



Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Wieliszew, 22 listopada 2016 r.

Szanowni Państwo, w związku z przesłanymi pytaniami do przedmiotu prowadzonego postępowania na dostawę, instalację i konfigurację sprzętu IT oraz licencje, w miejscach docelowych wskazanych przez Mazowiecki Szpital Onkologiczny w Wieliszewie, zamawiający przedstawia poniższe pytania, odpowiedzi i wyjaśnienia:

Pytanie nr 1

Serwery aplikacji oraz bazodanowe. Zamawiający wymaga od dostawcy aby serwery posiadały: „Minimum 6 slotów PCI-Express Generacji 3 Full-height, w tym minimum 4 sloty x16 i minimum dwa sloty Full-length.”

Czy zamawiający uzna za rozwiązanie równoważne serwery które będą posiadały: „Minimum 7 slotów PCI-Express Generacji 3, w tym minimum 4 sloty x16 i minimum dwa sloty Full-length.”?

Odpowiedź: Zamawiający uzna za rozwiązanie równoważne

Pytanie nr 2

Serwery aplikacji oraz bazodanowe. Prosimy o wykreślenie zapisu: „Inne: Wbudowany wewnętrzny napęd DVD-RW.” Zapis ten ogranicza tylko i wyłącznie możliwość zaoferowania rozwiązania tylko jednego producenta, napędy DVD-RW nie są wykorzystywane przez klientów ze względu na inną funkcjonalność która jest opisana w podpunkcie „Zarządzanie i obsługa techniczna” a która pozwala na zdalne podłączenie dowolnego napędu do serwera.

Odpowiedź: Według najlepszej wiedzy zamawiającego funkcjonalność jest oferowana przez więcej niż jednego producenta. Zamawiający podtrzymuje zapis.

Pytanie nr 3

Serwery aplikacji oraz bazodanowe. Zamawiający wymaga od dostawcy aby kontrolery macierzowe posiadały: „Możliwość rozbudowy pamięci cache do 4GB poprzez rozbudowę lub wymianę kontrolera.” – według naszej najlepszej wiedzy tego typu rozwiązanie posiada tylko i wyłącznie kontroler macierzowy firmy HPE prosimy o wykreślenie tego zapisu

Odpowiedź: Według najlepszej wiedzy zamawiającego funkcjonalność jest oferowana przez więcej niż jednego producenta. Zamawiający podtrzymuje zapis.

Pytanie nr 4



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Serwery aplikacji oraz bazodanowe. Zamawiający wymaga aby: „Minimum 4 wbudowane porty Ethernet 10/100/1000 Mb/s RJ45 z możliwością rozbudowy do minimum 8 bez zajmowania wymaganych slotów PCI-Express.”

Prosimy o wykreślenie zapisu „z możliwością rozbudowy do minimum 8 bez zajmowania wymaganych slotów PCI-Express” według naszej najlepszej wiedzy tego typu rozwiązanie posiadają tylko i wyłącznie systemy HPE, prosimy o uznanie jako rozwiązania równoważnego dodatkowej czteroportowej karty sieciowej 1Gbit/s Ethernet zajmującej jeden ze slotów PCIe serwera.

Odpowiedź: Zamawiający zgadza się na wykreślenie zapisu.

Pytanie nr 5

Serwery aplikacji oraz bazodanowe. Zamawiający wymaga aby serwery posiadały : „7 x USB (w tym minimum 3 z przodu i dwa z tyłu obudowy)”, Zapis ten wskazuje bezpośrednio na serwery HPE ograniczając inne rozwiązania, prosimy o ograniczenie ilości portów USB do „5 x USB (w tym minimum 1 z przodu i dwa z tyłu obudowy)” – tego typu zapis nie zmniejsza głównych cech serwera takich jak wydajność czy pojemność, a ma na celu jedynie ograniczenie możliwości składania oferty.

Odpowiedź: Według najlepszej wiedzy zamawiającego funkcjonalność jest oferowana przez więcej niż jednego producenta. Zamawiający podtrzymuje zapis.

Pytanie nr 6

Serwery aplikacji oraz bazodanowe. Zamawiający wymaga „Zainstalowany z przodu obudowy panel udostępniający informacje o takich elementach jak: procesory, pamięci, wentylatory, karty sieciowe, zasilacze, sloty PCI, temperatura, numer SN.”

