OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa urządzeń brzegowych UTM wraz z migracją konfiguracji, uruchomieniem oraz wsparciem technicznym.

Rozdział I. OGÓLNE WARUNKI REALIZACJI ZAMÓWIENIA

1. PRZEDMIOT ZAMÓWIENIA:

1) Dostawa i instalacja 2 szt. urządzeń zabezpieczeń firewall zgodnie ze specyfikacją techniczną opisaną w Rozdziale II pkt 1
2) Przeprowadzenie warsztatów szkoleniowych. Wymagania dotyczące warsztatów opisane są w Rozdziale III w punktach od 18 do 33.
3) Asysta techniczna eksperta w ilości 1000 roboczogodzin. Wymagania do asysty uszczegółowione są w Rozdziale III w punktach od 7 do 15.
4) Uruchomienie urządzeń wraz z migracją konfiguracji.

2. TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA:

1) w zakresie wymienionym w pkt 1 ppkt 1) - w terminie do 90 dni od dnia zawarcia umowy;
2) w zakresie wymienionym w pkt 1 ppkt 2) – w okresie 24 miesięcy od podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji - **Załącznik nr 8** do Umowy.
3) w zakresie wymienionym w pkt 1 ppkt 3) - przez okres 48 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Odbioru Jakościowego Urządzeń i Licencji – **Załącznik nr 6** do Umowy, albo do wyczerpania puli roboczogodzin, w zależności które zdarzenie nastąpi wcześniej.
4) Uruchomienie urządzeń wraz z migracją konfiguracji 60 dni 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.
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) Zamawiający zastrzega sobie prawo do zmiany miejsca umieszczenia urządzeń będącego przedmiotem zamówienia – bez utraty prawa do gwarancji.
4) Zamawiający wymaga realizacji zgłoszeń w miejscu określonym w ppkt. 1.
5) Zamawiający nie dopuszcza napraw sprzętowych poza miejscem realizacji przedmiotu zamówienia.
6) Komunikacja oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.

4. GWARANCJA

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 zawierającej 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 dla urządzeń i oprogramowania bez ponoszenia dodatkowych kosztów.

   Wykonawca zobowiązuje się wdrożyć i stosować przez cały okres obowiązywania Umowy powyższe 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 uwzględnienia i przedstawienia do ponownej akceptacji przez Zamawiającego.
2) W przypadku jakichkolwiek zmian danych, o których mowa jest powyżej, w tym o których mowa w pkt 1 lit. c), Wykonawca niezwłocznie poinformuje o tym Zamawiającego pisemnie. Instrukcje, 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 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:
   - awaria krytyczna, tj. całkowita niedostępność urządzenia: czas reakcji do 1 godziny od chwili zgłoszenia awarii przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do ……. godzin (zgodnie z ofertą Wykonawcy, 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;
   - awaria niekrytyczna (niepowodująca całkowitej niedostępności urządzenia): czas reakcji do 1 godziny od chwili zgłoszenia usterki przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności) do godzin…….(zgodnie z ofertą Wykonawcy, nie mniej niż 8 godzin i więcej niż 16 godzin) 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:

