

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Informacje ogólne

1. W chwili obecnej Zamawiający posiada urządzenia NGFW (Next Generation Firewall) Palo Alto Networks PA-5020 skonfigurowane w klaster active-passive. Powyższy klaster z uwagi na potrzebę zcentralizowanego zarządzania, zbierania logów i generowanie raportów jest podłączony do oprogramowania Palo Alto Networks Panorama.
2. Przedmiotem zamówienia jest dostawa systemu bezpieczeństwa sieci w postaci urządzeń typu NGFW wraz z usługą wdrożenia oraz wsparcie technicznym w tym zapewnieniem licencji i lub subskrypcji niezbędnych do poprawnego działania.
3. Celem wdrożenia jest migracja wszystkich funkcjonalności z posiadanego rozwiązania na urządzenia będące przedmiotem tego postępowania. W chwili obecnej klaster realizuje poniższe:
 - brama vpn dla zdalnego dostępu z weryfikacją stanu/kondycji hostów klienckich
 - brama vpn dla rozwiązań clientless application ssl vpn
 - brama vpn dla tuneli site-to-site
 - kontrola ruchu sieciowego bazująca na aplikacjach wraz z inspekcjami bezpieczeństwa, analizą ruchu i zagrożeń, filtracją ruchu URL, deszyfracją ruchu, ochroną przed atakami DoS
 - kontrola korzystania z zasobów sieci Internet przez użytkowników
 - ochrona serwerów przez atakami zagrożeniami zarówno z Internetu jak i z wnętrza organizacji
 - ochrona IPS, AV, antyspyware oraz możliwością wysyłania plików wykonywalnych do środowiska typu sandbox
 - obsługa środowiska terminalowego MS w kontekście ruchu generowanego per konkretny użytkownik.
 - integracja z AD i mapowanie użytkowników w celu tworzenia polityk i logowania zdarzeń
 - definiowanie stref DMZ
 - NAT, DHCP
 - statystyka i monitorowanie aktywności w kontekście ruchu i zagrożeń
4. Zamawiający dopuszcza system bezpieczeństwa w postaci dwóch fizycznych urządzeń połączonych w klaster niezawodnościowy.
5. System musi zapewnić ochronę dla co najmniej 7000 osób (w tym pracowników UMK jak i pracowników podmiotów zewnętrznych bez względu na tryb pracy zdalny/lokalny).

Wymagania ogólne

1. Urządzenia będące przedmiotem zamówienia muszą być fabrycznie nowe, wcześniej nie używane w innych projektach oraz pochodzące z legalnego kanału dystrybucyjnego, dopuszczony do obrotu na terenie Polski.
2. Zamawiający wymaga, aby wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Urządzenie oraz jego oprogramowanie systemowe (firmware) musi być dostępne co najmniej 6 miesięcy przed terminem składania ofert. Musi być objęte pełnym wsparciem/serwisem producenta (niedopuszczalne jest oferowanie rozwiązań np. testowych czy oprogramowania w wersji Beta) co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania

3. Zaoferowane urządzenia muszą być dostępne i objęte serwisem Producenta. Zamawiający nie dopuszcza także by przedmiot oferty był przewidziany do wycofania ze sprzedaży i wsparcia (tzn. nie mogą być wpisane na listy End-of-Sale, End-of-Life danego Producenta lub równoważne).

6. Wykonawca może zrealizować przedmiot umowy wykorzystując dodatkowe systemy/urządzenia czy komponenty w celu realizacji wymaganych funkcjonalności i przedmiotu umowy jeśli będzie to zgodne ze szczegółowym opisem technicznym oraz poniższymi warunkami:

a) Stosowanie dodatkowych systemów/urządzeń nie może dotyczyć funkcji ochronnych NGFW (np. wykrywania aplikacji, obsługi IPS, AV, NAT, deszyfracja SSL/TLS).

b) Stosowanie dodatkowych systemów/urządzeń nie może powodować omińnięcia reguł bezpieczeństwa (np. weryfikacja stanu/kondycji czy bezpieczeństwa stacji roboczej nie może odbywać się w oparciu o integrację z systemem logowania i raportowania, bez wykorzystania reguł bezpieczeństwa)

c) Stosowanie dodatkowych systemów/urządzeń jest dopuszczalne, tylko jeśli są one konieczne dla:

- weryfikacji tożsamości użytkowników – system uwierzytelniania
- uzyskania informacji o kondycji bezpieczeństwa hostów (w kontekście oprogramowanie agenta na stacjach roboczych)
- realizacji funkcji zarządzania firewallem i uprawnieniami administratorów
- zatwierdzanie i praca na konfiguracji kandydackiej
- realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania

d) Stosowanie dodatkowych systemów/urządzeń jest dopuszczone tylko przy założeniu zapewnienia ich wysokiej dostępności. Oznacza to, że należy dostarczyć każdy taki system:

- jako dedykowane rozwiązanie (urządzenie z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta) a system/urządzenie musi być dostarczony jako klastery niezawodnościowy – tzn. identyczne urządzenia pracujące równolegle w modelu 1+1 lub N+1, wyposażone w redundantne zasilacze z możliwością ich wymiany „na gorąco” (hot-swap). Wymaganie dotyczące wysokiej dostępności i zapewnienia redundancji nie dotyczy oprogramowania agenta na stacjach roboczych.
- jako usługę realizowaną z chmury – dotyczy tylko zaawansowanej ochrony DSN, filtrowania URL i sandboxingu.

e) Dodatkowe systemy/urządzenia muszą być zaoferowane z pełnym wsparciem producenta co oznacza wymóg zaoferowania pakietów serwisowych dostępnych dla danego rozwiązania na okres taki sam jak dla oferowanych urządzeń NGFW.

f) W przypadku stosowania systemów/urządzeń dodatkowych Zamawiający wymaga, aby były one oferowane i serwisowane przez tego samego producenta co oferowane urządzenia NGFW.

g) Zamawiający wymaga, aby wszystkie dostarczane systemy/urządzenia dodatkowe spełniały warunki wymagań ogólnych pkt. 1, 2 oraz 3.

- h) Wszystkie systemy/urządzenia dodatkowe muszą być dobrane w sposób zapewniający obsługę co najmniej 7000 osób oraz nie mniej niż 5 administratorów.

Szczegółowy wymagania techniczne

I.Opis techniczny

1. Urządzenia NGFW będące przedmiotem umowy muszą być dostarczone jako dedykowane urządzenia w ilości 2 sztuk – pracujące w klastrze niezawodnościowym
2. Muszą obsługiwać:
 - a) 60 Gbps przepustowości Firewall/kontroli aplikacji
 - b) 35 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware
 - c) 15 Gbps dla IPsec VPN
 - d) 20 000 000 jednoczesnych sesji
 - e) 600 000 nowych połączeń na sekundę
 - f) 10.000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN
 - g) 25 wirtualnych routerów posiadających odrębne tablice routingu
 - h) 25 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu. Możliwość licencyjnego zwiększenia liczby wirtualnych instancji firewall do 100.
 - i) 200 stref bezpieczeństwa
 - j) Protokołów routingu
 - a. OSPFv2 oraz OSPFv3
 - b. BGP4
 - k) Lokalnej przestrzeni dyskowej na system co najmniej 240GB (przestrzeń użyteczna) działającej w RAID-1
 - l) Lokalnej przestrzeni dyskowej na logi o pojemności co najmniej 4TB
3. Cechy fizyczne urządzenia:
 - a) Wysokość maksymalnie 8U wraz z zestawem montażowym do szafy RACK 19”;
 - b) Redundantne zasilacze AC 230V Hot-Swap z kompletami kabli
 - c) Porty:
 - 4 porty 1 GigabitEthernet RJ45 lub 4 porty 10-GigabitEthernet RJ45
 - 12 portów 10 GigabitEthernet SFP+ obsługujące moduły optyczne 10GE, moduły optyczne 1GE i moduły miedziane 1GE przy czym 8 z tych portów musi być obsadzonych modułami miedzianymi 1GE tego samego producenta co producent urządzenia
 - 2 porty 40 / 100 GigabitEthernet QSFP+/OSFP28 lub alternatywnie 2 porty 40 GigabitEthernet QSFP+ i 2 porty 100 GigabitEthernet QSFP28
 - 1 port 1 GigabitEthernet RJ45 wyłącznie do celów zarządzania
 - 1 port konsoli szeregowej
 - Urządzenie musi posiadać porty (10GE lub szybsze) dedykowane dla celów połączenia urządzeń w klastr. Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu konfiguracji/zestawienia klastra, portów opisanych powyżej. Zamawiający dodatkowo wymaga dostarczenia wkładek i okablowania

światłowodowego w ilości niezbędnej do połączenia dostarczanych w ramach postępowania urządzeń firewall do pracy w trybie klastra active-passive w obrębie 4 sąsiadujących ze sobą szaf rack.

