Opis przedmiotu zamówienia

Do zapytania ofertowego WEK.1333.1.2022.LPI z dnia 16.08.2022.

Część nr.1

Rozbudowa klastra serwerowego (zakup dwóch procesorów, pamięci ram oraz dodatkowych dysków do macierzy, zakup systemu Microsoft Windows serwer)

Klaster aktualnie składa się z dwóch serwerów Huawei RH2288H V3

Każdy serwer posiada:

procesor: 1x CPU E5-2609 v4 @ 1.70GHz
pamięć ram 32GB (2 x 16GB)

oraz macierzy OceanStore 2600 V3

z dyskami 1.2TB 10K RPM SAS Disk Unit(2.5") model: L2-S-SAS1200

rozbudowa ma polegać na:

- zwiększeniu liczby procesorów do 2szt dla każdego serwera
- zwiększeniu pamięci ram do 96GB dla każdego serwera
- zwiększeniu powierzchni dyskowej macierzy o 1 dysk

wykonawca powinien dostarczyć odpowiednie podzespoły do wskazanego sprzętu wraz z usługa montażu oraz udzielić gwarancji na okres min 24 miesięcy

Dostawa oprogramowania Microsoft lub równoważnego wraz ze wsparciem technicznym przez okres 36 miesięcy, umożliwiającego rozszerzenie funkcjonalności istniejącej platformy witalizacyjnej.

Microsoft Windows Server Standard 16 core - 1szt

Licencje muszą zostać dostarczone w ramach dystrybucji MPSA w oparciu o umowę MBSA nr. 4100013999 zgodnie z definicją https://www.gov.pl/web/cyfryzacja/komunikat-dotyczacy-umowy-z-microsoft

Część nr.2

Zakup oprogramowania (e-usługa) do wysyłania spersonalizowanych powiadomień (E-mail, SMS) dla oprogramowania dziedzinowego księgowość zobowiązań firmy INFO-SYSTEM Roman i Tadeusz Groszek sp.j.

Funkcjonalność

- Predefiniowane szablony komunikatów
- Szablony komunikatów uzupełnianie o zmienne
- Szablony komunikatów w podziale na systemy
- Wymuszenie korzystania z polskich znaków
- Wysyłka do jednej osoby
- Wysyłka hurtowa
- Nadrzędna kontrola i autoryzacja wysyłki SMS-ów
- Przeglądanie wysłanych paczek SMS szczegółowo
- Drukowanie wysłanych paczek SMS szczegółowo
- Przeglądanie wysłanych SMS-wg różnych filtrów
- Możliwość wysyłania pojedynczych powiadomień pocztą e-mail
- Możliwość masowej wysyłki powiadomień pocztą e-mail
- Edycja bazy osobowej
- Statystyki wysłanych paczek
- Wysłane SMS-y
- Wysłane E-Maile
- Korekty numer telefonów

Wydruki i zestawienia

- Statystyki wysłanych paczek
- Wysłane SMS-y
- Wysłane E-Maile

Oprogramowanie musi być w 100% powiązane i kompatybilne z oprogramowaniem które posiada zamawiający firmy INFO-SYSTEM Roman i Tadeusz Groszek sp.j.

- Księgowość Zobowiązań
- Podatki

Wykonawca powinien udzielić gwarancji, wsparcia merytoryczno-technicznego na okres min 12 miesięcy

Część nr.3

Rozbudowa zabezpieczeń logicznych UTM

Dostarczenie oprogramowania maszyna wirtualna typu firewall (wraz ze wsparciem przy wdrożeniu przez zamawiającego) spełniająca następujące funkcjonalności:

1. Musi być dostarczone w formie maszyny wirtualnej z możliwością uruchomienia w środowisku vmware ESXi
2. Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
3. Rozwiązanie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
4. Obsługa dla IPv6.
5. Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
6. Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.
7. Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.
8. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
9. Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
10. Firewall musi działać w następujących trybach:
    a. routera (tzn. w warstwie 3 modelu OSI),
    b. przełącznika (w warstwie 2 modelu OSI),
    c. transparentnym
    d. pasywnego nasłuchu.

