

Opis przedmiotu zamówienia

Dostawa urządzeń brzegowych UTM

WSTĘP

Zamawiający w ramach przedmiotowego postępowania zamierza rozbudować posiadaną infrastrukturę sieciową złożoną z klastra HA urządzeń NGFW firmy Check Point tj. QUANTUM 16200 SECURITY GATEWAY.

Celem Zamawiającego jest:

1. zbudowanie ośrodków przetwarzania danych rozlokowanych geograficznie oraz pracujących w trybie ACTIVE-ACTIVE z wykorzystaniem posiadanej infrastruktury oraz zakupywanej w ramach tego postępowania infrastruktury.
2. utrzymanie centralnego zarządzania wszystkimi urządzeniami NGFW poprzez posiadany System Centralnego Zarządzania (SCZ) Check Point Security Management.

Scentralizowane zarządzanie zapewnia Zamawiającemu szybszą analizę potencjalnych problemów, zwiększa bezpieczeństwo poprzez ujednolicenie polityk bezpieczeństwa zarówno na poziomie pojedynczych firewall'i, jak również dla ich grup.

Jednolita infrastruktura, zarządzana przez SCZ, zwiększy automatyzację poprzez automatyczne aktualizacje i zarządzanie regułami bezpieczeństwa, upraszczając procesy administracyjne i poprawiając poziom bezpieczeństwa.

Rozdział I. OGÓLNE WARUNKI REALIZACJI ZAMÓWIENIA

1. PRZEDMIOT ZAMÓWIENIA:

- 1) dostawa 2 szt. urządzeń bezpieczeństwa sieciowego zgodnie ze specyfikacją opisaną w Rozdziale II pkt 1 („Urządzenia”), co obejmuje opracowanie projektu wdrożeniowego, montaż (instalację fizyczną) i uruchomienie Urządzeń, konfigurację zgodnie z projektem wdrożeniowym lub migrację istniejącej konfiguracji na Urządzenia oraz opracowanie dokumentacji powdrożeniowej;
- 2) świadczenie usług asysty technicznej eksperta, o których mowa w Rozdziale III pkt 6-13;
- 3) zorganizowanie i przeprowadzenie warsztatów, o których mowa w Rozdziale III pkt 16.

2. TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA:

- 1) Wykonawca zobowiązany jest dostarczyć Urządzenia jednorazowo, nie później niż 90 dni od zawarcia Umowy. Urządzenia uznaje się za dostarczone z chwilą potwierdzenia pozytywnej weryfikacji ilościowej przez Zamawiającego.
- 2) montaż Urządzeń, ich uruchomienie oraz konfiguracja urządzeń lub migracja konfiguracji, muszą zostać wykonane w ciągu 60 dni od dnia dostarczenia Urządzeń, w godzinach urzędowania Departamentu Informatyzacji i Rejestrów Sądowych Ministerstwa Sprawiedliwości.
- 3) dokumentacja powdrożeniowa zostanie opracowana i dostarczona Zamawiającemu nie później niż w ciągu 14 dni od daty zakończenia prac, o których mowa w pkt. 2 powyżej, potwierdzonych pozytywną weryfikacją przez Zamawiającego, w oryginale (2 egz.) oraz w postaci elektronicznej (plik .doc lub .docx).
- 4) nie później niż w dacie montażu Urządzeń, Wykonawca zobowiązany jest przekazać Zamawiającemu wystawione przez producenta Urządzeń instrukcje ich użytkowania, atesty, deklaracje zgodności, itp.
- 5) termin realizacji usług asysty technicznej obejmuje okres od daty zawarcia Umowy do upływu 48 miesięcy od daty zawarcia Umowy, z tym że nie dłużej niż do wyczerpania limitu 1000 roboczogodzin. W rzeczonym okresie, Zamawiający może składać Wykonawcy zlecenia, a Wykonawca zobowiązany jest takie zlecenia przyjąć do realizacji na zasadach opisanych w Rozdziale III OPZ.
- 6) warsztaty zostaną zrealizowane w ciągu 24 miesięcy od daty zawarcia Umowy, w terminach uzgodnionych w trybie roboczym (po zawarciu Umowy), jak przewidziano w Rozdziale III OPZ.

3. MIEJSCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

- 1) Miejscem realizacji dostawy są dwie lokalizacje: (i) obiekt Ministerstwa Sprawiedliwości przy ul. Czerniakowskiej 100 w Warszawie, oraz (ii) inny obiekt na terenie m.st. Warszawy, którego adres zostanie Wykonawcy wskazany po zawarciu Umowy. To, w której lokalizacji ma być umieszczone dane Urządzenie wynikać będzie z przyjętej architektury rozwiązania;
- 2) Zamawiający zastrzega sobie prawo do zmiany lokalizacji, w których umieszczone są urządzenia infrastruktury sieciowej, w tym Urządzeń będących przedmiotem zamówienia – bez utraty uprawnień z gwarancji i rękojmi;
- 3) Zamawiający wymaga realizacji zgłoszeń w ramach serwisu gwarancyjnego w lokalizacji Urządzeń wynikającej z ppkt 1-2;
- 4) Zlecenia w ramach świadczonych usług asysty technicznej mogą być realizowane zdalnie, przy czym Zamawiający może wymagać ich realizacji w danej lokalizacji, w której umieszczone są poszczególne urządzenia infrastruktury sieciowej;
- 5) Komunikacja oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.

