OPIS PRZEDMIOTU ZAMÓWIENIA

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest:

1) dostawa dwóch urządzeń TYP – HA do zabezpieczenia ruchu sieciowego w postaci rozwiązań Next Generation Firewall (NGFW) (dalej jako: „Urządzenia"). Całościowy system bezpieczeństwa musi być zrealizowany poprzez dwa urządzenia działające w klasterze niezawodnościowym;
2) dostawa trzech urządzeń TYP – VPN do zabezpieczenia ruchu sieciowego w postaci rozwiązań Next Generation Firewall (NGFW) na potrzeby tunelowania ruchu sieciowego;
3) dostawa dwóch urządzeń TYP – MGMT do zabezpieczenia ruchu sieciowego w postaci rozwiązań Next Generation Firewall (NGFW). Całościowy system bezpieczeństwa musi być zrealizowany poprzez dwa urządzenia działające w klasterze niezawodnościowym;
4) wdrożenie dostarczonych Urządzeń na podstawie przyjętego projektu technicznego;
5) udzielenie lub zapewnienie udzielenia licencji na oprogramowanie wskazane w niniejszym Załączniku
6) opracowanie i dostarczenie projektu technicznego oraz dokumentacji powdrożeniowej;
7) świadczenie usługi asysty technicznej inżyniera w liczbie 1000 roboczogodzin ;
8) przeprowadzenie warsztatów powdrożeniowych;
9) świadczenie przez Wykonawcę usług serwisu gwarancyjnego.

2. TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1) w zakresie wymienionym w pkt 1 ppkt 1 – 6 – w terminie do 90 dni kalendarzowych od dnia zawarcia umowy;
2) w zakresie wymienionym w pkt 1 ppkt 9 – przez okres 44 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji;
3) w zakresie wymienionym w pkt 1 ppkt 7 – przez okres 44 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji albo do wyczerpania puli roboczogodzin, w zależności które zdarzenie nastąpi wcześniej;
4) w zakresie wymienionym w pkt 1 ppkt 8 – przez okres 24 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji;

3. MIEJSCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1) Miejscem realizacji przedmiotu zamówienia jest budynek Ministerstwa Sprawiedliwości przy ul. Czerniakowskiej 100 w Warszawie lub inna lokalizacja wynikająca z punktu 2.
2) Zamawiający zastrzega sobie prawo do zmiany lokalizacji Urządzeń w trakcie trwania umowy, wynikającą ze zmian organizacyjnych Zamawiającego, w tym m.in. w związku ze zmianą siedziby Zamawiającego lub zmianą miejsca realizacji przedmiotu zamówienia w obrębie województwa mazowieckiego, po pisemnym zawiadomieniu Wykonawcy, na co najmniej 5 dni przed terminem zmiany.

3) Koszt transportu oraz zadanie przeniesienia Urządzeń do nowej siedziby Zamawiającego pokrywa Wykonawca. Wykonawca zapewni transport do nowej siedziby Zamawiającego. Zamawiający gwarantuje, iż maksymalna ilość zmian lokalizacji nie przekroczy 2 w trakcie trwania umowy.
4) Zamawiający zastrzega sobie prawo do zmiany miejsca umieszczenia Urządzeń będącego przedmiotem zamówienia – bez utraty prawa do gwarancji.
5) Zamawiający wymaga realizacji zgłoszeń w miejscu określonym w ppkt 1 i 2.
6) Zamawiający nie dopuszcza napraw Urządzeń poza miejscem realizacji przedmiotu zamówienia.
7) Komunikacja oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.

4. NIETECHNICZNE CECHY URZĄDZEŃ

1) Przedmiot zamówienia musi być legalny, fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu, spełniający normy CE.
2) Zamawiający wymaga, aby wszystkie dostarczane Urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje jak też samo Urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.
3) Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełną gwarancją producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili dostawy i 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
4) Zamawiający wymaga, aby zaoferowane Urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

5. GŁÓWNE ZASTOSOWANIA

Rozwiązanie NGFW powinno realizować co najmniej następujące funkcje
1) ochronę zasobów serwerowych Zamawiającego przed ingerencją z zewnątrz;
2) ochronę zasobów serwerowych Zamawiającego przez atakami z wnętrza sieci własnej;
3) kontrolę korzystania z zasobów internetowych przez użytkowników;
4) kontrolę przesyłanych danych z podmiotów współpracujących z Zamawiającym;
5) zdalny dostęp do sieci.

6. DODATKOWE SYSTEMY ZEWNĘTRZNE

Zamawiający dopuszcza, aby całościowy system bezpieczeństwa był zbudowany w oparciu o wymagane komponenty opisane w OPZ wraz z elementami dodatkowymi, których zastosowanie jest opcjonalne i dobrowolne. Decyzja o ich zastosowaniu leży w gestii Wykonawcy – jeżeli uzna on, iż dla osiągnięcia opisanych wymagań niezbędne są dodatkowe systemy zewnętrzne to Zamawiający zezwala na ich zastosowanie pod warunkami opisanymi poniżej:

1) stosowanie dodatkowych systemów nie może dotyczyć funkcji ochronnych NGFW (np. wykrywania aplikacji, obsługi IPS, AV czy NAT);
2) stosowanie dodatkowych systemów nie może powodować ominięcia reguł bezpieczeństwa (np. weryfikacja kondycji bezpieczeństwa stacji końcowej nie może odbywać się w oparciu o integrację z systemem logowania i raportowania, bez wykorzystania reguł bezpieczeństwa);

Stosowanie dodatkowych systemów jest dopuszczalne, tylko jeśli są one konieczne dla:
1) weryfikacji tożsamości użytkowników – system uwierzytelniania;
3) realizacji funkcji zarządzania firewallem i uprawnieniami administratorów;
4) zatwierdzania i pracy na konfiguracji kandydackiej;
5) realizacji funkcji inspekcji ruchu SSL;
6) realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania.

Stosowanie dodatkowych systemów jest możliwe 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);
- system musi być dostarczony jako klaster 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). Konfiguracja analogiczna dla konfiguracji urządzeń NGFW.
- Systemy wspomagające muszą być zaoferowane z pełnym wsparciem producenta co oznacza wymóg zaoferowania wszystkich pakietów serwisowych dostępnych dla danego rozwiązania,

W przypadku stosowania systemów wspomagających Zamawiający wymaga by były one oferowane przez tego samego producenta co oferowany system firewall i całościowo serwisowane przez tego producenta.
Zamawiający wymaga, aby wszystkie dostarczane systemy wspomagające były sprawdzone w praktyce rynkowej i spełniały wymagania w tym obszarze analogicznie do firewalli, oznacza to, iż oprogramowanie systemowe realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.
Maksymalna wysokość wszystkich Urządzeń – oferowanego klastra firewalli (dotyczy NGFW **TYP – HA**) wraz z wszystkimi systemami wspomagającymi nie może być większa niż 2x2U (determinowane jest to przez wysokość migrowanych urządzeń).

