Toruń, dn. 04.11.2019

Urząd Miasta Torunia
Biuro Projektów Informatycznych
Ul. Wały gen. Sikorskiego 8
e-mail: bpi@um.torun.pl

--- Wg. rozdzielnika ---

Zapytanie ofertowe poniżej 30 000 Euro
nr BPI/3400/53/2019

postępowanie o udzielenie zamówienia publicznego o wartości nieprzekraczającej 30 000 euro prowadzone jest poza przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, (tekst jednolity Dz.U. z 2017r., poz. 1579) zgodnie z zarządzeniem nr 9 PMT z dnia 09.01.2018 r w sprawie zasad udzielania zamówień publicznych w Urzędzie Miasta Torunia

Biuro Projektów Informatycznych
Urząd Miasta Torunia
87-100 Toruń
ul. Wały gen. Sikorskiego 8

zwraca się z prośbą o przygotowanie oferty na: zakup i wdrożenie systemu zarządzania siecią lokalną wraz z niezbędnymi licencjami i kontrolą dostępu do sieci NAC.

(Treść opisu przedmiotu zamówienia stanowi załącznik nr 2 do Zapytania ofertowego).

1. Proszę podać jako kryterium 1:
   a) ryczałtową cenę **netto i brutto w złotych na zakup i wdrożenie**
   b) ryczałtową cenę **netto i brutto w złotych na szkolenie**
2. Proszę podać jako kryterium 2: **ilość roboczogodzin** (według kryterium) do wykorzystania w ramach powdrożeniowego wsparcia technicznego w ramach całego okresu trwania umowy.
3. Wraz z ofertą Oferent złoży wypełniony formularz oferty – załącznik nr 1.
4. Wraz z ofertą Oferent złoży aktualny pełny odpis z KRS bądź z CEiDG.
5. Termin realizacji: Zamawiający oczekuje realizacji zadania, o którym mowa w pkt A w terminie do 21 dni kalendarzowych od dnia podpisania umowy.
6. Kryterium wyboru ofert: Dla porównania ofert zostaną zastosowane kryteria:
   a) Kryterium 1: Cena (suma 1a i 1b)– 80%
   b) Kryterium 2: ilość roboczogodzin w ramach wsparcia technicznego zgodnie z wartościami podanymi poniżej w opisie kryterium – maksymalnie 20 punktów

   Za korzystniejszą ofertę zostanie uznana oferta, która otrzyma największą liczbę punktów stanowiących sumę punktów za kryterium a) i b).

   Każda oferta może uzyskać za dane kryterium określoną liczbę punktów przy zastosowaniu wzorów:

a) Kryterium 1:

$$\text{cena oferty} = \frac{Cn}{Cb} \times 80 \text{ (znaczenie kryterium tj. 80 \%)}$$

gdzie:
Cn = najniższa oferowana cena spośród złożonych ofert
Cb = cena oferty badanej

b) Kryterium 2:

0 roboczogodzin godzin	0 pkt
10 roboczogodzin godzin	5 pkt
20 roboczogodzin godzin	10 pkt
30 roboczogodzin godzin	15 pkt
40 roboczogodzin godzin	20 pkt

7. Miejsce składania ofert: Ofertę proszę dostarczyć do Biura Projektów Informatycznych UMT ul. Wały gen. Sikorskiego 8 pok. 62, osobiście lub na adres e-mail (np. w formacie PDF): bpi@um.torun.pl
8. Warunki płatności: przelew, **21 dni od dnia dostarczenia faktury**.
9. Termin składania ofert: do **12.11.2019r. do godz. 12:00 (decyduje godzina otrzymania oferty przez Zamawiającego)**
10. Wykonawca, który prowadzi jednoosobową działalność gospodarczą zobowiązany jest dołączyć do oferty oświadczenie czy w swojej jednoosobowej działalności:
    - zatrudnia / nie zatrudnia pracowników
    - zawiera / nie zawiera umowy ze zleceniobiorcami
11. Wymagania i warunki Zamawiającego:
    a) Zamawiający nie dopuszcza składania ofert wariantowych, chyba, że zostało wskazane inaczej.
    b) Zamawiający nie dopuszcza składania ofert częściowych, chyba, że zostało wskazane inaczej.
    c) W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Oferentami w celu uzupełnienia lub doprecyzowania ofert.
    d) Z wyłonionym Wykonawcą zostanie zawarta pisemna umowa zgodnie z procedurami obowiązującymi w UMT. Umowa do podpisania zostanie wysłana do Wykonawcy w formie elektronicznej i papierowej.
    e) Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu sporządzania niniejszego zapytania Ofertowego.
    f) Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny na każdym etapie postępowania do zawarcia umowy.
    g) Ze względu na założenia budżetowe i ograniczenia finansowe, w przypadku, gdy kwoty przedstawione w ofertach na zapytanie będą wyższe od zaplanowanych w budżecie na ww. zadanie Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez negocjacji z Oferentami.

