



Unia Europejska
Europejski Fundusz Społeczny



GMINA MIASTA DĘBICA
39-200 Dębica, ul. Ratuszowa 2

Miasto Dębica

IZP.271.12.2019.MK

Dębica 10-05-2019 r.

Otrzymują Wykonawcy biorący udział w postępowaniu

Zapytania z wyjaśnieniami 2

Dotyczy: postępowania przetargowego na „Dostawa sprzętu komputerowego oraz oprogramowania niezbędnego do realizacji e-Usług wraz z usługą wdrożenia i szkolenia.”

Gmina Miasta Dębica działając w oparciu o art. 38 ust. 1 i 2 Ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (t.j. Dz. U. z 2018 r. poz. 1986 z późn.zm.) informuje, iż od Wykonawców wpłynęły zapytania do SIWZ. Treść zapytań wraz z wyjaśnieniami poniżej.

Pytanie 1:

Wymaganie:

System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, o zalecanej przez producenta mocy obliczeniowej wystarczającej do zabezpieczenia około 200 komputerów w sieci LAN oraz minimum 6 aplikacji webowych zainstalowanych w infrastrukturze Zamawiającego w trybie HA z obsługą loadbalancingu.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które pracuje w trybie HA bez funkcji loadballancinu?

Odpowiedź:

Zamawiający dopuści rozwiązanie bez wbudowanego loadbalancera.

Pytanie 2:

Wymaganie:

Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które pozwala zdefiniować 500 interfejsów wirtualnych IEEE 802.1Q?

Odpowiedź:

Zamawiający dopuści rozwiązanie posiadające min 500 interfejsów vlan

Pytanie 3:

Wymaganie:

Minimalna liczba równoczesnych tuneli IPSec VPN: 1000

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które pozwala na zestawienie 500 równoczesnych tuneli IPSec VPN?

Odpowiedź:

Zamawiający dopuści urządzenie obsługujące min. 500 tuneli IPSec

Pytanie 4:

Wymaganie:

Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie posiada zintegrowanego dysku SSD ale w którym dostarczony zostanie system centralnego logowania i raportowania?

Odpowiedź:

Zamawiający dopuści rozwiązanie w którym dostarczony zostanie system centralnego logowania i raportowania.

Pytanie 5:

Wymaganie:

Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie posiada wiersza poleceń w interfejsie graficznym ale oferuje go za pośrednictwem portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 6:

Wymaganie:

Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, w którym możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis – zostanie spełnione przy zastosowaniu centralnego systemu zarządzania?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 7:

Wymaganie:

System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. – Przy integracji z AD można to zrobić poprzez AD policy

Pytanie:

Czy Zamawiający dopuści rozwiązanie, w którym polityka dla haseł administratorów będzie mogła być realizowana na Windows AD - przy integracji z Windows AD?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 8:

Wymaganie:

Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). – lokalnie może być przechowywanych kilka konfiguracji ale nie jest to automatyczne.

Pytanie:

Automatyczna aktualizacja oprogramowania systemów bezpieczeństwa nie jest dobrą praktyką a w wręcz nie jest zalecana i praktykowana.

Czy Zamawiający dopuści rozwiązanie, w którym proces instalacji oprogramowania nie będzie automatyczny?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie z zachowaniem funkcji informowania o aktualizacjach.

Pytanie 9:

Wymaganie:

Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora (np. zmiana zapomnianego hasła).

Pytanie:

Czy Zamawiający jest w stanie zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 10:

Wymaganie:

System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. – nie ma w Web UI.

