruchu TLS/SSL,
- konfiguracji serwera DHCP,
- konfiguracji różnych wariantów NAT,
- konfiguracji i wykorzystania wszystkich dodatkowych funkcji urządzenia wskazanych przez zamawiającego,

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk - **Poznańskie Centrum Superkomputerowo-Sieciowe**
61-704 Poznań, ul. Z. Noskowskiego 12/14, tel. (+48) 61 858 20 01, fax: (+48) 61 852 59 54, e-mail: office@man.poznan.pl,
www.pcss.pl, Numer konta: Bank Gospodarstwa Krajowego, Oddział w Poznaniu,
58 1130 1088 0001 3144 8520 0069 (dla waluty PLN), 54 1130 1088 0001 3144 8520 0044 (dla waluty EUR), NIP: 777-00-02-062
Adres korespondencyjny: Poznańskie Centrum Superkomputerowo-Sieciowe, 61-139 Poznań, ul. Jana Pawła II 10