



URZĄD MIEJSKI W GDAŃSKU
BIURO ZAMÓWIEŃ PUBLICZNYCH

Gdańsk, dnia 12 sierpnia 2015 r.

WYKONAWCY

dot. przetargu nieograniczonego na „Utrzymanie i rozbudowa infrastruktury sieciowej w Urzędzie Miejskim w Gdańsku” (sygn. post.: BZP-271-043/BI/15/MSK)

ODPOWIEDZI NA PYTANIA WYKONAWCÓW

Działając na podstawie art. 38 ust. 1 ustawy Prawo zamówień publicznych (t.j. Dz.U. z 2013 r., poz. 907 ze zm.) Zamawiający informuje, że wpłynęły pytania dotyczące ww. postępowania, na które Zamawiający udziela następujących odpowiedzi:

Pytanie 1

SIWZ - punkt II, 1 - Dostawa subskrypcji i kontraktów serwisowych na urządzenia i oprogramowanie Zamawiającego oraz wsparcia producenta na wybrane urządzenia sieciowe. Oferent zwraca się z prośbą o przekazanie numerów seryjnych urządzeń Fortinet i Cisco posiadanych przez Zamawiającego. Numery seryjne są niezbędne do sporządzenia prawidłowej wyceny subskrypcji lub wsparcia.

Odpowiedź na pytanie:

Numerы urządzeń sieciowych Fortinet i Cisco:

FG: FGT1KB3910600523; FGT1KB3911600626

FA: FL300D3M13000072

C6509: SMC14430073

C2960S: FOC1436Y21W; FOC1437Z459; FOC1437Z451; FOC1437Z45D; FOC1436Y21E; FOC1437Z44W

C2960X: FOC1837S7N0; FOC1837S7RQ; FOC1837S7NU; FOC1837S7S9; FOC1837S7NZ; FOC1815S6Z0; FOC1815S6T8; FOC1837S7S6; FOC1837S7RL; FOC1837S7S1; FOC1837S7RZ; FOC1837S7SA; FOC1837S7RX; FCW1838B1J4; FOC1837S7RP; FOC1837S7SY; FCW1836A5S4

C3600X: FOC1621X00T; FOC1621X006

Pytanie 2

SIWZ - rozdział 1, punkt II, 2. Asysta techniczna i utrzymanie aktywnej infrastruktury sieciowej Zamawiającego, polegającymi na pełnej obsłudze administracyjnej urządzeń sieciowych przez Wykonawcę. Zamawiający wyspecyfikował dla urządzeń firmy Cisco pakiety serwisowe "SMARTnet". Czy Zamawiający oczekuje świadczenia takiego serwisu bezpośrednio przez firmę Cisco, czy zgłoszenia serwisowe będą kierowane do Wykonawcy? Jeśli do Wykonawcy, to czy Zamawiający dopuszcza realizowanie usługi w oparciu o kontrakty Cisco Partner Support Service?



Odpowiedź na pytanie:

Zgłoszenia będą kierowane do Wykonawcy. Zamawiający nie zna pojęcia ani mechanizmów - na czym polega kontrakt „Cisco Partner Support Service”, ale jeśli spełnia on wszystkie wymagania zawarte w SIWZ, Zamawiający dopuszcza realizowanie usługi w oparciu o niego.

Pytanie 3:

Jakie są godziny pracy określone w Regulaminie Pracy Zamawiającego?

Odpowiedź na pytanie:

Regulaminowe godziny pracy Zamawiającego określone są następująco:

Poniedziałek , Wtorek Czwartek	8:00-16:00
Środa	8:00-17:00
Piątek	8:00-15:00

Pytanie 4:

Jakie systemy zarządzania siecią używane są przez Zamawiającego, czy Zamawiający jest ich właścicielem i czy mają być one używane w dalszym ciągu?

Odpowiedź na pytanie:

Zamawiający informuje, że nie posiada systemów zarządzania siecią, a przedmiotem niniejszego postępowania jest dostawa i wdrożenie systemu zarządzania siecią.

Pytanie 5:

Ile średnio zmian konfiguracyjnych jest obecnie wykonywanych w sieci Zamawiającego?

Odpowiedź na pytanie:

Średnio wykonywanych jest około 10 zmian konfiguracyjnych na dzień.

Pytanie 6:

SIWZ - punkt II, 3.2c - przełącznik 48 portów - Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów i kabli należy je dostarczyć, kable długość min. 1m. Czy w/w wymaganie, nieopisane w przypadku punktu II, 3.1 - przełącznik 24 portowy ma też obowiązywać?

Odpowiedź na pytanie:

Nie, do przełączników 24 portowych Zamawiający wykorzysta posiadane karty i kable.