Tego typu rozwiązanie w serwerach 24 dyskowych posiada jedynie HPE prosimy o wykreślenie zapisu.

Odpowiedź: Zamawiający zgadza się na wykreślenie zapisu dotyczącego informacji tylko i wyłącznie numeru SN. Według najlepszej wiedzy zamawiającego pozostałe funkcjonalności są oferowane przez więcej niż jednego producenta. Ponadto Zamawiający nie wymaga dostarczenia serwera z 24 dyskami.

Pytanie nr 7

Serwery aplikacji oraz bazodanowe. Zamawiający wymaga: „Minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta”

Czy zamawiający uzna jako parametr równoważny zapis: „Minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem reakcji do 4 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta” ?

Tego typu zapis pozwoli na zaoferowanie innego rozwiązania.

Odpowiedź: Zamawiający wymaga gwarantowanego przez serwis producenta 6 godzinnego czasu naprawy. Według najlepszej wiedzy te dwa poziomy wsparcia znacząco różnią się w związku z tym Zamawiający nie uzna czasu reakcji za równoważny z czasem naprawy.

Pytanie nr 8

Macierze dyskowe. Zamawiający wymaga: „Oferowana macierz musi wspierać poziomy Raid 0, Raid 1, Raid 1+0, Raid3, Raid 5, Raid 5+0, Raid 6.” RAID

Czy zamawiający dopuści rozwiązanie które będzie zapewniało RAID1, RAID0 RAID5, RAID10, RAID50 a nie będzie posiadało wsparcia dla RAID3 który jest nieaktualnym standardem wypartym przez RAID5?

Odpowiedź: Zamawiający wyraża zgodę na zaoferowane rozwiązanie bez wsparcia RAID3, a które będzie wspierać RAID0, RAID1, RAID1+0, RAID5, RAID5+0, RAID6.

Pytanie nr 7

Macierze dyskowe. Zamawiający wymaga aby oferowana macierz posiadała: „Macierz musi wspierać dyski: min. 400GB SSD, 300/450/600/900/1200GB SAS oraz 1TB, 2TB, 3TB, 4TB, 6TB, 8TB NL-SAS. Macierz musi się rozbudować do min. 190 dysków w ramach oferowanych kontrolerów macierzowych.” Stosowanie dysków 300, 450 GB SAS oraz 1TB, 2TB NL_SAS oraz 8TBze względu na niskie stany magazynowe producentów dysków zostało zakończone, oferowanie tego typu dysków będzie się wiązało

z utrudnionym dostępem do nowych części w przyszłości jak również ze zwiększonym kosztem zakupu tych dysków w przyszłości dlatego też wielu producentów rezygnuje z oferowania ich w swoich rozwiązaniach.

Czy zamawiający dopuści rozwiązanie które nie będzie umożliwiała budowania przestrzeni dyskowej w oparciu o 300, 450 GB SAS oraz 1TB, 2TB NL_SAS a będzie umożliwiała budowanie o dyski 600/900/1200/1800GB a w przyszłości będzie wspierało dyski 8TB?





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Odpowiedź: Zamawiający wyraża zgodę.

Pytanie nr 8

Macierze dyskowe. Zamawiający opisał: „18. Gwarancja - minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.”

Czy zamawiający uzna zapis: Gwarancja - minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem reakcji do 4 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.”?

Odpowiedź: Zamawiający wymaga gwarantowanego przez serwis producenta 6 godzinowego czasu naprawy. Według najlepszej wiedzy te dwa poziomy wsparcia znacząco różnią się w związku z tym Zamawiający nie uzna czasu reakcji za równoważny z czasem naprawy.

Pytanie nr 9

Macierze dyskowe. Zamawiający opisał „Oferowana macierz musi posiadać certyfikat Energy Star lub równoważny”

Czy zamawiający uzna certyfikat EU RoHS Directive 2011/65/EU jako certyfikat równoważny?

Odpowiedź: Według najlepszej wiedzy Zamawiającego certyfikaty dotyczą zupełnie innych norm. Zamawiający nie uzna ich równoważności.