II.Opis funkcjonalny NGFW

1. Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach tcp i udp. Urządzenie NFGW musi wykrywać co najmniej 2500 aplikacji predefiniowanych przez Producenta.
2. Realizowanie funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:
 - a) Intrusion Prevention System (IPS)
 - b) Antywirus (AV)
 - c) Anty-Spyware / Anty-Malware
 - d) Podstawowa ochrona DNS
 - e) Filtrowanie URL
 - f) Sandbox lokalny lub chmurowy tego samego producenta
3. Bazy sygnatur IPS, AV, Anty-Spyware (lub Anty-Malware jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na urządzeniu NGFW oraz regularnie aktualizowane w sposób automatyczny.
4. Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.
5. Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta.
6. Urządzenie NGFW musi umożliwiać konfigurację AV i IPS w szczególności możliwość wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa – nie dopuszcza się by IPS /lub AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego
7. Urządzenie musi posiadać funkcję wykrywanie aktywności sieci typu Botnet.
8. Urządzenie musi posiadać możliwość zdefiniowania ruchu TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. Deszyfracja ruchu TLS musi być realizowana przed politykami bezpieczeństwa. Wymagane jest wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3 również w wariancie STARTTLS.
9. Urządzenie musi posiadać możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME.
10. Urządzenie musi realizować filtrowanie URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW. Kategorie stron muszą obejmować kategorie wynikające z treści stron www oraz z ryzyka. Musi istnieć możliwość tworzenia własnych list URL bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta. Własne listy muszą mieć wyższy priorytet niż klasyfikacja na bazie kategorii

dostarczanych przez producenta. Musi istnieć możliwość pobierania listy URL z zewnętrznego zasobu dostępnego po https.

11. Urządzenie musi posiadać możliwość wysyłania plików wykonywalnych (co najmniej pliku w formacie PE i ELF) oraz dokumentów (co najmniej ms office i pdf) wykrytych w ruchu sieciowym obsługiwanych przez urządzenie do lokalnego lub chmurowego systemu sandbox celem wykrywania nieznanych ataków.

12. W zakresie podstawowej ochrony DNS urządzenie musi realizować co najmniej:

- a) wykrywanie zapytań do domen złośliwych
- b) fałszowanie odpowiedzi na zapytania DNS zaklasyfikowane jako złośliwe (tzw. DNS sinkholing)

13. Urządzenie musi umożliwiać zestawianie tuneli VPN site-to-site w oparciu o standardy IPsec i IKE.

14. Urządzenie musi umożliwiać zestawianie tuneli VPN dla zdalnego dostępu z wykorzystaniem IPsec i IKE oraz SSL/TLS:

- a) Wymagane jest zestawianie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW - obsługa co najmniej 7000 tuneli/użytkowników.
- b) Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS, Android i iOS
- c) Oprogramowanie klienta VPN dla Windows 10 i macOS 10.15 musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej co najmniej w zakresie sprawdzenia:
 - o czy zainstalowano oprogramowanie anty-wirusowe i czy posiada ono aktualne sygnatury
 - o czy włączony jest osobisty firewall
 - o czy włączone jest szyfrowanie dysku

15. Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora – bez konieczności korzystania z centralnych narzędzi zarządzania.

16. Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.

17. Urządzenie musi obsługiwać 4094 VLAN zgodnie z 802.1q.

18. Urządzenie musi obsługiwać tworzenia „pod interfejsów” na interfejsach pracujących w L2 i L3.

19. Interfejsy urządzenia muszą umożliwiać konfigurację co najmniej następujących trybów pracy: tryb routera (L3), tryb L2, tryb transparentny i tryb nasłuchu. Musi istnieć możliwość konfiguracji różnych interfejsów w wybranym trybie pracy. Tryb pracy nie może być określany globalnie dla wszystkich interfejsów.

20. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, „pod interfejsy” L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.