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 urządzenia, 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 zapewnił urządzenie zastępcze, a naprawa urządzenia Zamawiającego trwa dłużej niż 6 tygodni lub gdy ten sam element/podzespół/cześć urządzenia będzie podlegać naprawie trzykrotnie w okresie obowiązywania umowy i nastąpi kolejna (czwarta) awaria, Zamawiający ma prawo żądać wymiany urządzenia 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 dostawą, wolne od wad, fabrycznie nowe - bez śladów używania 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 urządzenia dostarczonego w ramach wymiany. Z chwilą podpisania protokołu na Zamawiającego przechodzi prawo własności nowego urządzenia.
11) Wykonawca każdorazowo w terminie 7 od usunięcia awarii dostarczy Zamawiającemu raport z naprawy urządzenia, zawierający datę i godzinę zgłoszenia, informację co było przedmiotem naprawy oraz w przypadku przekroczenia czasu usunięcia awarii, o którym mowa w ppkt 7, wskazanie z naprawy czasu przekroczenia 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 otrzymania raportu dokonuje jego akceptacji lub zgłasza do niego uwagi, przesyłając je na adres poczty elektronicznej Wykonawcy. Wykonawca zobowiązany jest w terminie 2 dni roboczych od dnia otrzymania uwag do ich uwzględniania 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 to w przypadku awarii dysku twardego, powodującej konieczność jego wymiany, uszkodzony dysk pozostanie u Zamawiającego. Koszty dysków twardych 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 zapewnił:
    a) dostęp do portali internetowych zawierających narzędzia wsparcia elektronicznego urządzeń i systemu stanowiącego przedmiot umowy oraz zapewni 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) W okresie trwania umowy Zamawiający ma prawo do instalowania, wymiany standardowych kart rozszerzeń/modułów (np. modułów optycznych itp.) oraz rozbudowy urządzeń oraz instalacji pobranych poprawek, aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego posiadanych urządzeń (firmware) zgodnie z zasadami wiedzy technicznej przez Zamawiającego lub podmiotu zewnętrznego, któremu zleci te prace Zamawiający.
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 systemów zabezpieczeń firewall. Dokładny opis wymagań dla pojedynczego systemu znajduje się poniżej:**
    a) System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez tego samego producenta.
    b) System zabezpieczeń firewall 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 32 000 000 jednoczesnych połączeń. Testy wydajności powinny być opublikowane na stronie producenta w dniu składania ofert. Nie dopuszcza się wykonywania testów dedykowanych dla przedmiotowego postepowania przetargowego.
    c) System zabezpieczeń firewall musi być wyposażony 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 postępowania należy dostarczyć:
        a. 4 szt. wkładek SFP+ 10GB SR. Wkładki muszą pochodzić od producenta urządzenia.
        b. 2 szt. wkładek światłowodowych 40GBase-SR4 QSFP+ do urządzenia. Wkładki muszą pochodzić od producenta urządzenia.
        c. 2 szt. wkładek światłowodowych 40GBase-SR4 QSFP+ do przełącznika CISCO Nexus 9508, wkładki muszą poprawnie współpracować z wkładkami wyspecyfikowanymi w punkcie powyżej.
        d. 2 szt. Wkładek światłowodowych 100GBase-SR4 QSFP28. Wkładki muszą pochodzić od producenta urządzenia.
        e. 2 szt. Wkładek światłowodowych 100GBase-SR4 QSFP28 do przełącznika CISCO Nexus 9508, wkładki muszą poprawnie współpracować z wkładkami wyspecyfikowanymi w punkcie powyżej.
        f. 4 szt. kabli typu patchcord MPO - MPO do wyspecyfikowanych wkładek 40G/100G SR4, OM4 o długości 10 m.
    e) Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie

transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.

f) Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall 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) System zabezpieczeń firewall 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) System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.
i) System zabezpieczeń firewall 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 postępowania na min. 5 wirtualnych routerów.**
j) Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPFv2 i v3.
k) System zabezpieczeń firewall 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) System zabezpieczeń firewall 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) System zabezpieczeń firewall 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. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 27 Gbit/s.
p) Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
q) Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
r) Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
s) System zabezpieczeń firewall 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) System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
u) System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
v) System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
w) System zabezpieczeń firewall 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.
x) System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.
y) System zabezpieczeń firewall 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 przedmiotowym postępowaniu.
z) System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. 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 przedmiotowym postępowaniu.
aa) System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
bb) System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
cc) System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
dd) Wymagania podstawowe identyfikacja użytkowników
ee) System zabezpieczeń firewall 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, ustalanie tożsamości musi odbywać się również transparentnie.
ff) System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
gg) System zabezpieczeń firewall 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 sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

hh) Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

ii) System zabezpieczeń firewall 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 postępowania.**

jj) System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.**

kk) System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.

ll) System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

mm) System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania 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 etapie postępowania. Licencja na cały okres wsparcia technicznego.**

nn) System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie postępowania. Licencja na cały okres wsparcia technicznego.**

oo) System zabezpieczeń firewall musi posiadać modułu 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 przechowywania 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 etapie postępowania**. **Licencja na cały okres wsparcia technicznego.**

pp) System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie postępowania. Licencja na cały okres wsparcia technicznego.**

qq) System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie postępowania. Licencja na cały okres wsparcia technicznego.**

rr) System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania 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 etapie postępowania. Licencja na cały okres wsparcia technicznego.**

ss) System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie postępowania. Licencja na cały okres wsparcia technicznego.**

tt) System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. **Jeżeli funkcjonalność wymaga dodatkowej licencji to jest ona wymagana na etapie postępowania. Licencja na cały okres wsparcia technicznego.**

uu) System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.**

vv) System zabezpieczeń firewall 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).

ww) System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

xx) System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

yy) System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany. Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.