Pytanie nr 10

Urządzenie do archiwizacji. Zamawiający wymaga aby: „Minimum 4 wbudowane porty Ethernet 10/100/1000 Mb/s RJ45 z możliwością rozbudowy do minimum 8 bez zajmowania wymaganych slotów PCI-Express.”

Prosimy wykreślenie zapisu „z możliwością rozbudowy do minimum 8 bez zajmowania wymaganych slotów PCI-Express”

Według naszej najlepszej wiedzy tego typu rozwiązanie posiadają tylko i wyłącznie systemy HPE, prosimy o uznanie jako rozwiązania równoważnego dodatkowej czteroportowej karty sieciowej 1Gbit/s Ethernet zajmującej jeden ze slotów PCIe serwera.

Odpowiedź: Zamawiający zgadza się na wykreślenie zapisu.

Pytanie nr 11





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Urządzenie do archiwizacji. Zamawiający opisał: „18. Gwarancja - minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.”

Czy zamawiający uzna zapis: Gwarancja - minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem reakcji do 4 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.”?

Odpowiedź: Zamawiający wymaga gwarantowanego przez serwis producenta 6 godzinowego czasu naprawy. Według najlepszej wiedzy te dwa poziomy wsparcia znacząco różnią się w związku z tym Zamawiający nie uzna czasu reakcji za równoważny z czasem naprawy.

Pytanie nr 12

Kontrolery sieci WLAN. Zamawiający opisał : „17. Kontroler musi zostać dostarczony z licencjami do obsługi minimum 50 punktów dostępowych, zapory sieciowej oraz WIDS/WIPS i analizatora widma. Wymagana zgodność z normami: a. EN 55022 Class B

Czy zamawiając dopuści rozwiązanie które będzie posiadało certyfikat EN 55022 Class A? Certyfikat EN 55022 Class B jest związany z małymi urządzeniami i nie istnieje na rynku urządzenie które by spełniało powyższe wymagania w całości?

Odpowiedź: Zamawiający wyraża zgodę na zaoferowane rozwiązania z certyfikatem EN 55022 Class A.

Pytanie nr 13

Zgodnie z zapytaniem ofertowym :

„Składając ofertę Wykonawca zobowiązuje się do:

1. terminowej dostawy do siedziby Miejskiego Szpitala Onkologicznego w Wieliszewie, w miejsce wskazane przez Zamawiającego fabrycznie nowego sprzętu, w oryginalnym opakowaniu, gotowego do pracy, o parametrach nie gorszych niż wskazano w Opisie przedmiotu zamówienia - załącznik nr 3 do zapytania ofertowego,
2. terminowej instalacji i konfiguracji sprzętu oraz licencji
3. podpisania protokołu zdawczo-odbiorczego i udzielenia gwarancji min. 60 miesięcy od daty uruchomienia w siedzibie Miejskiego Szpitala Onkologicznego w Wieliszewie
4. dla zadań 1-5 (zgodnie z Opisie przedmiotu zamówienia - załącznik nr 3 do zapytania ofertowego) zapewnić czas naprawy do 6 godzin.”





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Jednocześnie nie jest sprecyzowany sposób spełnienia tego wymogu. Czy w związku z tym jest wymagane oświadczenie producenta sprzętu dla zadań 1-5, że sprzęt dostarczony na potrzeby postępowania będzie fabrycznie nowy, w oryginalnym opakowaniu, gotowy do pracy, o parametrach nie gorszych niż wskazano w Opisie przedmiotu zamówienia oraz, że objęty będzie 5 letnią gwarancją serwisu producenta z gwarantowanym czasem naprawy 6 godzin, oraz pozostawieniem dysków twardej w siedzibie zamawiającego?

Odpowiedź: Tak. Zamawiający wymaga takiego oświadczenia producenta.

Pytanie nr 14

Zamawiający wymaga aby serwery aplikacji oraz bazodanowe posiadały:

Zainstalowany z przodu obudowy panel udostępniający informacje o takich elementach jak: procesory, pamięci, wentylatory, karty sieciowe, zasilacze, sloty PCI, temperatura, numer SN.

