Zapytanie ofertowe z dnia 30 Października 2023 r. dotyczące zakupu urządzenia sieciowego przez Wojewódzki Inspektorat Farmaceutyczny w Warszawie

Mazowiecki Wojewódzki Inspektor Farmaceutyczny zaprasza do składania ofert cenowych na zakup

Zapora UTM , Serwer , dysk sieciowy , Drukarki Konica Minolta 227

I. Nazwa Zamawiającego:

Wojewódzki Inspektorat Farmaceutyczny w Warszawie
ul. Floriańska 10
03-707 Warszawa
Tel. 22 628 28 60
Fax 22 629 52 53
mail: wif@wif.waw.pl
NIP: 526-17-23-680
Regon: 010034422

II. Przedmiot zamówienia i forma postępowania

1. Zapora UTM(4 sztuki) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 1 do umowy dostawy
2. Serwer(1 sztuka) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 2 do umowy dostawy
3. Synology RS822RP+, Synology RKS-02 (1 sztuka) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 3 do umowy dostawy
4. Drukarka Wielofunkcyjna Konica Minolta 227 (2 sztuki) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 4 do umowy dostawy

Forma postępowania: zapytanie ofertowe

Postępowanie nie podlega ustawie z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605) ponieważ jego wartość nie przekracza wyrażonej w złotych równowartości 130000 PLN.

III. Kryteria oceny i wyboru oferty :

Zamawiający dokona wyboru Wykonawcy, którego oferta spełnia kryteria ustalone w zapytaniu ofertowym oraz została uznana za najkorzystniejszą pod względem ceny.
Wybór oferty dokonany zostanie na podstawie: cena brutto całego zamówienia.
Z Wykonawcą zostanie zawarta umowa - wzór załącznik nr 2. Złożenie oferty jest równoznaczne z akceptacją wszystkich zapisów zawartych we wzorze umowy.

IV. Termin składania ofert:

Do dnia 6 listopada 2023 r. do godz. 9:00 na adres : Wojewódzki Inspektorat Farmaceutyczny w Warszawie

ul. Floriańska 10

03-707 Warszawa lub na adres e-mail : pswiderski@wif.waw.pl

Osobiście , lub doręczenia przez operatora- liczy się data i godz. wpływu oferty do Urzędu.

Zamawiający zastrzega sobie prawo do unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu sporządzania niniejszego zapytania ofertowego.

V. Termin realizacji zamówienia :

14 dni od dnia złożenia zamówienia

VI. Opis sposobu przygotowania oferty :

Ofertę należy złożyć na przygotowanym formularzu ofertowym - załącznik nr 2.

VII. Załączniki do zapytania:

1. wzór umowy z załącznikami
2. formularz oferty

VIII. Kontakt:

Piotr Świderski tel. 22 628 28 60 wew. 25 email: pswiderski@wif.waw.pl

MAZOWIECKI WOJEWÓDZKI
INSPEKTOR FARMACEUTYCZNY
mgr farm. Mariola Kostewicz

Załącznik nr 1 do zapytania ofertowego - wzór umowy

UMOWA DOSTAWY

Zawarta w dniu..... r. w Warszawie pomiędzy:
Wojewódzkim Inspektoratem Farmaceutycznym w Warszawie , 03-707 Warszawa, ul. Floriańska 10,
reprezentowanym przez:
Panią Mariolę Kostewicz-Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego

zwaną w treści umowy „Zamawiającym" a .....

zwaną w treści umowy „Wykonawcą",
o następującej treści:

§1

Przedmiotem umowy jest dostawa sprzętu określonego w ofercie Wykonawcy:

1. Zapora UTM(4 sztuki) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 1
2. Serwer(1 sztuka) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 2
3. Synology RS822RP+(1 sztuka) , Synology RKS-02 (1 sztuka) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 3
4. Drukarka Wielofunkcyjna Konica Minolta 227 (2 sztuki) - Szczegółowa specyfikacja przedmiotu zamówienia - zał. nr 4

1. Do oferowanego sprzętu dołączone będą karty gwarancyjne i instrukcje obsługi.
2. Oferowany sprzęt będzie fabrycznie nowy i dostarczony w oryginalnym opakowaniu.

§2

1. Wykonawca zobowiązuje się zrealizować zamówienie w terminie 14 dni po podpisaniu umowy.
2. Wykonawca zawiadomi przedstawiciela Zamawiającego o rozpoczęciu realizacji umowy z co najmniej dwudniowym wyprzedzeniem.

3. Miejsce dostawy - Wojewódzki Inspektorat Farmaceutyczny w Warszawie 03- 707 Warszawa, ul.

Floriańska 10

4. Odbiór sprzętu w miejscu następuje dwuetapowo:
   - odbiór ilościowy - w chwili dostawy,
   - odbiór jakościowy - po rozpakowaniu urządzenia i uruchomieniu zgodnie z dostarczoną instrukcją przez Zamawiającego z możliwością udziału Wykonawcy.
5. Odbiory sprzętu zakończone są protokołami odbioru (zał. nr 4) z wyszczególnieniem ilościowym sprzętu wraz z numerami seryjnymi oraz potwierdzeniem jego kompletności (odbiór ilościowy) i sprawności (odbiór jakościowy).

§3

1. \N ramach dostawy, Wykonawca zapewni gwarancję na urządzenia będące przedmiotem zamówienia oraz wsparcie techniczne w zakresie konfiguracji oraz obsługi przez okres obowiązywania licencji tj. na okres 12 miesięcy.
2. Wykonawca podejmie czynności zmierzające do naprawy lub wymiany uszkodzonego sprzętu w 24 godziny od momentu zgłoszenia awarii.
3. Wykonawca zapewni naprawę sprzętu w ciągu 14 dni od momentu zgłoszenia awarii.
4. \N przypadku nie podjęcia lub nie wykonania naprawy we wskazanych terminach Zamawiający uprawniony jest do jej wykonania zastępczego na koszt Wykonawcy z zachowaniem gwarancji.

§4

1. Cena za zrealizowanie przedmiotu umowy wynosi ..... zł brutto (słownie: .....).
2. Podstawę do zapłaty należności stanowi faktura VAT sporządzona po wykonaniu przedmiotu zamówienia potwierdzonego protokołami odbioru ilościowego i jakościowego.
3. Zapłata nastąpi przelewem w terminie do 14 dni od daty wpływu faktury do Zamawiającego.

§5

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej, pod rygorem nieważności.

§6

Integralną część umowy stanowi oferta Wykonawcy.

§7

W sprawach nie uregulowanych postanowieniami niniejszej umowy mają zastosowanie odpowiednie

przepisy Kodeksu Cywilnego.

§8

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Załączniki do umowy:

Załączniki nr 1 do 4 - Szczegółowa specyfikacja przedmiotu zamówienia

Załącznik nr 5- Protokół odbioru ilościowego/jakościowego;

Wykonawca Zamawiający

Zał. nr 1 do umowy dostawy
Szczegółowa specyfikacja przedmiotu zamówienia

1. Zapora UTM

Szczegółowe wymagania techniczne dla zapory UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4,4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

Zał. nr 2 do umowy dostawy

Szczegółowa specyfikacja przedmiotu zamówienia

1.Serwer

Typ:	Serwer
Rodzaj produktu:	Do instalacji w szafie RACK - 1U
Ilość kieszeni z funkcją hot-swap:	4
Procesor	
Procesor	Jeden procesor, minimum 6 rdzeniowy, 12 wątkowy, maksymalny TDP dla procesora – 65W.
Częstotliwość zegara:	2.9 GHz
Max Turbo Speed:	4.8 GHz
RAM	
Zainstalowana:	16 GB DDR4 ECC 3200 MHz
Napęd dyskowy	
Typ:	SSD - wymiana podczas pracy - 2.5"
Pojemność:	2 x 480 GB
Typ interfejsu:	SATA 6Gb/s
Cechy:	1 DWPD, Read Intensive
Kontroler pamięci masowej	
Typ:	1 x kontroler sprzętowy, obsługiwane typy RAID 0,1,10
Interfejsy	
Interfejsy sieciowe:	2 x LAN (Gigabit Ethernet) - RJ-45
Akcesoria	
Akcesoria w zestawie:	Szyny do szafy typu RACK
Zasilanie	
Rodzaj urządzenia:	Zasilacz nadmiarowy z funkcją hot-swap
Zasilanie nadmiarowe:	Tak
Certyfikat 80 PLUS:	80 PLUS Platinum
System operacyjny / Oprogramowanie	
Dołączony system operacyjny:	Windows Server Standard 2022
Gwarancja	
Gwarancja producenta:	36 miesięcy w miejscu instalacji

Zał. nr 3 do umowy dostawy
Szczegółowa specyfikacja przedmiotu zamówienia

1.Synology RS822RP+ ,Synology RKS-02

Zapisy przetargowe	
Typ urządzenia	Serwer NAS
Obudowa	Rack 1U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na październik 2023 co najmniej 4 580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Dyski twarde	Możliwość zainstalowania 4 dysków klasy Enterprise
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA.
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 port eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 2.0	Min. 1x 4-liniowe gniazdo x8 gen. 3
Wentylator obudowy	Min. 2 wentylatory (40 × 40 × 20 mm)
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6,

	RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2 048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500* **Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM.*
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji
Wirtualizacja	Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack®

	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy.
Usługa katalogowa	
Bezpieczeństwo	
Obsługiwane przeglądarki	
Oprogramowanie	

	Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	• Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Zasilanie	150W
Gwarancja	3 lata gwarancji z reakcją NBD na wszystkie komponenty serwera, realizowaną w miejscu instalacji urządzenia z możliwością zgłoszenia awarii w dni robocze pomiędzy godziną 7:00 a 20:00. Gwarancja zapewnia min: • Wsparcie dla całej warstwy sprzętowej (wszystkie elementy zainstalowane w urządzeniu głównym posiadają jednolity okres gwarancyjny) • zapewnienie części zamiennych • naprawa na miejscu instalacji Zamawiającego • urządzenie zastępcze o nie gorszych parametrach w sytuacji braku możliwości naprawy na miejscu • pakiet wsparcia serwisowego obejmuje dyski twarde • uszkodzone dyski twarde (HDD, SSD) w przypadku awarii zostają u Zamawiającego • możliwość zgłaszania awarii mailowo oraz telefonicznie • obsługa infolinii w języku polskim lub angielskim firma serwisująca musi posiadać ISO 9001:2015 w zakresie świadczenia usług serwisowych oraz musi być autoryzowanym partnerem serwisowym producenta serwera NAS.

Zał. nr 4 do umowy dostawy
Szczegółowa specyfikacja przedmiotu zamówienia

1. Drukarka Wielofunkcyjna Konica Minolta 227

Specyfikacja kopiarki

Proces kopiowania	Elektrostatyczne kopiowanie laserowe; pośrednie
System tonera	Toner polimeryzowany Simitri® HD
Prędkość druku / kopiowania A4 w czerni	Do 22 kopii/minutę
Prędkość druku / kopiowania A3 w czerni	Do 14 kopii/minutę
Prędkość w dupleksie A4 w czerni	Do 22 kopii/minutę
Czas pierwszej kopii / wydruku w czerni	5,3 s.
Czas nagrzewania (sek.)	Ok. 20 s. Czas przygotowania do pracy może różnić się w zależności od środowiska pracy i stosowania
Rozdzielczość kopiowania (dpi)	600 x 600 dpi
Skala szarości	256 poziomów
Kopiowanie wielokrotne	1 - 9,999
Format oryginału	A5 - A3
Skalowanie	25-400% w odstępach 0,1 %; automatyczny zoom
Funkcje kopiowania	Wstawianie rozdziałów; okładek i stron; kopia próbna (drukowana i ekranowa); druk próbny do regulacji; funkcje grafiki cyfrowej; pamięć ustawień zadań; tryb plakatu; powtarzanie obrazu; nakładanie (opcjonalne); pieczętowanie;

Specyfikacja drukarki

Rozdzielczość drukowania (dpi)	1 800 (odpowiednik) x 600 dpi
Język opisu strony	PCL6 (PCL 5 + XL 3.0); PostScript 3 (CPSI 3016); XPS
Systemy operacyjne	Windows VISTA (32/64)Windows 7 (32/64)Windows 8 (32/64)Windows 8.1 (32/64)Windows Server 2003/2003 R2Windows Server 2008/2008 R2 (32/64)Windows Server 2012/2012 R2 (64)Macintosh OS X 10.xUnix; Linux; Citrix
Czcionki drukarki	80 PCL Latin, 137 PostScript 3 Emulation Latin
Funkcje drukowania	Bezpośredni wydruk plików PCL; PS; TIFF; XPS; PDF (wer. 1.7); szyfrowanych plików PDF i OOXML (DOCX; XLSX; PPTX); Mixmedia i Mixplex; programowanie zadań "Easy Set"; nakładka; znak wodny' ochrona kopii; tryb "carbon copy"

Specyfikacja skanera

Prędkość skanowania w kolorze	Do 45 obrazów/min.
Prędkość skanowania w czerni	Do 45 obrazów/min.
Rozdzielczość skanowania (dpi)	Maks.: 600 x 600 dpi
Tryby skanowania	Skanowanie do e-mail (Scan-to-Me)Skanowanie do SMB (Scan-to-Home)Skanowanie do FTPSkanowanie do skrzynki użytkownikaSkanowanie do USBSkanowanie do HDD1 Skanowanie do DPWSSkanowanie sieciowe TWAIN
Formaty plików	TIFF; PDF; Kompaktowy PDF; JPEG; XPS; Kompaktowy XPS; DOCX; XLSX; przeszukiwalny PDF; PDF/A; linearyzowany PDF
Miejsca docelowe skanowania	2 100 (pojedynczo i grupami); obsługa LDAP
Funkcje skanowania	Komentarze (tekst/godzina/data) dla PDF; do 400 programów prac; Podgląd skanowania w czasie rzeczywistym

Specyfikacja faksu

Standard faksu	G3
Transmisja faksu	Analogowai-FaxKolorowy i-Fax (RFC3949-C)IP-Fax

Rozdzielczość faksu (dpi)	Maks.: 600 x 600 dpi (ultra-fine)
Kompresja faksu	MH, MR, MMR, JBIG
Prędkość modemu (Kbps)	Do 33.6 Kbps
Miejsca docelowe faksowania	2,100 (pojedyńczo + grupami)
Funkcje faksowania	Odpytywanie; przesunięcie czasowe; PC-Faks; odbiór do skrzynki poufnej; Odbiór do e-mail/FTP/SMBB; do 400 programów zadań

Specyfikacja skrzynek użytkownika

Maks. ilość przechowywanych dokumentów	Do 3 000 dokumentów lub 10 000 stron
Rodzaje skrzynek	PublicznyPrywatny (z hasłem lub uwierzytelnieniem)Grupowy (z uwierzytelnieniem)
Rodzaje skrzynek systemowych	Bezpieczny drukDruk szyfrowanych PDFOdbiór faksuOdpytywanie faksu
Funkcjonalność skrzynek użytkownika	Przedruk; kombinacjaPobieranieWysyłanie (e-mail/FTP/SMB i faks)Kopiowanie ze skrzynki do skrzynki

Specyfikacja systemu

Standardowa pamięć systemu (MB)	2048 MB
Opcjonalny dysk twardy (GB)	250 GB
Standardowe interfejsy	10Base-T/100Base-T/1000Base-T Ethernet, USB 2.0
Protokoły sieciowe	TCP/IP (FTP; SMB; SMTP; WebDAV) (IPv4/IPv6)
Rodzaje ramek	Ethernet 802.2; Ethernet 802.3; Ethernet II; Ethernet SNAP
Automatyczny podajnik dokumentów	Do 100 oryginałów; A6-A3; 35-163 g/m² Opcjonalnie dostępne RADF
Gramatura papieru (g/m²)	60-220 g/m²
Pojemność papieru (arkusze)	Standard:1,100 arkuszy, Maksymalnie.: 3,600 arkuszy

Standardowe podajniki papieru	**Taca 1:** 500 arkuszy, A5 - A4, 60 - 220 g/m² **Taca 2:** 500 arkuszy, A5 - A4, 60 - 220 g/m² **Podajnik ręczny:** 100 arkuszy, A6-A3, własne rozmiary; 60 - 220 g/m²
Opcjonalne podajniki papieru	**Taca 3:** 500 arkuszy, A5 - A3, 60 - 220 g/m² **Taca 3 + 4:** 2x 500 arkuszy, A5 - A3, 60 - 220 g/m² **Kaseta o dużej pojemności:** 2,500 arkuszy, A4, 60 - 220 g/m²
Automatyczny dupleks	A5-A3; 60-209 g/m²
Tryby wykańczania (opcja)	Przesunięcie; grupowanie; sortowanie; zszywanie; dziurkowanie; składanie na pół; broszurowanie
Pojemność wyjścia (z finiszerem)	Maksymalnie 3,300 arkuszy
Pojemność wyjścia (bez finiszera)	Maksymalnie 250 arkuszy
Zszywanie	Maks.: 50 arkuszy lub 48 arkuszy + 2 okładki (do 209 g/m²)
Pojemność zszywania	Maksymalnie 1,000 arkuszy
Broszura	Maks.: 20 arkuszy lub 19 arkuszy + 1 okładka (do 209 g/m²)
Pojemność tacy odbiorczej na broszury	Maks.: 100 arkuszy (podajnik); bez ograniczeń
Rekomendowane obciążenie miesięczne (kopie/wydruki)	10000
Maksymalne obciążenie miesięczne (kopie/wydruki)	19 000 Osiągnięcie maksymalnego wolumenu w ciągu roku wymaga przeprowadzenia cyklu konserwacyjnego
Wydajność tonera czarno-białego	23 000 stron
Wydajność sekcji obrazowania czarno-białego	80 000 stron/600 000 stron (Bęben/Wywoływacz)
Pobór energii	220-240 V / 50/60 Hz; Poniżej 1,5 kW (system)
Wymiary systemu (Sz.xGł.xWys., mm)	585 x 660 x 735 mm (Standardowa konfiguracja urządzenia głównego)

Funkcje systemu

Bezpieczeństwo	ISO 15408 EAL3 (w trakcie oceny); filtrowanie IP i blokowanie portów; komunikacja sieciowa SSL2; SSL3 i TSL1.0; obsługa IPsec; obsługa IEEE 802.1x; uwierzytelnianie użytkowników; rejestr uwierzytelniania; bezpieczne drukowanie; nadpisywanie dysku twardego (8 metod); szyfrowanie danych na dysku twardym (AES 246); automatyczne

	usuwanie danych z pamięci; odbiór poufnych faksów; szyfrowanie danych druku użytkownika
Konta użytkowników	Do 1,000 kont użytkowników; Obsługa Active Directory (nazwa użytkownika + hasło + e-mail + folder smb)Definiowanie dostępu do funkcji użytkownikaUwierzytelnianie biometryczne (skaner naczyń krwionośnych w palcu) opcjonalnieUwierzytelnianie kart ID (czytnik kart ID) opcjonalnie
Aplikacje	PageScope Net Care Device ManagerPageScope Data AdministratorPageScope Box OperatorPageScope Direct PrintPrint Status NotifierDriver Packaging UtilityLog Management Utility

- Wszystkie specyfikacje dotyczą papieru o formacie A4 i gramaturze 80 g/m2.
- Obsługa i dostępność wymienionych specyfikacji i opcji może różnić się w zależności od systemów operacyjnych, aplikacji, protokołów sieciowych oraz konfiguracji sieci i systemu.
- Deklarowana trwałość materiałów eksploatacyjnych zależy od warunków eksploatacji takich jak pokrycie strony w danym formacie (5% pokrycia A4). Rzeczywista wydajność użytkowa materiału eksploatacyjnego zmienia się w zależności od sposobu użytkowania oraz pod wpływem takich zmiennych jak pokrycie papieru, format strony, rodzaj nośnika, praca ciągła lub przerywana, temperatura otoczenia i wilgotność.
- Na niektórych ilustracjach widoczne jest wyposażenie dodatkowe.
- Specyfikacja i dane wyposażenia dodatkowego oparte są na informacjach dostępnych w momencie wydruku i mogą zostać zmienione bez uprzedniego powiadomienia.
- Firma Konica Minolta nie gwarantuje bezbłędności podawanych specyfikacji.
- Wszystkie inne nazwy marek i produktów mogą być zastrzeżonymi znakami handlowymi lub znakami handlowymi, które należą do odpowiednich właścicieli, co niniejszym zostaje uznane.

Zał. nr 5 do umowy dostawy

Protokół odbioru ilościowego i jakościowego

Wykonawca:

Zamawiający:
Wojewódzki Inspektorat Farmaceutyczny w
Warszawie 03-707 Warszawa, ul. Floriańska 10

W dniu ..... 2023 roku, przedstawiciele Wykonawca przeprowadził odbiór ilościowy i jakościowy sprzętu dostarczonego na podstawie umowy nr ..... z dnia ..... 2023 roku.

Przedmiot dostawy i odbioru

lp	Nazwa	Nr seryjny

Konfiguracja i wyposażenie dostarczonego sprzętu jest zgodna ze specyfikacją zawartą w/w umowie.
Data podpisania protokołu jest datą rozpoczęcia okresu gwarancyjnego.
Niniejszy protokół sporządzono w dwóch j jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Wykonawca

Zamawiający

Załącznik nr 2 do zapytania ofertowego

FORMULARZ OFERTY

Oferta dla:
Wojewódzki Inspektorat Farmaceutyczny w Warszawie

Nazwa: .....

Siedziba i adres: .....

NIP: .....

Nr tel.:

e-mail: .....

Osoba do kontaktu: .....

<u>Oświadczenia Wykonawcy:</u>

1. Oświadczamy, że zapoznaliśmy się z warunkami zawartymi w zapytaniu ofertowym i przyjmujemy je bez zastrzeżeń.
2. Oświadczamy, że w cenie oferty zostały uwzględnione wszystkie koszty związane z realizacją zamówienia, w tym koszty transportu.
3. Oświadczamy, że zrealizujemy przedmiot zamówienia w terminie 14 dni od dnia złożenia zamówienia.

(miejscowość, data)
(podpis i pieczęć osoby upoważnionej)

Odpowiadając na zapytanie z dnia..... października 2023 r., oferujemy:

Lp.	Zakres przedmiotu zamówienia	Ilość	Cena brutto razem
1.			
2.			
3.			
4.			

Całość zamówienia :

wartość brutto: ..... zł

słownie: .....