ZAŁĄCZNIK NR 2 DO SIWZ – OPIS PRZEDMIOTU ZAMÓWIENIA (ZADANIE NR 1)

Wydzierżawiający w ramach realizacji umowy zobowiązany jest do:

1. Udostępnienia fizycznych serwerów o parametrach nie gorszych niż wskazane w Tabeli 1 w ilości 2 sztuk na okres 3 lat.
2. Udostępnienia pamięci masowej o parametrach nie gorszych niż wskazane w Tabeli 2 w ilości 1 sztuki na okres 3 lat.
3. Udostępnienia przełączników sieciowych o parametrach nie gorszych niż wskazane w Tabeli 3 w ilości 2 sztuk na okres 3 lat.
4. Zapewnienia Dzierżawcy, licencji oprogramowania dla wirtualizacji fizycznych serwerów w ilości odpowiadającej łącznej ilości procesorów fizycznych serwerów określonych w Tabeli 1 wraz z 3 letnim uprawnieniem do uzyskania aktualizacji, nowych wersji oprogramowania oraz wsparcia technicznego producenta oprogramowania lub podmiotu przez niego uprawnionego. Wymagania dotyczące minimalnych wymaganych funkcjonalności określono w tabeli 4.
5. Zapewnienia Dzierżawcy, licencji oprogramowania dla zarządzania oprogramowaniem dla wirtualizacji fizycznych serwerów w wersji odpowiadającej możliwość zarządzania środowiskiem dla co najmniej czterech serwerów fizycznych określonych w Tabeli 1 wraz z 3 letnim uprawnieniem do uzyskania aktualizacji, nowych wersji oprogramowania oraz wsparcia technicznego producenta oprogramowania lub podmiotu przez niego uprawnionego.
6. Instalacji, konfiguracji oraz aktualizacji oprogramowania udostępnianej infrastruktury oraz wykonania usług związanych z migracją istniejących serwerów wirtualnych w ilości minimum 37 szt. wraz z migracją danych zapisanych na aktualnie eksploatowanej pamięci masowej. Dzierżawca informuje, że aktualnie eksploatuje środowisko oparte na oprogramowaniu VMWare 5.5 Enterprise Plus, oparte na dwóch fizycznych serwerach, przełącznikach sieciowych w technologii Fiber Channel oraz pamięć masową posiadającą pojemność użytkową 12 TB. Wydzierżawiający zobowiązany jest przeprowadzić migrację posiadanych przez Dzierżawcę zasobów do nowego środowiska w sposób minimalizujący czas niedostępności i przestojów. Wydzierżawiający winien w terminie 14 dni od podpisania Umowy przedstawić Dzierżawcy planowany scenariusz migracji, a Dzierżawca w terminie kolejnych 7 zatwierdzić lub wnieść uwagi.

Wymagania ogólne dla udostępnianego sprzętu i oprogramowania:

1. Wszystkie urządzenia udostępniane Dzierżawcy muszą być fabrycznie nowe i wyprodukowane nie później niż 6 miesięcy przed datą dostawy.
2. Wszystkie urządzenia udostępniane Dzierżawcy muszą być objęte gwarancją producenta na okres od chwili uruchomienia produkcyjnego środowiska, potwierdzonego protokołem zdawczo – odbiorczym do ostatniego dnia miesiąca, w którym nastąpi zapłata ostatniej 35 - raty dzierżawnej, a Dzierżawca musi zachować prawo do bezpośredniego kontaktu z producentem sprzętu udostępnionego przez Wydzierżawiającego.
3. Serwis gwarancyjny dla urządzeń udostępnianych przez Wydzierżawiającego musi zapewniać prawo do składania zleceń związanych z serwisem 24 godziny na dobę przez 7 dni w tygodniu. Obsługa serwisowa musi być realizowana za pośrednictwem dedykowanego oprogramowania dla obsługi sprzętu udostępnionego. Gwarantowany czas usunięcia awarii przez producenta lub jego upoważnionego przedstawiciela nie może przekroczyć 24 godzin. W całym okresie trwania gwarancji wszystkie usługi serwisu gwarancyjnego mają być świadczone w siedzibie Dzierżawcy. Dzierżawca nie dopuszcza dostawy sprzętu zastępczego na czas wykonania naprawy o parametrach innych niż ujęte w zgłoszeniu tj. Dzierżawca, z uwagi na specyfikę środowiska, nie dopuszcza podstawienia sprzętu o innych parametrach.
4. Wydzierżawiający zobowiązany jest dostarczyć wszystkie elementy komunikacyjne pochodzące od producenta oferowanego sprzętu.