7. WYMAGANIA TECHNICZNE DLA NGFW

A. <u>TYP - HA</u>

I. NGFW – sztuk 2, urządzenia pracujące w klastrze niezawodnościowym

1) Firewall'e muszą być dostarczone w postaci dedykowanych urządzeń.
2) Muszą zapewniać obsługę minimum:
    a. 70 Gbps przepustowości Firewall/kontroli aplikacji;
    b. 40 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;

c. 42 Gbps dla IPsec VPN;
d. 7 000 000 jednoczesnych sesji;
e. 350 000 nowych połączeń na sekundę;
f. 5 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
g. 20 wirtualnych routerów posiadających odrębne tabele routingu;
h. 20 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 120.
i. 200 stref bezpieczeństwa;
j. Protokołów routingu: OSPFv2 i OSPFv3, BGP4;
k. Lokalnej przestrzeni na logi co najmniej o pojemności 480GB

3) Cechy urządzenia:
   a. Wysokość maksymalnie 2U wraz z zestawem montażowym do szafy RACK 19”;
   b. dwa redundantne zasilacze AC 230V Hot-Swap z kompletami kabli;
   c. 8 portów 1-GigabitEthernet RJ45 lub 8 portów 10-GigabitEthernet RJ45
   d. 12 portów 10 Gigabit Ethernet SFP+ obsługujące moduły optyczne SR oraz LR
   e. 4 porty 25 Gigabit Ethernet SFP28
   f. 4 porty 40/100 Gigabit Ethernet QSFP28 lub alternatywnie 4 porty 40 Gigabit Ethernet QSFP+ i 4 porty 100 Gigabit Ethernet QSFP28
   g. 1 port 1-GigabitEthernet RJ45 wyłącznie do celów zarządzania;
   h. Urządzenie musi posiadać port (40GE lub szybsze) dla celów połączenia urządzeń w klaster (high availability). Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.

II. Założenia podstawowe dla rozwiązań 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 NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 3000 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. URL Filtering,
   f. Sandbox lokalny lub chmurowy tego samego producenta – co najmniej dla plików wykonywalnych,

3) Bazy sygnatur IPS, AV, Anty-Spyware (lub Anty-Malware jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, 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 (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
6) Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności 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) Wykrywanie aktywności sieci typu Botnet.
8) Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:
    a. Realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 10 Gbps inspekcji TLS dla sesji http 64K;
    b. Jest wyposażone w co najmniej 4 interfejsy 10 Gigabit Ethernet SFP+;
    c. Zapewnia redundancję zasilaczy analogicznie do urządzeń firewall;
    d. Musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewall'a;
    e. obsługujące w chwili dostawy co najmniej 20 instancji wirtualnych pozwalających na powiązanie ich z wirtualnymi instancjami realizowanymi przez urządzenia firewall oraz umożliwiające docelowo obsługę 50 instancji (np. poprzez dokupienie odpowiedniej licencji);
    f. Musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewall'a;
    g. W przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.
9) Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
10) Filtrowanie ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp) oraz określenie ryzyka do niej przypisanego (co najmniej wysokie – średnie – niskie). Możliwość tworzenia własnych list stron („whitelist" oraz „blacklist") bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta. Własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.

11) Możliwość wysyłania plików przesyłanych przez urządzenie do lokalnego lub chmurowego systemu Sandbox (który należy zapewnić w ofercie bądź w postaci fizycznego urządzenia bądź usługi subskrypcji):
    a. Urządzenie firewall musi pozwalać na przesyłanie do systemu Sandbox plików zdefiniowanych przez administratora – co najmniej exe, dll, java, MS Office
    b. Urządzenie firewall musi być aktualizowane o nowo wykryte (w Sandbox zagrożenia).
    c. Administrator musi posiadać dostęp do raportów z Sandbox'a dotyczących plików wysłanych przez urządzenie firewall oraz posiadać możliwość manualnego wysłania pliku do Sandbox (np. poprzez upload poprzez stronę www)
    d. Dopuszcza się zaoferowanie lokalnego rozwiązania Sandbox (zapewnianego przez producenta firewall'i) – należy wówczas przewidzieć urządzenie pozwalające na jednoczesną analizę co najmniej 30 próbek/plików (VM Sandboxing)
    e. Dopuszcza się zaoferowanie chmurowego rozwiązania Sandbox (realizowanego przez producenta firewall'i). W przypadku, jeżeli producent licencjonuje dostęp do chmurowego Sandbox'a należy przewidzieć licencję pozwalającą na jednoczesną analizę minimum 30 próbek/plików (VM Sandboxing)
    f. Wymagane jest by możliwa była analiza 30 próbek/plików jednocześnie bez względu na to czy pliki te wysłane będą automatycznie czy manualnie przez administratora, czy też będzie to „mix" plików pochodzących zarówno bezpośrednio z firewall'a i od administratorów.
12) Podstawowa ochrona DNS co najmniej w zakresie:
    a. wykrywanie zapytań do domen złośliwych.
    b. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS Sinkholing)
13) Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
14) Zestawianie tuneli SSL VPN w konfiguracji Remote – Access VPN.
    a. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW – obsługa co najmniej 5000 tuneli/użytkowników,
    b. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows i MacOS,
    c. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewall'a.
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) Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
17) Obsługa 4094 VLAN zgodnych z 802.1q.
18) Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
19) Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
20) Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. 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.

21) Transparentne ustalenie tożsamości w oparciu o:
    a. integrację z kontrolerem domeny Active Directory;
    b. integrację z serwerami Microsoft Exchange;
    c. integrację z serwerami terminalowymi;
    d. integrację bazującą na informacji z logów SYSLOG pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX;
22) 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.
23) Uwierzytelnianie administratorów NGFW za pomocą:
    a. bazy lokalnej;
    b. zewnętrznej usługi katalogowej dostępnej po LDAPS;
    c. RADIUS lub TACACS+.
24) 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
25) Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
26) Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).
~~27)~~ Integracja funkcji orkiestratora SSL/Decryption Brokera połączeń wychodzących w urządzeniu NGFW z zewnętrznymi narzędziami bezpieczeństwa – funkcjonalności deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS. Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do NGFW, w celu jego dalszego przetwarzania. NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3.
28) Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają 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 (m.in. polityk, konfiguracji interfejsów, routingu itp.), z wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

III. WYMAGANIA LICENCYJNE

1) Całość rozwiązania będzie pochodziła od jednego producenta.
2) W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres co najmniej 44 miesięcy od daty odbioru bez zastrzeżeń potwierdzonego protokołem.
3) 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 podstawowej ochrony DNS,
g. Możliwość realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN).