21. Urządzenie musi umożliwiać translację adresów IP (NAT) statyczną i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
22. Transparentne ustalenie tożsamości w oparciu o:
- a) integrację z kontrolerem domeny Active Directory
 - b) integracji z serwerami Microsoft Exchange
 - c) integracji z serwerami terminalowymi
 - d) integracji bazującej na informacji z logów SYSLOG
23. Firewall musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.
24. Uwierzytelnianie administratorów NGFW za pomocą:
- a) bazy lokalnej
 - b) zewnętrznej usługi katalogowej dostępnej po LDAPS
 - c) RADIUS lub TACACS+
25. Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory, kondycja bezpieczeństwa stacji końcowej.
26. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla wybranych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
27. Deszyfracja komunikacji SSH w celu wykrywania transmisji plików i przekazywania portów.
28. Praca na NGFW musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej muszą odbywać się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian z wcześniejszymi wersjami konfiguracji.
29. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji - rozwiązanie pozwoli na:
- a) wykrycie aplikacji,
 - b) przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
30. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware - rozwiązanie pozwoli na:
- a) wykrycie aplikacji,
 - b) przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych,
 - c) inspekcje IPS całego ruchu
 - d) Inspekcję antywirusową całego ruchu

- e) Inspekcję antymalware/AntySpyware całego ruchu
- f) przesyłanie plików do sandboxa lokalnego i/lub chmurowego w tym przechwytywanie i blokowanie plików określonego typu.

Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

III.Centralne zarządzanie urządzeniami NGFW

Zamawiający wymaga dostarczenia systemu centralnego zarządzania tylko i wyłącznie w przypadku, gdy zaoferowany system bezpieczeństwa sieci w postaci urządzeń typu NGFW nie będzie mógł być podłączony do obecnie posiadanego przez Zamawiającego systemu zarządzania Palo Alto Networks Panorama.

III.a) Wymagania funkcjonalne dla systemu centralnego zarządzania

1. Umożliwia centralne monitorowanie funkcjonowania wszystkich oferowanych urządzeń NGFW.
2. Umożliwia zarządzanie:
 - a) nie mniej niż 10 firewallami rozumianymi jako firewalle fizyczne
 - b) nie mniej niż 100 firewallami rozumianymi jako wirtualne instancje firewall (określane jako kontekst/domena/system) i umożliwia docelowo rozbudowę do systemu dla 200 instancji wirtualnych.
3. Umożliwia zarządza obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
4. Umożliwia dystrybucję i zdalną instalację nowych sygnatur oraz wersji oprogramowania systemowego.
5. Przechowuje różne wersje konfiguracji zarządzanych urządzeń NGFW.
6. Zbiera logi zdarzeń z oferowanych urządzeń NGFW co najmniej o ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
7. Umożliwia korelację logów zdarzeń z zarządzanych firewalli.
8. Umożliwia tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych NGFW.
9. Umożliwia tworzenie raportów na podstawie gromadzonych w logach informacji.

10. Umożliwia tworzenie raportów na podstawie zbudowanych kontenerów/grup urządzeń NGFW.
11. Umożliwia zapisywanie stworzonych raportów, uruchamianie ich w sposób manualny lub automatyczny w określonych przedziałach czasu oraz eksport do formatu tekstowego.
12. Graficzny interfejs centralnego systemu zarządzania (Web GUI) musi być dostępny po protokole HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii Java czy Flash.
13. Umożliwia tworzenie i używanie ról administracyjnych różniących się poziomem dostępu.

III.b) Cechy techniczne systemu centralnego zarządzania

1. System może być dostarczony jako maszyna wirtualna dla środowiska VMware ESXi
2. Zamawiający dedykuje dla celu instalacji systemu następujące zasoby:
 - a) 16 vCPU
 - b) 64 GB pamięci RAM
 - c) 1TB przestrzeni dyskowej (bez uwzględnienia przestrzeni na logi)
3. W zakresie logów ruchowych obsługuje co najmniej:
 - a) 18 TB użytecznej przestrzeni dyskowej na logi inspekcyjne
 - b) Pozwala na obsługę do 150GB logów inspekcyjnych dziennie.
 - c) 5000 logów na sekundę
4. W zakresie logów systemowych obsługuje co najmniej:
 - a) 2 TB użytecznej przestrzeni dyskowej na logi administracyjne (management logs) z możliwością jej rozszerzenia do 5TB w ramach dostarczanej licencji
 - b) Pozwala na obsługę do 2 GB logów administracyjnych (management logs) dziennie,
 - c) 50 logów na sekundę.
5. System może być zbudowany w oparciu o pojedynczą instancję zarządzającą lub w oparciu o dwie osobne maszyny wirtualne, współpracujące pomiędzy sobą, gdzie:
 - a) Jedna maszyna jest dedykowana dla centralnego logowania zdarzeń i raportowania, obsługująca logi inspekcyjne
 - b) Druga maszyna jest dedykowana dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne
6. W przypadku gdy system będzie składał się z dwóch komponentów/maszyn muszą zostać spełnione następujące warunki:
 - a) Oba komponenty muszą pochodzić od jednego producenta i zarazem producenta oferowanego systemu firewall.
 - b) Każdy z komponentów z osobna musi spełniać wymagania w zakresie:
 - o liczby zarządzanych firewalli
 - o liczby docelowo zarządzanych firewalli
 - c) Maszyna dedykowana dla centralnego logowania zdarzeń i raportowania, obsługująca logi inspekcyjne musi spełnić wymagania opisane w p III.b).3