5. Udostępniany sprzęt wskazany z tabeli 1, 2 oraz 3 winien pochodzić od tego samego producenta. W przypadku zaoferowania sprzętu pochodzącego od różnych producentów Wydzierżawiający zobowiązany jest załączyć do oferty oświadczenia producentów w zakresie kompatybilności oferowanego sprzętu.
6. Wydzierżawiający zobowiązany jest do wskazania konkretnych parametrów sprzętu i oprogramowania będącego przedmiotem oferty w sposób umożliwiających ich identyfikację w sposób jednoznaczny i niebudzący wątpliwości.

Tabela 1 - Serwery

|  |  |  |
| --- | --- | --- |
| Nazwa elementu, parametru lub cechy | Opis wymagań | Parametry dodatkowo punktowane |
| Ilość sztuk | 2 szt. |  |
| Obudowa | Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych | Nie dotyczy |
| Procesor | Architektura x86, maksymalny TDP dla procesora 85W. Co najmniej 8 rdzeni w każdym procesorze. Wynik wydajności procesora instalowanego w oferowanym serwerze, w konfiguracji dwuprocesorowej, powinien wynosić co najmniej 60,4 punktów w SPEC w teście SPECint2006 Results -- Results opublikowanych przez SPEC.org ([www.spec.org](http://www.spec.org)) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów. | Dodatkowe kolejne rdzenie procesora –5 punktów |
| Liczba zainstalowanych procesorów | Min. 2 | Nie dotyczy |
| Płyta główna | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania co najmniej dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon) | Nie dotyczy |
| Pamięć operacyjna | Zainstalowane co najmniej 128 GB pamięci RAM co najmniej DDR4 w modułach o pojemności co najmniej 16GB każdy, o taktowaniu co najmniej 2666MHz.  Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM.  Pamięć o częstotliwości co najmniej 2666MHz. Możliwość rozbudowy RAM do co najmniej 3TB (dopuszcza się wymianę modułów pamięci) | Dodatkowe 32 GB zainstalowanej pamięci RAM – 10 punktów |
| Zabezpieczenie pamięci | ECC, Memory Mirroring, Memory Rank Sparing, Patrol Scrubbing oraz Demand Scrubbing. | Nie dotyczy |
| Procesor Graficzny | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz z głębią koloru co najmniej 16 bitów/piksel. | Nie dotyczy |
| Dyski | Zainstalowane dyski na system operacyjny:  - 2 dyski M.2, skonfigurowane w RAID 1, o pojemności co najmniej 32GB każdy.  Wymagana jest możliwość zastosowania w obudowie serwera modułu dyskowego (lub modułów dyskowych), którego gniazda dyskowe pozwalają na zamienne zastosowanie dysków SAS/SATA 2,5” oraz dysków NVMe w formacie 2,5” w tym samym gnieździe dyskowym, z możliwością uzyskania co najmniej 8 takich gniazd dyskowych w pojedynczym serwerze. | Nie dotyczy |
| Zasilacz | Minimum dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie przekraczającej 750W, z certyfikatem minimum Platinum. | Nie dotyczy |
| Interfejsy sieciowe | Zainstalowane i w pełni funkcjonalne interfejsy:  - co najmniej 1 port 10/100/1000 Ethernet RJ-45 dedykowany do celów administracyjnych  - co najmniej 2 porty 10Gbps Ethernet SFP+ SR, rozłożone równo pomiędzy co najmniej dwie niezależne od siebie karty. Wszystkie karty LAN 10Gbps muszą być zbudowane z zastosowaniem technologii tego samego producenta.  - co najmniej 2 porty 16Gbps FC, rozłożone równo pomiędzy co najmniej dwie niezależne od siebie karty. Wszystkie karty FC muszą być zbudowane z zastosowaniem technologii tego samego producenta. | Nie dotyczy |
| Dodatkowe porty | * z przodu obudowy: 1x USB 3.0, 1x USB 2.0 z dostępem dla podsystemu zarządzania (modułu administracyjnego) serwera, niezależnie od zainstalowanego systemu operacyjnego. * z tyłu obudowy: 2x USB 3.0, 1x DB-15 VGA. | Nie dotyczy |
| Chłodzenie | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 | Nie dotyczy |
| Zarządzanie | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania, umożliwiający:   * Zbieranie i przeglądanie informacji o systemie oraz inwentaryzacja * Monitorowanie statusu systemu oraz jego stanu * Podnoszenie alarmów oraz wysyłanie informacji * Zapisywanie zdarzeń w dzienniku * Konfigurowanie połączeń sieciowych * Konfigurowanie bezpieczeństwa * Aktualizowanie oprogramowania wewnętrznego (firmware) * Konfigurowanie ustawień serwera oraz urządzeń * Monitorowanie zużycia energii elektrycznej w czasie rzeczywistym * Zdalne kontrolowanie zasilania serwera (włączenie, wyłączenie, restart) * Zarządzanie kluczami aktywacyjnymi funkcji na żądanie (FoD) * Przekierowywanie konsoli szeregowej poprzez IPMI * Przechwytywanie treści wyświetlanej na konsoli w przypadku zawieszenia się systemu operacyjnego * Zdalny podgląd treści konsoli w rozdzielczości co najmniej 1920x1200 przy odświeżaniu z częstotliwością 60 Hz i głębią koloru co najmniej 16 bitów / piksel * Zdalny dostęp do serwera z użyciem klawiatury i myszy zdalnej stacji klienckiej * Zdalne instalowanie systemu operacyjnego * Alarmowanie za pośrednictwem Syslog * Przekierowanie konsoli szeregowej poprzez SSH * Wyświetlanie grafiki z danymi w czasie rzeczywistym oraz z danymi historycznymi na temat poboru mocy i temperatury * Ograniczanie poboru mocy * Mapowanie obrazu ISO i plików obrazów nośników, zlokalizowanych w lokalnej stacji klienckiej jako wirtualnych napędów, dostępnych do użycia przez serwer * Montowanie zdalnych obrazów ISO I plików obrazów nośników poprzez HTTPS, SFTP, CIFS i NFS * Współpraca co najmniej sześciu użytkowników konsoli wirtualnej * Kontrolowanie jakości i wykorzystania pasma komunikacyjnego * Obsługa co najmniej następujących interfejsów komunikacyjnych: IPMI v2.0, SNMP v3, CIM, DCMI v 1.5, REST API, WWW na bazie HTML 5, CLI (wiersz komend). * Dostęp przy pomocy smartfona z systemem Android oraz z systemem iOS, z zainstalowaną aplikacją, dostarczaną przez producenta serwera, poprzez port USB z przodu serwera, z możliwością co najmniej sprawdzenia stanu i statusu serwera, poziomu firmware, ustawień sieciowych i alarmów, a także z możliwością włączenia, wyłączenia i zrestartowania serwera. Ze względów bezpieczeństwa, nie dopuszcza się komunikacji bezprzewodowej pomiędzy serwerem a smartfonem. | Nie dotyczy |
| Funkcje zabezpieczeń | Hasło włączania, hasło administratora, moduł TPM z możliwością przełączania w UEFI pomiędzy wersją 1.2 a 2.0.  Możliwość zastosowania zamykanego na klucz panelu przedniego serwera. | Nie dotyczy |
| Urządzenia hot swap | Co najmniej dyski, zasilacze oraz wentylatory | Nie dotyczy |
| Obsługa | Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane’y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych. | Nie dotyczy |
| Diagnostyka | Wbudowany system analizy predykcyjnej, pozwalający na przewidywanie możliwości wystąpienia awarii serwera. Analiza musi obejmować co najmniej: procesory, regulatory napięcia, pamięć operacyjną (RAM), dyski wewnętrzne, wentylatory, zasilacze, kontrolery RAID  Możliwość użycia aplikacji mobilnej na smartfonie z systemem Android oraz iOS, podłączonym do serwera poprzez port USB z przodu obudowy, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. Odpowiednie licencje należy uwzględnić w ofercie. | Nie dotyczy |
| Wspierane systemy operacyjne | Microsoft Windows Server 2012 R2 i 2016, Red Hat Enterprise Linux 6 oraz 7, SUSE Linux Enterprise Server 11 oraz 12, VMware vSphere (ESXi) 6.0 oraz 6.5. | Nie dotyczy |
| Waga | Nie więcej niż 32 kg w maksymalnej możliwej konfiguracji serwera. | Nie dotyczy |
| Gwarancja i serwis | Co na okres od chwili uruchomienia produkcyjnego środowiska, potwierdzonego protokołem zdawczo – odbiorczym  do ostatniego dnia miesiąca, w którym nastąpi zapłata ostatniej 35 - raty dzierżawnej producenta. Obsługa 24 godziny na dobę, 7 dni w tygodniu. Gwarantowany czas naprawy 24h. Wszelkie uszkodzone nośniki danych pozostają u Dzierżawcy.  W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie „Diagnostyka” (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji do 36 miesięcy 7/24 fix 4h oraz zainstalowania dodatkowego dla każdej lokalizacji systemu monitoringu (na dedykowanym serwerze o parametrach rekomendowanych przez producenta oprogramowania monitorującego).  Możliwość generowania zleceń serwisowych w dedykowanej aplikacji bezpośrednio połączonej z systemem obsługi technicznej dostawcy pozwalającej na nadawanie odpowiednich uprawnień operatorom a także zapewniający fizyczny sprzętowy klucz uwierzytelnienia operatora. Niezbędne licencje należy uwzględnić w ofercie. | Nie dotyczy |

Tabela 2 – Pamięć masowa

|  |  |  |
| --- | --- | --- |
| Nazwa elementu, parametru lub cechy | Opis wymagań | Parametry dodatkowo punktowane |
| Pamięć masowa | Pamięć masowa musi zostać dostarczona w postaci pamięci masowej produkcyjnej. | Nie dotyczy |
| Obudowa | Do montażu w szafie rack 19", obudowa kontrolera o wysokości nie większej niż 2U, umożliwiająca instalację co najmniej 24 dysków 2,5".  Obudowa zawierająca kontrolery musi również zawierać gniazda do instalacji co najmniej 24 dysków 2,5”. | Nie dotyczy |
| Zainstalowane dyski | - Co najmniej 5 dysków HotSwap SSD o pojemności co najmniej 400GB każdy  - Co najmniej 19 dysków HotSwap HDD o pojemności co najmniej 900GB każdy, o prędkości obrotowej co najmniej 10k rpm | Zestaw 5 dodatkowych dysków twardych typu NL-SAS 7200 obrotów na minutę o pojemności min 6TB – 10 punktów |
| Zasilanie | Co najmniej dwa zasilacze 230V/50Hz, pracujące redundantnie, Zasilacze muszą posiadać możliwość wymiany bez zatrzymywania pamięci masowej tzw. Hot Swap. | Nie dotyczy |
