(309788)

Opis Przedmiotu Zamówienia

Rozbudowa posiadanego Systemu DDI (DNS, DHCP, IPAM).

Definicje:

System DDI (DNS, DHCP, IPAM)	Posiadany przez Zamawiającego System DNS, DHCP, IPAM wraz z usługą bezpiecznego DNS producenta Infoblox zarządzany centralnie z konsoli Grid Manager.
Grid	Rozproszona architektura Systemu DDI, w której wszystkie serwery DNS są członkami (Grid Members) zarządzanymi i synchronizowanymi z jednego serwera zarządzającego (Grid Master).
Serwer DNS Internal	Licencja na serwer DNS pracujący jako członek Grid.
Serwer Network Insight	Licencja na serwer do posiadanego Systemu DDI umożliwiająca uruchomienie skanowania sieci i wykrywania nowych urządzeń w sieci.
Wdrożenie	Instalacja, konfiguracja i uruchomienie dostarczonego oprogramowania i licencji.
Licencje	Licencje, subskrypcje i klucze producenta niezbędne do uruchomienia i pracy Serwerów DNS Internal oraz Serwera Network Insight jako członków Grid, wraz z prawem do aktualizacji i wsparciem producenta.

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest rozbudowa posiadanego Systemu DDI o dwie licencje na wirtualne serwery DNS Internal oraz jedną licencję na wirtualny serwer Network Insight, zarządzane centralnie z poziomu Grid w ramach posiadanego Systemu DDI wraz z wdrożeniem wszystkich zakupionych licencji.

1.2. Dostarczone licencje i oprogramowanie mają być objęte wsparciem producenta, gwarancją i prawem do aktualizacji **przez 24 miesiące od dnia uruchomienia, poświadczonego w podpisanym protokole odbioru.**

1.3. Zamawiający nie przewiduje w ramach zamówienia dostawy sprzętu. Serwery zostaną uruchomione jako maszyny wirtualne na infrastrukturze wirtualizacyjnej Zamawiającego (VMware).

1.4. Wykonawca zapewni, że dostarczone Licencje umożliwią użytkowanie Serwerów przez cały okres ich ważności bez ponoszenia przez Zamawiającego dodatkowych kosztów nieprzewidzianych w OPZ i Umowie.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2. Elementy zamówienia

Tabela nr 1

L.p.	Element	Ilość	Okres gwarancji/licencji	Szczegółowy opis
1	Licencja na Serwer DNS Internal TE-1516-DDIGD-E*	2 szt.	24 miesiące	Załącznik nr 1 do OPZ
2	Licencja na Serwer Network Insight ND-1606NIGD-E*	1 szt.	24 miesiące	Załącznik nr 2 do OPZ

*** rozbudowa posiadanego Systemu DDI o dwie licencje na wirtualne serwery DNS Internal oraz jedną licencję na wirtualny serwer Network Insight, zarządzane centralnie z poziomu Grid w ramach posiadanego Systemu DDI wraz z wdrożeniem wszystkich zakupionych licencji, gwarancją, wsparciem producenta i prawem do aktualizacji przez okres 24 miesięcy.**

3. Termin realizacji i odbiór

3.1. Termin realizacji zamówienia wynosi **30 dni kalendarzowych od dnia zawarcia Umowy.**

3.2. Odbiór dostawy Licencji i Wdrożenia nastąpi protokołem odbioru podpisanym bez zastrzeżeń przez Zamawiającego, po weryfikacji poprawności aktywacji Licencji w Grid Master, weryfikacji Licencji na stronie producenta oraz wykonaniu testów akceptacyjnych uruchomionego oprogramowania w ramach dostarczonych licencji.

4. Posiadane środowisko i wymagania integracji

4.1. Zamawiający posiada System DDI producenta Infoblox w architekturze Grid, obejmujący w szczególności: 4 Serwery DNS Internal, 2 Serwery DNS External, 2 Serwery Management, 1 Serwer Raportujący oraz usługę bezpiecznego DNS. Wszystkie komponenty pracują jako maszyny wirtualne VMware.

