KOMENDA GŁÓWNA POLICJI
BIURO FINANSÓW
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH

ul. Domaniewska 36/38; 02-672 Warszawa; tel. 22 60 120 44; fax 22 60 118 57
zamowieniakgp@policja.gov.pl

L.dz. FZ...72.38./15

Warszawa, 29.... 09.2015 r.

Do uczestników postępowania
ubiegających się o udzielenie zamówienia

dot. Przebudowa Centralnego Węzła Internetowego Komendy Głównej Policji – nr sprawy 181/BŁiI/15/MT

Działając na podstawie art. 38 ust. 1, 2 i 4 ustawy Prawo zamówień publicznych (tj. Dz. U. z 2013 poz. 907 z późn. zm.) uprzejmie udzielam następujących wyjaśnień:

Pytanie nr 1

Dotyczy punktu 2. Zakup pamięci operacyjnej RAM HP 32GB (1x32GB) Quad Rank x4 PC3L-10600 (ZDDR3-1333) LRDIMM CAS-9 LP-szt.120

Wyżej opisana pamięć RAM nie jest kompatybilna z serwerami BL-490c G7 i HP Blade Server BL 4460c G7.

Czy zatem zamawiający dopuści pamięć (szt. 120) o parametrach HP 32GB (1x32GB) Quad Rank x4 PC3L-8500 (DDR3-1066) Registered CAS-7 LP, która jest oficjalnie wspierna z serwerami BL490c G7 i HP Blade Server BL 460c G7?

Odpowiedź:

W odpowiedzi na powyższe pytanie Zamawiający informuje, iż dopuszcza pamięć o parametrach HP 32GB (1x32GB) Quad Rank x4 PC3L-8500 (DDR3-1066) Registered CAS-7 LP.

W związku z powyższym Zamawiający dokonuje zmiany ilości zamawianych pamięci z 120 szt. na 96 szt.

Jednocześnie Zamawiający dokonuje zmiany sposobu odbioru szkoleń.

W załączeniu Załącznik nr 1 i 5 do SIWZ z uwzględnionymi zmianami.

Pozostałe zapisy nie ulegają zmianie.

Powyższe odpowiedzi i zmiany są wiążące dla stron postępowania.

ZASTĘPCA NACZELNIKA
WYDZIAŁU ZAMÓWIEŃ PUBLICZNYCH
BIURA FINANSÓW
KOMENDY GŁÓWNEJ POLICJI
Anna ŁUCHCIŃSKA

wykonano w 1 egz.:
przesłano faksem wg rozdzielnika
opr./wyk. M.Tobar
tel. 022 60 119-82

Załącznik nr 1 do SIWZ
nr sprawy 181/BŁiI/15/MT

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest:

„Przebudowa Centralnego Węzła Internetowego Komendy Głównej Policji", Etap III – Podniesienie poziomu bezpieczeństwa i dostępności usług:

1. **Zakup modułów SFP+:**

a. **moduł Intel 10GBASE-SR 10G Ethernet - szt. 2**
lub równoważny spełniający warunki:
- moduł posiada pełną kompatybilność i wsparcie dla karty sieciowej Intel Ethernet Converged Network Adapter X520-DA2

b. **moduł HP 10Gb SFP+ SR Transceiver - szt. 8**
lub równoważny spełniający warunki:
- moduł posiada pełną kompatybilność i wsparcie dla karty sieciowej HP NC552SFP 10GbE 2-port Ethernet Server

c. **moduł 10Gbps (XFP) Multimode SR - szt. 4**
lub równoważny spełniający warunki:
- moduł posiada pełną kompatybilność i wsparcie dla Check Point DDoS Protector 4412

d. **moduł 1G SFP SR – szt. 4**
lub równoważny spełniający warunki:
- moduł posiada pełną kompatybilność i wsparcie dla urządzenia Check Point DDoS Protector 4412

2. **Zakup pamięci operacyjnej RAM HP 32GB (1x32GB) Quad Rank x4 PC3L-8500 (DDR3-1066) Registered CAS-7 LP – szt. 96**
lub równoważny spełniający warunki:
- moduł posiada pełną kompatybilność i wsparcie dla urządzenia HP Blade Server BL 490c G7 i HP Blade Server BL 460c G7

3. **Zakup systemu zabezpieczającego środowisko VMware z usługą wsparcia technicznego na okres 12 miesięcy w ukompletowaniu:**
   - Deep Security – Intrusion Prevention & Firewall for Physical Server or VM – szt. 100
   - Deep Security – Compliance Pack for Pshysical or Virtual Desktop (VM) – per agent – szt. 10
   - Silver Premium Service Program – szt. 1

   lub równoważny spełniający warunki:

   a) System musi zapewniać bezpieczeństwo fizycznych i wirtualnych serwerów oraz stacji użytkowników końcowych,
   b) System musi umożliwiać instalację konsoli zarządzającej na systemach operacyjnych Microsoft Windows oraz RedHat Linux,
   c) System musi posiadać możliwość dopasowania się do nowej wersji kernela w czasie rzeczywistym lub poprzez uaktualnienie odpowiedniego agenta,
   d) System musi pozwalać na swobodny wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych, oraz zwirtualizowanych desktopów,
   e) Wszystkie funkcjonalności systemu w przypadku serwerów wirtualnych, oraz zwirtualizowanych desktopów muszą być zapewniane bezagentowo,
   f) System powinien zawierać zaawansowane funkcje zarzadzania, upraszczające zakres zadań ochrony,
   g) Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa,
   h) System musi mieć możliwość konfiguracji rozwiązania, które będzie dla wyznaczonych agentów punktem dystrybuującym uaktualnienia i poprawki oprogramowania,
   i) System musi umożliwiać zdefiniowanie harmonogramu lub częstotliwości pobierania aktualizacji baz zagrożeń i reguł od producenta systemu,
   j) System musi umożliwiać instalację i konfigurację lokalnego serwera skorelowanej reputacji plików, adresów e-mail oraz adresów URL, synchronizującego się z chmurą producenta, który pozwalał będzie na weryfikację reputacji plików i adresów URL bez konieczności łączenia się z Internetem,
   k) System musi posiadać możliwość pracy w trybie multi-tenancy, tj. Pozwalać na równoległe współistnienie wielu użytkowników posiadających dostęp do widoku jedynie wydzielonej części infrastruktury i zarządzania jej bezpieczeństwem. Użytkownicy powinni mieć możliwość jednoczesnej, bezkonfliktowej w stosunku do siebie pracy z systemem,
   l) System musi pozawalać na dostęp do API każdego „tenanta/użytkownika",
   m) System musi pozwalać na generowanie raportów z wykorzystania poszczególnych modułów przez „tenantów/użytkowników",
   n) System musi wykorzystywać VMware vShield API do zapewnienia bezpieczeństwa chronionych systemów,
   o) W obrębie jednej konsoli zarządzającej system musi pozwalać na kontrolę integralności hypervisora środowiska wirtualnego,

p) System musi wykorzystywać mechanizmy cache i deduplikacji w celu optymalizacji czasu skanowania i wykrywania zmian,
q) System musi pozwalać na zarządzanie zdarzeniami i natychmiastowe alarmowanie i raportowanie o aktywności wirusów w chronionej infrastrukturze na kilka sposobów,
r) System musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa,
s) System musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, itd.,
t) System musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów,
u) Rozwiązanie musi chronić systemy oparte na HP-UX. Ochrona ta powinna zawierać:
    a. Monitorowanie wybranych procesów
    b. Monitorowanie wybranych portów
    c. Zmiany w krytycznych oraz wskazanych przez administratora plikach i katalogach
    d. Analiza wskazanych przez administratora plików typu log,
v) Rozwiązanie musi chronić systemy oparte na Linux (RHEL,SuSE) w czasie rzeczywistym. Ochrona ta powinna zawierać:
    a. Ochronę przed złośliwym oprogramowaniem
    b. Monitorowanie wybranych procesów
    c. Monitorowanie wybranych portów
    d. Analiza ruchu wykorzystującego SSL
    e. Zmiany w krytycznych oraz wskazanych przez administratora plikach i katalogach,
w) Zarządzanie systemem musi odbywać się poprzez standardową przeglądarkę WWW i połączenie https, która nie wymaga instalacji żadnych dodatkowych komponentów,
x) System musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP lub wywołania komendy,
y) System musi umożliwiać tworzenie administratorów o różnych stopniach uprawnień w stosunku do różnych modułów i funkcjonalności systemu, a także w stosunku do różnych chronionych obiektów lub grup obiektów,
z) Zarządzanie rolami w systemie musi pozwalać zdefiniowanie uprawnień dających możliwość administrowania wyłącznie jednym chronionym obiektem oraz pojedynczymi funkcjonalnościami systemu bez możliwości zmiany nadrzędnego profilu bezpieczeństw,
aa) System musi pozwalać na tworzenie struktur zarządzanych komputerów również poprzez adresacje IP komputera który podlega zarządzaniu,
bb) System musi być przygotowany do pracy w strefie DMZ tak aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną,
cc) System musi prezentować dane w formie graficznej w panelu głównym,
dd) System musi pozwalać na rozbudowę o moduł zapewniający monitorowanie integralności chronionych systemów poprzez wykrywanie zmian w zdefiniowanych zasobach (wskazane katalogi i elementy rejestru systemu),
ee) System musi pozwalać na rozbudowę o moduł umożliwiający śledzenie i korelację zdarzeń występujących na chronionych obiektach ze zdefiniowanych dzienników lub plików typu log,
ff) System musi umożliwiać na jednoczesny dostęp do konsoli zarządzającej niezależnie przez kilku administratorów,

gg) System musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta,

hh) System nie może wymagać restartu chronionych komputerów i serwerów po dokonaniu aktualizacji mechanizmów skanujących i definicji reguł,

ii) System musi pozwalać na rozbudowę o moduł umożliwiający wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan",

jj) System musi pozwalać na automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa,

kk) System musi zapewniać w procesie skanowania ręcznego i automatycznego przeskanowania dowolnego celu pod względem złośliwego oprogramowania,

ll) System musi posiadać możliwość kontroli oraz blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną,

mm) Rozwiązanie powinno pozwalać na notyfikację (powiadomienie użytkownika) w przypadku skorzystania z niebezpiecznych zasobów lub pobrania niebezpiecznego pliku. Notyfikacja powinna dotyczyć pracy w trybie agentowym lub bezagentowym,

nn) System musi posiadać predefiniowaną bazę najpopularniejszych aplikacji oraz komunikatorów (włączając w to gadu-gadu),

oo) System musi posiadać możliwość heurystycznego wykrywania transmisji na podstawie częstotliwości jej występowania oraz zdefiniowanego zakresu portów,

pp) System musi posiadać możliwość wykrywania ataków typu SQL injection oraz cross-site-scripting wraz z możliwością ustanowienia progów alarmu jak dodawania i edytowania nowych ciągów danych,

qq) System musi posiadać możliwość przełączania pomiędzy trybem blokowania ruchu i trybem detekcji zdarzeń w sposób globalny dla wszystkich reguł,

rr) System musi posiadać moduł umożliwiający blokowanie transmisji na podstawie zdefiniowanej charakterystyki ruchu na podstawie sygnatury oraz zdefiniowanego ciągu znaków (patternu). Funkcjonalność ta powinna być dostarczana zarówno w ramach agenta zainstalowanego na chronionym obiekcie jak i bezagentowo w przypadku środowisk wirtualnych VMware,

ss) System musi pozwalać na sprawdzanie w czasie rzeczywistym poziomu bezpieczeństwa nieznanych aplikacji poprzez zapytania przesyłane poprzez siec do systemu serwerów producenta,

tt) System musi posiadać pełnostanowy firewall (stateful firewall) pozwalający na łatwą izolacje interfejsów i nie wymagający restartów systemu. Funkcjonalność ta powinna być dostarczana zarówno w ramach agenta zainstalowanego na chronionym obiekcie jak i bezagentowo w przypadku środowisk wirtualnych VMware,

uu) System musi pełni wspierać IPv6,

vv) System musi umożliwiać kontrolę połączeń wychodzących i przychodzących w komunikacji sieciowej z możliwością kontroli niestandardowych portów TCP (możliwość zdefiniowania na podstawie numeru protokołu oraz numeru typu ramki). Funkcjonalność ta powinna być dostarczana zarówno w ramach agenta zainstalowanego na chronionym obiekcie jak i bezagentowo w przypadku środowisk wirtualnych VMware,

ww) System musi posiadać możliwość przełączenia trybu działania reguł firewalla z trybu blokowania ruchu w tryb detekcji zdarzeń,