| Kontrolery | Co najmniej dwa kontrolery, pracujące redundantnie. Kontrolery muszą być posiadać możliwość wymiany bez zatrzymywania pamięci masowej tzw. Hot Swap. | Nie dotyczy |
| Obsługiwane grupy RAID | Co najmniej RAID 0, 1, 5, 6, 10 | Nie dotyczy |
| Pamięć cache | Co najmniej po 8GB na każdym kontrolerze - mirroring pomiędzy kontrolerami. Wymagane zabezpieczenie pamięci cache przed utratą zawartości przy utracie zasilania. | 16GB na każdym kontrolerze mirroring pomiędzy kontrolerami. Wymagane zabezpieczenie pamięci cache przed utratą zawartości przy utracie zasilania – dodatkowe 15 punktów |
| Możliwość rozbudowy systemu dyskowego | Dostępność półek dyskowych na dyski 2,5" oraz na dyski 3,5" z możliwością mieszania półek na dyski 2,5" i dyski 3,5" w tej samej macierzy dyskowej. Możliwość dołączenia co najmniej 10 dodatkowych półek dyskowych do półki z kontrolerami, przy zachowaniu redundancji połączeń. | Nie dotyczy |
| Sposób podłączenia dodatkowych półek dyskowych | Każda dodatkowa półka dyskowa musi posiadać dwa pracujące redundantnie moduły komunikacyjne Hot Swap. Dodatkowa półka dyskowa musi być podłączona do macierzy dyskowej co najmniej dwoma pracującymi redundantnie połączeniami, każde w technologii SAS 12Gbps lub szybszej, przy czym każda półka dyskowa musi komunikować się z każdym kontrolerem. | Nie dotyczy |
| Rozbudowa pojemności | Rozbudowa pojemności pamięci masowej w zakresie zarówno instalowania dodatkowych dysków jak również dodatkowych półek dyskowych musi odbywać się bez konieczności zakupu dodatkowych licencji z tytułu rozbudowy pojemności/dokładania kolejnych dysków. W przypadku zaoferowania pamięci masowej objętej koniecznością zakupu licencji oprogramowania na rozbudowę pamięci masowej dostawca winien uwzględnić w cenie ich koszt dla deklarowanej przez producenta pojemności. | Nie dotyczy |
| Sposób podłączenia dysków do kontrolerów | Każdy dysk podłączony dwoma portami SAS 12Gbps, po jednym porcie do każdego kontrolera pamięci masowej. W przypadku dodatkowych półek dyskowych każdy dysk musi być podłączony dwoma portami SAS 12Gbps, po jednym porcie do każdego modułu komunikacyjnego w półce dyskowej. Wszystkie dyski muszą być Hot Swap. | Nie dotyczy |
| Interfejsy komunikacyjne do podłączenia hostów | - Co najmniej po dwa porty 1Gbps Ethernet z obsługą iSCSI na każdym kontrolerze.  - Co najmniej po dwa porty SAS 12Gbps na każdym kontrolerze  - Co najmniej po cztery porty 16Gbps FC na każdym kontrolerze. Porty FC musza być w standardzie SFP+ i muszą być obsadzone wkładkami optycznymi 16Gbps SW ze złaczami LC. Wkładki muszą zapewniać funkcjonalność wymiany bez zatrzymywania pamięci masowej tzw. Hot Swap. | Nie dotyczy |
| Wymagane funkcje kontrolerów - wymienione funkcje muszą być obecne w oferowanej macierzy i gotowe do użycia. | Thin Provisioning, kopie migawkowe (snapshoty) - co najmniej 64 relacje źródło - cel. Jednorazowa migracja danych z zewnętrznej macierzy dyskowej, w tym macierzy innego producenta niż oferowana macierz. Wykonywanie kopii synchronicznej danych z jednej macierzy na drugą pamięć masową tej samej rodziny. Grupy RAID 5 i RAID 6 z dyskami zapasowymi (spare disk). W grupach RAID 5 oraz RAID 6 z dyskami zapasowymi (spare drive) dyski zapasowe muszą być używane podczas normalnej pracy macierzy do zapisu danych, a przestrzeń zapasowa musi być rozdystrybuowana na wszystkie dyski w grupie RAID. Grupa RAID z rozdystrybuowaną przestrzenią zapasową musi umożliwiać obsługę co najmniej 128 dysków w jednej grupie RAID. Funkcja tieringu danych pomiędzy dyskami HDD i SSD. Macierz musi umożliwiać migrację danych z zewnętrznej macierzy dowolnego producenta, wyposażonej w interfejsy FC i udostępniającej dane standardowym protokołem FC. Migracja danych musi się odbywac z zastosowaniem wyłącznie metod dostępnych w oferowanej macierzy, bez pomocy zewnętrznego oprogramowania. Proces migracji danych z zewnętrznej macierzy na zasoby własne oferowanej macierzy musi przebiegać w taki sposób, aby hosty podłączone do oferowanej macierzy, a nie podłączone do zewnętrznej macierzy, mogły korzystać z migrowanych danych w trakcie ich migracji.  Oprogramowanie do realizacji zdalnej replikacji na macierz tego samego rodzaju dla całej proponowanej konfiguracji. Wymagane jest zapewnienie niezbędnych do tych celów licencji oprogramowania na okres min 3 lat. | Nie dotyczy |
| Wymagane możliwości rozbudowy funkcji macierzy - wymienione funkcje muszą być dostępne do zakupienia w chwili oferowania macierzy lub obecne w oferowanej macierzy | Możliwość zwiększenia liczby relacji źródło - cel dla kopii migawkowych do co najmniej 2000. | Nie dotyczy |