4.2. Dostarczone licencje na wirtualne Serwery DNS Internal muszą:

4.2.1. Pochodzić od producenta posiadanego Systemu (Infoblox),

4.2.2. Pracować jako członkowie (Grid Members) posiadanego Grid, zarządzani z posiadanej konsoli Grid Master, bez konieczności instalowania dodatkowej konsoli lub oprogramowania zarządzającego,

4.2.3. Synchronizować konfigurację, strefy DNS, dane IPAM oraz polityki bezpieczeństwa (w tym RPZ) z Grid Master w sposób automatyczny,

4.2.4. Współpracować z posiadanym Serwerem Raportującym oraz usługą bezpiecznego DNS w tym samym zakresie, co posiadane Serwery DNS Internal,

4.2.5. Być objęte tym samym mechanizmem aktualizacji oprogramowania, co pozostałe komponenty Grid.

4.3. Dostarczona licencja na wirtualny Serwer Network Insight musi:

4.3.1. Pochodzić od producenta posiadanego Systemu (Infoblox),

4.3.2. Pracować jako członek (Grid Members) posiadanego Grid, zarządzany z posiadanej konsoli Grid Master, bez konieczności instalowania dodatkowej konsoli lub oprogramowania zarządzającego.

4.3.3. Być objęte tym samym mechanizmem aktualizacji oprogramowania, co pozostałe komponenty Grid.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4.4. Wykonawca odpowiada za kompatybilność wersji oprogramowania dostarczanych Licencji z wersją oprogramowania pracującą w Grid Zamawiającego.

5. Gwarancja

5.1. W ramach świadczenia gwarancji:

5.1.1. Wykonawca zapewni Zamawiającemu dostęp do aktualizacji, nowych wersji i poprawek producenta dla oprogramowania objętego Umową oraz na zgłoszenie Zamawiającego, zapewni wsparcie przy planowaniu i wykonaniu aktualizacji. Wsparcie obejmuje co najmniej ocenę wpływu aktualizacji na środowisko Zamawiającego, rekomendację sposobu wdrożenia, uzgodnienie okna serwisowego, przygotowanie planu zmiany, przygotowanie planu wycofania, udział w pracach aktualizacyjnych oraz przekazanie informacji podsumowującej wykonane czynności. Wykonawca nie wykonuje zmian w środowisku produkcyjnym bez uprzedniej akceptacji Zamawiającego.

5.1.2. Wsparcie w rozwiązywaniu problemów z dostarczonym oprogramowaniem. Wykonawca zapewnia Zamawiającemu profesjonalne wsparcie techniczne w rozwiązywaniu wszelkich problemów z dostarczonym oprogramowaniem zgodnie z poniższą tabelą SLA:

Tabela nr 2.

Priorytet	Definicja	Czas reakcji	Eskalacja do producenta	Wymagany rezultat	Dokument zamknięcia
P1 – Krytyczny	Całkowity brak możliwości korzystania z Systemu lub kluczowych funkcji, uniemożliwiający prowadzenie podstawowej działalności Zamawiającego	2 godziny robocze	niezwłocznie (max 4 godziny robocze)	usunięcie usterki lub skuteczne obejście	potwierdzenie Zamawiającego + Raport RCA
P2 – Wysoki	Poważne ograniczenie kluczowych funkcji Systemu, powodujące istotny wpływ na działalność operacyjną	4 godziny robocze	w ciągu 8 godzin roboczych	usunięcie usterki lub skuteczne obejście	potwierdzenie Zamawiającego + Raport RCA
P3 – Średni	Częściowe ograniczenie funkcjonalności Systemu, nie powodujące znaczącego wpływu na działalność	24 godzin roboczych	w ciągu 48 godzin roboczych	usunięcie usterki lub skuteczne obejście	potwierdzenie Zamawiającego
P4 – Niski	Drobne usterki, błędy kosmetyczne lub pytania eksploatacyjne nie wpływające istotnie na działanie Systemu	72 godziny robocze	na żądanie Zamawiającego	usunięcie usterki lub udzielenie odpowiedzi	potwierdzenie Zamawiającego

5.1.3. Dodatkowe postanowienia:

5.1.3.1. Czas reakcji liczy się od momentu prawidłowego zgłoszenia incydentu przez Zamawiającego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

5.1.3.2. Wszystkie czasy reakcji oraz rozwiązywania incydentów (SLA) podane w niniejszym OPZ są liczone wyłącznie w godzinach roboczych Zamawiającego, tj. od poniedziałku do piątku w godzinach 8:00–16:00. Poza godzinami roboczymi (w tym w weekendy i dni ustawowo wolne od pracy) zgłoszenia, w tym incydenty o priorytecie P1, są obsługiwane bezpośrednio przez producenta. Wykonawca nie ma obowiązku monitorowania, eskalowania ani reagowania na zgłoszenia poza godzinami roboczymi Zamawiającego.

