**Numer sprawy: 13/2017 Załącznik nr 1c do SIWZ / Załącznik nr 1c do Umowy**

**OPIS PRZEDMIOTU ZAMÓWIENIA – zwany OPZ DLA CZĘŚCI 3.**

**I. Przedmiot zamówienia.**

1. Przedmiotem zamówienia jest **Dostawa oprogramowania dla Urzędu Pracy m.st. Warszawy.**
2. Definicje OPZ:
3. **Wykonawca** – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.
4. **Zamawiający** – Miasto st. Warszawa – Urząd Pracy m.st. Warszawy.
5. **Opiekun ze strony Zamawiającego lub Opiekun ze strony Wykonawcy,** zwany również Opiekunem – osoba upoważniona do kontaktów, wskazana w umowie.
6. **Wada** – cecha oprogramowania obniżająca właściwości funkcjonalne, objawiająca się poprzez brak pewnych funkcji, niższą wydajność lub niższą niezawodność pracy w porównaniu z oprogramowaniem pozbawionym wady. Wada może powodować utratę lub uszkodzenie danych. Za wadę uznaje się również niespełnianie przez oprogramowanie wymagań określonych w pkt III. OPZ dla części 3 – Warunki szczegółowe.
7. Zapotrzebowanie na oprogramowanie zostało opisane w pkt III. OPZ dla części 3 - Warunki szczegółowe.

**II. Warunki realizacji umowy** – Wymagania ogólne.

1. Wykonawca, co najmniej na 1 dzień przed planowaną dostawą, poinformuje Opiekuna ze strony Zamawiającego o terminie dostawy oprogramowania.
2. Dostawa/y oprogramowania realizowana/e będzie/będą do siedziby Urzędu Pracy m.st. Warszawy przy ul. Grochowskiej 171B w Warszawie. Oprogramowanie, gdzie producent przewiduje jedynie jego postać elektroniczną, Wykonawca dostarczy w postaci elektronicznej lub spowoduje, aby producent oprogramowania przesłał je do Opiekuna ze strony Zamawiającego na wskazany adres poczty elektronicznej, niezwłocznie po udzieleniu licencji na oprogramowanie lub po dokonaniu aktywacji przedłużenia wsparcia oprogramowania.
3. Wykonawca zrealizuje przedmiot zamówienia w ramach wynagrodzenia określonego w umowie w terminie określonym w umowie. Dostawy oprogramowania w postaci fizycznej realizowane będą w dni robocze, w godzinach 8:00 – 15:45.
4. Wykonawca dostarczy oprogramowanie spełniające wszystkie wymagania dotyczące bezpieczeństwa, określone w obowiązującym w Polsce prawie.
5. Zaoferowane oprogramowanie musi być ogólnodostępne na rynku oraz musi być w najnowszej wersji dostępnej na rynku na dzień składania ofert.
6. Oprogramowanie musi pochodzić z autoryzowanego kanału sprzedaży producenta i musi być dostarczone w formie licencji na warunkach producenta. Przedłużenie wsparcia na oprogramowanie musi pochodzić z autoryzowanego kanału sprzedaży producenta i musi być dostarczone na warunkach producenta oprogramowania.
7. Zamawiający wymaga dostarczenia oprogramowania przeznaczonego do użytkowania przez podmioty komercyjne lub instytucje rządowe i samorządowe, ponieważ Zamawiający jest jednostką samorządową. Oprogramowanie należy dostarczyć w formie przewidzianej przez producenta oprogramowania (np. nośniki magnetyczne, licencje papierowe, klucze dostępu, linki umożliwiające pobranie oprogramowania).
8. Okres użytkowania oprogramowania wyszczególnionego w pkt III. OPZ dla części 3 musi być bezterminowy, z wyłączeniem przypadków opisanych jako terminowe. Zaoferowane oprogramowanie musi być licencjonowane w formie licencji grupowych lub licencji pudełkowych, o ile nie określono innego typu licencjonowania w pkt III. OPZ dla części 3.
	1. **Warunki szczegółowe:**

