POLITECHNIKA GDAŃSKA

Kanclerz

Gdańsk, 27.05.2020r.

dot. przetargu nieograniczonego na dostawę wraz z uruchomieniem i wdrożeniem zestawu do transmisji bezprzewodowej wifi na potrzeby Centrum Usług Informatycznych Politechniki Gdańskiej ZP/98/055/D/20

ODPOWIEDŹ NA ZAPYTANIE OD WYKONAWCY ORAZ ZMIANA SIWZ

Na podstawie art. 38 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych Zamawiający (t.j. Dz. U. z 2019 r., poz. 1843z późn. zm.) Politechnika Gdańska udziela odpowiedzi na zapytanie od Wykonawcy dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ) oraz dokonuje zmiany (SIWZ).

Pytanie 1.

Korzystając z prawa jakie daje nam ustawa Prawo Zamówień Publicznych wnosimy o zmianę zapisów SIWZ, które sumarycznie jednoznacznie wskazują na to, że Zamawiający opisuje rozwiązanie, które spełnia tylko jeden producent – Cisco. Mając na uwadze ochronę praw potencjalnych wykonawców informujemy, że na zmiany w zapisach SIWZ będziemy czekać do 27 maja 2020r., rezerwując sobie czas na pogłębioną analizę treści SIWZ i ewentualne odwołanie do Krajowej Izby Odwoławczej.

I. Wymagania minimalne dla punktu dostępowego bezprzewodowej sieci WiFi kampusu PG zwanego dalej AP — szt. 150 w zamówieniu podstawowych plus 150 szt. w opcji

I.1. AP musi zapewniać obsługę poniższych standardów, protokołów, technologii i funkcjonalności przewidzianych dla sieci bezprzewodowych WiFi:

I.1.2. BSS Coloring

I.1.6. obsługa prędkości PHY do 3,47 Gbps (ac)

I.1.7. obsługa prędkości PHY do 5,38 Gbps (ax)

I.5. AP musi zapewniać zgodność z protokołem CAPWAP (RFC 5415), oraz zapewniać zarządzanie przez kontroler WLAN z poniższymi minimalnymi funkcjonalnościami:

I.5.7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN — przełączenie nie może powodować zerwania sesji użytkowników

I.5.8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.edu.pl

I.5.13. obsługa mechanizmów QoS:

I.5.13.2. obsługa TSPEC

I.6. AP musi zapewniać tryb pracy jako kontroler sieci bezprzewodowej o następujących minimalnych funkcjonalnościach:

I.6.9. AP musi zapewniać wykrywanie do 1000 obcych klientów bezprzewodowych oraz do 100 obcych AP

I.6.15. AP musi zapewniać analizę ruchu pozwalającą na:

I.6.15.1. identyfikację, klasyfikację na poziomic aplikacji w warstwie 7 (rozpoznawanie min. 1000 aplikacji)

I.6.16. AP musi zapewniać dwukierunkowe limitowanie transmisji (bidirectional rate-limiting ruchu) dla:

I.6.16.1. każdego klienta bezprzewodowego z osobna, 1.6.16.2. każdego WLAN z osobna,

I.6.16.3. każdego BSSID z osobna

I.6.26. AP musi posiadać zintegrowany moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz) i zapewniać poniższe min. parametry i funkcjonalności:

I.6.26.1. dokładność analizy (kwant próbkowania) max. 200 kHz

I.6.26.3. automatyczne wykrywanie i klasyfikację źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)

I.6.28. AP musi posiadać min. jeden interfejs konsoli RJ45

I.6.29. AP musi posiadać min. jeden port USB 2.0

I.6.30. AP musi posiadać min. 2 GB RAM, I GB Flash

I.6.35. AP musi posiadać diodową sygnalizację stanu urządzenia z możliwością deaktywacji

I.6.39. Punkt dostępowy musi być przygotowany na uruchamianie aplikacji w kontenerach dostępnych bezpośrednio na AP

II. Wymagania minimalne dla kontrolera sieci bezprzewodowej WiFi kampusu PG zwanego dalej kontrolerem - 1 szt.

II.1. Kontroler musi zapewniać centralną kontrolę punktów dostępu bezprzewodowego z pkt. I z obsługą poniższych standardów, protokołów, technologii i funkcjonalności:

II.1.5. Kontroler musi zapewniać zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415)

II.1.6. Kontroler musi zapewniać obsługę do 2000 punktów dostępowych AP z pkt. I

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

II.1.10. Kontroler musi zapewniać wydajność urządzenia dla ruchu tunelowanego o przepustowości 40 Gbps

II.1.11. Kontroler musi zapewniać obsługę 32000 klientów sieci bezprzewodowej

II.1.14. Kontroler musi zapewniać obsługę sieci kratowych z poniższymi funkcjonalnościami:

II.1.14.2. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)

II.1.14.3. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)

II.1.15.11. ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP

II.1.15.12. DHCP prozy

II.1.21. Kontroler musi zapewniać obsługę mechanizmów QoS w tym:

II.1.21.4. Call Admission Control, SIP CAC, Call Snooping

II.1.24. Kontroler musi zapewniać obsługę tagów telemetrycznych

II.1.30. Kontroler musi posiadać dedykowane interfejsy 1GE typu R.145 oraz SFP służące do połączenia dwóch kontrolerów w redundantną parę 1:1 (interfejs RJ45/SFP wykorzystywany zamiennie)

II.1.32. Kontroler musi zapewniać zbieranie i eksport statystyk ruchu sieciowego za pomocą protokołu NetFlow

II.1.33. Kontroler musi zapewniać profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z:

II.1.33.1. HTTP,

II.1.33.2. DHCP

oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak:

II.1.33.3. VLAN,

II.1.33.4. polityka QoS,

II.1.33.5. lista kontroli dostępu,

II.1.33.6. czas trwania sesji

II.1.35. Kontroler musi zapewniać zarządzanie przez min.:

II.1.35.4. NETCONF,

II.1.36. Kontroler musi zapewniać obsługę wbudowanego interpretera języka PYTHON

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

II.1.37. Kontroler musi zapewniać wsparcie API min. dla:

II.1.37.1. NETCONF - RFC4741

II.1.37.2. NETCONF - RFC4742

II.1.37.3. YANG - RFC6020

II.1.38. Kontroler musi posiadać wbudowaną bazę najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem

II.1.42. Kontroler musi być objęty 3 letnią gwarancją producenta w trybie:

II.1.42.2. „zachowaj dysk twardy" - nośniki informacji

III. Wymagania minimalne na system zarządzania siecią przewodową i bezprzewodową kampusu PG zwany dalej systemem - 1 szt.

III.2. System zarządzania musi posiadać następujące minimalne funkcjonalności ogólne:

III.2.3. Musi zapewniać dostęp do konfiguracji wszystkich wymienionych funkcjonalności z pkt. III.1 111.2 111.3 niniejszej specyfikacji z poziomu WebGUI

III.2.7. Musi posiadać narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące np.:

III.2.7.1. oddziały,

III.2.7.2. lokalizacje,

III.2.7.3. budynki

III.2.7.4. inne definiowalne podgrupy

III.2.1 1. Musi posiadać wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X)

III.2.13. Musi zapewniać tworzenie raportów dotyczących:

III.2.13.5. sprzedaży urządzeń

III.2.13.6. luk bezpieczeństwa na urządzeniach sieciowych

III.2.14. Musi zapewniać zbieranie Netflow z urządzeń sieciowych

III.2.15. Musi posiadać narzędzie pozwalające na monitoring wydajności sieci wraz z:

III.2.15.1. zbieraniem informacji o aplikacjach w sieci i parametrach ich działania,

III.2.16. Musi posiadać narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie min.:

III.2.16.3. połączenie się z urządzeniem przez min.:

III.2.16.3.3. http,

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

III.2.16.3.4. https

III.2.17. Musi zapewniać wyświetlanie wykresów korelujących zmiany w konfiguracji ze zdarzeniami na urządzeniu w celu lepszej i szybszej diagnostyki problemów

III.2.18. Musi posiadać narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych w sposób przewodowy oraz bezprzewodowy do infrastruktury; narzędzie powinno pozwalać na m.in.: zbieranie informacji o parametrach podłączenia i umożliwiać administratorowi szybką analizę problemów związanych z podłączeniem urządzenia do infrastruktury

III.2.22. Musi zapewniać wysoką dostępność i pracę w trybie active-standby w przypadku gdy Zamawiający zakupi kolejny system - bez ponoszenia dodatkowych kosztów i zakupu licencji przez Zamawiającego

III.3. System zarządzania musi posiadać min. szczególne funkcjonalności w zakresie zarządzania siecią przewodową:

III.3.1. Musi zarządzać i zbierać statystyki z wykorzystaniem co najmniej SNMP

III.3.2. Musi posiadać narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci, w tym możliwość manualnego oraz automatycznego dodawania urządzeń za pośrednictwem protokołów takich jak:

III.3.2.3. OSPF,

III.3.2.4. BGP

III.4. System zarządzania musi posiadać min. szczególne funkcjonalności w zakresie zarządzania siecią bezprzewodową:

III.4.4. Musi zapewniać monitorowanie informacji takich jak:

III.4.4.4. pochodzących z punktów dostępowych

III.4.7. Musi posiadać wbudowane formularze do tworzenia min.:

III.4.7.1. polityki bezpieczeństwa dla wielu punktów dostępu radiowego,

III.4.7.2. polityki QoS dla wielu punktów dostępu radiowego,

III.4.7.3. własnych

III.4.10. Musi posiadać narzędzie do zbierania ruchu z określonego punktu dostępowego oraz klienta bezprzewodowego do pliku pcap z możliwością określenia filtrów i czasu zbierania ruchu

III.4.12. Musi posiadać narzędzie do wykrywania czy nie autoryzowany punkt dostępowy podłączony jest do naszej infrastruktury przewodowej

III.4.17. Musi posiadać narzędzie do inspekcji poprawności rozmieszczenia punktów dostępowych pod kątem usług głosowych oraz usług lokalizacji

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

III.4.20. Musi zapewniać współpracę z systemami lokalizacji urządzeń radiowych z prezentacją graficzną na mapie (punktów dostępowych, klientów, itp.)

IV.8. Podstawowe min. cechy serwera UA

IV.8.5. Serwer UA musi zapewniać wydzielenie określonych elementów funkcjonalnych, w tym:

IV.8.5.3. Wydzielenie serwerów usługowych realizujących funkcje:

IV.8.5.3.1. serwera RADIUS dla infrastruktury sieciowej

IV.8.5.3.2. serwera polityk uwierzytelniania i kontroli dostępu 802.1X IV.8.5.3.3. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego

IV.8.5.3.4. serwera profilowania stacji końcowych

IV.8.6. Serwer UA musi zapewniać realizację wysokiej dostępności elementów funkcjonalnych, w tym:

IV.8.6.1. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu

IV.8.6.2. zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych

IV.8.7. Serwer UA musi zapewniać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych w tym min. przez:

IV.8.7.1. serwer TFTP,

IV.8.7.2. serwer FTP/SFTP,

IV.8.7.4. udział NFS

IV.8.8. Serwer UA musi zapewniać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).

IV.8.14. Serwer UA musi zapewniać podłączenie i identyfikację urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520

IV.9. Mechanizmy uwierzytelniania 802.1x

IV.9.1. Serwer UA musi zapewniać wsparcie dla następujących protokołów uwierzytelniania i standardów:

IV.9.1.1. RADIUS, zgodnie z dokumentami:

IV.9.1.1.1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)

IV.9.1.1.2. RFC 2139 — RADIUS Accounting

IV.9.1.1.5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support

IV.9.1.1.6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

IV.9.5. Serwer UA musi zapewniać wsparcie dla następujących protokołów uwierzytelniania:

IV.9.5.6. LEAP

IV.9.5.8. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:

IV.9.5.8.4. Serwer UA musi zapewniać konfigurację mechanizmów:

IV.9.5.8.4.1. PEAP Session Resume,

IV.9.5.8.4.2. PEAP Session Timeout

IV.9.5.8.4.3. Fast Reconnect

IV.9.10. Serwer UA musi posiadać lokalną bazę użytkowników:

IV.9.10.2. w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)

IV.9.13. Serwer UA musi zapewniać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:

IV.9.13.5. mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny

IV.9.13.7. mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA.

IV.9.13.13. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników

IV.9.15. Serwer UA musi zapewniać wsparcie dla min. następujących urządzeń sieciowych, jako klientów RADIUS (NAD - Network Access Device):

IV.9.15.2. Kontrolery sieci bezprzewodowej dedykowane do współpracy z Access Point'ami z pkt I - co najmniej w zakresie:

IV.9.15.2.5. Guest Originating URL,

IV.9.15.2.7. MDM

IV.10. Realizacja dostępu gościnnego

IV.10.4. Serwer UA musi zapewniać konfigurację uprawnień sponsora, w tym uprawnienia do:

IV.10.4.4. importowania kont gościnnych z pliku CSV

IV.10.4.5. wysyłania wiadomości e-mail po utworzeniu konta gościnnego

IV.10.4.6. wysyłania wiadomości SMS po utworzeniu konta gościnnego

IV.10.8. Serwer UA musi zapewniać automatyczne kasowanie wygasłych kont gościnnych w tym:

IV.10.8.3. określonej godzinie.

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

IV.10.9. Serwer UA musi zapewniać wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych

IV.10.14. Serwer UA musi zapewniać honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.

IV.10.16. Serwer UA musi zapewniać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługę min 20 urządzeń per konto gościnne.

IV.10.17. Serwer UA musi zapewniać konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach.

IV.10.18. Serwer UA musi zapewniać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny

IV.10.21. Serwer UA musi zapewniać tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.

IV.10.22. Serwer UA musi zapewniać przypisanie do każdego portalu gościnnego niezależnego:

IV.10.22.1. wzorca językowego,

IV.10.22.2. interfejsu IP,

IV.10.22.3. portu HTTPS

IV.10.22.4. certyfikatu SSL dla FQDN

IV.10.25. Serwer UA musi zapewniać wsparcie API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

IV.11. Profilowanie urządzeń

IV.11.3. Serwer UA musi zapewniać profilowanie stacji końcowych poprzez analizę informacji pochodzących z min. następujących źródeł:

IV.11.3.2. DHCP SPAN

IV.11.3.5. DNS

IV.11.4. Serwer UA musi zapewniać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.

IV.11.6. Serwer UA musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:

IV.11.6.1. Stacji roboczych pracujących z systemami:

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

IV.11.6.1.5. Sun,

IV.11.6.2.Urządzeń mobilnych:

IV.11.6.2.3. Blackberry

IV.11.9. Serwer UA musi zapewniać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

IV.12. Analiza stacji końcowej (Posture Assessment)

IV.12.4. Serwer UA musi zapewniać przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP) w tym:

IV.12.4.1.Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji.

IV.12.4.2.Zawartość dokumentu AUP jest konfigurowalna.

IV.12.5. Serwer UA musi zapewniać głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym:

IV.12.5.2.wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)

IV.12.5.3.daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)

IV.12.9. Serwer UA musi zapewniać tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem:

IV.12.9.1.parametrów dostępu do sieci, w tym:

IV.12.9.1.1. lokalizacji stacji końcowej

IV.12.9.1.2. nazwy użytkownika

IV.12.9.1.3. adresu IP stacji

IV.12.9.1.4. metody uwierzytelnienia

IV.12.9.1.5. statusu uwierzytelnienia

IV.12.9.1.6. repozytorium użytkowników użytych dla uwierzytelnienia IV.12.9.1.7. atrybutów RADIUS, w tym:

IV.12.9.1.7.1. Calling-Station-ID

IV.12.9.1.7.2. Framed-IP-Address

IV.12.9.1.7.3. NAS-Identifier

IV.12.9.1.7.4. NAS-IP-Address

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

a

IV.12.9.1.7.5. NAS-Port-Type

IV.12.9.1.7.6. Service-Type

IV.12.9.1.7.7. User-Name

IV.12.9.1.8. parametrów sesji w tym:

IV.12.9.1.8.1. typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)

IV.12.9.1.8.2. architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)

IV.12.9.1.8.3. adresu URL, z którego nastąpiło przekierowanie

IV.14. Raportowanie

IV.14.1. Serwer ua musi zapewniać generowanie m.in. następujących raportów:

IV.14.1.1. raportów dla protokołów AAA:

IV.14.1.1.3. accountingu RADIUS

IV.14.1.2. raportów dozwolonych protokołów:

IV.14.1.2.2. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Topy), w tym:

IV.14.1.2.2.1. uwierzytelnień pomyślnych

IV.14.1.2.2.2. uwierzytelnień nieudanych

IV.14.1.3. raportów dla poszczególnych instancji serwerów systemu, w tym:

IV.14.1.3.3. monitorowania Online Certificate Status Protocol (OCSP)

IV.14.1.3.5. logowania administratorów do systemu

IV.14.1.3.9. zmian haseł przez użytkowników

IV.14.1.4. raportów dla stacji końcowych, w tym:

IV.14.1.4.5. działań podsystemu profilera per adres MAC

IV.14.1.4.6. czasu wymaganego na sprofilowanie stacji per adres MAC

IV.14.1.5. raportów dla błędów, w tym:

IV.14.1.5.1. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił

IV.14.1.5.2. sumarycznych przyczyn nieudanych uwierzytelnień

IV.14.1.5.3. Top „N" uwierzytelnień per rodzaj błędu

IV.14.1.6. raportów dla urządzeń sieciowych:

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

IV.14.1.6.3. niedostępności serwera AAA dla urządzenia sieciowego IV.14.1.6.4. wiadomości logowanych przez urządzenia sieciowe

IV.14.1.6.5. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP

IV.15. Alarmy

IV.15.2. Alarmy muszą być generowane w następujących sytuacjach:

IV.15.2.2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego

IV.15.2.3. status krytycznych procesów będzie niepożądany, w tym status:

IV.15.2.3.1. procesu wewnętrznej bazy danych systemu

IV.15.2.3 .2. serwera aplikacyjnego systemu

IV.15.2.3 .3. bazy danych sesji

IV.15.2.3.4. kolektora i procesora wiadomości log

IV.15.2.3.5. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)

IV.15.2.3.6. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:

IV.15.2.3.6.1. obciążenie systemu (load)

IV.15.2.3.6.2. zajętość pamięci

IV.15.3. Serwer UA musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

IV.15.3.2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:

IV.15.3.2.1. nazwy użytkownika

IV.15.3.2.2. adresu MAC

IV.15.3.2.3. statusu uwierzytelnienia (udana lub nieudana) IV.15.3.2.4. powodu, jeżeli uwierzytelnienie nieudane IV.15.3.2.5. zakresu czasowego, co do dnia, godziny i minuty

IV.15.3.3. wykonanie zdalnego polecenia na urządzeniu sieciowym

IV.15.3.4. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:

IV.15.3.4.1. definicji serwerów AAA IV.15.3.4.2. protokołu RADIUS IV.15.3.4.3. odkrywania urządzeń IV.15.3.4.4. logowania

IV.15.3.4.5. uwierzytelniania Web IV.15.3.4.6. konfiguracji trybu 802.1X

IV.16. Wsparcie dla protokołu IPv6

IV.16.2. Serwer UA musi pozwalać na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacj i IPv6

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl

IV.16.5. Serwer UA musi zapewniać konfigurację serwerów SNMP w oparciu o adresację IPv6

IV.16.6. Serwer UA musi zapewniać wysyłanie SNMP Trap do serwera SNMP IPv6

Odpowiedź nr 1:

Przesłana przez Państwa 10-stronicowa lista (wyciąg z SIWZ) nie może być traktowana jako lista wymagań ograniczająca konkurencję, gdyż zawiera ona głównie odwołania do standardów i funkcjonalności, które zgodnie z aktualną wiedzą Zamawiającego spełnione są również przez innych producentów.
Wychodząc naprzeciw oczekiwaniom oferentów dokonaliśmy zmian w SIWZ usuwając zapisy, które mogłyby utrudnić złożenie oferty zachowując jednak te, które z punktu widzenia Zamawiającego są istotne i związane z realizacją bieżących zadań oraz planowanych projektów badawczych oraz inicjatyw studenckich.

Powyższa odpowiedź i zmiany stają się integralną część SIWZ i są wiążące dla wszystkich Wykonawców.

Załącznik:
1. Zmieniony Załącznik nr 6 do SIWZ – Szczegółowy opis przedmiotu zamówienia
2. Zmieniony Załącznik nr 3 do SIWZ – Formularz rzeczowo - cenowy

Kanclerz
Politechniki Gdańskiej
mgr inż. Mariusz Mańkowski

.....
(podpis kierownika zamawiającego
lub osoby upoważnionej)

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk

tel. +48 58 347 12 15
fax: +48 58 347 14 15
e-mail: kanclerz@pg.edu.pl
www.pg.gda.pl