B. TYP – VPN

I. NGFW – sztuk 3, urządzenia do tunelowania ruchu sieciowego.

1) Firewalle muszą być dostarczone w postaci dedykowanych urządzeń.
2) Obsługa:
   a. 2,2 Gbps przepustowości Firewall/kontroli aplikacji.
   b. 1 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
   c. 1,6 Gbps dla IPsec VPN;
   d. 200 000 jednoczesnych sesji;
   e. 37 000 nowych połączeń na sekundę;
   f. 1000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
   g. 3 wirtualnych routerów posiadających odrębne tabele routingu;
   h. 50 stref bezpieczeństwa;
   i. Protokołów routing: OSPFv2, OSPFv3 i BGP4;
   j. Lokalnej przestrzeni na logi co najmniej o pojemności 128GB

3) Cechy urządzenia:
   a. Wysokość maksymalnie 1U
   b. 8 portów 1 Gigabit Ethernet RJ45
   c. 1 port 1 Gigabit Ethernet RJ45 wyłącznie do celów zarządzania;

II. Założenia podstawowe dla rozwiązań 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 NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 3000 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. URL Filtering
   f. Sandbox lokalny lub chmurowy tego samego producenta – co najmniej dla plików wykonywalnych
3) Bazy sygnatur IPS, AV, Anty-Spyware (lub Anty-Malware jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, 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 (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
6) Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności 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) Wykrywanie aktywności sieci typu Botnet.
8) Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
9) Filtrowanie ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW. Możliwość tworzenia własnych list stron („whitelist" oraz „blacklist") bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta. Własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.
10) Możliwość wysyłania plików przesyłanych przez urządzenie do lokalnego lub chmurowego systemu Sandbox (który należy zapewnić w ofercie bądź w postaci fizycznego urządzenia bądź usługi subskrypcji).
    a. Urządzenie firewall musi pozwalać na przesyłanie do systemu Sandbox plików zdefiniowanych przez administratora – co najmniej exe, dll, java, MS Office,
    b. Urządzenie firewall musi być aktualizowane o nowo wykryte (w Sandbox zagrożenia),
    c. Administrator musi posiadać dostęp do raportów z Sandbox'a dotyczących plików wysłanych przez urządzenie firewall oraz posiadać możliwość manualnego wysłania pliku do Sandbox (np. poprzez upload poprzez stronę www).
    d. Dopuszcza się zaoferowanie lokalnego rozwiązania Sandbox (zapewnianego przez producenta firewalli) – należy wówczas przewidzieć urządzenie pozwalające na jednoczesną analizę co najmniej 30 próbek/plików (VM Sandbox'ing)
    e. Dopuszcza się zaoferowanie chmurowego rozwiązania Sandbox (realizowanego przez producenta firewall'i). W przypadku, jeżeli producent licencjonuje dostęp do chmurowego Sandbox'a należy przewidzieć licencję pozwalającą na jednoczesną analizę minimum 30 próbek/plików (VM Sandbox'ing).
    f. Wymagane jest by możliwa była analiza 30 próbek/plików jednocześnie bez względu na to czy pliki te wysłane będą automatycznie czy manualnie przez administratora, czy też będzie to „mix" plików pochodzących zarówno bezpośrednio z firewall'a i od administratorów.
11) Podstawowa ochrona DNS co najmniej w zakresie:
    a. wykrywanie zapytań do domen złośliwych,
    b. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing),
12) Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
13) Zestawianie tuneli SSL VPN w konfiguracji Remote Access VPN.
    a. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW – obsługa co najmniej 1000 tuneli/użytkowników,

   b. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows i MacOS,
   c. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewall'a.
14) 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.
15) Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
16) Obsługa 4094 VLAN zgodnych z 802.1q.
17) Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
18) Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
19) Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. 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.
20) Transparentne ustalenie tożsamości w oparciu o:
   a. integrację z kontrolerem domeny Active Directory,
   b. integrację z serwerami Microsoft Exchange,
   c. integrację z serwerami terminalowymi,
   d. integrację bazującą na informacji z logów SYSLOG pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX
21) 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.
22) Uwierzytelnianie administratorów NGFW za pomocą:
   a. bazy lokalnej,
   b. zewnętrznej usługi katalogowej dostępnej po LDAPS,
   c. RADIUS lub TACACS+.
23) 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
24) Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
25) Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).
26) Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają 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 (m.in. polityk, konfiguracji interfejsów, routingu itp.), z wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

III. WYMAGANIA LICENCYJNE

1) Całość rozwiązania będzie pochodziła od jednego producenta.

2) W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres co najmniej 44 miesięcy od daty odbioru bez zastrzeżeń potwierdzonego protokołem.
3) 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 podstawowej ochrony DNS,
    g. Realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN).

I. NGFW – sztuk 2, urządzenia pracujące w klastrze niezawodnościowym

1) Firewalle muszą być dostarczone w postaci dedykowanych urządzeń.
2) Obsługa:
    a. 37 Gbps przepustowości Firewall/kontroli aplikacji;
    b. 22 Gbps przepustowości Firewall / kontroli aplikacji / IPS / Antywirus / Antymalware;
    c. 20 Gbps dla IPsec VPN;
    d. 3 200 000 jednoczesnych sesji;
    e. 290 000 nowych połączeń na sekundę;
    f. 12 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
    g. 1 wirtualny router posiadający odrębne tabele routingu;
    h. 10 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 Sandbox'em), tablicy routingu oraz realizacji zdalnego dostępu. Możliwość licencyjnego zwiększenia liczby wirtualnych instancji firewall do 20 (nie jest wymagana na etapie postępowania).
    i. 200 stref bezpieczeństwa;
    j. Protokołów routingu: OSPFv2 i OSPFv3, BGP4;
    k. Lokalnej przestrzeni na logi co najmniej o pojemności 480GB

3) Cechy urządzenia:
    a. Wysokość maksymalnie 2U wraz z zestawem montażowym do szafy RACK 19";
    b. dwa redundantne zasilacze AC 230V Hot-Swap z kompletami kabli;
    c. 8 portów 1 Gigabit Ethernet RJ45 lub 8 portów 10 Gigabit Ethernet RJ45
    d. 12 portów 10 Gigabit Ethernet SFP+ obsługujące moduły optyczne SR oraz LR
    e. 4 porty 25 Gigabit Ethernet SFP28
    f. 4 porty 40/100 Gigabit Ethernet QSFP28 lub alternatywnie 4 porty 40 Gigabit Ethernet QSFP+ i 4 porty 100 Gigabit Ethernet QSFP28
    g. 1 port 1 Gigabit Ethernet RJ45 wyłącznie do celów zarządzania;
    h. Urządzenie musi posiadać port (10GE lub szybsze) dla celów połączenia urządzeń w klaster (high availability). Porty te muszą być traktowane jako

dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.