| Wymagana liczba udostępnianych wolumenów logicznych | nie mniej niż 2000 | Nie dotyczy |
| Wymagana wielkość logicznego wolumenu | nie mniej niż 256TB | Nie dotyczy |
| Wymagana liczba grup RAID | nie mnie niż 128 | Nie dotyczy |
| Wymagana liczba obsługiwanych hostów | nie mniej niż 256 | Nie dotyczy |
| Wymagana liczba portów per host | nie mniej niż 32 | Nie dotyczy |
| Wymagany dostęp administracyjny | Dwa porty 1Gbps Ethernet (po jednym na każdym kontrolerze) - porty mogą być te same co do obsługi iSCSI. Dostęp przez WEB-based GUI oraz SSH CLI oraz SMI-S oraz SNMP oraz notyfikacje poprzez e-mail. | Nie dotyczy |
| Wymagane metody zabezpieczenia dostępu administracyjnego | SSL oraz SSH oraz autentykacja LDAP. |  |
| Serwis | co najmniej 3 lata, zgłaszanie problemów 24h na dobę, 7 dni w tygodniu, z gwarantowanym czasem naprawy w 24 godziny w miejscu eksploatacji. Wymieniane dyski pozostają u Dzierżawcy. | Nie dotyczy |

Tabela 3 – Przełącznik Fibre Channel – 2 sztuki

|  |  |  |
| --- | --- | --- |
| Nazwa elementu, parametru lub cechy | Opis wymagań | Parametry dodatkowo punktowane |
| Obudowa | Przeznaczona do montażu w szafie rack 19”, o wysokości nie większej niż 1U.  Obudowa musi być wyposażona we wszystkie elementy, niezbędne do zamontowania przełącznika w szafie rack 19”. | Nie dotyczy |
| Porty | Co najmniej 24 gniazda na wkładki SFP+. Co najmniej 12 gniazd aktywnych i obsadzonych wkładkami 16Gbps FC, wielomodowymi, o zasięgu co najmniej 125m przy zastosowaniu światłowodu OM4 i przy prędkości transmisji 16Gbps. Aktywacja dodatkowych portów realizowana wyłącznie programowo za pośrednictwem odpowiednich licencji.  Wkładki SFP+ 16Gbps FC musza obsługiwać autosensing i muszą automatycznie dostosowywać się do pracy z przepustowościami 4Gbps, 8Gbps i 16Gbps. | Nie dotyczy |
| Obsługiwane typy portów | Obsługa trybu Full Fabric oraz trybu Access Gateway. Jesli wymagane odpowiednie licencje nalezy uwzględnić.  Obsługa portów FL\_Port, F\_Port, M\_Port, E\_Port, D\_Port oraz N\_Port NPIV. | Nie dotyczy |
| Obsługiwane rodzaje ruchu | Unicast, Multicast, Broadcast | Nie dotyczy |
| Class of Service | Class 2, Class 3 oraz Class F | Nie dotyczy |
| Zagregowana przepustowość | Co najmniej 384Gbps | Nie dotyczy |
| Zużycie energii | Nie więcej niż 3.4 watt na port zdefiniowany jako 16Gbps | Nie dotyczy |
| Port Zarządzania | Dedykowany do obsługi przełącznika min 10/100Mbps port w standardzie RJ45 oraz modulowany RS232 w oparciu o niezależny port fizyczny w standardzie RJ45 | Nie dotyczy |
| Port USB | Wymagany, dostępny od strony portów dostępowych przełącznika | Nie dotyczy |
| Opóźnienia | Nie większe niż 0,7 mikrosekundy (dopuszcza się wzrost do 1,1 mikrosekundy w przypadku włączenia FEC | Nie dotyczy |
| Zasilanie I chłodzenie | Dwa zasilacze. Każdy z zasilaczy wyposażony w min 2 wentylatory pracujące w trybie 2+2. | Nie dotyczy |
| Gwarancja | na okres od chwili uruchomienia produkcyjnego środowiska, potwierdzonego protokołem zdawczo – odbiorczym do ostatniego dnia miesiąca, w którym nastąpi zapłata ostatniej 35 - raty dzierżawnej producenta, 24x7, gwarantowany czas naprawy 24h. Gwarancja obejmuje uprawnienia do aktualizacji oprogramowania. | Nie dotyczy |

Tabela 4 – Oprogramowanie do wirtualizacji serwerów fizycznych i zarządzania środowiskiem wirtualnym

|  |
| --- |
| Wymagane jest dostarczenie licencji na oprogramowanie VMware vSphere ESXi,  w najnowszej dostępnej wersji, dla minimum 4 fizycznych CPU (lub większej w przypadku zaoferowania serwerów z większą ilością zainstalowanych procesorów niż 2 na serwer) z funkcjonalnościami: |
| * 1. Wirtualizator środowiska instalowany bezpośrednio na warstwie fizycznej umożliwiający współdzielenie zasobów sprzętowych typu procesor, pamięć, dysk, karta sieciowa przez różne systemy operacyjne |
| * 1. Sposób licencjonowania środowiska umożliwiający rozbudowę o kolejne fizyczne serwery bez potrzeby uprzedniej aktualizacji już działającego oprogramowania. |
| * 1. Technologia zapewniania wysokiej dostępności przy wykorzystaniu mechanizmu High Availability oraz Fault Tolerance. Technologia Fault Tolerance realizowana od 2 do 4 wirtualnych procesorów. |
| * 1. Technologia automatycznego przenoszenia działających maszyn wirtualnych w obrębie dostępnej infrastruktury wirtualnej dla równoważenia obciążenia poszczególnych maszyn wirtualnych |
| * 1. Technologia umożliwiająca uruchamianie wirtualnych przełączników sieci LAN |