Pytanie:

Czy Zamawiający dopuszcza rozwiązanie, w którym funkcja ta jest dostępna za pośrednictwem centralnego systemu zarządzania?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 11:

Wymaganie:

System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych, itp.). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do min. 12 miesięcy w ramach webowego interfejsu graficznego urządzenia.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, w którym nie są gromadzone statystyki dotyczące HDD, kiedy proces logowanie jest realizowany na zewnętrznym systemie centralnego logowania i raportowania?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 12:

Wymaganie:

Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego lub do serwera FTP.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które pozwala zapisywać konfigurację do pliku lokalnego ale nie oferuje zapisu do serwera FTP?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 13:

Wymaganie:

Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: np. codziennie, raz w tygodniu lub raz w miesiącu.

Pytanie:

Czy Zamawiający dopuści rozwiązanie w którym opisana funkcja jest możliwa przy zastosowaniu zewnętrznych skryptów poprzez SSH?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 14:

Wymaganie:

Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie posiada API do integracji z zewnętrznymi systemami ale umożliwia taką integrację z wykorzystaniem uniwersalnego interfejsu SSH?

Wymaganie:

Rozwiązanie powinno zapewniać obsługę:

- IGMP snooping.
- przekierowania ruchu do nadrzędnego serwera proxy (upstream/parent proxy).
- DHCP relay dla IPv6
- 6to4, 4in6.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie obsługuje wypranych, powyższych mechanizmów?

Odpowiedź:

Zamawiający dopuści rozwiązanie nieposiadające funkcji IGMP snooping oraz przekierowania ruchu do nadrzędnego serwera proxy (upstream/parent proxy).

Pytanie 15:

Wymaganie:

Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które pozwala na tworzenie limitów ilości danych bez określania kierunku, takie w którym limity są przyznawane tylko cyklicznie?

Odpowiedź:

Zamawiający wymaga aby system pozwalał określić limit przesyłania danych z określeniem kierunku, dopuści rozwiązanie posiadające jedynie cykliczny mechanizm.

Pytanie 16:

Wymaganie:

Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z wymagania Transparent Proxy Authentication (NTLM/Kerberos)?

Odpowiedź:

Zamawiający wymaga obsługi NTLM/Kerberos bez znaczenia jest natomiast tryb autentykacji.

Pytanie 17:

Wymaganie:

System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS, LDAP i TACACS+.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które zapewnia możliwość autentykacji w oparciu o Active Directory, RADIUS, LDAP ale nie TACACS+?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 18:

Wymaganie:

System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które oferuje możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego tylko dla platform Windows, Mac OS X?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 19:

Wymaganie:

Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które zapewnia możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, bez obsługi PPTP (który nie jest bezpiecznym protokołem) ale takie które obsługuje L2TP?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 20:

Wymaganie:

Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows, Mac OS X, Linux, iOS, Android.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które udostępnia plik z konfiguracją dla klienta SSL VPN tylko dla Windows, Mac OS X, w którym konfigurację dla open vpn można pobrać z GUI?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 21:

Wymaganie:

Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu portalu użytkownika).

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie wspiera protokołu PPTP (który nie jest bezpiecznym protokołem) ?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 22:

Wymaganie:

Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.

Pytanie:

Czy Zamawiający dopuszcza rozwiązanie, które nie ma możliwości lokalnego dodawania własnych sygnatur?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 23:

Wymaganie:

Udostępnianie zasobów w sieci LAN w postaci usług http/HTTPS, RDP, VNC, SSH, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które umożliwia udostępnienie tylko usług http/HTTPS, SSH za pośrednictwem szyfrowanej komunikacji ale umożliwia tunelowanie dowolnej innej aplikacji z wykorzystaniem klienta na stacji?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 24:

Wymaganie:

Rozwiązanie powinno zawierać zdefiniowane przez producenta kategorie stron www i umożliwiać tworzenie własnych kategorie. – lokalne wyjątki dla url

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie umożliwia definiowanie własnych kategorii ale pozwala definiować lokalną listę wyjątków dla url?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 25:

Wymaganie:

Rozwiązanie powinno umożliwiać blokowanie:

- aplikacji, które pozwalają na transfer plików (np. P2P).
- komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.
- proxy uruchamianych poprzez przeglądarki internetowe.
- streaming media (radio internetowe, Youtube, Vimeo). Support->security portal