II. Założenia podstawowe dla rozwiązań 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 NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 3000 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. URL Filtering,
    f. Sandbox lokalny lub chmurowy tego samego producenta – co najmniej dla plików wykonywalnych,
3) Bazy sygnatur IPS, AV, Anty-Spyware (lub Anty-Malware jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, 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 (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
6) Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności 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) Wykrywanie aktywności sieci typu Botnet.
8) Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:
    a. Realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 10 Gbps inspekcji TLS dla sesji http 64K,
    b. Jest wyposażone w co najmniej 4 interfejsy 10 Gigabit Ethernet SFP+
    c. Zapewnia redundancję zasilaczy analogicznie do urządzeń firewall

   d. Musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewall'a
   e. obsługujące w chwili dostawy co najmniej 10 instancji wirtualnych pozwalających na powiązanie ich z wirtualnymi instancjami realizowanymi przez urządzenia firewall oraz umożliwiające docelowo obsługę 20 instancji (np. poprzez dokupienie odpowiedniej licencji)
   f. Musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewall'a.
   g. W przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.
9) Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
10) Filtrowanie ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp) oraz określenie ryzyka do niej przypisanego (co najmniej wysokie – średnie – niskie). Możliwość tworzenia własnych list stron („whitelist" oraz „blacklist") bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta. Własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.
11) Możliwość wysyłania plików przesyłanych przez urządzenie do lokalnego lub chmurowego systemu Sandbox (który należy zapewnić w ofercie bądź w postaci fizycznego urządzenia bądź usługi subskrypcji):
   a. Urządzenie firewall musi pozwalać na przesyłanie do systemu Sandbox plików zdefiniowanych przez administratora – co najmniej exe, dll, java, MS Office,
   b. Urządzenie firewall musi być aktualizowane o nowo wykryte (w Sandbox zagrożenia),
   c. Administrator musi posiadać dostęp do raportów z Sandbox'a dotyczących plików wysłanych przez urządzenie firewall oraz posiadać możliwość manualnego wysłania pliku do Sandbox (np. poprzez upload poprzez stronę www),
   d. Dopuszcza się zaoferowanie lokalnego rozwiązania Sandbox (zapewnianego przez producenta firewall'i) – należy wówczas przewidzieć urządzenie pozwalające na jednoczesną analizę co najmniej 30 próbek/plików (VM Sandbox'ing),
   e. Dopuszcza się zaoferowanie chmurowego rozwiązania Sandbox (realizowanego przez producenta firewalli). W przypadku, jeżeli producent licencjonuje dostęp do chmurowego Sandbox'a należy przewidzieć licencję pozwalającą na jednoczesną analizę minimum 30 próbek/plików (VM Sandbox'ing),
   f. Wymagane jest by możliwa była analiza 30 próbek/plików jednocześnie bez względu na to czy pliki te wysłane będą automatycznie czy manualnie przez administratora czy też będzie to „mix" plików pochodzących zarówno bezpośrednio z firewall'a i od administratorów.
12) Podstawowa ochrona DNS co najmniej w zakresie:
   a. wykrywanie zapytań do domen złośliwych,
   b. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS Sinkholing).

13) Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
14) Zestawianie tuneli SSL VPN w konfiguracji Remote Access VPN.
    a. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW- obsługa co najmniej 12 000 tuneli/użytkowników,
    b. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows i MacOS,
    c. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewall'a.
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) Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
17) Obsługa 4094 VLAN zgodnych z 802.1q.
18) Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
19) Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
20) Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. 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.
21) Transparentne ustalenie tożsamości w oparciu o:
    a. integrację z kontrolerem domeny Active Directory,
    b. integrację z serwerami Microsoft Exchange,
    c. integrację z serwerami terminalowymi,
    d. integrację bazującą na informacji z logów SYSLOG pozwalającą na uwierzytelnienie użytkowników korzystających z systemów UNIX;
22) 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.
23) Uwierzytelnianie administratorów NGFW za pomocą:
    a. bazy lokalnej,
    b. zewnętrznej usługi katalogowej dostępnej po LDAPS,
    c. RADIUS lub TACACS+.
24) 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.
25) Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
26) Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).
~~27)~~ Integracja funkcji orkiestratora SSL/Decryption Brokera połączeń wychodzących w urządzeniu NGFW z zewnętrznymi narzędziami bezpieczeństwa – funkcjonalności deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS. Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do NGFW, w celu jego dalszego

przetwarzania. NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3.

28) Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają 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 (m.in. polityk, konfiguracji interfejsów, routingu itp.), z wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

III. WYMAGANIA LICENCYJNE

1) Całość rozwiązania będzie pochodziła od jednego producenta.
2) W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres co najmniej 44 miesięcy od daty odbioru bez zastrzeżeń potwierdzonego protokołem.
3) 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 podstawowej ochrony DNS,
    g. Możliwość realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN).

8. System Centralnego Zarządzania (SCZ) oferowanymi NGFW

Zamawiający posiada w swojej infrastrukturze urządzenie do Centralnego Zarządzania firewallami o nazwie PaloAlto Panorama, które zarządza posiadanymi urządzeniami PaloAlto 5250 oraz PaloAlto 5050. W ramach postępowania będą wymieniane dwa urządzenia PaloAlto 5050. Zamawiający wymaga, żeby oferowane urządzenia mogły być zarządzane przez posiadany system PaloAlto Panorama. Zamawiający dopuszcza wymianę systemu Centralnego Zarządzania na nowy spełniający poniższe wymagania:

1) SCZ – Wymagania funkcjonalne:
    a. Możliwość zarządzania posiadanymi przez Zamawiającego urządzeniami PA-5250.
    b. Pozwala na centralne monitorowanie funkcjonowania wszystkich oferowanych NGFW.
    c. Pozwala na zarządzanie
        i. nie mniej niż 20 firewallami rozumianymi jako firewalle fizyczne,
        ii. 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.
    d. Zarządza obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.

e. Dystrybucja i zdalna instalacja nowych sygnatur oraz wersji oprogramowania systemowego.
f. Przechowuje różne wersje konfiguracji zarządzanych NGFW.
g. Zbiera logi zdarzeń z oferowanych NGFW co najmniej o ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
h. Umożliwia korelację logów zdarzeń z zarządzanych firewalli.
i. Umożliwia tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych NGFW.
j. Pozwala na tworzenie raportów na podstawie gromadzonych w logach informacji.
k. Pozwala na tworzenie raportów na podstawie zbudowanych kontenerów/grup NGFW.
l. Pozwala na zapisywanie stworzonych raportów, uruchamianie ich w sposób manualny lub automatyczny w określonych przedziałach czasu oraz eksport do formatu tekstowego.
m. Graficzny interfejs SCZ (Web GUI) musi być dostępny z wykorzystaniem protokołu HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii Java czy Flash.
n. Umożliwia tworzenie i używanie ról administracyjnych różniących się poziomem dostępu.