5.1.3.3. Zamknięcie zgłoszenia może nastąpić wyłącznie za zgodą Zamawiającego.

5.1.3.4. Wykonawca jest zobowiązany do aktywnego prowadzenia zgłoszenia w imieniu Zamawiającego, w tym eskalacji do najwyższego poziomu wsparcia u producenta.
Wykonawca ponosi pełną odpowiedzialność za dotrzymanie parametrów SLA określonych powyżej.

5.1.4. Dostęp do bazy wiedzy producenta jest uprawnieniem wynikającym z aktywnego wsparcia producenta i nie stanowi odrębnego elementu odbioru. Wykonawca jest zobowiązany zapewnić aktywność wsparcia producenta w zakresie umożliwiającym Zamawiającemu korzystanie z dokumentacji, informacji technicznych i materiałów producenta zgodnie z zasadami producenta.

5.2. W ramach realizacji gwarancji, Wykonawca zobowiązany będzie do:

5.2.1. Informowania Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu. Wykonawca jest zobowiązany do niezwłocznego informowania Zamawiającego o zdiagnozowanych przyczynach wystąpienia problemów oraz proponowanych sposobach ich rozwiązania. W przypadku incydentów zakwalifikowanych jako priorytet P1 lub P2 Wykonawca jest zobowiązany do przygotowania i przekazania Zamawiającemu, nie później niż w ciągu 7 dni roboczych od zamknięcia zgłoszenia, szczegółowego Raportu Analizy Przyczyny Incydentu (RCA) lub Raportu Podsumowującego Incydent, zawierającego co najmniej:

5.2.1.1. Opis zdarzenia i jego chronologię.

5.2.1.2. Wpływ incydentu na funkcjonowanie Systemu i procesy Zamawiającego.

5.2.1.3. Zidentyfikowaną przyczynę pierwotną (root cause) lub hipotezę przyczyny.

5.2.1.4. Podjęte działania diagnostyczne i naprawcze.

5.2.1.5. Zastosowane obejście czasowe (workaround).

5.2.1.6. Rekomendowane trwałe rozwiązanie problemu.

5.2.1.7. Informacje o eskalacji zgłoszenia do producenta (w tym numer zgłoszenia).

5.2.1.8. Datę zamknięcia incydentu.

5.2.2. Raport przekazywany jest w formie pisemnej (PDF) w języku polskim. Wykonawca ponosi pełną odpowiedzialność za rzetelność, kompletność i terminowość przygotowania raportu.

5.2.3. W ramach gwarancji Wykonawca jest zobowiązany do wsparcia w zakresie eksploatacji, konfiguracji, bezpieczeństwa i rozwoju Systemu. Wsparcie realizowane jest wyłącznie na podstawie zgłoszeń Zamawiającego rejestrowanych w systemie ticketowym. Na zgłoszenia w ramach doradztwa technicznego mają zastosowanie czasy reakcji i rozwiązywania określone w tabeli SLA dla priorytetów P3 i P4. Rezultatem każdego zgłoszenia jest udokumentowane w systemie zgłoszeniowym wsparcie w postaci konsultacji technicznej, rekomendacji konfiguracyjnej, notatki lub stanowiska technicznego.