h) Oferent może złożyć wyłącznie jedną ofertę.
i) Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
j) Oferty złożone po terminie nie zostaną rozpatrzone.
k) Oferenci uczestniczą w postępowaniu ofertowym na własne ryzyko i koszt, nie przysługują im żadne roszczenia z tytułu odstąpienia przez Zamawiającego od postępowania ofertowego.
l) Oferenci biorący udział w postępowaniu zostaną poinformowani o wynikach postępowania pisemnie (drogą elektroniczną).
m) Zamawiający zastrzega sobie możliwość wyboru kolejnej wśród najkorzystniejszych ofert, jeżeli oferent, którego oferta zostanie wybrana jako najkorzystniejsza, uchyli się od zawarcia umowy w przedmiocie realizacji niniejszego zamówienia.
n) Oferenci mogą zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego drogą elektroniczną na adres e-mail: bpi@um.torun.pl
o) Ewentualne pytania dotyczące postępowania wraz z odpowiedziami Zamawiającego będą publikowane na BIP Zamawiającego.

12. Niniejsza oferta nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych.
13. Zaproszenie nie jest postępowaniem o udzielenie zamówienia publicznego w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert. Zamawiający zastrzega sobie prawo do rezygnacji z zamówienia bez wyboru którejkolwiek ze złożonych ofert.
14. Zamawiający, w przypadku wpłynięcia jednej oferty, zastrzega sobie prawo do negocjacji warunków zamówienia oraz ceny za jego wykonanie, a także do rezygnacji z zamówienia bez podania przyczyny.

DYREKTOR
Biura Projektów Informatycznych
Mariusz Szefera

Załącznik 1

PRZEDMIOT ZAMÓWIENIA	.....
ZAMAWIAJĄCY	Gmina Miasta Toruń - wydział prowadzący – Biuro Projektów Informatycznych UMT .....
WYKONAWCA **Adres** **Numer telefonu / fax** **Internet http: //** **e-mail**	
Kryterium 1a. CENA OFERTY NETTO / BRUTTO * (z obowiązującym podatkiem VAT) Zakup i wdrożenie	Cyfrowo netto: ..... Cyfrowo brutto: ..... Słownie brutto: .....
Kryterium 1a. CENA OFERTY NETTO / BRUTTO * (z obowiązującym podatkiem VAT) Szkolenie	Cyfrowo netto: ..... Cyfrowo brutto: ..... Słownie brutto: .....
Kryterium 2. Ilość roboczogodzin	.....
Osoba uprawniona do podpisania umowy	.....
Osoba uprawniona do podpisania protokołu odbioru	.....
Adres e-mail służący do zgłaszania reklamacji	.....
Data	

Podpis	

* Jeżeli Wykonawca poinformuje zamawiającego, że wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego i wskaże nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, wskazuje ich wartość bez kwoty podatku.

Przedmiotem zamówienia jest dostarczenie licencji i wdrożenie systemu zarządzania siecią lokalną wraz z kontrolą dostępu do sieci NAC. Zamawiający posiada system zarządzania Extreme XMC z licencją NMS-ADV-10. Należy dostarczyć dodatkowe licencje do posiadanego systemu umożliwiające przyłączanie większej liczby urządzeń lub dostarczyć system równoważny spełniający poniższe wymagania.

Zamawiający dysponuje następującymi urządzeniami sieciowymi, które mają zostać objęte systemem:

1. Przełączniki Alcatel OS6350 - 6 szt.
2. Przełączniki Alcatel OS6450 - 27 szt.
3. Przełączniki Alcatel OS6850 - 6 szt.
4. Przełączniki Alcatel OS6850E - 12 szt.
5. Przełączniki Alcatel OS6860 - 8 szt.
6. Przełączniki Dell S4128 - 2 szt.
7. Przełączniki Dell PC6224 - 2 szt.
8. Przełączniki Dell /inne/ - 4 szt.
9. Przełączniki HP2910al - 4 szt.
10. Firewall Barracuda NGF - 2 szt.
11. Firewall ASA - 4 szt.
12. serwer dhcp (Linux) - 1 szt.