Z uwagi na stały w czasie serial number serwera zamawiający zrezygnuje z wymogu wyświetlania serial numberu na przednim wyświetlaczu? Numer ten jest dostępny w innym miejscu na obudowie serwera.

Odpowiedź: Tak. Zamawiający zrezygnuje z wymogu wyświetlania „serial number”.

Pytanie nr 15

Czy w zakresie zakupu nr 9 Zamawiający wymaga pozostawienia dysków twardej w razie awarii w miejscu instalacji sprzętu?

Odpowiedź: Tak. Zamawiający wymaga pozostawienia dysków twardej w razie awarii w miejscu instalacji sprzętu.

Pytanie nr 16

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Dotyczy macierzy dyskowej opisanej w pkt. 3. Macierze dyskowe (2 szt.) pkt. 5

„Oferowana macierz musi wspierać poziomy Raid 0, Raid 1, Raid 1+0, Raid 3, Raid 5, Raid 5+0, Raid 6.”

Czy zamawiający dopuści macierz wspierającą poziomy Raid 0, Raid 1, Raid 1+0, Raid 3, Raid 5, Raid 6?

Odpowiedź: Zamawiający wyraża zgodę na rozwiązanie bez wsparcia RAID3, a które będzie wspierać RAID0, RAID1, RAID1+0, RAID5, RAID5+0, RAID6.

Pytanie nr 17





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Dotyczy macierzy dyskowej opisanej w pkt. 3. Macierze dyskowe (2 szt.) pkt. 15.

„Oferowana macierz musi umożliwiać skorzystanie z tzw. Sub-LUN Tiering, czyli możliwości migracji bloków danych dysku logicznego na podstawie analizy ich aktywności przez macierz (najbardziej i najmniej aktywne) pomiędzy trzema typami dysków (SSD, SAS, NL SAS).”

Czy zamawiający dopuści macierz bez funkcjonalności Sub-LUN Tieringu?

Nie. Zamawiający nie dopuści macierzy bez funkcjonalności Sub-LUN Tieringu.

Pytanie nr 18

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Czy Zamawiający oczekuje dostarczenia dokumentacji projektowej w postaci: Projektu technicznego budowanego rozwiązania, Planu i scenariuszy testów akceptacyjnych, Dokumentacji szkoleniowej, Dokumentacji powykonawczej?

Odpowiedź: Zamawiający wymaga: Projektu technicznego budowanego rozwiązania, Dokumentacji szkoleniowej, Dokumentacji powykonawczej?

Pytanie nr 19

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Zamawiający w punktach 1 i 2 OPZ oczekuje dostawy serwerów, na czym ma polegać uruchomienie tych elementów. Czy w gestii wykonawcy jest instalacja systemów operacyjnych, baz danych i aplikacja lub wirtualizatorów? Jeśli tak prosimy o doprecyzowanie zakresy prac dla tego typu urządzeń.

Odpowiedź: Zamawiający wymaga dostarczenia i montażu dostarczanych serwerów w miejscu wskazanym przez Zamawiającego oraz instalację systemów operacyjnych i wirtualizatorów. Ponadto wymaga utworzenie i konfigurację klastra z serwerów bazodanowych.

Pytanie nr 20

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Zamawiający w punktach 3 i 4 OPZ oczekuje dostawy urządzeń pamięci masowych, na czym ma polegać uruchomienie tych elementów. Prosimy o doprecyzowania zakresu prac dla tego typu urządzeń.





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Odpowiedź: Zamawiający wymaga dostarczenia i montażu dostarczanych macierzy w miejscu wskazanym przez Zamawiającego oraz instalację, konfigurację i przygotowanie do pracy z ww. serwerami.

Pytanie nr 21

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Zamawiający w punkcie 7 OPZ oczekuje dostawy 50 szt. Access Point, prosimy o informacje czy w zakresie prac Wykonawcy ma być pomiar propagacji fal radiowych (Sitesurvey WLAN) w celu wskazania miejsc montażu AP czy to Zamawiający wskaże miejsca montażu Access Point?

Odpowiedź: Zamawiający wymaga aby w zakresie prac Wykonawcy miał być pomiar propagacji fal radiowych w miejscach wskazanych przez Zamawiającego na terenie Szpitala.