Pytanie 7:

SIWZ - punkt II, 3.1 oraz 3.2 - Warunki gwarancji.

Czy Zamawiający dopuszcza zastąpienie rocznego kontraktu serwisowego realizowanego przez serwis producenta sprzętu w trybie 8x5xNBD gwarantującego przyjmowanie zgłoszeń przez 8 godzin dziennie w dni powszednie z czasem na naprawę lub wymię uszkodzonego urządzenia do końca następnego dnia roboczego na serwis partnerski producenta o wymaganych parametrach świadczony przez Wykonawcę?

Odpowiedź na pytanie:

Nie, Zamawiający nie dopuszcza takiego rozwiązania, Koncepcją Zamawiającego jest posiadanie kontraktów serwisowych na wypadek gdyby Wykonawca zerwał umowę, lub nie przystąpił do działań serwisowych.

Pytanie 8:

Zapis SIWZ Rozdział 2



Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków

1.2.2 dysponowania osobami zdolnymi do wykonywania zamówienia;

Opis sposobu dokonywania oceny spełniania warunku:

Warunek zostanie spełniony, jeżeli Wykonawca wykaże, że dysponuje osobą lub osobami, które będą wykonywać zamówienie, posiadających wiedzę i doświadczenie w każdym z następujących zakresów:

- a) wdrażania i serwisu infrastruktury sieciowej w podmiocie, o co najmniej 200 hostach sieciowych;
- b) administracji urządzeniami sieciowymi firm: FortiNet i Cisco;
- c) administracji urządzeniami sieciowymi producenta urządzeń dostarczanych w ramach postępowania.

Pytanie: Czy Zamawiający dopuści Wykonawcę który wykaże, iż dysponuje osobą posiadającą wiedzę i doświadczenie w administracji urządzeniami sieciowymi firmy FortiNet oraz dodatkową osobą posiadającą wiedzę i doświadczenie w administracji urządzeniami sieciowymi firmy Cisco, uwzględniając bez zmian pozostałe szczegóły wymogu 1.2.2.

Odpowiedź na pytanie:

Tak, Zamawiający dopuszcza takie spełnienie warunków udziału w postępowaniu.

Pytanie 9:

Zapis SIWZ

3.4.1.5. System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych, jako oddzielne maszyny fizyczne lub wirtualne, w tym (...) 3.4.1.5.3. Wydzielenie serwerów usługowych realizujących funkcje: 3.4.1.5.3.1. serwera RADIUS dla infrastruktury sieciowej 3.4.1.5.3.2. serwera polityk uwierzytelniania i kontroli dostępu 802.1X, 3.4.1.5.3.3. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego 3.4.1.5.3.4. serwera profilowania stacji końcowych

Pytanie: Czy Zamawiający dopuszcza rozwiązanie w którym poszczególne elementy funkcjonalne (np. WWW i profilowania stacji końcowych) znajdują się fizycznie w jednej instalacji systemu kontroli dostępu do sieci? Przy wykorzystaniu serwerów w konfiguracji redundantnej wydzielanie serwerów poszczególnych funkcji nie ma wpływu na wysoką dostępność całego systemu.

Odpowiedź na pytanie:

Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie 10:

Zapis SIWZ

3.4.1.7. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych - co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS

Pytanie: Czy Zamawiający dopuszcza rozwiązanie umożliwiające aktualizację oprogramowania poprzez interfejs CLI?

Odpowiedź na pytanie:

Zamawiający oprócz wymaganych protokołów dopuszcza również, (jako dodatkową funkcjonalność) możliwość aktualizacji oprogramowania przez CLI.

Pytanie 11:

Zapis SIWZ



3.4.1.11. System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym, co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę, co określoną ilość dni.

Pytanie: Przy wykorzystaniu repozytorium użytkowników w Windows Active Directory, o którym wspomina Zamawiający, jest możliwość wymuszenia tych reguł. Czy w związku z tym Zamawiający dopuszcza rozwiązanie, które umożliwia to poprzez integrację z AD/LDAP/RADIUS?

Odpowiedź na pytanie:

Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie 12:

Zapis SIWZ

3.4.2.10. System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)

Pytanie: Zamawiający oczekuje wsparcia dla serwera RADIUS i Windows Active Directory. W związku z tym nie do końca jasny kontekst wymogu obsługi lokalnej bazy użytkowników w systemie pośredniczącym w uwierzytelnianiu. Czy Zamawiający dopuszcza rozwiązanie z możliwością dodawania użytkowników do lokalnej bazy per użytkownik, z opcją zbiorowego importu danych logowania użytkowników poprzez ingerencję w bazę MySQL?