xx) System musi pozwalać na rozbudowę o moduł zapewniający możliwość skanowania i wykrywania zmian w strukturze chronionych obiektów, plików oraz wpisów w rejestrach,

yy) System musi posiadać możliwość skanowania i wykrywania zmian w strukturze chronionych obiektów,
zz) System musi pozwalać na rozbudowę o moduł umożliwiający analizowanie logów z programów zainstalowanych na chronionych systemach informatycznych,
aaa) Wszystkie funkcjonalności systemu muszą być zarządzane z jednej, centralnej konsoli,
bbb) System musi posiadać możliwość zdefiniowania własnych reguł wykrywających zmiany z zdefiniowanych fragmentach rejestrów systemowych windows,
ccc) System musi posiadać możliwość zdefiniowania własnych reguł wykrywających zmiany z zdefiniowanych folderach,
ddd) System musi umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu systemu i chronionych obiektów,
eee) System musi umożliwiać tworzenie dowolnej ilości profilów bezpieczeństwa zawierających predefiniowane reguły ochronne,
fff) System musi umożliwiać automatyzacje aplikowania profilów bezpieczeństwa poprzez zdefiniowanie filtra zawierającego nazwę, system operacyjny, serwer ESX czy instancję wykorzystującą chmurę,
ggg) System musi umożliwiać automatyczną zmianę przypisanych profilów bezpieczeństwa w przypadku zmiany IP przez chroniony system informatyczny,
hhh) System musi umożliwiać generowanie na żądanie oraz wg harmonogramu raportów w formatach minimalnie RTF oraz PDF oraz możliwość zabezpieczenie raportu poprzez jego zaszyfrowanie lub zabezpieczenie hasłem,
iii) System musi współpracować z bazami danych Oracle lub Microsoft SQL,
jjj) System musi integrować się z centralną konsolą informacyjną producenta,
kkk) System musi pozwalać na bezagentową ochronę środowisk wirtualnych opartych o platformę VMware vSphere w wersjach do 5.5,
lll) System musi pozwalać na bezproblemową integracje z vMware NSX,
mmm) System musi pozwalać na bezproblemową pracę w trybie mieszanym (NSX / nie NSX),
nnn) System musi posiadać możliwość zdefiniowania wykluczeń plików znajdujących się w obszarze objętych ochroną integralności,
ooo) System musi posiadać predefiniowane reguły chroniące krytyczne elementy chronionych systemów informatycznych,
ppp) System musi umożliwiać analizowanie logów z programów zainstalowanych na chronionych systemach informatycznych,
qqq) System musi umożliwiać analizowania logów ze zdefiniowanych plików znajdujących się na chronionych systemach informatycznych,
rrr) System musi umożliwiać analizowanie niestandardowych formatów plików typu log,
sss) W przypadku ochrony w trybie agentowym wszystkie funkcjonalności systemu muszą być dostępne w ramach pojedynczego agenta instalowanego na chronionych obiektach.

4. **Zakup oprogramowania do monitorowania i zarządzania siecią komputerową (SM) z usługą wsparcia technicznego na okres 36 miesięcy**

spełniającego warunki:

a) Wymagana nielimitowana ilość usług / sensorów oraz objęcie przedmiotowym oprogramowaniem urządzeń będących w dyspozycji Zamawiającego,

b) Jako jeden sensor należy liczyć każdą z poniższych pozycji:
   - monitorowanie ruchu (ang. traffic) / obciążenie sieci (ang. bandwidth) na jednym porcie urządzenia poprzez SNMP (np. switcha, firewalla, serwera) za pomocą standardu MIB2;
   - monitorowanie błędów/minimów, pakietów unicast, non-unicast na jednym porcie urządzenia poprzez protokół SNMP za pomocą MIB2,
   - monitorowanie innych parametrów systemowych poprzez SNMP (np.: procesor, wolne miejsce na dysku), które są dostępne poprzez wartość OID,
   - monitorowanie ruchu przechodzącego przez jedną kartę sieciową (NIC) poprzez Packet Sniffing. Jeśli jest używane filtrowanie, to każdy zestaw filtrów jest liczony jako jeden sensor,
   - monitorowanie strumienia danych poprzez xFlow (np.: NetFlow, sFlow, jFlow lub równoważne). Jeśli jest używane filtrowanie, to każdy zestaw filtrów jest liczony jako jeden sensor;
c) Monitorowanie ruchu/pasma per port urządzenia za pomocą protokołu SNMP (MIB2 standard),
d) Monitorowanie za pomocą protokołu SNMP (MIB2 standard): errors/min, unicast packets/s, non-unicast packet per port, port urządzenia oraz innych parametrów urządzeń za pomocą SNMP (np. cpu, dysk, etc.).
e) Monitorowanie strumienia danych za pomocą protokołów xFlow (np. NetFlow, sFlow, jFlow lub równoważne),
f) Monitorowanie przepustowości za pomocą SNMP, WMI, xFlow (np. NetFlow, sFlow, jFlow lub równoważne), Packet Sniffing,
g) Monitorowanie aplikacji,
h) Monitorowanie serwerów wirtualnych,
i) Monitorowanie SLA,
j) Monitorowanie QoS (np. przy użyciu VoIP),
k) Monitorowanie środowiska,
l) Monitorowanie LAN, WAN, VPN i Multiple Site Monitoring,
m) Rejestracja zdarzeń,
n) Obsługa i wsparcie dla IPv6 i IPv4,
o) Zaimplementowane technologie powiadamiania: wysyłka Email, SMS/Pager, syslog i SNMP Trap, żądanie z parametrem HTTP, wpis Event log, odtwarza pliki dźwiękowe, Amazon SNS, dowolna zewnętrzna technologia, która może być wywołana przez plik EXE lub .BAT,
p) Powiadamianie o stanie łączy (up, down, warning),
q) Stosowanie alarmów wg. limitów (wartość powyżej / poniżej x),

r) Stosowanie alarmów wg. wartości progowych (powyżej / poniżej x dla y minut),
s) Eskalacja alarmów (dodatkowe powiadomienia co x min podczas przestoju),
t) Opcja przyjęcia do wiadomości (nie ma więcej wysyłania not dla tego alarmu),
u) Zapewnienie dostępności komponentów sieciowych podczas pomiaru,
v) Brak wymagań względem dodatkowych modułów do działania typu (.NET, SQL Server, lub równoważnymi),
w) Posiadać interaktywny poradnik w programie,
x) Posiadać webowy interfejs użytkownika,
y) Aplikacja która pozwoli na przeglądanie danych z monitoringu kliku instancji w jednej aplikacji,
z) Udostępniać lokalny i zdalny dostęp do interfejsu użytkownika poprzez SSL,
aa) Obsługiwać m.in. poniższe typy sensorów: od Common Sensors poprzez Bandwidth Monitoring Sensors, Web Servers (http Sesnsors, SNMP Sensors, Windows/WMI Sensors, Linux/Unix/OS X Sensors, Virtual Servers Sensors, Mail Servers Sensors, SQL Database Sensors, File Servers Sensors, Various Servers Sensors, VoIP and Qos Sensors, Hardware Parameter Sensors i Custom Sensors,
bb) Umożliwiać tworzenie klastrów do 5 instancji („węzłów") w celu stworzenia zabezpieczenia na awarię systemu monitoringu,
cc) Stworzyć zabezpieczony na wypadek awarii klaster Systemu Monitoringu (SM), rozlokowany w co najmniej dwóch lokalizacjach,
dd) Aktualizacja oprogramowania nie powoduje przestoju klastra,
ee) Wsparcie rozwiązania automatycznego przełączania awaryjnego w przypadku awarii, którejś z instancji,
ff) Udostępnia na okres 2 miesięcy bezpłatną aktualizację,
gg) Możliwość objęcia Systemem Monitorowania usług:

- Serwer LDAP,
- Serwer syslog,
- Rsync,
- Windows file service,
- NFS service,
- Tftp,
- ftp,
- ftps,
- sftp,
- http,
- https

hh) Rozwiązanie których mowa w w/w wymaganiach funkcjonalnych powinno pochodzić od jednego producenta

5. **Zakup zintegrowanego systemu ochronnego typu Next-Generation Firewall z funkcjonalnością Next-Generation IPS i usługą wsparcia technicznego na okres 12 miesięcy – szt. 1 w ukompletowaniu:**
   - ASA 5585-X SSP-20 with FirePOWER Svcs. Chassis and Subs. - szt. 1,
   - ASA 5585-X SSP-20 FirePOWER SSP-60 12GE 8SFP+ AC 3DES/AES - szt. 1,
   - ASA 5585-X Hard Drive Blank Slot Cover – szt. 2,
   - ASA 5585-60 Control License – szt. 1,
   - Power Cord, 250Vac 16A, Europe – szt. 2,
   - ASA 9.2.2 Software Image for ASA 5500-X Series, 5585-X, ASA-SM – szt. 1,
   - 10GBASE-SR SFP Module – szt. 4,
   - VPN Client Software – szt. 1,
   - ASA 5585-X AC Power Supply – szt. 2,
   - ASA 5500 Strong Encryption License (3DES/AES) – szt. 1,
   - ASA 5585-X Fan Module – szt. 1,
   - ASA 5585-X Security Plus License (Enables 10G SFP+ Ports) – szt. 1,
   - ASA 5585-X FirePOWER SSP-60, 6GE, 4 SFP+ – szt. 1,
   - FirePOWER Software v 5.3.1 – szt. 1,
   - ASA 5585-60 FirePOWER IPS License – szt. 1,
   - ASA 5585-60 FirePOWER IPS 1YR Subscription – szt. 1,
   - FireSIGHT Management Center (VMware) for 2 devices – szt. 1

   lub równoważny spełniający warunki:
   Urządzenie pełniące funkcje ściany ogniowej i bramy VPN (Architektura urządzenia):
   - Urządzenie o konstrukcji modularnej pełniące funkcje bramy VPN i ściany ogniowej (firewall) typu Statefull Inspection. Urządzenie musi mieś możliwość dalszej rozbudowy sprzętowej.
   - Urządzenie wyposażone w co najmniej:
     - dwanaście interfejsów Gigabit Ethernet 10/100/1000 (RJ45),
     - sześć interfejsów 10Gigabit Ethernet definiowane przez wkładki SFP/SFP+/XFP.
     - Wraz z firewallem należny dostarczyć 4 (cztery) wkładki w specyfikacji SR,
     - min dwa dedykowane interfejsy Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania,

- Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych, nie mniej niż 1000 sumarycznie,
- Urządzenie wyposażone w moduł sprzętowego wsparcia szyfrowania 3DES i AES oraz licencje na szyfrowanie 3DES/AES,
- Urządzenie posiada dedykowany dla zarządzania port konsoli,
- Urządzenie posiada pamięć Flash o pojemności umożliwiającej przechowanie co najmniej 3 obrazów systemu operacyjnego i 3 plików konfiguracyjnych,
- Urządzenie posiada pamięć DRAM o pojemności nie mniejszej niż 48GB, umożliwiającej uruchomienie wszystkich dostępnych dla urządzenia funkcjonalności
- Urządzenie zapewnia możliwość klastrowania dla zwiększania wydajności pomiędzy dwoma odległymi fizycznie ośrodkami. Minimalna dopuszczalna ilość 8 urządzeń w klastrze.

Urządzenie pełniące funkcje ściany ogniowej i bramy VPN (Zasilanie urządzenia):

- Urządzenie posiada 2 redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V (niedopuszczalne rozwiązania zewnętrzne)

Urządzenie pełniące funkcje ściany ogniowej i bramy VPN (Wydajność urządzenia):

- Przepustowość firewalla stanowego z zagwarantowanym badaniem stanu połączeń sieciowych dla ruchu rzeczywistego nie mniejsza niż 10 Gb/s, z możliwością uzyskania do 20 Gb/s (maksymalna wydajność),
- Wydajność co najmniej 3 Gb/s dla ruchu szyfrowanego protokołami 3DES, AES,
- Urządzenie umożliwia terminowanie co najmniej 10000 jednoczesnych sesji VPN (IPSec VPN, SSL VPN),
- Obsługuje co najmniej 4.000.000 jednoczesnych sesji/połączeń z prędkością zestawiania 180 000 połączeń na sekundę. Dla pakietów 64 bajtowych urządzenie musi posiadać wydajność co najmniej 4.000.000 pakietów na sekundę,
- Posiada możliwość agregacji interfejsów fizycznych (IEEE 802.3ad) Ė min. 4 łączy zagregowanych. Pojedyncze łącze zagregowane może składać się z minimum 2 interfejsów,
- Urządzenie obsługuje funkcjonalność Access Control List (ACL) - zarówno dla ruchu wchodzącego, jak i wychodzącego. Minimalna obsługiwana ilość reguł 100.000 linii,
- Obsługa minimum 1024 VLAN-ów.