| * 1. Technologia umożliwiająca przenoszenie działających maszyn wirtualnych pomiędzy fizycznymi serwerami działającymi w ramach środowiska wirtualnego bez utraty działających usług i bez konieczności planowania przerw w działaniu maszyny wirtualnej |
| * 1. Technologia zapewniająca szyfrowanie maszyn wirtualnych zarówno w obszarze przydzielonej puli dyskowej jak również danych aplikacji. |
| * 1. Technologia optymalizująca zużycie energii poprzez automatyczne przenoszenie działających maszyn wirtualnych pomiędzy serwerami oraz wyłączanie niewykorzystywanych serwerów. |
| * 1. Technologia nadawania priorytetów dostępu do puli dyskowych maszyn wirtualnych poprzez monitoring obciążenia I/O dla woluminów dyskowych z jednoczesną, dynamiczną, priorytetyzacją ruchu dla wybranych maszyn wirtualnych. |
| * 1. Technologia obniżająca opóźnienia w ruchu sieciowym poprzez prezentowanie pojedynczego fizycznego adaptera serwera fizycznego jako wielu odseparowanych logicznych adapterów dla maszyn wirtualnych. |
| * 1. Technologia proaktywnego przenoszenia działających maszyn wirtualnych pomiędzy fizycznymi serwerami pracującymi w środowisku na wypadek detekcji /wykrycia potencjalnej awarii zasobu sprzętowego. |
| * 1. technologia pozwalająca na jednoczesne połączenie z zasobami sieci SAN za pomocą wielu światłowodów (multipathing), |
| * 1. technologia pozwalająca na wirtualizację aplikacji, |
| * 1. Technologia umożliwiająca przechowywanie konfiguracji i ustawień dla poszczególnych wirtualnych maszyn umożlwiająca ich przechowywanie jako wzorzec dla innych hostów środowiska. |
| * 1. Technologia monitorowania zmian konfiguracji poszczególnych hostów zapewniająca automatyczne powiadomienia dla administratora |
| * 1. Technologia udostępniania natywnej wydajności kart graficznych opatrzonych koprocesorami 2D/3D dla maszyn wirtualnych (vGPU) |
| * 1. technologia pozwalająca na tworzenie wirtualnych, rozproszonych przełączników sieciowych, |
| * 1. oprogramowanie serwera (licencja na 1 CPU, dla MS Windows Server 2012 lub nowszy) zapewniające ujednolicone zarządzanie za pomocą jednej konsoli wszystkimi hostami oraz urządzeniami wirtualnymi w środowisku wirtualnym Dzierżawcy, umożliwiające administratorom kontrolę nad środowiskiem i ułatwiające wykonywanie codziennych zadań, zgodne z wersją dostarczonego środowiska, |
| * 1. Wraz z oprogramowanie realizującym powyższe funkcjonalności Wydzierżawiający zapewni oprogramowanie zarządzające dedykowane dla administrowania środowiskiem. Oprogramowanie do zarządzania musi za pośrednictwem dedykowanej konsoli instalowanej na serwerach dostarczonej infrastruktury prezentować wszystkie zdefiniowanie maszyny wirtualne oraz umożliwiać administrowanie zasobami maszyn wirtualnych za pośrednictwem panelu administratora. Konsola zarządzania środowiskiem musi udostępniać usługi co najmniej dla wszystkich serwerów fizycznych dostarczonych dla potrzeby zadania a także zapewnić: |
| * + 1. Umożliwić działanie odrębnej instancji wirtualnego serwera zarządzania co najmniej w konfiguracji zapewniającej ciągłość dostępu do konsoli na wypadek awarii (funkcjonalność failover) |
| * + 1. Umożliwić prezentację treści wielu instancji konsoli zarządzania w postaci pojedynczego interfejsu administracyjnego. |
| * + 1. Automatyzację zadań związanych z administracją zasobami środowiska wirtualnego. |
| * 1. W przypadku ograniczeń prawnych dotyczących sposobu zakupu, wynikających  z postanowień licencyjnych Producenta Oprogramowania, Dzierżawca wymaga zakupu przez Wydzierżawiającego wymaganych licencji na rzecz Dzierżawcy. |

Tabela 5: Wirtualna zapora ogniowa następnej generacji (Next Generation FireWall)

|  |
| --- |
|  |
| Wymagania ogólne:  System zabezpieczeń firewall musi być dostarczony jako specjalizowane wirtualne urządzenie zabezpieczeń sieciowych (tzw. virtual appliance) do uruchomienia w środowisku VMware ESXi, VMware NSX lub Microsoft Hyper-V.  System zabezpieczeń firewall musi zapewniać wewnętrzne wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie architektury systemu, tj. w/w moduły muszą pracować na różnych wirtualnych rdzeniach procesora przydzielonych przez środowisko wirtualizacyjne. Musi istnieć możliwość niezależnego od siebie restartowania modułu zarządzania i modułu przetwarzania ruchu sieciowego.  System zabezpieczeń firewall musi umożliwiać działanie w następujących trybach pracy:  rutera (tzn. w warstwie 3 modelu OSI),  przełącznika (tzn. w warstwie 2 modelu OSI),  w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)  w trybie pasywnego nasłuchu (sniffer).  Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych.  System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tablice routingu. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.  System zabezpieczeń firewall musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active. |