2) SCZ – sposób realizacji:
   a. SCZ może być dostarczony jako maszyna wirtualna dla środowiska VMware ESXi.
   b. Zamawiający dedykuje dla celu instalacji systemu SCZ następujące zasoby:
      i. 16 vCPU,
      ii. 64 GB pamięci RAM,
      iii. 1TB przestrzeni dyskowej (bez uwzględnienia przestrzeni na logi)).
   c. W zakresie logów inspekcyjnych obsługuje co najmniej:
      i. 15 TB użytecznej przestrzeni dyskowej na logi inspekcyjne,
      ii. Pozwala na obsługę do 150GB logów inspekcyjnych dziennie,
      iii. 5000 logów na sekundę.
   d. W zakresie logów administracyjnych obsługuje co najmniej:
      i. 2 TB użytecznej przestrzeni dyskowej na logi administracyjne (management logs) z możliwością jej rozszerzenia do 5TB w ramach dostarczanej licencji,
      ii. Pozwala na obsługę do 2 GB logów administracyjnych (management logs) dziennie,
      iii. 50 logów na sekundę.
   e. SCZ może być zbudowany w oparciu o pojedynczą instancję zarządzającą lub w oparciu o dwie osobne maszyny wirtualne, współpracujące pomiędzy sobą, gdzie:
      i. Jedna maszyna jest dedykowana dla centralnego logowania zdarzeń i raportowania, obsługująca logi inspekcyjne,
      ii. Druga maszyna jest dedykowana dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne.
   f. W przypadku gdy SCZ będzie składał się z dwóch komponentów/maszyn muszą zostać spełnione następujące warunki:

i. Oba komponenty muszą pochodzić od jednego producenta i zarazem producenta oferowanego systemu firewall,
ii. Każdy z komponentów z osobna musi spełniać wymagania w zakresie:
    1. liczby zarządzanych firewall'i,
    2. liczby docelowo zarządzanych firewall'i.

g. W ofercie muszą zostać jednoznacznie wskazane (np. poprzez podanie kodu produktu) komponenty/produkty:
    i. Dedykowany dla centralnego logowania zdarzeń i raportowania, obsługujący logi inspekcyjne,
    ii. Dedykowany dla zarządzania urządzeniami, kontami administratorów i obsługujący logi administracyjne.
h. W ofercie musi zostać wykazane spełnienie wymagań dla każdej z maszyn składowych tworzących SCZ jak określono powyżej. Nie dopuszcza się, aby spełnienie wymagań odbywało się przez współdzielenie zasobów przez poszczególne maszyny (awaria pojedynczej maszyny nie może wpływać na drugą). Dlatego też wymagane jest spełnienie wymagań obu maszyn niezależnie. Do oferty należy dołączyć dodatkową dokumentację potwierdzającą spełnienie wymagań dla:
    i. Maszyny, która jest dedykowana dla centralnego logowania zdarzeń i raportowania (obsługująca logi inspekcyjne) – musi spełnić wymagania opisane w p 8.2).c.
    ii. Maszyny, która jest dedykowana dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne – musi spełnić wymagania opisane w p. 8.2).d.
i. SCZ może być alternatywnie dostarczony w postaci sprzętowej – w postaci dedykowanych urządzeń. W przypadku, jeżeli system SCZ będzie oferowany w postaci sprzętowej muszą zostać spełnione następujące warunki:
    i. System musi być dostarczony w postaci dedykowanych urządzeń – jako dedykowane rozwiązanie (urządzenie z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta).
    ii. Każdy z komponentów systemu musi posiadać minimum 2 interfejsy 10GE;
    iii. Użyteczna przestrzeń dyskowa zapewniana przez sprzętowy SCZ musi zostać zrealizowana w RAID-1;
    iv. W przypadku gdy SCZ będzie składał się z dwóch komponentów oba te komponenty muszą zostać dostarczone w postaci sprzętowej.

9. UJEDNOLICONA INTERPRETACJA PARAMETRÓW URZĄDZEŃ NGFW

1) Interpretacja parametrów wydajnościowych dla Firewall / kontroli aplikacji – rozwiązanie pozwala na:
    a. wykrycie aplikacji,
    b. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
2) Interpretacja parametrów wydajnościowych dla Firewall / kontroli aplikacji / IPS / Antywirus / Antymalware – rozwiązanie pozwala 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 Sandbox'a lokalnego i/lub chmurowego,
g. 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.

3) Charakterystyka ruchu sieciowego dla interpretacji parametrów wydajnościowych.

Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na oferowanym firewall'u zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako Enterprise Mix / Enterprise Testing Conditions / appmix lub dla równoważnego modelu ruchu.
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	*25%*
HTTPS	*60%*
SMTP, IMAP, POP3, FTP, SMB i inne	*12%*
DNS	*3%*

W przypadku gdy Wykonawca zaproponuje urządzenie, którego wydajność będzie oparta o model ruchu przedstawiony powyżej wówczas jest on zobowiązany do dodatkowego potwierdzenia spełnienia wymagań wydajnościowych. Zamawiający wymaga, aby potwierdzenie zostało dostarczone w postaci wyników testów przeprowadzonych przez publiczny ośrodek badawczo-rozwojowy w Polsce z wykorzystaniem dedykowanych testerów ruchu – IXIA lub Spirent lub Agilent.

4) Zamawiający wymaga, aby oferowane Urządzenia mogły być zarządzane przez posiadany system PaloAlto Panorama.

10. WSPARCIE TECHNICZNE i GWARANCJA

1) Wykonawca zobowiązuje się świadczyć usługi serwisu gwarancyjnego w miejscu użytkowania Urządzeń, z możliwością naprawy w serwisie Wykonawcy, jeżeli naprawa Urządzeń w miejscu użytkowania okaże się niemożliwa. W przypadku braku możliwości dokonania naprawy w miejscu użytkowania Urządzeń i konieczności ich dostarczenia do punktu serwisowego wskazanego przez Wykonawcę, koszty dostarczenia uszkodzonych Urządzeń do punktu serwisowego oraz z punktu serwisowego do miejsca użytkowania pokrywa Wykonawca.
2) Wykonawca zobowiązuje się do ponoszenia wszelkich kosztów naprawy Urządzeń, w tym kosztów części zamiennych i podzespołów, transportu, instalacji, konfiguracji i uruchomienia Urządzeń.
3) Wykonawca zobowiązuje się do świadczenia usług serwisu gwarancyjnego z należytą starannością z uwzględnieniem ogólnie przyjętych i stosowanych standardów i procedur przy tego rodzaju usługach, a także zaleceń lub procedur określonych przez producentów Urządzeń.
4) Nośniki informacji takie jak np. dyski twarde, pamięci flash, mogą być naprawiane jedynie w miejscu ich użytkowania, a w przypadku konieczności wymiany uszkodzonych nośników na nowe, wolne od wad, nośniki informacji pozostają u Zamawiającego. W przypadku konieczności dokonania naprawy Urządzeń wyposażonego w nośniki informacji poza miejscem użytkowania, nośniki te pozostają w siedzibie Zamawiającego.
5) Wykonawca zobowiązany jest, najpóźniej w dniu dostawy Urządzeń do dostarczenia Zamawiającemu niezbędnych danych do autoryzacji na stronie www producenta w celu pobierania nowych wersji oprogramowania sprzętu, poprawek, korzystania z bazy wiedzy, instrukcji obsługi itp.
6) Wykonawca zobowiązuje się przyjmować zgłoszenia serwisowe poprzez stronę www Wykonawcy dostępną przez całą dobę, 365 dni w roku. Wykonawca, najpóźniej w dniu dostawy Urządzeń dostarczy dane niezbędne do autoryzacji na stronie www Wykonawcy w celu dokonywania zgłoszeń serwisowych przez Zamawiającego. Zamawiający wymaga również zapewnienia możliwości dokonywania zgłoszeń serwisowych poprzez e-mail na adres .....@..... w przypadku braku możliwości dokonania zgłoszenia serwisowego przez stronę www (np. w przypadku braku dostępności dedykowanej strony www). Wzór formularza zgłoszenia serwisowego będzie stanowił załącznik do Umowy. Wykonawca potwierdzi otrzymanie zgłoszenia serwisowego poprzez wysłanie wiadomości e-mail na adres .....@..... Wszelkie wykonane przez Wykonawcę lub jego przedstawicieli czynności serwisowe wymagają dokumentowania w formie pisemnej.
7) W przypadku, jeżeli naprawa wymaga wymiany Urządzenia Zamawiający wymaga, aby Wykonawca każdorazowo w takiej sytuacji przedstawił informacje w tym zakresie przedstawicielowi Zamawiającego do akceptacji. Zamawiający zobowiązany jest do udzielenia odpowiedzi w terminie nie dłuższym niż 30 minut. Brak odpowiedzi w wyżej wymienionym terminie oznacza akceptację.
8) Wykonawca zobowiązuje się, że nie będzie dokonywał żadnych modyfikacji Urządzeń bez wcześniejszego uzgodnienia ich z Zamawiającym. Zamawiający zobowiązany jest do udzielenia odpowiedzi w terminie nie dłuższym niż 30 minut. Brak odpowiedzi w wyżej wymienionym terminie oznacza akceptację. Zamawiający zastrzega sobie prawo do samodzielnej rozbudowy Urządzeń i dokonywania zmian w konfiguracji.
9) Wykonawca zobowiązany jest do świadczenia serwisu gwarancyjnego na każde zgłoszenie serwisowe Zamawiającego.
10) Czas usunięcia awarii lub usterki liczony jest w godzinach od momentu wysłania przez Zamawiającego do Wykonawcy formularza „zgłoszenia serwisowego”.