|  |  |
| --- | --- |
| **Poz. 1. Oprogramowanie antywirusowe**  | **Ilość – 1 komplet** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania:** aktualizacja oprogramowania antywirusowego ESET Endpoint Antivirus Suite dla 310 stacji roboczych i serwerów, w tym liczba serwerów nie przekroczy 25.lub oprogramowanie równoważne spełniające następujące wymagania:Liczba stacji roboczych i laptopów opartych na systemie Windows i urządzeń mobilnych opartych na systemie Android objętych licencją: co najmniej 285 szt.Liczba serwerów plików objętych licencją: co najmniej 25 szt. (ochrona w zakresie plików udostępnianych klientom oraz lokalna ochrona systemu operacyjnego serwera).W ramach licencji, możliwość instalacji minimum 1 serwera do zarządzania oraz minimum 2 serwerów proxy, do minimalizowania ruchu sieciowego systemu antywirusowego pomiędzy lokalizacjami lub innego rozwiązania do zarządzania systemem, zapewniającego minimalizację ruchu sieciowego pomiędzy trzema lokalizacjami do serwera zarządzania.Pełna ochrona przed oprogramowaniem typu: wirusy komputerowe, trojany, robaki i inne zagrożenia.Wykrywanie i usuwanie niebezpiecznego oprogramowania typu: adware, spyware, dialer, phishing, narzędzia hakerskie, backdor, rootkit, narzędzia do szyfrowania dysków,Wykrywanie zagrożeń w czasie rzeczywistym, skanowanie plików na żądanie użytkownika, skanowanie zgodnie z harmonogramem lub w trakcie nieaktywności użytkownika.Ochrona plików, poczty przychodzącej i wychodzącej na poziomie stacji roboczej obsługiwanej przy pomocy programów pocztowych, co najmniej MS Outlook. Ochrona realizowana za pomocą automatycznej integracji odpowiednich modułów z programem pocztowym, bez konieczności dodatkowej konfiguracji, wraz z funkcją automatycznej zmiany rozszerzeń potencjalnie niebezpiecznych załączników.Ochrona w czasie rzeczywistym ruchu HTTP, HTTPS na poziomie stacji roboczej. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. Ochrona realizowana za pomocą automatycznej integracji odpowiednich modułów z przeglądarką internetową, bez konieczności dodatkowej konfiguracji wraz z możliwością definiowania odpowiednich wykluczeń.Małe obciążenie systemu stacji roboczej pracą oprogramowania antywirusowego.Możliwość blokowania co najmniej zewnętrznych nośników danych (pendrive).Możliwość definiowania, z poziomu konsoli centralnego zarządzania, polis dla ochrony czasu rzeczywistego i skanowania plików, dla poszczególnych grup komputerów, zawierająca co najmniej ustawienia: lista skanowanych napędów (wszystkie napędy lokalne, wszystkie napędy wymienne, wszystkie napędy sieciowe, itp.), sposób identyfikacji plików (wszystkie pliki, bazujący na rozszerzeniach, itp.), załączenie/wyłączenie skanowania archiwów, definicja wykluczeń ze skanowania, załączenie lub wyłączenie skanowania heurystycznego wraz ze zdefiniowaniem głębokości skanowania heurystycznego, tryb pracy oprogramowania antywirusowego (skanowanie przy dostępie do pliku, skanowanie przy wykonaniu pliku, itp.).Możliwość definiowania, z poziomu konsoli centralnego zarządzania, polis dla ochrony poczty przychodzącej i wychodzącej, dla poszczególnych grup komputerów, zawierająca co najmniej ustawienia: skanowanie załączników w zakresie załącz/wyłącz oraz określenie maksymalnego rozmiaru skanowanych archiwów, definicja poziomu skanowania heurystycznego w zakresie załącz/wyłącz oraz poziom skanowania heurystycznego, ochrona przed potencjalnie niebezpiecznymi załącznikami w zakresie usuwania ich z emaila lub/i zmiany rozszerzenia wraz z możliwością zdefiniowania rozszerzeń potencjalnie niebezpiecznych załączników.Możliwość definiowania, z poziomu konsoli centralnego zarządzania, polis dla ochrony HTTP i HTTPS, dla poszczególnych grup komputerów, zawierająca co najmniej ustawienia: definicja poziomu skanowania heurystycznego w zakresie załącz/wyłącz oraz poziom skanowania heurystycznego, załączenie/wyłączenie funkcji sprawdzających, czy adres nie jest zawarty w bazie danych potencjalnie niebezpiecznych stron, definicja wykluczeń - listy adresów IP i URL, które mają nie podlegać sprawdzaniu.Możliwość definiowania, z poziomu konsoli centralnego zarządzania, polis dla poszczególnych grup komputerów, definiująca załączenie/wyłączenie poszczególnych modułów oprogramowania (skanowanie antywirusowe, skanowanie poczty email, skanowanie stron WWW).Możliwość zablokowania, z konsoli centralnego zarządzania, możliwości modyfikacji ustawień oprogramowania antywirusowego przez użytkownika zalogowanego na stacji roboczej.Możliwość zdefiniowania hasła umożliwiającego odinstalowanie zainstalowanego na stacji roboczej oprogramowania antywirusowego i zabezpieczającego oprogramowanie przed samowolnym jego odinstalowaniem przez użytkownika.Cykliczna aktualizacja oprogramowania antywirusowego z możliwością pobierania aktualizacji z serwerów producenta oprogramowania oraz z serwerów do centralnego zarządzania i wewnętrznych serwerów proxy, aktualizacja inicjowana według harmonogramu oraz na żądanie. Producent oprogramowania musi publikować aktualizacje baz sygnatur co najmniej sześć razy dziennie.Możliwość, z poziomu konsoli centralnego zarządzania, uzyskania szczegółowej informacji o stanie zabezpieczenia poszczególnych stacji roboczych w zakresie terminu ostatniej aktualizacji baz sygnatur, ostatniego pełnego skanowania, ostatniej aktualizacji danych wraz z automatycznym wyróżnianiem na konsoli stacji roboczych, które od pewnego czasu nie komunikowały się z serwerem centralnego zarządzania lub mają nieaktualne bazy sygnatur.Możliwość, z poziomu konsoli centralnego zarządzania, ręcznego inicjowania zadań aktualizacji, skanowania plików dla poszczególnych stacji roboczych.Możliwość, z poziomu konsoli, centralnego zarządzania ręcznego inicjowania zadań aktualizacji kluczy licencyjnych, instalacji pakietu oprogramowania antywirusowego, usunięcia zainstalowanego oprogramowania antywirusowego.Cykliczne generowanie raportów i dostarczanie ich na zdefiniowane adresy email administratorów oraz generowanie raportów na żądanie administratora przez serwer do centralnego zarządzania o: wykrytym oprogramowaniu szkodliwym, wraz ze wskazaniem nazw stacji roboczych, gdzie oprogramowanie zostało wykryte, wersjach baz sygnatur i wersjach oprogramowania antywirusowego, ze wskazaniem nazw stacji roboczych, na których występują określone wersje oprogramowania, zainstalowanym innym oprogramowaniu.Oprogramowanie wyposażone w standardowy moduł wykrywania zagrożeń za pomocą sygnatur dostarczanych przez producenta oprogramowania oraz, w co najmniej jeden moduł heurystyczny, umożliwiający wykrywanie nieznanych zagrożeń oraz w technikę uczenia maszynowego i obserwacji uruchomionych w systemie procesów.Moduł skanujący musi pochodzić od innego producenta, w porównaniu do modułów skanujących zaoferowanego oprogramowania antywirusowego dla serwera poczty, o którym mowa w poz. 2.W przypadku oprogramowania równoważnego, należy zapewnić szkolenie z zakresu instalacji, wdrożenia i obsługi konsoli do centralnego zarządzania oprogramowaniem dla minimum 2 informatyków oraz należy zapewnić pomoc w sprawnym wdrożeniu oprogramowania w dniu 01.01.2018. W przypadku braku możliwości zapewnienia wsparcia we wdrożeniu oprogramowania równoważnego w dniu 01.01.2018, należy zapewnić odpowiednio dłuższy okres aktualizacji oprogramowania równoważnego tak, aby było możliwe płynne zastąpienie aktualnie eksploatowanego oprogramowania, oprogramowaniem równoważnym w terminie do 01.01.2018r. bez przesunięcia daty końca ważności o której mowa w wierszu 4. |
| 2. | **Obsługiwane systemy operacyjne:** Dla stacji roboczych co najmniej Windows 7 w wersji 32 i 64 bitowej, Windows 10 w wersji 32 i 64 bitowej.Dla serwerów plików co najmniej Windows 2012 R2, 2016, Linux RedHat/CentOs, Linux Suse. |
| 3. | **Certyfikaty i pozostałe wymagania:*** + - 1. Rodzina zaoferowanego oprogramowania musi wykazać się, iż wszystkie testy organizacji VB100 zostały zakończone przyznaniem znaku VB100 w ciągu ostatnich 2 lat, licząc od daty złożenia oferty. Testy muszą być przeprowadzone na rodzinie zaoferowanego oprogramowania.
			2. Producent oprogramowania antywirusowego musi być wymieniony na aktualnym raporcie „Magic Quadrant for Endpoint Protection Platforms” firmy Gartner.
 |
| 4. | **Okres aktualizacji oprogramowania:** jeden rok, koniec okresu aktualizacji oprogramowania nie może być wcześniejszy, jak od dnia 31.12.2018 r. w przypadku instalacji oprogramowania później niż do dnia 01.01.2018 r.  |