4. SERWIS GWARANCYJNY URZĄDZEŃ

- 1) Wykonawca nie później niż w ciągu 10 dni od dnia zawarcia Umowy ma obowiązek przekazać Zamawiającemu w formie pisemnej dokument „Instrukcja zgłaszania, obsługi i eskalacji zgłoszeń gwarancyjnych”, zawierający:
 - a) instrukcje zgłaszania awarii, w tym formularz Zgłoszenia awarii (Zamawiający będzie korzystał z ww. formularza np. w przypadku zgłoszenia składanego za pośrednictwem poczty elektronicznej czy faksu);
 - b) szczegółowy opis procedury eskalacji, zawierający co najmniej dodatkowy numer telefonu i adres e-mail (pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub reakcji na zgłoszenie);
 - c) dane Wykonawcy - adresy, numery telefonów i faksów, adresy poczty elektronicznej;
 - d) instrukcje dotyczące przeglądania statusu umowy oraz urządzeń nią objętych;
 - e) instrukcje dotyczące pobierania poprawek i nowych wersji oprogramowania ze strony internetowej producenta bez ponoszenia

dodatkowych kosztów.

Wykonawca zobowiązuje się wdrożyć i stosować przez cały okres obowiązywania Umowy powyższe instrukcje i procedury. Przekazane przez Wykonawcę instrukcje i procedury podlegają akceptacji Zamawiającego. Zamawiający może zgłosić uwagi i poprawki do instrukcji i procedur przekazanych przez Wykonawcę, a Wykonawca jest zobowiązany do ich niezwłocznego uwzględnienia i przedstawienia do ponownej akceptacji przez Zamawiającego.

- 2) W przypadku jakichkolwiek zmian danych, o których mowa jest powyżej, w tym danych, o których mowa jest w pkt 1 lit. c, Wykonawca niezwłocznie poinformuje o tym Zamawiającego pisemnie. Instrukcje i procedury, o których mowa powyżej, nie mogą być sprzeczne lub niezgodne z postanowieniami Umowy.
- 3) Zgłoszenie awarii może być dokonywane w postaci: zgłoszenia telefonicznego, za pomocą faksu, z wykorzystaniem serwisu www. udostępnionego przez Wykonawcę, za pomocą poczty elektronicznej. W przypadku dokonania zgłoszenia telefonicznego, Zamawiający potwierdzi je za pomocą faksu lub z wykorzystaniem serwisu www. udostępnionego przez Wykonawcę lub za pomocą poczty elektronicznej.
- 4) Wykonawca będzie przyjmował zgłoszenia awarii lub konsultacji technicznych w ramach wsparcia technicznego całodobowo - 24 godziny na dobę, 7 dni w tygodniu, 365 (366) dni w roku.
- 5) Wykonawca jest zobowiązany do potwierdzenia przyjęcia zgłoszenia awarii w terminie do 60 minut od jego zgłoszenia za pomocą faxu na numer (22) 39 76 111 lub na adres poczty elektronicznej zs@ms.gov.pl lub telefonicznie - na numer podany podczas rejestracji zgłoszenia. W przypadku braku potwierdzenia, po upływie 60 minut od zgłoszenia, Zamawiający wdroży procedurę eskalacji zgłoszenia.
- 6) Wykonawca jest zobowiązany do zapewnienia Zamawiającemu możliwości bieżącego śledzenia statusu zgłoszenia serwisowego za pośrednictwem co najmniej strony www – Wykonawca przekaże Zamawiającemu za pomocą poczty e-mail wszystkie niezbędne informacje, w tym login i hasło, niezbędne do śledzenia statusu zgłoszenia, nie później niż w ciągu 3 dni od dnia zawarcia Umowy.
- 7) Wykonawca będzie realizował zgłoszenia awarii w ramach gwarancji w następujący sposób:
 - a. Zgłoszenie o priorytecie krytycznym awaria krytyczna, tj. całkowita niedostępność Urzędu: czas reakcji do 1 godziny od chwili zgłoszenia awarii przez Zamawiającego, czas realizacji zgłoszenia (przywrócenie dostępności, usunięcie awarii i jej skutków) naprawy (przywrócenia funkcjonalności) do [•] godzin (zgodnie z ofertą Wykonawcy - wybrany Zestawem, o którym mowa w SWZ, nie mniej niż 4 godziny i nie więcej niż 6 godzin) od chwili zgłoszenia awarii krytycznej przez Zamawiającego bez względu na to, czy zgłoszenie zostało potwierdzone czy nie;
 - b. Zgłoszenie o priorytecie niekrytycznym, awaria niekrytyczna-tj. inne niż krytyczne, np. zmniejszenie wydajności (niepowodująca całkowitej niedostępności Urzędu): czas reakcji do 1 godziny od chwili zgłoszenia usterki przez Zamawiającego, czas realizacji zgłoszenia naprawy (przywrócenia pełnej funkcjonalności, usunięcie awarii i jej skutków) do [•] godzin (zgodnie z ofertą Wykonawcy, nie mniej niż 8 godzin i nie więcej niż 16 godzin – wybrany Zestawem, o którym mowa w SWZ) od chwili zgłoszenia awarii niekrytycznej przez Zamawiającego, bez względu na to, czy zgłoszenie zostało potwierdzone czy nie.
- 8) W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z ppkt 7 powyżej:
 - a) Zamawiający ma prawo bez oddzielnego wyroku sądu wypożyczyć, zainstalować i uruchomić urządzenie zastępcze, a kosztami naprawy obciążyć Wykonawcę, zachowując jednocześnie prawo do żądania kary umownej i odszkodowania,
 - b) Zamawiający ma prawo zlecić innemu podmiotowi naprawę Urzędu, a kosztami naprawy obciążyć Wykonawcę, zachowując jednocześnie prawo do żądania kary umownej i odszkodowania.
- 9) W ramach usunięcia awarii Zamawiający dopuszcza możliwość wymiany przez Wykonawcę po uzgodnieniu z Zamawiającym poszczególnych elementów lub podzespołów urządzenia lub całego urządzenia na fabrycznie nowe, wolne od wad, takie samo lub inne, o co najmniej takich samych parametrach, funkcjonalności i standardzie.
- 10) W przypadku, gdy w wyniku usuwania awarii Wykonawca zapewni urządzenie zastępcze, a naprawa Urzędu trwa dłużej niż 6 tygodni lub gdy ten sam element/podzespół/cześć Urzędu będzie podlegał naprawie trzykrotnie w okresie obowiązywania Umowy i nastąpi kolejna (czwarta) awaria, Zamawiający ma prawo żądać wymiany Urzędu na nowe, takie samo lub inne, uzgodnione z Zamawiającym, o co najmniej takich samych parametrach, funkcjonalności i standardzie, co urządzenie podlegające wymianie. Wykonawca zobowiązany jest wymienić urządzenie w ciągu 30 dni od zgłoszenia takiego żądania przez Zamawiającego. Dostarczone w ramach wymiany urządzenie musi być wyprodukowane nie wcześniej niż 6 miesięcy przed wymianą, wolne od wad, fabrycznie nowe - bez śladów użytkowania i bez uszkodzeń, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczypospolitej Polskiej i dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych, zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. W przypadku wymiany urządzenia na nowe, Wykonawca sporządzi protokół z wymiany Urzędu na nowe. Z chwilą podpisania protokołu na Zamawiającego przechodzi prawo własności nowego urządzenia.
- 11) Wykonawca każdorazowo w terminie 7 dni od dnia usunięcia awarii dostarczy Zamawiającemu raport z naprawy Urzędu, zawierający datę i godzinę zgłoszenia, informację, co było przedmiotem naprawy oraz w przypadku przekroczenia czasu usunięcia awarii, o którym mowa w ppkt 7, wskazanie przyczyn przekroczenia czasu usunięcia awarii. Raporty z naprawy będą przygotowywane przez Wykonawcę w języku polskim i przekazywane Zamawiającemu w formie pisemnej (papierowej) do siedziby Departamentu Informatyzacji i Rejestrów Sądowych. Zamawiający w terminie 3 dni roboczych od dnia otrzymania raportu dokonuje jego akceptacji lub zgłasza do niego uwagi, przysyłając je na adres poczty elektronicznej Wykonawcy. Wykonawca zobowiązany jest w terminie 2 dni roboczych od dnia otrzymania uwag do ich uwzględnienia i przedstawienia poprawionej wersji raportu, a w razie nieuwzględnienia uwag – do pisemnego uzasadnienia swojego stanowiska. W takim przypadku stosuje się postanowienie zdania poprzedniego.
- 12) Jeżeli urządzenia dostarczone przez Wykonawcę będą posiadały dyski twarde lub inne nośniki, to w przypadku awarii nośnika, powodującej konieczność jego wymiany, uszkodzony nośnik pozostanie u Zamawiającego. Koszty nośników wymienianych z powodu ich awarii ponosi Wykonawca.
- 13) W celu zapewnienia kompatybilności i poprawności eksploatacji infrastruktury informatycznej dostarczonej przez Wykonawcę, Zamawiający wymaga, aby w ramach gwarancji Wykonawca niezwłocznie po zawarciu Umowy zapewnił:
 - a) dostęp do portali internetowych zawierających narzędzia wsparcia elektronicznego urządzeń i systemu stanowiącego przedmiot umowy oraz zapewnił możliwość korzystania z nich,
 - b) przeszukiwanie portalu internetowego z bazą wiedzy dotyczącej urządzeń i systemu stanowiącego przedmiot umowy,
 - c) pobieranie z serwera WWW lub FTP poprawek i aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego urządzeń (firmware) stanowiących przedmiot umowy, umożliwiających jego instalację, udostępnionych w okresie trwania umowy; pobieranie tych aktualizacji musi być zgodne z zasadami licencjonowania producenta oprogramowania,
 - d) uzyskanie na portalu internetowym informacji o statusie umowy oraz o urządzeniach nią objętych.
- 14) Zamawiający ma prawo do instalowania, wymiany standardowych kart rozszerzeń/modułów (np. modułów optycznych itp.) oraz rozbudowy Urzędów oraz instalacji pobranych poprawek, aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego posiadanych Urzędów (firmware) zgodnie z zasadami wiedzy technicznej przez Zamawiającego lub podmiotu