Pytanie nr 22

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

Czy w zakresie prac Wykonawcy jest doprowadzenie okablowania strukturalnego do miejsc montażu Access Point?

Odpowiedź: Zamawiający wymaga doprowadzenia okablowania strukturalnego do miejsc montażu Access Pointów od szaf dystrybucyjnych (odległość do 100 m) znajdujących się na każdym piętrze Szpitala.

Pytanie nr 23

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.

W specyfikacji dostarczanego sprzętu nie ma przełączników sieciowych LAN umożliwiających podłączenie Access Point do sieci LAN, czy Zamawiający dysponuje takimi przełącznikami i będą one skonfigurowane do obsługi sieci WLAN czy wykonawca powinien przewidzieć konfiguracje niedostarczanych przełączników przez Wykonawcę do obsługi sieci WLAN?

Odpowiedź: Zamawiający dysponuje takimi przełącznikami i będą one skonfigurowane do obsługi sieci WLAN.

Pytanie nr 24

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3.





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



Zamawiający w punktach 9-11 oczekuje dostawy i uruchomienia urządzeń końcowych (PC, tablety, urządzenia wielofunkcyjne) prosimy o doprecyzowanie, jaki zakres prac jest oczekiwany dla tego typu urządzeń?

Odpowiedź: Zamawiający wymaga tylko dostarczenia ww. sprzętu do Mazowieckiego Szpitala Onkologicznego.

Pytanie nr 25

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3 oraz Wzoru Umowy.

Prosimy o potwierdzenie, że wymagane warunki gwarancyjne zostały sprecyzowane w dokumencie „3_OPZ_Wieliszew.docx” a zapisy umowy w zakresie terminów usunięcia awarii i usterek dotyczą jedynie elementów, dla których taki termin został określony w wyżej wymienionym dokumencie.

Odpowiedź: Zamawiający potwierdza, że warunki gwarancji zostały sprecyzowane w dokumencie „3_OPZ_Wieliszew.docx” .

Pytanie nr 26

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3 Urządzenie UTM.

Wymagania opisujące rozwiązanie wskazują jednoznacznie na rozwiązanie firmy Stormshield. Wymagania te uniemożliwiają zaoferowanie rozwiązań innych producentów, co jest ograniczaniem konkurencji. W związku z powyższym zwracamy się z pytaniem, czy Zamawiający dopuści rozwiązania alternatywne o równie zaawansowanych funkcjonalnościach, jak wymagane, a będących w ofercie innych wiodących producentów na rynku rozwiązań UTM? Alternatywne rozwiązania mogą zaoferować, co najmniej następującą wydajność oraz funkcjonalności:

1. Możliwość budowania klastra Active-Active lub Active-Passive (poprzez dokupienie dodatkowego elementu).
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. Funkcja Firewall daje możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System zapewnia minimum 8 portów Ethernet 10/100/1000 Base-TX, 8 gniazd SFP 1Gbps oraz 2 gniazda 10G SFP+.
6. System umożliwia zdefiniowanie, co najmniej 254 interfejsów wirtualnych – definiowanych, jako VLAN'y w oparciu o standard 802.1Q.





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



7. Firewall obsługuje nie mniej niż 5 milionów jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę.
8. Przepustowość Firewall'a: nie mniej niż 30 Gbps
9. Wydajność szyfrowania VPN IPsec: nie mniej niż 18 Gbps
10. System dla funkcji Firewall wyposażony w lokalny dysk o pojemności minimum 120 GB, który może być wykorzystany do celów logowania i raportowania.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem ma możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanymi dotąd zagrożeń.
12. System ochrony realizuje poniższe funkcje (mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych):
 - a) Kontrola dostępu - zaporą ogniową klasy Stateful Inspection
 - b) Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
 - c) Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN
 - d) Ochrona przed atakami - Intrusion Prevention System
 - e) Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
 - f) Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
 - g) Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
 - h) Kontrola aplikacji – system rozpoznaje aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
 - i) Analiza ruchu szyfrowanego protokołem SSL
 - j) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 6,5 Gbps
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 2,4 Gbps
15. W zakresie funkcji IPsec VPN system realizuje funkcje:
 - a) Tworzenia połączeń w topologii Site-to-site oraz Client-to-site