Urządzenie pełniące funkcje ściany ogniowej i bramy VPN (Funkcjonalność urządzenia):

- Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji,
- Urządzenie posiada możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory,
- Urządzenie musi posiadać możliwość budowania klastra złożonego z minimum 8 urządzeń. Każde urządzenie w klastrze ma aktywnie przetwarzać ruch dla sesji TCP, UDP dla dowolnej podsieci oraz VLAN-u,
- Klaster urządzeń musi mieć możliwość rozciągnięcia na minimum 3 ośrodki przetwarzania danych,
- Klaster urządzeń musi wspierać tryb transparentny oraz tryb routed,
- Urządzenie musi wspierać ruch asymetryczny oraz synchronizację stanów sesji dla minimum 3 ośrodków przetwarzania danych bez wykorzystania translacji adresów,
- Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos,
- Urządzenie nie posiada ograniczenia na ilość jednoczenie pracujących użytkowników w sieci chronionej,
- Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access),
- Urządzenie musi zapewniać zestawianie 10 000 tuneli SSL VPN w trybie client-based i clientless VPN,
- Urządzenie musi zapewniać w zakresie SSL VPN weryfikację uprawnień stacji do zestawiania sesji, poprzez weryfikację jej cech, co najmniej:
  - OS - System operacyjny,
  - IP Address Check - adres z jakiego następuje połączenie,
  - File Check - pliki w systemie,
  - Registry Check - wpisy w rejestrze systemu Windows,
  - Certificate Check - zainstalowane certyfikaty.
- Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN,
- Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP - wersje 32 i 64-bitowe) i Linux i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC,

- Oprogramowanie klienta VPN obsługuje protokoły szyfrowania 3DES/AES,
- Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połaczenia klientem VPN (wyłączanie tzw. split-tunnelingu),
- Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI,
- Urządzenie obsługuje protokół NTP,
- Urządzenie współpracuje z serwerami CA,
- Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) - zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego,
- Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standy, active/active dla kontekstów oraz praca w klastrze,
- Urządzenie realizuje synchronizację tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA,
- Urządzenie zapewnia możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia,
- Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN,
- Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli co najmniej następujących usług:
  - Hypertext Transfer Protocol (HTTP),
  - File Transfer Protocol (FTP),
  - Extended Simple Mail Transfer Protocol (ESMTP),
  - Domain Name System (DNS),
  - Simple Network Management Protocol v 1/2/3 (SNMP),
  - Internet Control Message Protocol (ICMP),
  - SQL*Net,
  - Inspekcji protokołów dla ruchu voice/video Ė H.323 (włącznie z H.239), SIP, MGCP, RTSP,
- Urządzenie umożliwia zaawansowaną normalizację ruchu TCP:
  - poprawność pola TCP ACK(invalid-ack),
  - poprawność sekwencjonowania segmentów TCP (seq-past-windows),
  - poprawność ustanawiania sesji TCP z danymi (synack-data),
  - limitowanie czasu oczekiwania na segmenty nie w kolejności,
  - poprawność pola MSS (exceed-mss),
  - poprawność pola długości TCP,

- poprawność skali okna segmentów TCP non-SYN,
- poprawność wielkości okna TCP,

- Urządzenie ma możliwość blokowania aplikacji (np. peer-to-peer czy Internetowy komunikator) wykorzystujących port 80,
- Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługę komend wprowadzonych wraz z protokołem ESMTP,
- Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe,
- Urządzenie zapewnia wsparcie stosu protokołów IPv6 w tym:
  - dla list kontroli dostępu dla IPv6
  - możliwość filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload,
  - wspiera inspekcję protokołu IPv6, pracując w trybie transparentnym,
  - wspiera adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover),
  - wspiera realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6,
- Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu,
- Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB,
- Urządzenie obsługuje routing statyczny i dynamiczny (min. dla protokołów RIP, OSPF i BGP),
- Urządzenie pozwala na osiągnięcie wysokiej dostępności dla protokołów routingu dynamicznego (min OSPF), tzn. trasy dynamiczne zawarte w tablicy routingu są synchronizowane z urządzenia active na urządzenie standby,
- Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL),
- Urządzenie umożliwia konfiguracji globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednoczenie,
- Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokołów lub numer portu,

- Urządzenie umożliwia pominiecie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu,
- Urządzenie wspiera Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN,
- Urządzenie wspiera użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD, bezpośrednio lub poprzez ACS, co najmniej dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła,
- Urządzenie obsługuje IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec,
- Urządzenie musi umożliwiać rozbudowę (poprzez zakup odpowiedniej licencji lub oprogramowania bez konieczności dokonywania zmian sprzętowych) o możliwość wirtualizacji konfiguracji poprzez wirtualne konteksty. Wymagana jest możliwość rozbudowy urządzenia o wsparcie dla co najmniej 250 wirtualnych kontekstów.

Funkcjonalność urządzenia - NGFW:

- Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż:
  - System automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
  - System IPS,
  - System ochrony przed malware,
  - System filtracji ruchu w oparciu o URL,
- System musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. Wymagane jest by system tworzył kontekst z wykorzystaniem co najmniej poniższych parametrów:
  - Wiedza o użytkownikach - uwierzytelnienie,
  - Wiedza o urządzeniach - pasywne skanowanie ruchu,
  - Wiedza o urządzeniach mobilnych,
  - Wiedza o aplikacjach wykorzystywanych po stronie klienta,
  - Wiedza o podatnościach,

- Wiedza o bieżących zagrożeniach,
- Baza danych URL,

- System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM,
- System Klasyfikacji i Rozpoznawania Aplikacji (SKRA) musi:
  - posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych,
  - zapewniać wydajność co najmniej 7Gb/s Ė adekwatnie do rzeczywistej wydajności firewalla stanowego,
  - pozwalać na tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego z którego korzysta użytkownik oraz wykorzystywanych usług,
  - pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji,
  - umożliwiać współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system SKRA oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach,
- System IPS musi:
  - Zapewniać skuteczność wykrywania zagrożeń i ataków na poziomie minimum 98% udokumentowany przez niezależne testy opublikowane w okresie ostatnich 18 miesięcy (np. niezależne testy NSS Labs)
  - Posiadaś możliwość pracy w trybie in-line (wszystkie pakiety, które mają byś poddane inspekcji muszą przechodzić przez system),
  - posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu),
  - posiadać możliwość wykrywania i uniemożliwiania szerokiej gamie zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługi VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.)
  - posiadać możliwość wykrywania modyfikacji znanych ataków jak i te nowo powstałe, które nie zostały jeszcze dogłębnie opisane,
  - zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
    - sygnatury ataków opartych na exploitach,
    - reguły oparte na zagrożeniach,
    - mechanizm wykrywania anomalii w protokołach,
    - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego,

- mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,
- posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives),
- mieś możliwość detekcji ataków/zagrożeń zgłoszonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń,
- posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastąpienie zawartości pakietów oraz mieś możliwość zapisywania pakietów,
- mieś możliwość detekcji ataków i zagrożeń opartych na protokole IPv6,
- posiadać możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności, takich jak systemy operacyjne, serwisy, otwarte porty, aplikacje oraz zagrożenia w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności,
- posiadać możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych,
- zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
- posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,
- zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,
- zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą byś pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne,
- zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie być zarządzany tylko poprzez system centralnego zarzadzania za pomocą szyfrowanego połączenia,
- zapewniać obsługę reguł Snort,
- Zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS,

- Zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
- Zapewniać mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa,
- Posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu - w szczególności musi posiadać możliwość pracy w trybie failover firewalla oraz w trybie klastrowania,
- System IPS powinien pozwalać na pracę z przepustowością co najmniej 6 Gb/s przy jednoczesnym działaniu systemu wykrywania aplikacji.

Zarządzanie i konfiguracja:

- Urządzenie posiada możliwość eksportu informacji przez syslog.
- Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogiczny,
- Urządzenie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ oraz obsługuje mechanizmy AAA (autentykacja, autoryzacja, accounting),
- Urządzenie jest konfigurowalne przez CLI oraz interfejs graficzny,
- Dostęp do urządzenia jest możliwy przez SSH,
- Urządzenie obsługuje protokół SNMP v 1/2/3,
- Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją,
- Urządzenie umożliwia zrzucenie obecnego stanu programu (coredump) dla potrzeb diagnostycznych,
- Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łączności w sieciach IP,
- Urządzenie umożliwia kontrolę dostępu administracyjnego protokołem tacacs+, za pomocą systemu ACS,

Obudowa:

- Urządzenie ma możliwość instalacji w szafie typu Rack 19"
- Wysokość urządzenia nie większa niż 2RU,

Dopuszczalne sposoby realizacji rozwiązania:

- Zamawiający wymaga spełnienia następujących warunków realizacji zadania ochrony styku z DC:

- Firewalle zastosowywane do ochrony styku z DC muszą pochodzić od jednego producenta,

- Funkcjonalność firewalla sieciowego i firewall NGFW musi byś realizowana na jednym urządzeniu,

- Dopuszcza się zastosowanie zewnętrznych urządzeń IPS w przypadku gdy funkcjonalność IPS realizowana na urządzeniach ochrony styku z DC byłaby innego producenta aniżeli dedykowane sondy IPS. W takim przypadku oferent zobowiązany jest do zapewnienia całościowej wymaganej funkcjonalności IPS na dostarczonych sondach. Dotyczy to także wymagań wydajnościowych. Oferent w przypadku zastosowania tego modelu wdrożenia zobowiązany jest:

  - do zapewnienia 2 dodatkowych portów 10Gbps w urządzeniu firewall,
  - do zastosowania urządzenia firewall o odpowiednio wyższej wydajności tj. minimum 10 Gbps większej wydajności (ruch full duplex - 5 Gbps do sondy IPS z firewalla oraz 5Gbps ruchu powrotnego),
  - odpowiedniego wyposażenia (porty) sondy IPS umożliwiającego realizację tego zadania,
  - do zapewnienia odpowiedniej liczby urządzeń (1:1 z firewallami) celem uzyskania niezbędnej redundancji. Niedopuszczalne jest zastosowanie mniejszej liczby urządzeń IPS niż firewalli,

Wymagania szczegółowe dotyczące konsoli zarządzającej IPS (Funkcjonalność konsoli zarządzania i konfiguracji):

- Platforma zarządzająca musi byś oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym,
- Platforma zarządzająca musi byś centralnym punktem, z którego możliwe jest zarzadzanie wszystkimi urządzeniami,
- Platforma zarządzająca musi umożliwiać agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działając w czasie rzeczywistym,
- Platforma zarządzająca musi byś dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego,
- Konsola zarządzająca musi zapewniać interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator musi posiadać możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria,

- Konsola zarządzająca musi mieś możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm,
- Konsola zarządzająca musi mieś możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Musi istnieć możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami,
- Konsola zarządzająca musi zapewniać zarzadzanie oparte o role, gdzie każdy z użytkowników systemu może mieś różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany,
- Konsola zarządzająca musi zapewniać funkcjonalność typu harmonogram zadań umożliwiając automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS,
- Konsola zarządzająca musi zapewniać więcej niż jedną predefiniowaną politykę bezpieczeństwa w celu ułatwienia wdrożenia systemu,
- Konsola zarządzająca musi zapewniać grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją,
- Konsola zarządzająca musi zapewniać przeglądanie, włączanie oraz wyłączanie zarówno indywidualnych reguł jak i grup oraz kategorii reguł,
- Konsola zarządzająca musi mieś możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak aby ułatwić czynności monitorowania sieci,
- Konsola zarządzająca musi pozwalać na dogłębne wykorzystanie informacji kontekstowych (takich jak informacje o konfiguracji, zachowaniu sieci i hostów) w celu poprawienia efektywności i dokładności procesu manualnej i automatycznej analizy incydentów,
- Oferowane rozwiązanie musi dawać możliwość znaczącej redukcji nakładów operacyjnych oraz przyspieszać reakcję na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skuteczności ataku na docelowego hosta,
- Oferowane rozwiązanie musi mieś możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora poprzez:
  - selekcję reguł,
  - zmianę konfiguracji polityki,
  - uaktualnianie polityki, itp.)