5.2.4. W przypadku wystąpienia wad, błędów lub usterek oprogramowania Wykonawca jest zobowiązany do:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

5.2.4.1. Założenia zgłoszenia serwisowego w systemie pomocy technicznej producenta.
5.2.4.2. Przekazania Zamawiającemu numeru zgłoszenia (Ticket ID).
5.2.4.3. Przekazywania Zamawiającemu na bieżąco całej korespondencji, załączników oraz innych dokumentów otrzymanych od producenta.
5.2.4.4. Zamknięcia zgłoszenia serwisowego wyłącznie za zgodą Zamawiającego i po potwierdzeniu przez Zamawiającego, że usterka została skutecznie usunięta.
5.2.5. Wykonawca zapewni wsparcie w zakresie konfiguracji oraz optymalizacji Systemu. Wszystkie zmiany konfiguracyjne, optymalizacyjne oraz inne modyfikacje wprowadzane w środowisku produkcyjnym mogą być realizowane wyłącznie zgodnie z procedurą zarządzania zmianami obowiązującą u Zamawiającego i wymagają:
5.2.5.1. Akceptacji Zamawiającego przed rozpoczęciem prac.
5.2.5.2. Przygotowania i zatwierdzenia Planu Zmiany.
5.2.5.3. Przygotowania Planu Wycofania (rollback).
5.2.5.4. Uzgodnienia okna serwisowego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

6. Testy akceptacyjne

6.1. Testy akceptacyjne mają na celu potwierdzenie poprawności instalacji, konfiguracji i działania rozbudowanego Systemu DDI zgodnie z wymaganiami OPZ. Zakres testów obejmuje Serwery DNS Internal, Serwer Network Insight oraz prace wdrożeniowe. Testy przeprowadzane są przez Wykonawcę w obecności przedstawicieli Zamawiającego, w uzgodnionym terminie, a prace mogące wpływać na działanie środowiska produkcyjnego wykonywane są w oknach serwisowych.

Tabela nr 3.

Numer testu	Nazwa przypadku testowego	Opis testu
Serwery DNS Internal		
T1	Rozwiązywanie nazw lokalnych	Weryfikacja poprawności rozwiązywania nazw DNS dla stref autorytatywnych oraz zasobów wewnętrznych organizacji.
T2	Rozwiązywanie nazw internetowych	Weryfikacja poprawności rozwiązywania nazw DNS dla domen internetowych z wykorzystaniem mechanizmów rekursji.
T3	Filtry kategorii (Category Filter)	Weryfikacja poprawności działania filtrów kategoryzujących treści internetowe oraz blokowania dostępu do wybranych kategorii zgodnie z polityką bezpieczeństwa.
T4	Funkcje raportowania	Weryfikacja poprawności działania funkcji raportowania oraz generowania raportów dotyczących usług DNS.
T5	Konfiguracja usług DNS, IPAM i polityk bezpieczeństwa	Weryfikacja konfiguracji usług DNS, IPAM oraz polityk RPZ pod kątem zgodności z konfiguracją pozostałych serwerów DNS Internal lub wytycznymi Zamawiającego.
T6	Wersja oprogramowania, licencje i członkostwo w Grid	Weryfikacja zgodności wersji oprogramowania z infrastrukturą Grid, aktywacji wymaganych licencji oraz poprawności dołączenia serwerów do Grid jako Grid Members.
T7	Testy przełączania awaryjnego	Weryfikacja ciągłości świadczenia usług DNS w przypadku niedostępności jednego z serwerów DNS Internal.
T8	Wsparcie producenta	Weryfikacja poprawności aktywacji oraz ważności licencji, subskrypcji i uprawnień do wsparcia producenta.
Serwer Network Insight		

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

T9	Wersja oprogramowania, licencje i członkostwo w Grid	Weryfikacja zgodności wersji oprogramowania z infrastrukturą Grid, aktywacji wymaganych licencji oraz poprawności dołączenia serwera do Grid jako Grid Member.
T10	Wykrywanie urządzeń sieciowych	Weryfikacja wykrywania urządzeń sieciowych, w tym routerów, przełączników warstwy 2 i 3 oraz zapór sieciowych (firewall).
T11	Prezentacja danych o urządzeniach	Weryfikacja prezentacji informacji o urządzeniach sieciowych, w szczególności interfejsach, adresach IP, sieciach oraz zasobach podłączonych do portów dostępowych.
T12	Uzupełnianie bazy IPAM o wykryte dane	Weryfikacja automatycznego uzupełniania bazy adresowej IPAM o informacje wykryte podczas procesu skanowania sieci.
T13	Status procesu wykrywania	Weryfikacja prezentacji statusu procesu wykrywania, w tym identyfikacji sieci, dla których proces został zakończony lub jest w trakcie realizacji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Opis wymagań szczegółowych – Licencja na wirtualny Serwer DNS Internal