Funkcjonując w trybie transparentnym rozwiązanie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.

11. Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
12. Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie

1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

13. Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.
14. Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
15. Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
16. Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.
17. Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
18. Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.
19. Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
20. Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.
21. System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
22. Firewall musi identyfikować co najmniej 3000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.
23. Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
24. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.
25. FW musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Rozwiązanie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.
26. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.
27. Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do

Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).

28. Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN przynajmniej dla platform Windows i Mac
29. Rozwiązanie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
30. Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.
31. FW musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu.
32. Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesję w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
33. Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.
34. Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
35. Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.
36. Rozwiązanie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
37. Firewall musi posiadać przepustowość w ruchu nie mniej niż 3 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 1,5 Gbps.
38. Firewall musi obsłużyć minimum 250 000 jednoczesnych sesji oraz 15 000 nowych połączeń na sekundę.
39. Firewall musi zapewniać wydajność przynajmniej 1 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.
40. Firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.
41. Musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili

ochrony (IPS, AV, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

42. Firewall musi zapewniać zestawienie przynajmniej 100 sesji SSL VPN.
43. Firewall musi posiadać możliwość rozbudowy o funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN.
44. Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
45. Firewall musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
46. Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
47. Rozwiązanie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia na okres 12 miesięcy.
48. Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym firewallem posiadającym taki sam zestaw licencji.
49. FW musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders" raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls" w raportach opublikowanych w przeciągu 2 ostatnich lat.
50. Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
51. Rozwiązanie nie może znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
52. Wsparcie serwisowe, dostęp do najnowszej wersji oprogramowania i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres 12 miesięcy.
53. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.

Warunki serwisu technicznego i procedura zgłoszeń

1. Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.
2. Wsparcie techniczne musi być świadczone przez okres min 12 miesięcy . Wraz z dostarczonym oprogramowaniem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym oprogramowaniem.

Część nr.4

e-Usługi udostepnienia informacji finansowych podatnika z możliwością płatności online

Dostarczony portal oraz aplikacja mobilna powinny być zintegrowane z finansowymi systemami dziedzinowymi Urzędu Miejskiego w Orzyszu firmy INFO-SYSTEM Roman i Tadeusz Groszek sp.j. oraz z Węzłem Krajowej Identyfikacji Elektronicznej

1. Dostęp interesantów do danych z systemów dziedzinowych odbywał się bezpośrednio z dostarczonego portalu i aplikacji mobilnej, był możliwy po potwierdzeniu swojej tożsamości za pomocą Węzła Krajowego Identyfikacji Elektronicznej w dostarczonym portalu i aplikacji mobilnej, bez konieczności zakładania nowego konta użytkownika oraz bez konieczności logowania do systemu trzeciego w celu udostępnienia należności. W przypadku logowania Profilem Zaufanym w ramach Krajowego Węzła Tożsamości system automatycznie przypisuje użytkownikowi jego adres skrytki ESP

2. Dostarczony portal wraz z aplikacją mobilną to system umożliwiający świadczenie e-usług oraz obsługę klientów urzędu, za pomocą którego mogą oni m.in. uzyskać informacje o zobowiązaniach finansowych wobec urzędu oraz dokonać płatności

3. Dostarczona aplikacja była pełnoprawną aplikacją natywną dostarczoną na system Android i iOS. Przygotowanie i przetwarzanie danych odbywa się bezpośrednio w aplikacji. Aplikacja komunikuje się z serwerem w celu zapisu oraz odczytu danych.