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



- b) Monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności
 - c) Pracy w topologii Hub and Spoke oraz Mesh
 - d) Możliwości wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
 - e) Obsługi mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN producent dostarcza klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie zapewnia: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń uwzględnia adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz umożliwia skanowanie archiwów typu zip, RAR.
23. Ochrona IPS opierać się na analizie protokołów i sygnatur. Baza sygnatur ataków zawiera minimum 5500 wpisów. Ponadto administrator systemu ma możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo jest możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości, co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www są dostępne takie kategorie stron jak: spyware, malware, spam, proxy. Administrator ma możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń umożliwia weryfikację tożsamości użytkowników za pomocą:





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



- a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
 - b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
 - c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
 - d) Rozwiązanie umożliwia budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
28. Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikaty:
- a) ICSA lub EAL4 dla funkcji Firewall
 - b) ICSA lub NSS Labs dla funkcji IPS
 - c) ICSA dla funkcji: SSL VPN, IPsec VPN
29. Elementy systemu mają możliwość zarządzania lokalnego (HTTPS, SSH) jak i możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
30. Poszczególne elementy funkcjonalne można włączać za pomocą dedykowanych kluczy licencyjnych, co zapewnia Zamawiającemu elastyczność w rozwijaniu systemu bezpieczeństwa w połączeniu z niezbędnymi do tego kosztami.

Odpowiedź: Zamawiający zgadza się na uwzględnienie w postępowaniu rozwiązania spełniającego zaproponowane zapisy, pod warunkiem spełnienia przez nie punktów dotyczących administracji, monitorowania i raportowania w tym co najmniej punkty:

ADMINISTRACJA URZĄDZENIEM

65. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskojęzycznego interfejsu graficznego.
67. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
68. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
70. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).
71. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



RAPORTOWANIE

73. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
 74. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
 75. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
 76. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
 77. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
 78. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
 79. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
- Według wiedzy zamawiającego, zawarte w specyfikacji funkcjonalność są oferowane przez więcej niż jednego producenta.

Pytanie nr 27

Dotyczy Opisu Przedmiotu Zamówienia Załącznik nr 3 Urządzenie System Antywirusowy. Wymagania opisujące rozwiązanie wskazują jednoznacznie na rozwiązanie firmy Kaspersky. Wymaganie te uniemożliwiają zaoferowanie rozwiązań innych producentów, co jest ograniczaniem konkurencji. W związku z powyższym zwracamy się z pytaniem, czy Zamawiający dopuści rozwiązania alternatywne o równie zaawansowanych funkcjonalnościach, jak wymagane, a będących w ofercie innych wiodących producentów na rynku rozwiązań Antywirus? Alternatywne rozwiązania mogą zaoferować, co najmniej następującą funkcjonalności:

W zakresie Ochrony komputerów (stacji roboczych):

- a. Rozwiązanie umożliwia ochronę do 10000 komputerów, z których może korzystać do 8500 użytkowników (co pozwala Zamawiającemu niemal na dowolną rozbudowę systemu zaczynając od wymaganych w OPZ 150 stacji roboczych i 9 serwerów).
- b. System zapewnia funkcje: antywirus, klasyfikację URL, lokalną i chmurową reputacja plików.