- Konsola zarządzająca musi zapewnić możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS,
- Konsola zarządzająca musi zapewnić możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń IPS jak i platformy zarządzającej,
- Konsola zarządzająca musi zapewnić funkcjonalność pozwalającą na zarzadzanie cyklem życia incydentu, od początkowego powiadomienia poprzez odpowiedzi, aż do rozwiązania,
- Konsola zarządzająca musi zapewnić możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu,
- Konsola zarządzająca musi zapewnić różne możliwości automatycznej odpowiedzi na zagrożenia - nie mniej niż:
  - alarmy,
  - rekonfiguracja zapory ogniowej,
  - rekonfiguracja routera,
- Konsola zarządzająca musi zapewnić możliwość przechowywania incydentów, logów oraz innych informacji generowanych przez system zarówno w wewnętrznej bazie danych jak i posiadać możliwość udostępniania do zabezpieczonego wglądu w te informacje zewnętrznym aplikacjom aportującym w trybie „tyko do odczytu",
- Konsola zarządzająca musi zapewnić możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP,
- Konsola zarządzająca musi zapewnić możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze,
- Rozwiązanie musi zapewniać logowanie przy użyciu zewnętrznego serwera LDAP zarówno do urządzeń IPS, jak i konsoli zarządzającej,
- Konsola zarządzająca musi zapewnić duże możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika,
- Konsola zarządzania musi posiadać możliwość automatycznej generacji raportów:
  - za wybrany okres (np. godzina, dzień, tydzień itp.),
  - dla konkretnego modułu generującego zdarzenia (np. Health (stan urządzeń),
  - dla przepływów ruchu - Flows (statystyki ruchu sieciowego),
  - Audit Log,
  - Compliance (polityka zgodności),
  - Dla wykrytych podatności,

- Dla zdarzeń związanych z wykrywaniem użytkowników,
- z importowania nowych paczek sygnatur/reguł, itp.).

- Konsola zarządzająca musi posiadać możliwość generowania statystyk dostępnych przez interfejs użytkownika oraz możliwość generowania raportów w różnych formatach (html, pdf, csv) i przesyłania ich e-mailem,
- Konsola zarządzająca musi zapewniać informowanie o zagrożeniach poprzez:
  - wysłanie e-maila,
  - wysłanie trap SNMP,
  - przesłanie informacji do serwera Syslog,
  - uruchomienie skryptu użytkownika,
  - wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze,
- Konsola zarządzająca musi pozwalać na monitorowanie stanu pracy wszystkich zainstalowanych urządzeń IPS,
- Konsola zarządzająca musi posiadać możliwość kreowania i edycji polityk monitorowania stanu pracy wszystkich urządzeń: zarówno konsoli zarządzających jak i urządzeń IPS,
- Konsola zarządzania musi pozwalać na gromadzenie logów ze wszystkich obsługiwanych sond IPS,
- Konsola zarządzania musi posiadać zaawansowany system przeszukiwania logów powalający na przeprowadzanie analizy:
  - aktualnego stanu danego urządzenia,
  - podglądu historii dostępnych zasobów,
  - możliwość eliminacji powtarzających się alarmów (tzw. Black Listing),
- System zarządzania musi pozwalać na tworzenie wielu polityk bezpieczeństwa zawierających różne zestawy sygnatur i przydzielania ich do segmentów zdefiniowanych na różnych urządzeniach. Powinny byś dostępne dwie opcje podczas instalacji przypisanej polityki:
  - wysłanie polityki tylko do przypisanego urządzenia IPS,
  - wysłanie polityki do każdego z dostępnych urządzeń IPS,
- Reguły wykrywające nowo ujawnione zagrożenia i luki muszą być wygenerowane przez dostawcę w przeciągu 48 godzin od ich ogłoszenia.
- Reguły wykrywania zagrożeń muszą mieć możliwość modyfikacji i rozszerzenia, muszą być oparte na ogólnodostępnym języku składni tak, aby użytkownicy mogli tworzyć je samodzielnie jak i edytować te dostarczane przez producenta systemu,

- Reguły dostarczone przez producenta muszą byś należycie udokumentowane, z pewnymi opisami własności, pochodzenia oraz istotności blokowanych ataków i zagrożeń,
- Konsola zarządzająca musi posiadać mechanizm konfiguracji wielkości poszczególnych baz danych w zależności od rodzaju logowanego zdarzenia wedle wymagań administratora,
- Polityki definiowane przez konsolę zarządzającą muszą posiadać historię zmian wraz z informacją o:
  - Osobie/administratorze modyfikującym polityki,
  - Czasie modyfikacji polityki,
  - Informacji porównawczej danej polityki z politykami wstecznymi (definiowanymi wcześniej),
- Konsola zarządzająca musi posiadać możliwość porównywania odrębnych polityk IPS w formie raportu,
- Konsola zarządzająca musi posiadać możliwość eksportowania dostępnych ustawień i polityki w formie paczek konfiguracyjnych dostępnych w odrębnych plikach,
- Konsola zarządzająca musi zapewniać tworzenie profilu ruchu sieciowego w normalnych warunkach (tzw. profil podstawowy) wykorzystując różne technologie analizy przepływów (np. NetFlow) i możliwość wykrycia odchylenia od profilu podstawowego (funkcjonalność Analizy Zachowania w Sieci),
- Funkcjonalność AZwS musi przedstawiać sposób wykorzystania pasma sieciowego w celu ułatwienia wykrywania przeciążeń i przestojów urządzeń sieciowych,
- Funkcjonalność AZwS musi zapewniać możliwość gromadzenia informacji o węzłach końcowych (np. serwerach, stacjach roboczych) w celu zapewnienia korelacji ze zdarzeniami bezpieczeństwa. Korelacja ma na celu umożliwienie priorytetyzacji zdarzeń bezpieczeństwa,
- Urządzenia sieciowe, na których uruchomiony jest system IPS muszą zapewniać jednocześnie funkcjonalność AZwS. Funkcjonalność AZwS nie może wymagać instalacji dodatkowych urządzeń,
- Konsola zarządzająca do system IPS musi być również wykorzystywana do zarządzania funkcjonalnością AZwS. Zarządzanie AZwS nie może wymagać instalacji dodatkowej konsoli zarządzającej,
- Oferowane rozwiązanie musi mieś możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym,

- Oferowane rozwiązanie musi mieś możliwość wykluczania poszczególnych hostów z polityk zgodności oraz blokowania odpowiednich zdarzeń i alarmów dla tych właśnie hostów,
- Oferowane rozwiązanie musi posiadać możliwość łatwej identyfikacji wszystkich hostów, które poosiadają dany atrybut lub nie spełniają zadanych warunków polityki zgodności,
- Całość komunikacji pomiędzy poszczególnymi komponentami systemu IPS musi byś zabezpieczona protokołem kryptograficznym,
- Platforma musi mieś możliwość uruchomienia funkcji nowej generacji zapory ogniowej, URL filtering, kontroli plików za pomocą dodatkowej licencji,
- Konsola musi umożliwiać skonfigurowanie i utrzymanie polityki dostępu zapory ogniowej i instrumentów oraz polityk IPS,
- Konsola musi prowadzić przegląd wszystkich zdarzeń związanych z bezpieczeństwem pod kątem analizy powłamaniowej i wczesnej prewencji włamań,
- Konsola musi umożliwiać dostrajanie polityki bezpieczeństwa do specyfiki monitorowanych segmentów sieciowych oraz zarzadzanie setkami urządzeń monitorujących,
- Użytkownik obsługujący konsolę zarządzającą musi mieś możliwość:
  - ustawienia i wykorzystania automatycznych rekomendacji strojenia polityki
  - zapobiegania zagrożeń IPS opartych na wiedzy kontekstowej o:
    - sieci,
    - użytkownikach,
    - systemach operacyjnych,
    - usługach i aplikacjach,
    - charakterystyce sesji ruchu sieciowego, które mają byś chronione,
- System zarządzania musi mieś możliwość integrowania się z rozwiązaniami firm trzecich typu Vulnerabilitity Scanner/Vulnerability Management, dostarczających dodatkowych informacji na temat luk i podatności istniejących w monitorowanych środowiskach w celu bardziej precyzyjnego szacowania skutków zagrożeń oraz automatycznego procesu strojenia polityki modułu IPS,
- Platforma musi mieś otwarty i rozszerzalny mechanizm zapobiegania zagrożeniom oraz możliwość definiowania własnych detektorów aplikacji,
- Rozwiązanie powinno mieś możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlan'ów i użytkowników:
  - dozwolone porty i protokoły,

- dozwolone aplikacje według różnych kategorii,
- dozwolone kategorie stron internetowych (URL filtering)
- dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej,
- sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne,

- Rozwiązanie musi zapewniać usługi dynamicznej reputacji znanych adresów IP propagujących zagrożenia w sieci Internetowej oraz możliwość definiowania własnych, zewnętrznych źródeł informacji. Adresy te powinny byś blokowane jako znane zagrożenia i kategoryzowane w między innymi następujące grupy, według typu stwarzanego zagrożenia:
  - Attackers,
  - Bogon,
  - Bots,
  - CNC,
  - Malware,
  - Open_proxy,
  - Open_relay,
  - Phishing,
  - Tor_exit_node,
- W ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie musi mieś możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji musi zostać zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia,
- Konsola zarządzające musi zapewniać obsługę zdalnych uaktualnień, wykonywania kopii zapasowych oraz przywracania jak i funkcjonalność odinstalowywania uaktualnień bez konieczności fizycznego dostępu do urządzenia,

Wydajność urządzenia i sposób realizacji konsoli zarządzania (Funkcjonalność konsoli zarządzania i konfiguracji):

- Konsola zarządzania musi byś dostępna w co najmniej dwóch postaciach pozwalających Zamawiającemu na swobodny dobór właściwego narzędzia zarządzania:
  - w formie tradycyjnych urządzeń fizycznych,

- jako maszyna wirtualna przy czym w tej wersji musi posiadać tożsame funkcje z konsolą w postaci urządzenia fizycznego (nie dotyczy to funkcji wymagających obecności dedykowanych układów ASIC).

- Konsola zarządzania musi zostać zaoferowana w postaci wirtualnej instancji serwera realizującego konsolę zarządzania,
- Konsola zarządzania musi posiadać odpowiednią wydajność pozwalająca docelowo na obsłużenie nie mniej niż 10 urządzeń IPS,
- Konsola zarządzająca musi byś przygotowana do ciągłej obsługi nie mniej niż 10 000 zdarzeń na sekundę,
- Konsola zarządzająca musi zapewniać możliwość przechowania co najmniej 10 milionów zdarzeń IPS.

6. **Zakup systemu zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i typu zero-day z usługą wsparcia technicznego na okres 12 miesięcy – szt. 1 spełniający warunki:**

System ochrony powinien zapewnić dwa tryby ochrony przed zagrożeniami typu zero-day:

a) prewencyjny – eliminujący z dokumentów elementy aktywne będące potencjalnym nośnikiem wirusów (makrodefinicje, aplety, akcje audio lub wideo itp.),
b) analityczny – analizujący zachowanie dokumentów w środowisku wirtualnym (tzn. Sandboxing)

System musi spełniać następujące wymagania techniczne w zakresie trybu prewencyjnego – parasolowa eliminacja potencjalnie niebezpiecznych elementów plików:

- w trybie prewencyjnym oferowany system ochrony musi umożliwiać eliminowanie z plików dostarczanych za pośrednictwem poczty elektronicznej całości aktywnej zawartości. W szczególności system musi umożliwiać dostarczenie dokumentu będącego załącznikiem poczty elektronicznej w postaci nowego pliku w formacie Adobe PDF o tożsamej treści, z zawartością pozbawioną wszelkiego aktywnego kodu.
- system wspiera protokół:
  - poczta SMTP,

- system obsługuje pliki MS Office i Adobe Acrobat:
  - pdf Adobe acrobat document,
  - fdf Adobe acrobat document,
  - xlam Excel add-in,
  - xlsb Excel binary worksheet,

- xltm Excel macro-enabled template,
- xlsm Excel macro-enabled workbook,
- xltx Excel template,
- pps Legacy PowerPoint slideshow,
- pot Legacy PowerPoint template,
- xls Microsoft Excel 97-2003 Worksheet,
- xlsx Microsoft Excel Worksheet,
- ppt Microsoft PowerPoint 97-2003 Presentation,
- pptx Microsoft PowerPoint Presentation,
- doc Microsoft Word 97-2003 Document,
- docx Microsoft Word Document,
- ppam PowerPoint add-In,
- pptm PowerPoint macro-enabled presentation,
- ppsm PowerPoint macro-enabled slideshow,
- potm PowerPoint macro-enabled template,
- ppsx PowerPoint slideshow,
- potx PowerPoint template,
- docm Word macro-enabled document,
- dotm Word macro-enabled template,
- dot Word Template,
- dotx Word template

