**Numer sprawy: 5/2019 Załącznik nr 1b do SIWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA – zwany OPZ DLA CZĘŚCI 2.**

**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 2 – Warunki szczegółowe.
7. Zapotrzebowanie na oprogramowanie zostało opisane w pkt III. OPZ dla części 2 - 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, zapisy na portalu licencyjnym producenta).
8. Okres użytkowania oprogramowania wyszczególnionego w pkt III. OPZ dla części 2 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 2.
	1. **Warunki szczegółowe:**

|  |  |
| --- | --- |
| **Poz. 1. Oprogramowanie antywirusowe**  | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania:** aktualizacja oprogramowania antywirusowego ESET Endpoint Antivirus Suite dla 330 stacji roboczych i serwerów, w tym liczba serwerów nie przekroczy 30.Lub oprogramowanie równoważne o podobnej funkcjonalności umożliwiającej w szczególności:Liczba stacji roboczych i laptopów opartych na systemie Windows i urządzeń mobilnych opartych na systemie Android objętych licencją: co najmniej 300 szt.Liczba serwerów plików objętych licencją: co najmniej 30 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, minimum w zakresie zajętości pamięci RAM i wykorzystania procesora.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, definicja wykluczeń – lista certyfikatów stron HTTPS zabronionych, dozwolonych, niepodlegających kontroli.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.Obsługa grup dynamicznych, do których konsola centralnego zarządzania dodaje poszczególne stacje robocze na podstawie ich specyficznych cech i przypisywanie im odpowiednich polis.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 kilka 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, informacji o wykrytych zagrożeniach (zawirusowanych plikach, mailach, stronach internetowych, które użytkownik próbował otwierać) 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, instalacji innego oprogramowania.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,wykaz zadań realizowanych przez agenty oprogramowania zainstalowane na stacjach roboczych, w określonym czasie,zadaniach realizowanych przez system centralnego zarządzania w określonym czasie,wynikach skanowania realizowanych w określonym czasie,plikach przesłanych do chmury, w celu ich dokładnej analizy, w określonym czasie,stacjach roboczych, na których oprogramowanie wykryło zagrożenie w określonym czasie,obiektach poddanych kwarantannie,zdarzeniach zarejestrowanych w dzienniku audytu.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, niż do moduł skanujący wykorzystywany przez Zamawiającego do kontroli poczty elektronicznej oparty na rozwiązaniu FortiMail.W przypadku oprogramowania równoważnego, należy zapewnić szkolenie z zakresu instalacji, wdrożenia i obsługi konsoli do centralnego zarządzania oprogramowaniem dla minimum 3 informatyków oraz należy zapewnić pomoc w sprawnym wdrożeniu oprogramowania przed dniem 01.01.2020. W tym celu należy zapewnić odpowiednio dłuższy okres aktualizacji oprogramowania równoważnego tak, aby było możliwe płynne zastąpienie aktualnie eksploatowanego oprogramowania, oprogramowaniem równoważnym, w terminie do 01.01.2020r. bez przesunięcia daty końca ważności o której mowa w Lp. 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, 2019, Linux RedHat/CentOs. |
| 3. | **Certyfikaty i pozostałe wymagania:*** + - 1. Rodzina zaoferowanego oprogramowania równoważnego musi spełniać warunek, 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 równoważnego 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 31.12.2020 r. w przypadku instalacji oprogramowania później niż do dnia 01.01.2020 r.  |

|  |  |
| --- | --- |
| **Poz. 2. Oprogramowanie do przeprowadzania audytu stacji roboczych i kontroli działań użytkowników na stacjach roboczych** | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego i prawa do aktualizacji oprogramowania Statlook na okres 1 roku (asysta serwisowa) dla 290 agentów i 5 konsol.Lub oprogramowanie równoważne o funkcjonalności umożliwiającej w szczególności: 1. Przeprowadzanie audytu oprogramowania, zainstalowanego i przechowywanego na komputerach pracowników.