|  |  |
| --- | --- |
| **Poz. 2. System ochrony dla serwerów poczty elektronicznej**  | **Ilość – 1 komplet** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** System ochrony musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową.System musi mieć możliwość pracy w trybie bramy i transparentnym.System ochrony musi wykorzystywać dedykowany system operacyjny, nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.System musi zapewniać:* 1. Obsługę minimum 3 domen internetowych,
	2. Obsługę minimum 2 bram internetowych przez które będzie wpływała poczta elektroniczna, umieszczonych w dwóch odrębnych lokalizacjach, gdzie dla każdej lokalizacji będzie uruchomiona osobna instancja systemu wraz z obsługą synchronizacji konfiguracji,
	3. Obsługę nie mniej niż 2 interfejsów Ethernet dla każdej lokalizacji,
	4. Obsługę nielimitowanej liczby użytkowników w trybie bramy,
	5. Obsługę co najmniej 3 serwerów wewnętrznych poczty elektronicznej,
	6. Obsługę protokołów TCP IP v4 i v6, SMTP, SMTP over ssl/tls, LDAP, RADIUS, SNMP,
	7. Polityki filtrowania oparte o adresy email (zarówno nadawców jak i odbiorców), nazwy domenowe, adresy IP,
	8. Możliwość zdefiniowania minimum 30 polityk na domenę,
	9. Możliwe akcje dla przetwarzanej poczty elektronicznej, w zależności od spełniania lub nie spełniania odpowiednich reguł: Accept, Relay, Reject, Discard, Kwarnatanna, Oznaczanie (Tagging),
	10. Ochronę poczty przychodzącej w zakresie spamu, wirusów i spyware. Szczegółowe wymagania zostały określone w pkt 5 i 6,
	11. Możliwość integracji systemu z zewnętrznym systemem typu Sandbox w postaci rozwiązania lokalnego i opartego o chmurę, bez konieczności dostarczania systemu Sandbox wraz z systemem ochrony dla serwerów poczty elektronicznej.
	12. Granularne, wielowarstwowe polityki wykrywania spamu i wirusów,
	13. Ochrona przed atakami DoS. Szczegółowe wymagania zostały określone w pkt 7,
	14. Archiwizacja poczty przychodzącej i wychodzącej na lokalnych dyskach systemu, wraz z możliwością definiowania okresu przechowywania i retencji oraz w lokalizacji zewnętrznej przy wykorzystaniu minimum protokołu SFTP,
	15. Usuwanie wewnętrznych nagłówków z poczty wychodzącej, wysyłanej za pośrednictwem rozwiązania,
	16. Obsługę funkcji greylist wraz z możliwością wskazania adresów poczty docelowych i źródłowych, dla których funkcja greylist nie będzie stosowana,
	17. Aktualizacje w czasie rzeczywistym bazy wiadomości spam,
	18. Aktualizacje zgodnie z harmonogramem definicji dla systemu antywirusowego,
	19. Możliwość zarządzania rozwiązaniem z poziomu przeglądarki internetowej, z wykorzystaniem protokołu HTTPS oraz z poziomu linii komend,
	20. Logowanie i raportowanie. Szczegółowe wymagania zostały określone w pkt 8.