| Wymagania dot. Platformy:  System zabezpieczeń firewall musi obsługiwać co najmniej 4096 interfejsów logicznych i fizycznych.  System zabezpieczeń firewall musi być wyposażony w co najmniej jeden dedykowany interfejs do zarządzania Out-of-Band z własną tablicą routingu.  System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać min. 4094 znaczników VLAN.  System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 8 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji,  System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 4 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering)  System zabezpieczeń firewall musi obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 60 000 połączeń na sekundę.  System zabezpieczeń firewall musi umożliwiać realizację połączeń VPN z przepustowością nie mniejszą niż 4 Gbps. |
| Podstawowe wymagania funkcjonalne:  System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).  Polityka zabezpieczeń firewall musi uwzględniać  strefy bezpieczeństwa,  adresy IP klientów i serwerów,  protokoły i usługi sieciowe,  aplikacje,  kategorie URL,  użytkowników aplikacji,  reakcje zabezpieczeń,  rejestrowanie zdarzeń i alarmowanie  zarządzanie pasmem w sieci w oparciu o  priorytet,  pasmo gwarantowane,  pasmo maksymalne,  oznaczenia DiffServ  System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.  System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.  Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach UDP i TCP. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.  Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole, gdzie definiowane są aplikacje i oddzielne pole, gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu, a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość” w polityce.  System zabezpieczeń firewall musi wykrywać co najmniej 2 500 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.  System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.  System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antymalware, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.  System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.  System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.  System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.  System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.  System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta musi być traktowana jako stanowiąca automatyczne wyjątki od ogólnych reguł deszyfracji.  System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.  System firewall musi automatycznie weryfikować spójność konfiguracji polityk bezpieczeństwa z punku widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook” potrzebne jest dodatkowo użycie aplikacji „SSL”, a administrator nie uwzględni tej aplikacji w polityce, to system powinien ostrzec o tym fakcie administratora w momencie zatwierdzania nowej polityki.  System firewall musi posiadać możliwość zastosowania jako kryteriów dopasowywania ruchu w regułach polityki firewall obiektów dynamicznych typu: listy adresów IP, listy nazw domen FQDN, listy URL. Zawartość list dynamicznych powyższych typów powinna być aktualizowana automatycznie ze wskazanych w definicji obiektu zewnętrznych źródeł, zgodnie z zadanym harmonogramem czasowym w przedziałach od 5 min. do 30 dni.  Urządzenia posiadają możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Istnieje możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie. |
| Wymaganie dotyczące identyfikacji użytkowników:  System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci  System zabezpieczeń firewall musi zapewniać integrację z  Active Directory,  Ms Exchange,  Citrix,  LDAP  serwerami Terminal Services  Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet, gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.  System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w system zabezpieczeń firewall, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia” logowania użytkowników.  System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku, gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