11) Wykonawca podejmie działania serwisowe w trybie 24x7x365 – zgłoszenie awarii lub usterki przez wszystkie dni tygodnia, 365 dni w roku, naprawa urządzeń (z wyłączeniem awarii oprogramowania) w ciągu 4 godzin od przesłania zgłoszenia przez Zamawiającego w przypadku awarii oraz naprawa urządzeń (z wyłączeniem usterek oprogramowania) w ciągu 8 godzin od przesłania zgłoszenia przez Zamawiającego w przypadku usterki. Przez **awarię** należy rozumieć stan niesprawności sprzętu uniemożliwiający jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie. Przez **usterkę** należy rozumieć stan, w którym następuje obniżenie sprawności urządzenia jednak nie wpływającą na jego funkcjonowanie (np. awaria jednego z dwóch redundantnych zasilaczy).
12) Zamawiający dopuszcza możliwość usunięcia awarii lub usterki poprzez dostarczenie i uruchomienie sprzętu zastępczego z zachowaniem terminów określonych w ust. 11. Wykonawca zobowiązany jest do dostarczenia w tym terminie Zamawiającemu kompatybilnego Urządzenia zastępczego, wolnego od wad, o parametrach wydajnościowych i funkcjonalnych nie gorszych niż Urządzenie podlegające naprawie. Wykonawca zobowiązuje się jednocześnie do naprawy uszkodzonego Urządzenia i jego konfiguracji, instalacji i uruchomienia (zamiast sprzętu zastępczego) w terminie nie dłuższym niż 30 dni od przesłania zgłoszenia serwisowego.
13) Wykonawca zobowiązany jest w dniu wykonania naprawy do potwierdzenia wykonania naprawy w protokole „zgłoszenia serwisowego", wskazując datę i godzinę naprawy. Data i godzina wykonania naprawy zostanie potwierdzona przez przedstawiciela Zamawiającego. Ww. dokument musi zostać podpisany (data, godzina) przez przedstawiciela Zamawiającego.
14) W przypadku wystąpienia awarii tego samego elementu po wykonaniu 3 napraw w okresie obowiązywania Umowy, Wykonawca zobowiązuje się na pisemne wezwanie Zamawiającego do wymiany tego elementu na fabrycznie nowy, nieużywany i wolny od wad, na sprawny, tego samego producenta i tego samego typu o parametrach wydajnościowych i funkcjonalnych nie gorszych niż element wymieniany w terminie 30 dni od dnia otrzymania wezwania do wymiany. Nowe elementy muszą być wyprodukowane nie wcześniej niż sześć miesięcy przed planowanym terminem składania ofert.
15) W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z ust. 11 Zamawiający na koszt Wykonawcy ma prawo wypożyczyć od dowolnego Wykonawcy Urządzenie zastępcze o nie gorszych parametrach od Urządzenia, które uległo awarii, zachowując jednocześnie prawo do naliczenia kary umownej i odszkodowania. Jednocześnie Zamawiający ma prawo zlecić dowolnej firmie naprawę uszkodzonego Urządzenia, a kosztami naprawy obciążyć Wykonawcę, zachowując jednocześnie prawo do naliczenia kary umownej i odszkodowania, nie tracąc gwarancji.
16) W przypadku dokonania naprawy przez Wykonawcę poprzez wymianę elementów, zostaną zainstalowane fabrycznie nowe elementy o parametrach wydajnościowych i funkcjonalnych nie gorszych niż elementy wymieniane. Wykonawca udzieli gwarancji na prawidłowe działanie wymienionych Urządzeń na okres 44 miesięcy od ich wymiany.
17) Po usunięciu awarii lub usterki, dostarczeniu Urządzenia zastępczego lub wymianie na Urządzenie nowe, wolne od wad, obowiązkiem Wykonawcy będzie również uruchomienie i odtworzenie konfiguracji Urządzenia wraz z oprogramowaniem w miejscu użytkowania. Odtworzenie konfiguracji jest zależne od dostarczenia przez Zamawiającego kopi konfiguracji. Przekazanie kopi konfiguracji Urządzenia do Wykonawcy nastąpi w terminie 1 dnia roboczego.

