Opis przedmiotu zamówienia

Urządzenia dostępowe do sieci WiFi (WLAN Access Points) oraz system NAC

Urządzenia dostępowe do sieci WiFi – 10 sztuk

Specyfikacja oczekiwanego sprzętu:

Parametry techniczne		
Lp.	**Parametr**	**Minimalna wartość parametru**
1	**Przeznaczenie**	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
2	**Obudowa**	Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: • Temperatura 0–50°C, • Wilgotność 5–90%. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3	**Moduły radiowe**	Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: • 2.4 GHz 802.11b/g/n, • 5 GHz 802.11a/n/ac/ax, • 2.4/5/6 GHz 802.11a/b/g/n/ac/ax
4	**SSID**	Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5	**Interfejsy sieciowe/zasilanie**	Urządzenie musi być wyposażone w: • dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX, • moduł BLE. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
6	**Tryby przesyłana danych**	Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: • Tunnel, • Bridge, • Mesh.
7	**Priorytety przesyłania danych**	Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
8	**Metody uwierzytelniania**	Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-

		TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
9	**Interfejs radiowy - funkcje**	Interfejs radiowy urządzenia powinien wspierać następujące funkcje: • MIMO – 2x2, • Maksymalna przepustowość dla poszczególnych modułów radiowych: • 574 Mbps; • 1201 Mbps; • 2401 Mbps; • Wymagana moc nadawania: • min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; • min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; • min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; • Wsparcie dla 802.11n 20/40Mhz HT, • Wsparcie dla kanałów 80 i 160MHz, • Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz. • Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
10	**Maksymalna liczba klientów**	Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512
11	**Funkcje dodatkowe**	Funkcje dodatkowe: • OFDMA UL i DL • Spatial Reuse (BSS Coloring) • UL-MU-MIMO • DL-MU-MIMO • Enhanced Target Wake Time (TWT) • Wbudowany analizator widma • Wbudowane mechanizmy WIPS/WIDS
12	**Gwarancja**	Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

SYSTEM KONTROLI I ZARZĄDZANIA DOSTĘPEM DO SIECI (SYSTEM NAC)

Przedmiotem zamówienia jest dostarczenie centralnego systemu kontroli i zarządzania dostępem do sieci LAN/WLAN współpracującego z posiadaną przez Zamawiającego infrastrukturą dostępową.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu NAC były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: Vmware vSphere oraz Microsoft Hyper-V.

Architektura

1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu (skalowanie).
2. Elementy Systemu muszą umożliwiać klastrowanie active-passive.
3. Wszystkie elementy Sytemu powinny być zarządzane centralnie.
4. System i jego wszystkie funkcje muszą w pełni współpracować z urządzeniami Zamawiającego (tj. można na nich wydawać polecenia konfiguracyjne z poziomu systemu kontroli i zarządzania dostępem do sieci):
   - Firewalle Fortigate 400E
   - Kontroler sieci bezprzewodowej Fortigate 400E i zarządzane przez niego urządzenia Access Point

Funkcje Systemu

1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:
   - standardu 802.1X
   - adresu MAC urządzenia
   - formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie.
2. System musi obsługiwać uwierzytelnianie w oparciu o: wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń.
3. System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS.
4. System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci.
5. System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje:
   - adresy MAC przełączników, urządzeń końcowych i dostępowych,
   - adresy IP ww. urządzeń
   - identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe

- stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena. w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów
- informacje o użytkownikach
- nazwa użytkownika do którego przypisany jest urządzenie końcowe
- nazwa zalogowanego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja
- profil/rola jak została przydzielona urządzeniowi końcowemu przez System
- data zarejestrowania urządzenia końcowego w Systemie
- data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia

6. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) opartych o złożone i wielowarunkowe polityki bezpieczeństwa. Powinny one obejmować co najmniej: lokalizacja urządzenia w sieci, przynależność do grupy administracyjnej, parametr opisujący urządzenie lub użytkownika.
7. System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny oraz blokowania.
8. System musi zapewniać możliwość powiadamiania poprzez SYSLOG oraz pocztę elektroniczną o sytuacjach krytycznych np. związanych z próbą nieautoryzowanego dostępu do sieci lub awarii wewnętrznych usług Systemu NAC.
9. System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API.
10. System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji.
11. System musi posiadać bazę minimum 30 kategorii urządzeń końcowych.
12. System musi mieć możliwość klasyfikacji jednorazowej przy wstępnym uwierzytelnianiu/rejestracji bądź klasyfikacji wielokrotnej. Klasyfikacja urządzeń i użytkowników musi bazować na harmonogramie z częstotliwością w przedziale od kilku minut do kilku tygodni.
13. System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa.
14. System musi obsługiwać telefony IP wraz z możliwością podłączenia do nich stacji końcowych (przez wbudowany przełącznik w telefonie) przypisując każdemu z urządzeń dedykowane polityki bezpieczeństwa.
15. System musi podejmować decyzję o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta.
16. Klasyfikacja urządzeń końcowych z użyciem agenta dedykowanego dla komputerów z systemem Windows i MAC OS X musi umożliwiać przeprowadzenie następujących testów:
    a. Sprawdzenie wersji agenta
    b. Sprawdzenie wersji systemu operacyjnego,
    c. Sprawdzenie obecności i stanu oprogramowania antywirusowego (niezainstalowany/zainstalowany, uruchomiona ochrona, zaktualizowany),
    d. test zapory (włączona/wyłączona),
    e. test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),
    f. test usługi Windows Update z opcją automatycznego naprawienia niezgodności
    g. test obecności/niewystępowania pliku o określonej nazwie

h. test obecności procesu (uruchomiony/nieuruchomiony)
i. test rejestru dla systemów Windows (obecność klucza o zdefiniowanej nazwie, typie wartości i wartości, równy bądź różny zadanemu)
j. test stanu usługi (uruchomiona/nieuruchomiona)
k. test obecności aplikacji (sprawdzenie czy aplikacja zdefiniowanej nazwie jest zainstalowana)

17. System musi mieć możliwość przeprowadzania różnych metod testowania w zależności od lokalizacji urządzenia w sieci, przynależności do grupy administracyjnej, parametru opisującego urządzenie lub użytkownika.
18. Podczas oceniania urządzenia końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów w przypadku braku zgodności.
19. System musi mieć możliwość przeniesienia urządzenia do kwarantanny w przypadku braku komunikacji z agentem.
20. Na urządzeniu podlegającym kwarantannie musi zostać wyświetlona informacja o fakcie przeniesienia urządzenia do kwarantanny oraz informacja z wytycznymi o działaniach jakie użytkownik urządzenia musi podjąć w celu usunięcia niezgodności.
21. Administrator musi mieć możliwość określenia poziomu niezgodności z politykami, po którym będzie następowało przeniesienia stacji do kwarantanny.
22. System musi zapewniać integrację z rozwiązaniami bezpieczeństwa (platformy Firewall, systemy SIEM, systemy Antymalware, systemy MDM) na potrzeby oceny stanu urządzeń końcowych oraz określenia ich zgodności z polityką bezpieczeństwa NAC. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect" przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci.
23. System musi zapewniać integrację z platformami typu Firewall/SIEM w ramach której:
    a. w przypadku wykrycia zagrożenia przez system Firewall/SIEM (np. wirus, malware) i przesłania takiej informacji do systemu NAC mogą zostać podjęte następujące akcje automatyczne:
        i. powiadomienie administratora o zdarzeniu.
        ii. oznaczenie urządzenia końcowego jako potencjalnie niebezpiecznego „z ryzykiem".
        iii. zablokowanie dostępu do sieci.
        iv. przeniesienie urządzenia do kwarantanny.
    b. System NAC - po udzieleniu stacji roboczej dostępu do sieci – przekazuje do systemu Firewall kontekst użytkownika, który jest zalogowany na tym urządzeniu.

Profilowanie urządzeń

1. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI
2. System musi posiadać funkcję automatycznego profilowania urządzeń nie posiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci.
3. System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych.
4. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu.
5. System musi rozpoznawać co najmniej następujące rodzaje urządzeń:
    - urządzenia z systemem Android,
    - urządzenia Apple (iPad, iPhone, iPod)
    - drukarki sieciowe,

- telefony IP,
- stacje robocza z systemem Microsoft Windows,
- stacje robocza z systemem MAC OS,
- stacje robocza z systemem Linux.

Logowanie, Raportowanie i Alarmowanie

1. System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
2. System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego.
3. System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie.
4. System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych.
5. System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy.
6. System musi oferować możliwość tworzenia własnych szablonów raportów.
7. System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog.
8. System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora.

Zarządzanie systemem

1. System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową w wersji oferowanej przez producenta przeglądarki lub dedykowaną aplikację.
2. System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników lub zewnętrzne repozytorium użytkowników (LDAP lub Radius).
3. System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania - RBA.
4. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do poszczególnych elementów systemu.
5. System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę koloru tła i czcionek, treści, grafiki.
6. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych.

Zarządzanie dostępem gościnnym

1. System musi umożliwiać przyznawanie dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez wypełnienie formularza w portalu rejestracyjnym.
2. System musi umożliwiać realizację usług BYOD dla urządzeń prywatnych pracowników.
3. Funkcja portalu rejestracyjnego powinna działać bez udziału lub przy minimalnym udziale pracowników IT. System powinien posiadać możliwość delegowania uprawnień do akceptowania kont gości przez pracowników nieposiadających uprawnień administracyjnych w Systemie.
4. Wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego.
5. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych.
6. System musi umożliwiać przyznanie dostępu czasowego dla gości.
7. System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.

Licencje i serwisy

1. W ramach postępowania koniecznym jest dostarczenie 500 licencji umożliwiających uruchomienie wszystkich wyżej wymienionych funkcji z zastosowaniem agenta na stacjach końcowych, z założeniem że są one równocześnie podłączone do sieci lokalnej LAN i sieci bezprzewodowej WLAN.
5. Licencje w ramach rozwiązania powinny być dostarczone w modelu subskrypcyjnym na okres min. 12 m-cy
6. Dostarczone elementy systemu NAC muszą zawierać wszystkie niezbędne komponenty programowe, na których możliwa będzie licencyjna rozbudowa do min. 500 urządzeń równocześnie podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN, z uwzględnieniem instalacji agentowej.
7. Wsparcie: elementy systemu muszą być objęte serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.