Komentarz [PK1]: Czyli nie określamy godzin serwisowych jak w innych tego typu umowach?

Komentarz [PK2]: Jw. Całą dobę?

zewnętrznego, któremu zleci te prace Zamawiający, bez utraty prawa do gwarancji.

- 15) Oferowane produkty w ramach zamówienia będą pochodziły z oficjalnego kanału dystrybucyjnego producenta na terenie Unii Europejskiej.

Rozdział II. SPECYFIKACJA TECHNICZNA

WYMAGANIA DOTYCZĄCE URZĄDZEŃ I SYSTEMU

1. Wykonawca musi dostarczyć i zainstalować 2 sztuki Urządzeń. Dokładny opis wymagań dla pojedynczego Urządzenia znajduje się poniżej:
 - a) Urządzenie musi być dostarczone jako wyspecjalizowane urządzenie zintegrowanej ochrony bezpieczeństwa sieci komputerowych (appliance). W architekturze systemu bezpieczeństwa sieciowego musi występować możliwość logicznego wydzielenia instancji routingu i rezerwacji CORE CPU. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez tego samego producenta.
 - b) Urządzenie musi posiadać przepływność w ruchu full-duplex nie mniej niż 27 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji (NGFW), nie mniej niż 15 Gbit/s dla kontroli zawartości tzw. Threat Protection/Threat Prevention (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 31 000 000 jednoczesnych połączeń. Testy wydajności muszą być opublikowane na stronie producenta na dzień składania ofert.
 - c) Urządzenie musi być wyposażone w co najmniej:
 - a. 1 port typu Management 10/100/1000 Base-T;
 - b. 1 port dedykowany niezależny od systemu operacyjnego (umożliwiający np. zdalne włączenie urządzenia i uruchomienie systemu);
 - c. 4 porty 10G SFP+;
 - d. 2 porty 40G QSFP+;
 - e. 4 porty 100G QSFP28 (z możliwością rozbudowy do 8 portów 100G QSFP28 po usunięciu innych modułów).
 - d) W ramach realizacji Umowy należy dostarczyć:
 - a. 4 szt. wkładki SFP+ 10GB SR. Wkładki muszą pochodzić od producenta Urządzenia.
 - b. 2 szt. wkładki światłowodowych 40GBase-SR4 QSFP+ do Urządzenia. Wkładki muszą pochodzić od producenta Urządzenia.
 - c. 2 szt. wkładki światłowodowych 40GBase-SR4 QSFP+ do przełącznika CISCO Nexus 9508, wkładki muszą poprawnie współpracować z wkładkami wyspecyfikowanymi w punkcie powyżej.
 - d. 2 szt. wkładki światłowodowych 100GBase-SR4 QSFP28. Wkładki muszą pochodzić od producenta Urządzenia.
 - e. 2 szt. wkładki światłowodowych 100GBase-SR4 QSFP28 do przełącznika CISCO Nexus 9508, wkładki muszą poprawnie współpracować z wkładkami wyspecyfikowanymi w punkcie powyżej.
 - f. 12 szt. kabli typu patchcord MPO - MPO do wyspecyfikowanych wkładek 40G/100G SR4, OM4 o długości 10 m.
 - g. 12 szt. kabli typu patchcord MPO - MPO, OM4 o długości 7 m
 - h. 12 szt. kabli typu patchcord MPO - MPO, OM4 o długości 3 m.
 - i. 12 szt. kabli typu patchcord MPO - MPO, OM4 o długości 2 m.
 - j. 12 szt. kabli typu patchcord MPO - MPO, OM4 o długości 1 m.
 - k. 20x rura peszel z 2 szt. kabla światłowodowego LC-LC MM OM4 duplex 7m.
 - l. 20x rura peszel z 2 szt. kabla światłowodowego LC-LC MM OM4 duplex 10 m.
 - m. 20x rura peszel z 4 szt. kabla światłowodowego LC-LC MM OM4 duplex 7m.
 - n. 20x rura peszel z 4 szt. kabla światłowodowego LC-LC MM OM4 duplex 10 m.
 - e) Interfejsy sieciowe Urządzenia muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI) oraz w trybie pasywnego nasłuchu (sniffer). Urządzenie musi wprowadzać segmentację sieci na odrębne domeny kolizyjne.
 - f) Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a Urządzenie musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
 - g) Urządzenie musi być wyposażony w dedykowany interfejs sieciowy umożliwiający dostęp do Urządzenia w trybie graficznym oraz umożliwiający co najmniej zdalne:
 - a. wyłączenie Urządzenia bez wyłączania systemu operacyjnego;
 - b. restart Urządzenia;
 - c. zamknięcie systemu operacyjnego, a następnie wyłączenie Urządzenia;
 - d. włączenie Urządzenia, gdy jest wyłączone;
 - e. wyłączenie Urządzenia, a następnie włączenie (tzw. cold boot);
 - f. inwentaryzację modułów zainstalowanych w Urządzeniu,
 - g. monitorowanie stanu Urządzenia.
 - h) Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.
 - i) Urządzenie musi obsługiwać nie mniej niż 250 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. **Jeżeli funkcjonalność wymaga dodatkowej licencji, to jest ona wymagana na etapie realizacji umowy na min. 5 wirtualnych routerów.**
 - j) Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPFv2 i v3.
 - k) Urządzenie zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
 - l) Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).

- m) Urządzenie musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
- n) Urządzenie musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
- o) Identyfikacja aplikacji nie może wymagać podania w konfiguracji Urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
- p) Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall.
- q) Nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall oraz mechanizm Application Control.
- r) Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
- s) Urządzenie musi mieć możliwość wykrywania co najmniej 8500 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
- t) Urządzenie musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji. Dopuszcza się użycie zewnętrznego, darmowego narzędzia.
- u) Urządzenie musi pozwalać na blokowanie transmisji plików np. wykonywalnych.
- v) Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
- w) Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. Licencja na tą funkcjonalność jest wymagana w ramach realizacji umowy.
- x) Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu HTTPS. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. Licencja na tą funkcjonalność jest wymagana w ramach realizacji umowy.
- y) Urządzenie musi posiadać osobny zestaw polityk definiujący ruch SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
- z) Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell).
- aa) Urządzenie musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, MS Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalenie tożsamości musi odbywać się również transparentnie.
- bb) Urządzenie musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesję w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do Urządzenia.
- cc) Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
- dd) Urządzenie musi mieć możliwość posiadania modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie realizacji umowy**
- ee) Urządzenie musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Dopuszcza się aby funkcja filtrowania stron WWW uruchamiana była per Urządzenie. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana w ramach realizacji umowy**
- ff) Urządzenie musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
- gg) Urządzenie musi posiadać moduł inspekcji antywirusowej. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na cały okres wsparcia technicznego w ramach realizacji umowy.**
- hh) Urządzenie musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywana na Urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń przez okres trwania gwarancji. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na cały okres wsparcia technicznego w ramach realizacji umowy.**
- ii) Urządzenie musi posiadać moduł IPS/IDS. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na cały okres wsparcia technicznego w ramach realizacji umowy.**
- jj) Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na Urządzeniu lub z użyciem zewnętrznych narzędzi i wsparcia producenta. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na cały okres wsparcia technicznego w ramach realizacji umowy.**
- kk) Urządzenie musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywana na Urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na cały okres wsparcia technicznego w ramach realizacji umowy.**
- ll) Urządzenie musi posiadać moduł anty-spyware. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na cały okres wsparcia technicznego w ramach realizacji umowy.**
- mm) Urządzenie musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie realizacji umowy.**