18) Strony zobowiązują się do wzajemnego przekazywania sobie niezwłocznie wszelkich informacji mogących mieć wpływ na realizację zamówienia. Wykonawca niezwłocznie udzieli odpowiedzi w formie pisemnej na zgłaszane przez Zamawiającego uwagi dotyczące realizacji zamówienia, w terminie nie dłuższym niż 2 dni robocze.
19) Osoby wskazane przez Wykonawcę do realizacji Umowy zobowiązane są do przestrzegania postanowień regulaminów wewnętrznych i stosowania odpowiednich procedur obowiązujących w Ministerstwie Sprawiedliwości. Osoby skierowane przez Wykonawcę do realizacji Umowy zobowiązane są do zapoznania się i stosowania się do zapisów polityki bezpieczeństwa Ministerstwa Sprawiedliwości. Powyższe zostanie potwierdzone pisemnym oświadczeniem każdej z osób wyznaczonych do realizacji Umowy.
20) Wykonawca zobowiązany jest do dostarczenia wszelkich części zamiennych, podzespołów i materiałów, które są niezbędne do utrzymania Urządzeń sieciowych i oprogramowania Urządzeń sieciowych objętych umową w należytym stanie technicznym. Części zamienne, podzespoły i materiały muszą być fabrycznie nowe, nieużywane i wolne od wad.
21) Wykonawca zobowiązany jest do zapewnienia niezbędnych części, podzespołów i materiałów w ramach wynagrodzenia za wykonanie przedmiotu umowy.
22) W ramach serwisu gwarancyjnego Wykonawca wykona aktualizację oprogramowania Urządzeń objętych serwisem gwarancyjnym, nie rzadziej niż raz na 180 dni za pomocą aktualnych narzędzi aktualizujących do wersji uzgodnionej z Zamawiającym.
23) Harmonogram wykonania wszystkich aktualizacji oprogramowania Urządzeń objętych serwisem gwarancyjnym zostanie uzgodniony z Zamawiającym w terminie do 30 dni przed przystąpieniem do ww. prac.
24) Przed przystąpieniem do prac związanych z aktualizacją oprogramowania Urządzeń Wykonawca przeprowadzi analizę wpływu dokonywanej aktualizacji na sprzęt podłączony do innego sprzętu i pozostałych urządzeń podłączonych do sprzętu.
25) W przypadku wystąpienia problemów, z Urządzeniami (lub wersją oprogramowania) objętymi serwisem gwarancyjnym, wynikającymi z przeprowadzonej aktualizacji oprogramowania Urządzeń (lub brakiem komunikacji sieciowej z/do Urządzeń podłączonych do sprzętu sieciowego), Wykonawca niezwłocznie wykona powrót do poprzednich wersji i na własny koszt zapewni rozwiązanie problemów z Urządzeniami, których prawidłową prace zakłóciły działania prowadzone przez Wykonawcę.
26) Wykonawca:
    a. przeprowadzi, nie rzadziej niż jeden raz na 180 dni analizę w zakresie uaktualnień poziomu oprogramowania Urządzeń, poziomu firmware'u (mikrokodów),
    b. przeprowadzi na żądanie Zamawiającego, nie częściej niż jeden raz na 60 dni aktualizację poziomu oprogramowania Urządzeń wynikającą z wykrytych podatności bezpieczeństwa,
    c. przedstawi Zamawiającemu raport po wykonanej obsłudze serwisowej,
    d. opracuje harmonogram prac optymalizacji instalacji uaktualnień,
    e. zweryfikuje poprawność działania Urządzeń i oprogramowania Urządzeń po wykonaniu obsługi serwisowej.
27) Wykonawca zobowiązany jest do zapewnienia dla Zamawiającego dostępu do dedykowanego portalu www producenta dla urządzeń, na którym będzie możliwe co najmniej pobieranie i instalacji nowych wersji dedykowanego dla danego Urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do baz wiedzy,

przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp.

28) Zamawiający wymaga zapewnienia dostępu do pomocy technicznej Wykonawcy i producenta oraz do zasobów pobierania oprogramowania do Urządzeń objętych serwisem gwarancyjnym. Wykonawca musi zapewnić dostęp Zamawiającemu do najnowszego oprogramowania do Urządzenia objętego serwisem gwarancyjnym. Wykonawca jest zobligowany do instalowania najnowszego oprogramowania na Urządzeniu oraz zapewnienia ciągłości działania Urządzenia.

11. ASYSTA TECHNICZNA

1) Wykonawca zapewni świadczenie asysty technicznej inżyniera (asysty technicznej), zgodnie z potrzebami Zamawiającego, jednego inżyniera, który będzie posiadał certyfikat na poziomie F5-CSE Security, PaloAlto PCNSE, CISCO CCIE – Sec, CISCO CCIE – Routing and Switching, Juniper JNCIP-ENT, Juniper JNCIP – SEC, HPE MASE lub równoważne. Osoby skierowane do realizacji zamówienia muszą posiadać aktualne certyfikaty w całym okresie obowiązywania Umowy. Usługi asysty technicznej inżyniera będą świadczone w wymiarze do 1000 roboczogodzin (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia, ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny). Usługa będzie świadczona dla infrastruktury Zamawiającego (Urządzeń i oprogramowania). Równoważność certyfikatów została opisana w SWZ.
2) Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym serwisem gwarancyjnym. W przypadku, gdy Zamawiający zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu gwarancyjnego, Wykonawca ma obowiązek poinformowania o tym fakcie Zamawiającego.
3) Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności rozwoju i modyfikacji Urządzeń, zaawansowanej konfiguracji Urządzeń, wsparciu w zakresie utrzymania Urządzeń.
4) Zamawiający będzie przekazywać Wykonawcy zlecenia w ramach asysty technicznej, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
5) Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia wraz z rozbiciem na poszczególne czynności.
6) 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.
7) W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, termin wykonania prac.
8) Rozliczenie wsparcia technicznego inżyniera odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Wykonawcę i Zamawiającego, Miesięcznych Protokołów odbioru usługi raz na miesiąc.
9) Zamawiający wymaga, aby inżynier na wezwanie Zamawiającego przybył do wskazanego miejsca/siedziby na terenie Warszawy i tam realizował zgłoszenie. Zamawiający nie dopuszcza zdalnej realizacji zgłoszenia w tym zakresie.

12. PROJEKT TECHNICZNY I DOKUMENTACJA POWDROŻENIOWA

1) Wykonawca opracuje projekt techniczny oraz dokumentację powdrożeniową w tym co najmniej:
    a. Dla projektu technicznego:
        i. diagramy połączeniowe dla wszystkich komponentów sieci zamawiającego powiązanych z dostarczonymi 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 powdrożeniowej:
        i. diagramy połączeń;
        ii. opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu;
        iii. pełne konfiguracje urządzeń;
        iv. wyniki testów redundancji.
2) Projekt techniczny i dokumentacja powdrożeniowa zostaną dostarczone na co najmniej dwóch nośnikach PenDrive w formacie .pdf oraz .docx.

13. WDROŻENIE

1) Wykonawca wykona wdrożenie dostarczonych Urządzeń w następującym zakresie:
    - Dostarczenie Urządzeń do serwerowni
    - Montaż Urządzeń, w tym montaż kabli LAN oraz kabli zasilających.
    - Podłączenie Urządzeń do sieci zasilającej.
    - Wykonanie projektu technicznego.
    - Migracja konfiguracji z urządzeń posiadanych przez Zamawiającego.
2) Wykonawca dostarczy wszystkie niezbędne kable, wkładki światłowodowe zarówno do oferowanych urządzeń jak również do przełączników posiadanych przez Zamawiającego (min. 40 GB) do prawidłowego uruchomienia sprzętu zgodnie z przyjętym i zaakceptowanym projektem wdrożeniowym. Wkładki muszą pochodzić od producenta Urządzeń.
3) Wykonawca dostarczy z oferowanymi Urządzeniami min.:
    a. 24 szt. wkładek 40G/100G QSFP+/QSFP28;
    b. 16 szt. wkładek 25G SFP28;
    c. 24 szt. wkładek 40G/100G QSFP+/QSFP28 do posiadanych przez Zamawiającego przełączników CISCO Nexus 9508;
    d. 16 szt. wkładek 25G SFP28 QSFP28 do posiadanych przez Zamawiającego przełączników CISCO Nexus 9508;

Uwaga!!!
Przerwa techniczna umożliwiająca uruchomienie produkcyjne Urządzeń z migrowaną konfiguracją nie może być dłuższa niż 60 min. W przypadku gdy uruchomienie produkcyjne nowych Urządzeń spowoduje dłuższą przerwę techniczną niż 60 min Wykonawca dokona powrotu do pierwotnej konfiguracji.