zz) System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.**

aaa) System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) 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 postępowania.**

bbb) Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box". **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.**

ccc) Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box". **Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.**

ddd) System zabezpieczeń firewall 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 postępowania.**

eee) Wymagania dodatkowe: NAT, DoS, IPSEC VPN, SSL VPN, QoS

fff) System zabezpieczeń firewall 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.

ggg) System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
hhh) System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
iii) System zabezpieczeń firewall 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 rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
jjj) System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
kkk) System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci. Jeżeli funkcjonalność wymaga dodatkowej licencji to nie jest ona wymagana na etapie postępowania.
lll) System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.
mmm) System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
nnn) System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
ooo) System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
ppp) Wymagania dodatkowe środowisko wirtualne vmware
qqq) System zabezpieczeń firewall 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 korzystał 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 jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
rrr) Wymagania zarządzanie i raportowanie
sss) Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dopuszczalna jest, instalaca dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
ttt) System zabezpieczeń firewall 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.
uuu) System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
vvv) System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
www) System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
xxx) 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.
yyy) System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
zzz) System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
aaaa) System zabezpieczeń firewall musi posiadać wbudowane dwa twarde dyski do przechowywania logów i raportów o pojemności nie mniejszej niż 2 x 480 GB SSD (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
bbbb) System zabezpieczeń firewall musi posiadać pamięć RAM min. 128 GB.
cccc) System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
dddd) System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
eeee) System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
ffff) System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
gggg) System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
hhhh) System zabezpieczeń firewall musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
iiii) System zabezpieczeń firewall 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 i XML.
jjjj) System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
kkkk) System zabezpieczeń firewall 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 łączy sieciowych.
llll) System zabezpieczeń firewall musi posiadać przynajmniej dwa redundantne zasilacze.
mmmm) Wysokość urządzenia nie większa niż 2 RU
nnnn) W przypadku wyspecyfikowanych wymagań wymagających dostarczenia licencji lub zapewnienia udzielenia licencji, Wykonawca zobowiązany jest do ich dostarczenia na okres trwania całego okresu gwarancji tj. 48 miesięcy.
oooo) Dostarczone urządzenia muszą współpracować z oprogramowaniem posiadanym przez Zamawiającego Check Point Security Management. Wykonawca w ramach umowy odnowi wsparcie techniczne do posiadanej licencji oraz podniesie posiadaną wersje Check Point Security Management R80.10 do najnowszej wersji wspieranej przez producenta.

pppp) W ramach przeniesienia całej konfiguracji z posiadanych urządzeń Check Point 12600 R77.30, Wykonawca zmieni wykorzystywane interfejsy z 10G na 40G lub 100 GB w zależności pod zaproponowanego rozwiązania w projekcie technicznym.

Rozdział III. DODATKOWE WYMAGANIA

1. Oferowane produkty będą pochodziły z oficjalnego kanału dystrybucyjnego producenta na terenie Unii Europejskiej.
2. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień poprzedzający dzień składania ofert.
3. Wykonawca zapewni gwarancję dla wszystkich dostarczonych urządzeń i licencji na okres 48 miesięcy oraz świadczenie usługi wsparcia eksperckiego dla wszystkich dostarczonych urządzeń i licencji na okres 48 miesięcy lub do wyczerpania puli roboczogodzin.
4. Zamawiający wymaga posiadania pełnej kontroli nad zgłoszeniami serwisowymi. Zamawiający musi mieć możliwość monitorowania statusu zgłoszeń serwisowych w systemie Wykonawcy lub producenta
5. Zamawiający wymaga uzyskania, w ramach gwarancji, bezpośredniego dostępu do zasobów internetowych (bazy wiedzy) udostępnianych przez producenta.
6. Rozszerzenie licencji o kolejne funkcjonalności nie może powodować utraty praw gwarancyjnych do oprogramowania oraz nie może wymagać zgody Wykonawcy.
7. 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 godziny na podstawie miesięcznego Protokołu odbioru usług asysty technicznej eksperta – Załącznik nr 7 do Umowy. Do roboczogodzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych na warunkach gwarancji.
8. Asysta techniczna eksperta będzie dotyczyła urządzeń oraz systemu dostarczonych w ramach postępowania.
9. Asysta techniczna będzie realizowana przez eksperta posiadającego niezbędne doświadczenie oraz certyfikację. Minimalny, wymagany certyfikaty to: Check Point Certified Security Expert (CCSE) lub równoważny.
   Jako certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu wskazanego certyfikatu, co jest rozumiane jako:
   a) analogiczna dziedzina merytoryczna wynikająca z roli (wiedzy), której dotyczy certyfikat,
   b) analogiczny stopień poziomu kompetencji,
   c) analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu,
   d) potwierdzenie certyfikatu egzaminem, jeśli uzyskanie certyfikatu wymaga złożenia egzaminu.