- nn) Urządzenie musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
- oo) Urządzenie musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url). Pobrane dane muszą być automatycznie wykorzystywane do blokowania lub wykrywania ruchu do tych zasobów.
- pp) Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie realizacji umowy.**
- qq) Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msoffice, java, swf) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 20 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie realizacji umowy.**
- rr) Integracja z zewnętrznymi systemami typu "Sand-Box". **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie realizacji umowy.**
- ss) Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msoffice, java, swf), oraz kierunku przesyłania (odbieranie, oba – odbieranie/wysyłanie) do określenia ruchu poddanego analizie typu „Sand-Box”. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie realizacji umowy.**
- tt) Urządzenie musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie realizacji umowy.**
- uu) Urządzenie musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
- vv) Urządzenie musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
- ww) Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
- xx) Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie realizacji umowy.**
- yy) Urządzenie musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentication) per user/grupa w celu autentykacji. Polityki definiujące muszą umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, SAML 2.0.
- zz) Urządzenie musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnego źródła, miejsca docelowego, portu. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie realizacji umowy.**
- aaa) System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych adresów IP lub podsieci.
- bbb) Urządzenie musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystać z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakkolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
- ccc) Zarządzanie systemem zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dopuszczalna jest instalacja dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
- ddd) Urządzenie musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na Urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji Urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
- eee) Urządzenie musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
- fff) Urządzenie musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
- ggg) Urządzenie musi być wyposażony w interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu Urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
- hhh) Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
- iii) Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+.
- jjj) Urządzenie musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej dwie metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
- kkk) Urządzenie musi posiadać wbudowane dwa twarde dyski do przechowywania logów i raportów o pojemności nie mniejszej niż 2 x 960 GB SSD (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na Urządzeniu. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
- III) Urządzenie musi posiadać pamięć RAM min. 128 GB.
- mmm) Urządzenie musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane muszą zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
- nnn) Urządzenie musi pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV.

- ooo) Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
- ppp) Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łącz sieciowych.
- qqq) Urządzenie musi posiadać przynajmniej dwa redundantne zasilacze.
- rrr) Wysokość urządzenia nie większa niż 2 RU
- sss) W przypadku wyspecyfikowanych wymagań dostarczenia licencji lub zapewnienia udzielenia licencji, zostaną one udzielone jako wieczyste (bezterminowe), względnie jako licencje czasowe na okres nie krótszy niż do końca okresu gwarancji tj. 48 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu odbioru dostawy urządzeń – Załącznik nr 2 do Umowy, przy czym Wykonawca zobowiązany jest do ich dostarczenia wraz ze wsparciem producenta oprogramowania na okres trwania całego okresu gwarancji tj. 48 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu odbioru dostawy urządzeń – Załącznik nr 2 do Umowy.
- ttt) Dostarczone Urządzenia muszą współpracować z oprogramowaniem posiadanym przez Zamawiającego Systemem Centralnego Zarządzania (SCZ) Check Point Security Management.
- uuu) Dostarczone Urządzenia muszą być wyprodukowane nie wcześniej niż 6 miesięcy przed terminem składania ofert, wolne od wad, fabrycznie nowe - bez śladów użytkowania i bez uszkodzeń, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczypospolitej Polskiej i dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych, zabezpieczających przed uszkodzeniem w trakcie transportu i składowania.
- vvv) Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego do posiadanego przez Zamawiającego Systemu Centralnego Zarządzania (SCZ) Check Point Security Management. Przez system równoważny do systemu Check Point Security Management Zamawiający rozumie system spełniający minimalne wymagania:
- a. Wymagania funkcjonalne:
 - i. Zarządzanie posiadanymi przez Zamawiającego urządzeniami Check Point QUANTUM 16200 R81.20 i Urządzeniami dostarczonymi w ramach przedmiotu Umowy.
 - ii. Pozwala na centralne monitorowanie funkcjonowania oferowanych Urządzeń jak i posiadanych Check Point QUANTUM 16200 R81.20.
 - iii. Pozwala na zarządzanie
 1. Nie mniej niż 10 firewallami rozumianymi jako firewalle fizyczne,
 2. nie mniej niż 15 firewallami rozumianymi jako wirtualne instancje firewall (określane jako kontekst/domena/system) i umożliwia docelowo rozbudowę do systemu dla 200 instancji wirtualnych.
 - iv. Zarządza obiektami używanymi przez wszystkie nowe Urządzenia jak i posiadane Check Point QUANTUM 16200 R81.20 w jednym, centralnym repozytorium.
 - v. Dystrybucja i zdalna instalacja nowych sygnatur oraz wersji oprogramowania nowe Urządzenia jak i posiadane Check Point QUANTUM 16200 R81.20.
 - vi. Przechowuje różne wersje konfiguracji zarządzanych urządzeń.
 - vii. Zbiera logi zdarzeń z oferowanych Urządzeń jak i posiadanych Check Point QUANTUM 16200 R81.20 co najmniej o ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
 - viii. Umożliwia korelację logów zdarzeń z zarządzanych urządzeń.
 - ix. Umożliwia tworzenie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych Urządzeń jak i posiadanych urządzeń Check Point QUANTUM 16200 R81.20.
 - x. Pozwala na eksport logów do plików .csv;
 - xi. Graficzny interfejs (GUI) musi być dostępny z wykorzystaniem protokołu HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii Java czy Flash oraz przez dedykowaną aplikację możliwą do pobrania bezpośrednio z systemu.
 - xii. Umożliwia tworzenie i używanie ról administracyjnych różniących się poziomem dostępu.
 - xiii. Tworzenie, modyfikacja, usuwanie i instalacja polityk bezpieczeństwa na różnych klastrach High Availability np. na nowych Urządzeniach jak i posiadanych przez Zamawiającego Check Point QUANTUM 16200 R81.20.
 - b. Sposób realizacji:
 - i. System musi być dostarczony jako maszyna wirtualna dla środowiska VMware ESXi.
 - ii. Zamawiający dedykuje dla celu instalacji systemu następujące zasoby:
 1. 16 vCPU,
 2. 64 GB pamięci RAM,
 3. 1TB przestrzeni dyskowej (bez uwzględnienia przestrzeni na logi)).
 - iii. W zakresie logów inspekcyjnych obsługuje co najmniej:
 1. 15 TB użytecznej przestrzeni dyskowej na logi inspekcyjne,
 2. Pozwala na obsługę do 150GB logów inspekcyjnych dziennie,
 3. 5000 logów na sekundę.
 - iv. W zakresie logów administracyjnych obsługuje co najmniej:
 1. 4 TB użytecznej przestrzeni dyskowej na logi administracyjne (management logs) z możliwością jej rozszerzenia do 6TB w ramach dostarczanej licencji,
 2. Pozwala na obsługę do 5 GB logów administracyjnych (management logs) dziennie,
 3. 100 logów na sekundę.
 - c. Wykonawca przeniesie całą konfigurację posiadanego systemu Check Point Security Management na nowy system bez utraty posiadanych funkcjonalności i konfiguracji i zapewni prawidłowe działanie zarówno starych jak i nowych Urządzeń dostarczanych w ramach przedmiotu Umowy