1. Funkcjonalność:

1.1. Obsługa **minimum 80 000 zapytań DNS na sekundę.**

1.2. Pojemność bazy systemu **DNS/IP na minimum 400 000 rekordów**.

1.3. Serwer musi dostarczać na bieżąco informacje o przyznawaniu adresów IP i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP).

1.4. Serwer musi dostarczać usługę zarządzania adresami IP – IPAM (IP Address Management).

1.5. Serwer musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją.

1.6. Serwer musi pozwalać na integrację z usługami VMware vCenter oraz OpenStack; w celu wykonywania procesu odnajdowania maszyn wirtualnych pracujących na infrastrukturze VMware/OpenStack oraz tworzenia rekordów DNS dla tych maszyn.

1.7. W przypadku kasowania maszyny wirtualnej system musi automatycznie usuwać powiązany rekord DNS.

1.8. Serwer musi posiadać możliwość generowania raportów z historii przydziałów adresów IP i rekordów DNS dla maszyn wirtualnych do wykorzystania w audytach bezpieczeństwa.

1.9. Serwer musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.).

1.10. Serwer musi umożliwiać dodawanie opisów i atrybutów dla obiektów sieci, adresów IP, domen. Atrybuty te muszą umożliwiać definicję typu i rozmiaru danego atrybutu. Musi być możliwość stosowania słowników atrybutów z wymuszeniem lub proponowaniem danego typu atrybutu dla danego typu obiektu. Serwer musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci.

1.11. Serwer musi mieć możliwość rozbudowy o mechanizm skanowania sieci i hostów/adresów IP (ang. network discovery). Mechanizm ten musi działać w trybie na żądanie oraz musi pozwalać na planowane powtarzalne rozpoznawania w przyszłości.

1.12. Serwer musi posiadać mechanizmy typu „znajdź 10 nieużywanych adresów z sieci X" oraz „znajdź 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16". Funkcja musi być dostępna dla IPv4 i IPv6.

1.13. Serwer musi umożliwiać import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych.

1.14. Producent rozwiązania musi udostępniać bezpłatnie narzędzie do importu danych z innych systemów DNS: Bind oraz Microsoft.

1.15. Serwer musi umożliwiać rozbudowę w przyszłości o zarządzanie usługami DNS na wielu serwerach Microsoft Windows bez potrzeby instalowania oprogramowania po stronie serwerów MS Windows. Wymagane jest wsparcie dla:

1.15.1. Microsoft Windows 2012 Standard i DataCenter Initial Release 64 bits.

1.15.2. Microsoft Windows 2016 Standard i DataCenter Initial Release 64 bits.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.15.3. Microsoft Windows 2019 Standard i DataCenter Initial Release 64 bits.
1.15.4. Microsoft Windows 2022 Standard i DataCenter Initial Release 64 bits.
1.16. Serwer musi wspierać integrację co najmniej z systemami bezpieczeństwa SIEM, Cisco ISE, Tenable Security Center, Rapid7, Qualys, FireEye NX, McAfee OpenDXL oraz posiadać otwarty interfejs Rest API do komunikacji z innymi systemami.
1.17. Serwer musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System).
1.18. Serwer musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Comments http://www.ietf.org/rfc.html).
1.19. Serwer musi obsługiwać dynamiczną aktualizację rekordów DNS (Dynamic Update) zgodnie z RFC 2136.
1.20. Serwer musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodny z dokumentem RFC 1996.
1.21. Serwer musi wspierać protokoły DNS w wersji IPv4 i IPv6.
1.22. Serwer musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF).
1.23. Serwer musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS.
1.24. Serwer musi wspierać rozbudowę o usługę DNS dla usług Active Directory.
1.25. Serwer musi wspierać usługę DDNS.
1.26. Serwer musi wspierać bezpieczną aktualizację rekordów DNS tzw. Secure Update, ze wsparciem dla protokołu GSS-TSIG.
1.27. Serwer musi wspierać obsługę MultiMaster DNS.
1.28. Serwer musi obsługiwać mechanizm IDN (Internationalized Domain Names), w tym polskie znaki i posiadać wbudowany konwerter tzw. Punycode.
1.29. Serwer musi mieć funkcjonalność DNS Firewall opartą o polityki bezpieczeństwa realizowane na bazie stref Response Policy Zone (RPZ).
1.30. Serwer musi być przystosowany do obsługi stref RPZ o łącznym rozmiarze nie mniejszym niż 20 mln rekordów.
1.31. Serwer musi posiadać funkcjonalność wykrywania i blokowania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych przez protokół DNS. W tym celu serwer dla nazw FQDN w zapytaniach DNS (w tym dla zapytań o rekordy A) musi co najmniej:
1.31.1. wyliczać entropię znaków.
1.31.2. sprawdzać popularność występowania w językach naturalnych wszystkich 2- i 3-znaków.
1.31.3. obliczać współczynnik liczby samogłosek do wszystkich znaków w nazwie.
1.31.4. obliczać współczynnik liczby cyfr do wszystkich znaków w nazwie.
1.31.5. analizować rozmiar zapytania.
1.31.6. analizować częstotliwość.
2. Zarządzanie i konfiguracja:
2.1. Serwer musi działać pod kontrolą systemu operacyjnego, przeznaczonego

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

do realizacji funkcjonalności określonych w OPZ. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.

2.2. Zarządzanie Systemem musi odbywać się z centralnej konsoli za pomocą jednolitego systemu graficznego.

2.3. Serwer musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian.

2.4. Zarządzanie systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.

2.5. Serwer musi dostarczać mechanizm REST API do kontroli systemu, wykonywania i automatyzacji zadań wykonywanych za pomocą GUI. Musi być dostarczona pełna dokumentacja systemu API z przykładami zastosowania itp.

2.6. Serwer musi pracować jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol).

2.7. Serwer musi posiadać funkcję budowy Systemu rozproszonego, która pozwoli na zbudowanie systemu rozproszonego z synchronizacją danych poprzez sieć IP z centralnym zarządzaniem całym systemem.

2.8. Serwer musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione).

2.9. Serwer musi mieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP).

2.10. Serwer musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów. Granulacja uprawnień powinna umożliwiać konfigurowanie uprawnień dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS.

2.11. Serwer musi wspierać uwierzytelnianie użytkowników poprzez: lokalną bazę użytkowników, protokół RADIUS, protokół TACACS+, SAML, LDAP, Microsoft Active Directory.

2.12. System musi udostępniać konsolę administracyjną poprzez protokół SSH w wersji SSHv2.

2.13. Serwer musi mieć możliwość monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol).

2.14. Dostęp do konsoli administracyjnej urządzeń Systemu powinien być możliwy poprzez:

2.14.1. Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2.

2.14.2. Interfejs znakowy dostępny poprzez port szeregowy, zabezpieczony hasłem dostępu, które jest powiązane z użytkownikiem.

2.15. Serwer musi umożliwiać wykonywanie planowanych kopii bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Opis wymagań szczegółowych – Licencja na wirtualny Serwer Network Insight

1. Architektura:

1.1. Serwer musi mieć możliwość implementacji w środowisku wirtualnym jako tzw. wirtualny serwer (ang. virtual appliance) dostarczony w postaci oprogramowania przygotowanego do uruchomienia na posiadanej przez Zamawiającego własnej platformie dla wirtualizacji VMware.

1.2. Dostarczone Licencje na oprogramowanie muszą umożliwiać przeniesienie ich na maszyny wirtualne na platformy Microsoft Hyper-V, KVM, Nutanix, Proxmox oraz na chmury publiczne Azure, AWS.

1.3. Serwer wykrywania musi być integralną częścią Urządzenia Usług Zarządzania Systemem DDI posiadanym przez Zamawiającego, musi być zarządzany przez ten system oraz uzupełniać bazę adresacji IP z tego systemu o wykryte informacje sieciowe.