Odpowiedź na pytanie:

Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie 13:

Zapis SIWZ

3.4.2.13.13. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników

Pytanie: Prośba o wyjaśnienie zapisu. Na podstawie jakich przesłanek Zamawiający zamierza segmentować domenę rozgłoszeniową użytkowników na wiele domen rozgłoszeniowych, w których obecność użytkownika w danej domenie zależeć będzie tylko i wyłącznie od hipotetycznego obciążenia już uwierzytelnionymi użytkownikami danego VLAN-u? Z punktu widzenia wydajnościowego dla przełącznika nie ma różnicy czy na przykład w jednym VLAN-ie jest 100 użytkowników, a w drugim 100 użytkowników, czy też jest jeden VLAN w którym funkcjonuje 200 użytkowników. Ponadto jaki jest cel segmentacji, skoro dla użytkowników nie ma znaczenia do którego (losowego) VLAN-u należą, a zatem VLAN-y te będą traktowane przez sieć w ten sam sposób, a zatem jest to tylko niepotrzebne komplikowanie konfiguracji? Co więcej, jest to funkcjonalność raczej przełącznika, gdyż system uwierzytelniania nie ma z zasady informacji o aktualnym obciążeniu VLAN-ów użytkownikami, czy to liczbowo czy to pod kątem zużycia wydajności przełącznika. Czy w związku z tym Zamawiający dopuszcza rozwiązanie bez takiej funkcji?

Odpowiedź na pytanie:

Zamawiający może segmentować domenę bez konkretnych przesłanek, celem segmentacji mogą być odniesienia organizacyjne lub związane z wymogami bezpieczeństwa, reasumując, Zamawiający nie dopuszcza rozwiązania bez opisanej funkcjonalności.

Pytanie 14:

Zapis SIWZ

3.4.2.13.17. możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika



Pytanie: Jest to funkcjonalność przełącznika (suplikant 802.1X), w dodatku występująca u jednego producenta. Czy zatem Zamawiający dopuszcza rozwiązanie bez takiej funkcji, a korzystające z niej na przełączniku?

Odpowiedź na pytanie:

Zamawiający nie dopuszcza rozwiązania bez opisanej funkcjonalności.

Pytanie 15:

Zapis SIWZ

3.4.3.4. System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do: 3.4.3.4.1. logowania się do systemu 3.4.3.4.2. tworzenia pojedynczego konta gościnnego 3.4.3.4.3. tworzenia wielu kont gościnnych 3.4.3.4.4. importowania kont gościnnych z pliku CSV 3.4.3.4.5. wysyłania wiadomości email po utworzeniu konta gościnnego 3.4.3.4.6. wysyłania wiadomości SMS po utworzeniu konta gościnnego 3.4.3.4.7. wyświetlenia hasła konta gościnnego 3.4.3.4.8. wydrukowania danych konta gościnnego 3.4.3.4.9. wyświetlenia danych stworzonych kont gościnnych 3.4.3.4.10. zawieszenia (suspend) i reinicjacji kont gościnnych

Pytanie: Czy Zamawiający dopuszcza rozwiązanie, w którym sponsor ma z góry ustalony zestaw uprawnień? Przy przeszkoleniu personelu ryzyko wykonania nieprawidłowej operacji przez sponsora jest zerowe.

Odpowiedź na pytanie:

Zamawiający dopuszcza rozwiązanie proponowane przez Wykonawcę, z zastrzeżeniem, że zestaw uprawnień sponsora zawiera te wyszczególnione w SIWZ.

Pytanie 16:

Zapis SIWZ

3.4.3.8. System musi umożliwiać automatyczne kasowanie wygaśniętych kont gościnnych: na żądanie i okresowo, co zadaną liczbę dni i o określonej godzinie. System musi umożliwiać wyświetlenie czasu ostatniego kasowania wygaśniętych kont gościnnych i następnego kasowania wygaśniętych kont gościnnych

Pytanie: Prośba do Zamawiającego o wyjaśnienie zasadności wymogu. Czy Zamawiający dopuszcza rozwiązanie, w którym dedykowany użytkownik może usuwać konta na żądanie, nadawać konkretne ramy czasowe ważności kont i domyślny czas ważności konta?

Odpowiedź na pytanie:

Zamawiający realizuje swoje zasady dotyczące bezpieczeństwa dostępu do sieci, a przedmiotem niniejszego postępowania nie jest wyjaśnianie zasadności stosowanych funkcjonalności. Zamawiający dopuszcza rozwiązanie, w którym dedykowany użytkownik może usuwać konta na żądanie, nadawać konkretne ramy czasowe ważności kont i domyślny czas ważności konta, pod warunkiem że funkcjonalność opisana w pkt 3.4.3.8 jest również dostępna.