- d. Wykonawca utworzy testowe polityki bezpieczeństwa, NAT, obiekty typu HOST, NETWORK, SERVICE i zaimplementuje zarówno na posiadanych przez Zamawiającego urządzeniach Check Point QUANTUM 16200 R81.20 jak i nowych Urządzeniach dostarczanych w ramach przedmiotu Umowy.
- e. Wykonawca skonfiguruje harmonogram wykonywania kopii bezpieczeństwa w równoważnym systemie zarządzania oraz wykona na żądanie Zamawiającego testowe przywrócenie konfiguracji na Urządzeniach dostarczonych w ramach przedmiotu zamówienia.
- f. Wykonawca przeniesie konfigurację tunelu VPN na nowe Urządzenia oraz będzie usuwał awarie/błędy w komunikacji w ramach migrowanego tunelu VPN.

Rozdział III. DODATKOWE WYMAGANIA

1. Zamawiający wymaga, by oprogramowanie sprzętowe (system operacyjny) Urządzeń było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień składania ofert.
2. Wykonawca zapewni gwarancję dla przedmiotu zamówienia w zakresie wskazanym w § 9 Umowy.
3. Zamawiający wymaga posiadania pełnej kontroli nad zgłoszeniami serwisowymi. Zamawiający musi mieć możliwość monitorowania statusu zgłoszeń serwisowych w systemie Wykonawcy lub producenta.
4. Zamawiający wymaga uzyskania, w ramach gwarancji, bezpośredniego dostępu do zasobów internetowych (bazy wiedzy) udostępnianych przez producenta.
5. Rozszerzenie licencji o kolejne funkcjonalności nie może powodować utraty praw gwarancyjnych do oprogramowania oraz nie może wymagać zgody Wykonawcy.
6. W roboczogodzinę asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie, tzn. nie ma znaczenia, ile osób będzie świadczyło asystę techniczną eksperta w danej roboczogodzinie/roboczogodzinach u Zamawiającego. Okresem rozliczeniowym dla usług wsparcia asysty technicznej eksperta jest miesiąc kalendarzowy. Rozliczenie roboczogodzin odbywać się będzie za faktycznie wykorzystane roboczogodziny na podstawie miesięcznego Protokołu odbioru usług asysty technicznej eksperta – Załącznik nr 2 do Umowy. Do roboczogodzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych na warunkach gwarancji.
7. Asysta techniczna eksperta będzie dotyczyła sprzętu i oprogramowania dostarczonych w ramach realizacji umowy.
8. Asysta techniczna będzie realizowana przez eksperta zgodnie z załącznikiem nr 7 do PPU - Wymagania w zakresie Zespołu Wykonawcy dedykowanego do realizacji Umowy oraz skład Zespołu. Zamawiający będzie przekazywać Wykonawcy zlecenia, w których każdorazowo określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
9. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą co najmniej wycenę prac zawartych w zleceniu, proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
10. Zamawiający może zaakceptować propozycję wykonania zlecenia albo odrzucić propozycję, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia.
11. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające co najmniej: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
12. Rozliczenie wsparcia technicznego eksperta odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Zamawiającego, Protokołów odbioru asysty technicznej eksperta.
13. W ramach roboczogodzin wsparcia ekspert na wezwanie Zamawiającego ma obowiązek przybyć do wskazanego miejsca/siedziby na terenie województwa mazowieckiego i tam realizować zgłoszenie.
14. Wykonawca uruchomi i skonfiguruje Urządzenia oraz wykona migrację konfiguracji z zastępowanych urządzeń bezpieczeństwa sieciowego na Urządzenia. Wszystkie prace muszą odbywać się przy obecności osób ze strony Zamawiającego. Plany migracyjne oraz sposób migracji oraz konfiguracji musi być zaakceptowany przez Zamawiającego przed przystąpieniem do prac.
15. Wykonawca w ramach wdrożenia Urządzeń wykona:
 - dostarczenie sprzętu do serwerowni;
 - montaż sprzętu, w tym montaż kabli LAN oraz kabli zasilających;
 - podłączenie sprzętu do sieci zasilającej;
 - opracowanie projektu wdrożeniowego;
 - konfiguracja/migracja konfiguracji z urządzeń posiadanych przez Zamawiającego lub wynikająca z projektu wdrożeniowego.

Uwaga!!!

Przerwa techniczna umożliwiająca uruchomienie produkcyjne urządzeń z migrowaną konfiguracją nie może być dłuższa niż 30 min. W przypadku gdy uruchomienie produkcyjne nowych urządzeń spowoduje dłuższą przerwę techniczną niż 30 min., Wykonawca dokona powrotu do pierwotnej konfiguracji.

16. Wykonawca przeprowadzi warsztaty szkoleniowe powdrożeniowe wedle poniższych opisów i ilości osób.

Warsztat 1 – Minimalny czas trwania - 3 dni. Warsztat dla maksymalnie 4 osób (tj. w 2 turach, każda po maksymalnie 2 osoby).

Warsztat musi dotyczyć urządzeń zaoferowanych w ramach realizacji umowy i obejmować co najmniej następujące zagadnienia:

- zarządzanie bezpieczeństwem;
- zarządzanie polityką bezpieczeństwa;
- warstwy polityki bezpieczeństwa;
- licencjonowanie;
- wizualizacja ruchu;
- podstawowe pojęcia VPN;
- zarządzanie dostępem użytkowników;
- praca z Cluster XL;
- praca z portalem GUI;

- modyfikacja istniejącej polityki bezpieczeństwa;
- inspekcja https;
- konfiguracja dynamicznego i statycznego NAT;
- zarządzanie dostępem administracyjnym;
- instalacja i zarządzanie zdalnym security gateway;
- zarządzanie kopiami zapasowymi;
- definiowanie warstw polityki dostępu;
- implementacja kontroli aplikacji i filtracji url;
- praca z licencjami i kontraktami;
- Praca z logami;
- Utrzymanie logów;
- Konfiguracja "Site-to-Site" VPN pomiędzy lokalizacjami;
- Zapewnienie dostępu użytkowników;
- Praca z Cluster XL;

Warsztat 2 – Minimalny czas trwania - 3 dni. Warsztat dla 4 maksymalnie osób (tj. w 2 turach, każda po maksymalnie 2 osoby) - Warsztat musi dotyczyć urządzeń zaoferowanych w ramach realizacji umowy i obejmować co najmniej następujące zagadnienia:

- zaawansowany firewall;
 - zaawansowane możliwości systemu operacyjnego NGFW;
 - automatyzacja i instrumentacja;
 - klastry VRRP;
 - optymalizacja i akceleracja;
 - akceleracja wielokorowa;
 - kolejkovanie ruchu;
 - identyfikacja zdarzenia;
 - monitorowanie sieci;
 - badanie zdarzeń bezpieczeństwa;
 - usuwanie skutków zdarzeń bezpieczeństwa;
 - raportowanie zdarzeń bezpieczeństwa;
 - środki zapobiegawcze;
 - środowisko wysokiej dostępności;
 - wybór rozwiązania zdalnego dostępu;
 - opcje zdalnego dostępu;
 - polityka dostępu mobilnego;
 - zagrożenia;
 - systemy wykrywania włamań (ips);
 - antywirus;
 - Anti-Bot;
 - technologia "sandbox";
 - zapobieganie zagrożeniom mobilnym;
 - wgrywanie hotfix;
 - konfiguracja nowego klastra firewall;
 - bazowe komendy linii poleceń w administracji firewall;
 - konfiguracja manualna NAT;
 - zarządzanie obiektami za pomocą API;
 - włączenie VRRP;
 - ocena zagrożeń przy pomocy systemu monitorowani;
 - zarządzanie dostępem mobilnym;
 - zrozumienie ochrony IPS;
 - wdrożenie IPS Geo Protections;
 - przegląd ustawień Threat Prevention i Protections;
- a. Wykonawca zobowiązany jest do przeprowadzenia warsztatów w ośrodku szkoleniowym na terenie Warszawy. Za zgodą Zamawiającego, warsztaty mogą zostać przeprowadzone na odległość, w trybie zdalnym uzgodnionym roboczo przez Strony.
 - b. Każdy uczestnik otrzyma certyfikat jego ukończenia.
 - c. Warsztaty muszą być prowadzone w języku polskim.
 - d. Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie warsztatów. Wykonawca zapewni co najmniej jedną osobę trenera, która posiada niezbędną wiedzę i doświadczenie do wykonania warsztatów, a w szczególności co najmniej 12-miesięczne doświadczenie praktyczne w przeprowadzaniu warsztatów z zakresu oferowanego rozwiązania.
 - e. Wykonawca musi dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazę szkoleniową z odpowiednimi pomieszczeniami wraz z zapleczem do przeprowadzenia warsztatów dla osób dorosłych, tj. sale dostosowane do prowadzenia zajęć, dobrze oświetlone (światło dzienne i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy, wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowania i pomoce dydaktyczne niezbędne do wykonania zamówienia.