- system zapewnia eliminację elementów aktywnych z dokumentów:
- bez zmiany typu dokumentu,
- z przetłumaczeniem pliku na statyczny plik PDF

- system powinien umożliwiać dostęp do oryginalnego dokumentu,
- system zapewnia eliminację z dokumentów elementów:
  - PDF JavaScript Action,
  - Microsoft Office macro,
  - PDF JavaScript code,
  - PDF Submit Form Action,
  - PDF Launch Action,
  - Linked Object,
  - Embedded Object,
  - Sensitive Hyperlink,
  - PDF Movie Action,
  - PDF Sound Action,

- PDF URI Action,
- PDF GoToR Action,
- Database Querry,
- Custom Properties

- system umożliwia pracę w trybach:
  - aktywnym: modyfikacja plików,
  - wykrywania/informowania (detect)

System musi spełniać następujące wymagania techniczne w zakresie trybu analitycznego (sandboxing):

- w trybie analitycznym oferowany system ochrony musi umożliwiać otwarcie dostarczanego za pośrednictwem żądanych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w wirtualnym systemie operacyjnym a następnie podjęcie akcji (zablokuj/prześlij do odbiorcy) w zależności od analizy skutków otwarcia pliku w wirtualnym systemie operacyjnym
- system zapewnia wsparcie dla protokołów:
  - poczta: SMTP,
  - www: HTTP i HTTPS

- system zapewnia obsługę plików MS Office, Adobe Acrobat, wykonywalnych, archiwów:

- pdf Adobe acrobat document,
- doc Microsoft Word 97-2003 Document,
- docx Microsoft Word Document,
- xls Microsoft Excel 97-2003 Worksheet,
- xlsx Microsoft Excel Worksheet,
- ppt Microsoft PowerPoint 97-2003 Presentation,
- pptx Microsoft PowerPoint Presentation,
- exe Executable File,
- tar Tar Archive,
- zip Zip Archive,
- rar Rar Archive,
- Seven-Z 7z Archive,
- rtf Rich Text Format File,
- dot Word Template,
- docm Word macro-enabled document,
- dotx Word template,

- dotm Word macro-enabled template,
- xlt Legacy Excel 97-2003 templates,
- xlm Excel macro,
- xltx Excel template,
- xlsm Excel macro-enabled workbook,
- xltm Excel macro-enabled template,
- xlsb Excel binary worksheet,
- xla Excel add-in or macro,
- xlam Excel add-in,
- xll Excel XLL (DLL based) add-in,
- xlw Excel workspace,
- pps Legacy PowerPoint slideshow,
- pptm PowerPoint macro-enabled presentation,
- potx PowerPoint template,
- potm PowerPoint macro-enabled template,
- ppam PowerPoint add-In,
- ppsx PowerPoint slideshow,
- ppsm PowerPoint macro-enabled slideshow,
- sldx PowerPoint slide,
- sldm PowerPoint macro-enabled slide,
- csv Comma-separated values file.

- system zapewnia wspieranie n/w środowisk emulacyjnych:
  - MS Windows XP, MS Windows 7,
  - MS Office 2003, 2007, 2010,
  - Adobe 9, 11,
  - system zapewnia możliwość rozbudowy o dodatkowe środowiska

- system zapewnia wsparcie dla pracy w trybach sieciowych:
  - tap/mirror port,
  - in-line,
  - MTA (Mail transfer agent)

- system umożliwia pracę w trybach:
  - blokowania / ochorny (prevent),
  - wykrywania / informowania (detect)

- system zapewnia pracę w trybie chmury prywatnej z możliwością całkowitego wyłączenia wysyłania informacji przez sieć Internet,

- system zapewnia wydajnośc i skalowalnośc:
  - obsługa do 40 tysięcy użytkowników,
  - obsługa do 40 tysięcy skrzynek pocztowych,
  - sandboxing do 2 milionów plików miesięcznie,
  - możliwość rozbudowy chmury prywantnej o dodatkowe urządzenia,
  - możliwość rozproszenia geograficznego elementów chmury prywatnej (geo-clustering)

System musi zapewnić wymagania w zakresie systemu zarządzania systemem zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i zagrożeń typu zero-day w zakresie:

- scentralizowane zarządzanie konfiguracją, polityką i logami. Zarządzanie systemem musi zostać dostarczone w ramach nieniejszego postępowania lub dostarczone rozwiązanie musi być zarządzane z posiadanego przez Zamawiającego systemu zarządzania – Check Point SmartCenter,
- korelacji zdarzeń generowanych przez system zapobiegania i wykrywania zagrożeń zmaskowanych, nierozpoznanych i zagrożeń typu zero-day ze zdarzeniami generowanymi przez posiadanych przez Zamawiającego systemem zapór sieciowych Check Point Security Gateway. System korealacji musi zostać doatarczony w ramach nieniejszego postępowania lub dostarczone rozwiązanie musi współpracować z posiadanym przez Zamawiającego systemem korelacji zdarzeń Check Point SmartEvent

System musi spełnić wymagania sprzętowe:

- system musi zostać dostarczony w postaci jednego dedykowanego urządzenia typu appliance posiadającego:
  - 2 szt. redundantnych zasilaczy,
  - kartę zarządzania typu Light-Out-Management,
  - minimum 64 GB pamięci RAM,
  - możliwość uruchomienie do 56 wirtualnych maszyn symulujących posiadane systemy operacyjne Zamawiającego.

- Dopuszcza się zrealizowanie części wymagań funkcjonalnych systemu zapobiegania i wykrywania zagrożeń zmaskowanych, nierozpoznanych i zagrożeń typu zero-day w postaci modułów uruchamianych na posiadanej przez Zamawiającego zaporze

sieciowej Check Point Security Gateway. W takim przypadku licencje pozwalające na korzystanie z tych modułów muszą zostać dostarczone wraz z oferowanym systemem.

7. **Zakup i dostawa voucherów (ważnych przez 12 miesięcy liczonych od podpisania protokołu odbioru produktu) na warsztaty szkoleniowe 18 szt.:**
   Warsztaty muszą spełniać poniższe wymgania:
   a) **Warsztat nr. 1 - certyfikowane szkolenie w zakresie administracji i zarządzania systemem zabezpieczającym środowisko VMware wymienionym w Pkt. 3,**

   b) **Warsztat nr. 2 - warsztat szkoleniowy w zakresie administracji i zarządzania systemem ochronnym typu Next-Generation Firewall z funkcjonalnością Next-Generation IPS wymienionym w Pkt. 5 spełniający wymagania:**

      Warsztaty będą obejmować:
      - Omówienie struktury systemów NGFW oraz IPS,
      - Przykładowe wdrożenie sondy IPS,
      - Prezentację nawigacji po systemie administracyjnym systemów NGFW oraz konsoli zarządzającej IPS,
      - Omówienie tworzenia oraz implementowania obiektów używanych w politykach kontroli dostępu,
      - Tworzenie przykładowych reguł i scenariuszy analizy ruchu w środowisku przy użyciu konsoli zarządzającej.

      Czas trwania warsztatów będzie zawierać się w przedziale 40-50 godzin zegarowych. Warsztaty zostaną przeprowadzone w siedzibie Wykonawcy.

      Szkolenie powinno zostać przygotowane dla grupy 6 osobowej.

   c) **Warsztat nr. 3 - certyfikowane szkolenie w zakresie administracji zarządzania systemem zapobiegania i wykrywania zagrożeń zmaskowanych, nierozpoznanych i typu zero-day w Pkt. 6**

Wymagania odnośnie warsztatów szkoleniowych zostały określone w Załączniku nr 4 do projektu Umowy.

Załącznik nr 5 do SIWZ
Nr sprawy 181/BŁiI/15/MT

PROJEKT UMOWY

UMOWA nr .....

zawarta w Warszawie w dniu .....2015 roku

pomiędzy:

Skarbem Państwa – Komendantem Głównym Policji z siedzibą w Warszawie przy ul. Puławskiej 148/150, zwanym w treści umowy **„Zamawiającym"**, reprezentowanym przez:

1. ..... - **Dyrektora Biura Łączności i Informatyki KGP**

oraz przy kontrasygnacie:

1. ..... - **Dyrektora Biura Finansów KGP**

a firmą ..... siedzibą w ..... , wpisaną do ....., KRS nr: ....., REGON .....; NIP ....., z kapitałem zakładowym wynoszącym ..... zwaną w treści Umowy „Wykonawcą", reprezentowaną przez:

1. .....

2. .....

zwanym dalej **Wykonawcą,**
zwanych łącznie **Stronami.**

Umowa zostaje zawarta na podstawie przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego (nr sprawy .....) zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2013 r., poz. 907, ze. zm.)

§ 1
Przedmiot umowy

Przedmiotem Umowy jest **„Przebudowa Centralnego Węzła Internetowego Komendy Głównej Policji", Etap III – Podniesienie poziomu bezpieczeństwa i dostępności usług"**.

1. Szczegółowy opis Przedmiotu Umowy wraz ze specyfikacją techniczną stanowi Załącznik nr 1 do Umowy.
2. Przedmiot Umowy obejmuje w szczególności:
   1) Zakup modułów SFP+;
   2) Zakup pamięci operacyjnej RAM;
   3) Zakup systemu zabezpieczającego środowisko VMware z usługą wsparcia technicznego na okres 12 miesięcy;
   4) Zakup oprogramowania do monitorowania i zarządzania siecią komputerową (SM) z usługą wsparcia technicznego na okres 36 miesięcy;

5) Zakup zintegrowanego systemu ochrony typu Next-Generation Firewall z funkcjonalnością Next-Generation IPS i usługą wsparcia technicznego na okres 12 miesięcy;
6) Zakup systemu zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i typu zero-day z usługą wsparcia technicznego na okres 12 miesięcy,
7) Zakup i dostawa voucherów na warsztaty szkoleniowe - 18 szt.

3. Specyfikację ilościowo-cenową zawiera **Załącznik nr 5 do Umowy**.
4. Ilekroć w dalszych postanowieniach umowy mowa jest o dostawie, instalacji, dokumentacji, sprzęcie, asyście, konserwacji itp. bez bliższego oznaczenia, należy przez to rozumieć Przedmiot Umowy, określony w **Załączniku nr 1 do Umowy**.
5. Postanowienia umowy obowiązują z dniem zawarcia.

§ 2
Organizacja projektu

1. W celu bezpośredniego nadzoru nad realizacją Przedmiotu Umowy, Zamawiający na Kierownika Projektu wyznacza nw. przedstawiciela:
   .....
2. W celu bezpośredniego nadzoru nad realizacją Przedmiotu Umowy, Wykonawca na Kierownika Projektu wyznacza nw. przedstawiciela:
   .....
3. Kierownicy Projektu o których mowa w ust. 1 i 2, odpowiednio ze strony Zamawiającego i Wykonawcy, odpowiadają za nadzór nad wykonaniem Przedmiotu Umowy zgodnie z wymaganiami, w założonym terminie, w ramach określonego budżetu, przy wykorzystaniu dostępnych zasobów i środków.
4. Kierownicy Projektu upoważnieni są do podejmowania decyzji i akceptacji zmian dotyczących realizacji przedmiotu Umowy, za wyjątkiem decyzji wymagających formy aneksu.
5. Obie Strony mogą zmienić swoich przedstawicieli w organizacji projektu informując drugą Stronę, z co najmniej 1-tygodniowym wyprzedzeniem. Zmiana taka nie wymaga aneksu do umowy.

§ 3
Realizacja umowy

1. Wykonawca zobowiązuje się do realizacji i dostarczenia Przedmiotu Umowy wskazanego w § 1 ust. 2 pkt 1-7 **w terminie 30 roboczych dni od dnia podpisania umowy.**, przy czym za termin wykonania przebudowy Centralnego Węzła Internetowego Komendy Głównej Policji", Etap III – Podniesienie poziomu bezpieczeństwa i dostępności usług przyjmuje się datę podpisania bez zastrzeżeń przez przedstawicieli Wykonawcy i Zamawiającego protokołu odbioru Przedmiotu Umowy, stanowiącego **Załącznik nr 8.**
2. Wykonawca w terminie 5 dni kalendarzowych od daty zawarcia umowy, przedstawi do akceptacji Zamawiającego harmonogram realizacji Umowy. Zamawiający dokona weryfikacji harmonogramu w ciągu 3 (trzech) Dni Roboczych. Brak uwag ze strony Zamawiającego w ww. terminie oznacza akceptację przez Strony Umowy przedstawionego harmonogramu.
3. Przedmiot Umowy podlegać będzie odbiorowi. Szczegółowe zasady odbioru przedmiotu umowy zawiera **Załącznik nr 2 do Umowy.**
4. Wszystkie czynności związane z odbiorami muszą zakończyć się w terminie wskazanym w ust. 1.
5. Wykonawca gwarantuje, że dostarczony sprzęt jest fabrycznie nowy, wolny od wad fizycznych i prawnych, pakowany w oryginalne bezzwrotne opakowania producenta, wyprodukowany w 2015 r.
6. Dostarczony sprzęt posiada certyfikat „znak CE".
7. Wykonawca jest zobowiązany do spełnienia wymogów w zakresie zapewnienia efektywności energetycznej dostarczanych urządzeń, wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (WE) 106/2008 z dnia 15.01.2008 w sprawie wspólnotowego programu znakowania efektywności energetycznej urządzeń biurowych.
8. Wykonawca gwarantuje, że dostarczony Zamawiającemu Przedmiot umowy odpowiadać będzie przeznaczeniu i użytkowi wynikającemu z Umowy, będzie w pełni zgodny ze specyfikacją wymaganą przez Zamawiającego.
9. Wykonawca oświadcza, iż posiada kwalifikacje i uprawnienia wymagane do prawidłowego wykonania przedmiotu umowy i zobowiązuje się do realizacji umowy w terminie oraz z należytą starannością, z uwzględnieniem profesjonalnego charakteru prowadzonej przez Wykonawcę działalności.
10. Wykonawca zobowiązuje się wykonać przedmiot umowy w najwyższej, jakości odpowiadającej najlepszym standardom rynkowym i potrzebom Zamawiającego.
11. Wykonawca ponosi pełną odpowiedzialność względem Zamawiającego za:
    1) Jakość, terminowość oraz bezpieczeństwo prac;

2) Szkody spowodowane z jego winy lub z winy innych podmiotów i osób fizycznych, którymi posługuje się przy wykonaniu lub przy okazji wykonywania zobowiązań wynikających z niniejszej umowy.

12. Wykonawca zobowiązuje się zaplanować i wykonywać prace związane z realizacją niniejszej umowy w taki sposób, by nie spowodowały one zakłóceń w pracy systemów komputerowych, które są użytkowane przez Zamawiającego,a w szczególności by nie uniemożliwiły ich użytkowania.
13. Zamawiający zobowiązuje się, w zakresie od niego zależnym, do zapewnienia Wykonawcy warunków do sprawnej i zgodnej z zasadami wynikającymi z niniejszej umowy realizacji przedmiotu umowy.

§ 4
Płatności

1. Wartość przedmiotu umowy określonego w § 1, Strony ustalają na kwotę netto ..... zł (słownie: .....), co wraz z podatkiem VAT stanowi łącznie ..... (.....) zł brutto.
2. Wartość Przedmiotu Umowy brutto obejmuje wszelkie koszty związane z realizacją umowy z uwzględnieniem podatku od towarów i usług VAT, innych opłat i podatków, opłat celnych, kosztów opakowań oraz ewentualnych upustów i rabatów, skalkulowanych z uwzględnieniem kosztów dostawy (transportu) do określonych umową lokalizacji, instalacji konfiguracji.
3. Zamawiający opłaci należność za wykonanie przedmiotu umowy na podstawie prawidłowo wystawionej przez Wykonawcę faktury VAT.
4. Wykonawca wystawi fakturę VAT, wskazując jako płatnika:

Komendę Główną Policji
02-624 Warszawa, ul. Puławska 148/150
NIP 521-31-72-762, REGON 012137497

5. Podstawę do wystawienia faktury VAT stanowi podpisany bez zastrzeżeń przez przedstawicieli Zamawiającego i Wykonawcy Protokół Odbioru Przedmiotu Umowy.
6. Płatność za realizację przedmiotu umowy dokonana będzie przelewem bankowym na rachunek Wykonawcy, wskazany na fakturze, w terminie 30 dni od daty dostarczenia faktury VAT do siedziby Biura Łączności i Informatyki KGP, ul. Wiśniowa 58, 02-520 Warszawa.
7. Za termin zapłaty przyjmuje się datę obciążenia przez bank rachunku Zamawiającego.
8. Zamawiający upoważnia Wykonawcę do wystawienia faktury VAT bez podpisu Zamawiającego.
9. Wszelkie rozliczenia finansowe między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
10. Przed zawarciem Umowy Wykonawca wniósł zabezpieczenie należytego wykonania umowy w wysokości 10% wartości brutto umowy tj. kwotę ..... złotych (słownie złotych: .....) w postaci gwarancji ubezpieczeniowej/pieniężnej
11. Zabezpieczenie należytego wykonania umowy zostanie zwrócone w następujących terminach:
    1) 70% zabezpieczenia należytego wykonania Umowy tj. kwotę ..... zł gwarantującą zgodnie z umową wykonanie całości Przedmiotu Umowy, w terminie 30 dni po ostatecznym, bezusterkowym odbiorze Przedmiotu Umowy,
    2) 30% zabezpieczenia należytego wykonania Umowy tj. kwotę ..... zł nie później niż 15 dni po upływie okresu rękojmi za wady dostarczonego sprzętu.
12. Wykonawca zobowiązuje się, że w przypadku wniesienia zabezpieczenia w gwarancjach bankowych lub ubezpieczeniowych, gwarancja bankowa lub ubezpieczeniowa będzie nieodwołalna, bezwarunkowa, płatna na każde pierwsze żądanie Zamawiającego.
13. Jeżeli z uwagi na przedłużenie terminu realizacji umowy, niezależnie od przyczyn tego przedłużenia, zabezpieczenie wniesione w formie gwarancji bankowych, ubezpieczeniowych lub poręczeniach wygasałoby przed upływem przedłużonego terminu realizacji umowy, Wykonawca na 7 dni roboczych przed wygaśnięciem tego zabezpieczenia przedstawi Zamawiającemu stosowny aneks do gwarancji/poręczenia lub nową gwarancję/poręczenie lub wpłaci odpowiednie zabezpieczenie w formie pieniądza. Jeżeli Wykonawca nie wypełni tego obowiązku Zamawiający może zażądać od gwaranta/poręczyciela wpłaty z gwarancji/poręczenia i zaliczyć uzyskaną w ten sposób kwotę na poczet zabezpieczenia.
14. Wykonawca oświadcza, że wyraża zgodę na bezpośrednie potrącenie przez Zamawiającego z zabezpieczenia wszelkich należności powstałych w wyniku niewykonania lub nienależytego wykonania umowy.

§ 5
Gwarancja i serwis

1. Wymagania gwarancyjne i serwisowe zawiera Załącznik nr 3 do Umowy.

§ 6
Własność i ryzyko przypadkowej utraty lub uszkodzenia

1. Tytuł własności, korzyści i ciężary oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia Infrastruktury sprzętowej i Oprogramowania wraz licencjami przechodzą na Zamawiającego z chwilą ich odbioru, potwierdzonej podpisanym przez Strony, bez uwag i zastrzeżeń ze strony Zamawiającego, Protokołu odbioru Przedmiotu Umowy.
2. W okresie pomiędzy przekazaniem Infrastruktury sprzętowej i Oprogramowania przez Wykonawcę Zamawiającemu, potwierdzonym podpisanym przez Strony Protokołu odbioru Przedmiotu Umowy a Dostawą Infrastruktury sprzętowej i Oprogramowania Wykonawca zobowiązany jest do przechowania Infrastruktury sprzętowej i Oprogramowania na własny koszt i ryzyko oraz do zapewnienia przestrzeni i warunków do ich przechowania.

§ 7
Kary

1. Wykonawca odpowiada za szkodę, wyrządzoną Zmawiającemu, w tym również za szkodę wyrządzoną przez osoby, którymi Wykonawca posłużył się przy wykonywaniu Umowy, chyba że szkoda została spowodowana działaniem siły wyższej, wyłączną winą Zamawiającego lub osoby trzeciej, za którą Wykonawca nie ponosi odpowiedzialności.
2. Wykonawca zobowiązuje się zapłacić Zamawiającemu następujące kary umowne:
   1) 10% wartości brutto Przedmiotu umowy w przypadku odstąpienia przez Zamawiającego lub Wykonawcę od Umowy w całości lub cześci z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy,
   2) 10% wartości brutto Przedmiotu umowy z tytułu niewykonania lub nienależytego wykonania Przedmiotu Umowy z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy,
   3) 0,15% wartości brutto Przedmiotu Umowy za każdy rozpoczęty dzień opóźnienia w wykonaniu przedmiotu umowy;
   4) 0,15 % wartości brutto Przedmiotu Umowy w przypadku przekroczenia czasu usunięcia awarii, za każdy rozpoczęty dzień opóźnienia w usunięciu awarii.
   5) 0,15% wartości brutto Przedmiotu umowy z tytułu przekroczenia wymaganego czasu naprawy gwarancyjnej o której mowa w Załączniku nr 3 za każdy dzień przekroczenia.
3. Zapłata kary umownej, o których mowa w ust. 2, pkt 2 i pkt 3 nie zwalnia Wykonawcy z obowiązku wykonania Przedmiotu Umowy.
4. Niezależnie od kar umownych określonych w ust. 2, Stronom przysługuje prawo dochodzenia odszkodowania na zasadach ogólnych prawa cywilnego, jeżeli poniesiona szkoda przekroczy wysokość zastrzeżonych kar umownych.
5. Prawo naliczenia kar umownych, o których mowa w ust. 2, nie ma zastosowania w przypadku, gdy opóźnienie wynika z winy Zamawiającego.
6. Kary umowne podlegają łączeniu.
7. Zamawiający jest uprawniony do potrącenia naliczonych kar umownych z wynagrodzenia przysługującego Wykonawcy. Doręczenie Wykonawcy wystawionej przez Zamawiającego noty obciążeniowej, w której określono: kwotę naliczonych kar umownych, podstawę ich naliczenia oraz wprowadzono oświadczenie o ich potrąceniu z wynagrodzenia, zastępuje wezwanie do zapłaty oraz oświadczenie Zamawiającego o potrąceniu kar umownych.
8. Żadna Strona nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań w ramach umowy, jeżeli takie niewykonanie lub nienależyte wykonanie jest wynikiem Siły Wyższej.
9. W rozumieniu umowy, „Siła Wyższa" oznacza okoliczności pozostające poza kontrolą Strony i uniemożliwiające lub znacznie utrudniające wykonanie przez tę Stronę jej zobowiązań, których nie można było przewidzieć w chwili zawierania umowy, ani im zapobiec przy dołożeniu należytej staranności.
10. Za Siłę Wyższą nie uznaje się niedotrzymania zobowiązań przez kontrahenta – dostawcę Wykonawcy.
11. W przypadku zaistnienia okoliczności Siły Wyższej, Strona, która powołuje się na te okoliczności, niezwłocznie zawiadomi druga Stronę na piśmie o jej zaistnieniu i przyczynach.
12. W razie zaistnienia Siły Wyższej wpływającej na termin realizacji umowy, Strony zobowiązują się w terminie 14 (czternastu) dni kalendarzowych od dnia zawiadomienia, o którym mowa w ust. 8, ustalić

nowy termin wykonania umowy lub ewentualnie podjąć decyzję o odstąpieniu od umowy za porozumieniem Stron.

§ 8
Zmiany umowy

1. Strony przewidują możliwość dokonywania zmian w treści umowy w stosunku do treści oferty Wykonawcy w sytuacji gdy:
   1) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań w zakresie oprogramowania, modelu/typu sprzętu w przypadku zakończenia produkcji i braku dostępności na rynku, pod warunkiem, że urządzenie będzie posiadało parametry nie gorsze od oferowanego modelu i nie spowoduje to podwyższenia ceny Umowy;
   2) po zawarciu umowy doszło do wydłużenia okresu gwarancyjnego przez producenta;
   3) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest korzystna dla Zamawiającego oraz konieczna w celu prawidłowego wykonania Umowy;
   4) wystąpiła zależność realizacji Przedmiotu Umowy od prac wykonywanych w ramach innych równoległe prowadzonych projektów teleinformatycznych.
   5) zachodzi konieczność zmiany terminu wykonania Przedmiotu Umowy w przypadku przedłużającej się procedury udzielenia zamówienia publicznego na skutek korzystania przez Wykonawców ze środków ochrony prawnej,
   6) nastąpiło istotne opóźnienie powstałe z winy Zamawiającego związane z realizacją Umowy, którego nie można było przewidzieć, a które w znaczący sposób wpływa na termin wykonania Umowy.
2. Zmiany, o których mowa w ust. 1, wymagają zgody obu stron i muszą być dokonywane w formie pisemnej pod rygorem nieważności w postaci aneksu.

§ 9
Licencje na Oprogramowanie Standardowe

1. Wykonawca oświadcza i gwarantuje, iż z chwilą podpisania Protokołu odbioru ilościowego Skarb Państwa - Zamawiający, w ramach wynagrodzenia wskazanego w § 4 ust. 1 Umowy uzyskuje prawo do korzystania z oprogramowania, wraz z niezbędną do korzystania z oprogramowania dokumentacją oraz ich aktualizacji na podstawie niewyłącznej, nieograniczonej terytorialnie licencji udzielonej przez producenta oprogramowania, której warunki tenże producent dołączył do licencji oprogramowania jednak nie gorsze niż wynikające z Umowy.
2. Z chwilą udzielenia licencji na korzystanie z oprogramowania, własność nośników, na których utrwalono oprogramowanie przechodzi na Zamawiającego.
3. W okresie od dnia dostarczenia do Zamawiającego Przedmiotu umowy w sposób określony w Umowie do dnia podpisania protokołu odbioru ilościowego Wykonawca zapewni Zamawiającemu korzystanie z oprogramowania na warunkach licencji zgodnie z Załącznikiem nr 1 do Umowy, bez pobierania z tego tytułu dodatkowego wynagrodzenia.
4. Wykonawca oświadcza i gwarantuje, że oprogramowanie, ani korzystanie z niego przez Zamawiającego, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów, ani praw do baz danych.
5. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z nabytym oprogramowaniem, w tym zarzucających naruszenie praw własności intelektualnej, Wykonawca podejmie wszelkie działania mające na celu zażegnanie sporu i poniesie w związku z tym wszelkie koszty, w tym koszty zastępstwa procesowego od chwili zgłoszenia roszczenia oraz koszty odszkodowań. W szczególności, w razie wytoczenia przeciwko Zamawiającemu powództwa z tytułu naruszenia praw własności intelektualnej, Wykonawca wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie Zamawiającego.
6. Ponadto, jeśli używane oprogramowanie stanie się przedmiotem jakiegokolwiek powództwa Strony lub osoby trzeciej o naruszenie praw własności intelektualnej, jak wymieniono powyżej, Wykonawca może na swój własny koszt wybrać jedno z poniższych rozwiązań:
   1) uzyskać dla Zamawiającego prawo dalszego użytkowania oprogramowania lub
   2) zmodyfikować oprogramowanie tak, żeby było zgodne z Umową, ale wolne od jakichkolwiek wad lub roszczeń osób trzecich.
7. Strony potwierdzają, że żadne z powyższych postanowień nie wyłącza:
   1) możliwości dochodzenia przez Zamawiającego odszkodowania na zasadach ogólnych kodeksu cywilnego lub wykonania uprawnień przez Zamawiającego wynikających z innych ustaw, ani
   2) dochodzenia odpowiedzialności z innych tytułów określonych w Umowie, a w szczególności jej §7.

§ 10
Inne postanowienia

1. Przy prowadzeniu korespondencji w sprawach związanych z realizacją przedmiotu umowy obowiązywać będzie forma pisemna.
2. W razie pilnej potrzeby zawiadomienia mogą być przesyłane faksem z pisemnym potwierdzeniem ich otrzymania.
3. Ustala się następujące adresy, numery faksów i telefonów:
   Adres Wykonawcy dla potrzeb korespondencji i składania zawiadomień:

   .....
   .....
   .....
   Tel. .....
   Fax. .....

   Adres Zamawiającego dla potrzeb korespondencji i składania zawiadomień:

   Biuro Łączności i Informatyki KGP
   02-520 Warszawa, ul. Wiśniowa 58
   tel. /22/ 60-141-90,
   fax./22/ 60-158-73

§ 11
Odstąpienie od Umowy

1. Zamawiający zastrzega sobie prawo do odstąpienia od Umowy w przypadku:
   1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy;
   2) w przypadku gdy opóźnienie Wykonawcy w stosunku do terminów, o których mowa w § 3 ust. 1 Umowy przekroczy 3 Dni Robocze;
   3) dostarczenia przez Wykonawcę Elementów Systemu niespełniających wymogów określonych w Dokumentacji,
   4) w przypadku dostarczenia Dokumentacji w sposób niezgodny z Umową,
   5) w przypadku gdy Wykonawca będzie wykonywał prace w sposób wadliwy albo sprzeczny z Umową.
2. Odstąpienie lub wypowiedzenie od umowy powinno nastąpić poprzez złożenie stosownego oświadczenia woli w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie. Odstąpienie lub wypowiedzenie wywołuje skutki z chwilą doręczenia, z tym, że dla zachowania terminu na odstąpienie wystarczy wysłanie oświadczenia o odstąpieniu przesyłką rejestrowaną na adres Strony przeciwnej wskazany w komparycji umowy albo na aktualny adres KRS.
3. Odstąpienie od umowy nie powoduje wygaśnięcia roszczeń o zapłatę kar umownych powstałych w czasie obowiązywania umowy (w tym roszczenia o zapłatę kary umownej z powodu odstąpienia od umowy).

§ 12
Poufność

1. W przypadku konieczności przekazania Wykonawcy informacji niejawnych, w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. nr 182, poz. 1228), Zamawiający zobowiązany jest niezwłocznie do pisemnego powiadomienia Wykonawcy o rodzaju informacji niejawnych, które zamierza przekazać oraz zastosowanej klauzuli tajności.
2. Wykonawca zobowiązany jest do przestrzegania zasad postępowania z informacjami niejawnymi oraz przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. nr 182, poz. 1228).
3. Wykonawcy nie wolno, bez uprzedniej pisemnej zgody Zamawiającego, ujawnić treści Umowy ani jakiejkolwiek specyfikacji, planu, rysunku, wzoru, lub informacji dostarczonej przez Zamawiającego lub na jego rzecz w związku z tą Umową, jakiejkolwiek osobie trzeciej.
4. Wykonawcy nie wolno, bez uprzedniej pisemnej zgody Zamawiającego, wykorzystywać jakichkolwiek dokumentów, do których ma dostęp w wyniku realizacji Umowy, w innych celach niż do jej realizacji.
5. Jakiekolwiek dokumenty inne niż Umowa, pozostają własnością Zamawiającego i podlegają zwrotowi na żądanie Zamawiającego wraz ze wszystkimi kopiami oraz nośnikami, na których dokumenty zostały zapisane w wersji elektronicznej po zakończeniu realizacji Umowy.

6. Strony zobowiązują się do zachowania poufności informacji oznaczonych jako poufne, w posiadanie których Strona wejdzie w trakcie wykonywania Umowy, oraz nie wykorzystywania ich do innych celów niż wykonywanie czynności wynikających z Umowy.
7. Obowiązek zachowania poufności nie dotyczy informacji powszechnie znanych oraz udostępniania informacji na żądanie sądu, prokuratury, organów podatkowych lub organów kontrolnych oraz wynikających z obowiązków informacyjnych w zakresie w szczególności przewidzianym przez ustawę z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz. U. 2009 r. Nr 185 poz. 1439 ze zm.), ustawę z dnia z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. 2010 r. Nr 211 poz. 1384) oraz przez ustawę z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym (Dz. U. 2005 r. Nr 184 poz. 1537 ze zm.) oraz ustawę z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. 2009 r. Nr 157, poz. 1240 ze zm.) i ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2001 nr 112poz. 1198 ze zm.).
8. Z zastrzeżeniem innych postanowień Umowy, zobowiązanie do zachowania poufności obejmuje:
   1) zakaz kopiowania i powielania informacji poufnych otrzymanych od drugiej Strony (a w przypadku Zamawiającego także informacji otrzymanych od podwykonawców Wykonawcy) jakąkolwiek techniką,

   2) zakaz informowania w sposób pośredni ani bezpośredni jakichkolwiek osób nieupoważnionych o fakcie posiadania informacji poufnych otrzymanych od drugiej Strony (a w przypadku Zamawiającego także informacji otrzymanych od podwykonawców Wykonawcy) i ich treści,

   3) zakaz przekazywania i udostępniania informacji poufnych otrzymanych od drugiej Strony (a w przypadku Zamawiającego także informacji otrzymanych od podwykonawców Wykonawcy) w sposób pośredni lub bezpośredni osobom nieupoważnionym,

   4) zapewnienie pełnego bezpieczeństwa posiadanych informacji poufnych otrzymanych od drugiej Strony (a w przypadku Zamawiającego także informacji otrzymanych od podwykonawców Wykonawcy) przed dostępem osób trzecich, zwłaszcza poprzez odpowiednie ich przechowywanie zabezpieczające przed zapoznaniem się z ich treścią, skopiowaniem lub zabraniem przez osoby nieupoważnione.

   5) Wykonawca uprawniony jest do przekazywania informacji poufnych swoim podwykonawcom w zakresie koniecznym do realizacji Umowy, co do których Zamawiający wyraził zgodę.

   6) Wykonawca przed zawarciem Umowy przedstawi Zamawiającemu do akceptacji listę osób z jego strony uprawnionych do realizacji Umowy W celu zapewnienia kontroli osób uzyskujących dostęp do policyjnych zasobów, w tym aktywów teleinformatycznych, Wykonawca wraz z listą osób dostarczy:

   a) dla każdej osoby zgłoszonej do realizacji Umowy kserokopię aktualnego zaświadczenia o niekaralności potwierdzonego za zgodność z oryginałem wystawionego nie wcześniej niż 3 miesiące przed dniem zawarcia Umowy lub alternatywnie dokument elektronicznie wygenerowany przez system e-Platforma Ministerstwa Sprawiedliwości. Kierowane do Krajowego Rejestru Karnego zapytanie o udzielenie informacji o osobie, powinno dotyczyć kartoteki karnej. Ponadto w ww. formularzu nie należy wypełniać pkt 11 pn. *Wskazanie postępowania, w związku z którym zachodzi potrzeba uzyskania informacji o osobie;*
   b) oświadczenie o zachowaniu poufności dla każdej osoby realizującej Umowę którego wzór określa załącznik nr 9 do Umowy.
   7) Zamawiający dopuści do realizacji Przedmiotu umowy jedynie osoby spełniające powyższe wymogi. Zamawiający dopuszcza zmianę listy osób wykonujących czynności serwisowe. Warunkiem akceptacji przez Zamawiającego nowej listy jest spełnienie wymogu, o którym mowa w ust. 6

   8) Postanowienia niniejszego paragrafu dotyczą również podwykonawców.

§ 13
Postanowienia końcowe

1. Wszelkie należności Wykonawcy wynikające z umowy objęte są zakazem sprzedaży oraz cesji wierzytelności (w tym również odsetek) i nie mogą być przelane na rzecz osób trzecich bez pisemnej zgody Zamawiającego.
2. W sprawach nieuregulowanych umową stosuje się przepisy Kodeksu Cywilnego, ustawy Prawo Zamówień Publicznych.
3. Sądem właściwym dla Stron umowy jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający i 1 (jeden) egzemplarz otrzymuje Wykonawca.
5. Załączniki stanowiące integralną część umowy:
   1) Załącznik nr 1 – Szczegółowy opis przedmiotu umowy;
   2) Załącznik nr 2 – Zasady odbioru przedmiotu umowy;
   3) Załącznik nr 3 – Wymagania gwarancyjne i serwisowe;
   4) Załącznik nr 4 – Wymagania w zakresie warsztatu szkoleniowego;
   5) Załącznik nr 5 - Specyfikacja ilościowo - cenowa
   6) Załącznik nr 6 - Protokół odbioru jakościowego - wzór;
   7) Załącznik nr 7 – Protokół odbioru ilościowego – wzór;
   8) Załącznik nr 8 – Protokół odbioru przedmiotu umowy – wzór.
   9) Załącznik nr 9 – Oświadczenie o zachowaniu poufności - wzór
6. W przypadku zaistnienia jakichkolwiek rozbieżności pomiędzy postanowieniami zawartymi w załącznikach a warunkami ustalonymi w umowie, wiążące są postanowienia umowy.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 2

ZASADY ODBIORU PRZEDMIOTU UMOWY

a. Zasady odbioru.

1. O przygotowaniu do odbioru Przedmiotu umowy Wykonawca powiadomi Kierownika Projektu Zamawiającego drogą mailową albo na nr faksu 22 60-158-73 z co najmniej trzy (3) dniowym (dni robocze) wyprzedzeniem, podając:

- numer Umowy,
- planowaną datę przystąpienia do odbioru

2. Zamawiający przystąpi do odbioru Przedmiotu umowy w ciągu pięciu (3) Dni Roboczych od otrzymania od Wykonawcy zgłoszenia gotowości do odbioru.
3. Odbiór zostanie przeprowadzony w obiekcie wskazanym przez Zamawiającego na terenie miasta Warszawy w obecności przedstawicieli Wykonawcy.
4. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego (Komisja do odbioru przedmiotu zamówienia) i Wykonawcy Protokołu odbioru produktu przedmiotu umowy, którego wzór stanowi **Załącznik nr 8 do Umowy**.
5. Przedmiot umowy podlega odbiorowi jakościowemu, odbiorowi ilościowemu, odbiorowi warsztatów szkoleniowych i odbiorowi przedmiotu umowy.
6. Wykonawca przed przystąpieniem do odbioru zobowiązany jest do wypełnienia i dostarczenia Zamawiającemu protokołów o których mowa w **załączniku nr 2 do umowy**.
7. Czynności związane z odbiorami muszą się zakończyć w terminie realizacji Umowy określonym w § 3 ust. 1 Umowy.
8. Wszystkie protokoły, sporządzone zostaną w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający i 1 (jeden) egzemplarz otrzymuje Wykonawca.

1. Odbiór jakościowy.

1. Celem czynności kontrolnych prowadzonych w ramach odbioru jakościowego jest sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy, wyszczególnionym w Załączniku nr 1 do Umowy.
2. Podstawą dokonania odbioru jakościowego jest przeprowadzenie z pozytywnym skutkiem zaakceptowanych przez Zamawiającego Testów akceptacyjnych dla Systemu.
3. Pozytywny wynik odbioru jakościowego zostanie potwierdzony podpisaniem protokołu odbioru jakościowego, który stanowi Załącznik nr 6 do Umowy.

1. Odbiór ilościowy

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowego jest sprawdzenie kompletności dostarczonego przedmiotu umowy i potwierdzenie zgodności z ilością określoną w umowie.

2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego Przedmiotu Umowy.

3. Pozytywny wynik odbioru ilościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowego, którego wzór określa Załącznik nr 7 do umowy.

2. Odbiór produktu przedmiotu umowy

1. Odbiór przedmiotu umowy kończy procedurę odbioru Przedmiotu Umowy.

2. Protokół Odbioru przedmiotu umowy, stanowiący Załącznik nr 8 do Umowy, zostanie podpisany przez przedstawicieli Zamawiającego i Wykonawcy po dokonaniu odbioru jakościowego i odbioru ilościowego z wynikiem pozytywnym.

Załącznik nr 3 do projektu Umowy

WYMAGANIA GWARANCYJNE I SERWISOWE

Warunki Ogólne

1. Usługę wsparcia technicznego Wykonawca będzie świadczył od dnia podpisania bez zastrzeżeń stosownego Protokołu Odbioru Przedmiotu Umowy i (wzór stanowi Załącznik nr 9).
2. Całość prac związanych z fizycznym dostępem do serwisowanego oprogramowania oraz urządzeń będzie przeprowadzana przez autoryzowany serwis wykonawcy.
3. W okresie świadczenia usługi Wykonawca zapewni stały kontakt w celu udzielania nieodpłatnych konsultacji i pomocy technicznej w dni robocze, w godz. 8:00-18:00. Należy podać kontakt do punktu konsultacyjnego (telefon, imię i nazwisko konsultanta).
4. Zgłoszenia o awariach i nieprawidłowościach przyjmowane będą przez 24 godziny, 7 dni w tygodniu.
5. Zgłoszenia awarii drogą mailową w godzinach od 18:00 do 8:00 muszą być potwierdzane telefonicznie przez Zgłaszającego.
6. Reakcja serwisu rozumiana jako przystąpienie do usunięcia awarii lub zaistniałych nieprawidłowości nastąpi nie później niż 2 godzin od momentu zgłoszenia przez zamawiającego drogą telefoniczną lub faksową do siedziby serwisu.

Warunki Szczególne

I. Zadanie nr 1

1. Wykonawca udzieli 12 miesięcznego wsparcia technicznego dla dostarczonych modułów SFP+.
2. Wsparcie będzie świadczone na zasadach standardowego wsparcia technicznego producenta.

II. Zadanie nr 2

1. Wykonawca udzieli minimum 12 miesięcznego wsparcia technicznego dla dostarczonych modułów pamięci operacyjnej RAM.
2. Wsparcie będzie świadczone na zasadach standardowego wsparcia technicznego producenta.

III. Zadanie nr 3

1. Wykonawca udzieli 12 miesięcznego wsparcia technicznego dla zakupionego systemu zabezpieczającego środowisko VMware.
2. Wsparcie techniczne będzie świadczone na zasadach wsparcia technicznego Silver Premium Service Program lub równoważnym zgodnie z Opisem Przedmiotu Zamówienia.
3. Wykonawca będzie niezwłocznie informował Zamawiającego o ukazaniu się nowych, stabilnych wersji produktu.

IV. Zadanie nr 4

1. Wykonawca udzieli 36 miesięcznego wsparcia technicznego dla zakupionego oprogramowania do monitorowania i zarządzania siecią komputerową.
2. Wsparcie będzie świadczone na zasadach standardowego wsparcia technicznego producenta.

V. Zadanie nr 5

1. Wykonawca udzieli 12 miesięcznego wsparcia technicznego dla dostarczonego systemu ochronnego typu Next-Generation Firewall z funkcjonalnością Next-Generation IPS.
2. Wsparcie techniczne będzie świadczone na zasadach standardowego wsparcia technicznego producenta.

VI Zadanie nr 6

1. Wykonawca udzieli 12 miesięcznego wsparcia technicznego dla dostarczonego systemu zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i typu zero-day.
2. Wsparcie techniczne będzie świadczone na zasadach standardowego wsparcia technicznego producenta.

Załącznik nr 4 do projektu umowy

WYMAGANIA W ZAKRESIE WARSZTATU SZKOLENIOWEGO

W ramach realizacji projektu Wykonawca przeprowadzi 3 warsztaty szkoleniowe (zakres wymieniony w załączniku nr 1)dla 6 osób zarówno z zakresu wdrożenia, obsługi i administracji urządzenia.

Zakres warsztatu szkoleniowego musi obejmować:
- możliwe warianty wdrożenia, konfiguracji
- zagadnienia związane z zarządzaniem i eksploatacją,
- obsługę systemu
- administrację systemem

Ogólnym założeniem celu przygotowanie pracowników i funkcjonariuszy Policji do samodzielnej obsługi Systemu w pełnym zakresie.

Wykonawca dostarczy również Zamawiającemu w postaci elektronicznej (z prawem do powielania i modyfikacji) podręczniki oraz inne materiały na te warsztaty szkoleniowe.

Ponadto wymienione wyżej warsztaty szkoleniowe będą się opierały na określonych poniżej ogólnych założeniach:

1. Wykonawca opracuje Plan warsztatu szkoleniowego
2. Plan, o którym mowa w pkt 1, Wykonawca przedstawi do akceptacji Zamawiającego w terminie 7 Dni Roboczych przed planowanym rozpoczęciem warsztatu szkoleniowego.
3. Wykonawca zobowiązany jest do zorganizowania i przeprowadzenia warsztatu szkoleniowego, zgodnie z zatwierdzonym Planem szkoleń.
4. Wszystkie szkolenia będą prowadzone w języku polskim na terytorium RP.
5. Wykonawca zapewni i przekaże uczestnikom warsztatu szkoleniowego odpowiednią dokumentację w języku polskim.
6. Wykonawca pokryje wszelkie koszty związane ze warsztatem szkoleniowym.
7. Wykonawca planuje realizacje warsztatu szkoleniowego na terenie Warszawy, jednakże jeżeli z jakichś powodów warsztat szkoleniowy odbędzie się poza terenem Warszawy wówczas Wykonawca zapewni uczestnikom zakwaterowanie w pokojach 1- osobowych oraz całodniowe wyżywienie (ciepły posiłek oraz napoje)..
8. Zamawiający określi na co należy zwrócić szczególną uwagę po zapoznaniu się z programem warsztatu szkoleniowego przedstawionym przez Wykonawcę.
9. Zamawiający zapewni, że w warsztatach szkoleniowych o poszczególnych profilach wezmą udział odpowiedni Użytkownicy.
10. Wykonawca zapewni, aby warsztaty szkoleniowe przeprowadzone zostały przez wykwalifikowaną kadrę szkoleniową posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia.
11. Wykonawca wystawi dla uczestników warsztatu szkoleniowego imienne zaświadczenia potwierdzające, że nabyli wiedzę zgodną z celem warsztatu szkoleniowego.

Załącznik nr 5
do projektu umowy

Specyfikacja ilościowo - cenowa

L.p.	Produkt	Ilość	VAT	Cena jednostkowa brutto	Wartość netto	Wartość brutto
1.						
2.						
3.						
4.						

Razem:		

Załącznik nr 6
do projektu umowy

PROTOKÓŁ ODBIORU JAKOŚCIOWEGO - wzór

Miejsce dokonania odbioru:

.....
Data dokonania odbioru:

.....
Ze strony Wykonawcy:

.....
(nazwa i adres)

.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)

W ramach odbioru jakościowego, przeprowadzonego w ramach umowy nr ..... z dnia..... 2015r. na _____, Komisja powołana na mocy Decyzji _____ z dnia _____2015r. przeprowadziła czynności kontrolne na podstawie zatwierdzonej przez Strony umowy procedury i potwierdza zgodność jakości dostarczonego produktu z parametrami/funkcjonalnością zawartymi w opisie przedmiotu umowy.

Wynik odbioru jakościowego:
a) Pozytywny*
b) Negatywny*

Uwagi:.....
.....
.....

Podpisy Komisji do odbioru przedmiotu zamówienia:

Przewodniczący:
.....

Członkowie:

1. .....
2. .....
3.....
(członkowie Komisji Przetargowej,

1.....
2.....
3.....
(Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 7
do projektu umowy

PROTOKÓŁ ODBIORU ILOŚCIOWEGO – wzór

Miejsce dokonania odbioru:

.....

Data dokonania odbioru:

.....

Ze strony Wykonawcy:

.....
(nazwa i adres)

.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:

.....
(nazwa i adres)

Przedmiotem odbioru ilościowego przeprowadzonego w ramach przedmiotowej umowy jest:

Lp.	Nazwa przedmiotu	Jednostka miary	Ilość	Nr seryjny	Wartość jednostkowa [netto]	Wartość łączna [brutto]	Dokumentacja techniczna/ instrukcja obsługi/świadectwo jakości	Uwagi
				Razem:				

Komisja do odbioru przedmiotu zamówienia, powołana na mocy ..... z dnia .....
przeprowadziła czynności kontrolne i potwierdza/nie potwierdza kompletność dostarczonego produktu. *
Uwagi:.....
.....
.....

Podpisy:

1. .....
2. .....
3.....

(w imieniu Zamawiającego)

1.....
2.....
3.....

(Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 8
do projektu umowy

PROTOKÓŁ ODBIORU PRZEDMIOTU UMOWY - wzór
do umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:

.....
Data dokonania odbioru:

.....
Ze strony Wykonawcy:

.....
(nazwa i adres)

.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)

Komisja do obioru przedmiotu zamówienia w składzie:
1.....

2. .....

3. .....

na podstawie przeprowadzonych czynności kontrolnych oraz Protokołów odbioru jakościowego / odbioru ilościowego / odbioru szkolenia / odbioru dokumentacji *, dostarczonych przez jednostki terenowe Policji* potwierdza:
1. kompletność dostarczonego przedmiotu umowy;*
2. zgodność jakości dostarczonego przedmiotu umowy;* z parametrami/funkcjonalnością z opisem przedmiotu umowy;*
3. wykonanie zamówienia zgodne z warunkami zawartymi w umowie.

Uwagi.....
.....
Podpisy Komisji do odbioru przedmiotu zamówienia:
Przewodniczący:

.....

Członkowie:

1. .....

2. .....

3.....
(ze strony Zamawiającego)

1.....

2.....

3.....
(ze strony Wykonawcy)

*niewłaściwe skreślić