Pytanie 17:

Zapis SIWZ

3.4.3.16. System musi umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym przedziale w dniach.

Pytanie: Prośba do Zamawiającego o wyjaśnienie zasadności wymogu, że dla kont gościnnych - co do zasady wykorzystywanych co najwyżej parę godzin lub parę dni - jest zasadne wymuszanie zmian hasła. Czy Zamawiający dopuszcza rozwiązanie posiadające możliwość określenia czasu ważności konta?



Odpowiedź na pytanie:

Zamawiający realizuje swoje zasady dotyczące bezpieczeństwa dostępu do sieci, a przedmiotem niniejszego postępowania nie jest wyjaśnianie zasadności stosowanych funkcjonalności. Zamawiający nie dopuszcza proponowanej funkcjonalności.

Pytanie 18:

Zapis SIWZ

3.4.3.17. System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny

Pytanie: Nie jest zasadne kreowanie domyślnego czasu ważności konta z dokładnością do daty, na przykład 20 lipca, gdyż 21 lipca konta nie będą ważne. Prośba o doprecyzowanie wymogu. Czy Zamawiający dopuszcza rozwiązanie, w którym domyślny czas ważności konta podawany jest w dniach?

Odpowiedź na pytanie:

Zamawiający realizuje swoje zasady dotyczące bezpieczeństwa dostępu do sieci, a przedmiotem niniejszego postępowania nie jest wyjaśnianie zasadności stosowanych funkcjonalności. Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie 19:

Zapis SIWZ

3.4.3.19. System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym, co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika

Pytanie: Czy Zamawiający dopuszcza rozwiązanie, w którym wszystkie informacje takie jak nazwa i adres e-mail są dostępne w podglądzie tożsamości systemu końcowego, a nazwa użytkownika gościnnego dla usprawnienia ewidencji urządzeń fizycznych składa się z wybranego prefiksu oraz adresu MAC urządzenia? Taka nazwa użytkownika, wraz z powiązanymi informacjami o tożsamości systemu końcowego i ew. poświadczeniem tożsamości przez e-mail bądź SMS są dostatecznie jednoznacznym kryterium identyfikacji użytkownika gościnnego. Czy w związku z tym Zamawiający dopuszcza rozwiązanie bez określania minimalnej długości nazwy użytkownika?

Odpowiedź na pytanie:

Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie 20:

Zapis SIWZ

3.4.3.21. System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.

Pytanie: Prośba do Zamawiającego o wyjaśnienie kontekstu wymogu. Wymaganie takiego zapisu wydaje się bezzasadne, w większości instalacji wystarczy jeden portal gościnny, a w przypadku instalacji z wieloma portalami gościnnymi system uwierzytelniania poprzez odpowiednie profilowanie systemu końcowego może decydować na tym samym interfejsie (IP/HTTPS/SSL), który portal gościnny powinien zostać użyty. Czy Zamawiający dopuszcza rozwiązanie, w którym system uwierzytelniania dostępu do sieci jest w stanie zagwarantować wiele portali gościnnych bez konieczności mnożenia interfejsów IP, portów HTTPS oraz certyfikatów SSL?

Odpowiedź na pytanie:

Zamawiający realizuje swoje zasady dotyczące bezpieczeństwa dostępu do sieci, a przedmiotem niniejszego postępowania nie jest wyjaśnianie zasadności stosowanych funkcjonalności. Zamawiający nie dopuszcza proponowanego rozwiązania.



Pytanie 21:

Zapis SIWZ

3.4.4.7. System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji: 3.4.4.7.1. reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci 3.4.4.7.2. reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie <http://standards.ieee.org/develop/regauth/oui/oui.txt> 3.4.4.8. System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie. 3.4.4.9. System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

Pytanie: System uwierzytelniania kontrolujący dostęp do sieci jest systemem krytycznym, nie należy do tzw. dobrej praktyki aktualizowanie go automatycznie po pojawieniu się aktualizacji, co może skutkować przerwą obsługą autoryzacji i związanym z tym problemem z dostępem do sieci. Dobra praktyka mówi by aktualizacje wykonywać w określonym czasie, podczas okna serwisowego. Czy zatem Zamawiający dopuszcza rozwiązanie, w którym funkcjonuje uaktualniana baza MAC OUI oraz aktualizowane w nowych wersjach oprogramowania profile urządzeń?

Odpowiedź na pytanie:

Zamawiający nie dopuszcza proponowanego rozwiązania.

Powyższe wyjaśnienia treści specyfikacji istotnych warunków zamówienia są wiążące dla Wykonawców i należy je uwzględnić przy sporządzaniu oferty.

Z poważaniem
Przewodniczący Komisji Przetargowej

Krzysztof Zielonkowski