| Wymagania dot. warstwy sieci:  System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.  System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.  System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.  System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.  System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.  System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).  System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów.  Polityki definiujące powinny umożliwiać wykorzystanie  adresów źródłowych,  adresów docelowych,  użytkowników,  numerów portów usług  kategorie URL.  System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia  RADIUS,  TACACS+,  LDAP,  Kerberos,  SAML 2.0.  System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.  System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.  System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. |
| Wymagania dotyczące zaawansowanych systemów ochrony:  System firewall musi posiadać mechanizm blokujący możliwości wprowadzania przez użytkowników swoich poświadczeń domenowych (nazwa użytkownika, hasło) podczas dostępu do niezaufanych kategorii stron WWW.  System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW, który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.  System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.  System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.  System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.  System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.  System zabezpieczeń firewall musi posiadać moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.  System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja antymalware lub antyspyware uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur antymalware lub antyspyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.  System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.  System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).  System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.  System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.  System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.  System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym .  Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".  Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.  System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.  System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. |
| Wymagania dotyczące zarządzania:  Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.  System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.  System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.  System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.  System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).  Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.  System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.  System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).  System zabezpieczeń firewall musi przechowywać logi i raporty. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie dopuszcza się, aby do tego celu konieczny był zakup zewnętrznych urządzeń, oprogramowania ani licencji.  System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.  System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.  System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.  System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.  System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.  System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:  ruchu sieciowym,  aplikacjach,  zagrożeniach  filtrowaniu stron www.  System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.  System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.  System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów programowych systemu zabezpieczeń oraz łączy sieciowych. |
| Wymagania dotyczące wsparcia technicznego:  Pomoc techniczna musi być świadczona w języku polskim poprzez centrum kompetencyjne zlokalizowane w Polsce.  Szkolenia dotyczące konfiguracji i obsługi systemu zabezpieczeń firewall muszą być dostępne i świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym zlokalizowanym w Polsce. |
| Wymagania dotyczące dostaw:  Dzierżawca wymaga dostawy 1 urządzenia opisanego powyżej z:  Serwisem 3 letnim obejmującym usuwanie usterek w oprogramowaniu systemowym oraz aktualizacje tego oprogramowania przez okres 3 lat  Subskrypcją na antywirus (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AV) na okres 3 lat  Subskrypcją na antyspyware (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AS) na okres 3 lat  Subskrypcją na IPS na okres 3 lat  Dzierżawca wymaga możliwości rozbudowy o następujące subskrypcje/licencje jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego  Subskrypcją na URL Filtering  Subskrypcja na Remote Access VPN oraz kontrolę stanu stacji  Subskrypcja umożliwiające przesyłanie plików do chmurowego/lokalnego sandboxa |