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



- c. Rozwiązanie obsługuje skanowanie plików skompresowanych obejmujące najpopularniejsze formaty, w tym co najmniej : TAR, GZIP, ZIP, RAR, 7z.
- d. Centralna konsola zarządzająca – jedna wspólna konsola zarówno dla stacji roboczych jak i serwerów. Również dla komputerów znajdujących się poza siecią lokalną.
- e. Pełne szyfrowanie dysku do 1000 komputerów z systemem Windows 7 Professional, wraz z centralnym zarządzaniem i mechanizmami klasy enterprise do centralnego zarządzania sytuacjami awaryjnymi. Rozwiązanie posiada mechanizm umożliwiający zdalne odblokowanie stacji lub reset hasła. Rozwiązanie posiada funkcjonalność SSO (*Single Sign-on*) dla komputerów z BIOS i systemem Windows 7: użytkownik dokonuje jednokrotnego logowania, dzięki któremu może uruchomić system z zaszyfrowanego dysku i zalogować się do systemu Windows.
- f. Rozwiązanie ma możliwość ochrony przed zmianą konfiguracji przez użytkownika pracującego na stacji końcowej oraz przed odinstalowaniem oprogramowania.
- g. Rozwiązanie posiada wbudowany i zarządzany centralnie moduł firewall'a.
- h. Rozwiązanie posiada moduł ochrony przed exploitami wykorzystującymi podatności systemów operacyjnych oraz najpopularniejszych aplikacji biurowych wykorzystywanych na komputerze.
- i. Rozwiązanie pozwala na wykrywanie i blokowanie wrogich procesów szyfrowania, a także bezstratne odzyskiwanie zaszyfrowanych plików (Ochrona przed *Ransomware* i *CryptoLockerem*).
- j. Rozwiązanie zapewnia integrację z Active Directory, zarówno w celu odwzorowania struktury komputerów jak i autentykacji administratorów do konsol zarządzających.
- k. Rozwiązanie skanuje pliki online jak i wg zdefiniowanego modyfikowalnego harmonogramu. Modyfikacja polega na ustawieniu czasu wykonania, zdefiniowaniu wykluczeń itp.
- l. Rozwiązanie zawiera zintegrowany system typu Host IPS, który wykrywa oznaki aktywnego malware'u i umożliwia wykrywanie nowego, nieznanego dotąd malware'u.
- m. Rozwiązanie posiadać możliwość kontrolowania instalowanych i uruchomianych przez użytkowników aplikacji, a w szczególności blokowania aplikacji wskazanych przez administratora systemu.





Krajowa Fundacja Medyczna
ORGANIZACJA POŻYTKU PUBLICZNEGO (NON-PROFIT)
ul. Łabiszyńska 25, 03-204 Warszawa
tel.: 22 814 32 37, 22 814 32 48 tel./faks: 22 675 88 66



- n. Instalacja rozwiązania w postaci paczki nienadzorowanej umożliwiającej dystrybucję za pomocą SCCM.

W zakresie Ochrona serwerów:

- a. Rozwiązanie umożliwia ochronę antywirusową 3000 serwerów, z których korzysta 8500 użytkowników (co pozwala Zamawiającemu niemal na dowolną rozbudowę systemu zaczynając od wymaganych w OPZ 150 stacji roboczych i 9 serwerów).
- b. Rozwiązanie skanuje pocztę przychodzącą i wychodzącą na serwerach MS Exchange. Obsługuje skanowanie załączników skompresowanych obejmujące najpopularniejsze formaty, w tym co najmniej: TAR, GZIP, ZIP, RAR, 7z.
- c. Rozwiązanie posiada wielowarstwową detekcję w tym także wykorzystującą reputację lokalną i chmurową, dla reputacji plików, url.
- d. Centralna konsola zarządzająca – jedna wspólna konsola zarówno dla stacji roboczych jak i serwerów.
- e. Rozwiązanie posiada system typu Host IPS, który wykrywa oznaki aktywnego malware'u, a także umożliwia wykrywanie nowego, nieznanego dotąd malware'u.
- f. Rozwiązanie obsługuje skanowanie plików skompresowanych obejmujące najpopularniejsze formaty, w tym co najmniej: TAR, GZIP, ZIP, RAR, 7z.
- g. Rozwiązanie posiada możliwość kontrolowania instalowanych i uruchamianych przez administratorów aplikacji na serwerach z rodziny Windows.
- h. Instalacja w postaci paczki nienadzorowanej.

Odpowiedź: Według wiedzy zamawiającego zawarte w specyfikacji funkcjonalność są oferowane przez więcej niż jednego producenta. Zamawiający podtrzymuje zapis.

Jednocześnie Zamawiający informuje, że powyższe pytania, odpowiedzi i wyjaśnienia stanowią integralną część dokumentacji przetargowej. Z uwagi na ich charakter, nie wpływają one na konieczność przedłużenia terminu składania ofert. **Zamawiający informuje, że termin składania i otwarcia ofert pozostaje bez zmian.**

CZŁONEK ZARZĄDU
Beata Kasinska
mgr Beata Kasinska

PREZES ZARZĄDU
Justyna Świeżek
mgr Justyna Świeżek



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