14. WARSZTATY POWDROŻENIOWE

1) Warsztat 1 – Minimalny czas trwania – 5 dni. Warsztat dla 4 osób (w turach po 2 osoby). Warsztat musi dotyczyć urządzeń zaoferowanych w przedmiotowym postępowaniu, w tym:
    a. Architektura rozwiązania Next Generation Firewall;
    b. Instalacje wirtualne oraz ochrona chmury;
    c. Konfiguracja podstawowa urządzenia;
    d. Konfiguracja interfejsów sieciowych;
    e. Polityki bezpieczeństwa oraz translacja adresów;
    f. Identyfikacja aplikacji, wyjaśnienie działania AppID;
    g. Podstawy ochrony Contend-ID (Mechanizm IPS, AV, Anty-Spyware);
    h. Kategoryzacja stron Internetowych URL filtering;
    i. Deszyfracja ruchu szyfrowanego SSL;
    j. Ochrona IPD/IDS;
    k. User-ID – identyfikacja użytkowników w sieci;
    l. Dostęp zdalny;
    m. Konfiguracja tuneli Site to Site;
    n. Monitorowanie urządzenia oraz tworzenie raportów;
    o. Konfiguracja klastra niezawodnościowego Active/Passive;
    p. Najlepsze praktyki konfiguracyjne.

2) Warsztat 2 – Minimalny czas trwania – 3 dni. Warsztat dla 4 osób (w turach po 2 osoby). Warsztat musi dotyczyć urządzeń zaoferowanych w przedmiotowym postępowaniu, w tym:
    a. Narzędzia i zasoby;
    b. CLI;
    c. Logika przekazywania pakietów;
    d. Tworzenie zrzutów ruchu;
    e. Logi diagnostyczne pakietów;
    f. Ruch hostowany na firewallu;
    g. Ruch tranzytowy;
    h. Usługi systemowe;
    i. Deszyfracja SSL;
    j. User-ID;
    k. Dostęp zdalny Client to Site;
    l. Eskalacje i RMA.

3) Warsztat 3 – Minimalny czas trwania – 2 dni. Warsztat dla 4 osób (w turach po 2 osoby) – warsztat musi dotyczyć Systemu Centralnego Zarządzania (SCZ) zaoferowanego w przedmiotowym postępowaniu lub posiadanego przez Zamawiającego systemu Panorama, w tym:
    a. Wstęp do systemu zarzadzania, logowania i raportowania;
    b. Wstępna konfiguracja;
    c. Dodawanie urządzeń firewall do systemu zarzadzania, logowania i raportowania;
    d. Wysoka dostępność systemu zarzadzania, logowania i raportowania (HA);
    e. Szablony;
    f. Grupy urządzeń;

g. Konta administratorów;
h. Przekazywanie i zbieranie logów;
i. Zagregowane monitorowanie i raportowanie;
j. Troubleshooting.

4) Wykonawca zobowiązany jest do przeprowadzenia warsztatów w ośrodku szkoleniowym na terenie Warszawy. Za zgodą Zamawiającego, szkolenia mogą zostać przeprowadzone na odległość, w trybie zdalnym uzgodnionym roboczo przez Strony.
5) Każdy uczestnik otrzyma certyfikat jego ukończenia.
6) Warsztaty muszą być prowadzone w języku polskim.
7) Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie warsztatówa. Wymagane jest, aby trenerzy posiadali udokumentowane co najmniej 2 – letnie doświadczenie w przedmiocie szkolenia z zakresu oferowanego rozwiązania.
8) Wykonawca powinien dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazą 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.
9) Wykonawca w terminie do 30 dni, od dnia podpisania bez zastrzeżeń protokołu odbioru w zakresie dostawy systemu będącego przedmiotem niniejszego zamówienia, przedstawi Zamawiającemu do akceptacji Program warsztatów. Program powinien zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów.
10) Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy warsztatów – z rozpisaniem na dni i godziny i dostarczy je do 30 dni, od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.
11) Zajęcia powinny odbywać się w dni powszednie od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin zegarowych dziennie. Harmonogram i program powinny zostać wydrukowane i rozdane uczestnikom szkolenia na pierwszym spotkaniu.
12) Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika do danego rodzaju warsztatu, pozwalające na samodzielną edukację z zakresu tematyki warsztatów (opracowania, wydruku materiałów szkoleniowych).
13) Komplet materiałów szkoleniowych dla każdego uczestnika warsztatu obejmuje:
    a. papierową wersję materiałów szkoleniowych. 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 szkolenia.
14) Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć.
15) Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.

16) Wykonawca zapewni: na potrzeby wyżywienia uczestników szkoleń odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca szkolenia; obiady powinny być zróżnicowane, dany zestaw obiadowy nie powinien powtarzać się częściej niż raz na 3 dni szkoleniowe; Wykonawca zapewni 2 przerwy kawowe podczas jednego dnia szkoleniowego.
    a. W zakresie wyżywienia uczestników szkoleń Wykonawca zapewni:
        i. obiad dwudaniowy dla wszystkich uczestników szkolenia – (z opcją wegetariańską) obejmujące: 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:
            1. zupa – co najmniej 0,25 l na uczestnika szkolenia,
            2. danie gorące (mięsne lub rybne, opcja wegetariańska – warzywne) – co najmniej 150 g na uczestnika szkolenia,
            3. zestaw surówek/sałatek – co najmniej 150 g na uczestnika szkolenia,
            4. dodatki skrobiowe – porcja ziemniaków lub frytek / makaronu / ryżu / kaszy – co najmniej 200 g na uczestnika szkolenia,
            5. kawa, herbata, woda mineralna gazowana i niegazowana – co najmniej 0,5 l na uczestnika szkolenia.
        iii. Przerwa kawowa dla wszystkich uczestników szkolenia podczas jego trwania:
            1. serwis będzie dostępny przy sali szkoleniowej;
            2. naczynia, w których serwowany jest serwis kawowy powinny być szklane lub ceramiczne;
            3. Serwis kawowy dla każdego uczestnika szkolenia obejmuje:
            4. butelkowaną wodę mineralną gazowaną i niegazowaną (0,5 l);
            5. świeżo parzoną, gorącą kawę z ekspresu lub zaparzacza oraz kawę sypaną i rozpuszczalną;
            6. herbatę – co najmniej 3 rodzaje herbat w torebkach;
            7. dodatki – cukier, mleko do kawy, cytrynę;
            8. dodatki – np. ciastka / wafelki i inne słodycze 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 szkolenia.

17) Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.
18) Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru szkolenia wraz z dołączonymi załącznikami, tj. oryginalną listą obecności, harmonogramem i programem warsztatu oraz ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.