- d) Maszyna dedykowana dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne musi spełnić wymagania opisane w p. III.b).4
7. Zamawiający dopuszcza także dostarczenie systemu centralnego zarządzania w postaci fizycznej - dedykowanych urządzeń. W takim przypadku wymagane jest dostarczenie redundantnego rozwiązania objętego w całości wsparciem i serwisem jednego producenta. Zamawiający wymaga by takie rozwiązanie dysponowało przynajmniej dwoma portami 10 GE SFP+

IV.Licencje oraz wymagania dot. serwisu urządzeń

1. Poniższe wymagania dot. wszystkich urządzeń będących przedmiotem umowy – w tym tych niewyspecyfikowanych a dostarczonych w wyniku konieczności realizacji określonych funkcjonalności.
2. Całość dostarczonego rozwiązania musi pochodzić od jednego producenta.
3. W przypadku, kiedy jakkolwiek funkcjonalność lub parametr ilościowy wymagają zapewnienia licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych funkcjonalności przez okres 36 miesięcy od daty odbioru bez zastrzeżeń potwierdzonego protokołem.
4. Dla systemu firewall należy dostarczyć usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla następujących funkcji
 - a) Aktualizacje bazy aplikacji
 - b) Aktualizacje baz sygnatur IPS
 - c) Aktualizacje baz sygnatur AV
 - d) Aktualizacje/dostęp do bazy URL z kategoryzacją stron
 - e) Możliwość współpracy z systemem sandbox
 - f) Aktualizacji baz dla ochrony DNS
5. Wsparcie techniczne i gwarancja (zwanej dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe niezależne od Wykonawcy realizowane we współpracy z producentem, przez okres 36 miesięcy od daty odbioru bez zastrzeżeń, potwierdzonego protokołem. Wsparcie obejmuje:
 - a) Dostęp do Centrum Wsparcia Technicznego (TAC) przez: stronę internetową, email oraz telefonicznie w języku polskim - wsparcie przy rozwiązywaniu problemów związanych z działaniem urządzeń NGFW oraz systemów dodatkowych w trybie 8x5, tj. co najmniej 8 godzin przez 5 dni w tygodniu;
 - o czas reakcji na zgłoszony drogą mailową lub telefoniczną problem – maks. 8 godzin, liczony w godzinach przyjmowania zgłoszeń, co najmniej 8 godzin przez 5 dni w tygodniu;
 - o przy wystąpieniu awarii urządzenia, któregośkolwiek z jego komponentów lub wyposażenia, w tym modułów optycznych – wymiana lub naprawa (RMA) w trybie NBD w terminie do 3 dni roboczych od daty zgłoszenia, świadczona w miejscu instalacji.
 - b) Dostęp (tj. uprawnienie do pobierania i instalowania) do wszystkich aktualizacji dotyczących oferowanych urządzeń NGFW oraz wszystkich systemów dodatkowych w ramach wymaganych funkcjonalności, wydawanych przez Producenta.
 - c) Dostęp do bazy wiedzy oraz dokumentacji producenta dotyczących instalacji, konfiguracji i utrzymania - w języku polskim lub angielskim.

- d) W przypadku wymiany urządzenia, któregośkolwiek z jego komponentów lub wyposażenia, w tym modułów optycznych – wymiana nastąpi na sprzęt równoważny w terminie zgodnym z pkt. 5.a)
- e) W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki pozostają w całości u Zamawiającego, w terminie zgodnym z pkt. 5.a).
- f) Każda z napraw lub wymian musi być potwierdzona Protokołem Naprawy, zawierającym wpisy dotyczące wykonanych czynności oraz listę naprawionych oraz wymienianych części i komponentów składowych urządzeń.

Zamawiający zastrzega sobie prawo do przeprowadzenia testów w celu weryfikacji deklarowanej przez Wykonawców wydajności urządzeń. W przypadku przeprowadzenia testów Zamawiający poinformuje Wykonawców do 14 dni przed planowanymi testami o potrzebie ich realizacji oraz przekaze wzorzec ruchu względem którego ma być zrealizowane badanie.