   Certyfikat równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy.
10. Zamawiający będzie przekazywać Wykonawcy zlecenia, w których każdorazowo określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
11. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
12. 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.
13. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
14. Rozliczenie wsparcia technicznego eksperta odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Zamawiającego, Protokołów odbioru asysty technicznej eksperta.
15. W ramach roboczogodzin wsparcia ekspert na wezwanie Zamawiającego ma obowiązek przybyć do wskazanego miejsca/siedziby na terenie województwa mazowieckiego i tam realizować zgłoszenie.
16. W ramach roboczogodzin wsparcia eksperckiego – asysty technicznej, w okresie 60 dni od dnia popisania protokół odbioru ilościowego urządzeń i licencji, Wykonawca uruchomi i skonfiguruje urządzenia dostarczone w ramach Umowy oraz wykona migrację konfiguracji z obecnie używanych urządzeń na dostarczone zgodnie z Umową. Wszystkie prace musza odbywać się przy obecności Zamawiającego. Plany migracyjne oraz sposób migracji oraz konfiguracji musi być Zaakceptowany przez Zamawiającego przed przystąpieniem do robót przez Wykonawcę. Na wykonanie wszystkich prac Wykonawca nie zutylizuje więcej niż 100 roboczogodzin wsparcia eksperckiego – asysty technicznej.
17. Wykonawca wykona wdrożenie dostarczonych urządzeń w następującym zakresie:
    - Dostarczenie sprzętu do serwerowni
    - Montaż sprzętu, w tym montaż kabli LAN oraz kabli zasilających.
    - Podłączenie sprzętu do sieci zasilającej.
    - Wykonanie projektu technicznego.
    - Migracja konfiguracji z urządzeń posiadanych przez Zamawiającego.

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.

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

Warsztat 1 – Minimalny czas trwania - 3 dni. Warsztat dla 4 osób (w turach po 2 osoby). Warsztat musi dotyczyć urządzeń zaoferowanych w przedmiotowym postępowaniu.

- 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 osób (w turach po 2 osoby) - Warsztat musi dotyczyć urządzeń zaoferowanych w przedmiotowym postępowaniu.

- zawansowany firewall;
- zaawansowane możliwości systemu operacyjnego NGFW;
- automatyzacja i instrumentacja;
- klastry VRRP;
- optymalizacja i akceleracja;
- akceleracja wielokorowa;
- kolejkowanie 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, szkolenia 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 warsztatówi. Wymagane jest, aby trenerzy posiadali udokumentowane co najmniej 2- letnie doświadczenie w przedmiocie szkolenia z zakresu oferowanego rozwiązania.

e. 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.

f. 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.

g. 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 -**Załącznik nr 6** do Umowy. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.

h. 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.

i. 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).

j. 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.

k. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć.

l. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.

m. 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:

         - zupa – co najmniej 0,25 l na uczestnika szkolenia,
         - danie gorące (mięsne lub rybne, opcja wegetariańska - warzywne) – co najmniej 150 g na uczestnika szkolenia,
         - zestaw surówek/sałatek – co najmniej 150 g na uczestnika szkolenia,
         - dodatki skrobiowe - porcja ziemniaków lub frytek / makaronu / ryżu / kaszy – co najmniej 200 g na uczestnika szkolenia,
         - 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:

         - serwis będzie dostępny przy sali szkoleniowej;
         - naczynia, w których serwowany jest serwis kawowy powinny być szklane lub ceramiczne;
         - Serwis kawowy dla każdego uczestnika szkolenia 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 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.

n. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.

o. Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru szkolenia – Załącznik nr 8 do Umowy wraz z dołączonymi załącznikami, tj. oryginalną listą obecności, harmonogramem i programem warsztatu oraz ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.

19. Wykonawca opracuje projekt wdrożeniowy oraz dokumentację powykonawczą w tym co najmniej:

   a. Dla projektu wdrożeniowego:

      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 powykonawczej:
i. diagramy połączeń;
ii. opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu;
iii. pełne konfiguracje urządzeń;
iv. wyniki testów redundancji.