Niektóre z przełączników Alcatel są połączone w stos należy więc przyjąć do licencji 10 adresów IP.

W zakresie ilości klientów końcowych (komputery, drukarki, telefony VoIP, urządzenia mobilne łączące się przez sieć Wi-Fi), zamawiający szacuje liczbę urządzeń na 2500 łącznie.

Wdrożenie systemu obejmuje:

1. Szkolenie co najmniej trzech administratorów zamawiającego, obejmujące swoim programem wszystkie wymienione funkcjonalności i umożliwiające samodzielne zarządzanie całym rozwiązaniem, 24h zajęć teoretycznych i praktycznych, łącznie.
2. W ramach wdrożenia Wykonawca podłączy 2 urządzenia pracujące we wskazanym budynku do systemu, skonfiguruje i wdroży ww. polityki w postaci uzgodnionej z administratorami Zamawiającego. Przewiduje się przygotowanie 5 polityk.
3. Wdrożenie polityk na wskazanych urządzeniach obejmuje także wdrożenie NAC oraz integrację z Active Directory.
4. Zakończeniem wdrożenie będzie przekazanie Zamawiającemu dokumentacji powdrożeniowej zaakceptowane przez administratorów, zawierającej wykaz wykonanych czynności z ich opisem oraz wykaz zastosowanych polityk również z ich opisem i komentarzem, umożliwiającym świadome modyfikacje parametrów w ramach bieżącej eksploatacji i strojenia systemu.
5. Wykonawca udzieli Zamawiającemu w liczbie ..... roboczogodzin powdrożeniowe wsparcie techniczne, wybiegające zakresem poza wsparcie producenta, polegające na dodatkowych konsultacjach, zmianach istniejącej konfiguracji, pomocy w eksploatacji systemu. W ramach wsparcia Zamawiający oczekuje 4h czasu reakcji oraz realizacji w trybie NBD, w godzinach pracy Zamawiającego, tj. $7^{30} - 15^{30}$.

Opis wymagań dla systemu:

1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera
   a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego VMware
   b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.
2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową.
3. Aplikacja zarządzająca musi obsługiwać minimum 10 urządzeń (adresów IP).
4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników.
5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego.
6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników.
7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES.
10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów.
12. Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB.
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów.
14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II.
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych.
16. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
17. Aplikacja musi posiadać wbudowany Syslog serwer
18. Aplikacja musi posiadać wbudowany BootP serwer.
19. Aplikacja musi wspierać protokół IPv4 oraz IPv6.
20. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.

21. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora.
22. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem:
    a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości,
    b. stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów,
    c. konfiguracji sieci VLAN,
    d. konfiguracji protokołu routingu OSPF.
24. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https.
25. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia,
    b. adresu MAC urządzenia,
    c. nazwy urządzenia,
    d. wersji oprogramowania,
    e. wersji bootrom,
    f. lokalizacji urządzenia,
    g. danych kontaktowych administratora,
    h. numeru seryjnego.
26. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie,
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia,
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych,
    d. możliwość obsługi urządzeń sieciowych różnych producentów (w szczególności wyżej wymienionych).
27. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie.
28. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach.
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp.
31. Tworzona polityka musi zawierać możliwość:
    a. blokowania lub zezwalania ruchu na podstawie:

i) źródłowy i docelowy adres MAC,
ii) źródłowy i docelowy adres IP,
iii) źródłowy i docelowy adres IP podsieci,
iv) źródłowy i docelowy port TCP/UDP,
v) źródłowy i docelowy zakres portów TCP/UDP,
vi) typ protokołu,
vii) pole IP TOS,

b. przydziału parametrów QoS:
i) priorytety,
ii) ograniczenia przepustowości,

c. przydziału użytkownika do wskazanej sieci VLAN,
d. przekierowania ruchu do zewnętrznego systemu analizującego pakiety.

32. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia.
33. Aplikacja musi pozwalać na łatwą modyfikację i ponowne wdrożenie na wszystkich urządzeniach przewodowych i bezprzewodowych.
34. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
d. generowanie raportów.

35. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową:
a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa),
b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac,
c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
i) adres IP kontrolera,
ii) liczba obsługiwanych klientów,
iii) szczytowe wartości zajmowanego pasma,
iv) wersja oprogramowania,
d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:

i) adres IP punktu dostępowego,
ii) MAC adres punktu dostępowego,
iii) wersja oprogramowania,
iv) typ punktu dostępowego,
v) kanały pracy poszczególnych interfejsów radiowych,
vi) szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych,

e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
i) adres IP klienta,
ii) MAC adres klienta,
iii) nazwa użytkownika,
iv) nazwa punktu dostępowego, do którego dołączony jest użytkownik,
v) BSSID, do którego dołączony jest użytkownik,
vi) SSID, do którego dołączony jest użytkownik,

f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
i) zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate),
ii) zaznaczenie kanałów pracy urządzeń,
iii) lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych.

36. Aplikacja zarządzająca musi być zintegrowana z systemem zapewniającym widoczność zautoryzowanych klientów w sieci z zapewnieniem widzialności następujących informacji:
a. adresu MAC,
b. adresu IP,
c. nazwy komputera,
d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.,
e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika,
f. adres IP urządzenia, do którego dołączony jest klient,
g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego,
h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.,
i. nazwa przydzielonej polityki bezpieczeństwa.

37. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.

38. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa.
39. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List.
40. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
41. System zapewniający widoczność zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.,
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.,
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android,
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa,
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
42. System musi umożliwiać ocenę stanu zabezpieczeń systemu końcowego (dla min. 2500 systemów końcowych). Ocenianie musi być możliwe zarówno bez dedykowanego agenta instalowanego na stacji końcowej jak i z użyciem agenta.
43. Ocenianie w oparciu o agenta dostępnego dla co najmniej komputerów z systemem Windows (7, 8, 8.1, 10, Server 2008, Server 2012) i MAC OS X musi umożliwiać następujące testy:
    a. minimalna wersja agenta,
    b. test wersji systemu operacyjnego,
    c. test antywirusa (niezainstalowany/zainstalowany, uruchomiony, zaktualizowany, uruchomione RTP),
    d. test zapory (uruchomiona/wyłączona) z możliwością automatycznego naprawienia niezgodności,
    e. test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),
    f. test usługi Auto Update z opcją automatycznego naprawienia niezgodności,
    g. test czasu od ostatniej aktualizacji systemu,
    h. test wygaszacza ekranu (włączony, zabezpieczony hasłem, z określonym czasem aktywacji,
    i. test obecności/niewystępowania pliku o określonej nazwie i sumie kontrolnej,
    j. test wymagający braku występowania albo braku uruchomienia oprogramowania P2P z możliwością automatycznego naprawienia niezgodności,
    k. test procesu (uruchomiony/nieuruchomiony) z opcją automatycznego naprawienia niezgodności,
    l. test rejestru dla systemów Windows (obecność klucza/zbioru kluczy o konkretnej nazwie, typie wartości i wartości, równy bądź różny zadanemu),
    m. test usługi (niezainstalowana/zainstalowana/uruchomiona),

n. test aplikacji (sprawdzenie obecności zainstalowanej aplikacji o konkretnej nazwie).

44. Musi być możliwość dowolnego dobierania testów ww. rodzajów tworząc schematy oceniania, które będą aplikowane dla wszystkich grup urządzeń i użytkowników bądź dla wybranej grupy urządzeń i użytkowników.
45. Podczas oceniania systemu końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów.
46. Musi być możliwość określenia oceniania jednorazowego przy wstępnym uwierzytelnianiu bądź oceniania wielokrotnego, o częstotliwości oceniania danej grupy urządzeń i użytkowników w zakresie od minut do tygodni.
47. Musi być możliwość przeniesienia systemu końcowego do kwarantanny w razie braku połączenia agenta z serwerem systemu kontroli dostępu do sieci.
48. System końcowy podlegający kwarantannie musi otrzymać informację o testach zakończonych niepowodzeniem wraz ze wskazówkami ich poprawienia.
49. Administrator musi mieć możliwość określenia punktacji oraz progu kwarantanny każdego testu wraz z jego charakterem (informacyjny, ostrzeżenie, wymagany do spełnienia).
50. Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z opcjami reagowania, rejestrowania i audytowania.
51. System ma zapewniać widoczność zautoryzowanych klientów. Jeśli jest licencjonowany na liczbę użytkowników, musi zapewniać obsługę min. 2500 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 100 punktów dostępowych oraz min. 10 przełączników sieciowych. System musi umożliwiać w przyszłości rozbudowę do minimum 250 urządzeń sieciowych. System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7.
52. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.
53. System zarządzania musi być objęty rocznym wsparciem serwisowym producenta obejmujące między innymi dokonywania aktualizacji, rozwiązywania zgłoszonych problemów, usuwania błędów. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.