- f. Wykonawca w terminie do 30 dni od dnia podpisania bez zastrzeżeń Protokołu odbioru dostawy urządzeń, przedstawi Zamawiającemu do akceptacji Program warsztatów. Program musi zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne. Program musi zawierać również informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu warsztatów.
 - g. Wykonawca, w uzgodnieniu z Zamawiającym, przygotowuje szczegółowe harmonogramy warsztatów – z rozpisaniem na dni i godziny i dostarczy je do 30 dni od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu odbioru dostawy urządzeń **-Załącznik nr 2** do Umowy. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.
 - h. Zajęcia muszą odbywać się w dni powszednie od poniedziałku do piątku, w godzinach od 8.00 do 17.00, z tym, że przez nie więcej niż 8 godzin zegarowych dziennie. Harmonogram i program muszą zostać wydrukowane i rozdane uczestnikom warsztatów na pierwszym spotkaniu.
 - i. Wykonawca przygotowuje i zapewni materiały warsztatowe dla każdego uczestnika do danego rodzaju warsztatu, pozwalające na samodzielną edukację z zakresu tematyki warsztatów (opracowania, wydruku materiałów warsztatowych).
 - j. Komplet materiałów warsztatowych dla każdego uczestnika warsztatu obejmuje:
 - a) papierową wersję materiałów warsztatowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych;
 - b) materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne niezbędne do realizacji warsztatów.
 - k. Komplet materiałów musi zostać rozdany uczestnikom warsztatów w pierwszym dniu zajęć.
 - l. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.
 - m. Wykonawca zapewni: na potrzeby wyżywienia uczestników warsztatów odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się warsztaty. Miejsce posiłku nie może być oddalone dalej niż 10 minut drogi pieszo od miejsca warsztatów; obiady powinny być zróżnicowane, dany zestaw obiadowy nie może powtarzać się częściej niż raz na 3 dni warsztatowe; Wykonawca zapewni 2 przerwy kawowe podczas jednego dnia warsztatów.
 - a) W zakresie wyżywienia uczestników warsztatów Wykonawca zapewni:
 - i. obiad dwudaniowy dla wszystkich uczestników warsztatów - (z opcją wegetariańską) obejmujący: zupę, gorące danie główne (mięsne lub rybne) z dodatkami skrobiowymi oraz surówką/sałatkami, deser (wyroby cukiernicze lub owoce sezonowe), kawę i herbatę wraz z dodatkami, wodę mineralną gazowaną i niegazowaną.
 - ii. Wykonawca zapewni następujące gramatury wymienionych powyżej posiłków:
 - zupa – co najmniej 0,25 l na uczestnika warsztatów,
 - danie gorące (mięsne lub rybne, opcja wegetariańska - warzywne) – co najmniej 150 g na uczestnika warsztatów,
 - zestaw surówek/sałatek – co najmniej 150 g na uczestnika warsztatów,
 - dodatki skrobiowe - porcja ziemniaków lub frytek / makaronu / ryżu / kaszy – co najmniej 200 g na uczestnika warsztatów,
 - kawa, herbata, woda mineralna gazowana i niegazowana - co najmniej 0,5 l na uczestnika warsztatów.
 - iii. Przerwa kawowa dla wszystkich uczestników warsztatów podczas jego trwania:
 - serwis będzie dostępny przy sali szkoleniowej;
 - naczynia, w których serwowany jest serwis kawowy powinny być szklane lub ceramiczne;
 - Serwis kawowy dla każdego uczestnika warsztatów obejmuje:
 - butelkowaną wodę mineralną gazowaną i niegazowaną (0,5 l);
 - świeżo parzoną, gorącą kawę z ekspresu lub zaparzacza oraz kawę sypaną i rozpuszczalną;
 - herbatę – co najmniej 3 rodzaje herbat w torebkach;
 - dodatki – cukier, mleko do kawy, cytrynę;
 - dodatki - np. ciastka / wafelki i inne słodkie oraz ciasto.
 - b) W zakresie wyżywienia Wykonawca zobowiązany jest do:
 - i. terminowego przygotowania i podania posiłków, zgodnie z ramowym programem warsztatu,
 - ii. zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowaniu posiłków i ich podawaniu,
 - iii. przygotowania posiłków zgodnie z zasadami racjonalnego wyżywienia, urozmaiconych z pełnowartościowych, świeżych produktów z ważnymi terminami przydatności do spożycia,
 - iv. przestrzegania w trakcie realizacji usług wchodzących w zakres przedmiotu umowy obowiązujących przepisów sanitarnych, w tym ustawy z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia. (Dz.U.2015.594 j.t. z późn. zm.).
 - c) Czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin zegarowych warsztatów.
 - n. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.
 - o. Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru warsztatów – Załącznik nr 2 do Umowy wraz z dołączonymi załącznikami, tj. oryginalną listą obecności, harmonogramem i programem warsztatu oraz ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.
17. Wykonawca opracuje projekt wdrożeniowy oraz dokumentację powykonawczą (oraz przeniesie wszelkie prawa autorskie do nich – jak to przewidziano w § 8 Umowy), w tym co najmniej:
- a. Dla projektu wdrożeniowego:
 - i. diagramy połączeniowe dla wszystkich komponentów sieci Zamawiającego powiązanych z Urządzeniami;
 - ii. konfigurację przewidzianą dla wszystkich urządzeń oraz propozycje zmian dla istniejących urządzeń połączonych z przedmiotem zamówienia;
 - iii. harmonogram wdrożenia;
 - iv. koncepcję testów następujących po wszystkich etapach wdrożenia;
 - v. plan awaryjny „backout” dla każdego kroku wdrożenia;
 - vi. koncepcję testów redundancji wykonywanych po zakończeniu wdrożenia.
 - b. Dla dokumentacji powykonawczej:
 - i. diagramy połączeń;

- ii. opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu;
 - iii. pełne konfiguracje urządzeń;
 - iv. wyniki testów redundancji.
18. Licencje na oprogramowanie sprzętowe, o których mowa w Rozdziale II, będą niewyłączne, nieograniczone terytorialnie i zostaną udzielone zgodnie z opublikowanymi przez producenta warunkami licencyjnymi, z tym zastrzeżeniem, że obejmą co najmniej następujące pola eksploatacji:
- a. prawo do instalowania oprogramowania, na które udzielana jest licencja, w liczbie kopii / stanowisk / serwerów / użytkowników charakterystycznej dla tego oprogramowania;
 - b. prawo do korzystania w dowolny sposób ze wszystkich funkcjonalności oprogramowania, na które udzielana jest licencja;
 - c. prawo do aktualizowania oprogramowania, na które udzielana jest licencja, poprzez zamówienie i zainstalowanie nowszych wersji oprogramowania, z zachowaniem wszystkich pól eksploatacji wymienionych w pkt 1 i 2 powyżej;
 - d. prawo do instalowania wszelkich poprawek opublikowanych na stronach producenta oprogramowania oraz na polach eksploatacji określonych w opublikowanych przez producenta oprogramowania warunkach licencyjnych.
19. Dla licencji na oprogramowanie sprzętowe, o których mowa w pkt 18, zostanie zapewnione wsparcie producenta oprogramowania, które obejmie co najmniej:
- a. diagnostykę zdarzeń dotyczących oprogramowania;
 - b. dostarczanie rozwiązań błędów oprogramowania;
 - c. zapewnienie łat (ang. patches), tj. poprawek lub aktualizacji mających na celu usunięcie problemów, błędów, rozszerzenie funkcjonalności lub zwiększenie wydajności wcześniejszej wersji oprogramowania;
 - d. zapewnienie aktualizacji do nowych, wyższych wersji oprogramowania (ang. upgrades);
 - e. udzielanie odpowiedzi na zapytania związane z instalacją i eksploatacją dostarczonego oprogramowania.