2. Funkcjonalność serwera

2.1. Serwer musi realizować dedykowane usługi wykrywania urządzeń sieciowych typu router, switch L2, switch L3, WLAN Access Point, Firewall oraz prezentowania i uzupełniania danych IPAM o informacje odkryte w ramach tych urządzeń sieciowych.

2.2. Serwer musi posiadać możliwość wykrywania i obsługi **minimum 5000 urządzeń sieciowych,** w tym co najmniej Cisco, HP, Palo Alto Networks, F5, Extreme Networks.

2.3. Serwer musi obsłużyć **minimum 145 000 interfejsów**.

2.4. Proces zbierania danych musi uwzględniać takie metody jak: kolekcja danych typu tablice routingu/VLAN/ARP/MAC poprzez SNMP i CLI, skanowanie portów usługowych, dla IPv4 inteligentne skanowanie ICMP/ping i pełne skanowanie ICMP/ping, NetBIOS.

2.5. Dla wspieranych urządzeń sieciowych musi być możliwość prezentacji informacji o: Interfejsach urządzenia, powiązanych adresach IP i sieciach IP, zasobach IP podłączonych do portów dostępowych urządzenia, sieciach VLAN, SSID.

2.6. Serwer wykrywania musi obsługiwać wykrywanie sieci IPv4 oraz IPv6.

2.7. Serwer wykrywania musi umożliwiać dokonanie rezerwacji interfejsu sieciowego, min. dla przełączników sieciowych Cisco.

2.8. Serwer wykrywania musi umożliwiać dokonanie uruchomienia nowej sieci IP łącznie z definicją domyślnej bramy, VLAN - przynajmniej na przełącznikach Cisco.

2.9. Serwer wykrywania musi umożliwiać zdefiniowanie okresów, w trakcie których zabronione jest wykonywanie operacji wykrywania (tzw. blackout).

2.10. Serwer musi umożliwiać definiowanie dla których sieci należy przeprowadzać wykrywanie a dla których sieci taka operacja nie jest wymagana.

2.11. Serwer wykrywania musi wskazywać dla których sieci IP proces wykrywania został zakończony a dla których jeszcze trwa.

2.12. Serwer musi posiadać dostęp do podstawowej konsoli administracyjnej Serwera poprzez interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Opis wymagań szczegółowych - Wdrożenie

1. Wdrożenie obejmuje:

1.1. Przygotowanie specyfikacji maszyn wirtualnych (vCPU, vRAM, dysk, interfejsy sieciowe) oraz wykazu wymaganych połączeń sieciowych (porty, protokoły, strona inicjująca).

1.2. Instalację i konfigurację 2 wirtualnych Serwerów DNS Internal jako virtual appliance na platformie VMware Zamawiającego.

1.3. Instalację i konfigurację wirtualnego Serwera Network Insight jako virtual appliance na platformie VMware Zamawiającego.

1.4. Aktualizację oprogramowania serwerów do wersji zgodnej z Grid.

1.5. Aktywację Licencji i dołączenie serwerów do Grid jako Grid Members.

1.6. Konfigurację usług DNS, IPAM i polityk bezpieczeństwa (w tym RPZ) zgodnie z konfiguracją pozostałych Serwerów DNS Internal lub wytycznymi Zamawiającego.

1.7. Konfigurację usługi skanowania i wykrywania nowych sieci oraz hostów.

1.8. Testy poprawności działania (w tym rozwiązywanie nazw, synchronizacja z Grid, raportowanie, przełączanie awaryjne).

1.9. Aktualizację dokumentacji powykonawczej Systemu DDI posiadanej przez Zamawiającego o zakres rozbudowy, przekazaną najpóźniej w dniu odbioru.

2. Wdrożenie realizowane jest w siedzibie Zamawiającego lub zdalnie, z zachowaniem procedur bezpieczeństwa obowiązujących u Zamawiającego. Prace wpływające na działanie Systemu wykonywane są w uzgodnionych oknach serwisowych.
3. Wdrożenie wykona osoba posiadająca certyfikat producenta oferowanego rozwiązania w zakresie wdrażania lub administrowania Systemem (np. Infoblox Certified Core DDI Professional lub równoważny).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU