Warszawa, dnia 3 października 2018 r.

DAG-SZP.262.38.2018

Wszyscy zainteresowani

Dotyczy: postępowania o udzielenie zamówienia publicznego (Nr 34/18/PN) na **dostawę i konfigurację infrastruktury sieciowej zarządzalnej oraz oprogramowania do zarządzania dla Narodowego Centrum Badań i Rozwoju**.

Działając na podstawie art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r., poz. 1579 z późn. zm.), zwanej dalej „ustawą Pzp", Zamawiający uprzejmie informuje, iż dokonuje zmiany w załączniku nr 1 do SIWZ – Szczegółowym opisie przedmiotu zamówienia poprzez nadanie ust. 8 tegoż następującego brzmienia:

8. System kontroli dostępu do sieci LAN oraz WLAN wraz z konfiguracją – 1 szt.

Zastosowanie: System klasy NAC (Network Access Control) do zarządzania elementami infrastruktury sieciowej

Lp.	**Konfiguracja minimalna Zamawiającego**	
1.	Ogólne	Wykonawca zaoferuje rozwiązanie które będzie wchodziło w skład rozwiązań Producenta zwanych jako „Wired and Wireless LAN Access Infrastructure" i będą zakwalifikowane w niezależnym opracowaniu firmy badawczej Gartner jako rozwiązanie Liderów raportach nie starszych niż z lipca 2017
2.	Architektura	System kontroli dostępu powinien być dostępny w postaci maszyny wirtualnej dostępnej na systemy wirtualizacyjne VMware oraz HyperV. Dopuszcza się zaoferowanie systemu na dedykowanej platformie sprzętowej w raz z niezbędnym sprzętem. System kontroli dostępu musi się składać z aplikacji zarządzającej pozwalającej na konfigurację systemu kontroli dostępu do sieci oraz wewnętrznego serwera

		RADIUS, który zapewnia uwierzytelnianie oraz autoryzację dostępu do sieci. Wymaga się, aby pojedynczy system kontroli dostępu był w stanie obsłużyć do min. zewnętrznych 5 systemów RADIUS oraz min. 2500 systemów końcowych. System musi być dostarczony z licencją umożliwiającą uwierzytelnienie 2500 systemów końcowych.
3.	Niezawodność	Wymagane jest zaoferowanie dwóch maszyn virtualnych pracujących w clustrze HighAvailability na potrzeby zapewnienia niezawodności. W przypadku uszkodzenia jednej z maszyn wirtualnych druga musi zapewnić obsługę wymaganej liczby systemów końcowych i gości.
4.	Uwierzytelnianie	System kontroli dostępu musi zapewniać możliwość uwierzytelniania użytkowników (Proxy) do innych systemów uwierzytelniających RADIUS, LDAP/Microsoft Active Directory oraz lokalnej bazy użytkowników. Musi istnieć możliwość wyboru systemu uwierzytelniającego na podstawie: • Typu uwierzytelnienia np. IEEE 802.1x, MAC authentication (PAP, CHAP, MsCHAP, EAP- MD5), dostęp do zarządzania urządzeń itp. • Nazwy użytkownika, MAC adresu lub nazwy Host urządzenia
5.	Autoryzacja	Po przeprowadzeniu uwierzytelnienia musi następować autoryzacja dostępu do sieci. Wybór konkretnej autoryzacji dostępu musi być możliwy na podstawie następujących parametrów: • Typu uwierzytelniania np. IEEE 802.1x, MAC authentication, Management Authentication wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MsCHAP), MAC (MD5) itp. • Grupy użytkowników bazujące na grupach LDAP/Microsoft Active Directory, grupach RADIUS lub grupach nazw użytkowników wpisanych ręcznie. • Systemów końcowych bazujących na nazwie systemu końcowego (Hostname), adresie IP, przynależności

		systemu końcowego do grupy LDAP/Microsoft Active Directory, MAC adresie • Typów urządzeń końcowych np. Android, iOS, Mac, Linux, Windows itp. • Lokalizacji - np. adresy IP przełączników, które przeprowadzają autoryzację wraz z możliwością wskazania konkretnych portów, SSID oraz konkretnych punktów dostępowych w przypadku sieci bezprzewodowej • Czasu - np. codziennie pomiędzy godziną 9:00 a 17:00.
6.	Polityki dostępu	Aplikacja powinna posiadać możliwość tworzenia Profili autoryzacyjnych, które określają biznesową rolę użytkownika w sieci np.: Administrator, Księgowość, Radcy Prawni, Goście, Studenci, Pracownicy itp. Rola taka powinna być powiązana z polityką jaką będziemy chcieli wymusić na urządzeniach klienckich (przełącznikach, sieci bezprzewodowej itp.). Profil autoryzacyjny powinien wskazywać na Politykę, jaka musi zostać wysłana do urządzenia aby zapewnić właściwą autoryzację dostępu systemu końcowego do sieci. Polityka musi zapewniać możliwość wysłania standardowych atrybutów RADIUS w ramach których będzie możliwe ustawienie: sieci VLAN do której użytkownika ma mieć dostęp, listy kontroli dostępu ACL oraz Quality of Service. Ponieważ oprócz przydziału sieci VLAN różne urządzenia mogą wymagać wysłania różnych atrybutów istnieje konieczność zapewnienia możliwości definiowania wysyłanych atrybutów dla każdego urządzenia z osobna. Przykładowo dla większości przełączników przydzielenie systemu końcowego do sieci VLAN wymaga wysłania następujących atrybutów: Tunnel-Type, Tunnel-Medium-Type oraz Tunnel-Private-Group-ID. Ten ostatni atrybut zawiera faktycznie wymagany VLAN ID lub nazwę VLAN. Niektóre urządzenia posiadają własne atrybuty VSA (Vendor Specyfic Attributes). Polityka musi zapewniać możliwość wysyłania atrybutów VSA dla uzyskania odpowiedniej autoryzacji systemu końcowego w sieci. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji CoA (Change of

		Authorization) zgodnie z RFC 3576 oraz RFC 5176. Ze względu na różną implementację powyższych RFC na różnych urządzeniach sieciowych wymaga się, aby istniała możliwość konfiguracji portu oraz formatu MAC adresu wysyłanego do urządzenia sieciowego w przypadku wymuszenia zmiany autoryzacji. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji z wykorzystaniem protokołu SNMP - rozwiązanie stosowane przez niektórych producentów sprzętu sieciowego.
7.	Zarządzanie	System kontroli dostępu musi zapewnić interfejs konfiguracyjny pracujący w architekturze klient/serwer. Preferowane jest rozwiązanie korzystające z przeglądarki www. System kontroli dostępu musi zapewniać bieżącą widzialność dopuszczonych do sieci systemów końcowych. Wymaga się, aby widziane były następujące parametry systemu końcowego i jego stanu: • MAC adres systemu końcowego • Adres IP systemu końcowego • Nazwa komputera - Host Name • Typ systemu końcowego oraz system operacyjny - możliwość wykrywania urządzeń na podstawie zapytań DHCP (DHCP fingerprinting) np. Windows/ Windows 2012, iPhone / Android itp. • Nazwa urządzenia, do którego dołączony jest klient - to może być nazwa kontrolera bezprzewodowego lub nazwa przełącznika sieciowego. • Adres IP urządzenia, do którego dołączony jest klient i które przeprowadza uwierzytelnienie i autoryzację systemu końcowego. • Typ uwierzytelniania systemu końcowego np. MAC authentication, IEEE 802.1x wraz z informacją o wykorzystywanym protokole EAP np. PEAP, EAP-MD5, EAP-TLS itp. System kontroli dostępu musi zapewniać przechowywanie historii dostępu systemu końcowego do sieci.

		System kontroli dostępu musi zapewniać możliwość wymuszenia ponownej autoryzacji wskazanego systemu końcowego z wykorzystaniem wymaganych powyżej funkcjonalności CoA
8.	Dostęp Gościnny	System kontroli dostępu musi posiadać wbudowany moduł dostępu gościnnego i dostarczone z licencją umożliwiającą obsługę 1000 gości dziennie. Moduł ten powinien umożliwiać przydzielanie dostępu do sieci poprzez stronę www tzw. Captive Portal. Captive System dostępu gościnnego powinien zapewniać: • Możliwość logowania do sieci klientów, którzy nie posiadają suplikanta IEEE 802.1x wraz z możliwością zapamiętania tego systemu na wskazany czas tak, aby nie trzeba było za każdym razem ponownie wprowadzać nazwy użytkownika i hasła na stronie www • Konieczność akceptacji regulaminu przed wpuszczeniem systemu końcowego do sieci • Możliwość rejestracji systemu końcowego z wymaganiem wprowadzenia przez użytkownika wymaganych danych np. imię, nazwisko, numer telefonu, adres e-mail i inne pola definiowane przez administratora. • Możliwość wpuszczania systemu końcowego do sieci po rejestracji systemu końcowego oraz wymaganej akceptacji dostępu przez tzw. sponsora, który musi zaakceptować dostęp dla zarejestrowanego gościa.
9.	Network Access Control	System kontroli dostępu musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa. Agent musi być dostępny min. na systemy operacyjne Windows oraz MAC OS. System musi zapewniać współpracę z systemami MDM (Mobile Device Management) w celu sprawdzania zgodności z polityką bezpieczeństwa dla urządzeń mobilnych. System kontroli dostępu powinien posiadać interfejs API pozwalający na prostą integrację systemu kontroli dostępu z systemami 3rd party.

		Wymagana jest funkcjonalność NAC realizująca weryfikację pod kątem bezpieczeństwa dla nie mniej niż 500 stacji końcowych. Kontrola stanu stacji końcowych musi odbywać się przez zestawienie połączenia w oparciu o dedykowanego agenta lub system Microsoft NAP. Musi istnieć możliwość kontroli komputerów z systemem operacyjnym Windows, MacOSX oraz Linux. Wymaga się funkcjonalności sprawdzania stanu aktualizacji i wersji oprogramowania przez repozytorium utrzymywane przez producenta zawierające informacje o aktualnych wersjach baz sygnatur antywirusowych, antyszpiegowskich itp. Wśród testów zgodności z polityką bezpieczeństwa NAC system musi mieć możliwości weryfikacji, czy użytkownik korzysta z przenośnej pamięci USB, czy ma zainstalowane najnowsze poprawki, czy ma zainstalowane oprogramowanie antywirusowe, czy nie ma uruchomionego oprogramowania Peer-to-peer, czy na stacji końcowej nie jest uruchomiona maszyna wirtualna. Agent systemu NAC musi posiadać wbudowany mechanizm automatycznej samo-aktualizacji i wykonywania działań na systemie końcowym w celu dopasowania do wymaganej polityki bezpieczeństwa.
10.	Wsparcie techniczne	Okres wsparcia: zgodnie z przedstawioną ofertą, minimum **3 lata** od daty dostawy w miejscu instalacji. Wsparcie producenta obejmuje: a) zgłaszanie usterek w godzinach 8.00-16.00 b) możliwość aktualizacji oprogramowania c) możliwość rozbudowy oprogramowania

Jednocześnie Zamawiający uprzejmie informuje, iż nie dokonuje zmiany terminów składania i otwarcia ofert.

Ponadto, działając na podstawie art. 38 ust. 1 pkt 1 ustawy Pzp, Zamawiający uprzejmie informuje, że udziela następującej odpowiedzi na pytanie dotyczące treści SIWZ:

Pytanie:

Dotyczy pkt 7 – System zarządzający elementami sieci WLAN i LAN – 1 szt. oraz pkt 8 – System kontroli dostępu do sieci LAN oraz WLAN wraz z konfiguracją – 1 szt.

Opisy wymagań w obu punktach są takie same, prosimy o podanie prawidłowych wymagań dla punktu 8 System kontroli dostępu do sieci LAN oraz WLAN wraz z konfiguracją.

Odpowiedź:

Zamawiający dokonał stosownej zmiany SIWZ, zgodnie z informacją powyżej.

Piotr Zerhau

Dyrektor

Działu Systemów Informatycznych