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie posiada zdefiniowanej aplikacji Vimeo, ale ma możliwość dodania takiej aplikacji poprzez portal producenta?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 26:

Wymaganie:

Rozwiązanie powinno oferować funkcjonalność pozwalającą na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie. Dla url in firewall policy as destination.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie pozwala na kształtowanie pasma w oparciu o kategorię stron oraz nie umożliwia gwarancji pasma osobno w kierunkach upload/download ale spełniające pozostałe funkcje?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 27:

Wymaganie:

Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Mail Transfer Agent.

Pytanie:

Czy Zamawiający dopuści rozwiązanie które pracuje tylko w trybie Transparent Email Proxy?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 28:

Wymaganie:

Rozwiązanie powinno oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora (np. numer PESEL).

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 29:

Wymaganie:

Rozwiązanie powinno umożliwiać archiwizowanie wiadomości email.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 30:

Wymaganie:

Rozwiązanie powinno współpracować z bazami RBL.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 31:

Wymaganie:

Rozwiązanie powinno blokować spam w postaci plików graficznych np. wiadomości z tekstem osadzonym w obrazku.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 32:

Wymaganie:

System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako zainfekowane przez malware.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, w którym funkcja ta jest możliwa z wykorzystaniem zewnętrznego serwera SMTP?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 33:

Wymaganie:

Rozwiązanie powinno zapewniać możliwość przeglądania kwarantanny z opcją wyszukiwania wiadomości i opcjami filtrowania wraz z opcją zwalniania lub usuwania wiadomości z kwarantanny (przez samoobsługowy portal użytkownika).

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które zapewnia możliwość przeglądania kwarantanny ale bez funkcji wyszukiwania i filtrowania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 34:

Wymaganie:

Funkcjonalność oparta o mechanizm Reverse Proxy

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 35:

Wymaganie:

System powinien pozwalać na podpisywanie plików cookies.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie oferuje funkcji podpisywania plików cookies ale umożliwi tworzenie reguł weryfikacji takich plików?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 36:

Wymaganie:

Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 37:

Wymaganie:

System powinien umożliwiać stosowanie operatorów logicznych AND/OR dla reguł.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania?

Odpowiedź:

Zamawiający podtrzymuje zapisy w tym zakresie.

Pytanie 38:

Wymaganie:

System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali zagrożenia.

Pytanie:

Czy Zamawiający jest skłonny zrezygnować z tego wymagania, jeżeli w ramach postępowania dostarczona zostanie funkcja analizy aktywności złośliwego oprogramowania na stacjach z automatycznymi akcjami aby nie dopuścić do kompromitacji stacji?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 39:

Wymaganie:

Rozwiązanie powinno generować raporty w PDF, HTML i XLS. –CSV manual export

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które z wykorzystaniem centralnego systemu logowania i raportowanie pozwala generować raporty w formatach PDF oraz CSV bez obsługi HTML oraz XLS?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 40:

Wymaganie:

Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 2 serwerów syslog.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które pozwala wysyłać logi systemowe do jednego serwera Syslog?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Pytanie 41:

Wymaganie:

Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, które nie posiada funkcji automatycznego pobierania oprogramowania (które umożliwia to w sposób manualny)?

Odpowiedź:

Zamawiający dopuści zaproponowane rozwiązanie.

Wykonawca B

Pytanie 1:

Prosimy o podanie docelowej maksymalnej liczby pracowników biblioteki, którzy będą równocześnie korzystali z systemu bibliotecznego.

Jest ona niezbędna do ustalenia ceny oferty

Odpowiedź:

Liczba pracowników korzystających równocześnie z systemu wynosi 18 osób.

Otrzymują:

- Wykonawcy
- a/a.

ZASTĘPCA BURMISTRZA

mgr inż. arch. Jerzy Sieradzki