Ochrona antywirusowa i antyspyware’owa musi zapewniać:Skanowanie antywirusowe wiadomości przychodzących, z wykorzystaniem protokołu SMTP,Skanowanie za pomocą minimum jednego modułu skanującego, moduł skanujący musi pochodzić od innego producenta, w porównaniu do modułu skanującego, zaoferowanego oprogramowania antywirusowego, o którym mowa w poz. 1,Kwarantannę dla zainfekowanych plików,Powiadomienia użytkowników wraz z możliwością definiowania treści powiadomienia w języku polskim,Skanowanie załączników skompresowanych wraz z możliwością konfiguracji poziomu zagnieżdżenia i wielkości załącznika, który zostanie poddany skanowaniu,Blokowanie załączników ze względu na ich typ,Modyfikacje tematu wiadomości w przypadku wykrycia zagrożenia, gdy zgodnie z konfiguracją, email ma być przekazany do serwera poczty,Obsługę minimum 40 profili antywirusowych.Ochrona antyspamowa musi zapewniać:1. Heurystyczną analizę spamu,
2. Filtrowanie treści wiadomości i załączników,
3. Szczegółową kontrolę nagłówka wiadomości,
4. Filtrowanie w oparciu o metodę Bayes’a z możliwością dostrajania dla poszczególnych użytkowników,
5. Filtrowanie w oparciu o sumy kontrolne spamu,
6. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF,
7. Wykrywanie spamu w oparciu o dynamiczną bazę spamu, dostarczaną przez producenta rozwiązania,
8. Wykorzystanie zewnętrznych serwisów RBL do filtrowania spamu,
9. Weryfikacja źródłowego adresu IP,
10. Wykorzystanie białych i czarnych list definiowanych globalnie,
11. Kwarantanna wiadomości spam,
12. Weryfikacje istniejących adresów docelowych z wykorzystaniem protokołu LDAP,
13. Oznaczanie wiadomości spam.

Ochrona przed atakami DoS musi zapewniać:1. Ochronę przed atakiem typu Mail Bombing,
2. Ochrona przed atakami na adres odbiorcy,
3. Definiowanie maksymalnych ilości wiadomości pocztowych przychodzących,
4. Kontrola Reverse DNS,
5. Weryfikacja poprawności adresu nadawcy.

Logowanie i raportowanie musi zapewniać:1. Raportowanie w trybie online stanu systemu w postaci dashboardu, na którym muszą być widoczne następujące elementy: obciążenie procesora/ów, zużycie pamięci, zajętość przestrzeni dyskowej, statystyki dotyczące liczby obsłużonych wiadomości wraz z podziałem na wiadomości uznane jako spam i wiadomości poprawne,
2. Raportowanie statystyczne we wskazanym okresie czasu z możliwością filtrowania na wiadomości przychodzące, wychodzące, wszystkie,
3. Raportowanie aktualnie otwartych sesji,
4. Raportowanie stanu kolejki, oraz reputacji poszczególnych adresów IP, skąd są wysyłane wiadomości email,
5. Logowanie każdego zdarzenia, jakie zachodzi w systemie,
6. Przekazywanie logów do zewnętrznego serwera Syslog,
7. Logowanie zmian w konfiguracji oraz krytycznych zdarzeń systemowych,
8. Możliwość przeglądu logów w czasie rzeczywistym,
9. Możliwość przeszukiwania logów i wyszukiwania informacji o poszczególnych wiadomościach wg kryteriów: okres, adres nadawcy, adres odbiorcy, temat wraz z możliwością szybkiego przejścia z widoku ogólnego wyszukanego logu do widoku zestawu logów, związanych z daną sesją,
10. Możliwość tworzenia raportów i planowania czasu generacji raportów wraz ze wskazaniem sposobu dostarczenia.
 |
| 2. | **Wydajność:**Systemu musi zapewniać wydajność nominalną skanowania antyspam minimum na poziomie 20 000 wiadomości pocztowych na godzinę, przy wielkości pojedynczej wiadomości 100kB. |
| 3. | **Platforma:**System musi być dostarczony w formie maszyny wirtualnej, możliwej do uruchomienia na bazie oprogramowania Vmware i Hyper-V. |
| 4. | **Certyfikaty:**System musi wykazać się, iż wszystkie testy organizacji VB100 w zakresie VBSpam, przeprowadzone na oferowanym systemie zostały zakończone przyznaniem znaku „SPAM + Verified” w ciągu ostatniego roku, licząc od daty złożenia oferty. |
| 5. | **Wsparcie techniczne:**System musi być dostarczony wraz ze wsparciem technicznym producenta oraz prawem do aktualizacji systemu, w tym aktualizacji definicji spamu i aktualizacji baz antywirusowych, zapewnionym na okres minimum trzech lat. Przy czym okres wsparcia i aktualizacji musi się kończyć z upływem ostatniego dnia trzyletniego okresu wsparcia technicznego i aktualizacji licząc od dnia wdrożenie rozwiązania, przy czym rozwiazanie musi być uruchomione w dniu 20.12.2017r. Wsparcie techniczne musi być realizowane w dni robocze przez 8 godzin roboczych. Ponadto wsparcie musi być realizowane w języku polskim.  |
| 6. | **Wdrożenie i szkolenie:**Wraz z systemem należy zapewnić pomoc w podstawowym wdrożeniu systemu oraz zapewnić szkolenie z obsługi systemu dla minimum 2 administratorów. Szkolenie może być realizowane w siedzibie Zamawiającego lub na terenie Warszawy. W ramach szkolenia należy poruszyć kwestie: konfiguracji urządzenia, mechanizmy zabezpieczające i konfiguracje profili/polityk, administrowanie kwarantanną, analizę raportów i logów, konfigurację klastra geograficznego, aktualizacje oprogramowania, wykonywanie kopii zapasowych oraz odtwarzanie konfiguracji, eksport logów i zarchiwizowanych wiadomości, diagnostykę i rozwiązywanie problemów z systemem. |

|  |  |
| --- | --- |
| **Poz. 3. Oprogramowanie biurowe**  | **Ilość – 30 licencji** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** oprogramowanie Microsoft Office 2016 Standard PL (licencja musi zawierać prawo do downgrade’u co najmniej do wersji 2010 ww. oprogramowania) lub oprogramowanie równoważne o podobnej funkcjonalności, wyposażone w interfejs API zgodny z oprogramowaniem Office oraz zapewniające bezobsługowe (nie wymagające wykonania dodatkowych czynności takich jak konwersja czy przepisanie oprogramowania na nowy język) działanie makr i programów napisanych w języku VBA, zawartych w dokumentach użytkowanych przez Zamawiającego.W przypadku dostarczenia oprogramowania równoważnego, należy zapewnić odpowiednie szkolenia dla użytkowników z zakresu obsługi i eksploatacji tego oprogramowania. |
| 2. | **Platforma systemowa:** co najmniej Windows 7, Windows 10 w wersji 32 i 64 bitowej. |
| 3. | **Typ licencjonowania:** Grupowe, bezterminowe. |

|  |  |
| --- | --- |
| **Poz. 4. Oprogramowanie do przeprowadzania audytu stacji roboczych i kontroli działań użytkowników na stacjach roboczych** | **Ilość – 1 komplet** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego i prawa do aktualizacji oprogramowania Statlook na okres 1 roku (asysta serwisowa) dla 270 agentów i 3 konsol zarządzania wraz ze zwiększeniem liczby równocześnie użytkowanych konsol do 4lub oprogramowanie równoważne o funkcjonalności umożliwiającej w szczególności: przeprowadzanie audytu oprogramowania, zainstalowanego i przechowywanego na komputerach pracowników, przeprowadzenie audytu plików multimedialnych, przechowywanych na komputerach pracowników, przeprowadzanie audytu sprzętu, monitoring zmian w konfiguracji komputerów w zakresie zmian w sprzęcie, jak i w oprogramowaniu, monitoring pracy pracowników w zakresie czasu wykorzystania poszczególnych aplikacji, ze szczególnym uwzględnieniem czasu przeglądania Internetu oraz wskazaniem odwiedzanych stron przez pracowników (statystyka musi być pobierana minimum z przeglądarek: IE, Firefox, Chrome), monitoring i raportowanie wydruków wraz z informacją o tytułach wydruków i liczbie wydrukowanych stron, monitoring i raportowanie użycia nośników wymiennych wraz z informacją, jakie pliki zostały otworzone/zapisane, możliwość blokowania nośników wymiennych, możliwość blokowania nośników wymiennych w tryb tylko do odczytu, moduł help-desk’u umożliwiający zgłaszanie przez pracowników problemów i obsługę zgłaszanych problemów przez pracowników obsługi technicznej, moduł raportowania, obejmujący wszelkie aspekty związane z audytami oprogramowania, bieżącą konfiguracją monitorowanych komputerów (sprzętową i programową) oraz prowadzeniem ewidencji posiadanego majątku w zakresie sprzętu i oprogramowania, moduł umożliwiający rejestrowanie posiadanych licencji na oprogramowanie i korelowanie ich ręczne oraz automatyczne, z wynikami przeprowadzonych audytów. Funkcjonalność audytu oprogramowania musi wspierać administratora w ocenie stanu legalności zainstalowanego oprogramowania, poprzez rozróżnienie programów komercyjnych od programów, które mogą być użytkowane bez opłat, moduł audytu oprogramowania musi uwzględniać części składowe, wchodzące w skład danego pakietu oprogramowania i raportować je w postaci jednego wpisu. Moduł pomocy zdalnej, gdzie informatyk ze swojej konsoli może się podłączyć do pulpitu pracownika zgłaszającego problem i dokonywać zdalnej diagnozy wraz z możliwością pobierania informacji o działających procesach w systemie zdalnym i możliwością edycji rejestru systemu zdalnego.Komunikacja pomiędzy agentem a serwerem musi być odpowiednio zabezpieczona przed podsłuchem i przejęciem przez obcy serwer.Oprogramowanie równoważne musi wykorzystywać nielimitowane bazy danych dostępne bezpłatnie, takie jak PostgreSQL.Oprogramowanie równoważne musi umożliwiać obsługę minimum 270 stacji roboczych i co najmniej 4 konsole zarządzania wraz z prawem do instalacji aktualizacji i wsparciem przez okres minimum jednego roku. |
| 2. | **Obsługiwane systemy operacyjne:** minimum Windows 7, Windows 10 w wersji 32 i 64 bitowej oraz Windows 2012 R2 i Windows 2016. |

|  |  |
| --- | --- |
| **Poz. 5. Oprogramowanie serwerowe – obsługujące wirtualizację**  | **Ilość – 2 komplety** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego na poziomie co najmniej podstawowym i prawa do aktualizacji na okres 1 roku dla dwóch kompletów posiadanego przez Zamawiającego oprogramowania VMware Essentials Plus Kit, dającego prawo do jego instalacji na 3 serwerach wyposażonych w 2 wielordzeniowe procesory fizyczne każdy. Przedłużenie do pierwszego kompletu oprogramowania VMware Essentials Plus Kit należy dostarczyć w terminie do 4 grudnia 2017 r. tak, aby przedłużyć posiadane przez Zamawiającego wsparcie, przedłużenie do drugiego kompletu oprogramowania VMware Essentials Plus Kit należy dostarczyć w terminie do 10 grudnia 2017 r. tak, aby przedłużyć posiadane przez Zamawiającego wsparcielub oprogramowanie równoważne dające prawo do jego instalacji na minimum 6 serwerach fizycznych, obsługujące co najmniej 2 wielordzeniowe procesory fizyczne na każdym serwerze, bez ograniczeń na liczbę rdzeni i bez ograniczeń na całkowitą pojemność pamięci RAM serwerów, umożliwiające przypisanie co najmniej 16 procesorów i 64GB pamięci RAM do każdej maszyny wirtualnej wykreowanej w tym oprogramowaniu, z możliwością obsługi co najmniej 50 maszyn wirtualnych, w miarę dostępnych zasobów serwera fizycznego, umożliwiające bezpośrednie podłączenie urządzenia serwera fizycznego (karty SCSI, napęd taśmowego podłączonego do karty SCSI w serwerze fizycznym, port szeregowy serwera fizycznego, port USB serwera fizycznego) do wykreowanej maszyny wirtualnej, tak aby ta maszyna sterowała urządzeniem w sposób wyłączny i bezpośrednio, za pośrednictwem właściwych sterowników dla ww. urządzenia. Z prawem do aktualizacji tego oprogramowania w okresie minimum 1 roku od daty udzielenia licencji Zamawiającemu do najnowszych wersji oprogramowania, gdy taka wersja zostanie opublikowana oraz prawem do wsparcia, w okresie 1 roku, od daty udzielenia licencji Zamawiającemu. Oprogramowanie równoważne musi zapewniać podobną wydajność pracy wykreowanych na nim maszyn wirtualnych zarówno w zakresie IOPS systemu dyskowego, wydajności procesora jak i przepustowości pamięci RAM. Oprogramowanie równoważne musi posiadać system centralnego zarządzania poszczególnymi instancjami zainstalowanymi na serwerach fizycznych w ramach licencji. Oprogramowanie równoważne musi zapewniać możliwość migracji maszyn wirtualnych pomiędzy serwerami fizycznymi w trakcie ich pracy oraz offline. Oprogramowanie równoważne musi zapewniać wsparcie dla maszyn wirtualnych wykorzystujących co najmniej następujące systemy operacyjne: Windows, Linux, UnixWare 7.1.4.W przypadku dostarczenia oprogramowania równoważnego, należy zapewnić odpowiednie szkolenia dla administratorów z zakresu obsługi i eksploatacji tego oprogramowania oraz migrację środowiska wirtualnego opartego na oprogramowaniu VMware Essentials Plus Kit na nowe oprogramowanie. |

|  |  |
| --- | --- |
| **Poz. 6. Oprogramowanie do wykonywania kopii zapasowych**  | **Ilość – 1 komplet** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie co najmniej podstawowego wsparcia technicznego i prawa do aktualizacji w okresie 1 roku dla oprogramowania Veeam Backup and Replication Standard licencjonowane dla 6 procesorów dla VMware vSphere.Lub oprogramowanie równoważne zapewniające możliwość wykonywania kopii zapasowych maszyn wirtualnych pracujących na serwerze VMware vSphere lub na oprogramowaniu, o którym mowa w poz. 5, w przypadku dostarczania produktu równoważnego, o którym tam mowa, zapewniające co najmniej następujące możliwości: wykonywanie kopii zapasowych maszyn wirtualnych bez konieczności instalowania na tych maszynach agenta, wykonywanie kopii maszyn wirtualnych w trakcie ich pracy bez wpływu na ich pracę, jak i maszyn wyłączonych, replikacja maszyn wirtualnych na inny serwer fizyczny wyposażony w oprogramowanie do wirtualizacji, zgodnie z harmonogramem, możliwość praktycznie natychmiastowego odtworzenia maszyny z backupu przy wykorzystaniu wystawianego przez oprogramowanie równoważne udziału sieciowego NFS, bazującego na kopii maszyny, obsługa napędów taśmowych LTO do wykonywania archiwizacji maszyn na taśmę, obsługa harmonogramów umożliwiających wykonywanie kopii zapasowych i replikacji danych w określonych odstępach czasowych, obsługa odtwarzania maszyn wirtualnych na dotychczasowym serwerze, jak i nowym serwerze wirtualizacji, obsługa odtwarzania pojedynczych plików maszyn wirtualnych opartych na systemach operacyjnych co najmniej Windows i Linux. Oprogramowanie równoważne musi posiadać prawo do aktualizacji i podstawowego wsparcia technicznego w okresie jednego roku od daty udzielenia licencji Zamawiającemu. Oprogramowanie równoważne musi zapewniać możliwość obsługi 3 serwerów fizycznych wyposażonych w 2 procesory każdy. Licencja oprogramowania równoważnego musi zapewniać możliwość dalszego zwiększenia ilości obsługiwanych serwerów poprzez zakup i dodanie przez Zamawiającego kolejnych licencji. |

|  |  |
| --- | --- |
| **Poz. 7. Oprogramowanie do obsługi systemu monitoringu wizyjnego**  | **Ilość – 1 licencja** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** aktualizacja oprogramowania go1984 edycja Ultimate dająca prawo do korzystania z nowych wersji oprogramowania, powstałych minimum w okresie jednego roku od daty udzielenia licencji na aktualizację Zamawiającemu, wraz z bezpłatnym wsparciem na okres jednego roku lub oprogramowanie równoważne o podobnej funkcjonalności w zakresie nielimitowanej obsługi kamer IP, wideoserwerów IP, metod składowania i prezentacji danych, obsługi wielu monitorów, obsługi strumieni video kodowanych kodekiem H.264, zapewnienie wsparcia technicznego na okres jednego roku od daty udzielenia licencji Zamawiającemu. |
| 2. | **Pozostałe:** Oprogramowanie w polskiej wersji językowej, jeśli taka wersja istnieje, w przeciwnym przypadku w angielskiej wersji językowej. |
| 3. | **Platforma systemowa:** co najmniej Windows 7, Windows 10. |

|  |  |
| --- | --- |
| **Poz. 8. Firewall** | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego do oprogramowania Barracuda NG Firewall Vx250 oraz zapewnienie aktualizacji oprogramowania i aktualizacji następujących modułów oprogramowania: Application Control, IPS/IDS, URL filter na okres co najmniej 3 lat wraz ze zwiększeniem liczby równocześnie obsługiwanych adresów IP do 500.lub oprogramowanie lub urządzenie o równoważnej funkcjonalności, cechujące się co najmniej następującymi możliwościami:1. Filtrowanie pakietów oparte na kontroli stanu połączenia (Stateful Inspection Firewall).2. Obsługa protokołów minimum IPv4, IPv6, ARP.3. Ochrona przed atakami minimum Dos/DDos, IP spoofing, SYN flooding, flood ping oraz ochrona przed skanowaniem portów i adresów.4. Obsługa flirtowania pakietów dla protokołów dynamicznych minimum: RPC (ONC-RPC, DCE-RPC), SIP, H.323, SCCP, FTP.5. Obsługa flirtowania pakietów dla protokołów wykorzystujących porty statyczne.6. Obsługa wielu łącz internetowych z możliwością automatycznego ich przełączania w momencie awarii, jak również z możliwością wykorzystywania kilku łącz równocześnie, minimum za pomocą technologii multipath routing.7. Obsługa pakietów o zwykłej wielkości jak i tzw. jumbo frame o wielkości minimum 9000B.8. Obsługa funkcjonalności przezroczystego Proxy minimum dla protokołu TCP.9. Obsługa w protokole IPv4 funkcji NAT (co najmniej source i destination), NAPT, PAT, Proxy ARP.10. Obsługa VPN w zakresie: zestawiania połączeń za pomocą protokołów PPTP, L2TP, IPSec, Tina, obsługa algorytmów szyfrowania minimum AES128, AES256, 3DES.11. Obsługa zarządzania ruchem w obrębie sieci VPN za pomocą technologii minimum traffic shaping z obsługą minimum 4 priorytetów, w tym jeden priorytet dla ruchu VoIP minimalizujący opóźnienia.12. Możliwość ograniczenia pasma, jakie dany tunel VPN ma wykorzystywać w ramach łącza, możliwość kompresji danych przesyłanych przez zestawiony tunel.13. Możliwość zestawiania tunelu VPN site to site przy wykorzystaniu kilku łączy, na zasadzie wykorzystywania kilku kanałów fizycznych, wchodzących w skład danego tunelu. Obsługa minimum 4 kanałów na jeden tunel wraz z możliwością agregacji wydajności poszczególnych kanałów na poziomie sesji i na poziomie pojedynczych pakietów, możliwość wyznaczania kanałów zapasowych, detekcja uszkodzenia danego kanału i przełączenie ruchu na sprawne kanały w przypadku uszkodzenia bez rozłączenia tunelu.14. Możliwość zestawiania tuneli VPN zarówno na łączach internetowych, jak i łączach dedykowanych do transmisji danych.15. Klient do zestawiania tuneli client to site dla minimum oprogramowania Windows wraz ze zintegrowanym firewallem i możliwością centralnej konfiguracji ustawień firewalla, ze wsparciem dla funkcji ESET Secure Authentication oraz klient do zestawiania tuneli client to site dla minimum oprogramowania Windows.16. Możliwość budowy tuneli VPN w strukturze gwiaździstej z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami.17. Zarządzanie ruchem w zakresie: limitowania pasma za pomocą technologii traffic shaping z obsługą minimum 4 priorytetów i dynamicznym podziałem dostępnego pasma, w zależności od poziomu ruchu wygenerowanego dla danego priorytetu ogólnie i, w zależności od przynależności do danej grupy, przez użytkownika, funkcja QoS.18. Monitoring ruchu sieciowego z możliwością osobnej obserwacji ruchu generowanego przez protokoły dynamicznie otwierające porty, takie jak SIP, RPC.19. Obsługa funkcji IPS i IDS wraz z aktualizacją sygnatur i możliwością tworzenia własnych polis i definiowania, w ramach własnych polis, sposobów reakcji systemu na pakiety zawierające poszczególne sygnatury będące w bazie systemu.20. Obsługa funkcji inspekcji ruchu w protokołach nieszyfrowanych, jak i w protokołach szyfrowanych minimum SSL/TLS.21. Obsługa funkcji filtrowania ruchu w warstwie 7 protokołu TCP/IP dla minimum 1000 aplikacji typu P2P, komunikatory, gry.22. Wbudowane w rozwiązanie równoważne serwery DHCP, DNS.23. Obsługa funkcji Proxy sip, http, ssh, ftp.24. Obsługa filtrowania url’i wraz z aktualizacja zbiorów url’i przez producenta.25. Bramka SMTP z filtrem protokołu SMTP.26. Uwierzytelnianie klientów za pomocą protokołów i technologii minimum x.509, NTLM, Radius, RSA Securit, LDAP/LDAPS, Active Directory.27. Funkcjonalność wprowadzenia modyfikacji reguł filtrowania i konfiguracji rozwiązania, a następnie aktywowania wszystkich wprowadzonych zmian wraz z logowaniem wprowadzonych zmian i możliwością weryfikacji i powrotu do stanu sprzed zmiany.28. Możliwość testowania reguł za pomocą wbudowanego narzędzia do weryfikacji.29. Możliwość tworzenia własnych obiektów sieciowych (minimum definiowane przez adresy IP, grupy adresów IP, zakresy adresów IP) wraz z możliwością nazywania zdefiniowanych obiektów i ich wykorzystywania w regułach.30. Możliwość tworzenia własnych obiektów dla protokołów opartych na portach statycznych, jak i portach dynamicznych.31. Możliwość tworzenia dynamicznych reguł firewalla opartych o przypisanie użytkownika do grupy, przedział czasowy, w jakim dana reguła ma działać.32. Możliwość podzielenia reguł firewalla na grupy w oparciu o adresacje IP, używane protokoły, następnie filtrowanie pakietów z wykorzystaniem zdefiniowanej kaskady bazującej na stworzonych grupach, tak aby filtrowany ruch sieciowy przechodził przez jak najmniej reguł.33. Generowanie statystyk ruchu przepływającego przez rozwiązanie w czasie zbliżonym do rzeczywistego.34. Obsługa routingu z trasami definiowanymi zarówno statycznie, jak i dynamicznie wraz z obsługą protokołów OSPF i RIP.35. Możliwość zarządzania rozwiązaniem zdalnie, za pomocą oprogramowania działającego na platformie Windows lub za pomocą przeglądarki Web.Rozwiązanie równoważne musi posiadać certyfikat zgodności ze standardem IPSec w zakresie VPNC Basic, a także musi spełniać wymagania normy ISO 15408 Common Criteria na poziomie EAL 4+ lub musi posiadać certyfikat ICSA Labs minimum w zakresie Network Firewall.Rozwiązanie równoważne musi mieć możliwość zestawienia tuneli VPN przy wykorzystaniu protokołu Tina VPN z pozostałymi firewallami Barracuda NG Firewall eksploatowanymi przez Zamawiającego.W przypadku zaoferowania sprzętowego rozwiązania równoważnego, takie urządzenie musi być wyposażone w minimum 8 niezależnych portów Ethernet zakończonych złączem RJ-45 o wydajności 10/100/1000, obsługujących funkcję 802.1q VLAN oraz minimum 1 port 10Gigabit, urządzenie takie musi zapewniać obsługę co najmniej 10 segmentów sieci. Wydajność takiego urządzenia w zakresie filtrowania pakietów nie może być mniejsza, jak 8 Gbps i, w zakresie filtrowania IPS, nie może być mniejsza jak 2 Gbps, liczba chronionych adresów IP nie mniejsza jak 500.W przypadku zaoferowania programowego rozwiązania równoważnego, takie rozwiązanie musi umożliwiać obsługę minimum 8 fizycznych kart sieciowych Ethernet o wydajności 10/100/1000 obsługujących funkcję 802.1q VLAN oraz minimum 1 kartę sieciową 10Gigabit, musi umożliwiać obsługę co najmniej 10 segmentów sieci, musi umożliwiać ochronę co najmniej 500 adresów IP. Oprogramowanie równoważne musi być dostarczone w formie maszyny wirtualnej, możliwej do uruchomienia na bazie oprogramowania VMware.Do rozwiązania równoważnego należy zapewnić, w okresie co najmniej 3 lat od daty zakupu, prawo do aktualizacji sygnatur i baz, prawo do aktualizacji rozwiązania, wsparcie techniczne realizowane minimum w trybie 8x5 (przez 8 godzin w dni robocze) minimum w języku polskim.W przypadku dostarczenia rozwiązania równoważnego, należy zapewnić szkolenie dla minimum 2 administratorów z zakresu eksploatacji i zaawansowanej konfiguracji ww. rozwiązania, szkolenie musi być zrealizowane w Warszawie oraz należy zapewnić migrację posiadanego przez Zamawiającego rozwiązania do rozwiązania równoważnego. |

|  |  |
| --- | --- |
| **Poz. 9. Licencje dostępowe**  | **Ilość – 25 licencji** |
| **L.p.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie Software assurance do licencji Windows Server User CAL. Przedłużenie należy dostarczyć w terminie do 24 listopada 2017. |
| 2. | **Pozostałe wymagania:** prawo do uzyskiwania dostępu do nowszych wersji ww. oprogramowania opublikowanych w okresie minimum 2 lat od daty przedłużenia, w przypadku pojawienia się takich wersji. |
| 3. | **Typ licencjonowania:** Grupowe. |