Wykonawca powinien udzielić gwarancji, wsparcia merytoryczno-technicznego na okres min 12 miesięcy

Część nr.5

Oprogramowanie do zarządzania infrastrukturą (sprzętem stacjonarnym jak i mobilnym)

ogólna specyfikacja

1. system powinien posiadać graficzny panel web do zarządzania urządzeniami mobilnymi
2. system powinien pracować na otwartej bazie danych w darmowym środowisku linux
3. wykonawca powinien dostarczyć system w postaci gotowej maszyny wirtualnej (vmware) z systemem linux wraz z oprogramowaniem, bądź zaoferować pełne wsparcie zamawiającego przy instalacji na systemie wykonawcy (linux)
4. wykonawca powinien zaoferować pełne wsparcie przy wdrażaniu

licencjonowanie systemu

- min 1 dostęp administratora
- min 15 licencji na urządzenia mobilne
- min 40 licencji na urządzenia z systemem windows

Zarządzanie komputerami z systemem windows

funkcje systemu:

1. posiadanie ewidencji zasobów komputera klienta
2. zarządzanie zasobami klienta
3. zdalne przejęcie pulpitu przez administratora (po wyrażeniu zgody)
4. możliwość podziału sprzętu na grupy

Zarządzanie urządzeniami mobilnymi Android

funkcje systemu:

1. zdalne czyszczenie - przywrócenie systemu do ustawień fabrycznych (np. w przypadku kradzieży, zgubienia)
2. przesyłanie zrzutu ekranu
3. pobieranie logów Agenta
4. wysyłanie powiadomień na ekran urządzenia
5. skan urządzenia w poszukiwaniu plików takich jak zdjęcia czy aplikacje
6. polityki dotyczące m.in. haseł
7. backup kontaktów, połączeń, smsów, rejestru połączeń
8. dodawanie oprogramowania do białych i czarnych list
9. zdalna instalacja programów

10. blokada możliwości instalacji i dezinstalacji aplikacji
11. blokada łączności, transmisji, połączeń, smsów blokada konfiguracji urządzenia
12. zabezpieczenie m.in. przed odinstalowaniem agenta
13. przesyła informacje nt. lokalizacji urządzenia

Przykładowe informacje w aplikacji dla urządzeń mobilnych Android

- szczegóły urządzenia, np. nazwa, model, wersja systemu, model urządzenia, rodzaj procesora, ilość pamięci RAM czy pamięci na karcie SD, karta SIM, nr telefonu, numer IMEI, nr seryjny, ostatnia aktywność
- rodzaj komunikacji uruchomionej na urządzeniu
- graficzne okno z prezentacją aktualnej lokalizacji urządzenia
- lista zainstalowanych aplikacji na urządzeniu
- lista plików znajdujących się na urządzeniu
- lista wykonanych zadań
- raport dotyczący urządzeń mobilnych: według producenta, wersji, aktywności, systemu operacyjnego

Wykonawca powinien udzielić gwarancji, wsparcia merytoryczno-technicznego na okres min 12 miesięcy

Część nr.6

Dyski sieciowe z możliwością uruchomienia wirtualizacji oraz z możliwością pracy w systemie wysokiej dostępności (HA)

- dwa dyski sieciowe z możliwością pracy w systemy wysokiej dostępności (HA)
- obudowy rack z odpowiednimi szynami montażowymi
- wsparcie wdrożeniowe zamawiającego w instalacji i konfiguracji

każdy dysk sieciowy powinien posiadać minimalnie:

- 8 kieszenie na dyski 2,5" lub 3,5" SATA HDD
- możliwość wymiany dysków podczas pracy hot-swap
- obsługa RAID5 + spare
- procesor min 4 rdzenie po min 2 GHz
- 4 GB ram z możliwością rozbudowy
- 2 porty 1GbE RJ-45 z możliwością agregacji i przełączania awaryjnego
- dwa redundantne zasilacze
- funkcja Wake on LAN
- możliwość uruchomienia serwera www + php
- możliwość uruchomienia przynajmniej jednej maszyny wirtualnej w ramach posiadanego środowiska
- każde z urządzeń powinno posiadać na start min 4 dyski (każdy po min 6TB) dedykowane przez producenta urządzenia

Gwarancja 3-letnia na sprzęt, z możliwością rozszerzenia do 5 lat

Wykonawca powinien udzielić wsparcia merytoryczno-technicznego na okres min 12 miesięcy