2. Przeprowadzenie audytu plików multimedialnych, przechowywanych na komputerach pracowników.
3. Przeprowadzanie audytu sprzętu, monitoring zmian w konfiguracji komputerów w zakresie zmian w sprzęcie, jak i w oprogramowaniu.
4. Zdalne wykonywanie zdefiniowanych przez administratora skryptów na monitorowanych stacjach roboczych w celu automatyzacji zadań administracyjnych.
5. Centralne zbieranie zalogowanych zdarzeń na komputerach podłączonych do oprogramowania wraz z możliwością filtrowania zdarzeń, które mają się znaleźć w centralnym repozytorium oraz wyszukiwanie na konsoli określonych wg. filtru zdarzeń.
6. Centralne monitorowanie stanu aktualizacji podłączonych stacji roboczych minimum z wykorzystaniem informacji zwracanych przez system Windows wraz z przechowywaniem historii zmian.
7. 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, Edge, Firefox, Chrome) wraz z przechowywaniem danych historycznych.
8. Monitoring i raportowanie wydruków wraz z informacją o tytułach wydruków i liczbie wydrukowanych stron wraz z przechowywaniem danych historycznych.
9. Monitoring i raportowanie użycia nośników wymiennych wraz z informacją, jakie pliki zostały otworzone/zapisane wraz z przechowywaniem danych historycznych.
10. Możliwość blokowania nośników wymiennych, możliwość blokowania nośników wymiennych w tryb tylko do odczytu wraz z przechowywaniem danych historycznych.
11. Moduł help-desk’u umożliwiający zgłaszanie przez pracowników problemów i obsługę zgłaszanych problemów przez pracowników obsługi technicznej.
12. 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.
13. Moduł umożliwiający rejestrowanie posiadanych licencji na oprogramowanie i korelowanie ich ręczne oraz automatyczne, z wynikami przeprowadzonych audytów.
14. 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.
15. 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, edycji rejestru systemu zdalnego, pobierania i zapisywania plików na zdalny komputer wraz z możliwością dostępu do plików, rejestru i zadań, w kontekście użytkownika i administratora.
16. Moduł wspomagający zarządzanie zgodnością organizacji z wymaganiami określonymi w RODO, umożliwiający w szczególności rejestrowanie zbiorów, dostępów do zbiorów, naruszeń bezpieczeństwa przetwarzania informacji, prośby o usunięcie danych ze zbioru, rejestr czynności przetwarzania, rejestr szkoleń związanych z przetwarzaniem danych osobowych.
17. Komunikacja pomiędzy agentem a serwerem musi być odpowiednio zabezpieczona przed podsłuchem i przejęciem przez obcy serwer.
18. Oprogramowanie równoważne musi wykorzystywać nielimitowane bazy danych dostępne bezpłatnie, takie jak PostgreSQL.
19. Oprogramowanie równoważne musi umożliwiać obsługę minimum 290 stacji roboczych i co najmniej 5 konsoli 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, 2016 i 2019. |

|  |  |
| --- | --- |
| **Poz. 3. 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, wideo serwerów IP w tym kamer i wideo serwerów, będących w posiadaniu Zamawiającego, 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. 4. Oprogramowanie serwerowe – obsługujące wirtualizację**  | **Ilość – 2 komplety** |
| **Lp.** | **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 2019 r. tak, aby przedłużyć posiadane przez Zamawiającego wsparcie, przedłużenie do drugiego kompletu oprogramowania VMware Essentials Plus Kit należy dostarczyć w terminie do 10 grudnia 2019 r. tak, aby przedłużyć posiadane przez Zamawiającego wsparcie.Lub oprogramowanie równoważne, dające prawo do jego instalacji na minimum 6 serwerach fizycznych, obsługujące co najmniej 2 wielordzeniowe procesory fizyczne na każdym serwerze, z obsługą minimum 256 rdzeni i obsługą minimum 1TB pamięci RAM zainstalowanej w każdym z serwerów, umożliwiające przypisanie co najmniej 32 procesorów, 128GB pamięci RAM i 10 kart sieciowych do każdej maszyny wirtualnej wykreowanej w tym oprogramowaniu, z możliwością obsługi co najmniej 60 maszyn wirtualnych na każdym serwerze, w miarę dostępnych zasobów serwera fizycznego, obsługujące dyski lokalne serwera i dyski zdalne przez protokół NFS, iSCSI, FC (sieć SAN), obsługujące karty sieciowe 1 i 10Gb Ethernet zainstalowane w serwerze, umożliwiające bezpośrednie podłączenie urządzenia fizycznego serwera (karty SAS, napęd taśmowego podłączonego do karty SAS 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, wpierający między innymi automatyzujące działania takie, jak migracja maszyny wirtualnej na działający serwer w przypadku awarii serwera, na którym dana maszyna pracowała. 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.W przypadku oprogramowania równoważnego należy dostarczyć odpowiednie oprogramowanie do wykonywania kopii zapasowych, o którym jest mowa w poz. 5.  |

|  |  |
| --- | --- |
| **Poz. 5. Oprogramowanie do wykonywania kopii zapasowych**  | **Ilość – 1 komplet** |
| **Lp.** | **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 8 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. 4, 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 zapasowych aplikacji zainstalowanych na maszynach wirtualnych Windows AD, MS SQL, Exchange w sposób w pełni konsystentny, z możliwością zarządzania logami transakcyjnymi tych aplikacji, wykonywanie kopii zapasowych w trybie całościowym i przyrostowym, możliwość tworzenia kopii całościowej w sposób syntetyczny na podstawie kopii przyrostowych, wykorzystywanie mechanizmu kompresji i deduplikacji do zmniejszenia ilości przechowywanych danych, obsługa trybu CBT, 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 wirtualnej z kopii zapasowej przy wykorzystaniu wystawianego przez oprogramowanie równoważne udziału sieciowego NFS, bazującego na kopii maszyny, obsługa co najmniej 2 napędów taśmowych LTO do wykonywania archiwizacji maszyn i plików na taśmę wraz z możliwością podłączenia tych napędów zarówno lokalnie, jak i zdalnie, za pośrednictwem odpowiedniego modułu oprogramowania dołączonego do oprogramowania równoważnego, w celu minimalizacji pasma sieciowego w lokalizacjach zdalnych, obsługa harmonogramów umożliwiających wykonywanie kopii zapasowych i replikacji danych w określonych odstępach czasowych, obsługa wykonywania kopii przechowywanej w co najmniej 2 magazynach jednocześnie, z możliwością osobnego określenia retencji przechowywanych kopii oraz harmonogramu replikacji kopii do drugiego magazynu, 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, obsługa co najmniej 4 zdalnych magazynów przechowywania danych tak, aby zminimalizować pasmo sieciowe przy wykonywaniu kopii w lokalizacjach zdalnych. Oprogramowanie równoważne musi umożliwiać równoczesną obsługę serwerów pojedynczych i serwerów zarządzanych przez oprogramowanie do centralnego zarządzania. 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 co najmniej 4 serwerów fizycznych wyposażonych w 2 procesory każdy. Licencja oprogramowania równoważnego musi zapewniać możliwość dalszego zwiększenia liczby obsługiwanych serwerów poprzez zakup i dodanie przez Zamawiającego kolejnych licencji. |

|  |  |
| --- | --- |
| **Poz. 6. Firewall Typ I** | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego do oprogramowania Barracuda CloudGen Firewall Vx250 oraz zapewnienie prawa do aktualizacji oprogramowania i następujących modułów tego oprogramowania: Application Control, IPS/IDS, URL filter na okres co najmniej 3 lat.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, z możliwością wskazywania wag dla łącz i technik: roud robin, random.7. Obsługa pakietów o zwykłej wielkości jak i tzw. jumbo frame o wielkości minimum 9000B.8. Obsługa funkcjonalności Proxy dla protokołów SIP, http, SSH, FTP.9. Obsługa w protokole IPv4 funkcji NAT (co najmniej source i destination), PAT, Proxy ARP.10. Obsługa VPN w zakresie: zestawiania połączeń za pomocą protokołów IPSec, Tina, obsługa algorytmów szyfrowania minimum AES128, AES256, 3DES wraz z możliwością zestawienia minimum 100 tuneli VPN jednocześnie.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 oraz przypisywania aplikacji do poszczególnych kanałów tunelu VPN.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 VPN. Obsługa minimum 8 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. Możliwość budowy tuneli VPN site to site w strukturze gwiaździstej, z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami.16. Wykorzystanie do uwierzytelniania tuneli VPN site to site certyfikatów do szyfrowania.17. Klient do zestawiania tuneli client to site dla minimum oprogramowania Windows wraz ze zintegrowanym firewallem i możliwością centralnej konfiguracji ustawień firewalla.18. Możliwość autoryzacji połączeń VPN client to site przy użyciu wewnętrznej bazy użytkowników, zewnętrznego serwera Radius, LDAP.19. 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.20. Monitoring ruchu sieciowego na konsoli graficznej zarządzania z możliwością osobnej obserwacji ruchu generowanego przez protokoły dynamicznie otwierające porty, takie jak SIP, RPC. W tym zbliżone do czasu rzeczywistego monitorowanie ruchu wg. zadanego filtra (minimum wg. IP źródłowego, docelowego, portu sieciowego) i widoczność zarówno połączeń zaakceptowanych jak i zablokowanych.21. 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.22. Obsługa funkcji inspekcji (IPS oraz aplikacyjna) ruchu w protokołach nieszyfrowanych, jak i w  protokołach szyfrowanych minimum SSL/TLS.23. Obsługa funkcji filtrowania ruchu w warstwie 7 protokołu TCP/IP dla minimum 1000 aplikacji typu P2P, komunikatory, gry.24. Wbudowane w rozwiązanie równoważne serwery DHCP, DNS.25. Obsługa filtrowania url’i wraz z aktualizacją zbiorów url’i przez producenta oraz możliwość definiowania własnych polis, w ramach których wskazane grupy adresów url dostarczane przez producenta są blokowane. Możliwość zdefiniowania własnych url’i. Zdefiniowane polisy filtrowania url’i muszą być możliwe do przypisania do poszczególnych reguł firewalla.26. 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 wraz z możliwością zdefiniowania kontroli protokołów, reakcji na niezgodność protokołu.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 CloudGen 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 10 Gbps i, w zakresie filtrowania IPS, nie może być mniejsza jak 4 Gbps, liczba chronionych adresów IP nie mniejsza jak 250, obudowa urządzenia musi być dostosowana do jego montażu w szafie 19 cali, wysokość obudowy 1U, w obudowie urządzenia muszą być zintegrowane minimum 2 zasilacze 230V zapewniające pracę urządzenia po awarii jednego z zasilaczy lub zaniku zasilania z jednego obwodu, wyświetlacz sygnalizujący stan pracy urządzenia, diody sygnalizacyjne oraz dysk lokalny do składowania logów o pojemności minimum 80GB, do urządzenia musza być dołączone akcesoria montażowe.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 250 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 zaoferowania sprzętowego rozwiązania równoważnego, dodatkowo należy zapewnić 3-letnią gwarancję, wymianę urządzenia w przypadku jego awarii w ciągu jednego dnia oraz prawo do wymiany urządzenia po 4-roletnim okresie eksploatacji.W przypadku dostarczenia rozwiązania równoważnego, należy zapewnić szkolenie dla minimum 3 informatyków 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. 7. Firewall Typ II** | **Ilość – 1 komplet** |
| **Lp.** | **Opis minimalnych wymagań lub konfiguracji** |
| 1. | **Wymagania ogólne:** przedłużenie wsparcia technicznego oraz prawa do aktualizacji urządzenia Barracuda CloudGen Firewall F380 (Barracuda NextGen Firewall F380 EU) oraz przedłużenie prawa do przyspieszonej wymiany w razie awarii urządzenia Barracuda CloudGen Firewall F380 (Barracuda NextGen Firewall F380 IR) na okres co najmniej 3 lat.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 z możliwością wskazywania wag dla łącz i technik: roud robin, random.7. Obsługa pakietów o zwykłej wielkości jak i tzw. jumbo frame o wielkości minimum 9000B.8. Obsługa funkcjonalności Proxy dla protokołów SIP, http, SSH, FTP.9. Obsługa w protokole IPv4 funkcji NAT (co najmniej source i destination), PAT, Proxy ARP.10. Obsługa VPN w zakresie: zestawiania połączeń za pomocą protokołów IPSec, Tina, obsługa algorytmów szyfrowania minimum AES128, AES256, 3DES wraz z możliwością zestawienia minimum 100 tuneli VPN jednocześnie.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 oraz przypisywania aplikacji do poszczególnych kanałów tunelu VPN.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 VPN. Obsługa minimum 8 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. Możliwość budowy tuneli VPN site to site w strukturze gwiaździstej z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami.16. Wykorzystanie do uwierzytelniania tuneli VPN site to site certyfikatów do szyfrowania.17. Klient do zestawiania tuneli client to site dla minimum oprogramowania Windows wraz ze zintegrowanym firewallem i możliwością centralnej konfiguracji ustawień firewalla.18. Możliwość autoryzacji połączeń VPN client to site przy użyciu wewnętrznej bazy użytkowników, zewnętrznego serwera Radius, LDAP.19. 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.20. Monitoring ruchu sieciowego na konsoli graficznej zarządzania z możliwością osobnej obserwacji ruchu generowanego przez protokoły dynamicznie otwierające porty, takie jak SIP, RPC. W tym zbliżone do czasu rzeczywistego monitorowanie ruchu wg. zadanego filtra (minimum wg. IP źródłowego, docelowego, portu sieciowego) i widoczność zarówno połączeń zaakceptowanych jak i zablokowanych.21. 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.22. Obsługa funkcji inspekcji (IPS oraz aplikacyjna) ruchu w protokołach nieszyfrowanych, jak i w  protokołach szyfrowanych minimum SSL/TLS.23. Obsługa funkcji filtrowania ruchu w warstwie 7 protokołu TCP/IP dla minimum 1000 aplikacji typu P2P, komunikatory, gry.24. Wbudowane w rozwiązanie równoważne serwery DHCP, DNS.25. Obsługa filtrowania url’i wraz z aktualizacją zbiorów url’i przez producenta oraz możliwość definiowania własnych polis w ramach których wskazane grupy adresów url dostarczane przez producenta są blokowane. Możliwość zdefiniowania własnych url’i. Zdefiniowane polisy filtrowania url’i muszą być możliwe do przypisania do poszczególnych reguł firewalla.26. 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 wraz z możliwością zdefiniowania kontroli protokołów, reakcji na niezgodność protokołu.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.Urządzenie 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 CloudGen Firewall, eksploatowanymi przez Zamawiającego.Urządzenie równoważne musi być wyposażone w minimum 8 niezależnych portów Ethernet zakończonych złączem RJ-45 o wydajności 10/100/1000, obsługujących funkcję 802.1q VLAN, urządzenie takie musi zapewniać obsługę co najmniej 10 segmentów sieci. Wydajność takiego urządzenia w zakresie filtrowania pakietów nie może być mniejsza, jak 4 Gbps i, w zakresie filtrowania IPS, nie może być mniejsza jak 1,5 Gbps, liczba chronionych adresów IP nieograniczona, obudowa urządzenia musi być dostosowana do jego montażu w szafie 19 cali, wysokość obudowy 1U, w obudowie urządzenia musi być zintegrowany minimum 1 zasilacz 230V, wyświetlacz sygnalizujący stan pracy urządzenia, diody sygnalizacyjne oraz dysk lokalny do składowania logów o pojemności minimum 80GB, do urządzenia muszą być dołączone akcesoria montażowe.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, gwarancje, wymianę urządzenia w przypadku jego awarii w ciągu jednego dnia oraz prawo do wymiany urządzenia po 4-roletnim okresie eksploatacji.W przypadku dostarczenia rozwiązania równoważnego, należy zapewnić szkolenie dla minimum 3 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. |